HP Operations Smart Plug-in for Microsoft Active Directory

for HP Operations Manager for Windows

Software Version: 5.10

Configuration Guide

Software Release Date: December 2007

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 2007 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

Documentation Updates

This guide's title page 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://ovweb.external.hp.com/lpe/doc_serv/

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

You can visit the HP software support web site at:

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

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels and HP Passport, go to:

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

Contents

1 Introducing the Microsoft Active Directory SPI

This chapter introduces you to the HP Operations Smart Plug-in for Microsoft Active Directory, offering an overview of its functions and components. The chapter covers the following:

What the Microsoft Active Directory SPI Does

The Smart Plug-in (SPI) for Microsoft Active Directory adds single master operations, replication, DNS, DIT, GC and trust monitoring/mapping capabilities to HP Operations Manager for Windows. The Microsoft Active Directory SPI keeps you informed of Active Directory-related conditions occurring across the network so that you are continually updated on the following:

- Data is consistent across all Domain Controllers.
- Replication is successfully completing in a timely manner.
- Systems are able to cope with outages.
- All role masters are running.
- Domain controllers are not contending with overly utilized CPUs.
- Active Directory is not experiencing capacity and fault-tolerance issues.
- Active Directory global catalog is replicating in a timely manner.
- Services, events, processes, and synchronizations are at acceptable performance levels.
- Index and query activities for example for authentications and that LDAP client sessions are occurring at acceptable levels.
- Trust relationship status between sites and DCs is as expected.

Components of the Microsoft Active Directory SPI

The Microsoft Active Directory SPI components include *policies* for service monitoring, *tools* for mapping replication connections among domain controllers, and *reports* and *graphs* for consolidating and charting the collected data.

P*olicies* allow you to control the monitoring schedule and receipt of collected information in the form of *service problem alerts* and *messages*. Service map *alerts* are shown in the OVO/HPOM service map, while *messages* are available in the OVO/HPOM message browser.

The **HP Operations Topology Viewer** *tool* provides you with a simple means for viewing the content and topology of your Microsoft Active Directory domains and sites. When used to connect to a domain controller, the Topology Viewer generates a tree showing your Microsoft Active Directory components as well as a graphical map that shows the Microsoft Active Directory site(s), forest(s), domains, and DC replication connections.

The **AD DC Demotion Preparation** *tool* is used in preparation for a domain controller demotion. This tool should be used only after you have installed and configured the Microsoft Active Directory SPI and begun to use it to monitor DCs in your Microsoft Active Directory environment. In preparation of a domain controller demotion, you use this tool to disable the Microsoft Active Directory SPI from continuing to monitor the demoted DC.

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

Microsoft Active Directory SPI integrates with OVO/HPOM's *reporting / graphing* capabilities to produce Web-based, management-ready reports as well as graphs. While Microsoft Active Directory SPI *message* and *service map alerts* provide you with information about present conditions on specific managed nodes, the OVO/HPOM reporting and graphing provide you an overview, helpful in determining needs for the long-term.

Microsoft Active Directory SPI Policy Group Descriptions

Two major subfolders for Microsoft Active Directory SPI policies are located under *Policy Groups→SPI for Active Directory;* they are **Auto-Deploy** and **Manual-Deploy**. The Auto-Deploy folder contains policies that are automatically deployed to any system running Microsoft Active Directory after services relevant to them are discovered. The Manual-Deploy folder contains policies that you must "push" out to the managed nodes as needed.

- **Auto-Deploy** policy subgroups and their functions are as follows:
  - **Discovery**: Microsoft Active Directory SPI includes *service discovery* policies that can detect *DIT, DNS, FSMO,PBHS, replication, global catalog,* and *trust* services/components running on OVO/ HPOM-managed nodes.
  - **DIT Monitoring**. (Size and activity) Checks the size of the Microsoft Active Directory database known as the directory information tree (DIT) and monitors the amount of free space. Also tracks the number of operations pending against the DIT.
  - **DNS Monitoring** (Configuration/Connectivity). 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 OVO/HPOM message browser. Other policies check the responsiveness and availability of specific DNS servers and DNS services used by Active Directory.
  - **FSMO Monitoring** (Operations Masters general responsiveness). Through bind/ping, 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 Latency**. Replication policies can measure the time required to propagate a change to all domain controllers within the domain. In addition, a policy can also monitor the replication time of inter-site and intra-site replication latency. Replication policies are run regularly in order to modify an Active Directory latency object to determine acceptable/unacceptable response times/conditions.

- **Response Time.** Response time policies measure the general responsiveness of Microsoft Active Directory as well as the responsiveness of global catalog binds and queries.
- **Global Catalog Replication**. These policies measure the time required for the global catalog to replicate from two perspectives: (1) a domain controller providing the service (GC) and (2) a domain controller 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 Active Directory health.
- **Trust Monitoring (for Windows 2003 systems only):** These policies monitor trust health and gather data that allows the Trust Relationships tool to provide updates in changes within trust relationships.

Manual-Deploy policy subgroups/functions are as follows:

- **Connector policies**: These policies use 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 policies:** These policies monitor domain and organization unit (OU) changes.
- **Global Catalog Access policies:** These policies monitor Global Catalog servers, gathering data from their performance monitor counters in regards to reads/writes/searches of the directory.
- **Health Monitors policies:** These policies check areas of Active Directory involving services, events, processes, and synchronizations essential to its acceptable 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 policies:** Monitors index and query activity for authentications, LDAP client sessions and others.

- **Replication (Manual-Deploy) policies:** 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 policy:** Monitors the Directory Service log for replication events.
- **Security policies:** Monitors (a) Security event logs for Active Directory related events, (b) Security group changes, (c) performance monitor counters associated with Security.
- **Site Structure policy:** Monitors the Active Directory Site to ensure that IP subnets are not being added, changed, or deleted unnecessarily.

What to Expect After Installing Microsoft Active Directory SPI

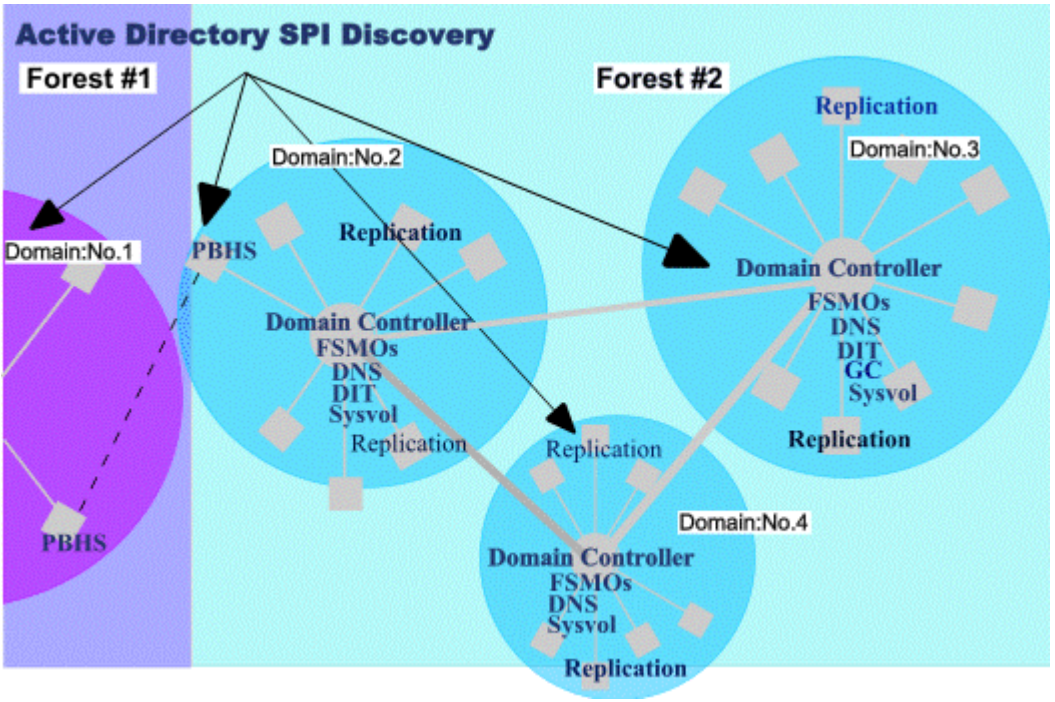
Like other Smart Plug-ins, the Microsoft Active Directory SPI adds specific monitoring capabilities to OVO/HPOM. After you have installed the Microsoft Active Directory SPI, discovery occurs and the OVO/HPOM console displays services in both the details (left) and content (right) panes. Within the details pane, the hierarchy expands to show the specific services present on each domain controller (DC). Likewise, the service map now includes another level of detail below each DC.

The Services and Components Discovered by the Microsoft Active Directory SPI

The Microsoft Active Directory SPI includes service/component discovery policies that build on the initial discovery that takes place with the Windows OS Smart Plug-in. Where the Windows OS SPI Auto-Discovery policies discover the Windows infrastructure, Microsoft Active Directory SPI expands that discovery to add multiple levels of detail at both higher and lower levels. At a higher level, the Microsoft Active Directory SPI identifies forest(s), while at a lower level Microsoft Active Directory SPI identifies each Domain Controller by its specified name and adds the services/components available on it. Finally the Microsoft Active Directory SPI shows the partitions in the discovered sites.

Below is a diagram of the Microsoft Active Directory SPI discovery, which includes forest(s), sites, domain controller services/components, and the preferred bridgehead servers (PBHS) connecting sites.

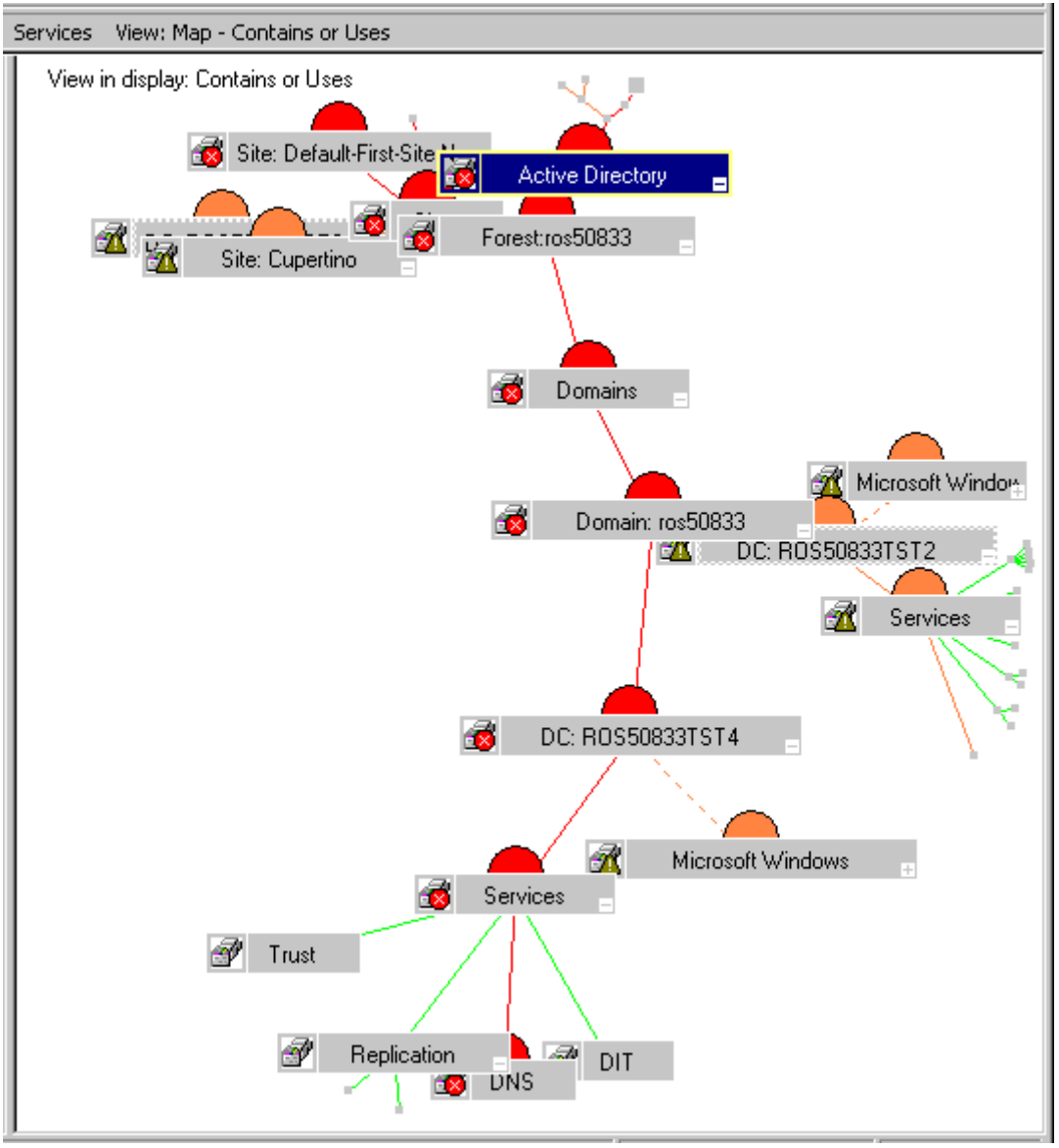
Figure 1 Example of an AD SPI Discovery.



After Microsoft Active Directory SPI discovery occurs, Active Directory services and components are displayed in the service map so that you are able to see the specific domain controllers and specific sites. More detail appears both above and below each domain controller, where you can now see Active Directory components and services, including forests, replication, and Sysvol, to name just a few.

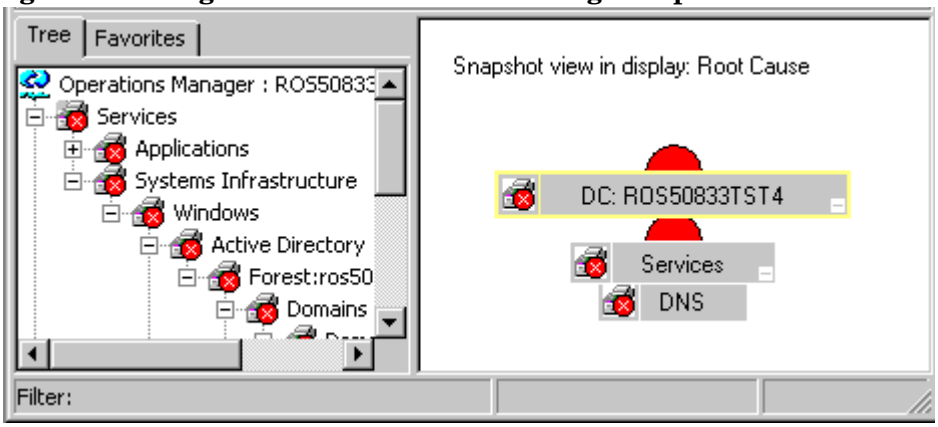
Below you see the OVO/HPOM service map in which Microsoft Active Directory SPI now identifies the Active Directory forest and DC services/components. With these additions, you can drill down from a service alert at the forest level to the domain controller service/component causing the problem.

Figure 2 Example of Active Directory discovered services



See below how by right-clicking a service where an alert is occurring (indicated by its having turned red) and choosing Root Cause, you can see where the problem is originating.

Figure 3 Using Root Cause view to see origin of problems



How Microsoft Active Directory SPI Policies Generate Information in the OVO/HPOM Console

Active Directory data is targeted and gathered according to rules and schedule specifications contained within *policies*. Policies control Active Directory data collection and interpretation and enable its display in the following formats.

Service map alerts: After the Microsoft Active Directory SPI discovery occurs, the OVO/HPOM Services tree is updated with more information on Forests/Domains/Sites/Domain Controllers (DCs). The service map is updated to graphically add specific forests, services and components to the Domain Controller names (DC: <*name*>). Those Active Directory DC services/components include replication (Replication), DIT, DNS, GC (global catalog), Sysvol, operations master (FSMO), and Sysvol (see Figure 2 on page 15). In addition, the Site map also shows the added Domain Controllers/Services, from a site-centric perspective.

Messages in the OVO/HPOM **message browser:** Using the measurement threshold policy settings and the collected values/states for each targeted domain controller, the OVO/HPOM agent software forwards appropriate messages to the console, where they are displayed with color-coded severity level.

OVO/HPOM reporting/graphing: Reports are available under Reports & Graphs in the OVO/HPOM console tree. These reports cover master operations connect times, DIT activity/size, DNS availability, GC replication delay times, and graphs on replication latency, DC availability, global catalog search response time levels, Sysvol size, and trust monitoring relationships. Each offers helpful information for analyzing trends and balancing server loads.

How the HP Operations Topology Viewer Displays Information

The Microsoft Active Directory SPI Topology Viewer is a tool that, once launched and then connected to a domain controller, opens a window of its own where it displays information about Active Directory partitions and connections. This tool allows a view of Active Directory information in two ways:

Expandable/collapsible tree: In the left pane of the HP Operations Topology Viewer window you can see the various components that comprise an Active Directory forest and its domains, the domain which hosts the domain controller, as well as the sites available through the connection.

Topological view of site connections: The right-pane of the window offers a graphical representation of forests, sites and site links, DCs, GCs, and the connection objects linking them. Sites and DCs can be moved to accommodate more effective viewing in the map. Double-clicking a DC retrieves further information, such as the version of Windows that is running, status information, and more. The map also has zoom-in/zoom-out functions and allows exporting the view of the topology to a bitmap.

SPI Changes/Uses

You can use Microsoft Active Directory SPI policies with no customization, or you can change them as you find necessary. Minor and major changes can occur as follows:

Modification of default policies: You can change a default policy by using the OVO/HPOM console to select the policy and change conditions within it. The changes you might make include: (1) frequency of the monitoring interval, (2) message text, and (3) severity of the alert.

Creation of custom data collection groups: You can also create custom data collections where you can change the monitoring interval and/or threshold for a single Domain Controller. To create a separate group of polices,

you can copy the desired polices into a folder with the new group name; after pasting the policies into the new group, you can then modify them and re-version them with your own version numbers (see, Modify a Monitoring Schedule or Measurement Threshold on page 59). 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.

Following are summaries for how the Microsoft Active Directory SPI policies are used.

Policy use: Microsoft Active Directory SPI policies are available in the OVO/HPOM console in two different ways: the first is according to group name under the *Policy groups* folder, and the second is according to type under the *Policies grouped by type* folder. You can view or edit a Microsoft Active Directory SPI policy within either of these categories.

- *Policy groups:* organizes policies according to deployment method and area to be targeted for discovery or monitoring. The Auto Deploy group allows you to deploy all subgroups at once. The sub-groups allow you to choose a specific task (such as discovery) or area to monitor (such as DIT, DNS, FSMO, GC, Replication, Response Time, Sysvol, or Trust*).
  *Trust relationship monitoring is available for Windows 2003 systems only.
- *Policies grouped by type:* organizes policies according to their function; for example, you can find the scheduling for GC, replication, or FSMO monitoring in *Scheduled Tasks policies;* you can find the conditions (thresholds) for those replication/FSMO policies in the *Measurement Threshold policies*.

A printable management-ready graph of Active Directory replication latency data is available through the Reports & Graphs area of the OVO/HPOM console. This graph provides baseline latency response time averages to help you determine how to adjust schedules/thresholds.

HP Operations Topology Viewer Tool

The *HP Operations Topology Viewer* generates a map that shows the selected Active Directory environment, its forest(s), and the connections between sites and servers. Other details also available in the map are the names of the domain controllers, the preferred bridgehead servers, and Sysvol servers. To use the tool requires only that you connect to a domain controller. Once connected to a server, the tool does the rest.

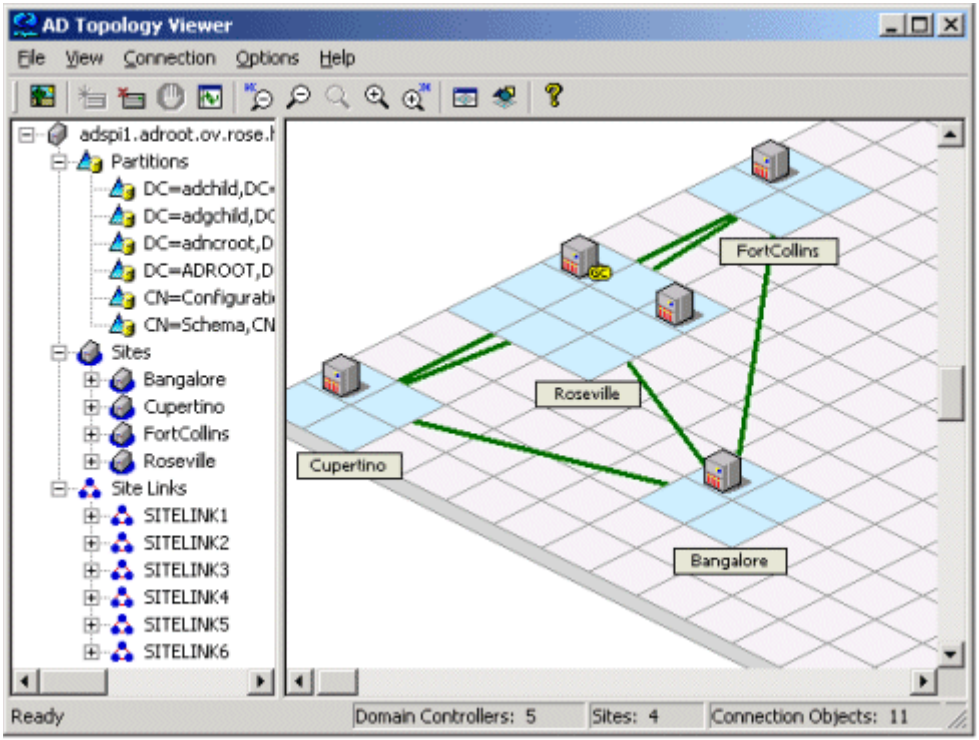
After you establish the DC connection, the tool is able to access the DC's information, which includes information on other DCs and their links as replicated across the Active Directory environment. With this information, the tool publishes current sites, partitions, and unique ID elements making up those Active Directory components in the left pane of the HP Operations Topology Viewer window. In the right pane the tool generates a 3-dimensional map that shows specific forest, site, and DC replication links among the Active Directory forest.

The information displayed in the Topology Viewer is static and reflects forests/sites/servers/connections at the time you use the tool to make the connection. Refresh the view using the Topology Viewer menu: Connections→Refresh Data.

The topology contains discovered components as follows:

- Forest(s)
- Partitions (ID component groupings)
- Sites (physical sites)
- Site Links (user-defined links between physical sites)

Figure 4 Replication map captures information on site links at the time of the map's generation.



2 Installing the Microsoft Active Directory SPI

The sections that follow show you how to install the *HP Operations Smart Plug-in for Microsoft Active Directory.* After you install the SPI, you can discover Active Directory services running on OVO/HPOM-managed nodes. Details are included on the discovery actions that automatically occur and those requiring manual steps, depending upon your environment.

For instructions on upgrading, installing, or uninstalling the Microsoft Active Directory SPI, refer to the specific sections following:

- Pre-Requisites before installing Microsoft Active Directory SPI on page 22
- Upgrade of the Microsoft Active Directory SPI on page 27
- Installation of the Microsoft Active Directory SPI on page 23.
- Uninstallation of the Microsoft Active Directory SPI on page 39

Pre-Requisites before installing Microsoft Active Directory SPI

If the management server is OVOW 7.5:

1. Install the patch OVOW_00254.
2. Upgrade the agent on the already managed domain controller nodes, to 7.35.
3. For newly managed domain controller nodes, install the agent version 7.35. If the installation is manual:

   `VC-Redistributable` should be installed manually after agent installation. VC-Redistributable installer can be found at `%OvAgentDir%`.

If the management server is OMW 8.0:

1. VC-Redistributable must be installed manually for the manually installed DCE agent nodes.

   `VC-Redistributable` installer can be found at `%OvAgentDir%`.

Installation of the Microsoft Active Directory SPI

The HP Operations Smart Plug-in for Active Directory is contained on the *HP Operations Smart Plug-ins* DVD.

Important! In Task 1 you install Active Directory; then you will see that Tasks 2 and 3 both contain methods for discovering Active Directory services. Complete Task 2 and/or 3 as relevant to your current configuration:

- Complete Task 2: if systems (nodes) running Active Directory *are currently managed* by HPOM or OVO for Windows.
- Complete Task 3 if systems (nodes) running Active Directory *are* ***not*** *currently managed* by HPOM or OVO for Windows.

Task 1: Install the Microsoft Active Directory SPI

Installation of the OVO/HPOM *Console, Management Server, and Agents* is required for Microsoft Active Directory SPI programs to work.

1. Insert the *HP Operations for Windows Smart Plug-ins* DVD.
2. Follow the instructions as they appear on screen and install the Microsoft Active Directory SPI by clicking the check box next to **Microsoft Active Directory**.
3. Deploy the Instrumentation group **SPI Data Collector** to the domain controller node before monitoring it

After you have installed the Microsoft Active Directory SPI, you should see the *SPI for Active Directory* folder in the console tree under the OVO/HPOM Policy Groups.

Task 2: Discover services on nodes already managed by OVO/HPOM

To discover Active Directory services on nodes already managed by OVO/HPOM, deploy the Microsoft Active Directory SPI service Discovery policies. By deploying these policies, you launch an automated process that adds the discovered services to the OVO/HPOM services tree/service map and deploys the relevant Microsoft Active Directory SPI policies on nodes running those services.

1. At the OVO/HPOM console, open **Policy Management→Policy Groups→SPI for Active Directory→Auto Deploy→Discovery**.

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

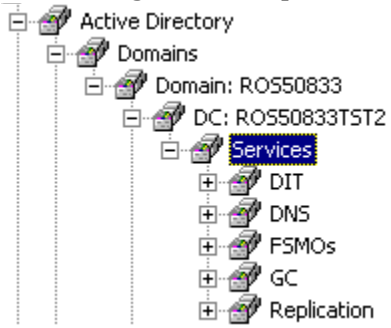
3 In the Deploy policies on... dialog select all nodes where Active Directory is running and click **OK**.

To view the deployment, under the Policy Management folder, you can right-click ***Deployment jobs****, select* ***New Window from Here*** *and choose* ***Window→Tile Horizontally****.*

In the tiled window you should see the executed processes complete as follows:

- Discovery of Active Directory DIT, DNS, FSMO, GC, Replication, Sysvol, and Trust services and consequent deployment of relevant policies.
- Update of the OVO/HPOM service map, showing DIT, DNS, FSMO, GC, Replication, and Sysvol services/components successfully discovered.

Starting at the *Services→Systems Infrastructure* folders of the OVO/HPOM console tree (in the left pane), you can navigate downward to each domain controller (DC: <*name*>), under which you should now see a Services folder that could contain *DIT, DNS, FSMOs, GC, Sysvol,* and/or *Replication*. The Services folder should always include Replication and may include FSMO if the DC runs any flexible single master operations [FSMO] service.



Task 3: Discover services on nodes not yet managed by OVO/HPOM

To discover services on unmanaged nodes, you add those nodes to the OVO/HPOM console's Nodes folder. By adding nodes, you launch an automated service discovery process that duplicates the manually invoked process described above.

1 At the console right-click the **Nodes** folder and select **Configure Nodes**.

2 In the Configure Managed Nodes dialog, you can add systems to the Nodes folder using any of three methods:

   — In the left pane double-click each system you want to add,

   or

   — Drag and drop systems from left to right

   or

   — In the left pane right-click each system and select **Manage.**

3 (As needed) If a system running OVO/HPOM agent software is not available in the Discovered Nodes folder in the left pane, in the details pane right-click the Nodes folder, select **New Node,** and enter the system name and other relevant information.

4 Click **OK**.

   When you close the dialog, first the Windows OS SPI discovery is run, then the Microsoft Active Directory SPI discovery occurs. The Microsoft Active Directory SPI discovery involves deployment of the Microsoft Active Directory SPI DIT, DNS, FSMO, GC, PBHS, and Replication, service discovery policies to each new system.

   To view the deployment, under the Policy Management folder, you can right-click ***Deployment jobs****, select* ***New Window from Here*** *and choose* ***Window→Tile Horizontally****.*

   In the tiled window you can watch the executed processes complete as follows:

   - Discovery of domains/sites using methods specific to the Windows OS discovery; then discovery of Microsoft Active Directory DIT, DNS, FSMO, GC, PBHS, and Replication services.
   - Update of OVO/HPOM service map, showing discovered DIT, DNS, FSMO, GC, PBHS, and replication services within domains/sites.
   - Deployment of relevant Microsoft Active Directory SPI policies for monitoring the discovered services.

   OVO/HPOM automatically places nodes within the correct Windows OS version folder when you close the dialog, but you can also define your own groups in which to place nodes.

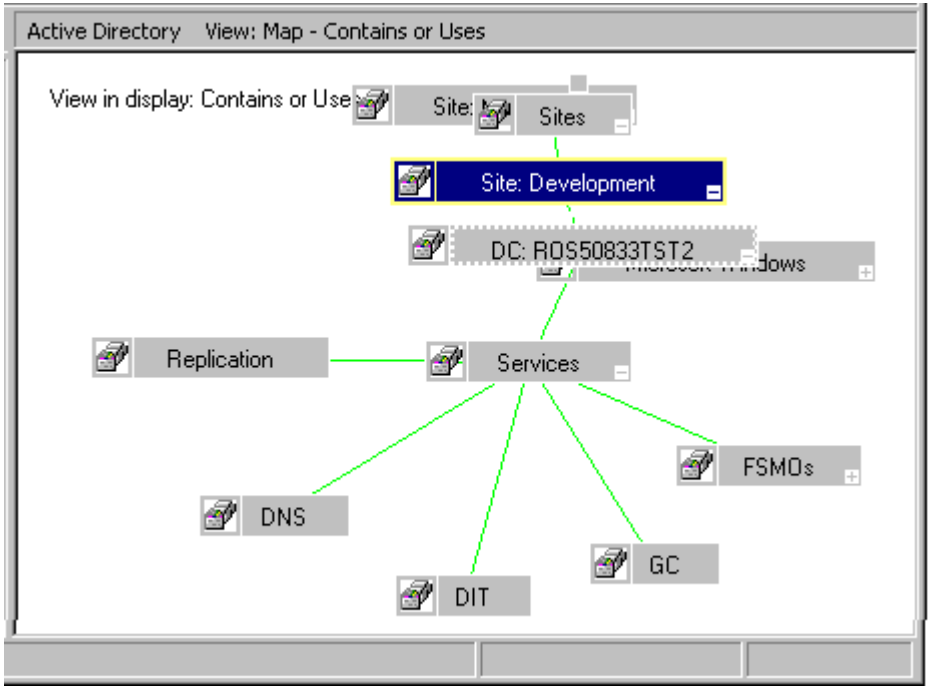
Task 4: View the service map with Active Directory services now added.

Now that auto-discovery has occurred, you should see the discovered services graphically represented under Domains and Sites within the OVO/HPOM service map.

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

In the console tree, when you select Services, you can view the service map in the right pane. There you see Domains/Sites/Domain Controller (DC:) names. For nodes managed by OVO/HPOM, you should now see discovered services/components under the Services box. Among the possible discovered services/components are *Replication*, *DNS*, *DIT*, *GC*, *FSMO*, *PBHS*, and *Sysvol*. You can further expand FSMO (clicking the plus [+]) to show the specific master operations services on the selected DC.

Figure 5 Service map showing site-centric perspective.



Upgrade of the Microsoft Active Directory SPI

No manual actions are required if you are upgrading a previous Microsoft Active Directory SPI installation. During an upgrade, using the common installer (which consolidates all smart plug-ins for installation purposes), the previous version is detected and the smart plug-in installation proceeds as expected. If however, you want to preserve any *policy customizations* made in your previous version, complete the procedure below before you begin your installation of the new Microsoft Active Directory SPI.

Prepare to Install the New Microsoft Active Directory SPI

Before you install the Microsoft Active Directory SPI using the *HP Operations Smart Plug-ins* DVD, you need to complete tasks that allow retention of customizations (as necessary) and successful discovery of additional services.

Prerequisite for preserving OVO/HPOM **service map customizations:** Before you complete the tasks below, follow the `WindowsOS_ReadMe.txt` file upgrade instructions that include steps for saving the OVO/HPOM console service map. These instructions explain how to download the service map into a file (to retain customizations), then restore to the console.

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

1. At the console, select **Operations Manager→Policy management→Policy groups→SPI for Active Directory→Auto-Deploy→ Discovery.**
2. Right-click **Discovery** and select **All Tasks→Uninstall from...**
3. Select all **Nodes** running Active Directory.
   (It is all right to select every node since you are removing only Microsoft Active Directory SPI Discovery policies and nothing else).
4. Click **OK**.

Task 2: Rename the SPI for Active Directory policy group

1. At the console, select **Operations Manager→Policy management→Policy groups**.
2. Select the **SPI for Active Directory** group and rename it (for example, SPI for Active Directory_old).

Install the New Microsoft Active Directory SPI

Having completed the preceding tasks, you are free to install the new Microsoft Active Directory SPI and customize it as desired.

Task 1: Install the SPI for Active Directory

Insert the *HP Operations Smart Plug-ins* DVD and follow the instructions as they appear on screen and select to install **Microsoft Active Directory**.

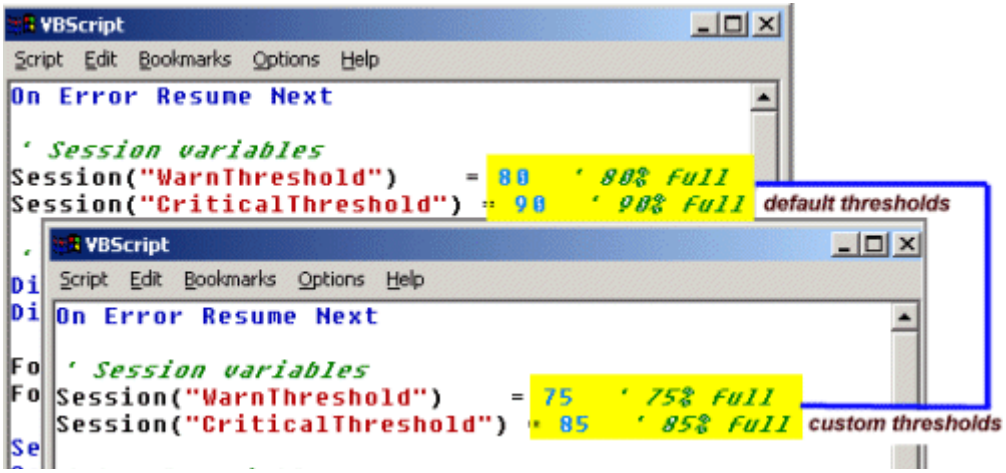
Task 2: Determine whether to change Microsoft Active Directory SPI policies:

Now that new policies are available in the SPI for Active Directory policy group, you can compare your previously customized policies with this new group (as desired). Open each policy, as explained below, to compare old/new policies as necessary.

1. Choose **Policy management→Policy groups→SPI for Active Directory**.
2. Select *<renamed policy group>*, created in the task: Rename the SPI for Active Directory policy group on page 27.
3. Compare old and new policies by opening them side by side and change the new policy to match the previous customization (as desired):

   Policies that have been customized show the original version number, followed by a decimal number; for example, 1.1.

Figure 6 Example of changing thresholds for a policy



4 When finished, delete the renamed group (if desired).

Task 3: Deploy updated instrumentation.

To enable the new/updated policies to work, you must deploy the updated Microsoft Active Directory SPI instrumentation. You can deploy instrumentation in one step on a group of nodes (if defined), or you can deploy on individual nodes.

1 At the OVO/HPOM console, open **Operations Manager→Nodes**.

2 Right-click any node running Active Directory (if you have an Active Directory group, you can right-click the group).

3 Select **All Tasks→Deploy instrumentation**.

4 From the Instrumentation Files area, select **ADSPI_Com** and **ADSPI_Disc**.

5 Click **OK**.

6 Repeat this process as necessary for remaining nodes running Active Directory.

Task 4: Deploy Microsoft Active Directory SPI Discovery policies.

To enable deployment of the new policies, manually deploy the Discovery group. Manual deployment of this group causes new services to be discovered and added to the OVO/HPOM services tree/service map. In turn, this discovery results in deployment of the relevant Microsoft Active Directory SPI policies on nodes running those services.

1 At the OVO/HPOM console, open **Policy Management→Policy Groups→SPI for Active Directory→Auto-Deploy**.

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

3 In the Deploy policies on... dialog select all nodes where Active Directory might be running and click **OK**.

Shortly, you should see additional Active Directory components listed within the **Services→DC** tree as well as additional Active Directory services in the OVO/HPOM services map. Also implemented through the Auto-Discovery process is the automatic deployment of relevant Microsoft Active Directory SPI policies to monitor every discovered Active Directory service.

Task 5: (optional) Deploy Microsoft Active Directory SPI Manual-Deploy policies.

You can choose policies from the Manual-Deploy policy group to deploy on nodes as desired.

Obtain a License/Password

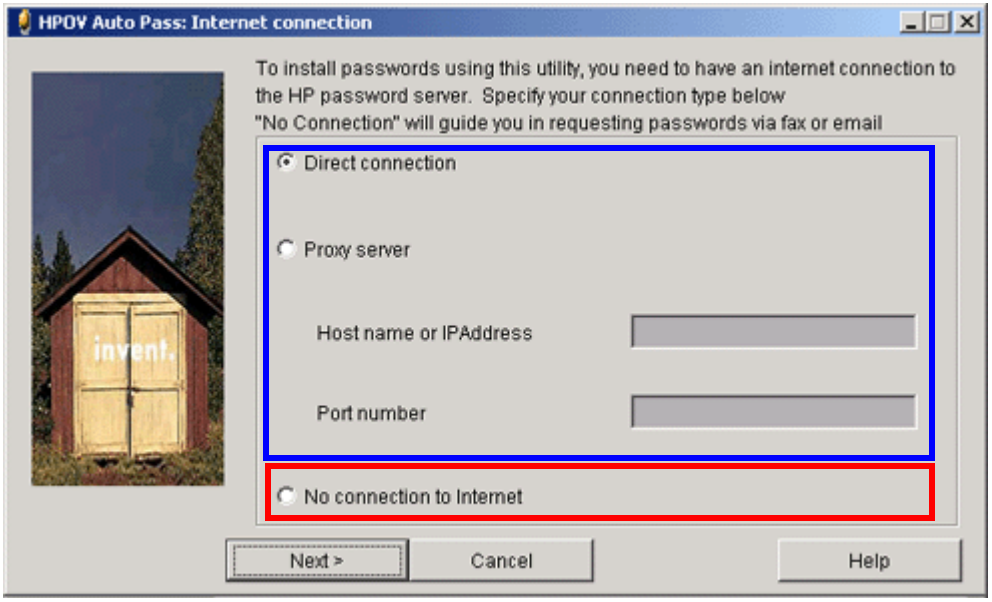
The Microsoft Active Directory SPI can be used for 60 days without a license. Within this time frame, however, you should obtain a license/password to avoid continued, uninterrupted use of the Microsoft Active Directory SPI.

The terms “license” and “password” are used interchangeably and mean essentially the same thing: a license key that allows permanent use of the Microsoft Active Directory SPI.

To obtain a license/password for the Microsoft Active Directory SPI, you will use the HP Operations Manager *Obtain License* tool. When you launch the tool, you will see that you can choose from two methods for obtaining the required license/password information:

- **Method #1, Install permanent password**: If you have an Internet connection from the OVO/HPOM console, you can directly access license/password key information. In addition, information about the server you are using is automatically detected (unless you are connecting to the Internet through a proxy server, in which case, you will have to enter the proxy server IP address).
- **Method #2, Import passwords:** If you do not have an Internet connection from the OVO/HPOM console, use this method, where you obtain the license/password information from an HP Web site (www.webware.hp.com). You store the information gained from the Web site in a file on the OVO/HPOM console and import it during the procedure.

Even though Method #1 describes the password (license) as “permanent,” both methods #1 and #2 shown in the sections that follow, install permanent passwords (licenses)


HPOV Auto Pass: Internet connection
To install passwords using this utility, you need to have an internet connection to the HP password server. Specify your connection type below
"No Connection" will guide you in requesting passwords via fax or email
Direct connection
Proxy server
Host name or IPAddress
Port number
No connection to Internet
Next >
Cancel
Help
Method #1
Method #2

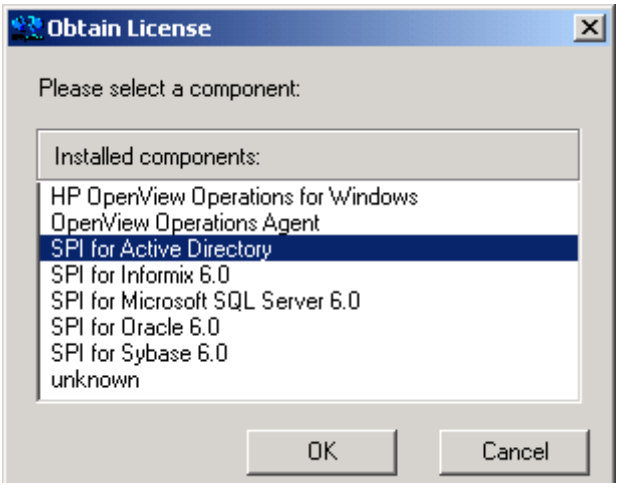
Using Method #1, Install permanent password

Prerequisite: The License Entitlement Certificate, included with the purchased HP Smart Plug-in for Active Directory. From the Certificate you retrieve the unique *Product Order#*.

1 At the OVO/HPOM console select **Tools→HP Operations Manager Tools→Licensing** and double-click **Obtain License.**

2 In the Obtain License dialog select **SPI for Active Directory** and click **OK**.

Figure 7 Selecting the SPI for Active Directory for licensing.



3 In the HPOV Auto Pass: Internet Connection dialog select the appropriate Internet connection method:

Direction connection. (if the console connects directly to the Internet)
or
Proxy server. (if the console connects to the Internet through a proxy server). Enter host name or IP address (required), and proxy port number (required); for example, 8088.

4 Click **Next**.

5 In the dialog that appears, enter the HP Order number (as it appears in the License Entitlement Certificate included with the product) and click **Next**.

6 In the **System identification and product details** dialog:
-In the Product profile **Select** column, click the product checkbox.
-In the **LTUs** column, enter the number of purchased licenses.

7 Select **Next**.

8 In the Member ID maintenance dialog enter your email address, then existing or first-time password/password verification, and click **Next.**

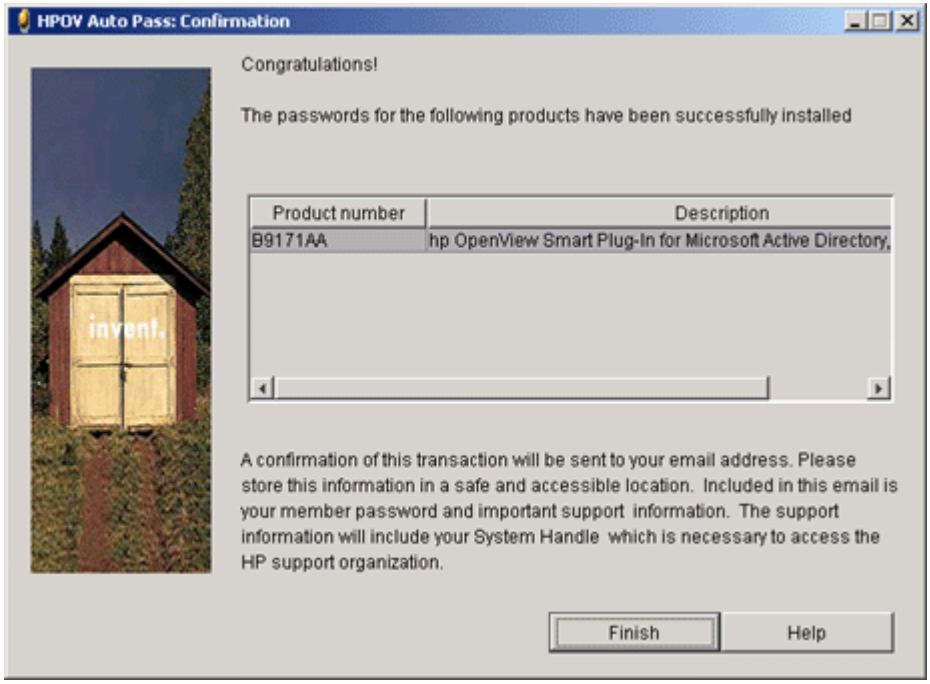
9 Enter customer information as required, then click **Next**.

10 In the dialog that appears verify that the IP address, host name, and any other information, is correct, then select the **Get password** button.

11 In the Confirmation window select **Finish**.

An email confirmation will be sent to you for your records containing the Permanent Password Certificate, which contains product information and password/license you have been issued.

Figure 8 Successful completion of the procedure for Method #1, Install permanent password, results in the following window, which also ensures that you are sent an email containing product license information.



Using Method #2, Import passwords

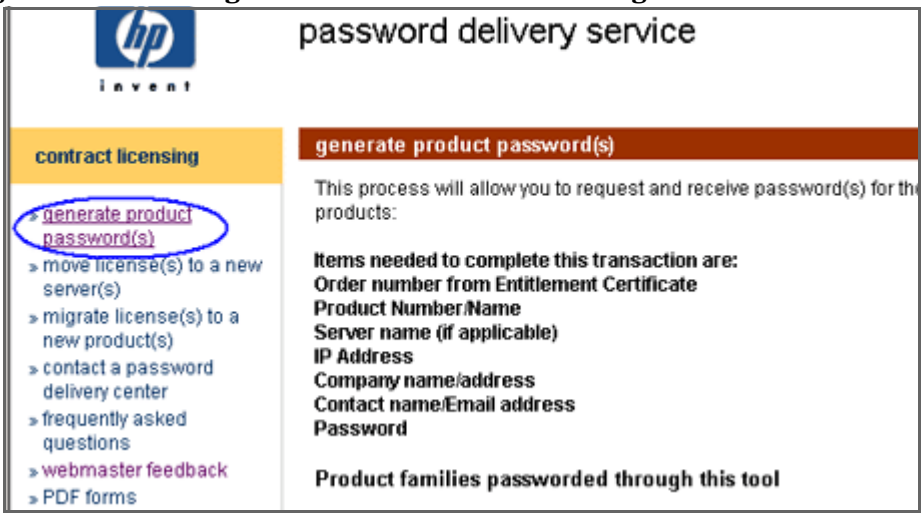
This method differs from the first in that it has a preliminary task where you open an HP Web site for information that you enter later in the second task.

Prerequisite: The License Entitlement Certificate, included with the purchased HP Smart Plug-in for Active Directory. From the Certificate you retrieve the unique *Product Order#*.

Task 1: Obtain license/password information from the Web:

1. At a system with Internet access, launch your Internet browser, and in the Address text box enter www.webware.hp.com.
2. Select **generate product password(s)**.

Figure 9 Accessing the HP Web site for licensing information.



3 In the page that appears, review the information, then scroll to the bottom of the page and click **Next**.

4 In the password delivery service page in the Order Number text box, enter the order number for your Microsoft Active Directory SPI (as it appears in the License Entitlement Certificate included with the product).

5 Click **Next**.

6 In the page that appears, select the check box next to **HP Operations Smart Plug-in for Microsoft Active Directory** and click **Next**.

7 In the page that appears showing your product number, name, version, enter information in columns as follows:

 # LTU: number of Microsoft Active Directory SPI licenses you have purchased

Management Server Host Name: name of the management server on which OVO/HPOM for Windows is installed.

IP Address: as above, the IP address of the OVO/HPOM for Windows server (must be correct or your license cannot be installed successfully)

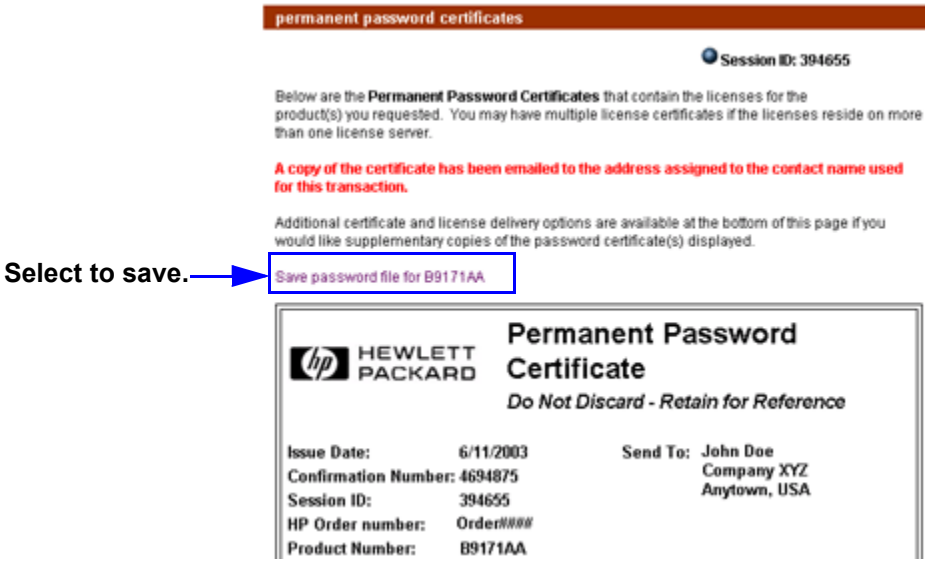
Platform: select the Windows version used on the OVO/HPOM for Windows server.

8 Click **Next**.

9 In the member login page enter your email address, then your existing or first-time password/password verification, and click **login**.

10 In the address information page, enter information as required and click **Next**.

11 In the permanent password certificates page above the certificate, click the text: **Save password file for** <*product_number*>.

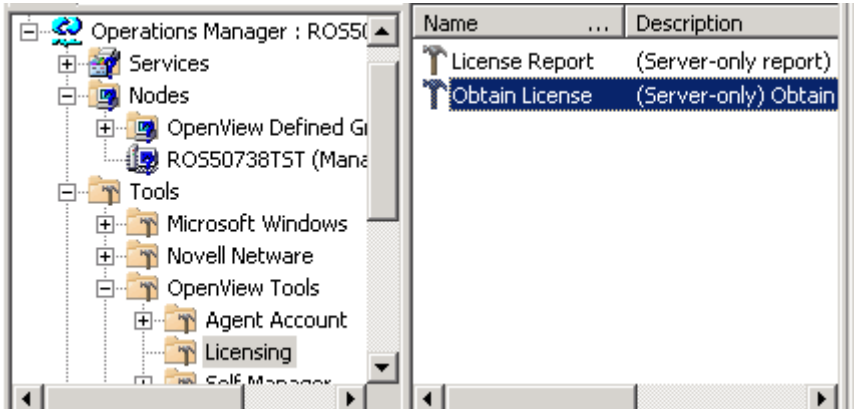


You will need to remember the location of the stored certificate for the next task. The file is titled <*product_number*>`.dat`. In addition, the Permanent Password Certificate is also mailed to the email address you entered.

Task 2: Import license/password information.

1 At the OVO/HPOM console in the contents pane, select **Tools→HP Operations Tools→Licensing** and double-click **Obtain License**

Figure 10 Starting the process to import a permanent password.

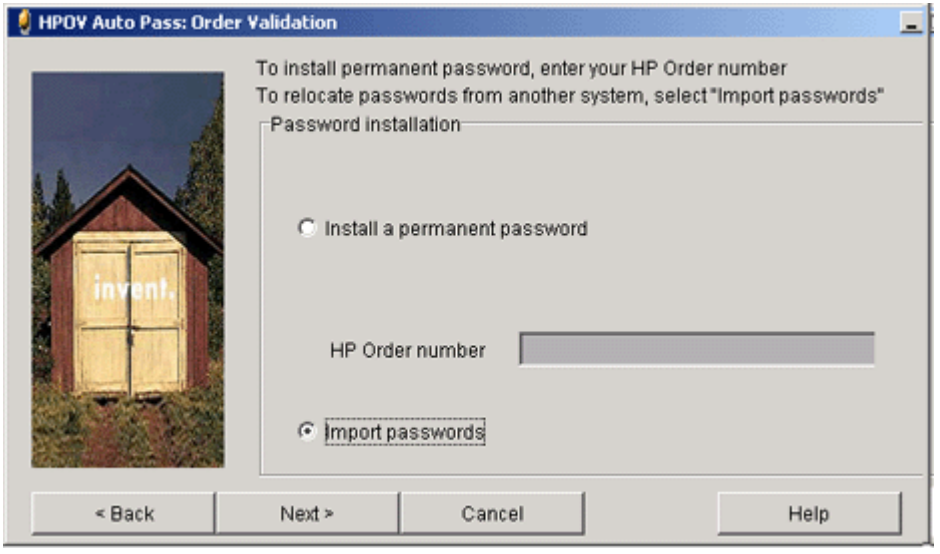


2 In the Obtain License dialog select **SPI for Active Directory** and click **OK**.

3 In the HPOV Auto Pass: Internet Connection dialog select **No Internet connection** and click **Next**.

4 In the Order Validation dialog, select **Import passwords** and click **Next**.

Figure 11 Choosing Import passwords to use previously saved Permanent Password Certificate from the Web.



5 In the Import passwords dialog click the **Browse...** button, navigate to the location of the file you stored in previous task, and select the file titled <*product_number*>`.dat`.

6 Select the **Choose** button.

7 (Required) Click the **View file contents** button.

8 Select **Permanent Password for Product Number** <*Microsoft Active Directory SPI_product#*>.
(For example, *Permanent Password for Product Number B917AA*.)

9 Click **Import**.

Successfully imported passwords are stored in
`\Program Files\Common Files\Hewlett-Packard\PPP\LicFile.txt`.

Uninstallation of the Microsoft Active Directory SPI

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

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

1. At the console expand the folder **Policy Management.**
2. Right-click SPI for **Active Directory** and select **All tasks→Uninstall from...**.
3. In the **Uninstall on...** window, select each check box next to the node(s) from which policies should be removed.
4. Click **OK**.

> To verify policies have been removed, at the OVO/HPOM console expand the *Nodes* folder, right-click a node, and select *View→Policy Inventory*.

Task 2: Remove the Microsoft Active Directory SPI policy group from the management server.

1. In the console expand the folder **Policy groups.**
2. Right-click **SPI for Active Directory** and select **Delete**.

Task 3: Remove the Microsoft Active Directory SPI tool group from the management server.

1. In the console expand the folder **Tools.**
2. Right-click **SPI for Active Directory** and select **Configure→Tools...**.
3. In the Configure Tools dialog right-click **SPI for Active Directory** and select **Delete**.

Task 4: Uninstall Microsoft Active Directory SPI programs from the OVO/HPOM management server.

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

(You are updated on the progress of the Microsoft Active Directory SPI program removal)

2 Click **Finish** to complete.

3 Using the Microsoft Active Directory SPI

After you complete your Microsoft Active Directory SPI setup, the OVO/HPOM console shows updates in areas as follows:

- Service map now shows newly added Active Directory services displayed in both the console Services tree and the service map.
- Message Browser now displays information in the form of messages (indicating problem severity level).
- Reports/Graphs are available, which consolidate Active Directory-related data as accumulated over time. The information contained in the reports and graphs can help you see trends so that you are better able to manage your Active Directory Server environment, implementing effective load balancing, capacity planning, and policy scheduling/thresholding adjustments.
- HP Operations Topology Viewer is available for connecting to an Active Directory domain controller and viewing your Active Directory topology (see The HP Operations Topology Viewer on page 60).

At the core of the Microsoft Active Directory SPI are the policies that enable the above information to be displayed. As you review the numbers of service map alerts, browser messages, and reporting/graphing data, you may determine that you need to make some adjustments to policy settings. If a policy warrants customizing, this chapter provides additional information for modifications.

More details concerning policies are also included in the online Help available in the OVO/HPOM console. The topics below offer information on what the policies do, what you can do to customize them, and what to do for some specific problems. The topics for these issues are covered as follows:

- Auto-Deploy Policies on page 42
- Basic Policy Modifications on page 59

This version of the Microsoft Active Directory SPI offers enhanced replication monitoring, see the section Replication Monitoring on page 53 for details.

Auto-Deploy Policies

Microsoft Active Directory SPI Auto-Deploy policies are divided into logical groups: one for service discovery and the others for monitoring Active Directory services/components DIT, DNS, GC, FSMO (flexible single master operations), replication, response time, and trust relationships. Please see the Microsoft Active Directory SPI online Help for individual policy descriptions.

Data-Source Creation

ADSPI Data Sources need to be created in CODA for policies to log data. The policy **ADSPI-CreateDataSources** under the policy group *SPI for Active Directory→Auto-Deploy→Discovery→Advanced Discovery* creates the required data sources in CODA.

NOTE: The instrumentation category **SPI for Data Collector** needs to be deployed before running this policy on the managed node.

Replication Monitoring

- **ADSPI-REP_ModifyObj:** This policy updates an object that is used by the ADSPI-Rep_Mon policy so that replication latency for both inter-site and intra-site purposes can be tracked.
- **ADSPI-Rep_Mon:** Windows 2000 Active Directory takes a multi master approach to common administrative tasks. Using this multi-master approach means that changes made to the directory on a domain controller are propagated too all other domain controllers. No single master is required. Every hour this policy modifies an Active Directory replication object. It works in conjunction with another policy that tracks the latency.
- **ADSPI-Rep_MonitorIntraSiteReplication:** Monitors whether replication is happening between the DCs with connection objects in the same site.

- **ADSPI-Rep_MonitorInterSiteReplication:** Monitors whether replication is happening between the bridge-head servers of sites.
- **ADSPI-Rep_ModifyUserObject:** Every hour this policy modifies an Active Directory user object. It works in conjunction with the ADSPI-Rep_GC_Check_and_Threshold policy to provide the means for tracking the replication delay time between domain controllers and the global catalog server and vice versa.
- **ADSPI-Rep-TimeSynch:** Windows 2000 (Win2K) uses a time service, known as Windows Time Synchronization Service (Win32Time), to ensure that all Win2K computers on a network use a common time. Win2K's default authentication protocol requires the service. Time synchronization is crucial because Kerberos protocol uses workstation time as part of the authentication process.

  The replication time synchronization policy measures the delta between the 'time master' and the local host. If the delta exceeds a given threshold, an alert message is sent to the OVO/HPOM console.
- **ADSPI-Rep_InboundObjs:** The number of connection objects inbound is an important metric to measure. A high number can indicate that a bridgehead may be getting overloaded and that a failure may have occurred. A failed bridgehead can cause a large number of DCs to retarget their requests; hence the high number of re-directed requests to another DC.

  This policy measures the DRA inbound object/sec counter and monitors the number of inbound replication objects.
- **ADSPI-Rep_ISM_Chk:** This policy checks the status of the InterSite Messaging service to determine whether or not the service is running and the number of associated processes currently running. When Intersite Messaging does not run properly, inter-site replication problems can occur, resulting in the inability of the KCC to calculate the replication topology.

FSMO Monitoring (Flexible Single Master Operations)

Two Microsoft Active Directory SPI scheduled task policies run checks on master operations (FSMO) configurations and performance. The two policies are: **ADSPI-FSMO_Consist** (configuration replication across DCs) and **ADSPI-FSMO_Logging** (FSMO service response time across DCs).

ADSPI-FSMO_Consist: When a domain controller is demoted from a domain, its operation master roles are transferred to another domain controller. If the domain controller is not properly demoted or is taken off line without transferring role responsibilities, operation master identification can become inconsistent. The ADSPI-FSMOConsist policy is a scheduled task policy that checks domain controller replication. Possible states are:

- state 0 = information is present and consistent
- state 1 = information is not present on the domain controller (critical)
- state 2 = information is not present on the replication partner (critical)
- state 3 = information is present on domain controller and replication partner, but is not consistent (warning)

The state is compared to the measurement threshold policy that matches the FSMO service, resulting in appropriate service map alerts and/or messages to the OVO/HPOM message browser.

- **ADSPI-FSMO_Logging**: This scheduled task policy adds to the configuration check by, once again, detecting FSMO services, then pinging and binding to those services. This policy logs the response times for each service. The data collected through this policy is used in the FSMO reports. It is also used to generate service map alerts and messages to the OVO/HPOM console when threshold policies have been deployed on the targeted managed node.

Measurement threshold policies allow the above master operations states and response times to be interpreted and acted upon in the form of messages/ service map alerts. The five master operations (FSMO) measurement threshold policy sets are:

1. **ADSPI-FSMO_Naming (Bind & Ping):** The domain-naming master is the domain controller responsible for making changes to the forest-wide domain name space. This domain controller is responsible for adding/ removing a domain from the forest and adding/removing cross-references to domains in external directories. Each forest has only one domain naming master. The ADSPI-FSMO_Naming policies measure the general

responsiveness of the domain naming master. To do this, the policies periodically bind to and ping the domain controller that is the domain naming master.

2 **ADSPI-FSMO_INFRA (Bind & Ping)**: The infrastructure master is the domain controller responsible for keeping track of objects referenced in multiple directories. The infrastructure master is responsible for maintaining security IDs and distinguished names for cross-domain references. Each domain in a forest has only one infrastructure master. The ADSPI-FSMO-INFRA_Bind policies measure the general responsiveness of the infrastructure master. They periodically bind to and ping the domain controller that is the infrastructure master.

3 **ADSPI-FSMO_SCHEMA (Bind & Ping)**: The schema master is the domain controller responsible for performing updates to the directory schema. The updated schema is replicated to the other domain controllers in the forest. There is one schema master per forest.

4 **ADSPI-FSMO_PDC (Bind & Ping)**: The PDC emulator is a Windows 2000 domain controller that acts as the primary domain controller to down-level workstations, member servers and domain controllers. In a Windows NT domain, there is one PDC master per domain in a forest, which performs the following functions:

   — Password changes, performed by other domain controllers in the domain are replicated preferentially to the PDC master.

   — Authentication failures occurring at a given domain controller in a domain because of an incorrect password, forwarded to the PDC master before a bad password failure message is reported to the user.

   — Account lockout, processed on the PDC master.

5 **ADSPI-FSMO_RID (Bind & Ping)**: The RID master is the domain controller responsible for processing RID pool requests from all domain controllers within a given domain. When a domain controller creates a security principal object such as a user, it attaches a unique Security ID (SID) to the object. The SID consists of a domain SID and a relative ID (RID).

   Each Windows 2000 domain controller is allocated a pool of RIDs. When a domain controller's pool falls below a threshold, that domain controller issues a request to the domain's RID master for a new pool. There is one RID master per domain in a forest.

The ADSPI-FSMO_RID policies measure the general responsiveness of the RID master. They periodically bind to and ping the domain controller that is the PDC master.

6 (a) **ADSPI-FSMO_Consist_INFRA**, (b) **ADSPI-FSMO_Consist_RID**, (c) **ADSPI-FSMO_Consist_PDC**, (d) **ADSPI-FSMO_Consist_SCHEMA**, and (e) **ADSPI-FSMO_Consist_NAMING**. These policies alarm when the ADSPI-FSMO_Consist policy determines that the domain controller running the policy and one or more of its replication partners do not agree on which domain controller holds the specified FSMO role.

Directory Information Tree Monitoring

Policies monitoring the Active Directory database, the directory information tree (DIT), ensure that DIT operations (as related to queue lengths), size, and occupied space on the disk of the hosting server fall within specific limits. Specifically, DIT policies monitor the following:

- **ADSPI-DIT_DITPercentFull**: Monitors the percentage of space used and the free space remaining on the logical drive hosting the DIT.
- **ADSPI-DIT_TotalDITSize:** Monitors the size of the Active Directory database and the remaining space on the logical hosting drive.
- **ADSPI-DIT_DIT QueueLength**: Monitors the queue length on the DIT logical drive, indicating the number of incomplete operations pending.
- **ADSPI-DIT_LogFilesQueueLength**: Monitors the log queue length, indicating the number of incomplete updates pending.
- **ADSPI-DIT_LogFilesPercentFull:** Calculates the percentage full of the logical drive hosting the DIT log files; the policy thresholds and logs the information.

Domain Name Server Monitoring

For DNS monitoring, the Microsoft Active Directory SPI checks DNS responsiveness and consistency with the data contained in Active Directory. To this end, Microsoft Active Directory SPI DNS policies show you whether or not: (1) DNS is returning the correct IP address for each domain controller, (2) DNS contains all SRV records that ADS dictates it should, and (3) each SRV record is accurate. The DNS group contains the following policies:

- **ADSPI-DNS_DC_A_Chk:** Checks the two DNS host records (A records) associated with a Domain Controller. There are two host records associated with each Domain Controller-one for its fully qualified domain name and one for the domain that it serves. A critical message is generated if one or both records are missing.
- **ADSPI-DNS_DC_CNAME_Chk:** Generates a critical message when a Domain Controller cannot be found using the alias: <*domain_controller_GUID*>._msdcs.<*domain*>
- **ADSPI-DNS_DC_Response:** Alerts the user when DNS queries made by the domain controller result in an unexpected or unacceptable response time; the policy thresholds on specified length of time and logs information for reporting.
- **ADSPI-DNS_Extra_GC_SRV_Chk:** Checks for expected and unexpected DNS host records registered for the global catalog. A GC record is unexpected if the domain controller does not host the global cataloguing a warning severity level is attached to the message because the situation may be intentional under certain circumstances.
- **ADSPI-DNS_Extra_Kerberos_SRV_Chk:** Generates a warning message if the domain controller is registered as a Kerberos KDC on a site in which it does not reside. Only a warning severity level is attached to the message because the situation may be intentional under certain circumstances.
- **ADSPI-DNS_Extra_LDAP-SRV_Chk:** Checks for extra DNS SRV resource records registered for the LDAP service. If an LDAP server is registered on a site in which it does not reside, a warning message is generated. The extra LDAP server incurs only a warning because the situation may be intentional under certain circumstances.

- **ADSPI-DNS_GC_A_Chk:** Checks for extra DNS host records registered for the registered for the global catalog. Checks for expected and unexpected DNS host records registered for the global catalog. A global catalog record is unexpected if the domain controller does not host the global catalog.
- **ADSPI-DNS_GC_SRV_Chk:** Checks for expected DNS SRV resource records registered for the global catalog.
- **ADSPI-DNS_GC_StrandedSite:** Checks for the existence of a global catalog on every site in the forest in which the domain controller resides.
- **ADSPI-DNS_Island_Server:** Generates a warning message if a domain controller is configured to use itself as a primary DNS server because replication problems can occur in such situations.
- **ADSPI-DNS_Kerberos_SRV_Chk:** Checks for missing resource records for Kerberos and generates a critical message when a domain controller is not properly registered in DNS as a Kerberos KDC server or Kerberos Password Change server. That is, it alerts the user when one or more SRV records that identify it as a Kerberos KDC server or Kerberos Password Change server are missing.
- **ADSPI-DNS_Obsolete_GUIDS:** Checks for hosts within the forest that the domain controller resides in that are registered under obsolete GUIDs.

Global Catalog Monitoring

The primary purpose of global catalog monitoring is to ensure that systems hosting global catalog (GC) servers are replicating in a timely manner. GC replication delay time is measured through two policies: the first is included in the Replication Monitoring group. This policy creates a user object and modifies it. The ADSPI-Rep_GC_Check_and_Threshold policy (contained in the GC Monitoring group) measures the delay time occurring in replicating this modified user object to other domain controllers and vice versa (from DC to GC, and from GC to other DCs). How this data is represented in the OVO/HPOM message browser and reports should show you how timely/slowly replicating is occurring throughout your Active Directory environment. Policies are automatically deployed through Auto-Deployment (following discovery) as follows:

- The **ADSPI-Rep_GC_Check_and_Threshold** is used to measure the replication time from domain controllers throughout the Active Directory forest to a domain controller hosting global catalog services. This policy is deployed only on systems hosting global catalog services.
- The **ADSPI-Rep_Modify_User_Object** is used to modify an object for the purpose of measuring how long it takes for the modification to be replicated to a domain controller hosting global catalog services. This policy is deployed on all Active Directory systems.

Sysvol Monitoring

Sysvol monitoring covers areas that are key to the health of Active Directory such as the Sysvol size, connectivity, and synchronization. Problems with Sysvol can initiate a cascading effect.

- **ADSPI-Sysvol_Connectivity:** The ability to connect to the Sysvol volume is a key indicator of the health of Active Directory. If Sysvol is unavailable, the Netlogon service cannot start. Group policies cannot replicate. It is not uncommon for a person to mistakenly un-share the Sysvol volume out of ignorance. When this happens, a cascading effect occurs.

  The ADSPI-Sysvol_Connectivity identifies the DC's replication partner and checks to see that the Sysvol is available to ensure its group replication and other services.
- **ADSPI-Sysvol_PercentFull:** Calculates the percent full of the Sysvol and collects information about its size and logs the information for later reporting.
- **ADSPI-Sysvol_FRS:** Monitors the file replication service in the Sysvol from one domain controller to another.
- **ADSPI-Sysvol_AD_Sync:** Checks that the Group Policy objects in Sysvol and Active Directory synchronized with each other.

Response Time Monitoring

Response time monitoring policies ensure that Active Directory operations are completing in acceptable time frames. Response time monitoring checks the general health of Active Directory operations, the time required for binding to the global catalog, and the time required for global catalog searches and queries. The policies in this group are:

ADSPI-ResponseTime_Logging: This scheduled task policy logs Active Directory response times.

ADSPI-Response Time_Query: This policy measures the time required for the Active Directory queries. It periodically queries Active Directory and monitors latency.

ADSPI-ResponseTime_GC_Bind: This policy measures the time required to bind to the global catalog. The data gathered is used for a graph, which aids in base-lining what the value should be for your environment.

ADSPI-ResponseTime_Bind: This policy periodically binds to Active Directory to measure the domain controller's bind response time, which is graphed in order to aid in base-lining what the value should be for your environment.

ADSPI-ResponseTime_GCQuery: Monitors response times of Active Directory global catalog queries.

Trust Monitoring

These policies monitor the trust relationships between domain controllers of managed nodes that are Windows 2003 systems. The policies log modifications as they occur. You can also review this information on demand by using the AD Trust Relationships tool. The tool is located within the console in Tools→SPI for Active Directory→AD Trust Relationships. The policies are as follows:

ADSPI-Trust_Mon_Add_Del: Monitors addition and deletion of trusts in Active Directory.

ADSPI-Trust_Mon_Modify: Monitors modification of trusts in Active Directory.

Accessing Trust Relationship Information

In addition to the policies that supply messages relating to additions, deletions, and changes in trust relationships, you can generate trust relationship information for each domain controller by using the AD Trust Relationships tool.

In a **Windows 2000 Server** environment for selected managed nodes, this tool displays a list showing the two-way trusts within a forest. In the **Windows 2003 Server** environment it not only reports two-way trusts within a forest but can also show trusts from one forest to another for the selected managed nodes. Please see the online Help for using the AD Trust Relationships tool.

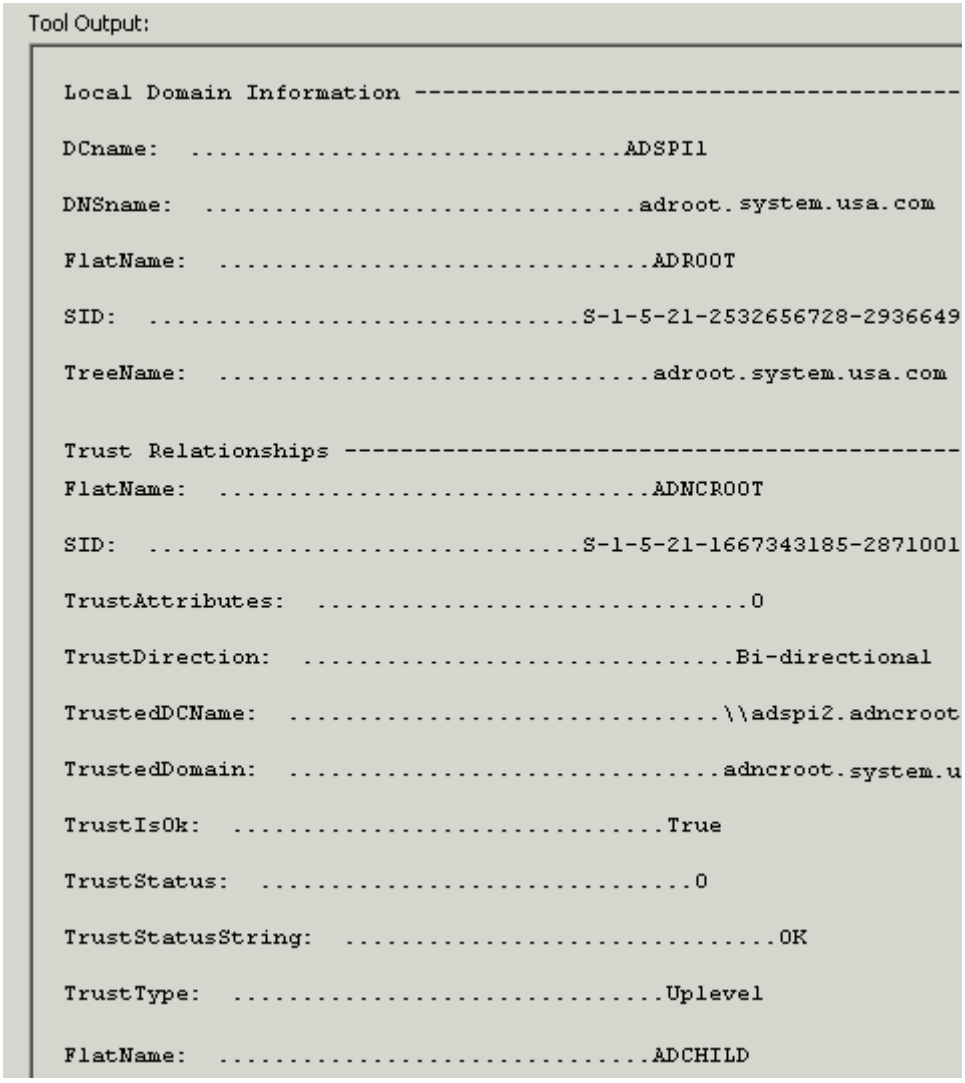
Microsoft Active Directory SPI and Demoting Domain Controllers

Use the AD DC Demotion Preparation tool before you demote any domain controller. This tool removes the OVReplication objects inserted into the directory to monitor replication.

This tool should be used only after you have installed and configured the Microsoft Active Directory SPI and begun to use it to monitor DCs in your Active Directory environment. Please see the Active Directory online Help for how to use this tool.

If you do not use the AD DC Demotion Preparation tool *before* demoting a domain controller, you can manually reconfigure Active Directory to no longer recognize the demoted domain controller by following the steps in the online Help topic “AD DC Demotion Preparation tool.”

Figure 12 The AD Trust Relationships tool lists information about the trust relationships for the selected managed node.



Manual-Deploy Policies

Microsoft Active Directory SPI Manual-Deploy policies are not automatically deployed, like the Auto-Deploy policies, after the Active Directory service occurs.

Manual-Deploy policies offer basic monitoring that cover areas of Active Directory involving connectivity, domain and organization unit structure, health, index and query, replication/replication activities, security, and site structure. For detailed descriptions, please see the online Help topic “Choosing a Microsoft Active Directory SPI policy.”

Replication Monitoring

Replication Monitoring Policies and Instrumentation

The following policies are offered by the Microsoft Active Directory SPI to monitor AD replication.

Pre-requisite supporting policies

These supporting policies must be deployed on all DCs where replication needs to be monitored.

- ADSPI-REP_ModifyObj
- ADSPI-Rep_Modify_User_Object
- ADSPI-Rep_Delete_OvRep_Object
- ADSPI-Rep_CheckObj

Core Replication Monitoring Policies

These are the policies which monitor replication and they must be deployed on all DCs where replication needs to be monitored.

The **ADSPI-Rep_Mon** policy has been moved from the Auto-Deploy policy group to the Manual-Deploy policy group. It is now located under **SPI for Active Directory→Manual-Deploy→Replication Activity.** This policy is optional.

The following policies are new, located under the policy group **SPI for Active Directory→Auto-Deploy→Replication Monitoring**:

- ADSPI-Rep_MonitorInterSiteReplication
- ADSPI-Rep_MonitorIntraSiteReplication

The replication monitoring executable

The ADSPI_RepMonI.exe has the logic for replication monitoring.

Replication Monitoring Scenarios

1 Intra-Site Replication Monitoring

The policy **ADSPI-Rep_MonitorIntraSiteReplicatio**n monitors Intra-Site Replication. It checks whether replication is happening between the DCs having connection objects in the same site.

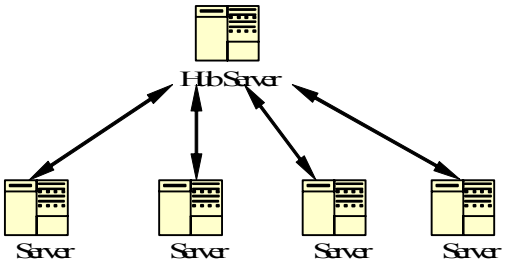
2 Inter-Site Replication Monitoring

The policy **ADSPI-Rep_MonitorInterSiteReplication** monitors inter-site replication. Bridge-Servers are responsible for replication between sites. This policy checks whether replication is happening between the bridge-head servers of sites.

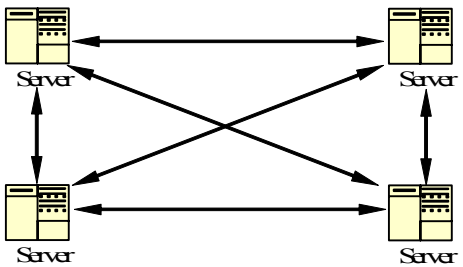
3 A number of Active Directory replication topologies are supported.

AD SPI can monitor the following Active Directory replication topologies:

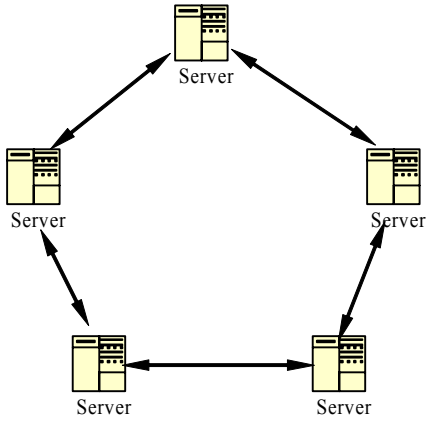
Hub and Spoke Topology Replication Monitoring



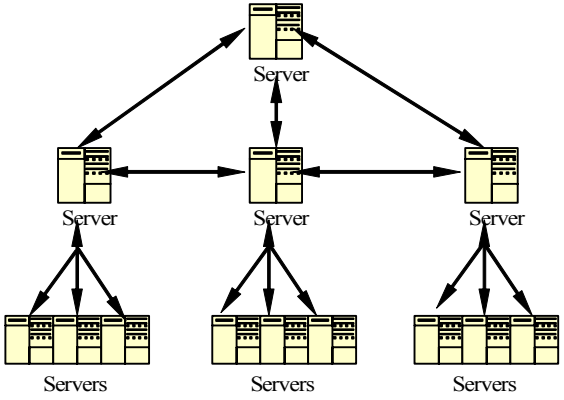
Full Mesh Topology Replication



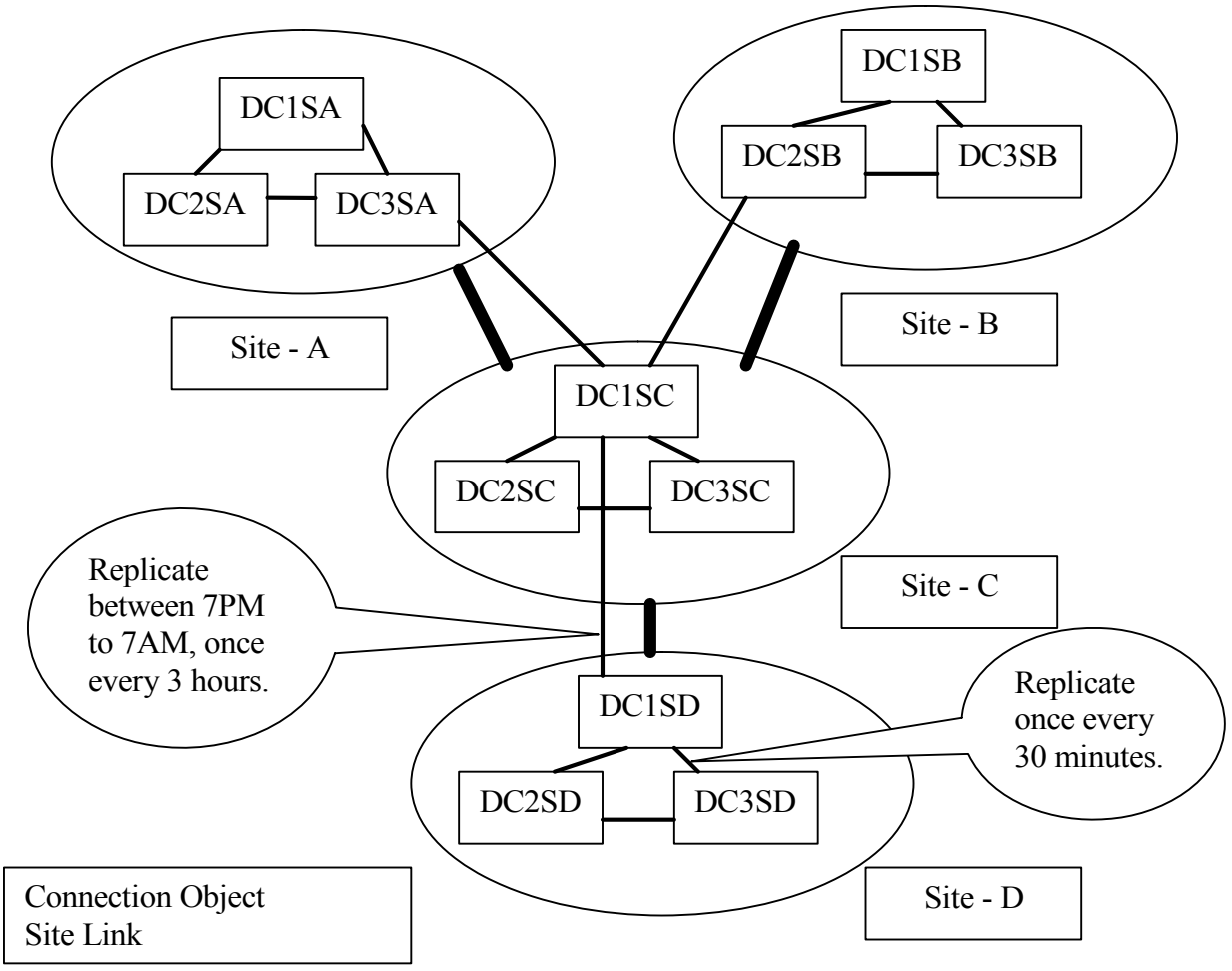
Ring Topology Replication Monitoring



Multi-tier Redundant Hub and Spoke Topology Replication Monitoring



Configuring the Replication Monitoring policies



Using the AD configuration in the above diagram as an example, Domain Controllers within site-D are configured to replicate once every 30 minutes. Bridge Head Servers of site-C and site-D are configured to replicate between 7PM to 7AM, once every 3 hours.

For the above configuration, the table below provides the recommended schedule times for policies and threshold values.

Policy	Policy Schedule	Critical Threshold	Warning Threshold
ADSPI-Rep_MonitorInterSiteReplication	4 hours	14 hours	13 hours
ADSPI-Rep_MonitorIntraSiteReplication	1 hour	2 hours	1 hour
ADSPI-REP_ModifyObj	30 minutes	n/a	n/a
ADSPI-Rep_Modify_User_Object	Default	n/a	n/a
ADSPI-Rep_Delete_OvRep_Object	Default	n/a	n/a
ADSPI-Rep_CheckObj	30 minutes	n/a	n/a

The values for Policy Schedule interval, and Critical and Warning Thresholds, have been chosen assuming that one complete inter-site replication cycle would take a maximum of 1 hour, and intra-site replication would take a maximum of 30 minutes.

Basic Policy Modifications

After using the Microsoft Active Directory SPI for awhile, you may decide that specific policies need some modification. Measurement threshold policies contain the rules for interpreting Active Directory states/conditions according to the thresholds set for the incoming data. Scheduled task policies also contain the rules for how often the data is monitored. How to change either policy type is described below. Specific policy descriptions are provided in the OVO/HPOM online Help.

When you modify a policy, OVO/HPOM assigns a version number to the modified policy; generally this means that an extension such as ".1" is added to the policy name. You can then deploy the new policy to managed nodes.

Below find suggestions for basic customizations that you might implement for every managed node.

Modify a Monitoring Schedule or Measurement Threshold

You can modify the monitoring schedule or measurement threshold polices for any Microsoft Active Directory SPI policy. After you update the policy for the nodes to which you want the latest change applied, you can right-click the policy group, select **All Tasks→Update to latest**, and then re-deploy the policy or policies to the node(s):

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

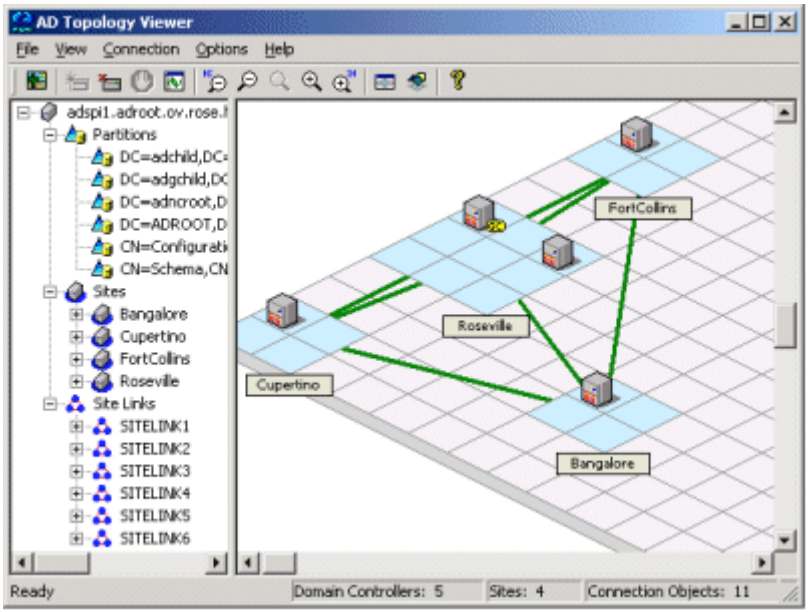
The HP Operations Topology Viewer

The HP Operations Topology Viewer supplements the information you receive from other Microsoft Active Directory SPI components and has no dependency on any Microsoft Active Directory SPI policies. Using this tool (located in the OVO/HPOM console under *Tools→SPI for Active Directory*), you are able to quickly see the various site/server connections within your Active Directory environment.

The information gathered by the HP Operations Topology Viewer is presented in both a tree (in the Viewer's left pane) and in a map that offers a 3-dimensional perspective (in the right pane). This map shows Active Directory-configured sites, and the servers located in those sites.

The site/server information shown in the HP Operations Topology Viewer is a snapshot of the data retrieved at the time of the connection to the specified server. It is not automatically updated, but can be refreshed (select *Connection→Refresh Data*). Modifications to the map's layout, however, are not preserved when data is refreshed.

Figure 13 The Topology Viewer shows the links between sites (green lines). To view server links, select View→Connections→Intersite [or Intrasite].



The HP Operations Topology Viewer requires only that you connect to any domain controller in the Active Directory forest. This single connection provides all the necessary data for the HP Operations Topology Viewer because each domain controller, as you know, has information that has been replicated across the forest on partitions, sites, site links, servers, and connections.

To launch the HP Operations Topology Viewer tool:

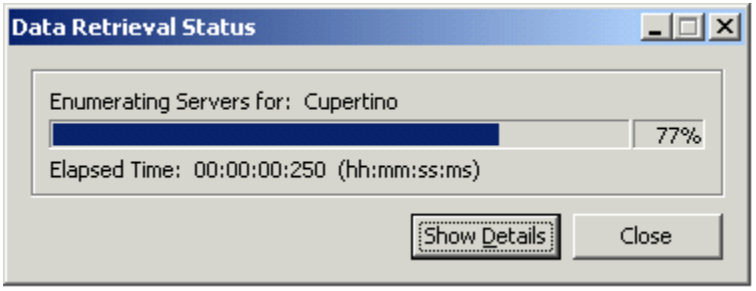
1. At the OVO/HPOM console select **Operations Master→Tools→SPI for Active Directory**.
2. Double-click **HP Operations Topology Viewer**.
3. In the window that appears, from the Connection menu select **Connect to Server...**.

   (You can also right-click on the root node of the tree.)

4 In the Connect to Server window enter the requested information and click **OK**.

If the HP Operations Topology Viewer system is running in the same domain as the domain controller to which you are connecting, you need enter only the DNS name or IP address of the domain controller if, as the logged-in user, you have the appropriate rights. In such cases, no alternate credentials are required.

Figure 14 Data retrieval progress.



Getting Started with the HP Operations Topology Viewer

Each time you launch the Viewer and make the server connection, you are presented with two window panes that represent the information gathered from the server. Even though some of the information is the same, the dual-paned window affords you two views.

On the left, you see folders containing partition, site, and site link information. On the right, you see the three-dimensional map that places the sites and site links within a context. While the left window lists components, the right pane shows the relationships among those components.

Site link cost: Site links, in addition to showing the connections between sites, show the associated "cost" of each connection. Site links with a lower cost are able to replicate data between those sites more easily than those site links showing a higher cost.

The initial view: The map shows only site links (represented by straight green lines), which are user-defined. These links are the foundation on which the Active Directory is able to build connections between servers.

Servers that function as InterSite Topology Generators (ISTGs) are identified with an "i," while servers that provide global catalog services display a "GC." To display the server connections (represented by curved blue lines), select View→Connections→Intersite (or Intrasite).

Red (error) connection lines in map: Any server connection shown as a red line indicates an error. The error situation could be due to a domain controller that has been removed from the site, but whose connection object still remains on the inbound domain controller. This connection object could have been user created (system administrator) or KCC created. In either case, the connection object should be manually removed.

Accessing functions: The HP Operations Topology Viewer's features can be accessed through its *menu commands*, its *toolbar buttons*, or by *mouse right-clicks* within areas of either side of the window pane. For a complete menu and toolbar descriptions, please refer to the SPI for Active Directory online Help.

Manipulating the 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 follows:

Table 1 Modifying the HP Operations Topology Viewer

Tree/map modification	How to do it
To move sites to different locations on the map.	Drag and drop the site to desired map tiles.
To move servers.	Drag and drop to desired tiles within the site.
To move the entire map.	Press the middle button or press both right/left mouse buttons together; drag and release.
To display server or site labels.	From the View menu select **Labels**→ **Servers** *or* **Sites**
To increase/decrease the size of the row/columns in the map's grid.	Right-click the unused space on or off the map and select **Map Properties**.

Table 1 Modifying the HP Operations Topology Viewer (cont'd)

Tree/map modification	How to do it
To find a site or server in the tree.	On the map, right-click the site or server on the map and select **Find Site/Find Server** in Tree. (Label appears in blue text.)
To find a server in the map.	In the tree, right-click on the site or server and select Find Site/Find Server on Map. (Label appears in blue text.)
Move a site outside the map area (two 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.

Using the keyboard to move around the map.

Table 2 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).

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: By right-clicking a server in either the tree or the map, you can open that server’s properties sheet, where you can view:

- Identification: Shows the GUID assigned to the server, its fully qualified domain name, distinguished name, date created, the operating system and OS version, and (if applicable) service pack and hot fix (as appropriate).
- Status: AD server type (for example global catalog and bridgehead)
- Partitions: Shows all named components associated with the server as displayed in the HP Operations Topology Viewer tree, grouping them either within the master read-write components, or the replicating read-only components.
- Replication: Shows information about completed and pending replication operations.
- Partners: Shows the replication partner(s) for the selected server.

The availability of some information in the server (DC) property sheet is dependent on the access rights of the domain account used to connect to the AD domain.

Map Properties: By right-clicking within any empty map cells (not occupied by a site), you can open the Map Properties sheet, where you can view/modify (as desired):

- Map Size: Shows the current map and tile sizes, which you can modify by using bar sliders. Use the Reset button to return to the default settings.
- Spacing: Shows the current number of columns and rows used to space sites, which you can modify by using the bar sizes. Use the Reset button to return to the default settings.

4 Reporting and Graphing

Report- and graph-generating templates are installed when you install the Microsoft Active Directory SPI. These reports cover availability/activity in *DIT*, *DNS*, *GC*, *replication*, *FSMO operations, Sysvol,* and *trust relationship changes* for each domain controller running those services.

Automatically generated every night, these Web-ready reports 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 domain controllers running master operations services. Also available for 2003 systems are reports covering trust relationship changes between domain controllers.

➤ If you use HP Reporter and it is installed on a separate system, you need to complete that installation on the Reporter system.

By showing consolidated information, available otherwise only in pieces, OVO/HPOM reporting provides you with a more complete view of how Active Directory services are performing over time.

Microsoft Active Directory SPI Reports and Data Sources

After you install the Microsoft Active Directory SPI, OVO/HPOM can generate reports using the Microsoft Active Directory SPI-collected data. These reports are generated after OVO/HPOM runs through its first nightly schedule. From that point on, you can expect to see updated reports every day since OVO/HPOM, by default, re-generates reports every night with the day's data.

➤ Customizing reports requires that you purchase **HP Reporter**. The Reporter documentation set details how to modify reports and includes a *Concepts Guide,* an *Installation and Special Configurations Guide*, online Help, and Release Notes.

Microsoft Active Directory SPI report data is collected according to metrics used for each report. This data is stored in the MS SQL “Reporter” database. The example metric formatting below (for the AD Domain Controller Availability report) shows how metric variables are identified for reporting purposes:

<report_table_name>.<Microsoft Active Directory SPI_metic_name>
as in:

ADSPI_RESPONSEMON. SYSTEMNAME

Microsoft Active Directory SPI reports are accessible from the *Reports & Graphs* area of the OVO/HPOM console. Complete descriptions of all reports and graphs are available in the OVO/HPOM online Help. The following table shows the data sources for all Microsoft Active Directory SPI reports.

Table 3 Active Directory Reports with Required Metrics

Microsoft Active Directory SPI Reports and Source Policies	Data Source Tables & Metrics
Report title: AD DIT Disk Queue Length Report **Policy:** ADSPI-DIT_DITQueueLength	**Tables:** ADSPI_Domain ADSPI_Site ADSPI_LogQueueLength **Metrics:** SYSTEMNAME INSTANCEVALUE DATETIME
Report title: AD DIT Disk Size Summary Report (weekly & monthly) **Policies:** (1) ADSPI-DIT_DITPercentFull and (2) ADSPI-DIT_TotalDitSize	**Tables:** ADSPI_DITDatabaseSize ADSPI_DITPercentFull ADSPII_Domain ADSPI_Site. **Metrics:** DATETIME INSTANCEVALUE SYSTEMNAME

Microsoft Active Directory SPI Reports and Source Policies	Data Source Tables & Metrics
Report title: AD DC DNS Availability Report (daily and weekly) **Policy:** ADSPI-DNS_DC_RESPONSE	**Table:** ADSPI_DNS_DCRESP **Metrics:** DATETIME RESPONSETIME
Report title: AD DNS Server Availability Report (daily and weekly) **Policy:** WINOSSPI-DNS_ServerResponse	**Table:** WINOSSPI_DNS_SVRRESP **Metrics:** DATETIME RESPONSETIME ISDOMAINCONTROLLER
Report title: AD DNS Server Memory Capacity Planning Report (weekly and monthly) **Policy:** WINOSSPI-DNS_LogDNSPagesSec	**Table:** WINOSSPI_DNS_SVRPLAN **Metrics:** DATETIME PAGESSEC(Avg) PAGESSEC (Max) PAGESSEC (Min)
Report title: AD Domain Controller Availability **Policy:** ADSPI-Response_Logging	**Table:** ADSPI_RESPONSEMON **Metrics:** SYSTEMNAME DATETIME
Report title: AD GC Rep Delay Times (DC to GC(s) and GC to DC(s) **Policies:** (1) ADSPI-Rep_Modify_User_Object (must be deployed to all domain controllers); (2) ADSPI-Rep_GC_Check_and_Threshold (must be deployed to all global catalog servers).	**Table:** ADSPI_REP_GC **Metrics:** SYSTEMNAME DATETIME LATENCYDELTA

Microsoft Active Directory SPI Reports and Source Policies	Data Source Tables & Metrics
Report title: AD GC Response Times (weekly and monthly) **Policy:** ADSPI-Reponse_Logging	**Tables:** ADSPI_RESPONSEMON ADSPI_REP_GC **Metrics:** SYSTEMNAME DATETIME (Date) GCPRESENT GCBINDTIME QUERYTIME
Report title: AD Log Files Disk Queue Length **Policy:** DSPI-DIT_LogFilesQueueLength	**Tables:** ADSPI_Domain ADSPI_Site ADSPI_LogQueueLength **Metrics:** SYSTEMNAME INSTANCEVALUE DATETIME
Report title: AD Log Files Disk Size Summary (weekly and monthly) **Policy:** ADSPI-DIT_LogFilesPercentFull	**Tables:** ADSPI_LogDiskSize ADSPI_Domain ADSPI_Site ADSPI_LogPercentFull **Metrics:** DATETIME INSTANCEVALUE INSTANCENAME

Microsoft Active Directory SPI Reports and Source Policies	Data Source Tables & Metrics
Report title: AD Operations Master Connection Time (by FSMO and by server) **Policies:** ADSPI-FSMO_NAMING_Bind (& Ping), ADSPI-FSMO_PDC_Bind (& Ping), ADSPI-FSMO_SCHEMA_Bind (& Ping), ADSPI-FSMO_INFRA_Bind (& Ping), ADSPI-FSMO_RID_Bind (& Ping). **NOTE:** *FSMO reports* graphically represent connections in both ping and bind measurements. The ping time measures the network connection time. Bind time measures the time between the ping connection and the connection to the targeted Active Directory service.	**Table:** ADSPI_FSMO_MET **Metrics:** FSMO GMT PINGTIME BINDTIME
Report title: AD Size of Sysvol Report (weekly and monthly) **Policy:** ADSPI-Sysvol_PercentFull	**Table:** ADSPI_SYSVOL_PCT_FULL **Metrics**: SYSTEMNAME DATETIME INSTANCENAME (SysVolFilePath) INSTANCEVALUE (SysvolDriveFreeSpace)
Report title: AD Domain and Forest Changes (weekly and monthly) **Policies:** ADSPI-Trust_Mon_Add_Del ADSPI-Trust_Mon_Modify	**Table:** ADSPI_TRUST **Metrics**: DATETIME CHANGETYPE TRUSTEDDOMAIN TRUSTATTRIBUTES TRUSTDIRECTION TRUSTSTATUSSTRING TRUSTTYPE TRUSTINGDOMAIN

Using Microsoft Active Directory SPI with HP Reporter

If you use HP Reporter, you can install the Microsoft Active Directory SPI reports on the Reporter system so that you can customize them and apply them, as desired, to groups of systems and single systems.

Install Report Package

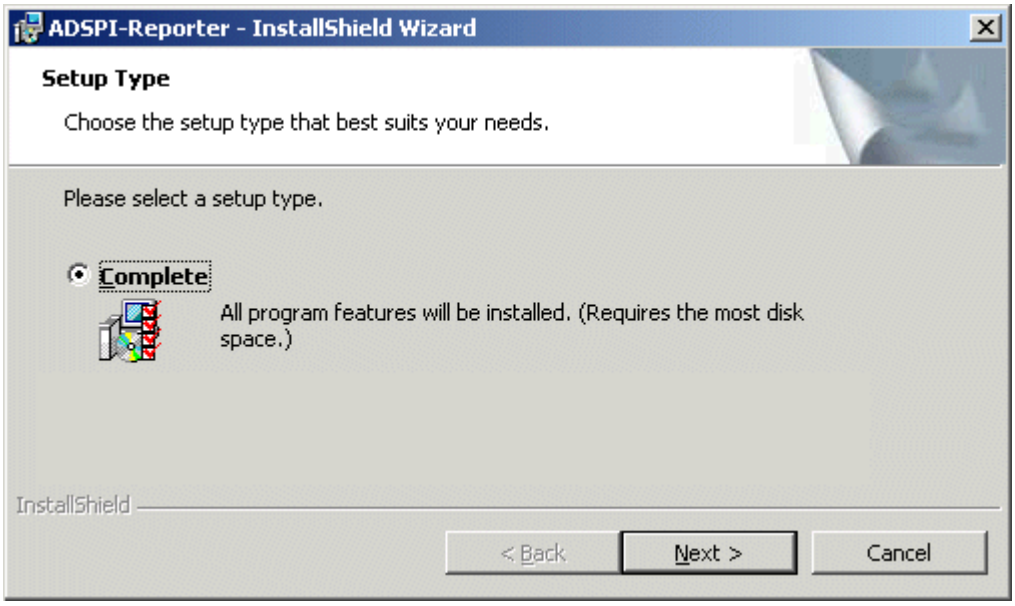
If Reporter and OVO/HPOM for Windows are installed on the same system, no separate installation for the Microsoft Active Directory SPI is necessary (as described in the tasks below).

However, stand-alone Reporter installations require that you run the ADSPI-Reporter.msi set up. This setup installs the Microsoft Active Directory SPI report package within Reporter.

To install the Microsoft Active Directory SPI Report Package on a Reporter standalone system:

1. Insert the OVO/HPOM for Windows Smart Plug-ins DVD.
2. Double-click the file: **ADSPI-Reporter.msi** (just as you did to install on the OVO/HPOM management server in Chapter 2).
3. In the dialog that appears, for the setup type select **Complete** and click **Next**.

Figure 15 The setup dialog allows you to install the Microsoft Active Directory SPI Reporter templates on a standalone Reporter system.



In the dialog that appears, you are updated as to the installation progress.

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

Microsoft Active Directory SPI Reports are automatically assigned to the ALL group in the Reporter main window. (See the preceding section Microsoft Active Directory SPI Reports and Data Sources on page 67 for OVO/HPOM Report list.)

5 Add group and single system reports by assigning reports as desired.

Reports are available for viewing the following day.

Group and single system Microsoft Active Directory SPI reports require that you identify systems by their full name; for example, **abc.xyz.com** is acceptable while **abc** is not.

Instructions are available in the 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 Reporter main window and

right-click it. Select **Report Help** or **Discovered Systems Help** from the submenu 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.

Microsoft Active Directory SPI Graphs and Data Sources

The Microsoft Active Directory SPI also includes graphs available in the OVO/HPOM console in Reports & Graphs→Graphs→SPI for Active Directory. OVO/HPOM graphs differ from reports in that you manually generate them and then view data that is more immediate and granular in nature.

Microsoft Active Directory SPI graphs, which consolidate collected data, are listed in the following table.

Graphs showing response times are meant to aid you in establishing baseline values for setting thresholds in other policies.

Table 4 Active Directory Graphs and Source Policies

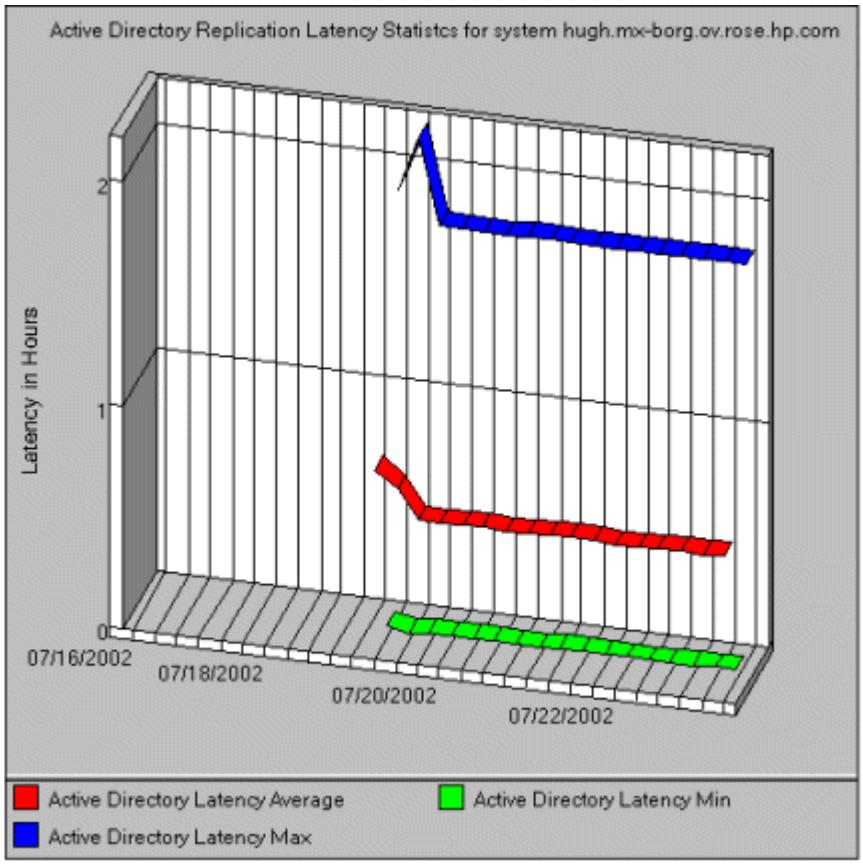
Microsoft Active Directory SPI Graphs and Policies	Source Metrics
Graph Title: Active Directory Replication Latency Graph **Source Policies:** ADSPI-Rep_ModifyObj and ADSPI-Rep_Mon	**Metrics:** LatencyMin LatencyMax LatencyAvg **NOTE:** The Replication Latency Graph can be generated only when one or more domain controllers exist in a forest; a forest with a single domain controller has no replication occurring, and so no data for graphing is available.
Graph Title: Active Directory Bind Response Time **Source Policy:** ADSPI-Response_Logging	**Metrics:** GCBindTime BindTime

Microsoft Active Directory SPI Graphs and Policies	Source Metrics
Graph Title: Active Directory GC Availability **Source Policy:** ADSPI-Response_Logging	**Metrics:** GCAVAILABILITY GCQueryTime
Graph Title: Active Directory Query Response Time Graph **Source Policy:** ADSPI-Response_Logging	**Metric:** GCQueryTime
Graph Title: Active Directory Replication Time by Global Catalog **Source Policy:** ADSPI-Response_Logging	**Metric:** GCBindTime

To access the Microsoft Active Directory SPI graphs:

1. Select **Reports & Graphs→Graphs→SPI for Active Directory**.
2. Right-click the graph name, such as **Active Directory Replication Latency Graph**, and select **Show Graph...**.
3. Select the Node and Date Range and click **Finish**.

Figure 16 In the right pane, you see the graph generated by the OVO/ HPOM grapher.



5 Troubleshooting

The situations described below offer methods of solving or detecting problems that may or may not require support assistance. Please see each for the relevancy to the problem you are experiencing.

Detecting Problems Through Tracing

On occasion you may have a problem for which you cannot easily find a solution. To capture all Active Directory information, including FSMO and replication conditions, status, and errors included in the Microsoft Active Directory SPI logs, you can turn on tracing to access this information.

To turn on tracing for FSMO service consistency monitoring:

1. At the OVO/HPOM console tree, expand the **Policies grouped by type** folder and select **Scheduled Task**.
2. In the right pane double-click the policy; for example **ADSPI-FSMO_Consist**.
3. In the Command* text box, place the cursor at the end of the command and type:
   -l 1
   (a minus sign [-], the letter “l” for “log”, a blank space, and the number “1”).
4. Click **Save and Close**.
5. Re-deploy the policy to the node for which you want to conduct the trace.

To turn on tracing for FSMO service response time monitoring:

Repeat the above procedure, substituting the policy **ADSPI-FSMO_Logging**.

To turn on tracing for Replication service latency and response times.

1 At the OVO/HPOM console tree, expand the **Policies grouped by type** folder and select **Measurement Threshold**.

2 In the right pane double-click the policy:
ADSPI-Rep_Mon
or
ADSPI-Rep_Sysvol
or
ADSPI-Rep_TimeSync

3 In the Program* text box, place the cursor at the end of the command and type:
-l 1
(a minus sign [-], the letter "l" for "log", a blank space, and the number "1").

4 Click **Save and Close**.

5 Re-deploy the policy to the node for which you want to conduct the trace.

To view trace logs.

1 At the managed node start your preferred text editor.

2 Open the directory: <*installed_drive*>:`\Program Files \HP Operations\installedpackages\<GUID>\log\`

3 In the `log` directory, open the file with a log extension and a name matching the command or program executable name used in the Command* or Program text box above.
For example:
`ADSPI_consist.log`

Graphing Problems

Errors that occur when trying to generate a graph could result from the following:

Problem (graphing): Error 33, no data available for the replication latency graph.

— **Cause(s):**
(1) Replication has not had sufficient time to occur.

(2) The **user account** settings for both the agent and the policy do not match. The default setting for the agent is to run as the Local SYSTEM account. However, the default setup may have been disabled though using the Tools→Operations Manager Tools→Agent Account tool group.

Solution(s):
(1) Check the Scheduled Task policy to see how often replication latency is scheduled to occur. Wait until sufficient time elapses and then try once again to view or generate the report/graph.

(2) Check the agent account by going to **Tools→Operations Manager Tools→Show agent account**. Check the four Microsoft Active Directory SPI Scheduled Task policies to ensure their user account settings match the agent account setup on the management server. Those policies are: ADSPI-FSMO_Consist, ADSPI-FSMO_Logging, ADSPI-REP_ModifyObj, ADSPI_Response_Logging. Double-click each policy and on the Task tabbed page of the Properties, see the Task type *Command* segment and note the *Execute* setting. The $AGENT_USER selection means that the agent runs as the Local SYSTEM account. Change the agent or policies as necessary to make all user account settings match.

— **Cause**: The Active Directory forest contains only a single domain controller; as a result, no replication occurs.

Solution: No replication latency graph can be generated when this configuration exists.

Problem (graphing): Error 33, data not available for the graph.

— **Cause:** The system selected for graphing purposes is not a domain controller and therefore has no Microsoft Active Directory SPI policies deployed on it. As a result, no data is available for the graph.

Solution: N/A; no real problem exists.

Reporting Problems

Errors that occur when trying to view a report could result from the following:

Problem (reporting): No data available for reports:

- **Cause:** The policies needed for the report's data have not been deployed.
- **Solution:** Examine the policy inventory on the node in question to determine whether or not the policy is there. If not, deploy the policy.

Problem: The agent appears to be failing; that is, not collecting the data necessary for reporting.

- **Cause:** The **user account** settings for both the agent and the policy do not match. The default setting for the agent is to run as the Local `SYSTEM` account. However, the default setup may have been disabled through using the **Tools→Operations Manager Tools→Agent Account** tool group.
- **Solution:** Check the agent account by going to **Tools→Operations Manager Tools→Show agent account**. Check the four Microsoft Active Directory SPI Scheduled Task policies to ensure their user account settings match the agent account setup on the management server. Those policies are: ADSPI-FSMO_Consist, ADSPI-FSMO_Logging, ADSPI-REP_ModifyObj, ADSPI_Response_Logging. Double-click each policy and on the Task tabbed page of the Properties, see the Task type *Command* segment and note the *Execute* setting. The $AGENT_USER selection means that the agent runs as the Local SYSTEM account. Change the agent or policies as necessary to make all user account settings match.

Problem: The report "AD Domain Controller Availability Report" shows a non-global catalog server with a GC as unavailable 100% of the time.

- **Cause:** This error occurs whenever a server that hosts no global catalog services has a response-time monitoring policy deployed on it. Because no global catalog services are running, no data is available.
- **Solution:** The report is in error and no action is necessary.

Index

G

H

I

L

M

N

P

R

S

T

U

V