

# HP Operations Smart Plug-in for Microsoft<sup>®</sup> Active Directory

for the HP Operations Manager for UNIX<sup>®</sup>

Software Version: 7.00

---

## Installation and Configuration Guide

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



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notices

© Copyright 2009 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](http://www.hp.com/go/hpsoftwaresupport)**

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

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

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

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

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

<b>1</b>	<b>Introducing the Smart Plug-in for Microsoft Active Directory on UNIX</b>	<b>9</b>
	About the Smart Plug-in for Microsoft Active Directory	9
	Components of the Microsoft Active Directory SPI	10
	Policies	10
	Tools	10
	Reports	10
	Graphs	10
	Functions of the Microsoft Active Directory SPI	11
	Collecting and Interpreting the Performance and Availability of Information	11
	Displaying Information	11
	Service Map	11
	Message Browser	13
	Instruction Text	13
	Reports and Graphs	13
	HP Operations Topology Viewer Tool	13
	Generating Reports Using HP Reporter	14
	Graphing Data with HP Performance Manager	14
	Customizing Policies	14
<b>2</b>	<b>Installing the Microsoft Active Directory SPI</b>	<b>15</b>
	Installation Packages	17
	SPI Package	17
	Graphing Package	17
	Reporting Package	17
	Installation Environments	17
	Standard Installation of SPI Components on the HPOM Server	17
	Standalone Installation on HP Reporter and HP Performance Manager	18
	Pre-requisites to Installing Microsoft Active Directory SPI	18
	Hardware Requirements	18
	Software Requirements	18
	Mounting the SPI DVD	18
	Mounting the DVD on HP-UX	19
	Mounting the DVD on Solaris	19
	Installing Microsoft Active Directory SPI	19
	Verifying the Installation of Microsoft Active Directory SPI	20
<b>3</b>	<b>Configuring Microsoft Active Directory SPI</b>	<b>21</b>
	Configuration Procedure	21
	Manage Domain Controller Nodes	21
	Assign Domain Controller Nodes to Node Group	22
	Assign Basic Discovery Policy Group to DC Nodes	23
	Assign Instrumentation Categories to Domain Controllers Nodes	25
	Deploy Configuration	27
	Assign other Microsoft Active Directory SPI Policies to Domain Controllers Nodes	28
	Deploy other Microsoft Active Directory SPI Policies to Domain Controller Nodes	30
	Assign Domain_Controllers Node Group and ADSPI Message Group to the Operator	31

Assign Microsoft Active Directory SPI Services to the Operator .....	34
Assign Tool Group to Operator .....	35
Create ADSPI Data Source .....	36
Data Logging Scenarios .....	37
<b>4 Customizing Policies</b> .....	<b>39</b>
Policy Group and Policy Type .....	40
Policy Group .....	40
Policy Type .....	40
Creating Custom Data Collection Groups .....	41
Using Auto-Deploy Policies .....	41
Discovery .....	41
DIT Monitoring .....	41
DNS Monitoring .....	41
FSMO Monitoring .....	41
Replication Monitoring .....	42
Response Time Monitoring .....	42
GC Monitoring .....	42
Sysvol Monitoring .....	42
Trust Monitoring .....	42
Using Manual-Deploy Policies .....	42
Using Auto-Baseline Policies .....	42
Connector policies (only for Windows Server 2003) .....	43
Domain and OU Structure .....	43
Global Catalog Access .....	43
Health Monitors .....	44
Index and Query .....	44
Replication .....	44
Replication Activity .....	44
Security .....	44
Site Structure .....	44
<b>5 Using Tools</b> .....	<b>45</b>
Starting Microsoft Active Directory SPI Tools .....	45
Using AD Trust Relationships Tool .....	46
Using HP Operations Topology Viewer Tool .....	47
Starting HP Operations Topology Viewer Tool .....	48
Getting Started with the HP Operations Topology Viewer Tool .....	48
Accessing Functions of HP Operations Topology Viewer Tool .....	49
Adjusting Map View .....	49
HP Operations Topology Viewer Menubar .....	52
HP Operations Topology Viewer Toolbar .....	55
Accessing Server and Map Properties .....	56
<b>6 Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions</b> .....	<b>57</b>
Using Reports and Graphs .....	57

Integrating Microsoft Active Directory SPI with HP Reporter.....	58
Installing Report Package .....	58
Configuring Report Package .....	58
Generating Reports .....	59
Integrating Microsoft Active Directory SPI with HP Performance Manager .....	60
Generating Graphs.....	61
<b>7 Troubleshooting .....</b>	<b>63</b>
Troubleshooting Discovery .....	63
Insufficient Privileges .....	63
Failed Binary on the Managed Node.....	63
Troubleshooting through Tracing.....	64
Troubleshooting Reports and Graphs .....	64
Reports and Graphs are not generated.....	64
Data Logging Policies cannot log Data .....	65
Browser crashes while viewing HTML Report.....	65
Reports Fail with Oracle Database .....	65
Modifying Policy Names .....	65
<b>8 Removing Microsoft Active Directory SPI .....</b>	<b>67</b>
Removing Microsoft Active Directory SPI from HPOM .....	67
Removing Other Components of Microsoft Active Directory SPI.....	67
Removing Microsoft Active Directory SPI Message Group .....	67
Removing All User Profiles .....	67
Removing Report Package .....	68
Removing Graph Package .....	68
Removing Reporting and Graphing Package using .msi File .....	68
Removing Reporting Package using .msi file .....	68
Removing Graphing Package using .msi File.....	69
<b>Index.....</b>	<b>71</b>





---

# 1 Introducing the Smart Plug-in for Microsoft Active Directory on UNIX

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

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

## About the Smart Plug-in for Microsoft Active Directory

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

- Data consistency across the domain controllers (DCs).
- Timely replication process.
- Systems outages capability.
- Successful functioning of role masters.
- DCs competing with over-utilized CPUs.
- Capacity and fault-tolerance issues in Microsoft Active Directory.
- Replication of Microsoft Active Directory Global Catalog (GC) in a timely manner.
- Acceptable performance levels of services, event, processes, and synchronizations.
- Occurrence of index and query activities such as authentications and lightweight directory access protocol (LDAP) client sessions at acceptable levels.
- Expected trust relationship status between sites and DCs.

# Components of the Microsoft Active Directory SPI

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

## Policies

Policies are pre-defined thresholds that keep a constant vigilance over the Microsoft Active Directory environment and improve monitoring schedules in the form of the service map alerts and messages. Service map alerts are shown in service map while 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 the utilities that gather Microsoft Active Directory related information. You can also launch tools to view the Microsoft Active Directory environment. For more information, see [Chapter 5, Using Tools](#).

## Reports

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

## Graphs

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

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

# Functions of the Microsoft Active Directory SPI

The Microsoft Active Directory SPI monitors the Microsoft Active Directory.

## Collecting and Interpreting the Performance and Availability of Information

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

## Displaying Information

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

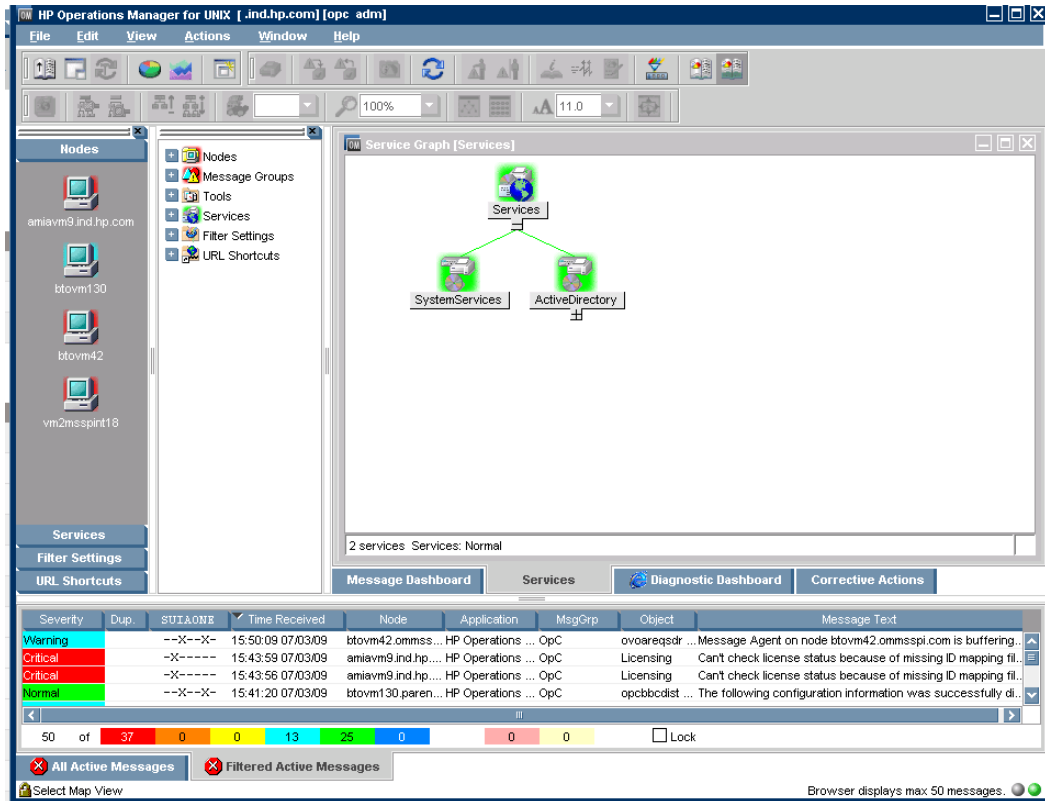
### Service Map

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

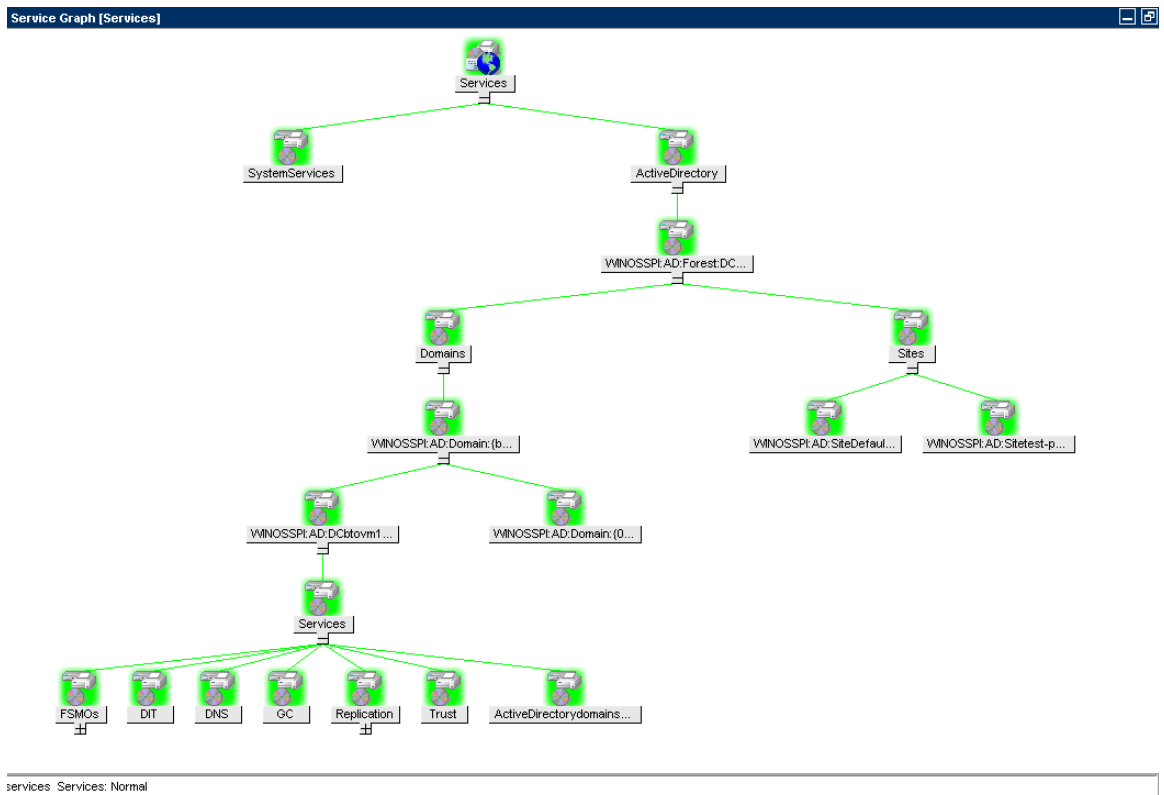
To view the Microsoft Active Directory services, log into the operator's GUI. Following these steps:

- 1 From the Administration UI, click **Integrations** → **HPOM for Unix Operational UI**. The login window appears.
- 2 Type the user name and password.

- Click **Services**. The service map appears.



- Expand the hierarchy to view the specific services present on each DC. Further expansion of each DC displays its components.



## Message Browser

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

Severity	Dup	SITA/OMI	Time Received	Node	Application	Msggrp	Object
Normal	--X--X--	13:03:31	08/13/09	btovm130.paren...	HP Operations ...	OpC	ovoregsdr... Successfully contacted the HP...
Normal	--X--X--	12:52:03	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Normal	--X--X--	12:51:59	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Normal	--X--X--	12:51:59	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Warning	--X--X--	12:42:38	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... %File Replication Se...
Warning	--X--X--	12:42:35	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... %File Replication Se...
Warning	--X--X--	12:42:35	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... %File Replication Se...
Warning	--X--X--	12:41:48	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... %File Replication Se...
Warning	--X--X--	12:41:48	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... %File Replication Se...
Warning	--X--X--	12:16:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	12:06:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	12:06:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:51:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:51:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:36:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:36:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:36:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Normal	--X--X--	11:31:44	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Normal	--X--X--	11:31:43	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Normal	--X--X--	11:31:41	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Normal	--X--X--	11:31:41	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Normal	--X--X--	11:31:41	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-101: EventID: 0x0000...
Warning	--X--X--	11:21:43	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:21:43	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:21:42	08/13/09	btovm130.paren...	Microsoft Activ...	MS_AD_SER...	Health Mont... ADSPI-103: EventID: 0x8000...
Warning	--X--X--	11:18:42	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... Logfile %File Replication Ser...
Warning	--X--X--	11:18:39	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... Logfile %File Replication Ser...
Warning	--X--X--	11:18:21	08/13/09	btovm130.paren...	HP OperView ...	OpC	opcle (Lo... Logfile %File Replication Ser...

## Instruction Text

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

## Reports and Graphs

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

## HP Operations Topology Viewer Tool

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

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

## Generating Reports Using HP Reporter

You can generate reports to analyze past or present Microsoft Active Directory conditions. These Web-based reports are automatically generated every night. They provide 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 covering the trust relationship changes between DCs are also available for Windows 2003 and Windows 2008 nodes. For more information on HP Reporter see, [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

## Graphing Data with HP Performance Manager

After you manually generate the graphs, you can view the data in a more specified and granular manner. You can access graphs in the HP Performance Manager console. You can integrate the Microsoft Active Directory SPI with HP Performance Manager to generate and view graphs. For more information on HP Performance Manager, see [Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions](#).

## Customizing Policies

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

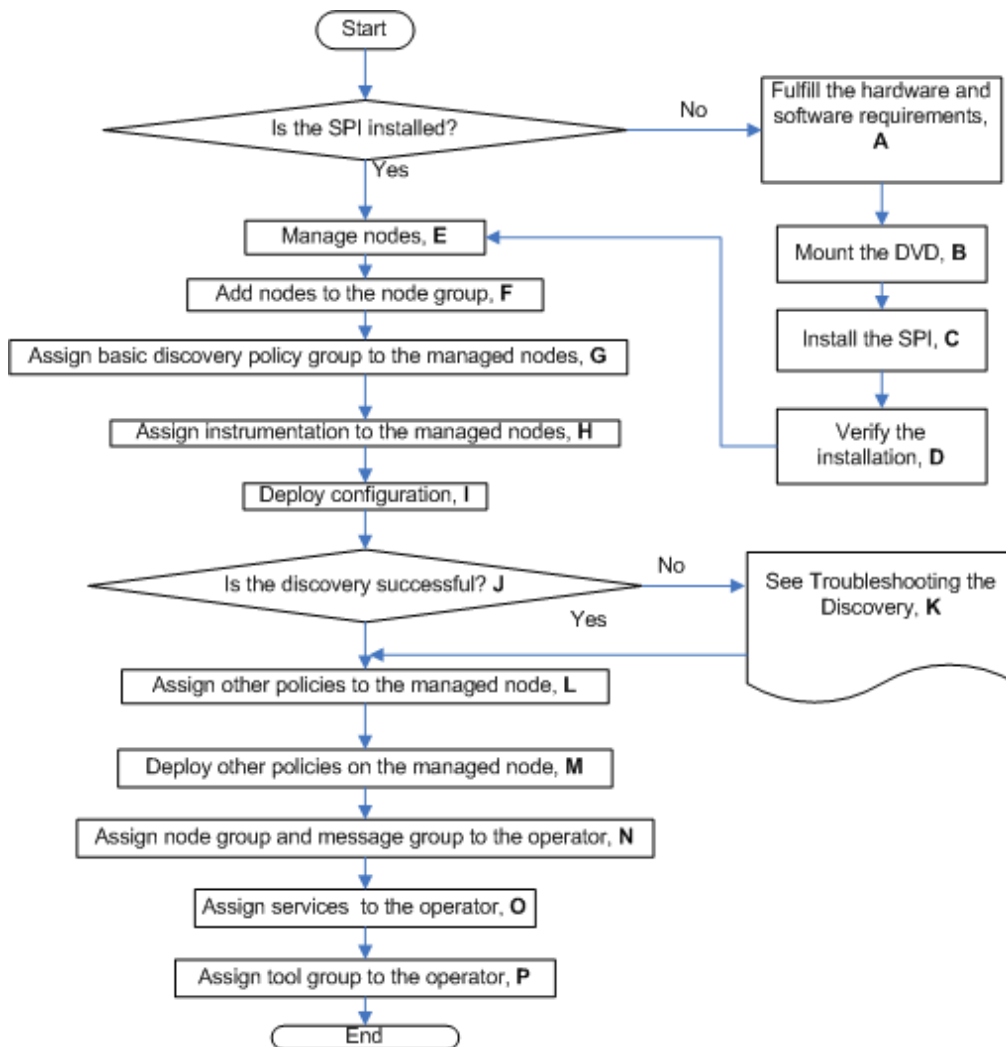
- Script-parameters
- Rules
- Options

## 2 Installing the Microsoft Active Directory SPI

Perform the tasks mentioned in the following sections to install the Microsoft Active Directory SPI on Operations Manager for UNIX.

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

**Figure 1 An Overview of Installation and Configuration Steps**



**Table 1 References of Legends of Flowchart**

<b>Legend</b>	<b>References</b>
<b>A</b>	Pre-requisites to Installing Microsoft Active Directory SPI on page 18
<b>B</b>	Mounting the SPI DVD on page 18
<b>C</b>	Installing Microsoft Active Directory SPI on page 19
<b>D</b>	Verifying the Installation of Microsoft Active Directory SPI on page 20
<b>E</b>	Manage Domain Controller Nodes on page 21
<b>F</b>	Assign Domain Controller Nodes to Node Group on page 22
<b>G</b>	Assign Basic Discovery Policy Group to DC Nodes on page 23
<b>H</b>	Assign Instrumentation Categories to Domain Controllers Nodes on page 25
<b>I</b>	Deploy Configuration on page 27
<b>J</b>	Service Map on page 11
<b>K</b>	Troubleshooting Discovery on page 63
<b>L</b>	Assign other Microsoft Active Directory SPI Policies to Domain Controllers Nodes on page 28
<b>M</b>	Deploy other Microsoft Active Directory SPI Policies to Domain Controller Nodes on page 30
<b>N</b>	Assign Domain_Controllers Node Group and ADSPI Message Group to the Operator on page 31
<b>O</b>	Assign Microsoft Active Directory SPI Services to the Operator on page 34
<b>P</b>	Assign Tool Group to Operator on page 35



# Installation Packages

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

## SPI Package

The SPI package is the core .depot (HP-UX) and .sparc (Solaris) package, which contains all the functionality of the SPI. Install the .depot or .sparc file on an HPOM server. You can find the SPI package in the following location:

For HP-UX: <SPI DVD>\HPUX\HP\_Operations\_Smart\_Plug-ins\_HPUX.depot

For Solaris: <SPI DVD>\SOLARIS\HP\_Operations\_Smart\_Plug-ins\_SOLARIS.sparc

## Graphing Package

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

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

## Reporting Package

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

<SPI DVD>\SPIS\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 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 PM) while installing the Microsoft Active Directory SPI on the HPOM server through the HP Operations Smart Plug-Ins DVD.

## Standalone Installation on HP Reporter and HP Performance Manager

For a standalone managed node (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 PM installed then the graphing package of the Microsoft Active Directory can be installed on the nodes.

## Pre-requisites to Installing 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 fulfilled:

On the management server:

- HP Operations Manager for UNIX: 9.0
- 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.

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)

## Mounting the SPI DVD

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

## Mounting the DVD on HP-UX

To mount the SPI DVD on HP-UX:

- 1 Log on as user root.
- 2 Set the user root's umask by entering:  
`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 mount it as user root by entering:  
`mount /dev/<dvdrom_drive_name> /<mount_point>`  
For example, for a local DVD, you can enter:  
`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.

## Mounting the DVD on Solaris

Insert the DVD into the DVD drive. The DVD is automatically mounted (and unmounted) on Sun Solaris systems.

## Installing Microsoft Active Directory SPI

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

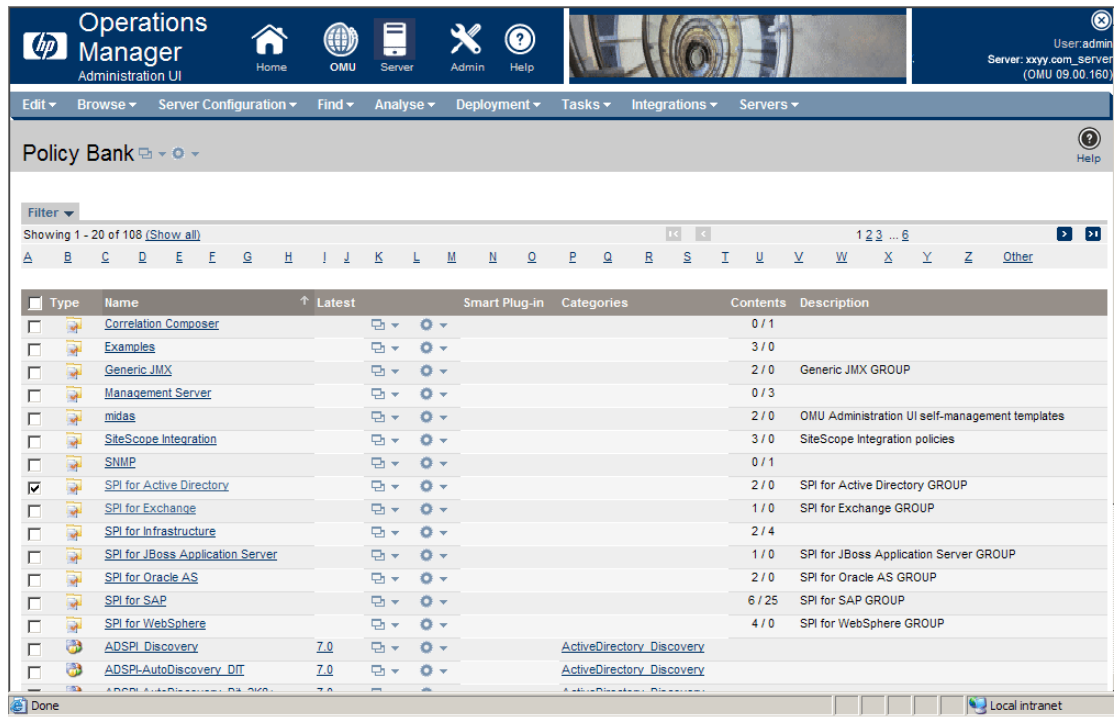
- 1 Insert the SPI DVD into the DVD-ROM drive of the management server.
- 2 Run the following commands:
  - HP-UX 11.x management server:  
`swinstall -s /cdrom/HPUX/HP_Operations_Smart_Plug-ins_HPUX.depot ADSPI`
  - Solaris management server:  
`pkgadd -s /cdrom/SOLARIS/HP_Operations_Smart_Plug-ins_SOLARIS.sparc ADSPI`

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

# Verifying the Installation of Microsoft Active Directory SPI

To verify the Microsoft Active Directory SPI has been installed properly, perform one of the following steps:

- Check the Policy Bank which contains SPI for Active Directory. For this, click **Policy Bank**. SPI for Active Directory is displayed. All Microsoft Active Directory SPI policies are in the policy group, Windows Server 2003 and Windows Server 2008.



- From the command prompt of HPOM 9.0 server, browse to `/var/opt/ov/share/databases/OpC/mgd_node/instrumentation`. You can see the Instrumentation groups **ActiveDirectory\_Core** and **ActiveDirectory\_Discovery**. All ADSPI 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 expands that discovery and adds multiple hierarchical levels of details.

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

This is shown in the service map. With each expansion you can drill down from a service alert at the forest level to the specific service or component in a specific DC that is the root cause.

### Configuration Procedure


Configure the Microsoft Active Directory SPI by performing the tasks in the following sections.

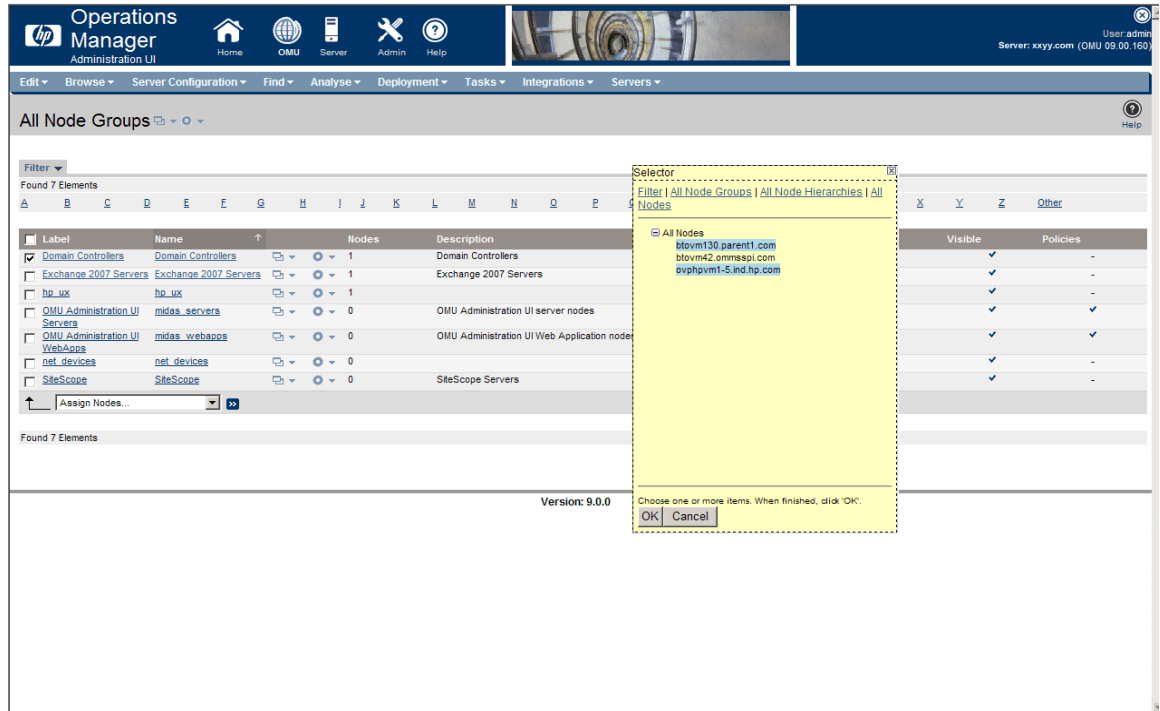
#### Manage Domain Controller Nodes

Start the configuration by managing the Domain Controller (DC) nodes. See section *Organizing Managed Nodes* of Chapter 3 *Configuring and Maintaining HPOM* in the *HP Operations Manager for UNIX Concepts Guide*.

## Assign Domain Controller Nodes to Node Group

Assign the DC nodes to the **Domain\_Controllers** node group. To assign nodes, perform the following:

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



The screenshot shows the HP Operations Manager Administration UI. The main content area displays a table of 'All Node Groups' with 7 elements found. The 'Domain\_Controllers' group is selected. The 'Assign Nodes...' dropdown menu is open, showing a list of nodes. A 'Selector' window is overlaid on the table, displaying a list of nodes under the 'All Nodes' section. The nodes listed are:

- blotvm130.parent1.com
- blotvm42.ommsapi.com
- gvptpvm1-5.ind.hp.com

The 'Selector' window also includes a filter bar and 'OK' and 'Cancel' buttons.

A message displays to report the successful assignment of the nodes to the Domain\_Controllers node group.

The screenshot shows the HP Operations Manager Administration UI. At the top, there is a navigation bar with the HP logo and 'Operations Manager Administration UI'. Below this is a secondary navigation bar with options like 'Edit', 'Browse', 'Server Configuration', 'Find', 'Analyse', 'Deployment', 'Tasks', 'Integrations', and 'Servers'. The main content area displays a 'Note' box with the message 'assign for nodegroup was successful.' Below the note is a 'Filter' section showing 'Found 7 Elements' and a table of node groups.


Label	Name	Nodes	Description	Visible	Policies
<input type="checkbox"/>	Domain_Controllers	1	Domain Controllers	<input checked="" type="checkbox"/>	-
<input type="checkbox"/>	Exchange 2007 Servers	1	Exchange 2007 Servers	<input checked="" type="checkbox"/>	-
<input type="checkbox"/>	hp_ux	1		<input checked="" type="checkbox"/>	-
<input type="checkbox"/>	OMU Administration UI Servers	0	OMU Administration UI server nodes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	OMU Administration UI WebApps	0	OMU Administration UI Web Application nodes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	net_devices	0		<input checked="" type="checkbox"/>	-
<input type="checkbox"/>	SiteScope	0	SiteScope Servers	<input checked="" type="checkbox"/>	-

## Assign Basic Discovery Policy Group to DC Nodes

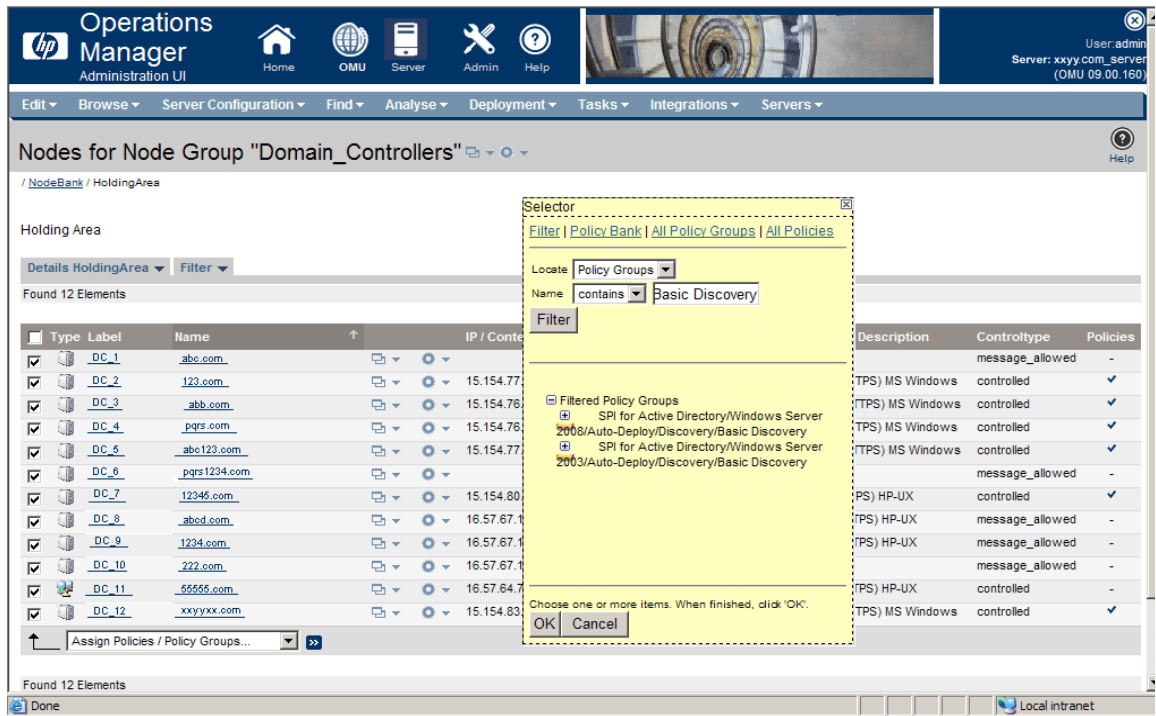
Assign Basic Discovery policy group to the DC nodes of the **Domain\_Controllers** node group to start the discovery process of the basic components of Microsoft Active Directory. The discovered components of Microsoft Active Directory can be viewed through the operator's interface.

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

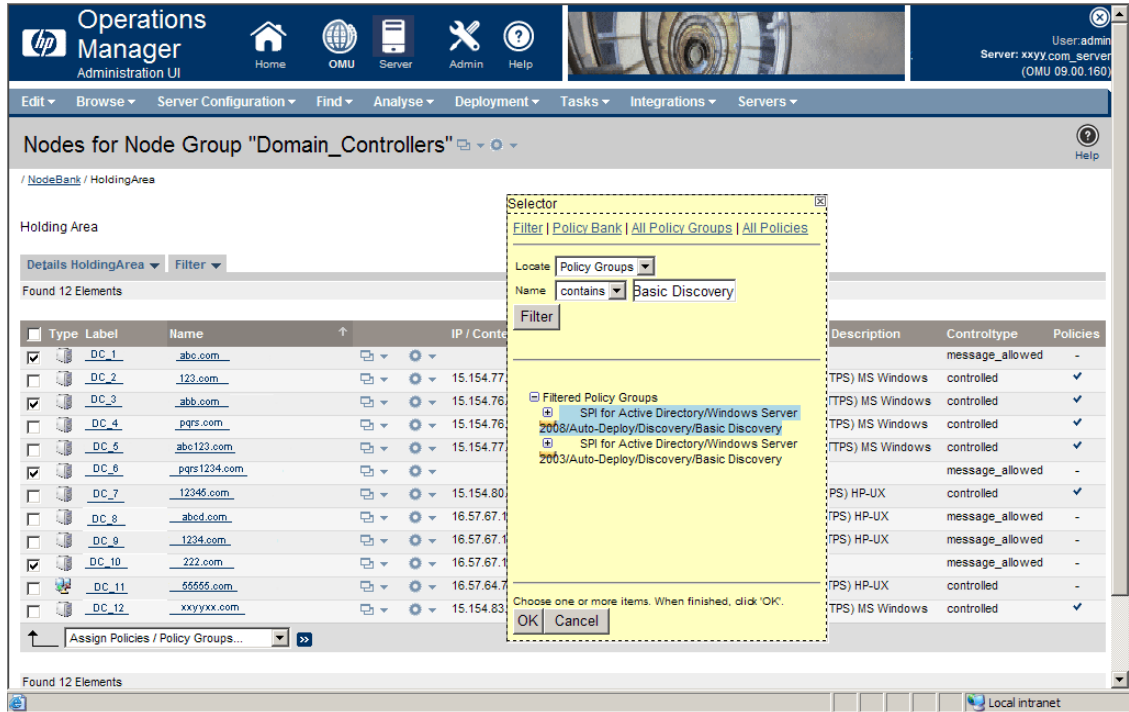
To assign the Basic Discovery policy group to the DC nodes:

- 1 Click **Browse** → **All Node Groups** and click the **Domain\_Controllers** node group.
- 2 Select all the **DC** nodes check box to assign the Basic Discovery policy group.
- 3 Click **Assign Policies / Policy Group...** from the drop down list and click **Submit** . A Selector window appears.

- Select **Policy Groups** from **Locate** and type **Basic Discovery** in **Name** and click **OK** to display the Basic Discovery for Windows Server 2003 and 2008.

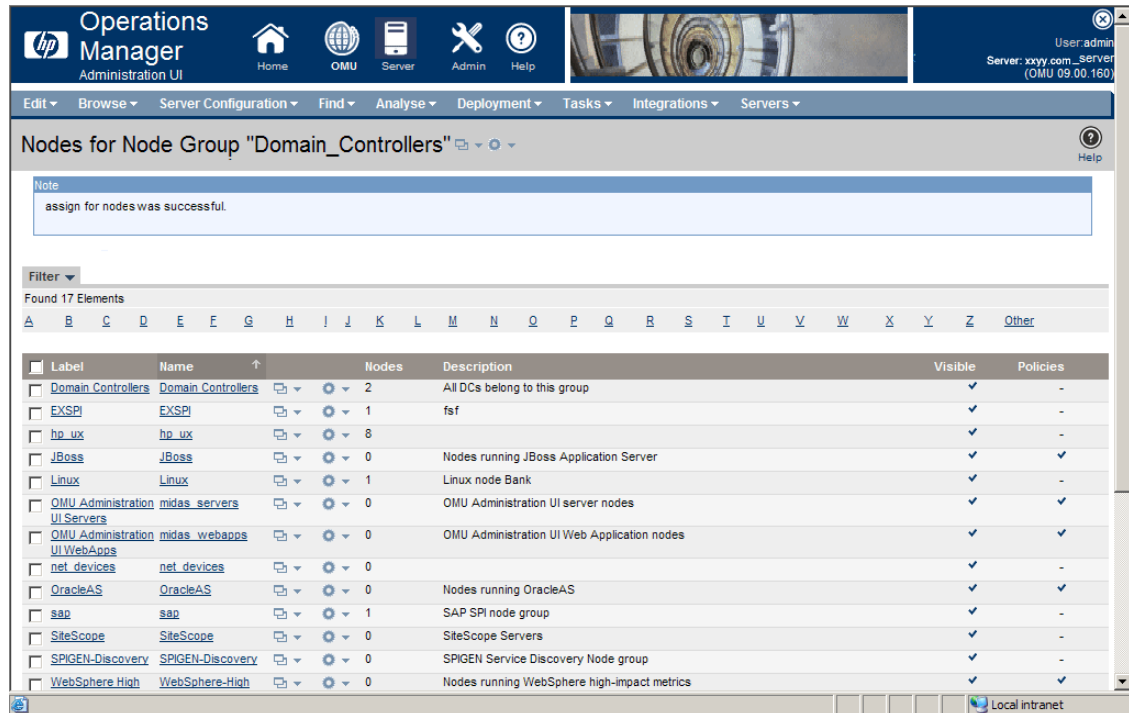


- Select **SPI for Active Directory/Windows Server 2008/Auto-Deploy/Discovery/Basic Discovery** or **SPI for Active Directory/Windows Server 2003/Auto-Deploy/Discovery/Basic Discovery**. Click **OK**.





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



## Assign Instrumentation Categories to Domain Controllers Nodes

Assign the following instrumentation categories to the DC nodes:

- SPIDataCollector
- ActiveDirectory\_Core
- ActiveDirectory\_Discovery.

To assign instrumentation to the DC nodes, perform the following:

- 1 Click **Browse** → **All Node Groups** and click the **Domain\_Controllers** node group.
- 2 Select all the **DC** nodes check box to assign the instrumentation categories.
- 3 Click **Assign Categories...** from the drop-down list and click **>>**. The Selector Window appears.
- 4 Select **SPI Data Collector**, **ActiveDirectory\_Core**, and **ActiveDirectory\_Discovery** and click **OK**.

Operations Manager Administration UI

Home OMU Server Admin Help

Edit Browse Server Configuration Find Analyse Deployment Tasks Integrations Servers

### Nodes for Node Group "Domain\_Controllers"

/ NodeBank / HoldingArea

Holding Area

Details HoldingArea Filter

Found 12 Elements

Type	Label	Name	IP / Contents
<input checked="" type="checkbox"/>	DC_1	abc.com	
<input checked="" type="checkbox"/>	DC_2	123.com	15.154.77.68
<input checked="" type="checkbox"/>	DC_3	abb.com	15.154.76.154
<input checked="" type="checkbox"/>	DC_4	pqr.com	15.154.76.213
<input checked="" type="checkbox"/>	DC_5	abc123.com	15.154.77.22
<input checked="" type="checkbox"/>	DC_6	pqr1234.com	
<input checked="" type="checkbox"/>	DC_7	12345.com	15.154.80.197
<input checked="" type="checkbox"/>	DC_8	abcd.com	16.57.67.137
<input checked="" type="checkbox"/>	DC_9	1234.com	16.57.67.138
<input checked="" type="checkbox"/>	DC_10	222.com	16.57.67.139
<input checked="" type="checkbox"/>	DC_11	55555.com	16.57.64.71
<input checked="" type="checkbox"/>	DC_12	xyyxx.com	15.154.83.116

Assign Categories...

Found 12 Elements

Selector

Filter | All Categories

Filter

Filtered Categories

- SPIDataCollector
- ActiveDirectory\_Core
- ActiveDirectory\_Discovery
- ADSPIDisc
- examples
- Exchange2k7\_Core
- Exchange2k7\_CoreExchange2k7\_Discovery
- Exchange2k7\_Discovery
- Generic JMX
- HP\_Storage\_Essentials\_SRM
- JBoss
- OASSPI Discovery
- OracleAS
- SAP\_Configuration

Choose one or more items. When finished, click 'OK'.

OK Cancel

The selected categories are assigned.

Operations Manager Administration UI

Home OMU Server Admin Help

User: admin Server: xxyy.com\_server (OMU 09.00.160)

Edit Browse Server Configuration Find Analyse Deployment Tasks Integrations Servers

### Nodes for Node Group "Domain\_Controllers"

/ NodeBank / HoldingArea

Note

assignto for node/layout group was successful.

Holding Area

Details HoldingArea Filter

Found 12 Elements

Type	Label	Name	IP / Contents	Network Type / Node Hierarchy	Machine Type / Description	Controltype	Policies
<input type="checkbox"/>	DC_1	abc.com		Other (non-IP)	other other	message_allowed	-
<input type="checkbox"/>	DC_2	123.com	15.154.77.68	IP	Intel/AMD x64(HTTPS) MS Windows	controlled	✓
<input type="checkbox"/>	DC_3	abb.com	15.154.76.154	IP	Intel/AMD x86 (HTTPS) MS Windows	controlled	✓
<input type="checkbox"/>	DC_4	pqr.com	15.154.76.213	IP	Intel/AMD x64(HTTPS) MS Windows	controlled	✓
<input type="checkbox"/>	DC_5	abc123.com	15.154.77.22	IP	Intel/AMD x86 (HTTPS) MS Windows	controlled	✓
<input type="checkbox"/>	DC_6	pqr1234.com		Other (non-IP)	other other	message_allowed	-
<input type="checkbox"/>	DC_7	12345.com	15.154.80.197	IP	HP PA-RISC (HTTPS) HP-UX	controlled	✓
<input type="checkbox"/>	DC_8	abcd.com	16.57.67.137	IP	Itanium 64/32(HTTPS) HP-UX	message_allowed	-
<input type="checkbox"/>	DC_9	1234.com	16.57.67.138	IP	Itanium 64/32(HTTPS) HP-UX	message_allowed	-
<input type="checkbox"/>	DC_10	222.com	16.57.67.139	IP	other other	message_allowed	✓
<input type="checkbox"/>	DC_11	55555.com	16.57.64.71	IP	Itanium 64/32(HTTPS) HP-UX	controlled	-
<input type="checkbox"/>	DC_12	xyyxx.com	15.154.83.116	IP	Intel/AMD x64(HTTPS) MS Windows	controlled	✓

Done Local intranet

## Deploy Configuration

Deploy configuration to the DC nodes. To deploy configuration, 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 drop-down list and click Submit **>>**.
- 4 A box appears which indicates the categories of configuration. Select **Distribute Policies** and **Distribute Instrumentation** check boxes and click **OK**.

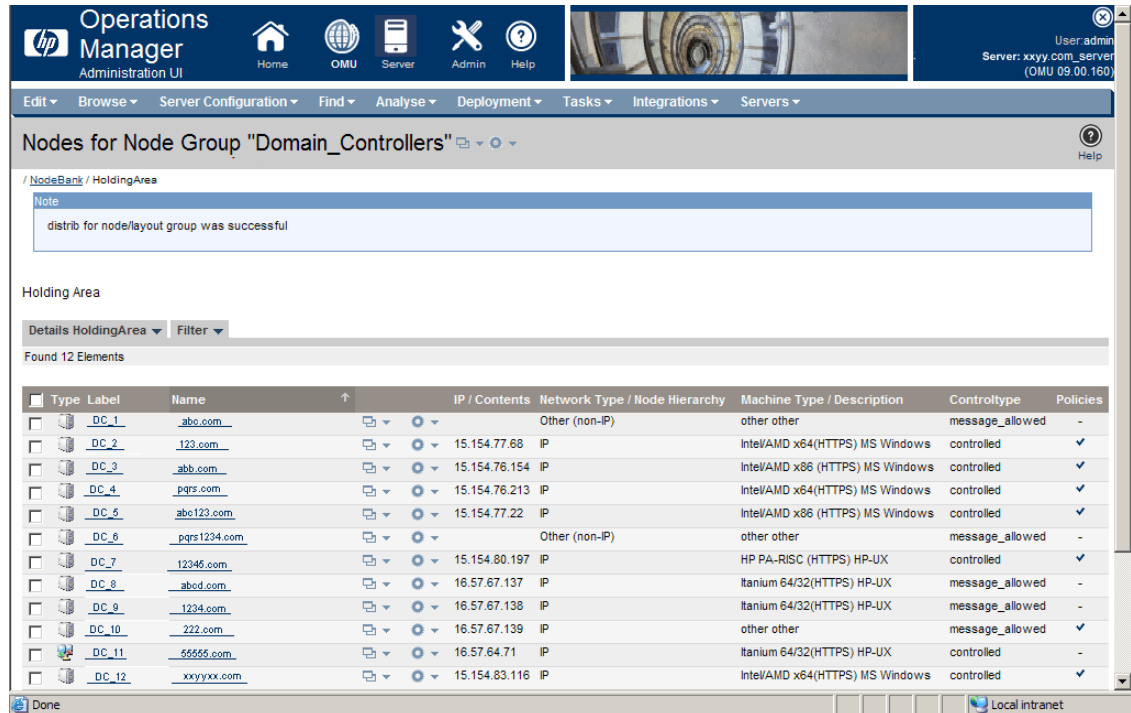
The screenshot shows the HP Operations Manager Administration UI. The main window displays the 'Nodes for Node Group "Domain\_Controllers"' page. A dialog box is open, showing a list of configuration categories to be distributed to the nodes. The categories are:

Category	Checked	Policy
Distribute Policies	<input checked="" type="checkbox"/>	*
Distribute Actions	<input type="checkbox"/>	*
Distribute Monitors	<input type="checkbox"/>	*
Distribute Commands	<input type="checkbox"/>	*
Distribute Instrumentation	<input checked="" type="checkbox"/>	*
Distribute Subagents	<input type="checkbox"/>	*
Force	<input type="checkbox"/>	
Purge	<input type="checkbox"/>	

The dialog box also has 'OK' and 'Cancel' buttons. The background window shows a table of 12 DC nodes with their respective details.

Type	Label	Name	IP	OS	Policy
DC	DC_1	abc.com	15.154.80.197	HP PA-RISC (HTTPS) HP-UX	controlled
DC	DC_2	123.com	16.57.67.137	Itanium 64/32(HTTPS) HP-UX	message_allowed
DC	DC_3	abb.com	16.57.67.138	Itanium 64/32(HTTPS) HP-UX	message_allowed
DC	DC_4	pqrs.com	16.57.67.139	other other	message_allowed
DC	DC_5	abc123.com	16.57.64.71	Itanium 64/32(HTTPS) HP-UX	controlled
DC	DC_6	pqrs1234.com	15.154.83.116	Intel/AMD x64(HTTPS) MS Windows	controlled
DC	DC_7	12345.com			
DC	DC_8	abcd.com			
DC	DC_9	1234.com			
DC	DC_10	222.com			
DC	DC_11	55555.com			
DC	DC_12	xyyxx.com			

The nodes are successfully configured.



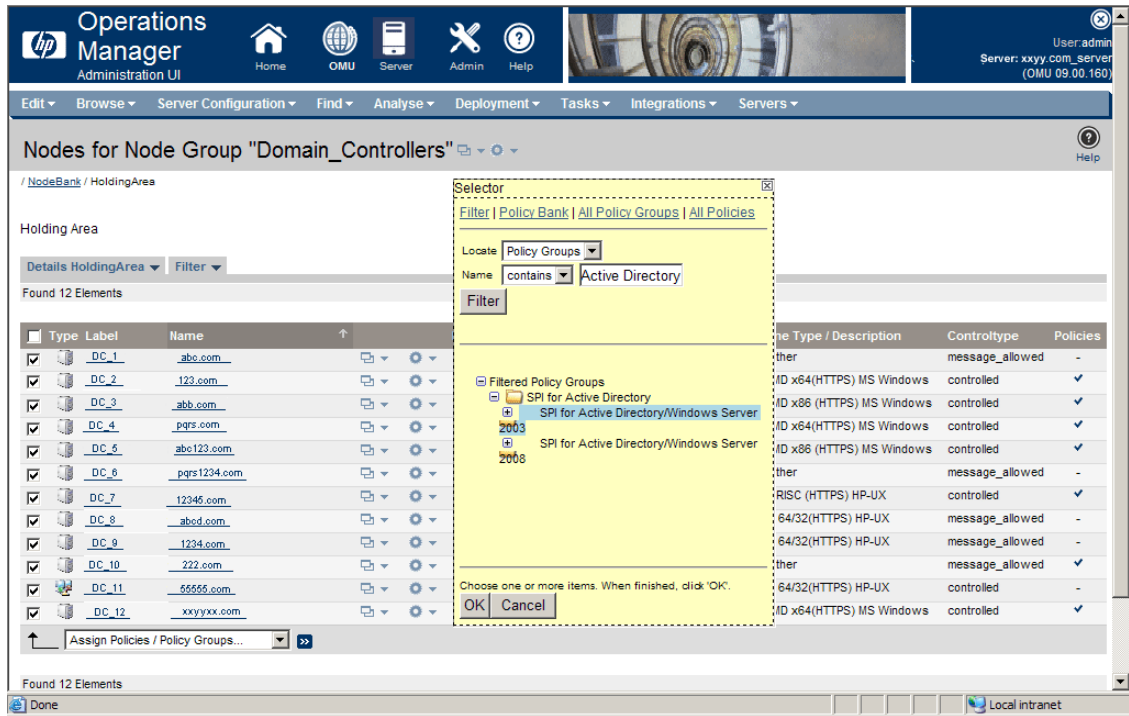
When you deploy the configuration, the basic components of the Microsoft Active Directory are discovered.

## Assign other Microsoft Active Directory SPI Policies to Domain Controllers Nodes

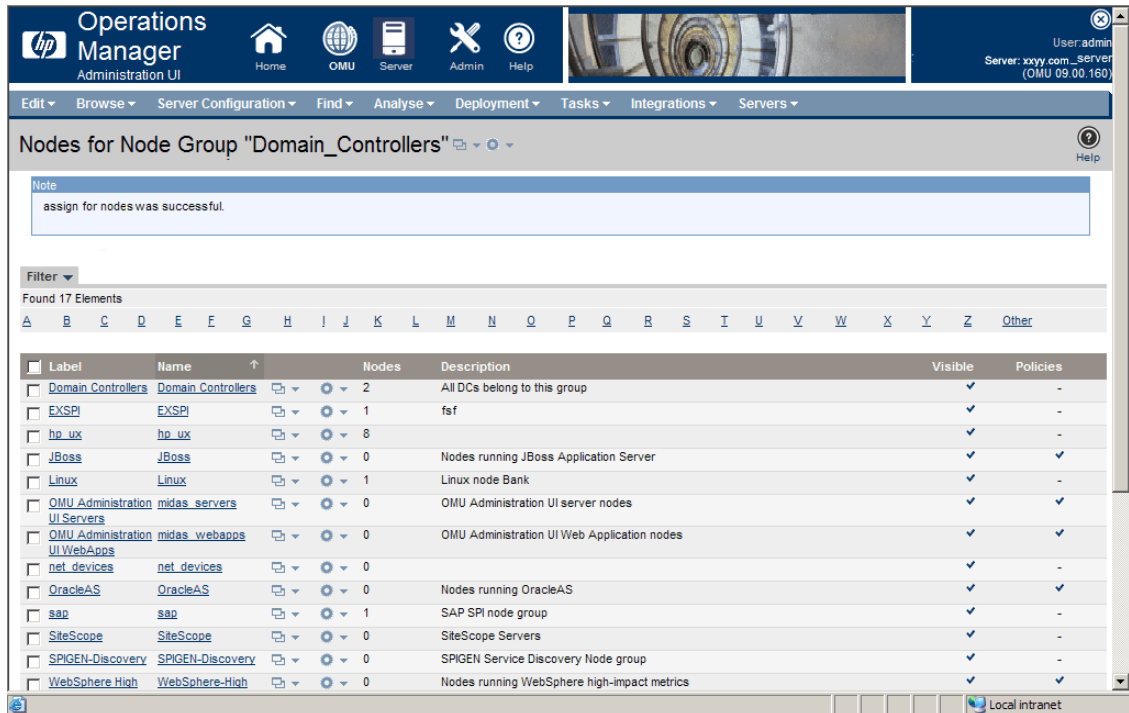
Assign other Microsoft Active Directory SPI policies to the DC nodes. Perform the following:

- 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 Click **Assign Policies / Policy Group...** from the drop down list and click **>>**. The Selector Window appears.
- 4 Click **Filter**.
- 5 Select **Policy Groups** in **Locate** and type **SPI for Active Directory** in **Name** box.

- Select **SPI for Active Directory/Windows Server 2008** or **SPI for Active Directory/Windows Server 2003**, and then click **OK**.




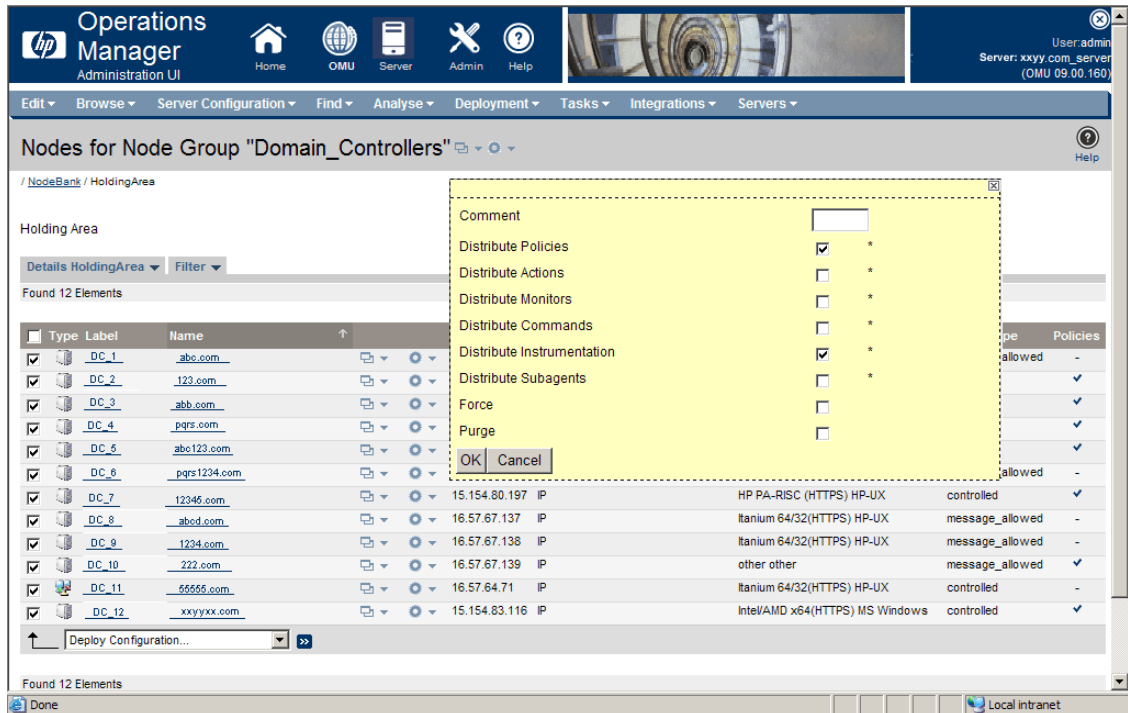
All the other Microsoft Active Directory SPI policies are assigned to the DC nodes.



## Deploy other Microsoft Active Directory SPI Policies to Domain Controller Nodes

To deploy the other Microsoft Active Directory SPI policies to the DC nodes, perform the following:

- 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 drop-down list and click **Submit** .
- 4 A box appears indicating the categories of configuration. Select the **Distribute Policies** and **Distribute Instrumentation** check boxes, and then click **OK**.



The screenshot shows the HP Operations Manager Administration UI. The main window displays a list of 12 domain controller nodes under the 'Domain\_Controllers' node group. A dialog box is open, showing the following configuration options:

Category	Checked	Required
Distribute Policies	<input checked="" type="checkbox"/>	*
Distribute Actions	<input type="checkbox"/>	*
Distribute Monitors	<input type="checkbox"/>	*
Distribute Commands	<input type="checkbox"/>	*
Distribute Instrumentation	<input checked="" type="checkbox"/>	*
Distribute Subagents	<input type="checkbox"/>	*
Force	<input type="checkbox"/>	
Purge	<input type="checkbox"/>	

The dialog box also includes a 'Comment' field, 'OK', and 'Cancel' buttons. The main window shows a table of nodes with columns for Type, Label, Name, IP, and Policies.

Type	Label	Name	IP	Policies
DC	DC_1	abc.com		
DC	DC_2	123.com		
DC	DC_3	abb.com		
DC	DC_4	pgfs.com		
DC	DC_5	abc123.com		
DC	DC_6	pgfs1234.com		
DC	DC_7	12345.com	15.154.80.197	HP PA-RISC (HTTPS) HP-UX controlled
DC	DC_8	abcd.com	16.57.67.137	Itanium 64/32(HTTPS) HP-UX message_allowed
DC	DC_9	1234.com	16.57.67.138	Itanium 64/32(HTTPS) HP-UX message_allowed
DC	DC_10	222.com	16.57.67.139	other other message_allowed
DC	DC_11	55555.com	16.57.64.71	Itanium 64/32(HTTPS) HP-UX controlled
DC	DC_12	xxxyxx.com	15.154.83.116	Intel/AMD x64(HTTPS) MS Windows controlled

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

The screenshot displays the HP Operations Manager Administration UI. At the top, there is a navigation bar with icons for Home, OMU, Server, Admin, and Help. Below this, a menu bar contains options like Edit, Browse, Server Configuration, Find, Analyse, Deployment, Tasks, Integrations, and Servers. The main content area shows the 'Nodes for Node Group "Domain\_Controllers"' page. A note indicates that the distribution for the node/layout group was successful. Below the note, there is a 'Holding Area' section with a 'Details HoldingArea' dropdown and a 'Filter' dropdown. A message states 'Found 12 Elements'. A table lists 12 Domain Controller nodes with the following columns: Type, Label, Name, IP / Contents, Network Type / Node Hierarchy, Machine Type / Description, and Controltype. The table data is as follows:


Type	Label	Name	IP / Contents	Network Type / Node Hierarchy	Machine Type / Description	Controltype
<input type="checkbox"/>	DC_1	abc.com		Other (non-IP)	other other	message_allowed
<input type="checkbox"/>	DC_2	123.com	15.154.77.68	IP	Intel/AMD x64(HTTPS) MS Windows	controlled
<input type="checkbox"/>	DC_3	abb.com	15.154.76.154	IP	Intel/AMD x86 (HTTPS) MS Windows	controlled
<input type="checkbox"/>	DC_4	pqrs.com	15.154.76.213	IP	Intel/AMD x64(HTTPS) MS Windows	controlled
<input type="checkbox"/>	DC_6	abc123.com	15.154.77.22	IP	Intel/AMD x86 (HTTPS) MS Windows	controlled
<input type="checkbox"/>	DC_6	pqrs1234.com		Other (non-IP)	other other	message_allowed
<input type="checkbox"/>	DC_7	12345.com	15.154.80.197	IP	HP PA-RISC (HTTPS) HP-UX	controlled
<input type="checkbox"/>	DC_8	abcd.com	16.57.67.137	IP	Itanium 64/32(HTTPS) HP-UX	message_allowed
<input type="checkbox"/>	DC_9	1234.com	16.57.67.138	IP	Itanium 64/32(HTTPS) HP-UX	message_allowed
<input type="checkbox"/>	DC_10	222.com	16.57.67.139	IP	other other	message_allowed
<input type="checkbox"/>	DC_11	55555.com	16.57.64.71	IP	Itanium 64/32(HTTPS) HP-UX	controlled
<input type="checkbox"/>	DC_12	xyyxxx.com	15.154.83.116	IP	Intel/AMD x64(HTTPS) MS Windows	controlled

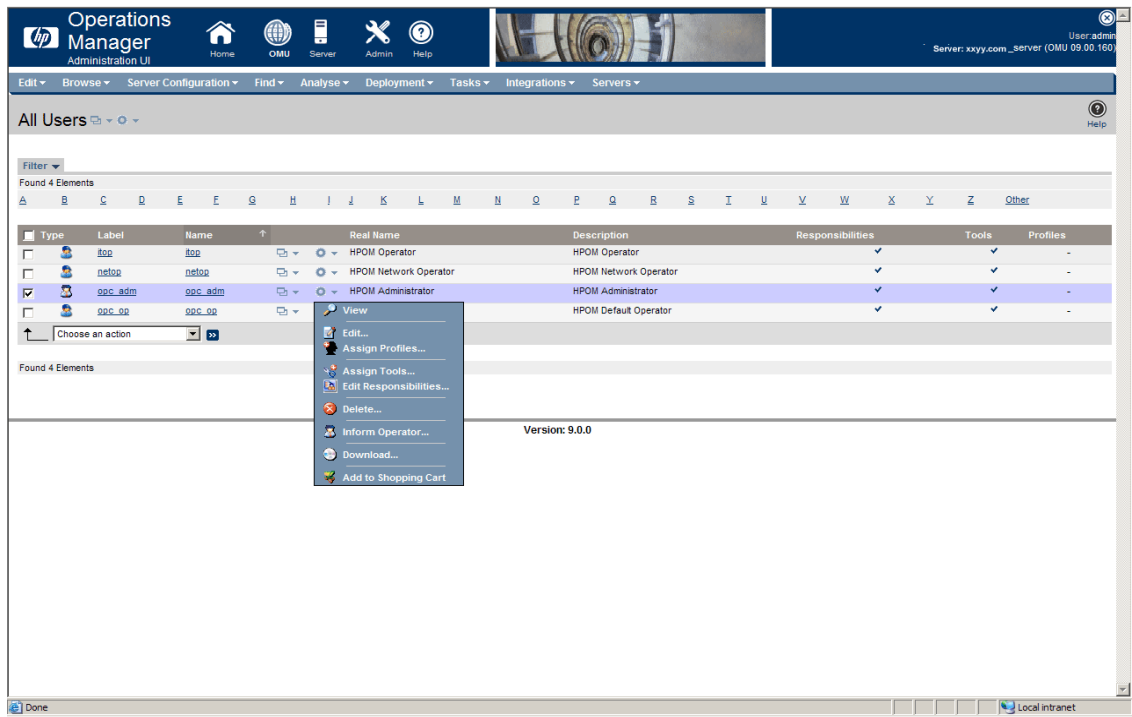
## Assign Domain\_Controllers Node Group and ADSPI Message Group to the Operator

Assign the Domain\_Controllers node group and ADSPI message group to the HP Operations Manager on UNIX operator. This enables the operator to view messages or alerts, or both which are generated from the DC nodes.

To assign the node group and the message group, perform the following:

- 1 Click **Browse** → **All Users**. All the users as operators are listed.


- 2 Select one or more operators for ADSPI, (for example, **opc\_adm**) check box, and then click **Edit Responsibilities...** from the Edit option  .

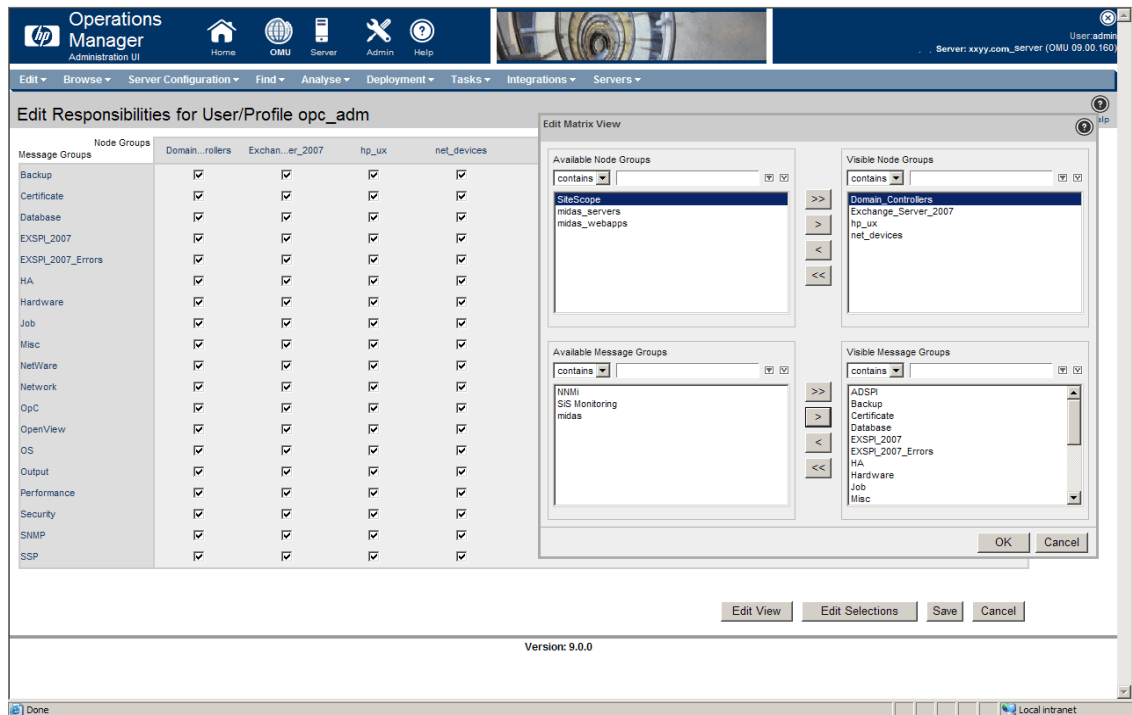


All the available nodes groups and message groups are displayed in the Edit Matrix View window.

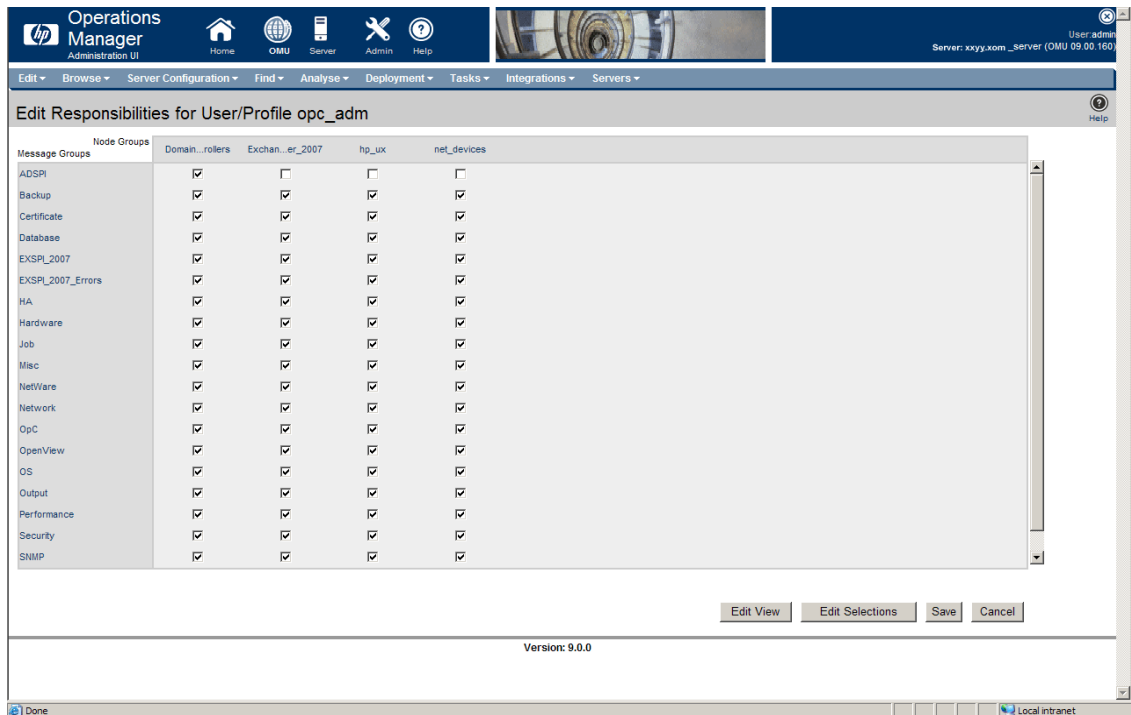
- 3 Click **Edit View**.



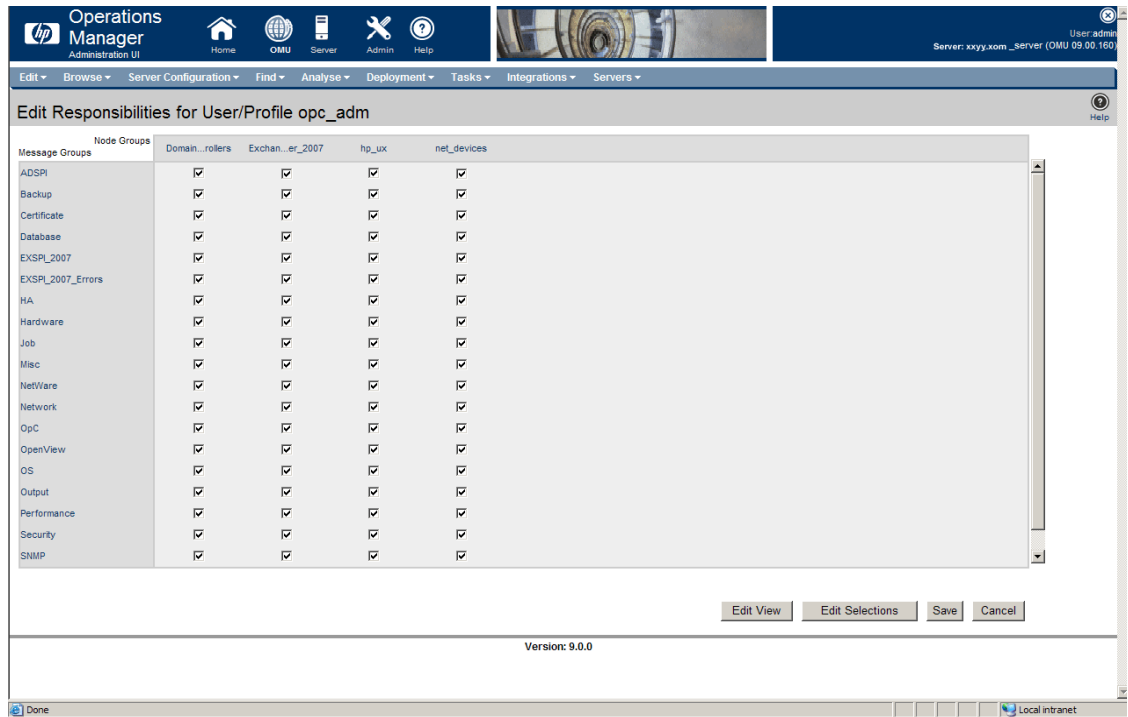
- 4 Select **Domain\_Controllers** node group and the **ADSPI** message group by shifting them from the available node groups and available message groups to visible node groups and visible message groups by clicking  .



The **Domain\_Controllers** node group and the **ADSPI** message group are added to the list.

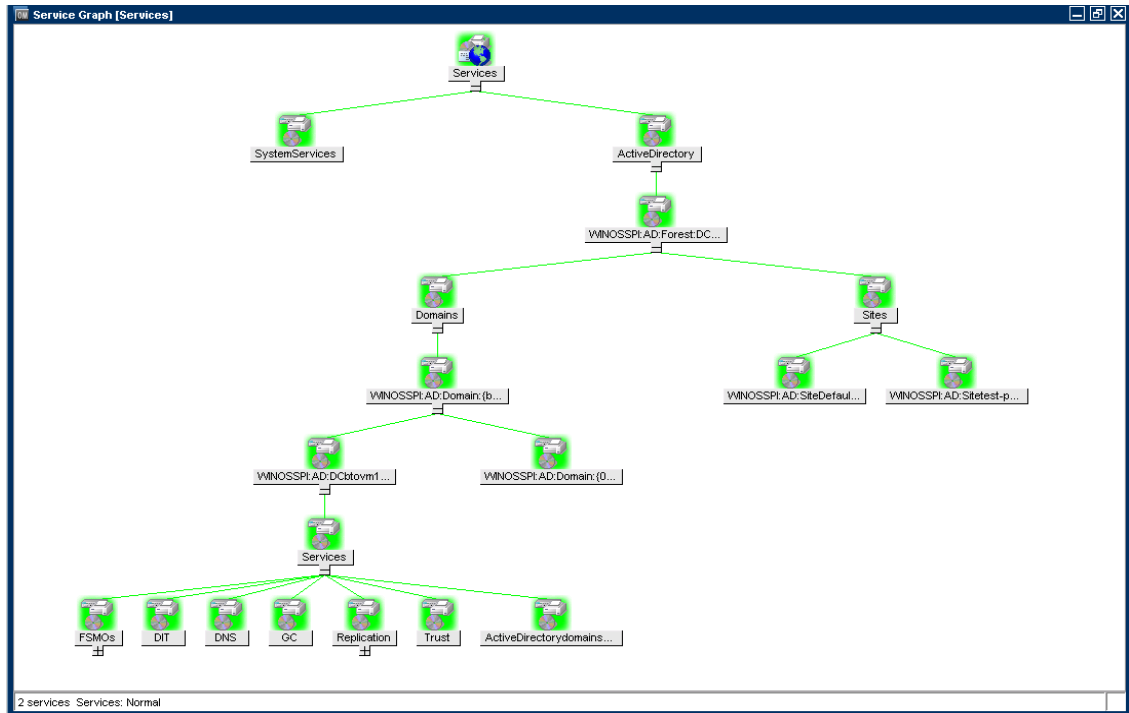


- Select the **Domain\_Controllers** node group and the **ADSPI** message group check boxes to which now enables the `opc_adm` operator to use the message browser and to view the alert. Click **Save**.




## Assign Microsoft Active Directory SPI Services to the Operator

Assign the WINOSSPI:AD services to the operator `opc_adm` (or any desired operator) by running the command `opcservice -assign opc_adm WINOSSPI:AD` after ADSPI discovery is run. The service navigator now shows the Microsoft Active Directory service map.

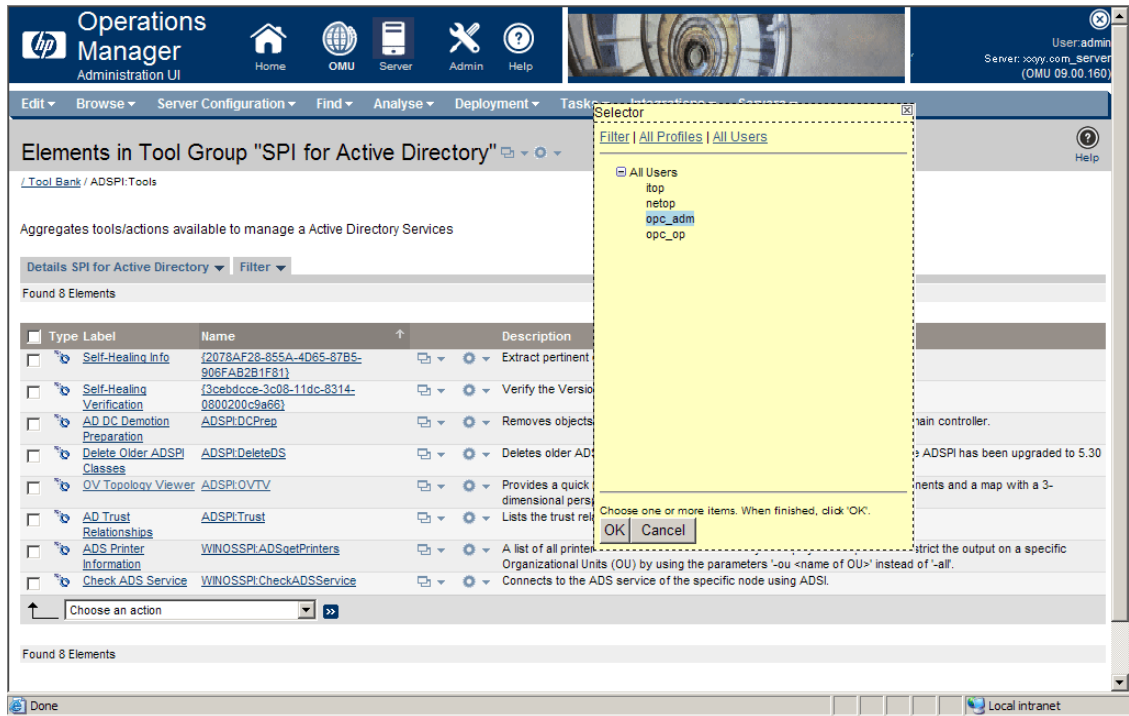


## Assign Tool Group to Operator

To assign the Microsoft Active Directory SPI tool group to the operator `opc_adm` (or any desired operator), perform the following,

- 1 Click **Tool Bank** → **SPI for Active Directory**. The Tool Group “SPI for Active Directory” is displayed.
- 2 Select **Assign to User/Profile...** from the Actions option  . A Selector window appears.

- 3 Select the operator **opc\_admin** (or any desired operator) from the **All Users** and click **OK**.  
Assigning Tool Group to the operator



- 4 The SPI for Active Directory Tool Group is assigned to the operator **opc\_admin**.

## Create ADSPi 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** → **ADSPi-CreateDataSources** creates the required data sources in the data store of the HP Operations agent or HP Performance Agent.



You must deploy the instrumentation category SPI for Data Collector before running this policy on the managed nodes.

## Data Logging Scenarios

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

To create data sources and to log data into CODA, while Performance Agent is installed, perform the following steps:

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

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

For more details on data logging metrics and description of each policy see *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide*.




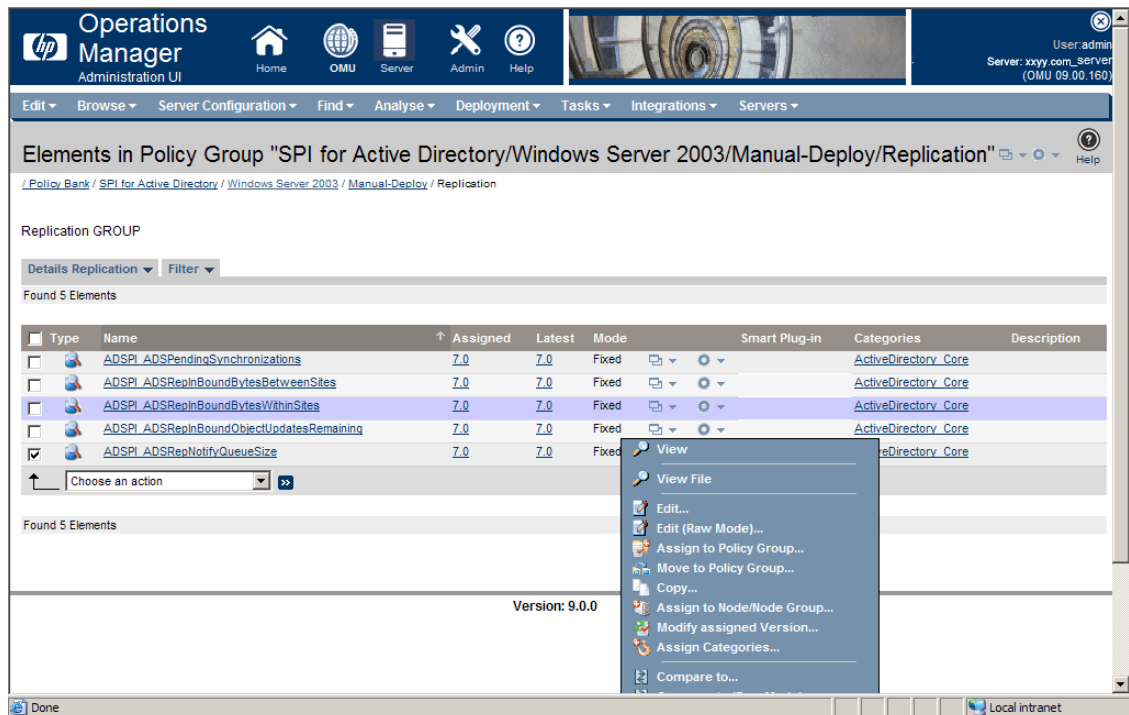
## 4 Customizing Policies

Policies monitor the Microsoft Active Directory environment and run according to rules and schedule specifications. Measurement threshold policies contain the rules for interpreting Microsoft Active Directory states or conditions. See *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide* for a detailed description of all policies.

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

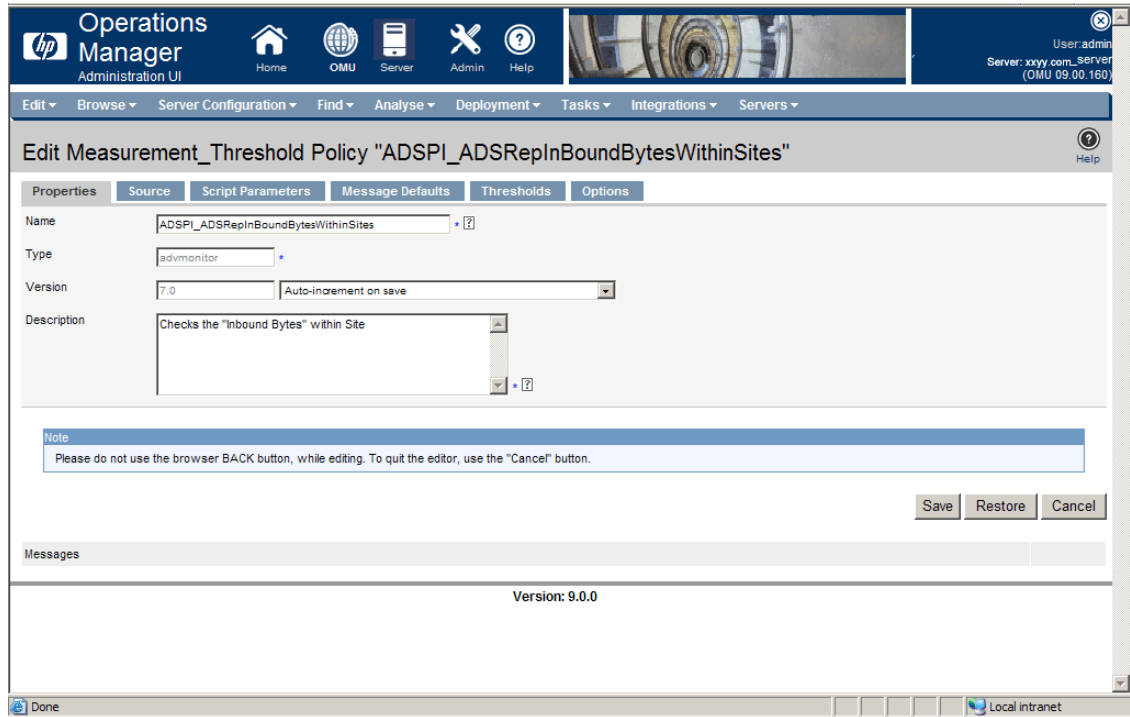
You can customize one or more policies to suit the Microsoft Active Directory environment. If you choose to customize one or more policies after deploying them, ensure to redeploy the policies after customizing them. To customize a policy, perform the following:

- 1 Click **Policy Bank** → **SPI for Active Directory** → **Windows Server 2003** (or **2008**) → **Auto-Deploy** (or **Manual-Deploy**) where the policy resides. For example, ADSPI\_ADSRepNotifyQueueSize in Replication Policy Group.
- 2 Select the **ADSPI\_ADSRepNotifyQueueSize** check box and click **Edit...** from the drop down box  .



- 3 The Edit Measurement\_Threshold Policy "ADSPI\_ADSRepNotifyQueueSize" window appears to enable you to edit the policy in terms of customizing its properties, settings parameters, or message threshold or all.

- 4 Customize the required settings and click **Save**.



## Policy Group and Policy Type

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 and area to be targeted for discovery or monitoring. Deployment can be auto and manual. To view auto and manually deployed policies in the Microsoft Active, click **Policy Bank** → **SPI for Active Directory** → **Windows Server 2003** (or **2008**) → **Auto-Deploy** (or **Manual-Deploy**).

The policies in each deployment are displayed. The Auto-Deploy group enables you to deploy all subgroups at the same time. You can further choose a specific task from the subgroup. For example, **Discovery** → **Advanced Discovery** or **Basic Discovery**. You can otherwise choose 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 collections to change the monitoring intervals or thresholds or both for a single DC. To create a separate group of policies, copy the desired policies into a folder with the new group name. After pasting the policies into the new group, you can then modify them and change the version numbers. The user-created versions make it possible to deploy specifically tailored policies to node groups to meet their monitoring needs. Using this method makes it possible to bring nodes and policies together in groups that are easily recognizable.

## Using Auto-Deploy Policies

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

### Discovery

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

### DIT Monitoring

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

### DNS Monitoring

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

### FSMO Monitoring

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

## Replication Monitoring

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

## Response Time Monitoring

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

## GC Monitoring

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

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

## Sysvol Monitoring

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

## Trust Monitoring

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

# Using Manual-Deploy Policies

The Manual-Deploy policies of Microsoft Active Directory SPI are not automatically deployed, after the Microsoft Active Directory service occurs. The manual-deploy policies offer basic monitoring that cover areas of the Microsoft Active Directory involving connectivity, domain, and organization unit structure, health, index and query, replication or replication activities or both, security, and site structure. The following sections describe the various sub-groups of the manual-deploy 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 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. The 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 would fall in range which would either be above or below a particular Standard deviation, that is, 68% / 95% / 99%. As the severity indicates, whenever the current values falls below the 1st Standard deviation, a warning message is generated, along with an attribute which says whether the current value is "above/higher" or "below/lower" the Standard deviation.

## Connector policies (only for Windows Server 2003)

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

## Domain and OU Structure

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

## Global Catalog Access

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

## Health Monitors

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

## Index and Query

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

## Replication

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

## Replication Activity

Monitors the Directory Service log for replication events.

## Security

These policies monitor:

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

## Site Structure

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

- *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.

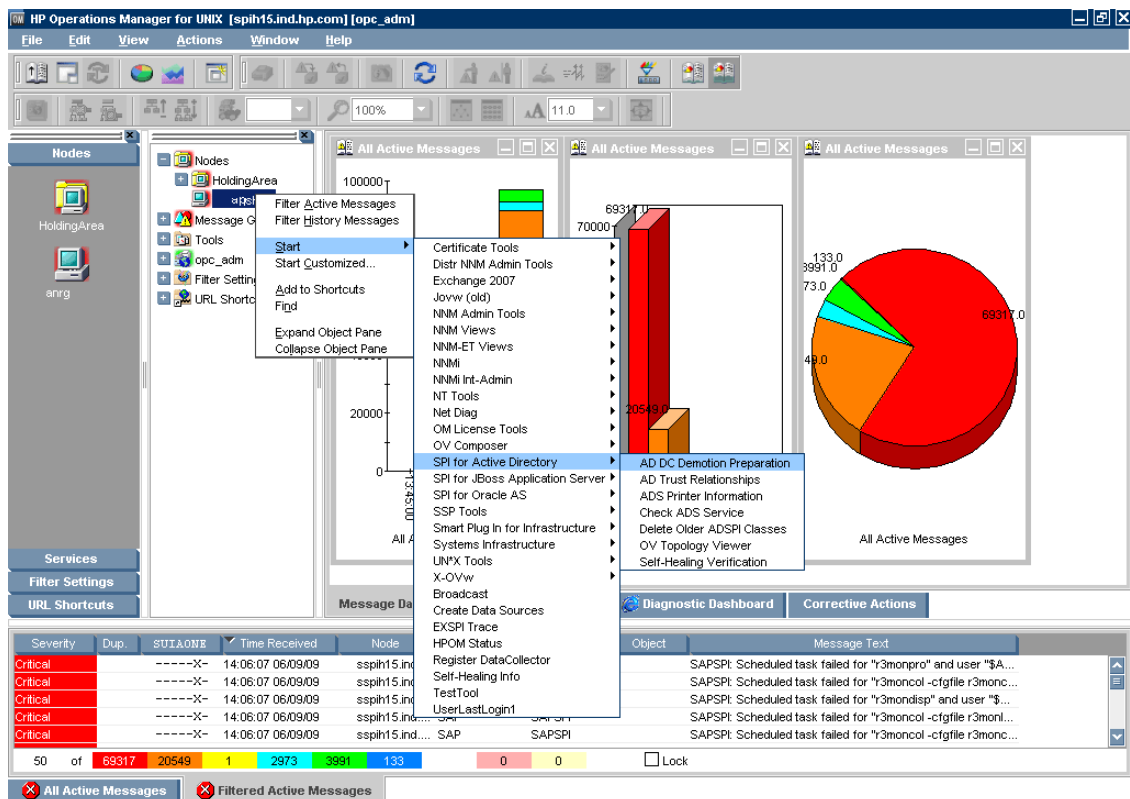
# 5 Using Tools

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

The operator can start the tool of the Microsoft Active Directory SPI from the operator GUI assigned by the administrator. To start a tool:

- 1 Right-click the node where the tool needs to be started.
- 2 Select **Start** → **SPI for Active Directory** → **AD DC Demotion Preparation** (example).
- 3 A message “Tool started. Please wait.” indicates the start of the selected tool.



## Using AD Trust Relationships Tool

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

```
Tool Output:

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

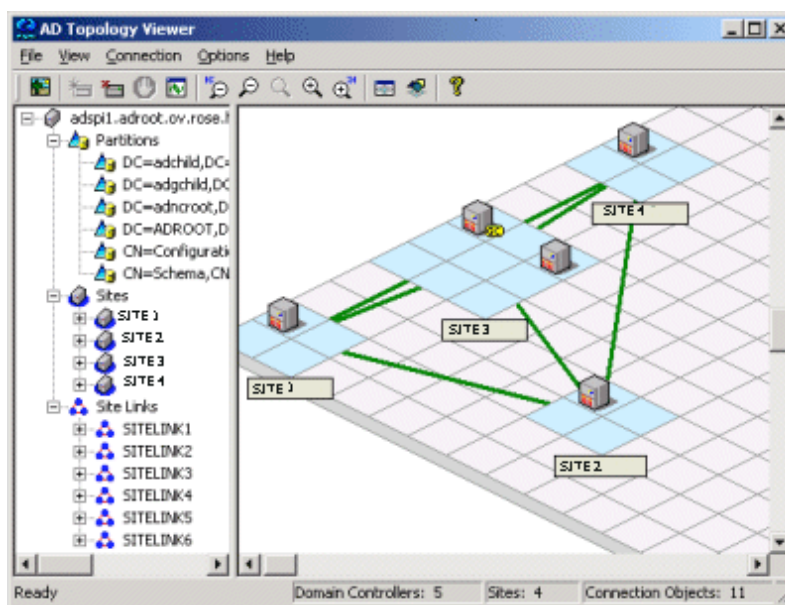
Trust Relationships -----
FlatName: .....ADNCROOT
SID: .....S-1-5-21-1667343185-2871001565-
TrustAttributes: .....0
TrustDirection: .....Bi-directional
TrustedDCName: .....\\adspi2.adncroot.system.usa.com
TrustedDomain: .....adncroot.system.usa.com
TrustIsOk: .....True
TrustStatus: .....0
TrustStatusString: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

## Using HP Operations Topology Viewer Tool

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

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

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



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



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

## Starting HP Operations Topology Viewer Tool

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 located in:  
`<INSTALLDIR>/install/ADSPI/ovtv.zip`
- 2 Extract the OVTV.zip.
- 3 Double-click on OVTV-Console.msi.
- 4 Browse to:  
`C:\Program Files\HP\HP BTO  
Software\install\ADSPI-Console\InstallScripts` and double-click `postinstall-console.vbs`. This registers the required DLLs.
- 5 Browse to `C:\Program Files\HP OpenView\bin\OVTV` and double-click `ovtv.exe` to start using OVTV.

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

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

▶ Your authentication becomes simple if the HP Operations Topology Viewer tool is running on the same DC of 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. Hence, no other alternate credentials are required.

## Getting Started with the HP Operations Topology Viewer Tool

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

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

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

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

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



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

## Accessing Functions of HP Operations Topology Viewer Tool

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

### Adjusting Map View

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

**Table 2 Adjusting Map View.**

<b>Tree/map modification</b>	<b>How to do it</b>
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 <b>Labels</b> → <b>Servers</b> or <b>Sites</b>
To increase/decrease the size of the row/columns in the map's grid.	Right-click the unused space on or off the map and select <b>Map Properties</b> .

<b>Tree/map modification</b>	<b>How to do it</b>
To find a site or server in the tree.	On the map, right-click the site or server on the map and select <b>Find Site/Find Server</b> 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><b>Method #1:</b></p> <ol style="list-style-type: none"> <li>1 Pressing the left mouse button, click the site and start to drag and drop to the desired area.</li> <li>2 Still holding the left mouse button down, press the right button and continue moving in the desired direction.</li> </ol> <p><b>Method #2</b></p> <ol style="list-style-type: none"> <li>1 Pressing the left mouse button, select the site and start to drag and drop to the desired area.</li> <li>2 Still holding the left mouse button down and use the arrow keys to change the view of the map.</li> </ol>

Use the keyboard as mentioned in the following table to move around the map.

**Table 3 Keyboard Functionality**

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

## HP Operations Topology Viewer Menubar

The HP Operations Topology Viewer menu commands are shown in the following table.

**Table 4 HP Operations Topology Viewer Menu**

<b>Menu</b>	<b>Command</b>	<b>Function</b>
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.












<b>Menu</b>	<b>Command</b>	<b>Function</b>
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.




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

## HP Operations Topology Viewer Toolbar

The HP Operations Topology Viewer toolbar functions are as shown in Table 4.

**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.
	Exports the current view and saves it to a graphic format of your choice, such as .png or .bmp. (The default format is .png.
	Allows you to add a forest by opening the Add Forest dialog, where you enter server connection information.
	Refreshes the data by checking information on the current connection.
	Zooms out the map view to the maximum degree.
	Zooms out the map view incrementally.
	Resets the map view to the default.
	Zooms in the map view incrementally.
	Zooms in the map view to the maximum degree.

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

## Accessing Server and Map Properties

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

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



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

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



---

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

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

For more details on each report and graph, see *HP Operations Smart Plug-in for Microsoft Active Directory Reference Guide*.

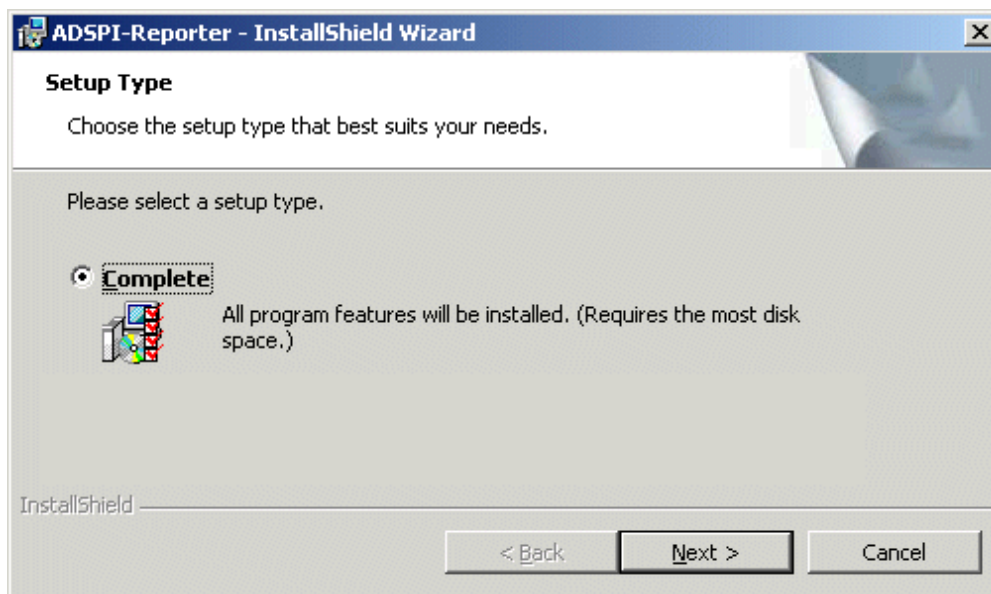
### Using Reports and Graphs

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

These web-based reports are automatically generated every night and provide you with a routine means of checking 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 covering 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 ADSPI Reporter package on HP Reporter Server to use the Microsoft Active Directory SPI reports. For this, run the `ADSPI-Reporter.msi` setup. This setup installs the Microsoft Active Directory SPI Report Package within the Reporter server. After this configure the 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-ins DVD.
- 2 Browse to the folder `SPIDVD>/WINDOWS/OV_REPORTER/AD_SPI` and double-click the file `ADSPI-Reporter.msi`.
- 3 Follow the instructions as they appear for the installation on Management Server for Windows till a dialog box opens indicating the completion of the installation.
- 4 Select **Complete** for the **Setup Type**, and click **Next**. The preceding dialog box updates you about the installation progress.

## Configuring Report Package

To configure the Microsoft Active Directory SPI Report Package:

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

Instructions are available in the HP Reporter Help for assigning Microsoft Active Directory SPI reports to the targeted nodes. To access Help, select **Reports** or **Discovered Systems** in the left panel of the HP Reporter main window and right-click it. Select **Report Help** or **Discovered Systems Help** from the sub-menu that appears. See the topic “To assign a report definition to a Discovered Systems Group.” Reporter also includes two online documents: the *Concepts Guide* and the *Installation / Special Configurations Guide* for further information.

## Generating Reports

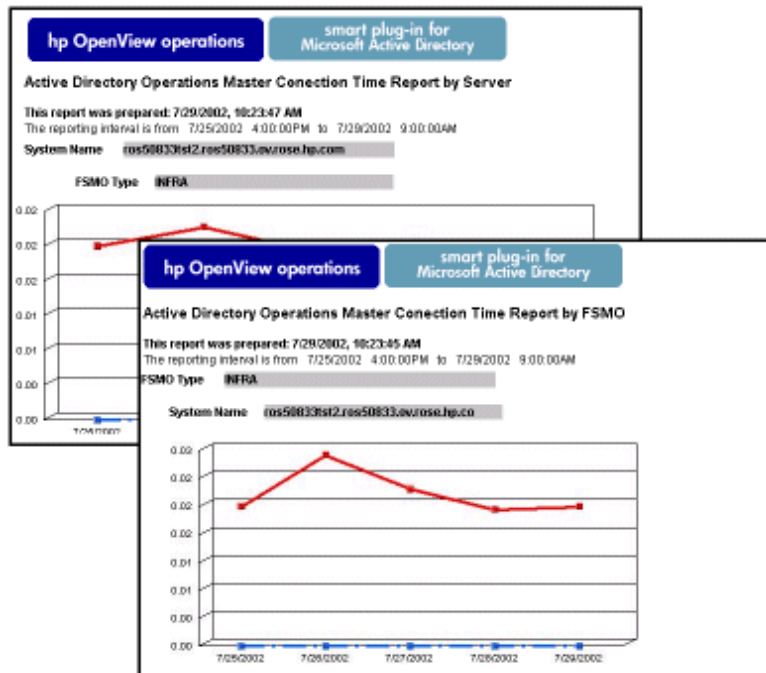
After you install the Microsoft Active Directory SPI, the HPOM generates reports using the SPI-collected data for Microsoft Active Directory. HPOM runs the reports regularly on a nightly schedule. You can see the updated reports every day because the HPOM, by default, re-generates reports every night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

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

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

```
<report_table_name>.<Microsoft Active Directory SPI_metric_name>  
is identified as ADSPI_RESPONSEMON.SYSTEMNAME
```

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



## Integrating Microsoft Active Directory SPI with HP Performance Manager

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

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

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

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

- a Insert the Smart Plug-ins DVD-ROM (that contains 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.

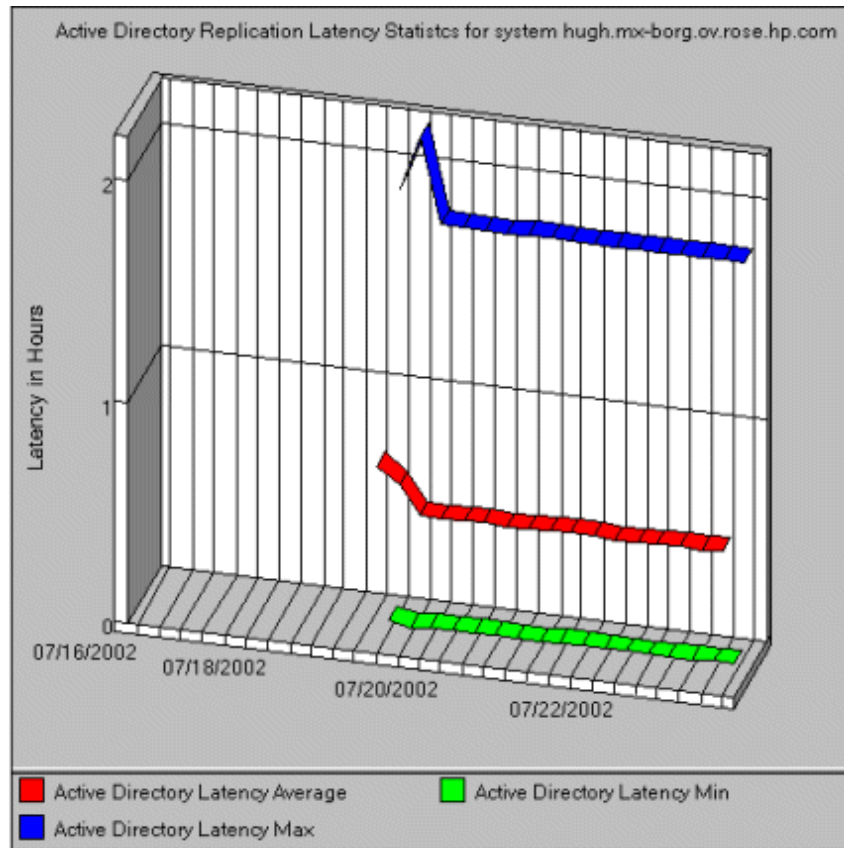
For information see the HP Performance Manager documentation.

## 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:

- 1 Insert the HP Operations Smart Plug-ins DVD.
- 2 Double-click the file `HPOvSpiAdGc.msi`. (Follow the steps of installation on Management Server for Windows.). A dialog box opens.
- 3 Select **Complete** for the **Setup Type**, and click **Next**. The preceding dialog box updates you about the installation progress.





# 7 Troubleshooting

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

## Troubleshooting Discovery

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

### Insufficient Privileges

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

- *Possible cause:* The account with which the Basic Discovery policy (**Policy 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 an administrator credentials are provided in the Basic Discovery policy and then redeploy the policy.

### Failed Binary on the Managed Node

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

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

## Troubleshooting through Tracing

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

All the Microsoft Active Directory SPI binaries 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 should change this command as:

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



You can find the trace file ADSPI\_DnsMon.log in the  
%ovagentdir%\bin\instrumentation folder.

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

## Troubleshooting Reports and Graphs

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

### Reports and Graphs are not generated

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

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



## Data Logging Policies cannot log Data

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

- *Possible cause:* The data source is not created in the datastores—CODA or OVPA or both.
- *Suggested action:* Check if the datasource ADSPI is created. To do this:
  - a Login to the managed node as an administrator.
  - b From the command prompt run the `ovcodutil -obj > out.txt` command.
  - c Check the `out.txt` file to ensure that the datasource ADSPI is created.

## Browser crashes while viewing 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 due to invalid Reporter ODBC driver.

- *Possible cause:* The versions of Oracle client to access Oracle database do not match.
- *Suggested action:* Use Oracle client 9.2.0 to access Oracle 9.2.0 database and 10gR2 client to access 10gR2 database.

## Modifying Policy Names

If you change the default name of the following Microsoft Active Directory SPI policy, ensure to 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

To remove the Microsoft Active Directory SPI you must first remove all the existing policies and instrumentation categories from all the managed nodes. Then you can remove the Microsoft Active Directory SPI from the management server.



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

### Removing Microsoft Active Directory SPI from HPOM

To remove the Microsoft Active Directory SPI on the HPOM management server from the command line interface, execute the following commands:

- 1 For an HP-UX 11.x management server:

```
swremove ADSPI
```

- 2 For a Solaris management server:

```
pkgremove ADSPI
```


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

### Removing Other Components of Microsoft Active Directory SPI

Remove other component, that is, message group, user profile, report and graph package.

#### Removing Microsoft Active Directory SPI Message Group


To remove the ADSPI message group:

- 1 Click **Browse** → **All Message Groups**. All the existing message groups are displayed.
- 2 Select the **ADSPI** message group check box.
- 3 From the drop down list, select **Delete** and click  to delete the ADSPI message group.

#### Removing All User Profiles

To remove the user profile:

- 1 Click **Browse** → **All Message Groups**. All the existing message groups are displayed.

- 2 Select the appropriate user profile check box.
- 3 From the drop down list, select **Delete** and click  to delete the user profile.

## Removing Report Package

The Reporter Package can be removed either through Control Panel or through msi file.

To remove the Report Package through Control Panel:

- 1 Click **Start** → **Control Panel**.
- 2 Click **Add or Remove Programs**.
- 3 Select **ADSPI Reporter Package**.
- 4 Click **Remove** and then **Yes** to confirm the removal.

## Removing Graph Package

The Graph Package can be removed either through Control Panel or through .msi file.

To remove the Graph Package:

- 1 Click **Start** → **Control Panel**.
- 2 Click **Add or Remove Programs**.
- 3 Select **ADSPI Graphs Package**.
- 4 Click **Remove** and then **Yes** to confirm the removal.

# Removing Reporting and Graphing Package using .msi File

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

## Removing Reporting Package using .msi file

To remove the reporting package using .msi file, perform the following steps:

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

## Removing Graphing Package using .msi File

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

1 Browse to:

<SPI DVD>\SPIs\AD SPI OVPM ConfigurationPackage\HPOvSpiAdGc.msi

2 Right-click HPOvSpiAdGc.msi, and then click **Uninstall**.

3 Confirm the removal of the graphing package by clicking **Yes**.



# Index

## Numerics

3-dimensional map, 47

## C

Components

- Graphs, 10
- Polices, 10
- Reports, 10
- Tools, 10

## D

Data sources, 36

Discovered services, 11

Discovery

- Advanced Discovery, 36
- Basic Discovery, 23

Domain\_Controllers node group and ADSPI message group, 31

Domain controllers, 9

## F

Functions

- Customize policies, 14
- Discover existing components, 11
- Display information, 11
- Generate graphs, 14
- Generate reports, 14

## G

Global Catalog, 9

Graphs

- HP Performance Manager, 60

## I

Installation Packages

- Graphing Package, 17
- Reporting Package, 17
- SPI Package, 17

Instrumentation categories, 25

InterSite Topology Generators, 48

## L

LDAP, 9

Legends, 15

## M

Managed node, 18

Microsoft Active Directory SPI, 9

- Configuration, 21
- Installation, 19
- Removing, 67

## P

Policies

- Auto-Deploy, 41
- Custom Data Collection Groups, 41
- Manual-Deploy, 42
- Policy Group, 40
- Policy Type, 40

Policy Bank, 20

Pre-requisites

- Hardware, 18
- Software, 18

## R

Reports

- HP Reporter, 58

## S

Service map alerts, 10

Smart Plug-in, 9

Smart Plug-in (SPI), 9

## T

Thresholds, 10

Tools

- AD Trust Relationships Tool, 46
- HP Operations Topology Viewer Tool, 47

Troubleshooting, 63





## 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:**

