HP Operations Smart Plug-in for Microsoft® Active Directory

for HP Operations Manager for Windows®

Software Version: 7.06

Installation and Configuration Guide

Document Release Date: January 2011
Software Release Date: January 2011

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

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

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

Oracle is a registered trademark of Oracle and/or its affiliates.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Smart Plug-in for Microsoft Active Directory

The HP Operations Smart Plug-in for Microsoft Active Directory (Microsoft Active Directory SPI) helps you manage the Microsoft Active Directory in your environment. The Microsoft Active Directory SPI provides information related to the Microsoft Active Directory and the following:

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

Components of Microsoft Active Directory SPI

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

Policies

Policies are pre-defined thresholds that monitor the Microsoft Active Directory environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts are available in the service map and messages are available in the message browser. The severity level of each message is represented by a color. The messages indicate the problem and help you to take action to resolve it. Policies can be deployed automatically while installing the Microsoft Active Directory SPI, or manually. For more information, see Chapter 4, Using Policies.

Tools

Tools are utilities to configure the Microsoft Active Directory SPI and gather related information. For more information about the Microsoft Active Directory SPI tools, see Chapter 5, Tools.

Reports

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

Graphs

Graphs are the pictorial representations of the various metrics of the Microsoft Active Directory. These representations can be in different forms like line graphs, pie charts, and bar graphs. Graphs contain data collected by the Microsoft Active Directory SPI. For more information, see Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions.

Reports and graphs are generated using HP Reporter and HP Performance Manager. To view the reports and graphs, you must install the HP Reporter and HP Performance Manager in your environment.

For more information about policies, tools, reports, and graphs, see *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* or *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* PDF.

Functions of Microsoft Active Directory SPI

The following section details the functions of Microsoft Active Directory SPI. These functions help in improving the performance of the Microsoft Active Directory SPI.

Collecting and Interpreting Server Performance and Availability Information

The Microsoft Active Directory SPI monitors the Microsoft Active Directory environment by discovering existing components such as DCs, forests, Preferred Bridgehead Servers (PBHS), SysVol, and replication sites. The Microsoft Active Directory SPI also maintains the thresholds set up by the policies, displays services of the Microsoft Active Directory, and adds multiple hierarchical levels of details.

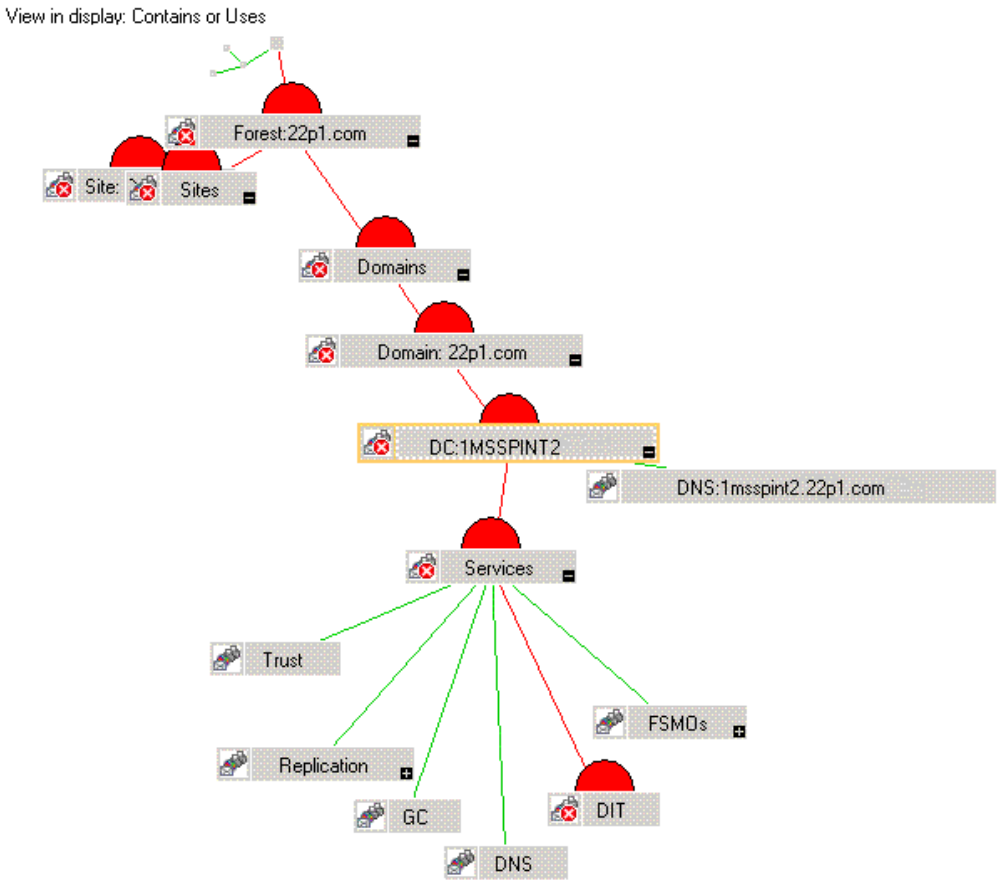
Displaying Information

The Microsoft Active Directory SPI displays information in the form of maps, texts, messages, reports, and graphs.

Service Map

The Service map shows the newly added and discovered Microsoft Active Directory services, displayed in both the console services tree and service map (on the right pane).

Figure 1 Service Map in Microsoft Active Directory SPI



Within the service map pane, you can expand the hierarchy to view the specific services present on each DC. Expanding the DC further shows the components of the DC.

Message Browser

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

Instruction Text

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

Reports and Graphs

Reports and graphs show 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 shows the Microsoft Active Directory topology, after it connects to a Microsoft Active Directory DC. For more information about HP Operations Topology Viewer tool, see Getting Started with HP Operations Topology Viewer Tool on page 34.

To access HP Operations Topology Viewer on the remote console, you must install the HP Operations Topology Viewer tool. For more information, see Installing HP Operations Topology Viewer on Remote Console on page 17.

Generating Reports Using HP Reporter

Reports help in analyzing the Microsoft Active Directory conditions. These reports are web-based and are automatically generated nightly. The reports provide you a routine means of checking the GC and Domain Naming System (DNS) availability, disk space, and queue length issues occurring with DIT, replication latency, and connection times specific to DCs running master operations services. Reports covering the trust relationship changes between DCs are also available for Windows 2003 and Windows 2008 nodes. For more information about HP Reporter, see Chapter 6, Integrating Microsoft Active Directory SPI with HP Reporting and Graphing Solutions.

Generating Graphs Using HP Performance Manager

After generating the graphs, you can view the data in a specified and granular manner. Graphs are accessed using 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

The Microsoft Active Directory SPI policies are grouped according to the policy types. For more information, see Microsoft Active Directory SPI Policies on page 25. You can customize the monitoring schedule or measurement thresholds for any Microsoft Active Directory SPI policies. Following are some of the parameters you can modify to customize the policy:

- Script-parameters
- Rules
- Options

Use HP Operations Smart Plug-in Upgrade Tool Kit 2.03 to retain the customization of the earlier versions of the Microsoft Active Directory SPI policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

2 Installing Microsoft Active Directory SPI

The Microsoft Active Directory SPI is packaged with the HP Operations Smart Plug-ins DVD. You must install the Microsoft Active Directory SPI on the HPOM management server. This chapter describes the procedures to install the Microsoft Active Directory SPI on the Management Server, remote console, and cluster environment.

Installation Packages

The Microsoft Active Directory SPI includes the following installation packages:

- SPI Package
- Graph Package
- Reporter Package
- Console Package

The Graph and Reporter packages are installed only if you want to generate graphs and reports. These packages are available at different locations on the HP Operations Smart Plug-ins DVD.

SPI Package

The SPI package is the `.msi` package that contains all the functionalities of the SPI. It is installed on the Management Server. You can find the Microsoft Active Directory SPI package at the following location: `<SPI DVD>\x64\SPIs\AD SPI\ADSPI.msi`

Graph Package

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

- `<SPI DVD>\x64\SPIs\AD SPI OVPM Configuration Package\HPOvSpiAdGc.msi`
- `<SPI DVD>\x86\SPIs\AD SPI OVPM Configuration Package\HPOvSpiAdGc.msi`

Reporter 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 HP Reporter package at the following locations:

- <SPI DVD>\x64\SPIs\AD SPI\ADSPI-Reporter.msi
- <SPI DVD>\x86\SPIs\AD SPI\ADSPI-Reporter.msi

Console Package

The Console package contains HP Operations Topology Viewer tool, which is used to view the Microsoft Active Directory topology. It displays all the components of the Microsoft Active Directory, like DCs, PBHS, and forests. You can find the Console package at the following locations:

- <SPI DVD>\x64\SPIs\SPIs Console Packages\OVTV-Console.msi
- <SPI DVD>\x86\SPIs\SPIs Console Packages\OVTV-Console.msi

Installation Environments

The HPOM for Windows enable monitoring enterprise application servers. SPIs are part of this scalable architecture, allowing for monitoring specific application servers. You can select SPIs from the HP Operations Smart Plug-ins DVD to install on servers managed by HPOM.

Standard Installation of SPI Components on an HPOM 9.00 Server

The HPOM for Windows 9.00 server does not have the OVPMLite and ReporterLite installed on it by default. Only the full versions of these products are available for installation. As a result, using the HP Operations Smart Plug-ins DVD you can select only the SPI packages and not the Reporter and the Graph packages. However, if the full version of Reporter or Performance Manager is installed on the same machine, then the corresponding packages can be installed or uninstalled on the HPOM 9.00 server.

Standard Installation on Remote Consoles

All the Remote Console packages on the HP Operations Smart Plug-ins DVD are installed at once on to the remote consoles. There is no option provided to select a particular remote console package.

Standalone HP Reporter or HP Performance Manager

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

Installation Overview

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

Figure 2 An Overview of Installation and Configuration Steps

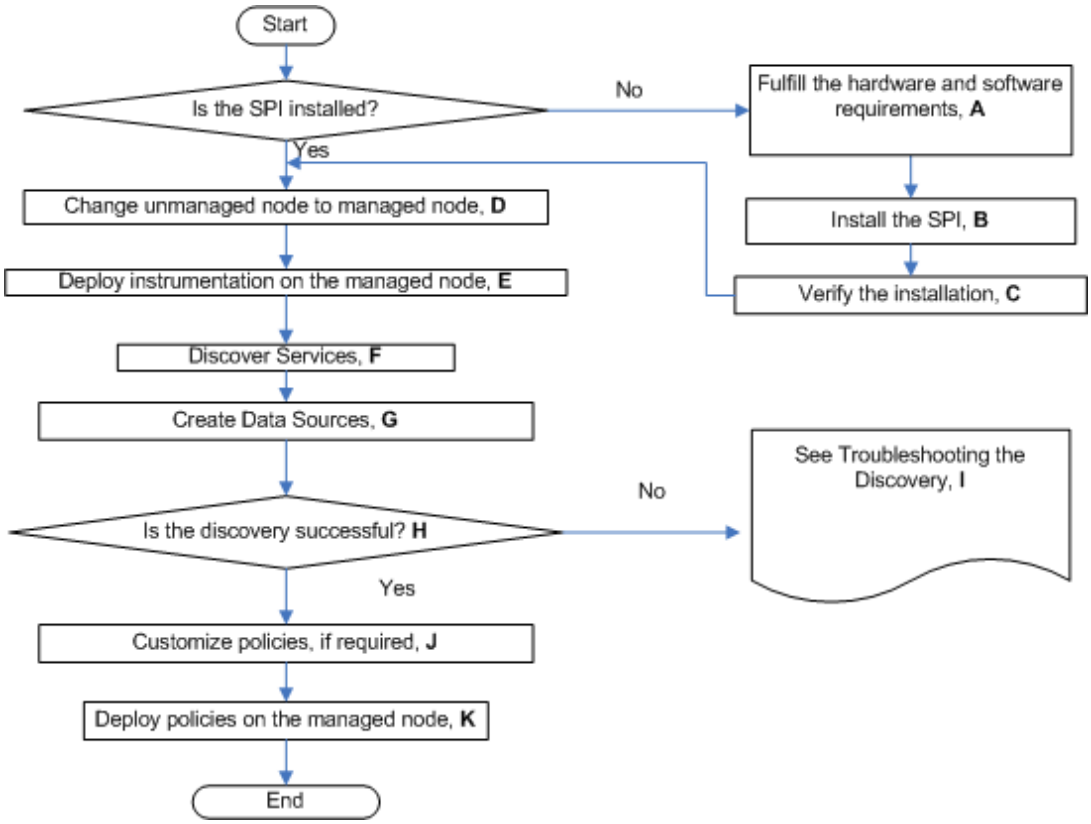


Table 1 References of Legends of Flowchart

Legend	References
A	Installation Prerequisites on page 16
B	Microsoft Active Directory SPI Installation on page 16
C	Verifying Microsoft Active Directory SPI Installation on page 18
D	Changing Unmanaged Node to Managed Node on page 19
E	Deploying Instrumentation Categories on Managed Nodes on page 19
F	Discovering Services on the Managed Nodes on page 20
G	Create Data Sources on page 21
H	Viewing Microsoft Active Directory Service Map on page 22
I	Troubleshooting on page 45
J	Customizing Policies on page 23
K	Deploying Microsoft Active Directory SPI Policies on page 23

Installation Prerequisites

For Microsoft Active Directory SPI to function properly on your system, you must fulfill the hardware and software requirements before installing the SPI. Install the HPOM server before installing the Microsoft Active Directory SPI. It is not necessary to stop HPOM sessions before beginning the installation of the Microsoft Active Directory SPI.

Hardware Requirements

Ensure that there is minimum 200 MB free hard-disk space.

Software Requirements

You must ensure that the following requirements are completed before installing the Microsoft Active Directory SPI:

- Install .net framework on Windows 2003 servers for the `ADUtility.exe` to function properly.
- SPIs must be installed on all servers in the HPOM Windows environment. If not, SPI policy upload using the **`ovpmutil`** command results in errors.

  When synchronizing policy configuration between the management servers, install the SPIs downloaded using the **`ovpmutil`** commands - **`ovpmutil cfg all dnl`** or **`ovpmutil cfg pol dnl`**, on the target server prior to uploading the policies.
- On the Management Server:
  - HPOM for Windows: 9.00
  - HP Reporter: 3.90
  - HP Performance Manager: 9.00 (Optional - for Graph package)
  - HP Operations SPI Data Collector (DSI2DDF): 2.41
  - HP SPI Self-Healing Services. (SPI-SHS-OVO, automatically installed while installing the SPI using SPIDVD): 3.04
  - HP Operations Smart Plug-in Upgrade Tool Kit (SUTK): 2.03
- Install HP Operations Agent 11.00 on the managed node.

If you are using both HP Operations agent and HP Performance Agent, the software versions are as follows:

- HP Operations agent 8.60 and above
- HP Performance Agent 5.00

Microsoft Active Directory SPI Installation

After installing the HPOM, use the HP Operations Smart Plug-ins DVD to install the Microsoft Active Directory SPI on a remote console or a Management Server. The following sections describe the installation of the SPI on a remote console or Management Server.

Installing HP Operations Topology Viewer on Remote Console

You can use the SPI DVD at the remote console to install the SPI packages located at `<SPI DVD>\<x64 or x86>\SPIs\SPIs Console Packages` on the SPI DVD by following these steps:

1. At the console-only system, insert the *HP Operations Smart Plug-ins DVD*.
2. Follow the instruction screens until a dialog box appears stating that a remote console installation is found.
3. Click **Next**.

   The installation of the remote console packages start.
4. Click **Finish** to complete the installation.

Installing Microsoft Active Directory SPI on Management Server

To install the Microsoft Active Directory SPI on the management server, follow these steps:

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

Installing Microsoft Active Directory SPI in HPOM Cluster Environment

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

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

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

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

Complete the steps described in Installing Microsoft Active Directory SPI on Management Server on page 17 before proceeding to the next management server.

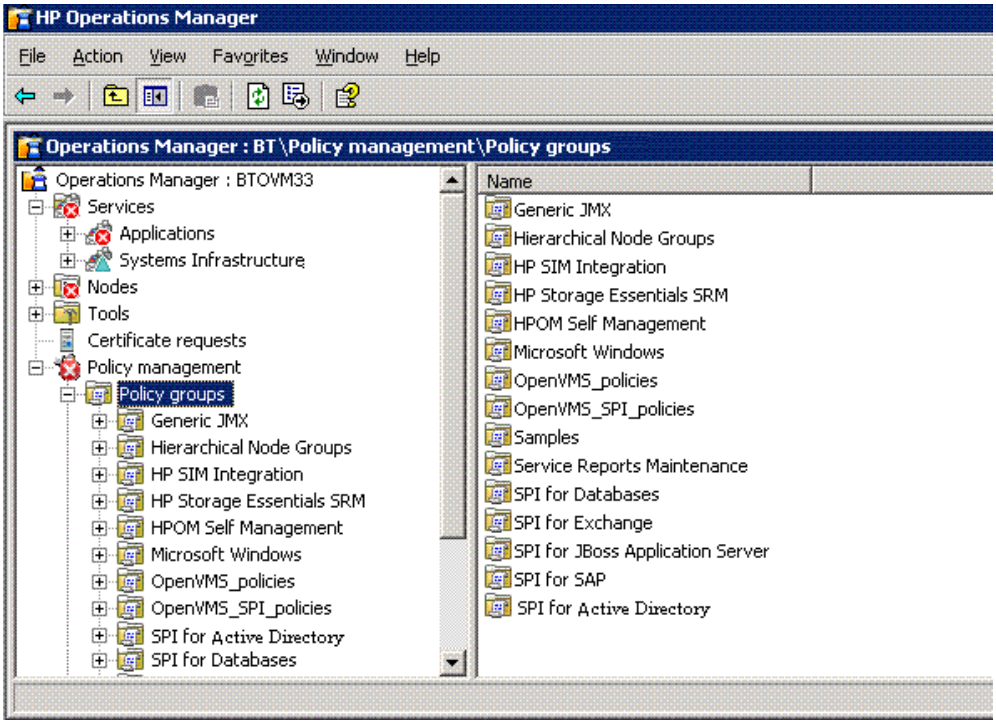
Task 2: At the next cluster-aware management server, install pre-selected Smart Plug-ins.

Repeat the steps described in Installing Microsoft Active Directory SPI on Management Server on page 17 on each Management Server in the cluster and continue to every Management Server (as mentioned in the HP Operations Manager cluster installation) until you finish.

Verifying Microsoft Active Directory SPI Installation

To verify the Microsoft Active Directory SPI installation, follow these steps:

- Check for the Microsoft Active Directory SPI under policy group.
  - Expand **Policy Group** under **Policy Management**. If **SPI for Active Directory** is in the list, it verifies that Microsoft Active Directory SPI is installed.



- Verify that the policies have 7.650 as the version.

Migration of Microsoft Active Directory SPI from Previous Version

For information on migrating the Microsoft Active Directory SPI from the previous version to the latest version, see *HP Operations Smart Plug-ins DVD Release Notes*.

3 Configuring Microsoft Active Directory SPI

This chapter describes the procedures to configure the Microsoft Active Directory SPI.

Changing Unmanaged Node to Managed Node

To change an unmanaged node to a managed node, add the nodes to the HPOM console nodes folder. By adding nodes, you can start an automated service discovery process that duplicates the manually invoked process. To change unmanaged node to managed node, follow these steps:

1. In the console, right-click **Nodes**, and select **Configure** → **Nodes**. The **Configure Managed Nodes** dialog box appears.
2. In the **Configure Managed Nodes** box, add the unmanaged nodes to the **Nodes** using any of the following methods:
   - In the left pane double-click each node you want to add.
   - Drag and drop nodes from left to right.
   - In the left pane, right-click each node and select **Manage**.

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

Deploying Instrumentation Categories on Managed Nodes

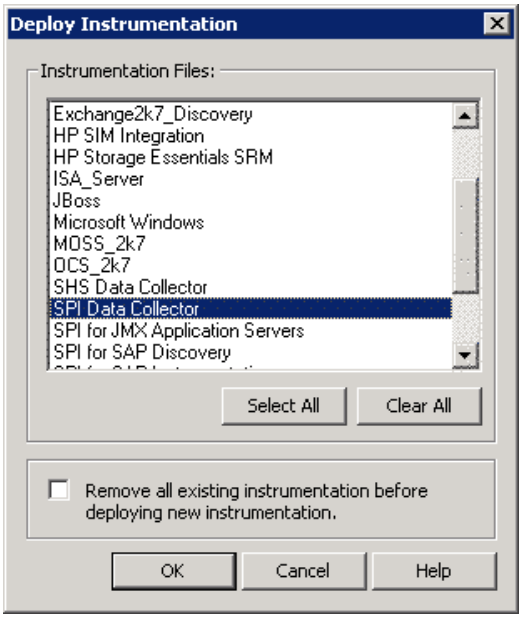
Deploy the following instrumentation categories for the Microsoft Active Directory SPI:

- SPI Data Collector
- ActiveDirectory_Core
- ActiveDirectory_Discovery

To deploy instrumentation, follow these steps:

1. In the console tree of HPOM, right-click a node and select **All Tasks** → **Deploy instrumentation...**. The **Deploy Instrumentation** dialog box opens.

2 Select the mandatory instrumentation category, **SPI Data Collector**.



3 Select **ActiveDirectory_Core** and **ActiveDirectory_Discovery** categories, and then click **OK**.

4 Perform steps 1 through 3 for all the Microsoft Active Directory SPI managed nodes

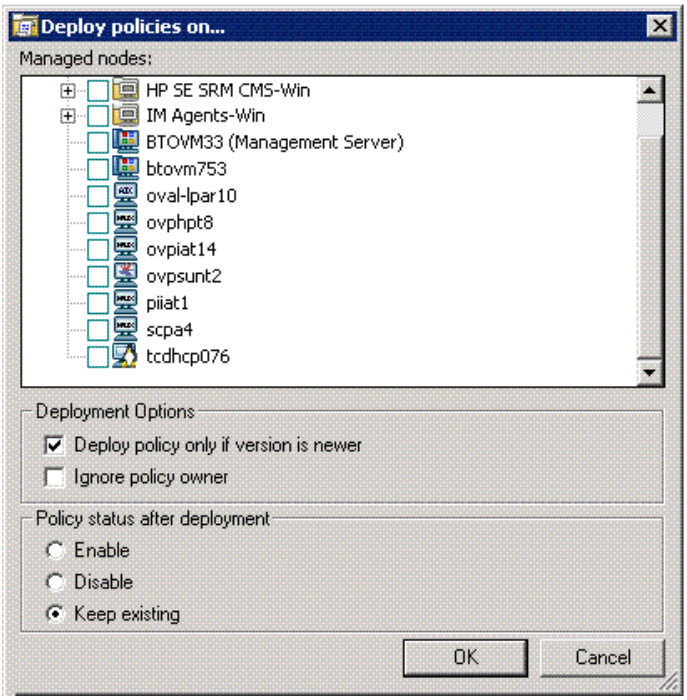
Discovering Services on the Managed Nodes

Deploy the discovery policy to discover the existing Microsoft Active Directory services on the managed nodes. To discover services, follow these steps:

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

2 Right-click **Discovery**, and select **All Tasks** → **Deploy on...**. The **Deploy Policies on** dialog box appears.

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



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

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

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

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

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

Create Data Sources

The Microsoft Active Directory SPI collects metric data on the managed nodes, and logs the data to a data store on the managed nodes. Data sources must be created in CODA (or HP Performance Agent) to enable the policies to log data.

The policy, **ADSPI-CreateDataSources**, available at **Policy groups** → **SPI for Active Directory** → **en** → **Windows Server 2008** (or **Windows Server 2003**) → **Auto-Deploy** → **Discovery**, creates the required data sources in the data store of the HP Operations agent or HP Performance Agent.

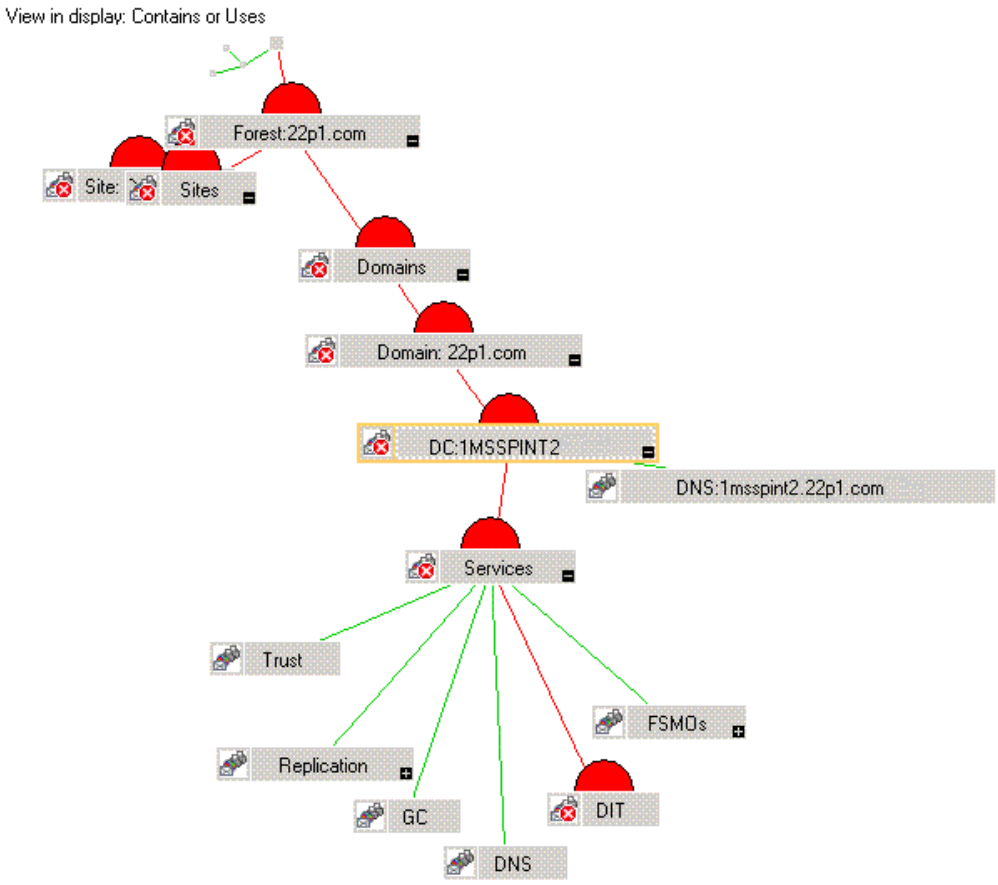
Ensure to deploy the instrumentation category **SPI for Data Collector** before running this policy on the managed nodes.

Viewing Microsoft Active Directory Service Map

After running auto-discovery, you can see the discovered services graphically represented as domains and sites within the HPOM service map.

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

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



Customizing Policies

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

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

If you customize the policies after deploying them, you must redeploy the customized policies. For more details on customizing policies, see Chapter 4, Using Policies.

Use HP Operations Smart Plug-ins Upgrade Tool Kit 2.03 to retain the customization of the earlier versions of the Microsoft Active Directory SPI policies. For more information, see *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide*.

Deploying Microsoft Active Directory SPI Policies

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

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

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

To deploy the Microsoft Active Directory SPI policies, follow these steps:

1. In the console tree, expand **Policy management** → **Policy groups** → **SPI for Microsoft Active Directory** → **en** → **Windows Server 2008** (or **Windows Server 2003**).
2. Right-click the <**Policy Group**>. Select **All Tasks** → **Deploy on...**. The Deploy policies on... dialog box appears listing all the managed nodes.
3. Select one or more managed nodes on which you want the <**Policy Group**> to be deployed, and then click **OK**. The <**Policy Group**> is deployed on the selected nodes.
4. Perform steps 1 through 3 on all the nodes.

Data Logging Scenarios

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

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

1. Create a folder `dsi2ddf` in the path `%OvAgentDir%\Conf`, if it does not exist.
2. Create an empty file `nocoda.opt`.

3 Enter the names of the other data sources *except ADSPI*, which are to be created and for which the data logging has to happen in Performance Agent into the file `nocoda.opt`.

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

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

4 Using Policies

Policies monitor the Microsoft Active Directory environment and are executed according to rules and schedule specifications. Microsoft Active Directory SPI policies contain the rules for interpreting Microsoft Active Directory states or conditions. You can customize specific policies to suit the requirements of the Microsoft Active Directory environment.

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

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

Microsoft Active Directory SPI Policies

The policies for the Microsoft Active Directory SPI in the HPOM console are organized into Policy Groups and Policy Types.

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 policies deployed automatically and manually in the Microsoft Active Directory, select **Policy management**→ **Policy groups** → **SPI for Active Directory** → **en** → **Windows Server 2003** or **Windows Server 2008**→ **Auto-Deploy** or **Manual-Deploy**.

The policies in each deployment appear. The **Auto-Deploy** group enables you to deploy all subgroups at the same time. You can choose an area to monitor such as DIT, DNS, FSMO, or Trust.

Policy Type

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

Auto-Deploy Policies

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

Discovery

The 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

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

DNS Monitoring

The 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

The 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

The 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)
- DC accessing the service (DC)

Sysvol Monitoring

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

Trust Monitoring

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

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 polices offer basic monitoring that cover areas of the Microsoft Active Directory involving connectivity, domain, and organization unit structure, health, index and query, replication or replication activities or both, security, and site structure. The following sections describe the various sub-groups of the Manual Deploy policies and their functions.

Auto-Baseline Policies

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

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

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

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

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

- Policy reads the historical values of the monitored metric. Historical values are stored into the data store.
- Policy calculates the arithmetic mean of the values of the metric.

  Arithmetic mean = Sum of all historical values/ Number of all historical data points
- Standard deviation of the metric is calculated using the following details:
  - Arithmetic mean of the metric
  - Historical data point
  - Number of all historical data points
- Policy sets a range of threshold values using the following calculation:
  - Maximum threshold = Arithmetic mean + Standard deviation
  - Minimum threshold = Arithmetic mean - Standard deviation
- Policy generates an alert when the metric value does not belong to the threshold range.

In the embedded vbscript of the AutoThreshold policies, there is a logic to evaluate the current value based on the historical values and then alert. From the historical values logged into the data store, standard deviation is calculated. The first Standard deviation consists of 68 percent of historical data, second Standard deviation consists of 95 percent of historical data, and third Standard deviation consists of 99 percent of data. The policy then calculates the current value, which is an average of the metric values for the last one hour.

Current value falls in the range that is either above or below a particular Standard deviation, that is, 68% / 95% / 99%. As the severity indicates, whenever the current value falls below the first Standard deviation, a warning message is generated, along with an attribute which states whether the current value is `above/higher` or `below/lower` the Standard deviation.

Connector Policies (Only for Windows Server 2003)

The Connector 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

The Domain and OU Structure policies monitor domain and Organization Unit (OU) changes.

Global Catalog Access

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

Health Monitors

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

Index and Query Monitor

Index and Query Monitor policies monitor the performance monitor counters associated with LDAP client sessions and Kerberos.

Replication Monitoring

Replication Monitoring policies monitor 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

Replication Activity policies monitor the Directory Service log of the Microsoft Active Directory for replication events.

Security

The Security policies monitor the following:

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

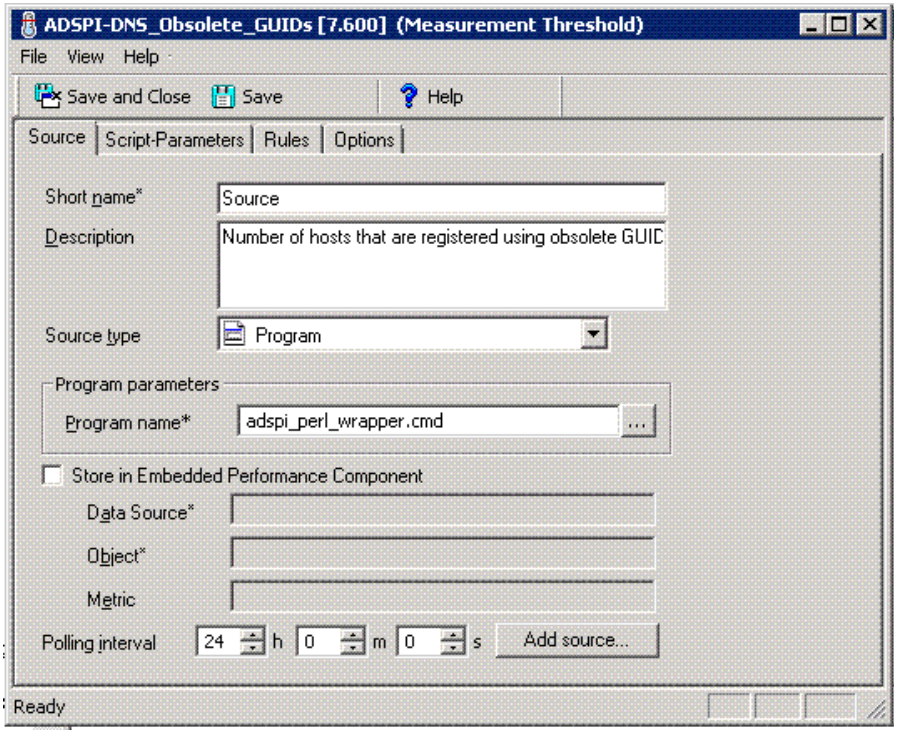
Site Structure

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

Customizing Default Policies

For customizing default policies, click **Policy management** → **Policy groups** → **SPI for Active Directory** → **en** → **Windows Server 2003** (or **2008**) → **Auto Deploy**. Double-click the specific policy to modify one or more conditions of the policy. Following are some of the parameters that can be customized:

- Script-parameters
- Rules
- Options



Use HP Operations Smart Plug-in Upgrade Tool Kit 2.03 to retain the customization of the earlier versions of the Microsoft Active Directory SPI policies. For more details, see *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide*.

Customizing Monitoring Schedule or Measurement Threshold Policies

You can customize the Monitoring Schedule or Measurement Threshold policies for Microsoft Active Directory SPI. After you update the policy for the nodes to which you want the latest change applied, right-click the **Policy group**, select **All Tasks** → **Update to latest**, and then re-deploy one or more policies to one or more managed nodes. Follow these steps:

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

Custom Data Collection Groups

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

5 Tools

The Microsoft Active Directory SPI uses different tools to gather information on the Microsoft Active Directory environment.

The Microsoft Active Directory SPI tools are as follows:

- AD Trust Relationships
- Topology Viewer
- Delete Older ADSPI Classes
- ADS Printer Information
- Check ADS Service
- AD DC Demolition Preparation
- Self Healing Verification
- Self Healing Info

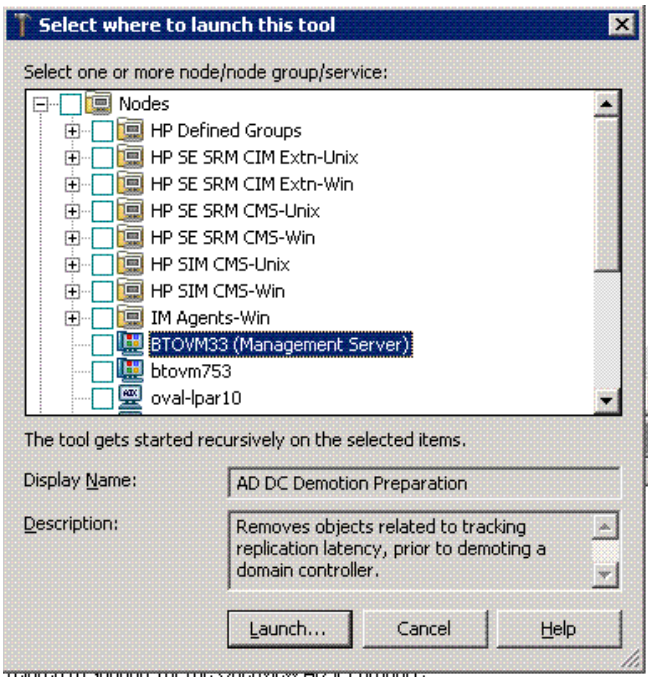
For more information on the tools, see the *HP Operations Smart Plug-in for Microsoft Active Directory Online Help.*

Starting Tools

To start the Microsoft Active Directory tools, follow these steps:

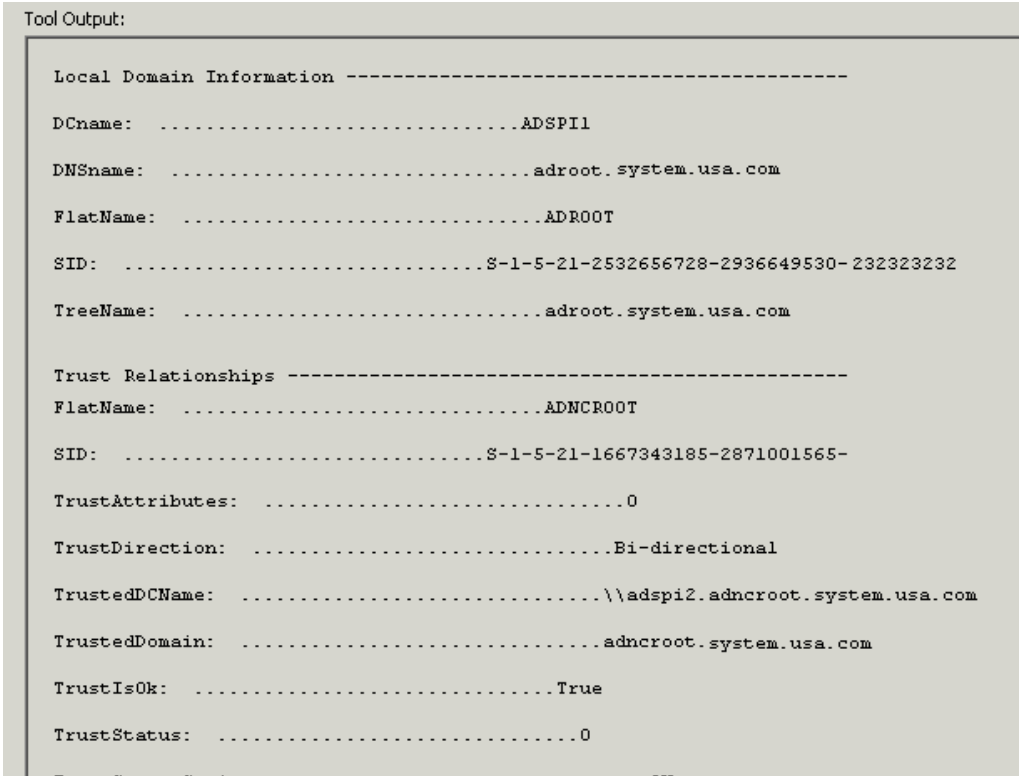
1. Click **Tools** → **SPI for Active Directory**.
2. Right-click the tool to be started. For example, **AD DC Demotion Preparation**.
3. Click **Launch**.

4 Select the managed nodes where the tool is to be started and click **Launch...**.



AD Trust Relationships Tool

The AD Trust Relationship tool is started on the Microsoft Active Directory managed node. It 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.



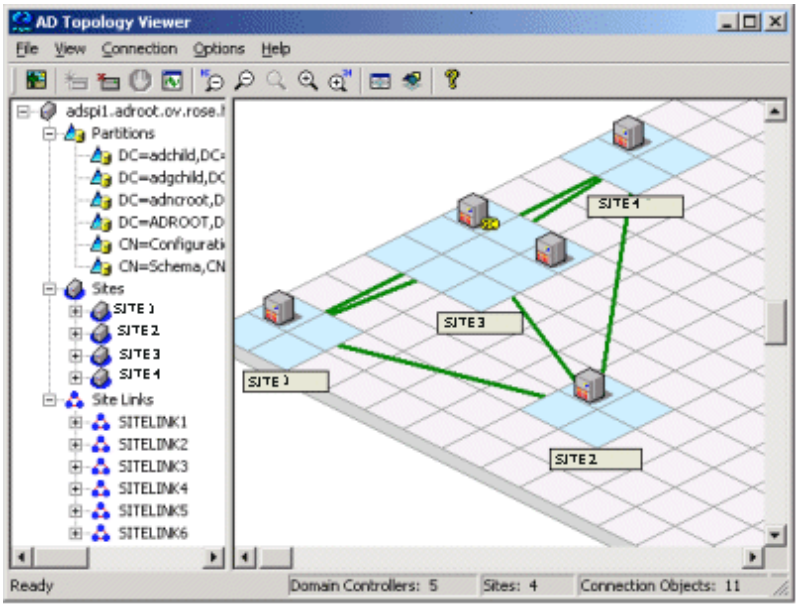
HP Operations Topology Viewer Tool

HP Operations Topology Viewer tool is a means of viewing the content and topology of the Microsoft Active Directory of your environment by generating a map. After you start 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 (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 running and status information. The map also has **zoom-in** and **zoom-out** functions and enables exporting the view of the topology to a bitmap image.

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

Figure 3 3-Dimensional View of Topology Viewer Tool



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

The modifications you make to the layout of the map are not preserved when you refresh the data.

Starting HP Operations Topology Viewer Tool

To start the HP Operations Topology Viewer tool, follow these steps:

1. Select **Operations Manager** → **Tools** → **SPI for Active Directory.** The right pane lists the Microsoft Active Directory SPI tools.
2. Right-click **Operations Topology Viewer** and select **All Tasks** → **Launch Tool...**.
3. In the Window that appears, from the **Connection** menu, select **Connect to Server...**.

   Alternatively, you can also right-click the root node of the tree.
4. In the **Connect to Server...** window, type the required information, and click **OK**.

After starting 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 is replicated across the forest on partitions, sites, site links, servers, and connections.

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

Getting Started with HP Operations Topology Viewer Tool

When you start the HP Operations Topology Viewer tool and connect it to a DC, it presents two views - tree and the 3-dimensional map. Some of the information is same and the tree lists the components of the server and the right pane shows the relationship between these components.

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

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

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

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

Accessing Features 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

When you view the HP Operations Topology Viewer replication map, sites or servers may not appear within the viewable area. You can resize the viewable area. The possible modifications to the map view are described in the following table.

Table 2 Adjusting Map View.

Tree/map modification	**How to Modify**
Move sites to different locations on the map	Drag and drop the site to desired map tiles.
Move servers	Drag and drop to desired tiles within the site.
Move the entire map	Press the middle button or press both right and left mouse buttons together; drag and release.
Display server or site labels	From the View menu select **Labels** → **Servers** *or* **Sites**
Increase or decrease the size of the row or columns in the map's grid	Right-click the unused space on or off the map and select **Map Properties**.
Find a site or server in the tree	On the map, right-click the site or server on the map and select **Find Site/Find Server** in Tree. (Label appears in blue text.)
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 method s are available)	**Method #1:** 1 Pressing the left mouse button, click the site and start to drag and drop to the desired area. 2 Still holding the left mouse button down, press the right button and continue moving in the desired direction. **Method #2** 1 Pressing the left mouse button, select the site and start to drag and drop to the desired area. 2 Still holding the left mouse button down and use the arrow keys to change the view of the map.

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

Table 3 Keyboard Functionality

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

HP Operations Topology Viewer menus

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

Table 4 HP Operations Topology Viewer Menu

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

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

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

Accessing Server and Map Properties

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

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

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

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

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

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

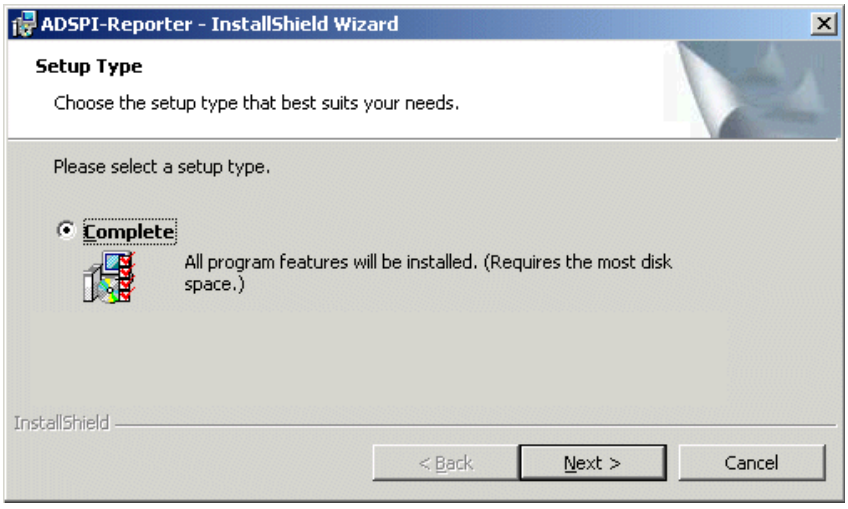
Reports and Graphs

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

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

Integrating Microsoft Active Directory SPI with HP Reporter

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



Installing and Upgrading Reporter Package

To install or upgrade the Microsoft Active Directory SPI Reporter Package on a stand-alone Reporter server, follow these steps:

1. Insert the *HP Operations Smart Plug-ins DVD*.
2. Double-click the file `setup.exe`.
3. Follow the instructions, as they appear, for the installation on management server for Windows till a dialog box opens indicating that the installation is complete.
4. Select **Finish** to complete the installation.

Configuring Reporter Package

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

1. Open the HP Reporter main window.
2. Check the status pane to note the changes to the Reporter configuration, which includes uploading the Microsoft Active Directory SPI reports.

   The Microsoft Active Directory SPI Reports are automatically assigned to the *ALL* group in the Reporter main window. (See Generating Reports for HPOM Report list.)
3. Add group and single system reports by assigning reports as required.

   Reports are available for viewing the following day.

You can identify the Microsoft Active Directory SPI reports of group and single systems by the full name. For example, **abc.xyz.com** is acceptable, but **abc** is not.

Accessing Reporter Help

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

To access HP Reporter Help, follow these steps:

1. Right-click **Reports** or **Discovered Systems** on the left pane of the HP Reporter main window.
2. Select **Report Help** or **Discovered Systems Help** from the sub-menu that appears. The HP Reporter Help appears.

For more information, see *Concepts Guide and the Installation and Special Configurations Guide* for HP Reporter.

Generating Reports

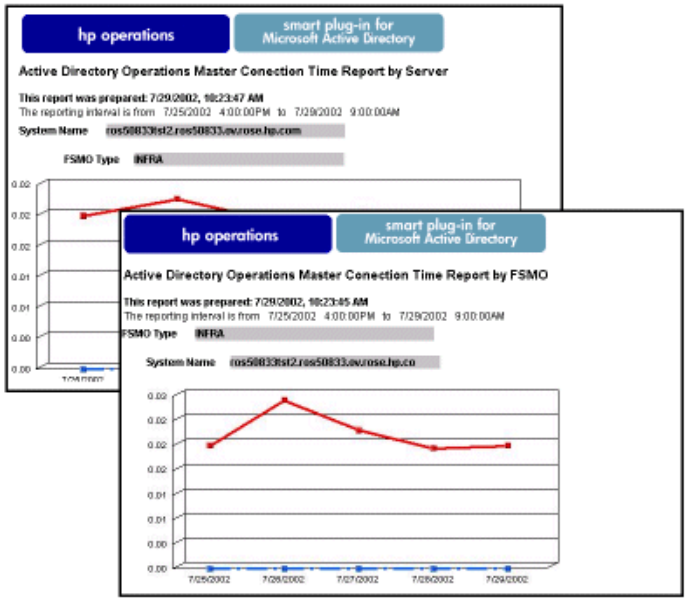
After you install the Microsoft Active Directory SPI, the HPOM generates reports using the data collected by the SPI for Microsoft Active Directory. HPOM runs the reports regularly on a nightly schedule and you can see the updated reports every day.

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 Microsoft Active Directory SPI reports from the **Reports** on the HPOM interface. For complete description of all the reports, see *Microsoft Active Directory SPI Online Help*.



Integrating Microsoft Active Directory SPI with HP Performance Manager

The Microsoft Active Directory SPI has 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. For more information, see Microsoft Active Directory SPI Installation on page 16.
2. Install the graph package using the following steps.

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

   a. Insert the *Smart Plug-ins DVD-ROM* into the DVD-ROM drive, and in Windows Explorer, double-click `setup.exe`.

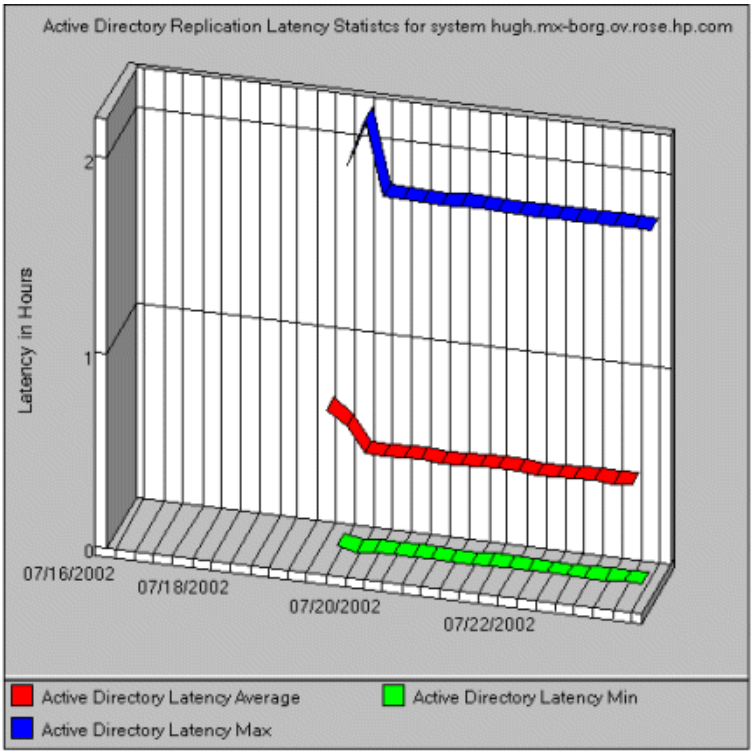
   b. Follow the instructions as they appear.
3. Select the graph package for Microsoft Active Directory SPI and complete the installation.

For more information, see the *Installation, Upgrade and Migration Guide* for HP Performance Manager.

Generating Graphs

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

1. Select **Graphs** → **SPI for Active Directory**.
2. Right-click the graph name. For example, **Active Directory Replication Latency Graph**, and select **Show Graph...**.
3. Select the node and the data range, and click **Finish**. The graph appears as shown in the following figure.



7 Troubleshooting

This chapter contains information about some problems of the Microsoft Active Directory SPI and provides solutions for troubleshooting. The methods described may or may not require support assistance.

Discovery

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

Failed Binary on Managed Node

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

- *Possible cause:* The output of the Microsoft Active Directory SPI discovery policy is not a properly formatted xml file.
- *Suggested action:* Run the Microsoft Active Directory SPI discovery binary on the managed node by performing the following steps:
  a. Log on to the managed node as an administrator.
  b. Open the instrumentation directory from the command prompt.
  c. Run the **`ovadsdisc.exe > out.xml`** command.
  d. Check if `out.xml` is in the required xml format by opening it in the web browser.

Tracing

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

You can trace all the Microsoft Active Directory SPI binaries with suffix -1 1.

Example:

The ADSPI-DNS_DC_A_Chk policy has the following command:

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

To trace the binary `ADSPI_DnsMon.exe`, you must change this command to:

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

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

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

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

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

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

Data Logging Policies Not Logging Data

The possible cause and the suggested action when the data logging policies cannot log data are as follows:

- *Possible cause:* The data source is not created in the data stores—CODA, HP Performance Agent, or both.
- *Suggested action:* Check if the data source ADSPI is created. To check if the data source is created, follow these steps:
  a. Log on to the managed node as an administrator.
  b. Run the `ovcodautil -obj > out.txt` command from the command prompt.
  c. Check the `out.txt` file to ensure that the data source ADSPI is created.

Browser Stops while Viewing HTML Report

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

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

- *Suggested action:* View the reports in PDF format.

Reports Fail with Oracle Database

Some reports fail because of invalid Reporter ODBC driver.

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

Modifying Policy Names

Make sure that you change the corresponding schedule commands, if you change the default name of the following Microsoft Active Directory SPI policies:

- 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 more information about each policy, see *HP Operations Smart Plug-in for Microsoft Active Directory Online Help* or *HP Operations Smart Plug-in for Microsoft Active Directory Online Help PDF*.

8 Removing Microsoft Active Directory SPI

The Microsoft Active Directory SPI can be removed from the Management Server using either of the following:

- SPI DVD
- Windows Control Panel

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

Removing Microsoft Active Directory SPI Components

The Microsoft Active Directory SPI components include policies, tools, reports, and graphs. Perform the following tasks to remove the Microsoft Active Directory SPI components.

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

1. On the interface, expand **Policy Management** → **Policy groups**.
2. Right-click **SPI for Active Directory**, and select **All tasks** → **Uninstall from...**

   The **Uninstall policies from...** window appears.
3. Select the check boxes corresponding to the nodes from which you want to remove the policies.
4. Click **OK**. The policies are removed from the specified nodes.

To verify if policies are removed, in the HPOM interface expand **Nodes**, right-click a node, and select **View** → **Policy Inventory**.

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

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

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

1. Expand **Policy Management** → **Policy grouped by type** → **Agent policies.**
2. Click each policy type. The right pane lists the policies in the policy group.
3. Select all versions of the policies starting with **ADSPI**.

4 Right-click the policy. Select **All Tasks** → **Delete version from server.**

Removing Microsoft Active Directory SPI from Management Server

To remove the Microsoft Active Directory SPI from the management server, follow these steps:

1 Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.

When you use the Windows Control Panel to remove a SPI, there are two options:

- to remove selected SPIs
- to remove HPOM for Windows.

If you want to remove both HPOM and the SPIs, you must first remove all SPIs from managed nodes and management server.

2 Select **HP Operations Smart Plug-ins**, and then click **Change**.

3 Click **Next** on the **Welcome** screen.

4 Select **Remove Programs**, and select **HP Operations Smart Plug-ins**.

5 Select **HP Operations Smart Plug-in for Microsoft Active Directory**.

6 Follow the instructions until a message appears stating that Microsoft Active Directory SPI is removed.

Removing Reporter Package

The HP Reporter package can be removed using the Control Panel or the `.msi` file.

Using Control Panel

To remove the Reporter package, follow these steps:

1 Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.

2 Select **HP Operations Smart Plug-in for Microsoft Active Directory - Reporter Component Integration**, and then click **Change**.

3 Follow the instructions until a message appears stating that HP Reporter is removed.

Using .msi File

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

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

2 Right-click `ADSPI-Reporter.msi`, and click **Uninstall**.

3 Click **Yes** to confirm the removal of the reporter package.

Removing Graphing Package

The Graph package can be removed using the Control Panel or the `.msi` file.

Using Control Panel

To remove the graph package, follow these steps:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select the **HP Operations Smart Plug-in for Microsoft Active Directory - Graph Component Integration**, and then click **Change**.
3. Follow the instructions until a message appears stating that HP Performance Manager is removed.

Using .msi File

To remove the graph 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 click **Uninstall**.
3. Click **Yes** to confirm the removal of the graph package.

Index

S

T

U

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: