

HP OpenView Operations Smart Plug-in for Microsoft Windows Operating System

Administrator's Reference Guide

Version A.08.80



**Manufacturing Part Number: None
December 2005**

© Copyright 2005 Hewlett-Packard Development Company, L.P.

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.

©Copyright 1999-2005 Hewlett-Packard Development Company, L.P., all rights reserved.

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

Trademark Notices

UNIX® is a registered trademark of The Open Group.

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

Motif® is a registered trademark of the Open Software Foundation in the U.S. and other countries.

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

Chapter 1	Introduction	9
	Introducing the WinOS SPI	10
	Features and Functionality	11
	WinOS SPI Policies and Applications	11
	Applications Supported by WinOS SPI	13
Chapter 2	Installation and Configuration	15
	Upgrading the WinOS SPI	16
	Managing Customized Components	16
	Installing the WinOS SPI	17
	Prerequisite for HP SIM Monitoring	17
	To Install the Software	17
	Configuring the WinOS SPI	19
	Assigning WinOS SPI Responsibilities	19
	Assigning Policies to the Management Server	21
	Assigning Policies to Windows Nodes	21
	Distributing Components to the Windows Nodes	24
	Uninstalling the WinOS SPI	26
	To Remove WinOS SPI Components from the Managed Nodes	26
	To Remove WinOS SPI Components from the Management Server	27
	Installed File Locations	31
Chapter 3	Using the WinOS SPI	35
	Message Groups	37
	Message Group Bank Window	37
	Application Groups	41
	Prerequisites to Run Windows OS SPI Applications	42
	Application Group: HP Systems Insight Manager	43
	Application Group: Metaframe Tools	46
	Application Group: Insight Manager	47
	Application Group: Microsoft Windows Core	49
	Application Group: MS BackOffice Application	55

Contents

Application Group: Web Servers	59
Application Group: WinOSSPI Discovery	65
Application Group: WinOSSPI Utils	65
Application Group: Microsoft Windows Cluster	66
Chapter 4 Policies and Policy Groups	69
Policies	70
WMI Policies Support	70
Prerequisites	70
Prerequisites for ADS Policies	71
Using Policies	72
Policy Groups	73
Anti Virus Applications	75
McAfee VirusScan → Diagnostic	75
Norton Anti-Virus → Diagnostic	75
Backup and Storage Applications	77
VERITAS Backup Exec → Diagnostic	77
Citrix Metaframe Applications	78
Citrix Metaframe → Diagnostic	78
Dell OpenManage	79
Dell OpenManage → Diagnostic	79
Discovery	80
Insight Manager	81
Insight Manager → Diagnostic → Foundation Agents	81
Insight Manager → Diagnostic → Hardware Traps	81
Insight Manager → Diagnostic → Storage Agents	85
Insight Manager → Diagnostic → Remote Insite Lights Out	85
Insight Manager → Diagnostic → NIC Agents	86
Insight Manager → Diagnostic → Server Agents	86
Insight Manager → Diagnostic → Version Control Agents	86
HP Systems Insight Manager	87
HP Systems Insight Manager → HPSIM Diagnostic	87
Microsoft BackOffice Applications	88

MS Certificate Server	88
MS Certificate Server → Diagnostic	88
MS Index Server	88
Index Server Win 2K,XP & 2K3 → Index Server Diagnostic	88
Index Server Windows NT 4.0 → Index Server WinNT Diagnostic	89
MS Message Queue Server	90
MS Message Queue Server → Diagnostic	90
MS Proxy Server 2.0	90
MS Proxy Server 2.0 → Diagnostic	90
MS SNA Server 4.0	92
MS SNA Server 4.0 → Diagnostic	92
MS Systems Management Server 2.0	92
MS Systems Management Server 2.0 → Diagnostic	92
MS Systems Management Server 2003	93
MS Systems Management Server 2003 → Diagnostic	93
MS Transaction Server 2.0	94
Microsoft Cluster Server	96
Cluster Server Diagnostic	96
Microsoft Windows Core	99
MS Active Directory Server	99
MS Terminal Server	115
Network Infrastructure	117
Operating System	119
Web Servers	130
MS IIS 4.0 → Diagnostic	131
MS IIS 5.0 → Additional	148
MS IIS 5.0 → Diagnostic	149
MS IIS 6.0 → Diagnostic	165
MS Site Server 3.0 → Diagnostic	167
Chapter 5 Service Discovery	171
Prerequisite for Service Discovery	172
WinOS SPI Discovery	173

Contents

Mechanism for Gathering Service Information	173
The Discovery Modules	173
Discovering Services	175
Assigning Nodes to the WinOS SPI Node Group	175
Distributing Policies and Commands to the Node Group	176
Discovering Windows Services on Managed Nodes	177
Service Discovery File Locations	179
The OVO Management Server	179
The OVO Managed Nodes for DCE Agents	180
The OVO Managed Nodes for HTTPS Agents	180
Chapter 6 Self-Healing Services	181
Starting SHS on a Management Server	182
Starting SHS on a Managed Node	183

Support

Please visit the HP OpenView support web site at:

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

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

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

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

<http://www.managementsoftware.hp.com/passport-registration.html>

1

Introduction

This chapter provides an overview of the main features and functionality that are provided with the Smart Plug-in for Microsoft Windows Operating System (WinOS SPI).

Introducing the WinOS SPI

The WinOS SPI is a software product which, by means of a full integration with OVO—formerly VPO/OpC, a market-leading management solution for networks, systems, databases, and applications in heterogeneous IT environments—extends OVO’s management scope to include distributed environments of Windows systems. Installed in an environment consisting of one or more OVO servers and one or more OVO managed nodes, the WinOS SPI can be used to monitor and manage the functionality and the availability of hardware and software of Windows 2003 Server, Windows XP, Windows 2000 and Windows NT 4.0 operating systems.

NOTE

SMART Plug-In for Microsoft Windows OS is also referred to as WinOS SPI or Windows OS SPI in this document.

Features and Functionality

The WinOS SPI enables you to:

- Deploy preconfigured policies that immediately start to monitor the operation and performance of the Windows nodes in your network.
- Discover system infrastructure and applications that are available on Windows nodes.
- Use applications to view information from remote Windows nodes, and to remotely start commands.

WinOS SPI Policies and Applications

The WinOS SPI provides preconfigured policies and applications that can manage the operations and performance of your Windows nodes. The policies and applications let you do the following:

- Assign WinOS SPI responsibilities

With HP OpenView Operations, you can assign operator responsibilities by means of user profiles. The WinOS SPI automatically creates an operator profile, which may be used as a policy for creating your own WinOS SPI operators. For details, see “Assigning WinOS SPI Responsibilities” on page 19.

- Assign policies to management server

WinOS SPI provides a discovery policy (`WINOSSPI-Discovery`) to discover Microsoft Windows services and applications. You can customize this policy to suit your requirements. Refer to “Discovery” on page 80 for more details about the discovery policy.

- Assign policies to Windows nodes

The WinOS SPI provides standard message-source policies for a wide variety of Windows applications. You can customize the preconfigured policies to match the specific requirements of your organization. For details, see “The WinOS SPI discovery policy (`WINOSSPI-Discovery`) is present in the `Discovery` policy group. Perform

steps 2 through 9 on page 23 to run the WinOS SPI discovery process on all the nodes in the Win OS SPI node group.” on page 21.

- Distribute components to Windows nodes

You can distribute WinOS SPI components to some or all Windows nodes from a central OpenView Operations console. For details, see “Distributing Components to the Windows Nodes” on page 24.

- Deploy WinOS SPI policies

The WinOS SPI provides policies that you can manually deploy according to your own requirements. Also, you can create custom policies by modifying the preconfigured policies to address specific needs For more information, refer to “Using Policies” on page 72.

NOTE

The terms template and policy are used interchangeably in WinOS SPI, and both terms refer to the same WinOS SPI component.

Applications Supported by WinOS SPI

The applications supported by WinOS SPI are:

- McAfee VirusScan
- Norton Anti-Virus
- Veritas Backup Exec
- Citrix Metaframe 1.8
- Dell OpenManage
- Insight Manager 7
- HP Systems Insight Manager 4.0, 4.1, and 4.2
- HP OpenView Self-healing services
- MS Certificate Server 1.0
- MS Cluster Server
- MS Index Server 2.0
- MS Message Queue Server 1.0
- MS Proxy Server 2.0
- MS SNA Server 4.0
- MS Systems Management Server 2.0 and 2003
- MS Transaction Server 2.0
- MS Active Directory Services
- MS Terminal Server
- MS IIS 4.0
- MS IIS 5.0
- MS IIS 6.0
- MS Site Server 3.0

2

Installation and Configuration

This chapter describes how to upgrade, install, configure, and uninstall the WinOS SPI software bundle on the HP OpenView Operations Management Server.

Upgrading the WinOS SPI

In earlier versions, component names had WIN_SPI or win_spi as prefix or did not have any prefix at all.

If you upgraded WinOS SPI from a version earlier than A.08.00, all the component names would be prefixed with one of the following strings:

- WINOSSPI
- WinOSSPI
- winosspi

The policies and applications are also grouped under new policy groups and application groups respectively. It is recommended that you back up customized Applications, Message Groups, Node Group, User Profile, Policy Groups and Policies before upgrading.

The SPI for Microsoft Windows policy group is renamed to MICROSOFT WINDOWS and appears under the group, Operating System SPIs.

Managing Customized Components

To manage your customized components, do as follows:

1. Make a copy with a unique name (for example, add "-" at the end for each name)
2. Uninstall the previous version of the SPI.
3. Install the new version of WinOS SPI.
4. You can repeat the customizations on the new components installed with the new version of the SPI.

Back up the components by copying and downloading the configuration. Refer to the HP OpenView Operations Administrator's Reference Volume I for more information on copying and downloading configuration. Once you install the new version of the SPI, you can upload the downloaded data (with changed names) and refer to them while customizing the new policies.

Installing the WinOS SPI

This section explains how to install the WinOS SPI software bundle from the installation compact disk (CD) to the HP OpenView Operations Management Server. Before you install WinOS SPI, read the Release Notes for specific patch installation information for your management server platform.

Prerequisite for HP SIM Monitoring

Make sure that JRE version 1.4.2 is installed on your system. You need to install JRE 1.4.2 to enable the monitoring of HP Systems Insight Manager (HP SIM) installed on the managed nodes. Run the application `Set JRE Path` from the HP Systems Insight Manager application group in the OVO Application Bank to set the Java path on the OVO management server.

To Install the Software

If you are installing WinOS SPI on an OVO 8.x management server, you can either choose to install WinOS SPI while installing the OVO management server or you can install it later. During OVO installation, you will be prompted to mount the HP OpenView Smart Plug-in CD-ROM. Mount the CD and follow the instructions given.

To separately install the WinOS SPI on an OVO 8.x management server or on an OVO 7.x management server, follow the steps given below.

1. Log on to the OVO management server as root user.
2. Mount the HP OpenView Smart Plug-in CD-ROM. Use the CD that contains the management server installation packages (HP OpenView Smart Plug-ins for OVO/UNIX). Refer to the *HP OpenView Smart Plug-ins for OVO/UNIX Release Notes* for more information.
3. Set the environment variable `OSSPI_INSTALLER_HOME` to the `installables` directory, `/<mount_point>/OV_DEPOT`
4. Type the following command to install the WinOS SPI filesets:

```
/<mount_point>/OV_DEPOT/WINOSSPI/winosspi_setup
```

NOTE You can also install WinOS SPI on a clustered OVO management server.

Refer to the *HP OpenView Smart Plug-ins for OVO/UNIX Release Notes* for more information about product locations and valid platform names.

The SPI-WIN-OVO product contains the file sets described in Table 1.

Table 1 File Sets and Descriptions

File Set	Description
SPI-WIN-OVO.WINOSSPI-CONF	Configuration files
SPI-WIN-OVO.WINOSSPI-DOC	Documentation and release notes
SPI-WIN-OVO.WINOSSPI-WIN	Package for Windows managed nodes
SPI-WIN-OVO.WINOSSPI-SRV	Package for OVO Unix Management Server

NOTE The HP Systems Insight Manager (HP SIM) applications and policies will not be installed on a Solaris management server, as HP SIM is not supported on Solaris management servers.

Configuring the WinOS SPI

This section explains how to use the HP OpenView Operations administrator graphical user interface (GUI) to integrate the WinOS SPI with OpenView Operations and bring all Windows application servers under OpenView Operations management.

You need to:

- Assign WinOS SPI responsibilities
- Assign policies to Windows nodes
- Assign policies to the management server
- Distribute components to the Windows nodes

Assigning WinOS SPI Responsibilities

With HP OpenView Operations, operator responsibilities can be assigned by means of user profiles. The WinOS SPI automatically creates an operator profile that can be used as a policy for creating your own WinOS SPI operators. The WinOS SPI specific user profile, Windows Operator, appears in the User Profile Bank window.

To work with the WinOS SPI, you must either create a new user, or assign the Windows Operator profile to an existing user. This profile enables the user to see WinOS SPI messages and to execute WinOS SPI applications.

TIP

The easiest way to add a new OpenView user is to copy an existing user, change the new user's name, and modify the responsibilities of the new user appropriately.

To Add a New OpenView User

1. In the `User Bank` window, select and right-click an existing user (for example, `opc_op`), then select the `Copy . . .` Menu item.

The `Copy User` window appears.

2. Change both the `Name` field and the `Label` field to the following:

`WIN_op`

3. Assign default responsibilities to the new user by clicking [Responsibilities...].

The `Responsibilities` window opens.

4. From the message groups provided with WinOS SPI, select the message groups in which you are interested, and then select `Close`.

For a complete list of message groups delivered with Windows OS SPI, see “Message Group Bank Window” on page 37.

5. Assign default applications to the new user by clicking [Applications...].

The `Applications` window opens.

6. Open the `Application Bank` window and drag the Windows OS SPI application group to the `Applications of <UserName>` window.

7. Close both windows.

8. Return to the `Copy User` window and click [OK].

The user `WIN_op` appears in the `User Bank` window with the combined (default) responsibilities of the Windows Operator user profile and the `opc_op` operator you used as a policy.

NOTE

The responsibilities assigned in a user profile are global and, therefore, not immediately visible in the responsibilities matrix of the individual user you create. Similarly, the responsibilities of the user you create are local and only visible in the user’s own responsibilities matrix. However, if you assign the Windows Operator user profile to the `WIN_op` user, all the message and node groups assigned to the Windows Operator user profile are assigned to the `WIN_op` user, even if it does not initially appear so.

To Change an Operator's Profile

1. In the `OVO User Bank` window, select and right-click an existing user (for example, `WIN-op`), and then select the `Modify...` Menu item.

The `Modify User` window appears.

2. Click the `Profiles` button and drag the profile `Windows Operator` from the `OVO User Profile Bank` to the `Profiles` window of the user to be modified.
3. Modify the policy as needed.
4. Save the changes by returning to the `Modify User` window and clicking `OK`.

To Assign Nodes to the Node Group WinOSSPI

1. Open the `OVO Node Group` window and double-click the node group `WinOSSPI`.
2. Open the `OVO Node Bank` window.
3. Drag the `Windows` nodes from the `OVO Node Bank` window to the node group `WinOSSPI`.

Assigning Policies to the Management Server

The `WinOS SPI discovery` policy (`WINOSSPI-Discovery`) is present in the `Discovery` policy group. Perform steps 2 through 9 on page 23 to run the `WinOS SPI discovery` process on all the nodes in the `Win OS SPI` node group.

Assigning Policies to Windows Nodes

Message-source policies for the `WinOS SPI` are organized into the following default groups:

- Anti-Virus Applications
- Backup & Storage Applications
- Citrix Metaframe 1.8
- Dell OpenManage

- Discovery
- Insight Manager
- HP Systems Insight Manager
- MS BackOffice Applications
- MS Cluster Server
- Microsoft Windows Core
- Web Servers

All the groups, except HP Systems Insight Manager, are part of the policy group MICROSOFT WINDOWS.

To Create your Own Policy Group

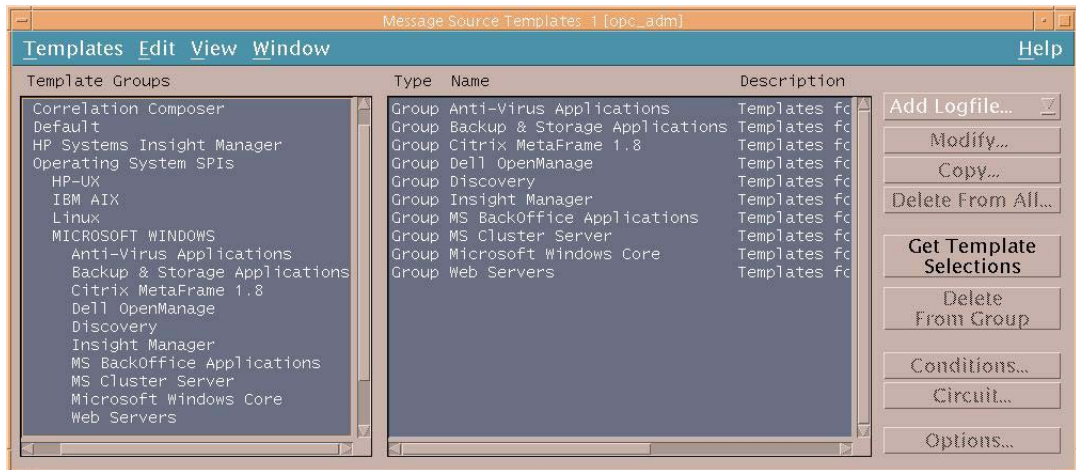
When creating your own policy group, copy the existing policy group, then modify the contents of the new group.

1. Make your own policy group.

Use the `Message Source Templates` window (see Figure 1) to make your own policy group:

- a. Open the `Message Source Templates` window, select the policy group you want to copy and click the `[Copy . . .]` button.
- b. Enter a name and description for the new policy group in the fields provided and click `[OK]`.
- c. In the left pane, select the new policy group.
- d. In the right pane, select the policies and monitors you do not need and remove them using the `Delete From Group` button.
- e. Configure the monitors and policies you need.

Figure 1 Message Source Template Window



2. In the Node Bank window, select the Windows nodes to which you want to assign policies.

Nodes selected together require the same policies (they must all have the same BackOffice applications running).

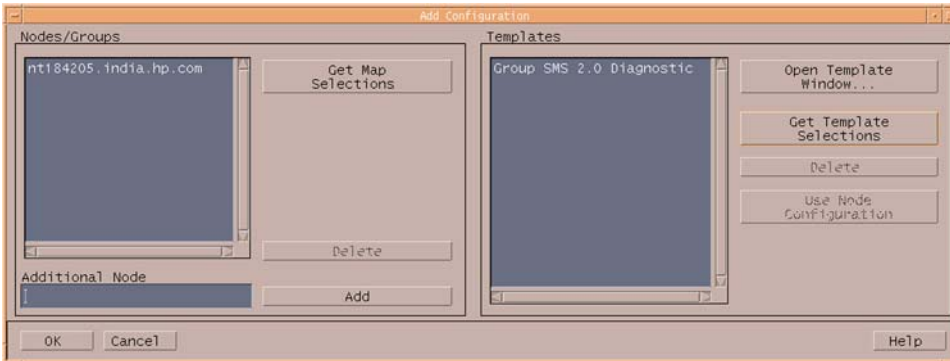
3. From the menu bar, select the Actions -> Agents -> Assign Templates... menu option.

The Define Configuration window opens.

4. Click [Add...].

The Add Configuration window opens (see Figure 2).

Figure 2 Add Configuration Window



5. Click [Open Template window...].
The Message Source Templates window appears.
6. In the left pane, expand the MICROSOFT WINDOWS policy group and select the policy group or groups you created (for example, SMS 2.0 Diagnostic).
The policy group or groups you created contain the policies you need.
7. Return to the Add Configuration window.
8. Click [Get Template Selections].
The newly assigned policy is displayed in the Policies list.
9. Click [OK] to finish assigning policies.

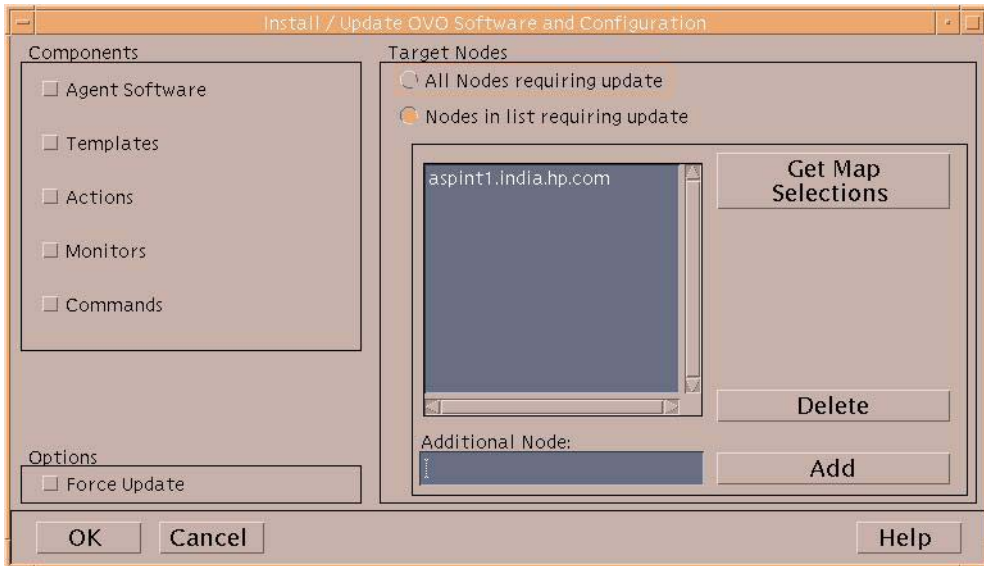
Distributing Components to the Windows Nodes

You can distribute Smart Plug-in components to some or all Windows nodes from a central console.

1. Select the Windows nodes to which you wish to distribute Smart Plug-in components.
2. From the menu bar of the Node Group window, select the Actions -> Agents -> Install / Update SW & Config... menu option.

The Install / Update OVO Software and Configuration window appears (see Figure 3).

Figure 3 Install / Update OVO Software and Configuration



3. Select `Force Update`.
4. Click [OK] to finish the distribution.

TIP

HP OpenView Operations administrators online help explains in detail the options for installing and updating software.

Uninstalling the WinOS SPI

To uninstall the WinOS SPI software, you need to:

- Remove WinOS SPI components from the managed nodes.
- Remove WinOS SPI components from the management server.

WinOS SPI components include the following:

- Applications
- Directory structure
- File sets
- Message groups
- Message source policies
- Node group
- Operator profile
- Software and documentation packages

Instructions are in “To Remove WinOS SPI Components from the Management Server” on page 27.

NOTE

To uninstall the software from managed nodes or from the OVO server, you must be logged on as the OVO administrator (user name `opc_adm`).

To Remove WinOS SPI Components from the Managed Nodes

1. From OVO Node Bank window menu bar, select:

Actions -> Agents -> Assign Templates...

The Define Configuration window, which shows a list of every combination of managed node and assigned policy, appears.

2. From the list, select entries where the policy is a WinOS SPI policy and the managed node is one from which you want to uninstall the WinOS SPI.
3. Click [Remove Selected], and then click [OK].

The policy configurations for the managed nodes are changed. You must now distribute the changed policies to the managed nodes.
4. In the OVO Node Bank window, select the managed nodes for which you changed the policy configurations.
5. From the menu bar, select:

`Actions -> Agents -> Install / Update SW & Config ...`

The Install / Update OVO Software Configuration window appears.
6. Check all listed items except Agent Software, and then click [OK].
7. Run the WinOS SPI Clean Node application to remove any WinOS SPI configuration data and instrumentation from the managed nodes.

NOTE

By default, the `Additional Parameter` is set to **No**. Ensure that you have set the `Additional Parameter` to **yes**, before you use the WinOS SPI Clean Node application.

To Remove WinOS SPI Components from the Management Server

You must remove the `WINOSSPI-Discovery` policy from the management server before uninstalling WinOS SPI from the management server.

Removing WINOSSPI-Discovery Policy

You can remove the `WINOSSPI-Discovery` policy from the management server as follows:

1. From OVO Node Bank window menu bar, select:

`Actions -> Agents -> Assign Templates...`

To Remove WinOS SPI Components from the Management Server

The `Define Configuration` window, which shows a list of every combination of managed node and assigned policy, appears.

2. From the list, select the `WINOSSPI-Discovery` policy and the management server from which you want to uninstall the policy.
3. Click `[Remove Selected]`, and then click `[OK]`.

The policy configurations for the management server are changed. You must now distribute the changed policies to the management server.

4. In the `OVO Node Bank` window, select the management server for which you changed the policy configurations.
5. From the menu bar, select:

`Actions -> Agents -> Install / Update SW & Config ...`

The `Install / Update OVO Software Configuration` window appears.

6. Check `Templates Install / Update OVO Software Configuration` window and then click `[OK]`.

This completes the removal of `WINOSSPI-Discovery` policy from the management server.

Before uninstalling the WinOS SPI software from the management server, make sure you have uninstalled the WinOS SPI components from all the managed nodes you were monitoring. Instructions are in “To Remove WinOS SPI Components from the Managed Nodes” on page 26.

1. Run the WinOS SPI Clean Server application to remove any WinOS SPI configuration data and instrumentation from the management server.

NOTE

By default, the `Additional Parameter` is set to **No**. Ensure that you have set the `Additional Parameter` to **yes**, before you use the WinOS SPI Clean Server application.

2. Remove all message groups installed with the WinOS SPI:
 - a. From the menu bar, select `Window -> Message Group Bank` to go to the `Message Group Bank` window.

- b. For each message group listed in Table 4 on page 39, select it, right-click the mouse, and select Delete from the pop-up menu that appears.

WARNING

Do not delete message groups other than the message groups listed in Table 4 on page 39.

3. Remove the Windows OS SPI and HP Systems Insight Manager application group:
 - a. From the menu bar, select `Window -> Application Bank` to go to the `Application Bank` window.
 - b. Select the Windows OS SPI application group, right-click the mouse, and select `Delete` from the pop-up menu that appears.
 - c. Select the HP Systems Insight Manager application group, right-click the mouse, and select `Delete` from the pop-up menu that appears.
4. Remove the WinOSSPI node group:
 - a. From the menu bar, select `Window -> Node Group Bank` to go to the `Node Group Bank` window.
 - b. Select the WinOSSPI node group, right-click the mouse, and select `Delete` from the pop-up menu that appears.
5. Remove the Windows Operator user profile:
 - a. From the menu bar, select `Window -> User Profile Bank` to go to the `User Profile Bank` window.
 - b. Select the Windows Operator user profile, right-click the mouse, and select `Delete` from the pop-up menu that appears.
6. Delete all the groups, subgroups, and policies delivered with the WinOS SPI:
 - a. From the menu bar, select `Window -> Message Source Templates` to go to the `Message Source Templates` window.
 - b. In the left pane of the bi-pane window, select `Operating System SPIs`, and under that select `MICROSOFT WINDOWS`.

To Remove WinOS SPI Components from the Management Server

The components of the `MICROSOFT WINDOWS` group appear in the right pane.

- c. Delete the `MICROSOFT WINDOWS` group.

The highest-level subgroup appears in the Message Source Templates window.

- d. Select and delete all subgroups of the `MICROSOFT WINDOWS` group.

The next highest-level subgroup appears in the Message Source Templates window

IMPORTANT

Repeat this step recursively until all `MICROSOFT WINDOWS` subgroups have been deleted and the `MICROSOFT WINDOWS` policies appear in the Message Source Templates window.

`MICROSOFT WINDOWS` policies have the following syntax:

```
WINOSSPI-<TemplateName>
```

- e. Select and delete all WinOS SPI policies.

7. Repeat the procedure described in the previous step to remove all groups, subgroups, and policies in the `HP Systems Insight Manager` policy group.
8. Remove all software packages that relate to the WinOS SPI by entering the following:

```
/usr/sbin/swremove
```

Select and remove the following package on your system:

```
- SPI-WIN-OVO
```

If problems occur during uninstallation, check the following log files:

- `/var/admin/sw/swremove.log`
- `/var/admin/sw/swagent.log`

Installed File Locations

Table 2 WinOS SPI File Locations on the OVO Management Server

File Type	Directory Location
Binaries	/opt/OV/lbin/winosspi/
Documentation	/opt/OV/paperdocs/winosspi/<LANG>/ <LANG> is the directory name that specifies the language version of the Windows OS SPI installed.
Log files	/var/opt/OV/share/log/winosspi/
Windows OS SPI Configuration files	/var/opt/OV/share/conf/winosspi/
Service Discovery Binaries	/opt/OV/lbin/SPISvcDisc/
Service Discovery Images	/opt/OV/www/htdocs/ito_op/images
Temporary and Runtime	/opt/OV/winosspi/tmp
OVO Integration	/var/opt/OV/share/tmp/OpC_appl/winosspi
Application Group Bitmaps	/etc/opt/OV/share/bitmaps/C/sw_utils /opt/OV/www/htdocs/bitmaps/C/sw_utils
Message Group Bitmaps	/etc/opt/OV/share/bitmaps/C/software /opt/OV/www/htdocs/bitmaps/C/software
Symbols	/etc/opt/OV/share/symbols/C/WinOSSPI/ appgroups /etc/opt/OV/share/symbols/C/WinOSSPI/ msggroups

To Remove WinOS SPI Components from the Management Server

Table 3 WinOS SPI File Locations on the OVO Managed Node for DCE Agents

File Type	Directory Location
Instrumentation	<%OvAgentDir%>\bin\OpC\actions <%OvAgentDir%>\bin\OpC\cmds <%OvAgentDir%>\bin\OpC\monitor
Log and Trace files	<%OvAgentDir%>\log\SPISvc-Disc\winosspi_discovery.log <%OvAgentDir%>\log\SPISvc-Disc\winosspi_discovery.trc <%OvAgentDir%>\log\winosspi\winosspi.log <%OvAgentDir%>\log\winosspi\winosspi.trace (This file is present only if you enable tracing.)
Registry Key	HKLM\SOFTWARE\Hewlett-Packard\HP Open-view\winosspi

OvAgentDir is the environment variable pointing to the directory where the OpenView Operations DCE agent software is installed.

Table 4 WinOS SPI File Locations on the OVO Managed Node for HTTPS Agents

File Type	Directory Location
Instrumentation	<OVINSTALLDIR>\data\bin\Instrumentation
Log and Trace files	<OVINSTALLDIR>\log\SPISvc-Disc\winosspi_discovery.log <OVINSTALLDIR>\log\SPISvc-Disc\winosspi_discovery.trc <OVINSTALLDIR>\data\log\winosspi\winosspi.log <OVINSTALLDIR>\data\log\winosspi\winosspi.trace (This file is present only if you enable tracing.)
Registry Key	HKLM\SOFTWARE\Hewlett-Packard\HP Open-View\winosspi

`OVINSTALLDIR` points to the directory where the OpenView Operations HTTPS agent software is installed.

3

Using the WinOS SPI

This chapter describes the components that are added to OVO during installation of the WinOS SPI software and how to use them.

The WinOS SPI comprises the following components on the OVO management server.

- Message Groups
- Applications and Application Groups
- Policies and Policy Groups
- Executables

Message Groups

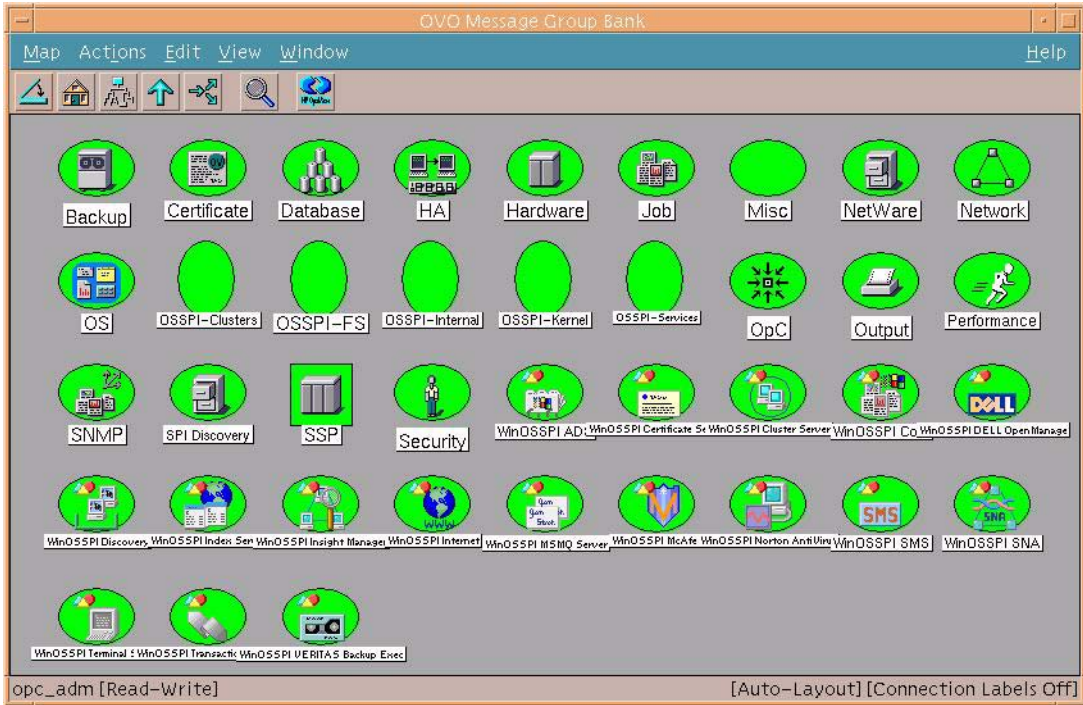
OVO uses message groups to combine management information about similar or related managed objects under a chosen name, and provide status information on a group level.

Messages are organized into groups to simplify message management, and to let you do your work in a task-oriented way. For example, one operator can be responsible for backups and output, and another operator can be responsible for network, operating system, and security aspects of message management.

Message Group Bank Window

The `Message Group Bank` window contains symbols for the message groups for which a particular operator is responsible. In this window, you can review the status of each group, and select specific groups for message review, as shown in Figure 4 on page 38.

Figure 4 OVO Message Group Bank Window



Message Group Colors

In the Message Group Bank window, the color of a particular symbol represents the current status. A change in the color of a symbol in the Message Group Bank window indicates a change in status of a managed node within an operator's environment. If a message with the severity level Critical arrives in your browser, the Message Group Bank window automatically opens and moves to the front of your display to notify you of the event. You can, however, configure OVO so that this window remains in its original position when a critical message arrives.

When you are logged on as an operator with WinOS SPI responsibilities, your Message Group Bank window contains some or all of the message

groups listed in Table 4, depending on the responsibilities assigned to you by the OVO administrator.

Table 4 **Message Groups and Labels**

Label	Message Group	Description
WinOSSPI ADS	WINOSSPI-ACTIVEDIRECTORY_SERVICE	Messages for Active Directory Services
WinOSSPI Certificate Server	WINOSSPI-MS_CERTIFICATE_SERVER	Messages for Microsoft Certificate Server
WinOSSPI Cluster Server	WINOSSPI-MS_CLUSTER_SERVER	Messages for Microsoft Cluster Server
WinOSSPI Core	WINOSSPI-CORE	Messages for Core Services
WinOSSPI DELL OpenManage	WINOSSPI-DELL_OPEN_MANAGE	Messages for DELL OpenManage
WinOSSPI Discovery	WINOSSPI-DISCOVERY	Messages for Service Discovery
WinOSSPI Index Server	WINOSSPI-MS_INDEX_SERVER	Messages for Microsoft Index Server
WinOSSPI Insight Manager	WINOSSPI-INSIGHT_MANAGER	Messages for Insight Manager
WinOSSPI Internet	WINOSSPI-INTERNET_SERVICE	Messages for Internet Services
WinOSSPI McAfee	WINOSSPI-MCAFEE	Messages for McAfee Virus Scan
WinOSSPI Norton AntiVirus	WINOSSPI-NORTON_ANTI_VIRUS	Messages for Norton AntiVirus
WinOSSPI Terminal Server	WINOSSPI-MS_TERMINAL_SERVER	Messages for Microsoft Terminal Server
WinOSSPI Transaction Server	WINOSSPI-MS_TRANSACTION_SERVER	Messages for Microsoft Transaction Server
WinOSSPI SMS	WINOSSPI-MS_SYSTEMS_MGMT_SERVER	Messages for Microsoft Systems Management Server
WinOSSPI SNA	WINOSSPI-MS_SNA	Messages for MS SNA
WinOSSPI MSMQ Server	WINOSSPI-MS_MESSAGE_QUEUE_SERVER	Messages for Microsoft Message Queue Server

Table 4 **Message Groups and Labels**

Label	Message Group	Description
WinOSSPI VERITAS Backup Exec	WINOSSPI-VERITAS_BACKUP_EXEC	Messages for VERITAS Backup Exec

Application Groups

The installation of the WinOS SPI adds two new application groups to the OVO Application Bank window. The new application groups are Windows OS SPI and HP Systems Insight Manager. The HP Systems Insight Manager application group contains applications for configuring and monitoring the status of HP Systems Insight Manager services. The Windows OS SPI application group contains the application groups shown in Figure 5.

Figure 5 Windows OS SPI Application Groups



This set of applications enables you to do the following:

- Enable or disable WinOS SPI tracing
- Self-Healing services tools to collect data and perform trace on management server and managed nodes
- Monitor the status of MS Cluster Server and run Cluster Server applications on the managed nodes.
- Start Windows services and processes.
- Stop Windows services and processes.
- Check the status of Windows services and processes.

Prerequisites to Run Windows OS SPI Applications

- Display information about a web server
- Configure trap destinations
- Provides core information about the operating system and networking
- Configure nodes with HP SIM installed

Prerequisites to Run Windows OS SPI Applications

You must install the agents on the management server before running the Windows OS SPI applications.

The following application groups installed by WinOS SPI are explained in greater detail in the sections that follow:

HP Systems Insight Manager	This group contains applications for configuring and monitoring the status of HP Systems Insight Manager services running on the nodes.
Metaframe Tools	This group contains applications for monitoring Citrix Metaframe services.
Insight Manager	This group contains applications for configuring hardware trap destinations on Insight Manager managed nodes, launching the Insight Manager agent web interface, and starting or stopping applications that provide service status information.
Microsoft Windows Core	This group contains applications that help manage MS Terminal, Active Directory, and networking services. They also offer in-depth coverage of the Windows NT4, 2000, XP, and 2003 Server operating systems.
MS BackOffice Application	This group contains applications for starting, stopping and querying the status of the services associated with key Microsoft BackOffice application servers.
Web Servers	This group contains applications that can be used to monitor and view information about web servers.
WinOSSPI Discovery	This group contains an application that launches Service Discovery on node(s) or node groups. The Discovery application, installed by the WinOS SPI, is used to discover the services that you want to monitor on the managed nodes.
WinOSSPI Utils	This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of the , WinOS SPI namely; uninstallation and tracing.
Microsoft Windows Cluster	This group contains applications that you can use to manage Microsoft Windows Cluster servers.

Application Group: HP Systems Insight Manager

Run the application `Set JRE Path` from the HP Systems Insight Manager application group in the OVO Application Bank to set the Java path on the

OVO management server. You must perform this activity before running any HP Systems Insight Manager applications.

This group contains applications for setting the configuration of HP Systems Insight Manager services. The applications also monitor the status of HP Systems Insight Manager services running on the nodes.

Table 5 lists the applications present in the HP Systems Insight Manager application group and provides a brief description.

Table 5 HP Systems Insight Manager Applications

Application Name	Description
Add nodes to HP SIM	Adds nodes to the HP Systems Insight Manager server.
Execute HP SIM Tool	Executes the specified HPSIM tool on the HPSIM- managed nodes. Based on the parameter specified, (WAIT or NOWAIT), the Execute HP Systems Insight Manager tool returns either of the following: <ul style="list-style-type: none"> • The status of the HPSIM tool executed (when the WAIT parameter is specified) • The job identification (jobid) of the HPSIM tool executed (when the NOWAIT parameter is specified). You can provide the jobid as a parameter to the Get HP SIM Tool Status to retrieve the status of the tool execution.
Get HP SIM Certificate	Gets certificate from the HP Systems Insight Manager server and stores it in a keystore to be used by other tools. This tool is used to get the certificate if you lose the keystore or you need to update it. The keystore is placed in the /var/opt/OV/share/conf/winosspi directory on the management server. The name is winosspi.keystore.

Table 5

HP Systems Insight Manager Applications

Application Name	Description
Get HP SIM Nodes	Gets nodes being managed by the HP Systems Insight Manager server.
Get HP SIM Port	Gets the SSL port to be used by other tools to communicate with the HPSIM server. This tool is useful when a custom SSL port is configured in the <code>mx.properties</code> file in the HPSIM server (the default port is 50001). That port can then be obtained by executing this tool. The obtained port must be manually added to the <code>/var/opt/OV/share/conf/winosspi/winosspi.properties</code> file as <code><hpsim server FQDN name>=<custom port></code> ; for example, <code>testbox.domain.com=50023</code> .
Get HP SIM Tool Status	Gets the status of tool execution on HP Systems Insight Manager managed nodes. Also displays the output of the tool execution.
Launch HP SIM Console	<p>Launches the HP Systems Insight Manager (HPSIM) console by default. If you specify the <code>system</code> names and <code>tool</code> name parameters, the corresponding HPSIM page is displayed. Refer to the HP SIM documentation for browser specifications to launch the HP SIM console on the management server.</p> <p>To run this application, you must include the path to the default browser application (installed on the management server) in the <code>PATH</code> environment variable on the management server. You must add the following line in the <code>.profile</code> file on the management server to export the <code>PATH</code> environment variable.</p> <pre>export PATH=\$PATH:<path to the browser application on the management server></pre>

Table 5 HP Systems Insight Manager Applications

Application Name	Description
Set JRE Path	Sets the JRE path on the management server for OVO-HP SIM integration
Start HP SIM Service	Starts the HP Systems Insight Manager service.
Start OpenSSH Service	Starts the OpenSSH service.
Start Pegasus WMI Mapper Service	Starts the WMI Mapper service.
Status HP SIM Service	Reports status of the HP Systems Insight Manager service.
Status OpenSSH Service	Reports status of the OpenSSH service.
Status Pegasus WMI Mapper Service	Reports status of WMI Mapper service.
Stop HP SIM Service	Stops the HP Systems Insight Manager service.
Stop OpenSSH Service	Stops the OpenSSH service.
Stop Pegasus WMI Mapper Service	Stops the WMI Mapper service.

Application Group: Metaframe Tools

This group contains applications for monitoring Citrix Metaframe services.

Table 6 lists the applications present in the Metaframe Tools application group and provides a brief description.

Table 6 Metaframe Tools Applications

Application Name	Description
ACL Info	Shows information about user rights.
AuditLog	Shows information about the software installed on the system.
Disconnect	Disconnects a terminal session.

Table 6 Metaframe Tools Applications

Application Name	Description
Flush	Synchronizes disk data.
License	Shows information about the license.
Processes	Lists processes on MF servers.
Send Message	Sends message to ICA client users.
Servers	Lists available MF servers.
Sessions	Lists open MF sessions.
Users	Lists connected users on an MF server.
Start ICABrowser	Starts the ICABrowser service.
Start Program Neighbourhood	Starts the ProgNeighbourhood service.
Stop ICABrowser	Stops the ICABrowser service.
Stop Program Neighbourhood	Stops the ProgNeighbourhood service.

Application Group: Insight Manager

This group contains applications for configuring hardware trap destinations on Insight Manager managed nodes, launching the Insight Manager agent web interface, and starting or stopping applications that provide service status information.

Table 7 lists the applications present in the Insight Manager application group and provides a brief description.

Table 7 Insight Manager Applications

Application Name	Description
Configure SNMP Trap Destination	Configures SNMP trap destination on the Insight Manager nodes.
IM Agent Web Interface	Starts the Insight Manager Agent web interface.

Table 7 **Insight Manager Applications**

Application Name	Description
Start Foundation Agents	Starts Insight Manager's Foundation Agents service.
Start NIC Agents	Starts Insight Manager's NIC Agents service.
Start Server Agents	Starts Insight Manager's Server Agents service.
Start Storage Agents	Starts Insight Manager's Storage Agents service.
Start Version Control Agent	Starts Insight Manager's Version Control Agent service.
Start Web Agent	Starts Insight Manager's Web Agent service.
Status Foundation Agents	Reports status of Insight Manager's Foundation Agents service and process.
Status NIC Agents	Reports status of Insight Manager's NIC Agents service and process.
Status Server Agents	Reports status of Insight Manager's Server Agents service and process.
Status Storage Agents	Reports status of Insight Manager's Storage Agents service and process.
Status Version Control Agent	Reports status of Insight Manager's Version Control Agent service and process.
Status Web Agent	Reports status of Insight Manager's Web Agent service and process.
Stop Foundation Agents	Stops Insight Manager's Foundation Agents service.
Stop NIC Agents	Stops Insight Manager's NIC Agents service.
Stop Server Agents	Stops Insight Manager's Server Agents service.

Table 7

Insight Manager Applications

Application Name	Description
Stop Storage Agents	Stops Insight Manager's Storage Agents service.
Stop Version Control Agent	Stops Insight Manager's Version Control Agent service.
Stop Web Agent	Stops Insight Manager's Web Agent service.

Application Group: Microsoft Windows Core

This group contains applications that help manage MS Terminal, Active Directory, and networking services. They also offer in-depth coverage of the Windows NT4, 2000, XP, and 2003 Server operating systems.

Figure 6 Microsoft Windows Core Application Group

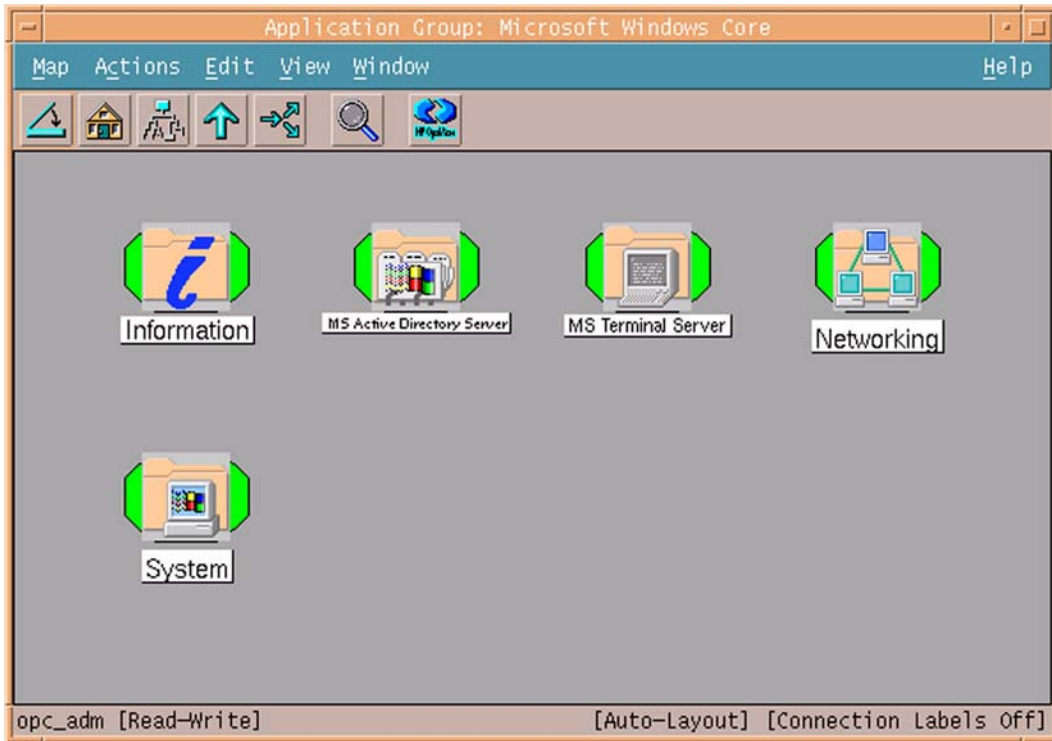


Table 8 lists the application sub groups and applications present in the Microsoft Windows Core and provides a brief description.

Table 8 Microsoft Windows Core Application Group and Applications

Application Group	Application	Description
Information	Drive Information	Displays all drives that are available on the node.
	Get System Overview	Displays information about operating system version, hardware, memory, network, drives, processes, CPU load, and IP configuration of the selected node.

Table 8

Microsoft Windows Core Application Group and Applications

Application Group	Application	Description
Information	Hardware Information	Displays hardware information.
	Memory Information	Displays memory information.
	OS Version	Displays information about the installed operating system.
	PerfMon Objects	Lists all available Performance Monitor Objects and Counters
	Session List	Lists all sessions on the node.
	User List	Lists all node users.
	Installed Software	Displays information about the software installed on the system.
	Job Status	Displays information about the job status on the system.
	Local User	Displays information about the local user on the system.
	Server Config	Shows the software and network attributes of the system.
	Server stats	Shows the server statistics for the system.
	Shares	Shows the list of shared drives and folders on the system.
	Show Drivers	Shows the list of Drivers on the system.
	Used Shares	Displays information about the mapped shares on the system.
Workst Stats	Displays information about network statistics of the system.	

Table 8

Microsoft Windows Core Application Group and Applications

Application Group	Application	Description
MS Active Directory Server	ADS Printer Information	Lists all printers known in the Active Directory. It is possible to restrict the output on specific Organizational Units (OU) by using the parameters "-ou <name of OU>" instead of "-all".
	Check ADS Service	Connects to the ADS service of the specific node using ADSI.
MS Terminal Server	Start Term Server Licensing	Starts TermServLicensing service.
	Start TermService	Starts TermService service
	Status	Reports status of Windows Terminal Server services and processes
	Stop Term Server Licensing	Stops TermServLicensing service.
	Stop TermService	Stops TermService service.

Table 8

Microsoft Windows Core Application Group and Applications

Application Group	Application	Description
Networking	IPX Information	Displays information on all the bindings that IPX is configured for.
	Name Server Lookup	Displays the fully qualified DNS name and IP address of the node specified in the parameter field (by default you start the command on the chosen nodes and get information about them) and its DNS server.
	Network Information	Displays network information of the node and its server.
	Show Hostname	Displays hostname of the selected node.
	Show IP Configuration	Displays IP configuration of the node.
	Show TCP/IP Connections	Displays current TCP/IP network connections.
	TCP/IP Statistics	Displays statistics for the TCP, IP, and UDP protocols.
	NetBios Sessions	Displays information about the NetBios connection table on the system.

Table 8

Microsoft Windows Core Application Group and Applications

Application Group	Application	Description
System	Cancel Shutdown	Cancels shutdown of the node.
	CPU Load	Displays information about the CPU load on the system.
	Enable Disk Performance Counters	Enables the disk performance counters for logical drives on a Windows 2000 system. The counters will NOT be enabled before the system is restarted.
	Kill Process	Kills a process specified with the "/name" or "/pid" parameters.
	List Processes	Lists all running processes and includes some detailed information about them.
	List Service	Lists all services with start mode and actual state.
	Scan Registry	Scans the registry of a node for a specified pattern. Usage: /scan <pattern> /initkey lm cu cr us cc /key <path> [/view]
	Send Message	Sends a message to the selected node(s).
	Show Directory	Returns the contents of the directory that is given as the parameter.

Table 8

Microsoft Windows Core Application Group and Applications

Application Group	Application	Description
System	Show Registry Key	Displays a specified registry key. Usage: /view /initkey lm cu cr us cc /key <path> [/valuename <name>] Abbreviations: lm - KEY_LOCAL_MACHINE cu - KEY_CURRENT_USER cr - KEY_CLASSES_ROOT us - KEY_CLASSES_ROOT cc - KEY_CURRENT_CONFIG
	List Sessions	Displays information about the sessions between the system and other systems on the network.
	Shutdown	Shuts down node. Parameters: /m <shutdown message> /t <timeout in sec> /a abort shutdown /r reboot after shutdown /f force shutdown /w popup window notification
	Start Service	Starts a service
	Stop Service	Stops a service

Application Group: MS BackOffice Application

This group contains applications for starting, stopping and querying the status of the services associated with key Microsoft BackOffice application servers.

Application Group: MS BackOffice Application

Figure 7 MS BackOffice Application Group

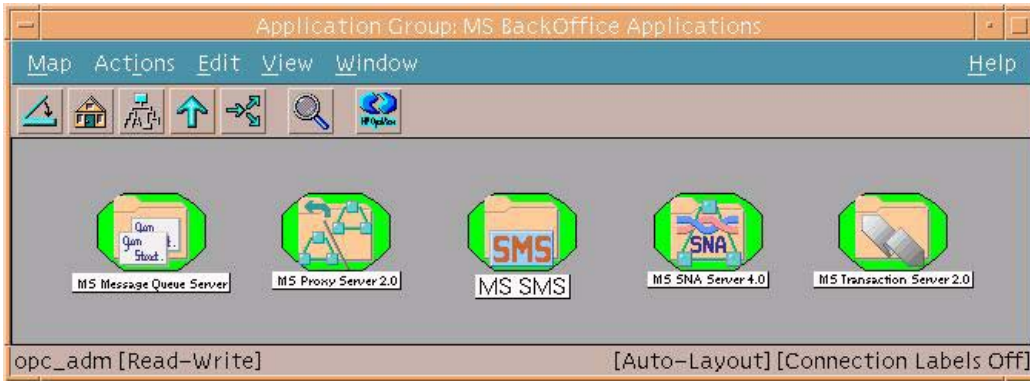


Table 9 lists the applications sub groups present in the MS BackOffice application group and provides a brief description.

Table 9 MS Back Office Application Group and Applications

Application Group	Application Name	Description
MS Message Queue Server	Start MSMQ	Starts MSMQ service.
	Status	Reports status of MSMQ 1.0 services and processes.
	Stop MSMQ	Stops MSMQ service.

Table 9

MS Back Office Application Group and Applications

Application Group	Application Name	Description
MS Proxy Server 2.0	Start MS PAN 2.0	Starts Microsoft Proxy Alert Notification service.
	Start MS PSA 2.0	Starts Microsoft Proxy Server Administration service.
	Start MS WPS 2.0	Starts Microsoft WinSock Proxy service.
	Status MS PAN 2.0	Reports status of Microsoft Proxy Alert Notification service.
	Status MS PSA 2.0	Reports status of Microsoft Proxy Server Administration service.
	Status MS WPS 2.0	Reports status of Microsoft WinSock Proxy service.
	Stop MS PAN 2.0	Stops Microsoft Proxy Alert Notification service.
	Stop MS PSA 2.0	Stops Microsoft Proxy Server Administration service.
	Stop MS WPS 2.0	Stops Microsoft WinSock Proxy service.

Table 9 MS Back Office Application Group and Applications

Application Group	Application Name	Description
MS SMS	Start SMS_CLIENT_SERVICE	Starts SMS_CLIENT_SERVICE service.
	Start SMS_EXECUTIVE	Starts SMS_EXECUTIVE service.
	Start SMS_SITE_COMPONENT_MANAGER	Starts SMS_SITE_COMPONENT_MANAGER service.
	Start_SMS_SQL_MONITOR	Starts the SMS_SQL_MONITOR service.
	Status	Reports status of SMS services and processes.
	Stop SMS_CLIENT_SERVICE	Stops SMS_CLIENT_SERVICE service.
	Stop SMS_EXECUTIVE	Stops SMS_EXECUTIVE service.
	Stop SMS_SITE_COMPONENT_MANAGER	Stops SMS_SITE_COMPONENT_MANAGER service.
	Stop_SMS_SQL_MONITOR	Stops the SMS_SQL_MONITOR service.
MS SNA Server 4.0	Start SnaBase	Starts SnaBase service.
	Start SnaServr	Starts SnaServr service.
	Status	Reports status of SNA 4.0 services and processes.
	Stop SnaBase	Stops SnaBase service.
	Stop SnaServr	Stops SnaServr service.

Table 9 MS Back Office Application Group and Applications

Application Group	Application Name	Description
MS Transaction Server 2.0	Start MSDTC	Starts MSDTC services.
	Status	Reports status of Trans Svr 2.0 services and processes.
	Stop MSDTC	Stops MSDTC service.

Application Group: Web Servers

The WinOS SPI provides a number of preconfigured applications for monitoring the most popular Microsoft web server applications:

- Microsoft Internet Information Server 4.0
- Microsoft Internet Information Server 5.0
- Microsoft Site Server 3.0, Commerce Edition

Figure 8 Web Server Application Group



Table 10 lists the application sub groups and applications present in the Web Server and provides a brief description.

Table 10 **Web Server Application Group and Applications**

Application Group	Application Name	Description
	Query Web Server	Displays information about a web server. The web server can be any server. Uses the proxy settings of Microsoft Internet Explorer.
MS IIS 4.0	Start FTP 4.0	Starts FTP publishing service.
	Start IISADMIN 4.0	Starts IISADMIN 4.0 service.
	Start Index 4.0	Starts Index 4.0 service.

Table 10

Web Server Application Group and Applications

Application Group	Application Name	Description
MS IIS 4.0	Start NNTP 4.0	Starts Network News Transfer Protocol 4.0 service.
	Start SMTP 4.0	Starts Simple Mail Transfer Protocol service.
	Start WWW 4.0	Starts World Wide Web publishing service.
	Status FTP 4.0 Service	Status FTP 4.0 Service
	Status FTP 4.0 Site(s)	Reports status of IIS 4.0 FTP publishing server site(s).
	Status IIS 4.0	Reports status of IIS 4.0 services and processes.
	Status Index 4.0	Reports status of Index 4.0 service.
	Status NNTP 4.0	Reports status of Network News Transfer Protocol 4.0 service.
	Status SMTP 4.0	Reports status of Simple Mail Transfer Protocol service.
	Status WWW 4.0 Service	Reports Status Of World Wide Web Publishing Services And Processes.
	Status WWW 4.0 Site(s)	Reports status of IIS 4.0 World Wide Web publishing server site(s).
	Stop WWW 4.0	Stops World Wide Web publishing service.
	Stop FTP 4.0	Stop FTP 4.0
	Stop IISADMIN 4.0	Stops IISADMIN 4.0 services.
Stop Index 4.0	Stops Index 4.0 services.	
Stop NNTP 4.0	Stops Network News Transfer Protocol 4.0 service.	

Table 10 **Web Server Application Group and Applications**

Application Group	Application Name	Description
MS IIS 4.0	Stop SMTP 4.0	Stops Simple Mail Transfer Protocol service
MS IIS 5.0	Restart IIS 5.0	Restarts IIS 5.0 services.
	Start FTP 5.0	Starts FTP publishing services.
	Start IIS 5.0	Starts IIS 5.0 services.
	Start Index 5.0	Starts Index 5.0 services.
	Start NNTP 5.0	Starts Network News Transfer Protocol 5.0 service.
	Start SMTP 5.0	Starts Simple Mail Transfer Protocol service.
	Start WWW 5.0	Starts World Wide Web publishing service.
	Status FTP 5.0 Service	Reports status of FTP publishing service.
	Status FTP 5.0 Site(s)	Reports status of IIS 5.0 FTP publishing server site(s).
	Status IIS 5.0	Reports status of IIS 5.0 services and processes.
	Status Index 5.0	Reports status of Index 5.0 service.
	Status NNTP 5.0	Reports status of Network News Transfer Protocol 5.0 service.
	Status SMTP 5.0	Reports status of Simple Mail Transfer Protocol service.
	Status WWW 5.0 Service	Reports status of World Wide Web publishing service.
	Status WWW 5.0 Site(s)	Reports status of IIS 5.0 World Wide Web publishing server site(s).
Stop FTP 5.0	Stops FTP 5.0 services.	

Table 10

Web Server Application Group and Applications

Application Group	Application Name	Description
MS IIS 5.0	Stop IIS 5.0	Stops IIS 5.0 services.
	Stop Index 5.0	Stops Index 5.0 services.
	Stop NNTP 5.0	Stops Network News Transfer Protocol 5.0 service.
	Stop SMTP 5.0	Stops Simple Mail Transfer Protocol service.
	Stop WWW 5.0	Stops World Wide Web publishing service.
MS Site Server 3.0	Start SS 3.0 ACM	Starts Microsoft Site Server 3.0 Active Channel Multicaster.
	Start SS 3.0 AS	Starts Microsoft Site Server 3.0 Authentication service.
	Start SS 3.0 CRS	Starts Microsoft Site Server 3.0 Content Deployment service.
	Start SS 3.0 Gatherer	Starts Microsoft Site Server 3.0 Gatherer service.
	Start SS 3.0 LBS	Starts Microsoft Site Server 3.0 List Builder service.
	Start SS 3.0 LDAP	Starts Microsoft Site Server 3.0 LDAP service.
	Start SS 3.0 MBS	Starts Microsoft Site Server 3.0 Message Building service.
	Start SS 3.0 SS	Starts Microsoft Site Server 3.0 Search service.
	Status SS 3.0 ACM	Reports status of Microsoft Site Server 3.0 Active Channel Multicaster.
	Status SS 3.0 AS	Reports status of Microsoft Site Server 3.0 Authentication service.

Table 10 **Web Server Application Group and Applications**

Application Group	Application Name	Description
MS Site Server 3.0	Status SS 3.0 CRS	Reports status of Microsoft Site Server 3.0 Content Deployment service.
	Status SS 3.0 Gatherer	Reports status of Microsoft Site Server 3.0 Gatherer service.
	Status SS 3.0 LBS	Reports status of Microsoft Site Server 3.0 List Builder service.
	Status SS 3.0 LDAP	Reports status of Microsoft Site Server 3.0 LDAP service.
	Status SS 3.0 MBS	Reports status of Microsoft Site Server 3.0 Message Builder service.
	Status SS 3.0 SS	Reports status of Microsoft Site Server 3.0 Search service.
	Stop SS 3.0 ACM	Stops Microsoft Site Server 3.0 Active Channel Multicaster.
	Stop SS 3.0 AS	Stops Microsoft Site Server 3.0 Authentication service.
	Stop SS 3.0 CRS	Stops Microsoft Site Server 3.0 Content Deployment service.
	Stop SS 3.0 Gatherer	Stops Microsoft Site Server 3.0 Gatherer service.
	Stop SS 3.0 LBS	Stops Microsoft Site Server 3.0 List Builder service.
	Stop SS 3.0 LDAP	Stops Microsoft Site Server 3.0 LDAP service.
	Stop SS 3.0 MBS	Stops Microsoft Site Server 3.0 Message Builder service.
Stop SS 3.0 SS	Stops Microsoft Site Server 3.0 Search service.	

Application Group: WinOSSPI Discovery

This group contains an application that launches Service Discovery on node(s) or node groups. The Discovery application is used to discover the services that you want to monitor on the managed nodes. Table 11 lists the application present in the WinOSSPI Discovery application group and provides a brief description.

Table 11

WinOSSPI Discovery Application

Application Name	Description
Service Discovery	discovers the services that you want to monitor on the managed nodes.

For more information on Service Discovery, see “Service Discovery” on page 171.

Application Group: WinOSSPI Utils

This group contains applications which are intended to be used by the OVO administrator who is responsible for the administration of the WinOS SPI uninstallation and tracing. Table 12 lists the applications present in the WinOSSPI Utils application group and provides a brief description.

Table 12

WinOSSPI Utils Application

Application Name	Description
Clean Node	removes the configuration data generated and used by the WinOS SPI on the OVO managed node. This application execution requires a few minutes for completion.
Clean Server	removes the configuration data generated and used by the WinOS SPI on the OVO management server.
Tracing Off	disables tracing and sets the trace level to 0.
Tracing On	enables tracing and sets the trace level to 1.
Self Healing Info	runs the WinOS SPI data collector on the specified nodes. This application collects the log files and the configuration data from the specified node. For more information, refer to “Self-Healing Services” on page 181.

Application Group: Microsoft Windows Cluster

Application Name	Description
Self Healing - Server Collector	runs on the management server and collects the log files stored on the management server. This application also retrieves the configuration information of the management server. To use this application, you must make sure that the OpenView Operations Agent is installed on the management server from which you want to collect data. For more information, refer to “Self-Healing Services” on page 181.
Stop Cluster Monitor	Stops the Windows OS SPI cluster monitoring process on the cluster managed node. You must run this tool if the Windows OS SPI cluster message interceptor policies and the cluster schedule policy are removed from the managed node.

Application Group: Microsoft Windows Cluster

The `Microsoft Windows Cluster` application group includes applications that you can use to manage Microsoft Cluster servers. This application group contains the following application groups:

- **MS Cluster Server-** Includes applications you can use to manage the Microsoft Cluster server running on a cluster node.
- **MS Cluster Resource Group-** Includes applications that you can use to manage the cluster resource group.
- **MS Cluster Node-** Includes applications that you can use to manage the cluster node.
- **MS Cluster Network-** Includes applications that you can use to view the status of the cluster network and the corresponding network interfaces installed on the cluster network.

You must run `Microsoft Windows Cluster` applications on the remote cluster node.

NOTE

You must select the Resource Group ID from the options provided for the applications listed in Table 14, “MS Cluster Resource Group Applications,” on page 67, except for the `List Resource Group` application.

Application Group: MS Cluster Server

Table 13

MS Cluster Server Applications

Application Name	Description
Status	provides the status of the cluster service (CLUSSVC) running on the remote cluster node. You must run this tool on an individual cluster node. This tool displays the status of the cluster service and its resource usage in the status window on the management server.
Stop Clussvc	stops the CLUSSVC service running on the remote cluster node. You must run this tool on an individual cluster node.
Start Clussvc	Restarts the CLUSSVC service on the remote cluster node. You must run this tool on an individual cluster node.

Application Group: MS Cluster Resource Group

Table 14

MS Cluster Resource Group Applications

Application Name	Description
Bring Online	makes the specified resource group online. To specify the resource group that must be made online, you must select the Resource Group Index number corresponding to the resource group from the MS Cluster Tool window shown in Figure 9.
Take Offline	makes the specified resource group offline. To specify the resource group that must be made offline, you must select the Resource Group Index number corresponding to the resource group from the MS Cluster Tool window shown in Figure 9.
MOVE Resource Group	moves the resource group to the next available owner cluster node. To move a specific resource group, you must select the Resource Group Index number corresponding to the resource group from the MS Cluster Tool window shown in Figure 9.
List Resource Group	lists the resource group owned by the remote cluster node and the status of each resource group.

Application Group: Microsoft Windows Cluster

Figure 9

MS Cluster Tool Window



Application Group: MS Cluster Node

Table 15

MS Cluster Node Applications

Application Name	Description
Pause Node	pauses the cluster node.
Resume Node	resumes the cluster node.
List Nodes	lists the nodes in the cluster and displays the status of these nodes.

Application Group: MS Cluster Network

Table 16

MS Cluster Network Applications

Application Name	Description
Cluster Network Status	retrieves the state of the cluster network available on the cluster which includes the specified remote cluster node.
Cluster Network Interface Status	retrieves the state of the network interfaces owned by the specified cluster node.

4

Policies and Policy Groups

This chapter provides an overview and detailed descriptions of HP OpenView Operations SPI for Microsoft Windows OS policies.

Policies

WinOS SPI provides a set of preconfigured policies for Microsoft Windows nodes. These policies enable you to monitor the operations and performance of the services that run on these nodes. A complete list of the policies available begins on page 72.

WinOS SPI enables you to deploy policies manually according to your own requirements. Also, by modifying the preconfigured policies you can quickly create custom policies for your own specialized purposes.

NOTE

Logfile policies that read the `Windows Event Log` files do not have a preconfigured interval. The policies do not require an interval for event log entries because the agent registers events triggered when an entry is made in the `Event Log` file.

WMI Policies Support

The WinOS SPI includes functionality that accesses Windows Management Instrumentation (WMI) as a data provider for monitoring data of different managed applications. In the current version of the WinOS SPI this functionality is provided as black-box functionality, not as an officially supported functionality for OVO.

You can set polling interval and threshold parameters for the existing policies.

The current version of OVO and the WinOS SPI do *not* support the following:

- Changing policy data collection
- Creating new, additional, or derived WMI policies based on the technology provided by WinOS SPI

Prerequisites

The prerequisites for some WinOS SPI policies are described below.

Prerequisites for ADS Policies

WINOSSPI-ADS_SiteChanges

Before deploying the WINOSSPI-ADS_SiteChanges policy, run the following script on the managed node:

```
winosspi_CreateWMIInstance-ds_site.vbs
```

This script is deployed to managed nodes with DCE agents in the following directory:

```
%OvAgentDir%\bin\opc\cmds directory
```

For managed nodes with HTTPS agents, the script is deployed in the following directory:

```
%OvInstallDir%\data\bin\Instrumentation
```

The script is not used for policies, but is rather an initialization of a monitored node. This initialization is required to monitor changes to the site structure. By default, Windows 2000 WMI does not create information about existing sites of a given forest. The script fills this gap. Before deploying the WINOSSPI-ADS_SiteChanges policy, use the script to create a WMI ds_site instance for the site the given node belongs to.

For example, to manage the site changes for Site1 in the hp.com domain on the node, enter:

```
CreateWMIInstance-ds_site.vbs
```

```
LDAP://CN=Site1,CN=Sites,CN=Configuration,DC=hp,DC=com
```

You need to make this entry for all sites you want to monitor.

You can either make this entry on each domain controller for the site and deploy the policy to each domain controller, or you can make all entries on one domain controller and deploy the policy only to that domain controller to monitor the site changes for all sites.

Using Policies

This section describes in detail the preconfigured policies provided by WinOS SPI.

The SPI for Microsoft Windows policy group is renamed to MICROSOFT WINDOWS and appears under the group, Operating System SPI's.

OVO Default policies and conditions for monitoring the Windows operating system are regrouped under existing or new WinOS SPI policy groups and policies respectively. These policies are not available in the Default group with HP OpenView Operations version 8.x.

Policy Groups

The installation of the WinOS SPI uploads a number of policy groups to the OVO database.

Figure 10 WinOS SPI Policy Group

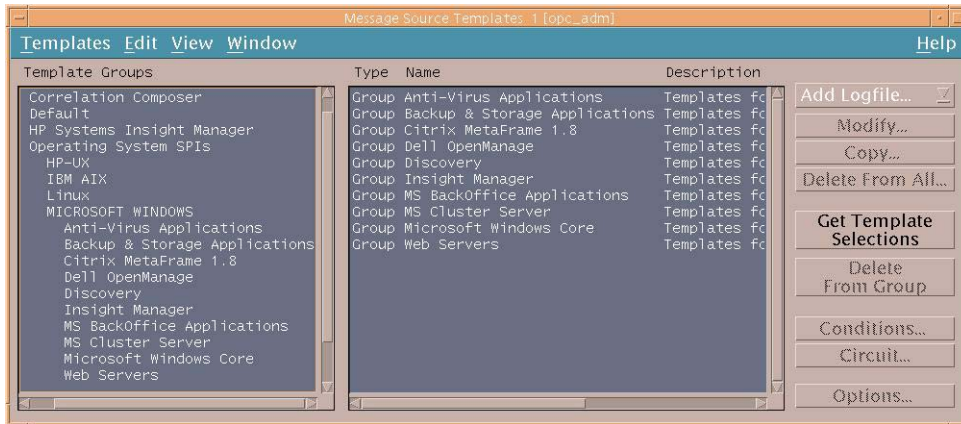


Figure 10 shows the high-level policy groups that are installed by default with the Win OS SPI software, namely:

- Anti-Virus Applications
- Backup & Storage Applications
- Citrix Metaframe 1.8
- Dell OpenManage
- Discovery
- Insight Manager
- HP Systems Insight Manager
- MS BackOffice Applications
- MS Cluster Server
- Microsoft Windows Core

Prerequisites for ADS Policies

- Web Servers

Anti Virus Applications

The policy groups under Anti Virus applications are:

- **McAfee VirusScan**
- **Norton Anti-Virus**

McAfee VirusScan → Diagnostic

WINOSSPI-McAfee_FwdAllWarnError

Description

Monitors the Application log for entries with a severity level of Warning or Error and the following sources: McAutoUpdate, McLogEvent. Forwards each found entry as a message to the active message browser.

WINOSSPI-McAfee_AVSyncMgr

Description

Checks the AV Sync Manager service and its corresponding process.

WINOSSPI-McAfee_McShield

Description

Checks the McShield service and its corresponding process.

Norton Anti-Virus → Diagnostic

WINOSSPI-NAV_FwdAllApplWarnError

Description

Forwards all Application log entries with a severity level of Warning or Error.

WINOSSPI-NAV_FwdAllSysWarnError

Description

Forwards all System log entries with a severity level of Warning or Error.

WINOSSPI-NAV_NortonAVServer

Description

Checks the Norton Anti-Virus Server

Backup and Storage Applications

The group of Backup and Storage application policies is:

- **VERITAS Backup Exec**

VERITAS Backup Exec -> Diagnostic

WINOSSPI-VeritasBackupExec_FwdAllWarnError

Description

Forwards all event log entries with severity level of Warning or Error.

Citrix Metaframe Applications

The group of Citrix metaframe application policies is:

- **Citrix Metaframe**

Citrix Metaframe -> Diagnostic

WINOSSPI-MF_FwdAllSysWarnError

Description

Forwards all System log entries with a severity level of Warning or Error.

WINOSSPI-MF_Process_PctProcessorTime_IBrowser

Description

Checks for IBrowser instances in the % Processor Time counter of the Terminal Service Session object.

WINOSSPI-MF_ICA_Browser

Description

Checks the ICABrowser service and its corresponding process.

WINOSSPI-MF_Prog_Neighborhood

Description

Checks the ProgNeighborhood service and its corresponding process.

Dell OpenManage

Dell OpenManage → Diagnostic

WINOSSPI-DellServerAgent_FwdEventLogEntries

Description

Forwards Dell OpenManage Server Agent's event log entries.

WINOSSPI-DellServer_FwdEventLogEntries

Description

Forwards Dell OpenManage Server Administrator's event log entries.

Discovery

WINOSSPI-opcmmsg

Description

Message policy that intercepts messages submitted by opcmmsg. Service Discovery messages are also intercepted by this policy when discovery is executed on the managed node. .

Severity	Message
Minor	Windows OS SPI Discovery failed with errors. See the log file on the node for details.

WINOSSPI-Discovery

Description

Executes the service discovery process on the nodes in the WinOS SPI node group. This scheduled template executes the discovery process on all the nodes that are present in the WinOS SPI node group. You can modify this template to run the discovery process at any scheduled time.

Insight Manager

Insight Manager → Diagnostic → Foundation Agents

WINOSSPI-InsightManager_FoundationAgents

Description

Checks the Foundation Agents service and its corresponding process.

Insight Manager → Diagnostic → Hardware Traps

NOTE

The Operator Initiated Action in the policies executes a Perl script named `winossapi_IMAgentInterface.pl`. This Perl script opens a web browser displaying the System Management Homepage of the Node from which the message is received. The Operator Initiated Action will function only if Perl 5.6.1 or above is installed on the machine and a link to it exists in `/usr/bin`.

WINOSSPI-InsightManager_FwdChannelArrayTraps

Description

Forwards Insight Manager Fibre Channel Array SNMP traps.

WINOSSPI-InsightManager_FwdICATraps

Description

Forwards Insight Manager Intelligent Cluster Administrator SNMP traps.

WINOSSPI-InsightManager_FwdClusterTraps

Description

Forwards Insight Manager Cluster SNMP traps.

WINOSSPI-InsightManager_FwdCIMTraps

Description

Implements SNMP traps for Giga Byte Ethernet (GbE) switches.

WINOSSPI-InsightManager_FwdRPMTraps

Description

Implements SNMP traps for the Resource Power Management (RPM) group, which includes Uninterruptible Power Supply (UPS) and Compaq Console Controller (CMC) devices.

WINOSSPI-InsightManager_FwdCMCTraps

Description

Forwards Insight Manager Console Management Controller SNMP traps.

WINOSSPI-InsightManager_FwdDMITraps

Description

Forwards Insight Manager DMI SNMP traps.

WINOSSPI-InsightManager_FwdDriveArrayTraps

Description

Forwards Insight Manager Intelligent Drive Array SNMP traps.

WINOSSPI-InsightManager_FwdHostOSTraps

Description

Forwards Insight Manager Host Operating System SNMP traps.

WINOSSPI-InsightManager_FwdICATraps

Description

Forwards Insight Manager Intelligent Cluster Administrator SNMP traps.

WINOSSPI-InsightManager_FwdIDEDriveTraps

Description

Forwards Insight Manager Manageable IDE Drive SNMP traps.

WINOSSPI-InsightManager_FwdNICTraps

Description

Forwards Insight Manager Network Interface Card SNMP traps.

WINOSSPI-InsightManager_FwdPCConfigTraps

Description

Forwards Insight Manager PC Equipment Configuration SNMP traps.

WINOSSPI-InsightManager_FwdRackTraps

Description

Forwards Insight Manager Rack Information SNMP traps.

WINOSSPI-InsightManager_FwdRaidControllerTraps

Description

Forwards Insight Manager RAID Controller SNMP traps.

WINOSSPI-InsightManager_FwdRecoverySvrTraps

Description

Forwards Insight Manager Recovery Server SNMP traps.

WINOSSPI-InsightManager_FwdSANTraps

Description

Forwards Insight Manager Storage Area Network SNMP traps.

WINOSSPI-InsightManager_FwdSCSIDevicesTraps

Description

Forwards Insight Manager SCSI Devices SNMP traps.

WINOSSPI-InsightManager_FwdServerMgrTraps

Description

Forwards Insight Manager Server Manager SNMP traps.

WINOSSPI-InsightManager_FwdSTEAMTraps

Description

Forwards Insight Manager StorageWorks Enterprise Array Manager SNMP traps.

WINOSSPI-InsightManager_FwdStorageSysTraps

Description

Forwards Insight Manager Storage Systems SNMP traps.

WINOSSPI-InsightManager_FwdSvrHealthTraps

Description

Forwards Insight Manager Server Health SNMP traps.

WINOSSPI-InsightManager_FwdSWCCTraps

Description

Forwards Insight Manager StorageWorks Command Console SNMP traps.

WINOSSPI-InsightManager_FwdSysInfoTraps

Description

Forwards Insight Manager System Information SNMP traps.

WINOSSPI-InsightManager_FwdThresholdMgmtTraps

Description

Forwards Insight Manager Threshold Management SNMP traps.

WINOSSPI-InsightManager_FwdUPSTraps

Description

Forwards Insight Manager Uninterrupted Power Supply SNMP traps.

Insight Manager -> Diagnostic -> Storage Agents

WINOSSPI-InsightManager_StorageAgents

Description

Checks the Storage Agents service and its corresponding process.

Insight Manager -> Diagnostic -> Remote Insite Lights Out

WINOSSPI-InsightManager_FwdRIBTraps

Description

Forwards Insight Manager Remote Insight Board SNMP traps.

Insight Manager -> Diagnostic -> NIC Agents

WINOSSPI-InsightManager_NICAgents

Description

Checks the NIC Agents service and its corresponding process.

Insight Manager -> Diagnostic -> Server Agents

WINOSSPI-InsightManager_ServerAgents

Description

Checks the Server Agents service and its corresponding process.

Insight Manager -> Diagnostic -> Version Control Agents

WINOSSPI-InsightManager_VCAgent

Description

Checks the Version Control Agent service and its corresponding process.

HP Systems Insight Manager

HP Systems Insight Manager -> HPSIM Diagnostic

WINOSSPI-HPSIM_HPSIMServiceMonitoring

Description

Checks the HP Systems Insight Manager service and the corresponding processes.

WINOSSPI-HPSIM_OpenSSHdServiceMonitoring

Description

Checks the OpenSSHd service and the corresponding processes.

WINOSSPI-HPSIM_WMIMapperServiceMonitoring

Description

Checks the Pegasus WMI Mapper service and the corresponding processes.

Microsoft BackOffice Applications

The policy groups under Microsoft BackOffice applications are:

- **MS Certificate Server**
- **MS Index Server**
- **MS Message Queue Server**
- **MS Proxy Server 2.0**
- **MS SNA Server 4.0**
- **MS Systems Management Server 2.0**
- **MS Systems Management Server 2003**
- **MS Transaction Server 2.0**

MS Certificate Server

MS Certificate Server -> Diagnostic

WINOSSPI-MSCertSvr_FwdAllWarnError

Description

Forwards all event log entries with a severity level of Information.

MS Index Server

Index Server Win 2K,XP & 2K3 -> Index Server Diagnostic

WINOSSPI-MSIndexServer_FwdAllWarnError

Description

Forwards all event log entries with a severity level of Information.

WINOSSPI-MSIndexServer_Indexing Service_FilesToBeIndexed

Description

Indexing Service Files To Be Indexed

WINOSSPI-MSIndexServer_IndexingService_NumDocumentsIndexed

Description

Indexing Service Number of Documents Indexed

Index Server Windows NT 4.0 -> Index Server WinNT Diagnostic

WINOSSPI-MSIndexServer_FwdAllWarnError

Description

Forwards all event log entries with a severity level of Information.

WINOSSPI-MSIndexServer_ContentIndex_FilesToBeFiltered

Description

Checks Files to be filtered counter of the Content Index object.

WINOSSPI-MSIndexServer_ContentIndex_NumDocumentsFiltered

Description

Provides information about the # documents filtered counter of the Content Index object.

MS Message Queue Server

MS Message Queue Server -> Diagnostic

WINOSSPI-MSMQ_FwdAllWarnError

Description

Forwards all Application log entries with a severity level of Warning or Error.

WINOSSPI-MSMQ_JournalQueue

Description

Checks the Journal queue.

WINOSSPI-MSMQ_MSMQ

Description

Checks the MSMQ service and its corresponding process.

WINOSSPI-MSMQ_QueueSize

Description

Checks the Queue size.

MS Proxy Server 2.0

MS Proxy Server 2.0 -> Diagnostic

WINOSSPI-MSPS20_FwdAllWarnError

Description

Forwards all System event log entries with Warning or Critical severity.

WINOSSPI-MSPS20_FailingRequestsSec

Description

Checks the Failing Requests/sec counter of the Web Proxy Server Service object.

WINOSSPI-MSPS20_SrvProcMon_ProxyAlrtNotificationSvc

Description

Checks the Proxy Alert Notification Service and its corresponding process.

WINOSSPI-MSPS20_SrvProcMon_ServerAdministration

Description

Checks the Microsoft Proxy Server Administration service and its corresponding process.

WINOSSPI-MSPS20_SrvProcMon_WinSockProxySvc

Description

Checks the Microsoft WinSock Proxy Service and its corresponding process.

WINOSSPI-MSPS20_ThreadPoolFailures

Description

Checks the Thread Pool Failures counter of the Web Proxy Server Service object.

WINOSSPI-MSPS20_TotalDroppedFrames

Description

Checks the Total Dropped Frames counter of the Packet Filtering object.

WINOSSPI-MSPS20_TotalFailedSocksSessions

Description

Checks the Total Failed Socks Sessions counter of the Web Proxy Server Service object.

WINOSSPI-MSPS20_TotalFailingRequests

Description

Checks the Total Failing Requests counter of the Web Proxy Server Service object.

MS SNA Server 4.0

MS SNA Server 4.0 -> Diagnostic

WINOSSPI-SNA40_FwdAllWarnError

Description

Forwards all Application log entries with Warning or Error severity, and all other event log entries with the following source:

- SNA Server
- SNA Manage Agent
- SNA Base Service
- SNA Print Server

WINOSSPI-SNA40_SNABASE

Description

Checks the SNABASE service and its corresponding process.

MS Systems Management Server 2.0

MS Systems Management Server 2.0 -> Diagnostic

WINOSSPI-SMS20_FwdAllWarnError

Description

Forwards all Application log entries with Warning or Error severity and the following source:

- SMS Client
- SMS Provider
- SMS Server
- SMSPerf

WINOSSPI-SMS20_SMS_CLIENT_SERVICE

Description

Checks the SMS_CLIENT_SERVICE service and its corresponding process.

WINOSSPI-SMS20_SMS_EXECUTIVE

Description

Checks the SMS_EXECUTIVE service and its corresponding process.

WINOSSPI-SMS20_SMS_SITE_COMPONENT

Description

Checks the SMS_SITE_COMPONENT_MANAGER service and its corresponding process.

WINOSSPI-SMS20_SMS_SQL_MONITOR

Description

Checks the SMS_SQL_MONITOR service and its corresponding process.

MS Systems Management Server 2003

MS Systems Management Server 2003 -> Diagnostic

WINOSSPI-SMS2003_SMS_SITE_COMPONENT

Description

Checks the SMS_SITE_COMPONENT_MANAGER service and the corresponding process.

WINOSSPI-SMS2003_SMS_CLIENT_SERVICE

Description

Checks the SMS_CLIENT_SERVICE service and the corresponding process.

WINOSSPI-SMS2003_SMS_EXECUTIVE

Description

Checks the SMS_EXECUTIVE service and the corresponding process.

WINOSSPI-SMS2003_SMS_SQL_MONITOR

Description

Checks the SMS_SQL_MONITOR service and the corresponding process.

WINOSSPI-SMS2003_FwdClientWarnError

Description

Forwards SMS client application log entries with a severity status of Warning or Error.

WINOSSPI-SMS2003_FwdGenericWarnError

Description

Forwards SMS generic application log entries with a severity status of Warning or Error.

WINOSSPI-SMS2003_FwdServerWarnError

Description

Forwards SMS sever application log entries with a severity status of Warning or Error.

MS Transaction Server 2.0

MS Transaction Server 2.0 -> Diagnostic

WINOSSPI-MTS20_FwdAllApplWarnError

Description

Forwards all Application log entries with a severity level of Warning or Error.

WINOSSPI-MTS20_MSDTC

Description

Checks the MSDTC service and its corresponding process.

Microsoft Cluster Server

You can use the policies in the `MS Cluster Server` policy group to manage Microsoft Cluster servers. This policy group includes the `Cluster Server Diagnostic` policy group.

Cluster Server Diagnostic

WINOSSPI-MSCS-FwdWarnError

Description

Forwards the event log entries of the cluster server that have a severity of `Warning` or `Error` to the management server.

WINOSSPI-MSCS_FwdQuorumWarnError

Description

Forwards the quorum event log entries of the cluster server that have a severity of `Warning` or `Error` to the management server.

WINOSSPI-MSCS_ClusterMonitor

Description

Monitors the status of the WinOS SPI cluster executable process. If the process is not running on the managed node, the policy runs the process on the managed node.

Cluster Server Diagnostic → Cluster Group

WINOSSPI-MSCS_ResourceGroup

Description

Checks the state of resource groups in the cluster. You can set the following conditions for this policy:

- Resource group is offline
- Resource group is failed

- Resource group is online
- Creation of resource group in cluster
- Deletion of resource group in cluster

Cluster Server Diagnostic → Cluster Network

WINOSSPI-MSCS_Network

Description

Checks the state of networks in the cluster. You can set the following conditions for this policy:

- Network in cluster is down
- Network in cluster is partitioned
- Network is up

WINOSSPI-MSCS_NetworkWarnError

Description

Forwards all event log entries of the cluster network that have a severity of `Warning` or `Error` to the management server.

WINOSSPI-MSCS_NetworkInterface

Description

Checks the state of network interfaces in the cluster. You can set the following conditions for this policy:

- Network interface is disabled
- Network interface is normal

Cluster Server Diagnostic → Cluster Node

WINOSSPI-MSCS_NodeWarnError

Description

Forwards all event log entries of the cluster node that have a severity of `Warning` or `Error` to the management server.

Cluster Server Diagnostic

WINOSSPI-MSCS_NodeState

Description

Checks the state of the cluster nodes. You can set the following conditions for this policy:

- Node is paused
- Node is down
- Node is up

Cluster Server Diagnostic → **Cluster Service**

WINOSSPI-MSCS_ClusterService

Description

Checks the `Cluster Server` service and the corresponding process associated with the service.

Microsoft Windows Core

MS Active Directory Server

MS Active Directory Server -> ADS Additional

AD Connector

WINOSSPI-ADS_ActiveAuthKerberos

Description

Checks the NTDS\Kerberos Authentications counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

WINOSSPI-ADS_ActiveAuthLogon

Description

Checks the Server\Logon/sec counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

WINOSSPI-ADS_ActiveAuthNTLM

Description

Checks the NTDS\NTLM Authentications counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

WINOSSPI-ADS_ADCFwdAllWarnErrorMSADC

Description

Monitors the Application log for entries from MSADC that have a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

Functions only with the integration of Exchange. Without Exchange, the `adc` process, which the policy observes, does not exist.

WINOSSPI-ADS_ADCImportFailures

Description

Checks the `PerfLib` counter `MSADC\Rate` of Import Failures for the number of imports that have failed. If the number is 1 or 2, the policy sends a warning message to the active message browser. If the number is 3 or higher, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process `adc`, which the policy observes, does not exist.

WINOSSPI-ADS_ADCPageFaults

Description

Checks the `PerfLib` counter `Process\Page Faults\adc` for the number of page faults for a process. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. A consistently high rate of page faults for a process usually indicates that its working set is not large enough to support the process efficiently. If the system does not have enough available memory to enlarge the working set, it cannot lower the page fault rate.

This policy functions only with the integration of Exchange. Without Exchange, the process `adc`, which the policy observes, does not exist.

WINOSSPI-ADS_ADCPrivateBytes

Description

Checks the `PerfLib` counter `Process\Private Bytes\adc` for the number of bytes allocated exclusively to the ADC process (that is, bytes that cannot be shared with other processes). If the number exceeds 250, the policy sends a

warning message to the active message browser. If the number exceeds 300, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process `adc`, which the policy observes, does not exist.

WINOSSPI-ADS_ADCProcessorTime

Description

Checks the PerfLib counter `Process\Processor Time\adc` for the percentage of processor time Active Directory ADC is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the Active Directory server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

This policy functions only with the integration of Exchange. Without Exchange, the process `adc`, which the policy observes, does not exist.

WINOSSPI-ADS_ADCWorkingSet

Description

Checks the PerfLib counter `Process\Working Set\adc` for the current number of bytes in the working set of the ADC process. If the number exceeds 15,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 bytes, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process `adc`, which the policy observes, does not exist.

AD Domain and OU Structure

WINOSSPI-ADS_DomainChanges

Description

Approximately every 20 minutes, checks for changes to the domain structure.

- Name Space
 Root\Directory\LDAP

- Event Class
 __InstanceOperationEvent
- WQL Filter
 TargetInstance ISA "ds_dnsdomain"

Successful changes in the domain structure affect the size and replication of the Active Directory database.

This policy may be deployed only on a domain controller.

WINOSSPI-ADS_OUChanges

Description

Checks, approximately every 20 minutes, for changes to the OU structure.

- Name Space
 Root\Directory\LDAP
- Event Class
 __InstanceOperationEvent
- WQL Filter
 TargetInstance ISA ds_organizationalunit

Successful changes in the OU structure affect the size and replication of the Active Directory database.

This policy may be deployed only on a domain controller.

AD Global Catalog Access

WINOSSPI-ADS_GlobalCatalogReads

Description

Checks the NTDS\DS Directory Reads/sec counter, approximately every 30 minutes, for the number of reads from the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed.

This policy may be deployed only to the Global Catalog server.

WINOSSPI-ADS_GlobalCatalogSearches

Description

Checks the NTDS\DS Directory Searches/sec counter, approximately every 30 minutes, for the number of searches of the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed.

This policy may be deployed only to the Global Catalog server.

WINOSSPI-ADS_GlobalCatalogWrites

Description

Checks the counter NTDS\DS Directory Writes/sec counter, approximately every 30 minutes, for the number of writes to the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed.

This policy may be deployed only to the Global Catalog server.

AD Health Monitors -> Additional

WINOSSPI-ADS_HMNTFRSPageFaults

Description

Checks the PerfLib counter Process\Page Faults/sec\NTFRS for the number of times a thread requested access to a memory page that was not in memory and therefore had to be read from disk. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the value obtained from this counter consistently generates messages, physical memory is low.

WINOSSPI-ADS_HMNTFRSPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\NTFRS for the number of bytes allocated exclusively to the LSASS process (that is, bytes that cannot be shared with other processes). If the number exceeds 15,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 bytes, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

WINOSSPI-ADS_HMNTFRSProcessorTime

Description

Checks the PerfLib counter Process\% Processor Time\NTFRS for the percentage of processor time the ADS LSASS process is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

WINOSSPI-ADS_HMNTFRSWorkingSet

Description

Checks the PerfLib counter Process\Working Set\NTFRS for the number of memory pages recently touched by threads in the process. If the number exceeds 15,000,000 pages, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 pages, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

WINOSSPI-ADS_NTFRS

Description

Checks whether the File Replication Service and its corresponding process, ntfrs.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

WINOSSPI-ADS_NtLmSsp

Description

Checks whether the NT LM Security Support Service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

WINOSSPI-ADS_SyncSchemaMissMatch

Description

Checks the PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch for the number of synchronization failures. If the number exceeds 1, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or require further replication tuning to optimize performance.

AD Replication

WINOSSPI-ADS_ADSRepInBoundBytesBetweenSites

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec for the number of bytes per second between sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

WINOSSPI-ADS_ADSRepInBoundBytesWithinSites

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec for the number of bytes per second within sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the

upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

WINOSSPI-ADS_ADSRepInBoundObjectUpdatesRemaining

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\DRA Inbound Object Updates Remaining in Packet for the number of objects remaining. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

WINOSSPI-ADS_ADSRepNotifyQueueSize

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\DS Notify Queue Size for the number of jobs in the queue. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

WINOSSPI-ADS_ADSPendingSynchronizations

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\DRA Pending Replication Synchronizations for the number of synchronizations pending. If the number exceeds 50, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

AD Replication Activity

WINOSSPI-ADS_ReplicationActivities

Description

Monitors the Directory Service log for replication events.

The granularity of the raised events depends on the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\  
Diagnostics\5 Replication Events
```

Set this value to **3** to get the following four directory replication events logged in the Directory Services log:

- 1487 – Internal event: The Directory Service has been asked to begin inbound replication
- 1488 – The Directory Service completed the sync request
- 1489 – Internal event: The Directory Service has been asked for outbound changes
- 1490 – Internal event: The Directory Service finished gathering outbound changes

AD Security -> Additional

WINOSSPI-ADS_DirUserCreationDeletion

Description

Checks, approximately every 15 minutes, whether any accounts in Directory User Accounts have been created or deleted. If so, the policy sends a message to the active message browser.

WINOSSPI-ADS_DirUserModif

Description

Checks, approximately every 15 minutes, whether any accounts in Directory User Accounts have been modified. If so, the policy sends a message to the active message browser.

WINOSSPI-ADS_KDCFailureGrantTicket

Description

Monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 676 in the Security Event Log:

```
676 Authentication Ticket Request Failed
```

This policy may be deployed only to servers running KDC.

WINOSSPI-ADS_PrivilegedObjects

Description

Forwards privileged object access events from the Security Event Log

WINOSSPI-ADS_SecErrAccessPermissions

Description

Checks, approximately every five minutes, the PerfMon counter Server\Errors Access Permissions for the number of attempts to access ADS elements that were denied. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. This counter warns of unauthorized access attempts that randomly seek inadequately protected files.

WINOSSPI-ADS_SecErrGrantedAccess

Description

Checks, approximately every five minutes, the PerfMon counter Server\Errors Granted Access for the number of access attempts that opened files successfully but were allowed no further access. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number is greater than 4, the policy sends an error message. This counter warns of attempts to access files without proper authorization.

MS Active Directory Server -> ADS Diagnostic

AD Health Monitors -> Diagnostics

WINOSSPI-ADS_SMTPEventLogs

Description

Monitors the System log for SMTP-specific events. Forwards them as messages to the active message browser.

WINOSSPI-ADS_DNSServ_FwdAllWarnError

Description

Monitors the DNS Server log for entries with a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

WINOSSPI-ADS_FwdAllWarnErrorDS

Description

Forwards all event log entries with a severity level of Warning or Error.

WINOSSPI-ADS_FwdAllWarnErrorFRS

Description

Forwards all event log entries with a severity level of Warning or Error.

WINOSSPI-ADS_HMLSASSPageFaults

Description

Checks the PerfLib counter Process\Page Faults/sec\lsass for the number of times a thread requested access to a memory page that was not in memory and therefore had to be read from disk. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the value obtained from this counter consistently generates messages, physical memory is low.

WINOSSPI-ADS_HMLSASSPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\lsass for the number of bytes allocated exclusively to the LSASS process (that is, bytes that cannot be shared with other processes). If the number exceeds 35,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 40,000,000 bytes, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

WINOSSPI-ADS_HMLSASSProcessorTime

Description

Checks the PerfLib counter Process\% Processor Time\lsass for the percentage of processor time the ADS LSASS process is consuming. If the value exceeds 60%, the policy sends a warning message to the active browser. If the value exceeds 70%, the policy sends an error message. If the

value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

WINOSSPI-ADS_HMLSASSWorkingSet

Description

Checks the PerfLib counter Process\Working Set\lsass for the number of memory pages recently touched by threads in the process. If the number exceeds 15,000,000 pages, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 pages, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

WINOSSPI-ADS_HMThreadsInUse

Description

Checks the PerfLib counter NTDS\DS Threads in Use for the number of threads in use by the directory service. (This number is different from the number of threads in use by the directory service process.) If the number exceeds 20, the policy sends a warning message to the active message browser. If the number exceeds 25, the policy sends an error message. These threads serve client API calls, and indicate whether additional processors should be used.

WINOSSPI-ADS_KDC

Description

Checks whether the Kerberos Key Distribution Center Service and its corresponding process lsass.exe are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

WINOSSPI-ADS_NetLogon

Description

Checks whether the Net Logon service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service

using an operator-initiated command. When the service is running again, the policy acknowledges the message.

WINOSSPI-ADS_PolicyAgent

Description

Checks whether the PolicyAgent service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser.

WINOSSPI-ADS_SamSs

Description

Checks whether the Security Accounts Manager service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

WINOSSPI-ADS_ADCFwdAllWarnErrorMSADC

Description

Monitors the Application log for entries from MSADC that have a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

Functions only with the integration of Exchange. Without Exchange, the `adc` process, which the policy observes, does not exist.

AD Index and Query Monitors

WINOSSPI-ADS_IQLDAPActiveThreads

Description

Checks the PerfLib counter NTDS\LDAP Active Threads for the number of LDAP Active Threads. If the number exceeds 40, the policy sends a warning message to the active message browser. If the number exceeds 50, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

WINOSSPI-ADS_IQLDAPBindTime

Description

Checks the PerfLib counter NTDS\LDAP Bind Time for the number of LDAP Client Sessions. If the number exceeds 100, the policy sends a warning message to the active message browser. If the number exceeds 200, the policy sends an error message. If the LDAP Bind Time exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

WINOSSPI-ADS_IQLDAPClientSessions

Description

Checks the PerfLib counter NTDS\LDAP Client Sessions for the number of LDAP Client Sessions. If the number exceeds 4,000 sessions, the policy sends a warning message to the active message browser. If the number exceeds 4,500 sessions, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

WINOSSPI-ADS_IQKerberos Authentication

Description

Checks the PerfLib counter Kerberos Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

WINOSSPI-ADS_IQNTLM Authentication

Description

Checks the PerfLib counter NTDS Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

AD Site Structure

WINOSSPI-ADS_SiteChanges

Description

Monitors the Active Directory Site to ensure that IP subnets are not being added, changed, or deleted unnecessarily:

- Name Space

`Root\Directory\LDAP`

- Event Class

`__InstanceOperationEvent`

- WQL Filter

`TargetInstance ISA "ds_site"`

Successful changes in the OU structure affect the size and replication of the Active Directory database.

This policy may be deployed only to one node within the forest. The additional script must be executed for all sites within this domain on this node (or deployed to several nodes and execute additional scripts on these nodes).

AD Security -> Diagnostic

WINOSSPI-ADS_SecAdminGroupChange

Description

Checks, approximately every 15 minutes, the following security groups for changes:

- Domain Admins
- Enterprise Admins

If there have been any changes, the policy sends a message to the active message browser with a severity level of Information.

WINOSSPI-ADS_SecErrorsLogon

Description

Checks, approximately every five minutes, the PerfMon counter Server\Errors Logon for the number of denied logon attempts to the server. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number is greater than 4, the policy sends an error message. This counter warns of attempts to log on with a password-guessing program.

WINOSSPI-ADS_SecNonTransMembEval

Description

Checks, approximately every five minutes, the PerfMon counter Server\SAM Non-Transitive Membership Evaluation/sec for the number of SAM non-transitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, the domain may be overloaded.

WINOSSPI-ADS_SecSDPropagatorQueue

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\DS Security Descriptor Propagator Runtime Queue for the number of objects remaining to be examined while processing the current directory service

security descriptor propagator event. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the higher threshold is exceeded, the domain controller may be overloaded.

WINOSSPI-ADS_SecTransMembEval

Description

Checks, approximately every five minutes, the PerfMon counter NTDS\SAM Transitive Membership Evaluations for the number of SAM transitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

MS Terminal Server

Terminal Server Win 2K,XP & 2K3 ->Terminal Server Additional

WINOSSPI-WTS_TerminalServiceSession_PctProcessorTime-Win2k

Description

Checks the % Processor Time counter of the Terminal Service Session object.

WINOSSPI-WTS_TerminalServiceSession_TotalErrors-Win2k

Description

Checks the Total Errors counter of the Terminal Service Session object.

WINOSSPI-WTS_TerminalServiceSession_TotalFrames-Win2k

Description

Checks the Total Frames counter of the Terminal Service Session object.

WINOSSPI-WTS_TerminalServiceSession_ActiveSessions-Win2k

Description

Checks the Active Sessions counter of the Terminal Services object.

Terminal Server Win 2K,XP & 2K3 -> Terminal Server Diagnostic

WINOSSPI-WTS_FwdAllSysWarnError

Description

Forwards all system log entries with a source of Term service or Term Serv Licensing and a severity level of warning or error.

WINOSSPI-WTS_TermServLicensing Service

Description

Checks the 'TermServLicensing' Service.

WINOSSPI-WTS_TermService

Checks the 'TermService' Service.

Terminal Server Windows NT -> Terminal Server WinNT Additional

WINOSSPI-WTS_System_PctProcessorTime-NT4

Description

Checks the % Processor Time counter of the System object.

WINOSSPI-WTS_User_PctProcessorTime-NT4

Description

Checks the % Processor Time counter of the User object.

WINOSSPI-WTS_System_TotalFrames-NT4

Description

Checks the Total Frames counter of the System object.

WINOSSPI-WTS_System_TotalErrors-NT4

Description

Checks the Total Errors counter of the System object.

Terminal Server Windows NT -> Terminal Server WinNT Diagnostic

WINOSSPI-WTS_FwdAllSysWarnError

Description

Forwards all system log entries with a source of Term service or Term Serv Licensing and a severity level of warning or error.

WINOSSPI-WTS_TermServLicensing Service

Description

Checks the 'TermServLicensing' Service.

WINOSSPI-WTS_TermService

Description

Checks the 'Term Service' Service.

Network Infrastructure

DHCP-> DHCP Client -> Diagnostic

WINOSSP-DHCPCL_DHCPClient

Description

Checks the DHCP Client Service.

DHCP-> DHCP Server -> Diagnostic

WינוSSP-DHCPsvr_MSDhcp Server

Description

Checks the Microsoft DHCP Server Service

DHCP -> Relay Agent -> Diagnostic

WינוSSPI-DHCP Relay_DHCP Relay Agent

Description

Checks the DHCP Relay Agent Service

DNS-> DNS Server -> Diagnostic

WינוSSPI-DNS_MSDnsServer

Description

Checks the Microsoft DNS Server Service.

RAS -> Additional

WינוSSPI-RAS_RASConnectionMgr

Description

Checks the Remote Access Connection Manager Service.

WינוSSPI-RAS_RASServer

Checks the Remote Access Server Service.

RAS -> Diagnostic

Description

WינוSSPI-RAS_RASAutodialManager

Checks the Remote Access Autodial Manager Service.

WINS -> WINS Server -> Diagnostic

WINOSSPI-WINS_WinInternetNameSvc

Description

Checks the Windows Internet Name Service.

Operating System

MS Windows 2K, XP & 2K3 -> MS Windows Diagnostic

WINOSSPI-SysMon_AvgDiskSecTransfer

Description

Checks the Average Disk sec/Transfer counter of the Logical Disk object.

WINOSSPI-SysMon_CacheFaultSec

Description

Checks the Cache faults/sec counter of the Memory object.

WINOSSPI-SysMon_Cache_DataMapSec

Description

Checks the Data Maps/Sec counter of the Cache Object

WINOSSPI-SysMon_Cache_MDLReadsSec

Description

Checks the MDL Reads/Sec counter of the Cache Object.

WINOSSPI-Cache_PinReadHitsPct

Description

Checks the Pin Read Hits % counter of the cache object.

WINOSSPI-Cache_ReadAheadsSec

Description

Checks the Read Aheads/sec counter of the cache object.

WINOSSPI-Net_Bytes TotalSec

Description

Checks the Bytes Total/sec counter of the Server object.

WINOSSPI-Net_CurrentCommands

Description

Checks the Current Commands counter of the Redirector object

WINOSSPI-Net_NetworkErrorsSec

Description

Checks the Network Errors/sec counter of the Redirector object.

WINOSSPI-Net_ReadsDeniedSec

Description

Checks the Reads Denied/sec counter of the Redirector object.

WINOSSPI-SysMon_Memory_PageInputSec

Description

Checks the Pages Input/sec counter of the Memory Object.

WINOSSPI-SysMon_Memory_PagesSec

Description

Checks the pages/sec counter of the Memory Object.

WINOSSPI-SysMon_PagefaultsSec

Description

Checks the Page Faults/sec counter of the Memory Object.

WINOSSPI-SysMon_PageFileSec

Description

Checks the % Usage counter of the Paging File object.

WINOSSPI-SysMon_PageReadsSec

Description

Checks the Page Reads/sec counter of the Memory object.

WINOSSPI-SysMon_PhysicalMemCheck

Description

Checks the Available Bytes counter of the Memory object.

WINOSSPI-SysMon_Redirector_WritesDeniedSec

Description

Checks the Writes Denied/sec counter of the Redirector object.

WINOSSPI-SysMon_Server_PoolNonpagedFailures

Description

Checks the Pool Nonpaged Failures counter of the Server object.

WINOSSPI-SysMon_Server_PoolPagedFailures

Description

Checks the Pool Paged Failures counter of the Server object.

WINOSSPI-SysMon_WorkitemShortages

Description

Checks the Work Item Storages counter of the Server object.

WINOSSPI-SysMon_ProcessorQueueLength

Description

Checks the Processor Queue Length counter of the System object.

WINOSSPI-SysMon_VirtualMemCheck

Description

Checks the % Committed Bytes in Use counter of the Memory object.

WINOSSPI-SysMon_CpuSpikeCheck-Win2k_PrivilegedTime

Description

Checks CPU concerning counter of object 'Processor' for Privileged Time Usage.

WINOSSPI-SysMon_CpuSpikeCheck-Win2k_ProcessorTime

Description

Checks CPU concerning counter of object 'Processor' for Processor Time Usage.

WINOSSPI-SysMon_CpuSpikeCheck-Win2k_UserTime

Description

Checks CPU concerning counter of object 'Processor' for User Time Usage.

WINOSSPI-SysMon_DiskBusyCheck_AvgDiskQueue

Description

Checks Average Disk Queue counter of object 'Logical Disk'.

WINOSSPI-SysMon_DiskBusyCheck_DiskTime

Description

Checks Disk Time counter of object 'Logical Disk'.

WINOSSPI-SysMon_DiskFullCheck_FreeMB

Description

Checks Free Megabytes counter of object 'Logical Disk'

WINOSSPI-SysMon_DiskFullCheck_PercentageFreeSpace

Description

Checks '% Free Space' counter of object 'Logical Disk'

WINOSSPI_EventLog Service

Description

Checks the Windows Event Log Service.

WינוSSPI_PlugnPlay Service

Description

Checks the plug and play service.

WינוSSPI_RPCService

Description

Checks the Remote Procedure Call (RPC) Service

WינוSSPI_Spooler Service

Description

Checks the Spooler service.

WינוSSPI-SCM_Sysinfo

Description

Checks the system event log for messages from the Service Control Manager.

WינוSSPI-NetLogon_SysInfo

Description

Checks the system event log for messages related to Netlogon.

MS Windows 2K, XP & 2K3 → MS Windows Additional

WינוSSPI-LogOn_SecInfo

Description

Checks the security event log for logon messages.

WינוSSPI-Logon_ApplInfo

Description

Checks the application event log for Windows logon user profile messages.

WינוSSPI-NetworkConfig_ApplInfo

Description

Checks the application event log for messages from the network control panel.

WינוSSPI-Process_SecInfo

Description

Checks the security event log for processes related messages.

WינוSSPI-SecEvLog_Operations

Description

Checks the security event log for operations to itself.

MS Windows NT 4.0 -> Diagnostic

WינוSSPI-SysMon_AvgDiskSecTransfer

Description

Checks the Average Disk sec/Transfer counter of the Logical Disk object.

WינוSSPI-SysMon_CacheFaultSec

Description

Checks the Cache Faults/Sec counter of the Memory Object.

WינוSSPI-SysMon_Cache_DataMapSec

Description

Checks the Data Maps/sec counter of the cache object

WינוSSPI-SysMon_Cache_MDLReadsSec

Description

Checks the MDL Reads/sec counter of the Cache object

WינוSSPI-Cache_PinReadHitsPct

Description

Checks the Pin Read Hits% counter of the Cache object.

WINOSSPI-Cache_ReadAheadsSec

Description

Checks the Read Aheads/sec counter of the Cache object.

WINOSSPI-Net_Bytes TotalSec

Description

Checks the Bytes Total/sec counter of the Server object.

WINOSSPI-Net_CurrentCommands

Description

Checks the Current Commands counter of the Redirector object.

WINOSSPI-Net_NetworkErrorsSec

Description

Checks the Network Errors/sec counter of the Redirector object.

WINOSSPI-Net_ReadsDeniedSec

Description

Checks the Reads Denied/sec counter of the Redirector object.

WINOSSPI-SysMon_Memory_PageInputSec

Description

Checks the Pages Input/sec counter of the Memory Object.

WINOSSPI-SysMon_Memory_PagesSec

Description

Checks the Pages/sec counter of the Memory Object.

WINOSSPI-SysMon_PagefaultsSec

Description

Checks the Page Faults/sec counter of the Memory Object.

WINOSSPI-SysMon_PageFileSec

Description

Checks the % Usage counter of the Paging File object.

WINOSSPI-SysMon_PageReadsSec

Description

Checks the Page Reads/sec counter of the Memory object.

WINOSSPI-SysMon_PhysicalMemCheck

Description

Checks the AvailableBytes counter of the Memory object.

WINOSSPI-SysMon_Redirector_WritesDeniedSec

Description

Checks the Writes Denied/sec counter of the Redirector object.

WINOSSPI-SysMon_Server_PoolNonpagedFailures

Description

Checks the Pool Non paged Failures counter of the Server object.

WINOSSPI-SysMon_Server_PoolPagedFailures

Description

Checks the Pool Paged Failures counter of the Server object.

WINOSSPI-SysMon_WorkitemShortages

Description

Checks the Work Item Storages counter of the Server object.

WINOSSPI-SysMon_ProcessorQueueLength

Description

Checks the Processor Queue Length counter of the System object.

WINOSSPI-SysMon_VirtualMemCheck

Description

Checks the % Committed Bytes in Use counter of the Memory object.

WINOSSPI-SysMon_CpuSpikeCheck-WinNT_PrivilegedTime

Description

Checks CPU concerning counter of object 'Processor' for Privileged Time Usage.

WINOSSPI-SysMon_CpuSpikeCheck-WinNT_ProcessorTime

Description

Checks CPU concerning counter of object 'Processor' for Processor Time Usage.

WINOSSPI-SysMon_CpuSpikeCheck-WinNT_UserTime

Description

Checks CPU concerning counter of object 'Processor' for User Time Usage.

WINOSSPI-SysMon_DiskBusyCheck_AvgDiskQueue

Description

Checks Average Disk Queue counter of object 'Logical Disk'.

WINOSSPI-SysMon_DiskBusyCheck_DiskTime

Description

Checks Disk Time counter of object 'Logical Disk'.

WINOSSPI-SysMon_DiskFullCheck_FreeMB

Description

Checks Free Megabytes counter of object 'Logical Disk'

WINOSSPI-SysMon_DiskFullCheck_PercentageFreeSpace

Description

Checks '% Free Space' counter of object 'Logical Disk'

WינוSSPI_EventLog Service

Description

Checks the Windows Event Log Service.

WינוSSPI_PlugnPlay Service

Description

Checks the plug and play service.

WינוSSPI_RPCService

Description

Checks the Remote Procedure Call (RPC) Service

WינוSSPI_Spooler Service

Description

Checks the Spooler service.

WינוSSPI-SCM_Sysinfo

Description

Checks the system event log for messages from the Service Control Manager.

WינוSSPI-NetLogon_SysInfo

Description

Checks the system event log for messages related to Netlogon.

MS Windows NT 4.0 -> Additional

WינוSSPI-LogOn_SecInfo

Description

Checks the security event log for logon messages.

WינוSSPI-Logon_ApplInfo

Description

Checks the application event log for Windows logon user profile messages.

WINOSSPI-NetworkConfig_AplInfo

Description

Checks the application event log for messages from the network control panel.

WINOSSPI-Process_SecInfo

Description

Checks the security event log for processes related messages.

WINOSSPI-SecEvLog_Operations

Description

Checks the security event log for operations to itself.

Web Servers

WINOSSPI-IIS40_IISGbl_CachedFileHandl

Description

Checks the Cached File Handles counter of the Internet Information Services Global object.

WINOSSPI-IIS40_InernetInformationServicesGbl_CachedHitsPct

Description

Checks the Cache Hits % counter of the Internet Information Services Global object.

WINOSSPI-IIS40_IISGbl_DirectoryList

Description

Checks the Directory Listings counter of the Internet Information Services Global object.

WINOSSPI-IIS40_InernetInformationServicesGbl_Objects

Description

Checks the Objects counter of the Internet Information Services Global object.

WINOSSPI-IIS40_Process_PageFaultsSec_inetinfo

Description

Checks `inetinfo` instance of the Page Faults/sec counter of the Process object.

WINOSSPI-IIS40_Process_PctProcessorTime_inetinfo

Description

Checks the `inetinfo` instance of the % Processor Time counter of the Process object.

WINOSSPI-IIS40_Process_PrivateBytes_inetinfo

Description

Checks the `inetinfo` instance of the Private Bytes counter of the Process object.

WINOSSPI-IIS40_Process_ThreadCount_inetinfo

Description

Checks the `inetinfo` instance of the Thread Count counter of the Process object

WINOSSPI-IIS40_Process_WorkingSet_inetinfo

Description

Checks the `inetinfo` instance of the Working Set counter of the Process object.

WINOSSPI-IIS40_Server_BytesTransmittedSec

Description

Checks the Bytes Transmitted/sec counter of the Server object.

WINOSSPI-IIS40_WebServices_CurrentAnonymousUsers

Description

Checks the Current Anonymous Users counter of the Web Services object.

MS IIS 4.0 → Diagnostic

WINOSSPI-IIS40_FtpServerFwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from MSFTPSVC. Forwards these as messages to the active message browser.

WINOSSPI-IIS40_FwdAllApplicationWarnError

Description

Monitors the application log for entries with the severity Warning or Error from IISADMIN or W3SVC. Forwards these as messages to the active message browser.

WINOSSPI-IIS40_FwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from IISADMIN or W3SVC. Forwards these as messages to the active message browser.

WINOSSPI-IIS40_IndexServerFwdAllApplicationWarnError

Description

Monitors the application log for entries with the severity Warning or Error from the Content Index Service (CISVC). Forwards these as messages to the active message browser.

WINOSSPI-IIS40_NntpServerFwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from the NNTP Service (NNTPSVC). Forwards these as messages to the active message browser.

WINOSSPI-IIS40_SmtpServerFwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from the SMTP Service (SMTPSVC). Forwards these as messages to the active message browser.

WINOSSPI-IIS40_SrvProcMon_CISVC

Description

Checks every five minutes whether the service CISVC and the corresponding process cisvc.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The

operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS40_SrvProcMon_IISADMIN

Description

Checks every five minutes whether the service IISADMIN and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS40_SrvProcMon_MSFTPSVC

Description

Checks every five minutes whether the service MSFTPSVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS40_SrvProcMon_NNTPSVC

Description

Checks every five minutes whether the service NNTPSVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS40_SrvProcMon_SMTPSVC

Description

Checks every five minutes whether the service SMTPSVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS40_SrvProcMon_W3SVC

Description

Checks every five minutes whether the service W3SVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the service's status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

MS IIS 4.0 Active Server Pages

ASP Error

WINOSSPI-IIS40_ASPErrorSec

Description

Checks every five minutes for the number of errors per second from Active Server Pages. Sends a critical message to the active message browser if the value is two or more, three times in a row. Sends a warning message if the value is one or more, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPScriptErrors

Description

Checks every five minutes for the number of ASP requests that failed because of a runtime error. Sends a critical message to the active message browser if the value is 40 or more, 16 times in a row. Sends a warning message if the value is between 15 and 40, 16 times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser

WINOSSPI-IIS40_ASPPreprocessorErrors

Description

Checks every five minutes for the number of ASP requests that failed because of a preprocessor error. Sends a critical message to the active message browser if the value is 40 or more, three times in a row. Sends a warning message if the value is between 15 and 40, three times in a row.

When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPScriptCompilerErrors

Description

Checks every five minutes for the number of ASP requests that failed because of an error during compilation. Sends a critical message to the active message browser if the value is 40 or more, three times in a row. Sends a warning message if the value is between 15 and 40, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser

ASP Memory Allocation

WINOSSPI-IIS40_ActiveServerPages_MemoryAllocated

Description

Checks the Memory Allocated counter of the Active Server Pages object.

WINOSSPI-IIS40_ASPScriptEnginesCached

Description

Checks every five minutes for the number of ASP script engines in the cache. Sends a critical message to the active message browser if the value is 40 or more, four times in a row. Sends a warning message if the value is between 15 and 40, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Requests

WINOSSPI-IIS40_ASPRequestBytesInTotal

Description

Checks every five minutes for the total size of all ASP requests, in bytes. Sends a critical message to the active message browser if the value is 20 million or more, four times in a row. Sends a warning message if the value is between 5000 and 20 million, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestBytesOutTotal

Description

Checks every five minutes for the total size in bytes of ASP responses sent, excluding the HTTP response headers. Sends a critical message to the active message browser if the value is 20 million or more, four times in a row. Sends a warning message if the value is between 5000 and 20 million, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestExecutionTime

Description

Checks every five minutes for the time in milliseconds that it took the last ASP request to execute. Sends a critical message to the active message browser if the value is 15000 or more, four times in a row. Sends a warning message if the value is between 5000 and 15000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestWaitTime

Description

Checks every five minutes for the time in milliseconds that the latest ASP request waited in the queue. Sends a critical message to the active message browser if the value is 15000 or more, three times in a row. Sends a warning message if the value is between 5000 and 15000, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsDisconnected

Description

Checks every five minutes for the number of ASP requests that were disconnected because of a communication failure. Sends a critical message to the active message browser if the value is 100 or more, four times in a row. Sends a warning message if the value is between 50 and 100, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsExecuting

Description

Checks every five minutes for the number of currently executing ASP requests. Sends a critical message to the active message browser if the value is more than 100, twice in a row. Sends a warning message if the value is between 50 and 100, twice in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsFailedTotal

Description

Checks every five minutes for the number of ASP requests that failed because of rejections, insufficient access rights, or errors. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsNotAuthorized

Description

Checks every five minutes for the number of ASP requests that failed because of insufficient access rights. Sends a critical message to the active message browser if the value is 1000 or more, three times in a row. Sends a warning message if the value is between 500 and 1000, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsNotFound

Description

Checks every five minutes for the number of ASP requests for files that could not be found. Sends a critical message to the active message browser if the value is 200 or more, three times in a row. Sends a warning message if the value is between 100 and 200, three times in row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsQueued

Description

Checks every five minutes for the number of ASP requests that are waiting in the queue. Sends a critical message to the active message browser if the value is 200 or more, three times in a row. Sends a warning message if the value is between 100 and 200, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsRejected

Description

Checks every five minutes for the number of ASP requests that were rejected due to insufficient resources. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser

WINOSSPI-IIS40_ASPRequestsSec

Description

Checks every five minutes for the number of ASP requests carried out per second. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsSucceeded

Description

Checks every five minutes for the number of ASP requests carried out successfully. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsTimedOut**Description**

Checks every five minutes for the number of ASP requests that timed out. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPRequestsTotal**Description**

Checks every five minutes for the total number of ASP requests that occurred since the service was last started. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Sessions**WINOSSPI-IIS40_AspSessionDuration****Description**

Checks every five minutes how long the most recent ASP session lasted in milliseconds. Sends a critical message to the active message browser if the value is more than 100000, four times in a row. Sends a warning message if the value is between 50000 and 100000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_AspSessionsCurrent**Description**

Checks every five minutes for the number of ASP sessions currently being serviced. Sends a critical message to the active message browser if the value is 250 or more, three times in a row. Sends a warning message if the value is between 200 and 250, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_AspSessionsTimedOut

Description

Checks every five minutes for the number of ASP sessions that timed out. Sends a critical message to the active message browser if the value is 100 or more, three times in a row. Sends a warning message if the value is between 50 and 100, three times in a row. When the value falls below the threshold again, sends the message to the active message browser.

WINOSSPI-IIS40_AspSessionsTotal

Description

Checks every five minutes for the total number of ASP sessions since the service was last started. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Policies

WINOSSPI-IIS40_ASPTemplateCacheHitRate

Description

Checks every five minutes for the percentage of ASP requests that could be met from the policy cache. Sends a critical message to the active message browser if this is 80% of requests or less. Sends a warning message if this is between 80% and 90% of requests. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASPTemplateNotifications

Description

Checks every five minutes for the number of policies in the cache that need to be updated. Sends a critical message to the active message browser if the value is 1000 or more, three times in a row. Sends a warning message if the value is between 500 and 1000, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Transactions

WINOSSPI-IIS40_ASP TransactionsAborted

Description

Checks every five minutes for the number of aborted ASP transactions. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASP TransactionsCommitted

Description

Checks every five minutes for the number of committed ASP transactions. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASP TransactionsPending

Description

Checks every five minutes for the number of ASP transactions currently in progress. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASP TransactionsSec

Description

Checks every five minutes for the number of ASP transactions started per second. Sends a critical message to the active message browser if the value is more than 100, four times in a row. Sends a warning message if the value is between 50 and 100, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_ASP TransactionsTotal

Description

Checks every five minutes for the total number of ASP transactions that occurred since the service was last started. Sends a critical message to the active message browser if the value is 10000 or more, four times in a row. Sends a warning message if the value is between 5000 and 10000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 4.0 FTP Server Health

WINOSSPI-IIS40_FtpBytesTotalSec

Description

Checks every five minutes for the number of bytes per second sent and received by the FTP service. Sends a critical message to the active message browser if the value is 64000 or more, four times in a row. Sends a warning message if the value is between 48000 and 64000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_FtpCurrentAnonymousUsers

Description

Checks every five minutes for the number of anonymous connections that are open to the FTP service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_FtpCurrentConnections

Description

Checks every five minutes for the total number of connections that are open to the FTP service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below

the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_FtpCurrentNonAnonymousUsers

Description

Checks every five minutes for the number of non-anonymous connections that are open to the FTP service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_FtpTotalFilesTransferred

Description

Checks every five minutes for the total number of files that the FTP service transferred since it was last started. Sends a critical message to the active message browser if the value is 640 or more, four times in a row. Sends a warning message if the value is between 480 and 640, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 4.0 HTTP Server Health

WINOSSPI-IIS40_HTTPCurrentBlockedAsyncIO

Description

Checks every five minutes for the number of requests that are blocked temporarily because of bandwidth throttling settings. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row.

WINOSSPI-IIS40_HTTPCurrentConnections

Description

Checks every five minutes for the total number of connections that are open to the web service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the

value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_HTTPFilesTotalSec

Description

Checks every five minutes for the number of files per second that the web service is sending and receiving. Sends a critical message to the active message browser if the value is 640 or more, four times in a row. Sends a warning message if the value is between 600 and 640, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_HTTPHealthPerformanceMonitor

Description

Checks every five minutes for the total number of bytes sent and received per second by the web service. Sends a critical message to the active message browser if the value is 64000 or more, four times in a row. Sends a warning message if the value is between 48000 and 64000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_HTTPMeasuredIOBandwidth

Description

Checks every five minutes for the percentage bandwidth used by asynchronous I/O (averaged over one minute). Sends a critical message to the active message browser if the value is 90 or more, four times in a row. Sends a warning message if the value is between 80 and 90, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_HTTPNotFoundErrors

Description

Checks every five minutes for the number of errors per second caused by requests to the web service for files that could not be found. Sends a critical message to the active message browser if the value is 250 or more, four

times in a row. Sends a warning message if the value is between 200 and 250, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_HTTPRequestsSec

Description

Checks every five minutes for the number of requests for files that the web service receives per second. Sends a critical message to the active message browser if the value is 640 or more, four times in a row. Sends a warning message if the value is 480 or more, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 4.0 Index Server Health

WINOSSPI-IIS40_IndexServerRequestsRejected

Description

Checks every five minutes for the total number of query requests that the index server rejected. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 4.0 NNTP Server Health

WINOSSPI-IIS40_NntpArticleMapEntriesSec

Description

Checks every five minutes for the number of entries per second inserted into the NNTP servers article mapping table. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_NntpArticlesDeletedSec

Description

Checks every five minutes for the number of articles deleted from the NNTP server per second since it was started. Sends a critical message to the active message browser if the value is 20 or more, three times in a row. Sends a warning message if the value is between 10 and 20, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_NntpArticlesPostedSec

Description

Checks every five minutes for the number of articles posted to the NNTP server per second. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_NntpArticlesReceivedSec

Description

Checks every five minutes for the number of articles received by the NNTP server per second. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_NntpArticleSentSec

Description

Checks every five minutes for the number of articles sent by the NNTP server per second. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_NntpServerCurrentConnections

Description

Checks every five minutes for the number of connections that the NNTP server currently has open. Sends a critical message to the active message browser if the value is 600 or more, three times in a row. Sends a warning message if the value is between 500 and 600, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 4.0 SMTP Server Health

WINOSSPI-IIS40_SmtpMessagesReceivedSec

Description

Checks every five minutes for the number of mail messages per second that the SMTP server is receiving. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_SmtpMessagesSentSec

Description

Checks every five minutes for the number of mail messages per second that the SMTP server is sending. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS40_SmtpNumberOfQueueFilesOpen

Description

Checks every five minutes for the number of open queue files. Sends a critical message to the active message browser if the value is 75 or more, three times in a row. Sends a warning message if the value is between 50 and 75, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

MS IIS 5.0 → Additional

WINOSSPI-IIS50_IndexingService_RunningQueries

Description

Checks the Running Queries counter of the Indexing Service object.

WINOSSPI-IIS50_IISGbl_FileCacheHitsPc

Description

Checks the File Cache Hits % counter of the Internet Information Services Global object.

WINOSSPI-IIS50_Process_PageFaultSec_Inetinfo

Description

Checks the `inetinfo` instance of the Page Fault/sec counter of the Process object.

WINOSSPI-IIS50_Process_PctProcessorTime_Inetinfo

Description

Checks the `inetinfo` instance of the % Processor Time counter of the Process object.

WINOSSPI-IIS50_Process_PrivateBytes_Inetinfo

Description

Checks the `inetinfo` instance of the Private Bytes counter of the Process object.

WINOSSPI-IIS50_Process_ThreadCount_Inetinfo

Description

Checks the `inetinfo` instance of the Thread Count counter of the Process object.

WINOSSPI-IIS50_Process_WorkingSet_Inetinfo

Description

Checks the `inetinfo` instance of the Working Set counter of the Process object.

WINOSSPI-IIS50_Process_BytesTransmittedSec

Description

Checks the Bytes Transmitted/sec counter of the Server object.

WINOSSPI-IIS50_WorkingSet_AvailableBytes

Description

Checks counter 'Working set' of object 'Process' along with 'Available bytes' counter of the 'Memory' Object

MS IIS 5.0 → Diagnostic

WINOSSPI-IIS50_FtpServerFwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from MSFTPSVC. Forwards these as messages to the active message browser.

WINOSSPI-IIS50_FwdAllApplicationWarnError

Description

Monitors the application log for entries with the severity Warning or Error from IISADMIN or W3SVC. Forwards these as messages to the active message browser.

WINOSSPI-IIS50_FwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from IISADMIN or W3SVC. Forwards these as messages to the active message browser.

WINOSSPI-IIS50_IndexServerFwdAllApplicationWarnError

Description

Monitors the system log for entries with the severity Warning or Error from the Content Index Service (CISVC). Forwards these as messages to the active message browser.

WINOSSPI-IIS50_NntpServerFwdAllSystemWarnError

Description

Monitors the system log for entries with Warning or Error severity from the NNTP Service (NNTPSVC). Forwards these as messages to the active message browser.

WINOSSPI-IIS50_SmtpServerFwdAllSystemWarnError

Description

Monitors the system log for entries with the severity Warning or Error from the SMTP Service (SMTPSVC). Forwards these as messages to the active message browser.

WINOSSPI-IIS50_SrvProcMon_CISVC

Description

Checks every five minutes whether the service CISVC and the corresponding process *cisvc.exe* are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS50_SrvProcMon_IISADMIN

Description

Checks every five minutes whether the service IISADMIN and the corresponding process *inetinfo.exe* are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS50_SrvProcMon_MSFTPSVC**Description**

Checks every five minutes whether the service MSFTPSVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again

WINOSSPI-IIS50_SrvProcMon_NNTPSVC**Description**

Checks every five minutes whether the service NNTPSVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS50_SrvProcMon_SMTPSVC**Description**

Checks every five minutes whether the service SMTPSVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

WINOSSPI-IIS50_SrvProcMon_W3SVC**Description**

Checks every five minutes whether the service W3SVC and the corresponding process inetinfo.exe are running. If not, sends a message to the active message browser, which gives details of the services status. The operator can restart the service using an operator-initiated command. Acknowledges the message when the service is running again.

IIS 5.0 Active Server Pages

ASP Error

WINOSSPI-IIS50_AspErrorSec

Description

Checks every five minutes for the number of errors per second from Active Server Pages. Sends a critical message to the active message browser if the value is two or more, three times in a row. Sends a warning message if the value is one or more, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_AspScriptErrors

Description

Checks every five minutes for the number of ASP requests that failed because of a runtime error. Sends a critical message to the active message browser if the value is 40 or more, 16 times in a row. Sends a warning message if the value is between 15 and 40, 16 times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_AspPreProcessorErrors

Description

Checks every five minutes for the number of ASP requests that failed because of a preprocessor error. Sends a critical message to the active message browser if the value is 40 or more, three times in a row. Sends a warning message if the value is between 15 and 40, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_AspScriptCompilerErrors

Description

Checks every five minutes for the number of ASP requests that failed because of an error during compilation. Sends a critical message to the active message browser if the value is 40 or more, three times in a row. Sends a warning message if the value is between 15 and 40, three times in a

row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Memory Allocation

WINOSSPI-IIS50_ASPScriptEnginesCached

Description

Checks every five minutes for the number of ASP script engines in the cache. Sends a critical message to the active message browser if the value is 40 or more, four times in a row. Sends a warning message if the value is between 15 and 40, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Requests

WINOSSPI-IIS50_ASPRequestBytesInTotal

Description

Checks every five minutes for the total size of all ASP requests, in bytes. Sends a critical message to the active message browser if the value is 20 million or more, four times in a row. Sends a warning message if the value is between 5000 and 20 million, four times in a

row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestBytesOutTotal

Description

Checks every five minutes for the total size in bytes of ASP responses sent, excluding the HTTP response headers. Sends a critical message to the active message browser if the value is 20 million or more, four times in a row. Sends a warning message if the value is between 5000 and 20 million, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser

WINOSSPI-IIS50_ASPRequestExecutionTime

Description

Checks every five minutes for the time in milliseconds that it took the last ASP request to execute. Sends a critical message to the active message

browser if the value is 15000 or more, four times in a row. Sends a warning message if the value is between 5000 and 15000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestWaitTime

Description

Checks every five minutes for the time in milliseconds that the latest ASP request waited in the queue. Sends a critical message to the active message browser if the value is 15000 or more, three times in a row. Sends a warning message if the value is between 5000 and 15000, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsDisconnected

Description

Checks every five minutes for the number of ASP requests that were disconnected because of a communication failure. Sends a critical message to the active message browser if the value is 100 or more, four times in a row. Sends a warning message if the value is between 50 and 100, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsExecuting

Description

Checks every five minutes for the number of currently executing ASP requests. Sends a critical message to the active message browser if the value is more than 100, twice in a row. Sends a warning message if the value is between 50 and 100, twice in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsFailedTotal

Description

Checks every five minutes for the number of ASP requests that failed because of rejections, insufficient access rights, or errors. Sends a critical message to the active message browser if the value is 150 or more, three

times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsNotAuthorized

Description

Checks every five minutes for the number of ASP requests that failed because of insufficient access rights. Sends a critical message to the active message browser if the value is 1000 or more, three times in a row. Sends a warning message if the value is between 500 and 1000, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsNotFound

Description

Checks every five minutes for the number of ASP requests for files that could not be found. Sends a critical message to the active message browser if the value is 200 or more, three times in a row. Sends a warning message if the value is between 100 and 200, three times in row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsQueued

Description

Checks every five minutes for the number of ASP requests that are waiting in the queue. Sends a critical message to the active message browser if the value is 200 or more, three times in a row. Sends a warning message if the value is between 100 and 200, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsRejected

Description

Checks every five minutes for the number of ASP requests that were rejected due to insufficient resources. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning

message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsSec

Description

Checks every five minutes for the number of ASP requests carried out per second. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsSucceeded

Description

Checks every five minutes for the number of ASP requests carried out successfully. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsTimedOut

Description

Checks every five minutes for the number of ASP requests that timed out. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPRequestsTotal

Description

Checks every five minutes for the total number of ASP requests that occurred since the service was last started. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in

a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Sessions

WINOSSPI-IIS50_AspSessionDuration

Description

Checks every five minutes how long the most recent ASP session lasted in milliseconds. Sends a critical message to the active message browser if the value is more than 100000, four times in a row. Sends a warning message if the value is between 50000 and 100000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_AspSessionsCurrent

Description

Checks every five minutes for the number of ASP sessions currently being serviced. Sends a critical message to the active message browser if the value is 250 or more, three times in a row. Sends a warning message if the value is between 200 and 250, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_AspSessionsTimedOut

Description

Checks every five minutes for the number of ASP sessions that timed out. Sends a critical message to the active message browser if the value is 100 or more, three times in a row. Sends a warning message if the value is between 50 and 100, three times in a row. When the value falls below the threshold again, sends the message to the active message browser.

WINOSSPI-IIS50_AspSessionsTotal

Description

Checks every five minutes for the total number of ASP sessions since the service was last started. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the

value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Policies

WINOSSPI-IIS50_ASPTemplateCacheHitRate

Description

Checks every five minutes for the percentage of ASP requests that could be met from the policy cache. Sends a critical message to the active message browser if this is 80% of requests or less. Sends a warning message if this is between 80% and 90% of requests. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASPTemplateNotifications

Description

Checks every five minutes for the number of policies in the cache that need to be updated. Sends a critical message to the active message browser if the value is 1000 or more, three times in a row. Sends a warning message if the value is between 500 and 1000, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

ASP Transactions

WINOSSPI-IIS50_ASP TransactionsAborted

Description

Checks every five minutes for the number of aborted ASP transactions. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASP TransactionsCommitted

Description

Checks every five minutes for the number of committed ASP transactions. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is

between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASP TransactionsPending

Description

Checks every five minutes for the number of ASP transactions currently in progress. Sends a critical message to the active message browser if the value is 1000 or more, four times in a row. Sends a warning message if the value is between 500 and 1000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASP TransactionsSec

Description

Checks every five minutes for the number of ASP transactions started per second. Sends a critical message to the active message browser if the value is more than 100, four times in a row. Sends a warning message if the value is between 50 and 100, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_ASP TransactionsTotal

Description

Checks every five minutes for the total number of ASP transactions that occurred since the service was last started. Sends a critical message to the active message browser if the value is 10000 or more, four times in a row. Sends a warning message if the value is between 5000 and 10000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 5.0 FTP Server Health

WINOSSPI-IIS50_FtpBytesTotalSec

Description

Checks every five minutes for the number of bytes per second sent and received by the FTP service. Sends a critical message to the active message browser if the value is 64000 or more, four times in a row. Sends a warning message if the value is between 48000 and 64000, four times in a row. When

the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_FtpCurrentAnonymousUsers

Description

Checks every five minutes for the number of anonymous connections that are open to the FTP service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser

WINOSSPI-IIS50_FtpCurrent Connections

Description

Checks every five minutes for the total number of connections that are open to the FTP service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_FtpCurrentNonAnonymousUsers

Description

Checks every five minutes for the number of non-anonymous connections that are open to the FTP service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_FtpTotalFilesTransferred

Description

Checks every five minutes for the total number of files that the FTP service transferred since it was last started. Sends a critical message to the active message browser if the value is 640 or more, four times in a row. Sends a warning message if the value is between 480 and 640, four times in a row.

When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 5.0 HTTP Server Health

WINOSSPI-IIS50_HTTPCurrentBlockedAsyncIO

Description

Checks every five minutes for the number of requests that are blocked temporarily because of bandwidth throttling settings. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row.

WINOSSPI-IIS50_HTTPCurrentConnections

Description

Checks every five minutes for the total number of connections that are open to the web service. Sends a critical message to the active message browser if the value is 64 or more, four times in a row. Sends a warning message if the value is between 48 and 64, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_HTTPFilesSec

Description

Checks every five minutes for the number of files per second that the web service is sending and receiving. Sends a critical message to the active message browser if the value is 640 or more, four times in a row. Sends a warning message if the value is between 600 and 640, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_HTTPHealthPerformanceMonitor

Description

Checks every five minutes for the total number of bytes sent and received per second by the web service. Sends a critical message to the active message browser if the value is 64000 or more, four times in a row. Sends a

warning message if the value is between 48000 and 64000, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_HTTPMeasuredIOBandwidth

Description

Checks every five minutes for the percentage bandwidth used by asynchronous I/O (averaged over one minute). Sends a critical message to the active message browser if the value is 90 or more, four times in a row. Sends a warning message if the value is between 80 and 90, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_HTTPNotFoundErrors

Description

Checks every five minutes for the number of errors per second caused by requests to the web service for files that could not be found. Sends a critical message to the active message browser if the value is 250 or more, four times in a row. Sends a warning message if the value is between 200 and 250, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_HTTPRequestsSec

Description

Checks every five minutes for the number of requests for files that the web service receives per second. Sends a critical message to the active message browser if the value is 640 or more, four times in a row. Sends a warning message if the value is 480 or more, four times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 5.0 Index Server Health

WINOSSPI-IIS50_IndexServerRequestsRejected

Description

Checks every five minutes for the total number of query requests that the index server rejected. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 5.0 NNTP Server Health

WINOSSPI-IIS50_NntpArticleMapEntriesSec

Description

Checks every five minutes for the number of entries per second inserted into the NNTP servers article mapping table. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_NntpArticlesDeletedSec

Description

Checks every five minutes for the number of articles deleted from the NNTP server per second since it was started. Sends a critical message to the active message browser if the value is 20 or more, three times in a row. Sends a warning message if the value is between 10 and 20, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_NntpArticlesPostedSec

Description

Checks every five minutes for the number of articles posted to the NNTP server per second. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if

the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser

WINOSSPI-IIS50_NntpArticlesReceivedSec

Description

Checks every five minutes for the number of articles received by the NNTP server per second. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_NntpArticleSentSec

Description

Checks every five minutes for the number of articles sent by the NNTP server per second. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_NntpServerCurrentConnections

Description

Checks every five minutes for the number of connections that the NNTP server currently has open. Sends a critical message to the active message browser if the value is 600 or more, three times in a row. Sends a warning message if the value is between 500 and 600, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

IIS 5.0 SMTP Server Health

WINOSSPI-IIS50_SmtpMessagesReceivedSec

Description

Checks every five minutes for the number of mail messages per second that the SMTP server is receiving. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_SmtpMessagesSentSec

Description

Checks every five minutes for the number of mail messages per second that the SMTP server is sending. Sends a critical message to the active message browser if the value is 150 or more, three times in a row. Sends a warning message if the value is between 100 and 150, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

WINOSSPI-IIS50_SmtpNumberOfQueueFilesOpen

Description

Checks every five minutes for the number of open queue files. Sends a critical message to the active message browser if the value is 75 or more, three times in a row. Sends a warning message if the value is between 50 and 75, three times in a row. When the value falls below the threshold again, sends the message to the acknowledged message browser.

MS IIS 6.0 → Diagnostic

LOGFILE_TEMPLATE "WINOSSPI-IIS60_FtpServerFwdAllSystemWarnError"

Description

Monitors the system event log entries with the severity Warning or Error from MSFTPSVC. Forwards these as messages to the active message browser.

LOGFILE_TEMPLATE "WINOSSPI-IIS60_FwdAllApplicationWarnError"

Description

Monitors the application event log for entries with the severity Warning or Error from CISVC. Forwards these as messages to the active message browser.

LOGFILE_TEMPLATE "WINOSSPI-IIS60_FwdAllSystemWarnError"

Description

Monitors the system event log entries with the severity Warning or Error from W3SVC, IISMAP, or IISLOG. Forwards these as messages to the active message browser.

LOGFILE_TEMPLATE "WINOSSPI-IIS60_IndexServerFwdAllApplicationWarnError"

Description

Monitors the application event log for entries with the severity Warning or Error from CISVC. Forwards these as messages to the active message browser.

LOGFILE_TEMPLATE "WINOSSPI-IIS60_NntpServerFwdAllSystemWarnError"

Description

Monitors the system event log entries with the severity Warning or Error from NNTPSVC. Forwards these as messages to the active message browser.

LOGFILE_TEMPLATE "WINOSSPI-IIS60_SmtpServerFwdAllSystemWarnError"

Description

Monitors the system event log entries with the severity Warning or Error from SMTPSVC. Forwards these as messages to the active message browser.

MS Site Server 3.0 → Diagnostic

WINOSSPI-SS30_AcmServerFwdAllApplicationWarnError

Description

Forwards all ACMSVC Active Channel Multicaster Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_AuthServerFwdAllApplicationWarnError

Description

Forwards all BROKSVC Authentication Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_CommerceServerFwdAllApplicationWarnError

Description

Forwards all Commerce Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_CrsServerFwdAllApplicationWarnError

Description

Forwards all CRS Content Deployment Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_GathererServerFwdAllApplicationWarnError

Description

Forwards all GTHRSVC Gatherer Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_LdapServerFwdAllSystemWarnError

Description

Forwards all LDAPSVC LDAP Server system event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_ListBldrServerFwdAllApplicationWarnError

Description

Forwards all `tmlbsvc` List Builder Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_MsgBldrServerFwdAllApplicationWarnError

Description

Forwards all `msgbldsvc` Message Builder Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_SearchServerFwdAllApplicationWarnError

Description

Forwards all `sssearch` Search Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_SiteServerFwdAllApplicationWarnError

Description

Forwards all Site Server application event log entries with a severity level of Warning or Error.

WINOSSPI-SS30_AcmSvcProcMon

Description

Checks the `ACMSVC` Active Channel Multicaster service and its corresponding process.

WINOSSPI-SS30_AuthSrvProcMon

Description

Checks the `BROKSVC` Authentication service and its corresponding process.

WINOSSPI-SS30_CrsSrvProcMon

Description

Checks the `CRS` Content Deployment service and its corresponding process.

WINOSSPI-SS30_GathererSrvProcMon

Description

Checks the `GTHRSVC` Gatherer service and its corresponding process.

WINOSSPI-SS30_LdapSrvProcMon

Description

Checks the LDAPSVC LDAP service and its corresponding process.

WINOSSPI-SS30_ListBldrSrvProcMon

Description

Checks the TMLBSVC List Builder service and its corresponding process.

WINOSSPI-SS30_MsgBldrSrvProcMon

Description

Checks the MSGBLDSVC Message Builder service and its corresponding process.

WINOSSPI-SS30_SearchSrvProcMon

Description

Checks the `SSSearch` service and its corresponding process.

WINOSSPI-SS30_WebServiceGetRequestSec

Description

Checks the Get Requests/sec counter of the Web Service object.

5

Service Discovery

This chapter explains the discovery process, prerequisites, and the discovery file locations.

Prerequisite for Service Discovery

You must install the Service Discovery Framework (SDF) and deploy the instrumentation on the managed node before initiating the service discovery process on the managed node.

Run the application `Set JRE Path` from the HP Systems Insight Manager application group in the OVO Application Bank to set the Java path on the OVO management server. You must perform this activity before discovering HP Systems Insight Manager services.

WinOS SPI Discovery

You can use one of the following options to initiate service discovery on the managed node:

- `WINOSSPI-Discovery` policy present in the `Discovery` policy group. By default, this policy runs every day at 2 a.m. on the managed nodes. Refer to “Discovery” on page 80 for more information about this policy.
- `Service Discovery` application present in the `WinOSSPI Discovery` application group. Refer to “Application Group: WinOSSPI Discovery” on page 65 for more information about the `Service Discovery` application.

The service graph generated by WinOS SPI Discovery is a snapshot of services present on the managed nodes when the application is run.

Mechanism for Gathering Service Information

The WinOS SPI uses a simple mechanism to gather the service information as follows:

- a discovery *server* script (`SPI_DiscServ.sh`) on the OVO management server uses the list of managed nodes as parameters to trigger a discovery *client* on each of the OVO managed nodes listed.
- discovery *clients* on the various OVO managed nodes use discovery modules that are deployed to the WinOS SPI managed nodes.

The Discovery Modules

The discovery modules used by the WinOS SPI reside together with the other SPI components on the OVO managed node. Once started by the discovery server, the discovery client locates and reads the `Module Registry` (`winosspi_discreg.txt`) on the managed node in order to find out which services have to be discovered and which modules are responsible for each service.

The Discovery Modules

The information that is discovered by the discovery modules is written to service-configuration files in a format (XML) that can be used by the OVO Service Navigator to display the services as a tree in the OVO Service Navigator GUI.

The discovery log messages are stored in the file `winosspi_discovery.log` on the managed node. If tracing is enabled, the trace messages are present in the `winosspi.trace` file.

Discovery client running on the managed node performs these actions:

1. Executes the discovery modules specified in the module registry.
2. Generates a service configuration file.

The management server validates and uploads the service configuration to the service tree, which can be viewed using OVO Service Navigator GUI.

Prerequisites on the managed node

- IE 4.0 or higher
- Perl 5.6.1 or higher
- Windows Script Host 5.6 or higher

NOTE

When you run Service Discovery application on the managed node, it will install Windows Script Host 5.6, if the latter is not found on the node. Upgrade to 5.6 if the node currently has an earlier version of Windows Script Host.

Prerequisites on the management server

- The OpenView Operations agent software has to be installed on the machine where the management server is running, and the machine should be a managed node of the management server running on it.
- OVO Service Navigator has to be installed on the management server.

Discovering Services

The discovery process can be executed in three steps:

- Assigning Nodes to the WinOS SPI Node Group
- Distributing Policies and Commands to the Node Group
- Discovering Windows Services on Managed Nodes

Win OS SPI performs service discovery on all nodes in the WinOS SPI node group. If you want to exclude any node from the discovery process and retain that node in the node group, include the `-e <node name>` option in the `WINOSSPI-Discovery` policy. `<node name>` specifies the node that you want to exclude from the discovery process.

You can include the `-i <nodename>` option in the `WINOSSPI-Discovery` policy to include a node (outside the node group) in the discovery process. This option does not add the specified node to the node group.

The WinOS SPI discovery process uses the `winosspi_disconfig.sh` configuration file. You must update only the following options in this file:

- `SPI_DISC_TRACE=ON|OFF`- Enables or disables tracing on both the management server and the managed node.
- `MSG_ALLOW=Y|N`- Enables or disables the forwarding of discovery message to the message browser. If you enable this option, WinOS SPI displays all the error messages generated during discovery on the message browser.

Assigning Nodes to the WinOS SPI Node Group

In order to facilitate the discovery of the services you want to monitor with the WinOS SPI policies on the various OVO managed nodes in your environment, you first have to add the managed nodes which you want to monitor with the WinOS SPI to the `winosspi` node group. This is the default node group added to the OVO Node Group Bank window during the installation of the WinOS SPI software.

Distributing Policies and Commands to the Node Group

To assign the nodes to the WinOS SPI node group, carry out the following steps:

1. Start the OVO GUI
2. If the nodes you want to monitor with the WinOS SPI are *already* present in the OVO Node Bank window, you can skip steps 3 to 6 and proceed directly to step 7.
3. If the nodes you want to monitor with the WinOS SPI are *not* yet present in the OVO Node Bank window, open the Node Bank window and select the following menu option:

Actions: Node > Add
4. The Add Node window opens.
5. Enter the requested details as appropriate (label, long hostname, etc), click the [IP Address] button to resolve automatically the IP address, and ensure the newly added nodes appear correctly in the Node Bank window. Repeat this step for each OVO managed node in your environment that you want to monitor with the WinOS SPI.
6. Install the agents on all managed nodes. Refer to the *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide*, for information about installing agents on managed nodes.
7. Open the Node Group Bank window and expand (by double-clicking) the winOSSPI node group.
8. Drag the managed nodes you want to monitor with the WinOS SPI from the Node Bank window and drop them into the winOSSPI node-group window.

Distributing Policies and Commands to the Node Group

To receive discovery messages from the managed node, assign the winOSSPI-opcmmsg policy to the winOSSPI node group. This policy is located in the Discovery policy group under the group MICROSOFT WINDOWS.

To assign and distribute WinOS SPI commands, carry out the following steps:

1. In the Node Group Bank Window, click the winOSSPI node group, and select the following menu option:

Actions: Agents > Assign Templates...

2. The Define Configuration Window opens. Click Add.
3. The Add Configuration Window opens. Click Open Template Window, to open the Message Source Template Window.
4. Select the template WINOSSPI-opcmmsg in the Discovery template group under MICROSOFT WINDOWS.
5. In the Add Configuration Window, click Get Template Selection.
6. Click [OK].
7. Click [OK] in the Define Configuration Window.
8. In the Node Group Bank Window, click the winOSSPI node group, and select the following menu option:

Actions: Agents > Install / Update S/W & Config...

9. The Install / Update OVO Software and Configuration... window opens. Verify that the correct nodes appear.
10. Next, select Templates and Commands to distribute.
11. Click [OK]

OVO opens a shell to indicate the progress of the distribution. When the distribution process has completed, a message appears in the Message Browser window indicating that the command distribution completed successfully. You can refresh the browser window using the following menu option in the Message Browser window:

Browser: Reload

Discovering Windows Services on Managed Nodes

Follow the steps explained below to discover the Windows services on the managed nodes.

1. Start the OVO GUI and open the Node Bank window.

Discovering Windows Services on Managed Nodes

2. Open the Application Bank window and expand the `winOSSPI Discovery` application group under the `Windows OS SPI` top level group.
3. Drag and drop the node (to perform discovery on a single node) or the `winOSSPI` node group (to perform discovery on all the nodes in the node group) on the application `Service Discovery`.
4. The `Discovery` application runs as root.
5. The application output window displays the progress of the `WinOS SPI Discovery`. To view messages in the active message browser, set the `MSG_ALLOW` flag to `Y` in the file `winosspi_disconfig.sh`. Note that error messages are written to the following file on the OVO management server:

```
/var/opt/OV/log/SPISvcDisc/discovery_error.log
```

You can also use the `WINOSSPI-Discovery` policy to discover services on a managed node.

NOTE

The discovery process takes a snap shot of the state of the services on the managed node at a given point in time. If the service configuration on a managed node subsequently changes, you will have to run the discovery process again to have the changes reflected in the `WinOS SPI` service tree.

Service Discovery File Locations

The location of the files that are created or used during the WinOS SPI service discovery process are listed below:

The OVO Management Server

If you need to locate a particular type of file on the OVO management server, use the following list:

File Type...	WinOS SPI File Location...
Logs	<code>/var/opt/OV/log/SPISvcDisc/ discovery_error.log</code>
Service Configuration File (XML)	<code>/var/opt/OV/share/conf/ SPISvcDisc/WINOSSPI/ WINOSSPISVCDISC_\${NODENAME}.xml</code>
Discovery Server Script	<code>/opt/OV/sbin/SPISvcDisc/ SPI_DiscServ.sh</code>
Discovery Configuration File	<code>/opt/OV/sbin/winosspi/ winosspi_disconfig.sh</code>

The OVO Service Navigator/Discovery Output files also contain information about errors that occur during the service-discovery process, for example, if a node is down or not responding.

NOTE

You can set values for variables in the discovery configuration file `winosspi_disconfig.sh` to enable tracing and to receive discovery related messages from the managed nodes. To enable tracing, the variable `SPI_DISC_TRACE` should be set to “ON” and to receive discovery related messages from the node, the variable `MSG_ALLOW` should be set to “Y”. By default, tracing is set to “OFF” and `MSG_ALLOW` is set to “N”

The OVO Managed Nodes for DCE Agents

The following list shows the directory locations for the files the WinOS SPI deploys on OVO managed nodes for DCE agents.

File Type...	WinOS SPI File Location...
Discovery Client Script	%OvAgentDir%\bin\OpC\cmds\SPI_DiscClient.pl
Discovery Modules	%OvAgentDir%\bin\OpC\cmds
Logs	%OvAgentDir%\SPISvcDisc\log\winosspi_discovery.log
	%OvAgentDir%\log\winosspi\winosspi.log
Trace (If tracing is enabled)	%OvAgentDir%\log\winosspi\winosspi.trace

The OVO Managed Nodes for HTTPS Agents

The following list shows the directory locations for the files the WinOS SPI deploys on OVO managed nodes for HTTPS agents.

File Type...	WinOS SPI File Location...
Discovery Client Script	%OvInstallDir%\data\bin\Instrumentation\SPI_DiscClient.pl
Discovery Modules	%OvInstallDir%\data\bin\Instrumentation
Logs	%OvInstallDir%\data\SPISvcDisc\log\winosspi_discovery.log
	%OvInstallDir%\data\log\winosspi\winosspi.log
Trace (If tracing is enabled)	%OvInstallDir%\data\log\winosspi\winosspi.trace

6

Self-Healing Services

HP OpenView Self-healing services (SHS) allows you to collect data from the managed node in the event of a problem or an error. The collected data is saved in a pre-defined format, which allows faster and easier troubleshooting.

Starting SHS on a Management Server

Use the `Self Healing - Server Collector` application to collect configuration information and log files from the management server.

To launch the application, drag the icon of the management server from which you want to collect data and place it on the `Self Healing - Server Collector` application icon in the `Application Bank` window.

NOTE

To use this application, you must make sure that the `OpenView Operations Agent` is installed on the management server from which you want to collect data. You must also deploy the SHS instrumentation on the management server.

Starting SHS on a Managed Node

Use the `Self Healing Info` application to collect configuration information and log files from the managed node.

To launch the application, drag the icon of the managed node from which you want to collect data and place it on the `Self Healing Info` application icon in the Application Bank window.

NOTE

You must deploy the SHS instrumentation on all the managed nodes.

Numerics

672–683 events 103
1487–1490 events 102

A

Active Directory
 database
 site changes 109
Add Configuration window 24
additional templates 22, 72
ADS prerequisites 68
applications
 message groups 36
 preconfigured 11
 supported 13
assigning
 nodes to discovery group 174
 nodes to Node Group windows 21
 responsibilities 11
 templates 11
authentication ticket logfile 103

C

changing operator profile 20
checking status of Windows services
 and processes 40
colors in Message Group window 36
configuration files 18
Configure
 assigning nodes to discovery
 group 174
 discovering OS services 177
CreateWMIInstance-ds_site.vbs 69

D

dcdiag tool
 updated version 68
deploying templates 12
diagnostic templates 22, 72
Directory Service logfile 102
Directory User Accounts logfiles 103
discovery group

 assigning nodes to 174
 distributing components 11
 documentation files 18
 Domain Admins logfiles 110
 download dcdiag update 68

E

Enterprise Admins logfiles 110

F

features, system 11
file sets 18
files
 configuration 18
 documentation 18
 Windows NT managed nodes 18

I

install
 nodes and node groups 174
Install/Update OVO Software and
 Configuration window 25
installing software options 25
IP subnet logfiles 109

L

labels, message group 36
logfiles
 Directory Service 102
 Security
 authentication tickets 103
 Windows Management
 Instrumentation
 Directory User Accounts 103
 Domain Admins 110
 Enterprise Admins 110
 IP subnets 109

M

managing Windows nodes 11
Message Group window
 colors 36
message groups

 organizing 35
 types 36
monitors
NT Performance Counter
 NTDS\DRS Inbound Bytes
 Compressed (Between
 Sites, Before
 Compression)/sec 101
 NTDS\DRS Inbound Bytes
 Not Compressed (Within
 Site)/sec 101
 NTDS\DRS Inbound Object
 Updates Remaining in
 Packet 102
 NTDS\DRS Pending
 Replication
 Synchronizations 102
 NTDS\DS Notify Queue Size
 102
 NTDS\DS Security Descriptor
 Propagator Runtime Queue
 110
 NTDS\SAM Transitive
 Membership Evaluations
 111
 Server\Errors Access
 Permissions 104
 Server\Errors Granted Access
 104
 Server\Errors Logon 110
 Server\SAM Non-Transitive
 Membership Evaluation/
 sec 110

N

Node Group windows, assigning
 nodes 21
nodes
 assign to WinOS SPI node groups
 174
 assigning to discovery group 174

- assigning to Node Group
 - Windows 21
 - discovering OS services on 177
 - managing 11
 - NT Performance Counter
 - NTDS\DRA Inbound Bytes
 - Compressed (Between Sites, Before Compression)/sec 101
 - NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec 101
 - NTDS\DRA Inbound Object
 - Updates Remaining in Packet 102
 - NTDS\DRA Pending Replication Synchronizations 102
 - NTDS\DS Notify Queue Size 102
 - NTDS\DS Security Descriptor
 - Propagator Runtime Queue 110
 - NTDS\SAM Transitive
 - Membership Evaluations 111
 - Server\Errors Access Permissions 104
 - Server\Errors Granted Access 104
 - Server\Errors Logon 110
 - Server\SAM Non-Transitive
 - Membership Evaluation/sec 110
 - NTDS\DRA Inbound Bytes
 - Compressed (Between Sites, Before Compression)/sec counter 101
 - NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec counter 101
 - NTDS\DRA Inbound Object Updates Remaining in Packet counter 102
 - NTDS\DRA Pending Replication Synchronizations counter 102
 - NTDS\DS Notify Queue Size counter 102
 - NTDS\DS Security Descriptor
 - Propagator Runtime Queue counter 110
 - NTDS\SAM Transitive
 - Membership Evaluations 111
 - Server\Errors Access Permissions 104
 - Server\Errors Granted Access 104
 - Server\Errors Logon 110
 - Server\SAM Non-Transitive
 - Membership Evaluation/sec 110
- NTDS\DS Security Descriptor
 - Propagator Runtime Queue counter 110
- NTDS\SAM Transitive
 - Membership Evaluations 111
- Evaluations counter 111
- O**
- operations, managing 11
 - operator
 - changing profile 20
 - WIN_op 20
 - options, software installation 25
 - organizing message groups 35
 - OS
 - discovering services on nodes 177
- P**
- PerfMon counters
 - NTDS\DRA Inbound Bytes
 - Compressed (Between Sites, Before Compression)/sec 101
 - NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec 101
 - NTDS\DRA Inbound Object
 - Updates Remaining in Packet 102
 - NTDS\DRA Pending Replication Synchronizations 102
 - NTDS\DS Notify Queue Size 102
 - NTDS\DS Security Descriptor
 - Propagator Runtime Queue 110
 - NTDS\SAM Transitive
 - Membership Evaluations 111
 - Server\Errors Access Permissions 104
 - Server\Errors Granted Access 104
 - Server\Errors Logon 110
 - Server\SAM Non-Transitive
 - Membership Evaluation/sec 110
- R**
- registry key 102
 - replication event logfiles 102
- S**
- security groups
 - Domain Admins 110
 - Enterprise Admins 110
 - Security logfiles
 - authentication tickets 103
 - Server\Errors Access Permissions
 - counter 104
 - Server\Errors Granted Access counter 104
 - Server\Errors Logon counter 110
 - Server\SAM Non-Transitive
 - Membership Evaluation/sec counter 110
 - Services
 - discovering OS on nodes 177
 - services
 - checking status 40
 - starting 40
 - stopping 40
 - sets, file 18
 - software
 - installation options 25
 - SPI for Windows
 - profile 19
 - template group 22

- SPI-WIN-OVO file set 29
 - SPI-WIN-OVO.WINOSSPI-CONF
 - file set 18
 - SPI-WIN-OVO.WINOSSPI-DOC
 - file set 18
 - SPI-WIN-OVO.WINOSSPI-SRV file set 18
 - SPI-WIN-OVO.WINOSSPI-WINNT
 - file set 18
 - starting Windows services and processes 40
 - status of Windows processes and services 40
 - stopping Windows services and processes 40
 - support, WMI 68
 - supported applications 13
- T**
- template group
 - SPI for Windows 22
 - templates
 - additional 22, 72
 - deploying 12
 - diagnostic 22, 72
 - preconfigured 11
 - WMI support 68
- U**
- updating dcdiag version 68
 - User Profile Bank window 19
- W**
- WIN_op user 20
 - WIN_SPI-ADS_SiteChanges
 - prerequisites 69
 - WIN_SPI-ADS_SiteChanges
 - template
 - description 109
 - Windows
 - assigning responsibilities 11
 - deploying templates 12
 - services and process
 - checking status 40
 - starting 40
 - stopping 40
 - windows
 - Add Configuration 24
 - Install/Update OVO Software and Configuration 25
 - Message Group
 - colors 36
 - Windows 2000 WMI 69
 - Windows Management
 - Instrumentation
 - logfiles
 - Directory User Accounts 103
 - Domain Admins 110
 - Enterprise Admins 110
 - IP subnets 109
 - support 68
 - Windows nodes
 - assigning templates 11
 - distributing components 11
 - managing 11
 - Windows NT managed nodes
 - package 18
 - Windows Terminal Server
 - support 13
 - WinOS SPI
 - file location
 - management server 178
 - nodes and node groups 174
 - WMI support 68