

HP OpenView Smart Plug-in for WebSphere Application Server

Configuration Guide

Software Version: B.03.61

For Windows OpenView Operations Management Servers



April 2005

© Copyright 2003-5 Hewlett-Packard Development Company, L.P.

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

© Copyright 2003-5 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Trademark Notices

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

Java™ is a U.S. trademark of Sun Microsystems, Inc.

UNIX® is a registered trademark of The Open Group.

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

Support

Please visit the HP OpenView web site at:

<http://www.managementsoftware.hp.com/>

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

You can also go directly to the support web site at:

<http://support.openview.hp.com/>

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

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

<https://passport2.hp.com/hpp/newuser.do>

contents

- Chapter 1 WBS-SPI Concepts 9**
- Chapter 2 Installing, Upgrading, and Removing WBS-SPI 11**
 - Installing WBS-SPI 11
 - Upgrading WBS-SPI 12
 - Policy Changes 12
 - Before Starting 13
 - Upgrading WBS-SPI 13
 - Removing WBS-SPI 15
 - Task 1: Uninstall All WBS-SPI Policies from the Managed Nodes 16
 - Task 2: Remove WBS-SPI Node Groups on the Management Server 16
 - Task 3: Remove Any SPI for WebSphere Groups 17
 - Task 4: Remove the WBS-SPI Software from the Management Server . . 17
- Chapter 3 Configuring WBS-SPI 19**
 - Configuration Prerequisites 19
 - Task 1: Add Managed Nodes 20
 - Task 2: Verify the Application Server Status 20
 - Task 3: Collect WebSphere Login Information 22
 - Task 4: Enable PMI 23
 - Basic WBS-SPI Configuration 23
 - Task 1: Run Discover WebSphere 23
 - Task 2: Verify the Discovery Process 26
 - Additional WBS-SPI Configuration 27
 - Deploying a Different Policy Group 28

Chapter 4	Using and Customizing the WBS-SPI	29
	Using WBS-SPI Policies	30
	WBS-SPI Policy Groups	30
	OVO Policy Types and WBS-SPI	32
	Basic Policy Customizations	33
	Modifying Metric Policies	33
	Threshold Level and Actions	34
	Message and Severity	39
	Advanced Policy Customizations	40
	Choosing Metrics To Monitor	40
	Using the WBS-SPI Collector/Analyzer Command with Parameters	41
	Using the Basic WebSphere Command Parameters	42
	Using JMX Actions Command Parameters	44
	Changing the Collection Interval for Scheduled Metrics	46
	Changing the Collection Interval for Selected Metrics	47
	Customize the Threshold for Different Servers	48
	Creating Custom, Tagged Policies	49
	Monitoring WebSphere Application Server on Unsupported Platforms	51
	Requirements for Monitoring Remote Nodes (running on Platforms not supported by WBS-SPI)	51
	Overview	52
	Remote Monitoring: How It Works	52
	Configure Remote System Monitoring	54
	Task 1: Configure the Remote WebSphere System	54
	Task 2: (optional) Integrate OpenView Performance Agent	55
	Task 3: Deploy Policies to the Local Node	56
	Configuring Remote Logfile Monitoring (Optional)	56
	Configure the logfile policy for remote logfiles	56
	Remote Monitoring Limitations	57
	Re-installing the WBS-SPI Policies	58
	Using Policies/Tools to View Annotation Reports	58
	Automatic Command Reports	59
	Reports	60

Chapter 5	Reports and Graphs	61
	Using the OpenView Performance Agent	63
	Using Reporter to Generate Reports.	64
	WBS-SPI Reports	65
	Removing the WBS-SPI Reporter Package	66
	Using OVPM to Generate Graphs.	67
	Viewing Graphs that Show Alarm Conditions	67
	Viewing Graphs that Show Past/Current Conditions.	68
	WBS-SPI Metrics Available for Graphs.	68
	Launching the Web Page display with an Operator Action that Generate Graphs	71
	Specifying a Date Range.	71
	Removing the WBS-SPI Grapher Package	71
Chapter 6	Troubleshooting WBS-SPI	73
	Using the Self-Healing Info Tool	74
	Log and Trace Files	75
	Management Server	75
	UNIX Managed Nodes	75
	Windows Managed Nodes.	77
	WBSSPI Discovery Policies	78
	Manually Deploying the Discovery Policies.	80
	Verify Discovery Policy Deployment is Currently Active	81
	The Configuration	81
	Tools	82

WBS-SPI Concepts

The HP OpenView Smart Plug-in for WebSphere Application Server (WBS-SPI) is a full-featured SPI that allows you to manage WebSphere servers from an HP OpenView Operations console. It is suggested you read about the WBS-SPI concepts from the online help. The following topics are covered in the online help:

- Concepts
- Configuration editor
- Tools
- Policies
- User defined metrics
- Reports and graphs
- Error messages

Installing, Upgrading, and Removing WBS-SPI

This chapter covers installing, upgrading, and removing the Smart Plug-in for WebSphere Application Server (WBS-SPI) for use with OpenView Operations.

Installing WBS-SPI

If OVO is already installed, it is not necessary to stop your OVO sessions before beginning the WBS-SPI installation. To install WBS-SPI, do the following:

- 1 Insert the Smart Plug-ins CD into the CD drive of the management server. The HP OpenView Operations InstallShield Wizard starts.
- 2 From the first screen, select **Next**.
- 3 In the Program Maintenance window, select **Install products**.
- 4 In the Product Selection window, select the check box next to **IBM WebSphere** and select **Next**.
- 5 Complete the installation by following the instructions in the windows that display. Refer to the *HP OpenView Operations / Performance for Windows Installation Guide* for more information.

Upgrading WBS-SPI

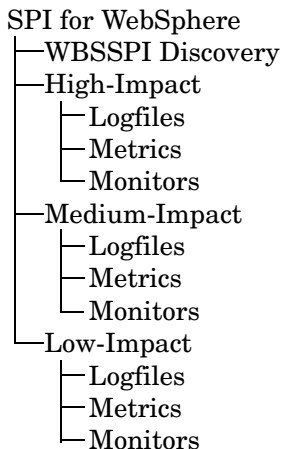
Detailed information about supported software, enhancements, fixes, and known problems and workarounds is available in the *HP OpenView Smart Plug-in for WebSphere Application Server Release Notes*, located on the *Smart Plug-ins, New and Upgraded CD, Volume 1*, in

`\Documentation\Releasenotes\WebSphere_AppServer_Releasenotes.html`.

Policy Changes

All policies have been changed in this release of the WBS-SPI. If you have customized any of the default WBS-SPI policies, you must make these same customizations to the new version of each policy. During the upgrade process, existing WBS-SPI policies in the SPI for WebSphere policy group are saved to another policy group. You can compare your old policies with the newly installed policies and customize the new policies, as needed.

A new policy group hierarchy has been implemented as follows:



In this version, the Impact policy groups are no longer categorized by the WebSphere server version. Also, the collector policies, WBSSPI-ConfigCheck policy, and WBSSPI-Performance policy have been move into a new group named Monitors.

Before Starting

Before upgrading to WBS-SPI version B.03.61, you must first upgrade OVOW to version 7.5. Then, install the new version of the WBS-SPI by running the InstallShield Wizard (installer). If the installer detects that an older version of the WBS-SPI is installed, it upgrades to the new version by doing the following:

- Renames the existing SPI for WebSphere policy group to SPI for WebSphere - Saved Policies. If you customized any of the default policies in the SPI for WebSphere policy group, the customized policies are available in the SPI for WebSphere - Saved Policies policy group.
- Updates the WBS-SPI instrumentation on the management server.
- Saves the existing WBS-SPI configuration file
<%OvInstallDir%>\SPI-Share\WBSSPI\English\conf\SiteConfig and reinstalls it with the upgraded version of the WBS-SPI.
- Deletes the existing <%OvInstallDir%>\SPI-Share\WBSSPI and <%OvInstallDir%>\install\WASSPI\WBSSPI directories on the management server.
- Installs new tools, policies, and graph file on the management server.

Upgrading WBS-SPI

To upgrade to WBS-SPI version B.03.61, do the following:

- 1 Install the WBS-SPI version B.03.61 software:
 - a Insert the *Smart Plug-ins and Integration Modules, New and Upgraded, Volume 1* CD into the CD drive of the management server. The InstallShield Wizard starts.
 - b From the first screen, select **Next**.
 - c In the Program Maintenance window, select **Install products**.
 - d In the Product Selection window, select the check box next to **IBM WebSphere** and select **Next**.
 - e Complete the installation by following the instructions in the windows that display. Refer to the *HP OpenView Operations/Performance for Windows Installation Guide* for more information.

- 2 Refresh the SPI for WebSphere node group:
 - a In the console tree, select **Tools** → **SPI for WebSphere** → **SPI Admin** → **Create WBSSPI Node Groups**.

All the nodes found in the WBS-SPI service map are placed in the SPI for WebSphere node group.
 - 3 Uninstall all older versions of WBS-SPI policies from existing nodes (versions 3.0 and lower). This includes any customized policies that you may have moved outside of the old SPI for WebSphere policy group and does not reside in the SPI for WebSphere - Saved Policies policy group.
 - a In the console tree, select **Policy management** → **Policy groups**.
 - b Select the **SPI for WebSphere - Saved Policies** policy group and right-click on it.
 - c Select **All tasks - Uninstall from**.
 - d Select the node group **SPI for WebSphere**.
 - e Select **OK**.
 - f Repeat these steps for any customized WBS-SPI policies that do not reside in the SPI for WebSphere - Saved Policies policy group.
 - 4 Deploy new instrumentation to the SPI for WebSphere node group:
 - a Select the **SPI for WebSphere** node group and right-click on it.
 - b Select **All Tasks** → **Deploy instrumentation**.
 - c Select **SPI for WebSphere**.
 - d Verify that the **Remove existing instrumentation before deploying new instrumentation** checkbox is *NOT* selected.
 - e Select **OK**.
 - 5 Customize the new policies in the SPI for WebSphere policy group to match old customized policies. Compare old and new policies by opening them side by side.
 - 6 Deploy the new policies.

To deploy the polices from the High Impact, Medium Impact, or Low Impact policy group to all WebSphere nodes:

 - a Drag and drop the policy group (High Impact, Medium Impact, or Low Impact) on the SPI for WebSphere node group.
-

To deploy a policy group to selected WebSphere nodes:

- a Right-click on the policy group (High Impact, Medium Impact, or Low Impact).
- b Select **All Tasks** → **Deploy on ...**
- c Select the node(s) on which to deploy the policy group.
- d Click **OK**.

To deploy a single policy:

- a Right-click on the policy.
- b Select **All Tasks** → **Deploy on ...**
- c Select the node(s) on which to deploy the policy.
- d Click **OK**.

7 Remove old policy groups (optional):

- a In the console tree, select **Policy management** → **Policy groups**.
- b Select the **SPI for WebSphere - Saved Policies** policy group and right-click on it.
- c Select **Delete**.
- d Select **Yes** to delete the SPI for WebSphere - Saved Policies policy group.
- e Select and remove any WBS-SPI policies you may have moved outside of the old SPI for WebSphere policy group and do not reside in the SPI for WebSphere - Saved Policies policy group.

Removing WBS-SPI

To completely remove the WBS-SPI, delete all WBS-SPI program components as well as the WBS-SPI policies.

Complete the tasks in the order listed

- Task 1: Uninstall All WBS-SPI Policies from the Managed Nodes
- Task 2: Remove WBS-SPI Node Groups on the Management Server
-
- Task 4: Remove the WBS-SPI Software from the Management Server


Task 1: Uninstall All WBS-SPI Policies from the Managed Nodes

If you have customized policies (copies of WBS-SPI default policies) residing in other OVO policy groups, you should remove them as well.

- 1 In the console tree, select **Policy management** → **Policy groups**.
- 2 Right-click on **SPI for WebSphere** and select **All Tasks** → **Uninstall from**. A node selection window appears.
- 3 Select the nodes on which the policies are installed.
- 4 Select **OK**.
- 5 Verify the policies are uninstalled. Check the status of the job in **Deployment jobs** under Policy groups. All WBS-SPI policies must be uninstalled before you start the next task.

Task 2: Remove WBS-SPI Node Groups on the Management Server

If you ran the Create WBSSPI Node Groups tool, the SPI for WebSphere node group was created and must be removed:

- 1 In the console tree, select **Nodes** → **SPI for WebSphere**.
- 2 Open the Node Configuration editor.
 - a Select the Nodes folder in the console tree.
 - b Click  on the Configuration toolbar to open the editor.
- 3 In the Nodes list, either select the name of the node group you want to delete and press the **Delete** key or right-click on the node group and select **Delete**.
- 4 Click **Yes** to continue the delete operation.

Task 3: Remove Any SPI for WebSphere Groups

- 1 Under **Tools, Policy management** → **Policy groups, Reports & Graphs** → **Reports**, and **Reports & Graphs** → **Graphs**, look for the **SPI for WebSphere** group.
- 2 If the **SPI for WebSphere** group exists, remove it and its contents.
- 3 If you upgraded the SPI, also remove the **SPI for WebSphere - Saved Policies** group from **Policy management** → **Policy groups**.

Task 4: Remove the WBS-SPI Software from the Management Server

- 1 Insert the Smart Plug-ins CD into the CD drive of the management server. The HP OpenView Operations InstallShield Wizard starts.
- 2 From the first screen, select **Next**.
- 3 In the Program Maintenance window, select **Remove products**.
- 4 In the Product Selection window, select the check box next to **IBM WebSphere** and select **Next**.
- 5 Complete the removal by following the instructions in the windows that display.

Configuring WBS-SPI

This chapter covers configuring the Smart Plug-in for WebSphere Application Server (WBS-SPI) for use with OpenView Operations and how to deploy a different policy group. To successfully configure WBS-SPI, you must complete all configuration prerequisites, complete basic configuration, and complete additional configuration based on your environment.

Configuration Prerequisites

Complete the following tasks before configuring WBS-SPI:

- [Task 1: Add Managed Nodes](#)
- [Task 2: Verify the Application Server Status](#)
- [Task 3: Collect WebSphere Login Information](#)
- [Task 4: Enable PMI](#)

Task 1: Add Managed Nodes

For each WebSphere server you want to manage from OVO, make sure each node on which the WebSphere servers are running is configured in OVO as a managed node.

To add a UNIX managed node, do the following:

- 1 Install the OVO agent on the node. Refer to the OVO online help topic “Agent Installation on UNIX computers” for more information.
- 2 Specify each WebSphere Server node on UNIX to be managed. Refer to the OVO online help topic “Configure Managed Nodes” for more information.

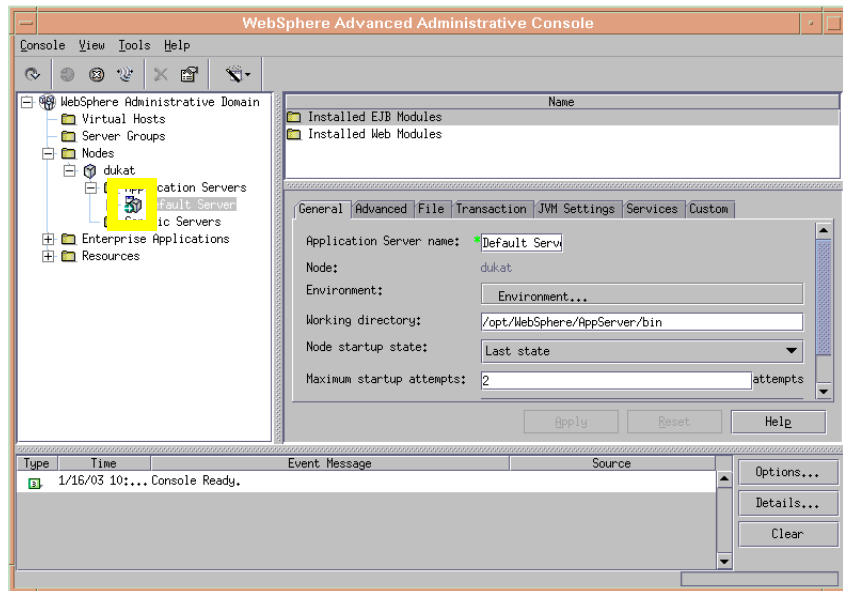
For a Windows managed node, do the following:

- 1 Specify each WebSphere node on Windows to be managed. Refer to the OVO online help topic “Configure Managed Nodes” for more information (the OVO agent is automatically installed when you complete this step).

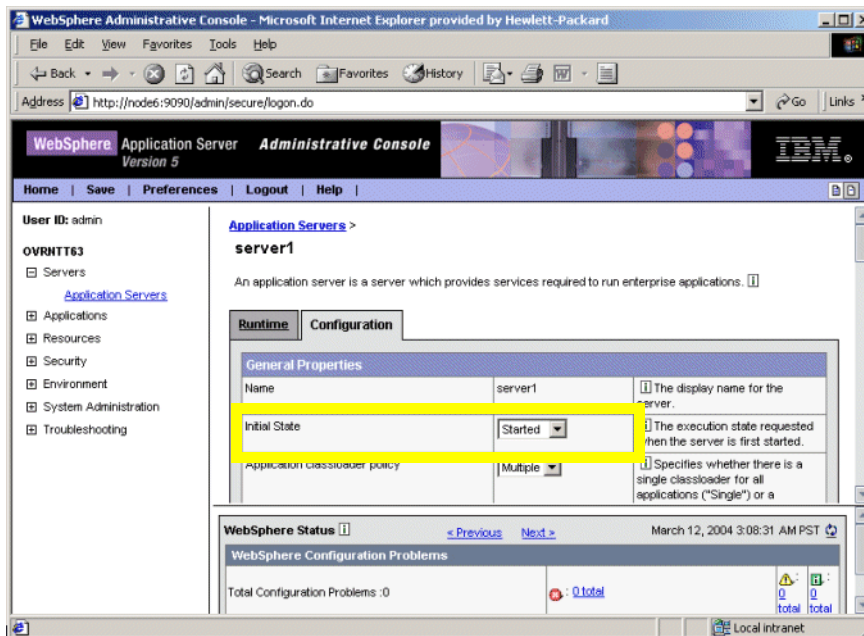
Task 2: Verify the Application Server Status

Verify that your WebSphere application servers are running.

For WebSphere Server version 4, verify the server's status from the WebSphere Administrative Console. A colored icon appears next to the Application Server name. A green icon means the server is running. A red icon means the server is not running. If the icon is red, start the server.



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



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

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

Task 3: Collect WebSphere Login Information

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

The username and password are needed by the WBS-SPI discovery process to gather basic configuration information and by the WBS-SPI data collector to collect metrics.

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

Task 4: Enable PMI

If you are running WebSphere Server version 5, enable PMI using the WebSphere Administrative Console and restart the server.

Basic WBS-SPI Configuration

To complete basic WBS-SPI configuration, complete the following tasks:

- Task 1: Run Discover WebSphere
- Task 2: Verify the Discovery Process

Task 1: Run Discover WebSphere

Discover WebSphere sets basic configuration properties needed for discovery, deploys the WBS-SPI discovery policies, and updates the service map.

To run Discover WebSphere, do the following:

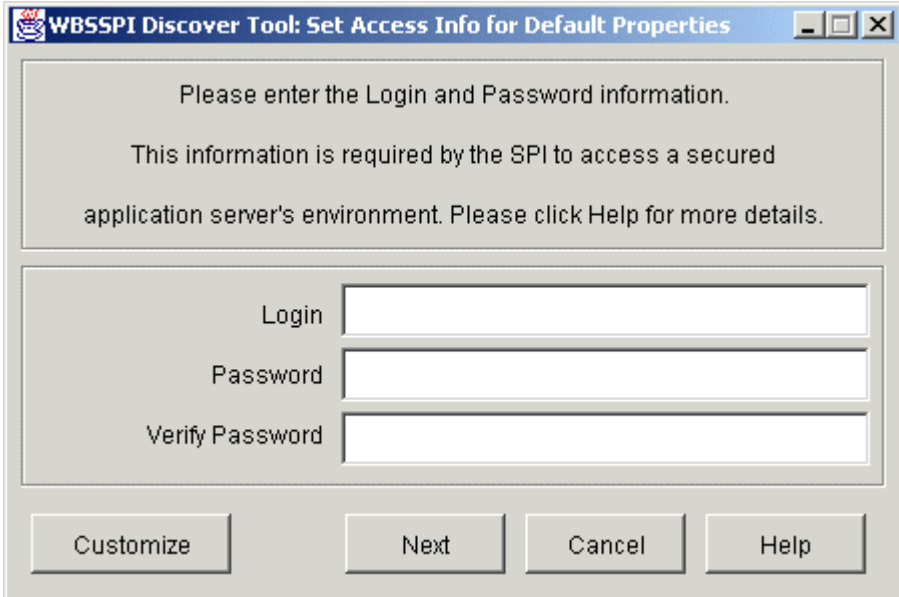
- 1 From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **SPI Admin**.
- 2 Double-click on **Discover WebSphere**.
- 3 Select the managed node(s) on which WebSphere is running.
- 4 Click **Launch**.
- 5 The “Console Status” window displays. Wait a few seconds for the “Introduction” window to display. This window contains brief information about the Discover WebSphere tool.

Select **Next**.

- 6 A second “Introduction” window displays. This window displays instructions about how to enter the WebSphere login and password information you collected.

Read these instructions and select **Next**.

- 7 If you have not set the WBS-SPI `LOGIN` and `PASSWORD` properties, the “Set Access Info for Default Properties” window displays.



The screenshot shows a dialog box titled "WBS-SPI Discover Tool: Set Access Info for Default Properties". The dialog contains the following text: "Please enter the Login and Password information. This information is required by the SPI to access a secured application server's environment. Please click Help for more details." Below the text are three input fields labeled "Login", "Password", and "Verify Password". At the bottom of the dialog are four buttons: "Customize", "Next", "Cancel", and "Help".

If you have already configured the `LOGIN` and `PASSWORD` properties, the configuration editor displays. Go to step 8.

Set the `LOGIN` and `PASSWORD` properties to the WebSphere login and password collected in [Task 3: Collect WebSphere Login Information](#) on page 22. The WebSphere Admin Server login information is required when security is enabled. If security is not enabled, leave these fields blank, select **Next**, and go to step 10.

The `LOGIN` and `PASSWORD` properties set in this window are used as the default WebSphere Admin Server login and password (they are set at the global properties level). That is, if no `NODE` level or server-specific `LOGIN` and `PASSWORD` properties are set, this WebSphere login and password are used by WBS-SPI to access all WebSphere Admin Servers. For more information about the configuration structure, refer to the online help topic “The configuration.”

If the WebSphere Admin Server login and password are the same for all application servers on all OVO managed nodes, do the following:

- a Set the `LOGIN` and `PASSWORD` in the “Set Access Info for Default Properties” window.
- b Select **Next**.
- c Go to step 10.

If the WebSphere Admin Server login and password are different for different instances of WebSphere, you must customize the WBS-SPI configuration by setting the `LOGIN` and `PASSWORD` properties at the `NODE` or server-specific level (for more information about the configuration structure, refer to the online help topic “The configuration.”):

- a Set `LOGIN` and `PASSWORD` to the most commonly used WebSphere login and password in the “Set Access Info for Default Properties” window.
- b Select **Customize** to start the configuration editor.
- 8 From the configuration editor, set the configuration properties. Refer to the online help for more information about using the configuration editor.
- 9 Select **Next** to save any changes and exit the editor.
- 10 The “Confirm Operation” window displays. Select **OK**. The discovery policies are deployed to the selected managed nodes.



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 Discover WebSphere tool, select those managed nodes, select **Next** from the configuration editor, and then select **OK**.

Scan the “Console Status” window for any error messages. If none display, click on **Close**.

If the window displays an error message, refer to [WBSSPI Discovery Policies](#) on page 78 in the [Troubleshooting WBS-SPI](#) chapter to diagnose the problem.

Task 2: Verify the Discovery Process

Depending on the number of managed nodes in your environment, verification takes several minutes to complete.

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

```
INFO - Updating the WBSSPI configuration data with discovered information
```

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

If this message is present and the letter “S” (for successful) appears in the A column, the WBSSPI Discovery policies have been successfully deployed.

If this message is not present or if the message is present but the letter “F” appears in the A column, check for any error messages. Also refer to [WBSSPI Discovery Policies](#) on page 78 in the [Troubleshooting WBS-SPI](#) chapter to diagnose the problem.

- 2 View the service map and verify that the WebSphere, WebSphere Admin Server, and application server instances are correctly represented.
 - a From the OVO console, select **Operations Manager** → **Services** → **Applications** → **WebSphere**. It may take 1 - 2 minutes for the service map to completely display.
- 3 After the discovery process has completed, the appropriate WBSSPI group policies are deployed on the managed node(s). An automatic procedure to set up a managed node for WBSSPI operations starts about 10 minutes after the policies are deployed. Wait 10 minutes and run the **Verify** tool to verify the version of the policies installed on a managed node:
 - a From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **SPI Admin**.
 - b Double-click on **Verify**.
 - c Select the node(s) to verify.
 - d The WBS-SPI version is displayed. The version should be B.02.09 or later.
 - e Click **Close**.

Additional WBS-SPI Configuration

Once you have successfully completed basic WBS-SPI configuration, you must finish the configuration by setting additional configuration properties (these properties are not automatically discovered by the Discovery policies) and/or installing and configuring additional components. The additional properties to set and components to configure depend on your environment.

Refer to the online help for a complete definition of the properties.

To run the Start WebSphere and Stop WebSphere tools from the OVO console, set the `START_CMD`, `STOP_CMD`, and `USER` properties.

If you are configuring user-defined metrics, refer to the JMX Metric Builder online help for additional installation and configuration information.

If HP OpenView Reporter is installed (must be purchased separately and is *not* the version of Reporter that is included with OVO), refer to [Using Reporter to Generate Reports](#) on page 64 for installation and configuration information.

If HP OpenView Performance Manager is installed (must be purchased separately) and you want to view graphs, set the `GRAPH_URL` property. Refer to [Using OVPM to Generate Graphs](#) on page 67 for additional installation and configuration information.

To update the configuration, do the following:

- 1 From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **SPI Admin**.
- 2 Double-click on **Configure WBSSPI**.
- 3 Select the managed node(s) to configure.
- 4 Click **Launch**.
- 5 Click **Next** in the “Introduction” window.
- 6 Set the properties. Refer to the online help for more information about using the editor.
- 7 Select **Save**.
- 8 Select **Next**.
- 9 Select **OK**.

Deploying a Different Policy Group

The WBS-SPI Discovery policy automatically deploys the Medium-Impact policy group to the managed node on which it discovers the presence of a WebSphere application server. If you want to deploy a different set of policies (High-Impact, Low-Impact, or your own custom policies), do the following:

- 1 Remove the existing Medium-Impact policy group:
 - a From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere**.
 - b Right click on **Medium-Impact** and select **All Tasks** → **Uninstall from**.
 - c Select the node(s) from which you want to remove the Medium-Impact policy group.
 - d Click **OK**.
- 2 Deploy the different policy group:
 - a From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere**.
 - b Right click on the policy group to deploy and select **All Tasks** → **Deploy on**.
 - c Select the node(s) from which you want to deploy the different policy group.
 - d Click **OK**.

▶ The PMI level of a node is automatically adjusted to a higher level when a higher impact level policy group is deployed. For example, deploying the High-Impact policy group on a node would result in a PMI setting of “high” for the node.

▶ However, PMI levels do not automatically revert to lower impact levels, even after removing policies from a node and/or deploying a lower impact level policy group. To lower a PMI level for a node, you must manually re-set the PMI level within WebSphere. Monitoring settings can be changed using the WebSphere Resource Analyzer tool.

Please see the IBM WebSphere documentation for more information about PMI.

Using and Customizing the WBS-SPI

Now that you have completed the tasks in the previous chapter of configuring the Smart Plug-in for WebSphere Application Server (WBS-SPI) and deploying the policies, you may be receiving messages in the OVO message browser. As you become familiar with the types of messages generated by the WBS-SPI as well as the graphs/reports available, you will discover what you find most useful.

As your familiarity with the WBS-SPI grows, you can determine the policies most beneficial to you in monitoring WebSphere and then determine if you need to make changes. This chapter assists you by providing further detail on the policies and how to make those changes.

In general the following topics are covered:

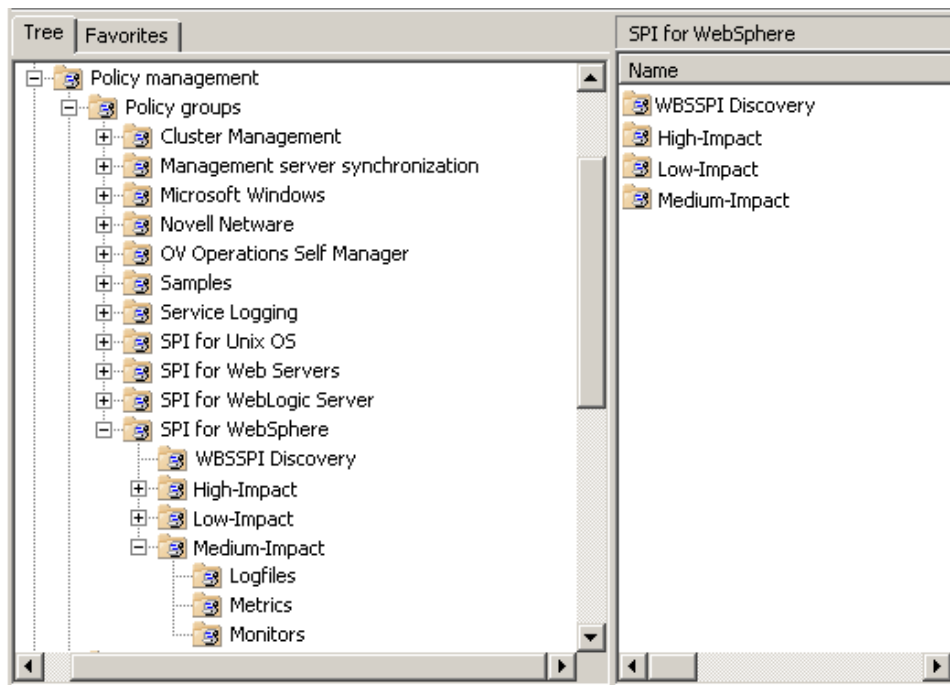
- Using the WBS-SPI Policies
- Basic Policy Customizations
- Advanced Policy Customizations
- Reinstalling WBS-SPI Policies
- Using Policies/Tools to Generate Reports

Using WBS-SPI Policies

You can customize WBS-SPI policies, although they work without any modifications. To help you understand how you might customize the WBS-SPI policies, the following sections cover the OpenView Operations policies in general and WBS-SPI policy groups in particular.

WBS-SPI Policy Groups

The *SPI for WebSphere* policy group organizes policies under the *Discovery*, *High-Impact*, *Medium-Impact*, and *Low-Impact* groups (as shown below).



WebSphere Policy Groups and System PMI levels: When you deploy a policy group on a managed node, the PMI level of the node is automatically adjusted to that of the policy group. For example, deploying the High-Impact policy group on a node would result in a PMI setting of “high” for the node.



PMI levels, once set, do not automatically revert to lower impact levels, even after removing policies from a node and/or deploying a lower impact level policy group. To lower a PMI level for a node requires that you manually re-set the PMI level within WebSphere. Monitoring settings can be changed using the WebSphere Resource Analyzer tool.

The *High-Impact*, *Medium-Impact*, and *Low-Impact* subgroups contain metric and collector policies that work as follows:

- **Metrics** interpret incoming values of WebSphere’s performance levels and availability. Each value is evaluated according to the metric with which it is associated. If it is acceptable, it is ignored; if it is not, a message is sent to the OVO Message browser and an automatic action may execute.

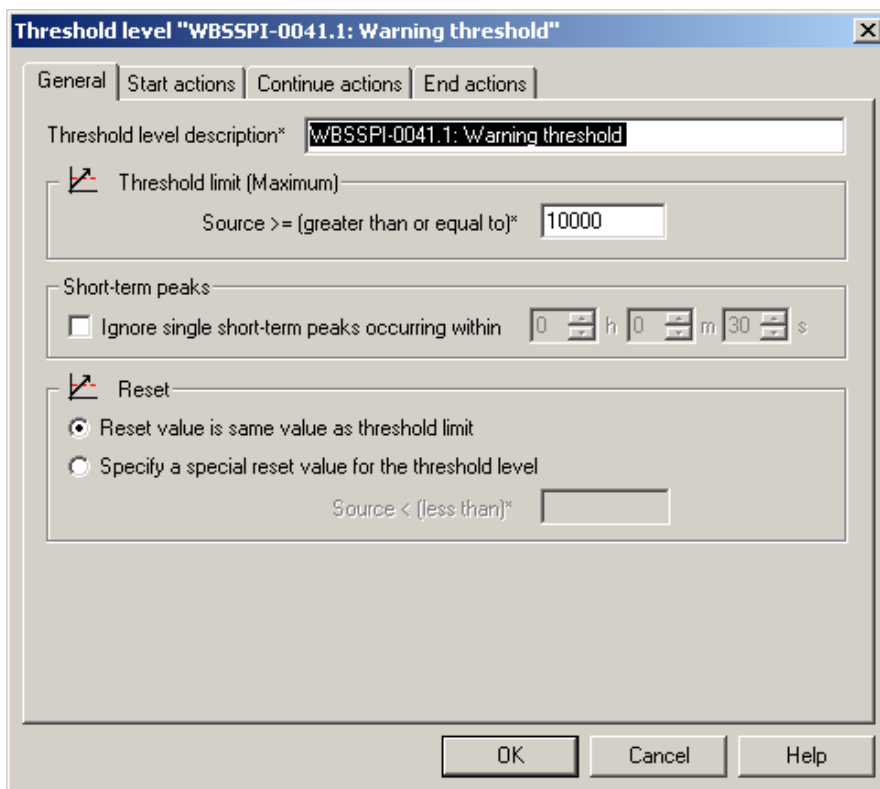
Metric policies contain defined thresholds that can trigger alerts/ messages. Incoming values are compared against those thresholds and when a value exceeds a threshold, a message/alert is sent to the OVO console.

- **Monitors** (collector policies) schedule when and what is collected. Specifically, the collector policy has two functions: (1) to run the collector/ analyzer at each collection interval and (2) to specify (and expose to you through its Program name text box) the metrics to target for that data collection interval.
- **Logfiles** monitor WebSphere- and WebSphere SPI-generated logfiles. The information from these logfiles covers changes to WebSphere configurations and errors that occur in the operation of the WebSphere or the WBS-SPI.

OVO Policy Types and WBS-SPI

Metric policies define how data is collected for the individual metric and set a threshold value that, when exceeded, generates alerts/messages in the Message Browser. You can change the threshold within a policy by double-clicking on the policy, clicking the **Threshold levels** tab, and clicking on **Threshold level** in the Level summary pane.

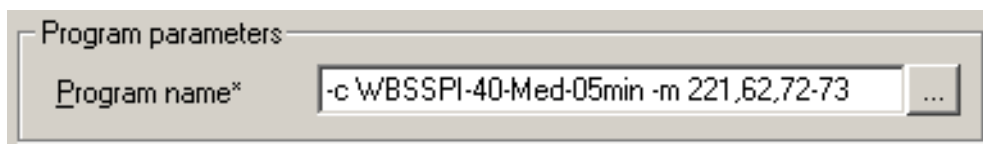
Incoming values for metric WBSSPI-0041.1 are compared against its policy settings. In the illustration below, the default threshold is set at 10000.



Collector policies define all metrics for the WebSphere application that are scheduled for collection at the specified interval. Though still identified as a “metrics policy” in the OVO lists of policies, notice that these policies have names different from the individual metric policies. Within the name of each collector policy is its collection interval (for example, WBSSPI-60-1h). When

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

The figure below shows the `Program name` text box, which contains the collector/analyzer command (`wasspi_wbs_ca`, not seen in the figure), followed by the collection parameter and collection name (`-c WBSspi-40-Med-05min`), followed by the metric parameter and each metric (`-m 221,62,72-73`).



Basic Policy Customizations

After you begin using the WBS-SPI, you may decide that some WBS-SPI policies need some modification. Descriptions contained in the previous section of metric policies (rules for interpreting metric data, such as thresholds,) and collector policies (rules for the scheduled metric collection) show you where to go to make the various changes. For example, to change a threshold, you would open a metric policy. To schedule or delete a metric from data collection, you open the collector policy. Those kinds of basic customizations are covered in this section.

- ▶ In most cases, it is advisable to make copies of the original policies so that the default policies remain intact.

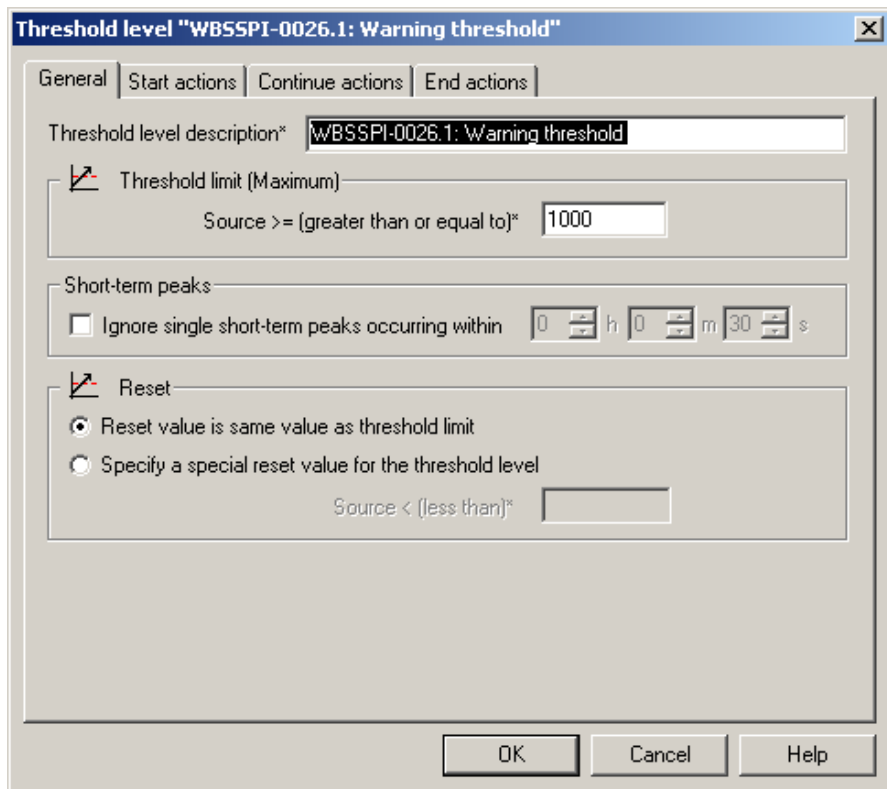
Modifying Metric Policies

Many metric attributes can be easily modified for all monitored instances of WebSphere. Attributes not mentioned here are defined in the online help.

Threshold Level and Actions

To modify the threshold level and actions of a policy, do the following

- 1 From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **Medium-Impact**.
- 2 Highlight Metrics.
- 3 Double-click on a policy.
- 4 Select the **Threshold levels** tab.
- 5 From the Level summary pane, click on **Threshold level**. The Threshold level window displays.



In the figure above, the threshold limit is set to 1000 for WBSSPI-0026. The incoming values for this metric show the total number of times per minute clients must wait for an available (Enterprise Java) bean. A value

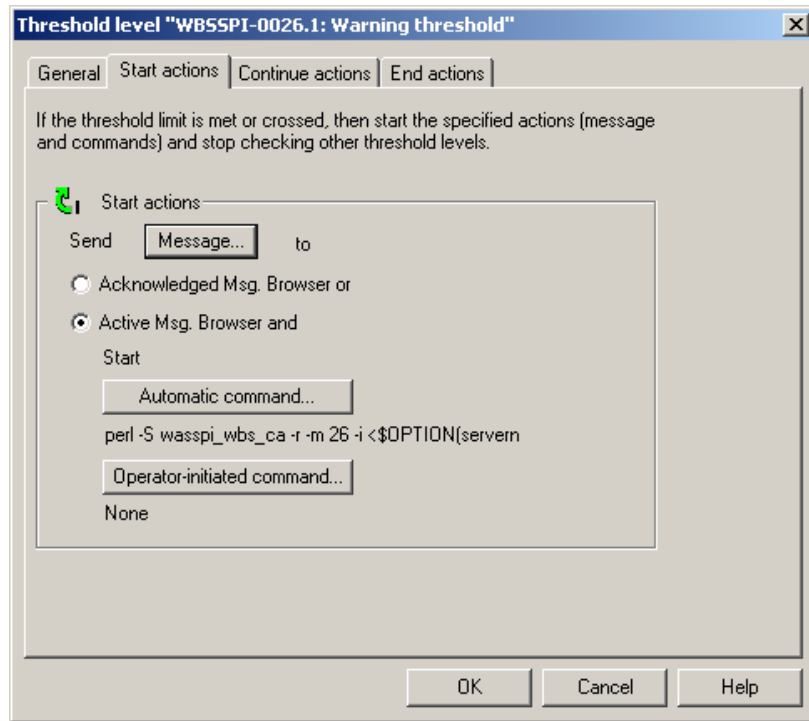
of more than 1000 would start to impact the server response time the client experiences, generating a Warning message.

The following attributes can be modified:

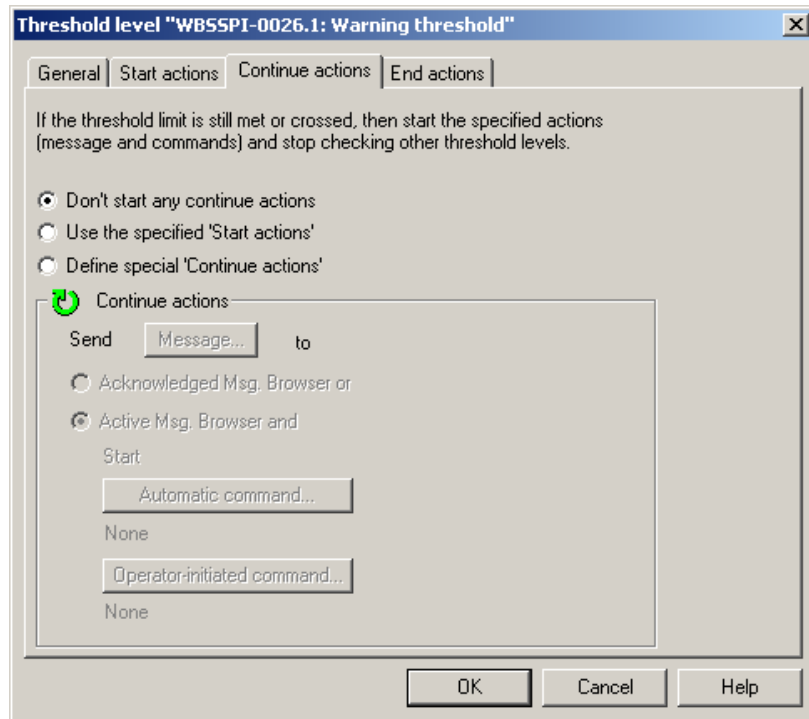
- **Threshold limit.** The value that triggers a message if it is met or crossed.
- **Short-term peaks.** A minimum time period over which the monitored value must exceed the threshold before generating a message. For a message to be sent, the value must be greater than the threshold each time the value is measured during a duration that you select. If the duration is set to 0 or the box is left empty, an alarm is generated as soon as OVO detects that the threshold has been equaled or crossed.
- **Reset.** A limit below which the monitored value must drop (or exceed, for minimum thresholds) to return the status of the monitored object to normal.

Click on one of the actions tabs to set the following:

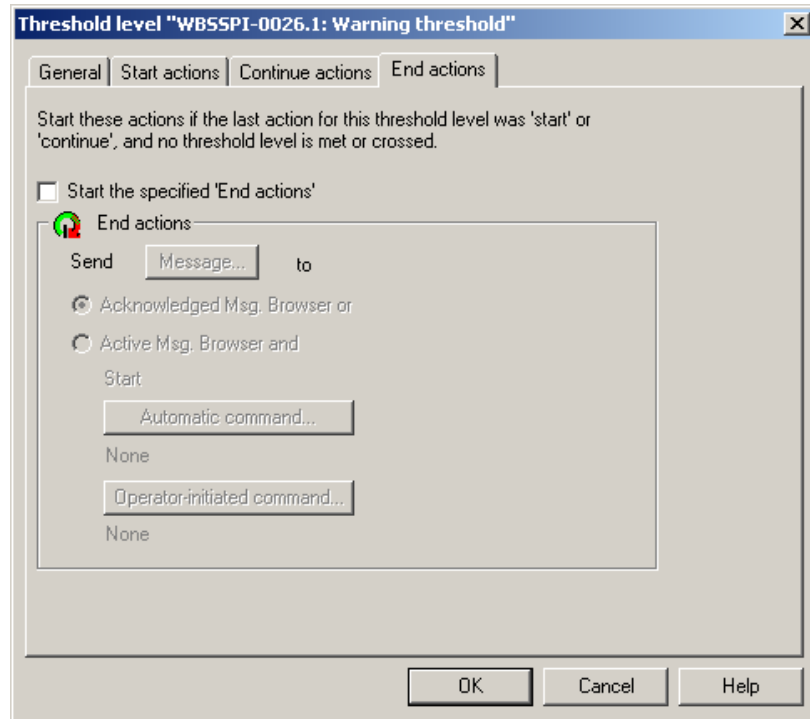
- **Start actions.** Actions carried out the first time that the threshold is crossed.



- **Continue actions.** Actions carried out at each subsequent polling interval if the reset value is not reached.



- **End actions.** Actions carried out after the threshold crosses the reset value.



In each of the actions tabs, you can set the type of actions to perform. The WBS-SPI provides the ability to generate graphs or reports, or to add custom programs. The reports or graphs are accessible to the user from:

- **Automatic command.** A command run when the rule is matched. The automatic command delivered with the WBS-SPI generates a snapshot *report* that shows the data values at the time the action was triggered from an exceeded threshold. You can view the report in the message annotations.
- **Operator-initiated command.** A command attached to the message that the rule sends to the message browser. This command can be started by the operator from the message browser. The operator-initiated command delivered with the WBS-SPI allows the operator to press the **Perform Action** button to view a *graph* of the metric whose exceeded threshold generated the message along with other related metric values.

Message and Severity

To modify the message and severity of a policy, do the following

- 1 Double-click on a policy.
- 2 Select the **Threshold levels** tab.
- 3 From the Level summary pane, click on **Message**. The Outgoing Message window displays.

The screenshot shows the 'Outgoing Message' dialog box with the following fields and values:

- Service ID: EJB <\$OPTION(m_servername)> <\$OPTION(m_port)>
- hosted on: <\$MSG_NODE_ID>
- Message Key: Empty
- Message Type: Empty
- Message Group: Empty
- Application: Empty
- Object: Empty
- Node: <\$MSG_NODE_NAME> (Local Node)
- Severity: Warning
- Message Text: WBSSPI-0026.1: Ave. # of bean objects in the pool (<\$VALU

The following attributes can be modified:

- **Severity.** Indicates to the operator the importance of the event which triggers this message.
- **Message Text.** Be careful not to modify any of the parameters—surrounded by <> brackets, beginning with \$—in a message.

Advanced Policy Customizations

The policy changes suggested here range from making copies of default policy groups in order to customize a few settings, to deleting whole groups of metrics within a policy's command line. This section is considered *advanced* because all changes described here, whether simple or complex, require some advanced knowledge of the WBS-SPI metrics.

Choosing Metrics To Monitor

As a start, determine which metrics you want to change and what policies within the group you want to use. Then proceed as follows:

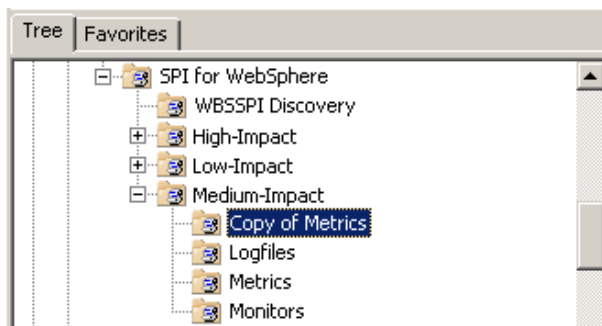
- 1 Create a new policy group:
 - a Right-click on the policy group you want to copy and select **Copy**.

For example, right-click on the Metrics policy group under Medium-Impact and select **Copy**.
 - b Right-click on the group under which this policy group is located and select **Paste**.

For example, right-click on Medium-Impact and select **Paste**.
 - c Rename the new group.

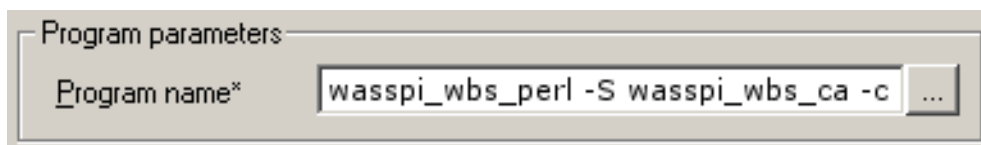
For example, right-click on **Copy of Metrics** and select **Rename**. Type in a new name.
- 2 Rename the original policies within the new policy group:
 - a Right-click on the policy and select **All Tasks** → **Edit**.
 - b Click on **File** → **Save As**.
 - c Enter a new policy name and select **OK**.
- 3 Delete all original policies within the new policy group:
 - a Highlight the policies and hit **Delete**.
- 4 Alter the renamed policies within the new group as necessary.

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



Using the WBS-SPI Collector/Analyzer Command with Parameters

The `wasspi_wbs_perl -S wasspi_wbs_ca` command is used in every collector policy, named according to its collection interval. You can view the default command line parameters within each collector policy in the **Program name** text box in OVO.



Using the Basic WebSphere Command Parameters

The command parameters described in this section are those used by the default collector policies.

Parameter	Description
-c Required	(collector) Specifies collector policy name. This <i>must</i> match the collector policy name in which it appears. Syntax: -c <collector_policy_name> Example: -c WBS-SPI-05min
-e	(exclude) Allows you to exclude specific servers; may not be used with -i option. Syntax: -e <server_name> Example: -e server1,server3
-i	(include) Allows you to list specific servers to monitor. This option may not be used with -e option. Syntax: -i <server_name> Example: -i server1,server3
-m	(metric) Specifies the metric numbers or number ranges on which to collect data. Syntax: -m <metric_number,metric_number_range> Example: -m 1,3-5,9-11,15
-matchver	(match version) Specifies the WebSphere application server version to monitor. This option may not be used with the -minver nor -maxver options. If no matching versions are found, the command does not execute. Syntax: -matchver <version_number> Example: -matchver 4
-maxver	(maximum version) Specifies the highest WebSphere application server version to monitor. Use with -minver to specify a range of version. If no versions are found, the command does not execute. Syntax: -maxver <version_number> Example: -maxver 5

Parameter	Description
-minver	(minimum version) Specifies the lowest WebSphere application server version to monitor. Use with -maxver to specify a range of version. If no versions are found, the command does not execute. Syntax: -minver <version_number> Example: -minver 4
-r	(report) Generate an ASCII report for the specified metric(s). Syntax: -r
-t	(tag) Allows you to create a new policy group by adding a prefix to an existing collector policy along with the metric number(s). Syntax: wasspi_wbs_perl -S wasspi_wbs_ca -c <prefix>-<collector_policy> -m <metric_number> -t <prefix>- Example: wasspi_wbs_perl -S wasspi_wbs_ca -c DEV-WBSSPI-40-Med-1h -m 220-223 -t DEV-
-x	Allows you to specify a property and value. Syntax: -x <property>=<property_value> where <property> can be one of the following:
alarm	When off, overrides any default alarming defined for the metric. Example: -x alarm=off
prefix	Default: JMXUDM_. Specify the prefix of the metric ID. Example: -x prefix=SALES_
print	When on, prints the metric name, instance name, and metric value to STDOUT in addition to any configured alarming or logging. Example: -x print=on
log	When off, prevents graphing or reporting functions. Example: -x log=off

Examples

- To collect specific data on all configured servers:

```
wasspi_wbs_perl -S wasspi_wbs_ca -c WBSSPI-40-Med-15min
-m 10-14,25,26
```

- To collect data from specific servers only:

```
wasspi_wbs_perl -S wasspi_wbs_ca -c STAGE-WBSSPI-40-Med-05min
-m 245,246,260 -i server1,server2
```

- To not collect data from specific servers:

```
wasspi_wbs_perl -S wasspi_wbs_ca -c STAGE-WBSSPI-40-Med-05min
-m 220-225 -e server1,server2
```

Using JMX Actions Command Parameters

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

Parameter	Description
-a	(action) Indicates a JMX action is performed.
Required	Syntax: -a
-i	(include) Allows you to list specific servers on which to perform the JMX actions. If this parameter is not specified, the JMX actions are performed on all configured servers. Syntax: -i <server_name> Example: -i server1,server3
-m	(metric) Specifies the metric ID containing the action to perform. This metric ID must be defined in a UDM file. This option may not be used with the -mbean nor -xml options. Syntax: -m <metric_id> Example: -m TestUDM_1000

Parameter	Description
-mbean	<p>Performs a JMX call on the specified MBean(s). This option may not be used with the -m nor -xml options.</p> <p>Syntax: -mbean <objectname> <action></p> <p>Example: -mbean WebSphere:type=ThreadPool,* -get maximumSize where <action> (a JMX call) is one of the following:</p>
-get	<p>Returns the value of the apecified attribute.</p> <p>Syntax: -mbean <objectname> -get <attribute></p> <p>Example: -get maximumSize</p>
-invoke [-type]	<p>Executes an MBean operation with the specified parameters. An operation may not require parameters (therefore, -type is not specified). A type parameter must be specified for operations which accept parameters. -type supports operation overloading.</p> <p>Syntax: -mbean <objectname> -invoke <operation> [-type <parameter_type> <parameter_value>]...</p> <p>where <parameter_type> is one of the following: short, int, long, double, float, boolean, java.lang.Short, java.lang.Integer, java.lang.Long, java.lang.Double, java.lang.Float, java.lang.Boolean, and java.lang.String.</p> <p>Example: -invoke setInstrumentationLevel -type java.lang.String pmi=L -type boolean true</p>
-set	<p>Assigns the specified value to the specified attribute.</p> <p>Syntax: -mbean <objectname> -set <attribute> <value></p> <p>Example: -set growable true</p>
-o	<p>(object) Specifies an MBean instance.</p> <p>Syntax: -o <mbean_instance></p> <p>Example: -o exampleJMSServer</p>
-xml	<p>Specifies the XML file that contains the JMX action(s) to perform. This option may not be used with the -m nor -mbean options.</p> <p>Syntax: -xml <filename></p> <p>Example: -xml myJMXActions.xml</p>

Examples

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

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

```
wasspi_wbs_perl -S wasspi_wbs_ca -a  
-mbean WebSphere:type=Perf,* -invoke setInstrumentationLevel  
-type java.lang.String pmi=L
```
- Use the sample UDM TestUDM_1000 in the `wbs_UDMMetrics-sample.xml` file:

```
wasspi_wbs_perl -S wasspi_wbs-ca -a -m TestUDM_1000  
-i examplesServer
```
- Use the sample actions xml file:

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

Changing the Collection Interval for Scheduled Metrics

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

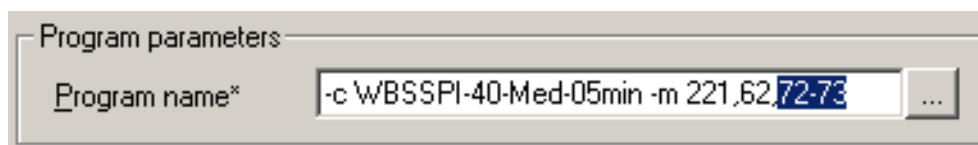
- 1 From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **Medium-Impact** → **Monitors**.
- 2 Right-click on the collector policy **WBSSPI-40-Med-05min** and select **All Tasks** → **Edit**.
- 3 Click on **File** → **Save As** and change the Name to **WBSSPI-40-Med-10min**.
- 4 Change the Polling Interval from 5m to **10m**.
- 5 Modify the command line `-c` parameter to reflect the new policy name (WBSSPI-WBS40-Med-10min) as follows:

```
wasspi_wbs_ca -c WBSSPI-WBS40-Med-10min...
```
- 6 Deploy the new policies.

Changing the Collection Interval for Selected Metrics

To change the collection interval for selected metrics, copy the appropriate collector policy and rename with a name reflecting the new interval, deleting all but the metrics you are changing. Set the new interval. Edit the original policy to remove the changing metrics. For example, to change the collection interval to 10 minutes for metrics 72-73, you would follow these steps:

Deleting metrics from the 5-minute policy to include in a new 10-minute policy.



- 1 From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **Medium-Impact** → **Monitors**.
- 2 Right-click on the collector policy **WBSSPI-40-Med-05min** and select **All Tasks** → **Edit...**
- 3 Click on **File** → **Save As** and change the Name to **WBSSPI-40-Med-10min**.
- 4 In the Program name text box, delete all metrics after the **-m** *except* **72-73**.
- 5 Change the **Polling Interval** to from 5m to **10m**.
- 6 Change the entry following **-c** to **WBSSPI-40-Med-10min**.
- 7 Select **Save and Close**.
- 8 Right-click on the **WBSSPI-40-Med-05min** policy and select **All Tasks** → **Edit**.
- 9 In the Program name text box, delete **72-73** after the **-m**.
- 10 Select **Save and Close**.
- 11 Deploy the modified policies.

Customize the Threshold for Different Servers

Customize the threshold as needed. For example, you may want to set the threshold for `SERVER_1` for metric 0212 to 20 and leave it at 10 for all other servers. To do so, copy the existing condition and modify it to serve as the exception. Follow these steps:

- 1 Double-click on the metric to open it for customization (for example, double-click on `WBSSPI-0213`).

The Measurement Threshold window displays.
- 2 Select the **Threshold levels** tab.
- 3 Press the **Specify instance filters** button.
- 4 Select the **Condition** tab.
- 5 Enter a Rule description (for example, "Rule for all servers except `SERVER_1`").
- 6 Press **OK**.
- 7 In the Measurement Threshold window, press the **Copy** button to make a copy of the rule.
- 8 Double-click on the copy of the rule. Enter a new Rule description (for example, "Rule for `SERVER_1`").
- 9 In the `Object name matches` field, enter the desired characters to use for pattern matching (in this example `SERVER_1`).
- 10 Select the **Actions** tab.
- 11 Double-click on the condition.
- 12 Change the name the condition to `WBSSPI-0213.2`.
- 13 Change the Threshold limit to **20**.
- 14 Press **OK**.
- 15 Press **OK**.
- 16 Verify the order of your rules (for example, make "Rule for `SERVER_1`" the first rule).
- 17 Click the **Matching test** button to test the pattern and verify pattern matching (you must set up a match file first).

Creating Custom, Tagged Policies

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

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

For example, you might create a group of policies and change each policy name to include `CLIENT01` in it. A metric policy might be named `CLIENT01-WBSSPI_0212` (retaining the metric number, which must be used). The collector policy name would be named `FIRST_CLIENT-40_05min`. You could then set up another group for `SECOND_CLIENT` and change all those policies to include the `SECOND_CLIENT` in the name.

To create the new policy group:

- 1 Copy the original policy group:
 - a Right-click on the policy group you want to copy and select **Copy**.

For example, right-click on the Metrics policy group under High-Impact and select **Copy**.
 - b Right-click on the group under which this policy group is located and select **Paste**.

For example, right-click on High-Impact and select **Paste**.
 - c Right-click on **Copy of Metrics** and select **Rename**. Rename the new group according to how you plan to identify the new metric and collector policies.

For example, rename the group to `CLIENT01HighImpactMetrics`.

- 2 Rename the original policies within the new policy group.

The names you give the new *metric policies* in the group would contain the new name followed by the original metric number. For example, a copy of WBSSPI_0001 could be called CLIENT01-WBSSPI_0001.

The name you give the new *collector policy* would also contain the identifying name. You would also modify the scheduled collection for the new group by inserting the `-t` property in the Program name text box. For example:

```
wasspi_wbs_ca -c FIRST_CLIENT-40-High-10min -m 16 -t CLIENT01-
```

In this case the copied collector policy has been renamed:
FIRST_CLIENT-40-High-10min

- a Right-click on the policy and select **All Tasks** → **Edit**.
 - b Click on **File** → **Save As**.
 - c Enter a new policy name and select **OK**.
- 3 Delete all original policies within the new policy group:

Highlight the original policies and hit **Delete**.

Monitoring WebSphere Application Server on Unsupported Platforms

The WBS-SPI supports monitoring WebSphere systems running on HP-UX, Solaris, AIX, Windows 2000 and 2003, Red Hat Linux, and Suse Linux. However, it is possible to configure the WBS-SPI to monitor WebSphere systems running on unsupported platforms—systems we refer to as “remote systems.”

The intent of this section is to help you determine if your environment is conducive to setting up remote monitoring. If you determine that your environment meets the criteria described below, and you have some expertise in using the WBS-SPI, this section offers an example to get you started.

Requirements for Monitoring Remote Nodes (running on Platforms not supported by WBS-SPI)

For a WebSphere system running on an unsupported platform, you can use WBS-SPI to monitor that remote system if the following conditions apply. The last condition is optional:

- The remote system is covered by a purchased license (using Tier 1 pricing).
- The WBS-SPI runs on at least one managed node on a supported platform: HP-UX, Solaris, AIX, Windows 2000, Windows 2003, Red Hat Linux, or Suse Linux.
- The local/proxy system and remote system must be running the same version of WebSphere Server. For example, if the proxy system is running WebSphere Server version 5, the remote system must also be running WebSphere Server version 5.
- (Optional, for logfile monitoring) The remote system runs on a platform supported by the OVO agent software.

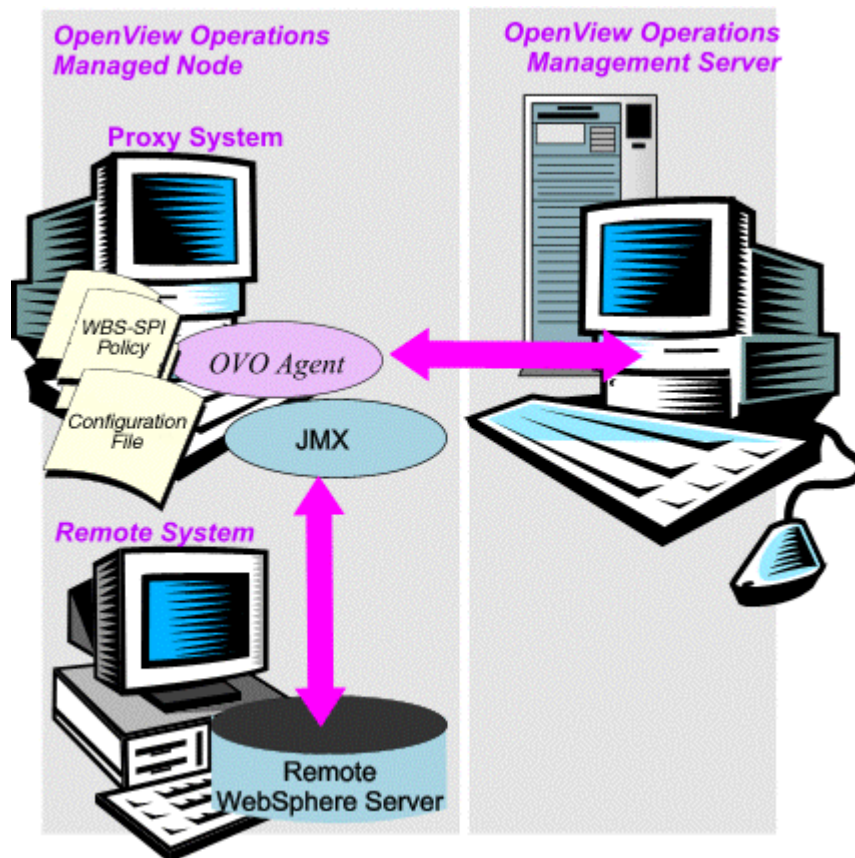
Overview

The following section provides an overview of remote monitoring and shows how it is implemented. Also included are details on how to set up the WBS-SPI to access WebSphere metrics and logfiles on unsupported platforms by using both the WBS-SPI and OVO agent software.

Remote Monitoring: How It Works

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

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



Configuration entries requirement: Within the configuration, entries for both local and remote systems are included. You can include multiple remote system entries in a local system's section. (Please refer to the example on [page 55](#), showing how the remote entry appears (with system IP address).

Policy deployment requirement: Policies for the correct WebSphere PMI level should be deployed on the local node. If you need a separate policy group (for example, High-Impact or Medium-Impact) to cover a different level, you can copy and rename the existing policies and specify the WebSphere Server name on the command line using the `-i` or `-e` options. Refer to a previous section in this chapter "Using WBS-SPI Policies, page 30" for details on using these command line parameters.

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



Monitoring remote systems using logfile versioning is not supported.

Configure Remote System Monitoring

You can monitor WebSphere Application Servers on remote systems (running on platforms other than HP-UX, Solaris, AIX, Windows 2000, Windows 2003, Red Hat Linux, or Suse Linux) by completing the following tasks.

Task 1: Configure the Remote WebSphere System

Using the Configure WBSSPI tool in the SPI Admin tools group, configure each local managed node that communicates with a remote WebSphere server. In the configuration, add entries for remote WebSphere servers.

- 1 At the OVO console, start the Configure WBSSPI tool.
- 2 Choose a WebSphere managed node from which to monitor the remote WebSphere server.

- 3** In the configuration that appears include an entry for each remote WebSphere system at the server-specific level:

`ADDRESS=<DNS server name or IP address>.`

The example configuration below shows how local and remote WebSphere servers are configured in the same file. Notice, however, that for the remote servers the `ADDRESS=<IP_address>` line is added:

```
ADDRESS=15.75.27.109 or
ADDRESS=harley.hp.com
```

Example Configuration

```
#
#####
HOME=C:/WebSphere/AppServer
JAVA_HOME=C:/WebSphere/AppServer/java

SERVER1_NAME=classact
SERVER1_PORT=900

SERVER2_NAME=harley
SERVER2_PORT=901
SERVER2_ADDRESS=harley.hp.com
```

There are two WebSphere servers configured in the preceding configuration. `SERVER1` is the local server, running on a Windows managed node. `SERVER2` is running on an OVO-managed node, that is a Linux system (a platform unsupported by WBS-SPI). The remote system is configured similar to that of the local system but contains the new line `SERVER2_ADDRESS=harley.hp.com`.

Task 2: (optional) Integrate OpenView Performance Agent

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

Task 3: Deploy Policies to the Local Node

Deploy a policy group to the local managed node. For example, deploy the High-Impact policy group on the local node if the local and remote managed nodes are to collect metrics that require the system be set at a high WebSphere PMI level.

- 1 From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere**.
- 2 Right-click on a policy group and select **All Tasks** → **Deploy on**.
- 3 Select the local managed node.
- 4 Click **OK**.

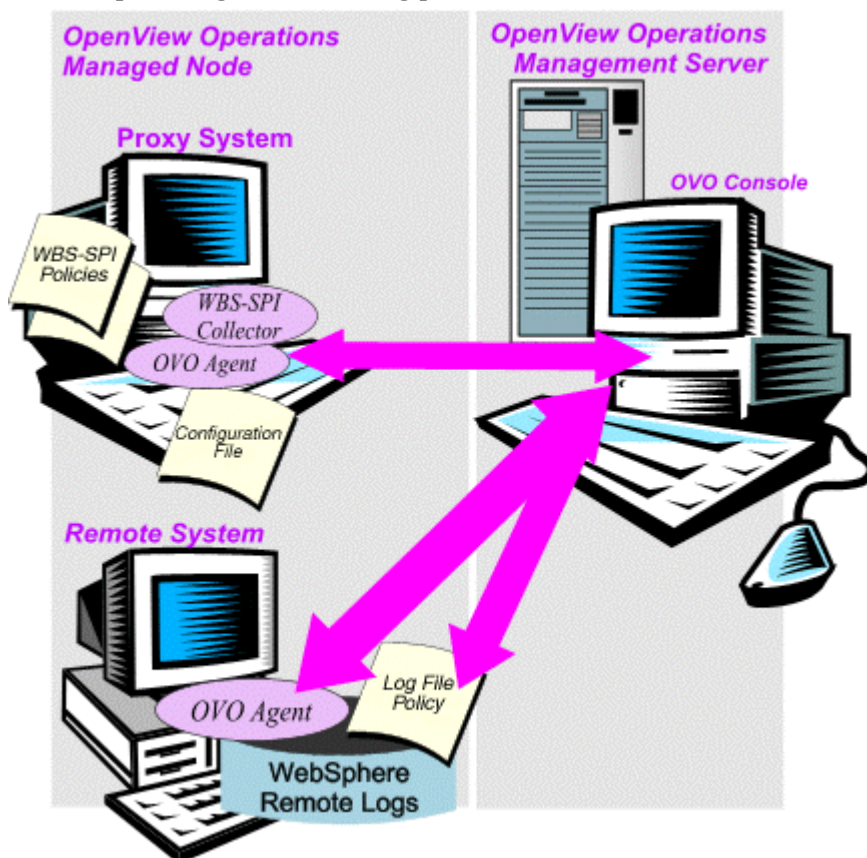
Configuring Remote Logfile Monitoring (Optional)

Monitoring remote system logfiles is supported if the following is true: (1) The remote system has an OVO agent running on it and (2) the system does not re-version logfiles when they roll. To set up logfile monitoring, at the OVO console, copy the WBS-SPI logfile policy and then configure, assign, and deploy the copied logfile policy to the remote system.

Configure the logfile policy for remote logfiles

- 1 Open a copy of the WebSphere Log Policy located under the WebSphere impact group.
 - a From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **High-Impact** → **Logfiles**.
 - b Double-click on the log policy
- 2 In the Logfile pathname text box, enter the location of the logfile on the remote system: `/<path>/<file_name>`.
- 3 Assign and deploy the logfile policy to the remote OVO-managed node.

The Log File Policy and the OVO Agent, both present on the remote system, make WebSphere logfile monitoring possible.



Remote Monitoring Limitations

- The WBS-SPI and the OVO agent do not support access to logfiles that are re-versioned each time the logs are rolled.
- When no OVO agent is present on the remote system, monitoring of WebSphere logfiles on the remote system cannot occur.
- WBS-SPI tools cannot be executed on remote systems.
- The proxy system and remote system must be running the same version of the WebSphere Server.

Re-installing the WBS-SPI Policies

To restore the default WebSphere policy group(s) you originally installed, you must remove and reinstall WBS-SPI. Refer to [Removing WBS-SPI](#) on page 15 and [Installing WBS-SPI](#) on page 11 for more information.

Using Policies/Tools to View Annotation Reports

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

Other policies have operator actions associated with them that allow you to generate a graph.



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

You can access the data as follows:

- **To view the Message Properties.** Double-click on a message in the OVO message browser. Reports are available in the Annotations tab area, showing data values on a single server.
- **To view reports.** From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **Metric Reports**. Double-click on the report. A report is generated for all WebSphere application servers on the selected managed node.
- **To view graphs.** Double-click on a message in the OVO message browser. Graphs can be generated in the Commands tab area, if an operator-initiated command has been configured and data has been collected. Select **Start** to generate the graph.

The View Graphs application launches your Web browser, which displays the graphing feature available in HP OpenView Performance Manager (which must be purchased separately).

Checking for indications of Automatic Reports in the OVO Message Browser

Severity	S	U	I	A	O	Received	Group	
Normal	-	-	X	-	-	1/27/2003 3:21:42 PM	OpC	
Normal	-	-	X	-	-	1/27/2003 3:21:42 PM	OpC	
Normal	-	-	X	-	-	1/27/2003 3:21:42 PM	OpC	
Critical	-	-	X	-	-	1/27/2003 3:21:42 PM	OpC	
Critical	O	-	X	S	S	X	1/27/2003 3:21:43 PM	WebSphere
Normal	-	-	X	-	-	1/27/2003 3:21:43 PM	OpC	
Normal	-	-	X	-	-	1/27/2003 3:21:43 PM	OpC	

Summary: 1156 Critical, 0 Warning, 0 Error, 13 Info, 263 Normal, 0 Unread, 0 Active.

Automatic Command Reports

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

How you know a report has been generated

When an Automatic Command Report is executed from OVO, the server is queried for additional data. If your message browser is set to display the "A" column, you will see an "S" under the "A" column (see illustration), which indicates that a successfully generated report is available in the *Annotations* area of the Message Properties.

How to view an automatic command report

To view the report, double-click on the message and select the *Annotations* tab. Column descriptions provide further clarification.

Reports

Reports run for all WebSphere instances configured on the managed node. The reports generated reflect the current state of WebSphere on the managed node. To generate a report in OVO, simply navigate down the console tree to the individual SPI for WebSphere reports, double-click on the report, and enter the name of a managed node.

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

Performance Impact Ratings (PMI Levels) of Reporting Metrics

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

The report below was generated for Metric 5 (I005):

```

Report for Application Server: Default Server
      Jan 29, 2003 11:25:50 AM
      Metric I005_JVMMemUtilPct

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

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

```

Reports and Graphs

The Smart Plug-in for WebSphere Application Server (WBS-SPI) can be integrated with the following HP OpenView reporting and graphing products (these products must be purchased separately):

- HP OpenView Reporter (Reporter)
- HP OpenView Performance Insight (OVPI)
- HP OpenView Performance Manager (OVPM)

HP OpenView Reporter. Reporter produces management-ready, web page reports, showing historical and trending information. This is *not* the version of Reporter that is included with HP OpenView Operations for Windows.

Working in conjunction with Reporter, the WBS-SPI produces a variety of reports showing consolidated information on the WebSphere Application Server.

Refer to [Using Reporter to Generate Reports](#) on page 64 for more information on how to integrate WBS-SPI with Reporter. After integrating WBS-SPI with Reporter, every night, Reporter generates reports that show the performance and availability of a WebSphere Application Server on configured managed nodes.

HP OpenView Performance Insight. OVPI is a network management system that collects, processes, and reports data. The data is used to generate reports. Refer to the *HP OpenView Performance Insight Administration Guide*

for more information about OVPI. Refer to the *Application Server Report Pack User Guide* for more information about WBS-SPI reports and how to integrate WBS-SPI with OVPI.

HP OpenView Performance Manager. OVPM provides graphing capability. This is *not* the version of OVPM that is included with HP OpenView Operations for Windows.

Refer to [Using OVPM to Generate Graphs](#) on page 67 for more information on how to integrate WBS-SPI with OVPM. After integrating WBS-SPI with OVPM, graphs are available the following day.

Using the OpenView Performance Agent

WBS-SPI relies on the default performance subagent (CODA) to collect and store performance data. CODA is automatically deployed on all OVO managed nodes. The performance data collected by CODA is used by integrated OVO for Windows graphing and reporting features (WBS-SPI Metric Reports tools, automatic command reports, and operator-generated graphs), Reporter, OVPI, and OVPM. The integrated OVO for Windows reporting and graphing features only work with data collected by CODA.

However, you may want to use the OpenView Performance Agent 3.x (OVPA or MeasureWare Agent) to collect and store performance data (OVPA is a product that must be purchased separately). The data collected by OVPA is used by Reporter, OVPI, and OVPM. The integrated OVO for Windows reporting and graphing features cannot use data collected by OVPA and therefore these features do not work if you use OVPA.



If you are running OVPA 4.x for Linux, you do not need to configure the WBS-SPI data collector to use OVPA. By default, the WBS-SPI detects and uses this version of OVPA to collect and store performance data. This version of OVPA works with the integrated OVO for Windows reporting and graphing features.

To configure the WBS-SPI data collector to use OVPA, do the following:

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

Operating System	File Location
HP-UX, Linux, or Solaris	<code>/var/opt/OV/conf/dsi2ddf/</code>
AIX	<code>/var/lpp/OV/conf/dsi2ddf/</code>
Windows	<code>\Program Files\HP OpenView\Installed Packages\{790C06B4 ...}\conf\dsi2ddf\</code>

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

- 2 Edit the `nocoda.opt` file to contain the following single line:
ALL
- 3 Save the file.

Using Reporter to Generate Reports

Prerequisite: You must configure the WBS-SPI, which includes software deployment, server connection configuration, and assignment/deployment of policies to targeted nodes.

The WBS-SPI report package must be installed on the Windows system running Reporter. You can install it directly from the CD as explained below.

- 1 Install the WBS-SPI report package on the Windows system running Reporter:
 - a Insert the Smart Plug-ins CD into the CD drive of the Windows system running Reporter.
 - b Go to the `WebSphere SPI Reporter Package` directory.
 - c Double-click on **WBSSPI-Reporter.msi**
 - d Complete the installation by following the instructions in the windows that display.
- 2 Check the Reporter status pane to note changes to the Reporter configuration.



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



For NT 4.0 managed nodes, during the installation you may get the error: 1604: This setup does not contain the Windows Installer engine [INSTMSIW.EXE] required to run the installation on this operating system.

In this case you must install the Microsoft Windows Installer from the Microsoft Web site.

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

You can find instructions in the Reporter Help for assigning WBS-SPI reports to the targeted nodes. To access Help, select **Reports** or **Discovered Systems** in the left panel of the Reporter main window and right-click it.

Select **Report Help** or **Discovered Systems Help** from the submenu that appears. See the topic “To assign a report definition to a Discovered Systems Group.”

- 3 Add group and single system reports by assigning reports as desired. (See the Reporter Help and the online *Concepts Guide* for complete information.)



Group and single system WBS-SPI reports require that you identify systems by their full name (for example, **abc.xyz.com** is acceptable while **abc** is not).

WBS-SPI Reports

The reports available through the integration of HP OpenView Reporter and WBS-SPI show consolidated data on server performance and availability on all WebSphere systems. In addition, other reports show data for single systems. These reports are available the day following your installation of the WBS-SPI report package on the Reporter Windows system. (Please refer to [page 64](#) if you have not yet completed the report package installation.)

The table that follows shows all pre-defined reports.

Table 1 All/Group Reports

Report Title	Description	Metric
DB Connection Pool Tput - Top 20	Shows the average number of connections allocated per day for the top 20 servers.	260
EJB Method Calls Rate - Top 20	Shows the number of all EJB method calls per minute for the top 20 servers.	22
Entity EJB Load/Stores - Top 20	Shows the number of all Entity EJB loads and stores to/from the database per minute for the top 20 servers.	24
Servlet Avg. Response - Top 20	Shows the average response time for the top 20 requested servlets for all servers for the reporting period.	245

Table 1 All/Group Reports

Report Title	Description	Metric
Servlet Requests - Top 20	Shows the total servlet request rate for the top 20 servers.	45
Servlet Sessions - Top 20	Shows the total servlet sessions being handled by the top 20 servers.	41
Transaction Throughput - Top 20	Shows the average throughput for the top 20 execute queues of all servers.	77

Removing the WBS-SPI Reporter Package

- 1 From the Control Panel, double-click on **Add/Remove Programs**.
- 2 From the Add/Remove Programs window, select **WBSSPI-Reporter**.
- 3 Click on **Remove**.
- 4 Complete the removal by following the instructions in the windows that display.

Using OVPM to Generate Graphs

To use Performance Manager, you must purchase and install it separately. To integrate WBS-SPI with OVPM, do the following:

- 1 Install the WBS-SPI graph package on the Windows system running Performance Manager:
 - a Insert the Smart Plug-ins CD into the CD drive of the Windows system running Performance Manager.
 - b Go to the /WebSphere SPI OVPM Configuration Package directory.
 - c Double-click on **WBSSPI-Grapher.msi**
 - d Complete the installation by following the instructions in the windows that display.
- 2 To graph any WebSphere metric, use the data source name:
`WBSSPI_METRICS`

Graphs are available the day following your installation of the WBS-SPI.

Viewing Graphs that Show Alarm Conditions

For graphing purposes, the WBS-SPI organizes metrics according to type. When a message is generated for any metric appearing in a table in the section that follows, you can view a chart of its and other metric values.

To view a graph associated with an alarm condition (operator-initiated action has been defined with the WBS-SPI policy), complete these steps:

- 1 In the OVO Message Browser double-click the message.
- 2 In the Message Properties window select the Commands tab.
- 3 Press **Start** to start the operator-initiated command.

The resulting action displays the metric's WBS-SPI graph, which charts its values along with the values of other metrics in the same group.

Viewing Graphs that Show Past/Current Conditions

You can generate any of the available graphs manually:

- 1 From the OVO console, select **Operations Manager** → **Reports & Graphs** → **Graphs** → **SPI for WebSphere**.
- 2 Select the type of graph you want to view.
- 3 Double-click on the graph you want to generate.

WBS-SPI Metrics Available for Graphs

The following tables show the graphs available for mapping collected metric values. If you are interested in viewing any one of the metrics included in any of these tables, you can use the View Graphs tool to launch the graph, which appears in your Web browser.

Table 2 Enterprise Java Beans (EJB): 20, 22, 24, 25, 26

Graph Label	Metric Name	Metric Description
EJB Pool Utilization	I020_EJBPoolUtil	Percentage of active beans in the pool.
EJB Method Calls Rate	I022_EJBMethCallsRt	Number of EJB method calls per minute.
EJB Entity Data Load Stored Rate	I024_EJBEntDatLdStRt	Number of times an EJB was written to or loaded from the database per minute.
EJB Pool Missed Percentage	I025_EJBPoolMissPct	Average percentage of time a call to retrieve an EJB from the pool failed.
EJB Connected Lives	I026_EJBConcLives	Average number of bean objects in the pool.

Table 3 JDBC: 61, 62, 65, 66

Graph Label	Metric Name	Metric Description
JDBC Connect Pool Waits	I061_JDBCConPoolWait	Average number of threads waiting for a connection from connections pools.
JDBC Connections Pool Wait Time	I062_JDBCConPoolWtTim	Average time that a client waited for a connections in milliseconds.
JDBC Connection Pool Timeout Rate	I065_JDBCConPoolTimRt	Number of times a client timed out waiting for a connection from the pool per minute.
JDBC Connection Pool Throughput	I066_JDBCConPoolThru	Number of connections allocated and returned by applications per second.

Table 4 Servlet: 40, 41, 42

Graph Label	Metric Name	Metric Description
Servlet Session Average Life	I040_ServSessAveLife	Average lifetime of a servlet session in milliseconds.
Servlet Active Sessions	I041_ServSessActSess	Number of sessions currently being accessed.
Servlet Invalidated Session Rate	I042_ServInvSessRt	Number of sessions being invalidated per second.

Table 5 ThreadPool: 13, 14

Graph Label	Metric Name	Metric Description
Thread Pool Percentage Maximum	I013_ThrdPoolPctMax	Percentage of time number of threads in pool reached configured maximum size.
Thread Pool Create Rate	I014_ThrdPoolCrtRt	Number of threads created per minute.

Table 6 Transaction: 70, 71, 72, 73, 74, 75, 76, 77, 78

Graph Label	Metric Name	Metric Description
Transaction (global) Duration	I070_TranGlobDur	Average duration of global transactions.
Transactions (local) Duration	I071_TranLocDur	Average duration of local transactions.
Transaction (global) Commitment Rate	I072_TranGlobCommDur	Average duration of commits for global transactions.
Transaction (Local) Commitment Duration	I073_TranLocCommDur	Average duration of commits for local transactions.
Transaction Rollback Rate	I074_TranRollbackRt	Number per second of global and local transactions rolled back.
Transaction Timeout Rate	I075_TranTimeoutRt	Number per second of timed out global and local transactions.
Transaction Commitment Rate	I076_TranCommitRt	Number per second of global and local transactions that were committed.
Transaction Throughput Rate	I077_TranThruput	Number per second of global and local transactions that were completed.
Transaction Start Rate	I078_TranStartRt	Number per second of global and local transactions that were begun.

Table 7 Web Application:

Graph Label	Metric Name	Metric Description
Web Application Servlet Request Rate	I045_WebAppServReqRt	Number of requests for a servlet per second.
Web Application Servlet Error Rate	I047_WebAppServErrRt	Number of errors in a servlet per second.
Web Application Servlet Load	I048_WebAppServLoad	Number of servlets currently loaded for a web application.
Web Application Server Reload Rate	I049_WebAppServRelRt	Number of servlets reload for a web application per minute.

Launching the Web Page display with an Operator Action that Generate Graphs

Performance Manager graphs can be generated from most WBS-SPI alarm messages by double-clicking on the message, selecting the `Commands` tab, and selecting **Start** in the `Operator Initiated` section. The operator action launches your Web browser, which can then display a graph of the metric that generated the message as well as other related metrics.

Specifying a Date Range

Within the Web page display, you can specify a date range of one day, one week, one month, or one year. Please see the online Help for instructions on changing display settings.

Removing the WBS-SPI Grapher Package

- 1 From the Control Panel, double-click on **Add/Remove Programs**.
- 2 From the Add/Remove Programs window, select **WBSSPI-Grapher**.
- 3 Click on **Remove**.
- 4 Complete the removal by following the instructions in the windows that display.

Troubleshooting WBS-SPI

This chapter covers troubleshooting the Smart Plug-in for WebSphere Application Server (WBS-SPI).

Error messages (listed by number) are available in the online help.

Using the Self-Healing Info Tool

Preferred troubleshooting method: Troubleshooting information is enhanced with cross-referencing capabilities available through the HP support site: http://support.openview.hp.com/self_healing.jsp. To access this information and the search capabilities available on the site, you must first download and configure the Self-Healing Services client software, an added benefit of your HP support contract. A link is then automatically set up to the self-healing services web site, where your SPI problem can be matched to similar SPI problems/solutions for increased troubleshooting effectiveness. Refer to the Self-Healing Services section in the *SPI CD Installation Guide* for information on how to download, configure, and use the software and its automatic link to the HP web site support service.

Alternative troubleshooting method: If self-healing services is not installed/configured on the node, you can use the Self-Healing Info tool. This tool also gathers SPI troubleshooting data and stores it in a file that you submit to HP support for assistance. Refer to the online help for more information about using this tool.

Log and Trace Files

Management Server

The following log file is found on the management server (typically, `\<%OvInstallDir%>\is \Program Files\HP OpenView\Data\shared\`):

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

UNIX Managed Nodes

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

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

File Type	Log
Directory	/ <i><OvAgentDir></i> /wasspi/wbs/log/config.log
Description	Records output from configuration scripts.
File Type	Log
Directory	/ <i><OvAgentDir></i> /wasspi/wbs/log/errorlog
Description	Records WBS-SPI error messages. This log file is monitored by WBS-SPI policies.
File Type	Trace
Filename	/tmp/wasspi_wbs_disc.trc (archived files have a three digit number appended to the filename)
Description	Discovery binary trace file used by your HP support representative. By default, tracing to this file is enabled. To disable tracing, in <i><OvAgentDir>/bin/instrumentation/wasspi_wls_discoveryUnix.pl</i> , set the <i>\$trace_on</i> variable to 0. To disable this trace, set the <i>\$trace_on</i> to 1. When instrumentation is deployed, the <i>wasspi_wls_discoveryUnix.pl</i> file is overwritten (therefore, if you disable tracing, it becomes enabled when instrumentation is deployed). Five archived versions are kept. A new trace file is created when the discovery policy is run.
File Type	Trace
Directory	/ <i><OvAgentDir></i> /wasspi/wbs/log/trace.log (archived files have a three digit number appended to the filename)
Description	Trace file used by your HP support representative. By default, tracing to this file is disabled. To enable this tracing, use the WLS SPI Trace - Start tool.

Windows Managed Nodes

The following log and trace files are found on the managed nodes running on Windows (typically, `<%OvAgentDir%>` is

`\Program Files\HP OpenView\Installed Packages\{790 ...}\`):

File Type	Log
Filename	<code>\<%OvAgentDir%>\log\javaagent.log</code>
Description	OVO discovery agent log file containing the status of the OVO discovery agent. By default, logging to this file is enabled at <code>LOG_LEVEL 3</code> . Set the <code>LOG_LEVEL</code> variable in <code><%OvInstallDir%>\conf\svcDisc\OvJavaAgent.cfg</code> to 6 or higher (up to 9) to capture troubleshooting information (the higher the number, the more information is collected). To disable this log, set the <code>LOG_LEVEL</code> to 0. Additional information can be configured in this file to define log file size and the number of archived files kept. By default, the log file size is 1MB and five archived versions are kept.
File Type	Log
Directory	<code>\<%OvAgentDir%> \wasspi\wbs\log\config.log</code>
Description	Records output from configuration scripts.
File Type	Log
Directory	<code>\<%OvAgentDir%> \wasspi\wbs\log\errorlog</code>
Description	Records WBS-SPI error messages. This log file is monitored by WBS-SPI policies.

File Type	Trace
Filename	C:\temp\wasspi_wbs_disc.trc (archived files have a three digit number appended to the filename)
Description	Discovery binary trace file used by your HP support representative. By default, tracing to this file is enabled. To disable tracing, in <code>\<%OvInstallDir%>\bin\instrumentation\wasspi_wbs_discoveryWin.pl</code> , set the <code>\$trace_on</code> variable to 0. To disable this trace, set the <code>\$trace_on</code> to 1. When instrumentation is deployed, the <code>wasspi_wls_discoveryWin.pl</code> file is overwritten (therefore, if you disable tracing, it becomes enabled when instrumentation is deployed). Five archived versions are kept. A new trace file is created when the discovery policy is run.

File Type	Trace
Directory	<code>\<%OvAgentDir%> \wasspi\wbs\log\trace.log</code> (archived files have a three digit number appended to the filename)
Description	Trace file used by your HP support representative. By default, tracing to this file is disabled. To enable this tracing, use the <code>WLSSPI Trace - Start</code> tool.

WBSSPI Discovery Policies

- If the WBSSPI Discovery policies do not automatically discover and update the WBS-SPI configuration, do the following:
 - Check if the WBSSPI Discovery policies are still being deployed:

From the OVO console, select **Operations Manager** → **Policy management** → **Deployment jobs**.

If the state of a WBSSPI Discovery policy is `Active`, then the policy is still being deployed. Wait for the deployment of the policy to complete.

If the state of a WBSSPI Discovery policy is `Suspended` or `Error`, then check for any error messages in the message browser and continue to troubleshoot the problem by reading the rest of this section.

If the WBSSPI Discovery policies are not listed, check the message browser for the following message:

```
WASSPI-502: INFO - Updating the WBSSPI configuration
data with discovered information
```

If this message is present and the letter “S” (for successful) appears in the A column, the WBSSPI Discovery policies have been successfully deployed.

If this message is not present or the letter “F” appears in the A column, the WBSSPI Discovery policies were not successfully deployed.

Continue to troubleshoot the problem by reading the rest of this section.

- Verify the WebSphere application server status. The application server must be working. See [Task 2: Verify the Application Server Status](#) on page 20 for more information.
- If the software registry file or key of the WebSphere application server is not found (see [Table 1](#) for locations), verify the installation directory of the server. If the WebSphere application server is not installed in the default path (see [Table 2](#) for the default path), configure the HOME property using the non-default installation path (refer to the online help for more information about setting the properties).

The software registry file or key can be found in the following locations:

Table 1 Software Registry File/Key Locations

Operating System	Software Registry File/Key
AIX	/usr/lpp/IBMWebAS.base.WASserver/deinst1/IBMWebAS.base.WASserver.prc_d
HP-UX	/var/adm/sw/products/IBMWebAS/WASserver/INDEX
Solaris	/var/sadm/pkg/WASserver/pkginfo
Windows	HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere Application Server\4.0\APPSERVER_ROOT

The default installation path for the WebSphere application server is:

Table 2 WebSphere Application Server Default Installation Path

Operating System	Default Installation Path
AIX	/usr/WebSphere/AppServer
HP-UX, Linux, Solaris	/opt/WebSphere/AppServer
Windows	C:\Program Files\WebSphere\AppServer

- Verify that the Configure WBSSPI tool is not running and/or a configuration is not open in an editor. Only one process can access a configuration at a time. If a configuration is open, other processes that must access that file (like the discovery policy) hang until the file becomes available.
- If the service map is not updated and the Medium-Impact policy group is not deployed, do the following:
 - Verify the WebSphere application server status. The application server must be running. See [Task 2: Verify the Application Server Status](#) on page 20 for more information.
 - Verify that the WebSphere Admin Server is running on the managed node. If you can start the WebSphere Admin Console, the WebSphere Admin Server is running.

Manually Deploying the Discovery Policies

If the WBSSPI Discovery policies do not deploy successfully when you run the Discover WebSphere tool, you can manually deploy them to the managed nodes on which the WebSphere Admin Servers are running (they *must* be deployed in the order shown):

- 1 From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0** → **WBSSPI Discovery**.
- 2 Right-click on **WBSSPI-Messages** and select **All Tasks** → **Deploy on**.
- 3 Select the node(s) on which to deploy the auto-discovery policies.
- 4 Click **OK**.

- 5 Right-click on **WBSSPI Service Discovery** and select **All Tasks** → **Deploy on**.
- 6 Select the node(s) on which to deploy the auto-discovery policies.
- 7 Click **OK**.

Verify Discovery Policy Deployment is Currently Active

To check if the WBSSPI Discovery policies are still being deployed, from the OVO console, select **Operations Manager** → **Policy management** → **Deployment jobs**.

- If the state of a WBSSPI Discovery policy is **Active**, then the policy is still being deployed. Wait for the deployment of the policy to complete.
- If the state of a WBSSPI Discovery policy is **Suspended** or **Error**, then check for any error messages in the message browser and continue to troubleshoot the problem by reading the rest of this section.
- If the WBSSPI Discovery policies are not listed, the policy has been deployed.

The Configuration

- Verify that the node name specified in a node or group block matches the primary node name configured in OVO. To display the primary node name, do the following:
 - From the OVO console, select **Operations Manager** → **Nodes**.
 - Right-click on the node and select **Properties**.
 - Select the **Network** tab.

Tools

Message	Configuration variable SERVER<n>_START_CMD missing for server "Default Server"
Solution	Before you can successfully run the Start WebSphere tool, you must set the START_CMD and USER properties. Set these properties using the Configure WBSSPI tool. Refer to the online help for more information about this tool.

Message	Configuration variable SERVER<n>_STOP_CMD missing for server "Default Server"
Solution	Before you can successfully run the Stop WebSphere tool, you must set the STOP_CMD and USER properties. Set these properties using the Configure WBSSPI tool. Refer to the online help for more information about this tool.

C

Coda, overriding with MeasureWare Agent **63**

collection intervals
 changing for all servers **46**
 changing for selected metrics **47**

collector policy
 description of **31**

collector/analyzer
 description of **33**
 what it does **31**

command
 wasspi._wbs_ca, description of **33**

customizations
 creating new policies **49**

D

defaults, restoring policy **58**

deinstallation
 removing WBS-SPI **17**

directories
 locations for trace file/error logs **75, 77**

F

files, locations on management server/
 managed nodes **75, 77**

G

graphs
 generating with Reporter's graphing capabilities **67**
 instructions for manually generating **68**
 launching display within Web browser **71**
 list of metrics for server status graph **68**
 OVPM **62**
 policies available for **68**
 showing alarm conditions **67**
 specifying date range within **71**

H

HP OpenView Reporter, integrating WBS-SPI with **61**

HP Performance Manager, using WBS-SPI with **61**

L

Linux, monitoring WebSphere installed on **51**

M

messages

policy configuration for **39**

Message Source policy groups, description of
WBS-SPI groups **30**

metric policies

description of **32**

metrics

modifying collections in the collector
policy **41**

O

OpenView Performance Agent

(MeasureWare Agent), using **63**

operator actions

graphs generated from **67**

P

performance impact rating, metrics in tools
60

Performance Manager, using WBS-SPI with
61

policies

changing **33**

customizing message displayed for alerts
39

customizing message text **39**

customizing thresholds **35**

customizing with the tag option **49**

deploying **23**

description of **31**

modifying **33**

re-installing defaults **58**

policy groups

changing collection intervals **47**

creating custom with the tag parameter
49

description **30**

proxy configured monitoring **51**

R

remote monitoring

requirements for **54**

remote systems

setup procedure for monitoring **54**

remote systems, monitoring **51**

removing WBS-SPI software **15**

Reporter

integrating WBS-SPI to work with **61**

setting up WBS-SPI to work with **64**

reports

generated from HP OpenView Reporter
65

OVPI **61**

Reporter **61**

tool generated **58**

using HP OpenView Reporter to
generate **61**

reports (automatic action)

how they are generated **58**

S

servers

setting thresholds for different **48**

T

tag option

creating custom policy groups with **49**

thresholds

customizing **35**

exceeded

viewing graphs resulting from **67**

settings for different servers **48**

U

unsupported platforms, monitoring
 WebSphere on **54**

upgrading WBS-SPI **12**

W

wasspi_wbs_ca, description of **33**

WBS-SPI
 removing **15**
 upgrading **12**

