

HP Operations Smart Plug-in for Microsoft® Active Directory

for HP Operations Manager for HP-UX, Linux, and Solaris

Software Version: 7.06

Installation and Configuration Guide

Document Release Date: November 2010
Software Release Date: November 2010



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2009–2010 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

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 user 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
	Components of the Microsoft Active Directory SPI	9
	Policies	9
	Tools	10
	Reports	10
	Graphs	10
	Functions of the Microsoft Active Directory SPI	10
	Displaying Information	10
	Service Map	10
	Message Browser	12
	Instruction Text	12
	Reports and Graphs	12
	HP Operations Topology Viewer Tool	13
	Generating Reports Using the HP Reporter	13
	Graphing Data with the HP Performance Manager	13
	Customizing Policies	13
2	Installing the Microsoft Active Directory SPI	15
	Installation Packages	15
	SPI Package	15
	Graph Package	15
	Reporter Package	16
	Installation Environments	16
	Standard Installation of SPI Components on the HPOM Server	16
	Standalone Installation on HP Reporter and HP Performance Manager	16
	Installation Overview	16
	Prerequisites to Install Microsoft Active Directory SPI	18
	Hardware Requirements	18
	Software Requirements	18
	Installing Microsoft Active Directory SPI on a Local Management Server	20
	For HP-UX:	20
	Mounting the DVD on HP-UX	20
	Installing Microsoft Active Directory SPI	20
	For Solaris and Linux:	20
	Installing the Microsoft Active Directory SPI on HPOM Cluster Servers	22
	Verifying the Installation of Microsoft Active Directory SPI	23
3	Configuring Microsoft Active Directory SPI	25
	Configuration Procedure	25
	Manage Domain Controller Nodes	25

Assign DC Nodes to Node Group	25
Assign Basic Discovery Policy Group to DC Nodes	26
Assign Instrumentation Categories to DC Nodes	26
Deploy Configuration	27
Assign other Microsoft Active Directory SPI Policies to DC Nodes	28
Deploy other Microsoft Active Directory SPI Policies to DC Nodes	28
Assign Domain_Controllers Node Group and Message Group to the Operator	28
Assign Microsoft Active Directory SPI Services to the Operator	29
Assign Tool Group to Operator	30
Create Data Source	31
Data Logging Scenarios	31
4 Customizing Policies	33
Policies	34
Policy Group	34
Policy Type	34
Creating Custom Data Collection Groups	34
Using Auto-Deploy Policies	34
Discovery	35
DIT Monitoring	35
DNS Monitoring	35
FSMO Monitoring	35
Replication Monitoring	35
Response Time Monitoring	35
GC Monitoring	35
Sysvol Monitoring	36
Trust Monitoring	36
Using Manual-Deploy Policies	36
Using Auto-Baseline Policies	36
Connector Policies (only for Windows Server 2003)	37
Domain and OU Structure	37
Global Catalog Access	37
Health Monitors	37
Index and Query	37
Replication	37
Replication Activity	37
Security	37
Site Structure	38
5 Using Tools	39
Starting Microsoft Active Directory SPI Tools	39
Using AD Trust Relationship Tool	40
Using HP Operations Topology Viewer Tool	40
Starting HP Operations Topology Viewer Tool	41
Getting Started with the HP Operations Topology Viewer Tool	42
Accessing Functions of HP Operations Topology Viewer Tool	42
Adjusting Map View	43

HP Operations Topology Viewer Menu bar	44
HP Operations Topology Viewer Toolbar	45
Accessing Server and Map Properties	46
6 Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions	49
Using Reports and Graphs	49
Integrating Microsoft Active Directory SPI with HP Reporter	49
Installing Report Package	49
Configuring Report Package	50
Accessing Reporter Help	50
Generating Reports	51
Integrating Microsoft Active Directory SPI with the HP Performance Manager	52
Generating Graphs	52
7 Troubleshooting	55
Failed Discovery	55
Insufficient Privileges	55
Failed Binary on the Managed Node	55
Tracing	56
Reports and Graphs	56
Reports and Graphs are not generated	56
Data Logging Policies cannot log Data	56
Browser crashes while viewing HTML Report	57
Reports Fail with Oracle Database	57
Modifying Policy Names	57
8 Removing Microsoft Active Directory SPI	59
Removing Microsoft Active Directory SPI from HPOM	59
For HP-UX:	59
For Solaris and Linux:	59
Removing Other Components of the Microsoft Active Directory SPI	61
Removing the Microsoft Active Directory SPI Message Group	61
Removing All User Profiles	61
Removing Report Package	61
Removing Report Package using Control Panel	61
Removing Report Package using .msi file	61
Removing Graph Package	62
Removing Graph Package using Control Panel	62
Removing Graphing Package using .msi File	62
Index	63

1 Introducing the Smart Plug-in for Microsoft Active Directory

This chapter introduces you to some basic concepts of the HP Operations Smart Plug-in for Microsoft Active Directory (Microsoft Active Directory SPI) and gives you an overview of the Microsoft Active Directory SPI components that, once installed, appear in the HP Operations Manager (HPOM) Administration interface.

The Microsoft Active Directory SPI helps you to manage the Microsoft Active Directory in your environment on HP-UX, Solaris, or Linux management servers. The Microsoft Active Directory SPI provides information about the Microsoft Active Directory and the following:

- Data consistency across the Domain Controllers (DCs)
- Timely replication process
- Systems outages capability
- Successful functioning of role masters
- DCs competing with over-utilized CPUs
- Capacity and fault-tolerance issues in the Microsoft Active Directory
- Replication of Microsoft Active Directory Global Catalog (GC) in a timely manner
- Performance levels of services, events, 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 the 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 constantly monitor the Microsoft Active Directory environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts appear in the service map and messages are available in the message browser. The messages indicate the problem and help you to take preventive action. Policies can be deployed automatically or manually. For more information, see [Chapter 4, Customizing Policies](#).

Tools

Tools are utilities that gather Microsoft Active Directory related information. You can also use the 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. For more information, see [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

Graphs

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

Reports and graphs are generated with the help of HP Reporter and HP Performance Manager.

Functions of the Microsoft Active Directory SPI

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 maintains the thresholds set up by the policies. The Microsoft Active Directory SPI expands the discovered services and adds multiple hierarchical levels of details.

Displaying Information

The Microsoft Active Directory SPI displays information using the following:

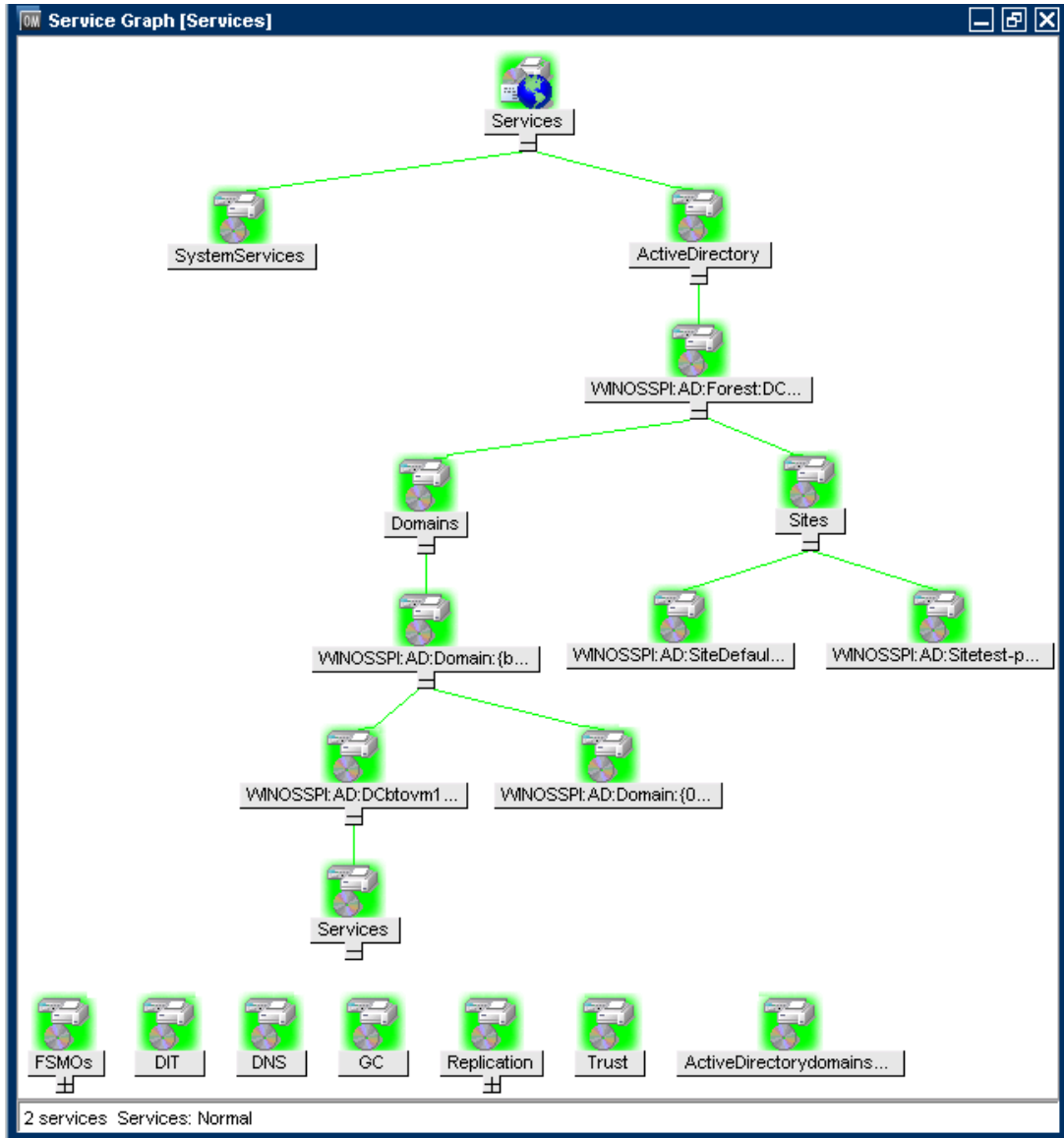
Service Map

Service map displays the newly added and discovered Microsoft Active Directory services displayed in both the console services tree and the service map. Within the service map pane, you can expand the hierarchy to show the specific services present on each DC.

To view the Microsoft Active Directory services, follow these steps:

- 1 From the Administration UI, click **Integrations** → **HPOM for Unix Operational UI**. The login window appears.
- 2 Type the user name and password. The console opens.
- 3 Click **Services**. The service map appears on the right pane.

- 4 Expand the hierarchy to view the specific services and components present on each DC.



Message Browser

The Microsoft Active Directory SPI monitors events and services on the managed nodes and generates messages. The message browser displays the messages based on the severity level of the problem.

Severity	Dup.	SUIAONE	Time Received	Node	Application	MsgGrp	Object	Message
Normal		--X--X-	13:03:31 08/13/09	btovm130.paren...	HP Operations ...	OpC	ovoareqsdr ...	Successf...
Normal		--X----	12:52:03 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	12:51:59 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	12:51:59 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	12:51:59 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	12:42:38 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	:ati
Warning		--X----	12:42:38 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	:ati
Warning		--X----	12:42:35 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	:ati
Warning		--X----	12:42:35 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	:ati
Warning		--X----	12:41:48 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	:ati
Warning		--X----	12:41:48 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	:ati
Warning		--X----	12:16:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	12:06:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	12:06:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	12:06:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:51:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:51:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:51:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:36:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:36:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:36:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:36:42 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	11:31:44 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	11:31:43 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	11:31:41 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	11:31:41 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	11:31:41 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Normal		--X----	11:31:41 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:21:43 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:21:43 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:21:43 08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SEF	Health Monit...	ADSPI-0x
Warning		--X----	11:18:42 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	Logfiletio
Warning		--X----	11:18:42 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	Logfiletio
Warning		--X----	11:18:39 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	Logfiletio
Warning		--X----	11:18:39 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	Logfiletio
Warning		--X----	11:18:21 08/13/09	btovm130.paren...	HP OpenView ...	OpC	opcle (Lo...	Logfiletio

Instruction Text

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

Reports and Graphs

Reports and graphs present information related to load balancing, capacity planning, and policy scheduling 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 42.

To start the HP Topology Viewer tool, you must install it on a 32 bit Windows system. This tool is not listed in the **Tool Bank**.

Generating Reports Using the HP Reporter

You can generate reports to analyze Microsoft Active Directory activities. These web-based reports are automatically generated every night. Reports showing 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 the HP Performance Manager

After you manually generate the graphs, you can view the data in a specified and granular manner. You can access graphs in the HP Performance Manager console by integrating Microsoft Active Directory SPI with HP Performance Manager. 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. Following are some of the parameters that can be modified:

- Script-parameters
- Rules
- Options

2 Installing the Microsoft Active Directory SPI

The Microsoft Active Directory SPI must be installed on the HPOM management server. The following sections provide detailed information on installing the Microsoft Active Directory SPI.

Installation Packages

The Microsoft Active Directory SPI version 7.06 is a patch release. You can download the patches from the following location: <http://support.openview.hp.com/selfsolve/patches>. Instructions to install a patch are available in the patch text.

The Microsoft Active Directory SPI installation package includes the following:

- SPI Package
- Graph Package
- Reporter Package

These packages are available only when you install the Microsoft Active Directory SPI from any *one* of the following:

- SPI DVD for UNIX (SPI DVD 2009)
- SPI DVD for Linux
- SPI DVD for Solaris

SPI Package

The Microsoft Active Directory SPI package contains all the functionalities of the Microsoft Active Directory SPI. Install the package file on an HPOM server. The SPI packages are available at the following locations in the respective DVDs:

For HP-UX: <SPI DVD>\HPUX\HP_Operations_Smart_Plug-ins_HPUX.depot

For Linux: <SPI DVD>\HP_Operations_Smart_Plug-ins_Linux_setup.bin

For Solaris: <SPI DVD>\HP_Operations_Smart_Plug-ins_Solaris_setup.bin

Graph Package

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

<SPI DVD>\WINDOWS\HP_PM\AD_SPI\HPOvSpiAdG.msi

Reporter Package

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

```
<SPI DVD>\WINDOWS\HP_REPORTER\AD_SPI\ADSPI-Reporter.msi
```

Installation Environments

You can install the Microsoft Active Directory SPI in the following environments:

- Standard installation of SPI components on an HPOM 9.0x or 9.10 Server.
- Standalone HP Reporter and HP Performance Manager.

Standard Installation of SPI Components on the HPOM Server

You can install the reporting and graphing packages (HP Reporter and HP Performance Manager) while installing the Microsoft Active Directory SPI on the HPOM server using the HP Operations Smart Plug-Ins DVD.

Standalone Installation on HP Reporter and HP Performance Manager

For a standalone managed node or 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 the node has only HP Performance Manager installed then the graphing package of the Microsoft Active Directory can be installed on the node.

Installation Overview

The following flowchart explains the tasks involved in installing and configuring the Microsoft Active Directory SPI.

Figure 1 Overview of Installation and Configuration Steps

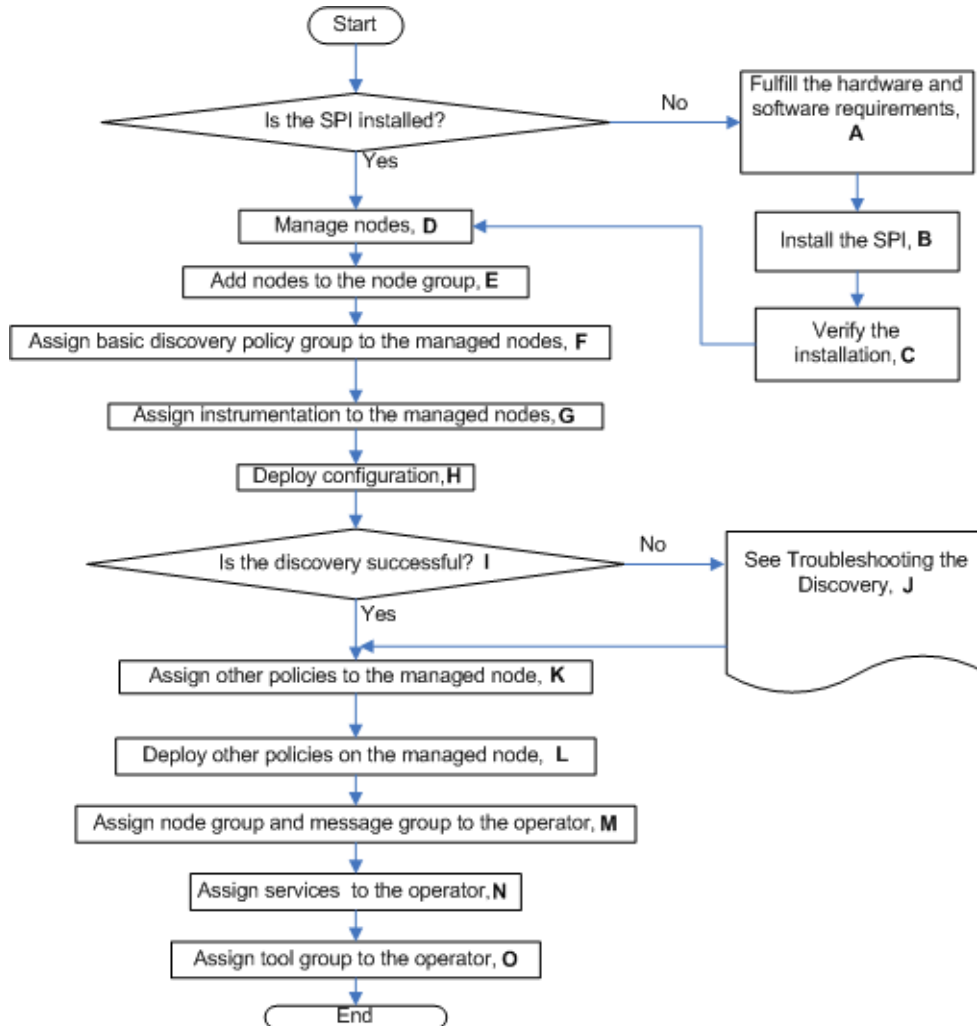


Table 1 Legend of Installation and Configuration Steps

Legend	References
A	Prerequisites to Install Microsoft Active Directory SPI on page 18
B	Installing Microsoft Active Directory SPI on a Local Management Server on page 20
C	Verifying the Installation of Microsoft Active Directory SPI on page 23
D	Manage Domain Controller Nodes on page 25
E	Assign DC Nodes to Node Group on page 25
F	Assign Basic Discovery Policy Group to DC Nodes on page 26
G	Assign Instrumentation Categories to DC Nodes on page 26
H	Deploy Configuration on page 27
I	Service Map on page 10
J	Failed Discovery on page 55

Legend	References
K	Assign other Microsoft Active Directory SPI Policies to DC Nodes on page 28
L	Deploy other Microsoft Active Directory SPI Policies to DC Nodes on page 28
M	Assign Domain_Controllers Node Group and Message Group to the Operator on page 28
N	Assign Microsoft Active Directory SPI Services to the Operator on page 29
O	Assign Tool Group to Operator on page 30

Prerequisites to Install Microsoft Active Directory SPI

Ensure that the hardware and software requirements are fulfilled before installing the SPI. Also, install the HPOM management server before installing the Microsoft Active Directory SPI. It is not necessary to stop HPOM sessions before beginning the Microsoft Active Directory SPI installation.

Hardware Requirements

Ensure that there is minimum 200 MB Free Hard-Disk space.

Software Requirements

Ensure that the following software requirements are met:

For HP-UX:

On the management server:

- HP Operations Manager for UNIX: 9.0x or 9.10
- HP Reporter 3.80 for ADSPI-Reporter
- HP Performance Manager 8.20 on Windows for ADSPI-Graphs
- A 32-bit Windows system for HP Operations Topology Viewer tool
- Service Navigator to view the Microsoft Active Directory Service Map
- HP Operations SPI Data Collector (DSI2DDF): 2.40
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.00

You can install these products from HPOM Smart Plug-ins DVD.

- Install the hotfix available for all Microsoft Exchange Server 2007 nodes with Windows Server 2008 - x64:

For more information, see *HP Operations Smart Plug-in for Microsoft Active Directory Release Notes*.

On the managed node:

- HP Performance Agent 5.00 (required if you want to use HP Performance Agent for data logging)

- HP Operations Agent version 8.60 installed and configured

For Solaris:

On the management server:

- HP Operations Manager for Solaris 9.0x or 9.10
- HP Reporter 3.80 for ADSPI-Reporter
- HP Performance Manager 8.21 on Windows for ADSPI-Graphs
- A 32-bit Windows system for HP Operations Topology Viewer tool
- Service Navigator to view the Microsoft Active Directory Service Map
- HP Operations SPI Data Collector (DSI2DDF): 2.41
- HP Operations SPI Upgrade Toolkit (SUTK): 2.02
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.02

You can install these products from HPOM Smart Plug-ins DVD.

- Install the hotfix available for all Microsoft Exchange Server 2007 nodes with Windows Server 2008 - x64:

For more information, see *HP Operations Smart Plug-in for Microsoft Active Directory Release Notes*.

On the managed node:

- HP Performance Agent 5.00 (required if you want to use HP Performance Agent for data logging)
- HP Operations Agent version 8.60 installed and configured

For Linux:

On the management server:

- HP Operations Manager for Linux: 9.0x or 9.10
- HP Reporter 3.80 for ADSPI-Reporter
- HP Performance Manager 8.21 on Windows for ADSPI-Graphs
- A 32-bit Windows system for HP Operations Topology Viewer tool
- Service Navigator to view the Microsoft Active Directory Service Map
- HP Operations SPI Data Collector (DSI2DDF): 2.41
- HP SPI Self-Healing Services (SPI-SHS-OVO): 3.01

You can install these products from HPOM Smart Plug-ins DVD.

- Install the hotfix available for all Microsoft Exchange Server 2007 nodes with Windows Server 2008 - x64:

For more information see, *HP Operations Smart Plug-in for Microsoft Active Directory Release Notes*.

On the managed node:

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

Installing Microsoft Active Directory SPI on a Local Management Server

For HP-UX:

This section describes steps required to install the Microsoft Active Directory SPI on HP-UX:

Mounting the DVD on HP-UX

To mount the SPI DVD on HP-UX, follow these steps:

- 1 Log on as user *root*.
- 2 Type the following command to set the user *root*'s unmask:

```
umask 027
```

- 3 Create a directory to mount the DVD:

```
mkdir /<mount_point>
```

For example: **mkdir /dvdrom**

- 4 Insert the DVD into the disk drive and type the following command to mount it as user *root*:

```
mount /dev/<dvdrom_drive_name> /<mount_point>
```

For example, for a local DVD, you can use the following command:

```
mount /dev/dsk/c0t2d0 /dvdrom
```

You can also run SAM and mount the DVD to a specific path in the Disks and File Systems window.

Installing Microsoft Active Directory SPI

To install the Microsoft Active Directory SPI on the HPOM management server from the command line interface, follow these steps:

- 1 Insert the SPI DVD into the DVD-ROM drive of the management server.
- 2 Run the following commands:

HP-UX 11.x management server:

```
swinstall -s /cdrom/HPUX/HP_Operations_Smart_Plug-ins_HPUX.depot  
ADSPI
```

The installer installs Microsoft Active Directory SPI on the management server.

For Solaris and Linux:

You can install the Microsoft Active Directory SPI on the Solaris or Linux Management Server using the following interfaces:

- Graphical User Interface
- Command Line Interface

Installing the Microsoft Active Directory SPI using the Graphical User Interface

To install the Microsoft Active Directory SPI using X-Windows client software, follow these steps:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the management server DVD drive.
- 3 Start the X-windows client software and export the `DISPLAY` variable by typing the following command:

```
export DISPLAY=<ip address>:0.0
```

- 4 To start the installation, type the following command:

For Solaris:

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

For Linux:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

The Initialization window opens.

- 5 Select the language from the list and click **OK**.
The Introduction (Install) window opens.
- 6 Click **Next**.
The License Agreement window opens.
- 7 Select **I accept the terms of the License Agreement** and click **Next**.
The Select Features window opens.
- 8 Select the **HP Operations Smart Plug-In for Microsoft Active Directory** and click **Next**.
The Install Checks window opens

▶ During installation of the SPIs on HPOM for Solaris or Linux, select the previously installed SPIs, if any. If you do not select the previously installed SPIs, the installer automatically removes the previously installed SPIs and installs only the selected SPIs.

- 9 Click **Next**. The Pre-Install Summary window opens.
- 10 Click **Install**.

▶ Select **Force reinstallation** to reinstall the selected components.

- 11 When the installation is complete, click **Done**.

Installing the Microsoft Active Directory SPI using the Command Line Interface

To install the Microsoft Active Directory SPI using the command line interface, follow these steps:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the Solaris or Linux management server DVD drive.
- 3 To start the installation, type the following command:

For Solaris:

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin -i console
```

For Linux:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin -i console
```

- 4 When the option, 'Choose Locale...' appears, type the number corresponding to the language you want to choose and press **Enter**.

The HP Software Installer content appears.

- 5 Press **Enter** to continue.

The Introduction content appears.

- 6 Press **Enter** to continue.

The License agreement content appears.

- 7 When the License agreement prompt, '**I accept the terms of the License Agreement**' appears, type **Y** and press **Enter** to accept the terms and continue with the installation.

The Feature selection options list appears.

- ▶ During installation of the SPIs on HPOM for Solaris or Linux, select the previously installed SPIs, if any. If you do not select the previously installed SPIs, the installer automatically removes the previously installed SPIs and installs the selected ones.

- 8 Type the number corresponding to the feature you want to install and press **Enter**.

The installer selects the other required features.

- 9 Press **Enter** to continue.

The Install Requirements Checks content appears.

- 10 Press **Enter** to continue.

The Pre-Installation Summary content appears.

- 11 Press **Enter** to continue.

The selected features are installed.

When the installation is complete, a message appears stating that the installation is completed successfully.

Installing the Microsoft Active Directory SPI on HPOM Cluster Servers

Before installing the Active Directory SPI in a cluster environment, ensure that HPOM for UNIX 9.0x or 9.10 is installed on each system of the cluster.

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

To install the Active Directory SPI on cluster servers, perform the following tasks:

Task 1: At the first cluster-aware management server, select and install the Microsoft Active Directory SPIs

Complete the steps described in [Installing Microsoft Active Directory SPI on a Local Management Server](#) on page 20 before proceeding to the next management server.

- Before starting, ensure that sufficient disk space is available on each management server for the Active Directory SPI. Cancelling the installation process before the completion leads to partial installations and the partially installed components must be removed manually.

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

Repeat the steps described in [Installing Microsoft Active Directory SPI on a Local Management Server](#) on page 20 on each management server in the cluster and continue to every management server until you have finished.

- The HPOM console will not function properly until you complete all the installations on all the nodes in the cluster.

Verifying the Installation of Microsoft Active Directory SPI

To verify the installation of the Microsoft Active Directory SPI, perform one of the following:

- Check the Policy Bank, which contains SPI for Active Directory.

To check the Policy Bank, click **Policy Bank**. The system displays the **SPI for Active Directory**.

- From the command prompt of HPOM 9.0x or 9.10 for UNIX server, go to the directory: `/var/opt/OV/share/databases/OpC/mgd_node/instrumentation`. You can see the Instrumentation groups `ActiveDirectory_Core` and `ActiveDirectory_Discovery`. All Microsoft Active Directory SPI instrumentation files are in these directories.

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 in your environment and maintaining the thresholds set up by the policies. The Microsoft Active Directory SPI enhances the role of discovery by adding multiple hierarchical levels of details.

The Microsoft Active Directory SPI discovers forests, and then discovers each DC with its name. Then it discovers the Microsoft Active Directory services and components available with it including sites, the preferred PBHS connecting the sites, replication, and sysvol. This way, the Microsoft Active Directory SPI shows partitions in the discovered sites 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.

Configuration Procedure


You can configure the Microsoft Active Directory SPI by performing the tasks in the following sections.

Manage Domain Controller Nodes

Before configuring the Microsoft Active Directory SPI, you must manage the Domain Controller (DC) nodes.

Assign DC Nodes to Node Group

To assign the DC nodes to the **Domain_Controllers** node group, follow these steps:

- 1 Click **Browse** → **All Node Groups** and select the **Domain_Controllers** node group check box.
- 2 Select **Assign Nodes...** from the list, and click **Submit** .
- A Selector window appears.
- 3 Click **All Nodes** in the Selector window. A list of all the existing nodes appears.
- 4 Select the nodes for the **Domain_Controllers** node group, and then click **OK**.

A message appears indicating the successful assignment of the nodes to the **Domain_Controllers** node group.

Assign Basic Discovery Policy Group to DC Nodes

You must assign the Basic Discovery policy group to the DC nodes of the **Domain_Controllers** node group to start the discovery process of the basic components of Microsoft Active Directory. The discovered components of Microsoft Active Directory can be viewed using the operator's interface.

- ▶ To log on to the operator's interface, click **Integrations** → **HPOM for Unix Operational UI**, and enter your credentials.

To assign the Basic Discovery policy group to the DC nodes, follow these steps:

- 1 Click **Browse** → **All Node Groups** and click the **Domain_Controllers** node group.
- 2 Select all the **DC** nodes check boxes to assign the Basic Discovery policy group.
- 3 Select **Assign Policies / Policy Group...** from the list and click **Submit** **>>**. A Selector window appears.
- 4 Select **Policy Groups** from the Locate list, type **Basic Discovery** in Name box and click **OK** to display the Basic Discovery components for Windows Server 2003 and 2008.

The screenshot shows the HPOM interface for the 'Domain_Controllers' node group. A table lists 11 DC nodes, all of which are selected. A 'Selector' dialog box is open, showing the search results for 'Basic Discovery' policy groups. The dialog box has a 'Locate' dropdown set to 'Policy Groups' and a 'Name' field containing 'Basic Discovery'. The search results show two filtered policy groups: 'SPI for Active Directory/Windows Server 2008/Auto-Deploy/Discovery/Basic Discovery' and 'SPI for Active Directory/Windows Server 2003/Auto-Deploy/Discovery/Basic Discovery'. The dialog box also has 'OK' and 'Cancel' buttons.

Type	Label	Name
<input checked="" type="checkbox"/>	DC_1	abc.com
<input checked="" type="checkbox"/>	DC_2	123.com
<input checked="" type="checkbox"/>	DC_3	abb.com
<input checked="" type="checkbox"/>	DC_4	pqrs.com
<input checked="" type="checkbox"/>	DC_5	abc123.com
<input checked="" type="checkbox"/>	DC_6	pqrs1234.com
<input checked="" type="checkbox"/>	DC_7	12345.com
<input checked="" type="checkbox"/>	DC_8	abcd.com
<input checked="" type="checkbox"/>	DC_9	1234.com
<input checked="" type="checkbox"/>	DC_10	222.com
<input checked="" type="checkbox"/>	DC_11	55555.com

- 5 Select **SPI for Active Directory/Windows Server 2008/Auto-Deploy/Discovery/Basic Discovery** or **SPI for Active Directory/Windows Server 2003/Auto-Deploy/Discovery/Basic Discovery** and click **OK**.

The Basic Discovery policy group is assigned to the selected DC nodes.

Assign Instrumentation Categories to DC Nodes

You must assign the following instrumentation categories to the DC nodes:

- SPIDataCollector
- ActiveDirectory_Core
- ActiveDirectory_Discovery.

To assign instrumentation categories to the DC nodes, follow these steps:

- 1 Click **Browse** → **All Node Groups** and click the **Domain_Controllers** node group.
- 2 Select all the **DC** nodes check boxes to assign the instrumentation categories.
- 3 Click **Assign Categories...** from the list and click **>>**. The Selector Window appears.
- 4 Select **SPIDataCollector**, **ActiveDirectory_Core**, and **ActiveDirectory_Discovery** and click **OK**.
The selected categories are assigned to the DC nodes.

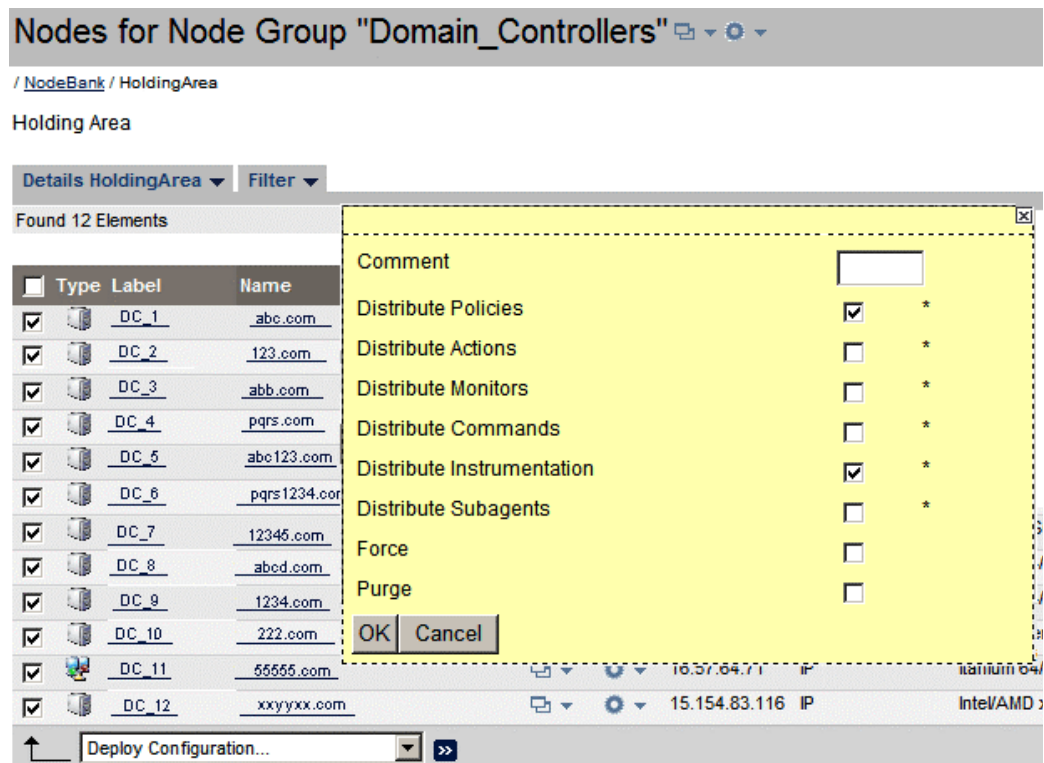
Deploy Configuration

To deploy configuration to the DC nodes, perform the following steps:

- 1 Click **Browse** → **All Node Groups** and click the **Domain_Controllers** node group.
- 2 Select all the **DC** nodes check box to deploy configuration.
- 3 Select **Deploy Configuration...** from the list and click **Submit >>**.

A dialog box appears, which indicates the categories of configuration.

- 4 Select **Distribute Policies** and **Distribute Instrumentation** check boxes and click **OK**.




A message appears stating that the nodes are successfully configured.

When you deploy the configuration, the basic components of the Microsoft Active Directory are discovered.

Assign other Microsoft Active Directory SPI Policies to DC Nodes


To assign other Microsoft Active Directory SPI policies to the DC nodes, follow these steps:

- 1 Click **Browse** → **All Node Groups** and click the **Domain_Controllers** node group.
- 2 Select all the **DC** nodes check boxes to assign other Microsoft Active Directory SPI policies.
- 3 Click **Assign Policies / Policy Group...** from the list and click . The Selector Window appears.
- 4 Select **Policy Groups** from the **Locate** list and type **SPI for Active Directory** in the **Name** box. The policy groups corresponding to the search criteria are listed.
- 5 Select **SPI for Active Directory/Windows Server 2008** or **SPI for Active Directory/Windows Server 2003**, and then click **OK**.

All the other Microsoft Active Directory SPI policies are assigned to the DC nodes.

Deploy other Microsoft Active Directory SPI Policies to DC Nodes

To deploy the other Microsoft Active Directory SPI policies to the DC nodes, follow these steps:


- 1 Click **Browse** → **All Node Groups** and click the **Domain_Controllers** node group.
- 2 Select all the **DC** nodes check boxes to deploy other Microsoft Active Directory SPI policies.
- 3 Select **Deploy Configuration...** from the list and click **Submit** .
A box appears displaying the categories of configuration.
- 4 Select **Distribute Policies** and **Distribute Instrumentation**, and then click **OK**.

All other Microsoft Active Directory policies are deployed on the DC nodes.

Assign Domain_Controllers Node Group and Message Group to the Operator

Assigning the Domain_Controllers node group and Microsoft Active Directory SPI message group to the HPOM for UNIX operator enables the operator to view the messages and alerts generated from the DC nodes.

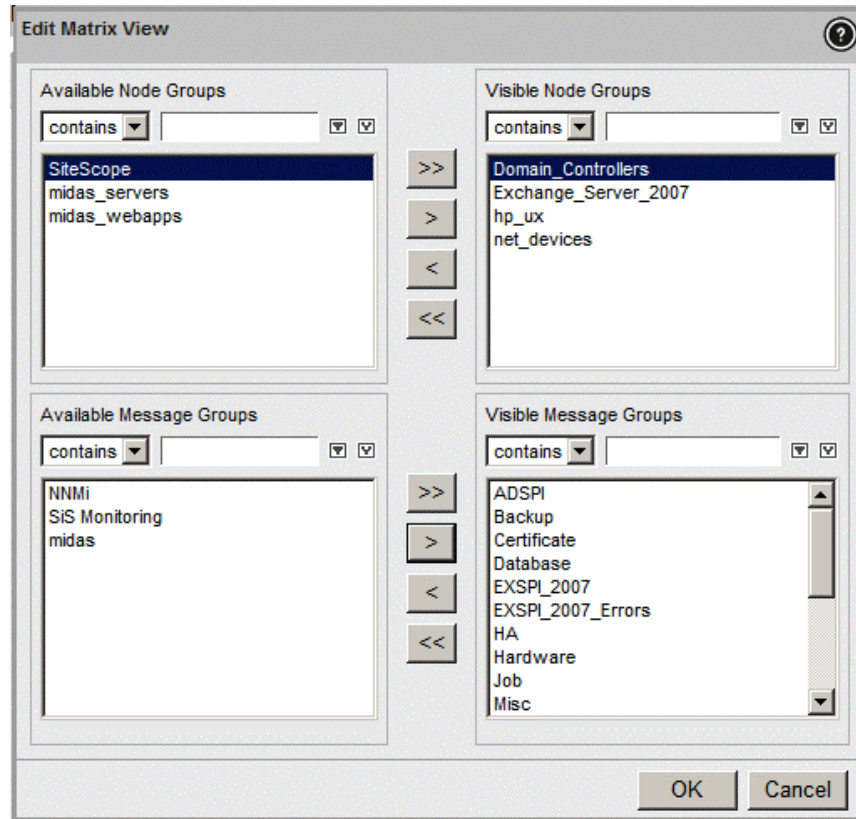
To assign the node group and the message group to the operator, follow these steps:

- 1 Click **Browse** → **All Users**. The system displays all the users.
- 2 Select the required operator check box.
- 3 Select **Edit Responsibilities....** from the  list to edit the properties.

The Edit Responsibilities window for the particular user displays the available nodes groups and message groups.

- 4 Click **Edit View**. The Edit Matrix dialog box appears.
- 5 Select **Domain_Controllers** from the Available Node Groups pane and **ADSPI** from the Available Message Groups pane.

- Click **>** to shift the selected node group and message group to the visible node group and message group pane.



- Click **OK**. The **Domain_Controllers** node group and the **ADSPI** message group are added to the list.
- Select the **Domain_Controllers** node group and the **ADSPI** message group check boxes to enable the operator to use the message browser and view alerts.
- Click **Save** to save the changes.

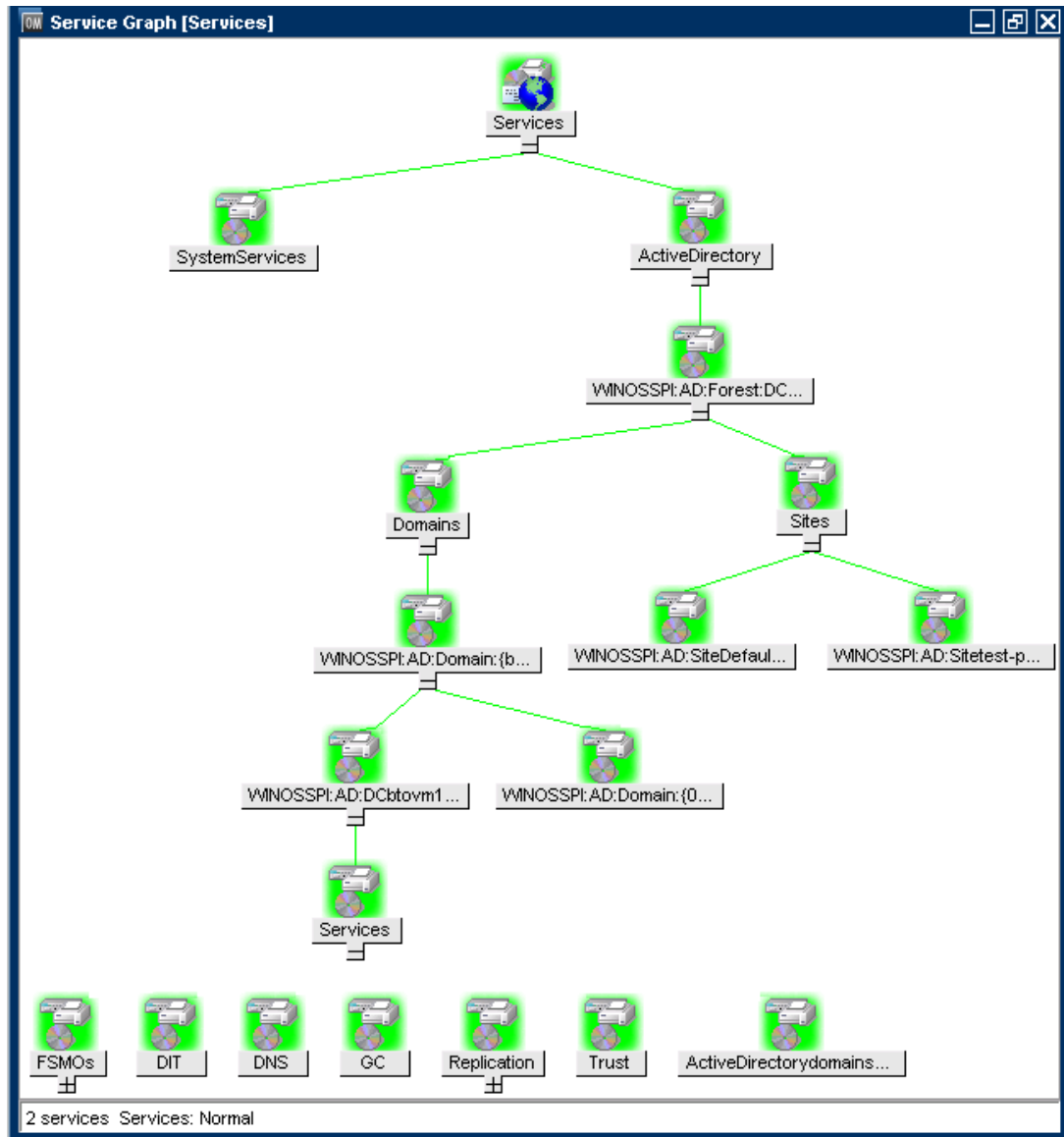
Assign Microsoft Active Directory SPI Services to the Operator

To assign the Microsoft Active Directory SPI services to the operator, follow these steps:

- Run the Active Directory SPI Discovery.
- Run the following command to assign the WINOSSPI:AD services to the required operator:


```
opcservice -assign opc_admin WINOSSPI:AD.
```

The service navigator displays the Microsoft Active Directory service map.



Assign Tool Group to Operator

To assign the tool group to the required operator, follow these steps:

- 1 Click **Browse** → **Tool Bank** → **SPI for Active Directory**. The Tool Group for Microsoft Active Directory SPI appears.
- 2 Select the required tool check box.
- 3 Select **Assign to User/Profile...** from the Actions  list. A Selector window appears.
- 4 Click the **All Users** tab and select the required operator to assign.
You can search for the operators using the **Filter** and **All Profiles** tabs also.
- 5 Click **OK**.

The Tool Group is assigned to the operator.

Create Data Source

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 **Policy Bank** → **SPI for Active Directory** → **Windows Server 2003 (or 2008)** → **Auto-Deploy** → **Discovery** → **Advanced Discovery** creates the required data sources in the data store of the HP Operations agent or HP Performance Agent.



You must deploy the instrumentation category *SPIDataCollector* before running this policy on the managed nodes.

Data Logging Scenarios

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

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

- 1 Create a folder `dsi2ddf` in the path `%OvAgentDir%\Conf`, if it does not exist.
- 2 Create a file `nocoda.opt`.
- 3 Type the names of the other data sources *except ADSPI*, which are to be created and for which the data logging must 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 logging metrics and description of each policy see *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide*.

4 Customizing Policies


Policies monitor the Microsoft Active Directory environment and run according to specific rules and schedules. Measurement threshold policies contain the rules for interpreting Microsoft Active Directory states or conditions. For more information on all the Microsoft Active Directory SPI policies, see *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide*.



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

You can customize one or more policies to suit the Microsoft Active Directory environment. If you customize policies after deployment, ensure that you redeploy the policies after customization.

To customize a policy, follow these steps:

- 1 Click **Policy Bank** → **SPI for Active Directory** → **Windows Server 2003** (or **2008**) → **Auto-Deploy** (or **Manual-Deploy**) for the corresponding policy group.
- 2 Select the check box corresponding to the required policy to customize and click **Edit...** from the  list.

The corresponding policy group window appears.

- 3 In this window you can customize the policy properties, settings parameters, and message threshold using the **Properties**, **Source**, **Script Parameters**, **Message Defaults**, **Thresholds**, and **Options** tabs.

Edit Measurement_Threshold Policy "ADSPI_ADSReplnBoundBytesWithinSite"

Properties Source Script Parameters Message Defaults Thresholds Options

Name: ADSPI_ADSReplnBoundBytesWithinSites

Type: advmonitor

Version: 7.0

Description: Checks the "Inbound Bytes" within Site

Note: Please do not use the browser BACK button, while editing. To quit the editor, use the "Cancel" button.

Save Restore Cancel

- 4 Click **Save**.

Policies

The policies for the Microsoft Active Directory SPI in the HPOM console are organized as Policy Group and Policy Type.

Policy Group

A policy group organizes policies according to the deployment method, area to be targeted for discovery, or monitoring. Deployment method can be auto or manual. To view auto and manually deployed policies, click **Policy Bank** → **SPI for Active Directory** → **Windows Server 2003** (or **2008**) → **Auto-Deploy** (or **Manual-Deploy**). The system displays the policies in each deployment type.

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 otherwise choose the 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.

Creating Custom Data Collection Groups

You can create custom data collection groups 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 creating a copy of the policies into the new group, you can modify them and change the version numbers. The user-created versions make it possible to deploy custom policies to node groups to meet their monitoring needs. Using this method makes it possible to bring nodes and policies together in groups that are easily recognizable.

Using Auto-Deploy Policies

The Auto-Deploy policies of Microsoft Active Directory SPI are divided into logical groups—for the discovery services and for monitoring the Microsoft Active Directory services and components. Some of the components are DIT, DNS, GC, FSMO, replication, response time, and trust relationships. The following sections describe the various sub groups of Auto-Deploy polices 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

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

FSMO Monitoring 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 measure the time required to propagate a change to all DCs within the domain. In addition, this policy also monitors 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

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

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

Sysvol Monitoring

Sysvol Monitoring 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

Trust Monitoring policies monitor trust health and gather data that allows the Trust Relationships tool to provide updates on 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 include connectivity, domain, organization unit structure, health, index query, replication or replication activities or both, security, and site structure. The following sections describe the various sub-groups of the Manual-Deploy policy and their functions.

Using 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.

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 the following 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.

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 would consist of 68% of the historical data, 2nd Standard deviation would consist of 95% of the historical data and 3rd Standard deviation would consist 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 is either above or below a particular Standard deviation, that is, 68% / 95% / 99%. As the severity indicates, whenever the current values fall below the 1st Standard deviation, a warning message is generated, along with an attribute which indicates whether the current value is higher or lower than the Standard deviation.

Connector Policies (only for Windows Server 2003)

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

Domain and OU Structure

Domain and OU Structure policies monitor domain and organization unit (OU) changes.

Global Catalog Access

Global Catalog Access policies monitor GC servers, gathering data from their performance monitor counters in regard to reads or writes or searches or all of the directory.

Health Monitors

Health Monitors policies check the Microsoft Active Directory services, events, processes, and synchronizations that are 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 System log.

Index and Query

Index and Query policy monitors index and query activity for authentications and LDAP client sessions.

Replication

Replication policy monitors replication using 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

Replication activity policy monitors the Directory Service log for replication events.

Security

The Security policies monitor the following:

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

Site Structure

Site Structure policies consist of the following:

- Security policies: These policies monitor:
 - Security event logs for Microsoft Active Directory related events
 - Security group changes
 - Performance monitor counters associated with Security
- *Site Structure policy*: Monitors the Microsoft Active Directory Site to ensure that IP subnets are not being added, changed, or deleted unnecessarily.

5 Using Tools

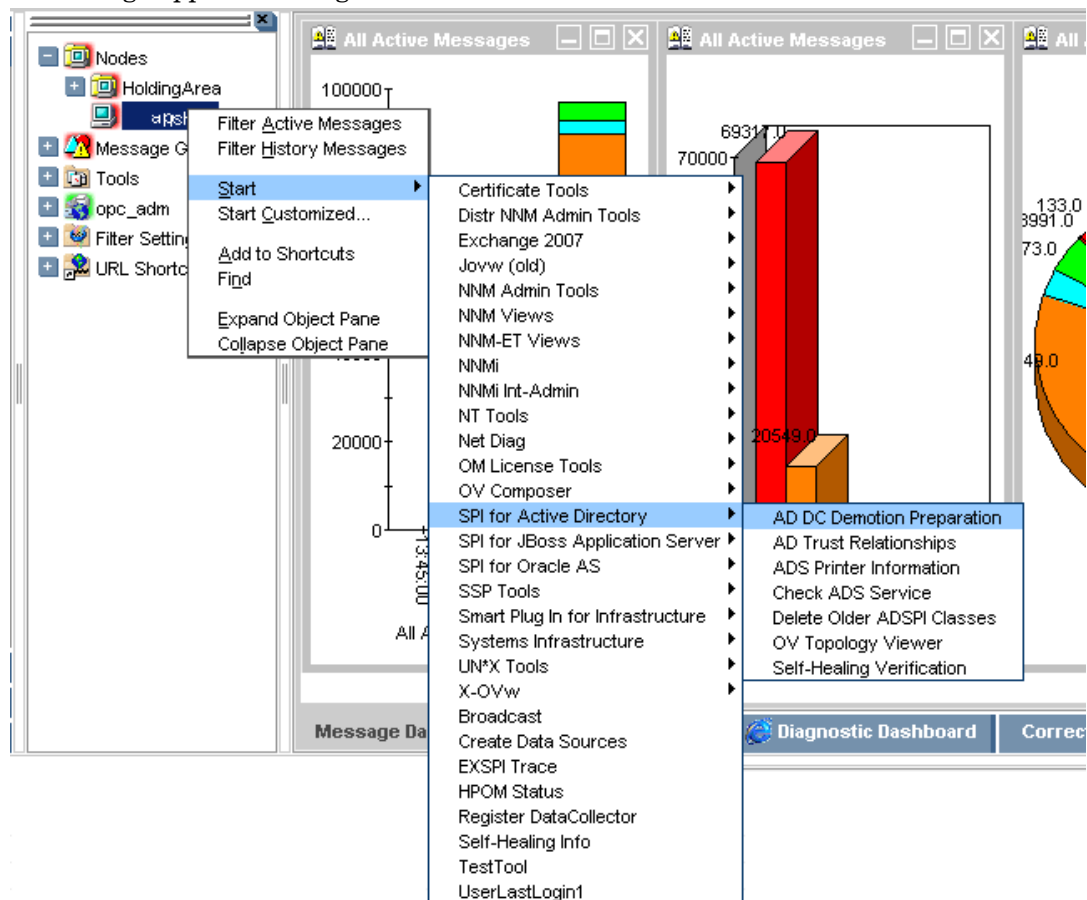
The Microsoft Active Directory SPI uses different tools to monitor the Microsoft Active Directory environment. For more information on the functioning of the tools, see the *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide*.

Starting Microsoft Active Directory SPI Tools

You can start the Microsoft Active Directory SPI tools from the interface assigned by the administrator. To start the Microsoft Active Directory SPI tools, follow these steps:

- 1 Right-click the node, on which, the tool is to be started.
- 2 Select **Start** → **SPI for Active Directory** → **<Specific Tool>**

A message appears stating that the tool is started.



Using AD Trust Relationship Tool

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

The following is an example of the Tool Output generated by the AD Trust Relationship tool.

```
Tool Output:

Local Domain Information -----
DCName: .....ADSP11
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

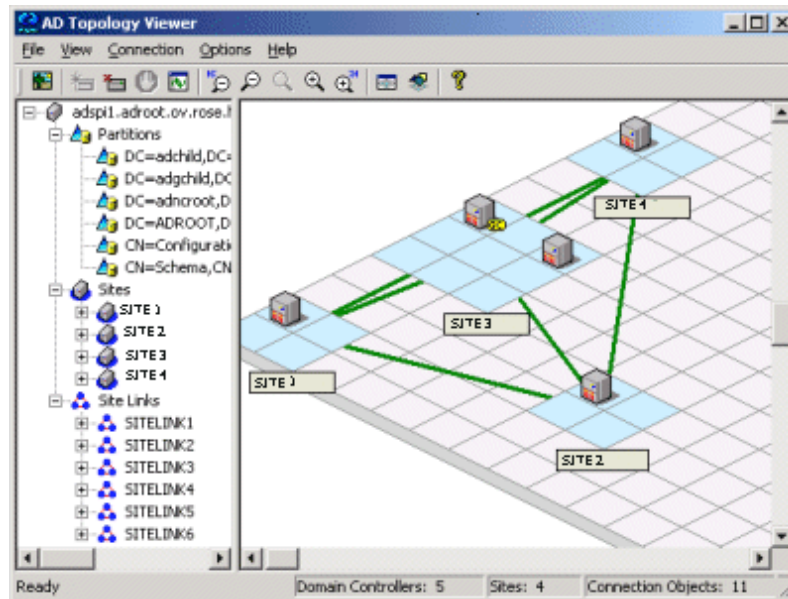
HP Operations Topology Viewer tool helps to view the content and topology of the Microsoft Active Directory in your environment by generating a map. After you launch the tool, you must connect to a DC to enable the functioning of the tool. When the connection is established, a window opens, displaying information about the Microsoft Active Directory partitions, connections and its link as replicated across the Microsoft Active Directory environment. The HP Operations Topology Viewer tool enables you to view the Microsoft Active Directory information in the following 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 hosting the DC, and the sites available through the connection.

- **Topological view of site connections:** The tool displays a graphical representation (three-dimensional map) of the configured sites, servers located in those sites, site links, forests, DCs, GCs, and connection objects linking them. You can move sites and DCs to accommodate more information in the map and for effective viewing.

To retrieve more information, such as, the version of Windows running and its status information, double-click the appropriate DC. The map has a zoom functionality and also allows exporting the view of the topology to a bitmap image.

The HP Operations Topology Viewer tool supplements the information you receive from other components of the Microsoft Active Directory SPI and has no dependency on any of the policies. Using this tool you can quickly view the various sites and server connections within the Microsoft Active Directory of your environment.



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



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

Starting HP Operations Topology Viewer Tool

The HP Operations Topology Viewer operates on Windows. This tool is not listed in the **Tool Bank**.

To start this tool:

- 1 Copy the file on a 32-bit Windows system, which is available in the following path:
<INSTALLDIR>/install/ADSPI/ovtv.zip
- 2 Extract the OVTV.zip.
- 3 Double-click on OVTV-Console.msi.
- 4 Go to the following directory:

`%ovinstalldir%\install\ADSPI-Console\InstallScripts` and double-click `postinstall-console.vbs`.

This registers the required DLLs.

- 5 Browse to `%ovdatadir%\bin\OVTV` and double-click `ovtv.exe` to start using OVTV.



If the logged-in user account has access to the DC to which you are attempting to connect, no alternate credentials are required.

After launching the HP Operations Topology Viewer 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 if the HP Operations Topology Viewer tool is running on the same DC to which you are connected. In such a case, you must 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. So, no other alternate credentials are required.

Getting Started with the HP Operations Topology Viewer Tool

When you launch the HP Operations Topology Viewer tool and connect it to a DC, it displays the tree view and the three-dimensional map. The tree lists the components of the server and the map shows the relationship among these components.

The map shows only the site links, which are 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:** The site link costs show the established connections between the sites and 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:** A server connection shown in red line indicates an error. This error can be because of a DC that no longer exists and is removed from the site, but the 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, you can remove the connection object manually.

Accessing Functions of HP Operations Topology Viewer Tool

You can access the functions of the HP Operations Topology Viewer using its menu commands, toolbar, or by right-clicking within the areas on either side of the Window pane.

Adjusting Map View

You can resize the viewable area of the map view to view all the sites and servers listed in the HP Operations Topology Viewer replication map. The following table lists the modifications you can make to a map view:

Table 2 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 or decrease the size of the rows or 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	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.

The following table lists the keyboard functionalities to move around the map:

Table 3 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.

Keystroke	Map function
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 Menu bar

The following table lists the HP Operations Topology Viewer menu and commands.

Table 4 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.
View	Toolbar	Toggles between the on or off display of the Topology Viewer toolbar buttons.
	Status Bar	Toggles between the on or off display of the Topology Viewer status bar (located at the bottom of the Topology Viewer window).
	Properties...	Opens the Site Topology Properties dialog box, which allows you to hide or show elements in the map and to modify the map appearance.












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.
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 following table lists the HP Operations Topology Viewer toolbar functions.

Table 5 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.

Icon	Function
	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.
	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, which results in a populated tree and topological map, you can access the following information:

- **Server Properties:** Right-click a server in either the tree or map to view the Server Properties sheet. It contains the following information:
 - *Identification:* This shows the GUID assigned to the server, its fully qualified domain name, distinguished name, date created, 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 an empty map cell (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 SPI.

For more information about reports and graphs, see *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide*.

Using Reports and Graphs

Report and graph-generating templates are installed installing the Microsoft Active Directory SPI. These templates provide 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.

The reports are web-based and are automatically generated every night. It provides you with a routine means of checking the 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 showing the trust relationship changes between DCs are also available for Windows 2003 and 2008 systems.

Integrating Microsoft Active Directory SPI with HP Reporter

You must install Microsoft Active Directory SPI Reporter package on HP Reporter Server to use the Microsoft Active Directory SPI reports. For this, run the `ADSPI-Reporter.msi setup` and install the Microsoft Active Directory SPI Report Package on the Reporter server. After the installation you can configure the HP Reporter to generate reports.

Installing Report Package

To install the Microsoft Active Directory SPI Report Package on a stand-alone Reporter server:

- 1 Insert the HP Operations Smart Plug-in DVD.
- 2 Browse to the folder `<DVD>/WINDOWS/OV_REPORTER/AD_SPI` and double-click the file `ADSPI-Reporter.msi`.
- 3 Follow the instructions as they appear for the installation on the management server for Windows till a dialog box opens indicating the completion of the installation.
- 4 Select **Complete** for the **Setup Type**, and click **Next**. A dialog box updates you about the installation progress.

For HP Performance Manager on HP-UX, Solaris, or Linux, copy the graph templates to the required directory, if HP Performance Manager is installed on a separate node. You need not do this task if HP Performance Manager is installed on an HPOM management server system.

When you install the Microsoft Active Directory SPI on the HPOM management server, the HP Performance Manager also is installed. If you want to generate a graph successfully, you must identify the appropriate installation scenario and proceed accordingly.

Following are the three possible scenarios of installation requirement:

Scenario #1 — English/Japanese environments where the HPOM management server and HP Performance Manager are installed on the same system: No further installation is necessary.

Scenario #2 — English environments where the HPOM management server and HP Performance Manager are installed on separate systems: Copy the HP Performance Manager files from the HPOM management server directories to the identical directories of the HP Performance Manager HP-UX, Linux, or Solaris system. Directory and file are as follows:

```
/opt/OV/newconfig/OVPM/VPI_Graphs_Active_Directory.txt
```

Scenario #3 — Japanese environments where the HPOM management server and HP Performance Manager are installed on separate systems: Copy the HP Performance Manager files from the HPOM management server directories to the identical directories on the HP Performance Manager HP-UX, Linux, or Solaris system. Directory and file are as follows:

```
/opt/OV/newconfig/OVPM/jpn/VPI_Graphs_Active_Directory.txt
```

Configuring Report Package

To configure the Microsoft Active Directory SPI Report Package, follow these steps:

- 1 Open the Reporter main window and check the status pane to note the changes to the Reporter configuration that 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 [Integrating Microsoft Active Directory SPI with HP Reporter](#) 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.

Accessing Reporter Help

Instructions are available in the HP Reporter Help for assigning Microsoft Active Directory SPI reports to the targeted nodes.

To access HP Reporter Help, follow these steps:

- 1 Right-click **Reports** or **Discovered Systems** in the left panel of the HP Reporter main window.

- 2 Select **Report Help** or **Discovered Systems Help** from the sub-menu that appears. The HP Reporter Help appears.

Generating Reports

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



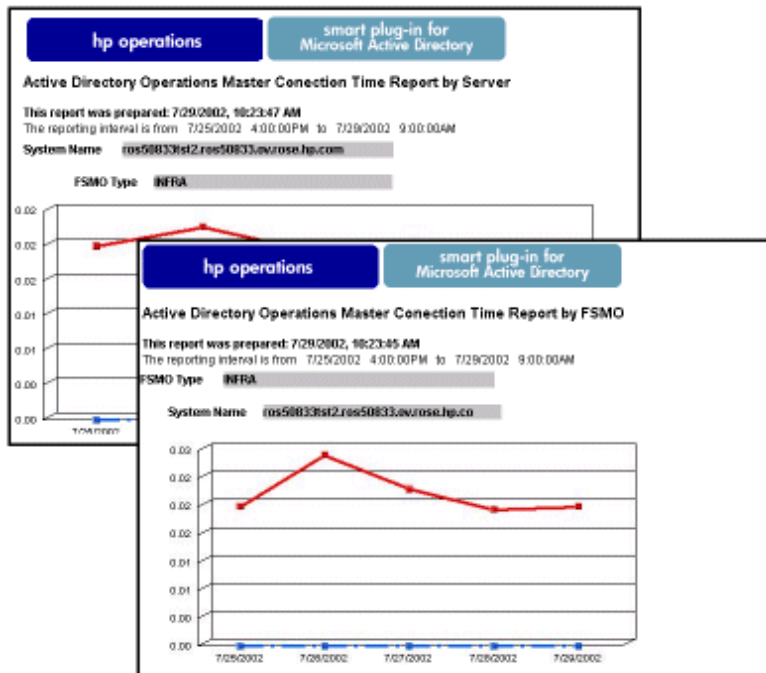
If you want to customize your reports you must install HP Reporter. For more information on modifying the reports, see the Concepts Guide, Installation Guide and Special Configuration Guide, Online Help, and Release Notes.

The report data of Microsoft Active Directory SPI is collected based on metrics used for each report. The HP Reporter identifies the data using metric variables. This data is stored in the MS SQL Reporter database. The following example shows the metric variable identified for reporting:

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

is identified as `ADSPI_RESPONSEMON.SYSTEMNAME`

You can access the reports of Microsoft Active Directory SPI from the **Reports** option on the HPOM console. See *HP Operations Smart Plug-in for Microsoft Active Directory SPI Reference Guide* for a complete description of reports.



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

- a Insert the Smart Plug-ins DVD-ROM containing the reporting packages into the DVD-ROM drive, and in Windows Explorer, double-click **<SPIDVD>/WINDOWS/OV_PM/AD_SPI/HPOvSpiAdGc.msi**
- b Follow the instructions as they appear.

For more information on HP Performance Manager, see the HP Performance Manager documentation.

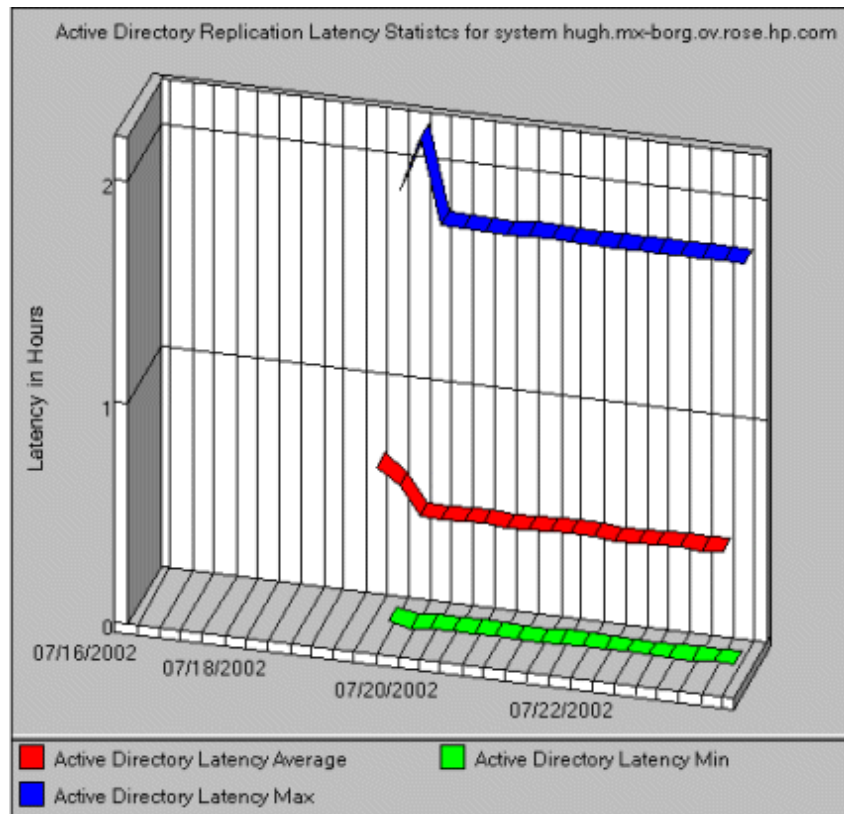
Generating Graphs

You can generate the Microsoft Active Directory SPI graphs on OVPM, on a stand-alone Windows Server.

To install the Microsoft Active Directory SPI Graphs Package on a stand-alone OVPM Windows Server, follow these steps:

- 1 Insert the HP Operations Smart Plug-ins DVD.
- 2 Double-click the file `HPOvSpiAdGc.msi`.
- 3 Follow the installation steps on the management server for Windows. A dialog box opens.

- 4 Select **Complete** for the **Setup Type**, and click **Next**. The preceding dialog box updates you on the installation progress.



7 Troubleshooting

This chapter includes troubleshooting information for the Microsoft Active Directory SPI and provides solutions to resolve the problems. The methods described may or may not require support assistance.

Failed Discovery

The following sections describe the possible causes and suggested actions 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 are as follows:

- *Possible cause:* The account with which the Basic Discovery policy (**Policy Bank → SPI for Active Directory → Windows Server 2003 (or 2008) → 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 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 are 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. Follow these steps:
 - a Log on 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 if the `out.xml` is in the required xml format by opening it in the web browser.

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 are 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 must change this command as follows:

```
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** in the script.

Reports and Graphs

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

Reports and Graphs are not generated

In some cases, when 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. So the policy fails to collect the data that the HP Reporter generates as report. Failure to deploy the appropriate policy also disables the HP Performance Manager 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 policies accordingly.

Data Logging Policies cannot log Data

In some cases when 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 data stores—CODA or OVPA or both.

- *Suggested action:* Check if the data source 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 data source ADSPI is created.

Browser crashes while viewing HTML Report

While viewing the report, the browser crashes. The possible cause and suggested action are as follows:

- *Possible cause:* The browser cannot handle huge amount of data.
- *Suggested action:* View the report in PDF format.

Reports Fail with Oracle Database

Some of the reports fail because of 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, make sure that you change the 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 Reference Guide*.

8 Removing Microsoft Active Directory SPI

Before removing the Microsoft Active Directory SPI you must remove all the existing policies and instrumentation categories from all the managed nodes.

Removing Microsoft Active Directory SPI from HPOM

For HP-UX:

To remove the Microsoft Active Directory SPI from the HPOM management server using the command line interface, run the following command:

```
swremove ADSPI
```

The installer removes Microsoft Active Directory SPI from the management server.

For Solaris and Linux:

You can remove the Microsoft Active Directory SPI from the Solaris or Linux management servers, using any of the following interfaces:

- Graphical User Interface
- Command Line Interface

Removing the Microsoft Active Directory SPI Using Graphical User Interface

To remove the Microsoft Active Directory SPI using X-Windows client software, follow these steps:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the Solaris or Linux management server DVD drive.
- 3 Start the X-windows client software and export the **DISPLAY** variable by typing the following command:

```
export DISPLAY=<ip address>:0.0
```

- 4 To start the installation, type the following command:

For Solaris:

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin
```

For Linux:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin
```

The Initialization window opens

- 5 Select the language from the drop-down list and click **OK**.

The Application Maintenance window opens.

- 6 Select **Uninstall** and click **Next**.



When you have, more than a SPI installed on the Solaris or Linux management server and you want to remove only a SPI out of the installed SPIs, select the Modify option and then select the SPI you want to retain. Do not select the SPI that you want to remove.

The Pre-Uninstall Summary window opens.

- 7 Click **Uninstall**.

The Uninstall window opens.

- 8 Click **Done** when the Microsoft Active Directory SPI is uninstalled.

Removal of the Microsoft Active Directory SPI Using Command Line Interface

To remove the Microsoft Active Directory SPI using the command line interface, follow these steps:

- 1 Log on as a **root** user.
- 2 Insert the HP Operations Smart Plug-ins DVD into the Solaris or Linux management server DVD drive. Mount the DVD, if necessary.
- 3 To start the removal of the Microsoft Active Directory SPI, type the following command and press Enter:

For Solaris:

```
./HP_Operations_Smart_Plug-ins_Solaris_setup.bin -i console
```

For Linux:

```
./HP_Operations_Smart_Plug-ins_Linux_setup.bin -i console
```

- 4 When the option, 'Choose Locale...' appears, enter the number corresponding to the language you want to choose and press **Enter**.

The HP Software Installer content appears.

- 5 Press **Enter** to continue.

The Maintenance Selection content appears.

- 6 Enter the appropriate option (number) to start the removal of the Microsoft Active Directory SPI and Press **Enter**.



If you have more than one SPI installed on the HPOM for Solaris or Linux server and you want to remove some of the SPIs, select the Modify (1) option from the installer and select the SPIs you want to retain. Do not select the SPIs that you want to remove.

The Pre-Installation Summary content appears.

- 7 Press **Enter** to continue.

The selected features are removed.


When the removal process is complete, a message appears stating that the removal of Microsoft Active Directory SPI is completed successfully.

Removing Other Components of the Microsoft Active Directory SPI

You can remove other components of Microsoft Active Directory SPI, that is, message group, user profile, report, and graph package.

Removing the Microsoft Active Directory SPI Message Group


To remove the Microsoft Active Directory SPI message group, follow these steps:

- 1 Click **Browse** → **All Message Groups**. The system displays all the existing message groups.
- 2 Select the **ADSPI** message group check box.
- 3 Select **Delete** from the list and click  to delete the Microsoft Active Directory SPI message group.

The Microsoft Active Directory SPI message group is removed successfully.

Removing All User Profiles

To remove the all user profiles, follow these steps:

- 1 Click **Browse** → **All User Profiles**. The system displays all the existing user profiles.
- 2 Select the check box corresponding to user profile to be deleted.
- 3 Select **Delete** from the list and click  to delete the user profile.

The user profile is removed successfully.

Removing Report Package

You can remove the Reporter Package using the Control Panel or the `.msi` file.

Removing Report Package using Control Panel

To remove the Report Package using the Control Panel, follow these steps:

- 1 Click **Start** → **Control Panel** → **Add or Remove Programs**.
- 2 Select **HP Operations Smart Plug-in for Microsoft Active Directory - Reporter Component Integration**.
- 3 Click **Remove** and then **Yes** to confirm the removal.

The Report Package is removed from the system.

Removing Report Package using `.msi` file

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

- 1 Go to the following directory:

<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 Graph Package

You can remove the Graph Package using the Control Panel or .msi file.

Removing Graph Package using Control Panel

To remove the Graph Package using the Control Panel, follow these steps:

- 1 Click **Start** → **Control Panel** → **Add or Remove Programs**.
- 2 Select **HP Operations Smart Plug-in for Microsoft Active Directory - Graphing Component Integration**.
- 3 Click **Remove** and then **Yes** to confirm the removal.

The Graph Package is removed from the system.

Removing Graphing Package using .msi File

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

- 1 Go to the following directory:
<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

Numerics

3-dimensional map, 41

C

Components

- Graphs, 10
- Policies, 9
- Reports, 10
- Tools, 10

D

Data sources, 31

Discovered services, 10

Discovery

- Advanced Discovery, 31
- Basic Discovery, 26

Domain_Controllers node group and ADSPI message group, 28

Domain controllers, 9

F

Functions

- Customize policies, 13
- Discover existing components, 10
- Display information, 10
- Generate graphs, 13
- Generate reports, 13

G

Global Catalog, 9

Graphs

- HP Performance Manager, 52

H

HP Reporter Help, 50

I

Installation Packages

- Graphing Package, 15
- Reporting Package, 16
- SPI Package, 15

Instrumentation categories, 26

InterSite Topology Generators, 42

L

LDAP, 9

M

Managed node, 16

Microsoft Active Directory SPI

- Configuration, 25
- Installation, 20
- Removing, 59

P

Policies

- Auto-Deploy, 34
- Custom Data Collection Groups, 34
- Manual-Deploy, 36
- Policy Group, 34
- Policy Type, 34

Policy Bank, 23

Pre-requisites

- Hardware, 18
- Software, 18

R

Reports

- HP Reporter, 49

S

Service map alerts, 9

T

Thresholds, 9

Tools

AD Trust Relationships Tool, 40

HP Operations Topology Viewer Tool, 40

Troubleshooting, 55

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:

