

HP Operations Smart Plug-in for Microsoft[®] Active Directory

for HP Operations Manager for Microsoft Windows[®]

Software Version: 7.00

Installation and Configuration Guide

Document Release Date: December 2009
Software Release Date: December 2009



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2008–2009 Hewlett-Packard Development Company, L.P.

Trademark Notices

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Pentium® is a U.S. registered trademark of Intel Corporation.

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:

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

1	Introducing the Smart Plug-in for Microsoft Active Directory	9
	About Smart Plug-in for Microsoft Active Directory	9
	Components of the Microsoft Active Directory SPI	10
	Policies	10
	Tools	10
	Reports	10
	Graphs	10
	Functions of Microsoft Active Directory SPI	11
	Collecting and Interpreting the Performance and Availability of Information	11
	Displaying Information	11
	Service Map	12
	Message Browser	12
	Instruction Text	13
	Reports and Graphs	13
	HP Operations Topology Viewer Tool	13
	Generating Reports Using HP Reporter	13
	Graphing Data with HP Performance Manager	13
	Customizing Policies	14
2	Installing and Upgrading the Microsoft Active Directory SPI	15
	Installation Packages	17
	SPI Package	17
	Graphing Package	17
	Reporting Package	18
	Console Package	18
	Installation Environments	18
	Standard Installation of SPI Components on an HPOM 8.10 Server	18
	Standard Installation on Remote Consoles	18
	Standalone HP Reporter or HP Performance Manager	18
	Prerequisites to Installing the Microsoft Active Directory SPI	19
	Hardware Requirements	19
	Software Requirements	19
	Software Prerequisites on Management Server	19
	Installing the Microsoft Active Directory SPI	20
	Installing the Microsoft Active Directory SPI on a Remote Console	20
	Installing the Microsoft Active Directory SPI on a Standalone Management Server	20
	Installing the Microsoft Active Directory SPI in an HPOM Cluster Environment	22
	Upgrading the Microsoft Active Directory SPI	22
	Upgrading the Microsoft Active Directory SPI on a Remote Console	23

Upgrading the Microsoft Active Directory SPI on a Standalone Management Server.	23
Upgrading the Microsoft Active Directory SPI in an HPOM Cluster Environment.	25
Verifying the Installation/Upgrade of Microsoft Active Directory SPI	26
3 Configuring Microsoft Active Directory SPI	27
Configuration Procedure of Microsoft Active Directory SPI	29
Change Unmanaged Node to Managed Node	29
Deploy Instrumentation Categories on Managed Nodes	30
Discover Services on the Managed Nodes	30
Create Data Sources	33
View the Microsoft Active Directory Service Map	33
Customize Policies	35
Deploy Microsoft Active Directory SPI Policies.	35
Data Logging Scenarios	36
4 Customizing Policies	37
Customizing Default Policies	37
Customizing Monitoring Schedule or Measurement Threshold Policies	38
Creating Custom Data Collection Groups	38
Deploying Policies	39
Policy Group	39
Policy Type	39
Using Auto-Deploy Policies	40
Discovery	40
DIT Monitoring	40
DNS Monitoring	40
FSMO Monitoring	40
Replication Monitoring	40
Response Time Monitoring.	40
GC Monitoring	41
Sysvol Monitoring	41
Trust Monitoring.	41
Using Manual-Deploy Policies.	41
Auto-Baseline Policies	41
Connector Policies (Only for Windows Server 2003).	42
Domain and OU Structure	42
Global Catalog Access.	42
Health Monitors	43
Index and Query	43
Replication.	43
Replication Activity	43
Security	43
Site Structure	43
5 Using Tools	45
Launching Tools	45
AD Trust Relationships Tool	46
Using HP Operations Topology Viewer Tool.	47

Launching HP Operations Topology Viewer Tool	48
Getting Started with the HP Operations Topology Viewer Tool	48
Accessing Functions of HP Operations Topology Viewer Tool	49
Adjusting Map View	49
HP Operations Topology Viewer menus	51
HP Operations Topology Viewer Toolbar	54
Accessing Server and Map Properties	55
6 Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions	57
Using Reports and Graphs	57
Integrating the Microsoft Active Directory SPI with HP Reporter	58
Installing and/or Upgrading the Report Package	58
Configuring the Report Package	59
Generating Reports	59
Integrating Microsoft Active Directory SPI with HP Performance Manager	60
Generating Graphs	61
7 Troubleshooting	63
Troubleshooting Discovery	63
Insufficient Privileges	63
Failed Binary on the Managed Node	63
Troubleshooting through Tracing	64
Troubleshooting Reports and Graphs	64
Reports and Graphs are not generated	64
Data Logging Policies cannot log Data	65
Browser Crashes while Viewing the HTML Report	65
Reports Fail with Oracle Database	65
Modifying Policy Names	65
8 Removing Microsoft Active Directory SPI	67
Using DVD	67
Removing Microsoft Active Directory SPI Components	67
Using the Windows Control Panel	68
Removing Microsoft Active Directory SPI from Management Server	68
Removing Reporting Package	68
Removing Graphing Package	69
Removing Reporting and Graphing Package using .msi File	69
Removing Reporting Package using .msi file	69
Removing Graphing Package using .msi File	69
Index	71

1 Introducing the Smart Plug-in for Microsoft Active Directory

A Smart Plug-in (SPI) is an add-in software for the HP Operations Manager (HPOM). It functions as a modular component of HPOM and further improves its monitoring capabilities in managing your IT resources. SPIs help you to simplify the tasks of your environment by:

- Monitoring availability and health
- Detecting performance lapse
- Detecting, preventing, and solving problems
- Documenting problem solutions
- Generating reports

About Smart Plug-in for Microsoft Active Directory

The Smart Plug-in for Microsoft Active Directory (Microsoft Active Directory SPI) helps you to manage the Microsoft Active Directory in your environment. The Microsoft Active Directory SPI keeps you informed about the conditions related to the Microsoft Active Directory and provides updated information on:

- Data consistency across the domain controllers (DCs).
- Timely replication process.
- Systems outages capability.
- Successful functioning of role masters.
- DCs not contending with over-utilized CPUs.
- Capacity and fault-tolerance issues in Microsoft Active Directory.
- Replication of Microsoft Active Directory Global Catalog (GC) in a timely manner.
- Acceptable performance levels of services, event, processes, and synchronizations.
- Occurrence of index and query activities such as authentications and lightweight directory access protocol (LDAP) client sessions at acceptable levels.
- Expected trust relationship status between sites and DCs.

Components of the Microsoft Active Directory SPI

The components of Microsoft Active Directory SPI are policies, tools, reports, and graphs. Each of these components enhances the monitoring capability of the Microsoft Active Directory SPI.

Policies

Policies are pre-defined thresholds that keep a constant vigilance over the Microsoft Active Directory environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts are shown in the service map while messages are available in the 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. Policies can be deployed automatically (while installing the Microsoft Active Directory SPI) or manually. For more information, see [Chapter 4, Customizing Policies](#).

Tools

Tools are the utilities that gather more Microsoft Active Directory related information. You can also launch tools to view the Microsoft Active Directory environment. For more information, see [Chapter 5, Using Tools](#).

Reports

Reports represent a summarized data generated by policies. Data collected by policies are used to generate reports. For more information, see [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

Graphs

Graphs are the pictorial representation of the various metrics of the Microsoft Active Directory. Reports contain the data that are collected by policies. For more information, see [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

Reports and graphs generated with the help of HP Reporter and HP Performance Manager which are available as separate products, provide information that can help you to determine corrective actions to be taken in the long term.

See *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* or *HP Operations Smart Plug-in for Microsoft Active Directory Online Help PDF* for a detailed description of policies, tools, reports, and graphs.

Functions of Microsoft Active Directory SPI

The Microsoft Active Directory SPI monitors the Microsoft Active Directory.

Collecting and Interpreting the Performance and Availability of Information

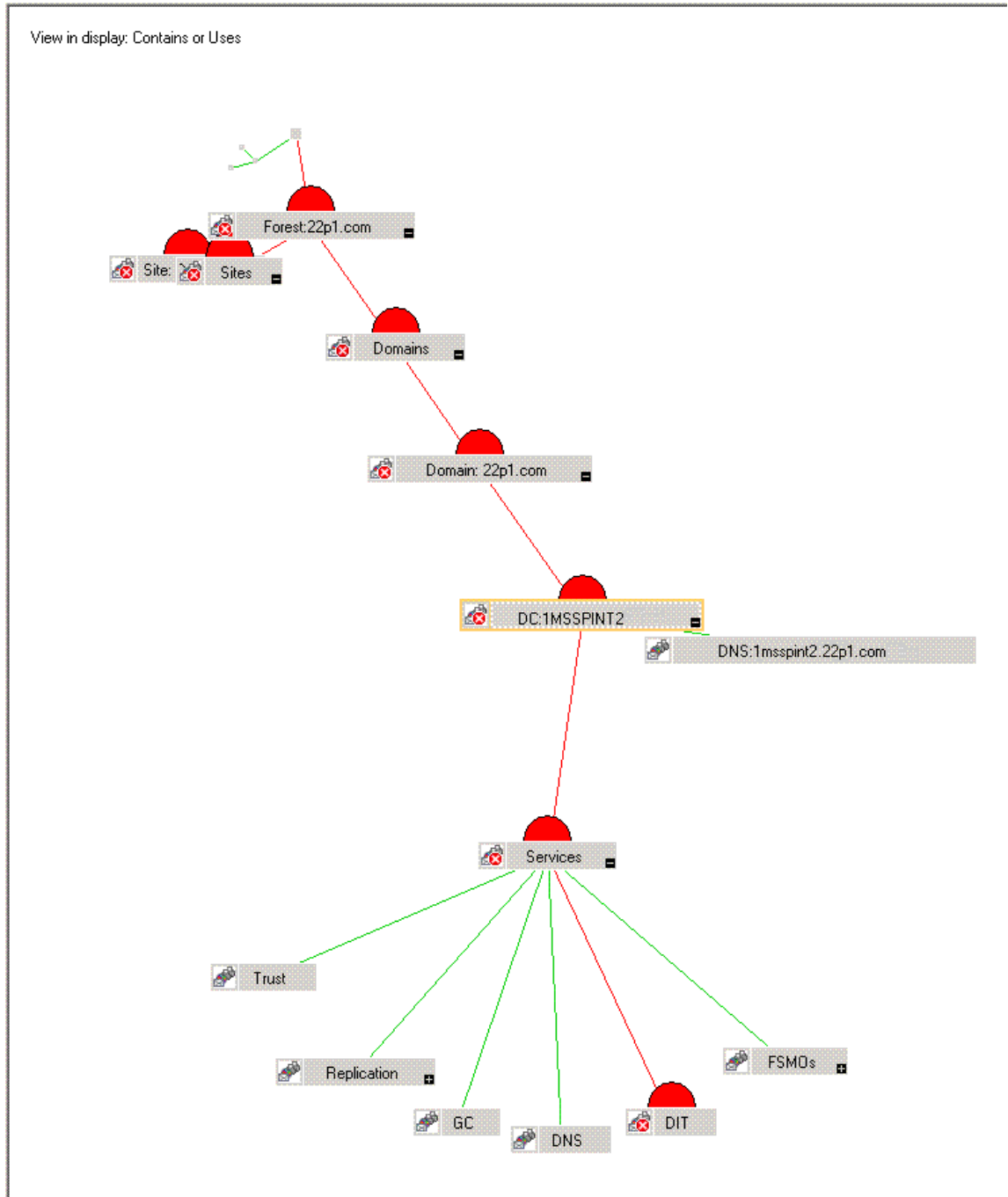
The Microsoft Active Directory SPI monitors the Microsoft Active Directory environment by discovering existing components such as the Domain Controllers (DCs), forests, preferred bridgehead servers (PBHS), SysVol, and replication sites and maintaining the thresholds set up by the policies. The Microsoft Active Directory SPI displays the services of the Microsoft Active Directory and adds multiple hierarchical levels of details.

Displaying Information

The Microsoft Active Directory SPI displays information in the following ways.

Service Map

Service map shows the newly added and discovered Microsoft Active Directory services displayed in both the console services tree and the service map (right). Within the service map pane, the hierarchy expands to show the specific services present on each DC. Further expansion of each DC displays its components.



Message Browser

The Microsoft Active Directory SPI monitors events and services on the managed nodes and generates messages, which are displayed on the message browser of HPOM console. The message browser displays messages identified with the severity level of the problem.

Instruction Text

Messages generated by the Microsoft Active Directory SPI policies contain instruction text which mentions probable cause and preventive action to resolve problems.

Reports and Graphs

Reports and graphs present the information that manage the Microsoft Active Directory in your environment when you implement efficient load balancing, capacity planning, and policy scheduling and threshold adjustments.

HP Operations Topology Viewer Tool

The HP Operations Topology Viewer tool enables you to view the Microsoft Active Directory topology after it connects to a Microsoft Active Directory DC. For more information on HP Operations Topology Viewer tool, see [Getting Started with the HP Operations Topology Viewer Tool](#) on page 48..



To access Topology Viewer on the remote console, you must install the HP Operations Topology Viewer tool.

Generating Reports Using HP Reporter

You can generate reports to analyze past or present Microsoft Active Directory conditions. These Web-based reports are automatically generated every night and provide you with a routine means of checking the Global Catalog (GC) and Domain Naming System (DNS) availability, disk space, and queue length issues occurring with DIT, replication latency, and connection times specific to DCs running master operations services. Reports covering the trust relationship changes between DCs are also available for Windows 2003 and Windows 2008 nodes. For more information on HP Reporter, see [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

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 Active Directory SPI with HP Performance Manager to generate and view graphs. For more information on HP Performance Manager, see [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

Customizing Policies

You can customize the monitoring schedule or measurement threshold policies for any Microsoft Active Directory SPI policy. Some of the modifications that can be performed are:

- Script-parameters
- Rules
- Options



Use Software Upgrade Tool Kit 2.0 to retain the customization of the earlier versions of the Microsoft Active Directory SPI policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

2 Installing and Upgrading the Microsoft Active Directory SPI

Perform the tasks mentioned in the following sections to install and upgrade the Microsoft Active Directory SPI.

The following flowchart shows an overview of installing and configuring the Microsoft Active Directory SPI. See Table 1 for references of the legends.

Figure 1 An Overview of Installation and Configuration Steps

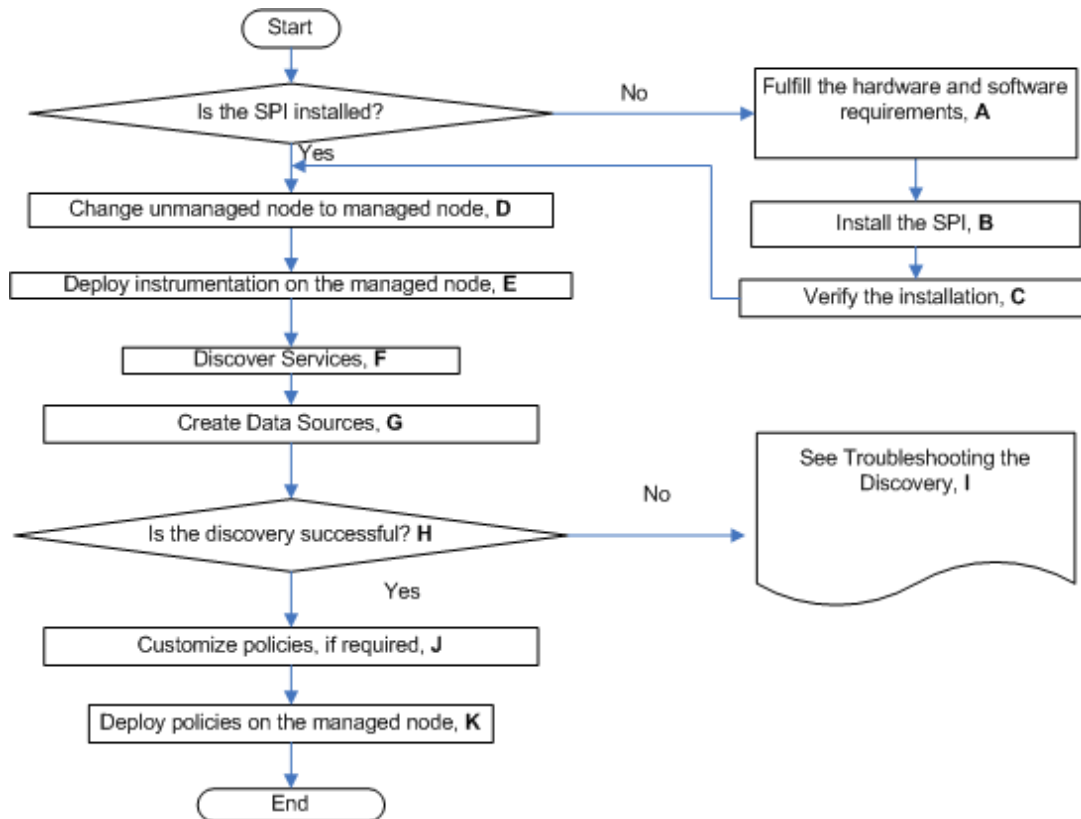


Table 1 References of Legends of Flowchart

Legend	References
A	Prerequisites to Installing the Microsoft Active Directory SPI on page 19
B	Upgrading the Microsoft Active Directory SPI on a Standalone Management Server on page 23
C	Verifying the Installation/Upgrade of Microsoft Active Directory SPI on page 26

Legend	References
D	Change Unmanaged Node to Managed Node on page 29
E	Deploy Instrumentation Categories on Managed Nodes on page 30
F	Discover Services on the Managed Nodes on page 30
G	Create Data Sources on page 33
H	View the Microsoft Active Directory Service Map on page 33
I	Troubleshooting Discovery on page 63
J	Customize Policies on page 35
K	Deploy Microsoft Active Directory SPI Policies on page 35

The following flowchart shows an overview of upgrading the Microsoft Active Directory SPI. See Table 2 for references of the legends.

Figure 2 An Overview of Upgrade Steps

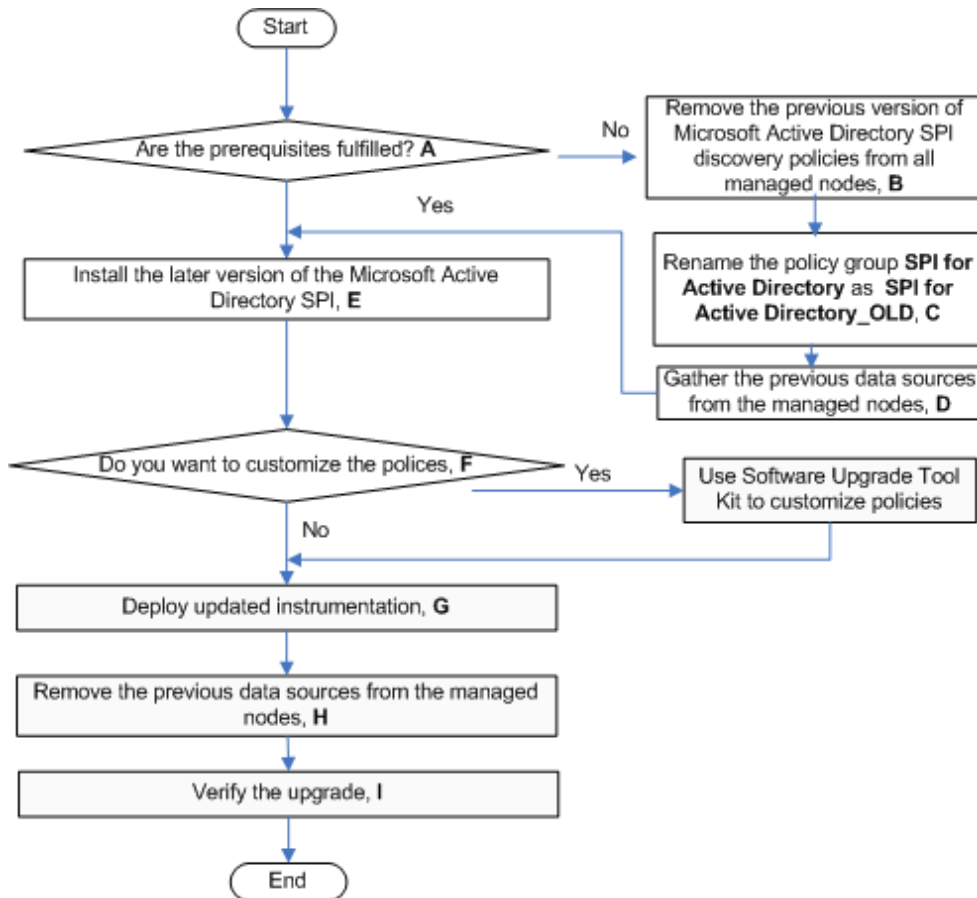


Table 2 References of Legends of Flowchart

Legend	References
A	Prepare to install the later version of the Microsoft Active Directory SPI on page 23
B	Remove the Microsoft Active Directory SPI discovery policies: on page 23
C	Rename the Microsoft Active Directory SPI policy group: on page 23
D	Gather data from all the managed nodes. on page 24
E	Upgrading the Microsoft Active Directory SPI on a Standalone Management Server on page 23
F	Customize the policies of Microsoft Active Directory SPI, if required. on page 24
G	Deploy updated instrumentation. on page 24
H	Remove data sources from the nodes on page 25
I	Verifying the Installation/Upgrade of Microsoft Active Directory SPI on page 26

Installation Packages

The Microsoft Active Directory SPI installation packages includes the following packages.

SPI Package

The SPI package is the .msi package, which contains all the functionality of the SPI. It must be installed on a server managed by HPOM. You can find the Microsoft Active Directory SPI package at the following location:

```
<SPI DVD>\SPIS\AD SPI\ADSPI.msi
```

Graphing Package

The Graphing package contains the graphs provided by the SPI. Graphs are drawn from metrics that are collected in the datasources created by the SPI. You can find the Microsoft Active Directory graphing package at the following location:

```
<SPI DVD>\SPIS\AD SPI OVPM ConfigurationPackage\HPOvSpiAdGc.msi
```

Reporting Package

The Reporter package contains the reports provided by the SPI. The HP Reporter gathers the data from the nodes managed by the SPI through the HPOM, stores the data in its local database, and creates .html reports based on the default SPI report policies. You can find the Microsoft Active Directory reporting package in the following location:

```
<SPI DVD>\SPIs\AD SPI\ADSPI-Reporter.msi
```

Console Package

The Console package contains HP Operations Topology Viewer tool, which is used to view the Microsoft Active Directory topology. It displays all the components of the Microsoft Active Directory like DCs, PBHS, forests, and so on.

```
<SPI DVD>\SPIs\SPIs Console Packages\OVTV-Console.msi
```

Installation Environments

HPOM for Windows provide 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 SPI DVD to install on servers managed by HPOM.

Standard Installation of SPI Components on an HPOM 8.10 Server

An HPOM for Windows 8.10 server does not have the OVPMLite and ReporterLite installed by default. Only the full versions of these products are available for installation. As a result, through 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 uninstalled on the HPOM 8.10 server.

Standard Installation on Remote Consoles

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

Standalone HP Reporter or HP Performance Manager

For such a system only the corresponding package of any SPI is enabled and 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 PM.

Prerequisites to Installing the Microsoft Active Directory SPI

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

Hardware Requirements

See the *HP Operations Manager for Windows Installation Guide* for information on hardware requirements.

Software Requirements

Ensure that the following software requirements are fulfilled:

On the Management Server:

- HP Operations Manager for Windows: 8.10 and the latest patch
- HP Reporter: 3.80
- HP Performance Manager: 8.20 (if you want to generate graphs)
- HP Operations SPI Data Collector (DSI2DDF): 2.40
- HP SPI Self-Healing Services. (SPI-SHS-OVO, automatically installed while installing the SPI using SPIDVD): 3.00
- Software Upgrade Tool Kit: 2.0
- VC-Redistributable for all manually installed DCE (7.35 or higher) managed nodes. VC-Redistributable can be located at %OvAgentDir% on managed node.

On the managed node:

- HP Operations Agent (version 8.53 or 8.60 (HTTPS) and 7.35 (DCE)) installed and configured
- HP Performance Agent: 5.00 (required if you want to use HP Performance Agent for data logging)

Software Prerequisites on Management Server

Install HPOM console, Management Server, and agents to enable the Microsoft Active Directory SPI.

Installing the Microsoft Active Directory SPI

You can install the Microsoft Active Directory SPI on a remote console or a management server.

Installing the Microsoft Active Directory SPI on a Remote Console

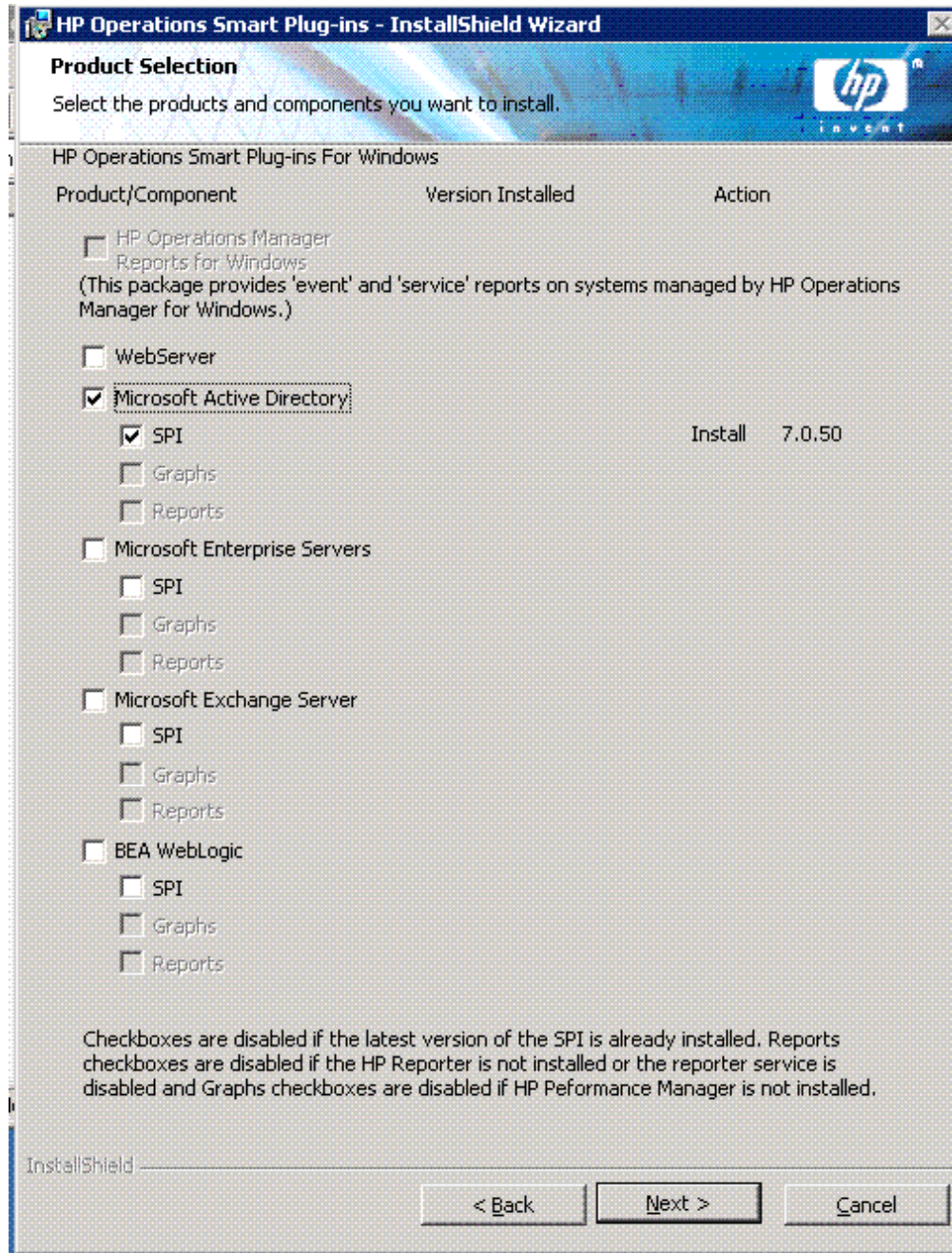
Install only the Microsoft Active Directory SPI console packages on the HPOM remote consoles.

Installing the Microsoft Active Directory SPI on a Standalone Management Server

The HP Operations Smart Plug-ins DVD contains the Microsoft Active Directory SPI.

- 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 Active Directory** check box, and then click **Next**. The Enable/Disable AutoDeployment screen appears. Select Graphs and Reports check box also if HP Performance Manager and HP Reporter are installed.
- 5 Select the **Enable** button, 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 Active Directory SPI.
- 8 Click **Finish** after the installation is complete.

Installing the Microsoft Active Directory SPI in an HPOM Cluster Environment

Before installing the Microsoft Active Directory SPI in a cluster environment, make sure that HPOM for Windows 8.10 is installed on each system of the cluster.

- ▶ The HPOM console does not function properly until you install the Microsoft Active Directory SPI on all nodes in the HPOM cluster.

Task 1: [At the first cluster-aware management server, select and install Smart Plug-ins.](#)

Complete the steps described in [Installing the Microsoft Active Directory SPI on a Standalone Management Server](#) before proceeding to the next management server.

- ▶ Before beginning, ensure that sufficient disk space is available on each management server for the Microsoft Active Directory SPI. Cancelling the installation process before completion can result in partial installations and require manual removal of the partially installed components.

Task 2: [At the next cluster-aware management server, install pre-selected Smart Plug-ins.](#)

Repeat the steps described in [Installing the Microsoft Active Directory SPI on a Standalone Management Server](#) 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.

- ▶ The HPOM console does not function properly until installations are completed on all the managed nodes in the cluster.

Upgrading the Microsoft Active Directory SPI

You can upgrade the Microsoft Active Directory SPI on a remote console, on a management server, and on clustered environment.

Use the common installer to detect if any previous version of Microsoft Active Directory 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.

- ▶ Delete all policies under the policy groups SPI for Active Directory → Windows Server 2003 / Windows Server 2008 → Auto Deploy → Discovery → Advanced Discovery

Upgrading the Microsoft Active Directory SPI on a Remote Console

If you use 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 the Microsoft Active Directory SPI on a Standalone Management Server

Perform the following tasks to upgrade the Microsoft Active Directory SPI on a management server:

Task 1: Prepare to install the later version of the Microsoft Active Directory SPI

Before you install the HP Operations Smart Plug-ins DVD, complete the following steps. These steps enable retention of customizations (as necessary) and successful discovery of additional services:

- 1 Remove the Microsoft Active Directory SPI discovery policies:
 - a At the console, click **Operations Manager** → **Policy Management** → **Policy Groups** → **SPI for Active Directory** → **en** (or **ja**) → **Windows Server 2008** (or **Windows Server 2003**) → **Auto Deploy** → **Discovery** → **Basic Discovery**.
 - b Right-click **Discovery**, and then select **All Tasks** → **Uninstall from...**
 - c Select **Nodes** which run on the Microsoft Active Directory environment, and then click **OK**.

You can select all the managed nodes to remove the Microsoft Active SPI discovery policies.
- 2 Rename the Microsoft Active Directory SPI policy group:
 - a At the console, select **Operations Manager**.
 - b Double-click **Policy management**, and **Policy groups**.
 - c Select the **SPI for Active Directory** group and right-click it to rename it (for example, **SPI for Active Directory_OLD**).

3 Gather data from all the managed nodes.

Gather all the previous data sources from all the managed Microsoft Active Directory nodes. To accomplish this, follow these steps on HP Reporter Server:

- a Make sure that you install the .NET Framework 2.x (or higher) on the HP Reporter server. Insert the HP Operations Smart Plug-ins DVD on the HP Reporter server.
- b Open the command prompt and run the following command to set the HP Reporter trace level to 9:

```
repmaint -trace 9
```

- c Run the discovery command to discover all the managed nodes on the HP Reporter server. Make sure that all the Microsoft Active Directory managed nodes are discovered by checking the %OvDataDir%\trace.discover file.

- d Open a command prompt and browse to the following path:

```
<DVD-Drive>\SPIs\AD SPI
```

- e Make sure that all the Microsoft Active Directory managed nodes are discovered by HP Reporter, and then run the following command:

```
ADSPI_run_gatherCODA.exe <reporter_system_dsn> <reporter_db_username>  
<reporter_db_password>
```

In this instance, <reporter_system_dsn> is the system DSN for the HP Reporter database;

<reporter_db_username> and <reporter_db_password> are the user name and password to access the HP Reporter database.

- f Check the %OvDataDir%\trace.gather file for any errors. Make sure that the data is collected for all the metric lists from all the managed Microsoft Active Directory nodes.

Task 2: Install the later version of the Microsoft Active Directory SPI

- 1 Insert the HP Operations Smart Plug-ins DVD and follow the instructions as they appear on the screen. See [Installing the Microsoft Active Directory SPI](#).
- 2 Select **Microsoft Active Directory SPI** to install.

Task 3: Customize the policies of Microsoft Active Directory SPI, if required.

Use Software Upgrade Tool Kit 2.0 to retain the customization of the previous versions of the Microsoft Active Directory SPI policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

If you choose to customize one or more policies after deploying them, ensure to redeploy the policies after customizing them.

Task 4: Deploy updated instrumentation.

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

- 1 At the HPOM console, open **Operations Manager** → **Nodes**.
- 2 Right-click any managed node which runs on the Microsoft Active Directory environment (or the Microsoft Active Directory group).
- 3 Select **All Tasks** → **Deploy instrumentation**.

- 4 From the Instrumentation Files area, select **ActiveDirectory_Core** and **ActiveDirectory_Discovery**, and then click **OK**.
- 5 Repeat steps 1 through 5 as necessary for the remaining nodes which run on the Microsoft Active Directory environment.

Task 5: Remove data sources from the nodes

This version of Microsoft Active Directory SPI uses a different format of data to be logged into the data stores on the managed nodes, which is used by HP Reporter. Hence delete the previous version of the Microsoft Active Directory SPI data stores before creating the updated data stores. To remove all the older data sources, perform these steps:

- 1 Deploy the **SPI Data Collector** and **ActiveDirectory_Core** instrumentation groups on all Microsoft Active Directory nodes.
- 2 Run the Delete Older ADSPI Classes tool on all the managed which run on the Microsoft Active Directory environment.

Task 6: Configure the Microsoft Active Directory SPI

Perform the steps mentioned in [Configuration Procedure of Microsoft Active Directory SPI](#) on page 29.

Upgrading the Microsoft Active Directory SPI in an HPOM Cluster Environment

Before upgrading the Microsoft Active Directory SPI in a cluster environment, make sure that HPOM for Windows 8.10 is installed on each system of the cluster.



The HPOM console does not function properly until you upgrade the Microsoft Active Directory SPI on all the managed nodes in the HPOM cluster.

Task 1: At the first cluster-aware management server, select and install Smart Plug-ins.

Complete the steps described in [Upgrading the Microsoft Active Directory SPI on a Standalone Management Server](#) on page 23 before proceeding to the next management server.



Before beginning, ensure that sufficient disk space is available on each management server for the Microsoft Active Directory SPI. Cancelling the installation process before completion can result in partial installations and require manual removal of the partially installed components.

Task 2: At the next cluster-aware management server, install pre-selected Smart Plug-ins.

Repeat the task 1 (steps 1 and 2 only), task 2-4 and task 6 in [Upgrading the Microsoft Active Directory SPI on a Standalone Management Server](#) on page 23 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



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

Verifying the Installation/Upgrade of Microsoft Active Directory SPI

To verify the Microsoft Active Directory SPI has been installed/updated properly check any one of the following:

- Check the SPI under policy group. Expand **Policy Group** under **Policy Management**. The **SPI for Active Directory** in the list verifies the installation. You can further expand **SPI for Active Directory** and check for **Windows Server 2003** and **Windows Server 2008**.

The screenshot displays the HP Operations Manager interface. The top window is titled "Operations Manager : BT \Policy management \Policy groups". The left pane shows a tree view with "Policy management" expanded to "Policy groups". The right pane lists various policy groups, including "SPI for Active Directory".

The bottom window is titled "Operations Manager : BTOVM33 \Nodes". The left pane shows a tree view with "Nodes" selected. The right pane displays a table of events:

Severity	Duplicates	S	U	I	A	O	N	Received
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0
Warning	47	-	-	X	-	-	-	6/10/2009 2:0

- Verify that the policies and binaries have 7.00 version.

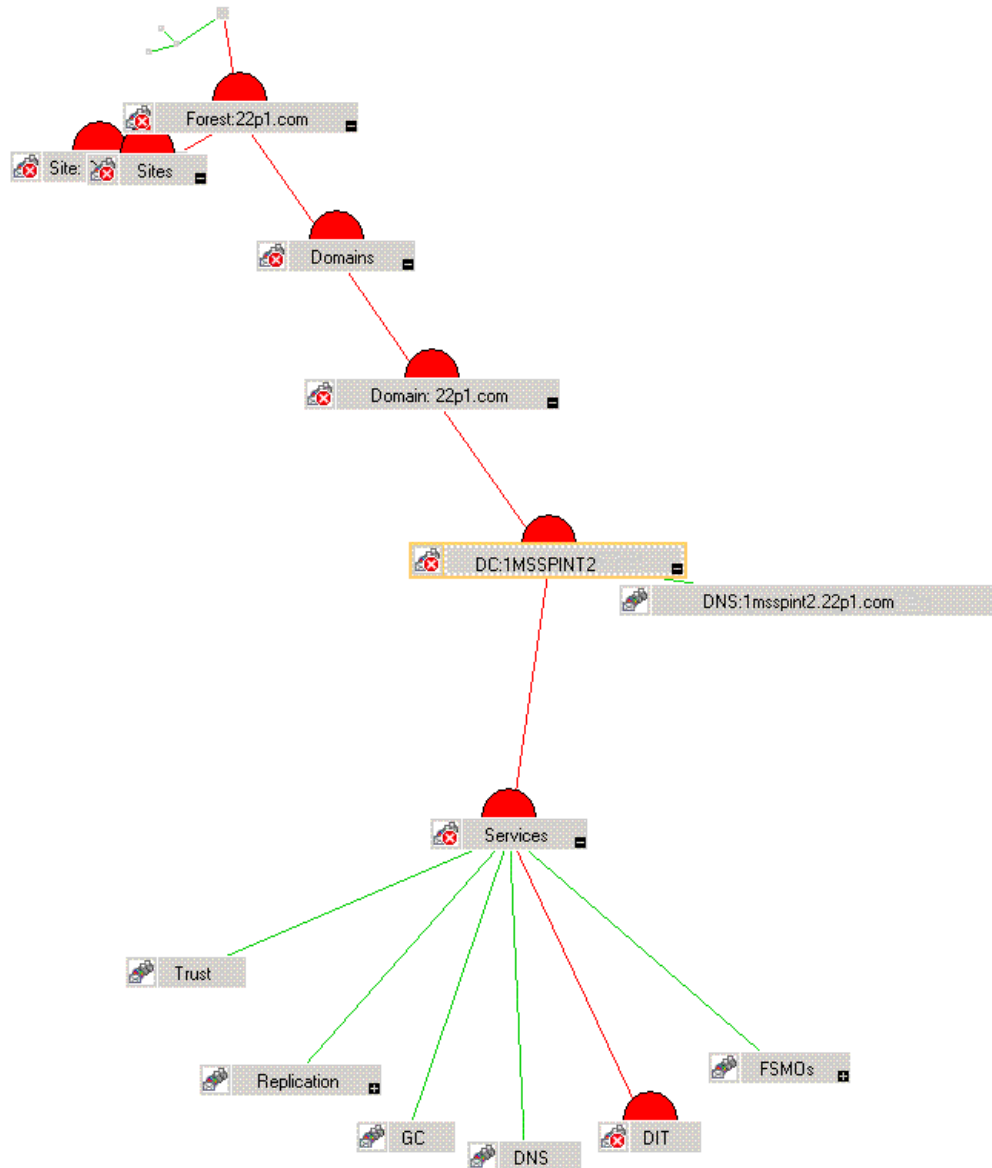
3 Configuring Microsoft Active Directory SPI

The Microsoft Active Directory SPI monitors the Microsoft Active Directory by discovering the existing components of the Microsoft Active Directory and maintaining the thresholds set up by the Microsoft Active Directory SPI policies. The Microsoft Active Directory SPI adds multiple hierarchical levels of details.

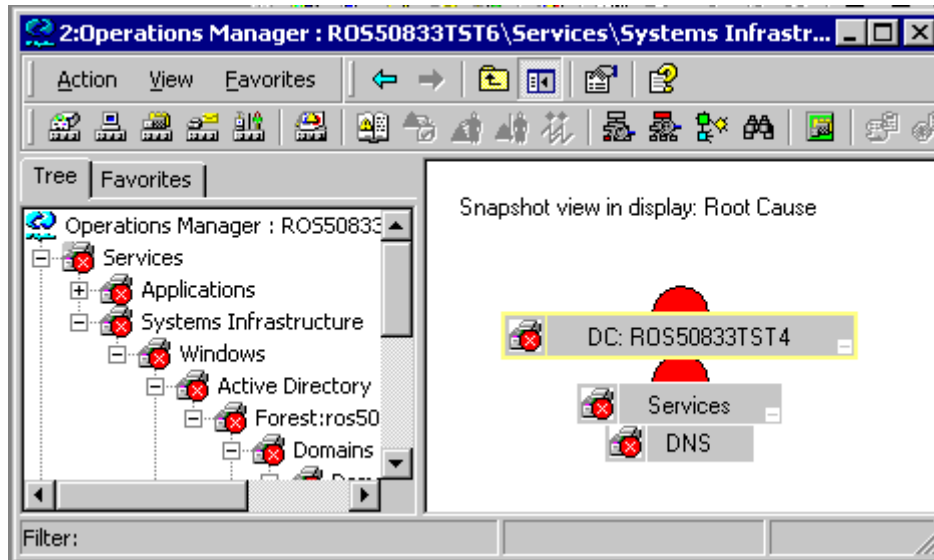
At a higher level, the Microsoft Active Directory SPI discovers forests. It then discovers each DC with its name. Lastly it discovers the Microsoft Active Directory services and components available including sites, the preferred PBHS connecting the sites, replication, and sysvol.

In this way the Microsoft Active Directory SPI shows partitions in the discovered sites. This is shown in the service map. With each expansion you can drill down from a service alert at the forest level to the specific service or component in a specific DC that is the root cause.

View in display: Contains or Uses



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**.



Configuration Procedure of Microsoft Active Directory SPI

Perform the following tasks to configure the Microsoft Active Directory SPI.

Change Unmanaged Node to Managed Node

To change unmanaged node to a managed node, add the nodes to the HPOM console's nodes folder. By adding nodes, you can launch an automated service discovery process that duplicates the manually invoked process. To change unmanaged node to managed node, perform the following steps:

- 1 In the 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:
 - In the left pane double-click each node you want to add.
 - Drag and drop nodes from left to right.
 - In the left pane, right-click each node, and then select **Manage**.
- 3 (As needed) 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**.

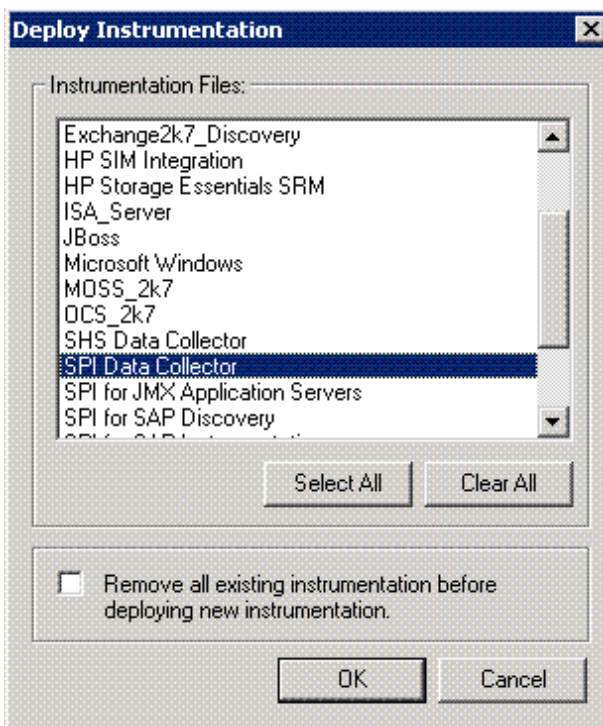
Deploy Instrumentation Categories on Managed Nodes

Deploy the following instrumentation categories for the Microsoft Active Directory SPI:

- SPIDataCollector
- ActiveDirectory_Core
- ActiveDirectory_Discovery

To deploy instrumentation, perform the following steps:

- 1 In the console tree of HPOM, right-click a node and select **All Tasks**. Select **Deploy instrumentation....** The Deploy Instrumentation box opens.
- 2 Select the mandatory instrumentation category, **SPI Data Collector**.
- 3 Select **ActiveDirectory_Core** and **ActiveDirectory_Discovery** categories, and then click **OK**.
- 4 Perform steps 1 through 3 for all the Microsoft Active Directory SPI managed nodes.



Discover Services on the Managed Nodes

Deploy the discovery policy to discover the existing Microsoft Active Directory services on the managed nodes. To discover services, perform the following:

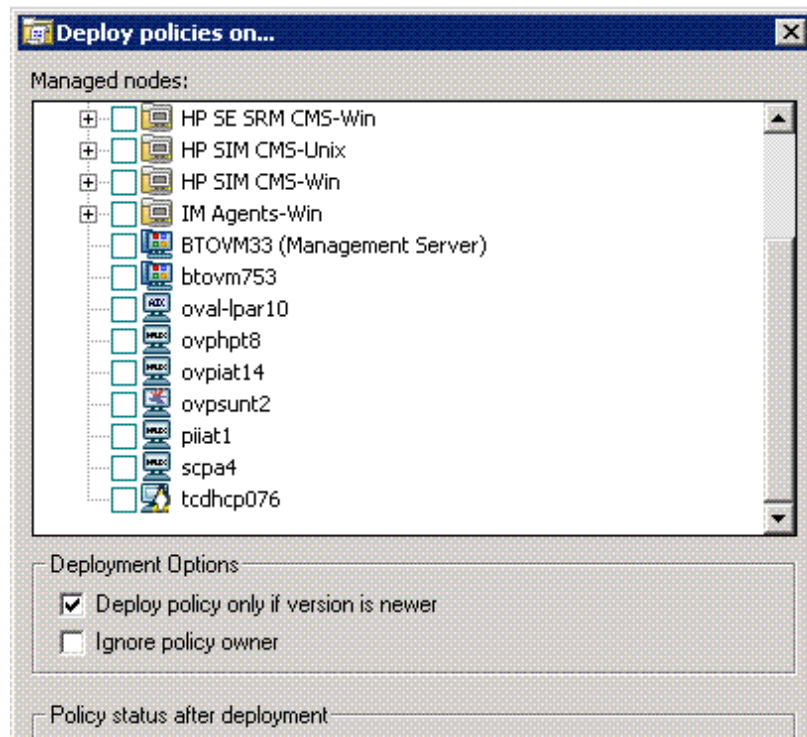
- 1 In the console tree, expand **Policy Management** → **Policy Groups** → **SPI for Active Directory** → **en** (or **ja**) → **Windows Server 2008** (or **2003**) → **Auto Deploy** → **Discovery** → **Basic Discovery**.



Select your language interface as English (**en**) or Japanese (**ja**). Select the policy group as **Windows Server 2008** or **Windows Server 2003**.

- 2 Right-click **Basic Discovery**, and select **All Tasks** → **Deploy on....**

- 3 In the **Deploy policies on...** dialog box, select all the Microsoft Active Directory managed nodes, and then click **OK**.



- 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**.

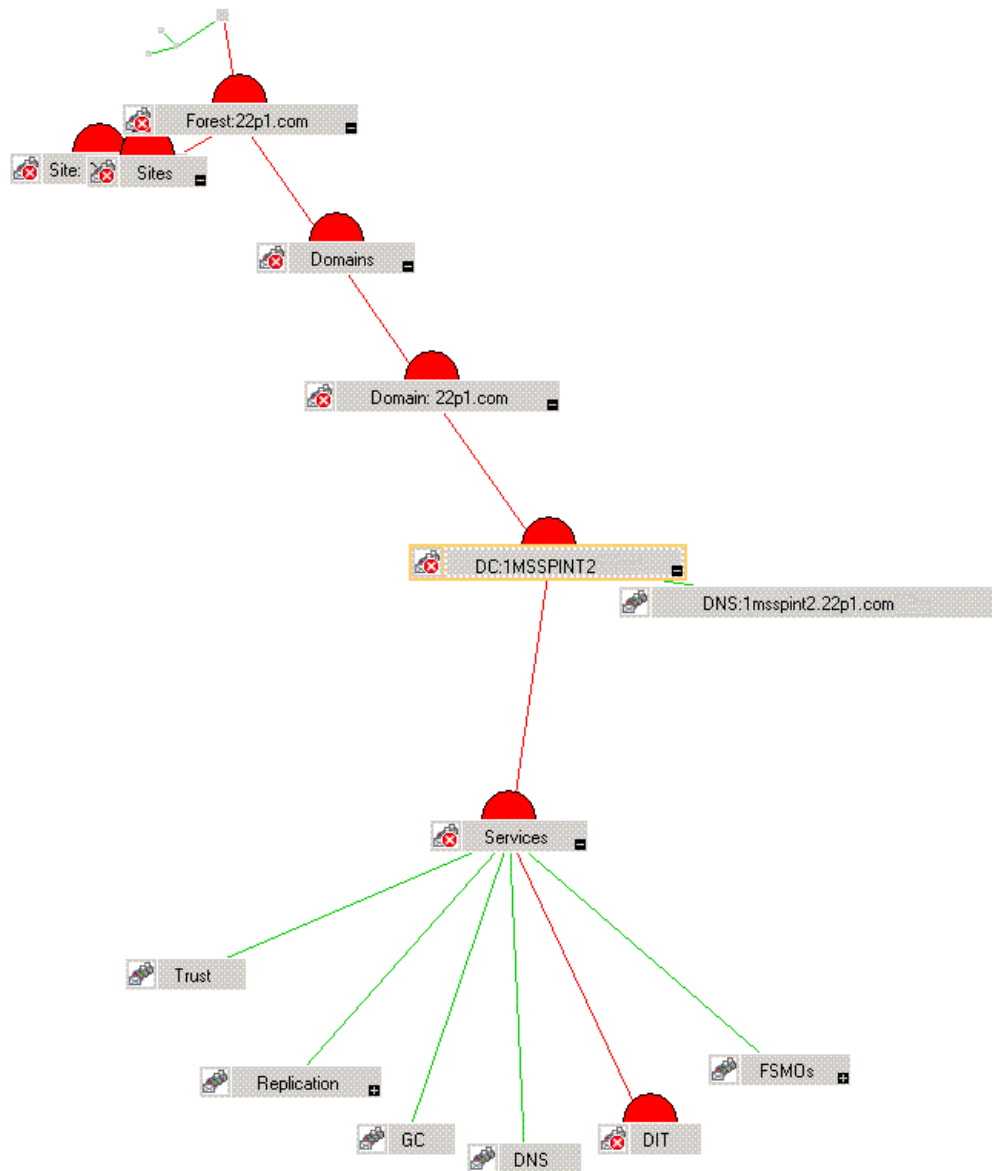
In the tiled window, you can see the executed processes of the Microsoft Active Directory—directory information tree (DIT), Replication, PBHS, Sysvol, Trust, DNS, flexible single master operations (FSMO), GC services discovered and the service map updated.



If you do not enable the **Auto-Deploy** option on a managed node, ensure to deploy the **Advanced Discovery** policy under **Policy Management** → **Policy Groups** → **SPI for Active Directory** → **en** (or **ja**) → **Windows Server 2008** (or **2003**) → **Auto Deploy** → **Discovery** manually to that node to complete the discovery process.

Starting at the **Services** → **Systems Infrastructure** → **Active Directory** of the console tree (in the left pane), you can navigate downward to each DC (DC: <name>), under which you can see a **Services** folder that contains the required components such as DIT, DNS, FSMOs, GC, Sysvol, and Replication.

View in display: Contains or Uses



Among the components of the Microsoft Active Directory; DIT, Replication, Sysvol, and Trust services form the core part. Other components such as DNS, FSMO, and GC are optional depending on your Microsoft Active Directory environment.

Create Data Sources

The Microsoft Active Directory SPI collects metric data on the managed nodes, and logs the data to a data store on the managed nodes.

Data sources must be created in CODA (or HP Performance Agent) to enable the policies to log data. The policy **ADSPI-CreateDataSources** under the **Policy groups** → **SPI for Active Directory** → **en** (or **ja**) → **Windows Server 2008** (or **Windows Server 2003**) → **Auto-Deploy** → **Discovery** → **Advanced Discovery** creates the required data sources in the data store of the HP Operations agent or HP Performance Agent.



Ensure to deploy the instrumentation category **SPI for Data Collector** before running this policy on the managed nodes.

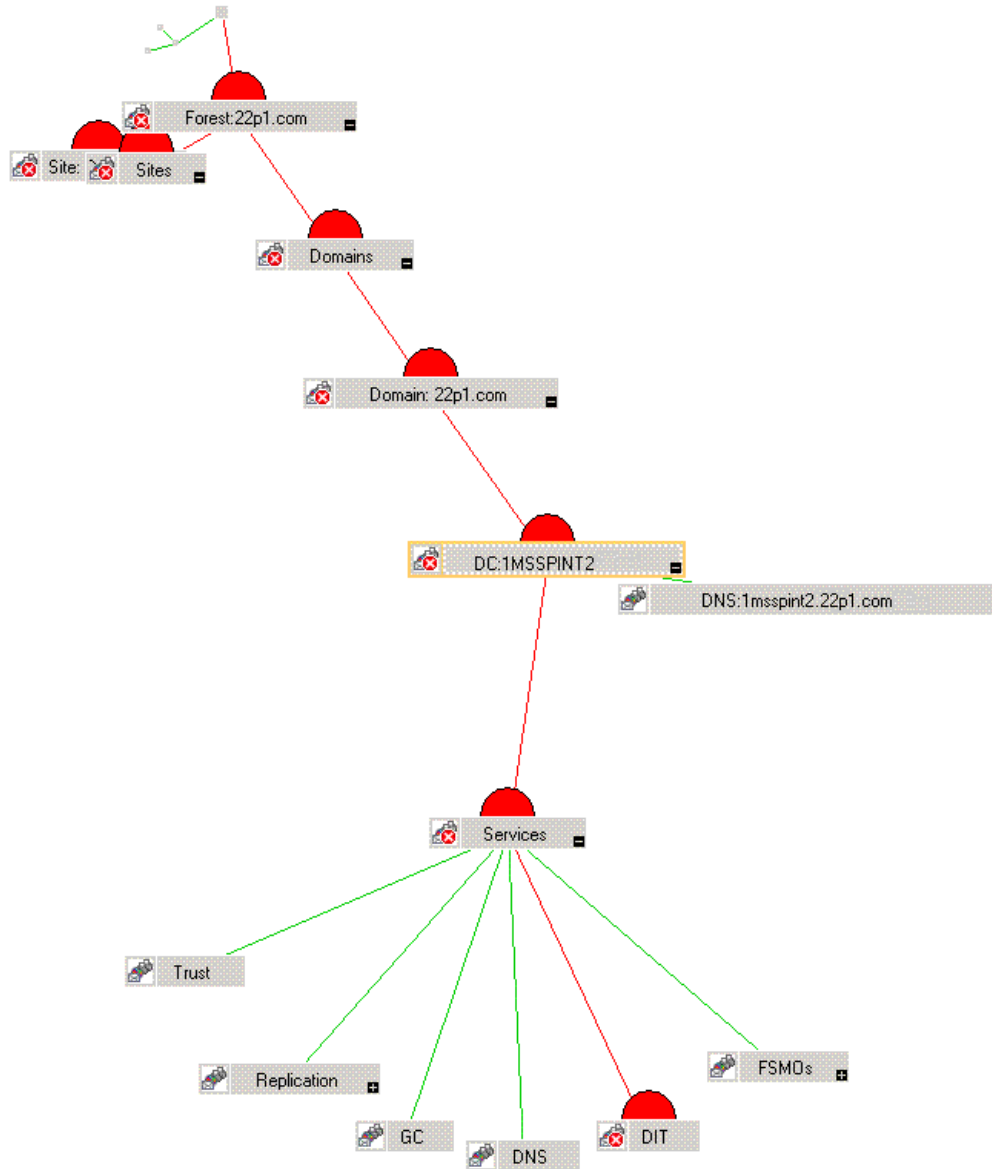
View the Microsoft Active Directory Service Map

After the auto-discovery has occurred, you can now see the discovered services graphically represented under domains and sites within the HPOM service map.

- 1 In the console details pane select **Services** → **System Infrastructure**.
- 2 Select **Active Directory**.

In the console tree, when you select **Services**, you can view the service map in the right pane. You can see domains, sites, and DC names. For nodes managed by OVO or HPOM, you can now see discovered services or components, or both under the **Services**. You can further expand each component, for example FSMO to show the specific master operations services on the selected DC.

View in display: Contains or Uses



Customize Policies

You can customize the manual deploy policies, if required. To customize the policies, perform the following:

- 1 Right-click the policy and select **All Tasks**, and then **Edit...**
- 2 Click the **Thresholds level** or **Options** tab or both customize. Set the required thresholds and other options, if required.
- 3 Click **Save and Close**.



If you customize the policies after deploying them, you must redeploy the customized policies. For more details on customizing policies, see [Chapter 4, Customizing Policies](#).

Use Software Upgrade Tool Kit 2.0 to retain the customization of the earlier versions of the Microsoft Active Directory SPI policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

Deploy Microsoft Active Directory SPI Policies

You can choose Microsoft Active Directory SPI policies from the policy group to deploy on nodes.

If the policy-auto deployment setting, while installing the Microsoft Active Directory SPI, is enabled, the discovery policies are automatically deployed on the already added Microsoft Active Directory nodes, and then the Microsoft Active Directory SPI deploys the necessary auto-deploy policies.

If the policy-auto deployment setting is disabled, you must manually deploy the appropriate auto-deploy policies on the nodes.

To deploy the Microsoft Active Directory SPI policies, perform the following:

- 1 In the console tree, expand **Policy management** → **Policy groups** → **SPI for Microsoft Active Directory** → **en** (or **ja**) → **Windows Server 2008** (or **Windows Server 2003**).
- 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 on all the nodes.

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, perform the following:

- 1 Create a folder `dsi2ddf` in the path `%OvAgentDir%\Conf`, if it does not exist.
- 2 Create an empty file `nocoda.opt`.
- 3 Enter the names of the other data sources *except ADSPI*, which are to be created and for which the data logging has to happen in Performance Agent into the file `nocoda.opt`.

The data source ADSPI is created and data logging happens in CODA.

For more details on data store metrics and policy logging details, see *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* or *HP Operations Smart Plug-in for Microsoft Active Directory Online Help PDF*.

4 Customizing Policies

Policies monitor the Microsoft Active Directory environment and run according to rules and schedule specifications. Measurement threshold policies contain the rules for interpreting Microsoft Active Directory states or conditions.

You can customize specific policies to suit your requirements of the Microsoft Active Directory environment.

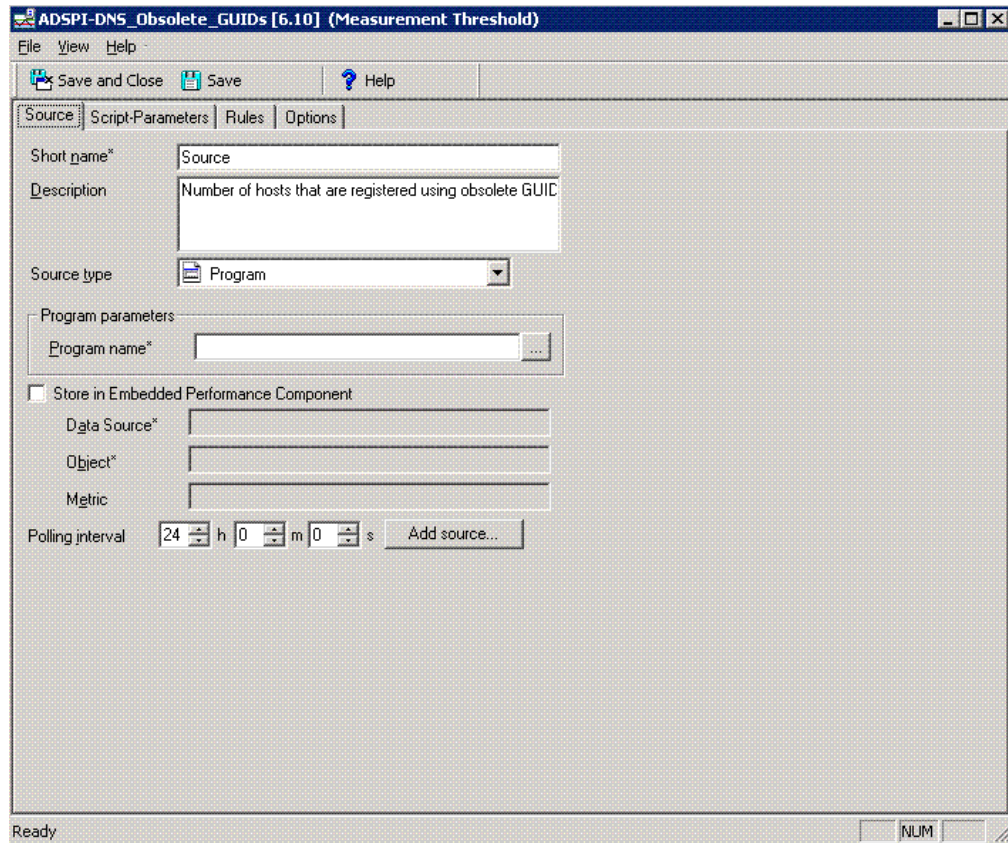
- ▶ Use Message Identifier to find the exact source of the message from the Microsoft Active Directory SPI policies.

See *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* for details of each Microsoft Active Directory policy and their data store details.

Customizing Default Policies

Double-click the specific policy to modify one or more conditions of the policy. Click **Policy management** → **Policy groups** → **SPI for Active Directory** → **en** → **Windows Server 2003 (or 2008)** → **Auto Deploy**. Some of the modifications that can be performed are:

- Script-parameters
- Rules
- Options



Use Software Upgrade Tool Kit 2.0 to retain the customization of the earlier versions of the Microsoft Active Directory SPI policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

Customizing Monitoring Schedule or Measurement Threshold Policies

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

- 1 Expand the **Agent policies grouped by type**, and select **Scheduled Task**.
- 2 In the details pane of the console double-click the specific policy, for example, ADSPI *<policy name>*.
- 3 Select the **Schedule** tab and modify the scheduled task as desired.

Creating Custom Data Collection Groups

You can create custom data collections to change the monitoring intervals or thresholds or both for a single DC. To create a separate group of policies, copy the desired policies into a folder with the new group name. After you have pasted 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 the managed nodes and policies together in groups that are easily recognizable.

Deploying Policies

The policies for the Microsoft Active Directory SPI in the HPOM console are organized as Policy Group and Policy Type. The *HP Operations for Microsoft Active Directory SPI Online Help* provides the policies available in each policy group.

Policy Group

A policy group organizes policies according to the deployment method and area to be targeted for discovery or monitoring. Deployment can be auto and manual. To view auto and manually deployed policies in the Microsoft Active Directory in your environment, perform the following steps:

- 1 Expand **Policy groups**, and click **SPI for Active Directory** in the console tree.
- 2 Click **en** (or **ja**) as the language interface.
- 3 Select **Windows Server 2003** or **Windows Server 2008**.
- 4 Select **Auto-Deploy** or **Manual-Deploy**.

The policies in each deployment are displayed. The **Auto-Deploy** group enables you to deploy all subgroups at the same time. You can further choose a specific task from the subgroup. For example, **Discovery** → **Advanced Discovery** or **Basic Discovery**. You can choose an area to monitor such as DIT, DNS, FSMO, or Trust.

Policy Type

Agent policies grouped by type organize policies according to type. For example, you can find the scheduling for GC, replication, or FSMO monitoring in *Scheduled Tasks* policies and you can find the conditions of thresholds for those replication or FSMO policies in the *Measurement Threshold* policies.

Using Auto-Deploy Policies

The Auto-Deploy policies of Microsoft Active Directory SPI are divided into logical groups; one for the discovery services and the others for monitoring the Microsoft Active Directory services and components such as DIT, DNS, GC, FSMO, replication, response time, and trust relationships. The following sections describe the various sub-groups of the Auto-Deploy policies and their functions.

Discovery

Microsoft Active Directory SPI includes *service discovery* policies that can detect DIT, DNS, FSMO, RODC, PBHS, replication, GC, and trust services and components running on the managed nodes.

DIT Monitoring

Checks the size and activity of the Microsoft Active Directory database known as the DIT and monitors the amount of free space. It also tracks the number of operations pending against the DIT.

DNS Monitoring

DNS monitoring policies check the existence, visibility, and validity of various service resource records on a DNS server. The SRV records enable DNS clients to locate specific services available on other servers; when a DNS policy encounters missing or incorrect information, it sends an alert to the HPOM message browser. Other policies check the responsiveness and availability of specific DNS servers and DNS services used by the Microsoft Active Directory.

FSMO Monitoring

Through binds and pings, this policy monitors general responsiveness of operations master services that include domain naming, schema master response, infrastructure master, schema master PDC master, and RID master (RID pool requests).

Replication Monitoring

Replication policies can measure the time required to propagate a change to all DCs within the domain. In addition, this policy can also monitor the replication time of inter-site and intra-site replication latency. Replication policies are run regularly to modify a Microsoft Active Directory latency object to determine acceptable or unacceptable response times or conditions or both.

Response Time Monitoring

Response time policies measure the general responsiveness of Microsoft Active Directory and the responsiveness of the GC binds and queries.

GC Monitoring

These policies measure the time required for the GC to replicate from two perspectives:

- DC providing the service (GC) and
- DC accessing the service (DC).

Sysvol Monitoring

These policies monitor Sysvol file replication service (FRS), Sysvol size, connectivity, and synchronization with Group Policy Objects (GPOs), all of which are major indicators of Microsoft Active Directory health.

Trust Monitoring

These policies monitor trust status and gather data that allows the Trust Relationships tool to provide updates in changes within the trust relationships in Microsoft Active Directory.

Using Manual-Deploy Policies

The Manual-Deploy policies of Microsoft Active Directory SPI are not automatically deployed, after the Microsoft Active Directory service occurs. The manual-deploy policies offer basic monitoring that cover areas of the Microsoft Active Directory involving connectivity, domain, and organization unit structure, health, index and query, replication or replication activities or both, security, and site structure. The following sections describe the various sub-groups of the Manual Deploy policies and their functions.

Auto-Baseline Policies

Auto-baseline Policies make use of historical data logged into the data store (CODA) to calculate threshold.



- Auto-baseline policies do not work on nodes configured with HP Performance Agent.
- If you have upgraded the Microsoft Active Directory SPI from a previous version, the auto-baseline policies cannot use the historical data of the previous version of the Microsoft Active Directory SPI.

Auto-baseline policies calculate threshold values based on the analyzed historical data. Every auto-baseline policy associates the *trust* status with every generated alert. The auto-baseline policies assign three types of trust status to the generated alerts:

- **Low Trust:** Threshold value calculated with less than two weeks of data.
- **Medium Trust:** Threshold value calculated with less than three weeks of data.
- **High Trust:** Threshold value calculated with up to four weeks of data.

The auto-baseline policies use the standard deviation method to calculate the threshold value. These policies use the following mechanism to calculate the threshold:

- The policy reads the historical values of the metric that it is monitoring. The historical values are stored into the data store.
- The policy calculates the arithmetic mean of the values of the metric.
Arithmetic mean = Sum of all historical values/ Number of all historical data points
- The standard deviation of the metric is calculated with the following details:
 - Arithmetic mean of the metric
 - Historical data point
 - Number of all historical data points
- The policy sets a range of threshold values using the following calculation:
 - Maximum threshold = Arithmetic mean + Standard deviation
 - Minimum threshold = Arithmetic mean - Standard deviation
- The policy generates an alert when the metric value does not belong to the threshold range.

In the embedded vbscript of the AutoThreshold policies, there is a logic to evaluate the current value based on the historical values and then alert as described further. First, from the historical values logged into the data store (CODA), standard deviation is calculated. The 1st Standard deviation consists of 68% of the historical data, 2nd Standard deviation consists of 95% of the historical data, and 3rd Standard deviation consists of 99% of the data. The policy then calculates the current value, which is an average of the metric values for the last one hour.

The current value falls in the range which would be either above or below a particular Standard deviation, that is, 68% / 95% / 99%. As the severity indicates, whenever the current values falls below the 1st Standard deviation, a warning message is generated, along with an attribute which says whether the current value is "above/higher" or "below/lower" the Standard deviation.

Connector Policies (Only for Windows Server 2003)

These policies use Microsoft Active Directory Connector performance monitor counters to check activities occurring around connection issues involving logon authentication, pages in memory (working set), page faults, warnings, errors, and processing time.

Domain and OU Structure

These policies monitor domain and organization unit (OU) changes.

Global Catalog Access

These policies monitor GC servers, gathering data from their performance monitor counters in regards to reads or writes or searches or all of the directory.

Health Monitors

These policies check the areas of the Microsoft Active Directory involving services, events, processes, and synchronizations essential to its performance. Key services and their associated processes include Kerberos Key Distribution Center (KDC), NetLogon, NT LM Security Support Service, directory, and Security Account Manager. Log monitoring checks for the occurrence of specific events in the Windows Event Log and the System log.

Index and Query

Monitors index and query activity for authentications, LDAP client sessions and others.

Replication

Monitors replication through measurement of inbound objects between and within sites, verification of synchronization of replication updates, pending updates, and queue size in replication inbound objects.

Replication Activity

Monitors the Directory Service log of the Microsoft Active Directory for replication events.

Security

These policies monitor:

- Security event logs for Microsoft Active Directory related events
- Security group changes
- Performance monitor counters associated with Security

Site Structure

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

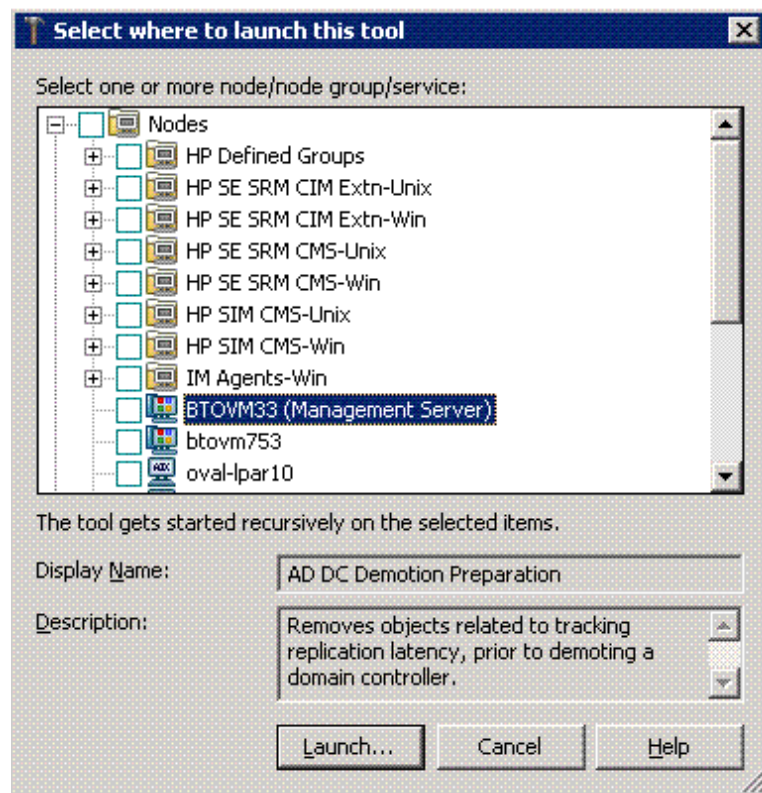
5 Using Tools

The Microsoft Active Directory SPI uses different tools to gather information on the Microsoft Active Directory environment. For more information on the description of the tools, see the *HP Operations Smart Plug-in for Microsoft Active Directory SPI Online Help* or *HP Operations Smart Plug-in for Microsoft Active Directory SPI Online Help PDF*.

Launching Tools

Perform the following to launch the Microsoft Active Directory tools:

- 1 Click **Tools** → **SPI for Active Directory**.
- 2 Right-click the tool to be launched. For example, **AD DC Demotion Preparation**. Click **Launch**.
- 3 Select the managed nodes where the tool is to be launched and click **Launch....**



AD Trust Relationships Tool

The AD Trust Relationship tool, when launched on the Microsoft Active Directory managed node, generates information about the DC and its trust relationship within its domain that includes trust type, trust status, and the tree (in the console) in which it resides.

```
Tool Output:

Local Domain Information -----
DCName: .....ADSPI1
DNSName: .....adroot.system.usa.com
FlatName: .....ADROOT
SID: .....S-1-5-21-2532656728-2936649530-232323232
TreeName: .....adroot.system.usa.com

Trust Relationships -----
FlatName: .....ADNCROOT
SID: .....S-1-5-21-1667343185-2871001565-
TrustAttributes: .....0
TrustDirection: .....Bi-directional
TrustedDCName: .....\\adspi2.adncroot.system.usa.com
TrustedDomain: .....adncroot.system.usa.com
TrustIsOk: .....True
TrustStatus: .....0
TrustStatusString: .....OK
TrustType: .....Uplevel
FlatName: .....ADCHILD
```

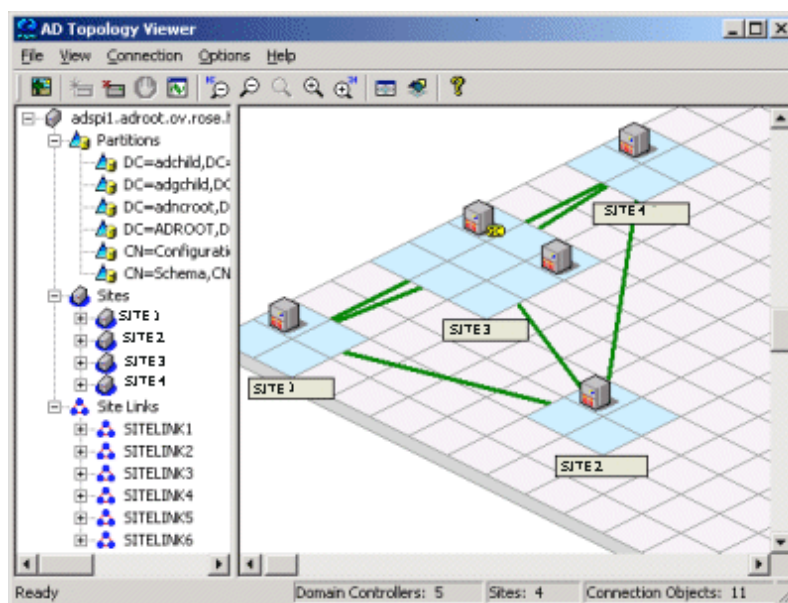
Using HP Operations Topology Viewer Tool

HP Operations Topology Viewer tool provides a simple means of viewing the content and topology of the Microsoft Active Directory of your environment by generating a map. After you launch the tool, you must *connect to a DC* to enable the functioning of the tool. After the connection is established, a window opens which displays information about the Microsoft Active Directory partitions and connections and its link as replicated across the Microsoft Active Directory environment. This tool enables a view of the Microsoft Active Directory information in two ways:

- **Expandable or collapsible tree:** In the left pane of the HP Operations Topology Viewer window, you can see various components that comprise a Microsoft Active Directory forest and its domains, the domain which hosts the DC, and the sites available through the connection.
- **Topological view of site connections:** The right-pane of the window offers a graphical representation (a 3-dimensional map) of the configured sites, the servers located in those sites, site links, forests, DCs, GCs, and the connection objects linking them. You can move sites and DCs to accommodate more effective viewing in the map. Double-click a DC to retrieve additional information such as, the version of Windows that is running, status information, and so on. The map also has **zoom-in** and **zoom-out** functions and enables exporting the view of the topology to a bitmap image.

The HP Operations Topology Viewer tool is located in the console under **Tools** → **SPI for Active Directory**. This tool supplements the information which you receive from other components of the Microsoft Active Directory SPI and has no dependency on any of the policies. With the help of this tool you can quickly view the various site and server connections within the Microsoft Active Directory of your environment.

Figure 3 Dimensional View of Topology Viewer Tool



The Topology Viewer shows the site and server related information as a snapshot of the data retrieved at the time of the connection to the specified server. The data is not automatically updated; hence you have to refresh it. For this, select **Connection** → **Refresh Data**.



Modifications to the map's layout, however, are not preserved when you refresh the data.

Launching HP Operations Topology Viewer Tool

To launch the HP Operations Topology Viewer:

- 1 In the console, under **Operations Manager** → **Tools** → **SPI for Active Directory**, double-click **OV Topology Viewer** (on the service map).
- 2 Right-click **OV Topology Viewer** and select **All Tasks** → **Launch Tool...**
- 3 In the Window that appears, from the **Connection** menu, select **Connect to Server...**
Alternatively you can also right-click on the root node of the tree.
- 4 In the **Connect to Server...** window, enter the requested information, and then click **OK**.

After you launch the tool, connect to a DC in the Microsoft Active Directory forest. This single connection provides all the necessary data for the HP Operations Topology Viewer because each DC has the information that has been replicated across the forest on partitions, sites, site links, servers, and connections..



Your authentication becomes simple in case the HP Operations Topology Viewer is running on the same DC of which you are connected. In such case you have to enter only the DNS name or the IP address of the DC, as you are recognized as the logged-in user with the appropriate rights. Hence, no other alternate credentials are required.

Getting Started with the HP Operations Topology Viewer Tool

Each time you launch the HP Operations Topology Viewer tool and connect it to a DC, it presents two views in the form of tree (left pane) and the 3-dimensional map (right pane). Even though some of the information is the same, the dual-paned window presents you these two views. While the tree lists the components of the server, the right pane shows the relationship among these components.

The map shows only the site links represented by straight green lines. These site links are user-defined. They are the foundation on which the Microsoft Active Directory can build connections between servers.

Servers that function as InterSite Topology Generators (ISTGs) are identified with an **i** while servers that provide GC services display a **GC**.

- **Site link costs:** In addition to showing the established connections between the sites, site link costs show the associated *cost* of each connection. The site links with a lower cost can replicate data between those sites more easily than the site links with a higher cost.

To display the server connections represented by curved blue lines, select **View** → **Connections** → **Intersite** (or **Intrasite**).

- **Error connection lines:** Any server connection shown in red line indicates an error. This error occurs because a DC no longer exists and has been removed from the site, but whose connection object still remains on the inbound DC. This connection object could have been user-created (by System Administrator) or KCC-created. In either case, remove the connection object manually.

Accessing Functions of HP Operations Topology Viewer Tool

You can access the multiple features of the HP Operations Topology Viewer through its menu commands, toolbar, or mouse right-clicks within the areas of either side of the Window pane.

Adjusting Map View

You may find when you view the HP Operations Topology Viewer replication map that sites or servers do not appear within the viewable area. You may also want to resize the viewable area. These and other changes are possible as shown in Table 3.

Table 3 Adjusting Map View.

Tree/map modification	How to do it
To move sites to different locations on the map.	Drag and drop the site to desired map tiles.
To move servers.	Drag and drop to desired tiles within the site.
To move the entire map.	Press the middle button or press both right/left mouse buttons together; drag and release.
To display server or site labels.	From the View menu select Labels → Servers or Sites
To increase/decrease the size of the row/columns in the map's grid.	Right-click the unused space on or off the map and select Map Properties .
To find a site or server in the tree.	On the map, right-click the site or server on the map and select Find Site/Find Server in Tree . (Label appears in blue text.)
To find a server in the map.	In the tree, right-click on the site or server and select Find Site/Find Server on Map . (Label appears in blue text.)
Move a site outside the map area (two methods are available).	<p>Method #1:</p> <ol style="list-style-type: none">1 Pressing the left mouse button, click the site and start to drag and drop to the desired area.2 Still holding the left mouse button down, press the right button and continue moving in the desired direction. <p>Method #2</p> <ol style="list-style-type: none">1 Pressing the left mouse button, select the site and start to drag and drop to the desired area.2 Still holding the left mouse button down and use the arrow keys to change the view of the map.

Use the following keystrokes of the keyboard to move around the map.

Table 4 Keyboard Functionality

Keystroke	Map function
← left arrow	Scrolls the map view to the left approximately one tile width.
→ right arrow	Scrolls the map view to the right approximately one tile width.
↑ up arrow	Scrolls the map view up approximately one tile height.
↓ down arrow	Scrolls the map view down approximately one tile height.
Page Up	Scrolls the map view up approximately 20 tiles.
Page Down	Scrolls the map view down approximately 20 tiles
Shift+Page Up	Scrolls the map view to the left approximately 20 tiles.
Shift+Page Down	Scrolls the map view to the right approximately 20 tiles.
Home	Scrolls the map view to the left extent. (Vertical position remains the same).
End	Scrolls the map view to the right extent. (Vertical position remains the same).

HP Operations Topology Viewer menus

The HP Operations Topology Viewer menu commands are shown in Table 5.

Table 5 HP Operations Topology Viewer Menu

Menu	Command	Function
File	New...	Opens a new file (empty grid); allows you to transition from the current view to a new view.
	Open...	Opens a selected, saved file that shows the layout as it was saved.
	Save	Saves the layout as the default layout.
	Save as...	Saves the layout to a file so that you can load it when desired.
	Export View...	Saves the currently displayed map in a graphical format of your choice.
	Add Forest...	Opens the Add Forest dialog, where successful connection to a server generates the replicated information within that forest and displays the information in the HP Operations Topology Viewer tree and map.
	Refresh Data	Reconnects to the server and updates the view with changes, if any, since the last connection.












Menu	Command	Function
View	Zoom	Allows you to zoom-in closer for greatest magnification or zoom-out farther for overall view. Minimum is at greatest degree zoomed out. Maximum is at greatest degree zoomed in.
	Next View	Shows the next view available in the right pane.
	Navigator	Shows a thumbnail of the entire map (including any area outside the current display) with a blue box indicating the current visible display.
	Legend	Displays the legend, which explains the meaning of the symbols used in the map located next to each server.
	Clear Find	When enabled, means that a server or site in the tree or the map has been right-clicked and Find in View or Find in Tree selected, resulting in selecting the corresponding item; clicking Clear Find returns the display to its default status with no elements selected.




Menu	Command	Function
View	Toolbar	Toggles on/off the display of the Topology Viewer toolbar buttons.
	Status Bar	Toggles on/off the display of the Topology Viewer status bar (located at the bottom of the Topology Viewer window).
	Properties...	Opens the Site Topology Properties dialog, which allows you to hide/show elements in the map and to modify the map appearance.
Window	Title Page	Displays the HP Operations Topology Viewer title page.
	Site Topology	Displays the Active Directory topology of the current forest.
	Exchange Topology	Displays the Exchange messaging view (with routing groups) of the current forest.
Help	HP Operations Topology Viewer Help	Displays online Help for HP Operations Topology Viewer.
	About HP Operations Topology Viewer...	Displays the HP Operations Topology Viewer version number.

HP Operations Topology Viewer Toolbar

The HP Operations Topology Viewer toolbar functions are as shown in Table 5.

Table 6 HP Operations Topology Viewer Toolbar

Icon	Function
	Starts a new file, which appears as an empty grid; you can then click the Add Forest button to populate the empty view. The New button allows you to transition to a new view (for example, an Add a Forest), without adding to or changing the current view if the current view has been saved.
	Allows you to open a file of a previously saved view.
	Saves the current view to a file.
	Exports the current view and saves it to a graphic format of your choice, such as .png or .bmp. (The default format is .png.
	Allows you to add a forest by opening the Add Forest dialog, where you enter server connection information.
	Refreshes the data by checking information on the current connection.
	Zooms out the map view to the maximum degree.
	Zooms out the map view incrementally.
	Resets the map view to the default.
	Zooms in the map view incrementally.
	Zooms in the map view to the maximum degree.

Icon	Function
	Shows the next available top-level view in the forest.
	Displays the navigator, which shows a thumbnail of the entire map, surrounding the area of focus with a blue square. You can change the map focus by repositioning the blue square in the Navigator.
	Displays the Topology Viewer online Help.

Accessing Server and Map Properties

After you have successfully connected to a server, resulting in a populated tree and topological map, you can access the following information:

- **Server Properties:** Right-click a server in either the tree or the map to view the Server Properties sheet, which contains the following:
 - *Identification:* This shows the GUID assigned to the server, its fully qualified domain name, distinguished name, date created, the operating system and its version, and (if applicable) service pack and hot fix, as appropriate.
 - *Status:* This shows the Microsoft Active Directory server type. For example, GC and bridgehead.
 - *Partitions:* This shows all the named components associated with the server as displayed in the tree in the HP OV Topology Viewer tool. The components are grouped either within the master read-write components, or the replicating read-only components.
 - *Replication:* This shows information about the completed and pending replication operations.
 - *Partners:* This shows one or more replication partners for the selected server..



The availability of some information in the server (DC) property sheet depends on the access rights of the domain account used to connect to the Microsoft Active Directory domain.

- **Map Properties:** Right-click within any empty map cells (not occupied by a site) to view the Map Properties sheet, which contains the following information:
 - *Map size:* This shows the current map and tile sizes, which you can modify by using the bar sliders. Use **Reset** to return to the default settings.
 - *Spacing:* This shows the current number of columns and rows used to space sites, which you can modify by using the bar sizes. Use **Reset** to return to the default settings.

6 Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions

Reports and graphs provide a complete view of the performance of the components of the Microsoft Active Directory.

See *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* for complete details of each report and graph.

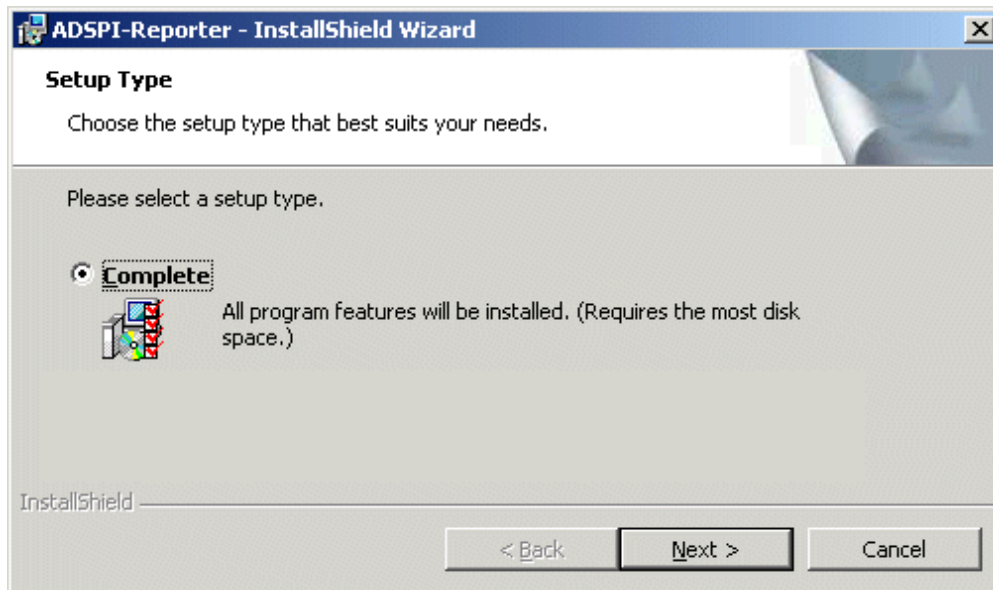
Using Reports and Graphs

Report- and graph-generating templates are installed after you install the Microsoft Active Directory SPI. They cover updates on the availability or the activity or both in Microsoft Active Directory components such as DIT, DNS, GC, replication, FSMO, Sysvol, and trust relationship changes for each DC running these services.

These Web-based reports are automatically generated every night and provide you with a routine means of checking GC and DNS availability, disk space, and queue length issues occurring with DIT, replication latency, and connection times specific to DCs running master operations services. Reports covering the trust relationship changes between DCs are also available for Windows 2003 and Windows 2008 nodes.

Integrating the Microsoft Active Directory SPI with HP Reporter

You must install ADSPI Reporter package on HP Reporter Server to use the Microsoft Active Directory SPI reports by running the `Setup.exe`. You can then configure the Reporter to generate reports.



Installing and/or Upgrading the Report Package

- ▶ Perform [step 3](#) on page 24 in [Upgrading the Microsoft Active Directory SPI on a Standalone Management Server](#) before upgrading the HP Reporter package for Microsoft Active Directory SPI.

To install and/or upgrade the Microsoft Active Directory SPI Report Package on a stand-alone Reporter server, perform the following:

- 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 till a dialog box opens indicating the completion of the installation.
- 3 Select **Finish** to complete the installation.

Configuring the Report Package

To configure the Microsoft Active Directory SPI Report Package, perform the following:

- 1 Open the Reporter main window and check the status pane to note the changes to the Reporter configuration, which include uploading the Microsoft Active Directory SPI reports.

The Microsoft Active Directory SPI Reports are automatically assigned to the ALL group in the Reporter main window. (See [Generating Reports](#) for HPOM Report list.)

- 2 Add group and single system reports by assigning reports as desired.

Reports are available for viewing the following day.



Identify the Microsoft Active Directory 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 Active Directory 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. See the topic “To assign a report definition to a Discovered Systems Group.” Reporter also includes two online documents: the *Concepts Guide* and the *Installation / Special Configurations Guide* for further information.

Generating Reports

After you install the Microsoft Active Directory SPI, the HPOM generates reports using the SPI-collected data for Microsoft Active Directory. 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.



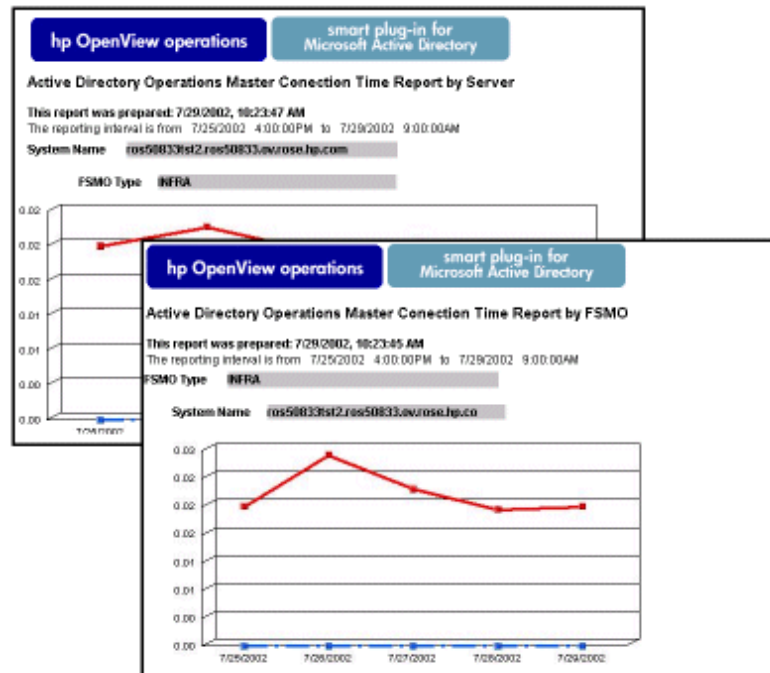
If you want to customize the reports you must install HP Reporter. The documentation on HP Reporter on modifying the reports is available in *Concepts Guide*, *Installation Guide* and *Special Configuration Guide*, Online Help, and Release Notes.

The report data of Microsoft Active Directory 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. The following example shows the metric variable identified for reporting purposes:

```
<report_table_name>.<Microsoft Active Directory SPI_metric_name>
```

is identified as ADSPI_RESPONSEMON.SYSTEMNAME

You can access the reports of SPI for Microsoft Active Directory from the **Reports** area of the HPOM console. You can find complete description of all the reports in *Microsoft Active Directory SPI Online Help*.



Integrating Microsoft Active Directory SPI with HP Performance Manager

The Microsoft Active Directory 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 or HP Performance Agent) runs on the managed node.

To integrate the Microsoft Active Directory SPI with HP Performance Manager, follow these steps:

- 1 Install and configure the Microsoft Active Directory SPI.
- 2 Install the graph package.

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

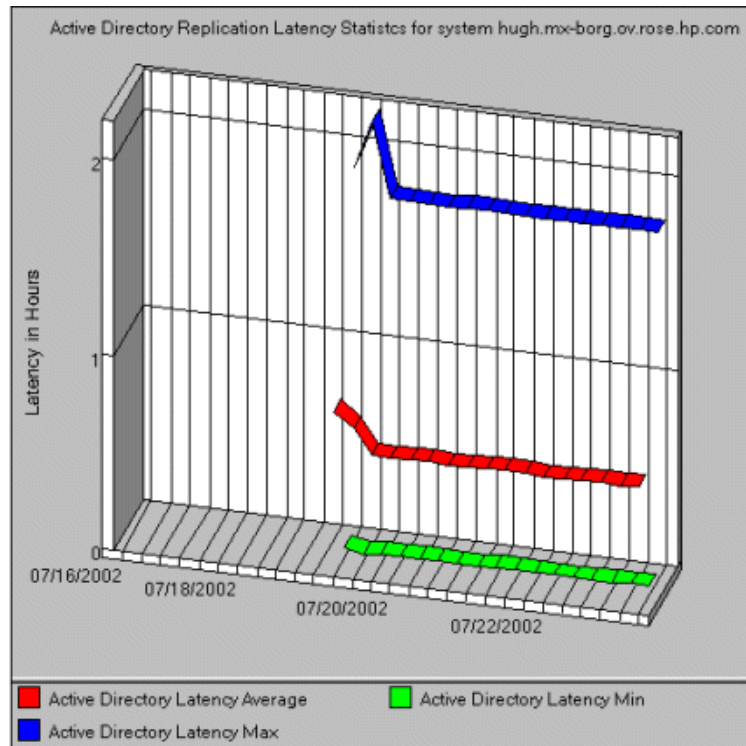
- a Insert the Smart Plug-ins DVD-ROM into the DVD-ROM drive, and in Windows Explorer, double-click `setup.exe`.
- b Follow the instructions as they appear.

For information see the HP Performance Manager documentation.

Generating Graphs

After you manually generate the graphs, you can view the data in a more specified and granular manner. You can access graphs in the HPOM console by selecting **Reports & Graphs** → **Graphs** → **SPI for Active Directory**. To access graphs of Microsoft Active Directory SPI:

- 1 Select **Graphs** → **SPI for Active Directory**.
- 2 Right-click the graph name, such as **Active Directory Replication Latency Graph**, and select **Show Graph....**
- 3 Select the node and the data range, and click **Finish**. The graph is displayed as shown in the Figure.



7 Troubleshooting

This chapter includes troubleshooting some areas of the Microsoft Active Directory SPI and provides solutions thereof. The methods described may or may not require support assistance.

Troubleshooting Discovery

The following sections describe the possible cause and suggested action for the failed discovery of the Microsoft Active Directory services.

Insufficient Privileges

In some cases the Microsoft Active Directory SPI fails to discover the Microsoft Active Directory services. The possible cause and suggested action is as follows:

- *Possible cause:* The account with which the Basic Discovery policy (**Policy Management** → **Policy Groups** → **SPI for Active Directory** → **en** (or **ja**) → **Windows Server 2008** (or **2003**) → **Auto Deploy** → **Discovery** → **Basic Discovery**) is run by the HP Operations Agent does not have the privileges to connect to the Microsoft Active Directory and retrieve data.
- *Suggested action:* Ensure that an administrator credentials are provided in the Basic Discovery policy and then redeploy the policy.

Failed Binary on the Managed Node

In some cases the Agent fails to update the discovered services to the HPOM management server. The possible cause and suggested action is as follows:

- *Possible cause:* The output of the Microsoft Active Directory SPI discovery policy is not a properly formatted `xml` file.
- *Suggested action:* Run the Microsoft Active Directory SPI discovery binary on the managed node. To do this:
 - a Login to the managed node as an administrator.
 - b From the command prompt, open the instrumentation directory.
 - c Run the `ovadsdisc.exe > out.xml` command.
 - d Check the `out.xml` is in the required `xml` format by opening it in the web browser.

Troubleshooting through Tracing

Tracing includes capturing all information related to Microsoft Active Directory, including FSMO and replication conditions, status, and errors included in the Microsoft Active Directory SPI logs.

All the Microsoft Active Directory SPI binaries can be traced with suffix `-1 1`.

Example:

The ADSPI-DNS_DC_A_Chk policy has the following command:

```
ADSPI_DnsMon.exe -svc ldap -rec host -type missing -n ADSPI-DNS_DC_A_Chk  
-L10N _en
```

To trace the binary ADSPI_DnsMon.exe, you should change this command as:

```
ADSPI_DnsMon.exe -svc ldap -rec host -type missing -n ADSPI-DNS_DC_A_Chk  
-L10N _en -1 1
```



You can find the trace file ADSPI_DnsMon.log in the `%ovagentdir%\bin\instrumentation` folder.

- All the Microsoft Active Directory SPI policies with embedded script are traced by changing the debug variable to **DEBUG=TRUE** found in the script.

Troubleshooting Reports and Graphs

The following sections describe the possible cause and suggested action for the failed generation of data in Microsoft Active Directory reports and graphs.

Reports and Graphs are not generated

In some cases, the reports and graphs are not generated. The possible cause and suggested action are as follows:

- *Possible cause:* The appropriate policies are not deployed to the respective Microsoft Active Directory reports and graphs. The policy, therefore, fails to collect the data which the HP Reporter generates as report. Failure to deploy the appropriate policy also disables the HP PM to generate graphs.
- *Suggested action:* See Appendix B Report, Report Table, Data Store, and Policy Mapping Details in *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide* to know the appropriate policy for each Microsoft Active Directory SPI report. See also Graphs, Data Store, and Policy Mapping Details in *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide* to know the appropriate policy for each Microsoft Active Directory SPI. Deploy the policy accordingly.

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 OVPA or both.
- *Suggested action:* Check if the datasource ADSPI is created. To do this:
 - a Login to the managed node as an administrator.
 - b From the command prompt run the `ovcodutil -obj > out.txt` command.
 - c Check the `out.txt` file to ensure that the datasource ADSPI is created.

Browser Crashes while Viewing the HTML Report

While viewing the reports in HTML format, the browser crashes. 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.

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.

Modifying Policy Names

If you change the default name of the following Microsoft Active Directory SPI policies, ensure to change their corresponding schedule command also:

- ADSPI-DNS_DC_A_Chk / ADSPI-DNS_DC_A_Chk_2k8+
- ADSPI-DNS_DC_CNAME_Chk / ADSPI-DNS_DC_CNAME_Chk_2k8+
- ADSPI-DNS_DC_Response / ADSPI-DNS_DC_Response_2k8+
- ADSPI-DNS_Extra_GC_SRV_Chk / ADSPI-DNS_Extra_GC_SRV_Chk_2k8+
- ADSPI-DNS_Extra_Kerberos_SRV_Chk / ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+
- ADSPI-DNS_Extra_LDAP_SRV_Chk / ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+
- ADSPI-DNS_GC_A_Chk / ADSPI-DNS_GC_A_Chk_2k8+
- ADSPI-DNS_GC_SRV_Chk / ADSPI-DNS_GC_SRV_Chk_2k8+
- ADSPI-DNS_GC_StrandedSite / ADSPI-DNS_GC_StrandedSite_2k8+
- ADSPI-DNS_Island_Server / ADSPI-DNS_Island_Server_2k8+
- ADSPI-DNS_Kerberos_SRV_Chk / ADSPI-DNS_Kerberos_SRV_Chk_2k8+

- ADSPI-DNS_LDAP_SRV_Chk / ADSPI-DNS_LDAP_SRV_Chk_2k8+
- ADSPI-DNS_LogDNSPagesSec / ADSPI-DNS_LogDNSPagesSec_2k8+
- ADSPI-DNS_Server_Response / ADSPI-DNS_Server_Response_2k8+
- ADSPI-Rep_ISM_Chk / ADSPI-Rep_ISM_Chk_2k8+
- ADSPI-Rep_MonitorInterSiteReplication /
ADSPI-Rep_MonitorInterSiteReplication_2k8+
- ADSPI-Rep_MonitorIntraSiteReplication /
ADSPI-Rep_MonitorIntraSiteReplication_2k8+
- ADSPI-Rep_TimeSync / ADSPI-Rep_TimeSync_2k8+
- ADSPI-Sysvol_Connectivity / ADSPI-Sysvol_Connectivity_2k8+
- ADSPI_KDC / ADSPI_KDC_2k8+
- ADSPI_NetLogon / ADSPI_NetLogon_2k8+
- ADSPI_NTFRS / ADSPI_NTFRS_2k8+
- ADSPI_NtLmSsp / ADSPI_NtLmSsp_2k8+
- ADSPI_SamSs / ADSPI_SamSs_2k8+
- ADSPI-FSMO_Consist_INFRA / ADSPI-FSMO_Consist_INFRA_2k8+
- ADSPI-FSMO_Consist_NAMING / ADSPI-FSMO_Consist_NAMING_2k8+
- ADSPI-FSMO_Consist_PDC / ADSPI-FSMO_Consist_PDC_2k8+
- ADSPI-FSMO_Consist_RID / ADSPI-FSMO_Consist_RID_2k8+
- ADSPI-FSMO_Consist_SCHEMA / ADSPI-FSMO_Consist_SCHEMA_2k8+
- ADSPI-FSMO_INFRA_Bind / ADSPI-FSMO_INFRA_Bind_2k8+
- ADSPI-FSMO_INFRA_Ping / ADSPI-FSMO_INFRA_Ping_2k8+
- ADSPI-FSMO_NAMING_Bind / ADSPI-FSMO_NAMING_Bind_2k8+
- ADSPI-FSMO_NAMING_Ping / ADSPI-FSMO_NAMING_Ping_2k8+
- ADSPI-FSMO_PDC_Bind / ADSPI-FSMO_PDC_Bind_2k8+
- ADSPI-FSMO_PDC_Ping / ADSPI-FSMO_PDC_Ping_2k8+
- ADSPI-FSMO_RID_Bind / ADSPI-FSMO_RID_Bind_2k8+
- ADSPI-FSMO_RID_Ping / ADSPI-FSMO_RID_Ping_2k8+
- ADSPI-FSMO_SCHEMA_Bind / ADSPI-FSMO_SCHEMA_Bind_2k8+
- ADSPI-FSMO_SCHEMA_Ping / ADSPI-FSMO_SCHEMA_Ping_2k8+
- ADSPI-FSMO_RoleMvmt_INFRA / ADSPI-FSMO_RoleMvmt_INFRA_2k8+
- ADSPI-FSMO_RoleMvmt_NAMING / ADSPI-FSMO_RoleMvmt_NAMING_2k8+
- ADSPI-FSMO_RoleMvmt_PDC / ADSPI-FSMO_RoleMvmt_PDC_2k8+
- ADSPI-FSMO_RoleMvmt_RID / ADSPI-FSMO_RoleMvmt_RID_2k8+
- ADSPI-FSMO_RoleMvmt_SCHEMA / ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

For details of each policy see *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* or *HP Operations Smart Plug-in for Microsoft Active Directory Online Help PDF*.

8 Removing Microsoft Active Directory SPI

You can remove the Microsoft Active Directory SPI through the following ways:

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

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

▶ Undeploy all Microsoft Active Directory SPI policies from all managed nodes before uninstalling.

Using DVD

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

Removing Microsoft Active Directory SPI Components

The Microsoft Active Directory SPI components include policies, reporting package, and graphing package.

Task 1: Remove the Microsoft Active Directory SPI policies from all managed nodes

- 1 At the console expand the folder **Policy Management**.
- 2 Right-click SPI for **Active Directory**, 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**.

▶ To verify if policies have been removed, at the HPOM console expand the **Nodes**, right-click a node, and then select **View** → **Policy Inventory**.

Task 2: Remove Microsoft Active Directory SPI programs from the HPOM management server

- 1 Insert the *HP Operations Smart Plug-ins* DVD.
- 2 Follow the instructions as they appear on the screen and start the uninstall procedure by selecting the **Remove programs**.
- 3 In the **Product Selection Uninstall** window, select **Microsoft Active Directory (SPI)**, and click **Next**.

4 In the next window select **Remove**.



Each window updates you with the status of uninstalling the Microsoft Active Directory SPI.

5 Click **Finish** to complete.

Task 3: Remove the Microsoft Active Directory SPI Policies from the Management Server

1 Expand the Agent Policies grouped by type.

2 From each policy type, delete all versions of the policies which start with the name **ADSPI**.

Using the Windows Control Panel

Remove the SPI components before removing the Microsoft Active Directory SPI from the management server. To remove the SPI components manually, perform the tasks in [Removing Microsoft Active Directory SPI Components](#).

Removing Microsoft Active Directory 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**.



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 **ADSPI**.

6 Complete the instructions until a message appears which shows that Microsoft Active Directory 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 which shows that HP Reporter has been removed.

Removing Graphing Package

To remove the graphing package:

- 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 which shows that HP Performance Manager has been 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, perform the following steps:

- 1 Browse to:
`<SPI DVD>\SPIs\AD SPI\ADSPI-Reporter.msi`
- 2 Right-click `ADSPI-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, perform the following steps:

- 1 Browse to:
`<SPI DVD>\SPIs\AD SPI OVPM ConfigurationPackage\HPOvSpiAdGc.msi`
- 2 Right-click `HPOvSpiAdGc.msi`, and then click **Uninstall**.
- 3 Confirm the removal of the graphing package by clicking **Yes**.

Index

A

Auto-discovery, 33

C

Clustered environment, 22

Components

- Graphs, 10
- Policies, 10
- Reports, 10
- Tools, 10

Components of the Microsoft Active Directory, 32

Console services tree, 12

Console tree, 34

D

Discover Services

- Advanced Discovery, 33
- Basic Discovery, 30, 63
- Discovery policy

Domain controllers, 9

E

Events, 12

F

Forests, 27

Functions

- Discover existing components, 11
- Display information, 11
- Generate graphs, 13
- Generate reports, 13

G

Global Catalog, 9

Graphs

- HP Performance Manager, 60

H

HPOM console, 22

I

Installation Environments

- Installation on HPOM, 18
- Installation on HP Reporter on HP Performance Manager, 18
- Installation on Remote Console, 18

Installation Packages

- Console Package, 18
- Graphing Package, 17
- Reporting Package, 18
- SPI Package, 17

Instrumentation categories, 30

L

LDAP, 9

Legends, 15

M

Master operations services, 13

Message Identifier, 37

Microsoft Active Directory SPI

- Configuration, 29
- Uninstallation, 67

O

Options, 14, 37

P

Policies

- Custom Data Collection Groups, 38
- Default Policies, 37
- Schedule or Measurement Threshold Policies, 38

Policy-auto deployment setting, 35

R

Remote Console packages, 18

Reports

- HP Reporter, 58

Rules, 14, 37

S

Script-parameters, 14, 37

Severity level, 10

Smart Plug-in, 9

Software Upgrade Tool Kit, 14, 24

T

Tools

- AD Trust Relationships Tool, 46

- HP Operations Topology Viewer, 47

Troubleshooting, 63

- Discovery, 63

- Reports and Graphs, 64

- Tracing, 64

Trust relationship status, 9

U

Unmanaged node, 29

V

VC-Redistributable, 19

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback:

