HP Operations Smart Plug-in for IBM WebSphere Application Server

For HP Operations Manager for Windows®

Software Version: 6.10

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.

Document Release Date: February 2009

Software Release Date: October 2008

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

Unknown	232

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 Configuration Guide* located on HP Operations Smart Plug-ins DVD in the file `\Documentation\SPI Guides\WebSphere_AppServer_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. 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. 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.

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 WebSphere SPI reporting tools to generate metric reports. In addition, you can generate graphs that show 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

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).

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-0005.1: % of heap space used (<$VALUE> <$NAME>] WBSSPI-0005.2: % of heap space used (<$VALUE> <$NAME>]
Instruction Text	Probable Cause : The JVM is running out of availab Potential Impact : N/A Suggested action : Open the Performance Tuner W Performance Tuner from the Administrative Console. *Java Virtual Machine (JVM) Heap Size* The Java Virtual Machine (JVM) Heap Size settings ir you increase the heap size, garbage collection occur settings depend strongly on your application and on Consider: ■ whether the JVM Heap for the selected applicatio application server JVM Heaps on the same machi ■ specifying JVM Heaps to reside in physical memo ■ setting the starting JVM Heap Size to one quarter ■ setting the maximum JVM Heap Size to the follow the machine:

	• 128 MB, for small systems with less than 1 GB • 256 MB, for systems with 2 GB of memory • 512 MB, for larger systems NOTE: A value of 0, or blank, indicates that no when initializing the JVM. On OS/400, the JVM Hea 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 milliseconds.
Impact	Medium
PMI Module	servletSessionsModule
Severity: Condition with Threshold	WBSSPI-0040.1: Warning threshold, 1000
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0040.1: Ave. servlet session lifetime (< (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average servlet session l Potential Impact : N/A Suggested action : Web Containers To route servlet requests from the Web server to a transport queue between the Web server plug- *Web container maximum thread size* Short description: Use the maximum thread size connections to use for the communications chan container. Each connection represents a request How to see or set: 1. In the administrative console, select the ap the Services tab. 2. Click Web Container Service and then click 3. In the Web Container Service window, click 4. Specify the value in the Maximum Thread S 5. Click Apply after returning to the Services 6. Stop and restart the application server.

	Default value: 50 NOTE: For Linux systems, the recommende Related parameters: See Adjusting WebSphere's Cache Size *URL invocation cache* Short description: The Invocation Cache holds in resources. A cache of the requested size is creat threads/processes is determined by the Web con Consider the following when increasing this cach A larger cache uses more of the Java heap, so yo heap size. For example, if each cache entry requ and the URL Invocation cache size is 100; then 5 When to try adjusting: If you have more than 50 page is a unique URL), increase this parameter. How to see or set: Specify the size of the cache parameters by: 1. In the administrative console, click the app 2. Click the JVM Setting tab. 3. On the same panel, click Add in the Systen 4. Add the name -DinvocationCacheSize and a 5. Click Apply to ensure that the changes are 6. Stop and restart the application server. Default value: 50
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-0041.1: # of sessions currently being a (>=<$THRESHOLD>) [Policy: <$NAME>]
Instruction Text	Probable Cause : The number of sessions curr threshold value. Potential Impact : N/A Suggested action : Web Containers To route servlet requests from the Web server t a transport queue between the Web server plug *Web container maximum thread size* Short description: Use the maximum thread siz connections to use for the communications char container. Each connection represents a reques How to see or set: 1. In the administrative console, select the a the Services tab. 2. Click Web Container Service and then clic 3. In the Web Container Service window, clic 4. Specify the value in the Maximum Thread 5. Click Apply after returning to the Services

	6. Stop and restart the application server. Default value: 50 NOTE: For Linux systems, the recommend Related parameters: See Adjusting WebSphere' Cache Size *URL invocation cache* Short description: The Invocation Cache holds i servlet resources. A cache of the requested size number of threads/processes is determined by setting. Consider the following when increasing this cacl A larger cache uses more of the Java heap, so y Java heap size. For example, if each cache entr 25, and the URL Invocation cache size is 100; tl When to try adjusting: If you have more than 5 page is a unique URL), increase this parameter. How to see or set: Specify the size of the cache JDK parameters by: 1. In the administrative console, click the ap 2. Click the JVM Setting tab. 3. On the same panel, click Add in the Syste 4. Add the name -DinvocationCacheSize and 5. Click Apply to ensure that the changes are 6. Stop and restart the application server. Default value: 50
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 second
Impact	Low
PMI Module	servletSessionsModule
Severity: Condition with Threshold	WBSSPI-0042.1: Warning threshold, 10000
Collection Interval	1h
Message Group	WebSphere
Message Text	WBSSPI-0042.1: # of sessions timed out per sec (>=<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	Probable Cause : The number of sessions being threshold value. Potentail Impact : N/A Suggested action: Web Containers To route servlet requests from the Web server to a transport queue between the Web server plug- *Web container maximum thread size* Short description: Use the maximum thread size connections to use for the communications chan container. Each connection represents a request How to see or set: 1. In the administrative console, select the ap the Services tab. 2. Click Web Container Service and then click 3. In the Web Container Service window, clicl 4. Specify the value in the Maximum Thread S 5. Click Apply after returning to the Services

	6. Stop and restart the application server. Default value: 50  NOTE: For Linux systems, the recommende Related parameters: See Adjusting WebSphere's Cache Size *URL invocation cache* Short description: The Invocation Cache holds in servlet resources. A cache of the requested size number of threads/processes is determined by t setting. Consider the following when increasing this cach A larger cache uses more of the Java heap, so yo heap size. For example, if each cache entry requ and the URL Invocation cache size is 100; then 5 When to try adjusting: If you have more than 50 page is a unique URL), increase this parameter. How to see or set: Specify the size of the cache parameters by: 1. In the administrative console, click the app 2. Click the JVM Setting tab. 3. On the same panel, click Add in the Syster 4. Add the name -DinvocationCacheSize and 5. Click Apply to ensure that the changes are 6. Stop and restart the application server. Default value: 50
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-0212.1: % of threads used (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0212.2: % of threads used (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0212.3: % of threads used (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	Probable Cause : The percent of threads in use in a pool has exceeded a threshold value Potential Impact : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. Web Container Pool Update the pool size within the normal range by adjusting the slider. Edit the numeric field to update the pool size within, or outside the normal range. Think about

	specifying the maximum number of Web container threads less than the number of connections accepted by the Web server. Consider setting the Web container maximum threads number significantly smaller than the number of connections accepted by the Web server, for a site with many static pages returned directly by the Web server. ORB Properties You can tune the following object request broker properties: ■ *Pass by Reference* : This option can provide better performance. Select Pass by Reference, only if appropriate for your application. Selecting this option can break remote transparency, since you can modify objects passed to an EJB method. Know your application before using this option. ■ *ORB Threads Pool Size* : A thread is needed for each EJB request. Enterprise beans are typically invoked from servlets in another JVM, using RMI/IIOP and remote EJB client applications, using RMI/IIOP. The ORB thread pool size should accommodate both request sources.
Report Type	ASCII
Area	Performance

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-0213.1: % of time # of threads reached configured maximum (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	Probable Cause : The percent of threads in use in a pool has exceeded a threshold value Potential Impact : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. Web Container Pool Update the pool size within the normal range by adjusting the slider. Edit the numeric field to update the pool size within, or outside the normal range. Think about specifying the maximum number of Web container threads less than the number of connections accepted by the Web server. Consider setting the Web container maximum threads number significantly smaller than the number of connections accepted by the Web server, for a site with many static pages returned directly by the Web server.

	ORB Properties You can tune the following object request broker properties: ■ *Pass by Reference* : This option can provide better performance. Select Pass by Reference, only if appropriate for your application. Selecting this option can break remote transparency, since you can modify objects passed to an EJB method. Know your application before using this option. ■ *ORB Threads Pool Size* : A thread is needed for each EJB request. Enterprise beans are typically invoked from servlets in another JVM, using RMI/IIOP and remote EJB client applications, using RMI/IIOP. The ORB thread pool size should accommodate both request sources.
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-0220.1: % of EJBs in the pool in use (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	Probable Cause : The utilization of the EJB cache has exceeded a threshold value. Potential Impact : N/A Suggested action : EJB Container *Object Request Broker thread pool size* Short description: Size of the thread pool. How to see or set: 1. In the administrative console, click the appropriate application server. 2. Click the Services tab. 3. Select Object Request Broker and then Edit Properties. The thread pool size is on the General Properties panel. *Cache settings* Short description: To determine a rough approximation of the cache absolute limit, multiply the number of enterprise beans active in any given transaction by the total number of concurrent transactions expected. Then add the number of active session

	bean instances. Use the Resource Analyzer to view bean performance information. How to see or set: Edit the EJB container service properties for the application server you are tuning. Default value: ■ Cache Size = 2047 ■ Cache preferred limit = 2000 ■ Cache clean-up interval = 1000 *Deployment descriptors* Short description: When creating deployment descriptors for your entity beans, pay close attention to the beans' functions and define your descriptors accordingly. When it is appropriate for the requirements of an application, set an entity bean's method to read-only in the deployment descriptor. How to see or set: Setting an entity bean's method to read-only can be done both in VisualAge for Java and in the Application Assembly Tool (AAT). In the AAT, within the methods extensions of the bean, set the access intent to 'read.' For each enterprise bean, the commit options are configured using the "Activate at" and "Load at" settings: ■ Commit Option A (exclusive database access) This option improves performance by caching entity bean data in memory. It requires that the EJB container has exclusive access to the database used by the bean (and therefore, the only copy of a bean's persistent state), or that the bean's data is accessed as read-only at all times. For this option, use "Activate at Once" and "Load at Activation" settings. ■ Commit Option B (shared database access) This option reloads the bean state from the database at the beginning of each transaction. If an enterprise bean contains a significant number of calls to the enterprise bean, "Activate" function, using option B is beneficial, because the required object is already in the cache. Otherwise, this option does not provide significant benefit over option A. For this option, use the "Activate at Once" and "Load at Transaction" settings. ■ Commit Option C (shared database access) Entity beans are not cached across transactions. This is the default and is necessary whenever the database is shared with other processes or EJB containers. To configure this option, use the "Activate at Transaction" and either "Load at Transaction" or "Load at Activation" settings.
Report Type	ASCII
Area	EJB

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-0221.1: Ave. EJB response time (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0221.2: Ave. EJB response time (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>
Instruction Text	Probable Cause : The average response time of an EJB has exceeded a threshold value. Potential Impact : N/A Suggested action : EJB Container *Object Request Broker thread pool size* Short description: Size of the thread pool. How to see or set: 1. In the administrative console, click the appropriate application server. 2. Click the Services tab. 3. Select Object Request Broker and then Edit Properties. The thread pool size is on the General Properties panel. *Cache settings*

	Short description: To determine a rough approximation of the cache absolute limit, multiply the number of enterprise beans active in any given transaction by the total number of concurrent transactions expected. Then add the number of active session bean instances. Use the Resource Analyzer to view bean performance information. How to see or set: Edit the EJB container service properties for the application server you are tuning. Default value: ■ Cache Size = 2047 ■ Cache preferred limit = 2000 ■ Cache clean-up interval = 1000 *Deployment descriptors* Short description: When creating deployment descriptors for your entity beans, pay close attention to the beans' functions and define your descriptors accordingly. When it is appropriate for the requirements of an application, set an entity bean's method to read-only in the deployment descriptor. How to see or set: Setting an entity bean's method to read-only can be done both in VisualAge for Java and in the Application Assembly Tool (AAT). In the AAT, within the methods extensions of the bean, set the access intent to 'read.' For each enterprise bean, the commit options are configured using the "Activate at" and "Load at" settings: ■ Commit Option A (exclusive database access) This option improves performance by caching entity bean data in memory. It requires that the EJB container has exclusive access to the database used by the bean (and therefore, the only copy of a bean's persistent state), or that the bean's data is accessed as read-only at all times. For this option, use "Activate at Once" and "Load at Activation" settings. ■ Commit Option B (shared database access) This option reloads the bean state from the database at the beginning of each transaction. If an enterprise bean contains a significant number of calls to the enterprise bean, "Activate" function, using option B is beneficial, because the required object is already in the cache. Otherwise, this option does not provide significant benefit over option A. For this option, use the "Activate at Once" and "Load at Transaction" settings. ■ Commit Option C (shared database access) Entity beans are not cached across transactions. This is the default and is necessary whenever the database is shared with other processes or EJB containers. To configure this option, use the "Activate at Transaction" and either "Load at Transaction" or "Load at Activation" settings.
Report Type	ASCII
Area	EJB

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-0222.1: # of EJB method calls per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$NAME>]
Instruction Text	Probable Cause : The number of EJB method calls per minute has exceeded a threshold value. Potential Impact : N/A Suggested action : EJB Container *Object Request Broker thread pool size* Short description: Size of the thread pool. How to see or set: 1. In the administrative console, click the appropriate application server. 2. Click the Services tab. 3. Select Object Request Broker and then Edit Properties. The thread pool size is on the General Properties panel. *Cache settings* Short description: To determine a rough approximation of the cache absolute limit, multiply the number of enterprise beans active in any given transaction by the total

	number of concurrent transactions expected. Then add the number of active session bean instances. Use the Resource Analyzer to view bean performance information. How to see or set: Edit the EJB container service properties for the application server you are tuning. Default value: ■ Cache Size = 2047 ■ Cache preferred limit = 2000 ■ Cache clean-up interval = 1000 *Deployment descriptors* Short description: When creating deployment descriptors for your entity beans, pay close attention to the beans' functions and define your descriptors accordingly. When it is appropriate for the requirements of an application, set an entity bean's method to read-only in the deployment descriptor. How to see or set: Setting an entity bean's method to read-only can be done both in VisualAge for Java and in the Application Assembly Tool (AAT). In the AAT, within the methods extensions of the bean, set the access intent to 'read.' For each enterprise bean, the commit options are configured using the "Activate at" and "Load at" settings: ■ Commit Option A (exclusive database access) This option improves performance by caching entity bean data in memory. It requires that the EJB container has exclusive access to the database used by the bean (and therefore, the only copy of a bean's persistent state), or that the bean's data is accessed as read-only at all times. For this option, use "Activate at Once" and "Load at Activation" settings. ■ Commit Option B (shared database access) This option reloads the bean state from the database at the beginning of each transaction. If an enterprise bean contains a significant number of calls to the enterprise bean, "Activate" function, using option B is beneficial, because the required object is already in the cache. Otherwise, this option does not provide significant benefit over option A. For this option, use the "Activate at Once" and "Load at Transaction" settings. ■ Commit Option C (shared database access) Entity beans are not cached across transactions. This is the default and is necessary whenever the database is shared with other processes or EJB containers. To configure this option, use the "Activate at Transaction" and either "Load at Transaction" or "Load at Activation" settings.
Report Type	ASCII
Area	EJB

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-0224.1: # of times EJB data was written to or loaded from the database per minute (<$VALUE>/min) too high (>=<$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 : N/A Suggested action : EJB Container *Object Request Broker thread pool size* Short description: Size of the thread pool. How to see or set: 1. In the administrative console, click the appropriate application server. 2. Click the Services tab. 3. Select Object Request Broker and then Edit Properties. The thread pool size is on the General Properties panel. *Cache settings* Short description: To determine a rough approximation of the cache absolute limit,

	multiply the number of enterprise beans active in any given transaction by the total number of concurrent transactions expected. Then add the number of active session bean instances. Use the Resource Analyzer to view bean performance information. How to see or set: Edit the EJB container service properties for the application server you are tuning. Default value: ■ Cache Size = 2047 ■ Cache preferred limit = 2000 ■ Cache clean-up interval = 1000 *Deployment descriptors* Short description: When creating deployment descriptors for your entity beans, pay close attention to the beans' functions and define your descriptors accordingly. When it is appropriate for the requirements of an application, set an entity bean's method to read-only in the deployment descriptor. How to see or set: Setting an entity bean's method to read-only can be done both in VisualAge for Java and in the Application Assembly Tool (AAT). In the AAT, within the methods extensions of the bean, set the access intent to 'read.' For each enterprise bean, the commit options are configured using the "Activate at" and "Load at" settings: ■ Commit Option A (exclusive database access) This option improves performance by caching entity bean data in memory. It requires that the EJB container has exclusive access to the database used by the bean (and therefore, the only copy of a bean's persistent state), or that the bean's data is accessed as read-only at all times. For this option, use "Activate at Once" and "Load at Activation" settings. ■ Commit Option B (shared database access) This option reloads the bean state from the database at the beginning of each transaction. If an enterprise bean contains a significant number of calls to the enterprise bean, "Activate" function, using option B is beneficial, because the required object is already in the cache. Otherwise, this option does not provide significant benefit over option A. For this option, use the "Activate at Once" and "Load at Transaction" settings. ■ Commit Option C (shared database access) Entity beans are not cached across transactions. This is the default and is necessary whenever the database is shared with other processes or EJB containers. To configure this option, use the "Activate at Transaction" and either "Load at Transaction" or "Load at Activation" settings.
Report Type	ASCII
Area	EJB

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-0246.1: Ave. response time for a web application servlet (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0246.2: Ave. response time for a web application servlet (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average response time for servlet in msec has exceeded a threshold value. Potential Impact : N/A Suggested action : *Web Applications* You can also set parameters specific to each Web application you deploy. The settings can affect performance. *Servlet Reload Interval and Reloading Enabled* Short description: WebSphere Application Server offers an auto reload capability. The default automatically reloads servlets in the Web application when the class files

	change. The auto reload capability can simplify the testing and management of your Web site's applications by enabling you to quickly modify your site without restarting the WebSphere Application Server. (Be sure that your Reload Interval is short). However, this ability to reload servlets dynamically and the associated polling affects performance negatively. When the application's resources (such as servlets and enterprise beans) are fully deployed, it is not as necessary to aggressively reload these resources as during development. When to try adjusting: When you are in a stable production mode, you need to either set a long Reload Interval or disable Reloading. For a production system, it is common to reload resources only a few times a day. How to see or set: The Reload Interval and Reloading Enabled can be set for your application by using the Application Assembler from the administrative console. When creating a new Web module, these parameters can be configured by selecting the IBM Extensions and 1. Unchecking the Reloading Enabled box. 2. Updating the Reload Interval field. Default value: Reload Interval = three seconds Reloading Enabled=true
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-0247.1: # of errors for a web application servlet per second (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	Probable Cause : The number of errors in a servlet per second has exceeded a threshold value. Potential Impact : N/A Suggested action : *Web Applications* You can also set parameters specific to each Web application you deploy. The settings can affect performance. *Servlet Reload Interval and Reloading Enabled* Short description: WebSphere Application Server offers an auto reload capability. The default automatically reloads servlets in the Web application when the class files change. The auto reload capability can simplify the testing and management of your Web site's applications by enabling you to quickly modify your site without restarting the WebSphere Application Server. (Be sure that your Reload Interval is short). However,

	this ability to reload servlets dynamically and the associated polling affects performance negatively. When the application's resources (such as servlets and enterprise beans) are fully deployed, it is not as necessary to aggressively reload these resources as during development. When to try adjusting: When you are in a stable production mode, you need to either set a long Reload Interval or disable Reloading. For a production system, it is common to reload resources only a few times a day. How to see or set: The Reload Interval and Reloading Enabled can be set for your application by using the Application Assembler from the administrative console. When creating a new Web module, these parameters can be configured by selecting the IBM Extensions and 1. Unchecking the Reloading Enabled box. 2. Updating the Reload Interval field. Default value: Reload Interval = three seconds Reloading Enabled=true
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-0261.1: Ave. # of threads waiting for a connection from connection pools (<$VALUE>) too high (>=<$THRESHOLD>) [Policy: <$NAME>] WBSSPI-0261.2: Ave. # of threads waiting for a connection from connection pools (<$VALUE>) too high (>=<$THRESHOLD>) [Policy: <$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 : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than

	the Web container maximum threads, if only a small percentage of servlet requests use these database connections. *Prepared Statement Cache Size* Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
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-0262.1: Ave. time a client waited for a connection (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>] WBSSPI-0262.2: Ave. time a client waited for a connection (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average time that a client waited for a connection in has exceeded a threshold value. Potential Impact : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than the Web container maximum threads, if only a small percentage of servlet requests

	use these database connections. *Prepared Statement Cache Size* Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
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-0263.1: % utilization of a connection pool (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0263.1: % utilization of a connection pool (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>]
Instruction Text	Probable Cause : The percent utilization of the connection pool has exceeded a threshold value. Potential Impact : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than the Web container maximum threads, if only a small percentage of servlet requests

	use these database connections. *Prepared Statement Cache Size* Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
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-0264.1: % of time all connections in a pool are in use (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$NAME>] WBSSPI-0264.2: % of time all connections in a pool are in use (<$VALUE>%) too high (>=<$THRESHOLD>%) [Policy: <$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 : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than the Web container maximum threads, if only a small percentage of servlet requests

	use these database connections. *Prepared Statement Cache Size* Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
Report Type	ASCII
Area	JDBC

Metric I265_JDBCConnPoolTimeoutRt

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-0265.1: # of times a client timed out waiting for a connection per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$NAME>] WBSSPI-0265.2: # of times a client timed out waiting for a connection per minute (<$VALUE>/min) too high (>=<$THRESHOLD>/min) [Policy: <$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 : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than

	the Web container maximum threads, if only a small percentage of servlet requests use these database connections. *Prepared Statement Cache Size* Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
Report Type	ASCII
Area	JDBC

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
Configure WBSSPI	Configure the WebSphere SPI.
Create WBSSPI Node Groups	Create WebSphere SPI node groups based on discovered services.
Discover WebSphere	Configure required WebSphere SPI properties and deploy the WebSphere SPI Discovery policies.
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

Configure WBSSPI

Configure WBSSPI tool launches the WebSphere SPI configuration editor using which you can view, edit, and set configuration properties .

If you are configuring the WebSphere SPI for the first time, use the Discover WebSphere tool to automatically set basic configuration properties. Refer to the *HP Operations Smart Plug-in for WebSphere Application Server Configuration Guide* located on the HP Operations Smart Plug-ins DVD in the file `\Documentation\SPI Guides\WebSphere_AppServer_Config.pdf` for complete instructions on how to configure WebSphere SPI.

Function

Configure WBSSPI does the following:

- 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 log files and WebSphere SPI error log file for monitoring.

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.

If a specific HPOM managed node is selected when this tool is launched, changes to the configuration affecting any WebSphere servers on that managed node are automatically saved on that managed node.

If no managed nodes are selected when this tool is launched, changes to the configuration are *not* saved on any managed nodes.

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 Configure WBSSPI tool

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

2. Double-click Configure WBSSPI .
3. Select the managed nodes to configure.
4. Click Launch . The "Console Status" window opens. Wait a few second for the "Introduction" window to open. Read the contents of the "Introduction" window.
5. Click Next . The configuration editor appears.
6. Set the configuration properties . Refer to Using the configuration editor for more information about how to use the configuration editor to set the properties.
7. Optionally, click Save to save any changes made to the configuration. After you save your changes, you cannot automatically undo them.
8. Click Finish or Next to save changes and exit the editor.

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

   NOTE:
   If you click Cancel but have saved your changes to the configuration, those changes remain in the configuration.

9. Check the "Console Status" window for error messages. If none appear, click Close .
10. If you have added an application server or added/edited one or more of the following properties:
    - HOME
    - PORT

    run Discover WebSphere on the managed nodes on which the application server/properties were added or edited. Running Discover WebSphere updates the service map.

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 4.0).
- Places all HPOM managed nodes running WebSphere 4.0 in the WebSphere 4.0 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:

    - Started/Starting - The tool is running.

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

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

Discover WebSphere

Discover WebSphere tool launches the configuration editor (allowing you to configure WebSphere SPI by setting initial configuration properties) and then deploys the Discovery group policies on the selected managed nodes.

Refer to the *HP Operations Smart Plug-in for WebSphere Application Server Configuration Guide* located on the HP Operations Smart Plug-ins DVD in the file `\Documentation\SPI Guides\WebSphere_AppServer_Config.pdf` for complete instructions on how to configure WebSphere SPI.

Function

Discover WebSphere does the following:

- Updates the configuration on the HPOM management server and selected managed nodes.
- Deploys the Discovery group policies to the 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 WebSphere tool

1. From the HPOM console, select Tools → SPI for WebSphere → SPI Admin .
2. Double-click Discover WebSphere .
3. Select the managed nodes to configure.
4. Click Launch . The "Console Status" window opens. After a few seconds the "Introduction" window opens. This window contains brief information about the Discover WebSphere tool.

5. Click Next . A second "Introduction" window opens. This window displays instructions about how to enter the WebSphere login and password information.
6. Click Next . If you have not set the LOGIN and PASSWORD properties, the "Set Access Info for Default Properties" window opens.

   If you have already set the LOGIN and PASSWORD properties, the configuration editor opens. Go to step 8.

   If security is not enabled on WebSphere, leave these fields blank, click Next , and go to step 10.

   If security is enabled on WebSphere, enter the WebSphere Admin Server username and password.

   Set LOGIN and PASSWORD in this window if the WebSphere administration username and password are the same for all instances of WebSphere on the managed nodes (the LOGIN and PASSWORD properties are set at the global properties level), click Next , and go to step 10.

   If the WebSphere administration username and password are different for each managed node, then you must set LOGIN and PASSWORD at the NODE level using the configuration editor. Select Customize .
7. From the configuration editor, set the configuration properties. Refer to Using the configuration editor for more information about how to use the configuration editor.
8. Click Next to save changes and exit the editor. The "Confirm Operation" window opens.
9. Click OK . The discovery policies are deployed.

   NOTE:
   If you select Cancel, the discovery policies are not deployed. However, if you made changes to the configuration, those changes remain in the configuration on the management server. To make the changes to the selected managed nodes' configuration, you must start the Configure WBSSPI tool, select those managed nodes, and then exit the tool.

10. Check the "Console Status" window for error messages. If none appear, click Close .

Self-Healing Info

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

Function

Self-Healing Info appliaction 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 or Stop Tracing tools allow you to start or stop gathering tracing information for the collection of metrics. Run this tool only when instructed by your HP support representative.

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 information about the collection of metrics into a file.

Stop Tracing does the following:

- Stops saving information about the collection of metrics.

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

Verify tool allows you to verify if WebSphere SPI is configured correctly on the managed node.

Function

Verify does the following:

- on UNIX managed nodes:
- on Windows managed nodes:

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

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

b. Double-click Verify .

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

d. Click Launch . The "Tool Status" window opens.

e. 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.

f. 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) or C:\Program Files\HP OpenView\Installed Packages\{790C06B4-844E-11D2-972B-080009EF8C2A} (for DCE 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 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:
   - Started/Starting - The tool is running.
   - 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

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:

- 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.
- 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.
- 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

Logfiles

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-Logfile-Monitor	Collects information from the WebSphere log file(s).
WBSSPI Error Log	Monitors the WebSphere SPI error log and sends the error messages to the message browser.
WebSphere Activity Log	Monitors the WebSphere activity log file.
WebSphere Logs	Detects critical errors and warnings in the WebSphere log file.

Related Topics:

- Metrics
- Monitors
- Policies
- Metric Naming/Numbering Conventions
- Metrics by Number
- Metrics Overhead

WBSSPI-Logfile-Monitor

Description	Collects information from the WebSphere's log file(s).
Polling Interval	2m
Help Text	N/A

WBSSPI Error 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

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 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.

Metrics

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
3	I003_AdminServerStat	Status of the Admin server	L	A	Critical	Availability
4	I004_AdminServerStatusRep	Status of the Admin 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

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

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_JDBCConnPoolTimeoutRt	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:

- Metric Naming/Numbering Conventions
- Metric Overhead
- Metrics by Number
- Monitors
- Logfiles

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-0001.1: Server status is down [Policy: <$NAME>]
Instruction Text	Probable Cause : NA Potential Impact : NA Suggested Action : NA
Report Type	N/A
Area	Availability

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 dow
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 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 I013_ThreadPoolPctMax

Policy Name	N/A--Used for reporting (HP Reporter) or
Metric Name	I013_ThreadPoolPctMax
Metric Type	Graphing
Description	Percentage of time Number of threads in
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 Manag
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 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

Metric I024_EJBEntDataLdStRt

Policy Name	N/A—Used for graphing (HP Performance Manage
Metric Name	I024_EJBEntDataLdStRt
Metric Type	Graphing and Reporting
Description	Number of times an EJB was written to or loaded
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 Manager) o
Metric Name	I025_EJBPoolMissPct
Metric Type	Graphing
Description	Average Percentage of time a call to retrieve an EJB
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 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

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-0026.1: Ave. # of bean objects in the pool [Policy: <$NAME>]
Instruction Text	Probable Cause : The average number of bean ob value. Potential Impact : N/A Suggested action : EJB Container *Object Request Broker thread pool size* Short description: Size of the thread pool. How to see or set: 1. In the administrative console, click the appro 2. Click the Services tab. 3. Select Object Request Broker and then Edit Pr General Properties panel. *Cache settings* Short description: To determine a rough approxima number of enterprise beans active in any given tran transactions expected. Then add the number of acti

	Use the Resource Analyzer to view bean performanc How to see or set: Edit the EJB container service properties for the app Default value: ■ Cache Size = 2047 ■ Cache preferred limit = 2000 ■ Cache clean-up interval = 1000 *Deployment descriptors* Short description: When creating deployment descr attention to the beans' functions and define your de for the requirements of an application, set an entity deployment descriptor. How to see or set: Setting an entity bean's method for Java and in the Application Assembly Tool (AAT) of the bean, set the access intent to 'read.' For each enterprise bean, the commit options are c At" settings: ■ Commit Option A (exclusive database access) Th entity bean data in memory. It requires that the database used by the bean (and therefore, the o the bean's data is accessed as read-only at all ti and "Load at Activation" settings. ■ Commit Option B (shared database access) This database at the beginning of each transaction. If number of calls to the enterprise bean, "Activate because the required object is already in the cac significant benefit over option A. For this option, Transaction" settings. ■ Commit Option C (shared database access) Entit This is the default and is necessary whenever the EJB containers. To configure this option, use the Transaction" or "Load at Activation" settings.
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 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-0245.1: Ave. request rate for a web application servlet (<$VALUE>/sec) too high (>=<$THRESHOLD>/sec) [Policy: <$NAME>]
Instruction Text	Probable Cause : The number of requests for a servlet per second has exceeded a threshold value. Potential Impact : N/A Suggested action : *Web Applications* You can also set parameters specific to each Web application you deploy. The settings can affect performance. *Servlet Reload Interval and Reloading Enabled* Short description: WebSphere Application Server offers an auto reload capability. The default automatically reloads servlets in the Web application when the class files change. The auto reload capability can simplify the testing and management of your Web site's

	applications by enabling you to quickly modify your site without restarting the WebSphere Application Server. (Be sure that your Reload Interval is short). However, this ability to reload servlets dynamically and the associated polling affects performance negatively. When the application's resources (such as servlets and enterprise beans) are fully deployed, it is not as necessary to aggressively reload these resources as during development. When to try adjusting: When you are in a stable production mode, you need to either set a long Reload Interval or disable Reloading. For a production system, it is common to reload resources only a few times a day. How to see or set: The Reload Interval and Reloading Enabled can be set for your application by using the Application Assembler from the administrative console. When creating a new Web module, these parameters can be configured by selecting the IBM Extensions and 1. Unchecking the Reloading Enabled box. 2. Updating the Reload Interval field. Default value: Reload Interval = three seconds Reloading Enabled=true
Report Type	ASCII
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 Manager) on
Metric Name	I048_WebAppServLoad
Metric Type	Alarming and Graphing
Description	Number of servlets currently loaded for a web applicat
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-0048.1: # of servlets currently loaded for a w (>=<$THRESHOLD>) [Policy: <$NAME>]
Instruction Text	Probable Cause : The number of servlets currently lo threshold value. Potential Impact : N/A Suggested action : *Web Applications* You can also set parameters specific to each Web appl performance. *Servlet Reload Interval and Reloading Enabled* Short description: WebSphere Application Server offer automatically reloads servlets in the Web application w The auto reload capability can simplify the testing and by enabling you to quickly modify your site without res (Be sure that your Reload Interval is short). However, the associated polling affects performance negatively. servlets and enterprise beans) are fully deployed, it is resources as during development. When to try adjusting: When you are in a stable produ

	Reload Interval or disable Reloading. For a production a few times a day. How to see or set: The Reload Interval and Reloading Enabled can be set Assembler from the administrative console. When crea can be configured by selecting the IBM Extensions and 1. Unchecking the Reloading Enabled box. 2. Updating the Reload Interval field. Default value: Reload Interval = three seconds Reload
Report Type	ASCII
Area	Web Applications

Metric I049_WebAppServRelRt

Policy Name	N/A—Used for graphing (HP Performance Manager)
Metric Name	I049_WebAppServRelRt
Metric Type	Graphing
Description	Number of servlets reloaded for a web application
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 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-0260.1: Ave. # of connections in the connection pool (<$VALUE>) too high (>=<$THRESHOLD>) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average number of connections in the connection pool has exceeded a threshold value. Potential Impact : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than the Web container maximum threads, if only a small percentage of servlet requests use these database connections. *Prepared Statement Cache Size*

	Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
Report Type	ASCII
Area	JDBC

Metric I061_JDBCConPoolWait

Policy Name	N/A—Used for graphing (HP Performance Manage
Metric Name	I061_JDBCConPoolWait
Metric Type	Graphing
Description	Average Number of threads waiting for a connect
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 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-0266.1: # of connections allocated and returned by applications (<$VALUE>/sec) too high (>=<$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 : N/A Suggested action : Open the Performance Tuner Wizard by clicking Console → Wizards → Performance Tuner from the Administrative Console. *Connection Pool Size* Each data source contains a pool of connections to the corresponding database. An upper bound for your application comes from the sum of the number of Web container threads and ORB threads. The servlet contribution to the connection pool size can be significantly smaller than the Web container maximum threads, if only a small percentage of servlet requests use these database connections.

	Prepared Statement Cache Size Make your prepared statement cache large enough for all prepared statements, by setting the cache size to the product of: The number of SQL prepared statements in your application The maximum number of configured data source connections *Database: (DB2 Only)* This panel is only available for DB2 databases. Tune the database after this wizard has completed, by selecting Tune database and entering the DB2 SYSADM ID and password. If you provided a cataloged database alias name when configuring the data source and this alias name differs from the real database name, enter the real database name in the field provided. After you select database tuning and complete the remaining panels, click Finish on the Summary panel. The tuning wizard then calls the DB2SmartGuide API, to tune the DB2 database associated with the data source. Stop and restart the database instance, for the DB2SmartGuide changes to take effect. NOTE: DB2SmartGuide tuning works better if the database is already populated. It is not necessary or recommended to tune the repository database (WAS). Before tuning a database, you might want to use the DB2 DBA utility to back up (db2cfexp) the database configuration. If the tuning fails, you can then restore (db2cfimp) your database configuration. You can also use: DB2 RESET DATABASE CONFIGURATION for database-name to restore the database to default values DB2 RESET DATABASE MANAGER CONFIGURATION to restore the DBM to default values The database being tuned must reside on a DB2 Server at Version 7.2.1, or higher. This tuning option is not available in DB2 servers for OS/390, OS/400, VM or VSE.
Report Type	ASCII
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-0070.1: Ave. duration of a global transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average duration of global transactions has exceeded a threshold value. Potential Impact : N/A 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-0071.1: Ave. duration of a local transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average duration of local transactions has exceeded a threshold value. Potential Impact : N/A 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-0072.1: Ave. duration of a commit for a global transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average duration of commits for global transactions has exceeded a threshold value. Potential Impact : N/A 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-0073.1: Ave. duration of a commit for a local transaction (<$VALUE>ms) too high (>=<$THRESHOLD>ms) [Policy: <$NAME>]
Instruction Text	Probable Cause : The average duration of commits for local transactions has exceeded a threshold value. Potential Impact : N/A 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 I074_TranRollbackRt

Policy Name	WBSSPI_0074
Metric Name	I074_TranRollbackRt
Metric Type	Alarming and Graphing
Description	Number per second of global and local transactions rolled back.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0074.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0074.1: # of global and local transactions rolled back (<$VALUE>/sec) too high (>=<$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 : N/A 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 per second of timed out global and local transactions.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0075.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0075.1: # of global and local transactions that timed out <$VALUE>/sec) too high (>=<$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 : N/A 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 I076_TranCommitRt

Policy Name	WBSSPI_0076
Metric Name	I076_TranCommitRt
Metric Type	Alarming and Graphing
Description	Number per second of global and local transactions that were committed.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0076.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0076.1: # of global and local transactions that were committed (<$VALUE>/sec) too high (>=<$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 : N/A 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 per second of global and local transactions that were committed.
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 per second of global and local transactions that were started.
Impact	Low
PMI Module	transactionModule
Severity: Condition with Threshold	WBSSPI-0078.1: Warning threshold, 1000
Collection Interval	5m
Message Group	WebSphere
Message Text	WBSSPI-0078.1: # of global and local transactions that were begun (<$VALUE>/sec) too high (>=<$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 : N/A 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

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-*X* 0-High-05min	5m	1-4, 22, 24, 26, 61-2, 65-6, 70-6, 78, 221-5, 260-6
	WBSSPI-*X* 0-High-15m	14m	5, 13-4, 210-3
	WBSSPI-*X* 0-High-1h	59m	20 40-2, 45, 47-9, 220, 245-7
Medium	WBSSPI-*X* 0-Medium-05m	5m	1-4, 22, 24, 62, 65-6, 72-6, 78, 221-2, 224-5, 262, 265-6
	WBSSPI-*X* 0-Medium-15m	14m	5, 14
	WBSSPI-*X* 0-Medium-1h	59m	40, 42, 45, 47-9, 245-7
Low	WBSSPI-*X* 0-Low-05m	5m	1-4, 22, 24, 65-6, 74-6, 78, 222, 224-5, 265
	WBSSPI-*X* 0-Low-15m	14m	5, 14
	WBSSPI-*X* 0-Low-1h	59m	42, 45, 47-9, 245, 247

where *X* represents the version of the WebSphere server (for example, WBSSPI-50-Low-1h is the collector policy name for WebSphere version 5).

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
- Metric Naming/Numbering Conventions
- Metrics Overhead
- Metrics by Number

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 both by the Configure WBSSPI and Discover WebSphere tools.

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 nod e

<*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.

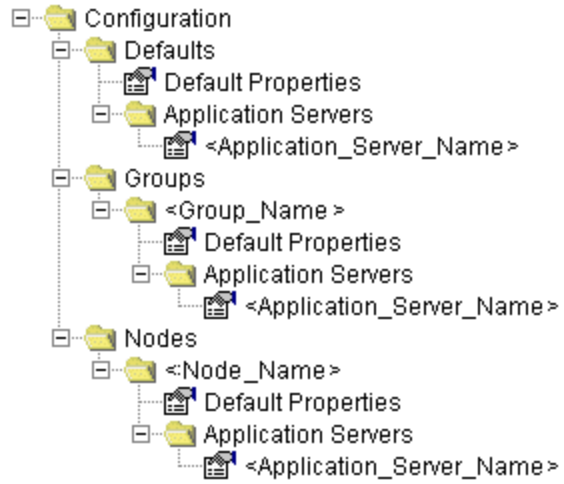
The configuration editor has three components:

- The configuration editor tree

  The Configure WBSSPI Tree, displayed in the left pane of the 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 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 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 Configure WBSSPI:

Button	Description
Cancel	Exit 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 Configure WBSSPI. Appears instead of the Next button if you launched Configure WBSSPI without selecting any nodes.
Next	Exit Configure WBSSPI. Takes you to the "Confirm Operation" window that lists the nodes you selected when 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 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

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.

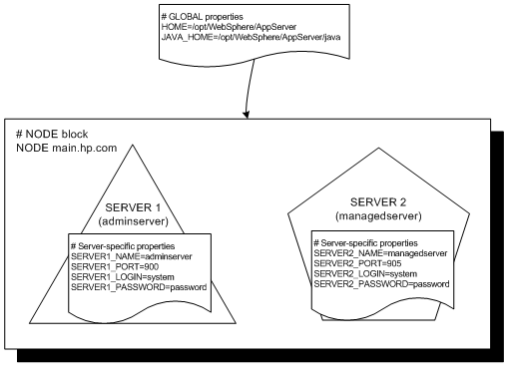
This sample configuration would be displayed at the Defaults level by selecting the View Configuration Settings tab .

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.

NOTE:
The discovery policy (if deployed) automatically updates the service map and WebSphere SPI configuration. Set the AUTO_DISCOVER property to "false" if you do not want the discovery policy to automatically overwrite this configuration information (unselect the AUTO_DISCOVER check box if you are using the configuration editor).

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	✓	Conditional	✓	✓
JAVA_HOME	Required	✓	N/A	✓	✓
NAME	Required	✓	N/A		✓
PORT	Required	✓ *	Conditional	✓	✓
ADDRESS	Conditional		Optional		✓
ALIAS	Conditional		N/A		✓
AUTO_DISCOVER	Conditional		N/A	✓	✓
COLLECT_METADATA	Conditional		Optional	✓	✓
HOME_LIST	Conditional		N/A	✓	

JMX_CLASSPATH	Conditional	N/A	✓	✓
LOGFILE	Conditional	N/A		✓
LOGIN	Conditional	Conditional	✓	✓
PASSWORD	Conditional	Conditional	✓	✓
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	✓	
MAX_ERROR_LOG_SIZE	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 WebSphere SPI (the "SPI for WebSphere" folder is available), but display an error message if they are run before data has been collected.

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

Related Topics:

- Tools
- Policies

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	501+
WASSPI-1	WASSPI-23	WASSPI-201	WASSPI-226	WASSPI-501
WASSPI-2	WASSPI-24	WASSPI-202	WASSPI-227	WASSPI-502
WASSPI-3	WASSPI-25	WASSPI-203	WASSPI-228	WASSPI-503
WASSPI-4	WASSPI-26	WASSPI-204	WASSPI-229	WASSPI-541
WASSPI-5	WASSPI-27	WASSPI-205	WASSPI-230	WASSPI-561
WASSPI-6	WASSPI-28	WASSPI-206	WASSPI-231	WASSPI-562
WASSPI-7	WASSPI-29	WASSPI-207	WASSPI-232	WASSPI-563
WASSPI-8	WASSPI-30	WASSPI-208	WASSPI-234	WASSPI-564
WASSPI-9	WASSPI-31	WASSPI-209	WASSPI-235	WASSPI-565
WASSPI-10	WASSPI-32	WASSPI-210	WASSPI-236	WASSPI-571
WASSPI-11	WASSPI-33	WASSPI-211	WASSPI-237	WASSPI-572
WASSPI-12	WASSPI-34	WASSPI-213	WASSPI-238	WASSPI-573
WASSPI-13	WASSPI-35	WASSPI-214	WASSPI-241	WASSPI-581
WASSPI-14	WASSPI-36	WASSPI-216	WASSPI-303	WASSPI-585
WASSPI-15	WASSPI-37	WASSPI-218		WASSPI-591

WASSPI-16	WASSPI-38	WASSPI-219		Unknown
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-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. Potential Impact : NA 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. Potential Impact : NA 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 → 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, e.g. 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 template. Potential Impact : NA 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 *WebSphere SPI 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. Potential Impact : NA 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 → 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 → 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 *SPI for WebSphere Configuration Guide* for more information on writing user-defined metrics. Reinstall your user-defined metric definition file. Run the SPI Admin → 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. Potential Impact : NA 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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 → 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. Potential Impact : NA 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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 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 → 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. Potential Impact : NA Suggested Action 1. If the metric is specified in an XML document that was provided by the user, correct the document. Refer to the *SPI for WebSphere 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 → 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. Potential Impact : NA 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. Potential Impact : NA Suggested Action Run the SPI Admin → 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. Potential Impact : NA Suggested Action Run the SPI Admin → 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. Potential Impact : NA 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-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*> . Potential Impact : NA 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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*> . Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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
Help Text	Probable Cause : NA Potential Impact : NA Suggested Action : NA

WASSPI-29

Description	Collector server <*server id*> for Java home <*path*> has been started.
Severity	Normal
Help Text	Probable Cause : NA Potential Impact : NA Suggested Action : NA

WASSPI-30

Description	Failed to start <*rmid_path*> on port <*port*> .
Severity	Critical
Help Text	Probable Cause The specified port is already in use. Potential Impact : NA Suggested Action Run the SPI Admin → 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
Help Text	Probable Cause : NA Potential Impact : NA Suggested Action : NA

WASSPI-32

Description	Unable to retrieve metadata for MBean <*JMX-ObjectName*> .
Severity	Warning
Help Text	Probable Cause : NA Potential Impact : NA Suggested Action : NA

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 server Potential Impact : NA Suggested Action If the action is valid on the server, then either adjust the JMXAction definition's FromVersion/

WASSPI-34

Description	Metric <*metric id*> does not define any actions.
Severity	Warning
Help Text	Probable Cause The metric ID specified with the action -m option does not define a JMXActions element. Potential Impact : NA Suggested Action Correct the action -m option if an incorrect metric ID was specified, otherwise add a JMXActi

WASSPI-35

Description	Error executing action <*action command-line*> .
Severity	Major
Help Text	Probable Cause An unexpected error occurred while executing the action. Potential Impact : NA Suggested Action View the managed node's error log to determine the root cause which is logged following the

WASSPI-36

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

WASSPI-37

Description	MBean <*JMX objectname*> on server <*server name*> , does not expose attribute <*attribute r*
Severity	Warning
Help Text	Probable Cause An action's JMXCalls element defines a write attribute exposed by the specified MBean as rea Potential Impact : NA Suggested Action If it's a custom MBean, update the MBean's management interface so the attribute is writable JMXCalls element.

WASSPI-38

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

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 manage Potential Impact : NA Suggested Action View the managed node's errorlog to determine the root cause which is logged following the

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 mana Potential Impact : NA Suggested Action View the managed node's errorlog to determine the root cause which is logged following the

WASSPI-42

Description	Error running command <*command*> .
Severity	Critical
Help Text	Probable Cause A command started by the WBSSPI collector reported an error. Potential Impact : NA 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 informatic

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. Potential Impact : NA Suggested Action View the managed node's errorlog to determine the root cause which is logged following the

WASSPI-201

Description	File <*filename*> not found
Severity	Critical
Help Text	Probable Cause A configuration file could not be found. Potential Impact : NA Suggested Action Run the SPI Admin → 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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 Potential Impact : NA 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 → 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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 → 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. Potential Impact : NA Suggested Action 1. Verify that WebSphere is up and running properly. 2. Run the SPI Admin → 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. Potential Impact : NA 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 → 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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 → 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA 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 Potential Impact : NA 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. Potential Impact : NA Suggested Action Log files: If there have never been any entries written to the file, no action is necessary. Otherwise, run the SPI Admin → Configure WBSSPI tool. Property files: Run the SPI Admin → 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. Potential Impact : NA Suggested Action If the file is a configuration file, run the SPI Admin → 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA 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 ‘Configure WBSSPI’?
Severity	Critical
Help Text	Probable Cause The logfile list is empty. Potential Impact : NA Suggested Action Run the SPI Admin → 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. Potential Impact : NA Suggested Action 1. Run the SPI Admin → 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA Suggested Action Run the SPI Admin → 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA Suggested Action 1. Specify a correct server name on the command line. 2. Run the SPI Admin → 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*> . Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA 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. Potential Impact : NA Suggested Action Run the SPI Admin → 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. Potential Impact : NA 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 WebSphere 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 → 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 WebSphere 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 → 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 Websphere tool again and select this node when the tool is launched. ■ Launch the SPI Admin → Discover WebSphere 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->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 WebSphere 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 → 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 WebSphere 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 → 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 WebSphere 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 → 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 WebSphere 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 → 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 WebSphere 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 run th Make sure that all of the application servers you want to monitor are running, before th Discover Websphere tool is launched. Only the servers that are running will be autom *WebSphere Application Server versions 5* : Unsuccessful login to the secured WebSpher *Verification* : Launch the WebSphere administrative console on the node and check if se PASSWORD variables (properties) for this node are present and valid in the WBSSPI co tool and verify the accuracy of the information. The PASSWORD information is encrypte 2. Run the SPI Admin → Discover Websphere tool and select the node from the list. S (overwrite the existing encrypted data). Allow the WBSSPI Discovery process to run ag NOTE: If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere App* Configuring the WebSphere SPI provides instructions on how to manually configure the Wel

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 missing fro *Verification:* Launch the WebSphere administrative console on the node and check if security is enabled. M (properties) for this node are present and valid in the WBSSPI configurations. Launch the SP accuracy of the information. The PASSWORD information is encrypted for security purposes. Potential Impact : NA Suggested Action : Run the SPI Admin → Discover Websphere tool and select the node from the list. Set the (overwrite the existing encrypted data). Allow the WBSSPI Discovery process to run again on NOTE: If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere App* Configuring the WebSphere SPI provides instructions on how to manually configure the Wel

WASSPI-573

Description	WebSphere 5 Login Error - Invalid Login Data
Help Text	Probable Cause : *WebSphere Application Server versions 5* he discovery application was unable to authenticate itself in a secured WebSphere server env and PASSWORD variables (properties) being provided in the WBSSPI configurations for this n *Verification:* Launch the WebSphere administrative console on the node and check if security is enabled. M (properties) for this node are present and valid in the WBSSPI configurations. Launch the SP accuracy of the information. The PASSWORD information is encrypted for security purposes. Potential Impact : NA Suggested Action : Run the SPI Admin → Discover Websphere tool and select the node from the list. Set the (overwrite the existing encrypted data). Allow the WBSSPI Discovery process to run again on NOTE: If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere App* Configuring the WebSphere SPI provides instructions on how to manually configure the Wel

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 WebSphere tool may not function properly due to one (or more) of the following conditions on the managed node: ■ A SPI Admin → Discover WebSphere 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 WebSphere 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 WebSphere 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 → 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 Websphere 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 Websphere 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 Websphere 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 Websphere tool again. NOTE: If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere Application Server 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 Websphere 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 Websphere tool are missing, have been removed, or are placed in non-standard directory paths. • Operations operator account that runs the SPI Admin → Discover Websphere 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 Websphere tool again. NOTE: If problem persists, refer to the document *HP Operations Smart Plug-in for WebSphere Application Server 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	Probable Cause : NA Potential Impact : NA 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: