HP OpenView Smart Plug-in for WebSphere Application Server

Configuration Guide

Version: B.02.09

For Windows OpenView Operations Management Servers

February 2004

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this manual, 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

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.

Support

Please visit the HP OpenView website at:

http://openview.hp.com/

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView website includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

contents

1

WBS-SPI Concepts

Introduction

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
- Reports and graphs
- Error messages

Software Requirements

Table 1 Management Server

Component	Supported Version(s)
HP OpenView Operations for Windows	7.2, 7.21

Table 2 Managed Nodes

Component	Supported Version(s)
HP OpenView Operations for Windows Agent	7.2, 7.21
AIX	4.3, 5.1, 5.2
HP-UX	11.00, 11.11, 11.23
Solaris	7, 8, 9
Windows	NT 4.0 and SP5+, Windows 2000 Server
Windows Script Host (for NT 4.0 only)	5.6[a]
WebSphere Application Server	Advanced Edition 4.0.1, 4.0.2[b], 4.0.3[b], 4.0.4[b] Enterprise Edition 4.1 Express 5.0 Regular 5.0
MeasureWare UNIX®	C.02.00 or higher
MeasureWare NT	C.02.00 or higher
MeasureWare Windows 2000	C.03.00 or higher
HP OpenView Reporter	A.03 or higher
HP OpenView Performance Manager	4.0 or higher

[a] Go to http://msdn.microsoft.com/library/default.asp?url=/downloads/list/webdev.asp/ to download this component. See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/wsconwhatiswsh.asp for more information about Windows Script Host.

[b] Install the WebSphere code fix. See "Installing the WebSphere Code Fix" on page 11 for more information.

Installing the WebSphere Code Fix

If you are running WebSphere Application Server version 4.0.2, 4.0.3, or 4.0.4, download the following WebSphere code fix:

1. Go to `http://www.ibm.com/software/webservers/appserv/support/`.
2. Under “Software downloads,” select **All code fixes and support tools**.
3. Under “Refine your search,” do the following:
   - a. For “Limit by type,” select **-Updates (code fixes)**.
   - b. In the “Limit by adding search terms” field, enter **`PQ68219`**.
   - c. Click **Submit**.
4. Click on the name of the item found.
5. Read the information and install the code fix.

2

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

The WBS-SPI can be installed in the following manner:

- Install WBS-SPI and OVO simultaneously
- Install WBS-SPI with OVO already installed

Installing WBS-SPI and OVO

If you are installing OVO for the first time, you can install WBS-SPI at the same time:

1. Follow the installation instructions in the *HP OpenView Operations/ Performance for Windows Installation Guide.*
2. When the Product Selection window displays, be sure to select the checkbox next to IBM WebSphere listed under the Smart Plug-ins section.

3. Complete the installation as described in the *HP OpenView Operations/Performance for Windows Installation Guide*.

Installing WBS-SPI with OVO Installed

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 *hp OpenView New and Upgraded Smart Plug-ins and Integration Modules for OV operations for Windows 7.10, 7.20, 7.21* 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

To upgrade to WBS-SPI version B.02.09, do the following:

1. Install the WBS-SPI. Refer to "Installing WBS-SPI" on page 13 for more information.
2. Create the WBSSPI node group:

   In the console tree, select **Tools** → **SPI for WebSphere Server** → **WBSSPI - WebSphere Server Admin** → **WBSSPI Create Node Groups**.

   All the nodes found in the WBS-SPI service map are placed in the WBSSPI node group.
3. Deploy new instrumentation to the WBSSPI node group:

   a. Select the **WBSSPI** node group and right-click on it.

   b. Select **All Tasks** → **Deploy instrumentation**.

4 Verify the version of the WBS-SPI policies:

a In the console tree, select **Policy management** → **Policies group by type** → **Measurement Threshold**.

b Verify that the following policies are version 3.0:

WBSSPI-40-High-05min
WBSSPI-40-High-15min
WBSSPI-40-High-1h
WBSSPI-40-Low-05min
WBSSPI-40-Low-15min
WBSSPI-40-Low-1h
WBSSPI-40-Med-05min
WBSSPI-40-Med-15min
WBSSPI-40-Med-1h

5 Deploy the polices listed above to all nodes on which they were previously deployed (when you deploy the policies, these nodes are automatically selected).

a Select a policy and right-click on it.

b Select **All Tasks** → **Deploy on**.

The nodes on which the policy was previously deployed should be selected by default.

c Select **OK**.

Repeat these steps for each policy.

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 3: 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 WBSSPI Create 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 the WBS-SPI Software from the Management Server

1. Insert the *hp OpenView New and Upgraded Smart Plug-ins and Integration Modules for OV operations for Windows 7.10, 7.20, 7.21* 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.

3

Configuring WBS-SPI

Introduction

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:

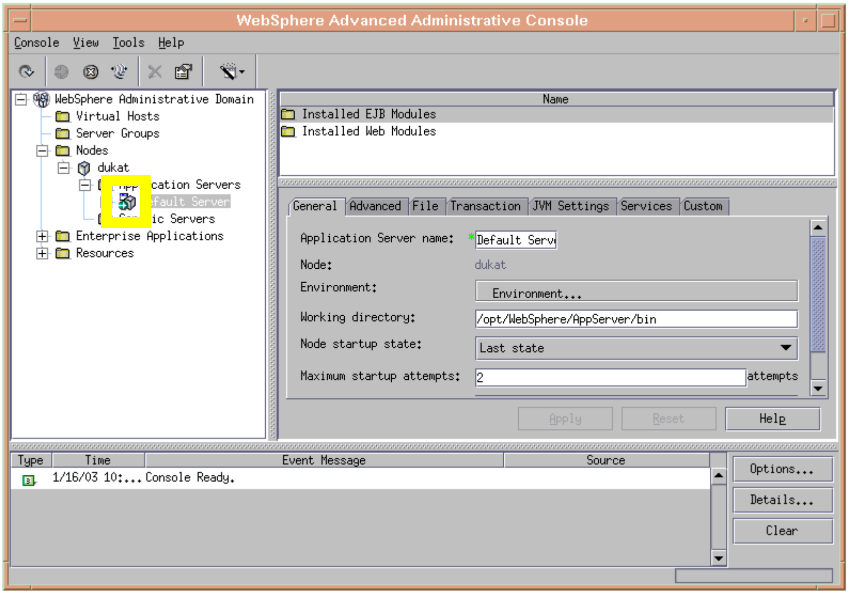
1. Install the OVO agent on the node. Refer to the OVO online help topic “Agent Installation on UNIX computers” for more information.
2. Specify each WebSphere Server node on UNIX to be managed. Refer to the OVO online help topic “Configure Managed Nodes” for more information.

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. 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.



Application Server name: Default Serv

Node: dukat

Environment: Environment...

Working directory: /opt/WebSphere/AppServer/bin

Node startup state: Last state

Maximum startup attempts: 2 attempts

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

Task 3: Collect WebSphere Login Information

If security is enabled on the WebSphere server, collect the username and password for each WebSphere Admin Server. This information is 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: Configure WBS-SPI with WebSphere Server 5 Information
- Task 2: Run WBSSPI Discover
- Task 3: Verify the Discovery Process

Task 1: Configure WBS-SPI with WebSphere Server 5 Information

If you are running WebSphere Server version 5 on a managed node, you must manually configure the WBS-SPI with the WebSphere Server version 5 information (the automatic discovery function of the WBSSPI Discover tool only supports WebSphere Server version 4). If you are not running WebSphere Server version 5 on any managed nodes, go to task 2.

To configure WBS-SPI, do the following:

1. From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **WBSSPI - SPI Admin**.
2. Double-click on **WBSSPI Configure**.
3. Select the managed node(s) to configure (the managed nodes on which WebSphere Server version 5 is running).
4. Click **Launch**.
5. Click **Next** in the “Introduction” window.
6. Set the properties. Select the help button to display more information about required and conditional properties and using the editor.
7. Select **Save**.
8. Select **Next**.

Select **OK**.

Task 2: Run WBSSPI Discover

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

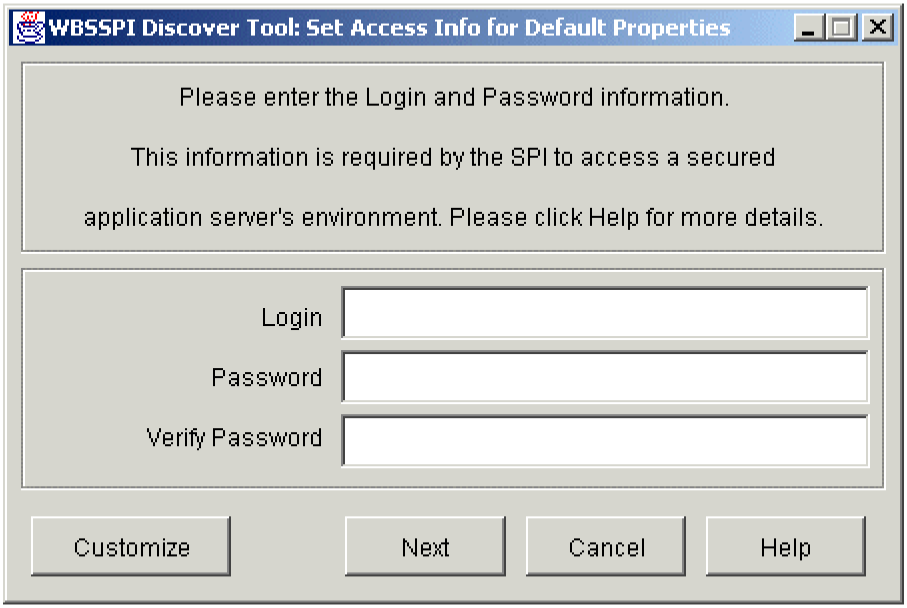
To run WBSSPI Discover, do the following:

1. From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **WBSSPI - SPI Admin**.
2. Double-click on **WBSSPI Discover**.
3. Select the managed node(s) on which WebSphere is running. If you completed task 1 (configure WBS-SPI with WebSphere Server 5 information), also select the managed node(s) on which WebSphere Server version 5 is running (WBSSPI Discover updates the service map with the WebSphere Server version 5 information).
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 WBSSPI Discover 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.



WBSSPI Discover Tool: Set Access Info for Default Properties

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.

Login

Password

Verify Password

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 21. 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 WBSSPI Discover 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 91 in the Troubleshooting WBS-SPI chapter to diagnose the problem.

Task 3: 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 91 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** → **WBSSPI - SPI Admin**.

   b Double-click on **WBSSPI 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. Setting some of these properties and configuring additional components depends on your environment.

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

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

If you are configuring user-defined metrics, set the UDM_DEFINITIONS_FILE property. Refer to "User Defined Metrics" on page 71 for additional 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 OpenView Reporter to Generate Reports" on page 61 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_SERVER property. Refer to "Integrating WBS-SPI with HP OpenView Performance Manager" on page 64 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** → **WBSSPI - SPI Admin**.
2. Double-click on **WBSSPI Configure**.
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 WBSSPI Discovery policy automatically deploys the WebSphere 4.0 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 (WebSphere 4.0 High Impact, WebSphere 4.0 Low Impact, or your own custom policies), do the following:

1. Remove the existing WebSphere 4.0 Medium Impact policy group:

   a. From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0.**

   b. Right click on **WebSphere 4.0 Medium Impact** and select **All Tasks** → **Uninstall from**.

   c. Select the node(s) from which you want to remove the WebSphere 4.0 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** → **WebSphere 4.0.**

   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 WebSphere 4.0 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 nod, 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.

4

Using and Customizing the WBS-SPI

Introduction

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:

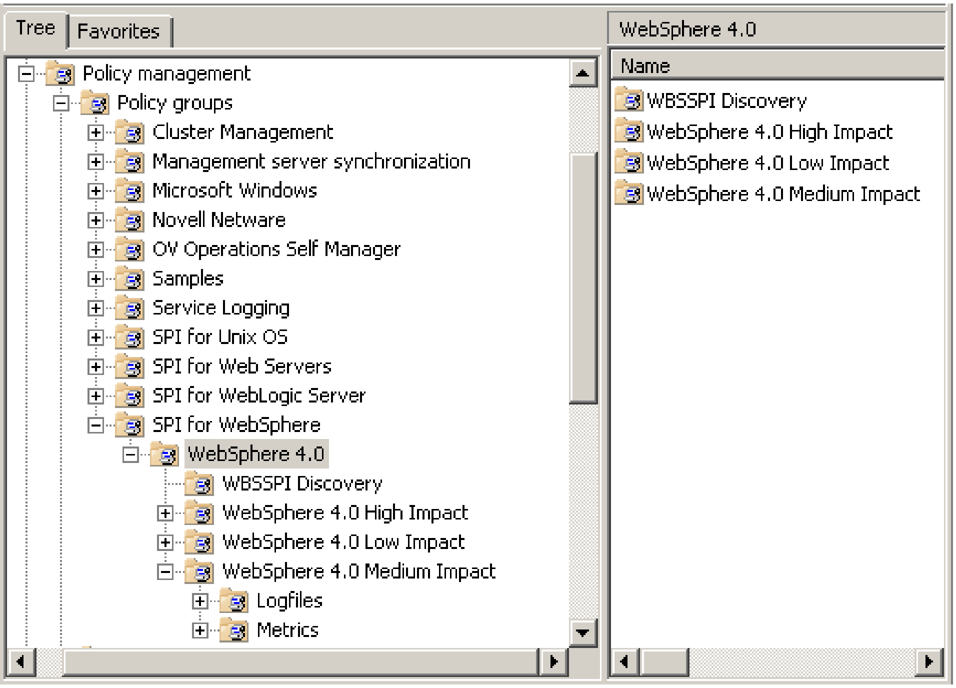
- Using the WBS-SPI Policies
- Basic Policy Customizations
- Advanced Policy Customizations
- Reinstalling WBS-SPI Policies
- Using Policies/Tools to Generate Reports

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 WebSphere 4.0 subgroup (as shown below) into *High*, *Medium*, and *Low* Impact groups.



Tree | Favorites

- Policy management
  - Policy groups
    - Cluster Management
    - Management server synchronization
    - Microsoft Windows
    - Novell Netware
    - OV Operations Self Manager
    - Samples
    - Service Logging
    - SPI for Unix OS
    - SPI for Web Servers
    - SPI for WebLogic Server
    - SPI for WebSphere
      - WebSphere 4.0
        - WBSSPI Discovery
        - WebSphere 4.0 High Impact
        - WebSphere 4.0 Low Impact
        - WebSphere 4.0 Medium Impact
          - Logfiles
          - Metrics

WebSphere 4.0

Name
WBSSPI Discovery
WebSphere 4.0 High Impact
WebSphere 4.0 Low Impact
WebSphere 4.0 Medium Impact

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 WebSphere 4.0 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 *WebSphere 4.0 High*, *Medium*, and *Low* subgroups contain metric and collector policies that work as follows:

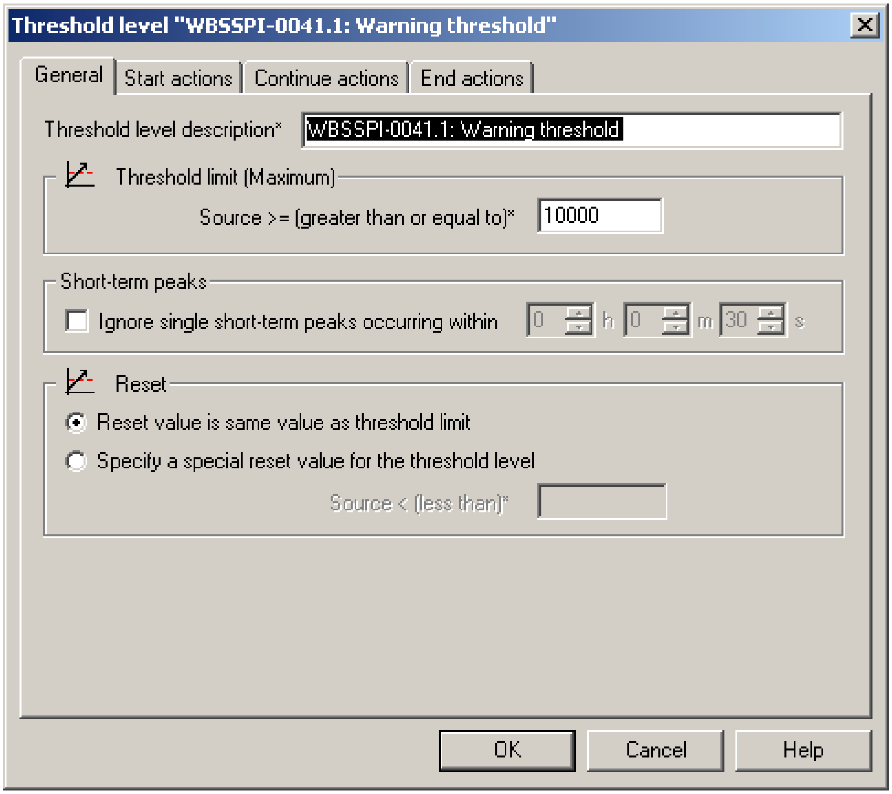
- ***Metrics*** interpret incoming values of WebSphere’s performance levels and availability. Each value is evaluated according to the metric with which it is associated. If it is acceptable, it is ignored; if it is not, a message is sent to the OVO Message browser and an automatic action may execute.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

- ***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.



Threshold level "WBSSPI-0041.1: Warning threshold"

General | Start actions | Continue actions | End actions

Threshold level description* WBSSPI-0041.1: Warning threshold

Threshold limit (Maximum)

Source >= (greater than or equal to)* 10000

Short-term peaks

□ Ignore single short-term peaks occurring within 0 h 0 m 30 s

Reset

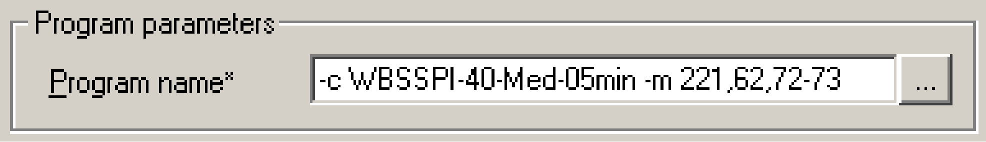
● Reset value is same value as threshold limit

○ Specify a special reset value for the threshold level

Source < (less than)*

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).



Program parameters

Program name* -c WBSSPI-40-Med-05min -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.

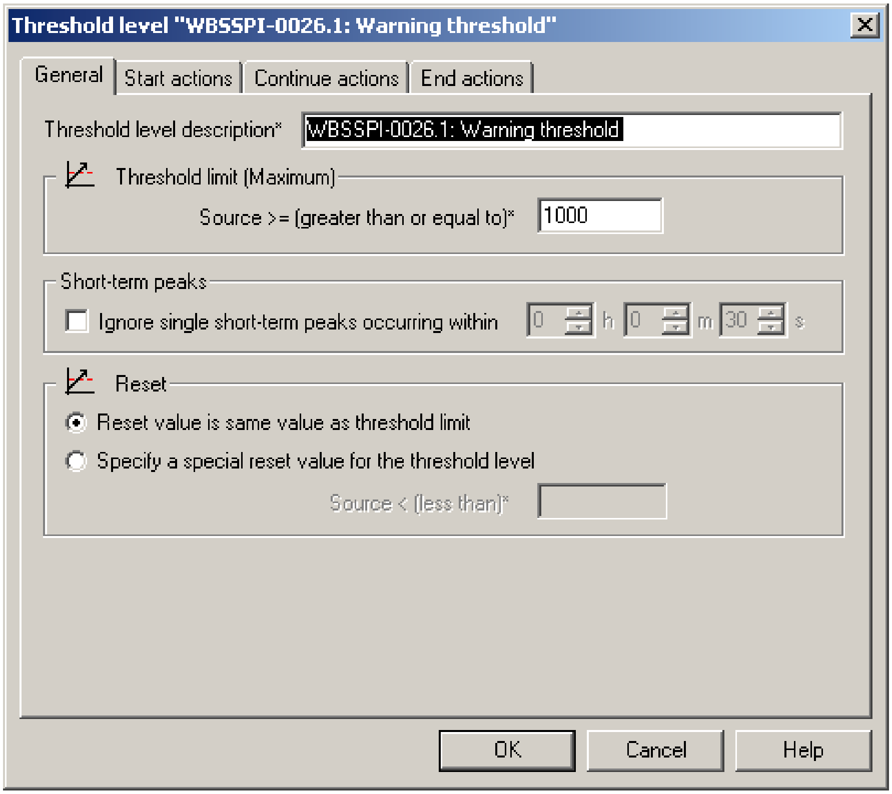
Modifying Metric Policies

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** → **WebSphere 4.0** → **WebSphere 4.0 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.



Threshold level "WBSSPI-0026.1: Warning threshold"

Threshold level description* WBSSPI-0026.1: Warning threshold

Threshold limit (Maximum)

Source >= (greater than or equal to)* 1000

Short-term peaks

□ Ignore single short-term peaks occurring within 0 h 0 m 30 s

Reset

● Reset value is same value as threshold limit

○ Specify a special reset value for the threshold level

Source < (less than)*

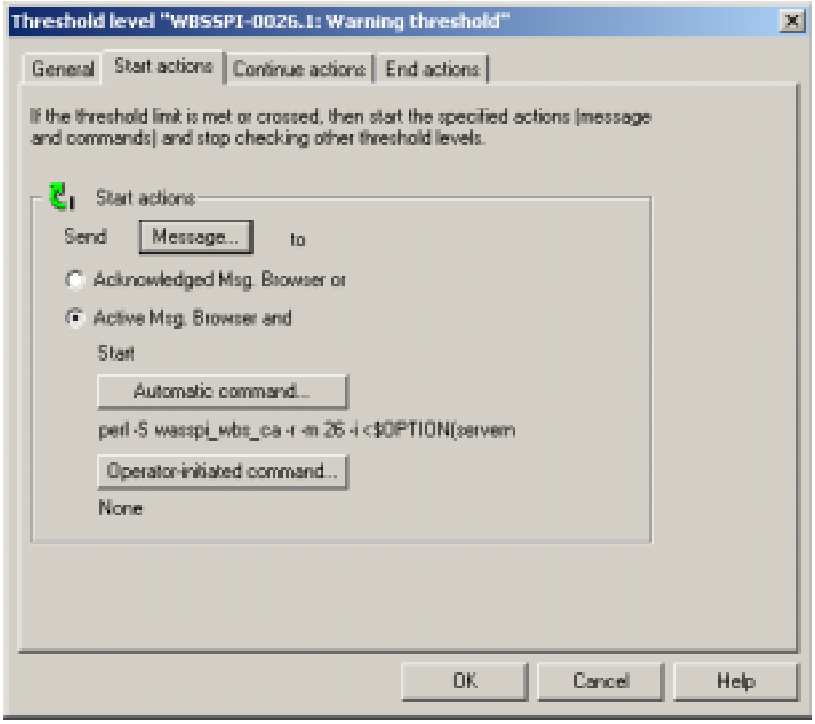
In the figure above, the threshold limit is set to 1000 for WBSSPI-0026. The incoming values for this metric show the total number of times per minute clients must wait for an available (Enterprise Java) bean. A value of more than 1000 would start to impact the server response time the client experiences,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



Threshold level "WBSSPI-0026.1: Warning threshold"

If the threshold limit is met or crossed, then start the specified actions (message and commands) and stop checking other threshold levels.

Start actions

Send Message... to

○ Acknowledged Msg. Browser or

● Active Msg. Browser and

Start

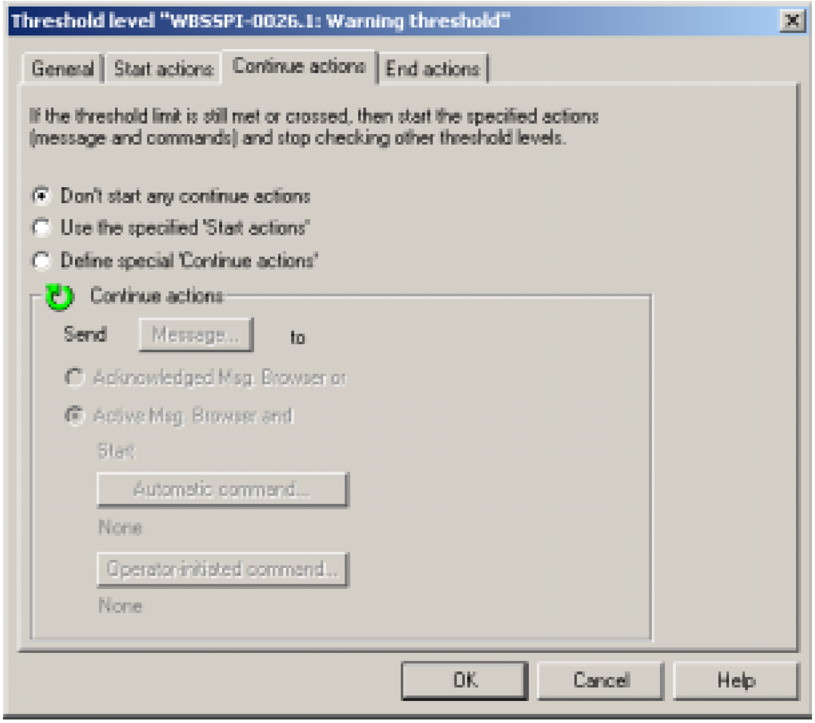
Automatic command...

```
perl -S wasspi_wbs_ca -t -m 26 -i <$OPTION(serverm
```

Operator-initiated command...

None

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



If the threshold limit is still met or crossed, then start the specified actions (message and commands) and stop checking other threshold levels.

● Don't start any continue actions
○ Use the specified 'Start actions'
○ Define special 'Continue actions'

Continue actions

Send [Message...] to

○ Acknowledged Msg. Browser or
● Active Msg. Browser and

Start

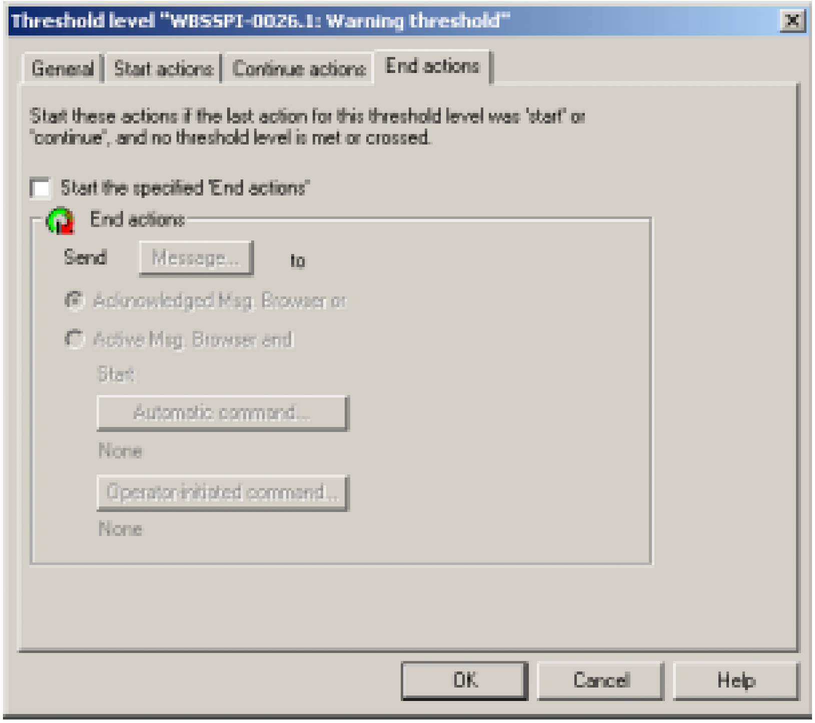
[Automatic command...]

None

[Operator-initiated command...]

None

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



Start these actions if the last action for this threshold level was 'start' or 'continue', and no threshold level is met or crossed.

□ Start the specified 'End actions'

End actions

Send Message... to

● Acknowledged Msg. Browser or

○ Active Msg. Browser and

Start:

Automatic command...

None

Operator-initiated command...

None

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:

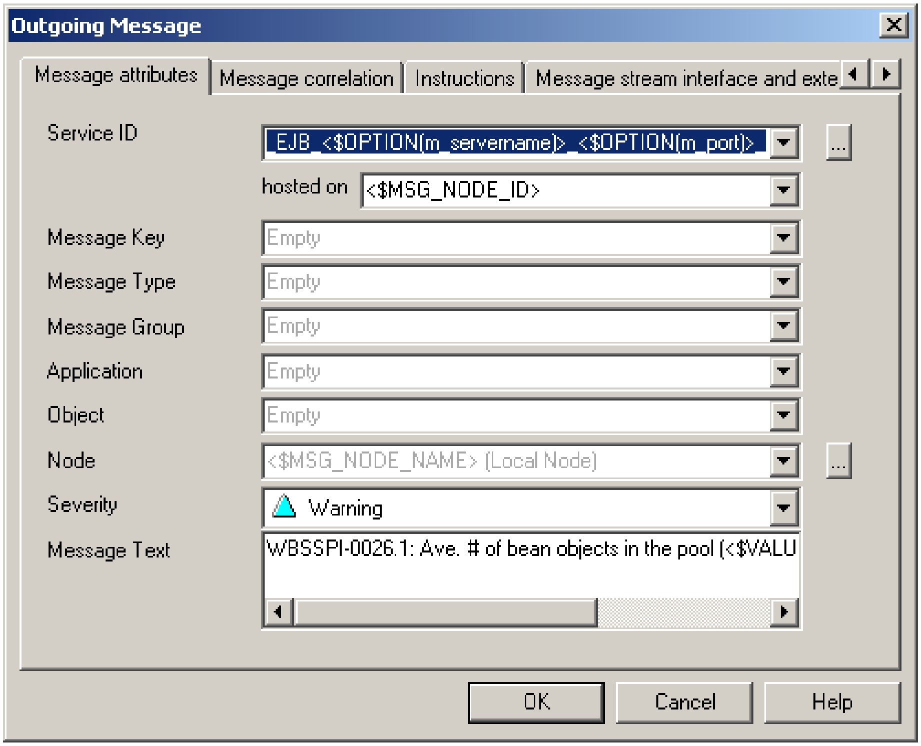
- **Automatic command**. A command run when the rule is matched. The automatic command delivered with the WBS-SPI generates a snapshot *report* that shows the data values at the time the action was triggered from an exceeded threshold. You can view the report in the message annotations.

- **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.



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 WebSphere 4.0 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 WebSphere 4.0 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**.

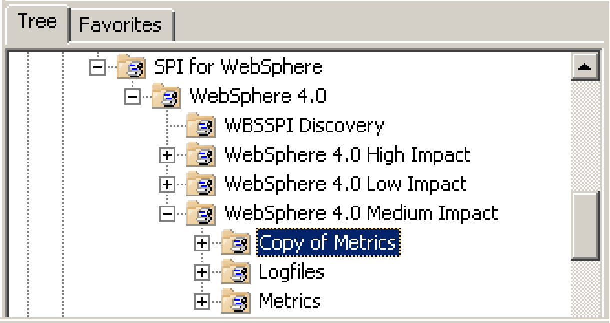
  c Enter a new policy name and select **OK**.

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.



SPI for WebSphere
WebSphere 4.0
WBSSPI Discovery
WebSphere 4.0 High Impact
WebSphere 4.0 Low Impact
WebSphere 4.0 Medium Impact
Copy of Metrics
Logfiles
Metrics

Using the WBS-SPI Collector/Analyzer Command with Parameters

The `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 WebSphere Command Parameters

WBS-SPI data collections are started with the `wasspi_wbs_ca` command, to which you can add other parameters, as identified in the following table.

Parameter	Function	Syntax with Example
`-c`	(**collector**) Specifies collector policy name. (**required**)	`-c` *<collector_policy_name>* **Note:** Must match the collector policy name in which it appears. **Example**: `-c WBSSPI-05min`
`-m`	(**metric**) Specifies the metric numbers or number ranges on which to collect data.	`-m` *<metric_number,metric_number_range>* **Example**: `-m 1,3-5,9-11,15`

Parameter	Function	Syntax with Example

-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).	`wasspi_wbs_ca <prefix>-<collector _policy> -m <metric_number> -t <prefix>-`
		Example:
		`wasspi_wbs_ca -c DEV-WBSSPI-40-Med-1h -m 220-223 -t DEV-`

-i	(**include**) Allows you to list specific servers to monitor. This option may not be used with `-e` option.	`-i <server_name>` **Example:** `-i server1,server3`
-e	(**exclude**) Allows you to exclude specific servers; may not be used with `-i` option.	`-e <server_name>` **Example:** `-e server1,server3`

-x	Allows you to specify a property/value as follows:
	alarm: when `off`, overrides any default alarming defined for the metric.
	print: when `on`, prints the metric name, instance name, and metric value to STDOUT in addition to any configured alarming or logging.
	log: when `off`, prevents graphing or reporting functions.
		`-x <property>=<property_value>`
		`-x alarm=off`
		`-x print=on`
		`-x log=off`

Syntax Examples:

- To specify metrics to collect:

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

```
wasspi_wbs_ca -c <measurement_threshold_policy_name> -m
<metric_number_range>, <metric_number>
```

- To differentiate server instances:

```
wasspi_wbs_ca -c STAGE-WBSSPI-40-Med-05min -m 245,246,260 -i
server_1,server_2 -t STAGE_
```

(Inserting “server_1” and “server_2” in the Program name text box of the collector policy results in collecting data for the specified metrics from these servers only.)

Changing the Collection Interval for Scheduled Metrics

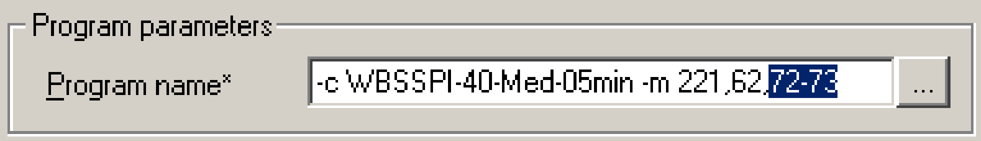
To change the metric collection interval, simply change the Polling Interval in the appropriate collector policy. For example, to change the collection of default metrics from 5 minutes to 10 minutes for the WebSphere 4.0 policy group, follow these steps:

1. From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0** → **WBS-4.0 Medium Impact**.
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.



Program name* -c WBSSPI-40-Med-05min -m 221,62,72-73

1. From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0** → **WBS-4.0 Medium Impact**.
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 WebSphere 4.0 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 WebSphere 4.0 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, and Windows NT/2000. 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 NT or Windows 2000.

- The local/proxy system and remote system must be running the same version of WebSphere Server. For example, if the proxy system is running WebSphere Server version 5, the remote system must also be running WebSphere Server version 5.
- (Optional, for logfile monitoring) The remote system runs on a platform supported by the OVO agent software.

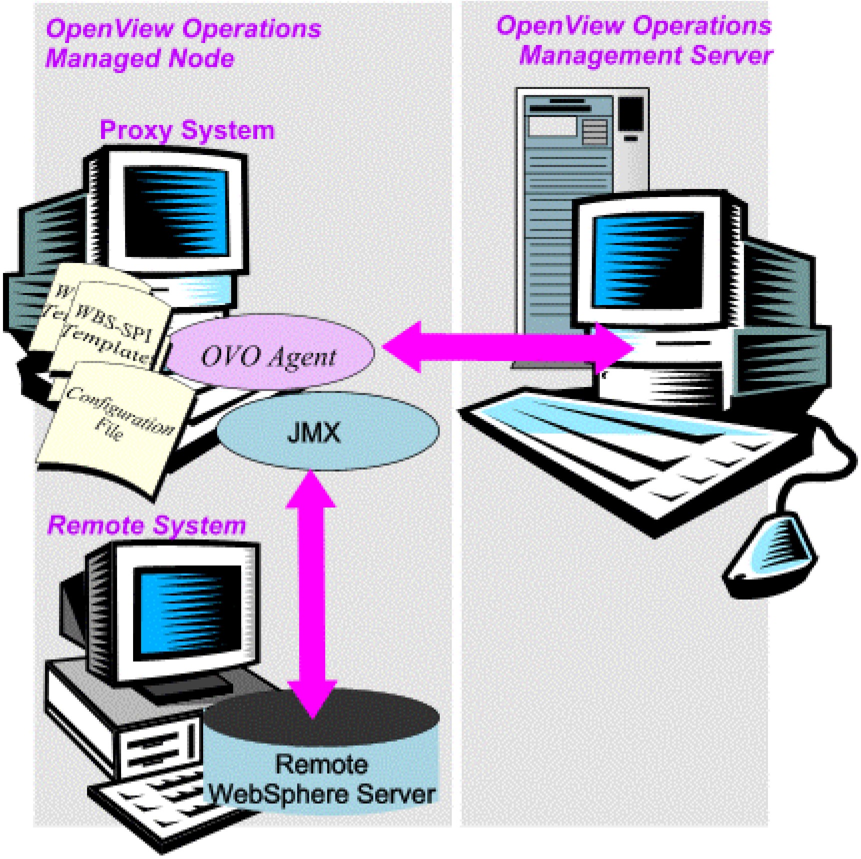
Overview

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 53, 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 4.0 High Impact or 4.0 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 32“ 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, or Windows NT/2000) by completing the following tasks.

Task 1: Configure the Remote WebSphere System

Using the **WBSSPI Configure** tool in the WBSSPI - 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 **WBSSPI Configure** 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 WBS 4.0 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.

4. From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0.**
5. Right-click on a policy group and select **All Tasks** → **Deploy on.**
6. Select the local managed node.
7. Click **OK**.

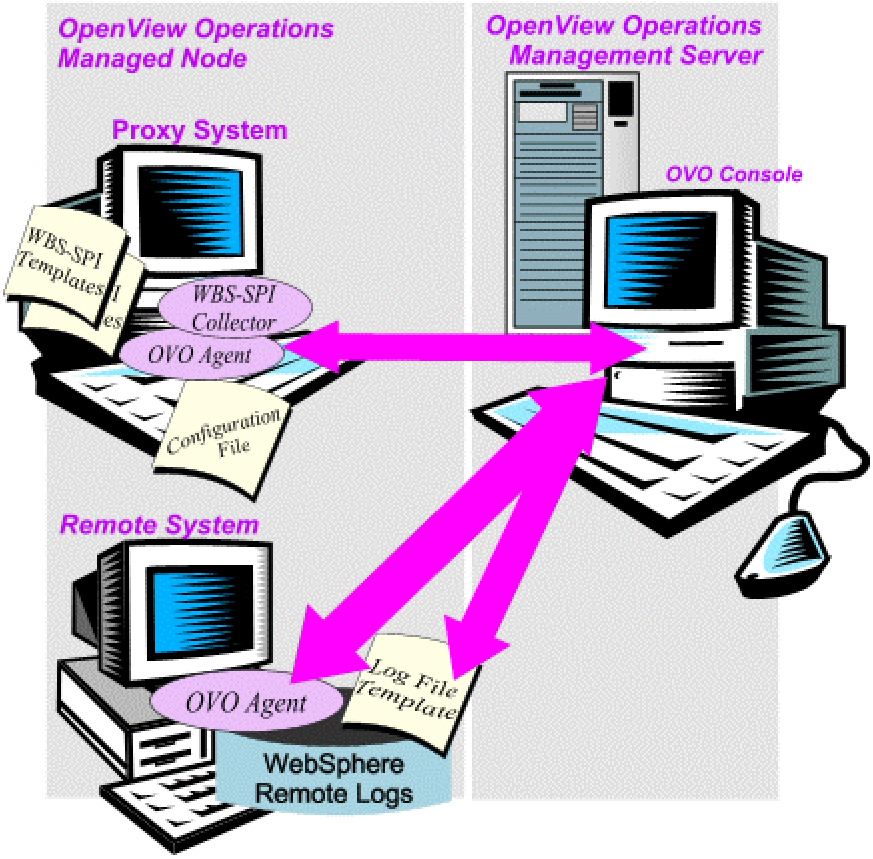
Configuring Remote Logfile Monitoring (Optional)

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.
   1. From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0** → **WebSphere 4.0 High Impact** → **WBSSPI-Logfiles**.
   2. 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 13 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 form the server around the time that the alarm occurred.

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

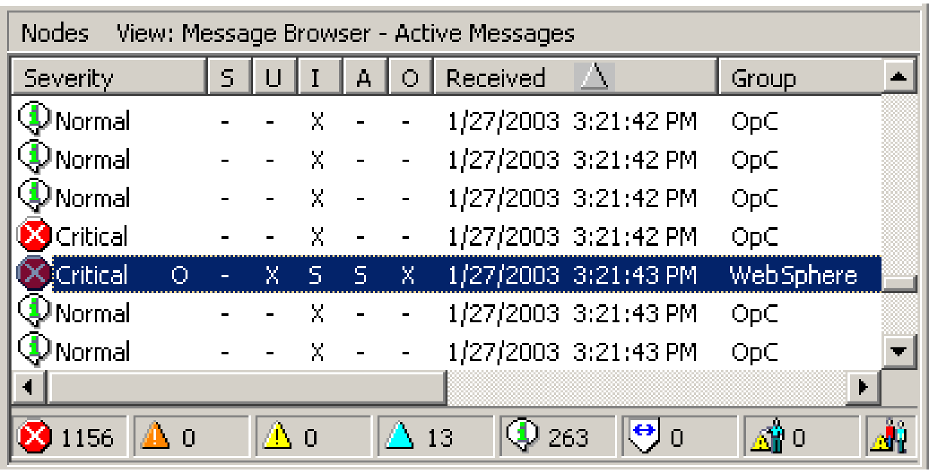
The reports discussed in this section should not be confused with those generated by OpenView Reporter, which show more consolidated, historical data generated as Web pages in management-ready presentation format.

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** → **WBSSPI - 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



Nodes View: Message Browser - Active Messages

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

1156 | 0 | 0 | 13 | 263 | 0 | 0

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

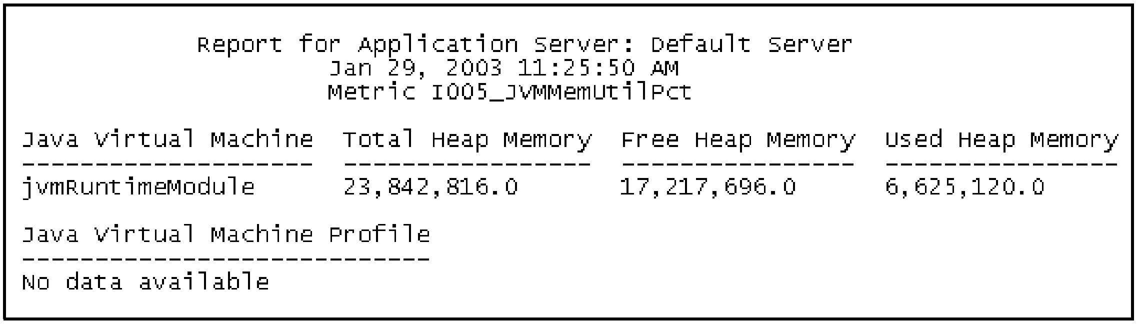
Reports run for all WebSphere instances configured on the managed node. The reports generated reflect the current state of WebSphere on the managed node. To generate a report in OVO, simply navigate down the console tree to the individual SPI for WebSphere reports, double-click on the report, and enter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

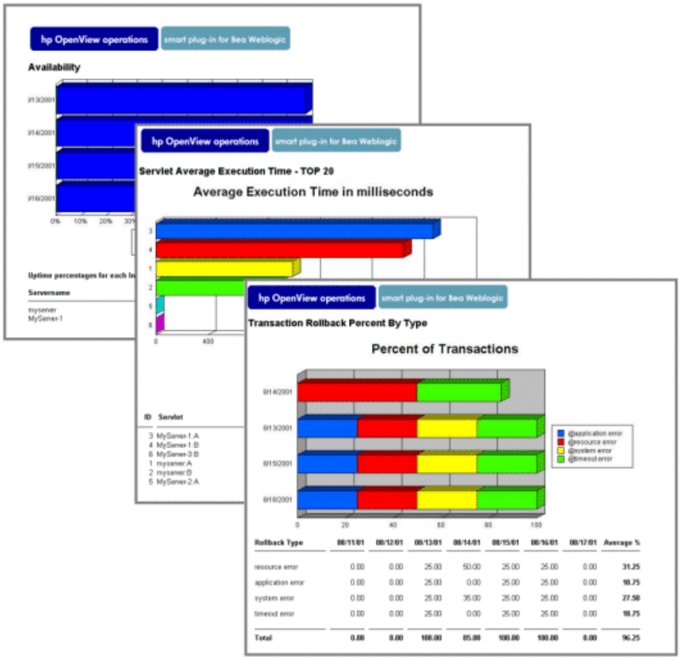
5

Reports and Graphs

Introduction

HP OpenView Reporter, which must be purchased separately (this is *not* the version of Reporter that is included with HP OpenView Operations for Windows), integrates fully with the Smart Plug-in for WebSphere Application Server (WBS-SPI). Reporter produces management-ready, Web page reports, showing historical and trending information.

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



Availability

Uptime percentages for each In

Servername

myserver
MySerrver-1

Servlet Average Execution Time - TOP 20

ID	Servlet
3	MyServer-1:A
4	MyServer-1:B
6	MyServer-3:B
1	myserver:A
2	myserver:B
5	MyServer-2:A

Transaction Rollback Percent By Type

Rollback Type	08/11/01	08/12/01	08/13/01	08/14/01	08/15/01	08/16/01	08/17/01	Average %
resource error	0.00	0.00	25.00	50.00	25.00	25.00	0.00	**31.25**
application error	0.00	0.00	25.00	0.00	25.00	25.00	0.00	**18.75**
system error	0.00	0.00	25.00	35.00	25.00	25.00	0.00	**27.50**
timeout error	0.00	0.00	25.00	0.00	25.00	25.00	0.00	**18.75**
Total	**0.00**	**0.00**	**100.00**	**85.00**	**100.00**	**100.00**	**0.00**	**96.25**

Another OpenView product, Performance Manager, provides graphing capability. Please refer to the Performance Manager documentation to use WBS-SPI with this product.

This chapter shows how to integrate WBS-SPI with HP OpenView Reporter. After you complete the instructions in this chapter, every night, Reporter generates reports that show the performance and availability of a WebSphere Application Server on configured managed nodes. You can also take advantage of the built-in graphing capabilities of the WBS-SPI, coupled with Performance Manager.

Using the OpenView Performance Agent

The OpenView performance subagent (CODA) is automatically deployed on all managed nodes. WBS-SPI relies on this default performance subagent to collect and store performance data used with OVO graphing and reporting. These reporting and graphing features only work with CODA.

However, you may want to use the OpenView Performance Agent (OVPA or MeasureWare Agent) which is supported by HP OpenView Reporter and HP OpenView Performance Manager (these products must be purchased separately).

You can configure the WBS-SPI data collector to use OVPA to collect and store performance data, but you cannot use the graphing and reporting features in OVO with this data.

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 or Solaris	`/var/opt/OV/conf/dsi2ddf/`
AIX	`/var/lpp/OV/conf/dsi2ddf/`
Windows	`\Program Files\HP OpenView\Installed Packages\{790C06B4 ...}\conf\dsi2ddf\`

   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 OpenView Reporter to Generate Reports

Prerequisite: Configuration of 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 *hp OpenView New and Upgraded Smart Plug-ins and Integration Modules for OV operations for Windows 7.10, 7.20, 7.21* 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 61 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/Sores - 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
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

Table 1 All/Group Reports

Report Title	Description	Metric
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.

Integrating WBS-SPI with HP OpenView Performance Manager

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

1. Configure the location of the graphing system within the WBS-SPI configuration. Refer to the online help for more information about setting the `GRAPH_SERVER` property.
2. Install the WBS-SPI graph package on the Windows system running Performance Manager:
   a. Insert the *hp OpenView New and Upgraded Smart Plug-ins and Integration Modules for OV operations for Windows 7.10, 7.20, 7.21* 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.

3 To graph any WebSphere metric, you need 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 also generate any of the available graphs manually by using the WBSSPI - SPI Admin Tool **View Graphs**.

To manually generate a graph:

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.

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

Graph Label	Metric Name	Metric Description
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.

6

User Defined Metrics

Introduction to User Defined Metrics

The Smart Plug-in for WebSphere Application Server (WBS-SPI) can collect data on roughly 50 metrics, but you can expand that number by adding your own. The advantage to defining your own metrics is that you can monitor your own applications. You can customize what you monitor by creating user-defined metrics (UDMs) that instruct the SPI to gather data from PMI counters.

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

You must understand the metric definitions DTD before creating your UDMs. The sections that follow assume you are familiar with XML (extensible markup language) and DTDs (Document Type Definitions).

Metric Definitions DTD

The `MetricDefinitions.dtd` file provides the structure and syntax for the XML file that you create. The WBS-SPI uses the DTD file to parse and validate the XML file you create. The `MetricDefinitions.dtd` file content is described and a sample XML shown in the sections that follow.

On a managed node, the `MetricDefinitions.dtd` file is located in the following directory:

Operating System	**Directory**
AIX	`/var/lpp/OV/wasspi/wbs/conf/`
HP-UX and Solaris	`/var/opt/OV/wasspi/wbs/conf/`
Windows	*`%OvAgentDir%`*`\wasspi\wbs\conf\`

Because the `MetricDefinitions.dtd` file is used at runtime, you should not edit, rename, or move it.

`MetricDefinitions.dtd` consists of the following elements:

- MetricDefinitions
- Metric
- PMICounter
- FromVersion/ToVersion
- Calculation/Formula

The MetricDefinitions Element

The *MetricDefinitions* element is the top-level element within the `MetricDefinitions.dtd` file. It contains one collection of metrics, consisting of one or more metric definitions.

```
<!ELEMENT MetricDefinitions (Metrics)>
<!ELEMENT Metrics (Metric+)>
```

Example

```
<MetricDefinitions>
  <Metrics>
   .
   .
   .
  </Metrics>
</MetricDefinitions>
```

The Metric Element

The *Metric* element represents one metric. Each metric has a unique ID (for example, “WBSSPI_0701”). If a user-defined metric is an alarming, graphing, or reporting metric, the metric ID must be “WBSSPI_XXX” where XXX must be a number from 700 through 799. Otherwise, if the metric is used only within the calculation of another metric, the metric ID must begin with a letter (case-sensitive) and can be followed by any combination of letters, numbers, and underscores (for example, "counter1").

A *Metric* element contains one or more elements that represent the metric data source. Two data sources are supported: PMI counters and calculations. Each metric data source element is scanned for a FromVersion or ToVersion child element to determine which metric data source element to use for the version of the application server being monitored.

```
<!ELEMENT Metric (PMICounter+ | Calculation+)>
<!ATTLIST Metric id           ID         #REQUIRED
                 name         CDATA         ""
                 alarm       (yes | no)    "no"
                 report      (yes | no)    "no"
                 graph       (yes | no)    "no"
                 previous    (yes | no)    "yes"
                 description  CDATA      #IMPLIED >
```

Metric element attributes are described in the following table.

Attribute	Type	Required	Default	Description
id	ID	yes	--	The metric ID.
name	text	no	"no"	The metric name, used for graphing and reporting. The name can be up to 20 characters in length.
alarm	"yes" "no"	no	"no"	If yes, the metric value is sent to the agent via opcmon.
report	"yes" "no"	no	"no"	If yes, the metric value is logged for reporting.
previous	"yes" "no"	no	"yes"	If yes, the metric value is saved in a history file so that deltas can be calculated. If you are not calculating deltas on a metric, set this to "no" for better performance.
graph	"yes" "no"	no	"no"	If yes, the user-defined metric is graphed.
description	text	no	""	A description of the metric.

Example

```
<Metric id="WBSSPI_0705" name="B005_JVMMemUtilPct" alarm="yes" graph="no">
  .
  .
  .
</Metric>
```

The PMI Counter Element

The *PMICounter* element is used when the metric data source is a PMI counter. The PMICounter element contains the following elements:

- **Path** - the location of the counter in the PMI data hierarchy. The content of this element begins with the PMI module name and may contain the wildcard character to specify multiple instances.
- **ID** - the PMI data id to be retrieved from the counter.

- **Load** (optional) - the data to be retrieved is of type load and thus various time-based values are available for retrieval. Use the data attribute to specify which value to retrieve.
- **Stat** (optional) - the data to be retrieved is of type stat and thus various sample-based values are available for retrieval. Use the data attribute to specify which value to retrieve.

```
<!ELEMENT PMICounter (FromVersion?, ToVersion?, Path, ID,
                      (Load | Stat)?)>
<!ATTLIST PMICounter instanceType (single | multi)     "single"
              impact  (low | medium | high) #REQUIRED>
<!ELEMENT Path (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT Load EMPTY>
<!ATTLIST Load data (mean | weight | sum | current) #REQUIRED>
<!ELEMENT Stat EMPTY>

<!ATTLIST Stat data (mean | count | sumOfSquares | variance |
                     standardDeviation | confidence) #REQUIRED>
```

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

PMICounter element attributes are described in the following table.

Attribute	Type	Required	Default	Description
instanceType	"single" "multi"	no	single	Indicates if there are multiple instances of this counter.
impact	"low" "medium" "high"	yes	no default	How the metric affects performance.

Load element attributes are described in the following table.

Attribute	Type	Required	Default	Description
data	"mean" "sum" "weight" "current"	yes	none	Specifies which time-based data to retrieve.

Stat element attributes are described in the following table.

Attribute	Type	Required	Default	Description
data	"mean" "count" "sumOfSquares" "variance" "standardDeviation" "confidence"	yes	no default	Specifies which sample-based data to retrieve.

Example

```
<PMICounter instanceType="multi" impact="high">
  <Path>threadPoolModule/*</Path>
  <ID>3</ID>
  <Load data="weight"/>
</PMICounter>
```

FromVersion and ToVersion Elements

The *FromVersion*/*ToVersion* elements are used to determine the version of the application server being monitored.

The following algorithm is used for determining what application server version is supported by each metric source element within the Metric element.

1. If a *FromVersion* element is not present, no lower limit exists to the server versions supported by this metric.
2. If a *FromVersion* element is present, the *server* attribute indicates the lowest server version supported by this metric. If an *update* attribute exists, it qualifies the lowest server version supported by specifying the lowest Fix Pack or patch supported for that version.
3. If a *ToVersion* element is not present, no upper limit exists to the *server* versions supported by this metric.
4. If a *ToVersion* element is present, the *server* attribute indicates the highest server version supported by this metric. If an *update* attribute exists, it qualifies the server version supported by specifying the highest Fix Pack or patch supported for that version.

```
<!ELEMENT FromVersion (EMPTY)>
<!ELEMENT ToVersion (EMPTY)>
```

```
<!ATTLIST FromVersion   server CDATA #REQUIRED
                        update CDATA     "*">
<!ATTLIST ToVersion     server CDATA #REQUIRED
                        update CDATA     "*">
```

FromVersion and *ToVersion* element attributes are described in the following table.

Attribute	Type	Required	Default	Description
server	string specifying version number	yes	none	Specifies a primary server version; for example, `<FromVersion server="6.0"/>`
update	string specifying version number	no	"*"	Specifies a secondary server version, such as "1" for service pack 1. A "*" indicates that a metric is valid for all secondary server versions.

Example

```
<FromVersion server="4.0" update="1"/>
<ToVersion server="4.0999"/>
```

Calculation and Formula Elements

The *Calculation* element is used when the data source of the metric is a calculation using other defined metrics. The Calculation element contains a *Formula* element whose content is a string that specifies the mathematical manipulation of other metric values to obtain the final metric value. The metrics are referred to in the calculation expression by their metric ID. The result of the calculation is the metric value.

```
<!ELEMENT Calculation (FromVersion?, ToVersion?,Formula)>
<!ELEMENT Formula (#PCDATA)>
```

Syntax

Calculations must use syntax as follows.

- Operators supported are +, -, /, *, and unary minus.
- Operator precedence and associativity follows the Java model.

- Parentheses can be used to override the default operator precedence.
- Allowable operands are metric IDs and literal doubles.

A metric ID can refer to either a PMICounter metric or another calculated metric. Literal doubles can be specified with or without the decimal notation. The metric ID refers to the `id` attribute of the Metric element in the metric definitions document.

Functions

The calculation parser also supports the following functions. All function names are lowercase and take a single parameter which must be a metric ID.

- `delta` returns the result of subtracting the previous value of the metric from the current value.
- `interval` returns the time in milliseconds that has elapsed since the last time the metric was collected.
- `sum` returns the summation of the values of all the instances of a multi-instance metric.
- `count` returns the number of instances of a multi-instance metric.

Examples

The following example defines a metric whose value is the ratio (expressed as a percent) of `Metric_1` to `Metric_3`.

```
<Formula>(Metric_1 / Metric_3) *100</Formula>
```

The following example could be used to define a metric that is a rate (number of times per second) for `Metric_1`.

```
<Formula>(delta(Metric_1)/interval(Metric_1))*1000</Formula>
```

Sample 1

Metric 710 uses metric "counter1" in its calculation. This calculated metric applies to all WebSphere versions. However, the PMICounter metric on which it is based has changed. Originally the PMICounter for metric 710 was introduced on server version 4.0, update 1. However in version 4.1, the id changed, and this change remains the same up to the most current server version.

```
<Metric id="counter1" alarm="no">
  <PMICounter instanceType="multi" impact="high">
```

```
    <FromVersion server="4.0" update="1"/>
    <ToVersion server="4.099"/>
    <Path>threadPoolModule/*</Path>
    <ID>3</ID>
  </PMICounter>
  <PMICounter instanceType="multi" impact="high">
    <FromVersion server="4.1"/>
    <Path>threadPoolModule/*</Path>
    <ID>30</ID>
  </PMICounter>
</Metric>
<Metric id="WBSSPI_0710" alarm="yes">
  <Calculation>
   <Formula>delta(counter1)/interval(counter1)*1000*60</Formula>
  </Calculation>
</Metric>
```

Sample 2

Using the example above, a decision was made to make metric 710 a per-minute rate instead of a per-second rate as of server version 5.0. The changes that had to be made to the metric definitions are in bold type.

```
<Metric id="counter1" alarm="no">
  <PMICounter instanceType="multi" impact="high">
    <FromVersion server="4.0" update="1"/>
    <ToVersion server="4.099"/>
    <Path>threadPoolModule/*</Path>
    <ID>3</ID>
  </PMICounter>
  <PMICounter instanceType="multi" impact="high">
    <FromVersion server="4.1"/>
    <Path>threadPoolModule/*</Path>
    <ID>30</ID>
  </PMICounter>
</Metric>
<Metric id="WBSSPI_0710" alarm="yes">
  <Calculation>
   <FromVersion server="4.0"/>
   <ToVersion server="4.999"/>
   <Formula>delta(counter1)/interval(counter1)*1000*60</Formula>
  </Calculation>
  <Calculation>
   <FromVersion server="5.0"/>
   <Formula>delta(counter1)/interval(counter1)*1000</Formula>
  </Calculation>
</Metric>
```

Sample 3: Metric Definitions File

The following is a sample metric definitions file to illustrate how you might create your own user-defined metrics. This sample file also contains examples of calculated metrics.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE MetricDefinitions SYSTEM "MetricDefinitions.dtd">
<!-- sample UDM metrics configuration File -->

<MetricDefinitions>
  <Metrics>

<!-- The following metrics illustrate some of the options
     available when creating user-defined metrics.
-->

  <!-- The following metric uses a PMICounter that can
       have multiple instances. Note the wildcard (*)
       character is used to specify multiple instances.
       The path element uses the standard PMI path syntax
       with the exception that it must start at the module
       level and can include the wildcard character at any
       point in the path.
  -->

  <Metric id="WBSSPI_0700" name="UDM_700" alarm="yes">
    <PMICounter instanceType="multi" impact="high">
      <FromVersion server="4.0"/>
      <Path>threadPoolModule/*</Path>
      <ID>3</ID>
      <Load data="weight"/>
    </PMICounter>
  </Metric>

  <!-- The following 2 metrics are "base" metrics. They
       are used in the calculation of a "final" metric but
       are not alarmed, reported, or graphed themselves.
       Base metrics may have an 'id' that begins with a letter
       (case-sensitive) followed by any combination of letters,
       numbers, and underscore. Base metrics normally have
       alarm="no".
  -->

  <Metric id="JVMRuntime_HeapSize" alarm="no" >
    <PMICounter instanceType="single" impact="low">
      <FromVersion server="4.0"/>
      <Path>jvmRuntimeModule</Path>
      <ID>1</ID>
    </PMICounter>
  </Metric>
  <Metric id="JVMRuntime_UsedSpace" alarm="no">
    <PMICounter instanceType="single" impact="low">
      <FromVersion server="4.0"/>
      <Path>jvmRuntimeModule</Path>
      <ID>3</ID>
    </PMICounter>
  </Metric>

  <!-- The following metric illustrates a calculated metric. The
       calculation is based on the previous 2 "base" metrics.
  -->

  <Metric id="WBSSPI_0705" name="B005_JVMMemUtilPct" alarm="yes"
graph="no">
    <Calculation>
      <FromVersion server="4.0"/>
      <Formula>((JVMRuntime_UsedSpace)/JVMRuntime_HeapSize)*100
      </Formula>
    </Calculation>
  </Metric>

  <!-- Metric IDs that are referenced from the collector
       command line must have a namespace prefix followed by
       4 digits. The default namespace prefix is 'WBSSPI_'.
       The 'namespace' option must be used on the command
       line for the following metric since this metric has a
       different prefix other than 'WBSSPI_'.
       Example:
       wasspi_wbs_ca -x namespace=Testing_ -m 992 ...
  -->

  <Metric id="Testing_0992" name="Testing_Metric">
    <PMICounter instanceType="single" impact="high">
      <FromVersion server="4.0"/>
      <Path>beanModule</Path>
      <ID>9</ID>
      <Load data="sum"/>
    </PMICounter>
  </Metric>

  </Metrics>
</MetricDefinitions>
```

Create User-Defined Metrics

Now that you have reviewed the structure for creating UDMs, do the following:

- Task 1: Disable graphing (if enabled)
- Task 2: Create a metric definitions file
- Task 3: Configure the metric definitions file name and location
- Task 4: Create a UDM policy group and policies
- Task 5: Deploy the policy group
- Task 6: Enable graphing

Task 1: Disable graphing (if enabled)

If graphing has been enabled, disable it:

1. From the OVO console, select **Operations Manager** → **Nodes**.
2. Right-click on the node on which you want to disable UDM graphing and select **All Tasks** → **Launch Tool** → **UDM Graph Disable**.

Task 2: Create a metric definitions file

The metrics definition file you create must be an XML file that follows the format defined by the metric definitions DTD file described in "Metric Definitions DTD" on page 71.

➤ Do not edit, rename, or move the `MetricDefinitions.dtd` file installed with the WBS-SPI.

The following sample WBS-SPI metric definitions file is installed on the managed node:

`/var/lpp/OV/wasspi/wbs/conf/UDMMetrics-sample.xml` (AIX),

`/var/opt/OV/wasspi/wbs/conf/UDMMetrics-sample.xml` (HP-UX and Solaris), or

`<`*`%OvAgentDir%`*`>\wasspi\wbs\conf\UDMMetrics-sample.xml` (Windows).

Task 3: Configure the metric definitions file name and location

In order for the UDM data collection to occur, the WBS-SPI configuration must include the name and location of the metric definitions file, preceded by the property name as shown below:

```
UDM_DEFINITIONS_FILE = <full path of metric definitions file>
```

where the path name should use only forward slashes ("/").

To add the UDM file name and its location to the WBS-SPI configuration:

1. From the OVO console, select **Operations Manager** → **Tools** → **SPI for WebSphere** → **WBSSPI - SPI Admin**.
2. Double-click on the **WBSSPI Configure** tool.
3. Select the managed node(s) on which the metrics definition file exists and select **Launch**.
4. A Console Status window appears.
5. The WBSSPI Configure Tool Introduction window appears. Read the information and select **Next**.
6. The WBSSPI Configure Tool window appears. If the metrics definition file uses the same name and location on all managed nodes, configure the UDM_DEFINITIONS_FILE property at the Defaults (global properties) level. Otherwise, set the property for each managed node selected in step 3:
   a. Single-click on **Default Properties** at the Defaults level or for a node.
   b. Select the **Set Configuration Properties** tab.
   c. From the **Select a Property to add** pulldown menu, select **UDM_DEFINITONS_FILE**.
   d. Select **Add Property.**
   e. Enter the value (metric definitions file name and its fully-qualified path name, using forward slashes in the path name only).
   f. Select **Save**.
   g. Select **Next**.
7. The WBSSPI Configure Tool: Confirm Operation window displays. Select **OK** to configure the selected managed nodes.

Any changes you made to managed nodes that were not selected are saved to the configuration on the management server. However, to configure those managed nodes, you must deploy the WBSSPI Service Discovery policy to these nodes.

Task 4: Create a UDM policy group and policies

To run the UDM data collection and establish thresholds for alarming, create a UDM policy group and policies:

1. Copy an existing WBS-SPI policy group:
   a. From the OVO console, select **Operations Manager** → **Policy management** → **Policy groups** → **SPI for WebSphere** → **WebSphere 4.0** → **WebSphere 4.0 *<impact>* Impact**.
   b. Right-click on the WBS-SPI group you want to use as a starting point, and select **Copy**.
   c. Right-click on **WebSphere 4.0 *<impact>* Impact** and select **Paste**.
2. Rename the policy group:

   Rename the new policy group according to how you plan to identify the new metric and collector policies. For example, you might include UDM in the name to clearly indicate that the group is made up of custom metric monitors.

   a. Right-click on the policy group and select **Rename**.
   b. Type in the new name.
3. Edit and rename each policy:
   a. Double-click on the policy you plan to use.
   b. Configure the collector policy command line (in the Program text box) to include the policy name and UDM metric number. Refer to"Advanced Policy Customizations" on page 42 for more information.
   c. Configure thresholds in the policy, as appropriate. Refer to"Advanced Policy Customizations" on page 42 for more information.
   d. Select **File** → **Save As**, and rename the policy according to your naming scheme.

The name you give the new *metric policy* in the group would contain each new UDM number. For example, a copy of `WBSSPI_0001` could be called `WBSSPI_0701.`

The name you give the new *collector policy* would also contain the identifying name. You also include the policy name after the `-c` parameter on the command line as in the example:

```
wasspi_wbs_ca -c UDM-40-15m -m 701
```

In this case, the copied collector policy has been renamed: `UDM-40-15min`

4. Delete all original policies from the new group:
   a. Right-click on the policy and select **Delete**.

Task 5: Deploy the policy group

1. Right-click on the policy group and select **All Tasks → Deploy on**.
2. Select the node(s) on which to deploy the policy group.
3. Click **OK**.

Task 6: Enable graphing

If you are using graphing (HP OpenView Performance Manager, also known as HP PerfView or MeasureWare, must be purchased and installed), enable data collecting for UDM graphing:

1. From the OVO console, select **Operations Manager → Nodes**.
2. Right-click on the node on which you want to enable UDM graphing and select **All Tasks → Launch Tool → UDM Graph Enable**.

Allow sufficient collection intervals to occur before attempting to view graphs.

7

Troubleshooting WBS-SPI

Introduction

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.

Log and Trace Files

Management Server

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

File Type Log

Filename `\<%OvInstallDir%>\install\WASSPI\WBSSPI\English\Discovery\log\<managed_node>_disc_server.log`

Description Records the updates done by the WBSSPI Discovery policy to the management server's configuration for each managed node. Log files are overwritten each time the discovery policy is run on the managed node. Logging to this file is always enabled.

UNIX Managed Nodes

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

File Type Log

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

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

File Type Log

Directory /*<OvAgentDir>*`/wasspi/wbs/log/config.log`

Description Records output from configuration scripts.

File Type Log

Directory /*<OvAgentDir>*`/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 *`<OvAgentDir>`*`/bin/instrumentation/wasspi_wls_discoveryUnix.pl`, set the `$trace_on` variable to 0. To disable this trace, set the $trace_on to 1. When instrumentation is deployed, the `wasspi_wls_discoveryUnix.pl` file is overwritten (therefore, if you disable tracing, it becomes enabled when instrumentation is deployed). Five archived versions are kept. A new trace file is created when the discovery policy is run.

File Type Trace

Directory /*<OvAgentDir>*`/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 `WLSSPI 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 \*<%OvAgentDir%>*`\log\javaagent.log`

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

File Type Log

Directory \*`<%OvAgentDir%>`* `\wasspi\wbs\log\config.log`

Description Records output from configuration scripts.

File Type Log

Directory \*<%OvAgentDir%>*\wasspi\wbs\log\errorlog

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 \*<%OvInstallDir%>*\bin\instrumentation\wasspi_wbs_discoveryWin.pl, set the $trace_on variable to 0. To disable this trace, set the $trace_on to 1. When instrumentation is deployed, the wasspi_wls_discoveryWin.pl file is overwritten (therefore, if you disable tracing, it becomes enabled when instrumentation is deployed). Five archived versions are kept. A new trace file is created when the discovery policy is run.

File Type Trace

Directory \*<%OvAgentDir%>*\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 WLSSPI Trace - Start 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 21 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/deinstl/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	/opt/WebSphere/AppServer
Solaris	/opt/WebSphere/AppServer
Windows	\WebSphere\AppServer

- Verify that the WBSSPI Configure 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 WebSphere 4.0 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 21 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 WBSSPI Discover 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 WBSSPI Start WebSphere tool, you must set the `START_CMD` and `USER` properties. Set these properties using the WBSSPI Configure 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 WBSSPI Stop WebSphere tool, you must set the `STOP_CMD` and `USER` properties. Set these properties using the WBSSPI Configure tool. Refer to the online help for more information about this tool.

index