HP Operations Smart Plug-in for IBM WebSphere Application Server

For HP Operations Manager for Windows®

Software Version: 7.00

PDF version of the online help

This document is a PDF version of the online help that is available in the IBM WebSphere Application Server SPI. It is provided to allow you to print the help, should you want to do so. Note that some interactive topics are not included because they will not print properly, and that this document does not contain hyperlinks.

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

AMD is a trademark of Advanced Micro Devices, Inc.

Intel®, Itanium®, and Pentium® are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

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

Windows Vista™ is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

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

TABLE OF CONTENTS

HP Operations Smart Plug-in for WebSphere Application Server

The HP Operations Smart Plug-in for WebSphere Application Server (WebSphere SPI) allows you to manage WebSphere servers from an HPOM console.

To install and configure the HP Operations Smart Plug-in for WebSphere Application Server (WebSphere SPI), refer to the *HP Operations Smart Plug-in for WebSphere Application Server Installation and Configuration Guide* located on HP Operations Smart Plug-ins DVD in the file `\Documentation\SPI Guides\WebSphere_AppServer_Install_Config.pdf` .

Related Topics:

- Overview
- Getting Started
- Components

Overview

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) adds monitoring capabilities otherwise unavailable to HP Operations Manager for Windows (HPOM).

Smart Plug-in integration uses : Used in conjunction with HPOM, the WebSphere SPI offers centralized tools that help you monitor and manage systems using WebSphere. From the HPOM console, you can monitor the availability, use, and performance of WebSphere running on HPOM managed nodes. The WebSphere SPI metrics are automatically sent to the HPOM agent and can be alarmed on or consolidated into reports and graphs which help you analyze trends in server usage, availability, and performance. The WebSphere SPI can be integrated with HP Reporter and HP Performance Manager (both products must be purchased separately) to provide additional reporting and graphing flexibility and capabilities.

Smart Plug-in data collection: After completing the WebSphere SPI installation and configuration, you will find key server-related metrics that cover the following areas:

- server availability

- server performance

- memory usage

- transaction rates

- servlet executing times, time-outs, request rates

- JDBC connection status

- Web application processing

Smart Plug-in data interpretation: WebSphere administrators can choose those metrics most crucial to the successful operation of WebSphere by modifying WebSphere SPI policies. These policies contain settings that allow incoming data to be measured against predefined rules that generate useful information in the form of messages. These messages with severity-level color-coding can be reviewed for problem analysis and resolution. Corrective actions are often available under the Instructions tab, as are automatically generated metric reports, under the Annotations tab, when you double-click on a message.

Related Topics:

- Introduction

- Getting Started

- Components

Getting started

Smart Plug-in for WebSphere Application Server (WebSphere SPI) messaging, reporting, and action-executing capabilities are based on the HPOM concept of policies . The settings within these policies define various conditions within the WebSphere. After the WebSphere SPI policies are in use, they allow information to be sent back to the HPOM management server to help you proactively address potential or existing problems and avoid serious disruptions to Web transaction processing. WebSphere SPI helps you perform the following functions:

- **Collect and interpret server performance/availability information**

  WebSphere SPI, after you configure and deploy it on the managed nodes, gathers data that is interpreted and acted on, according to settings within the deployed policies. Those WebSphere SPI policies define conditions that can occur within WebSphere, such as queue throughput rates, cache use percentages, timeout rates, and average transaction times. Default thresholds, set within the policies, monitor these conditions and trigger messages to the console when a threshold has been exceeded.

- **Display information**

  Messages in the Message Browser: Comparing the values gathered for WebSphere performance/availability against the policy settings relating to those specific areas, HP Operations agent software forwards the appropriate messages to the HPOM console. These messages are displayed with color-coded severity levels in the HPOM Message Browser.

  Instruction Text: Messages generated by WebSphere SPI programs contain instruction text to help diagnose and remedy problems. Double-click the message and select the Instructions tab to view the text.

  You can usually find instruction text in the message details; this same text is also available in the metric definition .

  ASCII-Text Reports: In addition to the instruction text mentioned above, metrics with alarms also have automatic action reports that are generated when a defined threshold is exceeded. These reports show conditions of specific WebSphere instance. When a report is available, double-click the message and select the Annotations tab.

- **Generate reports using HP Reporter**

  WebSphere SPI also integrates with HP Reporter to provide you with over 20 management-ready, Web-based reports. WebSphere SPI includes the policies for generating these reports within its Report package, which you can install on the Reporter Windows system. After you have installed the

product and completed some configuration steps, you can expect to see new reports of summarized, consolidated data generated nightly that can help you assess how WebSphere is performing over time.

- **Graph data with HP Performance Manager**

  WebSphere SPI can be used with HP Performance Manager to generate graphs showing the WebSphere SPI collected metric values. If you have purchased HP Performance Manager, use it according to its instructions.

- **Customize WebSphere SPI Policies**

  You can use WebSphere SPI policies with no customization, or you can change them as you find necessary. Possible minor modifications and major customizations are listed here:

  - **Modification of Default Policies:** Within a policy, you can change the default settings for (1) collection interval, (2) threshold, (3) message text, (4) duration (5) severity level of the condition, (6) actions assigned to the condition (operator-initiated or automatic).

  - **Creation of Custom Policy Groups:** Create custom policy groups, using default policies as a starting point.

  - **Custom Metrics:** The ability to define your own metrics or user-definable metrics (UDMs) is a powerful feature that you can use to expand the monitoring capabilities of WebSphere SPI.

Related Topics:

- Introduction

- Overview

- Components

Components

The WebSphere Smart Plug-in (WebSphere SPI) components include:

- Tools

- Policies

These components allow you to configure and receive data in the form of messages, annotations, and metric reports. The messages (available in the Message Browser), annotations (available through message properties), and metric reports (available through tools) provide you with information about conditions present in the server(s) running on specific managed nodes.

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

Related Topics:

- Tools

- Policies

- Reports and graphs

- How the WebSphere SPI works

Tools

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) tools include configuration and troubleshooting utilities. From the HPOM console, select **Tools** → **SPI for WebSphere** to access the tools which are divided into the following categories:

- Metric Reports tools group

- SPI Admin tools group

- WebSphere Admin tools group

Related Topics:

- Components

- Policies

SPI Admin tools group

The SPI Admin tools group allows the HPOM administrator to perform routine tasks relating to WebSphere SPI.

For a more detailed description of the tools, click the tool name in the table below.

Tool	Description
Discover or Configure WBSSPI	Discovers the WebSphere Application Server instances or Configures the WebSphere SPI.
Create WBSSPI Node Groups	Create WebSphere SPI node groups based on discovered services.
Self-Healing Info	Collect log, trace, and other information to be used by your HP support representative.
Start/Stop Monitoring	Starts/Stops WebSphere SPI monitoring.
Start/Stop Tracing	Starts/Stops tracing. The tracing information collected is to be used by your HP support representative.
Verify	Verifies the WebSphere SPI is properly installed on the managed node.
View Error File	View the WebSphere SPI error log.

Related Topics:

- Metric Reports tools group

- WebSphere Admin tools group

Discover or Configure WBSSPI

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

Function

The following functions are performed by the Configure Tool:

- Updates the configuration on the HPOM management server and selected managed nodes.

- Creates the directories and files required by 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.

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

Configuration information for all WebSphere servers on HPOM managed nodes is maintained on the HPOM management server. Configuration information for a specific WebSphere server on an HPOM managed node is maintained on that managed node (each managed node maintains a subset of the configuration information maintained on the HPOM management server).

When saved, changes made with the configuration editor are always saved on the HPOM management server.

An HPOM managed node must be selected when this tool is launched, and changes to the configuration affecting any WebSphere servers on that managed node are automatically saved on that managed node.

If a specific HPOM managed node is selected when this tool is launched and changes are made that affect a WebSphere server on a non-selected managed node, the changes are saved to the configuration on the HPOM management server, but are *not* saved to the non-selected managed node. You must re-run this tool, select the affected managed node and, on exiting the tool, the changes are saved to that managed node.

To launch Discover or Configure WBSSPI

To launch the Discover or Configure WBSSPI tool, perform these steps:

1. From the HPOM console for Windows, select **Tools** → **SPI for WebSphere** → **SPI Admin** .

2. Double-click **Discover or Configure WBSSPI** .

3. Select the managed nodes on which you want to launch the tool.

4. Click **Launch** .

   The "Tool Selector" window opens.

5. To run the discovery, select the Launch Discover Tool radio button and click **OK** . To run the configuration, select the Launch Configure Tool radio button and click **OK** . By default, the Launch Configure Tool radio button is selected.

See *HP Operations Smart Plug-in for IBM WebSphere Application Server Installation and Configuration Guide for Windows* for more information on how to launch Discover or Configure WBSSPI tool.

Create WBSSPI Node Groups

Create WBSSPI Node Groups tool allows you to create WebSphere SPI node groups that contains all the managed nodes running supported versions of WebSphere. Node groups are created based on discovered services.

If new managed nodes are added, run this tool again to add these managed nodes to the WebSphere SPI node groups.

Function

Create WBSSPI Node Groups does the following:

- In the Nodes folder, creates the SPI for WebSphere node group and a subgroup based on the version of WebSphere running (WebSphere 7.0).

- Places all HPOM managed nodes running WebSphere 7.0 in the WebSphere 7.0 group.

- Assigns tools, reports, and graphs to the nodes and node groups.

To launch Create WBSSPI Node Groups tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **SPI Admin** .

2. Double-click **Create WBSSPI Node Groups** . The "Tool Status" window opens.

3. In the Launched Tools field, check the Status of the tool for each node:

   ○ Started/Starting - The tool is running.

   ○ Succeeded - WebSphere SPI has successfully created the node groups. Scroll to the bottom of the Tool Output field. The message "Done" displays.

   ○ Failed - The tool did not succeed. Scroll through the Tool Output field for more information about the problem.

4. Click **Close** to close the "Tool Status" window.

5. To verify the node group has been created, select **Nodes** → **SPI for WebSphere** . A node group for each WebSphere server version is created containing the managed nodes running that WebSphere server version. If no managed nodes are running a particular version of the WebSphere server, that node group is not created. For example, if you do not have any managed

nodes running WebSphere server version 5.0, that node group is not created.

Start/Stop Monitoring

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

These metrics generate alarms (when thresholds are exceeded) and are used to create reports (automatically or manually generated) and graphs. The reports and graphs are used to analyze trends in server usage, availability, and performance.

Typically, the HPOM administrator would 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 Verify to determine if monitoring is started or stopped. By default, monitoring is on.

Function

Start Monitoring does the following:

- Starts the collection of metrics for one or all application servers on a managed node.

Stop Monitoring does the following:

- Stops the collection of metrics for one or all application servers on a managed node.

To launch Start/Stop Monitoring tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **SPI Admin** .

2. Double-click **Start Monitoring** or **Stop Monitoring** .

3. Select the managed nodes on which you want to start or stop collection of metrics.

4. Click **Launch** . The "Console Status" window and then the "Server Selection" window open.

5. From the "Server Selection" window, select one application server or all application servers on which to start/stop collection of metrics.

6. Click **OK** .

7. From the "Console Status" window in the Launched Tool field, check the Status of the tool for each node:

- o Started/Starting - The tool is running.

- o Finished - The tool has completed. Scroll through the Tool Output field for more information.

8. Click **Close** to close the "Console Status" window.

Self-Healing Info

Self-Healing Info tool allows you to collect data to be used by your HP support representative.

Function

Self-Healing Info application performs the following functions:

1. Saves data 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

2. Launches and saves data using the Verify application.

To launch Self-Healing Info tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **SPI Admin** .

2. Double-click **Self-Healing Info** .

3. Select the managed nodes on which to collect data.

4. Click **Launch** . The "Tool Status" window opens. In the Tool Output field, the location of the data appears.

5. Send the collected data to your HP support representative.

6. Click **Close** to close the Tool Status window.

Start/Stop Tracing

Start and Stop Tracing tools allow you to start or stop logging the information about each of the activity performed by the SPI on the managed node. Run this tool only when instructed by your HP support representative.

Self-Healing Info collects the files created by this tool as part of its data to be used by your HP support representative.

Function

Start Tracing does the following:

- Saves the information about each of the activity performed by the SPI on the managed node into a file.

Stop Tracing does the following:

- Stops saving the information about each of the activity performed by the SPI on the managed node into a file.

To launch Start/Stop Tracing tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **SPI Admin** .

2. Double-click **Start Tracing** or **Stop Tracing** .

3. Select the managed nodes on which you want to start or stop tracing.

4. Click **Launch** . The "Tool Status" window opens.

5. In the Launched Tools field, check the Status of the tool for each node:

   - Started/Starting - The tool is running.

   - Succeeded - Tracing is successfully started/stopped for WebSphere SPI on the managed node. Select the node in the Launched Tools field and scroll to the bottom of the Tool Output field. The message "Tracing is ON/OFF." appears.

   - Failed - The tool did not succeed. Select the node in the Launched Tools field and scroll through the Tool Output field for more information about the problem.

6. Click **Close** to close the "Tool Status" window.

Verify

The tool Verify enables you to verify whether the files required for the functioning of the SPI (instrumentation, library, configuration files, and so on) are properly deployed.

Function

The Verify tool verifies whether the files required for the functioning of the SPI (instrumentation, library, configuration files, and so on) are properly deployed. It gives a list of missing instrumentation files.

> ⓘ **NOTE:**
> Before you launch the Verify tool ensure that you have installed the latest version of Self-Healing Service (SHS) component from the SPI DVD.

To launch Verify tool

1. From the HPOM console, select **Tools** ⟶ **SPI for WebSphere** ⟶ **SPI Admin** .

2. Double-click **Verify** .

3. Select the managed nodes on which you want to verify the WebSphere SPI installation.

4. Click **Launch** . The "Tool Status" window opens.

5. In the Launched Tools field, check the Status of the tool for each node:

   - Started/Starting - The tool is running.
   - Succeeded - WebSphere SPI has been properly installed on the managed node. Select the node in the Launched Tools field and scroll to the bottom of the Tool Output field. The message "Installation is clean" appears.
   - Failed - The tool did not succeed. Select the node in the Launched Tools field and scroll through the Tool Output field for more information about the problem.

6. Click **Close** to close the "Tool Status" window.

View Error File

View Error File tool allows you to view the contents of the error log file.

Function

View Error File does the following:

- Displays the contents of the WebSphere SPI error file `<AgentDir>` `/wasspi/wbs/log/errorlog` .

where *<OvAgentDir>* typically is:

- On UNIX managed nodes: `/var/opt/OV` or `/var/lpp/OV`

- On Windows Managed Nodes: `\Program Files\HP\HP BTO Software` (for HTTPS managed nodes)

To lauch View Error File tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **SPI Admin** .

2. Double-click **View Error File** .

3. Select the managed nodes on which you want to view the WebSphere SPI error log file.

4. Click **Launch** . The "Tool Status" window opens.

5. In the Launched Tools field, check the Status of the tool for each node:

   ○ Started/Starting - The tool is running.

   ○ Succeeded - You can view the WebSphere SPI error log file. Select the node in the Launched Tools field and scroll through the Tool Output field to view the error log file.

   ○ Failed - The tool did not succeed. Select the node in the Launched Tools field and scroll through the Tool Output field for more information about the problem.

6. Click **Close** to close the "Tool Status" window.

WebSphere Admin tools group

WebSphere Admin tools group allows the HPOM administrator to perform routine tasks relating to WebSphere.

For a more detailed description of the tools, click the tool name in the table below.

Tool	Description
Check WebSphere	Checks the state of WebSphere.
Start/Stop WebSphere	Start/Stop WebSphere (requires setup).
View WebSphere Log	View the WebSphere log files.

Related Topics:

- Metric Reports tools group

- SPI Admin tools group

Check WebSphere

Check WebSphere tool allows you check the status of each application server running on a managed node. It displays a status report for WebSphere on the selected managed nodes.

Function

Check WebSphere displays the following information for each application server on the selected managed node(s):

Server Name	The name of the WebSphere Server.
Server State	The status of WebSphere.
Start Date	The date when WebSphere was started.
Admin Server State	The status of the WebSphere Administrative Console.
Admin Server Start Date	The date when the WebSphere Administrative Console was started.

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

> **NOTE:**
> Before you launch the Check WebSphere tool on a node ensure that the Collector is running for the WebSphere Application Server instance on that node.

To launch Check WebSphere tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **WebSphere Admin** .

2. Double-click **Check WebSphere** .

3. Select the managed nodes on which you want to view the status of the application servers.

4. Click **Launch** . The "Tool Status" window opens.

5. In the Launched Tools field, check the Status of the tool for each node:

   - Started/Starting - The tool is running.

   - Succeeded - A status report is available for each instance of the WebSphere server on the

managed node. Select the node in the Launched Tools field and scroll through the Tool Output field.

- ○ Failed - The tool did not succeed. Select the node in the Launched Tools field and scroll through the Tool Output field for more information about the problem.

6. Click **Close** to close the "Tool Status" window.

Related Topics:

- Start/Stop WebSphere

- View WebSphere Log

- Metric Reports tools group

- SPI Admin tools group

Start/Stop WebSphere

Start WebSphere and Stop WebSphere tools allow you to start or stop WebSphere from the HPOM console. You can start or stop one or more application server on the selected managed nodes without logging in to each WebSphere Administrative Console to perform these functions.

Required Setup

- The START_CMD, STOP_CMD, and USER properties **MUST** be set before this tool can run successfully. Refer to Configuration Properties and Discover or Configure WBSSPI for more information about setting these properties.

- If you are using WebSphere Application Server 6.1 with Admin security enabled, before launching the Stop WebSphere tool you **must** set the following values for the attributes in the `/WEBSPHERE_HOME>/profiles/<profile_name>/properties/soap.client.prop` file. Set these values for all the profiles that you want to stop.

  - Set the value of **loginSource** attribute to "properties" (the default value of **loginSource** 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>`

Function

Start/Stop WebSphere does the following:

- Starts/Stops an application server or all application servers on the selected managed node(s).

To launch Start/Stop WebSphere tool

1. From the HPOM console, select **Tools** ➝ **SPI for WebSphere** ➝ **WebSphere Admin** .

2. Double-click **Start WebSphere** or **Stop WebSphere** .

3. Select the managed nodes on which you want to start/stop WebSphere.

4. Click **Launch** .

A "Console Status" window and then the "Server Selection" window open.

5. From the "Server Selection" window, select one application server or all application servers to start or stop.

6. Click **OK** .

7. From the "Console Status" window in the Launched Tool field, check the Status of the tool for each node:

   o Started/Starting - The tool is running.

   o Finished - The tool has completed. Scroll through the Tool Output field for more information.

8. Click **Close** to close the "Console Status" window.

Related Topics:

- Check WebSphere
- View WebSphere Log
- Metric Reports tools group
- SPI Admin tools group

View WebSphere Log

View WebSphere Log tool allows you to select a WebSphere log file to view without logging in to the system on which WebSphere is running.

Function

View WebSphere Log does the following:

- If you run View WebSphere Log without entering a parameter, a numbered list of available log files for a managed node appears.

- If you run View WebSphere Log with a parameter entered, if the parameter is not valid (a non-numeric value is entered or the number entered does not correspond to the list of available log files), a numbered list of available log files for the managed node appears.

- If you run View WebSphere Log with a valid parameter, the contents of the corresponding log file for the managed appears.

You may only enter one numeric value in the parameter field. This is the number used to designate the log file to view for all managed nodes selected. Select one log file per managed node to view each time you launch the tool.

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

To launch View WebSphere Log tool

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **WebSphere Admin** .

2. Double-click **View WebSphere Log** .

3. Select the managed nodes on which you want to view the WebSphere log file.

4. Click **Launch** . The "Edit Parameters" window opens. If you know the number of the log file you want to view, type it in the Parameters field. Otherwise, leave this field blank to list available log files to view.

5. Click **Launch** . The "Tool Status" window displays.

6. In the Launched Tools field, check the Status of the tool for each node:

- Started/Starting - The tool is running.

- Succeeded - A list of available log files to view displays. Select the node in the Launched Tools field and scroll through the Tool Output field to view the list of available log files.

- Failed - The tool did not succeed. Select the node in the Launched Tools field and scroll through the Tool Output field for more information about the problem.

Leave the "Tool Status" window open.

7. Double-click **View WebSphere Log** .

8. Select the managed nodes on which you want to view the WebSphere log file.

9. Click **Launch** . The "Edit Parameters" window appears.

10. 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 "Tool Status" window, select the node in the Launched Tools field, scroll through the Tool Output field 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.

11. Click **Launch** .

12. In the "Tool Status" window, select the node on which to view the selected log file and scroll through the Tool Output field to view the log file.

13. Repeat steps 7 - 12 for each log file you want to view.

14. Click **Close** to close the "Tool Status" window.

Related Topics:

- Check WebSphere

- Start/Stop WebSphere

- Metric Reports tools group

- SPI Admin tools group

Metric Reports tools group

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) reports show information on WebSphere conditions in the server. Each report displays the condition of all configured server instances on the managed node in relation to the metric.

To generate a report, follow these steps:

1. From the HPOM console, select **Tools** → **SPI for WebSphere** → **Metric Reports** .

2. Double-click a report.

3. Select the nodes on which to run the report.

4. Click **Launch** .

WebSphere SPI reports generated from alarms

A WebSphere SPI Report can also be triggered by an alarm condition. When such a situation occurs, the report is generated *automatically* . This report is context sensitive, relating only to a single server on the managed node. The information in the report is generated at the time the report was run (when the alarm condition occurred). You can find the report by double-clicking on the message and selecting the Annotations tab.

If you configure your Message Browser to display the *A* column, then an "S" under the *A* column (adjacent to the message) indicates that the report was *successfully* generated and is waiting in the *Annotations* of the message.

Metric reports description

Name/Associated Metric	Description
I005_JVMMemUtilPct	Percentage of heap space used in the JVM.
I040_ServSessAverageLife	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.
I212_ThreadPoolUtilPct	Percentage of threads used in a pool during collection interval.
I213_ThreadPoolPctMax	Percentage of time number of threads in pool reached configured maximum size (drill down).
I220_EJBPoolUtil	Percentage of active beans in the pool (drill down).
I221_EJBMethRespTime	Average EJB response time in milliseconds.
I222_EJBMethodCallsRt	Number of EJB method calls per minute (drill down).
I224_EJBEntDataLdStRt	Number of times an EJB was written to or loaded from the database per minute (drill down).
I246_WebAppServletRespTime	Average response time in milliseconds for a servlet.
I247_WebAppServletErrorRt	Number of errors in a servlet per second (drill down).
I261_JDBCConnPoolWaiters	Average Number of threads waiting for a connection from connection pools (drill down).
I262_JDBCConnPoolWaitTime	Average time that a client waited for a connection in milliseconds (drill down).
I263_JDBCConnPoolUtil	Percentage of connection pool in use.
I264_JDBCConnPoolMaxPct	Percentage of time that all connections in a pool are in use.
I265_JDBCConnPoolTimeoutRt	Number of times a client timed out waiting for a connection from the pool per minute (drill down).
I810_MsgBackoutRate	The rate at which the messages failed to be delivered to the bean onMessage method (message driven beans).
I811_ReturnDiscrdRt	The rate at which the returning object was discarded because the pool was full (entity and stateless).
I814_Prdstcchdsrd Rt	The rate at which the prepared statements are discarded by the least recently used (LRU) algorithm of the statement cache.

Related Topics:

- SPI Admin tools group

- WebSphere Admin tools group

Metric I005_JVMMemUtilPct

Policy Name	WBSSPI_0005
Metric Name	I005_JVMMemUtilPct
Metric Type	Alarming
Description	Percentage of heap space used in the JVM.
Impact	Low
PMI Module	jvmRuntimeModule
Severity: Condition with Threshold	WBSSPI-0005.1: Critical threshold, 98 WBSSPI-0005.2: Major threshold, 95
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0005.10: % of heap space used (<$VAL [Policy: <$NAME>] WBSSPI-0005.11: % of heap space used (<$VAL (<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The JVM is running out of ava **Potential Impact** : The performance of all the J2l for the server becomes slow. **Suggested action** : For IBM i and distributed pla **WebSphere Application Servers** → <**server_na** click **Java and process management** → **Process** *Java Virtual Machine (JVM) Heap Size* The Java Virtual Machine (JVM) Heap Size settin objects. If you increase the heap size, garbage col longer. These settings depend strongly on your ap memory available. Consider: • whether the JVM Heap for the selected applicat

	other application server JVM Heaps on the sam
	
	• specifying JVM Heaps to reside in physical men
	
	• setting the starting JVM Heap Size to one quart
	
	• setting the maximum JVM Heap Size to the fol
	server on the machine:
	
	   ○ 128 MB, for small systems with less than 1 G
	
	   ○ 256 MB, for systems with 2 GB of memory
	
	   ○ 512 MB, for larger systems
	
	NOTE: A value of 0, or blank, indicates that
	passed, when initializing the JVM. On OS/400, t
	you should never set the maximum heap size.

Report Type	ASCII
Area	JVM

Metric I040_ServSessAverageLife

Policy Name	WBSSPI_0040
Metric Name	I040_ServSessAverageLife
Metric Type	Alarming and Graphing
Description	Average servlet session lifetime in millisecon
Impact	Medium
PMI Module	servletSessionsModule
Severity: Condition with Threshold	WBSSPI-0040.1: Warning threshold, 1000
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0040.10: Average servlet session lif (>=<$THRESHOLD>ms) [Policy: <$NAME> WBSSPI-0040.11: Average servlet session lif threshold (<$THRESHOLD>ms) [Policy: <$N
Instruction Text	Check or modify the session settings : In the administrative console page, click **Serv Application Servers** → <**Web container** →
Report Type	ASCII
Area	Servlets

Metric I041_ServSessActSess

Policy Name	WBSSPI_0041
Metric Name	I041_ServSessActSess
Metric Type	Alarming, Graphing, and Reporting
Description	Number of sessions currently being accessed
Impact	High
PMI Module	servletSessionsModule
Severity: Condition with Threshold	WBSSPI-0041.1: Warning threshold, 10000
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0041.10: # of sessions currently be: (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0041.11: # of sessions currently bei threshold (<$THRESHOLD>) [Policy: <$NA
Instruction Text	**Probable Cause** : The number of sessions cu threshold value. **Potential Impact** : If this number equals the sessions is not created. **Suggested action** : To check or modify the s counts: In the administrative console page, click **Ser Application Servers** → <**server_name** >→
Report Type	ASCII
Area	Servlets

Metric I042_ServInvSessRt

Policy Name	WBSSPI_0042
Metric Name	I042_ServInvSessRt
Metric Type	Alarming and Graphing
Description	Number of sessions being invalidated per seco
Impact	Low
PMI Module	servletSessionsModule
Severity: Condition with Threshold	WBSSPI-0042.1: Warning threshold, 10000
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0042.10: # of sessions timed out per (>=<$THRESHOLD>/sec) [Policy: <$NAME WBSSPI-0042.11: # of sessions timed out per threshold ($THRESHOLD>/sec) [Policy: <$N
Instruction Text	**Probable Cause** : The number of sessions bei threshold value. **Potentail Impact** : The average response time sessions get invalidated even before the reque **Suggested action:** To modify or increase the In the administrative console page, click **Serv Application Servers → <server_name >We** the Session timeout value accordingly.
Report Type	ASCII
Area	Servlets

Metric I212_ThreadPoolUtilPct

Policy Name	WBSSPI_0212
Metric Name	I212_ThreadPoolUtilPct
Metric Type	Alarming
Description	Percentage of threads used in a pool during collection interval.
Impact	High
PMI Module	threadPoolModule
Severity: Condition with Threshold	WBSSPI-0212.1: Critical threshold, 90 WBSSPI-0212.2: Major threshold, 85 WBSSPI-0212.3: Minor threshold, 80
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0212.10: % of threads used (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0212.11: % of threads used (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0212.20: % of threads used (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0212.21: % of threads used (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0212.30: % of threads used (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>]

	WBSSPI-0212.31: % of threads used (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The percent of threads in use in a pool has exceeded a threshold value **Potential Impact** : Small Thread pool size might have been chosen.This choice can have the following impact: • Thread pool saturation condition may occur. • CPU utilization may consistently keep shooting up. **Suggested action** : 1. To fix a saturated thread pool, keep changing the thread pool size in steps until CPU utilization reaches between 75 and 85 percent. 2. Tune the application using a code profiling tool. 3. To check the size of the threadpool, in the Admin Console click **Servers → Server Types → Application servers → <server_name > → Thread pools** or **Servers → Server Types → Application servers → server1 → ORB service → Thread Pool** .
Report Type	ASCII
Area	Performance

 NOTE:
If the ThreadPool Size is configured as growable, the value for the metric I212_ThreadPoolUtilPct can exceed 100%. In this case, modify the threshold to a desired value to avoid false or frequent alarms.

Metric I213_ThreadPoolPctMax

Policy Name	WBSSPI_0213
Metric Name	I213_ThreadPoolPctMax
Metric Type	Alarming
Description	Percentage of time number of threads in pool reached configured maximum size (drill down).
Impact	High
PMI Module	threadPoolModule
Severity: Condition with Threshold	WBSSPI-0213.1: Minor threshold, 10
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0213.10: % of time # of threads reached configured maximum (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0213.11: % of time # of threads reached configured maximum (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The percent of threads in use in a pool has exceeded a threshold value **Potential Impact** : Small Thread pool size may have been chosen.This choice can have the following impact:< ul> • Thread pool saturation condition may occur. • CPU utilization may consistently keep shooting up. **Suggested action** : 1. To fix a saturated thread pool, keep changing the thread pool size in steps until CPU utilization reaches between 75 and 85 percent.

	2. Tune the application using a code profiling tool.
	3. To check the size of the threadpool, in the Admin Console click **Servers** → **Server Types** → **Application servers** → <**server_name** > → **Thread pools** or **Servers** → **Server Types** → **Application servers** → **server1** → **ORB service** → **Thread Pool** .
Report Type	ASCII
Area	Performance

Metric I220_EJBPoolUtil

Policy Name	WBSSPI_0220
Metric Name	I220_EJBPoolUtil
Metric Type	Alarming and Reporting
Description	Percentage of active beans in the pool (drill down).
Impact	High
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0220.1: Warning threshold, 90
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0220.10: % of EJBs in the pool in use (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0220.11: % of EJBs in the pool in use (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The utilization of the EJB cache has exceeded a threshold value. **Potential Impact** : • Thread pool saturation condition may occur. • CPU utilization may consistently keep shooting up. **Suggested action** : 1. To fix a saturated thread pool, keep changing the thread pool size in steps until CPU utilization reaches between 75 and 85 percent. 2. Tune the application using a code profiling tool. 3. To check the size of the EJB Cache, in the Admin Console click

	Servers → Server Types → Application servers → <server_name > → EJB container → EJB Cache Settings .
Report Type	ASCII
Area	EJB

The metric WBSSPI_0220 returns a valid value only if Entity Beans are present in the application(s) deployed on the WebSphere Application Server(s).

Metric I221_EJBMethRespTime

Policy Name	WBSSPI_0221
Metric Name	I221_EJBMethRespTime
Metric Type	Alarming and Reporting
Description	Average EJB response time in milliseconds.
Impact	Medium
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0221.1: Major threshold, 5000 WBSSPI-0221.2: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0221.10: Average EJB response time (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0221.11: Average EJB response time (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME> WBSSPI-0221.20: Average EJB response time (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0221.21: Average EJB response time (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>
Instruction Text	**Probable Cause** : The average response time of an EJB has exceeded a threshold value. **Potential Impact** : • Not sufficient Beans in pooled state. • Beans getting destroyed frequently.

	• Application response time may increase. **Suggested action** : To check the size of the EJB Cache, in the Admin Console click **Servers** → **Server Types** → **Application servers** → <**server_name** > → **EJB container** → **EJB Cache Settings** .
Report Type	ASCII
Area	EJB

The metric WBSSPI_0221 returns a valid value only if Entity Beans are present in the application(s) deployed on the WebSphere Application Server(s).

Metric I222_EJBMethodCallsRt

Policy Name	WBSSPI_0222
Metric Name	I222_EJBMethodCallsRt
Metric Type	Alarming and Reporting
Description	Number of EJB method calls per minute (drill down).
Impact	Low
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0222.1: Warning threshold, 10
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0222.10: # of EJB method calls per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0222.11: # of EJB method calls per minute (<$VALUE>/min) is within the threshold (<$THRESHOLD>/min) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of EJB method calls per minute has exceeded a threshold value. **Potential Impact** : • Increase in the CPU utilization • Increase in the EJB pool utilization **Suggested action** : To check the size of the EJB Cache, in the Admin Console click **Servers** → **Server Types** → **Application servers** → **<server_name >** → **EJB container** → **EJB Cache Settings** .
Report Type	ASCII
Area	EJB

The metric WBSSPI_0222 returns a valid value only if Entity Beans are present in the application(s) deployed on the WebSphere Application Server(s).

Metric I224_EJBEntDataLdStRt

Policy Name	WBSSPI_0224
Metric Name	I224_EJBEntDataLdStRt
Metric Type	Alarming and Reporting
Description	Number of times an EJB was written to or loaded from the database per minute (drill down).
Impact	Low
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0224.1: Warning threshold, 10
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0224.10: # of times EJB data was written to or loaded from the database per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0224.11: # of times EJB data was written to or loaded from the database per minute (<$VALUE>/min) is within the threshold (<$THRESHOLD>/min) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of times an EJB was written to or loaded from the database per minute has exceeded a threshold value. **Potential Impact** : • Increase in the CPU usage • May reduce the response time of the applications, if the EJB pool is full since the container has to passivate a bean and provide space for active beans in the pool. **Suggested action** : Make sure the EJB pool utilization is not high so that the Data Loads and Stores can be performed quickly.

Report Type	ASCII
Area	EJB

The metric WBSSPI_0224 returns a valid value only if Entity Beans are present in the application(s) deployed on the WebSphere Application Server(s).

Metric I246_WebAppServletRespTime

Policy Name	WBSSPI_0246
Metric Name	I246_WebAppServletRespTime
Metric Type	Alarming and Reporting
Description	Average response time in milliseconds for a servlet.
Impact	Medium
PMI Module	webAppModule
Severity: Condition with Threshold	WBSSPI-0246.1: Major, 10000 WBSSPI-0246.2: Warning, 2000
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0246.10: Average response time for a web application servlet (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0246.11: Average response time for a web application servlet (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0246.20: Average response time for a web application servlet (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0246.21: Average response time for a web application servlet (<$VALUE>ms) is within the threshold <$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average response time for servlet in msec has exceeded a threshold value. **Potential Impact** : As the number of concurrent users for the application increases, the thread pool utilization of the servlet engine also increases and the new requests may not be serviced immediately. This increases the response

	time of the application. **Suggested action** : Check the application server or servlet engine documentation for information about thread pool and its configurations to handle increased number of concurrent users or requests.
Report Type	ASCII
Area	Web Applications

Metric I247_WebAppServletErrorRt

Policy Name	WBSSPI_0247
Metric Name	I247_WebAppServletErrorRt
Metric Type	Alarming
Description	Number of errors in a servlet per second (drill down).
Impact	Low
PMI Module	webAppModule
Severity: Condition with Threshold	WBSSPI-0247.1: Warning, 100
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0247.10: # of errors for a web application servlet per second (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0247.11: # of errors for a web application servlet per second (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of errors in a servlet per second has exceeded a threshold value. **Potential Impact** : Applications response time may increase drastically. **Suggested action** : - Verify thread pool size set. - Verify connection pool size set. - Verify JVM heap size set.
Report Type	ASCII
Area	Web Applications

Metric I261_JDBCConnPoolWaiters

Policy Name	WBSSPI_0261
Metric Name	I261_JDBCConnPoolWaiters
Metric Type	Alarming and Reporting
Description	Average number of threads waiting for a connection from connection pools (drill down).
Impact	High
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0261.1: Major, 10 WBSSPI-0261.2: Warning, 1
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0261.10: Average # of threads waiting for a connection from connection pools (<$VALUE>) too high (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0261.11: Average # of threads waiting for a connection from connection pools (<$VALUE>) is within the threshold (<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0261.20: Average # of threads waiting for a connection from connection pools (<$VALUE>) too high (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0261.21: Average # of threads waiting for a connection from connection pools (<$VALUE>) is within the threshold (<$THRESHOLD>) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average number of threads waiting for a connection from the connection pool has exceeded a threshold value.

	Potential Impact : The application slows down. **Suggested action** : Small pool size is chosen for JDBC connection pool. • To fix a saturated connection pool, keep changing the pool size in steps until number of blocked applications is significantly reduced. • To modify or view the JDBC settings, in the administration console, click **Resources → JDBC → JDBC providers →** <**JDBC_provider_name** > **→ Data sources → Default Datasource → Connection pools** .
Report Type	ASCII
Area	JDBC

Metric I262_JDBCConnPoolWaitTime

Policy Name	WBSSPI_0262
Metric Name	I262_JDBCConnPoolWaitTime
Metric Type	Alarming and Reporting
Description	Average time that a client waited for a connection in msec (drill down).
Impact	Medium
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0262.1: Major, 50 WBSSPI-0262.2: Warning, 0
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0262.10: Average. time a client waited for a connection (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0262.11: Average time a client waited for a connection (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0262.20: Average. time a client waited for a connection (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0262.21: Average time a client waited for a connection (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average time that a client waited for a connection in has exceeded a threshold value. **Potential Impact** : • The client requests is not processed if the wait time is less than or equal to

	connection timeout.
	• The application response time increases.
	Suggested action : In the WebSphere Administration console, click **Resources** ➞ **JDBC** ➞ **Datasources** ➞ <**datasource_name** > ➞ **Connection Pools** and configure the properties appropriately.
Report Type	ASCII
Area	JDBC

Metric I263_JDBCConnPoolUtil

Policy Name	WBSSPI_0263
Metric Name	I263_JDBCConnPoolUtil
Metric Type	Alarming and Reporting
Description	Percentage of connection pool in use.
Impact	High
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0263.1: Critical, 98 WBSSPI-0263.2: Major, 95
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0263.10: % utilization of a connection pool (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0263.11: % utilization of a connection pool (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0263.20: % utilization of a connection pool (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0263.21: % utilization of a connection pool (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The percent utilization of the connection pool has exceeded a threshold value. **Potential Impact** : • Connection pool saturation condition may soon occur. • JDBC connection timeouts occur on connection pool saturation.

- Application response time increases.

Suggested action : To modify or view the JDBC settings, in the administration console, click **Resources** → **JDBC** → **JDBC providers** → <**JDBC_provider_name** > → **Datasources** → <**datasource_name** > → **Connection Pools** and configure the properties appropriately.

Report Type	ASCII
Area	JDBC

Metric I264_JDBCConnPoolMaxPct

Policy Name	WBSSPI_0264
Metric Name	I264_JDBCConnPoolMaxPct
Metric Type	Alarming
Description	Percentage of time that all connections in a pool are in use.
Impact	High
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0264.1: Critical, 98 WBSSPI-0264.2: Major, 95
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0264.10: % of time all connections in a pool are in use (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0264.11: % of time all connections in a pool are in use (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0264.20: % of time all connections in a pool are in use (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0264.21: % of time all connections in a pool are in use (<$VALUE>%) is within the threshold (<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The percent of time that all connections in a pool are in use has exceeded a threshold value. **Potential Impact** : Small connection pool size may have been chosen.This choice can have the following impact:

	• Connection pool saturation condition may occur. • CPU utilization may consistently keep shooting up. **Suggested action** : 1. To fix a saturated connection pool, keep changing the thread pool size in steps until CPU utilization reaches between 75 and 85 percent. 2. To modify or view the JDBC settings, in the administration console, click **Resources → JDBC → JDBC providers →** <**JDBC_provider_name** > **→ Datasources →** <**datasource_name** > **→ Connection Pools** and configure the properties appropriately. .
Report Type	ASCII
Area	JDBC

Metric I265_JDBCConnPoolTimeoutRts

Policy Name	WBSSPI_0265
Metric Name	I265_JDBCConnPoolTimeoutRt
Metric Type	Alarming and Reporting
Description	Number of times a client timed out waiting for a connection from the pool (drill down) per minute.
Impact	Low
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0265.1: Critical, 98 WBSSPI-0265.2: Major, 95
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0265.10: # of times a client timed out waiting for a connection per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0265.11: # of times a client timed out waiting for a connection per minute (<$VALUE>/min) is within the threshold (<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0265.20: # of times a client timed out waiting for a connection per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0265.21: # of times a client timed out waiting for a connection per minute (<$VALUE>/min) is within the threshold (<$THRESHOLD>/min) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of times a client timed out waiting for a connection from the connection pool has exceeded a threshold value.

	Potential Impact : Increased number of timed out requests impacts the performance of the applications. **Suggested action** : To modify or view the JDBC settings, in the administration console, click **Resources** → **JDBC** → **JDBC providers** → <**JDBC_provider_name** > → **Datasources** → <**datasource_name** > → **Connection Pools** and configure the properties appropriately.
Report Type	ASCII
Area	JDBC

Metric I810_MsgBackoutRate

Policy Name	WBSSPI_0810
Metric Name	I810_MsgBackoutRate
Metric Type	Alarming, Reporting, and Graphing
Description	The rate at which the messages failed to be delivere (message driven beans).
Impact	Medium and Low
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0810.1: Warning threshold, 5
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0810.10: The rate at which the messages f onMessage method (message driven beans) (<$VAl (>=<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0810.11: The rate at which the messages f onMessage method (message driven beans) (<$VAl (<$THRESHOLD>/min) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The rate at which the messages f onMessage method (message driven beans) has exc **Potential Impact** : The message could be corrupt o messages could be sent again to the MDB based on retries are more, the application response slows dov **Suggested action** : Configure the Backout threshol tries for the backed out messages.
Report Type	ASCII
Area	EJB

Metric I811_ReturnDiscrdRt

Policy Name	WBSSPI_0811
Metric Name	I811_ReturnDiscrdRt
Metric Type	Alarming, Reporting, and Graphing
Description	The rate at which the returning object was discarded stateless).
Impact	High, Medium, and Low
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0811.1: Warning threshold, 10
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0811.10 ReturnsDiscardRate: The rate at because the pool was full (entity and stateless) (<$\$$V (>=<\$THRESHOLD>/min) [Policy: <\$NAME>] WBSSPI-0811.11 ReturnsDiscardRate: The rate at because the pool was full (entity and stateless) (<$\$$V (<\$THRESHOLD>/min) [Policy: <\$NAME>]
Instruction Text	**Probable Cause** : ReturnsDiscardRate: The rate at which the returning object was discarded stateless) has exceeded a threshold value **Potential Impact** : The performance of the applicat **Suggested action** : Modify the pool settings accord In the administrative console page, click **Servers** → <**server** > → **EJB Container Settings** → **EJB Co**
Report Type	ASCII
Area	EJB

Metric I814_PrdstcchdsrdRt

Policy Name	WBSSPI_0814
Metric Name	I814_PrdstcchdsrdRt
Metric Type	Alarming, Reporting, and Graphing
Description	The rate at which the prepared statements are discarded by the least recently used (LRU) algorithm of the statement cache.
Impact	High and Medium
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0814.1: Warning threshold, 10
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0814.10: The rate at which the prepared statements are discarded by the least recently used (LRU) algorithm of the statement cache (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0814.11: The rate at which the prepared statements are discarded by the least recently used (LRU) algorithm of the statement cache (<$VALUE> /min) is within the threshold (<$THRESHOLD>/min) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : ReturnsDiscardRate: The rate at which the returning object was discarded because the pool was full (entity and stateless) has exceeded a threshold value **Potential Impact** : The performance of the applications slows down.

	Suggested action : Modify the pool settings accordingly: In the administrative console page, click **Servers** → **WebSphere Application servers** → <**server** > → **EJB Container Settings** → **EJB Container** .
Report Type	ASCII
Area	EJB

Policies

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) policy group is organized according to the impact that their data collections incur on system performance. 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.

The SPI for WebSphere policy group contains the following subgroups:

- WBSSPI Discovery

- High-Impact

- Medium-Impact

- Low-Impact

WBSSPI Discovery

The WBSSPI Discovery policy group contains the following policies:

- **WBSSPI-Messages** – A single policy that intercepts messages related to the discovery process

- **WBSSPI Service Discovery** – A single policy that does the following:
  - Checks for the presence of a WebSphere application server installation on the managed node on which it is deployed.
  - Gathers data fro the WebSphere SPI configuration from the WebSphere Admin Server and configuration files.
  - Creates/Updates the service map.
  - Updates the WebSphere SPI configuration data for the WebSphere application on the managed node.
  - Automatically deploys the Medium-Impact policy group to the managed node on which it discovers the presence of a WebSphere application server.

High-, Medium-, and Low-Impact

The WebSphere SPI policies are grouped for convenient deployment according to the impact that their data collection incurs on system performance. Refer to Overhead Generated Through Data Collection for complete listings of the specific metrics included in each group.

The High-, Medium-, and Low-Impact policy groups contain the following subgroups and policy:

- **WBSSPI-Logfiles** – Monitors WebSphere-generated and WebSphere SPI-generated logfiles. The information captured from these logfiles includes changes to WebSphere configurations and errors that occur in the operation of WebSphere or WebSphere SPI.

- **WBSSPI-Metrics** – Determines the threshold conditions of a monitored metric, the message text sent when the threshold is exceeded, the actions to complete, and instructions to follow (if necessary). Also known as a monitor policy.

- **WBSSPI-Monitors** – Controls what metrics are collected by running the collector/analyzer at the specified polling interval and defining the monitor policies that are collected.

- **WBSSPI-Messages** – A single policy that intercepts WebSphere and internal WebSphere SPI messages.

Policy Variables

The following variables are used by the WebSphere SPI policies. If you are creating your own policies, you may 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 may 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`

Related Topics:

- Metrics

- Monitors

- Logfiles

- Components

- Tools

- Metrics Overhead

- Metrics Naming/Numbering Conventions

- Metrics by Number

Metrics

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) metric policies have pre-defined settings that simplify setup tasks for the WebSphere SPI. Over time, however, you may want to customize some of those settings. Basic pieces of information you need for those customizations are provided.

For easy reference, the tables list all metrics by area. Click the Metric Name in the metric summary table to display individual metric details for every WebSphere metric and, when available, its policy settings. For metrics used for reporting or graphing only, no settings exist, hence the setting is labeled "N/A" (not applicable).

Availability Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
1	I001_ServerStatus	Status of a server	L	A	Critical	Availability
2	I002_ServerStatusRep	Status of a server - reporting	L	R		Availability

JVM Metric

ID	Metric Name	Description	Impact	Type	Severity	Area
5	I005_JVMMemUtilPct	Percentage of heap space used in the JVM	L	A	Critical	JVM
6	I006_ClusterStatus	Status of the cluster	L	A	Critical	JVM
807	I807_JVMMemFreePct	Percent of JVM Free Memory available	ML	G	Critical	JVM
808	I808_JVMCpuUsagePct	The CPU Usage of the Java virtual machine	ML	G	Critical	JVM
809	I809_GCIntervalTime	The average garbage collection value in seconds between two garbage collections	HML	G	Critical	JVM

Performance Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
210	I210_ThreadPoolActThreads	Average number of active threads in a pool during collection interval	H	R	 	Performance
211	I211_ThreadPoolAveSize	Average number of threads (active and idle) in a pool during collection interval	H	R	 	Performance
212	I212_ThreadPoolUtilPct	Percentage of threads used in a pool collection interval	H	A	Critical Major Minor	Performance
13	I013_ThrdPoolPctMax	Percentage of time the number of threads in a pool reached the configured maximum	H	G	 	Performance
213	I213_ThreadPoolPctMax	Percentage of time the number of threads in a pool reached the configured maximum	H	A	Minor	Performance
14	I014_ThrdPoolCrtRt	Number of threads created per minute	L	G	 	Performance

EJB Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
20	I020_EJBPoolUtil	Percentage of active beans in the pool	H	G		EJB
220	I220_EJBPoolUtil	Percentage of active beans in the pool (drill down)	H	AR	Warning	EJB
221	I221_EJBMethRespTime	Average response time of an EJB	M	AR	Major Warning	EJB
22	I022_EJBMethCallsRt	Number of EJB method calls per minute	L	GR		EJB
222	I222_EJBMethodCallsRt	Number of EJB method calls per minute (drill down)	L	AR	Warning	EJB
223	I223_EJBPoolSize	Average size of the EJB pool	H	R		EJB
24	I024_EJBEntDatLdStRt	Number of times an EJB was written to or loaded from the database per minute	L	GR		EJB
224	I224_EJBEntDataLdStRt	Number of times an EJB was written to or loaded from the database per minute (drill down)	L	AR	Warning	EJB
25	I025_EJBPoolMissPct	Average percentage of time a call to retrieve an EJB from the pool failed	L	G		EJB
225	I225_EJBPoolMissPct	Average percentage of time a call to retrieve an EJB from the pool failed	L	R		EJB
26	I026_EJBConcLives	Average number of bean objects in the pool	H	AG	Warning	EJB
810	I810_MsgBackoutRate	The rate at which the messages failed to be delivered to the bean onMessage method (message driven beans)	ML	ARG	Critical	EJB
811	I811_ReturnDiscrdRt	The rate at which the returning object was discarded because the pool was full (entity and stateless)	HML	ARG	Critical	EJB

Servlets Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
40	I040_ServSessAveLife	Average lifetime of a servlet session in milliseconds	M	AG	Warning	Servlets
41	I041_ServSessActSess	Number of sessions currently being accessed	H	AGR	Warning	Servlets
42	I042_ServInvSessRt	Number of sessions being invalidated per second	L	AG	Warning	Servlets

Web Applications Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
45	I045_WebAppServReqRt	Number of requests for a servlet per second	L	GR	 	Web Applications
245	I245_WebAppServletReqRt	Number of requests for a servlet per second (drill down)	L	AR	Warning	Web Applications
246	I246_WebAppServletRespTime	Average response time for a servlet in milliseconds	M	AR	Major Warning	Web Applications
47	I047_WebAppServErrRt	Number of errors in a servlet per second	L	G	 	Web Applications
247	I247_WebAppServletErrorRt	Number of errors in a servlet per second (drill down)	L	A	Warning	Web Applications
48	I048_WebAppServLoad	Number of servlets currently loaded for a web application	L	AG	Warning	Web Applications
49	I049_WebAppServRelRt	Number of servlets reloaded for a web application per minute	L	G	 	Web Applications

JDBC Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
260	I260_JDBCConnPoolSize	Average number of connections in the connection pool	H	AR	Minor	JDBC
61	I061_JDBCConPoolWait	Average number of threads waiting for a connection from connection pools	H	G	 	JDBC
261	I261_JDBCConnPoolWaiters	Average number of threads waiting for a connection from connection pools (drill down)	H	AR	Major Warning	JDBC
62	I062_JDBCConPoolWtTim	Average time that a client waited for a connection in milliseconds	M	G	 	JDBC
262	I262_JDBCConnPoolWaitTime	Average time that a client waited for a connection in milliseconds (drill down)	M	AR	Major Warning	JDBC
263	I263_JDBCConnPoolUtil	Percentage of connection pool in use	H	AR	Critical Major	JDBC
264	I264_JDBCConnPoolMaxPct	Percentage of time that all connections are in use	H	A	Critical Major	JDBC
65	I065_JDBCConPoolTimRt	Number of times a client timed out waiting for a connection from the pool per minute	L	G	 	JDBC
265	I265_JDBCConnPoolTimeoutRts	Number of times a client timed out waiting for a connection from the pool per minute (drill down)	L	AR	Critical	JDBC
66	I066_JDBCConPoolThru	Number of connections allocated and returned by applications per second	L	GR	 	JDBC
266	I266_JDBCConnPoolThroughput	Number of connections allocated and returned by applications per second (drill down)	L	AR	Warning	JDBC

Transactions Metrics

ID	Metric Name	Description	Impact	Type	Severity	Area
70	I070_TranGlobDur	Average duration of global transactions	H	AG	Warning	Transactions
71	I071_TranLocDur	Average duration of local transactions	H	AG	Warning	Transactions
72	I072_TranGlobCommDur	Average duration of commits for global transactions	M	AG	Warning	Transactions
73	I073_TranLocCommDur	Average duration of commits for local transactions	M	AG	Warning	Transactions
74	I074_TranRollbackRt	Number of global and local transactions rolled back per second	L	AG	Warning	Transactions
75	I075_TranTimeoutRt	Number of global and local transactions that timed out per second	L	AG	Warning	Transactions
76	I076_TranCommitRt	Number of global and local transactions that were committed per second	L	AG	Warning	Transactions
77	I077_TranThruput	Number of global and local transactions that were completed per second	L	R	 	Transactions
78	I078_TranStartRt	Number of global and local transactions that were begun per second	L	AG	Warning	Transactions

Related Topics:

- Golden Metrics

- Metric Naming/Numbering Conventions

- Metric Overhead

- Metrics by Number

- Monitors

- Logfiles

Golden Metrics

Golden metrics are a set of metrics which monitor the basic functionality of your WebSphere Application server. The golden metrics cover the critical areas (such as server status) for which you would like to receive messages as a critical or major event happens on the WebSphere Application server. Implementing golden metrics and taking action against the events generated by these metrics ensure the smooth functioning of the WebSphere Application server.

WebSphere SPI contains the following golden metrics:

Metric Type	Metric Name
Availability	Metric I001_ServerStatus
JVM	Metric I005_JVMMemUtilPct
	Metric I006_ClusterStatus
Servlets	Metric I041_ServSessActSess
Transactions	Metric I074_TranRollbackRt
	Metric I075_TranTimeoutRt
Performance	Metric I212_ThreadPoolUtilPct
EJB	Metric I220_EJBPoolUtil
	Metric I221_EJBMethRespTime
Web Applications	Metric I245_WebAppServletReqRt
	Metric I247_WebAppServletErrorRt
JDBC	Metric I261_JDBCConnPoolWaiters
	Metric I263_JDBCConnPoolUtil
	Metric I266_JDBCConnPoolThroughput

Related Topics:

- Metrics

- Monitors

- Logfiles

- Metrics Naming/Numbering Conventions

- Metric Overhead

Metric I001_ServerStatus

Policy Name	WBSSPI_0001
Metric Name	I001_ServerStatus
Metric Type	Alarming
Description	Status of a server, monitors whether running or not.
Impact	Low
PMI Module	JMX MBean
Severity: Condition with Threshold	WBSSPI-0001.1: Critical threshold, 4.5
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0001.10: Server status is down [Policy: <$NAME>] WBSSPI-0001.11: Server status is up [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The server is not started. **Potential Impact** : Performance monitoring for the server is not possible, and all the deployed applications will not work, until the server is started. **Suggested Action** : Start the server using the WebSphere StartServer script.
Report Type	N/A
Area	Availability

Metric I006_ClusterStatus

Policy Name	WBSSPI_0006
Metric Name	I006_ClusterStatus
Metric Type	Alarming
Description	Status of the cluster.
Impact	Low
PMI Module	jvmRuntimeModule
Severity: Condition with Threshold	WBSSPI-0006.10: Critical threshold, 1.0 WBSSPI-0006.20: Major threshold, 2.0
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0006.10:Cluster is stopped [Policy: <$N WBSSPI-0006.11:Cluster is started [Policy: <$N WBSSPI-0006.20:Cluster is partially stopped [[P<
Instruction Text	**Probable Cause** : Cluster is stopped. **Potential Impact** : The cluster and all servers in **Suggested action** : For IBM i and distributed pla **WebSphere Application Servers** ⟶ <**server_na** click **Java and process management** ⟶ **Process** the admin console, click **Servers** ⟶ **Clusters** ⟶ ⟶ <**cluster_name** > and issue the start comma
Report Type	ASCII
Area	JVM

Metric I074_TranRollbackRt

Policy Name	WBSSPI_0074
Metric Name	I074_TranRollbackRt
Metric Type	Alarming and Graphing
Description	Number of global and local transactions rolled back per second.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0074.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0074.10: # of global and local transactions rolled back (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0074.11: # of global and local transactions rolled back (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of global and local transactions rolled back per second has exceeded a threshold value. **Potential Impact** : This indicates the number of transaction failed, either due to resource contention and deadlock, or due to timeouts. Increased transaction roll backs impacts the application performance. **Suggested action** : This metric includes both global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

When a transaction commits, all actions associated with that transaction are written to a log. In the event of system problems, those actions are repeated if necessary when the system's recovery mechanism replays the log.

When a transaction aborts, any changes made by the transaction are undone. After a transaction is undone (rolled back), the only remaining evidence of the transaction is in the transaction processing system's log.

Timeouts associated with transactions usually prevent any one transaction from holding resources at a server for too long. For example, if two transactions are competing for the same resource (one holds a lock on a resource and the other is requesting that lock, and the lock modes conflict), timeouts will eventually abort one of the transactions. The idle timeout will abort a transaction that is inactive too long, and the operation timeout will abort an active transaction that is taking too long.

Report Type	ASCII
Area	Transactions

Metric I075_TranTimeoutRt

Policy Name	WBSSPI_0075
Metric Name	I075_TranTimeoutRt
Metric Type	Alarming and Graphing
Description	Number of global and local transactions that timed out per second.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0075.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0075.10: # of global and local transactions that timed out (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0075.11: # of global and local transactions that timed out (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of global and local transactions that timed out per second has exceeded a threshold value. **Potential Impact** : Timed out transactions result in the rolling back of transactions. Increased number of timed out transactions impacts the performance of the applications. **Suggested action** : This metric includes both global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

When a transaction commits, all actions associated with that transaction are written to a log. In the event of system problems, those actions are repeated if necessary when the system's recovery mechanism replays the log.

When a transaction aborts, any changes made by the transaction are undone. After a transaction is undone (rolled back), the only remaining evidence of the transaction is in the transaction processing system's log.

Timeouts associated with transactions usually prevent any one transaction from holding resources at a server for too long. For example, if two transactions are competing for the same resource (one holds a lock on a resource and the other is requesting that lock, and the lock modes conflict), timeouts will eventually abort one of the transactions. The idle timeout will abort a transaction that is inactive too long, and the operation timeout will abort an active transaction that is taking too long.

Report Type	ASCII
Area	Transactions

Metric I245_WebAppServletReqRt

Policy Name	WBSSPI_0245
Metric Name	I245_WebAppServletReqRt
Metric Type	Alarming and Reporting
Description	Number of requests for a servlet per second (drill down).
Impact	Low
PMI Module	webAppModule
Severity: Condition with Threshold	WBSSPI-0245.1: Warning threshold, 10000
Collection Interval	1h
Message Group	N/A
Message Text	WBSSPI-0245.10: Average request rate for a web application servlet (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0245.11: Average request rate for a web application servlet (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of requests for a servlet per second has exceeded a threshold value. **Potential Impact** : As the number of concurrent users for the application increases, the thread pool utilization of the servlet engine also increases and the new requests may not be serviced immediately. This increases the response time of the application. **Suggested action** : Check the application server or servlet engine documentation for information about thread pool and its configurations to handle increased number of concurrent users or requests.
Report Type	ASCII

Area	Web Applications

Metric I266_JDBConnPoolThroughput

Policy Name	WBSSPI_0266
Metric Name	I266_JDBConnPoolThroughput
Metric Type	Alarming and Reporting
Description	Number of connections allocated and returned by applications per second (drill down).
Impact	Low
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0266.1: Warning, 10000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0266.10: # of connections allocated and returned by applications (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0266.11: # of connections allocated and returned by applications (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of connections allocated and returned by applications per second has exceeded a threshold value. **Potential Impact** : • This indicates an increased number of JDBC requests. • Results in increase in CPU Usage. **Suggested action** : To modify or view the JDBC settings, in the administration console, click **Resources** ⟶ **JDBC** ⟶ **JDBC providers** ⟶ <**JDBC_provider_name** > ⟶ **Datasources** ⟶ <**datasource_name** > ⟶ **Connection Pools** and configure the properties appropriately.

Report Type	ASCII
Area	JDBC

Metric Naming/Numbering Conventions

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) metrics are identified by a metric name/number. These numbers also appear in the policies and reports (if either exists for the parallel metric). The naming/numbering conventions are as follows:

- *metric names/numbers* : The "I" preceding each metric number designates the metric as an IBM WebSphere SPI metric. WebSphere SPI metrics can then be identified as IXXX, where XXX represents the number assigned to the metric; for example, I005.

- *metric number ranges* : WebSphere SPI metric numbers range from 0000 to 0999

  In addition, metrics defined by the user, or User Defined Metrics, range from 0700 to 0799 range and are reserved.

- *report names* : If available for a specific WebSphere SPI metric, the report name is the metric number followed by an underscore and the abbreviated metric name; for example, I005_JVMMemUtilPct.

- *policy names* : If a policy is available for a metric, the policy name omits the "I" and begins with WBSSPI followed by an underscore and the metric number. Zeroes are used as necessary to total a four-digit number; for example, metric number I005 = policy WBSSPI_0005

Metric Specification Description

Policy Name	Always begins with "WBSSPI," followed by the metric number. Within the policy you can change settings as described in the definition; for example, threshold value and severity
Metric Name	The name assigned to the metric.
Metric Type	Shows how the metric is used, such as: • *Alarming* (using policy settings) • *Reporting* (within a report of the separately purchased HP Reporter) • *Graphing* (within a graph of the separately purchased HP Performance Manager)
Description	What the metric represents.
Impact	Overhead cost rating:

	• *H (High)* : Data counters (metrics) with the highest impact on system performance • *M (Medium)* : Data counters with moderate impact on system performance • *L (Low)* : Data counters with nominal impact on system performance
PMI Module	PMI module mapped to the metric.
Severity: Condition with Threshold	The severity of the exceeded threshold condition. (Critical, Major, Minor, Warning, Normal). If multiple conditions--for example, graduated thresholds-- are defined within the metric, severity levels are identified according to the specific condition.
Collection Interval	How often the metric is collected and analyzed (for example, 5 min, 15 min, 1 hour, 1 time daily).
Min/Max Threshold	Because this setting is the same for all WebSphere metrics, which have maximum thresholds, it is omitted.
Default Threshold	Shows the default threshold for metrics with parallel policies. (*=Metrics that should have been assigned a threshold value of 0 are set at 0.5 because alarms must occur at <= or >= values. Since a 0 value would always trigger an alarm, the threshold is set to 0.5).
Threshold Type	Because this setting is the same for all WebSphere metrics, which are without reset, it is omitted.
Message Group	The message group to which the metric belongs: • *WBSSPI* : conditions occurring in the WebSphere SPI • *WebSphere* : conditions occurring in WebSphere.
Message Text	The message displayed for each condition.
Instruction Text	Problem-solving information (Probable causes, Potential impact, Suggested actions, and Reports).
Report Type	Indicates if an ASCII report is available or if no report is planned (N/A).
Area	The logical area to which the metric belongs (Availability, JVM, Performance, Servlets, EJB, Servlets, Web Applications, J2C, JDBC, Transactions).

Related Topics:

• Metrics

- Monitors

- Logfiles

- Golden Metrics

- Metric Overhead

- Metrics by Number

Overhead Generated Through Data Collection

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

The WebSphere SPI alarming metrics are grouped for deployment in policy groups according to the impact that their data collection has on system performance. The three groups are Low-Impact, Medium-Impact, and High-Impact. All alarming metrics are contained in each group. The collector policies determine which metrics are collected.

When deployed and collected, the Low-Impact group deploys only low impact policies and the collector policies collect only low impact metrics; the Medium-Impact group deploys low and medium impact policies and the collector policies collect low and medium impact metrics; and the High-Impact group deploys all policies and the collector policies collect all metrics.

Click the Metric Number in the metric table to display individual metric details for every WebSphere metric and, when available, its policy settings. For metrics used for reporting or graphing only, no settings exist, hence the setting is labeled "N/A" (not applicable).

Low Impact Metrics

Metric Number	Metric Name	Metric Type			PMI Module
		A	R	G	
WBSSPI_0001	Server Status	X			JMX MBean
WBSSPI_0002	Server Status Report		X		JMX MBean
WBSSPI_0005	JVM Memory Utilization	X			jvmRuntimeModule
WBSSPI_0006	Cluster Status	X			jvmRuntimeModule
WBSSPI_0014	Thread Pool Creation Rate			X	threadPoolModule
WBSSPI_0022	EJB Method Calls Rate		X	X	beanModule
WBSSPI_0222	EJB Method Calls Rate, Drill Down	X	X		beanModule

WBSSPI_0024	EJB Data Loads/Stores Rate		X	X	beanModule
WBSSPI_0224	EJB Data Loads/Stores Rate, Drill Down	X	X		beanModule
WBSSPI_0025	Web Application Servlet Request Rate, Drill Down			X	beanModule
WBSSPI_0225	Web Application Servlet Request Rate		X		beanModule
WBSSPI_0042	Server Invalidated Session Rate	X		X	servletSessionsModule
WBSSPI_0045	Web Application Servlet Request Rate		X	X	webAppModule
WBSSPI_0245	Web Application Servlet Request Rate, Drill Down	X	X		webAppModule
WBSSPI_0047	Web Application Servlet Error Rate			X	webAppModule
WBSSPI_0247	Web Application Servlet Error Rate	X			webAppModule
WBSSPI_0048	Web Application Servlet Load Rate	X		X	webAppModule
WBSSPI_0049	Web Application Servlet Reload Rate			X	webAppModule
WBSSPI_0065	JDBC Connection Pool Timeout Rate			X	connectionPoolModule
WBSSPI_0265	JDBC Connection Pool Timeout Rate, Drill Down	X	X		connectionPoolModule
WBSSPI_0066	JDBC Connection Pool Throughput		X	X	connectionPoolModule
WBSSPI_0266	JDBC Connection Pool Throughput	X	X		connectionPoolModule
WBSSPI_0074	Transaction Rollback Rate	X		X	transactionModule
WBSSPI_0075	Transaction Timeout Rate	X		X	transactionModule
WBSSPI_0076	Transaction Commit Rate	X		X	transactionModule
WBSSPI_0077	Transaction Throughput		X		transactionModule
WBSSPI_0078	Transaction Start Rate	X		X	transactionModule
WBSSPI_0807	JVM Memory Free Percent			X	jvmRuntimeModule
WBSSPI_0808	JVM CPU Usage Percent			X	jvmRuntimeModule
WBSSPI_0809	GCIntervalTime			X	jvmRuntimeModule
WBSSPI_0810	Message Backout Rate	X	X	X	beanModule
WBSSPI_0811	Return Discard Rate	X	X	X	beanModule
WBSSPI_0812	Thread Pool Hung Rate	X		X	threadPoolModule

WBSSPI_0813	Concurrent Thread Pool Hung Count			X	threadPoolModule

Medium Impact Metrics

Metric Number	Metric Name	Metric Type			PMI Module
		A	R	G	
WBSSPI_0221	EJB Method Response Time	X	X		beanModule
WBSSPI_0040	Servlet Session Average Life	X		X	servletSessionsModule
WBSSPI_0246	Web Applications Servlet Response Time	X	X		webAppModule
WBSSPI_0062	JDBC Connection Pool Wait Time			X	connectionPoolModule
WBSSPI_0262	JDBC Connection Pool Wait Time, Drill Down	X	X		connectionPoolModule
WBSSPI_0072	Transaction Global Commit Duration	X		X	transactionModule
WBSSPI_0073	Transaction Local Commit Duration	X		X	transactionModule
WBSSPI_0807	JVM Memory Free Percent			X	jvmRuntimeModule
WBSSPI_0808	JVM CPU Usage Percent			X	jvmRuntimeModule
WBSSPI_0809	GCIntervalTime			X	jvmRuntimeModule
WBSSPI_0810	Message Backout Rate	X	X	X	beanModule
WBSSPI_0811	Return Discard Rate	X	X	X	beanModule
WBSSPI_0812	Thread Pool Hung Rate	X		X	threadPoolModule
WBSSPI_0813	Concurrent Thread Pool Hung Count			X	threadPoolModule
WBSSPI_0814	PrdstcchdsrdRt	X	X	X	connectionPoolModule

High Impact Metrics

Metric Number	Metric Name	Metric Type			PMI Module
		A	R	G	
WBSSPI_0210	Thread Pool Active Threads		X		threadPoolModule
WBSSPI_0211	Thread Pool Average Size		X		threadPoolModule
WBSSPI_0212	Thread Pool Utilization Percentage	X			threadPoolModule
WBSSPI_0013	Thread Pool Percentage Maximum			X	threadPoolModule
WBSSPI_0213	Thread Pool Percentage Maximum, Drill Down	X			threadPoolModule
WBSSPI_0020	EJB Pool Utilization			X	beanModule
WBSSPI_0220	EJB Pool Utilization, Drill Down	X	X		beanModule
WBSSPI_0223	EJB Pool Size		X		beanModule
WBSSPI_0026	EJB Concurrent Lives	X		X	beanModule
WBSSPI_0041	Servlet Session Active Sessions	X	X	X	servletSessionsModule
WBSSPI_0260	JDBC Connection Pool Size	X	X		connectionPoolModule
WBSSPI_0061	JDBC Connection Pool Waiters			X	connectionPoolModule
WBSSPI_0261	JDBC Connection Pool Waiters, Drill Down	X	X		connectionPoolModule
WBSSPI_0263	JDBC Connection Pool Utilization	X	X		connectionPoolModule
WBSSPI_0264	JDBC Connection Pool Percentage Maximum	X			connectionPoolModule
WBSSPI_0070	Transaction Global Duration	X		X	transactionModule
WBSSPI_0071	Transaction Local Duration	X		X	transactionModule
WBSSPI_0809	GCIntervalTime			X	jvmRuntimeModule
WBSSPI_0811	Return Discard Rate	X	X	X	beanModule
WBSSPI_0812	Thread Pool Hung Rate	X		X	threadPoolModule
WBSSPI_0813	Concurrent Thread Pool Hung Count			X	threadPoolModule
WBSSPI_0814	PrprdstcachdiscrdRt	X	X	X	connectionPoolModule

PMI Modules Not Used

The following PMI modules are not used by the SPI (PMI module settings should be set to N, none, for

these modules):

- cacheModule

- orbPerfModule

- systemModule

- webServicesModule

Related Topics:

- Metrics

- Monitors

- Logfiles

- Golden Metrics

- Metrics Naming/Numbering Conventions

- Metrics by Number

Metrics by Number

1 - 26	40 - 66	70 - 78	210 - 225	245 - 266	807 - 814
I001	I040	I070	I210	I245	I807
I002	I041	I071	I211	I246	I808
I005	I042	I072	I212	I247	I809
I006	I045	I073	I213	I260	I810
I013	I047	I074	I220	I261	I811
I014	I048	I075	I221	I262	I812
I020	I049	I076	I222	I263	I813
I022	I061	I077	I223	I264	I814
I024	I062	I078	I224	I265	
I025	I065		I225	I266	
I026	I066				

Related Topics:

- Metrics

- Monitors

- Logfiles

- Golden Metrics

- Metrics Naming/Numbering Conventions

- Metric Overhead

Metric I002_ServerStatusRep

Policy Name	N/A--Used for reporting (HP Reporter) only.
Metric Name	I002_ServerStatusRep
Metric Type	Reporting
Description	Status of a server--reporting.
Impact	Low
PMI Module	JMX MBean
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Availability

Metric I003_AdminServerStat

Policy Name	WBSSPI_0003
Metric Name	I003_AdminServerStat
Metric Type	Alarming
Description	Status of the Admin server.
Impact	Low
PMI Module	WAS 4.x Specific
Severity: Condition with Threshold	WBSSPI-0003.1: Critical threshold, 4.5
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0003.1: Admin Server status is d
Instruction Text	**Probable Cause** : NA **Potential Impact** : NA **Suggested Action** : NA
Report Type	N/A
Area	Availability

Metric I004_AdminServerStatusRep

Policy Name	N/A--Used for reporting (HP Reporter) only.
Metric Name	I004_AdminServerStatusRep
Metric Type	Reporting
Description	Status of the Admin Server-reporting.
Impact	Low
PMI Module	WAS 4.x Specific
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Availability

Metric I013_ThreadPoolPctMax

Policy Name	N/A--Used for reporting (HP Reporter
Metric Name	I013_ThreadPoolPctMax
Metric Type	Graphing
Description	Percentage of time number of threads i
Impact	High
PMI Module	threadPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	15m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Performance

Metric I014_ThrdPoolCrtRt

Policy Name	N/A--Used for reporting (HP Reporter) only
Metric Name	I014_ThrdPoolCrtRt
Metric Type	Graphing
Description	Number of threads created per minute.
Impact	Low
PMI Module	threadPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	15m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Performance

Metric I020_EJBPoolUtil

Policy Name	N/A--Used for reporting (HP Reporter) only
Metric Name	I020_EJBPoolUtil
Metric Type	Graphing
Description	Percentage of active beans in the pool.
Impact	High
PMI Module	beanModule
Severity: Condition with Threshold	N/A
Collection Interval	1h
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	EJB

Metric I022_EJBMethCallsRt

Policy Name	N/A—Used for graphing (HP Performance M
Metric Name	I022_EJBMethCallsRt
Metric Type	Graphing and Reporting
Description	Number of EJB method calls per minute.
Impact	Low
PMI Module	beanModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	EJB

Metric I024_EJBEntDataLdStRt

Policy Name	N/A—Used for graphing (HP Performance M
Metric Name	I024_EJBEntDataLdStRt
Metric Type	Graphing and Reporting
Description	Number of times an EJB was written to or loa
Impact	Low
PMI Module	beanModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	EJB

Metric I025_EJBPoolMissPct

Policy Name	N/A—Used for graphing (HP Performance Manag
Metric Name	I025_EJBPoolMissPct
Metric Type	Graphing
Description	Average percentage of time a call to retrieve an EJ
Impact	Low
PMI Module	beanModule
Severity: Condition with Threshold	Warning: WBSSPI-0025.1, threshold 10.
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	EJB

Metric I026_EJBConcLives

Policy Name	WBSSPI_0026
Metric Name	I026_EJBConcLives
Metric Type	Alarming and Graphing
Description	Average number of bean objects in the pool.
Impact	High
PMI Module	beanModule
Severity: Condition with Threshold	WBSSPI-0026.1: Warning threshold, 1000
Collection Interval	5m
Default Threshold	10
Message Group	WebSphere
Message Text	WBSSPI-0026.10: Average # of bean objects in (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0026.11: Average # of bean objects in threshold (<$THRESHOLD>) [Policy: <$NAME
Instruction Text	**Probable Cause** : The average number of bean value. **Potential Impact** : The pool is coming close to the performance of the applications. **Suggested action** : Modify the thread pool settin In the administrative console page, click **Servers Application Servers** → <**server** >→ **EJB Cont**
Report Type	ASCII
Area	EJB

Metric I045_WebAppServReqRt

Policy Name	WBSSPI_0045
Metric Name	I045_WebAppServReqRt
Metric Type	Graphing and Reporting
Description	Number of requests for a servlet per second.
Impact	Low
PMI Module	webAppModule
Severity: Condition with Threshold	N/A
Collection Interval	1h
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Web Applications

Metric I047_WebAppServErrRt

Policy Name	N/A—Used for graphing (HP Performance Manager) only.
Metric Name	I047_WebAppServErrRt
Metric Type	Graphing
Description	Number of errors in a servlet per second.
Impact	Low
PMI Module	webAppModule
Severity: Condition with Threshold	N/A
Collection Interval	1h
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Web Applications

Metric I048_WebAppServLoad

Policy Name	N/A—Used for graphing (HP Performance Manage
Metric Name	I048_WebAppServLoad
Metric Type	Alarming and Graphing
Description	Number of servlets currently loaded for a web appli
Impact	Low
PMI Module	webAppModule
Severity: Condition with Threshold	WBSSPI-0048.1: Warning threshold, 100
Collection Interval	1h
Message Group	N/A
Message Text	WBSSPI-0048.10: # of servlets currently loaded for (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0048.11: # of servlets currently loaded fo the threshold (<$THRESHOLD>) [Policy: <$NAM
Instruction Text	**Probable Cause** : The number of servlets currently a threshold value. **Potential Impact** : Loading a large number of serv the performance **Suggested action** : *Web Applications* You can also set parameters specific to each Web a affect performance. *Servlet Reload Interval and Reloading Enabled* Short description: WebSphere Application Server o automatically reloads servlets in the Web applicatic The auto reload capability can simplify the testing a applications by enabling you to quickly modify you

	Application Server. (Be sure that your Reload Inter servlets dynamically and the associated polling affe application's resources (such as servlets and enterpr necessary to aggressively reload these resources as When to try adjusting: When you are in a stable pro Reload Interval or disable Reloading. For a product resources only a few times a day. How to see or set: The Reload Interval and Reloading Enabled can be application by using the Application Assembler fro administrative console. When creating a new Web these parameters can be configured by selecting the Extensions and: 1. Unchecking the Reloading Enabled box. 2. Updating the Reload Interval field. Default value: Reload Interval = three seconds Relo How to see or set: The Reload Interval and Reloading Enabled can be click **Applications → Application Types → Enter** <**application_name** >**→ Class loader** and modify
Report Type	ASCII
Area	Web Applications

Metric I049_WebAppServRelRt

Policy Name	N/A—Used for graphing (HP Performance Man
Metric Name	I049_WebAppServRelRt
Metric Type	Graphing
Description	Number of servlets reloaded for a web applicatio
Impact	Low
PMI Module	webAppModule
Severity: Condition with Threshold	N/A
Collection Interval	1h
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Web Applications

Metric I061_JDBCConPoolWait

Policy Name	N/A—Used for graphing (HP Performance Ma
Metric Name	I061_JDBCConPoolWait
Metric Type	Graphing
Description	Average number of threads waiting for a conne
Impact	High
PMI Module	connectionPoolModule
Severity: Condition with Threshold	Warning: WBSSPI-0061.1, threshold 100
Collection Interval	5m
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	ASCII
Area	JDBC

Metric I062_JDBConPoolWtTim

Policy Name	N/A—Used for graphing (HP Performance Manager) only.
Metric Name	I062_JDBConPoolWtTim
Metric Type	Graphing
Description	Average time that a client waited for a connection in milliseconds.
Impact	Medium
PMI Module	connectionPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	JDBC

Metric I065_JDBConPoolTimRt

Policy Name	N/A—Used for graphing (HP Performance Manager) only.
Metric Name	I065_JDBConPoolTimRt
Metric Type	Graphing
Description	Number of times a client timed out waiting for a connection from the pool per minute.
Impact	Low
PMI Module	connectionPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	ASCII
Area	JDBC

Metric I066_JDBConPoolThru

Policy Name	N/A—Used for graphing (HP Performance Manager) and reporting (HP Reporter) only.
Metric Name	I066_JDBConPoolThru
Metric Type	Graphing and Reporting
Description	Number of connections allocated and returned by applications per second.
Impact	Low
PMI Module	connectionPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	JDBC

Metric I070_TranGlobDur

Policy Name	WBSSPI_0070
Metric Name	I070_TranGlobDur
Metric Type	Alarming and Graphing
Description	Average duration of global transactions.
Impact	High
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0070.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0070.10: Average duration of a global transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0070.11: Average duration of a global transaction (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average duration of global transactions has exceeded a threshold value. **Potential Impact** : Transaction durations indicate the server load and/or resource contentions. **Suggested action** : Use this metric to monitor the server load over time. Slower transaction durations may indicate either increased server load or increased resource contention or both. WebSphere keeps transaction performance data separately for global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

Report Type	ASCII
Area	Transactions

Metric I071_TranLocDur

Policy Name	WBSSPI_0071
Metric Name	I071_TranLocDur
Metric Type	Alarming and Graphing
Description	Average duration of local transactions.
Impact	High
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0071.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0071.10: Average duration of a local transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0071.11: Average duration of a local transaction (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average duration of local transactions has exceeded a threshold value. **Potential Impact** : Transaction durations indicate the server load and/or resource contentions. **Suggested action** : Use this metric to monitor the server load over time. Slower transaction durations may indicate either increased server load or increased resource contention or both. WebSphere keeps transaction performance data separately for global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

Report Type	ASCII
Area	Transactions

Metric I072_TranGlobCommDur

Policy Name	WBSSPI_0072
Metric Name	I072_TranGlobCommDur
Metric Type	Alarming and Graphing
Description	Average duration of commits for global transactions.
Impact	Medium
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0072.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0072.10: Average duration of a commit for a global transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0072.11: Average duration of a commit for a global transaction (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average duration of commits for global transactions has exceeded a threshold value. **Potential Impact** : Transaction commit durations indicate the server load and/or resource contentions. **Suggested action** : Use this metric to monitor the server load over time. Slower transaction durations may indicate either increased server load or increased resource contention or both. WebSphere keeps transaction performance data separately for global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

Report Type	ASCII
Area	Transactions

Metric I073_TranLocCommDur

Policy Name	WBSSPI_0073
Metric Name	I073_TranLocCommDur
Metric Type	Alarming and Graphing
Description	Average duration of commits for local transactions.
Impact	Medium
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0073.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0073.10: Average duration of a commit for a local transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0073.11: Average duration of a commit for a local transaction (<$VALUE>ms) is within the threshold (<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average duration of commits for local transactions has exceeded a threshold value. **Potential Impact** : Transaction commit durations indicate the server load and/or resource contentions. **Suggested action** : Use this metric to monitor the server load over time. Slower transaction durations may indicate either increased server load or increased resource contention or both. WebSphere keeps transaction performance data separately for global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

Report Type	ASCII
Area	Transactions

Metric I076_TranCommitRt

Policy Name	WBSSPI_0076
Metric Name	I076_TranCommitRt
Metric Type	Alarming and Graphing
Description	Number of global and local transactions that were committed per second.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0076.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0076.10: # of global and local transactions that were committed (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0076.11: # of global and local transactions that were committed (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of global and local transactions that were committed per second has exceeded a threshold value. **Potential Impact** : Increased number of committed transactions impacts the performance of the applicaiton. **Suggested action** : This metric indicates the rate (number per second) of transactions that are successfully committed on the server. Use this information for capacity planning. This metric includes both global and local transactions. Local transactions are limited to a single server and its associated resource manager. Global transactions are controlled by an external transaction manager and can span multiple servers.

Report Type	ASCII
Area	Transactions

Metric I077_TranThruput

Policy Name	WBSSPI_0077
Metric Name	I077_TranThruput
Metric Type	Reporting
Description	Number of global and local transactions that were committed per second.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Transactions

Metric I078_TranStartRt

Policy Name	WBSSPI_0078
Metric Name	I078_TranStartRt
Metric Type	Alarming and Graphing
Description	Number of global and local transactions that were started per second.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0078.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0078.10: # of global and local transactions that were begun (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>] WBSSPI-0078.11: # of global and local transactions that were begun (<$VALUE>/sec) is within the threshold (<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The number of global and local transactions that were begun per second has exceeded a threshold value. **Potential Impact** : Increased number of transactions impacts the performance of the server. **Suggested action** : This metric indicates the rate (number per second) of transactions that are begun on this server. Use this information for capacity planning.
Report Type	ASCII
Area	Transactions

Metric I210_ThreadPoolActThreads

Policy Name	N/A--Used for reporting (HP Reporter) only.
Metric Name	I210_ThreadPoolActThreads
Metric Type	Reporting
Description	Average number of active threads in a pool during collection interval.
Impact	High
PMI Module	threadPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	15m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Performance

Metric I211_ThreadPoolAverageSize

Policy Name	N/A--Used for reporting (HP Reporter) only.
Metric Name	I211_ThreadPoolAverageSize
Metric Type	Reporting
Description	Average number of threads (active and idle) in a pool during collection interval.
Impact	High
PMI Module	threadPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	15m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	Performance

Metric I223_EJBPoolSize

Policy Name	N/A—Used for reporting (HP Reporter) only.
Metric Name	I223_EJBPoolSize
Metric Type	Reporting
Description	Average size of the EJB pool.
Impact	High
PMI Module	beanModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Message Group	N/A
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	EJB

The metric WBSSPI_0223 returns a valid value only if Entity Beans are present in the application(s) deployed on the WebSphere Application Server(s).

Metric I225_EJBPoolMissPct

Policy Name	N/A
Metric Name	I225_EJBPoolMissPct
Metric Type	Reporting
Description	Average percentage of time a call to retrieve an EJB from the pool failed (drill down).
Impact	Low
PMI Module	beanModule
Severity: Condition with Threshold	N/A
Collection Interval	5m
Default Threshold	10
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	EJB

The metric WBSSPI_0225 returns a valid value only if Entity Beans are present in the application(s) deployed on the WebSphere Application Server(s).

Metric I260_JDBCConnPoolSize

Policy Name	WBSSPI_0260
Metric Name	I260_JDBCConnPoolSize
Metric Type	Alarming and Reporting
Description	Average number of connections in the connection pool.
Impact	High
PMI Module	connectionPoolModule
Severity: Condition with Threshold	WBSSPI-0260.1: Minor, 100
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0260.10: Average # of connections in the connection pool (<$VALUE>) too high (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0260.11: Average # of connections in the connection pool (<$VALUE>) is within the threshold (<$THRESHOLD>) [Policy: <$NAME>]
Instruction Text	**Probable Cause** : The average number of connections in the connection pool has exceeded a threshold value. **Potential Impact** : • Connection pool saturation condition may occur. • Applications may block on connection objects. **Suggested action** : • To fix a saturated thread pool, keep changing the pool size in steps until number of blocked applications is significantly reduced. • To modify or view the JDBC settings, in the administration console click

	Resources → **JDBC** → **JDBC providers** → **<JDBC_provider_name** > → **Data sources** → **Default Datasource** → **Connection pools** .
Report Type	ASCII
Area	JDBC

Metric I807_JVMMemFreePct

Policy Name	WBSSPI_0807
Metric Name	I807_JVMMemFreePct
Metric Type	Graphing
Description	Percent of JVM Free Memory available .
Impact	Medium and Low
PMI Module	jvmRuntimeModule
Severity: Condition with Threshold	N/A
Collection Interval	15m
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	JVM

Metric I808_JVMCpuUsagePct

Policy Name	WBSSPI_0808
Metric Name	I808_JVMCpuUsagePct
Metric Type	Graphing
Description	The CPU Usage of the Java virtual machine.
Impact	Medium and Low
PMI Module	jvmRuntimeModule
Severity: Condition with Threshold	N/A
Collection Interval	15m
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	JVM

Metric I809_GCIntervalTime

Policy Name	WBSSPI_0809
Metric Name	I809_GCIntervalTime
Metric Type	Graphing
Description	The average garbage collection value in seconds between two garbage collections. .
Impact	High, Medium, and Low
PMI Module	jvmRuntimeModule
Severity: Condition with Threshold	N/A
Collection Interval	1h
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	JVM

Metric I812_ThrdPoolHungRt

Policy Name	WBSSPI_0812
Metric Name	I812_ThrdPoolHungRt
Metric Type	Alarming and Graphing
Description	The rate at which the threads are declared hung.
Impact	High, Medium, and Low
PMI Module	threadPoolModule
Severity: Condition with Threshold	WBSSPI-0812.1: Warning threshold, 10
Collection Interval	15m
Message Group	WebSphere
Message Text	WBSSPI-0812.10: The rate at which the threads are high (>=<$THRESHOLD> /min) [Policy: <$NAM. WBSSPI-0812.11: The rate at which the threads are within the threshold (<$THRESHOLD>/min) [Poli
Instruction Text	**Probable Cause** : The rate at which the threads are value. **Potential Impact** : A hung thread can result from a infinite loop) or a more complex cause (for example such as CPU time, might be consumed by this hung code paths, such as when the code is running in an i become unresponsive even though all resources are **Suggested action** : Check the code for hung thread
Report Type	N/A
Area	ThreadPool

Metric I813_CcrtThdPlHngCt

Policy Name	WBSSPI_0813
Metric Name	I813_CcrtThdPlHngCt
Metric Type	Graphing
Description	The number of concurrently hung threads .
Impact	High, Medium, and Low
PMI Module	threadPoolModule
Severity: Condition with Threshold	N/A
Collection Interval	High - 1h, Med - 15m
Message Group	WebSphere
Message Text	N/A
Instruction Text	N/A
Report Type	N/A
Area	ThreadPool

Data Store Table for WebSphere Application Server

The WebSphere SPI creates the following data tables for WebSphere AS SPI metrics in the data store on the node to facilitate the data-collection procedure.

Table Name	Area	Metric Description	Column Name
WBSSPI_RPT_METRICS	Server	Status of a server-reporting	I002_ServerStatusRep
WBSSPI_METRICS	JVM	Percentage of heap space used in the JVM	I005_JVMMemUtilPct
	ThreadPool	Percentage of time number of threads in pool reached configured maximum size	I013_ThrdPoolPctMax
		Number of threads created per minute	I014_ThrdPoolCrtRt
WBSSPI_METRICS WBSSPI_RPT_METRICS	EJB	Percentage of active beans in the pooly	I020_EJBPoolUtil
		Number of EJB method calls per minute	I022_EJBMethCallsRt
		Number of times an EJB was written to or loaded from the database per minute	I024_EJBEntDtLdStRt
		Average percentage of time a call to retrieve an EJB from the pool failed	I025_EJBPoolMissPct

WBSSPI_METRICS		Average number of bean objects in the pool	I026_EJBConcLives
	WebModule	Average servlet session lifetime in milliseconds	I040_ServSessAveLfe
WBSSPI_METRICS WBSSPI_RPT_METRICS		Number of sessions currently being accessed	I041_ServSessActSes
WBSSPI_METRICS		Number of sessions being invalidated per second	I042_ServInvSessRt
WBSSPI_METRICS WBSSPI_RPT_METRICS		Number of requests for a servlet per second	I045_WebApServReqRt
		Number of errors in a servlet per second	I047_WebAppServErRt
		Number of servlets currently loaded for a web application	I048_WebAppServLoad
		Number of servlets reloaded for a web application per minute	I049_WebApServRelRt
WBSSPI_METRICS		Average number of threads waiting for a connection from connection pools	I061_JDBCConPoolWt
		Average time that a client waited for a connection in milliseconds	I062_JDBConPoolWtTm
		Number of times a client timed out waiting for a connection from the pool per minute	I065_JDBConPlToutRt

WBSSPI_METRICS WBSSPI_RPT_METRICS		Number of connections allocated and returned by applications per second	I066_JDBCConPlThru
WBSSPI_METRICS	JDBC	Average duration of global transactions	I070_TranGlobDur
		Average duration of local transactions	I071_TranLocDur
		Average duration of commits for global transactions	I072_TrGlbComDurNew
		Average duration of commits for local transactions	I073_TranLocCommDur
		Number per second of global and local transactions rolled back	I074_TranRollbackRt
		Number per second of timed out global and local transactions	I075_TranTimeoutRt
		Number per second of global and local transactions that were committed	I076_TranCommitRt
WBSSPI_METRICS WBSSPI_RPT_METRICS		Number per second of global and local transactions that were committed	I077_TranThroughput
WBSSPI_METRICS		Number per second of global and local transactions that were started	I078_TranStartRt
		Average number of	

		active threads in a pool during collection interval	I210_ThreadPoolActThreads
	ThreadPool	Average number of threads (active and idle) in a pool during collection interval	I211_ThreadPoolAveSize
WBSSPI_RPT_METRICS	EJB	Percentage of active beans in the pool (drill down)	I220_EJBPoolUtil
		Average EJB response time in milliseconds	I221_EJBMethRespTime
		Number of EJB method calls per minute (drill down)	I222_EJBMethodCallsRate
		Average size of the EJB pool	I223_EJBPoolSize
		Number of times an EJB was written to or loaded from the database per minute (drill down)	I224_EJBEntDataLdStRt
		Average percentage of time a call to retrieve an EJB from the pool failed (drill down)	I225_EJBPoolMissPct
	WebModule	Number of requests for a servlet per second (drill down)	I245_WebAppServletReqRt
		Average response time in milliseconds for a servlet	I246_WebAppServletRespTime
		Average number of	

		connections in the connection pool	I260_JDBCConnPoolSize
	JDBC	Average # of threads waiting for a connection from connection pools (drill down)	I261_JDBCConnPoolWaiters
		Average time that a client waited for a connection in msec (drill down)	I262_JDBCConnPoolWaitTime
		% of connection pool in use	I263_JDBCConnPoolUtil
		# of times a client timed out waiting for a connection from the pool per minute (drill down)	I265_JDBCConnPoolTimoutRts
		# of connections allocated and returned by applications	I266_JDBCConnPoolThroughput
WBSSPI_METRICS	JVM	Percent of JVM Free Memory available	I807_JVMMemFreePct
		The CPU Usage of the Java virtual machine	I808_JVMCpuUsagePct
		The average garbage collection value in seconds between two garbage collections	I809_GCIntervalTime
WBSSPI_METRICS WBSSPI_RPT_METRICS	EJB	The rate at which the messages failed to be delivered to the bean onMessage method (message driven beans)	I810_MsgBackoutRate

WBSSPI_RPT_METRICS		The rate at which the returning object was discarded because the pool was full (entity and stateless)	I811_ReturnDiscrdRt
WBSSPI_METRICS	ThreadPool	The rate at which the threads are declared hung	I812_ThrdPoolHungRt
		The number of concurrently hung threads	I813_CcrtThdPlHngCt
WBSSPI_METRICS WBSSPI_RPT_METRICS	JDBC	The rate at which the prepared statements are discarded by the least recently used (LRU) algorithm of the statement cache	I814_PrdstcchdsrdRt

Related Topics:

- Metrics

- JBoss AS SPI Golden Metrics

- JBSSPI Logfiles

- JBSSPI Policies

Monitors

Smart Plug-in for WebSphere Application Server (WebSphere SPI) Monitors policy group contains:

- collector policies

- WBSSPI-ConfigCheck policy

- WBSSPI-Performance policy

Collector Policies

Collector policies control what metrics are collected by running the collector/analyzer at the specified polling interval and defining the metrics that are collected.

Impact	Collector Policy Name	Polling Interval	Metrics Collected
High	WBSSPI-High-05min	5m	1-2, 22, 24, 26, 61-2, 65-6, 70-6, 78, 221-5, 260-6
	WBSSPI-High-15m	14m	5, 13-4, 210-3, 811-12, 814
	WBSSPI-High-1h	59m	20 40-2, 45, 47-9, 220, 245-7, 809, 813
Medium	WBSSPI-Medium-05m	5m	1-2, 22, 24, 62, 65-6, 72-6, 78, 221-2, 224-5, 262, 265-6
	WBSSPI-Medium-15m	14m	5, 14, 807-8, 810-14
	WBSSPI-Medium-1h	59m	40, 42, 45, 47-9, 245-7, 809
Low	WBSSPI-Low-05m	5m	1-2, 22, 24, 65-6, 74-6, 78, 222, 224-5, 265
	WBSSPI-Low-15m	14m	5-6, 14, 807-8, 810-14
	WBSSPI-Low-1h	59m	42, 45, 47-9, 245, 247, 809

WBSSPI-ConfigCheck

WBSSPI-ConfigCheck is a single policy that checks if the managed node is configured.

WBSSPI-Performance

WBSSPI-Performance is a single policy that logs performance data.

Related Topics:

- Metrics

- Logfiles

- Golden Metrics

- Metric Naming/Numbering Conventions

- Metrics Overhead

- Metrics by Number

Logfiles

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) logfile policies monitor WebSphere-generated and WebSphere SPI-generated logfiles. The information captured from these logfiles includes changes to WebSphere configurations and errors that occur in the operation of WebSphere Application Server or WebSphere SPI.

Logfiles Policy Name	Description
WBSSPI Error Log	Monitors the WebSphere SPI error log and sends the error messages to the message browser.
WebSphere Activity Log via JMX Notification	Monitors the WebSphere activity log file.
WebSphere Text Logs	Detects critical errors and warnings in the WebSphere log file.
WBSSPI Java Discovery Error Log	Monitors the WBSSPI Java Discovery error log.
WBSSPI Java Collector Error Log	Monitors the WBSSPI Java Discovery error log.

Related Topics:

- Metrics

- Monitors

- Policies

- Golden Metrics

- Metric Naming/Numbering Conventions

- Metrics by Number

- Metrics Overhead

WBSSPI Error Log

This logfile policy monitors the WBSSPI log file located at
`%OvAgentdir%\wasspi\wbs\log\wasspi_perl.log.`

Description	Monitors the WebSphere SPI error log and sends critical errors to the message browser.
Polling Interval	30s
Help Text	Refer to the specific error message listed in WebSphere SPI error messages for information about the error message.

WebSphere Activity Log via JMX Notification

Description	Monitors the WebSphere activity log file.
Polling Interval	30s
Severity	Critical Warning
Message Group	WebSphere
Help Text	**Probable Cause** : Critical - A message with the indicator "ERROR" or "FATAL" was detected in the WebSphere activity log. Warning - A message with the indicator "WARNING" or any non-critical message was detected in the WebSphere activity log. **Suggested Action** : Refer to the WebSphere documentation (manuals or online help) for more information about the error.

WebSphere Text Logs

Description	Detects critical errors and warnings in the WebSphere log file.
Polling Interval	30s
Severity	Critical Warning Normal
Message Group	WebSphere
Help Text	**Probable Cause** : Critical - A message with the indicator "ERROR" or "FATAL" was detected in the WebSphere log file. Warning - A message with the indicator "WARNING" was detected in the WebSphere log file. Normal - A message with the indicator "INFORMATIONAL" or "AUDIT" was detected in the WebSphere log file. **Suggested Action** : Refer to the WebSphere documentation (manuals or online help) for more information about the error.

WBSSPI Java Discovery Error Log

This logfile policy monitors the WBSSPI discovery error log file located at
`%OvAgentdir%\wasspi\wbs\log\Discovery.log`.

Description	Monitors the WBSSPI Java Discovery Error Log.
Polling Interval	30s
Severity	Normal Major Critical Warning
Message Group	WBSSPI
Help Text	Available for each error as detected: WASSPI-1 through WASSPI-241. For detailed help text for all error messages, see the specific error message listed in WebSphere SPI error messages for information about the error message.

WBSSPI Java Collector Error Log

This logfile policy monitors the WBSSPI collector error log file located at
`%OvAgentdir%\wasspi\wbs\log\Collector.log .`

Description	Monitors the WBSSPI Java Collector Error Log.
Polling Interval	30s
Severity	Normal Major Critical Warning
Message Group	WBSSPI
Help Text	Available for each error as detected: WASSPI-1 through WASSPI-241. For detailed help text for all error messages, see the specific error message listed in WebSphere SPI error messages for information about the error message.

Configuration editor

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) maintains a configuration that consists of property value assignments. The configuration editor is a graphical user interface used to view and edit the configuration.

The configuration editor is used by the Discover or Configure WBSSPI tool.

Related Topics:

- The configuration

- Using the configuration editor

- Example configurations

- Configuration properties

The configuration editor- getting started

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) maintains a configuration that consists of property value assignments.

On the HPOM management server, the configuration maintains information for your entire environment and contains information for all WebSphere servers on all managed nodes.

On a managed node, the configuration contains only information for the WebSphere servers running on that node. This information is extracted from the configuration on the management server.

Structure

The structure of the configuration is (lines beginning with "#" are treated as comments and ignored):

```
# Global Properties

  <config_property >=<value > ...


# GROUP Block

  GROUP <group_name >
  {
     <nodename > ...
  }


# NODE Block

  NODE [<group_name > | <nodename >]
  {
     <config_property >=<value > ...
  }
```

- **Global Properties**

```
# Global Properties

  <config_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.

Using the configuration editor, view, set, or edit global properties by selecting the Default Properties item in the Defaults folder.

- **GROUP Block**

```
# GROUP Block

   GROUP <group_name >
   {
       <nodename > ...
   }
```

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 file, the last definition takes precedence.

<nodename > lists the nodes in the group and is the primary node names configured in HPOM.

Set the common properties 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 [<group_name > | <nodename >]
   {
       <config_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 *<nodename >* (to set properties for a single node).

For a group, enter the *<group_name >* defined by the GROUP block and define the common properties.

For a single node, enter the *<nodename >* and define the properties.

<nodename > is the primary node name configured in HPOM.

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 >_config_property* refers to a specific WebSphere server instance. When more than one WebSphere server 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.

Using the configuration editor, view, set, or edit server-specific properties by selecting the *<Application_Server_Name>* item in the Application Servers folder.

Configuration property precedence

The order of precedence of properties defined in the configuration file are:

1. SERVER*<n >_config_property* (server-specific)

2. NODE *nodename* block *config_property*

3. NODE *group_name* block *config_property*

4. Global *config_property*

Primary node name

The *<nodename >* specified in a GROUP and NODE block is the primary node name configured in HPOM. To display the primary node name, do the following:

1. From the HPOM console, select **Operations Manager ➜ Nodes** .

2. Right-click the node and select **Properties** .

3. Select the **Network** tab.

Configuration location

The location of the configuration file is listed for your convenience. Edit the configuration using the configuration editor only.

- **Management server**

<ShareInstallDir> \SPI-Share\wasspi\wbs\conf\SiteConfig

where *<ShareInstallDir>* by default is `C :\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared`

This file contains all configuration information for all managed nodes on which WebSphere is running.

- **Windows managed node**

<OvAgentDir> `\wasspi\wbs\conf\SiteConfig`

where *<AgentDir>* is typically `\Program Files\HP\HP BTO SOftware\` (for HTTPS managed nodes) or
`C:\Program Files\HP OpenView\Installed Packages\{790C06B4-844E-11D2-972B-080009EF8C2A}` (for DCE managed nodes)

This file contains the local configuration information for this managed node on which WebSphere is running.

- **Unix managed node**

<OvAgentDir> `/conf/wbsspi/SiteConfig`

where *<OvAgentDir>* is typically `/var/opt/OV/` or `/var/lpp/OV/`

This file contains the local configuration information for this managed node on which WebSphere is running.

Related Topics:

- Using the configuration editor

- Example configurations

- Configuration properties

Components of configuration editor

The configuration editor is provided by the Smart Plug-in for WebSphere Application Server (WebSphere SPI) to view and edit the configuration. You must update the configuration using this editor only.

The configuration editor has three components:

- **The configuration editor - Tree**

  The Configuration Editor - Tree, displayed in the left pane of the Discover or Configure WBSSPI Tool main window, displays the WebSphere SPI configuration file in a tree structure.

  The following is an example of the tree.

  > 🛈 **NOTE:**
  > If no application servers or groups are configured, the "Application Servers" and "Groups" folders are not displayed. If you are running Discover or Configure WBSSPI for the first time and you did not select any nodes when you launched the tool, the "Nodes" folder is not displayed.
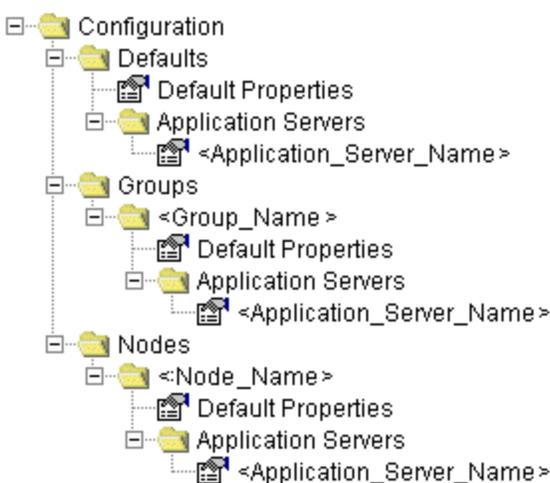
  The 📁 icon denotes that you can view configuration properties.

  The 🖼 icon denotes that you can view and set configuration properties.

  The following table lists each item in the tree and a brief description of the item.

Item Name	Description
Application Servers	A folder that contains a list of all the application servers. This folder can appear under Defaults (global properties level), Group_Name(s) (GROUP level), or Node_Name(s) (NODE level).
<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 have been set. This item appears under Defaults (global properties level), Group_Name(s) (GROUP level), or Node_Name(s) (NODE level).
Defaults	A folder that represents the global properties level .
Groups	A folder that represents the GROUP level .
<Group_Name >	A folder that identifies the name of a group of nodes with common properties.
Nodes	A folder that represents the NODE level .
<Node_Name >	A folder that represents a single node whose name must match the primary node name configured in HPOM.

- **Actions to perform**

   Actions that you can perform depend on the item that is selected in the tree. The following actions are available either using the Actions menu or by right-clicking on an item in the tree.

   In the table below, click the action for a more detailed description (if available) of how to perform that action.

Action	Description	Selected Tree Item
Add Application Server	Add an application server.	📁 Application Servers 📁 Defaults 📁 *<Group_Name >* 📁 *<Node_Name >*
Add Group	Create a group to which you can assign nodes that have common properties.	📁 Any item in the tree 📄 Any item in the tree
Add Node	Add a managed node to the Nodes folder.	📁 Any item in the tree 📄 Any item in the tree
Exit	Exit the Discover or Configure WBSSPI tool. This action is available from the File menu. If any changes were made that have not been saved, the "Confirm Cancel" window displays.	📁 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.	📁 Application Servers 📄 *<Application_Server_Name >*
Remove Group/Remove ALL Groups	Remove a WebSphere SPI group or all listed WebSphere SPI groups.	📁 Groups 📁 *<Group_Name >*
Remove Node/Remove ALL Nodes	Remove a managed node or remove all managed nodes.	📁 Nodes 📁 *<Node_Name >*
Save	Save changes to the configuration file. This action is available from the File menu only if changes were made to the configuration file.	📁 Any item in the tree 📄 Any item in the tree
Set Configuration Properties tab	Set WebSphere SPI configuration properties.	📄 *<Application_Server_Name >* 📄 Default Properties
View Configuration Settings tab	View WebSphere SPI configuration properties.	📁 Any item in the tree 📄 Any item in the tree

- **The configuration editor buttons**

The following buttons are available in Discover or Configure WBSSPI:

Button	Description
Cancel	Exit Discover or Configure WBSSPI. If you have 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 have modified a configuration property, a "Confirm Cancel" window displays. Select **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 file (changes are not saved).
Finish	Exit Discover or Configure WBSSPI. Appears instead of the **Next** button if you launched Discover or Configure WBSSPI without selecting any nodes.
Next	Exit Discover or Configure WBSSPI. Takes you to the "Confirm Operation" window that lists the nodes you selected when Discover or Configure WBSSPI was started. The selected managed nodes' configuration files 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 file, but to make the changes to those managed node's configuration file, you must restart Discover or Configure WBSSPI, select those nodes, and then exit.
Save	Save changes to the HPOM management server's configuration file and continue editing the configuration file. You may also select **File → Save** to save your changes.

Related Topics:

○ The configuration

○ Example configurations

○ Configuration properties

Add Application Server

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

To add an application server, do the following:

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

   The "Configure WBSSPI Tool: Add App Server" window displays.

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."

   If the "Use inherited Server Port" check box is selected, you may 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 may 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 , and NODE level.

   If the PORT property is set at the global properties level ...

   WebSphere SPI uses this same port number on all nodes and groups 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, only one server can use the inherited server port. You must edit the PORT property for the other application servers.

   If the PORT property is set at the GROUP level ...

WebSphere SPI uses 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 uses this same port number for that node 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, 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. Select **OK** .

    The NAME and PORT properties are set.

    The application server is added and its properties are displayed. You may also set additional configuration properties for this server. Refer to Set Configuration Properties tab for more information.

6. Select **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 select **Save** .

Related Topics:

- Add Group

- Add Node

- Remove Application Server/Remove ALL App Servers

- Remove Group/Remove ALL Groups

- Remove Node/Remove ALL Nodes

- Set Configuration Properties tab

- View Configuration Settings tab

- Using the configuration editor

Add Group

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

To add a group, do the following:

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

   The "Configure WBSSPI Tool: Add Group" window displays.

2. Enter the "Group Name." The group name identifies the group of nodes with common properties and is NOT case-sensitive.

3. Select **OK** .

   The group is added and the Set Configuration Properties tab for the group displays.

4. Select **Add Node to Group** , select one node from the list to add to the group, and then select **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. Refer to Set Configuration Properties tab for more information.

6. Select **Save** to save your changes.

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

Related Topics:

- Add Application Server

- Add Node

- Remove Application Server/Remove ALL App Servers

- Remove Group/Remove ALL Groups

- Remove Node/Remove ALL Nodes

- Set Configuration Properties tab

- View Configuration Settings tab

- Using the configuration editor

Add Node

Add a managed node to the WebSphere SPI configuration file.

To add a node, do the following:

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

   If no additional managed nodes are available to add to the configuration file, the message "All available managed nodes have been added to the configuration." displays. Click **OK** to exit this action.

   Otherwise, the "Configure WBSSPI Tool: Add Node" window displays.

2. From the pulldown menu, select a node to add.

3. Select **OK** .

   The node is added and the Set Configuration Properties tab for the node displays.

4. Set the configuration properties for this node using the **Select a Property to Set** pulldown list. Refer to Set Configuration Properties tab for more information.

5. Select **Save** to save your changes.

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

Related Topics:

- Add Application Server

- Add Group

- Remove Application Server/Remove ALL App Servers

- Remove Group/Remove ALL Groups

- Remove Node/Remove ALL Nodes

- Set Configuration Properties tab

- View Configuration Settings tab

- Using the configuration editor

Remove Application Server/Remove ALL App Servers

Remove a WebSphere server or all listed WebSphere servers from the WebSphere SPI configuration file.

To remove an application server, do the following:

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 file.

2. Select **Cancel** to cancel the removal of the application server (the application server name appears the next time you run Discover or Configure WBSSPI). In the "Confirm Cancel" window, select **Exit without Save** .

   Otherwise, select **Save** to permanently remove the application server.

To remove ALL application servers, do the following:

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 file).

2. Select **Cancel** to cancel the removal of all application servers (the Application Servers folder and all application server names listed in the folder appear the next time you run Discover or Configure WBSSPI). In the "Confirm Cancel" window, select **Exit without Save** .

   Otherwise, select **Save** to permanently remove the application servers.

Related Topics:

- Add Application Server

- Add Group

- Add Node

- Remove Group/Remove ALL Groups

- Remove Node/Remove ALL Nodes

- Set Configuration Properties tab

- View Configuration Settings tab

- Using the configuration editor

Remove Group/Remove ALL Groups

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

To remove a group, do the following:

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 file.

2. Select **Cancel** to cancel the removal of the group (the group name appears the next time you run Discover or Configure WBSSPI). In the "Confirm Cancel" window, select **Exit without Save** .

   Otherwise, select **Save** to permanently remove the group.

To remove ALL groups, do the following:

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

   The selected Groups folder and all groups listed in the selected folder are removed (all configuration properties for the listed groups are removed from the configuration file).

2. Select **Cancel** to cancel the removal of all groups (the Groups folder and all group names listed in the folder appear the next time you run Discover or Configure WBSSPI). In the "Confirm Cancel" window, select **Exit without Save** .

   Otherwise, select **Save** to permanently remove the groups.

Related Topics:

- Add Application Server

- Add Group

- Add Node

- Remove Application Server/Remove ALL App Servers

- Remove Node/Remove ALL Nodes

- Set Configuration Properties tab

- View Configuration Settings tab

- Using the configuration editor

Remove Node/Remove ALL Nodes

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

To remove a node, do the following:

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 file.

2. Select **Cancel** to cancel the removal of the node (the node name appears the next time you run Discover or Configure WBSSPI). In the "Confirm Cancel" window, select **Exit without Save** .

   Otherwise, select **Save** to permanently remove the node.

To remove ALL nodes, do the following:

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 file).

2. Select **Cancel** to cancel the removal of all nodes (the Nodes folder and all node names listed in the folder appear the next time you run Discover or Configure WBSSPI). In the "Confirm Cancel" window, select **Exit without Save** .

   Otherwise, select **Save** to permanently remove the nodes.

Related Topics:

- Add Application Server

- Add Group

- Add Node

- Remove Application Server/Remove ALL App Servers

- Remove Group/Remove ALL Groups

- Set Configuration Properties tab

- View Configuration Settings tab

- Using the configuration editor

Set Configuration Properties tab

Set WebSphere SPI configuration properties at the global properties level or for the selected application server(s), group(s) (GROUP level), or node(s) (NODE level).

Items with the icon are the only items for which you can set the 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 file, do the following:

1. Select a property from the "Select a Property to Set" pulldown menu.

2. Select **Set Property** . The property and an empty value field appear in the table.

3. Click the empty value field and enter a value.

4. Repeat steps 1 - 3 for each property to set.

5. Click **Save** .

> **NOTE:**
> For the `LOGIN` and `PASSWORD` properties, when you select **Set Property** , a separate window displays.
> Enter the login and password values in this window.

For more information about individual properties, refer to Configuration properties .

Modifying a property

To modify a property (except `LOGIN`) in the configuration file, do the following:

1. Select the property from the table.

2. Double-click the value field.

3. Edit the value.

4. Repeat steps 1 - 3 for each property to modify.

5. Click **Save** .

To modify the LOGIN property in the configuration file, do the following:

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 displays.

3. Enter the new password and verify password.

4. Click **OK** .

5. Click **Save** .

For more information about individual properties, refer to Configuration properties .

Removing a property

To remove a property from the configuration file, do the following:

1. Select the property from the table.

2. Click **Remove Property** .

3. Repeat steps 1 - 2 for each property to remove.

4. Click **Save** .

Related Topics:

- Add Application Server

- Add Group

- Add Node

- Remove Application Server/Remove ALL App Servers

- Remove Group/Remove ALL Groups

- Remove Node/Remove ALL Nodes

- View Configuration Settings tab

- Using the configuration editor

View Configuration Settings tab

View all WebSphere SPI configuration properties set in the configuration file on the HPOM management server or the WebSphere SPI configuration properties for the selected application server(s), group(s), or node(s).

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 file on the HPOM management server.
Default Properties	View all set configuration properties (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 all 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, it 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

Related Topics:

- Add Application Server

- Add Group

- Add Node

- Remove Application Server/Remove ALL App Servers

- Remove Group/Remove ALL Groups

- Remove Node/Remove ALL Nodes

- Set Configuration Properties tab

- Using the configuration editor

Example Configurations

The sample Smart Plug-in for WebSphere Application Server (WebSphere SPI) configuration files illustrate various features and utilization methods. Lines preceded by "#" are treated as comments and are ignored.

This sample configuration would be displayed at the Defaults level by selecting the View Configuration Settings tab .

Select an example to view:

Single node/two servers

Click the image to zoom in or out.

This example shows a single node running two servers, the Administration Server and a 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.
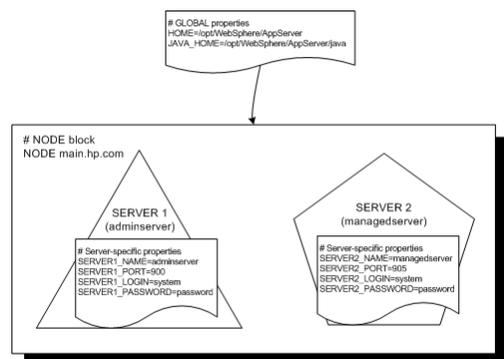

```
HOME = /opt/WebSphere/AppServer
JAVA_HOME = /opt/WebSphere/AppServer/java

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
```

}

Related Topics:

- The configuration

- Using the configuration editor

- Configuration properties

Configuration properties

The Smart Plug-in for WebSphere Application Server (WebSphere SPI) maintains a configuration that consists of property value assignments.

If you are not using the discovery process, configure all the required properties.

The table lists, in this order, required configuration properties , conditional configuration properties , and optional configuration properties . To display a description of the property, Click the property name in the table below, or use the pull-down menu at the bottom of the page. To display the descriptions of all properties based on configuration requirements (required, conditional, or optional), use the pull-down menu at the bottom of the page.

Do not use the "Back" button to navigate to any properties viewed previously. Instead, use the pull-down menu at the bottom of the page.

Property	Configuration	Automatically Discovered	Discovery	Level of Configuration	
				Default Properties	Application Server
HOME	**Required**	✓	**Required**	✓	✓
JAVA_HOME	**Required**	✓	**Required**	✓	✓
NAME	**Required**	✓	N/A		✓
PORT	**Required**	✓ *	Conditional	✓	✓
ADDRESS	Conditional		Optional		✓
ALIAS	Conditional		N/A		✓
COLLECT_METADATA	Conditional		Optional	✓	✓
JMX_CLASSPATH	Conditional		N/A	✓	✓
LOGFILE	Conditional		N/A		✓
LOGIN	**Required**		**Required**	✓	✓
PASSWORD	**Required**		**Required**	✓	✓
JMB_JAVA_HOME	**Conditional**		Optional	✓	✓
RMID_PORT	Conditional		N/A	✓	
RMID_START_TIME	Conditional		N/A	✓	

START_CMD	Conditional	N/A		✓
STOP_CMD	Conditional	N/A		✓
TYPE	Conditional	N/A	✓	✓
USER	Conditional	N/A	✓	✓
VERSION	Conditional	N/A		✓
GRAPH_SERVER	Optional	N/A	✓	
GRAPH_URL	Optional	N/A	✓	
TIMEOUT	Optional	N/A	✓	✓

Related Topics:

- The configuration

- Using the configuration editor

- Editing the Configuration File

- Example configurations

Reports and graphs

In addition to metric reports and operator-initiated graphs, the Smart Plug-in for WebSphere Application Server (WebSphere SPI) provides a limited version of HP Reporter reports and HP Performance Manager graphs. These reports and graphs show consolidated data on server performance and availability on all WebSphere application server systems.

Reports are:

- generated daily at 2 A.M.

- not available until after one full day of metric collection (the "SPI for WebSphere" folder does not appear until then).

Graphs are:

- generated at the time they are run.

- are available after installing the WebSphere SPI (the "SPI for WebSphere" folder is available), but display an error message if they are run before data has been collected.

The WebSphere SPI can be integrated with HP Reporter and HP Performance Manager (both products must be purchased separately) to provide additional reporting and graphing flexibility and capabilities.

For more information about integrating the WebSphere SPI with HP Reporter and HP Performance Manager, refer to the *HP Operations Smart Plug-in for WebSphere Application Server Installation and Configuration Guide* located on the HP Operations Smart Plug-ins DVD in the file `\Documentation\SPI Guides\WebSphere_AppServer_Install_Config.pdf` .

Related Topics:

- Tools

- Policies

HP Reporter Reports for the WebSphere SPI

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.

The following tables show all pre-defined reports.

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 or from the database per minute for the top 20 servers.	24

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 or 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
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

Data Store Details for Reports

The WebSphere SPI creates the following data store details for reports for WebSphere Application Server.

Report Name	Report Table Name *and* Data Store Class Name	Report Table Attributes	Policy Logging Data
a_wbs_availability.rpt g_wbs_availability.rpt s_wbs_availability_det ails.rpt			WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
a_wbs_ejb_meth_call_rate_top.rpt g_wbs_ejb_meth_call_rate_top.rpt			WBSSPI_High_05min
a_wbs_ejb_ent_load_str_rate_top.rpt g_wbs_ejb_ent_load_str_rate_top.rpt			WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
a_wbs_servlet_sessions_top.rpt g_wbs_servlet_sessions_top.rpt			WBSSPI_0041 WBSSPI_High_1h
a_wbs_servlet_request_top.rpt g_wbs_servlet_request_top.rpt			WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h
a_wbs_db_con_pool_tput_top.rpt g_wbs_db_con_pool_tput_top.rpt			WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
a_wbs_transaction_tput_top.rpt g_wbs_transaction_tput_top.rpt s_wbs_trans_throughput.rpt			WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
s_wbs_thread_pool_activity.rpt			WBSSPI_High_15min

s_wbs_ejb_pool_util_top.rpt			WBSSPI_0220 WBSSPI_High_1h
s_wbs_ejb_meth_call_rate_top.rpt s_wbs_ejb_resp_time_top.rpt			WBSSPI_0221 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
s_wbs_ejb_meth_call_rate_top.rpt s_wbs_ejb_resp_time_top.rpt		ID SYSTEMNAME DATETIME	WBSSPI_0222 WBSSPI_High_05min
s_wbs_ejb_pool_size_top.rpt		GMT SHIFTNAME METRICID	WBSSPI_High_05min
s_wbs_ejb_ent_load_str_rate_top.rpt	WEBSPHERE	OBJECTNAME SERVERNAME SORTID VALUE VALUEID	WBSSPI_0224 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
s_wbs_ejb_pool_miss_top.rpt			WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
a_wbs_servlet_resp_time_top.rpt g_wbs_servlet_resp_time_top.rpt s_wbs_servlet_request_rate.rpt s_wbs_servlet_resp_time.rpt			WBSSPI_0245 WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h
a_wbs_servlet_resp_time_top.rpt g_wbs_servlet_resp_time_top.rpt s_wbs_servlet_request_rate.rpt s_wbs_servlet_resp_time.rpt			WBSSPI_0246 WBSSPI_High_1h WBSSPI_Med_1h
s_wbs_db_conn_pools_size_wtime.rpt			WBSSPI_0260 WBSSPI_High_05min
s_wbs_db_conn_pools_clnwt_trate.rpt			WBSSPI_0261 WBSSPI_High_05min

s_wbs_db_conn_pools_size_wtime.rpt			WBSSPI_0262 WBSSPI_High_05min
s_wbs_db_conn_pools_tput_util.rpt			WBSSPI_0263 WBSSPI_High_05min
s_wbs_db_conn_pools_clnwt_trate.rpt			WBSSPI_0265 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min
s_wbs_db_conn_pools_tput_util.rpt			WBSSPI_0266 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min

Graphing Metrics

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.

JVM

Metric Number/Name	Metric Description
I005_JVMMemUtilPct	Percentage of heap space used in the JVM.
I807_JVMMemFreePct	Percent of JVM Free Memory available
I808_JVMCpuUsagePct	The CPU Usage of the Java virtual machine
I809_GCInterval Time	The average garbage collection value in seconds between two garbage collections

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.

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.
I810_MsgBackoutRate	The rate at which the messages failed to be delivered to the bean onMessage method (message driven beans)
I811_ReturnDiscrdRt	The rate at which the returning object was discarded because the pool was full (entity and stateless)
I814_PrdstcchdsrdRt	The rate at whch the prepared statements are discarded by the least recently used (LRU) algorithm of the statement cache

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.

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.

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.

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.
I075_TranTimeoutRt	Number of timed out global and local transactions per second.
I076_TranCommitRt	Number of global and local transactions that were committed per second.
I078_TranStartRtt	Number of global and local transactions that were begun per second.

ThreadPool

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.
I812_ThrdPoolHungRt	The rate at which the threads are declared hung
I813_CcrtThdPlHngCt	The number of concurrently hung threads

Data Store Details for Graphs

The WebSphere SPI creates the following data store details for graphs for WebSphere Application Server.

Graph Name	Policy Logging Data	Spec File	Data StoreData Class
JVM Utilization	WBSSPI_0005 WBSSPI_High_15min		
ThreadPool	WBSSPI_0013 WBSSPI_High_15min		
	WBSSPI_0014 WBSSPI_High_15min		
EJB Activity	WBSSPI_0024 WBSSPI_High_05min		
	WBSSPI_0025 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
EJB Pool	WBSSPI_0040 WBSSPI_High_1hn		
EJB Pool Size	WBSSPI_0026 WBSSPI_High_05min		
Servlet Session Activity	WBSSPI_0041 WBSSPI_High_1h		
	WBSSPI_0042 WBSSPI_High_1h WBSSPI_Med_1h		

Servlet Session Invalidations	WBSSPI_0045 WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h		
	WBSSPI_0047 WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h		
WebApplication	WBSSPI_0048 WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h		
	WBSSPI_0049 WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h		
JDBC Pool Waits	WBSSPI_0061 WBSSPI_High_05min		
	WBSSPI_0062 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
JDBC Pool Performance	WBSSPI_0065 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
	WBSSPI_0066 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
	WBSSPI_0070 WBSSPI_Med_05min WBSSPI_High_05min		

	WBSSPI_0071 WBSSPI_Med_05min WBSSPI_High_05min	wasspi_wbs_graph.sp	wasspi_wbs_graph
Transaction Duration Times	WBSSPI_0072 WBSSPI_Med_05min WBSSPI_High_05min		
	WBSSPI_0073 WBSSPI_Med_05min WBSSPI_High_05min		
	WBSSPI_0074 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
	WBSSPI_0075 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
Transaction Activity	WBSSPI_0076 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
	WBSSPI_0077 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
	WBSSPI_0078 WBSSPI_Med_05min WBSSPI_High_05min WBSSPI_Low_05min		
	WBSSPI_0807 WBSSPI_Low_15min WBSSPI_Med_15min		

JVM Utilization	WBSSPI_0808 WBSSPI_Low_15min WBSSPI_Med_15min		
	WBSSPI_0809 WBSSPI_Low_1h WBSSPI_High_1h WBSSPI_Med_1h		
EJB Activity	WBSSPI_0810 WBSSPI_Low_15min WBSSPI_Med_15min		
	WBSSPI_0811 WBSSPI_Low_15min WBSSPI_High_15min WBSSPI_Med_15min		
ThreadPool	WBSSPI_0812 WBSSPI_Low_15min WBSSPI_High_15min WBSSPI_Med_15min		
	WBSSPI_0813 WBSSPI_Low_15min WBSSPI_Med_15min WBSSPI_High_1h		
JDBC SQL Statistics	WBSSPI_0814 WBSSPI_High_15min WBSSPI_Med_15min		

Error Messages

The listed error messages result from conditions detected in the operation of the Smart Plug-in for WebSphere Application Server (WebSphere SPI), not WebSphere itself. Click on the error message number to display detailed information about that error message.

1 - 21	23 - 43	201 - 225	226 - 303
WASSPI-1	WASSPI-23	WASSPI-201	WASSPI-226
WASSPI-2	WASSPI-24	WASSPI-202	WASSPI-227
WASSPI-3	WASSPI-25	WASSPI-203	WASSPI-228
WASSPI-4	WASSPI-26	WASSPI-204	WASSPI-229
WASSPI-5	WASSPI-27	WASSPI-205	WASSPI-230
WASSPI-6	WASSPI-28	WASSPI-206	WASSPI-231
WASSPI-7	WASSPI-29	WASSPI-207	WASSPI-232
WASSPI-8	WASSPI-30	WASSPI-208	WASSPI-234
WASSPI-9	WASSPI-31	WASSPI-209	WASSPI-235
WASSPI-10	WASSPI-32	WASSPI-210	WASSPI-236
WASSPI-11	WASSPI-33	WASSPI-211	WASSPI-237
WASSPI-12	WASSPI-34	WASSPI-213	WASSPI-238
WASSPI-13	WASSPI-35	WASSPI-214	WASSPI-241
WASSPI-14	WASSPI-36	WASSPI-216	Unknown
WASSPI-15	WASSPI-37	WASSPI-218	

WASSPI-16	WASSPI-38	WASSPI-219	
WASSPI-18	WASSPI-39	WASSPI-221	
WASSPI-19	WASSPI-40	WASSPI-222	
WASSPI-20	WASSPI-41	WASSPI-223	
WASSPI-21	WASSPI-42	WASSPI-224	
WASSPI-22	WASSPI-43	WASSPI-225	

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 may 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 WebSphere SPI has been configured correctly by running the SPI Admin Verify tool. If the configuration is not correct, run the **SPI Admin ➝ Discover or Configure WBSSPI** tool. 2. Refer to the text following the error message in the WBSSPI error log to help identify the underlying cause of the problem, for example, an I/O exception. You can view the SPI error log for a managed node by using the **SPI Admin ➝ View Error File** tool. The error message can be identified by the date/time stamp.

WASSPI-3

Description	Error parsing command line
Severity	Critical
Help Text	**Probable Cause** The WebSphere SPI data collector command line is incorrectly specified in a schedule policy. **Suggested Action** 1. Refer to the text following the error message in the WBSSPI error log to help identify the underlying cause of the problem, for example an I/O exception. You can view the SPI error log for a managed node by using the **SPI Admin → View Error File** tool. The error message can be identified by the date/time stamp. 2. Correct the policy that contains the incorrect command line and redeploy. Refer to the *HP Operations Smart Plug-in for WebSphere SPI Installation and Configuration 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 WBSSPI 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. Refer to the text following the error message in the WBSSPI error log to help identify the underlying cause of the problem, for example, an I/O exception. You can view the SPI error log for a managed node by using the **SPI Admin → View Error File** tool. The error message can be identified by the date/time stamp. 2. If the UDM_DEFINITIONS_FILE property is missing from the WBSSPI configuration file, run the **SPI Admin → Discover or Configure WBSSPI** tool and set the value for this property. 3. If the problem is with the metric definitions file (`MetricDefinitions.xml`) that is shipped with the SPI for WebSphere, then reinstall the SPI for WebSphere. Run the **SPI Admin → Discover or Configure WBSSPI** tool. 4. If the problem is with a user-defined metric definitions file that is not shipped with the SPI for WebSphere, verify that this XML file adheres to the MetricDefinitions.dtd specification. Refer to the *HP Operations Smart Plug-in for WebSphere Installation and Configuration Guide* for more information on writing user-defined metrics. Reinstall your user-defined metric definition file. Run the **SPI Admin → Discover or Configure WBSSPI** tool and verify that the UDM_DEFINITIONS_FILE property in the SPI configuration, is specified correctly. 5. If the underlying error is 'ClassNotFound', this is an internal error. Report the problem 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** Refer to the text following the error message in the WBSSPI error log to help identify the underlying cause of the problem. The error messages previous to this one may also provide more information about the problem. You can view the WBSSPI error log for a managed node by using the **SPI Admin** ⟶ **View Error File** tool. The error message can be identified by the date/time stamp.

WASSPI-6

Description	Required property *<property_name>* is missing from the WBSSPI configuration.
Severity	Major
Help Text	**Probable Cause** The specified required property is missing from the WBSSPI configuration file. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct server information for the WebSphere servers on this managed node. 2. Verify the property is specified correctly in the WBSSPI configuration file (`/var/opt/OV/conf/wbsspi/SiteConfig` on UNIX platforms or `\%OvAgentDir%\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. **SPI Admin → View Error File** tool. Verify that you have specified the correct server name and port information for the WebSphere servers on this managed node. 2. Verify that the properties, SERVERx_NAME and SERVERx_PORT, are specified correctly in the WBSSPI configuration file (`/var/opt/OV/conf/wbsspi/SiteConfig` on UNIX platforms or `\%OvAgentDir%\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** 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. Refer to 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 **SPI Admin → View Error File** tool . The error message can be identified by the date/time stamp. 2. Identify the steps to reproduce the problem. 3. Run the **SPI Admin → Start Tracing** tool to turn on tracing. Try to reproduce the problem. 4. Run the **SPI Admin → Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-9

Description	Unable to retrieve property *<property_name>*
Severity	Critical
Help Text	**Probable Cause** A required property is missing from one of the WebSphere SPI configuration files. **Suggested Action** 1. Refer to the text following the error message in the WebSphere SPI error log to help identify the missing property. You can view the SPI error log for a managed node by using the **SPI Admin → View Error File** tool . The error message can be identified by the date/time stamp. 2. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct information for the WebSphere servers on the managed node in question. 3. Verify that the missing property is now specified in the WBSSPI configuration file (`/var/opt/OV/conf/wbsspi/SiteConfig` on UNIX platforms or `\%OvAgentDir%\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. Refer to the text following the error message in the WebSphere SPI error log to help identify the file in question and the underlying cause of the problem. You can view the SPI error log for a managed node by using the **SPI Admin → View Error File** tool. The error message can be identified by the date/time stamp. 2. Verify that you have enough disk space to create temporary files.

WASSPI-11

Description	No servers have been specified in the WebSphere SPI configuration file.
Severity	Critical
Help Text	**Probable Cause** The number of WebSphere servers specified in the WBSSPI configuration file for the managed node in question is 0. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct server name and port information for the WebSphere servers on this managed node. 2. Verify that the property, NUM_SERVERS, in the WBSSPI configuration file (`/var/opt/OV/conf/wbsspi/SiteConfig` on UNIX platforms or `\%OvAgentDir%\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 an error exit code *\<exit code>*
Severity	Critical
Help Text	**Probable Cause** A command started by the WBSSPI collector has returned an error (non-zero) exit code. **Suggested Action** 1. Identify the steps to reproduce the problem. 2. Run the **SPI Admin → Start Tracing** tool to turn on tracing. 3. Reproduce the problem. 4. Run the **SPI Admin → Stop Tracing** tool to turn off tracing. 5. Run the **SPI Admin → Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-13

Description	Exception occurred while running an 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 SPI data collector could not be found. **Suggested Action** 1. Refer to the text following the error message in the WebSphere SPI error log to help identify the file in question and the underlying cause of the problem. You can view the SPI error log for a managed node by using the **SPI Admin → View Error File** tool. The error message can be identified by the date/time stamp. 2. **SPI Admin → View Error File** tool on this managed node.

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. Refer to 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 **SPI Admin → View Error File** tool. The error message can be identified by the date/time stamp. 2. If the XML document was provided by the user, correct the document. Refer to the *SPI for WebSphere Installation and Configuration Guide* for more information on writing user-defined metrics. 3. If the XML document is a document that is shipped with the WBSSPI, run the **SPI Admin → Discover or Configure WBSSPI** tool to reinstall the WBSSPI 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. Refer to the *HP OPerations Smart Plug-in for WebSphere Installation and 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 Admin → Discover or Configure WBSSPI** tool to reinstall the WBSSPI configuration files.

WASSPI-18

Description	Data logging failed: ddflog returned error *<error_number>* .
Severity	Critical
Help Text	**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. Run the **SPI Admin** → **Start Tracing** tool to turn on tracing. Try to reproduce the problem. 3. Run the **SPI Admin** → **Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-19

Description	Encountered problem instantiating XSLT transformer with *\<file_name\>*
Severity	Major
Help Text	**Probable Cause** The XSL document that specifies the auto action report output contains errors. **Suggested Action** Run the **SPI Admin** → **Discover or Configure WBSSPI** tool with the managed node selected.

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** Run the **SPI Admin → Discover or Configure WBSSPI** tool with the managed node selected.

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 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. **Suggested Action** : NA

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. Refer to the text following the error message in the WBSSPI 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 **SPI Admin ➞ View Error File** tool. The error message can be identified by the date/time stamp. 2. Identify the steps to reproduce the problem. 3. Run the **SPI Admin ➞ Start Tracing** tool to turn on tracing. Try to reproduce the problem. 4. Run the **SPI Admin ➞ Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-24

Description	Error logging in to server *<server_name>* with login *<login>*
Severity	Critical
Help Text	**Probable Cause** A security exception occurred while logging in to the specified server. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool on the managed node on which the error occurred and verify that you have specified the correct login and password properties. 2. Verify 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 the 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. Refer to the text following the error message in the WBSSPI 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 **SPI Admin** ‑‑► **View Error File** tool. The error message can be identified by the date/time stamp. 2. Identify the steps to reproduce the problem. 3. Run the **SPI Admin** ‑‑► **Start Tracing** tool to turn on tracing. Try to reproduce the problem. 4. Run the **SPI Admin** ‑‑► **Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-28

Description	RMID on port *\<port>* has been *\<status>* .
Severity	Normal

WASSPI-29

Description	Collector server *<server id>* for Java home *<path>* has been started.
Severity	Normal

WASSPI-30

Description	Failed to start *<rmid_path>* on port *<port>* .
Severity	Critical
Help Text	**Probable Cause** The specified port is already in use. **Suggested Action** Run the **SPI Admin ⇀ Discover or Configure WBSSPI** tool. Set the RMID_PORT property to a port number which is not currently in use.

WASSPI-31

Description	Lost connection to RMI collector while processing *<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 element(s) define FromVersion and ToVersion tags which do not match the **Suggested Action** If the action is valid on the server, then either adjust the JMXAction definition's FromV 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 elemer **Suggested Action** Correct the action -m option if an incorrect metric ID was specified, otherwise add a JM

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 error log to determine the root cause which is logged followin

WASSPI-36

Description	MBean *<JMX objectname>* on server *<server name>* , does not expose operation *<ope*
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 *<attri*
Severity	Warning
Help Text	**Probable Cause** An action's JMXCalls element defines a write attribute exposed by the specified MBean **Suggested Action** If it's a custom MBean, update the MBean's management interface so the attribute is wri JMXCalls element.

WASSPI-38

Description	MBean *<JMX objectname>* on server *<server name>* , does not expose attribute *<attri*
Severity	Warning
Help Text	**Probable Cause** An action's JMXCalls element defines an attribute not exposed by the specified MBean **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 **Suggested Action** View the managed node's errorlog to determine the root cause which is logged following

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 ma **Suggested Action** View the managed node's errorlog to determine the root cause which is logged following

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 **Suggested Action** View the managed node's errorlog to determine the root cause which is logged following

WASSPI-42

Description	Error running command *<command>* .
Severity	Critical
Help Text	**Probable Cause** A command started by the WBSSPI collector reported an error. **Suggested Action** 1. Identify the steps to reproduce the problem. 2. Run the **SPI Admin → Start Tracing** tool to turn on tracing. 3. Reproduce the problem. 4. Run the **SPI Admin → Stop Tracing** tool to turn off tracing. 5. Run the **SPI Admin → Self-Healing Info** tool. Contact HP support with the infori

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 errorlog to determine the root cause which is logged following

WASSPI-201

Description	File *<filename>* not found
Severity	Critical
Help Text	**Probable Cause** A configuration file could not be found. **Suggested Action** Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that the correct information has been 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** 1. A file could not be opened or it could not be found. 2. Permissions may be incorrect or a directory may be corrupt. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct information for the WebSphere servers on the managed node on which the error occurred. 2. Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-203

Description	Cannot write file *<filename>*
Severity	Critical
Help Text	**Probable Cause** Permissions may be incorrect, or a file or directory may be corrupt. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that the correct information has been specified for the WebSphere servers on the managed node on which the error occurred. 2. Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-204

Description	Error sending opcmsg *<message>*
Severity	Critical
Help Text	**Probable Cause** There was a problem running opcmsg. 'opcmsg' may be missing or not have permissions to execute (HPOM installation errors) or the system process table may be full. **Suggested Action** Confirm that the WBSSPI-Messages policy has been deployed on the managed node.

WASSPI-205

Description	Error sending opcmon *<command>*
Severity	Critical
Help Text	**Probable Cause** There was a problem running opcmon. 'opcmon' may be missing or not have permissions to execute (HPOM installation errors) or the system process table may be full. **Suggested Action** Confirm that HPOM 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 HP Operations agent user from reading it or the directory is corrupt. **Suggested Action** Verify that the permissions are correct for the HP Operations agent 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 HP Operations agent user. 2. Verify that there is enough disk space to create files. 3. Run the **SPI Admin → Discover or Configure WBSSPI** tool.

WASSPI-208

Description	The SPI must be configured before it can be used
Severity	Critical
Help Text	**Probable Cause** The SPI has not been configured on this node. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct information for the WebSphere servers on the managed node on which the error occurred. 2. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct information for the WebSphere servers on the managed node on which the error occurred.

WASSPI-209

Description	Cannot contact WebSphere server
Severity	Critical
Help Text	**Probable Cause** 1. The server could be down or not responding. 2. The SPI may be configured incorrectly. **Suggested Action** 1. Verify that WebSphere is up and running properly. 2. Run the **SPI Admin → Discover or Configure WBSSPI** tool. 3. Run the **SPI Admin → Verify** tool on the managed node to confirm that the SPI has been successfully configured.

WASSPI-210

Description	Cannot configure the SPI
Severity	Critical
Help Text	**Probable Cause** The SPI configuration process failed. **Suggested Action** 1. Refer to 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 will provide more information about the problem. You can view the SPI error log for a managed node by using the **SPI Admin ⇒ View Error File** tool. The error message can be identified by the date/time stamp. 2. Run the **SPI Admin ⇒ Discover or Configure WBSSPI** tool.

WASSPI-211

Description	Cannot create directory *\<directory\>*
Severity	Critical
Help Text	**Probable Cause** There are insufficient permissions for the HP Operations agent user to create the directory or there is insufficient disk space. **Suggested Action** 1. Verify that the permissions are correct for the HP Operations agent user for this directory. 2. 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 may be missing, permissions may be incorrect, the process table may be full. **Suggested Action** 1. Verify that the file exists. If it is a SPI program and the file is missing, run the Run the **SPI Admin** ➞ **Discover or Configure WBSSPI** tool with the managed node selected. 2. Verify that the permissions are correct for the HP Operations agent user.

WASSPI-216

Description	Configuration variable *<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 **SPI Admin → Discover or Configure WBSSPI** tool. 2. Verify that the correct information has been specified in the configuration for the managed node on which the error occurred.

WASSPI-218

Description	WebSphere monitoring has been turned OFF for *<server_name>*
Severity	Warning
Help Text	**Probable Cause** Collection has been turned off for the specified server. **Suggested Action** If desired, collection can be turned on by running the **SPI Admin ➞ Start Monitoring** tool.

WASSPI-219

Description	WebSphere monitoring has been turned ON for *<server_name>*
Severity	Critical
Help Text	**Probable Cause** Collection has been turned on for the specified server **Suggested Action** If desired, collection can be turned off by running the **SPI Admin → Stop Monitoring** tool.

WASSPI-221

Description	*<file_name>* does not exist
Severity	Critical
Help Text	**Probable Cause** The specified file does not exist. If it is a log file, no entries have ever been logged to it. If it is a property file, then 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 **SPI Admin** ➞ **Discover or Configure WBSSPI** tool. Property files: Run the **SPI Admin** ➞ **Discover or Configure WBSSPI** tool.

WASSPI-222

Description	*<file_name>* is empty
Severity	Critical
Help Text	**Probable Cause** The specified file is empty. If it is a log file, no entries have ever been logged to it, or the entries have been cleaned out. If it is a property file, then it is not properly configured. **Suggested Action** If the file is a configuration file, run the **SPI Admin** → **Discover or Configure WBSSPI** tool.

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 may be incorrect or a directory may be corrupt. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. Verify that you have specified the correct information for the WebSphere servers on the managed node on which the error occurred. 2. Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-224

Description	ddfcomp returned an error configuring *<name>*
Severity	Warning
Help Text	**Probable Cause** ddfcomp returned an error. This could be because neither OVPA nor CODA is installed on the system or because an error occurred while configuring the performance agent. **Suggested Action** 1. If the performance agent is not installed, this error can be ignored. 2. Otherwise, identify the steps to reproduce the problem. 3. Run the **SPI Admin → Start Tracing** tool to turn on tracing. Try to reproduce the problem. 4. Run the **SPI Admin → Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-225

Description	No logfiles were found. Did you run 'Discover or Configure WBSSPI'?
Severity	Critical
Help Text	**Probable Cause** The logfile list is empty. **Suggested Action** Run the **SPI Admin → Discover or Configure WBSSPI** tool.

WASSPI-226

Description	Cannot read file *<file_name>*
Severity	Critical
Help Text	**Probable Cause** 1. A file could not be opened or it could not be found. 2. Permissions may be incorrect or a directory may be corrupt. **Suggested Action** 1. Run the **SPI Admin → Discover or Configure WBSSPI** tool. 2. Verify that you have specified the correct information for the WebSphere servers on the managed node on which the error occurred. 3. Verify that the permissions are correct for the HP Operations agent user to read this file.

WASSPI-227

Description	No Operations performance agent is installed. Data source will not be configured.
Severity	Warning
Help Text	**Probable Cause** If an Operations performance tool is available, the SPI will integrate with it. This warning indicates that none is available. **Suggested Action** If you should 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 *<datasource>* : *<message>*
Severity	Critical
Help Text	**Probable Cause** ddflog returned an error. This could be because the SPI was not properly configured to support logging performance data. **Suggested Action** 1. Redeploy SPI for WebSphere and SPI Data Collector instrumentation on the node having the problem. 2. Otherwise, examine the system error message, if any, for clues to the problem. 3. Run the **SPI Admin → Start Tracing** tool to turn on tracing. Try to reproduce the problem. 4. Run the **SPI Admin → Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

WASSPI-229

Description	Cannot connect to directory *<directory-name>*
Severity	Critical
Help Text	**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** Run the **SPI Admin → Discover or Configure WBSSPI** tool.

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. Also could be 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 or running Java (the core of the SPI collector is written in Java). This could be that the specified JVM does not exist, or that the collector had some error. • The JAVA_HOME variable in the SPI configuration is not set correctly. **Suggested Action** Check for other errors generated at the same time, they may indicate the real cause. If the specified file does not exist, check your JAVA_HOME or HOME variables in the SPI configuration.

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 file. The collector only knows about servers listed in the configuration file. **Suggested Action** 1. Specify a correct server name on the command line. 2. Run the **SPI Admin → Discover or Configure WBSSPI** tool. 3. Verify the WebSphere server names are correctly listed and spelled in the SPI configuration. Note that the server name is case-sensitive.

WASSPI-234

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

WASSPI-235

Description	Restart of PA agent failed
Severity	Warning
Help Text	**Probable Cause** The SPI attempted to automatically restart the PA agent and the automatic attempt failed. **Suggested Action** Restart the PA agent manually with 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, the UDM XML is translated. This message indicated that 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	**Probable Cause** This is an informational message that an HP Performance Manager or PA datasource was setup.

WASSPI-238

Description	No User Defined Metrics found
Severity	Warning
Help Text	**Probable Cause** The **JMX Metric Builder → WBSSPI → UDM Graph Enable** tool was run, but no UDM metrics had been defined. **Suggested Action** Run the **SPI Admin → Discover or Configure WBSSPI** tool and check that the UDM XML file (UDM_DEFINITIONS_FILE property) has been named correctly.

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 may be that the protection of the file is set so that the HP Operations agent 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-303

Description	WBSSPI Configuration on the Server Updated.
Severity	Normal
Help Text	**Probable Cause** : NA **Potential Impact** : NA **Suggested Action** : NA

WASSPI-501

Description	Retrieving configuration data from the HPOM server
Severity	Normal
Help Text	This is a normal operation performed by the WBSSPI Discovery policy. The entry in the *A* (Action) column of the Active Messages view should change from *R* (running) to *S* (Success). If the entry in this column changes to *F* (Fail), the discovery operation cannot be completed successfully. Run the **SPI Admin → Discover or Configure WBSSPI** tool again and select this node when the tool is launched. If problem persists, select the *Help on HP Operations* option from the Help menu. The section titled *Smart Plug-in for WebSphere* provides instructions on how to use the **SPI Admin → Discover or Configure WBSSPI** tool to manually configure the SPI for WebSphere.

WASSPI-502

Description	Updating the WBSSPI configuration data with discovered information
Severity	Normal
Help Text	This is a normal operation performed by the WBSSPI Discovery policy. The entry in the *A* (Action) column of the Active Messages view should change from *R* (running) to *S* (Success). If the entry in this column changes to *F* (Fail), the discovery operation cannot be completed successfully. Run the **SPI Admin → Discover or Configure WBSSPI** tool again and select this node when the tool is launched. If problem persists, select the *Help on HP Operations* option from the Help menu. The section titled *Smart Plug-in for WebSphere* provides instructions on how to use the **SPI Admin → Discover or Configure WBSSPI** tool to manually configure the SPI for WebSphere.

WASSPI-503

Description	SPI configuration on the management server has been updated by the Auto-Discovery.
Help Text	**Probable Cause** : NA **Potential Impact** : NA **Suggested Action** : NA

WASSPI-541

Description	No application server found
Severity	Major
Help Text	**Probable Cause** WebSphere AdminServer 4.0 is not running on the node. **Potential Impact** : NA **Suggested Action** • Verify that the WebSphere 4.0 AdminServer is running by launching the administrative console on the node. If the administrative console fails to launch, start the WebSphere 4.0 AdminServer. Run the Discover or Configure WBSSPI tool again and select this node when the tool is launched. • Launch the **SPI Admin → Discover or Configure WBSSPI** tool from the HP Operations console and select the node from the list. 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:** A WebSphere 4.0 AdminServer is identified by the port number it uses. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, verify that the correct information is entered for each specific instance of the AdminServer in the WebSphere SPI configuration file.

WASSPI-561

Description	WBS Admin Server Error
Severity	Critical
Help Text	**Probable Cause** WebSphere Application Server versions 4: Unsuccessful login to the secured WebSphere environment. **Potential Impact** : NA **Suggested Action** • Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD variables (properties) for this node are present and valid in the WBSSPI configurations. Using the 'SPI Admin->Discover or Configure WBSSPI' Tool from the HP Operations Operations console, verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. • Launch the **SPI Admin → Discover or Configure WBSSPI** tool from the HP Operations Operations console and select the node from the list. 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:** A WebSphere 4.0 AdminServer is identified by the port number it uses. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, verify that the correct information is entered for each specific instance of the AdminServer in the WebSphere SPI configuration file. If the suggested solutions fail and the problem persists, contact your HP Operations representative for assistance.

WASSPI-562

Description	Security access failure. Missing or invalid LOGIN/PASSWORD parameter for the WebSphere AdminServer on port: *<port_number >*
Severity	Critical
Help Text	**Probable Cause** • WebSphere Application Server versions 4: The values for the LOGIN and PASSWORD variables (properties) for this node are missing from the WBSSPI configurations, or incorrect information was entered. **Potential Impact** : NA **Suggested Action** • Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD variables (properties) for this node are present and valid in the WBSSPI configurations. Using the **SPI Admin → Discover or Configure WBSSPI** tool from the HP Operations console, verify the accuracy of the information. The PASSWORD information is encrypted for security purposes. • Launch the **SPI Admin → Discover or Configure WBSSPI** tool from the HP Operations Operations console and select the node from the list. 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:** > A WebSphere 4.0 AdminServer is identified by the port number it uses. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, verify that the correct information is entered for each specific instance of the AdminServer in the WebSphere SPI configuration file. • If the suggested action does not fix the problem, contact your HP support representative.

WASSPI-563

Description	Security access failure. Invalid LOGIN/PASSWORD parameter for the WebSphere AdminServer on port: *<port_number >*
Severity	Critical
Help Text	**Probable Cause** • WebSphere Application Server versions 4: The LOGIN and PASSWORD properties for this node are missing from the WebSphere SPI configuration file or are incorrect. **Potential Impact** : NA **Suggested Action** • Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD variables (properties) for this node are present and valid in the WBSSPI configurations. Using the **SPI Admin ⟶ Discover or Configure WBSSPI** tool from the HP Operations Operations console, verify the LOGIN and PASSWORD information for the node. The PASSWORD information is encrypted for security purposes. • Launch the **SPI Admin ⟶ Discover or Configure WBSSPI** tool from the HP Operations console and select the node from the list. 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:** A WebSphere 4.0 AdminServer is identified by the port number it uses. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, verify that the correct information is entered for each specific instance of the AdminServer in the WebSphere SPI configuration file. • If the suggested action does not fix the problem, contact your HP support representative.

WASSPI-564

Description	Security access failure. Unable to communicate with the WebSphere AdminServer on port: *<port_number >*
Severity	Critical
Help Text	**Probable Cause** • WebSphere AdminServer 4.0 is not running on the node. • The LOGIN and PASSWORD properties for this node are missing from the WebSphere SPI configuration file or are incorrect. **Potential Impact** : NA **Suggested Action** • Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD variables (properties) for this node are present and valid in the WBSSPI configurations. Using the **SPI Admin → Discover or Configure WBSSPI** tool from the HP Operations Operations console, verify the LOGIN and PASSWORD information for the node. The PASSWORD information is encrypted for security purposes. • Launch the **SPI Admin → Discover or Configure WBSSPI** tool from the HP Operations console and select the node from the list. 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:** A WebSphere AdminServer is identified by the port number it uses. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, verify that the correct information is entered for each specific instance of the AdminServer in the WebSphere SPI configuration file. If the suggested actions do not fix the problem, contact your HP support representative.

WASSPI-565

Description	Security access failure. Unable to login to the WebSphere AdminServer on port: *<port_number >*
Severity	Critical

Help Text	**Probable Cause**
	
	WebSphere Application Server versions 4: The LOGIN and PASSWORD properties for this node are missing from the WebSphere SPI configuration file or are incorrect.
	
	Potential Impact : NA
	
	Suggested Action
	
	• Launch the WebSphere administrative console on the node and check if security is enabled. Also make sure that the LOGIN and PASSWORD variables (properties) for this node are present and valid in the WBSSPI configurations. Using the **SPI Admin** ⇀ **Discover or Configure WBSSPI** tool from the HP Operations Operations console, verify the LOGIN and PASSWORD information for the node. The PASSWORD information is encrypted for security purposes.
	
	• Launch the **SPI Admin** ⇀ **Discover or Configure WBSSPI** tool from the HP Operations console and select the node from the list. 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:**
	    A WebSphere 4.0 AdminServer is identified by the port number it uses. If the port number is not the default value (port 900) or if multiple instances of the AdminServer are present, verify that the correct information is entered for each specific instance of the AdminServer in the WebSphere SPI configuration file.
	
	• If the suggested action does not fix the problem, contact your HP support representative.

WASSPI-571

Description	Failed to Communicate with WebSphere 5 Application Server.
Help Text	**Probable Cause** : NA **Potential Impact** : NA **Suggested Action** : 1. Create or start one or more application servers on the node. Select the node and rur tool again. Make sure that all of the application servers you want to monitor are running, befo **Admin → Discover or Configure WBSSPI** tool is launched. Only the servers tha *WebSphere Application Server versions 5* : Unsuccessful login to the secured Web *Verification* : Launch the WebSphere administrative console on the node and chec and PASSWORD variables (properties) for this node are present and valid in the V **Discover or Configure WBSSPI** tool and verify the accuracy of the information. ' purposes. 2. Run the **SPI Admin → Discover or Configure WBSSPI** tool and select the node properties for the node (overwrite the existing encrypted data). Allow the WBSSPI ⓘ **NOTE:** If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere Guide* . The chapter called Configuring the WebSphere SPI provides instructions on hc

WASSPI-572

Description	WebSphere 5 Login Error - Missing Login Data
Help Text	**Probable Cause** : *WebSphere Application Server versions 5* The values for the LOGIN and PASSWORD variables (properties) for this node are mis *Verification:* Launch the WebSphere administrative console on the node and check if security is enab variables (properties) for this node are present and valid in the WBSSPI configurations. **WBSSPI** tool and verify the accuracy of the information. The PASSWORD informatio **Potential Impact** : NA **Suggested Action** : Run the **SPI Admin** ⟶ **Discover or Configure WBSSPI** tool and select the node from for the node (overwrite the existing encrypted data). Allow the WBSSPI Discovery proc **ⓘ NOTE:** If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere* *Guide* . The chapter called Configuring the WebSphere SPI provides instructions on hc

WASSPI-573

Description	WebSphere 5 Login Error - Invalid Login Data
Help Text	**Probable Cause** : *WebSphere Application Server versions 5* The discovery tool was unable to authenticate itself in a secured WebSphere server envi LOGIN and PASSWORD variables (properties) being provided in the WBSSPI configu *Verification:* Launch the WebSphere administrative console on the node and check if security is enab variables (properties) for this node are present and valid in the WBSSPI configurations. **WBSSPI** tool and verify the accuracy of the information. The PASSWORD information **Potential Impact** : NA **Suggested Action** : Run the **SPI Admin → Discover or Configure WBSSPI** tool and select the node from for the node (overwrite the existing encrypted data). Allow the WBSSPI Discovery proc **NOTE:** If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere* *Guide* . The chapter called Configuring the WebSphere SPI provides instructions on ho

WASSPI-581

Description	Internal Error - Discovery fails to initialize: *<error_message >*
Severity	Critical
Help Text	**Probable Cause** Read the [Error Message] that accompanies the message text to determine the cause of the problem. The **SPI Admin ⇢ Discover or Configure WBSSPI** tool may not function properly due to one (or more) of the following conditions on the managed node: • A **SPI Admin ⇢ Discover or Configure WBSSPI** tool, script, or data file is missing, has been removed, or is placed in non-standard directory paths. • There were problems with the Operations agent installation. • The Operations agents installation directory cannot be determined. • Operations operator account that runs the **SPI Admin ⇢ Discover or Configure WBSSPI** tool does not have the permission to open/read the specified file or execute the required script/command. • General network errors. **Potential Impact** : NA **Suggested Action** • Check with the IT specialist in the organization on matters related to these issues. After the problems have been resolved, run the **SPI Admin ⇢ Discover or Configure WBSSPI** tool again and select this node when the tool is launched. • Select the Help on HP Operations option from the Help menu. The section titled Smart Plug-in for WebSphere provides instructions on how to use the **SPI Admin ⇢ Discover or Configure WBSSPI** tool to manually configure the SPI for WebSphere. • If the suggested solutions fail and the problem persists, contact your HP Operations representative for assistance.

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 **SPI Admin → Discover or Configure WBSSPI** tool may not function properly due to one (or more) of the following conditions on the managed node:
	
	   ○ Operating system commands used by **SPI Admin → Discover or Configure WBSSPI** tool are missing, have been removed, or are placed in non-standard directory paths.
	
	   ○ The system's PATH variable has not been set for certain system commands.
	
	   ○ Required operating system file(s) or software installation registry cannot be found or is in a non-standard directory path.
	
	   ○ Operations operator account that runs the **SPI Admin → Discover or Configure WBSSPI** tool does not have the permission to open/read system files or execute the necessary system commands.
	
	   ○ General network errors.
	
	Potential Impact : NA
	
	Suggested Action
	
	Check with the Operations or the IT specialist in the organization on matters related to these issues. After the problems have been resolved, select the node and run the **SPI Admin → Discover or Configure WBSSPI** tool again.
	
	NOTE:
	If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere Application Server Installation and Configuration Guide* . The chapter called Configuring the WebSphere SPI provides instructions on how to manually configure the WebSphere SPI.

WASSPI-591

Description	WBSSPI Discovery - 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 **SPI Admin → Discover or Configure WBSSPI** tool may not function properly due to one (or more) of the following conditions on the managed node:
	
	   ○ Operating system commands used by **SPI Admin → Discover or Configure WBSSPI** tool are missing, have been removed, or are placed in non-standard directory paths.
	
	   ○ Operations operator account that runs the **SPI Admin → Discover or Configure WBSSPI** tool does not have the permission to open/read system files or execute the necessary system commands.
	
	Potential Impact : NA
	
	Suggested Action
	
	Check with the Operations or the WebSphere application server specialist in the organization on matters related to these issues. After the problems have been resolved, select the node and run the **SPI Admin → Discover or Configure WBSSPI** tool again.
	
	--- 	
	NOTE:
	If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere Application Server Installation and Configuration Guide* . The chapter called Configuring the WebSphere SPI provides instructions on how to manually configure the WebSphere SPI.

All Other Errors

Description	An unknown error appears in the WebSphere SPI error log
Severity	Warning
Help Text	**Suggested Action** 1. Refer to the text following the error message in the WBSSPI error log to help identify the problem. You can view the SPI error log for a managed node by using the **SPI Admin → View Error File** tool. The error message can be identified by the date/time stamp. 2. Identify the steps to reproduce the problem. 3. Run the **SPI Admin → Start Tracing** tool to turn on tracing. Try to reproduce the problem. 4. Run the **SPI Admin → Self-Healing Info** tool. Contact HP support with the information gathered by this tool.

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: