HP Operations Smart Plug-in for Microsoft Enterprise Servers

For the HP Operations Manager for Windows® operating system

Software Version: 8.05

Installation and Configuration Guide

Document Release Date: October 2013

Software Release Date: October 2013

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe ® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

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

HP Software online 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 valued support customer, you can benefit by using the support web site to:

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Chapter 1

Introduction

The Smart Plug-in for Microsoft Enterprise Servers (Microsoft Enterprise Servers SPI) helps you to manage the Microsoft Enterprise Servers in your environment. The Microsoft Enterprise Servers SPI keeps you informed about the conditions related to the following Microsoft Enterprise Servers:

- BizTalk Server 2006 and 2006 R2
- BizTalk Server 2010
- Internet Security and Acceleration Server 2006
- Microsoft Office SharePoint Server 2007
- Microsoft Office Communications Server 2007 and R2
- Microsoft Lync Server 2010
- Microsoft Lync Server 2013
- Microsoft SharePoint Server 2013

Microsoft Office Communications Server 2007 Deployment Configurations

The Microsoft Office Communications Server 2007 *supports* the following deployment configurations:

- Microsoft Office Communications Server Standard Edition
- Microsoft Office Communications Server Enterprise Edition Consolidated Configuration
- Microsoft Office Communications Server Enterprise Edition Expanded Configuration
- The Microsoft Office Communications Server *does not support* the following deployment configurations:
- Microsoft Office Communications Server 2007 configured with load balancing
- Microsoft Office Communications Server 2007 installed on clustered environment

Components of Microsoft Enterprise Servers SPI

The components of Microsoft Enterprise Servers SPI are policies, tools, reports, and graphs.

Policies

Policies are pre-defined thresholds to keep a constant vigilance over the Microsoft Enterprise Servers environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts are shown in service map while messages are available in message browser. The severity level of each message, whether it is a minor, major, or critical is shown by a color-code. The messages indicate the problem and help you to take preventive action. For more information about policies, see "Using Policies and Tools" on page 53.

Tools

Tools are the utilities to gather more Microsoft Enterprise Server related information. Self Healing tools are used for troubleshooting any of the Microsoft Enterprise Servers SPI. The MSES_BTS_DB_Configuration tool is used to configure the BizTalk Server of the Microsoft Enterprise Servers SPI. For more information about tools, see "Using Policies and Tools" on page 53.

Reports

Reports are the pictorial representation of various metrics of Microsoft Enterprise Servers. Data collected by policies are used to generate reports. For more information about reports, see "Integrating Microsoft Enterprise Servers SPI with HP Reporting and Graphing" on page 57.

Graphs

Graphs represent various metrics of the Microsoft Enterprise Servers. Graphs contain the data that are collected by policies. For more information about graphs, see "Integrating Microsoft Enterprise Servers SPI with HP Reporting and Graphing" on page 57.

Reports and graphs generated with the help of HP Reporter and HP Performance Manager provide you an overview to determine corrective actions to be taken in the long term.

For more information about the components of Microsoft Enterprise Servers SPI, see *HP Operations Smart Plug-in for Microsoft Enterprise Servers SPI Online Help* or *HP Operations Smart Plug-in for Microsoft Enterprise Servers SPI Online Help* PDF.

Functions of Microsoft Enterprise Servers SPI

The Microsoft Enterprise Servers SPI monitors the following Microsoft Enterprise Servers:

- BizTalk Server 2006
- BizTalk Server 2010
- Internet Security and Acceleration Server 2006
- Microsoft Office SharePoint Server 2007
- Microsoft Office Communications Server 2007
- Microsoft Lync Server 2010

- Microsoft Lync Server 2013
- Microsoft SharePoint Server 2013

> **Note:** All artifacts used for monitoring BizTalk Server 2010 are backward compatible with BizTalk Server 2009 and can be used for monitoring BizTalk Server 2009.

Monitoring the Availability, Performance, and Event Log

The Microsoft Enterprise Servers SPI monitors the Microsoft Enterprise Servers in your environment and maintains the thresholds set by the policies. The Microsoft Enterprise Servers SPI ensures complete availability of the services, monitors Windows performance counters, and Windows Events Logs. The Microsoft Enterprise Servers SPI notifies you if the threshold limits have exceeded.

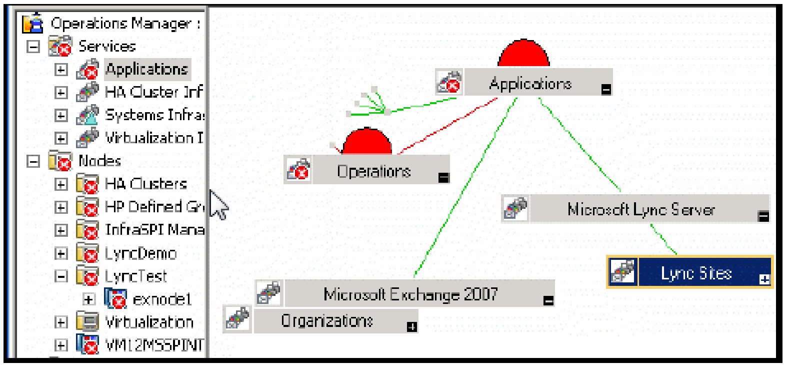
Displaying Information

The Microsoft Enterprise Servers SPI displays information in the following ways.

Service Map

Service map shows the newly added and discovered Microsoft Enterprise Servers displayed in both the console services tree (left) and the service map (right). Within the service map pane, the hierarchy expands to show the specific services present on each Microsoft Enterprise Server.

Service Map



Message Browser

The Microsoft Enterprise Servers SPI monitors events and services on the managed nodes and generates messages, which are displayed on the message browser of HPOM (HP Operations Manager) console. The message browser displays messages identified with the problem severity level.

Instruction Text

Error messages generated by the policies of the Microsoft Office Communications Server 2007 SPI of the Microsoft Enterprise Servers SPI contain instruction text which mentions probable cause and preventive action to resolve problems.

Reports and Graphs

Reports and graphs present information that help you see the trends required to manage the Microsoft Enterprise Servers in your environment by implementing efficient load balancing, capacity planning, and policy scheduling and threshold adjustments.

Generating Reports Using HP Reporter

You can generate reports to analyze the past or present conditions of the Microsoft Enterprise Servers. These web-based reports are automatically generated at periodical intervals. For more information about HP Reporter see "Integrating Microsoft Enterprise Servers SPI with HP Reporting and Graphing" on page 57.

Graphing Data with HP Performance Manager

After you manually generate the graphs, you can view the data in a more specified and granular manner. You can access graphs in the HP Performance Manager console. You can integrate the Microsoft Enterprise Servers SPI with HP Performance Manager to generate and view graphs. For more information about HP Performance Manager see "Integrating Microsoft Enterprise Servers SPI with HP Reporting and Graphing" on page 57.

Customizing Policies

You can customize the monitoring schedule or measurement threshold policies for any Microsoft Enterprise Servers SPI policy. Some of the modifications that can be made are:

- Script-parameters
- Rules
- Options

For more information about Customizing Policies, "Using Policies and Tools" on page 53.

Chapter 2

Installing Microsoft Enterprise Servers SPI

You must install the Microsoft Enterprise Servers SPI on the Windows management server. The following sections provide detailed information about the installation.

Installation Packages

The Microsoft Enterprise Servers SPI installation packages include the SPI, graphing, and reporting packages.

The graphing and reporting packages are available at different locations on the HP Operations Smart Plug-ins DVD. Install these packages if you want to generate reports and graphs.

SPI Package

The SPI package is the .msi package, which contains all the functionality of the SPI. It must be installed on a HPOM server. You can find the Microsoft Enterprise servers SPI in the following location:

<SPI DVD>\x64\SPIs\MSESSPI\MSESSPI.msi

Perform the tasks mentioned in the following sections to install the Microsoft Enterprise Servers SPI.

Graphing Package

The Graphing package contains the graphs provided by the SPI. Graphs are drawn from metrics that are collected in the data sources created by the SPI. You can find the Microsoft Enterprise Servers SPI graphing packages at the following locations:

<SPI DVD>\x64\SPIs\MSESSPI OVPM ConfigurationPackage\HPOvSpiMsesGc.msi

<SPI DVD>\x86\SPIs\MSESSPI OVPM ConfigurationPackage\HPOvSpiMsesGc.msi

Reporting Package

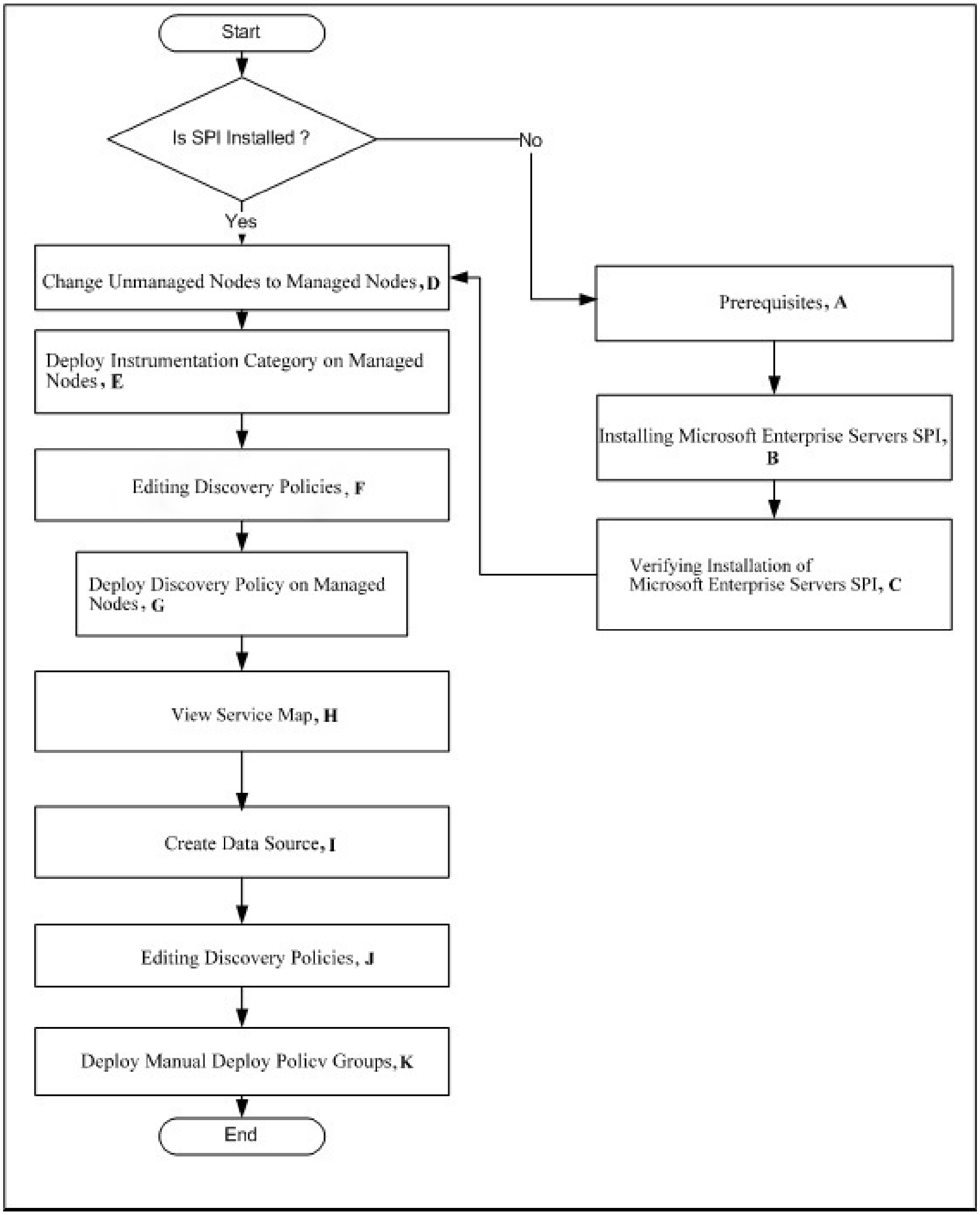
The Reporter package contains the reports provided by the SPI. The Reporter gathers the data from the nodes managed by the SPI, stores the data in its local database, and creates .HTML reports based on the default SPI report policies. You can find the Microsoft Enterprise Servers SPI reporting packages at the following locations:

<SPI DVD>\x64\SPIs\MSES Reporter Package\MSESSPI-Reporter.msi

<SPI DVD>\x86\SPIs\MSES Reporter Package\MSESSPI-Reporter.msi Installation Overview

Installation Overview

The following flowchart provides an overview of the tasks involved in the installation and configuration of Microsoft Enterprise Servers SPI.


Start
Is SPI Installed ?
No
Yes
Change Unmanaged Nodes to Managed Nodes, D
Prerequisites, A
Deploy Instrumentation Category on Managed Nodes, E
Installing Microsoft Enterprise Servers SPI, B
Editing Discovery Policies, F
Verifying Installation of Microsoft Enterprise Servers SPI, C
Deploy Discovery Policy on Managed Nodes, G
View Service Map, H
Create Data Source, I
Editing Discovery Policies, J
Deploy Manual Deploy Policv Groups, K
End

Legends of Installation and Configuration Steps

Legend	References
A	See Prerequisites
B	See Installing Microsoft Enterprise Servers SPI
C	See Verifying Installation of Microsoft Enterprise Servers SPI
D	See Change Unmanaged Nodes to Managed Nodes
E	See Deploy Instrumentation Categories on Managed Nodes
F	See Editing Discovery Policies
G	See Deploy Discovery Policy on Managed Nodes
H	See View Service Map
I	See Create Data Source
J	See Editing Discovery Policies
K	See Deploy Manual Deploy Policy Groups

Installation Environments

HPOM for Windows provides the scalable feature of monitoring enterprise application servers. SPIs are part of this scalable architecture, allowing for monitoring specific application servers. You can select SPIs from the DVD to install on servers managed by HPOM.

Standard Installation of SPI Components on an HPOM 9.00 Server

Using the HP Operations Smart Plug-ins DVD, you can select to install only the SPI packages and not the reporter and the graphing packages. However, if the full version of Reporter or Performance Manager is installed on the same machine, then the corresponding packages can be installed or removed on the HPOM 9.00 server.

Standard Installation on Remote Consoles

All the Remote Console packages on the SPI DVD are installed at once on to remote consoles. No option is provided to select a particular remote console package.

Standalone HP Reporter or HP Performance Manager

For a system with Standalone HP Reporter or HP Performance Manager, only the corresponding package of the SPI is enabled and is available for selection from the HP Operations Smart Plug-Ins DVD. For example, if a system has only HP Reporter installed then you can install the reporter package of any SPI on it. The same applies to the graphing package on the HP Performance Manager.

Prerequisites

Fulfill the hardware and software requirements before installing the SPI. Also, ensure that you install the HPOM server before installing the Microsoft Enterprise Servers SPI. It is not necessary to stop HPOM sessions before beginning the installation of the Microsoft Enterprise Servers SPI.

Hardware Requirements

For information about the hardware requirements, see the *HP Operations Manager for Windows Installation Guide*.

Software Requirements

Ensure that the following software requirements are met:

In Operations Manager for Windows (OMW) management environment, SPIs must be installed on all servers. Otherwise, SPI policy upload using the ovpmutil command results in errors. When you synchronize policy configuration between the management servers, install the SPIs downloaded using the ovpmutil commands **- ovpmutil cfg all dnl** or **ovpmutil cfg pol dnl**, on the target server prior to uploading the policies.

- HP Operations Manager for Windows: 9.00
- HP Reporter: 4.00
- HP Performance Manager: 9.x (if you want to generate graphs)
- MSES SPI version 8.2.xx for OMW9 and version 8.0 for OMW8
- HP Operations SPI Data Collector (DSI2DDF): 2.41
- HP SPI Self-Healing Services. (SPI-SHS-OVO, automatically installed while installing the SPI using SPIDVD): 3.04

On the managed node:

- HP Operations agent version 8.60 or higher
- HP Operations agent 11.00
- HP Performance Agent: 5.00 (required if you want to use HP Performance Agent for data logging)

Installing Microsoft Enterprise Servers SPI

The Microsoft Enterprise Servers SPI version 8.05 is a patch release. You can download the patches from the following location: **http://support.openview. hp.com/selfsolve/patches.** Instructions to install the patch are available in the patch text. The following sections describe procedures to install the Microsoft Enterprise Servers SPI on a management server.

Installing Microsoft Enterprise Servers SPI on a Management Server

The HP Operations Smart Plug-ins DVD contains the Microsoft Enterprise Servers SPI. To install Microsoft Enterprise Servers SPI on the management server, perform the following steps:

1. Insert the *HP Operations Smart Plug-ins* DVD into the DVD-ROM drive of the management server. The installation wizard opens.
2. Click **Next**. The Smart Plug-in Release Notes and Other Documentation screen appears.
3. Click **Next**. The Product Selection screen appears.
4. Select **Microsoft Enterprise Servers** check box, and click **Next**. The Enable/Disable AutoDeployment screen appears.
5. Select the **Enable** button to deploy the Auto-Deploy policies, and click **Next**. The License Agreement screen appears.
6. Accept the terms by selecting the option **I accept the terms in the license agreement**, and click **Next**. The Ready to Install the Program screen appears.
7. Click **Install**. The installation begins. The wizard installs the core SPIs, all necessary packages, and the Microsoft Enterprise Servers SPI.
8. Click **Finish** after the installation is complete.

Installing Microsoft Enterprise Servers SPI on a Remote Console

Install only the Microsoft Enterprise Servers SPI console packages on the HPOM remote consoles.

Installing Microsoft Enterprise Servers SPI in an HPOM Cluster Environment

Before installing the Microsoft Enterprise Servers SPI in a cluster environment, make sure that HPOM for Windows 9.00 is installed on each system of the cluster.

> **Note:** The HPOM console does not function properly until you install the Microsoft Enterprise Servers SPI on all nodes in the HPOM cluster.

At the first cluster-aware management server, select and install Smart Plug-ins.

Complete the steps described in "Installing Microsoft Enterprise Servers SPI" on previous page before proceeding to the next management server.

> **Note:** Before beginning, be sure that sufficient disk space is available on each management server for the Microsoft Enterprise Servers SPI. Cancelling the installation process before completion could result in partial installations and require manual removal of the partially

installed components.

At the next cluster-aware management server, install pre-selected Smart Plug-ins.

Repeat the steps described in "Installing Microsoft Enterprise Servers SPI on a Management Server" on previous page on each management server in the cluster and continue to every management server (as was defined in the HP Operations Manager cluster installation) until you have finished.

Note: The HPOM console will not function properly until installations are completed on all the nodes in the cluster.

Upgrading Microsoft Enterprise Servers SPI

You can upgrade the Microsoft Enterprise Servers SPI on a management server or on a remote console.

Use the common installer to detect if any previous version of Microsoft Enterprise Servers SPI is already installed. If the previous version is found, then perform the followings tasks for upgrade. The common installer also consolidates all SPIs for installation purposes.

Upgrading Microsoft Enterprise Servers SPI on a Remote Console

If you are using HPOM on a remote console, follow the Smart Plug-ins upgrade procedure for console-only systems:

1. At the console-only system, insert the *HP Operations Smart Plug-ins* DVD.
2. Follow the instruction screens until a dialog appears saying that a remote console installation has been found.
3. Click **Next**. The upgrade of all previously installed packages now occurs.

Upgrading Microsoft Enterprise Servers SPI on a Standalone Management Server

Perform the following tasks to upgrade the Microsoft Enterprise Servers SPI on a management server:

Prepare to install the latest version of the Microsoft Enterprise Servers SPI

1. Rename the Microsoft Enterprise Servers SPI policy group.
2. At the console, select **Operations Manager.**
3. Double-click **Policy management, and Policy groups**.

4. Select the **SPI for Microsoft Enterprise Servers** group and right-click it to rename it (for example, **SPI for Microsoft EnterpriseServers_OLD**).

Install the latest version of the Microsoft Enterprise Servers SPI

1. Insert the HP Operations Smart Plug-ins DVD and follow the instructions as they appear on the screen. See "Installing Microsoft Enterprise Servers SPI on a Management Server" on page 17.
2. Select **Microsoft Enterprise Servers** to install.

Deploy Updated Instrumentation.

To enable the functioning of the new or updated policies, you must deploy the updated Microsoft Enterprise Servers SPI instrumentation. You can deploy instrumentation either on a group of nodes (if defined), or on individual nodes.

1. At the HPOM console, open **Operations Manager** → **Nodes.**
2. Right-click any node running the Microsoft Enterprise Server.
3. Select **All Tasks** → **Deploy instrumentation**.
4. From the Instrumentation Files area, select **SPI Data Collector**, **SHS Data Collector**, **BizTalk_Server**. **ISA_Server**, **MOSS_2k7**, **OCS**, **LS2010** (depending on your server environment setup), and click **OK**.
5. Repeat steps 1 through 4 as necessary for the remaining nodes which are running Microsoft Enterprise Servers.

Upgrading Microsoft Enterprise Servers SPI in an HPOM Cluster Environment

Before upgrading the Microsoft Enterprise Servers SPI in a cluster environment, make sure that HPOM for Windows 9.00 is installed on each system of the cluster.

> **Note:** The HPOM console does not function properly until you upgrade the Microsoft Enterprise Servers SPI on all nodes in the HPOM cluster.

At the first cluster-aware management server, select, and install Smart Plug-ins.

Complete the steps described in "Upgrading Microsoft Enterprise Servers SPI on a Standalone Management Server" on previous page before proceeding to the next management server.

> **Note:** Before beginning, be sure that sufficient disk space is available on each management server for the Microsoft Enterprise Servers SPI. Canceling the installation process before completion could result in partial installations and require manual removal of the partially installed components.

At the next cluster-aware management server, install pre-selected Smart Plug-ins.

Repeat the steps described in "Upgrading Microsoft Enterprise Servers SPI on a Standalone Management Server" on previous page on each management server in the cluster and continue to every management server (as was defined in the HP Operations Manager cluster installation) until you have finished.

Note: The HPOM console does not function properly until installations are completed on all the nodes in the cluster.

Verifying Installation/Upgrade of Microsoft Enterprise Servers SPI

To verify the Microsoft Enterprise Servers SPI is installed/upgraded properly check any one of the following:

To verify the installation of the Microsoft Enterprise Servers SPI, follow these steps:

1. Check if the **%ovinstalldir%\install\MSESSPI** directory is created.
2. In the HPOM console tree, click **Policy Management** →**Policy Group**. Check whether **SPI for Microsoft Enterprise Servers** is listed under the policy group. Depending on your environment setup, you can further expand SPI for Microsoft Enterprise Servers and check whether the Microsoft Enterprise Servers - BizTalk Server 2006, BizTalk Server 2010, Internet Security and Acceleration Server 2006, Microsoft Lync Server 2010, Microsoft Office Communication Server 2007, Microsoft Lync Server 2013, Microsoft SharePoint Server 2013 are listed in the policy group.
3. Verify that Lync Server 2013 and SharePoint Server 2013 policy version is 8.500. Policy versions of all other Microsoft Enterprise servers do not change.

Migrating Microsoft Enterprise Servers SPI from Previous Versions

For information about migrating the Microsoft Enterprise Servers SPI from the previous versions to the latest Microsoft Enterprise Servers SPI version, see *HP Operations Smart Plug-ins DVD Release Notes.*

Chapter 3

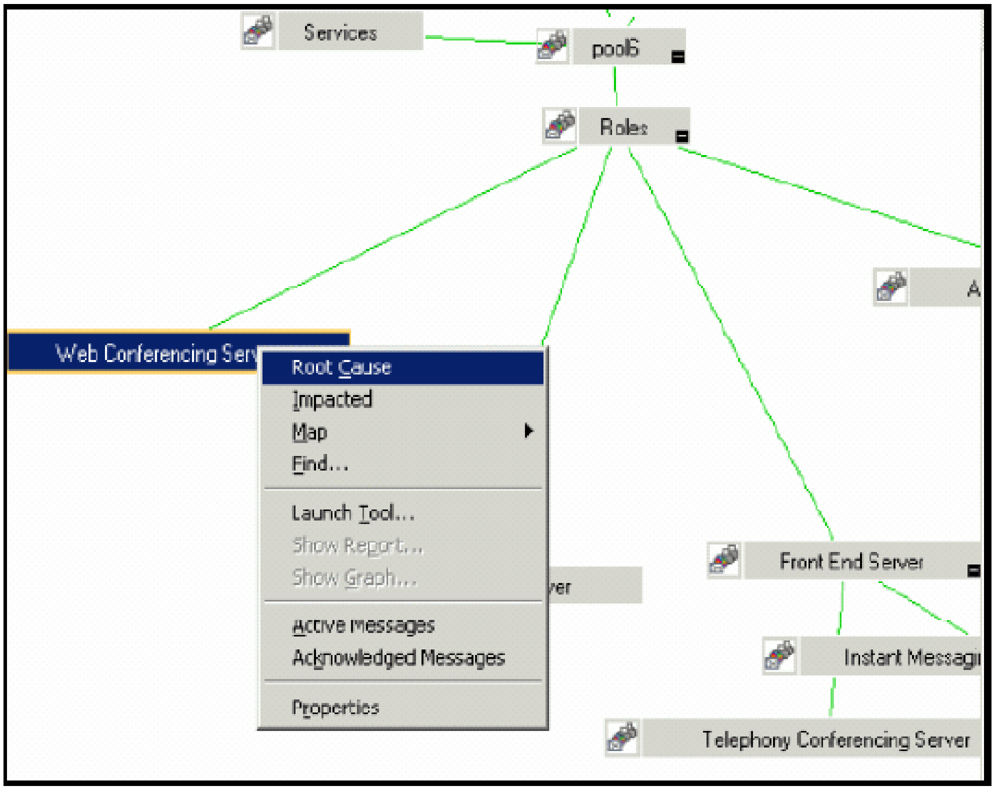
Configuring the Microsoft Enterprise Servers SPI

The SPI monitors the Microsoft Enterprise Servers by discovering the existing servers (BizTalk, Internet Security and Acceleration, SharePoint Portal, and Microsoft Office Communications Server) in your environment and maintaining the thresholds set by the policies. The Microsoft Enterprise Servers SPI expands that discovery and adds multiple hierarchical levels of details to each server.

The service map identifies the Microsoft Enterprise Servers. You can drill down each component of each existing server and find the root cause.

To find the origin of the problem, right-click the service in the service map where the alert occurs (indicated by the red color), and select **Root Cause**.

Root Cause



Basic Configuration Procedure

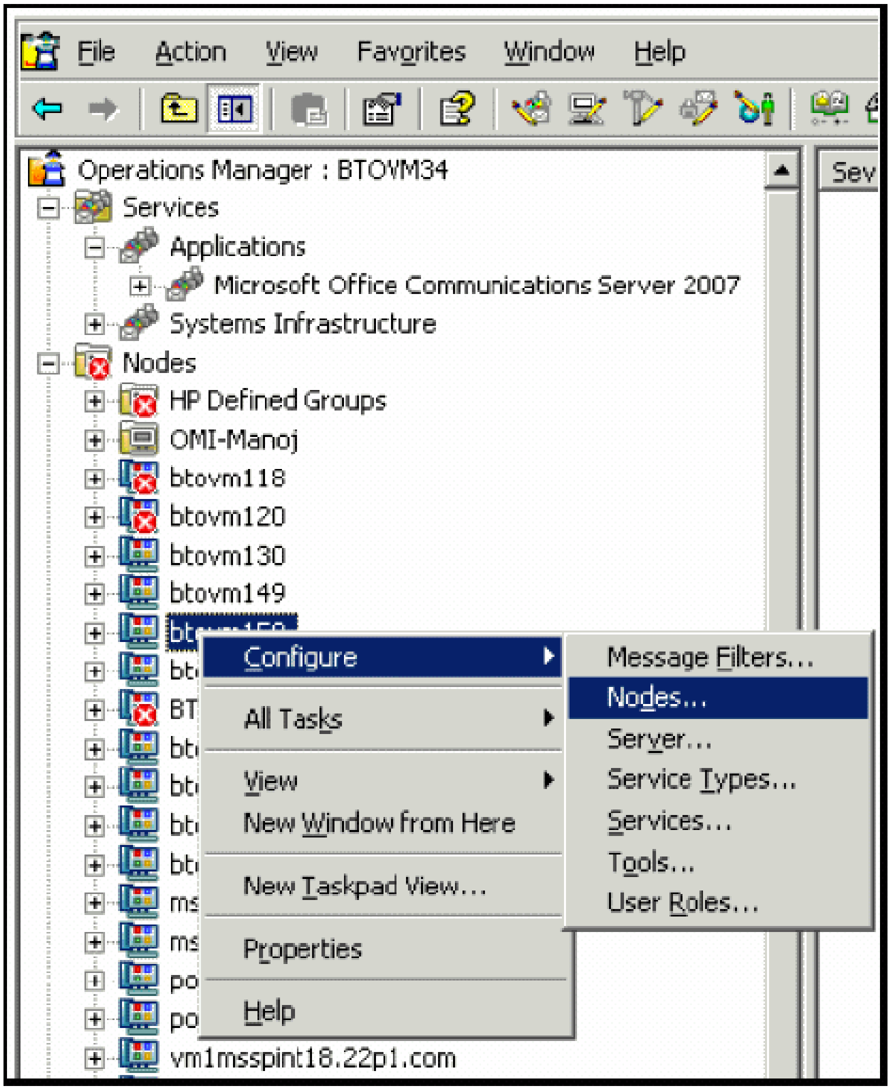
Perform the following tasks for all the Microsoft Enterprise Servers SPI in your environment.

Deploy the discovery policies to discover or detect the existing services and components of the Microsoft Enterprise Servers environment in the managed nodes. Deploying these policies launches an automated process that adds the discovered services to the HPOM service tree and service map.

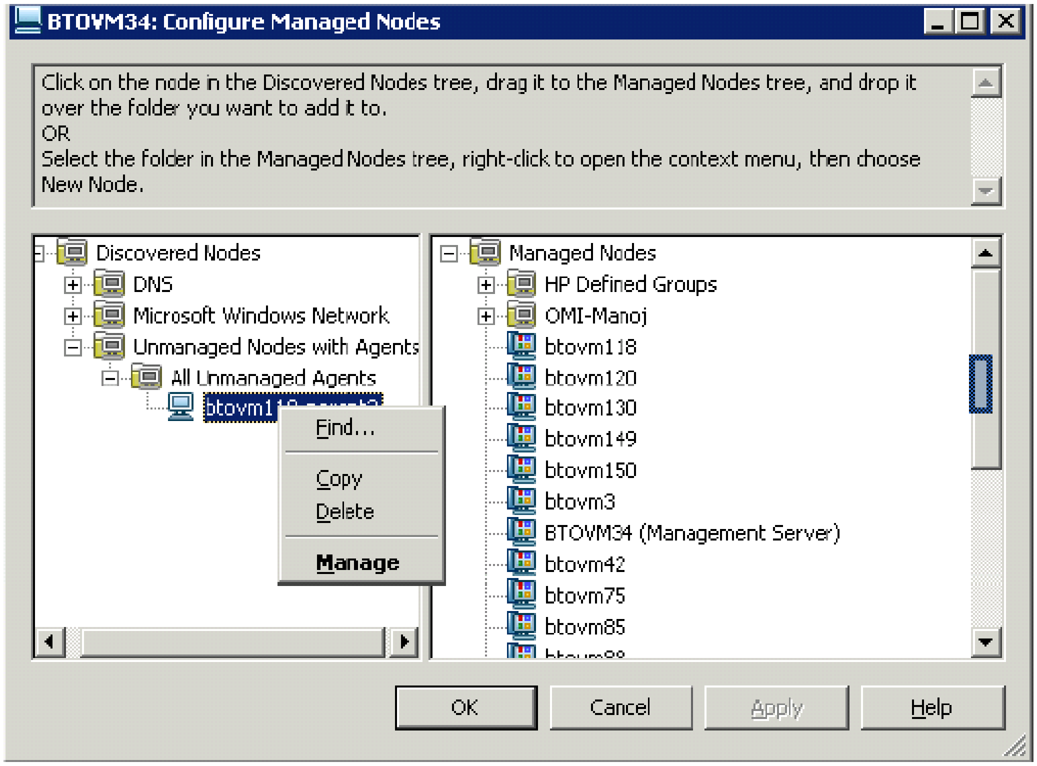
Change Unmanaged Nodes to Managed Nodes

To change unmanaged node to a managed node, add the nodes to the HPOM console's nodes folder.

1. In the HPOM console, right-click **Nodes**, and select **Configure** →**Nodes**.



2. In the **Configure Managed Nodes** box, add the unmanaged nodes to the **Nodes** using any of the following methods:
3. In the left pane double-click each node you want to add.
4. Drag and drop nodes from left to right.
5. In the left pane, right-click each node, and then select **Manage**.



BTOVM34: Configure Managed Nodes

Click on the node in the Discovered Nodes tree, drag it to the Managed Nodes tree, and drop it over the folder you want to add it to.
OR
Select the folder in the Managed Nodes tree, right-click to open the context menu, then choose New Node.

6. (Optional) If a system running the HP Operations agent software is not available in the discovered nodes folder in the left pane, in the details pane right-click **Nodes**, select **New Node,** and then type the system name and other relevant information, and then click **OK**.

Deploy Instrumentation Categories on Managed Nodes

Deploy the instrumentation categories to the Microsoft Enterprise Servers SPI on the managed nodes. To deploy the instrumentation, perform the following steps:

1. In the HPOM console, right-click a node and select **All Tasks**. Select **Deploy instrumentation.... The Deploy Instrumentation box opens.**
2. Select the mandatory instrumentation categories, **SPI Data Collector** and **SHS Data Collector** categories.

3. Select **BizTalk_Server**, **ISA_Server**, **MOSS_2k7**, **OCS**, **LS2010** (depending on your server environment setup), and click **OK**.
4. Perform steps 1 and 2 for all the Microsoft Enterprise Servers SPI managed nodes.

Create Data Sources

> **Note:** Before creating data sources, discover the services of the Microsoft Enterprise Servers SPI. For this, complete the steps in "Additional Configuration Procedure for Office Communication Server" on page 35.

The Microsoft Enterprise Servers SPI collects metric data on the managed nodes, and logs the data to a data store on the managed nodes. By default, the SPI stores the data in the embedded performance component, also known as CODA of the HP Operations agent.

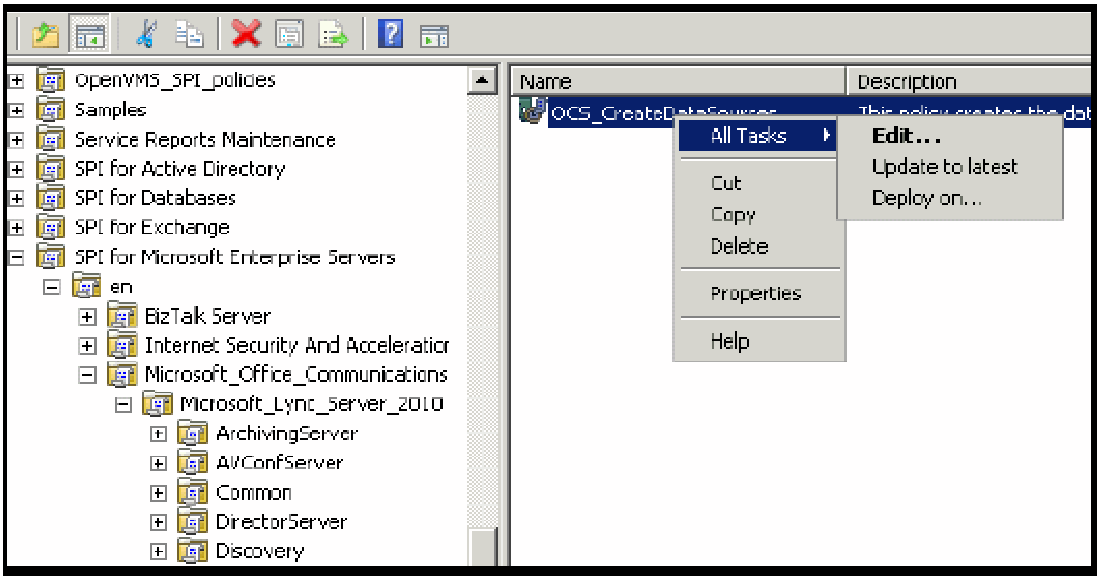
Deploy the Create Data Sources policy for each Microsoft Enterprise Servers SPI to create the required data sources in the data store.

> **Note:** BizTalk Server, ISA Server, and Microsoft Lync Server 2010 use tools to create data sources on the managed nodes. See "Using Tools" on page 55 for more information.

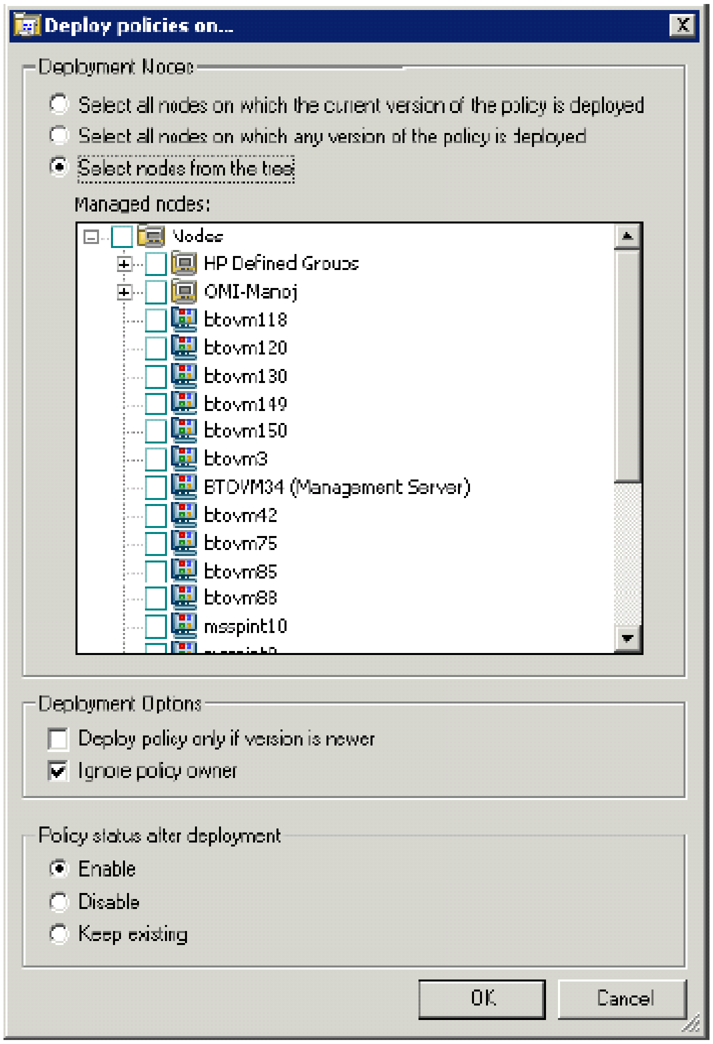
> **Note:** For the Microsoft Office Communications Server 2007, you must deploy the OCS_CreateDataSources policy to create data sources manually whereas for Internet Security and Acceleration Server 2006 there is no specific policy to create data sources. Data source is automatically created after you manual deploy the policies.

To deploy the Create Data Sources policy:

1. In the HPOM console, click **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft_Office_Communications_Server** → **Microsoft_Office_Communications_Server_2007** → **Configuration**.
2. Right-click Configuration, and select **All Tasks** → **Deploy on....**. A windows lists all the managed nodes.



3. Select one or more managed nodes on which you want to deploy the OCS_CreateDataSources policy, and then click **OK**. The policy is deployed on the selected managed nodes.



Deploy policies on...

Deployment Nodes

○ Select all nodes on which the current version of the policy is deployed
○ Select all nodes on which any version of the policy is deployed
● Select nodes from the tree

Managed nodes:

- □ Nodes
  - □ HP Defined Groups
  - □ OMI-Manoj
  - □ btovm118
  - □ btovm120
  - □ btovm130
  - □ btovm149
  - □ btovm150
  - □ btovm3
  - □ BTOVM34 (Management Server)
  - □ btovm42
  - □ btovm75
  - □ btovm85
  - □ btovm88
  - □ msspint10

Deployment Options

□ Deploy policy only if version is newer
☑ Ignore policy owner

Policy status after deployment

● Enable
○ Disable
○ Keep existing

Editing Discovery Policies

Before deploying the Discovery policies, you must to edit the discovery policies.

BizTalk_Discovery

This policy discovers the systems infrastructure of the BizTalk Server 2006 in the environment. This policy requires BizTalk administrator privileges, local administrator privileges, and privileges to access all the databases.

BTS_Discovery

This policy discovers the systems infrastructure of the BizTalk Server 2010 in the environment. This policy requires BizTalk administrator privileges, local administrator privileges, and privileges to access all the databases.

BTS_Cluster_Re_Discovery

The BTS_Cluster_Re_Discovery policy updates the service map when a cluster failover occurs.

For more information about editing the discovery policies for BizTalk Server 2006 and BizTalk Server 2010, see "Additional Configuration Procedure for Microsoft Enterprise Servers SPI for BizTalk Server 2006 and BizTalk Server 2010" on page 30

LS_Discovery

The LS_Discovery policy discovers the roles and services of the Microsoft Lync Server 2010, along with sites, pools, and pool members, and displays them in the service tree on the console of the management server.

The Microsoft Lync Server 2010 requires the following user privileges:

- CSViewOnlyAdministrator
- RTCUniversalReadOnlyAdminsw
- "Execute" permission to the %OvAgentDir%\bin\instrumentation folder on the managed node.

The Configure Edge server Discovery for Lync Server 2010 tool stores user information required to run the LS_Discovery policy on the Edge Server in an encrypted format. The SPI Discovery instrumentation reads the user information that is stored on the Edge Server.

For more information about editing the LS_Discovery policy, see "Additional Configuration Procedure for Microsoft Enterprise Servers SPI for Microsoft Lync Server 2010" on page 34

Microsoft Office SharePoint Server 2007 and OCS_ Discovery

These policies discover the application services of the Microsoft Office SharePoint Server 2007 and the Microsoft Office Communications Server 2007. These policies require SharePoint administrator and local administrator privileges and privileges to access the SharePoint databases. If the agent on the node is not running under the default Local System account, the OCS_Discovery policy should run as a user who is member of the RTCUniversalGuestAccessGroup group, if the node is a member of the OCS pool. For Edge Servers, provide the privileges of a Local Administrator. For more information about editing these policies, see "Additional Configuration Procedure for Office Communication Server" on page 35.

Customizing Policies

You can customize the policies, if required. To customize policies, follow these steps:

1. Right-click the policy and select **All Tasks**, and then **Edit**.
2. Click the **Thresholds level** (or **Rules**) or **Options** tab or both.
3. Click **Save and Close**.

> **Note:** If you choose to customize one or more policies after deploying them, ensure to redeploy the policies after customizing them. For information about customizing policies for BizTalk Server 2010, see "Customizing BizTalk Server 2010 Policies" on page 54

Deploy Manual-Deploy Policy Groups

The BizTalk Server 2006 and Microsoft Office SharePoint Server 2007 have auto-deploy policy groups. These policies are automatically deployed on the managed nodes on the respective server.

To manually deploy policy groups, follow these steps:

Note: The BizTalk Server 2006 and Microsoft Office SharePoint Server 2007 have auto-deploy policy groups. These policies are automatically deployed on the managed nodes on the respective server. The Microsoft Lync Server 2010 has manual-deploy policy groups. Deploy the Discovery and Common policies on all the nodes.

1. In the HPOM console, expand **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → <**Microsoft Enterprise Server**> → **<Policy Group>**. For example, **Internet Security and Acceleration Server 2007** → **Availability Monitoring**.

Note: For the BizTalk SPI policies, MSES_BizTalk_MessageBox_DatabaseSize and MSES_BizTalk_DTA_DatabaseSize, deployed *only* on the Microsoft BizTalk database nodes.

2. Right-click the <**Policy Group**>. Select **All Tasks** → **Deploy on...**. Deploy policies on... Window appears listing all the managed nodes.
3. Select one or more managed nodes on which you want the <**Policy Group**> to be deployed, and then click **OK**. The <**Policy Group**> is deployed on the selected nodes.
4. Perform steps 1 through 3 for all the remaining policy groups.

Note: Assign only those policy groups on the managed nodes which host the roles that the policy group is related to. For example if the managed node hosts the AccessEdge Enterprise Server, deploy only the AccessEdge Server policy group, and so on.

See the following table to deploy the specific policy group for the specific Microsoft Enterprise Server role.

Server and Policy Group

Server	Policy Group
BizTalk Server 2006	**Policy Management** → **Policy groups**→**SPI for Microsoft Enterprise Servers** →**en** →**BizTalk Server** → **Biztalk Server 2006**
BizTalk Server 2010	**Policy Management** →**Policy groups**→**SPI for Microsoft Enterprise Servers** → **en** →**BizTalk Server** → **Biztalk Server 2010**

Server	Policy Group
Internet Security and Acceleration Server	**Policy Management → Policy groups→SPI for Microsoft Enterprise Servers →en →Internet Security and Acceleration Server → Internet Security and Acceleration Server 2006**
Microsoft SharePoint Portal Server	**Policy Management → Policy groups→SPI for Microsoft Enterprise Servers →en →SharePoint Portal Server → Microsoft Office SharePoint Server 2007**
Microsoft Office Communications Server	**Policy Management →Policy groups→SPI for Microsoft Enterprise Servers → en →Microsoft_Office_Communications_Server → Microsoft_Office_Communications_Server_2007**
Microsoft Lync Server 2010	**Policy Management → Policy groups→SPI for Microsoft Enterprise Servers → en →Microsoft_Office_Communications_Server → Microsoft_Lync_Server_2010**

Deploy the following policy groups for all the managed nodes of *Microsoft Office Communications Server 2007* irrespective of the specific server role:

Discovery

Policy Management → Policy groups→SPI for Microsoft Enterprise Servers → en →Microsoft_Office_Communications_Server → Microsoft_Office_Communications_Server_2007 →Discovery

Configuration

Policy Management →Policy groups→SPI for Microsoft Enterprise Servers → en →Microsoft_Office_Communications_Server → Microsoft_Office_Communications_Server_2007 →Configuration

Others

Policy Management →Policy groups→SPI for Microsoft Enterprise Servers →en →Microsoft_Office_Communications_Server → Microsoft_Office_Communications_Server_2007 →Others

Data Logging Scenarios

If you use Performance Agent as the datastore, data source creation and data logging happens in Performance Agent, by default. There is no configuration required.

To create data sources and to log data into CODA, while Performance Agent is installed, follow these steps:

> **Note:** You do not need to perform the following steps for BizTalk Server 2010. The BTS 2010 create data source tool can be used to perform this operation. By default, this tool configures the BizTalk Server 2010 datasource in CODA. For more information, see "Using Policies and Tools" on page 53

1. Create a folder **dsi2ddf in the path %OvAgentDir%\Conf**, if it does not exist.
2. Create an empty file **nocoda.opt**.
3. Type the names of the other data sources *except* OCS, ISASERVER2006, MOSS_2007, MSES_BIZTALKSERVER_INTERVAL, BTS_DATA, and CS which are to be created and for which the data logging has to happen in Performance Agent into the file **nocoda.opt**.
4. The data sources OCS,ISASERVER2006, MOSS_2007, MSES_BIZTALKSERVER_INTERVAL, and CS are created and data logging happens in CODA.

> **Note:** It is mandatory to exclude CS, the name of the data source for Microsoft Lync Server 2010, from the **nocoda.opt** file as Microsoft Lync Server 2010 only supports data logging into CODA.

For more details on the data store (CODA) metrics and policy logging details, see *Microsoft Enterprise Servers SPI Online Help*.

Additional Configuration Procedure for Microsoft Enterprise Servers SPI for BizTalk Server 2006 and BizTalk Server 2010

The following section describes configuration procedures for Microsoft Enterprise Servers SPI for BizTalk Server 2006 and BizTalk Server 2010.

Using Discovery Policies

BizTalk_Discovery

This policy discovers the systems infrastructure of the BizTalk Server 2006 in the environment. This policy requires BizTalk administrator privileges, local administrator privileges and privileges to access all the BizTalk databases. You can specify the administrator privileges by editing the discovery policy. To edit the BizTalk_Discovery policy, follow these steps:

In the HPOM console tree, click **Policy Management** → **SPI for Microsoft Enterprise Servers** → **en** → **BizTalk Server** → **Biztalk Server 2006** → **Discovery**.

Double-click **BizTalk_Discovery**.

The BizTalk_Discovery window opens.

In the right pane, specify the user credentials.

Click **Save** and **Close**.

BTS_Discovery

This policy discovers the systems infrastructure of the BizTalk Server 2010 in the environment.This policy requires BizTalk administrator privileges, local administrator privileges and privileges to access all the BizTalk databases. You can specify the administrator privileges by editing the discovery policy. To edit the BTS2010_Discovery policy, follow these steps:

In the HPOM console tree, click **Policy Management** → **SPI for Microsoft Enterprise Servers** → **en** → **BizTalk Server** → **Biztalk Server 2010** → **Discovery**.

Double-click **BTS_Discovery**.

The BTS_Discovery window opens.

In the right pane, specify the user credentials.

Click **Save** and **Close**.

BTS_Cluster_Re_Discovery

This windows event log policy updates the server map with BizTalk Server 2010 entities operating in a cluster environment when a cluster fail over occurs. This policy should be deployed only on BizTalk Server 2010 nodes which are members of a cluster.

Using MSES_BTS_DB_Configuration Tool

You can use the MSES_BTS_DB_Configuration tool to configure the Microsoft Enterprise Servers SPI for BizTalk Server 2006 and BizTalk Server 2010.

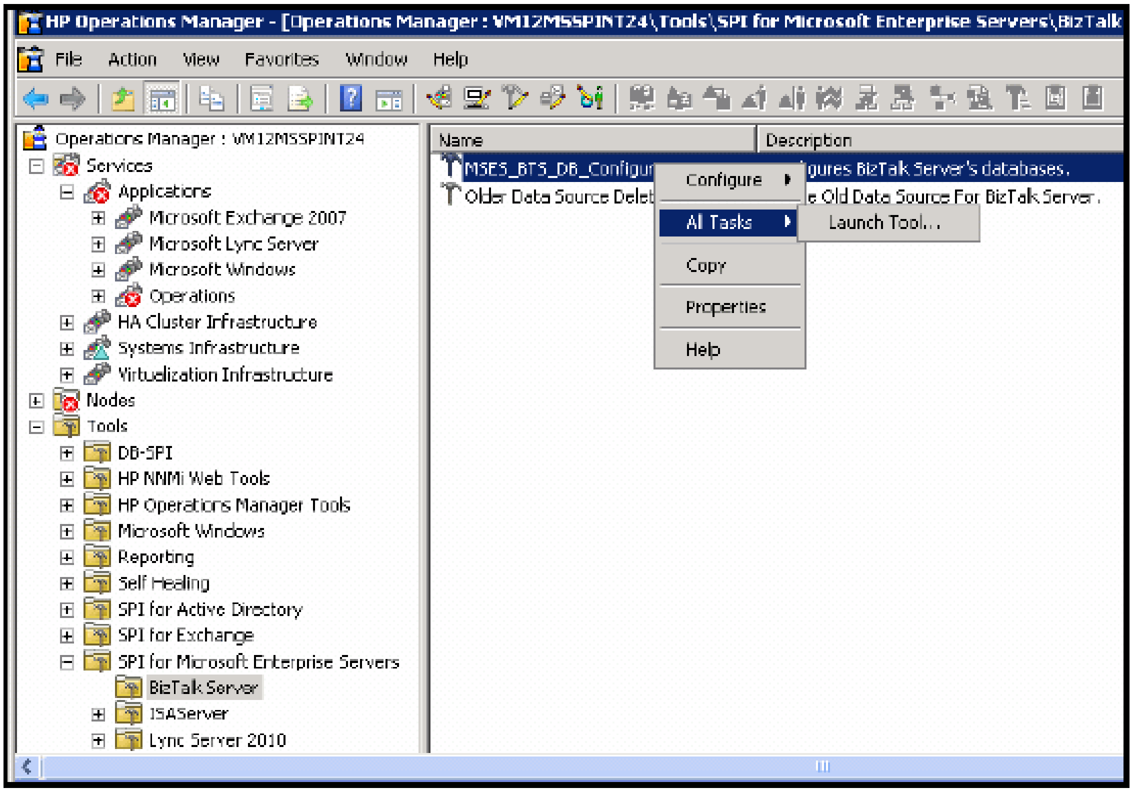
The BizTalk Server 2006 and 2010 stores data in SQL server instead of the WMI CIMV2 database. The Microsoft Enterprise Servers SPI must connect to the BizTalk Server’s SQL database to collect the related data it needs.

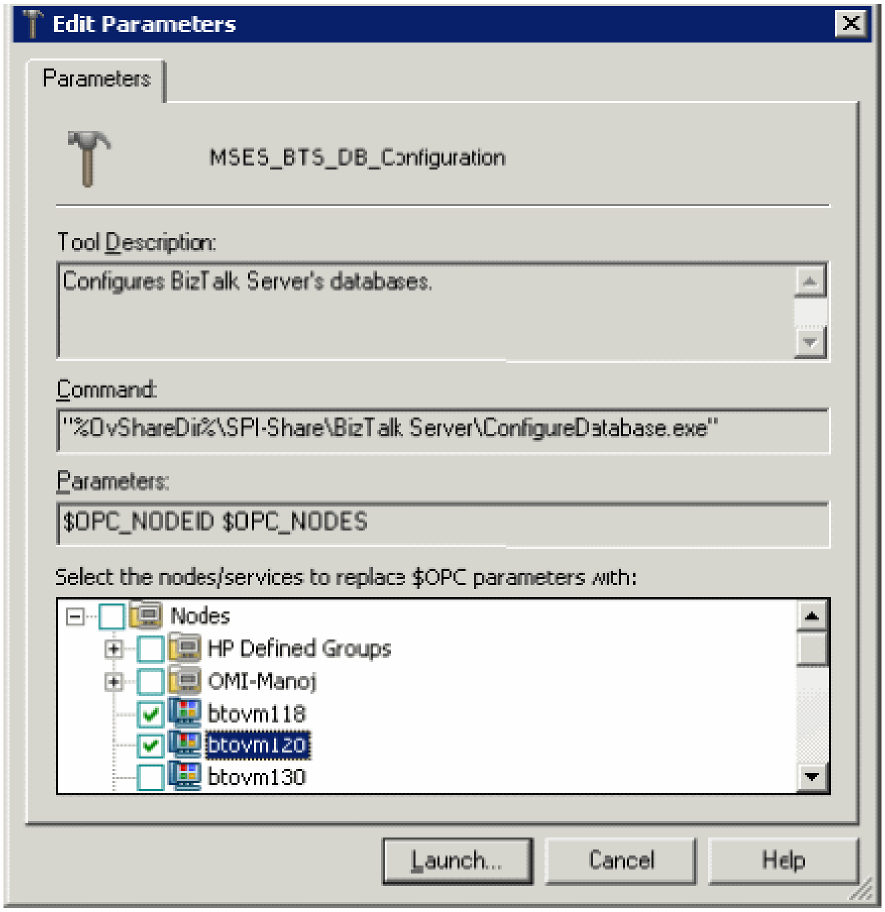
Before running Discovery, the HPOM administrator must configure the SQL database for all nodes with BizTalk Server installed. Windows integrated security (SSPI mode) does not work if the SQL authentication mode is set for SQL server. If SQL authentication is "users /", the HPOM console needs to know the SQL user name and password. To connect to SQL server even when it is in SQL authentication mode, the HPOM administrator can use the MSES_BTS_DB_Configuration tool to store the corresponding SQL server name, and the SQL user name and password. If this configuration is not done for BizTalk Server 2006 and 2010 nodes, the default SQL user name and password's value is considered.

Launching the MSES_BTS_DB_Configuration Tool

To launch the MSES_BTS_DB_Configuration tool:

1. In the HPOM console, click **Tools** → **SPI for Microsoft Enterprise Servers** → **BizTalk Server**.
2. Right-click the **MSES_BTS_ DB_Configuration** tool. Select **All Tasks**, and then **Launch Tool...**. The Edit Parameters window appears.


HP Operations Manager - [Operations Manager : VM12MSSPINT24\Tools\SPI for Microsoft Enterprise Servers\BizTalk
File
Action
View
Favorites
Window
Help
Operations Manager : VM12MSSPINT24
Services
Applications
Microsoft Exchange 2007
Microsoft Lync Server
Microsoft Windows
Operations
HA Cluster Infrastructure
Systems Infrastructure
Virtualization Infrastructure
Nodes
Tools
DB-SPI
HP NNMi Web Tools
HP Operations Manager Tools
Microsoft Windows
Reporting
Self Healing
SPI for Active Directory
SPI for Exchange
SPI for Microsoft Enterprise Servers
BizTalk Server
ISAServer
Lync Server 2010
Name
Description
MSES_BTS_DB_Configur
gures BizTalk Server's databases.
Older Data Source Delet
e Old Data Source For BizTalk Server.
Configure
All Tasks
Launch Tool...
Copy
Properties
Help



MSES_BTS_DB_Configuration

Tool Description: Configures BizTalk Server's databases.

Command: "%OvShareDir%\SPI-Share\BizTalk Server\ConfigureDatabase.exe"

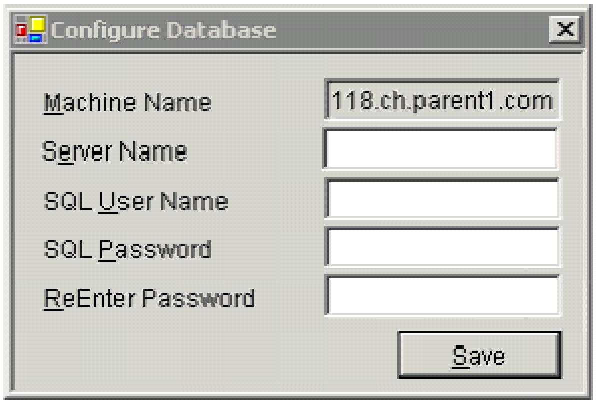
Parameters: $OPC_NODEID $OPC_NODES

Select the nodes/services to replace $OPC parameters with:

- □ Nodes
  - □ HP Defined Groups
  - □ OMI-Manoj
  - ☑ btovm118
  - ☑ btovm120
  - □ btovm130

3. Select one or more nodes where you want to configure BizTalk Server 2006 by launching the tool, and then click **Launch...**. A Configure Database window appears for each selected node.

4. The Machine Name field is read only. Type the Server Name (for BizTalk Database), SQL User Name and SQL password and confirm the password.



Machine Name: 118.ch.parent1.com

5. Save the configuration.

Additional Configuration Procedure for Microsoft Enterprise Servers SPI for Microsoft Lync Server 2010

The LS_Discovery policy discovers the roles and services of the Microsoft Lync Server 2010, along with sites, pools, and pool members, and displays them in the service tree on the console of the management server.

The Microsoft Lync Server 2010 requires the following user privileges:

- CSViewOnlyAdministrator
- RTCUniversalReadOnlyAdminsw
- "Execute" permission to the %OvAgentDir%\bin\instrumentation folder on the managed node.

The Configure Edge server Discovery for Lync Server 2010 tool stores user information required to run the LS_Discovery policy on the Edge Server in an encrypted format. The SPI Discovery instrumentation reads the user information that is stored on the Edge Server.

Configuring LS_Discovery Policy

To run the LS_Discovery policy on all servers, except the Edge Server, follow these steps:

1. Create a domain user to run the discovery policy with the following user privileges:
   - CSViewOnlyAdministrator
   - RTCUniversalReadOnlyAdmins

     "Execute" permission to the %OvAgentDir%\bin\instrumentation folder on the managed node.
2. Open the LS_Discovery policy.
3. Edit the username and password in the policy and enter the user credentials - CSViewOnlyAdministrator and RTCUniversalReadOnlyAdmins.
4. Deploy the policy on all Lync servers, except the Edge Server.

To run the LS_Discovery policy on the Edge Server, follow these steps:

1. Create a user under the CSViewOnlyAdministrator account.
2. Open the Edge Server configuration tool **Configure Edge server Discovery for Lync Server 2010.**
3. In the HPOM console, click **Tools →SPI for Microsoft Enterprise Servers →Lync Server 2010.**
4. Double-click the **Configure Edge server Discovery for Lync Server 2010** tool in the details pane.
5. Right Click **All Tasks →Launch Tool**
6. Select **Edge Sever**.

7. Click **Launch**.

   Fill in details Edge Server details, such as:

   Domain: < Lync Server domain name>

   User Name: <CSViewOnlyAdministrator>

   Password: <Password>

8. Click **OK.**
9. Run the tool. Information related to the Lync Server is deployed on the Edge Server.
10. Create another user on the Edge Server with the user privilege 'Local Administrator' for the Edge Server.
11. Open the LS_Discovery policy.
12. Edit the username and password in the policy and enter the user credentials of the 'Local Administrator' created on the `Edge`Server.

Additional Configuration Procedure for Office Communication Server

The following section describes configuration procedures for Microsoft Office SharePoint Server 2007 Discovery and OCS_Discovery Policies.

Configuring Microsoft Office SharePoint Server 2007 Discovery and OCS_Discovery Policies

These policies discover the application services of the Microsoft Office SharePoint Server 2007 and the Microsoft Office Communications Server 2007. These policies require SharePoint administrator and local administrator privileges and privileges to access the SharePoint databases. If the agent on the node is not running under the default Local System account, the OCS_Discovery policy should run as a user who is member of the RTCUniversalGuestAccessGroup group, if the node is a member of the OCS pool. For Edge Servers, provide the privileges of a Local Administrator.

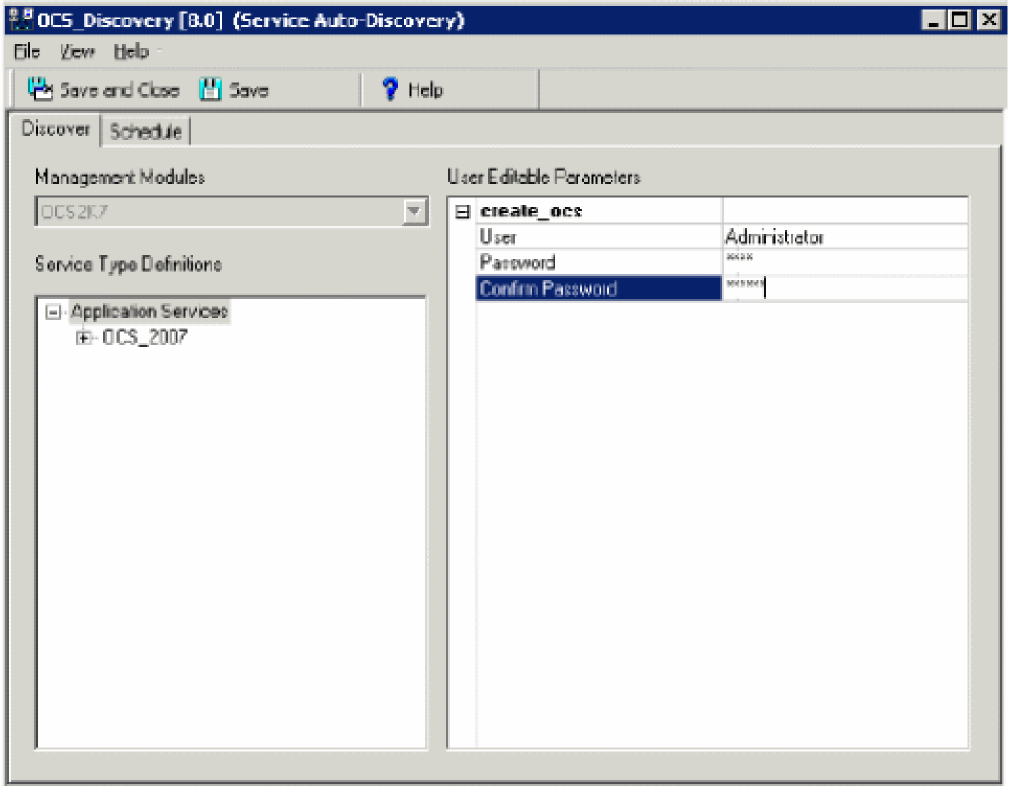
To edit the Discovery policy:

1. In the HPOM console, expand **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft_Office_Communications_Server** → **Microsoft_ Office_Communications_Server_2007** → **Discovery**.
2. Select the **OCS_Discovery** policy (on the right pane) and double-click to open the editor. The OCS_Discovery window appears with the **Discover** tab opened by default.
3. Type the user credentials and the password in the **User Editable Parameters** box. The username format for:

   DCE agent is domain\user

   HTTPS gent is domain\\user

4. Click **Save and Close**.



Management Modules

OCS 2K7

Service Type Definitions

- Application Services
  - OCS_2007

User Editable Parameters

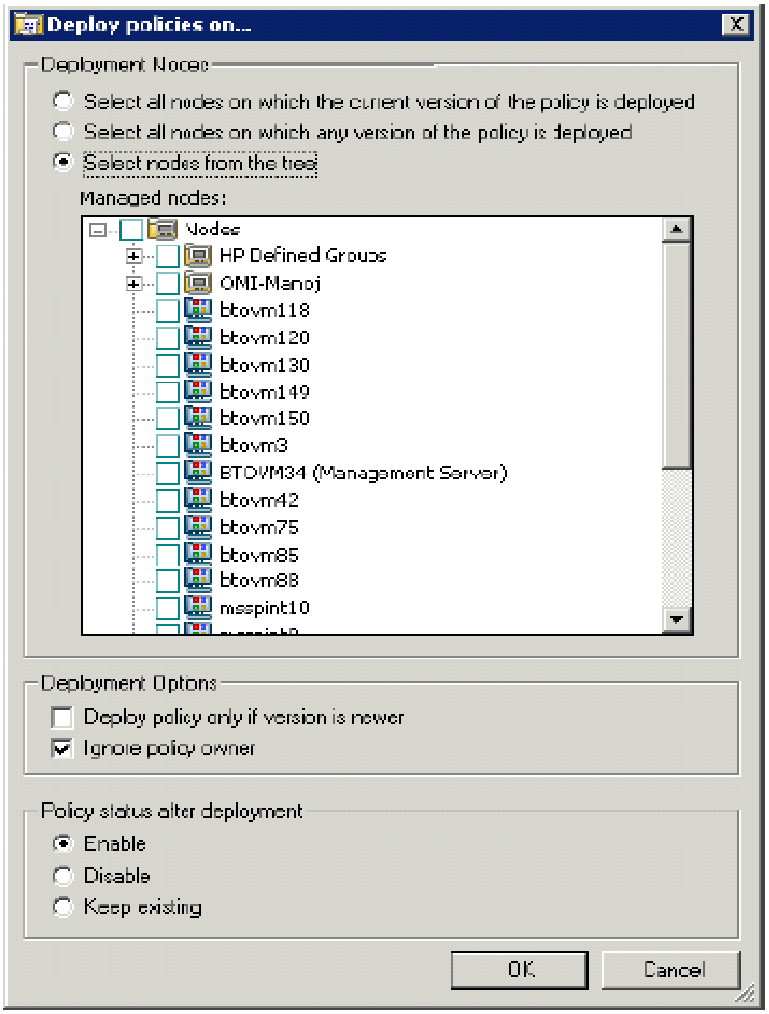
create_ocs	
User	Administrator
Password	****
Confirm Password	*****

5. Perform the same steps for the BizTalk_Discovery policy and Microsoft Office SharePoint Server 2007 Discovery policy.

Deploy Discovery Policy on Managed Nodes

Deploy the Discovery policy group for each Microsoft Enterprise Servers SPI on the managed nodes. To deploy the Discovery policy, follow these steps:

1. In the HPOM console, click **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → <**Microsoft Enterprise Server**> → **Discovery**.
2. Right-click **Discovery** of the respective Server, and select **All Tasks** →**Deploy on...**.
3. In the **Deploy policies on...** box, select one or more Microsoft Enterprise Servers nodes, and click **OK**. The Discovery policy of the <Microsoft Enterprise Server> is deployed on the selected nodes.



Deploy policies on...

Deployment Nodes

○ Select all nodes on which the current version of the policy is deployed
○ Select all nodes on which any version of the policy is deployed
● Select nodes from the tree

Managed nodes:

- □ Nodes
  - □ HP Defined Groups
  - □ OMI-Manoj
  - □ btovm118
  - □ btovm120
  - □ btovm130
  - □ btovm149
  - □ btovm150
  - □ btovm3
  - □ BTOVM34 (Management Server)
  - □ btovm42
  - □ btovm75
  - □ btovm85
  - □ btovm88
  - □ msspint10

Deployment Options

□ Deploy policy only if version is newer
☑ Ignore policy owner

Policy status after deployment

● Enable
○ Disable
○ Keep existing

4. To view the deployment, under the **Policy Management**, right-click **Deployment jobs**, select **New Window from Here.** From the menu, select **Window** →**Tile Horizontally**.

5. In the tiled window, you can see the executed processes of the <Microsoft Enterprise Server> services discovered and the service map updated.

6. Starting at the **Services** →**Systems Infrastructure** (for BizTalk Server 2006) and **Application Services** (for Microsoft Office SharePoint Server 2007) of the console tree (in the left pane), you can navigate downward to each component, under which you can see a **Services** folder.

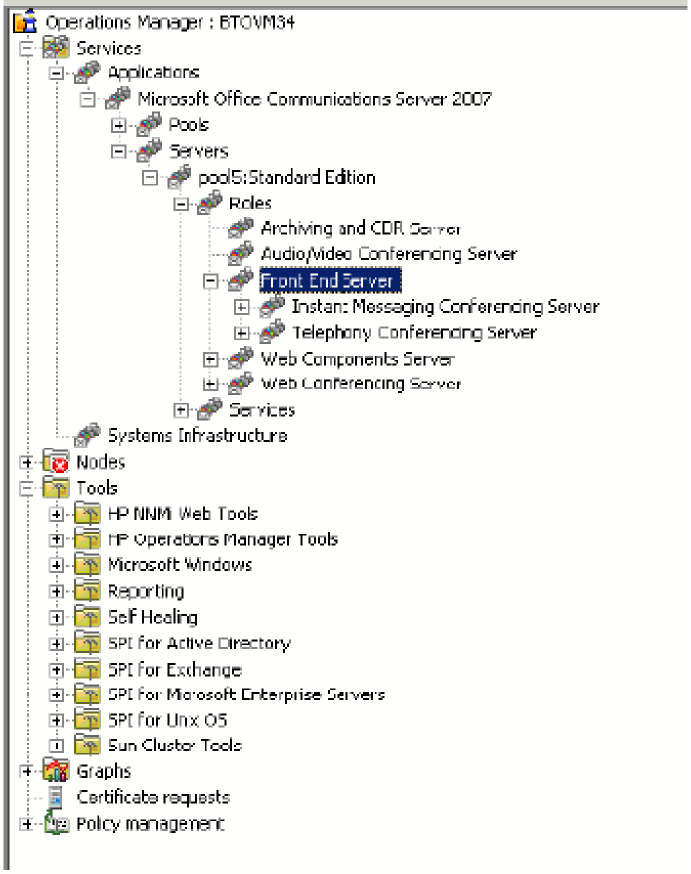
View Service Map

After running the discovery policy, you can see the discovered services graphically represented under the **<Microsoft Enterprise Server>** in the HPOM service map.

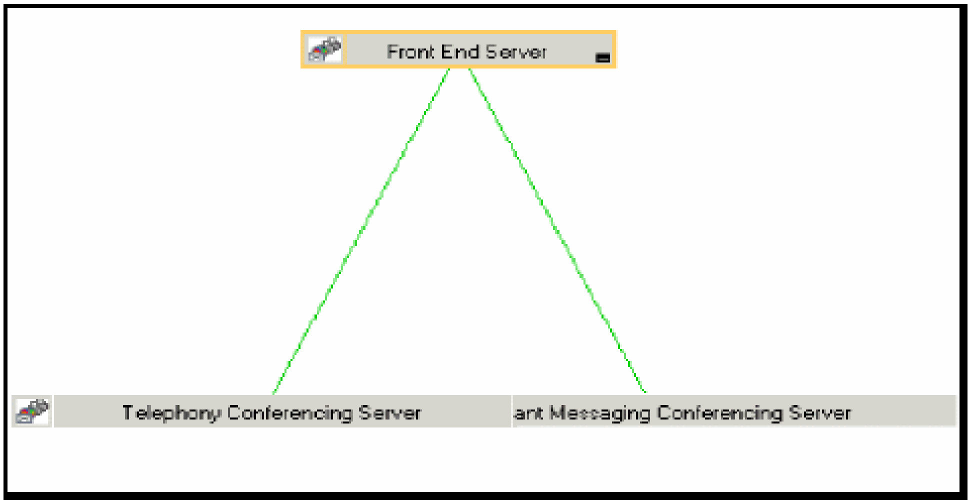
1. In the HPOM console, select **Services** →**Applications** / **Systems Infrastructure**.

2. Select the <**Microsoft Enterprise Server>**.

3. Expand the respective component (servers or roles) in the left pane to make it visible in the service map in the right pane.



- Operations Manager : BTOVM34
  - Services
    - Applications
      - Microsoft Office Communications Server 2007
        - Pools
        - Servers
          - pool5:Standard Edition
            - Roles
              - Archiving and CDR Server
              - Audio/Video Conferencing Server
              - Front End Server
                - Instant Messaging Conferencing Server
                - Telephony Conferencing Server
              - Web Components Server
              - Web Conferencing Server
            - Services
    - Systems Infrastructure
  - Nodes
  - Tools
    - HP NNM Web Tools
    - HP Operations Manager Tools
    - Microsoft Windows
    - Reporting
    - Self Healing
    - SPI for Active Directory
    - SPI for Exchange
    - SPI For Microsoft Enterprise Servers
    - SPI for Unix OS
    - Sun Cluster Tools
  - Graphs
  - Certificate requests
  - Policy management


Front End Server
Telephony Conferencing Server
ant Messaging Conferencing Server

Chapter 4

Configuring the Microsoft Enterprise Servers SPI (2013)

The Microsoft Enterprise Servers SPI helps you to manage the Microsoft Enterprise Servers in your environment. The Microsoft Enterprise Servers SPI informs you about the conditions related to the following Microsoft Enterprise Servers:

- Microsoft Lync Server 2013
- Microsoft SharePoint Server 2013

Configuring the Microsoft Lync Server

To configure Microsoft Enterprise Servers SPI with Microsoft Lync Server, complete the following tasks:

1. Deploy Instrumentation
2. Run Tools
3. Deploy Discovery Policy
4. Configure Collections and Metrics
5. Deploy Schedule Task Policies
6. Deploy Measurement Threshold Policies
7. Deploy Event Log Policies

Deploy Instrumentation

Deploy the following Microsoft Lync Server instrumentation categories to the Microsoft Lync Server 2013 nodes:

- MS_Core
- SPIDataCollector
- SHS_Data_Collector
- LS2013

For more information about deploying instrumentation, see Deploy Instrumentation Categories on Managed Nodes.

Run Tools

Run the following Microsoft Lync Server tools on Microsoft Lync Server nodes:

- **Create Datasource for Lync Server**

  Tools -> SPI for Microsoft Enterprise Servers → Lync Server → Create Datasource for Lync Server

> **Note:** Create DataSource for Lync Server tool creates data sources in PA.

To create data sources in CODA, follow these steps:

1. Run the following command on node to delete the datasource created in PA.

   ```
   ddfutil "%OVAgentDir%bin\LYNC\dsi\log\LYNC.log" -rm all
   ```

2. Create `nocoda.opt` file on node at the following location:

   ```
   %ovdatadir%/conf/dsi2ddf
   ```

3. Launch the tool.

- **Configure Edge server Discovery for Lync Server**

  Tools -> SPI for Microsoft Enterprise Servers → Lync Server → Configure Edge server Discovery for Lync Server

> **Note:** Run this tool only on Edge Server.

For more information about Configure Edge server Discovery for Lync Server, see Configuring LS_ Discovery Policy

Deploy Discovery Policy

Deploy Microsoft Lync Server discovery policy on the managed node.

- **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft_Office_Communications_Server → Microsoft_Lync_Server_2013 → Discovery → Microsoft Lync Server Discovery**

For more information about deploying Discovery Policy, see Deploy Discovery Policy on Managed Nodes.

Configure Collections and Metrics

Collections and metrics enables you to configure the Microsoft Lync Server SPI to monitor different aspects of Microsoft Lync Server 2013. You can enable or disable the collections, configure the collection schedule, configure the collections to raise alarm in case of threshold violation, and create custom collections based on your monitoring requirements.

This section explains how to configure Microsoft Lync Server collections.

Enabling and Disabling Collections

To enable or disable Lync Server collections, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013 → Configuration**

   The LYNC_MetricDefinition policy appears.

2. Double-click **LYNC_MetricDefinition**.

   The LYNC_MetricDefinition policy editor opens and lists the collections.

3. Select the collection you want to edit and set the value of enabled to `true` or `false` to enable or disable the collection.

   For example, set `enabled= "true"` to enable the collection or `enabled= "false"` to disable the collection.

4. Click **Save and Close**.

Changing Schedule of a Collection

To change the schedule of Microsoft Lync Server collection, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013 → Configuration**

   The LYNC_CollectionSchedule policy appears.

2. Double-click **LYNC_CollectionSchedule**.

   The LYNC_CollectionSchedule policy editor opens and lists the collections and schedules.

3. Select the collection you want to edit and set the value of schedule parameter to `Very High` or `High` according to your requirement.

   For example, `schedule= "High"` to set collection schedule as high.

4. Click **Save and Close**.

Changing Frequency of Schedule Task Policy

To change frequency of a schedule task policy, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013**

2. Select the schedule task policy from the appropriate policy group.

3. Double-click the appropriate schedule task policy.

   The schedule task policy editor window opens.

4. From the policy editor window, select **Schedule** tab.

   Schedule tab opens and lists Schedule task, Time and Schedule Summary options.

5. Select appropriate option from the Schedule Task drop-down list as per your requirement.

   For example, select `Every hour` if you want to run the related collection every hour.

> **Note:** You can also change the frequency to a specific time, multiple times or intervals using the available options.

6. Click **Save and Close**.

Enabling and Disabling Collection Alarms

To enable or disable Collection Alarms, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013 → Configuration**

   The LYNC_MetricDefinition policy appears.

2. Double-click **LYNC_MetricDefinition** policy.

   The LYNC_MetricDefinition policy editor opens and lists the collections.

3. Select the metric in the collection you want to edit and set the value of `alarm` parameter to `true` or `false` to enable or disable the alarm.

   For example, `set alarm = "true"` to enable alarm.

4. Click **Save and Close**.

Adding New Collection

To create a new Microsoft Lync Server collection entry, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013 → Configuration**

   The LYNC_MetricDefinition policy appears.

2. Double-click **LYNC_MetricDefinition** policy.

   The LYNC_MetricDefinition policy editor opens and lists the collections.

3. From the LYNC_MetricDefinition policy, copy and paste any existing collection with source as per your requirement.

> **Note:** Collection parameters are enclosed within the `<collection></collection>` block.

4. To edit the collection, follow these steps:
   a. Type the collection name and ID.

      For example: `Collection name="LYNC_Custom Collection" id="LYNC_C10070"`

   b. Edit the table parameter and provide the collection name in the given format:

      ```
      table="LYNC_CUSTOMCOLL"
      ```

> **Note:** Table parameter is required only if you want to log data. Remove the table parameter from the collection block if you do not want to log data.

c. Edit the `<Command>` parameter and provide object name.

   For example, `<Command>Perfmon Object Name</Command>`

d. Edit `<Field>` parameter and provide Instance Name and Counter Name. Fields parameter is enclosed within the `<Fields></Fields>` block.

   For example:

```
<Fields>

<Field>Instance_Name</Field>

<Field>Counter_Name 1</Field>

</Fields>
```

e. Edit the Metric id, name, position, and category of the metrics in the collection.

   For example:

   Metric with Category as KEY;

```
<Metric id="LYNC_M17001" name="LYNC_MyCustomInstance"
alarm="false" formulae="value" position="1" category="KEY">
```

   Metric with category as METRIC;

```
<Metric id="LYNC_M17002" name="LYNC_Counter_1_Value"
alarm="true" formulae="value" position="4" category="METRIC">
```

f. Edit the `<AlarmDef>` block to configure alarm or alert for the metrics.

   For example:

```
<AlarmDef>

<Policy>LYNC_Counter_1_Value</Policy>

<Object>

<MetricId>LYNC_M10101</MetricId>

</Object>

<Options>

<Option>

 <Name>ServiceName</Name>

<Value>

<MetricId>LYNC_M17001</MetricId>

</Value>

</Option>
```

```
<Option>

<Name>ServiceStatus</Name>

<Value>

<MetricId>LYNC_M17002</MetricId>

</Value>

</Option>

</Options>

</AlarmDef>
```

g. From the policy editor window, click **Save and Close**.

5. To add Collection Schedule:
   a. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013 → Configuration**

      The LYNC_CollectionSchedule policy appears.

   b. Double-click **LYNC_CollectionSchedule** policy.

   c. Add new collection in the format as shown in the following example:

      For example, `<Collection name="LYNC_CustomColl" id="LYNC_C10070" schedule="HIGH" role="|Edge Server|" />`

   d. From the policy editor window, click **Save and Close**.

6. To create a spec file to log the collected metric:

   Note: Spec file is required only if you want to log data.

   a. From the Instrumentation folder, rename default spec file.

   b. Edit the spec file. Give values to the following parameters:

      `spec file name, class, label, and counter name`

      For example:

```
LYNC_CUSTOMCOLL.spec

# DATASOURCE = LYNC_DATA

CLASS LYNC_CUSTOM = 10002

LABEL "LYNC_CUSTOM";

METRICS

COUNTER_1 = 10201

# COUNTER_1_LENGTH CODA_DATATYPE = UINT64

#  COUNTER_1_LENGTH CODA_CATEGORYTYPE = GAUGE
```

```
Label "COUNTER_1"

PRECISION 0;

TYPE TEXT LENGTH 256;

COUNTER_2 = 10202

# COUNTER_2_LENGTH CODA_DATATYPE = UINT64

#  COUNTER_2_LENGTH CODA_CATEGORYTYPE = GAUGE

Label "COUNTER_2"

PRECISION 0;
```

7. Click **Save and Close**.
8. Run **Create Datasource for Lync Server** tool. The class specified in the spec file is added to DataSource.
9. Deploy the updated policies to activate the collections.

Create Measurement Threshold Policy

Create measurement threshold policy for generating alerts. To create measurement threshold policy, follow these steps:

1. From the HPOM console, go to **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft Office Communications Server** → **Microsoft Lync Server 2013**
2. **Copy** and paste any measurement threshold policy as per your requirement.

   > **Note:** A sample policy for each role of Lync Server is provided with the Microsoft Enterprise Servers SPI.

3. Right-click the policy and select **All Tasks -> Edit...**
4. Provide the metric name as policy name.

   For example, `LYNC_Counter_1_Value`
5. From the policy editor window, click **Save and Close**.

Deploy Schedule Task Policies

Deploy Microsoft Lync Server schedule task policies on the managed node. You must select the appropriate schedule task policy based on the roles supported by the Microsoft Lync Server 2013.

Policy Location: Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013

Deploy Measurement Threshold Policies

Deploy Microsoft Lync Server measurement threshold policies. You must select the appropriate measurement threshold policy based on the roles supported by the Microsoft Lync Server 2013.

Policy Location: Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013

Deploy Event Log Policies

Deploy Microsoft Lync Server Event log policies if you want to monitor Lync Server events logs.

Policy Location: Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → Microsoft Office Communications Server → Microsoft Lync Server 2013

Configuring the Microsoft SharePoint Server

To configure Microsoft Enterprise Servers SPI with Microsoft SharePoint Server, complete the following tasks:

1. Deploy Instrumentation
2. Run Tools
3. Deploy Discovery Policy
4. Configure Collections and Metrics
5. Deploy Schedule Task Policies
6. Deploy Measurement Threshold Policies
7. Deploy Event Log Policies

Deploy Instrumentation

Deploy the following Microsoft SharePoint Server instrumentation categories to the Microsoft Enterprise Servers 2013 nodes:

- MS_Core
- SPIDataCollector
- SP2013

For more information about deploying instrumentation, see Deploy Instrumentation Categories on Managed Nodes.

Run Tools

Run the following Microsoft SharePoint Server tool on Microsoft SharePoint Server 2013 nodes:

- **Create Datasource for Sharepoint Server**

  Tools → SPI for Microsoft Enterprise Servers → Sharepoint Server Tools → Create Datasource for Sharepoint Server

Note: Create DataSource for Sharepoint tool creates data sources in PA.

To create data sources in CODA. follow these steps:

1. Run the following command on node to delete the datasource created in PA.

   ```
   ddfutil "%OVAgentDir%bin\Sharepoint\dsi\log\Sharepoint.log" -rm all
   ```

2. Create `nocoda.opt` file on node at the following location:

   ```
   %ovdatadir%/conf/dsi2ddf
   ```

3. Launch the tool.

Deploy Discovery Policy

Deploy Microsoft SharePoint Server discovery policy on the managed node.

- *Policy Location:* **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013 → Discovery --> SharePoint2013_Discovery**

For more information about deploying Discovery Policy, see Deploy Discovery Policy on Managed Nodes.

Configure Collections and Metrics

Collections and metrics enables you to configure the Microsoft SharePoint Server SPI to monitor different aspects of Microsoft Enterprise Server 2013. You can enable or disable the collections, configure the collection schedule, configure the collections to raise alarm in case of threshold violation, and create custom collections based on your monitoring requirements.

This section explains how to configure Microsoft Sharepoint Server collections.

Enabling and Disabling Collections

To enable or disable Microsoft SharePoint Server collections, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013 → Configuration**

   The SharePoint_MetricDefinition policy appears.

2. Double-click **SharePoint_MetricDefinition**.

   The SharePoint_MetricDefinition policy editor opens and lists the collections.

3. Select the collection you want to edit and set the value of enabled to `true` or `false` to enable or disable the collection.

   For example, set `enabled= "true"` to enable the collection or `enabled= "false"` to disable the collection.

4. Click **Save and Close**.

Changing Schedule of a Collection

To change the schedule of Microsoft SharePoint Server collection, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013 → Configuration**

   The SharePoint_CollectionSchedule policy appears.

2. Double-click **SharePoint_CollectionSchedule**.

   The SharePoint_CollectionSchedule policy editor opens and lists the collections and schedules.

3. Select the collection you want to edit and set the value of schedule parameter to `Very High`, or `High` according to your requirement.

   For example, `schedule= "High"` to set collection schedule as high.

4. Click **Save and Close**.

Changing Frequency of Schedule Task Policy

To change frequency of a schedule task policy, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013**

2. Select the schedule task policy from the appropriate policy group.

3. Double-click the appropriate schedule task policy.

   The schedule task policy editor window opens.

4. From the policy editor window, select **Schedule** tab.

   Schedule tab opens and lists Schedule task, Time and Schedule Summary options.

5. Select appropriate option from the Schedule Task drop-down list as per your requirement.

   For example, select `Every hour` if you want to run the related collection every hour.

6. Click **Save and Close**.

> **Note:** You can also change the frequency to a specific time, multiple times or intervals using the available options.

Enabling and Disabling Collection Alarms

To enable or disable Collection Alarms, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013 → Configuration**

   The SharePoint_MetricDefinition policy appears.

2. Double-click **SharePoint_MetricDefinition**.

   The SharePoint_MetricDefinition policy editor opens and lists the collections.

3. Select the metric in the collection you want to edit and set the value of `alarm` parameter to

`true` or `false` to enable or disable the alarm.

For example, set `alarm = "true"` to enable alarm.

4. Click **Save and Close**.

Adding New Collection

To create a new Microsoft SharePoint Server collection entry, follow these steps:

1. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013 → Configuration**

   The SharePoint_MetricDefinition policy appears.

2. Double-click **SharePoint_MetricDefinition**.

   The SharePoint_MetricDefinition policy editor opens and lists the collections.

3. From the SharePoint_MetricDefinition policy, copy, and paste any existing collection with source as per your requirement.

   > **Note:** Collection parameters are enclosed within the `<collection></collection>` block.

4. To edit the collection, follow these steps:
   a. Type the collection name and ID.

      For example: `Collection name="SHAREPOINT_Custom Collection" id="SHAREPOINT_C10070"`

   b. Edit the table parameter and provide the collection name in the given format:

      ```
      table="SHAREPOINT_CUSTOMCOLL"
      ```

      > **Note:** Table parameter is required only if you want to log data. Remove the table parameter from the collection block if you do not want to log data.

   c. Edit the `<Command>` parameter and provide object name.

      For example, `<Command>Perfmon Object Name</Command>`

   d. Edit `<Field>` parameter and provide Instance Name and Counter Name. Fields parameter is enclosed within the `<Fields></Fields>` block.

      For example:

      ```
      <Fields>

      <Field>Instance_Name</Field>

      <Field>Counter_Name 1</Field>

      </Fields>
      ```

   e. Edit the Metric id, name, position, and category of the metrics in the collection.

      For example:

Metric with Category as KEY;

```
<Metric id="SHAREPOINT_M17001" name="SHAREPOINT_
MyCustomInstance"

alarm=“false" formulae="value" position=“1" category=“KEY">
```

Metric with category as METRIC;

```
<Metric id="SHAREPOINT_M17002" name="SHAREPOINT_Counter_1_Value"
alarm=“true" formulae="value" position=“4" category=“METRIC">
```

f. Edit the `<AlarmDef>` block to configure alarm or alert for the metrics.

For example:

```
<AlarmDef>

<Policy>SHAREPOINT_Counter_1_Value</Policy>

<Object>

<MetricId>LYNC_M10101</MetricId>

</Object>

<Options>

<Option>

 <Name>ServiceName</Name>

<Value>

<MetricId>SHAREPOINT_M17001</MetricId>

</Value>

</Option>

<Option>

<Name>ServiceStatus</Name>

<Value>

<MetricId>SHAREPOINT_M17002</MetricId>

</Value>

</Option>

</Options>

</AlarmDef>
```

g. Click **Save and Close**.

5. To add Collection Schedule:
   a. From the HPOM console, go to **Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013 → Configuration**

The SharePoint_CollectionSchedule policy appears.

b. Double-click **SharePoint_CollectionSchedule**.

c. Add new collection in the format as shown in the following example:

For example, `<Collection name="SHAREPOINT_CustomColl" id="SHAREPOINT_C10070" schedule="High" role="|FrontEnd|" />`

d. From the policy editor window, click **Save and Close**.

6. To create a spec file to log the collected metric:

> **Note:** Spec file is required only if you want to log data.

a. From the Instrumentation folder, rename default spec file.

b. Edit the spec file. Give values to the following parameters:

`spec file name, class, label, and counter name`

For example:

```
SHAREPOINT_CUSTOMCOLL.spec

# DATASOURCE = SHAREPOINT_DATA

CLASS SHAREPOINT_CUSTOM = 10002

LABEL "SHAREPOINT_CUSTOM";

METRICS

COUNTER_1= 10201

# COUNTER_1_LENGTH CODA_DATATYPE = UINT64

#  COUNTER_1_LENGTH CODA_CATEGORYTYPE = GAUGE

Label “COUNTER_1"

PRECISION 0;

TYPE TEXT LENGTH 256;

COUNTER_2 = 10202

# COUNTER_2_LENGTH CODA_DATATYPE = UINT64

#  COUNTER_2_LENGTH CODA_CATEGORYTYPE = GAUGE

Label “COUNTER_2"

PRECISION 0;
```

7. Click **Save and Close**.

8. Run **Create Datasource for Sharepoint Server** tool. The class specified in the spec file is added to DataSource.

9. Deploy the updated policies to activate the collections.

Create Measurement Threshold Policy

Create measurement threshold policy for generating alerts. To create measurement threshold policy, follow these steps:

1. From the HPOM console, go to **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → **SharePoint Portal Server** → **Microsoft Office Sharepoint Server 2013**
2. **Copy** and paste any measurement threshold policy as per your requirement.

   > **Note:** A sample policy for SharePoint Server is provided with the Microsoft Enterprise Servers SPI.

3. Right-click the policy and select **All Tasks -> Edit...**
4. Provide the metric name as policy name.

   For example, `SHAREPOINT_Counter_1_Value`
5. From the policy editor window, click **Save and Close**.

Deploy Schedule Task Policies

Deploy Microsoft SharePoint Server Schedule Task Policies on the managed node. You must select the appropriate schedule task policy based on the roles supported by the Microsoft SharePoint Server 2013.

Policy Location: Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013

Deploy Measurement Threshold Policies

Deploy Microsoft SharePoint Server measurement threshold policies. You must, select the appropriate measurement threshold policy based on the roles supported by the Microsoft SharePoint Server 2013.

Policy Location: Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013

Deploy Event Log Policies

Deploy Microsoft SharePoint Server Event log policies if you want to monitor SharePoint Server events logs.

Policy Location: Policy management → Policy groups → SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office Sharepoint Server 2013

Chapter 5

Using Policies and Tools

Policies and tools monitor the Microsoft Enterprise Servers environment.

Customizing Policies

Policies run according to rules and schedule specifications. Measurement threshold policies contain the rules for interpreting Microsoft Enterprise Servers states or conditions.

You can customize specific policies to suit your requirements of the Microsoft Enterprise Servers environment.

Customizing Auto-Deploy (Default) Policies

The BizTalk Server 2006 and Microsoft Office SharePoint Server 2007 have auto-deploy policy groups. The polices are automatically deployed on the managed nodes on the respective server.

To customize the auto-deploy policy:

1. In the HPOM console tree, click **Policy management** → **Policy groups** → **SPI for Microsoft Enterprise Servers** → **en** → <**Microsoft Enterprise Server**> → **Auto-Deploy**.
2. Double-click Auto-Deploy. All the auto-Deploy policies of the <Microsoft Enterprise Server> are listed.
3. Right-click the policy and click **All Tasks**, and then **Edit.** A window appears to enable you to customize the policy.
4. Click **Task** or **Schedule** or both tabs to customize the policy.

Customizing Monitoring Schedule or Measurement Threshold Policies

You can customize the monitoring schedule or measurement threshold policies for any Microsoft Enterprise Servers SPI policy. After you update the policy for the nodes to which you want the latest change applied, right-click the Policy group, and select **All Tasks** → **Update to latest**, and then re-deploy one or more policies to one or more nodes. by following these steps:

1. In the HPOM console tree, click the **Agent policies grouped by type**, and select **Scheduled Task**.
2. Right-click the specific <**Microsoft Enterprise Servers SPI** >policy, and select **All Tasks** → **Edit...** in the details pane of the console. Alternatively, you can also double-click the specific Microsoft Enterprise Servers SPI policy.
3. Click the **Task** or **Schedule** or both tabs to modify the scheduled task policy.

Creating Custom Data Collection Groups

You can create custom data collections to change the monitoring intervals or thresholds. To create a separate group of policies, copy the desired policies into a folder with the new group name. After pasting the policies into the new group, you can then modify them and change the version numbers. The user-created versions make it possible to deploy specifically tailored policies to node groups to meet their monitoring needs. Using this method makes it possible to bring nodes and policies together in groups that are easily recognizable.

Customizing BizTalk Server 2010 Policies

You can change the policy thresholds by editing the config file policies. To change the policy thresholds, follow these steps:

1. In the HPOM console tree, click **SPI for Microsoft Enterprise Servers** → **Biztalk Server** → **Biztalk Server 2010**→ **<Policy Group>** .
2. Double-click **<BTS_CFG_MetricID>**.The ConfigFile window opens.

   For example, BTS_CFG_841403.
3. Click **Data** tab. The following XML code appears.

   a.

```
<Rule>
<RuleName>Rule_Critical</RuleName>
<ShortTermPeakCount>0</ShortTermPeakCount>
<Set>
<Threshold>0</Threshold>
<Message>
<Severity>CRITICAL</Severity>
<MessageText>One or more BizTalk Server Application Service is disabled.</MessageText>
</Message>
</Set>
<Reset>
<Threshold>4</Threshold>
<Message>
<Severity>NORMAL</Severity>
 <MessageText>All BizTalk Server Application Service is now running.</MessageText>
</Message>
</Reset>
</Rule>
```

To change the threshold for a specific rule, specify the threshold value in the following XML code:

<Set>

`<Threshold>0</Threshold>`

<Reset>

<Threshold>4</Threshold>

For instance, <Threshold>5</Threshold>

> **Note:** You must specify the threshold value for set and reset conditions. The Set threshold is used to identify if the value of the monitored metric matches the condition to generate alarm. The Reset threshold is used to identify if the value of the monitored metric, for which an alarm has already generated, is now normal and the previously generated alarm can be acknowledged. For more information about, set and reset threshold conditions see the *HP Operations Manager Online Help.*

4. Click Save and Close.

> **Note:** For more information about policies, see the *Microsoft Enterprise Servers SPI Online Help*.

Using Tools

The Microsoft Enterprise Servers tools are:

- **MSES_BTS_DB_Configuration** tool for the BizTalk Server 2006, BizTalk Server 2009 and BizTalk Server 2010 nodes.
- **Create Datasource for ISA Server** tool for ISA Server
- **Configure Edge server Discovery** for Lync Server 2010 and **Create Datasource** for Lync Server 2010 tool for Microsoft Lync Server 2010
- **Create Datasource** for BizTalk Server 2006 - This tool is used to configure the datasource for BizTalk Server 2006.
- **BTS 2010 Cluster Config** for BizTalk Server 2010 - This tool generates the apminfo.xml file for BizTalk Server 2010. The apminfo.xml file provides necessary information to enable the Microsoft Enterprise Servers SPI to detect and monitor BizTalk Server 2010 cluster nodes.. To run the BTS 2010 Cluster Config tool, follow these steps:
  - In the HPOM console tree, click **Tools** → **SPI for Microsoft Enterprise Servers** → **Biztalk Server.**
  - Select the **BTS 2010 Cluster Config** tool.
  - In the details pane, double-click **Exchange Cluster Configuration**. The Select where to launch this tool dialog box opens.
  - Click **Launch**. The Tool Status window opens and displays the output under the Tool Output section.

- Select and copy the text content under the Tool Output section to a text editor. Save the text as **apminfo.xml** in the following locations on cluster nodes of BizTalk Server 2010 Cluster:

  For DCE managed nodes - %OvAgentDir%\conf\OpC\

  For HTTPs managed nodes - %OvAgentDir%conf\conf\

> **Note:** If the folder does not exist, create the folder manually.

> **Note:** You can use the following commands to start and stop the agents:
>
> **opcagt -kill**
>
> **opcagt -start**

BTS 2010 Enable Trace for BizTalk Server 2010 - This tool can be used to enable tracing for the BizTalk SPI data collector. The tool collects troubleshooting information and sets the trace level on the node where the tool is run. This tool can be run on the BizTalk Server 2010 nodes.

Depending on the level of troubleshooting that is required, the following trace levels can be passed as the parameter:

0 - Errors. Only errors are logged. If the trace level is not specified, this is the default trace value.

1 - Warnings. All warnings and errors are logged.

2- Info. All trace statements which are informational, warnings, and errors are also logged.

3 - Debug. Apart from all other information all Debug trace statements are also logged.

4 - Verbose, This is the maximum trace level and all trace statements are logged.

The log files are created in the **%OvDataDir%\bin\BTS\log** folder. Separate log files are created for each collection. All trace files have the prefix **BTS**.

The tool is run on the BizTalk Server 2010 Nodes.

BTS 2010 Create Datasource for BizTalk Server 2010 - This tool configures the datasource for BizTalk Server 2010. By default, the datasource is created in CODA. The name of the datasource is BTS_DATA.

Launching the Microsoft Enterprise Servers SPI Tools

To launch the Microsoft Enterprise Servers SPI tool, follow these steps:

1. In the HPOM console tree, click **Tools** → **SPI for Microsoft Enterprise Server**.
2. Right-click the tool, and select **All Tasks** and then click **Launch Tool**. All the nodes are listed.
3. Select one or more nodes where the tool is to be launched and then click **Launch**.

> **Note:** For more information about tools and policies, see the *Microsoft Enterprise Servers SPI Online Help*.

Chapter 6

Integrating Microsoft Enterprise Servers SPI with HP Reporting and Graphing

Reports and graphs provide you with a complete view of the performance of the components of the Microsoft Enterprise Servers.

Using Reports and Graphs

Reports and graphs cover updates on the availability or the activity or both in Microsoft Enterprise Servers for each server running the services.

These web-based reports are automatically generated every night and provide you with a routine means of checking the Microsoft Enterprise Server availability on the nodes.

> **Note:** If the Microsoft Enterprise Servers SPI is not installed in the Operations Manager Window server, you must install it on this server to enable the HP Reporter function in one or more managed nodes.

Integrating Microsoft Enterprise Servers SPI with HP Reporter

You must install MSESSPI Reporter package on HP Reporter Server to use the Microsoft Enterprise Servers SPI reports. For this, run the **Setup.exe**. This setup installs the Microsoft Enterprise Servers SPI Report Package within the Reporter server. After you complete the installation, configure the Reporter to generate reports.

Installing Report Package

To install the Microsoft Enterprise Servers SPI Report Package on a stand-alone Reporter server:

1. Insert the HP Operations Smart Plug-ins DVD.
2. Double-click the file **Setup.exe**. Follow the instructions as they appear for the installation on Management Server for Windows. Select Reports for Microsoft Enterprise Servers SPI. Continue the next steps till a dialog box opens indicating the completion of the installation.
3. Select **Finish** to complete the installation.

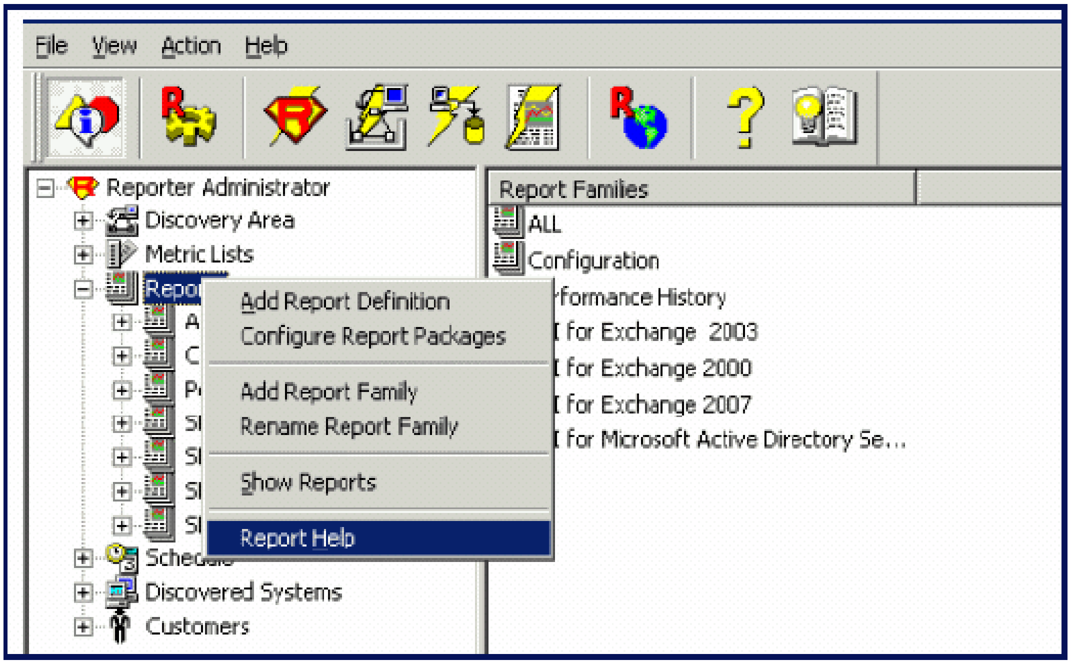
Configuring Report Package

To configure the Microsoft Enterprise Servers SPI Report Package:

1. Open the Reporter main window and check the status pane to note the changes to the Reporter configuration, which include uploading the Microsoft Enterprise Servers SPI reports.
2. The Microsoft Enterprise Servers SPI Reports are automatically assigned to the **ALL** group in the Reporter main window. (See "Generating Reports" below for HPOM Report list.)
3. Add group and single system reports by assigning reports as desired. Reports are available for viewing the following day.

> **Note:** Identify the Microsoft Enterprise Servers SPI reports of group and single systems by their full name; for example, **abc.xyz.com** is acceptable while **abc** is not.

Instructions are available in the HP Reporter Help for assigning Microsoft Enterprise Servers SPI reports to the targeted nodes. To access Help, select **Reports** or **Discovered Systems** in the left panel of the HP Reporter main window and right-click it. Select **Report Help** or **Discovered Systems Help** from the sub-menu that appears. For more information about HP Reporter, see the *HP Reporter documentation*.



Generating Reports

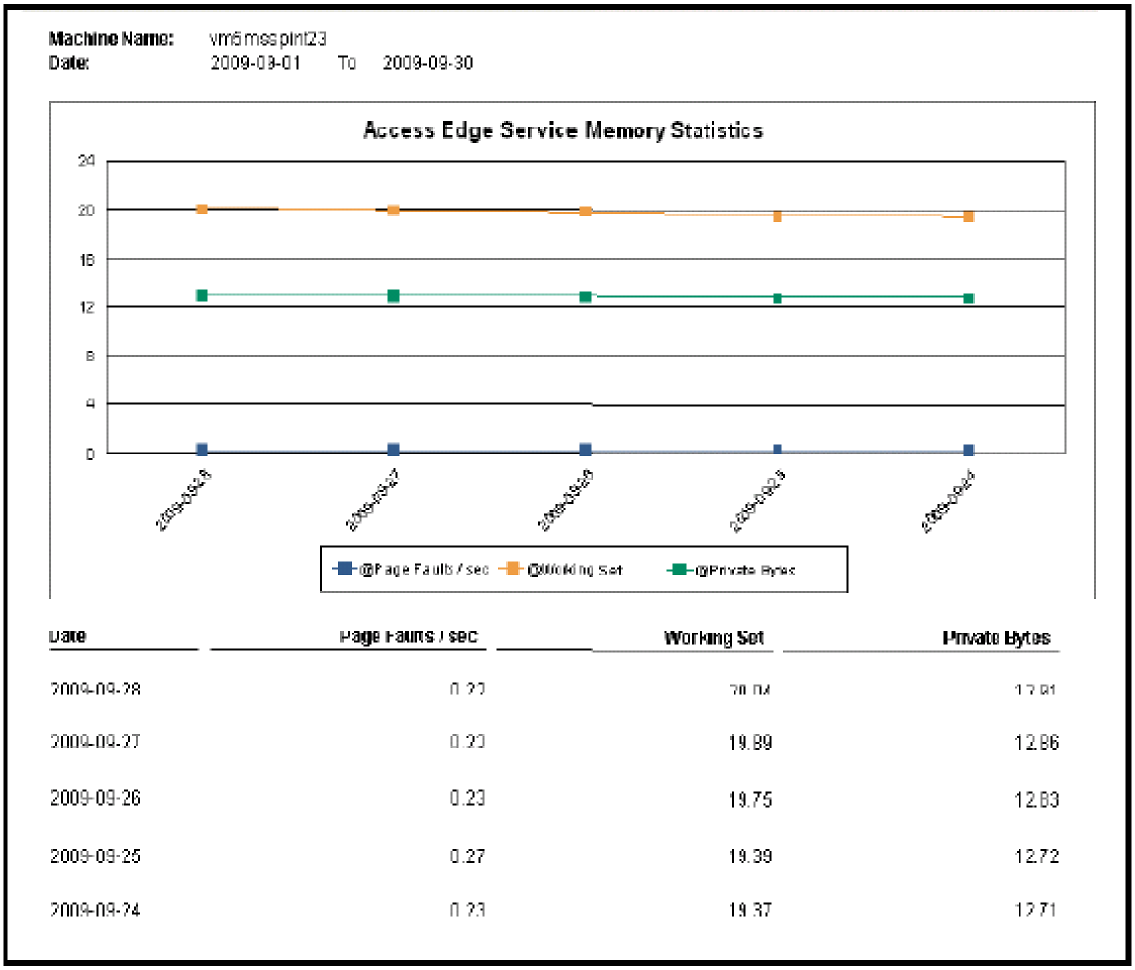
After you install the Microsoft Enterprise Servers SPI, the HPOM generates reports using the SPI-collected data for Microsoft Enterprise Servers. HPOM runs the reports regularly on a nightly schedule. You can see the updated reports every day because the HPOM, by default, re-generates reports every night with the day’s data.

> **Note:** If you want to customize your reports you must install HP Reporter. For more information about HP Reporter and modifying the reports, see the *HP Reporter documentation*.

Generate the reports using HTML format. The report data of Microsoft Enterprise Servers SPI is collected based on metrics used for each report. The HP Reporter identifies the data through metric variables. This data is stored in the MS SQL Reporter database

> **Note:** If the report contains a huge amount of data, there is a possibility that the browser might crash when the reports are viewed in HTML format. In such situations, view the reports in pdf format.

You can access the reports of SPI for Microsoft Enterprise Servers from the **Reports** area of the HPOM console. For more information about Reports, see *Microsoft Enterprise Servers SPI Online Help* or *Microsoft Enterprise Servers SPI Online Help PDF*.



Machine Name: vm6mssplnt23
Date: 2009-09-01 To 2009-09-30

Date	Page Faults / sec	Working Set	Private Bytes
2009-09-28	0.23	20.04	12.91
2009-09-27	0.23	19.89	12.86
2009-09-26	0.23	19.75	12.83
2009-09-25	0.27	19.39	12.72
2009-09-24	0.23	19.37	12.71

Reports Fail with Oracle Database

Some of the reports fail due to invalid Reporter ODBC driver.

Possible cause: The versions of Oracle client to access Oracle database do not match.

Suggested action: Use Oracle client 9.2.0 to access Oracle 9.2.0 database and 10gR2 client to access 10gR2 database

Integrating Microsoft Enterprise Servers SPI with HP Performance Manager

The Microsoft Enterprise Servers SPI comes with a set of preconfigured graph templates. Ensure that these graph templates are installed on an HP Performance Manager system, and that the data store (CODA) runs on the managed node.

> **Note:** If you are using HP Performance Agent for viewing the graphs, the Microsoft Enterprise Servers SPI shows incorrect data.

To integrate the Microsoft Enterprise Servers SPI with HP Performance Manager, follow these steps:

1. Install and configure the Microsoft Enterprise Servers SPI.
2. Install the graph package.

On a Windows system that has HP Performance Manager, follow these steps:

1. Insert the Smart Plug-ins DVD-ROM (that contains the reporting packages) into the DVD-ROM drive, and in Windows Explorer, double-click:

   <DVD-Drive>\SPIs\MSES SPI OVPM Configuration Package

   HPOvSpiMsesGc.msi.
2. Follow the instructions as they appear. Select graphs for Microsoft Enterprise Servers SPI.

For more information about HP Performance Manager, see the *HP Performance Manager documentation*.

Chapter 7

Removing Microsoft Enterprise Servers SPI

You can remove the Microsoft Enterprise Servers SPI by the following ways:

- Using the DVD
- Using the Windows Control Panel - Add/Remove Programs

To remove the Microsoft Enterprise Servers SPI, remove all policies and policy groups from the managed nodes, and then from the management server.

Using DVD

You must remove the SPI components manually before removing the SPI from the management server using a DVD.

Removing Microsoft Enterprise Servers SPI Components

The Microsoft Enterprise Servers SPI components include policies, reporting package, and graphing package.

Remove the Microsoft Enterprise Servers SPI policies from all Managed Nodes

1. In the HPOM console, click **Policy Management**.
2. Right-click **SPI for Microsoft Enterprise Servers**, and select **All tasks →Uninstall from...**.
3. In the **Uninstall on...** window, select each check box next to one or more nodes from which you want to remove the policies.
4. Click **OK**.

> **Note:** To verify policies are removed, at the HPOM console expand the **Nodes**, right-click a node, and then select **View** → **Policy Inventory**.

Remove Microsoft Enterprise Servers SPI policy group from the Management Server

1. In the HPOM console tree, expand **Policy groups**.
2. Right-click **SPI for Microsoft Enterprise Servers**, and select **Delete**.
3. Remove Microsoft Enterprise Servers SPI programs from the HPOM management server
4. Insert the *HP Operations Smart Plug-ins* DVD.

5. Follow the instructions as they appear on the screen and start the uninstall procedure by selecting the **Remove products**.
6. In the **Product Selection Uninstall** window, select **Microsoft Enterprise Servers (SPI)**, and click **Next**.
7. In the next window select **Remove.**

> **Note:** Each window updates you with the status of removing the Microsoft Enterprise Servers SPI.

8. Click **Finish** to complete.

Remove the Microsoft Enterprise Servers SPI Policies from the Management Server

1. In the HPOM console tree, expand the Agent Policies grouped by type.
2. From each policy type, delete all the versions of the policies of the Microsoft Enterprise Servers SPI.

Using the Windows Control Panel

Remove the SPI components before removing the Microsoft Enterprise Servers SPI from the management server. To remove the SPI components manually, perform the tasks in "Removing Microsoft Enterprise Servers SPI Components" on previous page.

Removing Microsoft Enterprise Servers SPI from Management Server

To remove the SPI from the management server, perform the following steps:

1. From the Start menu, select **Settings** → **Control Panel** and open **Add/Remove Programs**.

> **Note:** When you use the Windows Control Panel to remove any SPI, you have two options: (1) to remove selected SPIs or (2) to remove HPOM for Windows. If you want to remove both HPOM and the SPIs, you must first remove all Smart Plug-ins from managed nodes then from the management server. You can then remove SPI from HPOM.

2. Select **HP Operations Smart Plug-ins**, and then click **Change**.
3. Click **Next** on the Welcome screen.
4. Select **Remove Programs**, and select **HP Operations Smart Plug-ins**.
5. Select **MSESSPI**.
6. Complete the instructions until a message appears stating that Microsoft Enterprise Servers SPI is removed.

Removing Reporting Package

You can remove the reporting package. To remove the reporting package:

1. From the Start menu, select **Settings** →**Control Panel** and open **Add/Remove Programs**.
2. Select the reporting package, and then click **Change**.
3. Complete the instructions until a message appears stating that HP Reporter is removed.

Removing Graphing Package

To remove the graphing package, follow these steps:

1. From the Start menu, select **Settings** →**Control Panel** and open **Add/Remove Programs**.
2. Select the graphing package, and then click **Change**.
3. Complete the instructions until a message appears stating that HP Performance Manager is removed.

Removing Reporting and Graphing Package using .msi File

You can also remove the reporting and graphing package by using **.msi** file.

Removing Reporting Package using .msi file

To remove the reporting package using **.msi** file, follow these steps:

1. Browse to one of the following locations:
   - **<SPI DVD>\x64\SPIs\MSES Reporter Package\MSESSPI-Reporter.msi**
   - **<SPI DVD>\x86\SPIs\MSES Reporter Package\MSESSPI-Reporter.msi**
2. Right-click **MSESSPI-Reporter.msi**, and then click **Uninstall**.
3. Confirm the removal of the reporting package by clicking **Yes**.

Removing Graphing Package using .msi File

To remove the graphing package using the **.msi** file, follow these steps:

1. Browse to one of the following locations:
   - **<SPI DVD>\x64\SPIs\MSESSPI OVPM ConfigurationPackage\HPOvSpiMsesGc.msi**
   - **<SPI DVD>\x86\SPIs\MSESSPI OVPM ConfigurationPackage\HPOvSpiMsesGc.msi**
2. Right-click **HPOvSpiMsesGc.msi**, and then click **Uninstall**.
3. Confirm the removal of the graphing package by clicking **Yes**.

Chapter 8

Troubleshooting SPI for Microsoft Enterprise Servers

This chapter provides information about certain problems in the Microsoft Enterprise Servers SPI and solutions for troubleshooting them.

Discovery

The following section describes the possible cause and suggested action for the failure of discovery policy

Insufficient Privileges

In some cases, the Microsoft Enterprise Servers SPI fails to discover the services. The possible cause and suggested action are as follows:

Possible cause: The account with which the Discovery policy of a Microsoft Enterprise Server (Policy Bank → SPI for Microsoft Enterprise Server → en →<Specific Server> → <Server Type> →Discovery is run by the HP Operations agent does not have the privileges to connect to the corresponding Microsoft Enterprise Server and retrieve data.

Suggested action: Ensure that administrator credentials are provided for the appropriate Discovery policy by editing the policy and then redeploy it. Run the policy as Enterprise Server Administrator.

Edge Server Discovery Fails

The Microsoft Enterprise Servers SPI fails to discover the Edge Server.

Possible cause: The tool Configure Edge Server Discovery for Lync Server 2010 is not started.

Suggested action: Ensure that you start the Configure Edge Server Discovery for Lync Server 2010 tool and configure the username and password for the Edge Server before deploying the Discovery policy. For more information, see Configuring LS_Discovery Policy.

BizTalk Server Discovery Fails

A missing configuration file can fail the service discovery for BizTalk Server.

Possible cause: In some cases, the BizTalk Server’s service discovery policy fails when the configuration file is missing on the managed BizTalk Server node.

Suggested action: Launch the MSES_BTS_DB_Configuration tool before deploying the service discovery on the managed node.

Reports and Graphs

The following sections describe the possible cause and suggested action for failed data generation in Microsoft Enterprise Server reports and graphs.

Reports and Graphs not having data

The possible cause and suggested action for reports and graphs not getting generated are as follows:

Possible cause*:* The appropriate policies are not deployed to the respective Microsoft Enterprise Server nodes. The policy, therefore, fails to collect the data that the HP Reporter generates as reports. Failure to deploy the appropriate policy also disables the HP Performance Manager to generate graphs.

Suggested action: To know the appropriate policy for each Microsoft Enterprise Servers SPI report, see Appendix B Report, Report Table, Data Store, and Policy Mapping Details in *HP Operations Smart Plug-in for Microsoft Enterprise Server Reference Guide*. To know the appropriate policy for each Microsoft Enterprise Servers SPI, see Graphs, Data Store, and Policy Mapping Details in *HP Operations Smart Plug-in for Microsoft Enterprise Server Reference Guide.* Deploy the policies accordingly.

Browser Stops while Viewing HTML Report

Sometimes the browser stops while viewing the reports in HTML format. The possible cause and the suggested action are as follows:

Possible cause: The browser cannot handle huge amount of data.

Suggested action: View the reports in PDF format.

Data Logging Policies Cannot Log Data

In some cases, the data logging policies cannot log data. The possible cause and the suggested action are as follows:

Possible cause: The data source is not created in the datastores—CODA or HP Performance Agent

Suggested action: Check if the appropriate data source is created. To check, perform the following steps:

1. Log on to the managed node as an administrator.
2. From the command prompt run the ovcodautil -obj > out.txt command.
3. Check the out.txt file to ensure that the appropriate data source is created.
4. If the data source is not created, deploy the policy or run the tool to create the appropriate data source in the managed Microsoft Enterprise Server node. For more information about creating datasources, see "Create Data Sources" on page 24.

Policies

The following section describes the possible cause and suggested action for troubleshooting policies.

Measurement Threshold Policy

In some cases, when you try to save the Measurement Threshold policy after editing, it does not get saved. The system shows an error stating that the form is not valid.

Possible cause: In Edit Measurement Threshold policy window, under Threshold tab, value for Use Instance Filters is set to Yes.

Suggested action: Set the value for Use Instance Filters to No and save the policy.

Chapter 9

Troubleshooting SPI for Microsoft Enterprise Servers (2013)

This chapter provides information about certain problems in the Microsoft Enterprise Servers SPI and solutions for troubleshooting them.

SharePoint Server Discovery Fails

The Microsoft Enterprise Servers SPI fails to discovered Microsoft SharePoint servers.

Possible cause: The account with which the Discovery policy of Microsoft Enterprise Server SPI is run does not have the privileges to connect to the Microsoft SharePoint Server and retrieve data.

Suggested action: Verify the **DB** permission for the user. Make sure the user have **db_owner** rights on sharepoint_config database. Verify **System.txt** and **SP_Discovery.log** for any other errors.

Alerts not Generated for Some Metrics

The Microsoft Enterprise Servers SPI fails to generate alerts for some metrics.

Possible cause: Monitor policy is not deployed on the node. `<Server Name>_MetricDefinition` config file policy is not updated and deployed after modifying a policy.

Suggested action: Deploy appropriate monitor policies on the node. Update and deploy `<Server Name>_MetricDefinition` configuration file policy. Enable Trace and check for errors in the trace file.

Data not Logged in SPI Datasource

The collected data is not logged into the specific server's SPI Datasource.

Possible cause: Existing Datasource of the server is having errors. Collections run for logging data is returning errors.

Suggested action: Verify if a Datasource is created using the command `ovcodautil -obj`. Enable trace and check trace files for errors. Execute `MsCollectionManager.exe` manually for any one of the collections and verify the output.

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Operations Smart Plug-in for Microsoft Enterprise Servers, 8.05 Installation and Configuration Guide

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.