HP Operations Smart Plug-in for Microsoft® Active Directory

For HP Operations Manager for Windows®

Software Version: 6.10

PDF version of the online help

This document is a PDF version of the online help that is available in the Microsoft Active Directory SPI. It is provided to allow you to print the help, should you want to do so. Note that some interactive topics are not included because they will not print properly, and that this document does not contain hyperlinks.

Document Release Date: February 2009

Software Release Date: October 2008

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

Copyright Notices

Trademark Notices

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

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

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

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

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

Support

You can visit the HP Software Support Online web site at:

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

TABLE OF CONTENTS

Overview

The Smart Plug-in (SPI) for Microsoft Active Directory is plug-in or add-on software for OpenView Operations (OVO) or HP Operations Management (HPOM). It functions as a modular component of OVO or HPOM and further improves the monitoring capabilities of OVO or HPOM in managing your Active Directory environment.

The Microsoft Active Directory SPI monitors the Active Directory related conditions occurring across your network and alerts you if there are signs of dysfunctional occurrence with the following activities:

- Data consistency across the Domain Controllers (DCs)
- Availability of sufficient free space in the Active Directory database
- Timely replication process
- Systems outages capability
- Successful functioning of role masters
- DCs competing with overly utilized CPUs
- Capacity and fault-tolerance issues in Active Directorydata is accessible and 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 used CPUs,
- Active Directory is not experiencing capacity or fault-tolerance issues,
- Sysvol size and capacity is at tolerable levels,
- trust relationship changes are by design and as expected.

After you complete the Microsoft Active Directory SPI installation, you have access to **service map alerts** and **browser messages** as well as **reports** , **graphs** , a **topology map** , and **trust relationship** information that vividly represent Active Directory service use/conditions/connections.

Related Topics:

- Getting Started with the Active Directory SPI

- Microsoft Active Directory SPI Components

Getting Started

To install the AD-SPI, complete the steps as listed below. See the *Smart Plug-in for Microsoft Active Directory Configuration Guide* for detailed installation instructions.

The procedure below relates only to those Active Directory policies included in the Auto-Deploy group. No **Manual-Deploy** policies are deployed with this procedure. Manual-Deploy policies are there for you to deploy as needed from either their subgroups or individually. See Choosing a Microsoft Active Directory SPI policy for descriptions of policies within this group.

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

1. Install the Microsoft Active Directory SPI: Insert the HP Operations for Windows Smart Plug-ins DVD in the DVD-ROM drive and follow the instructions as they appear on screen.
2. For *managed* nodes (those already appearing in the managed tree), deploy the AD-SPI Auto-Deploy (service discovery) policies:
   — Select **Policy Groups → SPI for Active Directory** . Right-click **Auto-Deploy** and select **All Tasks → Deploy on...** .
   —Select nodes running Active Directory Server services.
3. For *unmanaged* nodes, right-click **Nodes** and select **Configure→Nodes** . Drag and drop those nodes that are running Active Directory services from the Discovered Nodes tree to the Managed Nodes tree.
   (AD-SPI service discovery policies are automatically deployed on the added nodes after you click **OK** or Apply in the Configure Nodes dialog.)

Result: As services are discovered on the nodes, policies relevant to those services are deployed. Those policies can then monitor Active Directory processes, reporting on status/problems through service map alerts and messages in the HPOM browser.

NOTE: Reports are available the day following your installation. Using the previous day's data, HPOM generates Active Directory reports each night. **Graphs** are available through two methods: (1) manual generation where you can select a graph under the console's Graphs area and (2) through an Operator action associated with a message. You can also use the **HP Operations Topology Viewer** to display Active Directory components (in the details pane of the console) as well as a map that shows the DC connections (in the contents pane of the console).

Related Topics:

- Microsoft Active Directory SPI Components
- Microsoft Active Directory SPI Overview

>

Components

The Microsoft Active Directory SPI installation/configuration adds components to the HPOM console tree (left pane) as follows:

Services →Systems Infrastructure ... Domains: DC:<domain_controller_name> When you select to manage a node, AD-SPI Discovery policies are deployed to that node. This adds any discovered services to the HPOM Services tree.
To view: select Services→ Systems Infrastructure→Windows→Active Directory→Domains→ DC:<dc_name>→Services.

In the right pane, the service map graphically represents the discovered DIT, DNS, operations masters/replication, and GC services running on the Active Directory domain controllers. You can view the service map by clicking any item under the Services folder.

Tools→ SPI for Active Directory:

→ **HP Operations Topology Viewer :** The Topology Viewer tool supplies information about Active Directory forests, partitions, sites, and the relationships between sites and servers in each forest. The left pane of the console display shows the hierarchy contained in one or more forests; the map in the right pane shows the selected forest topology. (The map shows only one forest at a time.)
To use the tool: at the console expand the folders **Tools →SPI for Active Directory** folder. Double-click Topology Viewer to launch the Topology Viewer window. From the File menu select **Add Forest...** and enter the fully qualified DNS name of the Domain Controller (or its IP address).
△ **Advanced Exchange Data Collection:** If you click this check box, the gathering of additional Exchange data significantly impacts the efficiency of the Active Directory display generation. You may need to wait possibly hours, depending on the size of your environment, for the process to complete.

→ **AD Trust Relationships :** This tool supplies information about trust relationships for a domain. In a Windows 2003 Server environment, it reports both two-way trusts within a forest and trusts from one forest to another for the selected nodes. In a Windows 2000 Server environment, it displays only the two-way trusts within a forest.

→**AD DC Demotion Preparation :** This tool is intended for use after you have installed the Microsoft Active Directory SPI and have begun using it. Use the tool before demoting any domain controller in your Active Directory environment to prevent the Microsoft Active Directory SPI from continuing to monitor the DC's services.

→ **Check ADS Service** : This tool connects to the ADS service of the specific node using the Microsoft Active Directory SPI.

→ **ADS Printer Information** : This tool creates a list of all printers known in the Active Directory.

→**AD Self-Healing Info** : This tool gathers error-relating data for troubleshooting operational SPI problems.

→**Self-Healing Verification** : This tool verifies the version of the ADSPI instrumentation (executables). When launched on a managed node, the tool reports to the console if there are differences in the version of Microsoft Active Directory SPI and the Microsoft Active Directory SPI executables present on the system.

Policy groups: SPI for Active Directory — Active Directory SPI-specific policy groups are grouped for easy service discovery and policy deployment under the **Auto-Deploy** group. You need only deploy the Auto-Deploy group to all managed nodes. Then whatever Active Directory services are discovered on those nodes automatically trigger the deployment of relevant policies. The **Manual-Deploy** group is also included for you to choose from among the subgroup or individual policies for those appropriate to your Active Directory environment needs. Descriptions are available of the individual policies in Choosing a Microsoft Active Directory SPI policy .

Reports: SPI for Active Directory — Active Directory-specific reports include daily, weekly, and monthly updates. In most cases, they are updated every night. After you have installed the AD-SPI, you can view the Web-based reports the following day.

Graphs: SPI for Active Directory — Like the reports area, AD-SPI offers Active Directory-specific graphs. You can generate the graph of your choice by selecting **Graphs→SPI for Active Directory** . In the right pane right-click the graph name and selecting **Show Graph...** .

Related Topics:

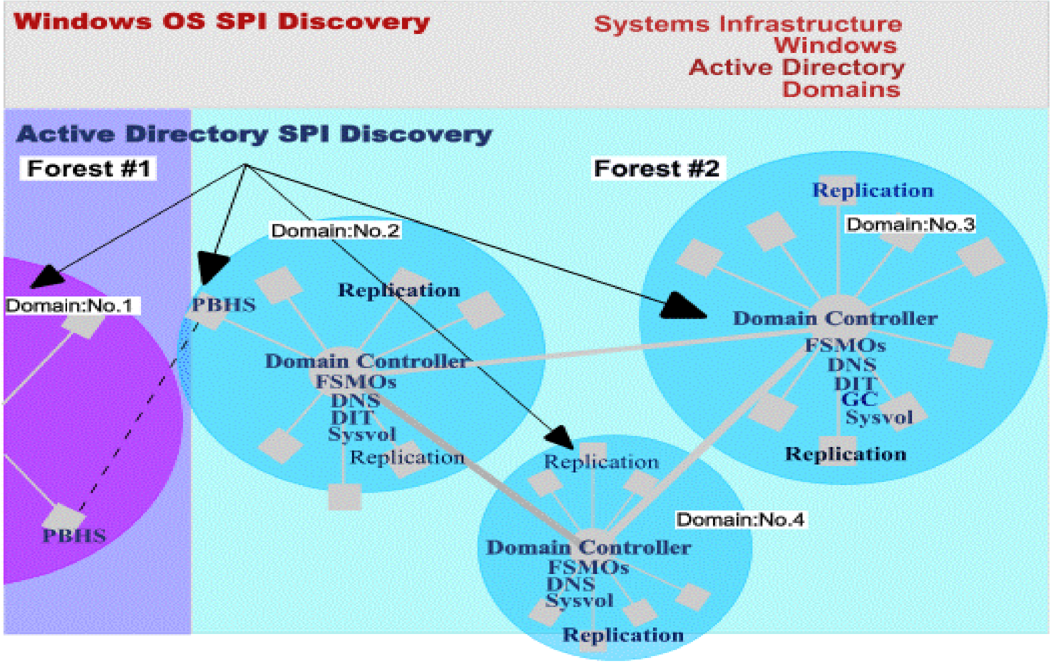
- Getting Started with the Active Directory SPI
- Microsoft Active Directory SPI Policy Catalog
- Choosing a Microsoft Active Directory SPI policy

Service/Component Discovery

When you deploy the AD-SPI **Auto-Deploy** group, all service discovery policies are deployed. These policies discover the services and components associated with each domain controller (DC), which can include Active Directory DIT, DNS, replication, preferred bridgehead servers (PBHS), global catalog hosting servers (GC), SysVol, and FSMO components.

See Getting Started for the two service discovery methods—for managed and unmanaged HPOM nodes.

The discovery process finds these Active Directory services and components, then maps them in a graphical map of your network environment, see the example in the diagram below.



Related Topics:

- Getting Started with the Active Directory SPI
- Microsoft Active Directory SPI Components

Policies

The Microsoft Active Directory SPI policies are duplicated but organized differently in the HPOM *Policy groups* and the *Policies grouped by type* folders. The policy organization within these two groups is as follows:

Policy management (Policy groups) : The SPI for Active Directory group organizes policies according to discovery and the types of services monitored. The groups are as follows:

- **SPI for Active Directory:** All Microsoft Active Directory SPI policy subgroups can be found under this group. You can use the group or one of its subgroups to deploy policies in one step. The top-level subgroup (containing all other groups) is:
    - **Auto-Deploy** : Deploy this group on nodes to discover services and automatically deploy relevant policies (FSMO and Replication Monitoring). The Auto-Deploy group is automatically deployed on any unmanaged node after it is added to the HPOM Nodes folder. FSMO and Replication Monitoring are also part of this group and are deployed as appropriate to relevant discovered services.
    - **Manual-Deploy** : The Windows OS SPI service discovery automatically discovers the Active Directory services associated with these policies, but deployment of the policies is not automatic. You can deploy these policies as necessary either individually or as a group.

Policy Types (Policies grouped by type) : All individual Microsoft Active Directory SPI policy names begin with "ADSPI" and are easy to find in the console details pane after selecting from one of the relevant categories listed below:

- **Service Auto-Discovery** : Includes one discovery policy each for detecting Active Directory replication and Active Directory master operations (FSMO) services.
- **Scheduled Task policies** : Determine how often Active Directory processes/states are monitored. Monitoring intervals can be defined in minutes, hours, or days.
- **Measurement Threshold policies** : Define conditions to monitor, including severity levels associations. When a defined condition occurs, depending on its severity level, a service map alert may be displayed and a message sent to the HPOM message browser.

Related Topics:

- Getting started
- Choosing a Microsoft Active Directory SPI policy
- Policy catalog

Choosing a Microsoft Active Directory SPI policy

The complete list of Microsoft Active Directory SPI policies appears below. To view a list of policies that monitor a particular Active Directory service, select from the drop-down menu and click the **Filter** button.

For example, to check the threshold of a policy monitoring replication (for example, ADSPI-Rep_GC_Check_and_Threshold), select Global Catalog in the first drop-down list, and Measurement Threshold in the second drop-down list, and click Filter.

Select an Active Directory service area (scroll to see all):

Any

Select a policy type:

Any

Enter a full or partial policy name (optional):

Filter Loading policies...

Show short descriptions

Policy: ADSPI_Discovery

Description

This policy performs the discovery of Active Directory from **System Infrastructure** through **Domain Controller -> Services** . It makes use of *OvAdsDisc.exe* to discover all AD components.

Type

Scheduled Task

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Basic Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Basic Discovery

Details

Policy: ADSPI-AutoDiscovery_Delete

Description

Deployed automatically with other discovery policies, this policy verifies the continued presence of an already discovered service on each domain controller. Whenever a previously discovered service is detected as no longer present on the domain controller, this policy starts the process of removing the service from the console tree and the service map. After five verifications (which—by default—takes five hours), the removal occurs. The ADSPI-AutoDiscovery_Delete policy ensures that the HPOM console's Services tree and Service Map stay up to date if ever a service is shifted from one domain controller to another.

Type

Scheduled Task

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-AutoDiscovery_DIT (ADSPI-AutoDiscovery_DIT_2k8+)

Description

This policy runs the auto discovery program for Directory Information Tree (DIT) services. The policy is deployed to all HPOM managed nodes, where it searches for DIT services on the DC. When discovered, DIT is shown under the DC name and also with the DC in the service map.

Result: The discovered service results in the automatic deployment of relevant Microsoft Active Directory SPI DIT policies on the HPOM managed node. With the DIT-related services policies deployed to the node, the system detects potential problems developing with the DIT for each DC.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-AutoDiscovery_DNS (ADSPI-AutoDiscovery_DNS_2k8+)

Description

This policy runs the auto discovery program for DNS services. This policy is deployed to all HPOM managed nodes, where it searches for DNS services on the DC. When discovered, DNS is shown under the DC name and also with the DC in the service map.

Result: The discovered service results in the automatic deployment of relevant Active Directory-SPI DNS policies on the HPOM managed node. With the DNS-related services policies deployed to the node, the system can then be monitored for DNS service health.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-AutoDiscovery_FSMO (ADSPI-AutoDiscovery_FSMO_2k8+)

Description

This service discovery policy runs the auto discovery program for FSMO monitoring. The policy searches for Active Directory FSMO services including PDC Master, RID Master, Infrastructure Master, Schema Master, and Domain Naming Master.

Result: If the domain controller is identified as a host for any FSMO service, that FSMO service appears under the DC name in the console tree as well as with the DC name in the service map. Discovered services also result in the automatic deployment of relevant FSMO policies on the system.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-AutoDiscovery_Rep (ADSPI-AutoDiscovery_Rep_2k8+)

Description

This policy runs the auto discovery program for Active Directory replication monitoring. The policy searches for Active Directory replication and replication-related services including Sysvol, inbound replication objects, and time synchronization.

Result: The discovered services result in deployment of relevant Microsoft Active Directory SPI replication monitoring policies on the HPOM managed nodes. The domain controller can then be checked and message alerts sent when problems appear in services having to do with replication.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-AutoDiscovery_PBHS

Description

This schedule policy runs the auto discovery program for Preferred Bridgehead Server Monitoring within replication.

Preferred Bridgehead Servers, one per site, provide the communication links between sites. Within each site the KCC automatically designates a single server as the bridgehead server to perform site-to-site replication. Subsequent replication occurs by replication within a site.

When you establish site links, you can designate the bridgehead servers that you want to receive replication between sites. By designating a specific server to receive replication between sites, rather than using any available server, you can specify the most beneficial conditions for the connection between sites. Bridgehead servers ensure that replication can occur more frequently within the site than between the sites.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-AutoDiscovery_GC (ADSPI-AutoDiscovery_GC_2k8+)

Description

This policy runs the auto discovery program for the Active Directory Global Catalog (GC). The policy searches for hosted Global Catalog services.

Result: If the domain controller hosts the Global Catalog, then GC displays under the DC name in the console details pane as well as in the service map. The discovered service also results in the automatic deployment of Microsoft Active Directory SPI GC policies on the HPOM managed node so that the domain controller can be monitored for potential global catalog service problems.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI-DIT_DITPercentFull

Description

This policy helps address the common problem that occurs when the size of the DIT file increases and goes unobserved, while the available free space on the DIT hosting disk drive decreases. This policy calculates the percentage full of the drive hosting the DIT, logs, and thresholds on the data.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DIT Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring

Details

Policy: ADSPI-DIT_DITQueueLength

Description

The DIT log files queue size shows the number of operations pending against the DIT log files drive. When this number is higher than zero for a sustained period of time, it indicates that the particular volume on which the DIT log files reside is unable to handle the number of necessary updates.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DIT Monitoring Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring

Details

Policy: ADSPI-DIT_LogfilesPercentFull

Description

This policy calculates the percentage full of each drive hosting the DIT log file. The policy logs the information and also checks for an exceeded threshold.

A common problem occurs when the DIT logfile expands over time and goes unobserved, while the available free space on the disk drive which hosts the DIT logs decreases. This policy calculates the percentage amount occupied by the DIT logfiles in proportion to the drive hosting the DIT.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DIT Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring

Details

Policy: ADSPI-DIT_LogfilesQueueLength

Description

The DIT log files queue size shows the number of operations pending against the DIT log files drive.

When this number is higher than zero for a sustained period of time, it indicates that the particular volume on which the DIT log files reside is unable to handle the number of necessary updates.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DIT Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring

Details

Policy: ADSPI-DIT_TotalDITSize

Description

The Active Directory database file, or DIT, can cause problems when it expands over time and no one has been watching it. This policy monitors the size of the Active Directory database and the amount of remaining free disk space on the logical drive where Active Directory database resides.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DIT Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring

Details

Policy: ADSPI-DNS_DC_A_Chk

Description

This policy checks the 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 another for the domain that it serves. If one or both records are missing the policy generates a critical message.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS

Monitoring

Details

Policy: ADSPI-DNS_DC_CNAME_Chk

Description

This policy verifies that the domain controller can be located through use of its alias. The policy does this by verifying the domain controller's GUID alias, using: < *Domain_Controller GUID* → ._msdcs.<*Domain* →

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_DC_Response

Description

This policy alerts the user when DNS queries made by the domain controller result in an unexpected response or an unacceptable response time. This policy contains threshold settings for a specified allowable time and when exceeded, sends a message to the HPOM browser.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring Or,
SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_Extra_GC_SRV_Chk

Description

This policy checks for extra or missing records that register the domain controller as a global catalog host on multiple sites.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_Extra_Kerberos_SRV_Chk

Description

This policy checks for records that register the domain controller as a Kerberos KDC on multiple sites

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_Extra_LDAP_SRV_Chk

Description

This policy checks for records that register a domain controller as an LDAP server on multiple sites.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_GC_A_Chk

Description

This policy checks DNS for a domain controller hosting global catalog services. It does this by looking for the DNS host record (A record) associated with a domain controller that hosts the global catalog.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_GC_Missing

Description

This policy checks the forest for at least one registered global catalog in DNS. Without access to the forest's global catalog, an Active Directory environment becomes unusable. The user should be notified if DNS is showing no path to a forest's global catalog. Even though this policy is deployed to all managed domain controllers, it runs only on the PDC emulator for the forest's root domain to minimize monitoring time.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_GC_SRV_Chk

Description

This policy checks DNS for a domain controller hosting global catalog services. It does this by looking for the DNS service record (SRV record) associated with a domain controller that hosts the global catalog.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_GC_StrandedSite

Description

Without access to the forest's global catalog, an Active Directory environment becomes unusable. This policy generates a warning message when no domain controller within the Active Directory site can provide access to the global catalog. This situation occurs when an Active Directory site relies completely on one or more other sites (meaning inter-site connections) for Global Catalog access.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_Island_Server

Description

Replication problems can occur when a Domain Controller has been configured to use itself as a DNS server. When such problems occur, the domain controller\DNS server is referred to as an 'island' (see Microsoft Knowledge Base article Q275278 for more information on the 'island' problem). This policy checks for potential 'island' problems.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_Kerberos_SRV_Chk

Description

Active Directory domain controllers hosting Kerberos authentication services make their services visible through Service Resource Records (SRV records), which are generated when the service is registered in the DNS.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-DNS_Obsolete_GUIDs

Description

Each Domain Controller is registered in DNS under two GUIDs:(1) a GUID referring to itself and (2) a GUID referring to the domain it serves. When a domain controller is demoted, its GUID alias can remain in DNS, even though it refers to nothing. The same situation can occur when a domain is removed from the Active Directory environment. Because obsolete GUIDs can create replication problems, this policy checks for them.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DNS Monitoring

Details

Policy: ADSPI-FSMO_Consist

Description

A scheduled task policy that performs configuration checks. First the policy identifies the FSMO master operations running on the domain controller (DC); then the policy verifies that the information is also present on the DC's replication partner.

Replication problems can occur when a domain controller is demoted from a domain and its master operation roles are not transferred to another domain controller. Such a situation can happen if the domain controller is not properly demoted or is taken off line without transferring role responsibilities. In such cases, master operation identification becomes inconsistent. This policy ensures that inconsistencies are known.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_GC_Infra_Check

Description

With the help of the ADSPI-FSMO_GC_Infra_Check policy, the Microsoft Active Directory SPI sends alert messages to the HPOM console if a domain controller with the Infrastructure Master role is found to be a global catalog server.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_Consist_INFRA

Description

The ADSPI-FSMO_Consist_INFRA policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_INFRA alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the INFRA Master FSMO role.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_Consist_NAMING

Description

The ADSPI-FSMO_Consist_NAMING policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_NAMING alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the Naming Master FSMO role.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_Consist_PDC

Description

The ADSPI-FSMO_Consist_PDC policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_PDC alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the PDC FSMO role.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_Consist_RID

Description

The ADSPI-FSMO_Consist_RID policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_RID alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the RID Master FSMO role.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_Consist_SCHEMA

Description

The ADSPI-FSMO_Consist_SCHEMA policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_SCHEMA alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the Schema Master FSMO role.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_INFRA_Bind

Description

Measures the bind response time of the Infrastructure FSMO. The policy periodically binds to the domain controller that is the infrastructure master.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_INFRA_Ping

Description

This policy measures the general responsiveness of the infrastructure master by periodically pinging the domain controller that is the infrastructure master.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_Logging

Description

A scheduled task policy that binds and pings each of the five FSMO role holders. It logs the bind and ping response times, and sends the response times to the appropriate ADSPI-FSMO_(role)_Ping and ADSPI-FSMO_(role)_Bind policies.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_NAMING_Bind

Description

Receives information from the ADSPI-FSMO_Logging policy, on which it can alarm when the bind time exceeds the configured threshold.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_NAMING_Ping

Description

Receives information from the ADSPI-FSMO_Logging policy, on which it can alarm when the ping time exceeds the configured threshold.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_PDC_Bind

Description

Receives information from the ADSPI-FSMO_Logging policy, on which it can alarm when the bind time exceeds the configured threshold.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_PDC_Ping

Description

Receives information on the PDC from the ADSPI-FSMO_Logging policy, on which it can alarm when the ping time exceeds the configured threshold.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_RID_Bind

Description

Receives information on the RID FSMO from the ADSPI-FSMO_Logging policy, on which it can alarm when the bind time exceeds the configured threshold.

This policy works in conjunction with the ADSPI-FSMO_Logging policy.

Details

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Policy: ADSPI-FSMO_RID_Ping

Description

Receives information on the RID FSMO from the ADSPI-FSMO_Logging policy, on which it can alarm when the ping time exceeds the configured threshold.

This policy works in conjunction with ADSPI-FSMO_Logging policy.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_SCHEMA_Bind

Description

Receives information on the SCHEMA FSMO from the ADSPI-FSMO_Logging policy, on which it can alarm when the bind time exceeds the configured threshold.

Works in conjunction with the ADSPI-FSMO_Logging policy.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_SCHEMA_Ping

Description

Receives information on the SCHEMA FSMO from the ADSPI-FSMO_Logging policy, on which it can alarm when the ping time exceeds the configured threshold.

This policy works in conjunction with the scheduled task policy: ADSPI-FSMO_Logging.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_RoleMvmt

Description

This scheduled task policy runs once every hour to determine if the domain controller it is running on has gained or lost one of the five FSMO roles. This policy works in conjunction with the five measurement threshold policies focusing on role movement.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_RoleMvmt_Infra

Description

Monitors the domain controller's ownership of the Infrastructure Master FSMO role. To work, this policy requires the deployment of the ADSPI-FSMO_RoseMvmt scheduled task policy.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO

Monitoring

Details

Policy: ADSPI-FSMO_RoleMvmt_Naming

Description

Monitors the domain controller's ownership of the Domain Naming Master FSMO role. To work, this policy requires the deployment of the ADSPI-FSMO_RoseMvmt scheduled task policy.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_RoleMvmt_PDC

Description

Monitors the domain controller's ownership of the PDC Emulator FSMO role. To work, this policy requires the deployment of the ADSPI-FSMO_RoseMvmt scheduled task policy.

Default Policy Group

SPI for Microsoft Active Directory → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_RoleMvmt_RID

Description

Monitors the domain controller's ownership of the RID Master FSMO role. To work, this policy requires the deployment of the ADSPI-FSMO_RoseMvmt scheduled task policy.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-FSMO_RoleMvmt_SCHEMA

Description

Monitors the domain controller's ownership of the RID Master FSMO role. To work, this policy requires the deployment of the ADSPI-FSMO_RoseMvmt scheduled task policy.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Details

Policy: ADSPI-Rep_GC_Check_and_Threshold

Description

Monitors delay times of global catalog inter- and intra-site replication. Delays can be measured by means of a timestamp available from an object created by the ADSPI-Rep_Modify_User_Object policy. This object, which contains a timestamp, is created specifically for the DC\GC on which it is deployed. After it is created, the object timestamp can be modified by the ADSPI-Rep_Modify_User_Object policy. Since global catalog policies are deployed to every DC\GC, each DC\GC has a specific object stored in the global catalog.

The ADSPI-Rep_GC_Check_and_Threshold policy checks the current timestamp against the timestamp of objects created by other DC\GCs in the forest. An alarm occurs whenever the timestamp on any of those objects is more than 24 hours old, meaning that replication has not occurred from that DC\GC for more than 24 hours.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → GC Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → GC Monitoring

Details

Policy: ADSPI-Rep_CheckObj

Description

Checks that an HPOM replication object exists for all domain controllers. The AD-SPI monitors replication latency by inserting an object into Active Directory and measuring the amount of time required to replicate an attribute through the Active Directory forest. This policy works in conjunction with the ADSPI-Rep_Modify_User_Object policy (none of the two policies should be deployed without the other one).

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_InboundObjs (ADSPI-Rep_InboundObjs_2k8+)

Description

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.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_ISM_Chk

Description

This policy monitors the status of the "InterSite Messaging" service. It checks whether the service is running or not and how many processes of this service are running. If this service does not run properly, then inter-site replication might have problems and the KCC will be unable to calculate the replication topology.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_Mon_Fwd_Ping_Messages

Description

This is an Open Message Interface policy which forwards the alert messages sent by ADSPI_RepMon.exe to the HPOM Console. This policy helps to form the message correlation key.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_Delete_OvRep_Object

Description

The ADSPI-Rep_Delete_OvRep_Object policy automatically deletes the "OvReplication" and "OvReplication-<DCName>" objects from a domain controller if their timestamps are not updated for a certain period of time.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_Modify_User_Object

Description

This scheduled task policy creates and updates a user object on the domain controller hosting the policy. This policy is deployed to all managed domain controllers.

This scheduled task policy provides the means for checking replication as measured by the **ADSPI-GC_Check_and_Threshold** policy, which monitors the delay times of global catalog inter-site and intra-site replication.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-REP_ModifyObj

Description

This scheduled task policy creates and updates an object on the domain controller hosting the policy. This policy is deployed to all managed domain controllers as a means for checking replication as measured by the following policies:

- The Rep_Mon policy: verifies timely replication between DC replication partners.
- The Rep_CheckObj policy: verifies the object's existence on the DC's replication partners. If the object is missing, the policy generates a message.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_TimeSync

Description

This 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 HPOM console. If the delta is 4 minutes or more, the policy generates a warning; 5 minutes or more it generates a critical alert.

Windows 2000 uses a time service, known as Windows Time Synchronization Service (Win32Time), to ensure that all Windows 2000 computers on a network use a common time. This service is required and therefore crucial to Windows 2000s default authentication processes (which uses Kerberos protocol).

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_MonitorIntraSiteReplication

Description

This policy monitors whether replication is happening between the DCs having connection objects in the same site.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Rep_MonitorInterSiteReplication

Description

This policy monitors whether replication is happening between the bridge-head servers of sites.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Replication Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Replication Monitoring

Details

Policy: ADSPI-Response_Logging

Description

This scheduled task policy logs Active Directory response times. The logged response times are available for graphing purposes.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Response Time Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Response Time Monitoring

Details

Policy: ADSPI-ResponseTime_Bind

Description

This policy periodically binds to Active Directory and measures latency, which is important in assessing the general responsiveness of Active Directory. A significant increase in the bind and query time indicates that something needs to be investigated. A DC may have gone down and queries are being directed to another DC over a WAN link, or a DC is having resource contention.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Response Time Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Response Time Monitoring

Details

Policy: ADSPI-ResponseTime_GCBind

Description

Measures the time required for the domain controller to bind to the Active Directory GC (Global Catalog). The global catalog, which is a partial replica of every domain directory in the forest, is used to quickly find an object in Active Directory. The global catalog contains an entry for every object in the forest but does not store every property for every object. Instead it contains only the properties that are marked in the schema for inclusion in the global catalog. Only domain controllers can serve as global catalog servers.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Response Time Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Response Time Monitoring

Details

Policy: ADSPI-ResponseTime_GCQuery

Description

Monitors the global catalog query response time of Active Directory by measuring the time required to perform a global catalog search.

The global catalog is used to quickly find an object in Active Directory. It is a partial replica of every domain directory in the forest. The global catalog contains an entry for every object in the forest, but does not store every property for every object. Instead it contains only the properties, which are marked in the schema for inclusion in the global catalog. Only domain controllers can serve as global catalog servers.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Response Time Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Response Time Monitoring

Details

Policy: ADSPI-ResponseTime_Query

Description

Measures the time required for the Active Directory queries. It periodically queries Active Directory and monitors latency. Monitoring the general responsiveness of Active Directory is important because significant increases in the amount of time required for binding then querying can indicate a serious problem. For example, a DC may have gone down and queries are being directed to another DC over a WAN link, or a DC is running hot.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Response Time Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Response Time Monitoring

Details

Policy: ADSPI-Sysvol_FRS

Description

Checks the File Replication Service (FRS) event log for error/warning events.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Sysvol Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Sysvol

Monitoring

Details

Policy: ADSPI-Sysvol_Connectivity

Description

Connects to each replication's partner's Sysvol to validate connectivity.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Sysvol Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Sysvol Monitoring

Details

Policy: ADSPI-Sysvol_AD_Sync

Description

Checks synchronization of Group Policy Objects (GPO) in Active Directory and Sysvol.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Sysvol Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Sysvol Monitoring

Details

Policy: ADSPI-Sysvol_PercentFull

Description

Calculates the percent full of the Sysvol disk drive and collects information about its size and logs the information to Coda for later reporting.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Sysvol Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Sysvol Monitoring

Details

Policy: ADSPI-Trust_Mon_Add_Del

Description

Monitors the trust changes in Active Directory on Windows 2003 domain controllers.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Trust Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Trust Monitoring

Policy: ADSPI-Trust_Mon_Modify

Description

This policy monitors any modification of trusts in the Active Directory forest.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Trust Monitoring

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Trust Monitoring

Details

Policy: ADSPI-CreateDataSources

Description

Schedule task policy that creates the data sources in the HPOM subagent.

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Discovery → Advanced Discovery

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery

Details

Policy: ADSPI_ActiveAuthKerberos

Description

Checks the NTDS\Kerberos Authentications counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ActiveAuthLogon

Description

Checks the Server\Logon/sec counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Policy: ADSPI_ActiveAuthNTLM

Description

Checks the NTDS\NTLM Authentications counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Policy: ADSPI_ADCFwdAllWarnErrorMSADC

Description

Monitors the Application log for entries from MSADC that have a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

Functions only with the integration of Exchange. Without Exchange, the adc process, which the policy observes, does not exist.

Type

Windows Event Log (Application)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Policy: ADSPI_ADCImportFailures

Description

Checks the PerfLib counter MSADC\Rate of Import Failures for the number of imports that have failed. If the number is 1 or 2, the policy sends a warning message to the active message browser. If the number is 3 or higher, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Policy: ADSPI_ADCPageFaults

Description

Checks the PerfLib counter Process\Page Faults\adc for the number of page faults for a process. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. A consistently high rate of page faults for a process usually indicates that its working set is not large enough to support the process efficiently. If the system does not have enough available memory to enlarge the working set, it cannot lower the page fault rate.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Details

Policy: ADSPI_ADCPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\adc for the number of bytes allocated exclusively to the ADC process (that is, bytes that cannot be shared with other processes). If the number exceeds 15,000,000, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000, the policy sends a critical message.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Details

Policy: ADSPI_ADCProcessorTime

Description

Checks the PerfLib counter Process\Processor Time\adc for the percentage of processor time Active Directory ADC is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the Active Directory server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Connector

Policy: ADSPI_ADCWorkingSet

Description

Checks the PerfLib counter Process\Working Set\adc for the current number of bytes in the working set of the ADC process. If the number exceeds 15,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 bytes, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_DomainChanges

Description

Approximately every 20 minutes, checks for changes to the domain structure.

- **Name Space**
  Root\Directory\LDAP
- **Event Class**
  __InstanceOperationEvent
- **WQL Filter**
  TargetInstance ISA "ds_dnsdomain"

Successful changes in the domain structure affect the size and replication of the Active Directory database.

Deploy this policy on a domain controller only.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Domain and OU Structure

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Domain and OU Structure

Policy: ADSPI_OUChanges

Description

Checks, approximately every 20 minutes, for changes to the OU structure.

- **Name Space**
  Root\Directory\LDAP
- **Event Class**
  __InstanceOperationEvent
- **WQL Filter**
  TargetInstance ISA "ds_organizationalunit"

Successful changes in the OU structure affect the size and replication of the Active Directory database.

Deploy this policy on a domain controller only.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Domain and OU Structure

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Domain and OU Structure

Policy: ADSPI_GlobalCatalogWrites

Description

Checks the counter NTDS\DS Directory Writes/sec counter, approximately every 30 minutes, for the number of writes to the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Global Catalog Access

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_GlobalCatalogReads

Description

Checks the NTDS\DS Directory Reads/sec counter, approximately every 30 minutes, for the number of reads from the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Global Catalog Access

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_GlobalCatalogSearches

Description

Checks the NTDS\DS Directory Searches/sec counter, approximately every 30 minutes, for the number of searches of the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Global Catalog Access

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_DNSServ_FwdAllWarnError

Description

Monitors the DNS Server log for entries that have a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

Type

Windows Event Log (DNS Server)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllWarnErrorDS

Description

Forwards all event log entries with a severity level of Warning or Error.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllWarnErrorFRS

Description

Forwards all event log entries with a severity level of Warning or Error.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSPageFaults

Description

Checks the PerfLib counter Process\Page Faults/sec\lsass for the number of times a thread requested access to a memory page that was not in memory and therefore had to be read from disk. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the value obtained from this counter consistently generates messages, physical memory is low.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_NTDS_2k8+

Description

The ADSPI_NTDS_2k8+ policy checks if the Active Directory Domain service and `lsass.exe` process are running on the Active Directory node. If they are not running, the policy sends a warning message to the active message browser. You can restart the service with the operator-initiated command. When the Active Directory Domain service starts running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Health Monitors

Policy: ADSPI_DFSR_2k8+

Description

The ADSPI_DFSR_2k8+ policy checks if the DFS Replication service and `dfsrs.exe` process are running on the Active Directory node. If they are not running, the policy sends a warning message to the active message browser. You can restart the service with the operator-initiated command. When the DFS Replication service starts running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\lsass for the number of bytes allocated exclusively to the LSASS process (that is, bytes that cannot be shared with other processes). If the number exceeds 35,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 40,000,000 bytes, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSProcessorTime

Description

Checks the PerfLib counter Process\% Processor Time\lsass for the percentage of processor time the ADS LSASS process is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSWorkingSet

Description

Checks the PerfLib counter Process\Working Set\lsass for the number of memory pages recently touched by threads in the process. If the number exceeds 15,000,000 pages, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 pages, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health

Monitors

Policy: ADSPI_HMNTFRSPageFaults

Description

Checks the PerfLib counter Process\Page Faults/sec\NTFRS for the number of times a thread requested access to a memory page that was not in memory and therefore had to be read from disk. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the value obtained from this counter consistently generates messages, physical memory is low.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\NTFRS for the number of bytes allocated exclusively to the LSASS process (that is, bytes that cannot be shared with other processes). If the number exceeds 15,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 bytes, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSProcessorTime

Description

Checks the PerfLib counter Process\% Processor Time\NTFRS for the percentage of processor time the ADS LSASS process is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSWorkingSet

Description

Checks the PerfLib counter Process\Working Set\NTFRS for the number of memory pages recently touched by threads in the process. If the number exceeds 15,000,000 pages, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 pages, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_HMThreadsInUse

Description

Checks the PerfLib counter NTDS\DS Threads in Use for the number of threads in use by the directory service. (This number is different from the number of threads in use by the directory service process.) If the number exceeds 20, the policy sends a warning message to the active message browser. If the number exceeds 25, the policy sends an error message. These threads serve client API calls, and indicate whether additional processors should be used.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health

Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_KDC

Description

Checks whether the Kerberos Key Distribution Center Service and its corresponding process lsass.exe are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_NetLogon

Description

Checks whether the Net Logon service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_NTFRS

Description

Checks whether the File Replication Service and its corresponding process, ntfrs.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_SamSs

Description

Checks whether the Security Accounts Manager service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_SMTPEventLogs

Description

Monitors the System log for SMTP-specific events. Forwards them as messages to the active message browser.

Type

Windows Event Log (System)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health

Monitors

Policy: ADSPI_SyncSchemaMissMatch

Description

Checks the PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch for the number of synchronization failures. If the number exceeds 1, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or require further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_IQKerberosAuthentications

Description

Checks the PerfLib counter NTDS\Kerberos Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPActiveThreads

Description

Checks the PerfLib counter NTDS\LDAP Active Threads for the number of LDAP Active Threads. If the number exceeds 40, the policy sends a warning message to the active message browser. If the number exceeds 50, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPBindTime

Description

Checks the PerfLib counter NTDS\LDAP Bind Time for the number of LDAP Client Sessions. If the number exceeds 100, the policy sends a warning message to the active message browser. If the number exceeds 200, the policy sends an error message. If the LDAP Bind Time exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPClientSessions

Description

Checks the PerfLib counter NTDS\LDAP Client Sessions for the number of LDAP Client Sessions. If the number exceeds 4,000 sessions, the policy sends a warning message to the active message browser. If the number exceeds 4,500 sessions, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and

Query Monitors

Policy: ADSPI_IQNTLMAuthentications

Description

Checks the PerfLib counter NTDS\NTLM Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 300, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_ADSPendingSynchronizations

Description

Checks the PerfLib counter NTDS\DRA Pending Replication Synchronizations for the number of synchronizations pending. If the number exceeds 50, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_ADSRepInBoundBytesBetweenSites

Description

Checks the PerfLib counter NTDS\DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec for the number of bytes per second between sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_ADSRepInBoundBytesWithinSites

Description

Checks the PerfLib counter NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec for the number of bytes per second within sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_ADSRepInBoundObjectUpdatesRemaining

Description

Checks the PerfLib counter NTDS\DRA Inbound Object Updates Remaining in Packet for the number of objects remaining. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_ADSRepNotifyQueueSize

Description

Checks the PerfLib counter NTDS\DS Notify Queue Size for the number of jobs in the queue. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Index and Query Monitors

Policy: ADSPI_ReplicationActivities

Description

Monitors the Directory Service log for replication events.

The granularity of the raised events depends on the following registry key:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Diagnostics\5 Replication Events`

Set this value to 3 to get the following four directory replication events logged in the Directory Services log:

- 1487 Internal event: The Directory Service has been asked to begin inbound replication
- 1488 The Directory Service completed the sync request
- 1489 Internal event: The Directory Service has been asked for outbound changes
- 1490 Internal event: The Directory Service finished gathering outbound changes

Type

Windows Event Log (Directory Service)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication Activities

Or,

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Replication Activities

Policy: ADSPI_DirUserCreationDeletion

Description

Checks, approximately every 15 minutes, whether any accounts in Directory User Accounts have been created or deleted. If any have, the policy sends a message to the active message browser.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_KDCFailureGrantTicket

Description

Monitors the Security log for failures to grant authentication tickets. Failures are indicated by event

672 or 676 in the Security Event Log:
676 Authentication Ticket Request Failed
Deploy this template only to servers running KDC.

Type

Windows Event Log (Security)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_PrivilegedAccounts

Description

Monitors the Security log for entries with the following IDs (success and failure):

- 576 Special privileges assigned to new logon
- 577 Privileged Service Called
- 578 Privileged object operation

Forwards these entries as messages to the active message browser. Windows 2000 does not let you choose which rights to audit. As a result, auditing Use of User Rights will generate a very large number of audits. In most cases, the sheer volume of this information outweighs its usefulness. Do not audit Use of User Rights unless absolutely necessary for your environment. If you decide to audit Use of User Rights, you should purchase or write an event-analysis tool that can filter only the user rights of interest to your organization. If Use of User Rights is enabled, not all user rights are audited. The following user rights are never audited:

- Bypass Traverse Checking (SeChangeNotifyPrivilege)
- Generate Security Audits (SeAuditPrivilege)
- Create A Token Object (SeCreateTokenPrivilege)
- Debug Programs (SeDebugPrivilege)
- Replace A Process Level Token (SeAssignPrimaryTokenPrivilege)

The following user rights are audited only if a specific Windows Registry setting is present:

- Backup Files and Directories (SeBackupPrivilege)
- Restore Files and Directories (SeRestorePrivilege) To enable auditing of the backup and restore

privileges, set the following Windows Registry value to 1:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing (REG_DWORD)
.

Type

Windows Event Log (Security)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecAdminGroupChange

Description

Monitors changes in the Enterprise and Domain Admin group.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecDirectoryServiceAccess

Description

Forwards all Security event log entries with Directory Service Access category.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecErrAccessPermissions

Description

Checks the PerfLib counter Server\Errors Access Permissions for the number of attempts to access ADS elements that were denied. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. This counter warns of unauthorized access attempts that randomly seek inadequately protected files.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecErrGrantedAccess

Description

Checks the PerfLib counter Server\Errors Granted Access for the number of access attempts that opened files successfully but were allowed no further access. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number is greater than 4, the policy sends an error message. This counter warns of attempts to access files without proper authorization.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecErrorsLogon

Description

Checks the PerfLib counter Server\Errors Logon for the number of denied logon attempts to the server. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number is greater than 4, the policy sends an error message. This counter warns of attempts to log on with a password-guessing program.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecNonTransMembEval

Description

Checks the PerfLib counter Server\SAM Non-Transitive Membership Evaluation/sec for the number of SAM nontransitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, the domain may be overloaded.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecSDPropagatorQueue

Description

Checks the PerfLib counter NTDS\DS Security Descriptor Propagator Runtime Queue for the number of objects remaining to be examined while processing the current directory service security descriptor propagator event. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the higher threshold is exceeded, the domain controller may be overloaded.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecTransMembEval

Description

Checks the PerfLib counter NTDS\SAM Transitive Membership Evaluations for the number of SAM transitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy ends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SiteChanges

Description

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

- **Name Space**
  Root\Directory\LDAP
- **Event Class**
  __InstanceOperationEvent
- **WQL Filter**
  TargetInstance ISA "ds_site"

Successful changes in the OU structure affect the size and replication of the Active Directory database. Deploy this policy to only one node within the forest. The additional script must be executed for all sites within this domain on this node (or deployed to several nodes and execute additional scripts on these nodes).

Prerequisite: See the online Help for the Smart Plug-in for Windows overview>Using Windows OS SPI policies>"Prerequisites for Windows policies."

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Site Structure

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Site Structure

Policy: ADSPI_DNSServ_FwdAllInformation

Description

Monitors the DNS Server log for entries of the type "Information", and forwards these entries as messages to the active message browser.

Type

Windows Event Log (DNS Server)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllInformationDS

Description

Monitors the Directory Service log for entries of the type "Information", and forwards them as messages to the active message browser.

Type

Windows Event Log (Directory Service)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllInformationFRS

Description

Monitors the File Replication Service log for entries of the type "Information", and forwards them as messages to the active message browser.

Type

Windows Event Log (File Replication Service)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_Logging

Description

Logs selected performance data for Microsoft Active Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_DSReads

Description

Checks the NTDS\DS Directory Reads/sec counter for the number of reads from the DS. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Deploy this policy only to the DS server.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000→ Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and

Query Monitors

Policy: ADSPI_DSSearches

Description

Checks the NTDS\DS Directory Searches/sec counter approximately every 30 minutes for the number of searches of the DS. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Deploy this policy only to the DS server.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000→ Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSWrites

Description

Checks the NTDS\DS Directory writes/sec counter approximately every 30 minutes for the number of writes to the DS. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Deploy this policy only to the DS server.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000→ Manual-Deploy → Index and Query Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy Groups Catalog

The Microsoft Active Directory SPI groups policies at the highest level according to deployment:
- **Auto-Deploy** policies are deployed automatically whenever a relevant Active Directory service is discovered.
- **Manual-Deploy** policies may be deployed as needed.

See the policy sub groups below, or follow the group links to individual policy descriptions:

Auto-Deploy Policies

Discovery : used to discover all Active Directory services.

DIT Monitoring : used to monitor all Directory Information Tree services.

DNS Monitoring : used to monitor DNS services related to Active Directory.

FSMO Monitoring : used to monitor Flexible Single Master Operations services.

Replication Monitoring : used to monitor replication latency throughout the Active Directory forest.

GC Monitoring : a policy deployed only to DCs hosting global catalog services that measures global catalog replication latency.

Response Time Monitoring : used to monitor Active Directory response times for purposes of checking the general responsiveness of Active Directory.

Sysvol Monitoring : used to monitor connectivity, space use, and replication as related to SysVol.

Trust Monitoring : used to create the trust report and monitor trust relationship changes between DCs.

Manual-Deploy Policies

Auto Baseline: These policies calculate appropriate adaptive threshold values for Measurement Threshold policies, based on previously collected historical data.

Connector: Monitors Active Directory performance monitor counters.

Domain & OU Structure: Monitors domain and organizational unit (OU) changes.

Global Catalog Access: Monitors the performance monitor counters on Global Catalog servers.

Health Monitors: Monitors the health of DNS, Kerberos and NetLogon Services.

Index and Query Monitors: Monitors the performance monitor counters associated with LDAP and Kerberos.

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

Replication Activities: Monitors the Directory Service log for replication events.

Security: Monitors (1) Security event logs for Active Directory related events, (2) Security group changes and, (3) performance monitor counters associated with Security.

Site Structure: Monitors site changes.

NOTE:
[1] The policies under the Auto Baseline group do not work on nodes configured with HP Performance Agent.

[2] The policies under the Connector group can be used with Windows Server 2003 nodes only.

Related Topics:

- Choosing a Microsoft Active Directory SPI policy
- Group Policy Catalog
- Manual-Deploy Policies
- Auto-Deploy Policy Catalog

Auto-Deploy Policy Catalog

After you deploy the **Auto-Deploy** group, the service discovery process starts. Service discovery kicks off another automatic deployment of policies relevant to the detected services on a node. For **Manual-Deploy** policy descriptions, see Manual-Deploy policies . For a description of any policy listed below, click its name and link to details.

Discovery Policies	**DIT Monitoring Policies**
ADSPI-AutoDiscovery Delete *	ADSPI-DIT LogfilesQueueLength
ADSPI-AutoDiscovery_DIT *	ADSPI-DIT Total DIT Size
ADSPI-AutoDiscovery_DNS *	ADSPI-DIT LogfilesPercent Full
ADSPI-AutoDiscovery_FSMO *	ADSPI- DITQueueLength
ADSPI-AutoDiscovery_GC *	ADSPI-DITPercent Full
ADSPI-AutoDiscovery_PBHS *	**GC Monitoring Policies**
ADSPI-AutoDiscovery_Rep *	ADSPI-Rep_GC Check and Threshold
ADSPI-AutoDiscovery_Trust *	**Replication Monitoring Policies**
ADSPI_Discovery *	ADSPI-RepMonitorInterSiteReplication / ADSPI-RepMonitorIntraSiteReplication
ADSPI-CreateDataSources *	ADSPI-Rep_Mon_Fwd_Ping_Messages
ADSPI-AutoDiscovery_RODC_2K8+	ADSPI-Rep_Delete_OvRep_Object
FSMO Monitoring Policies	ADSPI-Rep_CheckObj
ADSPI-FSMO_Consist *	ADSPI-Rep_InboundObjs
ADSPI-FSMO_GC-Infra_Check	ADSPI-Rep_ISM_Chk
ADSPI-FSMO_Consist_INFRA	ADSPI-Rep_TimeSync
ADSPI-FSMO_Consist_NAMING	**ADSPI-Rep_Modify_User_Object** *
ADSPI-FSMO_Consist_PDC	**ADSPI-Rep_ModifyObj** *
ADSPI-FSMO_Consist_RID	**DNS Monitoring Policies**
ADSPI-FSMO_Consist_SCHEMA	ADSPI-DNS_GC_StrandedSite

ADSPI-FSMO_Logging *

ADSPI-FSMO_NAMING_Ping

ADSPI-FSMO_NAMING_Bind

ADSPI-FSMO_INFRA_Ping

ADSPI-FSMO_INFRA_Bind

ADSPI-FSMO_PDC_Ping

ADSPI-FSMO_PDC_Bind

ADSPI-FSMO_RID_Ping

ADSPI-FSMO_RID_Bind

ADSPI-FSMO_RoleMvmt_SCHEMA

ADSPI-FSMO_RoleMvmt_RID

ADSPI-FSMO_RoleMvmt_PDC

ADSPI-FSMO_RoleMvmt_NAMING

ADSPI-FSMO_RoleMvmt_INFRA

ADSPI-FSMO_RoleMvmt

ADSPI-FSMO_SCHEMA_Ping *

ADSPI-FSMO_SCHEMA_Bind

Response Time Monitoring Policies

ADSPI-Response Time Query

ADSPI-Response Time GCQuery

ADSPI-Response Logging *

ADSPI-Response Time GC Bind

ADSPI-Response Time Bind

ADSPI DNS_Extra_GC_SRV_Chk

ADSPI-DNS_Kerberos_SRV_Chk

ADSPI-DNS_Extra_Kerberos_SRV_Chk

ADSPI-DNS_LDAP_SRV_Chk

ADSPI DNS_Extra_LDAP_SRV_Chk

ADSPI-DNS_GC_A_Chk

ADSPI DNS_DC_A_Chk

ADSPI DNS_DC_Response

ADSPI-DNS_Island_Server

ADSPI-DNS_LogDNSPagesSec

ADSPI DNS_DC_CNAME_Chk

ADSPI-DNS_GC_SRV_Chk

ADSPI-DNS_Server_Response

ADSPI-DNS_Obsolete_GUIDS

Sysvol Monitoring Policies

ADSPI-Sysvol_AD_Sync

ADSPI-Sysvol_Connectivity

ADSPI-Sysvol_FRS

ADSPI-Sysvol_PercentFull

Trust Monitoring

ADSPI-Trust_Mon_Add_Del

ADSPI_Trust_Mon_Modify

*Scheduled task policy, required for collecting data on related measurement threshold policies.

Related Topics:

- Policy groups & types
- Group policy catalog

Discovery Policies

Discovery policies discover Active Directory services when either automatically deployed to newly added nodes or manually deployed to already managed nodes.

Service discovery policies are as follows:

- ADSPI-CreateDataSources
- ADSPI-Discovery
- ADSPI-AutoDiscovery_DIT (for Windows Server 2003/2000)
- ADSPI-AutoDiscovery_DIT_2k8+ (for Windows Server 2008)
- ADSPI-AutoDiscovery_DNS (for Windows Server 2003/2000)
- ADSPI-AutoDiscovery_DNS_2k8+ (for Windows Server 2008)
- ADSPI-AutoDiscovery_FSMO (for Windows Server 2003/2000)
- ADSPI-AutoDiscovery_FSMO_2k8+ (for Windows Server 2008)
- ADSPI-AutoDiscovery_Rep (for Windows Server 2003/2000)
- ADSPI-AutoDiscovery_Rep_2k8+ (for Windows Server 2008)
- ADSPI-AutoDiscovery_GC (for Windows Server 2003/2000)
- ADSPI-AutoDiscovery_GC_2k8+ (for Windows Server 2008)
- ADSPI-AutoDiscovery_PBHS (preferred bridgehead servers)
- ADSPI-AutoDiscovery_Trust (for Windows Server 2003/2000)
- ADSPI-AutoDiscovery_Trust_2k8+ (for Windows Server 2008)
- ADSPI-AutoDiscovery_RODC_2k8+ (for Windows Server 2008)

The Microsoft Active Directory SPI can also detect a previously discovered service that, for whatever reason, may no longer be present. After five checks (by default, five hourly checks), the domain controller's absent service is removed from the service tree and from the service map.

The Microsoft Active Directory SPI discovery, by default, *runs every hour* and identifies the services running on each Domain Controller (DC). After services are discovered on HPOM-managed nodes, automatic deployment of relevant policies occurs for those systems.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Descriptions

Policy: ADSPI_Discovery

Description: This policy performs the discovery of Active Directory from **System Infrastructure** through **Domain Controller -> Services** . It makes use of *OvAdsDisc.exe* to discover all AD components.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-AutoDiscovery_Delete

Description: Deployed automatically with other discovery policies, this policy verifies the continued presence of an already discovered service on each domain controller. Whenever a previously discovered service is detected as no longer present on the domain controller, this policy starts the process of removing the service from the console tree and the service map. After five verifications (taking five hours by default), the removal occurs.

Policy type: Open Message Interface

Result: The ADSPI-AutoDiscovery_Delete policy ensures that the HPOM console's Services tree and Service Map stay up to date if ever a service is shifted from one domain controller to another.

Schedule : Hourly

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-AutoDiscovery_DIT

Description: This policy runs the auto discovery program for Directory Information Tree (DIT) services. The policy is deployed to all HPOM managed nodes, where it searches for DIT services on the DC. When discovered, DIT is shown under the DC name and also with the DC in the service map. Use this policy for Windows Server 2003/2000 nodes.

Result: The discovered service results in the automatic deployment of relevant Microsoft Active Directory SPI DIT policies on the HPOM managed node. With the DIT-related services policies deployed to the node, the system detects potential problems developing with the DIT for each DC.

Policy: ADSPI-AutoDiscovery_DIT_2k8+

Description: This policy runs the auto discovery program for Directory Information Tree (DIT) services. The policy is deployed to all HPOM managed nodes, where it searches for DIT services on the DC. When discovered, DIT is shown under the DC name and also with the DC in the service map. Use this policy for Windows Server 2008 nodes.

Result: The discovered service results in the automatic deployment of relevant Microsoft Active Directory SPI DIT policies on the HPOM managed node. With the DIT-related services policies deployed to the node, the system detects potential problems developing with the DIT for each DC.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Catalog
- Discovery Policies

Policy: ADSPI-AutoDiscovery_DNS

Description: This policy runs the auto discovery program for DNS services. This policy is deployed to all HPOM managed nodes, where it searches for a domain controller and then creates a DNS service on the DC. After it is created, DNS is shown under the DC name and also with the DC in the service map. Use this policy for Windows Server 2003/2000 nodes.

The service results in the automatic deployment of relevant Active Directory-SPI DNS policies on the HPOM managed node. With the DNS-related services policies deployed to the node, the system can then be monitored for DNS service health.

Policy: ADSPI-AutoDiscovery_DNS_2k8+

Description: This policy runs the auto discovery program for DNS services. This policy is deployed to all HPOM managed nodes, where it searches for a domain controller and then creates a DNS service on the DC. After it is created, DNS is shown under the DC name and also with the DC in the service map. Use this policy for Windows Server 2008 nodes.

The service results in the automatic deployment of relevant Active Directory-SPI DNS policies on the HPOM managed node. With the DNS-related services policies deployed to the node, the system can then be monitored for DNS service health.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-AutoDiscovery_FSMO

Description: This service discovery policy runs the auto discovery program for FSMO monitoring. The policy searches for Active Directory FSMO services including PDC Master, RID Master, Infrastructure Master, Schema Master, and Domain Naming Master. Use this policy for Windows Server 2003/2000 nodes.

Result: If the domain controller is identified as a host for any FSMO service, that FSMO service appears under the DC name in the console tree as well as with the DC name in the service map. Discovered services also result in the automatic deployment of relevant FSMO policies on the system.

Schedule: Daily at 02:00 AM every night.

Policy: ADSPI-AutoDiscovery_FSMO_2k8+

Description: This service discovery policy runs the auto discovery program for FSMO monitoring. The policy searches for Active Directory FSMO services including PDC Master, RID Master, Infrastructure Master, Schema Master, and Domain Naming Master. Use this policy for Windows Server 2008 nodes.

Result: If the domain controller is identified as a host for any FSMO service, that FSMO service appears under the DC name in the console tree as well as with the DC name in the service map. Discovered services also result in the automatic deployment of relevant FSMO policies on the system.

Schedule: Daily at 02:00 AM every night.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-AutoDiscovery_GC

Description: This policy runs the auto discovery program for the Active Directory Global Catalog (GC). The policy searches for hosted Global Catalog services. Use this policy for Windows Server 2003/2000 nodes.

Result: If the domain controller hosts the Global Catalog, then GC displays under the DC name in the console details pane as well as in the service map. The discovered service also results in the automatic deployment of Microsoft Active Directory SPI GC policies on the HPOM managed node. The domain controller can then be monitored for potential problems developing with GC services.

Policy: ADSPI-AutoDiscovery_GC_2k8+

Description: This policy runs the auto discovery program for the Active Directory Global Catalog (GC). The policy searches for hosted Global Catalog services. Use this policy for Windows Server 2008 nodes.

Result: If the domain controller hosts the Global Catalog, then GC displays under the DC name in the console details pane as well as in the service map. The discovered service also results in the automatic deployment of Microsoft Active Directory SPI GC policies on the HPOM managed node. The domain controller can then be monitored for potential problems developing with GC services.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-AutoDiscovery_PBHS

Between sites in an Active Directory forest, the Knowledge Consistency Checker (KCC) generates the connections and thereby causes the domain controllers that store the connections to act as bridgeheads in the topology. A "bridgehead" is a point where a connection leaves or enters a site. These servers provide inter-site connections as follows:

- **Bridgehead servers:** These servers have connection objects for connections between sites. A destination bridgehead server has a connection object with a "from (source)" server in another site, while a source bridgehead server has a connection objection with a "to (destination)" server.
- **Preferred bridgehead servers (PBHS):** You can limit the KCC's choices of servers that it can designate as bridgeheads (that is, restrict the domain controllers in which the KCC can create connections between sites). You do this by selecting one or more domain controllers in a site as a "preferred" bridgehead server. The KCC then will always consider the "preferred" bridgehead servers when it establishes the source/destination servers fro intersite connections. Peferred bridgehead servers are used exclusively to replicate changes collected from the site.

Policy description: This schedule policy runs the auto discovery program for Preferred Bridgehead Server Monitoring within replication.

Policy result: After it is discovered, the Preferred Bridgehead Server is identified on the DC hosting it and appears in the HPOM Services tree, beneath Replication services, and in the service map as part of the Active Directory services, illustrating the status of this service.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Catalog
- Look-up a policy description (includes both Auto- & Manual-Deploy groups)
- Discovery Policies

Policy: ADSPI-AutoDiscovery_Rep

Description: This policy runs the auto discovery program for Active Directory replication monitoring. The policy searches for Active Directory replication and replication-related services including Sysvol, inbound replication objects, and time synchronization. Use this policy for Windows Server 2003/2000 nodes.

Many things can go wrong which can cause replication failures and, as a result, are important to measure. For example, Sysvol, as the shared/replicated directory, stores the server copy of the domain's public files. These files are replicated among all domain controllers in the domain. Updates result in inbound connection objects. An increase in the number of inbound connection objects can indicate that updates are being redirected, which could mean a failed or overloaded bridgehead.

Result: The discovered services result in deployment of relevant Microsoft Active Directory SPI replication monitoring policies on the HPOM managed nodes. The domain controller can then be checked and message alerts sent when problems appear in services having to do with replication. In the HPOM service map, the DC hosting the Sysvol is identified and a service node is provided in the service map (DC: DC_name→Replication→ Sysvol) to illustrate the status of it.

NOTE:
The Preferred Bridgehead Server is also displayed as a Replication service (DC: DC_name→Replication → Bridgehead), although another discovery policy (ADSPI-AutoDiscovery_PBHS) runs a separate program for the Bridgehead discovery.

Policy: ADSPI-AutoDiscovery_Rep_2k8+

Description: This policy runs the auto discovery program for Active Directory replication monitoring. The policy searches for Active Directory replication and replication-related services including Sysvol, inbound replication objects, and time synchronization. Use this policy for Windows Server 2008 nodes.

Many things can go wrong which can cause replication failures and, as a result, are important to measure. For example, Sysvol, as the shared/replicated directory, stores the server copy of the domain's public files. These files are replicated among all domain controllers in the domain. Updates result in inbound connection objects. An increase in the number of inbound connection objects can indicate that updates are being redirected, which could mean a failed or overloaded bridgehead.

Result: The discovered services result in deployment of relevant Microsoft Active Directory SPI replication monitoring policies on the HPOM managed nodes. The domain controller can then be checked and message alerts sent when problems appear in services having to do with replication. In the HPOM service map, the DC hosting the Sysvol is identified and a service node is provided in the service map (DC:

DC_name→Replication→ Sysvol) to illustrate the status of it.

NOTE:
The Preferred Bridgehead Server is also displayed as a Replication service (DC: DC_name→Replication → Bridgehead), although another discovery policy (ADSPI-AutoDiscovery_PBHS) runs a separate program for the Bridgehead discovery.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Groups
- Policy Catalog

Policy: ADSPI-AutoDiscovery__RODC_2k8+

This policy is grouped under the Windows Server 2008 group. The ADSPI-AutoDiscovery_RODC_2k8+ policy discovers the read-only domain controllers.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Catalog
- Look-up a policy description (includes both Auto- & Manual-Deploy groups)
- Discovery Policies

Policy: ADSPI-AutoDiscovery_Trust

Description: This scheduled task policy runs the auto discovery program for Trust Monitoring. It creates the Trust service in the HPOM service map for Windows 2003 domain controllers. Use this policy for Windows Server 2003 nodes.

Schedule: Daily at 2:00 A.M.

Policy: ADSPI-AutoDiscovery_Trust_2k8+

Description: This scheduled task policy runs the auto discovery program for Trust Monitoring. It creates the Trust service in the HPOM service map for Windows 2008 domain controllers. Use this policy for Windows Server 2008 nodes.

Schedule: Daily at 2:00 A.M.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-CreateDataSources

Microsoft Active Directory SPI data sources need to be created in CODA for policies to log data. The ADSPI-CreateDataSources (under the policy groups **SPI for Active Directory→Windows Server 2003/2000→Auto-Deploy→Discovery→Advanced Discovery** and **SPI for Active Directory→ Windows Server 2008→Auto-Deploy→Discovery→Advanced Discovery**) policy creates the required data sources in CODA or HP Performance Agent.

> **NOTE:**
> Before running this policy on the managed node, deploy the instrumentation category **SPI for Data Collector** .

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

DIT Monitoring Policies

ADSPI-DIT LogfilesQueue Length

ADSPI- DIT_DITPercent Full

ADSPI-DIT_DITQueue Length

ADSPI-DIT_TotalDIT Size

ADSPI-DIT_LogfilesPercentFull

The DIT policies are available under both the policy groups (Windows Server 2003/2000 and Windows Server 2008).

These policies are located under the following policy groups:

- *For Windows Server 2003/2000 nodes*
  SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → DIT Monitoring
- *For Windows Server 2008 nodes*
  SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring

Related Topics:

- Descriptions of Policy Groups & Types
- Catalog of Policy Groups
- Catalog of Individual Policies
- Discovery Policies

Policy: ADSPI-DIT_LogfilesQueueLength

The DIT log files queue size shows the number of operations pending against the DIT log files drive. When this number is higher than zero for a sustained period of time, it indicates that the particular volume on which the DIT log files reside is unable to handle the number of necessary updates.

Description	This policy measures the disk queue length on the DIT Log files drive; the policy also logs and thresholds on the data.
Interval	5 min
Threshold	Warning: Logfile queue length >=1 Error: Logfile queue length >=2
Warning/Error Message Text:	**Start Actions:** The queue length (i.e, the number of outstanding requests) on the Active Directory log files disk drive on <$MSG_NODE_NAME> is <$SESSION(LogFilesQueueLength)>. The log files disk drive is '<$SESSION(LogFilesDrive)>'. **End Actions:** The queue length on the Active Directory log files disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>.
Instruction Text	**Probable Cause(s):** (1) A large queue length could indicate that the particular disk volume may be unable to handle the amount of updates necessary. **Potential Impact:** The domain controller may be slow in responding to (1) the addition and modification of objects in Active Directory. (2) the update one or more Active Directory partitions after it receives a change notification from a replication partner. **Suggested Action(s):** (1) Install additional disks, or upgrade the existing hard disks. Update the bus and disk controllers. (2) If the database files and logs are co-located, you can

separate them using the \"ntdsutil\" utility program.

For more information see the Microsoft Knowledge Base Article:
(1) Q222019 - DCPROMO Space Requirements for Active Directory Database and Log Files
http://support.microsoft.com/default.aspx?scid=kb;en-us;222019 >
(2) Q315131 - HOW TO: Use Ntdsutil to Manage Active Directory Files from the Command Line in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;315131

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the following columns of the ADSPI_LOGQUEUELENGTH table:

- Instance Name
- InstanceValue

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DIT_DITQueueLength

The DIT queue size is the measure of the number of operations pending against the DIT drive that are not completed. When this number is higher than zero for a sustained period of time, it indicates that the particular volume that the DIT is on is unable to handle the amount of updates necessary.

Description	Monitors the queue length on the DIT disk drive. The policy also logs and thresholds on the data.
Interval	5 min
Threshold	Warning: DITQueueLength>=1 Critical: DITQueueLength>=2
Warning/Error Message Text	**Start Actions:** The queue length (i.e, the number of outstanding requests) on the Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> is <$SESSION(DitQueueLength)>. The DIT disk drive is '<$SESSION(DitDrive)>'. **End Actions:** The queue length on the Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>.
Warning/Error Instruction Text	**Probable Cause(s):** (1) A large queue length could indicate that the particular disk volume may be unable to handle the amount of updates necessary. **Potential Impact:** The domain controller may be slow in responding to (1) the addition and modification of objects in Active Directory. (2) the update one or more Active Directory partitions after it receives a change notification from a replication partner. **Suggested Action(s):** (1) Install additional disks, or upgrade the existing hard disks. Update the bus and disk controllers. (2) If the database files and logs are co-located, you can separate them using the \"ntdsutil\" utility program.

For more information see the Microsoft Knowledge Base Article:
(1) Q222019 - DCPROMO Space Requirements for Active Directory Database and Log Files
http://support.microsoft.com/default.aspx?scid=kb;en-us;222019
(2) Q315131 - HOW TO: Use Ntdsutil to Manage Active Directory Files from the Command Line in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;315131

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Result: If the DIT queue length exceeds 0 for a prolonged time period, a message is sent to the console.

The policy stores the collected data into the following table:

ADSPI_DITQUEUELENGTH

The following columns are used to log data:

- Instance Name
- InstanceValue

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DIT_TotalDITSize

The Active Directory database file, or DIT, can cause problems when it expands over time and no one has been watching it.

Description	Monitors the total amount of free space on the DIT disk drive in MB.
Interval	24 hour
Threshold	Threshold 1: DitFreeSpace <= 10% or <100MB of the logical disk drive hosting the DIT. Threshold 2 (logical drive): When Dit Drive Free Space > 10% size of DIT< /P>< /P>
Warning/Error Message Text:	**Start Actions:** The freespace on the Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> is only <$SESSION(DitDriveFreeSpace)> MB. It is less than the threshold value of <$SESSION(minFreeSpaceMB)>MB. **End Actions:** The freespace on the Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> is greater than <$SESSION(minFreeSpaceMB)> MB.
Warning/Error Instruction Text:	Metric(s): (1) root\cimv2 Win32_LogicalDisk.FreeSpace **Possible Problem(s):** (1) The disk drive that hosts the AD database (ntds.dit) may soon run out of disk space. **Probable Cause(s):** (1) The AD database file (ntds.dit) has expanded over time. (2) Some other application is taking up the disk space. (3) The disk may not be big enough to allow for the growth in the AD database size. **Potential Impact:** The domain controller may NOT (1) allow addition and modification of objects in Active Directory. (2) update one or more Active Directory partitions after it

receives a change notification from a replication partner.
Suggested Action(s):
(1) Free some space on the drive by deleting unnecessary files or moving them to another volume.
(2) If the disk is a RAID set, you may be able to add additional disks to increase the storage.
(3) If the database files and logs are co-located, you can separate them using the "ntdsutil" utility program.
(4) Perform offline defragmentation of the Active Directory database.

For more information see the Microsoft Knowledge Base Article:
(1) Q229602 - Defragmentation of the Active Directory Database
http://support.microsoft.com/default.aspx?scid=kb;en-us;229602
(2) Q232122 - Performing Offline Defragmentation of the Active Directory Database
http://support.microsoft.com/default.aspx?scid=kb;en-us;232122

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the following tables:

- **ADSPI_DITDATABASESIZE**

  The following columns are used to log data:

  - Instance Name
  - InstanceValue

- **ADSPI_DOMAIN**

  The following columns are used to log data:

Metric	Column Name
Domain Name	InstanceName
Domain Value	InstanceValue

- **ADSPI_SITE**

  The following columns are used to log data:

Metric	Column Name
Site Name	InstanceName
Site Value	InstanceValue

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DIT_LogfilesPercentFull

A common problem occurs when the DIT logfile expands over time and goes unobserved, while the available free space on the disk drive which hosts the DIT logs decreases. This policy calculates the percentage amount occupied by the DIT logfiles in proportion to the drive hosting the DIT.

Description	This policy calculates the percentage full of each drive hosting the DIT log file. The policy logs the information and also checks for an exceeded threshold.
Interval	24 hour
Warning/Error Message Text	**Start Actions:** The Active Directory log files disk drive on <$MSG_NODE_NAME> is <$SESSION(PercentFull)>%. **End Actions:** The percentage full on the Active Directory log files disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.
Warning/Error Instruction Text:	**Probable Cause(s):** (1) The disk drive that hosts the AD log files may soon run out of disk space. **Potential Impact:** The domain controller may NOT (1) allow addition and modification of objects in Active Directory. (2) update one or more Active Directory partitions after it receives a change notification from a replication partner. **Suggested Action(s):** (1) Free some space on the drive by deleting unnecessary files or moving them to another volume. (2) If the disk is a RAID set, you may be able to add additional disks to increase the storage. (3) If the database files and logs are co-located, you can separate them using the \"ntdsutil\" utility program. (4) Perform offline defragmentation of the Active Directory database.

	For more information see the Microsoft Knowledge Base Article: (1) Q229602 - Defragmentation of the Active Directory Database http://support.microsoft.com/default.aspx?scid=kb;en-us;229602 (2) Q232122 - Performing Offline Defragmentation of the Active Directory Database http://support.microsoft.com/default.aspx?scid=kb;en-us;232122

Result: If the DIT-occupied percentage of the drive hosting the DIT exceeds the defined threshold, a message is sent to the console.

The policy stores the collected data into the following columns of the ADSPI_LOGPERCENTFULL table:

- Instance Name
- InstanceValue

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DIT_DITPercentFull

This policy helps address the common problem that occurs when the size of the DIT file increases and goes unobserved, while the available free space on the DIT hosting disk drive decreases. This policy calculates the percentage full of the drive hosting the DIT.

Description	Monitors the percentage used space on the disk drive holding the AD database (DIT).
Interval	24 hour
Threshold	Warning: Percentage disk full=80% Critical: Percentage disk full=90%
Warning/Error Message Text	Start Actions: The Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> is <$SESSION(PercentFull)>% full. End Actions: The percentage full on the Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.
Warning Error Instruction Text:	**Probable Cause(s):** (1) The disk drive that hosts the AD database (ntds.dit) may soon run out of disk space. **Potential Impact:** The domain controller may NOT (1) allow addition and modification of objects in Active Directory. (2) update one or more Active Directory partitions after it receives a change notification from a replication partner. **Suggested Action(s):** (1) Free some space on the drive by deleting unnecessary files or moving them to another volume. (2) If the disk is a RAID set, you may be able to add additional disks to increase the storage. (3) If the database files and logs are co-located, you can separate them using the \"ntdsutil\" utility program. (4) Perform offline defragmentation of the Active Directory database. For more information see the Microsoft Knowledge Base Article: (1) Q229602 - Defragmentation of the Active Directory Database

	http://support.microsoft.com/default.aspx?scid=kb;en-us;229602 (2) Q232122 - Performing Offline Defragmentation of the Active Directory Database http://support.microsoft.com/default.aspx?scid=kb;en-us;232122 **Disclaimer:** Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the following columns of the ADSPI_DITPERCENTFULL table:

- Instance Name
- InstanceValue

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

DNS Monitoring Policies

These policies are available under the Windows Server 2003/2000 group as well as the Windows Server 2008 group.

ADSPI- DNS_DC_A_Chk

ADSPI-DNS_DC_CNAME_Chk

ADSPI-DNS_DC_Response

ADSPI-DNS_Extra_GC_SRV_Chk

ADSPI-DNS_Extra_Kerberos_SRV_Chk

ADSPI-DNS_Extra_LDAP_SRV_Chk

ADSPI-DNS_GC_A_Chk

ADSPI-DNS_GC_StrandedSite

ADSPI-DNS_GC_SRV_Chk

ADSPI-DNS_Kerberos_SRV_Chk

ADSPI-DNS_Island_Server

ADSPI-DNS_LDAP_SRV_Chk

ADSPI-DNS_Obsolete_GUIDS

ADSPI-DNS_LongDNSPageSec

ADSPI-DNS_Server_Response

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_DC_A_Chk

This policy checks the 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 another for the domain that it serves. The policy generates a critical message if one or both records are missing.

Description	Ensures that DNS contains the expected DNS host resource records for the LDAP service by checking for expected DNS A resource records.
Interval	1 hour
Threshold	Critical: >=1 Types of failures: “REG_RECORDS_FLAG_NOT_SET = 2” “DNS_SERVER_PING_FAILURE = 3” “NO_FOREST_RECOGNITION = 5” “PROBLEM_NOT_DETECTED =13”
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is missing the following records in DNS: <$OPTION(missing)> The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> <$SESSION(NetLogon)><$OPTION(NetLogonStatus)> <$SESSION(RegRecordsFlag)> <$SESSION(ServerPing)><$OPTION(FailingServers)> <$SESSION(NoForest)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Error Instruction Text	**Possible Problem(s):**
	(1) The domain controller sending this message may not be found by other machines in the forest.
	Probable Cause(s):
	One or more of the following will be true if records are missing in DNS.

The domain controller sending this message:

(1) has had a Net Logon service failure.

(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.

(3) the configuration is set to use DNS servers which are unresponsive.

(4) is configured to use DNS servers which are not able to resolve queries for the Active Directory forest.

(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:

(1) Domain controllers that are missing records in DNS may not be found by other machines in the forest. This can lead to replication failures and user logon failures.

Suggested Action(s):

Check the 'Message Text' section of this message for specific failures found on the domain controller.

(1) For the case of a failing Net Logon service:

- Restart the Net Logon service on the domain controller sending this message.

(2) If the domain controller is not configured to register its records in DNS:

- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.
- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.

(3) For the case of unresponsive DNS servers:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates:
This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.

For more information on troubleshooting Active Directory related DNS problems, see the Microsoft Knowledge Base Articles:
(1) Q247811 - How Domain Controllers Are Located in Windows http://support.microsoft.com/default.aspx?scid=kb;EN-US;247811
(2) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(3) Q287156 - Troubleshooting Windows 2000 Domain Name System Dynamic Update Problems http://support.microsoft.com/default.aspx?scid=kb;en-us;287156

(4) Q240943 - Dynamic DNS Host Name Registrations http://support.microsoft.com/default.aspx?scid=kb;en-us;240943

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_DC_CName_Chk

This policy verifies that the domain controller can be located through use of its alias. The policy does this by verifying the domain controller's GUID alias, using: < *Domain_Controller GUID* >._msdcs.<*Domain* >

Description	Checks for expected DNS CNAME resource records for the LDAP service.
Interval	1 hour
Threshold	Error Level: Threshold limit >= 1 Types of failures: “REG_RECORDS_FLAG_NOT_SET = 2” “DNS_SERVER_PING_FAILURE = 3” “NO_FOREST_RECOGNITION = 5” “PROBLEM_NOT_DETECTED = 13”
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is missing the following records in DNS: <$OPTION(missing)> The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> <$SESSION(NetLogon)><$OPTION(NetLogonStatus)> <$SESSION(RegRecordsFlag)> <$SESSION(ServerPing)><$OPTION(FailingServers)> <$SESSION(NoForest)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.
Error Instruction Text	**Metric information:** The value obtained by this policy may be ignored by the user. All points of failure that can be detected by this policy have been assigned a prime number. The value sent to this policy is the product of the prime numbers associated with detected points of failure. It is factored to determine what went wrong, and the result

is a customized 'Message Text'.

Possible Problem(s):
(1) The domain controller sending this message may not be found by other machines in the forest.

Probable Cause(s):
One or more of the following will be true if records are missing in DNS.
The domain controller sending this message:
(1) has had a Net Logon service failure.
(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.
(3) the configuration is set to use DNS servers which are unresponsive.
(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.
(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:
(1) Domain controllers that are missing records in DNS may not be found by other machines in the forest. This can lead to replication failures and user logon failures.

Suggested Action(s):
Check the 'Message Text' section of this message for specific failures found on the domain controller.

(1) For the case of a failing Net Logon service:
- Restart the Net Logon service on the domain controller sending this message.

(2) If the domain controller is not configured to register its records in DNS:
- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.
- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.

(3) For the case of unresponsive DNS servers:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates:
This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information on configuring a DNS zone to enable dynamic updates.

For more information on troubleshooting Active Directory related DNS problems, see the Microsoft Knowledge Base Articles:
(1) Q247811 - How Domain Controllers Are Located in Windows http://support.microsoft.com/default.aspx?scid=kb;EN-US;247811
(2) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(3) Q287156 - Troubleshooting Windows 2000 Domain Name System Dynamic Update Problems
http://support.microsoft.com/default.aspx?scid=kb;en-us;287156

(4) Q241505 - SRV Records Missing After Implementing Active Directory and Domain Name System
http://support.microsoft.com/default.aspx?scid=kb;EN-US;241505

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_DC_Response

This policy alerts the user when DNS queries made by the domain controller result in an unacceptable response time or no response. This policy contains threshold settings for a specified allowable time and when exceeded, sends a message to the HPOM browser.

The policy also logs information for reporting. Reports can be found in Reports → SPI for Active Directory.

Description	Monitors the response time of DNS queries made by the domain controller in milliseconds. Reports on whether DNS response is too long (Rule 1) or does not occur (Rule 2).
Interval	5 min
Threshold	Warning Level: ResponseTime >= 1000 (Rule 1 applies) Critical Level: ResponseTime >= 2000 (Rule 1 applies) Critical Level: Response Time = 0 (Rule 2 applies)
Message Text **Rule 1: slow response** **Rule 2: no response**	**Start Action (Rule #1, for slow response):** Domain controller <$MSG_NODE_NAME> is getting a DNS response time of <$SESSION(value)> milliseconds! It has crossed the threshold of <$SESSION(Critical\WarningThreshold)> milliseconds. The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds. **Start Action (Rule #2, for no response):** Domain controller <$MSG_NODE_NAME> is getting no response from DNS! The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> **End Action:** Domain controller <$MSG_NODE_NAME> is now getting a response from DNS.
Warning/Error Instruction Text	**Metric information:** A value of 0 milliseconds indicates that the DNS servers used by

(Rule 1: slow response)	the Domain Controller sending this message are unable to resolve a query for the Active Directory forest. A value between 1000 and 2000 milliseconds produces a 'Warning' message. A value greater than 2000 milliseconds produces a 'Critical' message. **Possible Problem(s):** The Domain Controller sending this message is getting a slow response from DNS, and may be at risk for getting no response from DNS. **Probable Cause(s):** - The Domain Controller has been configured to use one or more offline DNS Servers. - The Domain Controller has been configured to use a DNS server that is running low on resources. **Potential Impact:** This Domain Controller will experience delayed response times when attempting to contact other machines in the forest. **Suggested Action(s):** The DNS servers used by this Domain Controller are listed on the 'Message Text' tab. - Ensure that the DNS servers are functioning properly - Check the load on the DNS servers. Are they running short on resources? This could be an indicator to use a more available DNS Server or to add another DNS Server to the environment. For more information, see the Microsoft Knowledge Base Articles: 1) Q313563 - HOW TO: Configure a Secondary Name Server in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;en-us;313563 2) Q812785 - Slow Response Times Occur If a Delegated Name Server Is Down http://support.microsoft.com/default.aspx?scid=kb;en-us;812785 **Disclaimer:** Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Warning/Error Instruction Text (Rule 2: no response)	**Possible Problem(s):**
	This Domain Controller sending this message is unable to contact a DNS server.
	Probable Cause(s):
	- The Domain Controller has been configured to use DNS servers that are not available.

- A network problem is preventing the Domain Controller from contacting the DNS servers.

Potential Impact:

This Domain Controller may not be able to advertise itself in DNS or locate its replication partner.

Suggested Action(s):

The DNS servers used by this Domain Controller are listed on the 'Message Text' tab.
- Ensure that the domain controller is able to contact the DNS servers.
- Ensure that the DNS servers are functioning properly.
- Check the load on the DNS servers. Are they running short on resources? This could be an indicator to use a more available DNS Server or to add another DNS Server to the environment.

For more information, see the Microsoft Knowledge Base Article:
(1) Q169790 - How to Troubleshoot Basic TCP/IP Problems
http://support.microsoft.com/default.aspx?scid=kb;en-us;169790
(2) Q313563 - HOW TO: Configure a Secondary Name Server in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;313563

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Extra_GC_SRV_Chk

Description	**Checks for extra DNS SRV resource records registered for the global catalog.**
Interval	**24 hour**
Threshold	**Warning Level: >= 1** **Warning condition: Generates a warning message if the domain controller is registered as a Global Catalog host on a site in which it does not reside.** **The message has only warning level severity level because the situation may be intentional under certain circumstances.** **Critical Level: <= -1** **Critical condition: Checks also to see whether DC is Registered in DNS as a GC, but not registered in Active Directory as a global catalog.**
Message Text	**Start Action (Rule 1):** **Domain controller <$MSG_NODE_NAME> is registered as a global catalog for the following sites, but does not reside at them:** **<$OPTION(extraSites)>** **The domain controller has been configured to use the following DNS servers:** **<$OPTION(DnsServers)>** **End Action:** **Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a global catalog for sites that it does not reside on.** **Start Action (Rule 2):** **Domain controller <$MSG_NODE_NAME> is not a global catalog host, but it is registered as one in DNS!** **The domain controller has been configured to use the following DNS servers:** **<$OPTION(DnsServers)>** **End Action:** **Domain controller <$MSG_NODE_NAME> is no longer mis-registered as a global catalog in DNS.**
Warning (Rule 1) Instruction Text	**Metric information (Rule 1):** **A value of zero indicates that the Domain Controller that sent this message is registered in DNS to serve only the site it resides on.** **A value greater than 0 indicates that the Domain Controller that sent this message is registered in DNS as a Global Catalog for sites that it does not reside on.** **A value less than 0 indicates that the Domain Controller that sent this message**

	is registered as a Global Catalog in DNS, but does not actually host the Global Catalog. Possible Problem(s): The Domain Controller sending this message may be serving more sites than expected. Probable Cause(s): This message indicates that the specified site(s) lack a local Global Catalog. Potential Impact: The specified site(s) may experience delayed response times. In addition, those sites are at a greater risk of failure since they rely on an inter-site connection for their Global Catalog access. Suggested Actions(s): This situation may be in the AD topology by design, and therefore requires no action. If a Global Catalog is desired for each site, the 'Sites and Services' snap-in may be used to promote a domain controller on each site to fill a Global Catalog role. See Q296882 - How to promote a domain controller to a global catalog server: http://support.microsoft.com/default.aspx?scid=kb;en-us;296882 for more information on Global Catalog promotion. For more information, see the Microsoft Knowledge Base Articles: (1) Q306602 - How to Optimize the Location of a Domain Controller or Global Catalog That Resides Outside of a Client's Site http://support.microsoft.com/default.aspx?scid=kb;en-us;306602 Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.
Error (Rule 2) Instruction Text	Metric Description (Rule 2): A value of zero indicates that the Domain Controller that sent this message is registered in DNS to serve only the site it resides on. A value greater than 0 indicates that the Domain Controller that sent this message is registered in DNS as a Global Catalog for sites that it does not reside on. A value less than 0 indicates that the Domain Controller that sent this message is registered as a Global Catalog in DNS, but does not actually host the Global Catalog. Possible Problem(s): This Domain Controller is mis-advertised in DNS as a host of the Global Catalog. Probable Cause(s): This Domain Controller was most likely a former host of the Global Catalog.

Its records have been left in DNS even though it no longer hosts the Global Catalog.
Potential Impact:
Queries of the Global Catalog may be directed to this domain controller. Since the Domain Controller is not a Global Catalog host, these queries will fail causing delayed response times.
Suggested Actions(s):
The records that register this machine as a Global Catalog host may be manually removed from DNS.

For more information, see the Microsoft Knowledge Base Articles:
Q216970 - Global Catalog Server Requirement for User and Computer Logon
http://support.microsoft.com/default.aspx?scid=kb;en-us;216970
Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Extra_Kerberos_SRV_Chk

Description	Checks for records that register the domain controller as a Kerberos KDC on multiple sites.
Interval	24 hour
Threshold	**Warning** Level: >= 1
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is registered as a kerberos server for the following sites, but does not reside at them: <$OPTION(extraSites)> The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a Kerberos server for sites that it does not reside on.
Instruction Text	**Metric Description:** A value of zero indicates that the Domain Controller that sent this message is registered in DNS to serve only the site it resides on. A value greater than 0 indicates that the Domain Controller that sent this message is registered in DNS as a Kerberos server for sites that it does not reside on. **Possible Problem(s):** The Domain Controller sending this message may be serving more sites than expected. **Probable Cause(s):** This message indicates that the specified site(s) lack a local Domain Controller. **Potential Impact:** The specified site(s) may experience delayed response times. In addition, those sites are at greater risk of failure since they rely on an inter-site connection for their Kerberos access. **Suggested Actions(s):** This situation may be in the AD topology by design, and therefore requires no action. If a Domain Controller is desired for each site, a server on each site may be promoted to a Domain Controller. See Q238369 - HOW TO:

Promote and Demote Domain Controllers in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;EN-US;238369 for more information.

For more information, see the Microsoft Knowledge Base Articles:
(1) Q306602 - How to Optimize the Location of a Domain Controller or Global Catalog That Resides Outside of a Client's Site
http://support.microsoft.com/default.aspx?scid=kb;en-us;306602

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Possible Result: This policy generates a warning message if the domain controller is registered as a Kerberos KDC on a site in which it does not reside. The condition is rated at only a warning severity level because this situation may be desired under certain circumstances.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Extra_LDAP_SRV_Chk

Description Checks for records that register a domain controller as an LDAP server on multiple sites.

Interval 24 hour

Threshold Warning Level: >= 1

Message Text

Start Action:
Domain controller <$MSG_NODE_NAME> is registered as a domain controller for the following sites, but does not reside at them:
<$OPTION(extraSites)>
The domain controller has been configured to use the following DNS servers:
<$OPTION(DnsServers)>
End Action:
Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a domain controller for sites that it does not reside on.

Warning Instruction Text

Metric information:
A value of zero indicates that the Domain Controller that sent this message is registered in DNS to serve only the site it resides on.
A value greater than 0 indicates that the Domain Controller that sent this message is registered in DNS as a Domain Controller for sites that it does not reside on.

Possible Problem(s):
The Domain Controller sending this message may be serving more sites than expected.

Probable Cause(s):
This message indicates that the specified site(s) lack a local Domain Controller.
Potential Impact:
The specified site(s) may experience delayed response times. In addition, those sites are at greater risk of failure since they rely on an inter-site connection for their Domain Controller access.
Suggested Actions(s):
This situation may be in the AD topology by design, and therefore requires no action. If a Domain Controller is desired for each site, a server on each site may be promoted to a Domain Controller. See Q238369 - HOW TO: Promote and Demote Domain Controllers in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;EN-US;238369 for more information.

For more information, see the Microsoft Knowledge Base Articles:
(1) Q306602 - How to Optimize the Location of a Domain Controller or Global Catalog

That Resides Outside of a Client's Site
http://support.microsoft.com/default.aspx?scid=kb;en-us;306602

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Possible Result: This policy generates a warning message if the domain controller is registered as an LDAP server on a site in which it does not reside. The message severity level is rated warning because this can be the desired situation under certain circumstances.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_GC_A_Chk

This policy checks DNS for a domain controller hosting global catalog services. It does this by looking for the DNS host record (A record) associated with a domain controller that hosts the global catalog.

Description:	Ensures that the DNS contains the expected DNS A resource records for the global catalog.
Interval	1 hour
Threshold	Error Level: Threshold limit >= 1 Types of failures: “REG_RECORDS_FLAG_NOT_SET = 2” “DNS_SERVER_PING_FAILURE = 3” “NO_FOREST_RECOGNITION = 5” “PROBLEM_NOT_DETECTED =13”
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is missing the following records in DNS: <$OPTION(missing)> The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> <$SESSION(NetLogon)><$OPTION(NetLogonStatus)> <$SESSION(RegRecordsFlag)> <$SESSION(ServerPing)><$OPTION(FailingServers)> <$SESSION(NoForest)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.
Error Instruction Text	**Metric information:** The value obtained by this policy may be ignored by the user. All points of failure that can be detected by this policy have been assigned a prime number. The value sent to this policy is the product of the prime numbers associated with detected points of failure. It is factored to determine what went wrong, and the result is a customized 'Message Text'. **Possible Problem(s):**

(1) The domain controller sending this message may not be found by other machines in the forest.

Probable Cause(s):

One or more of the following will be true if records are missing in DNS.

The domain controller sending this message:

(1) has had a Net Logon service failure.

(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.

(3) the configuration is set to use DNS servers which are unresponsive.

(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.

(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:

(1) Domain controllers that are missing records in DNS may not be found by other machines in the forest. This can lead to replication failures and user logon failures.

Suggested Action(s):

Check the 'Message Text' section of this message for specific failures found on the domain controller.

(1) For the case of a failing Net Logon service:

- Restart the Net Logon service on the domain controller sending this message.

(2) If the domain controller is not configured to register its records in DNS:

- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.
- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.

(3) For the case of unresponsive DNS servers:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active

Directory forest:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates: This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.

For more information on troubleshooting Active Directory related DNS problems, see the Microsoft Knowledge Base Articles:
(1) Q247811 - How Domain Controllers Are Located in Windows
http://support.microsoft.com/default.aspx?scid=kb;EN-US;247811
(2) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(3) Q287156 - Troubleshooting Windows 2000 Domain Name System Dynamic Update Problems http://support.microsoft.com/default.aspx?scid=kb;en-us;287156
(4) Q240943 - Dynamic DNS Host Name Registrations
http://support.microsoft.com/default.aspx?scid=kb;en-us;240943

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_GC_Missing

This policy checks the forest for at least one registered global catalog in DNS. Without access to the forest's global catalog, an Active Directory environment becomes unusable. The user should be notified if DNS is showing no path to a forest's global catalog. Even though this policy is deployed to all managed domain controllers, it runs only on the PDC emulator for the forest's root domain to minimize monitoring time.

Description	Checks for expected DNS host record (A record) associated with a domain controller that hosts the global catalog. It generates a critical message if this record is missing.
Interval	12 hour
Threshold	Critical Level: >= 1 (Maximum number of missing records)
Message Text	No Global Catalog is registered for the following forest: <$OPTION(forest)>.
Instruction Text	Missing SRV records can typically be resolved by restarting the Netlogon service on the managed node. If this fails to solve the problem, the following are typical causes of continued failure: · The managed node is not configured to register its records dynamically in DNS. · DNS is unreachable from the managed node. · The DNS zone is not enabled for dynamic updates. · DNS records have been secured with the wrong credentials.

Possible Result: The policy generates a critical message when an Active Directory forest has no Global Catalog registered in DNS.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_GC_SRV_CHK

Active Directory Domain Controllers make their services visible in DNS by using Service Resource Records (SRV records). Clients participating in an Active Directory forest rely on these records to find Domain Controllers that host LDAP, Kerberos, and Global Catalog services.

This policy generates a critical message when a Domain Controller (DC) is not properly registered in DNS as a Global Catalog host. That is, it alerts the user when one or more SRV records that identify it as a Global Catalog host are missing. This policy is deployed to all DCs, but only runs if the DC hosts the Global Catalog. This allows the user to modify their Active Directory environment without having to modify their management software.

Description	Ensures that DNS contains the expected DNS SRV resource records for the global catalog.
Interval	1 hour
Threshold	Error Level: Threshold limit >= 1 Types of failures: “REG_RECORDS_FLAG_NOT_SET = 2” “DNS_SERVER_PING_FAILURE = 3” “NO_FOREST_RECOGNITION = 5” “PROBLEM_NOT_DETECTED = 13”
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is missing the following records in DNS: <$OPTION(missing)> The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> <$SESSION(NetLogon)><$OPTION(NetLogonStatus)> <$SESSION(RegRecordsFlag)> <$SESSION(ServerPing)><$OPTION(FailingServers)> <$SESSION(NoForest)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer missing host

records in DNS.

Instruction Text

Metric information:

The value obtained by this policy may be ignored by the user. All points of failure that can be detected by this policy have been assigned a prime number. The value sent to this policy is the product of the prime numbers associated with detected points of failure. It is factored to determine what went wrong, and the result is a customized 'Message Text'.

Possible Problem(s):

(1) The domain controller sending this message may not be found by other machines in the forest.

Probable Cause(s):

One or more of the following will be true if records are missing in DNS.
The domain controller sending this message:
(1) has had a Net Logon service failure.
(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.
(3) the configuration is set to use DNS servers which are unresponsive.
(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.
(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:

(1) Domain controllers that are missing records in DNS may not be found by other machines in the forest. This can lead to replication failures and user logon failures.

Suggested Action(s):

Check the 'Message Text' section of this message for specific failures found on the domain controller.
(1) For the case of a failing Net Logon service:
- Restart the Net Logon service on the domain controller sending this message.
(2) If the domain controller is not configured to register its records in DNS:
- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.
- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.
(3) For the case of unresponsive DNS servers:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates: This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.

For more information on troubleshooting Active Directory related DNS problems, see the Microsoft Knowledge Base Articles:
(1) Q247811 - How Domain Controllers Are Located in Windows http://support.microsoft.com/default.aspx?scid=kb;EN-US;247811
(2) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(3) Q287156 - Troubleshooting Windows 2000 Domain Name System Dynamic Update Problems http://support.microsoft.com/default.aspx?scid=kb;en-us;287156

(4) Q241505 - SRV Records Missing After Implementing Active Directory and Domain Name System http://support.microsoft.com/default.aspx?scid=kb;EN-US;241505

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Getting Started

- Microsoft Active Directory SPI Policy Catalog

Policy: ADSPI-DNS_GC_StrandedSite

Without access to the forest's Global Catalog, an Active Directory environment becomes unusable. This policy generates a warning message when an Active Directory site relies completely on one or more other sites to provide its access to the Global Catalog. It is dependent on inter-site connections for its Global Catalog access. The message severity is only at the warning level because this situation may be desirable under certain circumstances. It also generates a critical message when no Global Catalog is registered in DNS. The user should be notified if DNS is showing no path to a forest's Global Catalog.

Even though this policy is deployed to all managed Domain Controllers, it runs only on a forest’s Domain Naming Master. This minimizes monitoring time.

Description	Checks for the existence of a global catalog on every site within the forest in which the Domain Naming Master resides.
Interval	24 hour
Threshold	**Warning:** A threshold value of 1 indicates that the site this message was sent to is registered in DNS to use a Global Catalog from a different site. **Minor:** A threshold value of 2 indicates that the site this message was sent to is not registered in DNS to use any Global Catalog. **Error:** A threshold value of 3 indicates that DNS shows no site that hosts a Global Catalog.
Warning Level Message Text (scroll down for Minor/Error message and instruction text)	**Start Action:** Site <$INSTANCE> of forest <$OPTION(forest)> has no local global catalog! It is using global catalogs from the following site(s): <$OPTION(sitesUsed)> The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> **End Action:** Site <$INSTANCE> of forest <$OPTION(forest)> now has a local global catalog.
Warning Level Instruction Text	**Metric information:** A value of 3 indicates that DNS shows no site that hosts a Global Catalog. A value of 2 indicates that the site this message was sent to is not registered in DNS to use any Global Catalog. A value of 1 indicates that the site this message was sent to is registered in DNS to use a Global Catalog from a different site. A value of 0 indicates that the site this message was sent to has a local Global Catalog registered in DNS.

Possible Problem(s):
Machines at this site may experience delayed response times for operations such as user logins.

Probable Cause(s):
This message indicates that the specified site lacks a local Global Catalog.

If a Global Catalog exists on the site and its records are not showing up in DNS, then one or more of the following will be true for the Domain Controller that hosts the Global Catalog:
(1) has had a Net Logon service failure.
(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.
(3) the configuration is set to use DNS servers which are unresponsive.
(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.
(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:
The site may experience delayed response times. In addition, the site relies on an inter-site connection for its Global Catalog access.

Suggested Actions(s):
This situation may be in the AD topology by design, and therefore requires no action. If a Global Catalog is desired for the site, the 'Sites and Services' snap-in may be used to promote a domain controller on the site to fill a Global Catalog role. See Q296882 - How to promote a domain controller to a global catalog server: http://support.microsoft.com/default.aspx?scid=kb;en-us;296882 for more information on Global Catalog promotion.

If this situation is in the AD topology by design, the following may be done to avoid receiving this message in the future:

- Go to Policy Management\Policy Groups\SPI for Active Directory\Auto-Deploy\DNS Monitoring in the scope pane of the HPOM console
- Double-click the ADSPI-DNS_GC_StrandedSite policy
- click the 'Rules' tab
- Double-click 'Site has no local global catalog'
- click the 'Actions' tab
- Double-click 'Minor: A site has no local global catalog'
- Set the 'Threshold limit (Maximum)' to 2
- Click **OK** on all property sheets
- Click the 'Save and Close' button on the Policy Editor
- Right-click ADSPI-DNS_GC_StrandedSite and select All Tasks
- Select 'Deploy on...'

- Click the **OK** button

If a Global Catalog exists on the site, then check for the following conditions on the Domain Controller that hosts the Global Catalog and respond accordingly:
(1) For the case of a failing Net Logon service:
- Restart the Net Logon service on the domain controller sending this message.
(2) If the domain controller is not configured to register its records in DNS:
- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.
- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.
(3) For the case of unresponsive DNS servers:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.
(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- Verify that these are the intended DNS servers and that they are functioning properly.
(5) For the case of a DNS zone that is not enabled for dynamic updates:
This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.
For more information, see the Microsoft Knowledge Base Articles:
(1) Q306602 - How to Optimize the Location of a Domain Controller or Global Catalog That Resides Outside of a Client's Site
http://support.microsoft.com/default.aspx?scid=kb;en-us;306602

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Minor Level Message Text

Start Action:
Site <$INSTANCE> of forest <$OPTION(forest)> has no global catalog SRV record registered in DNS!
The domain controller has been configured to use the following DNS servers:
<$OPTION(DnsServers)>
End Action:
Site <$INSTANCE> of forest <$OPTION(forest)> now has a global catalog SRV record registered in DNS.

Minor Level Instruction Text

Metric information:

A value of 3 indicates that DNS shows no site that hosts a Global Catalog.

A value of 2 indicates that the site this message was sent to is not registered in DNS to use any Global Catalog.

A value of 1 indicates that the site this message was sent to is registered in DNS to use a Global Catalog from a different site.

A value of 0 indicates that the site this message was sent to has a local Global Catalog registered in DNS.

Possible Problem(s):

Machines at the specified site may experience delayed response times for operations such as user logins.

Probable Cause(s):

This message indicates that the specified site has no site-specific Global Catalog record registered in DNS.

If a Global Catalog exists on the site and its records are not showing up in DNS, then one or more of the following will be true for the Domain Controller that hosts the Global Catalog:

(1) has had a Net Logon service failure.

(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.

(3) is configured to use DNS servers which are unresponsive.

(4) is configured to use DNS servers which are not able to resolve queries for the Active Directory forest.

(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:

The machines at this site will perform a query for all Global Catalogs in the forest. Each machine will iterate through the list of returned Global Catalogs seeking a response. The first Global Catalog to respond will be the Global Catalog used. Since that Global Catalog may reside anywhere in the forest, machines at this site may experience delayed response times.

Suggested Actions(s):

If no Global Catalog exists on the site, the 'Sites and Services' snap-in may be used to promote a domain controller on the site to fill a Global Catalog role. See Q296882

- How to promote a domain controller to a global catalog server: http://support.microsoft.com/default.aspx?scid=kb;en-us;296882 for more information on Global Catalog promotion.

If a Global Catalog exists on the site, then check for the following conditions on the Domain Controller that hosts the Global Catalog and respond accordingly:

(1) For the case of a failing Net Logon service:

- Restart the Net Logon service on the domain controller sending this message.

(2) If the domain controller is not configured to register its records in DNS:

- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.

- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.

(3) For the case of unresponsive DNS servers:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.

- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.

- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates:
This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.

For more information, see the Microsoft Knowledge Base Articles:
(1) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(2) Q306602 - How to Optimize the Location of a Domain Controller or Global

Catalog That Resides Outside of a Client's Site
http://support.microsoft.com/default.aspx?scid=kb;en-us;306602

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Error Level Message Text

Start Action:
Forest <$OPTION(forest)> has no global catalog!
The domain controller has been configured to use the following DNS servers:
<$OPTION(DnsServers)>
End Action:
Forest <$OPTION(forest)> now has a global catalog registered in DNS.

Error Level Instruction Text

Metric Description:
A value of 3 indicates that DNS shows no site that hosts a Global Catalog.
A value of 2 indicates that the site this message was sent to is not registered in DNS to use any Global Catalog.
A value of 1 indicates that the site this message was sent to is registered in DNS to use a Global Catalog from a different site.
A value of 0 indicates that the site this message was sent to has a local Global Catalog registered in DNS.
Possible Problem(s):
This forest may deny all user logins due to a lack of a Global Catalog.
Probable Cause(s):
This message indicates that the forest has no Global Catalog registered in DNS.
If a Global Catalog exists in the forest and its records are not showing up in DNS, then one or more of the following will be true for the Domain Controller that hosts the Global Catalog:
(1) has had a Net Logon service failure.
(2) the configuration is not set to register its records in DNS, or manual entry of the record(s) has failed.
(3) the configuration is set to use DNS servers which are unresponsive.
(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.
(5) is using a DNS zone which is not enabled for dynamic updates.
Potential Impact:
Global catalogs are used to process user logins. Therefore, it is imperative that one be present in an Active Directory forest.
Suggested Actions(s):
If no Global Catalog exists in the forest, the 'Sites and Services' snap-in may be used to promote a domain controller to fill a Global Catalog role. See Q296882 - How to promote a domain controller to a global catalog server:
http://support.microsoft.com/default.aspx?scid=kb;en-us;296882 for more

information on Global Catalog promotion.

If a Global Catalog exists in the forest, then check for the following conditions on the Domain Controller that hosts the Global Catalog and respond accordingly:

(1) For the case of a failing Net Logon service:

- Restart the Net Logon service on the domain controller sending this message.

(2) If the domain controller is not configured to register its records in DNS:

- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.

- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.

(3) For the case of unresponsive DNS servers:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.

- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.

- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates:

- This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.

For more information, see the Microsoft Knowledge Base Articles:

(1) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371

(2)Q216970 - Global Catalog Server Requirement for User and Computer Logon
http://support.microsoft.com/default.aspx?scid=kb;en-us;216970

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Result: (1) The data for this policy is pulled from the Embedded Performance Component and logged to Reporter to generate a capacity planning report for the DNS server. (2) When necessary, the policy also generates a critical message alerting the user that the Active Directory forest has no Global Catalog registered in DNS.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Island_Server

Replication problems can occur when a domain controller has been configured to use itself as a DNS server. When such problems occur, the domain controller\DNS server is referred to as an 'island' (see Microsoft Knowledge Base article Q275278 for more information on the 'island' problem).

This policy checks for potential 'island' problems. It generates a warning message if a domain controller has been configured to use itself as a DNS server.

Description	Generates a warning message if a domain controller has been configured to use itself as a DNS server.
Interval	24 hour
Threshold	Warning Level: >=1 (Domain Controller uses itself as a DNS server.)
Message Text	**Start Action:** Domain Controller <$MSG_NODE_NAME> has been configured to use itself as a DNS server! The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> **End Action:** Domain Controller <$MSG_NODE_NAME> is no longer configured to use itself as a DNS server.
Warning Instruction Text	**Metric information:** A value of 0 indicates that the Domain Controller does not use itself as a DNS server A non-zero value indicates that the Domain Controller does use itself as a DNS server. **Possible Problem(s):** The Domain Controller sending this message may fail to replicate changes to its replication partner. **Probable Cause(s):** If the Domain Controller is running Windows 2000, it is most likely a configuration oversight. If Windows 2003 is being used, it is not a problem. **Potential Impact:** The following are problems that may be caused by an 'Island Server': - The CNAME for the Domain Controller\DNS Server is missing from _msdcs. - Changes are not replicated from the Domain Controller\DNS Server to its partners (data comes in but does not go out).

- The KCC is complaining about DNS.
- The KCC is complaining about closure.

Suggested Actions(s):

- Configure the Domain Controller to use machines other than itself for both the primary and secondary DNS servers.
- Restart the Domain Controller's NetLogon service to register CNAME and SRV records.

For more information, see the Microsoft Knowledge Base Articles:
(1) Q275278 - DNS Server Becomes an Island When a Domain Controller Points to Itself for the _Msdcs.ForestDnsName Domain
http://support.microsoft.com/default.aspx?scid=kb;en-us;275278

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_LogDNSPagesSec

The policy records pages per second that can be used to create capacity planning graphs. This is a measurement threshold policy and the default global polling interval for this policy is 10 seconds.

The policy stores the collected data into the following columns of the ADSPI_DNSSP table:

- IsDomainController
- pagesPerSec

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Kerberos_SRV_Chk

Active Directory domain controllers hosting Kerberos authentication services make their services visible through Service Resource Records (SRV records), which are generated when the service is registered in the DNS.

Checks for extra DNS SRV resource records registered for the Kerberos service. This policy generates a critical message if the domain controller is registered as a Kerberos KDC on a site in which it does not reside.

Description	Ensures that DNS contains the expected DNS Kerberos SRV resource records for the LDAP service.
Interval	1 hour
Threshold	Error Level: Threshold limit >= 1 Types of failures: "REG_RECORDS_FLAG_NOT_SET = 2" "DNS_SERVER_PING_FAILURE = 3" "NO_FOREST_RECOGNITION = 5" "PROBLEM_NOT_DETECTED = 13"
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is missing the following records in DNS: <$OPTION(missing)> The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> <$SESSION(NetLogon)><$OPTION(NetLogonStatus)> <$SESSION(RegRecordsFlag)> <$SESSION(ServerPing)><$OPTION(FailingServers)> <$SESSION(NoForest)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.
Error Instruction Text	**Metric information:** The value obtained by this policy may be ignored by the user. All points of failure that can be detected by this policy have been assigned a prime number. The value sent to this policy is the product of the prime numbers associated with detected points of failure. It is factored to determine what went wrong, and the result is a customized 'Message Text'.

Possible Problem(s):

(1) The domain controller sending this message may not be found by other machines in the forest.

Probable Cause(s):

One or more of the following will be true if records are missing in DNS.

The domain controller sending this message:

(1) has had a Net Logon service failure.

(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.

(3) the configuration is set to use DNS servers which are unresponsive.

(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.

(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:

(1) Domain controllers that are missing records in DNS may not be found by other machines in the forest. This can lead to replication failures and user logon failures.

Suggested Action(s):

Check the 'Message Text' section of this message for specific failures found on the domain controller.

(1) For the case of a failing Net Logon service:

- Restart the Net Logon service on the domain controller sending this message.

(2) If the domain controller is not configured to register its records in DNS:

- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.

- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.

(3) For the case of unresponsive DNS servers:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.

- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.

(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:

- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.

- Verify that these are the intended DNS servers and that they are functioning properly.

(5) For the case of a DNS zone that is not enabled for dynamic updates:
This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.

For more information on troubleshooting Active Directory related DNS problems, see the Microsoft Knowledge Base Articles:
(1) Q247811 - How Domain Controllers Are Located in Windows http://support.microsoft.com/default.aspx?scid=kb;EN-US;247811
(2) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(3) Q287156 - Troubleshooting Windows 2000 Domain Name System Dynamic Update Problems http://support.microsoft.com/default.aspx?scid=kb;en-us;287156

(4) Q241505 - SRV Records Missing After Implementing Active Directory and Domain Name System http://support.microsoft.com/default.aspx?scid=kb;EN-US;241505

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The ADSPI-DNS_Kerberos_SRV_Chk policy verifies that SRV records are available in the DNS for the Kerberos KDC server or Kerberos Password Change server. If these records are missing, a critical message alerts the user.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_LDAP_SRV_Chk

Active Directory Domain Controllers make their services visible in DNS by using Service Resource Records (SRV records). Clients participating in an Active Directory forest rely on these records to find Domain Controllers that host LDAP, Kerberos, and Global Catalog services.

This policy generates a critical message when a Domain Controller is not properly registered in DNS as an LDAP server. That is, it alerts the user when one or more SRV records that identify it as an LDAP server are missing.

Description	Ensures that DNS contains the expected DNS LDAP SRV resource records for the LDAP service.
Interval	1 hour
Threshold	Error Level: Threshold limit >= 1 Types of failures: “REG_RECORDS_FLAG_NOT_SET = 2” “DNS_SERVER_PING_FAILURE = 3” “NO_FOREST_RECOGNITION = 5” “PROBLEM_NOT_DETECTED = 13”
Message Text	**Start Action:** Domain controller <$MSG_NODE_NAME> is missing the following records in DNS: <$OPTION(missing)> The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> <$SESSION(NetLogon)><$OPTION(NetLogonStatus)> <$SESSION(RegRecordsFlag)> <$SESSION(ServerPing)><$OPTION(FailingServers)> <$SESSION(NoForest)> **End Action:** Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.
Instruction Text	**Metric information:** The value obtained by this policy may be ignored by the user. All points of failure that can be detected by this policy have been assigned a prime number. The value sent to this policy is the product of the prime numbers associated with detected points of failure. It is factored to determine what went wrong, and the result is a customized 'Message Text'.

Possible Problem(s):
(1) The domain controller sending this message may not be found by other machines in the forest.

Probable Cause(s):
One or more of the following will be true if records are missing in DNS.
The domain controller sending this message:
(1) has had a Net Logon service failure.
(2) has not been configured to register its records in DNS, or manual entry of the record(s) has failed.
(3) the configuration is set to use DNS servers which are unresponsive.
(4) the configuration is set to use DNS servers which are not able to resolve queries for the Active Directory forest.
(5) is using a DNS zone which is not enabled for dynamic updates.

Potential Impact:
(1) Domain controllers that are missing records in DNS may not be found by other machines in the forest. This can lead to replication failures and user logon failures.

Suggested Action(s):
Check the 'Message Text' section of this message for specific failures found on the domain controller.
(1) For the case of a failing Net Logon service:
- Restart the Net Logon service on the domain controller sending this message.
(2) If the domain controller is not configured to register its records in DNS:
- This may be done by design-- some environments are set up for manual DNS entry. In this case, verify that the missing records have been correctly entered in DNS.
- If a domain controller should be dynamically entering its records in DNS, a simple change must be made on the domain controller. See Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for instructions on making this change.
(3) For the case of unresponsive DNS servers:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- The DNS servers may be down, the connection to the DNS servers may be down, or the IP addresses for the DNS servers may be entered incorrectly on the domain controller. Verify that the domain controller configuration is set to use the desired DNS servers, verify that the DNS servers can be connected, and verify that the DNS servers are functioning properly.
(4) For the case of DNS servers unable to resolve queries for the Active Directory forest:
- The DNS servers used by the domain controller are listed on the 'Message Text' tab of this message.
- Verify that these are the intended DNS servers and that they are functioning properly.
(5) For the case of a DNS zone that is not enabled for dynamic updates:

This may be done by design-- some environments are set up for manual DNS entry. If this is not the case, see Q317590 - HOW TO: Configure DNS Dynamic Update in Windows 2000: http://support.microsoft.com/default.aspx?scid=kb;en-us;317590 for information about configuring a DNS zone to enable dynamic updates.
For more information on troubleshooting Active Directory related DNS problems, see the Microsoft Knowledge Base Articles:
(1) Q247811 - How Domain Controllers Are Located in Windows http://support.microsoft.com/default.aspx?scid=kb;EN-US;247811
(2) Q260371 - Troubleshooting Common Active Directory Setup Issues in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;260371
(3) Q287156 - Troubleshooting Windows 2000 Domain Name System Dynamic Update Problems http://support.microsoft.com/default.aspx?scid=kb;en-us;287156
(4) Q241505 - SRV Records Missing After Implementing Active Directory and Domain Name System http://support.microsoft.com/default.aspx?scid=kb;EN-US;241505

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Possible Result: This policy generates a critical message when a Domain Controller is not properly registered in DNS as an LDAP server. A service alert is also generated to alert the user that one or more SRV records that identify the Domain Controller as hosting an LDAP service are missing.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Server_Response

This policy generates messages/alerts when the DNS service is not responding to queries within a specified period of time. An unresponsive DNS server can have an adverse effect on the performance of Active Directory.

Possible Result: When a threshold is exceeded, the policy generates a message/alert to the HP Operations message browser/service map. The policy also logs data for reports.

The policy stores the collected data into the following columns of the ADSPI_DNSSR table:

- ResponseTime
- IsDomainController

Related Topics:

- Descriptions of Policy Groups and Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-DNS_Obsolete_GUIDs

Each domain controller registers in DNS by two GUIDs— a GUID referring to itself and a GUID referring to the domain it serves. When a domain controller is demoted, its GUID alias can remain in DNS even though it no longer refers to anything. The same situation can happen when a domain is removed from the Active Directory environment. These GUIDs that no longer refer to anything, or obsolete GUIDs, can create replication problems. This policy generates a critical message if any host in the forest is registered in DNS using an obsolete GUID.

This policy is deployed to all managed domain controllers, but to minimize monitoring time, the policy runs only on a forest's Infrastructure Master.

Description	In the forest in which the domain controller resides, this policy checks for hosts that are registered under obsolete GUIDs. The policy also alerts you to situations where no data is available.
Interval	1 hour
Threshold	**Error** Level: Threshold limit >= 1 (maximum number obsolete GUIDs) **Warning** Level: Threshold limit = -1 Unable to get Zone Transfer
Message Text	**Error Message Text- Start Action:** The following resource records make use of obsolete GUIDs: <$OPTION(cname)> <$OPTION(domain)> This is an indication that the following hosts have been ungracefully demoted: <$OPTION(hosts)> The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)> **End Action:** Obsolete GUIDs are no longer being used in DNS resource records. **Warning Message Text - Start Action:** The permissions on the DNS server used by this node will not allow a zone transfer. This policy uses a zone transfer to find DNS resource records that use obsolete GUIDs. Therefore, this policy is not reporting the obsolete GUIDs registered in DNS for this Active Directory forest. The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

	End Action: The DNS server used by this domain controller has been modified to allow zone transfers. This policy will now report any DNS resource records, registered for this Active Directory forest, that use obsolete GUIDs
Error Instruction Text	**Metric information:** A value less than 0 indicates that a check for DNS resource records containing obsolete GUIDs could not be performed. A value of 0 indicates that no DNS resource records containing obsolete GUIDs were found. A value greater than 0 indicates that DNS resource records containing obsolete GUIDs were found. **Possible Problem(s):** The forest may experience replication delays. **Probable Cause(s):** - In the case of dynamic DNS, this indicates one or more ungraceful Domain Controller demotions. - In the case of a manually maintained DNS, this indicates that one or more resource records have not been manually removed. **Potential Impact:** Resource records that make use of obsolete GUIDs can cause replication delays. **Suggested Action(s):** The specified records may be manually removed from DNS. For more information, see the Microsoft Knowledge Base Articles: (1) Q224544 - Determining the Server GUID of a Domain Controller http://support.microsoft.com/default.aspx?scid=kb;en-us;224544 (2) Q216498 - HOW TO: Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion http://support.microsoft.com/default.aspx?scid=kb;en-us;216498 **Disclaimer:** Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.
Warning Instruction Text	**Metric information:** A value less than 0 indicates that a check for DNS resource records containing obsolete GUIDs could not be performed. A value of 0 indicates that no DNS resource records containing obsolete GUIDs were found. A value greater than 0 indicates that DNS resource records containing obsolete GUIDs were found. **Possible Problem(s):** The forest cannot be checked for DNS resource records that use obsolete GUIDs.

Probable Cause(s):

The DNS server(s) being used by the Domain Controller that sent this message are not configured to allow zone transfers.

Potential Impact:

A check for DNS resource records that use obsolete GUIDs cannot be made.

Resource records that make use of obsolete GUIDs can cause replication problems.

Suggested Action(s):

To allow this policy to check for DNS resource records that use obsolete GUIDs:

- The Domain Controller that sent this message may be configured to use a DNS server that allows a zone transfer.
- The permissions on the DNS server(s) currently used by the managed node may be changed to allow zone transfers.

If checking done by this policy is not desired, this message may be avoided in the future by removing this policy from the Domain Controller.

For more information, see the Microsoft Knowledge Base Articles:
(1) Q193837 - Windows NT 4.0 DNS Server Default Zone Security Settings
http://support.microsoft.com/default.aspx?scid=kb;EN-US;193837
(2) Q164017 - Explanation of a DNS Zone Transfer
http://support.microsoft.com/default.aspx?scid=kb;EN-US;164017

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Possible Result: This policy generates a critical message if any host in the forest is registered in DNS using an obsolete GUID. Even though this policy is deployed to all managed domain controllers, it runs only on the PDC emulator for the forest's root domain to minimize monitoring time.

Related Topics:

- Descriptions of Policy Groups & Types
- Group Policy Catalog
- Discovery Policies

FSMO Monitoring Policies

ADSPI-FSMO_Logging *

ADSPI-FSMO_NAMING_Ping

ADSPI-FSMO_NAMING_Bind

ADSPI-FSMO_INFRA_Ping

ADSPI-FSMO_INFRA_Bind

ADSPI-FSMO_PDC_Ping

ADSPI-FSMO_PDC_Bind

ADSPI-FSMO_RID_Ping

ADSPI-FSMO_RID_Bind

ADSPI-FSMO_SCHEMA_Ping

ADSPI-FSMO_SCHEMA_Bind

ADSPI-FSMO_GC-Infra_Check*

ADSPI-FSMO Consist *

ADSPI-FSMO_Consist_INFRA

ADSPI-FSMO_Consist_NAMING

ADSPI-FSMO_Consist_PDC

ADSPI-FSMO_Consist_RID

ADSPI-FSMO_Consist_SCHEMA

ADSPI-FSMO_RoleMvmt *

ADSPI-FSMO_RoleMvmt_INFRA

ADSPI-FSMO_RoleMvmt_NAMING

ADSPI-FSMO_RoleMvmt_PDC

ADSPI-FSMO_RoleMvmt_RID

ADSPI-FSMO_RoleMvmt_SCHEMA

***** These scheduled task policies are required for the FSMO policies under them; the FSMO logging and FSMO consist policies collect the data that the other FSMO measurement threshold policies can then check for exceeded/acceptable service level objectives.

The FSMO policies are available under both the policy groups (Windows Server 2003/2000 and Windows Server 2008).

These policies are located under the following policy groups:

- *For Windows Server 2003/2000 nodes*
  SPI for Microsoft Active Directory → en (or ja) → Windows Server 2003/2000 → Auto-Deploy → FSMO Monitoring
- *For Windows Server 2008 nodes*
  SPI for Microsoft Active Directory → en (or ja) → Windows Server 2008 → Auto-Deploy → FSMO Monitoring

Related Topics:

- Descriptions of Policy Groups & Types

- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_INFRA_Bind

The infrastructure master is the DC 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.
There is one Infrastructure master per domain in a forest.

Description	Measures the response time length in seconds for the INFRA master. For this purpose, the policy periodically binds to the domain controller that is the INFRA master.
Threshold	Warning: 1 Error: 2
Message Text	**Start Actions:** The bind response time of the Infrastructure Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** Infrastructure Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text:	**Possible Problem(s):** (1) The bind response time of the Infrastructure Master FSMO role is high. (2) Infrastructure Master FSMO role is unresponsive. **Probable Cause(s):** Infrastructure Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Group-to-user and cross-domain references might not be updated by the Infrastructure Master FSMO role. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the Infrastructure Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the same domain.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_INFRA_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. There is one Infrastructure master per domain in a forest.

Description	Measures the response time length in seconds for the INFRA master. For this purpose, the policy periodically pings the domain controller that is the INFRA master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The ping response time of the Infrastructure Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** Infrastructure Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning/ Error Instruction Text:	**Possible Problem(s):** (1) The ping response time of the Infrastructure Master FSMO role is high. (2) Infrastructure Master FSMO role is unresponsive. **Probable Cause(s):** Infrastructure Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** Group-to-user and cross-domain references might not be updated by the Infrastructure Master FSMO role. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the Infrastructure Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the same domain. For more information see the Microsoft Knowledge Base Article: (1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process

http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_Logging

Description

A scheduled task policy that binds and pings each of the five FSMO role holders. It logs the bind and ping response times, and sends the response times to the appropriate ADSPI-FSMO_<role>_Ping and ADSPI-FSMO_<role>_Bind policy.

Interval

5 min

Instruction Text

Possible Problem(s):
(1) Failed to run ADSPI_FSMO.exe.

Probable Cause(s):
(1) The user does not have sufficient privileges to run this command.
(2) The policy is not running on a domain controller.

Potential Impact:
The policy will not be able to log the bind and ping response times of the FSMO roles into CODA.

Suggested Action(s):
(1) Fix any GPOs that restrict the privileges of the agent user account($AGENT_USER).

For more information see the Microsoft Knowledge Base Article:
(1) Q321709 - HOW TO: Use the Group Policy Results Tool in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;IT;321709
(2) Q226243 - HOW TO: Reset User Rights in the Default Domain Group Policy
http://support.microsoft.com/default.aspx?scid=kb;EN-US;226243

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the following columns of the ADSPI_FSMO table:

- SERVER
- FSMO
- PINGTIME
- BINDTIME

Related Topics:

- FSMO Policies
- Descriptions of Policy Groups & Types
- Group Policy Catalog
- Choosing a Microsoft Active Directory SPI policy

Policy: ADSPI-FSMO_NAMING_Bind

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. There is only one domain naming master in the forest.

Description	Measures the response time length in seconds for the domain-naming master. For this purpose, the policy periodically binds to the domain controller that is the domain-naming master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The bind response time of the Domain Naming Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** Domain Naming Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text:	**Possible Problem(s):** (1) The bind response time of the Domain Naming Master FSMO role is high. (2) Domain Naming Master FSMO role is unresponsive. **Probable Cause(s):** Domain Naming Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Active Directory administrators might be unable to add/remove domains. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the Domain Naming Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise. For more information see the Microsoft Knowledge Base Article: (1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process

http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Group Policy Catalog
- Discovery Policies

Policy: ADSPI-FSMO_NAMING_Ping

This policy, working in conjunction with the scheduled task policy ADSPI-FSMO_Logging, measures the general responsiveness of the domain-naming master and allows thresholding on that measurement. The policy periodically pings the domain controller that is the domain-naming master.

Description	Measures the response time length in seconds for the domain-naming master. For this purpose, the policy periodically pings the domain controller that is the domain-naming master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The ping response time of the Domain Naming master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** Domain Naming Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text:	**Possible Problem(s):** (1) The ping response time of the Domain Naming Master FSMO role is high. (2) Domain Naming Master FSMO role is unresponsive. **Probable Cause(s):** Domain Naming Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Active Directory administrators might be unable to add/remove domains. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the Domain Naming Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise. For more information see the Microsoft Knowledge Base Article: (1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process

http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787

(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller

http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The domain-naming master is the DC 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. There is only one domain-naming master in the forest.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_PDC_Bind

The PDC master is a Windows 2000 domain controller that acts as the primary domain controller to down-level workstations, member servers and domain controllers.

Description	Measures the response time length in seconds for the PDC master. For this purpose, the policy periodically binds to the domain controller that is the PDC master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The bind response time of the PDC Emulator FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** PDC Emulator bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text	**Possible Problem(s):** (1) The bind response time of the PDC Emulator FSMO role is high. (2) PDC Emulator FSMO role is unresponsive. **Probable Cause(s):** PDC Emulator FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Time might not be synchronized in the Active Directory enterprise. (2) Password changes might not be replicated preferentially to the PDC Emulator. (3) The PDC emulator might not be able to advertise itself as the primary domain controller (PDC) to workstations, member servers, and domain controllers that are running earlier versions of Windows. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the PDC Emulator FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

In a Windows 2000 domain, the PDC master also performs the following functions:

- Password changes performed by other domain controllers in the domain are replicated preferentially to the PDC master.
- Authentication failures that occur at a given domain controller in a domain because of an incorrect password go to the PDC master before a bad password failure message is reported to the user.
- Account lockout is processed on the PDC master.

There is one PDC master per domain in a forest.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_RID_Bind

The RID master is the DC responsible for processing RID Pool requests from all domain controllers within a given domain. When a DC 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.

This policy works in conjunction with the ADSPI-FSMO_Logging policy.

Description	Measures the response time length in seconds for the RID master. For this purpose, the policy periodically binds to the domain controller that is the RID master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The bind response time of the RID Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** RID Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text	**Possible Problem(s):** (1) The bind response time of the RID Master FSMO role is high. (2) RID Master FSMO role is unresponsive. **Probable Cause(s):** RID Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Users will not be able to create objects in the domain, if it runs out of relative identifiers. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and

detecting Active Directory attacks.
(2) If the RID Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_RID_Ping

The RID master is the DC responsible for processing RID Pool requests from all domain controllers within a given domain. When a DC 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).

This policy works in conjunction with ADSPI-FSMO_Logging policy.

Description	Measures the response time length in seconds for the RID master. For this purpose, the policy periodically pings the domain controller that is the RID master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The ping response time of the RID Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** RID Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text	**Possible Problem(s):** (1) The ping response time of the RID Master FSMO role is high. (2) RID Master FSMO role is unresponsive. **Probable Cause(s):** RID Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Users will not be able to create objects in the domain, if it runs out of relative identifiers. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the RID Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_RoleMvmt

This scheduled task policy runs once every hour to determine if the domain controller it is running on has gained or lost one of the five FSMO roles. It sends the role movement information that it collects to the following policies:

- ADSPI-FSMO_RoleMvmt_INFRA
- ADSPI-FSMO_RoleMvmt_NAMING,
- ADSPI-FSMO_RoleMvmt_PDC,
- ADSPI-FSMO_RoleMvmt_RID
- ADSPI-FSMO_RoleMvmt_SCHEMA

These five policies then, as changes occur, send tailored messages back to the management server.

Description	Determines when a FSMO role is seized or transferred from one domain controller to another.
Interval	1 hour
Warning Error Instruction Text:	**Possible Problem(s):** (1) Failed to run ADSPI_RoleMvmt.exe. **Probable Cause(s):** (1) The user does not have sufficient privileges to run this command. (2) The policy is not running on a domain controller. **Potential Impact:** The policy will not be able to determine the movement of FSMO roles on this domain controller. **Suggested Action(s):** (1) Fix any GPOs that restrict the privileges of the agent user account($AGENT_USER). For more information see the Microsoft Knowledge Base Article: (1) Q321709 - HOW TO: Use the Group Policy Results Tool in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;IT;321709 (2) Q226243 - HOW TO: Reset User Rights in the Default Domain Group

	Policy http://support.microsoft.com/default.aspx?scid=kb;EN-US;226243

The policy stores the collected data into the following columns of the ADSPI_FSMO_ROLEMVMT table:

- FSMO
- ISROLEHOLDER

Related Topics:

- Descriptions of Policy Groups & Types
- Active Directory SPI FSMO Policies
- Discovery Policies

Policy: ADSPI-FSMO_RoleMvmt_INFRA

FSMO roles may be transferred between domain controllers by an administrator. In addition, a FSMO role will be automatically transferred if a domain controller that hosts the role is demoted. This policy sends alarms to the management server if the local domain controller acquires or loses ownership of the Infrastructure Master FSMO role.

Description	Monitors the domain controller's ownership of the Infrastructure Master FSMO role.
Threshold	Change in FSMO role assigned to domain controller.
Message Text	**Rule 1:** Domain Controller Acquired FSMO Role Ownership Message Text: **Start Actions:** Domain controller <$MSG_NODE_NAME> has acquired the Infrastructure Master FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>. **Rule 2:** Domain Controller Lost FSMO Role Ownership Message Text: **Start Actions:** Domain controller <$MSG_NODE_NAME> no longer owns the Infrastructure Master FSMO role for domain <$OPTION(domain)>. This role is now owned by <$OPTION(holder)>.
Warning & Error Instruction Text	**Rule 1:** The local domain controller has acquired ownership of the Infrastructure Master FSMO role. **Possible Problem(s:** (1) The former owner of the Infrastructure Master FSMO role may have been demoted. (2) An unplanned transfer of the Infrastructure Master FSMO role can indicate human error or a security breach. **Probable Cause(s):** (1) The former owner of the Infrastructure Master FSMO role has been demoted. (2) An administrator has transferred or seized the Infrastructure Master FSMO role to the local domain controller. **Potential Impact:** (1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information. **Suggested Action(s):** (1) Verify that the transfer of the Infrastructure Master FSMO role was an expected

event in your environment.

For more information see the Microsoft Knowledge Base Article:
(1) Q223346 - FSMO placement and optimization on Windows 2000 domain controllers
http://support.microsoft.com/kb/223346/EN-US/
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Rule 2: The local domain controller has given up ownership of the Infrastructure Master FSMO role.
Possible Problem(s):
(1) An unplanned transfer of the Infrastructure Master FSMO role can indicate human error or a security breach.
Probable Cause(s):
(1) An administrator has transferred or seized the Infrastructure Master FSMO role to another domain controller.
Potential Impact:
(1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information.
Suggested Action(s):
(1) Verify that the transfer of the Infrastructure Master FSMO role was an expected event in your environment.

For more information see the Microsoft Knowledge Base Article:
(1) Q223346 - FSMO placement and optimization on Windows 2000 domain controllers
http://support.microsoft.com/kb/223346/EN-US/
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Active Directory SPI FSMO Policies
- Discovery Policies

Policy: ADSPI-FSMO_RoleMvmt_NAMING

FSMO roles may be transferred between domain controllers by an administrator. In addition, a FSMO role will be automatically transferred if a domain controller that hosts the role is demoted. This measurement threshold policy sends alarms to the management server if the local domain controller acquires or loses ownership of the Domain Naming Master FSMO role.

Description	Monitors the domain controller's ownership of the Domain Naming Master FSMO role.
Threshold	Change in FSMO role assigned to domain controller.
Message Text	**Rule 1:** Domain Controller Acquired FSMO Role Ownership **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> has acquired the Domain Naming Master FSMO role forest <$OPTION(forest)>. This role was formerly owned by <$OPTION(holder)>. **Rule 2:** Domain Controller Lost FSMO Role Ownership **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> no longer owns the Domain Naming Master FSMO role forest <$OPTION(forest)>. This role is now owned by <$OPTION(holder)>.
Warning & Error Instruction Text	**Rule 1 Condition:** The local domain controller has acquired ownership of the Domain Naming Master FSMO role. **Possible Problem(s):** (1) The former owner of the Domain Naming Master FSMO role may have been demoted. (2) An unplanned transfer of the Domain Naming Master FSMO role can indicate human error or a security breach. **Probable Cause(s):** (1) The former owner of the Domain Naming Master FSMO role has been demoted. (2) An administrator has transferred or seized the Domain Naming Master FSMO role to the local domain controller. **Potential Impact:** (1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information. **Suggested Action(s):**

(1) Verify that the transfer of the Domain Naming Master FSMO role was an expected event in your environment.

Rule 2 Condition:
The local domain controller has given up ownership of the Domain Naming Master FSMO role.
Possible Problem(s):
(1) An unplanned transfer of the Domain Naming Master FSMO role can indicate human error or a security breach.
Probable Cause(s):
(1) An administrator has transferred or seized the Domain Naming Master FSMO role to another domain controller.
Potential Impact:
(1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information.
Suggested Action(s):
(1) Verify that the transfer of the Domain Naming Master FSMO role was an expected event in your environment.

For more information see the Microsoft Knowledge Base Article:
(1) Q223346 - FSMO placement and optimization on Windows 2000 domain controllers
http://support.microsoft.com/kb/223346/EN-US/
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site.
HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Active Directory SPI FSMO Policies
- Discovery Policies

Policy: ADSPI-FSMO_RoleMvmt_PDC

FSMO roles may be transferred between domain controllers by an administrator. In addition, a FSMO role will be automatically transferred if a domain controller that hosts the role is demoted. This measurement threshold policy sends alarms to the management server if the local domain controller acquires or loses ownership of the PDC Emulator FSMO role.

Description	Monitors the domain controller's ownership of the PDC Emulator FSMO role.
Threshold	Change in FSMO role assigned to domain controller.
Message Text	**Rule 1:** Domain Controller Acquired FSMO Role Ownership| **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> has acquired the PDC Emulator FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>.
Warning & Error Instruction Text	**Rule 1 Condition:** The local domain controller has acquired ownership of the PDC Emulator FSMO role. **Possible Problem(s):** (1) The former owner of the PDC Emulator FSMO role may have been demoted. (2) An unplanned transfer of the PDC Emulator FSMO role can indicate human error or a security breach. |**Probable Cause(s):** (1) The former owner of the PDC Emulator FSMO role has been demoted. (2) An administrator has transferred or seized the PDC Emulator FSMO role to the local domain controller.| **Potential Impact:** (1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information. **Suggested Action(s):** (1) Verify that the transfer of the PDC Emulator FSMO role was an expected event in your environment. **Rule 2 Condition:** The local domain controller has acquired ownership of the PDC Emulator FSMO role. Possible Problem(s): (1) The former owner of the PDC Emulator FSMO role may have been demoted. (2) An unplanned transfer of the PDC Emulator FSMO role can indicate human error or a security breach.

Probable Cause(s):
(1) The former owner of the PDC Emulator FSMO role has been demoted.
(2) An administrator has transferred or seized the PDC Emulator FSMO role to the local domain controller.
| **Potential Impact:**
(1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information.

Suggested Action(s):
(1) Verify that the transfer of the PDC Emulator FSMO role was an expected event in your environment.

For more information see the Microsoft Knowledge Base Article:
(1) Q223346 - FSMO placement and optimization on Windows 2000 domain controllers
http://support.microsoft.com/kb/223346/EN-US/
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Active Directory SPI FSMO Policies
- Discovery Policies

Policy: ADSPI-FSMO_RoleMvmt_RID

FSMO roles may be transferred between domain controllers by an administrator. In addition, a FSMO role will be automatically transferred if a domain controller that hosts the role is demoted. This measurement threshold policy sends alarms to the management server if the local domain controller acquires or loses ownership of the RID Master FSMO role.

Description	Monitors the domain controller's ownership of the RID Master FSMO role.
Threshold	Change in FSMO role assigned to domain controller.
Message Text	**Rule 1:** Domain Controller Acquired FSMO Role Ownership **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> has acquired the RID Master FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>. **Rule 2:** Domain Controller Lost FSMO Role Ownership **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> no longer owns the RID Master FSMO role for domain <$OPTION(domain)>. This role is now owned by <$OPTION(holder)>.
Warning & Error Instruction Text	**Rule 1 Condition:** The local domain controller has acquired ownership of the RID Master FSMO role. **Possible Problem(s):** (1) The former owner of the RID Master FSMO role may have been demoted. (2) An unplanned transfer of the RID Master FSMO role can indicate human error or a security breach. **Probable Cause(s):** (1) The former owner of the RID Master FSMO role has been demoted. (2) An administrator has transferred or seized the RID Master FSMO role to the local domain controller. **Potential Impact:** (1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information. **Suggested Action(s):**

(1) Verify that the transfer of the RID Master FSMO role was an expected event in your environment.

Rule 2 Condition: The local domain controller has given up ownership of the RID Master FSMO role.
Possible Problem(s):
(1) An unplanned transfer of the RID Master FSMO role can indicate human error or a security breach.
Probable Cause(s):
(1) An administrator has transferred or seized the RID Master FSMO role to another domain controller.
Potential Impact:
(1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information.

Suggested Action(s):
(1) Verify that the transfer of the RID Master FSMO role was an expected event in your environment.

For more information see the Microsoft Knowledge Base Article:
(1) Q223346 - FSMO placement and optimization on Windows 2000 domain controllers
http://support.microsoft.com/kb/223346/EN-US/
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Active Directory SPI FSMO Policies
- Discovery Policies

Policy: ADSPI-FSMO_RoleMvmt_SCHEMA

FSMO roles may be transferred between domain controllers by an administrator. In addition, a FSMO role will be automatically transferred if a domain controller that hosts the role is demoted. This measurement threshold policy sends alarms to the management server if the local domain controller acquires or loses ownership of the Schema Master FSMO role.

Description	Monitors the domain controller's ownership of the Schema Master FSMO role.
Threshold	Change in FSMO role assigned to domain controller.
Message Text	**Rule 1:** Domain Controller Acquired FSMO Role Ownership **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> has acquired the Schema Master FSMO role forest <$OPTION(forest)>. This role was formerly owned by <$OPTION(holder)>. **Rule 2:** Domain Controller Lost FSMO Role Ownership **Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> no longer owns the Schema Master FSMO role forest <$OPTION(forest)>. This role is now owned by <$OPTION(holder)>.
Warning & Error Instruction Text	**Rule 1 Condition:** The local domain controller has acquired ownership of the Schema Master FSMO role. **Possible Problem(s):** (1) The former owner of the Schema Master FSMO role may have been demoted. (2) An unplanned transfer of the Schema Master FSMO role can indicate human error or a security breach. **Probable Cause(s):** (1) The former owner of the Schema Master FSMO role has been demoted. (2) An administrator has transferred or seized the Schema Master FSMO role to the local domain controller. **Potential Impact:** (1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information. **Suggested Action(s):** (1) Verify that the transfer of the Schema Master FSMO role was an expected event in your environment.

Rule 2 Condition: The local domain controller has given up ownership of the Schema Master FSMO role.
Possible Problem(s):
(1) An unplanned transfer of the Schema Master FSMO role can indicate human error or a security breach.
Probable Cause(s):
(1) An administrator has transferred or seized the Schema Master FSMO role to another domain controller.
Potential Impact:
(1) The location of your FSMO role holders can affect the performance of your Active Directory environment. See Q223346 - FSMO Placement and Optimization on Windows 2000 Domain Controllers http://support.microsoft.com/kb/223346/EN-US/ for more information.
Suggested Action(s):
(1) Verify that the transfer of the Schema Master FSMO role was an expected event in your environment.

For more information see the Microsoft Knowledge Base Article:
(1) Q223346 - FSMO placement and optimization on Windows 2000 domain controllers
http://support.microsoft.com/kb/223346/EN-US/
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Active Directory SPI FSMO Policies
- Discovery Policies

Policy: ADSPI-FSMO_SCHEMA_Bind

The schema master is the domain controller responsible for performing updates to the directory schema. After the schema update is complete, it is replicated to the other domain controllers in the forest. There is only one schema master in a forest.

This policy works in conjunction with the ADSPI-FSMO_Logging policy.

Description	Measures the response time length in seconds for the schema master. For this purpose, the policy periodically binds to the domain controller that is the schema master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The bind response time of the Schema Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** Schema Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text	**Possible Problem(s):** (1) The bind response time of the Schema Master FSMO role is high. (2) Schema Master FSMO role is unresponsive. **Probable Cause(s):** Schema Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Administrators might NOT be able to modify the Active Directory schema. (2) Administrators might NOT be allowed to install an application that modifies the schema during installation. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the Schema Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Discovery Policies

Policy: ADSPI-FSMO_SCHEMA_Ping

The schema master is the domain controller responsible for performing updates to the directory schema. After the schema update is complete, it is replicated to the other domain controllers in the forest. There is only one schema master in a forest.

This policy works in conjunction with the ADSPI-FSMO_Logging policy.

Description	Measures the response time length in seconds for the schema master. For this purpose, the policy periodically pings the domain controller that is the schema master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	Start Actions: The ping response time of the Schema Master FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. End Actions: Schema Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.
Warning & Error Instruction Text	**Possible Problem(s):** (1) The ping response time of the Schema Master FSMO role is high. (2) Schema Master FSMO role is unresponsive. **Probable Cause(s):** Schema Master FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Administrators might NOT be able to modify the Active Directory schema. (2) Administrators might NOT be allowed to install an application that modifies the schema during installation. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the Schema Master FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

This policy, working in conjunction with the ADSPI-FSMO_Logging policy, measures the general responsiveness of the schema master. It periodically pings the domain controller that is the schema master and monitors the ping response time.

The schema master is the domain controller responsible for performing updates to the directory schema. After the schema update is complete, it is replicated to the other domain controllers in the forest. There is only one schema master in a forest.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_Consist

Replication problems can occur when a domain controller is demoted from a domain and its master operation roles are not transferred to another domain controller. Such a situation can happen if the domain controller is not properly demoted or is taken off line without transferring role responsibilities. In such cases, master operation identification becomes inconsistent.

Description	A scheduled task policy that performs configuration checks. First the policy identifies the FSMO master operations running on the domain controller (DC); then the policy verifies that the information is also present on the DC's replication partners.
Interval	24 hours
Consistency State	The detected state is compared to the measurement threshold policy that matches the FSMO service, resulting in appropriate service map alerts and messages to the HPOM message browser. • state 0 = DC information is present and consistent • state 1 = DC information is not present on the domain controller (critical) • state 2 = DC information is not present on the replication partner (critical) • state 3 = DC information is present on domain controller and replication partner, but is not consistent (warning)
Instruction Text:	**Possible Problem(s):** (1) Failed to run ADSPI_Consist.exe. **Probable Cause(s):** (1) The user does not have sufficient privileges to run this command. (2) The policy is not running on a domain controller. **Potential Impact:** The policy will not be able to calculate the consistency of the FSMO roles on this domain controller with respect to its replication partners. **Suggested Action(s):** (1) Fix any GPOs that restrict the privileges of the agent user account($AGENT_USER). For more information see the Microsoft Knowledge Base Article: (1) Q321709 - HOW TO: Use the Group Policy Results Tool in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;IT;321709 (2) Q226243 - HOW TO: Reset User Rights in the Default Domain Group Policy http://support.microsoft.com/default.aspx?scid=kb;EN-US;226243 Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site.

HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_Consist_INFRA

The ADSPI-FSMO_Consist_INFRA policy is used to monitor any domain controller running infrastructure master services. This measurement threshold policy works in conjunction with the ADSPI-FSMO_Consist scheduled task policy, by comparing its defined threshold to the data it receives from the FSMO_Consist scheduled task policy.

Description	The ADSPI-FSMO_Consist_INFRA policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_INFRA alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the FSMO INFRA role.
Interval	N/A
Consistency State	• state 0 = infrastructure master information is present on the domain controller and is consistent on the replication partner (desired state; no action) • state 1 = infrastructure master information is not present on the domain controller (critical) • state 2 = infrastructure master information is not present on the replication partner (critical) • state 3 = infrastructure master information is present on domain controller and replication partner, but is not consistent (warning)
Message Text	**Start Actions:** Infrastructure Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE> **End Actions:** Infrastructure Master FSMO Role on domain controller <$MSG_NODE_NAME> is consistent with that of the replication partner <$INSTANCE>.
Instruction Text	**Possible Problem(s):** (1) Infrastructure Master FSMO role is not defined on the domain controller. (2) Infrastructure Master FSMO role is not defined on one or more of the replication partners. (3) Infrastructure Master FSMO role on the domain controller is inconsistent with respect to that of the replication partner. **Probable Cause(s):** A domain controller in the domain (1) is not properly demoted. (2) is taken offline without transferring role responsibilities.

Potential Impact:
(1) Group-to-user and cross-domain object references might not be updated.
Suggested Action(s):
(1) Remove the data in Active Directory using \"Ntdsutil\" if there was an unsuccessful domain controller demotion attempt.
For more information see the Microsoft Knowledge Base Article:
(1) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
(2) Q216498 - HOW TO: Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion
http://support.microsoft.com/default.aspx?scid=kb;EN-US;216498
(3) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_Consist_NAMING

Description

The ADSPI-FSMO_Consist_NAMING policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_NAMING alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the FSMO Naming role.

Threshold

The FSMO_Consist_NAMING policy can execute an action in the form of a service map alert or message to the HPOM console when the data it receives on the domain-naming master matches a detected state as follows:

- state 0 = domain-naming master information is present on the domain controller and is consistent on the replication partner (desired state; no action)
- state 1 = domain-naming master information is not present on the domain controller (critical)
- state 2 = domain-naming master information is not present on the replication partner (critical)
- state 3 = domain-naming master information is present on domain controller and replication partner, but is not consistent (warning< /LI >< /LI >< /LI >< /LI >

Message Text

Start Actions:
Domain Naming Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
End Actions:
Domain Naming Master FSMO Role on domain controller <$MSG_NODE_NAME> is consistent with that of the replication partner <$INSTANCE>.

Instruction Text

Possible Problem(s):
(1) Domain Naming Master FSMO role is not defined on the domain controller.
(2) Domain Naming Master FSMO role is not defined on one or more of the replication partners.
(3) Domain Naming Master FSMO role on the domain controller is inconsistent with respect to that of the replication partner.

Probable Cause(s):
A domain controller in the domain
(1) is not properly demoted.

(2) is taken offline without transferring role responsibilities.

Potential Impact:
(1) Active Directory administrators might be unable to add/remove domains.

Suggested Action(s):
(1) Remove the data in Active Directory using \"Ntdsutil\" if there was an unsuccessful domain controller demotion attempt.

For more information see the Microsoft Knowledge Base Article:
(1) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
(2) Q216498 - HOW TO: Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion
http://support.microsoft.com/default.aspx?scid=kb;EN-US;216498
(3) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_Consist_PDC

The ADSPI-FSMO_Consist_PDC policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_PDC alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the PDC FSMO role.

Description	The ADSPI-FSMO_Consist_PDC policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_PDC alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the FSMO PDC role.
Threshold	The FSMO_Consist_PDC policy can execute an action in the form of a service map alert or message to the HPOM console when the data it receives on the PDC master matches a detected state as follows: • state 0 = local and remote FSMOs are consistent • state 1 = no FSMO found for local host • state 2 = no FSMO found on replication partner • state 3 = replication partner and local FSMO are different
Message Text	**Start Actions:** PDC Emulator FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>. **End Actions:** PDC Emulator FSMO Role on domain controller <$MSG_NODE_NAME> is consistent with that of the replication partner <$INSTANCE>.
Instruction Text	**Possible Problem(s):** (1) PDC Emulator FSMO role is not defined on the domain controller. (2) PDC Emulator FSMO role is not defined on one or more of the replication partners. (3) PDC Emulator FSMO role on the domain controller is inconsistent with respect to that of the replication partner. **Probable Cause(s):** A domain controller in the domain (1) is not properly demoted. (2) is taken offline without transferring role responsibilities. **Potential Impact:** (1) Time might not be synchronized in the Active Directory enterprise. (2) Password changes might not be replicated preferentially to the PDC Emulator. (3) The PDC emulator might not be able to advertise itself as the primary domain controller (PDC) to workstations, member servers, and domain controllers that are

running earlier versions of Windows.
Suggested Action(s):
(1) Remove the data in Active Directory using \"Ntdsutil\" if there was an unsuccessful domain controller demotion attempt.

For more information see the Microsoft Knowledge Base Article:
(1) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
(2) Q216498 - HOW TO: Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion
http://support.microsoft.com/default.aspx?scid=kb;EN-US;216498
(3) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_PDC_Ping

This policy, working in conjunction with the ADSPI-FSMO_Logging policy, measures the general responsiveness of the PDC master and allows thresholding on that measurement. It periodically pings the domain controller that is the PDC master. Monitors the ping response time of the PDC FSMO.

Description	Measures the response time length in seconds for the PDC master. For this purpose, the policy periodically pings the domain controller that is the PDC master.
Threshold	Warning: 1 second Error: 2 seconds
Message Text	**Start Actions:** The ping response time of the PDC Emulator FSMO role <$INSTANCE> on domain controller <$MSG_NODE_NAME> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec. **End Actions:** PDC Emulator ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>.
Waring & Error Instruction Text	**Possible Problem(s):** (1) The ping response time of the PDC Emulator FSMO role is high. (2) PDC Emulator FSMO role is unresponsive. **Probable Cause(s):** PDC Emulator FSMO role (1) is over-used. (2) might be under a denial-of-service attack. (3) is unavailable. **Potential Impact:** (1) Time might not be synchronized in the Active Directory enterprise. (2) Password changes might not be replicated preferentially to the PDC Emulator. (3) The PDC emulator might not be able to advertise itself as the primary domain controller (PDC) to workstations, member servers, and domain controllers that are running earlier versions of Windows. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the PDC Emulator FSMO role is unavailable and cannot be brought back into

the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(2) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The PDC master 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 2000 domain, the PDC master also performs the following functions:

- Password changes performed by other domain controllers in the domain are replicated preferentially to the PDC master.
- Authentication failures that occur at a given domain controller in a domain because of an incorrect password go to the PDC master before a bad password failure message is reported to the user.
- Account lockout is processed on the PDC master.

There is one PDC master per domain in a forest.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-FSMO_Consist_RID

The ADSPI-FSMO_Consist_NAMING policy is used to monitor any domain controller responsible for processing relative identification (RID) pool requests from all domain controllers within a given domain. This measurement threshold policy works in conjunction with the ADSPI-FSMO_Consist scheduled task policy, by comparing its defined threshold to data received from the FSMO_Consist scheduled task policy.

Description

The ADSPI-FSMO_Consist_RID policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. ADSPI-FSMO_Consist_RID alarms if the local domain controller does not agree with one or more of its replication partners on which machine hosts the FSMO RID role.

Consistency State

The FSMO_Consist_RID policy can execute an action in the form of a service map alert or message to the HPOM console when the data it receives on the RID master matches a detected state as follows:

- state 0 = local and remote FSMOs are consistent
- state 1 = no FSMO found for local host
- state 2 = no FSMO found on replication partner
- state 3 = replication partner and local FSMO are different

Message Text

Start Actions:
RID Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
End Actions:
RID Master FSMO Role on domain controller <$MSG_NODE_NAME> is consistent with that of the replication partner <$INSTANCE>.

Instruction Text

Possible Problem(s):
(1) RID Master FSMO role is not defined on the domain controller.
(2) RID Master FSMO role is not defined on one or more of the replication partners.
(3) RID Master FSMO role on the domain controller is inconsistent with respect to that of the replication partner.
Probable Cause(s):
A domain controller in the domain
(1) is not properly demoted.
(2) is taken offline without transferring role responsibilities.
Potential Impact: Users will not be able to create objects in the domain, if it runs out of relative identifiers.

Suggested Action: Remove the data in Active Directory using \"Ntdsutil\" if there was an unsuccessful domain controller demotion attempt.

For more information see the Microsoft Knowledge Base Article:
(1) Q197132 - Windows 2000 Active Directory FSMO Roles
http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132
(2) Q216498 - HOW TO: Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion
http://support.microsoft.com/default.aspx?scid=kb;EN-US;216498
(3) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Replication Monitoring Policies

Policies for Windows Server 2003/2000

ADSPI-Rep_Mon_Fwd_Ping_Messages

ADSPI-Rep_Delete_OvRep_Object

ADSPI-Rep_InboundObjs

ADSPI-Rep_CheckObj

ADSPI-REP_ModifyObj *

ADSPI-Rep_Modify_User_Object *

ADSPI-Rep_MonitorIntraSiteReplication

ADSPI-Rep_MonitorInterSiteReplication

ADSPI-Rep_ISM_Chk

ADSPI-Rep_TimeSync

Policies for Windows Server 2008

ADSPI-Rep_Mon_Fwd_Ping_Messages

ADSPI-Rep_Delete_OvRep_Object

ADSPI-Rep_InboundObjs_2k8+

ADSPI-Rep_CheckObj

ADSPI-REP_ModifyObj *

ADSPI-Rep_Modify_User_Object *

ADSPI-Rep_MonitorIntraSiteReplication

ADSPI-Rep_MonitorInterSiteReplication

ADSPI-Rep_ISM_Chk

ADSPI-Rep_TimeSync

***** These scheduled task policies provide the required data for other replication-checking policies, **ADSPI-Rep_Mon** , **ADSPI-Rep_CheckObj** , and **ADSPI-Rep_GC_Check_and_Threshold** , to measure. These measurement threshold policies rely on the scheduled task policy to periodically modify an object, which can then check for its replication on other DCs.

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Policy: ADSPI-Rep_CheckObj

The ADSPI monitors replication latency by inserting an object into AD and measuring the amount of time required to replicate an attribute through the Active Directory forest.

- ADSPI-Rep_Modify_User_Object (creates the object to be replicated)
- ADSPI-Rep_Mon (measures the time it takes to replicate the object)

Description:	Identifies DCs that do not contain the replication object and issue an alert when found.
Interval	24 hour
Threshold	N/A
Message:	**Start Actions:** An HPOM replication object doesn't exist for domain controller(s) <$SESSION(DC)>! **End Actions:** -- none --
Warning Instruction Text:	**Possible Problem(s):** (1) OvReplication object is not present on the domain controller. **Probable Cause(s):** (1) As part of the demotion process, the DCPROMO utility removes the configuration data for the domain controller from the Active Directory. This data takes the form of an \"NTDS Settings\" object, which exists as a child to the server object in the Active Directory Sites and Services Manager. One might get this alarm when the NTDS Settings object is not removed properly during a demotion attempt. **Potential Impact:** (1) The replication latency between this domain controller and its replication partners will not be calculated. **Suggested Action(s):** (1) Remove the data in Active Directory using \"Ntdsutil\" if there was an unsuccessful domain controller demotion attempt. For more information see the Microsoft Knowledge Base Article: (1) Q216498 - HOW TO: Remove Data in Active Directory After an Unsuccessful Domain Controller Demotion http://support.microsoft.com/default.aspx?scid=kb;en-us;216498 Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The ADSPI-Rep_CheckObj policy checks for the replicated object. If unfound, the policy identifies DCs that do not contain the replicated object and sends a message regarding the DCs missing the replicated object.

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Policy: ADSPI-Rep_Delete_OvRep_Object

The ADSPI introduces an “OvReplication” container object into the configuration context and an “OvReplication-<DCName>" user object into the domain naming context of every domain controller. These objects are replicated to every other domain controller in the forest and their timestamps are updated regularly by the “ADSPI-Rep_ModifyObj” and the “ADSPI-Rep_Modify_User_Obj” policies.

Description:	The ADSPI-Rep_Delete_OvRep_Object policy automatically deletes the "OvReplication" and "OvReplication-<DCName>" objects from a domain controller if their timestamps are not updated for a certain period of time.
Warning Threshold	24 hrs
Critical Threshold	48 hrs

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Group policy catalog
- Discovery policies

Policy: ADSPI-Rep_InboundObjs

This policy measures the DRA inbound object/sec counter and monitors the number of inbound replication objects for Windows Server 2003/2000 nodes.

Description:	Monitors the number of inbound replication objects.
Interval	5 min
Message,	**Start Action:** The number of inbound replication objects on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> objects. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)> objects. **End Action:** The number of inbound replication objects on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)> objects.
Warning/Error Instruction Text:	Metric Description: Number of inbound replication objects on the domain controller. **Possible Problem(s):** (1) The number of inbound replication objects is high. **Probable Cause(s):** (1) The last replication attempt might have been unsuccessful because of the schedule or a possible bridgehead overload. **Potential Impact:** (1) Users and computers might not receive updated policies. (2) SYSVOL share content might not be replicated to the domain controllers. **Suggested Action(s):** (1) Use RepAdmin.exe to further troubleshoot Active Directory replication. For more information see the Microsoft Knowledge Base Article: (1) Q229896 - Using Repadmin.exe to Troubleshoot Active Directory Replication http://support.microsoft.com/default.aspx?scid=kb;EN-US;229896 (2) Q249256 - HOW TO: Troubleshoot Intra-Site Replication Failures http://support.microsoft.com/default.aspx?scid=kb;en-us;249256 Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Policy: ADSPI-Rep_InboundObjs_2k8+

This policy measures the DRA inbound object/sec counter and monitors the number of inbound replication objects for Windows Server 2008 nodes.

Description:	Monitors the number of inbound replication objects.
Interval	5 min
Message,	**Start Action:** The number of inbound replication objects on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> objects. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)> objects. **End Action:** The number of inbound replication objects on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)> objects.
Warning/Error Instruction Text:	Metric Description: Number of inbound replication objects on the domain controller. **Possible Problem(s):** (1) The number of inbound replication objects is high. **Probable Cause(s):** (1) The last replication attempt might have been unsuccessful because of the schedule or a possible bridgehead overload. **Potential Impact:** (1) Users and computers might not receive updated policies. (2) SYSVOL share content might not be replicated to the domain controllers. **Suggested Action(s):** (1) Use RepAdmin.exe to further troubleshoot Active Directory replication. For more information see the Microsoft Knowledge Base Article: (1) Q229896 - Using Repadmin.exe to Troubleshoot Active Directory Replication http://support.microsoft.com/default.aspx?scid=kb;EN-US;229896 (2) Q249256 - HOW TO: Troubleshoot Intra-Site Replication Failures http://support.microsoft.com/default.aspx?scid=kb;en-us;249256 Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Group policy catalog
- Discovery policies

Policy: ADSPI-Rep_ISM_Chk

This policy monitors the status of the "InterSite Messaging" service. It checks whether the service is running or not and how many processes of this service are running. If this service does not run properly, then inter-site replication might have problems and the KCC will be unable to calculate the replication topology.

Description: Checks the intersite messaging service (ISM).

Interval: 12 min

Message: **Start Actions:**

```
' setting the state variable corresponding to the value delivered by the external program
Select Case Service.Value
   Case 0 State = \"Running\"
   Case 1 State = \"Stopped\"
   Case 2 State = \"Start Pending\"
   Case 3 State = \"Stop Pending\"
   Case 4 State = \"Continue Pending\"
   Case 5 State = \"Pause Pending\"
   Case 6 State =  \"Paused\"
   Case 7 State = \"Not Existing\"
End Select

' finally the check
If (Service.Value > 0) And (Service.Value < 8) Then
   Session(\"MSG\") = \"The service '\" & Session(\"ServiceName\")  & \"' has the state: '\
\"'.\"
   Policy.MsgSeverity = \"Warning\"

   If Process.Value < Session(\"nProcesses\") Then
      If Session(\"nProcesses\") = 1 Then
         Session(\"MSG\") = Left (Session(\"MSG\"), Len(Session(\"MSG\"))-1) & \" and
corresponding process '\" _
         & Session(\"ProcessName\") & \"' is not running.\"
      Else
         Session(\"MSG\") = Left (Session(\"MSG\"), Len(Session(\"MSG\"))-1) & \" and
corresponding process '\" _
         & Session(\"ProcessName\") & \"' is running less than \" & Session(\"nProcesses\"
      End If
```

```
        Policy.MsgSeverity = \"Critical\"
    End If
    Rule.Status = True
End If
```

End Actions:
-- none --

Warning/Error Instruction Text:

Status of Inter-site Messaging service(ISM).

Possible Problem(s):
(1) ISM Service might not be running properly.

Probable Cause(s):
(1) ISM might be disabled.
(2) The user might not have sufficient privileges to run the service.

Potential Impact:
Without ISM service
(1) Intersite communication will not be possible.
(2) The KCC will be unable to calculate intersite topology.

Suggested Action(s):
(1) The policy will try to re-start the service automatically.
If not, try starting the service manually.
(2) Fix any GPOs that restrict the privileges of the user account.

For more information see the Microsoft Knowledge Base Article:
(1) Q229896 - Step-by-Step Guide to Setting up ISM-SMTP Replication
http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/ismsmtp.asp#

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. H
control the information of any non-HP site.

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Policy: ADSPI-Rep_Modify_User_Object

This scheduled task policy creates and updates a user object on the domain controller hosting the policy. This policy is deployed to all managed domain controllers.

This scheduled task policy provides the means for checking replication as measured by the **ADSPI-GC_Check_and_Threshold** policy, which monitors the delay times of global catalog inter-site and intra-site replication.

Description:	**Identifies DCs that do not contain this replication object and issue an alert when found.updates the OvReplication object. Used in conjunction with the ADSPI-Rep_GC_Check_and_Threshold will Monitor the replication times of global catalog inter-site, and intra-site replication latency.**
Interval:	**15 min**
Message:	**Start Actions: <$MSG_TEXT> (Command and User)** **End Actions:-- none --**
Diagnostic Instruction Text:	**Failed to run the embedded vbscript.** **Probable Cause(s):** **(1) The user does not have sufficient privileges to run this command.** **(2) The policy is not running on a domain controller.** **Potential Impact:** **The policy will not be able to calculate the replication latency between global catalog servers in Active Directory.** **Suggested Action(s):** **(1) Fix any Group Policy Objects that restrict the privileges of the agent user account($AGENT_USER).** **For more information see the Microsoft Knowledge Base Article:** **(1) Q321709 - HOW TO: Use the Group Policy Results Tool in Windows 2000** **http://support.microsoft.com/default.aspx?scid=kb;IT;321709** **(2) Q226243 - HOW TO: Reset User Rights in the Default Domain Group Policy** **http://support.microsoft.com/default.aspx?scid=kb;EN-US;226243** **Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.**

Related Topics:

- Descriptions of policy groups & types

- Microsoft Active Directory SPI group catalog
- Discovery policies

Policy: ADSPI-Rep_ModifyObj

This scheduled task policy creates and updates an object on the domain controller hosting the policy. This policy is deployed to all managed domain controllers as a means for checking replication as measured by the following policies:

- The Rep_Mon policy: verifies timely replication between DC replication partners.
- The Rep_CheckObj policy: verifies the object's existence on the DC's replication partners. If the object is missing the policy generates a message.

Description:	Monitors the number of inbound replication objects.
Message:	Message Text: **Start Actions:** <$MSG_TEXT> (Command and User) **End Actions:** -- none --
Diagnostic Instruction Text:	Possible Problem: Failed to run the ADSPI_ModifyObject.js. **Probable Cause(s):** (1) The user does not have sufficient privileges to run this command. (2) The policy is not running on a domain controller. **Potential Impact:** The policy will not be able to calculate the replication latency between domain controllers in Active Directory. **Suggested Action(s):** (1) Fix any Group Policy Object that restrict the privileges of the agent user account($AGENT_USER). For more information see the Microsoft Knowledge Base Article: (1) Q321709 - HOW TO: Use the Group Policy Results Tool in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;IT;321709 (2) Q226243 - HOW TO: Reset User Rights in the Default Domain Group Policy http://support.microsoft.com/default.aspx?scid=kb;EN-US;226243 Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of policy groups & types
- Microsoft Active Directory SPI group catalog

- Discovery policies

Policy: ADSPI-Rep_Mon

The **ADSPI-Rep_Mon** measurement threshold policy measures the replication latency response times in hours. This policy works with two other policies:

1. ADSPI-Rep_ModObj, which creates and periodically modifies an object.
2. ADSPI-Rep_CheckObj, which verifies the existence of the replicated object on the DC's replication partners.

Description	Monitors the replication latency between DCs in hours.
Interval	12 hours
Threshold	Critical Level: >= 1 (Maximum number of missing records)
Message Text	**Start Action:** The domain controller <$MSG_NODE_NAME> has not replicated from the domain controller <$INSTANCE> for <$SESSION(lastRep)>hours. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>hours. **End Action:** The replication latency between domain controllers <$MSG_NODE_NAME> and <$INSTANCE> no longer exceeds <$SESSION(CriticalThreshold)>hours.
Instruction Text	**Possible Problem(s):** (1) Replication between the domain controllers has not occurred in a long time. **Probable Cause(s):** Replication might not have occurred due to the following reason(s): (1) schedule. (2) bridgehead overload. (3) network overload. **Potential Impact:** (1) Users and computers might not receive updated policies. (2) SYSVOL share content might not be replicated to the domain controllers. (3) The domain controllers might not contain up-to-date information. **Suggested Action(s):** (1) Use RepAdmin.exe to further troubleshoot Active Directory replication. For more information see the Microsoft Knowledge Base Article: (1) Q229896 - Using Repadmin.exe to Troubleshoot Active Directory Replication http://support.microsoft.com/default.aspx?scid=kb;EN-US;229896 (2) Q249256 - HOW TO: Troubleshoot Intra-Site Replication Failures

http://support.microsoft.com/default.aspx?scid=kb;en-us;249256

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

All three policies ensure that changes occurring on one DC are propagated (replicated) in a timely manner to all other domain controllers. The policy measures not only inter-site latency but intra-site replication latency. Every hour this policy checks the Active Directory latency object to obtain these measurements.

Related Topics:

- Descriptions of policy groups & types
- Group Policy Catalog
- Discovery policies

Policy: ADSPI-Rep_Mon_Fwd_Ping_Messages

Windows 2000 Active Directory takes a multimaster approach to common administrative tasks. Changes made to the directory on any domain controller are propagated (replicated) to all other domain controllers. The exceptions are the tasks that require an operations master.

Description:	This is an Open Message Interface policy which forwards the alert messages sent by ADSPI_RepMon.exe to the HPOM Console. This policy helps to form the message correlation key

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Group policy catalog
- Discovery policies

Policy: ADSPI-Rep_TimeSync

Windows 2000 uses a time service, known as Windows Time Synchronization Service (Win32Time), to ensure that all Windows 2000 computers on a network use a common time. This service is required and therefore crucial to Windows 2000s default authentication processes (which uses Kerberos protocol).

The policy measures in seconds the delta between the 'time master' and the local host. If the delta exceeds a given threshold, the policy generates an alarm and a message appears in the HPOM message browser. If the delta is 4 minutes or more, it generates a warning; 5 minutes or more - a critical alert.

Description: Validates time synchronization with time master in seconds.

Interval: 5 min

Message:

Start Action:
The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec.

End Action:
The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Diagnostic Instruction Text:

Probable Cause(s):
(1) The PDC Emulator might be unavailable or over-used.
(2) The network link between the domain controller and the PDC Emulator might be slow.
(3) Windows Time Service might not be running.

Potential Impact:
If the time difference between domain controllers drifts beyond the skew allowed by Kerberos, then
(1) authentication between the two domain controllers may not succeed.
(2) replication problems and RPC error messages can result.

Suggested Action(s):
(1) Use the net time command to synchronize the time with the computer that holds the PDC Emulator FSMO role. To do this, use the following command:

    net time \\\\mypdc /set /y (where mypdc is the PDC Emulator).

(2) Check whether Windows Time Service is running.
(3) If the PDC Emulator FSMO role is unavailable and cannot be brought back into the environment, the administrator can seize the role from another domain controller in the enterprise.

For more information see the Microsoft Knowledge Base Article:
(1) Q257187 - RPC Error Messages Returned for Active Directory Replication When Time Is Out of Synchronization
http://support.microsoft.com/default.aspx?kbid=257187
(2) Q223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787
(3) Q255504 - Using Ntdsutil.exe to Seize or Transfer FSMO Roles to a Domain Controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the TIMESYNC column of the ADSPI_TIMESYNC table.

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

GC Monitoring policies

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).

***** ADSPI-Rep_Modify_User_Object (actually in Replication Monitoring group)

ADSPI-Rep_GC_Check_and_Threshold

***** Scheduled task policy necessary for ADSI-Rep_GC_Check_and_Threshold to work.

The GC policies are available under both the policy groups (Windows Server 2003/2000 and Windows Server 2008).

These policies are located under the following policy groups:

- *For Windows Server 2003/2000 nodes*
  SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → GC Monitoring
- *For Windows Server 2008 nodes*
  SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → GC Monitoring

Related Topics:

- Descriptions of policy groups & types
- Policy Catalog
- Discovery policies

Policy: ADSPI-Rep_GC_Check_and_Threshold

This policy is deployed only on servers hosting global catalog services. It works in conjunction with the scheduled task policy ADSPI-Rep_Modify_User_Object.

The ADSPI-Rep_GC_Check_and_Threshold policy monitors delay times of global catalog inter- and intra-site replication. Delays can be measured by means of a timestamp available from an object created by the ADSPI-Rep_Modify_User_Object policy. This object, which contains a timestamp, is created specifically for the DC\GC on which it is deployed. After it is created, the object timestamp can be modified by the ADSPI-Rep_Modify_User_Object policy. Since global catalog policies are deployed to every DC\GC, each DC\GC has a specific object stored in the global catalog.

The ADSPI-Rep_GC_Check_and_Threshold policy checks the current timestamp against the timestamp of objects created by other DC\GCs in the forest. An alarm occurs whenever the timestamp on any of those objects is more than 24 hours old, meaning that replication has not occurred from that DC\GC for more than 24 hours.

Description:	Calculates, stores, and sends messages/alerts when threshold hours for global catalog replication latency are exceeded.
Interval	5 min
Threshold	24 hours
Message Text:	**Start Action:** The global catalog server <$MSG_NODE_NAME> has not replicated from the domain controller(s) <$SESSION(DC)> for at least <$SESSION(THRESHOLD)> hours. **End Action:** The replication latency between global catalog server <$MSG_NODE_NAME> and the domain controller(s) <$SESSION(DC)> no longer exceeds the critical threshold value of <$SESSION(THRESHOLD)> hours.
Error Instruction Text:	**Possible Problem(s):** (1) Replication between the global catalog server and the other domain controllers has not occurred in a long time. **Probable Cause(s):** Replication might not have occurred due to the following reason(s): (1) schedule. (2) bridgehead overload. (3) network overload.

Potential Impact:
(1) Users and computers might not receive updated policies.
(2) The global catalog server might not contain up-to-date information about the universal groups.
(3) The global catalog server might not provide correct global address list to the Exchange Servers.

Suggested Action(s):
(1) Use RepAdmin.exe to further troubleshoot Active Directory replication.

For more information see the Microsoft Knowledge Base Article:
(1) Q229896 - Using Repadmin.exe to Troubleshoot Active Directory Replication
http://support.microsoft.com/default.aspx?scid=kb;EN-US;229896
(2) Q249256 - HOW TO: Troubleshoot Intra-Site Replication Failures
http://support.microsoft.com/default.aspx?scid=kb;en-us;249256

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the following columns of the ADSPI_GCREP table:

- Instance name
- LatencyDelta

Related Topics:

- Policy catalog

Response Time Monitoring Policies

ADSPI Response Time GC Query

ADSPI Response Logging

ADSPI Response Time Bind

ADSPI SPI Response Time GC Bind

ADSPI Response Time Query

The response time policies are available under both the policy groups (Windows Server 2003/2000 and Windows Server 2008).

These policies are located under the following policy groups:

- *For Windows Server 2003/2000 nodes*
  SPI for Microsoft Active Directory → en → Windows Server 2003/2000 → Auto-Deploy → Response Time Monitoring
- *For Windows Server 2008 nodes*
  SPI for Microsoft Active Directory → en → Windows Server 2008 → Auto-Deploy → Response Time Monitoring

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Policy: ADSPI-ResponseTime_Bind

It is important to monitor the general responsiveness of Active Directory. When the bind and query time to Active Directory increases significantly, this is a key indicator that something needs to be investigated. A DC may have gone down and queries are being directed to another DC over a WAN link, or a DC is having resource contention. This policy periodically binds to active directory and measures latency.

Description:	Monitors bind response time in seconds of Active Directory with thresholds as follows: - A warning message occurs when bind time exceeds one second. - A critical message occurs when bind time exceeds two seconds. In either case, the message is sent only when the bind time threshold is exceeded for two consecutive samplings (this is controlled by the variable nwConsecLimit in the script). You can change these values in the script, depending on what is suitable for your environment. If your environment has no problem tolerating greater bind and query times, you should increase the warning, critical, and nwConsecLimit values in the script.
Interval	N/A
Threshold	Warning Level: >1 second Critical Level: >2 seconds
Message Text	**Warning Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> has a bind response time of <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(WarningThreshold)> second(s) for the last <$SESSION(nWConsec)> consecutive times. **End Actions:** Domain controller <$MSG_NODE_NAME> has a bind response time of <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(WarningThreshold)> second(s). **Error Message Text:** **Start Actions:** Domain controller <$MSG_NODE_NAME> has a bind response time of <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(CriticalThreshold)> second(s) for the last <$SESSION(nEConsec)> consecutive times. **End Actions:** Domain controller <$MSG_NODE_NAME> has a bind response time of <$SESSION(value)> second(s). It no longer exceeds the warning threshold of

	<$SESSION(CriticalThreshold)> second(s).
Instruction Text	The bind response time of the domain controller is high. **Probable Cause(s):** The domain controller (1) is over used. (2) might be under a denial-of-service attack. **Potential Impact:** (1) Users may experience delays in logging on. (2) Services dependent on domain controllers may experience failures due to delays in contacting the domain controller. **Suggested Action(s):** (1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks. (2) If the domain controller is over used, the administrator can add another domain controller to the site(s) this domain controller serves. For more information see the Microsoft Knowledge Base Article: (1) Q238369 - HOW TO: Promote and Demote Domain Controllers in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;EN-US;238369 **Disclaimer:** Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Policy Catalog :

Policy: ADSPI-ResponseTime_GCBind

This policy measures the time required for the domain controller to bind to the Active Directory GC (Global Catalog). The Global Catalog is used to quickly find an object in Active Directory. It is a partial replica of every domain directory in the forest. The global catalog contains an entry for every object in the forest but does not store every property for every object. Instead it contains only the properties that are marked in the schema for inclusion in the global catalog. Only domain controllers can serve as global catalog servers.

Description:	Monitors GC bind response time in seconds of Active Directory.
Interval	N/A
Threshold	Warning Level: >1 second Critical Level: >2 seconds
Message	**Warning Message Text:** **Start Actions:** The bind response time of the global catalog on domain controller $MSG_NODE_NAME> is <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(WarningThreshold)> second(s) for the last <$SESSION(nWConsec)> consecutive times. **End Actions:** The bind response time of the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(WarningThreshold)> second(s). **Error Message Text:** **Start Actions:** The bind response time of the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(CriticalThreshold)> second(s) for the last <$SESSION(nEConsec)> consecutive times. **End Actions:** The bind response time of the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(CriticalThreshold)> second(s).
Instruction Text	**Warning/Error Instruction Text** Metric Description: Bind response time of the global catalog on this domain controller in seconds.

Possible Problem(s):
(1) The bind response time to the global catalog on this domain controller is high.

Probable Cause(s):
The domain controller
(1) is over used.
(2) might be under a denial-of-service attack.

Potential Impact:
(1) Users may experience delays in logging on.
(2) Services dependent on the global catalog may experience failures due to delays in binding to the global catalog.

Suggested Action(s):
(1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks.
(2) If the domain controller is over used, the administrator can add another global catalog to the site(s) this global catalog serves.

For more information see the Microsoft Knowledge Base Article:
(1) Q296882 - How to promote a domain controller to a global catalog server
http://support.microsoft.com/default.aspx?scid=kb;en-us;296882

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Policy catalog

Policy: ADSPI-Response Time_GCQuery

Monitors the global catalog query response time of Active Directory by measuring the time required to perform a global catalog search.

The global catalog is used to quickly find an object in Active Directory. It is a partial replica of every domain directory in the forest. The global catalog contains an entry for every object in the forest, but does not store every property for every object. Instead it contains only the properties, which are marked in the schema for inclusion in the global catalog. Only domain controllers can serve as global catalog servers.

Description:	Monitors bind response time in seconds of Active Directory global catalog queries.
Interval	N/A
Threshold	Warning Level: >1 second Critical Level: >2 seconds
Message Text	**Start Actions:** The response time of queries made to the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(WarningThreshold)> second(s) for the last <$SESSION(nWConsec)> consecutive times. **End Actions:** The response time of queries made to the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(WarningThreshold)> second(s). **Error Message Text:** Start Actions: The response time of queries made to the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(CriticalThreshold)> second(s) for the last <$SESSION(nEConsec)> consecutive times. End Actions: The response time of queries made to the global catalog on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(CriticalThreshold)> second(s).
Instruction Text	Query response time of the global catalog on this domain controller in seconds. **Possible Problem(s):** (1) The query response time to the global catalog on this domain controller is high.

Probable Cause(s):
The domain controller
(1) is over used.
(2) might be under a denial-of-service attack.

Potential Impact:
(1) Users may experience delays in logging on.
(2) Services dependent on the global catalog may experience failures due to delays in retrieving information from the global catalog.

Suggested Action(s):
(1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks.
(2) If the domain controller is over used, the administrator can add another global catalog to the site(s) this global catalog serves.

For more information see the Microsoft Knowledge Base Article:
(1) Q296882 - How to promote a domain controller to a global catalog server
http://support.microsoft.com/default.aspx?scid=kb;en-us;296882

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Policy catalog

Policy: ADSPI-Response_Logging

This scheduled task policy logs Active Directory response times for global catalog searches. The logged response times are available for graphing purposes and aid in base-lining what the value should be for each customer.

Description:	This scheduled task policy logs Active Directory response times.
Interval	5 min

A graph is available from the data logged through this policy that aids in base-lining what the value should be for each customer.

The policy stores the collected data into the following columns of the ADSPI_RESPONSETIME table:

- BINDTIME
- QUERYTIME
- GCBINDTIME
- GCQUERYTIME
- GCPRESENT
- AVAILABILITY
- GCAVAILABILITY

Related Topics:

- Global Catalog Monitoring Policies
- Policy catalog

Policy: ADSPI-ResponseTime_Query

This policy measures the time required for the Active Directory queries. It periodically queries Active Directory and monitors latency. Monitoring the general responsiveness of Active Directory is important because significant increases in the amount of time required for binding then querying can indicate a serious problem. For example, a DC may have gone down and queries are being directed to another DC over a WAN link, or a DC is running hot.

Description:	Measures the general responsiveness of Active Directory in seconds. It periodically queries Active Directory and monitors latency.
Interval	N/A
Threshold	Warning Level: >1 second Critical Level: >2 seconds
Message Text	**Warning Message Text:** **Start Actions:** The response time of queries made to domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(WarningThreshold)> second(s) for the last <$SESSION(nWConsec)> consecutive times. **End Actions:** The response time of queries made to domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(WarningThreshold)> second(s). **Error Message Text:** **Start Actions:** The response time of queries made to domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It has crossed the warning threshold of <$SESSION(CriticalThreshold)> second(s) for the last <$SESSION(nEConsec)> consecutive times. **End Actions:** The response time of queries made to domain controller <$MSG_NODE_NAME> is <$SESSION(value)> second(s). It no longer exceeds the warning threshold of <$SESSION(CriticalThreshold)> second(s).
Instruction Text	Query response time of the domain controller in seconds. **Possible Problem(s):** (1) The query response time of the domain controller is high.

Probable Cause(s):
The domain controller
(1) is over used.
(2) might be under a denial-of-service attack.

Potential Impact:
(1) Users may experience delays in logging on.
(2) Services dependent on domain controllers may experience failures due to delays in retrieving information from the domain controller.

Suggested Action(s):
(1) Secure your Active Directory enterprise by protecting domain controllers against known threats, creating administrative policies and practices to maintain security and detecting Active Directory attacks.
(2) If the domain controller is over used, the administrator can add another domain controller to the site(s) this domain controller serves.

For more information see the Microsoft Knowledge Base Article:
(1) Q238369 - HOW TO: Promote and Demote Domain Controllers in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;EN-US;238369

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The data is also logged for graphing.

Related Topics:

- Policy catalog

Sysvol Monitoring Policies

ADSPI-Sysvol_AD_Sync

ADSPI-Sysvol_Connectivity

ADSPI-Sysvol_FRS

ADSPI-Sysvol_PercentFull

The Sysvol policies are available under both the policy groups (Windows Server 2003/2000 and Windows Server 2008).

These policies are located under the following policy groups:

- *For Windows Server 2003/2000 nodes*
  SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Sysvol Monitoring
- *For Windows Server 2008 nodes*
  SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Sysvol Monitoring

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI-Sysvol_FRS

Description: Checks the File Replication Service (FRS) event log for error/warning events.

Threshold
Rule 1: Major
Rule 2: Information, Warning, Error

Warning/Error Message Text
Start Actions: None
End Actions: None

Error Instruction Text

Rule 1, Possible Problem:
FRS has not replicated one or more files in the Sysvol to other domain controllers.

Probable Cause(s):
(1) Another process on the domain controller is holding the file(s) open.
(2) Files can fail to replicate for a wide range of underlying reasons: DNS, communication i
space, FRS servers in an error state, or sharing violations.

Potential Impact:
(1) FRS is used by Active Directory to synchronize group policies and logon scripts that are
across domain controllers. If FRS fails to replicate one or more files in the Sysvol, then the
be applied to the user/computer.

Suggested Action(s):
(1) Use the Ntfrsutl.exe ver command from the source to the destination computer, and vice
Verify RPC connectivity between the source and destination. Also verify that FRS is runnin
(2) Check for files that are larger than the amount of free space on the source or destination
area directory limit in the registry. Resolve the disk space problem or increase the maximun
(3) Check whether the file is locked on either computer. Use the net file command on the so
command indicates which users are holding the file open on the network, but will not repor
processes. If the file is locked on the source computer, then FRS will be unable to read the f
replication will be delayed. If the file is locked on the destination computer, then FRS will l
FRS continues to retry the update until it succeeds. The retry interval is 30 to 60 seconds. If
you can use the net file <id> /close command to force the file closed.

For more information see the Microsoft Knowledge Base Article(s):
(1) Troubleshooting FRS
http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirec
(2) Q323247 - Overview of Basic File Replication Service Concepts and Terminology
http://support.microsoft.com/default.aspx?scid=kb;en-us;323247
(3) Q264822 - File Replication Service Stops Responding When Staging Area is Full
http://support.microsoft.com/default.aspx?scid=kb;en-us;264822

Rule 2, Possible Problem(s):
FRS has stopped responding because the staging area is full.

Probable Cause(s):
(1) When the server replicates large amounts of data, staging areas can reach their limit bec staging area at a rate faster than the data can be transferred across the network to the stagin

Potential Impact:
(1) FRS is used by Active Directory to synchronize group policies and logon scripts that are across domain controllers. If FRS fails to replicate one or more files in the Sysvol, then the be applied to the user/computer.

Suggested Action(s):
(1) Check whether the file is locked on either computer. Use the net file command on the so command indicates which users are holding the file open on the network, but will not repor processes. If the file is locked on the source computer, then FRS will be unable to read the f replication will be delayed. If the file is locked on the destination computer, then FRS will FRS continues to retry the update until it succeeds. The retry interval is 30 to 60 seconds. If you can use the net file <id> /close command to force the file closed.

For more information see the Microsoft Knowledge Base Article(s):
(1) Troubleshooting FRS
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/maintain/opsguide/part1/adogd11.asp >
(2) Q323247 - Overview of Basic File Replication Service Concepts and Terminology
<http://support.microsoft.com/default.aspx?scid=kb;en-us;323247 >
(3) Q264822 - File Replication Service Stops Responding When Staging Area is Full
<http://support.microsoft.com/default.aspx?scid=kb;en-us;264822 >

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP non-HP site.

Related Topics:

- Descriptions of policy groups & types
- Policy group catalog
- Discovery policies

Policy: ADSPI-Sysvol_AD_Sync

Checks that the Group Policy Objects in Active Directory and SysVol are in synch.

Description:	Checks synchronization of Group Policy Objects (GPO) in Active Directory and Sysvol.
Interval	24 hr
Threshold	Critical >= 2 Warning >= 1
Warning/Error Message Text	**Start Actions:** **End Actions:**
Error Instruction Text	**Possible Problem(s):** (1) The version number of GPOs in AD and Sysvol is different. **Probable Cause(s):** (1) Active Directory or File Replication Service (FRS) replication problems might be causi **Potential Impact:** (1) GPOs are stored in two places: Group Policy Configuration (GPC) data is stored in Act Template (GPT) data is stored as files and directories in the system volume. If the version r Sysvol, then the GPO will not be applied to the user/computer. **Suggested Action(s):** (1) Verify that Active Directory replication is functioning. Each domain controller must ha domain controller in the same domain. (2) Use the Ntfrsutl.exe ver command from the source to the destination computer, and vice Verify RPC connectivity between the source and destination. Also verify that FRS is runnir (3) Check for files that are larger than the amount of free space on the source or destination area directory limit in the registry. Resolve the disk space problem or increase the maximur (4) Check whether the file is locked on either computer. Use the net file command on the so command indicates which users are holding the file open on the network, but will not repor If the file is locked on the source computer, then FRS will be unable to read the file to gene delayed. If the file is locked on the destination computer, then FRS will be unable to update the update until it succeeds. The retry interval is 30 to 60 seconds. If files are being held op <id> /close command to force the file closed. For more information see the Microsoft Knowledge Base Article(s): (1) Troubleshooting FRS http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedire

(2) Q216359 - HOW TO: Identify Group Policy Objects in the Active Directory and SYSV
http://support.microsoft.com/default.aspx?scid=kb;en-us;216359
(3) Q250842 - Troubleshooting Group Policy Application Problems
http://support.microsoft.com/default.aspx?kbid=250842
(4) Q229896 - Using Repadmin.exe to Troubleshoot Active Directory Replication
http://support.microsoft.com/default.aspx?scid=kb;EN-US;229896

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site.

Related Topics:

- Descriptions of policy groups & types
- Policy group catalog
- Discovery policies

Policy: ADSPI-SysVol_PercentFull

The size of the SysVol is a key indicator of the health of Active Directory. This policy calculates the percentage full of the system's disk space and collects information about disk space size. This information is logged for later reporting.

Description:	Monitors the amount of free space on the Sysvol disk drive in terms of percentage used.
Interval	N/A
Threshold	Warning Level: Disk full=80% Critical Level: Disk full=90%
Warning/Error Message Text	**Start Action:** The Sysvol disk drive on <$MSG_NODE_NAME> is <$SESSION(PercentFull)>% full. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>%. **End Action:** The percentage full on the Sysvol disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.
Warning/Error Instruction Text	**Metric information:** % Used Space on the disk drive holding the Sysvol is calculated from Disk FreeSpace and Disk Size metrics. The default location of the Sysvol folder is %SystemRoot%\\SYSVOL\\Sysvol. Metric(s): (1) root\\cimv2 Win32_LogicalDisk.Size (2) root\\cimv2 Win32_LogicalDisk.FreeSpace **Possible Problem(s):** (1) The disk drive that hosts the Sysvol may soon run out of disk space. **Probable Cause(s):** (1) The number of Group Policy Objects (GPO) has increased over time. (2) Some other application is taking up the disk space. (3) The disk may not be big enough to allow for the growth in the GPOs in Sysvol. **Potential Impact:** (1) The domain controller may NOT allow addition and modification of GPOs in Sysvol. (2) Insufficient disk space can prevent the replication of Sysvol files. **Suggested Action(s):**

	(1) Free some space on the drive by deleting unnecessary files or moving them to another volume. (2) If the disk is a RAID set, you may be able to add additional disks to increase the storage. (3) Microsoft recommendation for Sysvol drive freespace is at least 50 percent of the amount of content you are trying to replicate and three times the largest file size being replicated. For more information see the Microsoft Knowledge Base Article(s): (1) Q228460 - Location of ADM (Administrative Template) Files in Windows http://support.microsoft.com/default.aspx?kbid=228460 (2) Q216359 - HOW TO: Identify Group Policy Objects in the Active Directory and SYSVOL http://support.microsoft.com/default.aspx?scid=kb;EN-US;216359 (3) Q250842 - Troubleshooting Group Policy Application Problems http://support.microsoft.com/default.aspx?scid=kb;en-us;250842 **Disclaimer:** Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

The policy stores the collected data into the following columns of the ADSPI_SYSVOLPERCENTFULL table:

- InstanceValue
- Instance Name

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Policy: 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 an uncommon situation for a person to mistakenly un-share the Sysvol volume out of ignorance. Such a mistake can result in a cascading effect.

Description:	Connects to each replication partner's SYSVOL to validate connectivity.
Interval	2 hr
Threshold	Error Level: Sysvol connection does not exist
Warning/Error Message Text	**Start Actions:** The domain controller <$MSG_NODE_NAME> was unable to connect to the Sysvol on its replication partner <$INSTANCE>. **End Actions:** The domain controller <$MSG_NODE_NAME> has established the connection to the Sysvol on its replication partner <$INSTANCE>.
Error Instruction Text	**Metric information:** Sysvol Connectivity between replication partners. The default location of the Sysvol folder is %SystemRoot%\\SYSVOL\\Sysvol. **Possible Problem(s):** (1) The domain controller is unable to connect to the Sysvol share on its replication partner. **Probable Cause(s):** (1) Someone might have disabled the share on the Sysvol folder. (2) Administrative shares might have been removed by editing the registry. (3) Sysvol share is missing on the domain controller. **Potential Impact:** (1) Sysvol folder on the domain controller might not be replicated to its replication partners. (2) Group Policies might not be applied to the users and computers in the domain. (3) Users might not be able to add, delete or update Group Policy Objects on the domain controller. **Suggested Action(s):** (1) Verify whether Active Directory replication occurs between the domain

controllers in the domain (especially if this domain controller is promoted recently) using repadmin.exe.
(2) Check whether NTDS Connection objects exist in the DS of each replication partner using the \"Active Directory Sites and Services\" snap-in.

For more information see the Microsoft Knowledge Base Article(s):
(1) Q257338 - Troubleshooting Missing SYSVOL and NETLOGON Shares on Windows 2000 Domain Controllers
http://support.microsoft.com/default.aspx?scid=kb;it;257338
(2) Q318755 - HOW TO: Restore Administrative Shares That Have Been Deleted
http://support.microsoft.com/default.aspx?scid=kb;it;318755

Disclaimer: Clicking on the URL in the above text may take the user to a non-HP site. HP does not control the information of any non-HP site.

Related Topics:

- Descriptions of policy groups & types
- Policy group catalog
- Discovery policies

Trust Monitoring Policies

ADSPI-Trust_Mon_Add_Del

ADSPI_Trust_Mon_Modify

The trust monitoring policies are available under both the policy groups (Windows Server 2003/2000 and Windows Server 2008).

These policies are located under the following policy groups:

- *For Windows Server 2003 nodes*
  SPI for Microsoft Active Directory → Windows Server 2003/2000 → Auto-Deploy → Trust Monitoring
- *For Windows Server 2008 nodes*
  SPI for Microsoft Active Directory → Windows Server 2008 → Auto-Deploy → Trust Monitoring

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Policy: ADSPI_Trust_Mon_Modify

Description:	This policy monitors any modification of trusts in the Active Directory forest.
Type:	Windows Management Interface
Default Policy Group:	SPI for Active Directory → Auto-Deploy → Trust Monitoring (Windows Server 2003)

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Policy: ADSPI_Trust_Mon_Add_Del

Description:	This policy monitors additions and deletions of trusts in the Active Directory forest.
Type:	Windows Management Interface
Default Policy Group:	SPI for Active Directory → Auto-Deploy → Trust Monitoring (Windows Server 2003)

Related Topics:

- Descriptions of policy groups & types
- Policy catalog
- Discovery policies

Manual-Deploy Policies

These policies are divided into the following sub-groupings and are available for group or individual deployment. They are not automatically deployed through service discovery.

- **Auto Baseline Policies**
- **Connector**
- **Domain & OU Structure**
- **Global Catalog Access**
- **Health Monitors**
- **Index and Query Monitors**
- **Replication**
- **Replication Activity**
- **Security**
- **Site Structure**

Auto Baseline Policies

Policy: ADSPI-Rep_InboundObjects_AT

Description

This is an auto-threshold policy which monitors the number of inbound replication objects.

Type

Measurement Threshold (Auto Threshold)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Auto Baseline Policies

Policy: ADSPI-Rep_TimeSync_Monitor_AT

Description

This is an auto-threshold policy which validates time synchronization with the time master, in seconds.

Type

Measurement Threshold (Auto Threshold)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Auto Baseline Policies

Policy: ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT

Description

The ADSPI-Rep_GC_Check_and_Threshold is an auto-threshold policy which monitors delay times of global catalog inter- and intra-site replication.

Type

Measurement Threshold (Auto Threshold)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Auto Baseline Policies

Policy: ADSPI-Rep_InboundObjects_AT_2K8+

Description

The ADSPI-Rep_GC_Check_and_Threshold is an auto-threshold policy which monitors the number of inbound replication objects.

Type

Measurement Threshold (Auto Threshold)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Auto Baseline Policies

Connector Policies

Policy: ADSPI_ActiveAuthKerberos

Description

Checks the NTDS\Kerberos Authentications counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ActiveAuthLogon

Description

Checks the Server\Logon/sec counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ActiveAuthNTLM

Description: Checks the NTDS\NTLM Authentications counter for the number of successful authentications processed by the domain controller. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 30 or more, the policy sends an error message. If the value exceeds the upper threshold, the existing domain controllers should be upgraded or additional domain controllers should be installed.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ADCFwdAllWarnErrorMSADC

Description

Monitors the Application log for entries from MSADC that have a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

Functions only with the integration of Exchange. Without Exchange, the adc process, which the policy observes, does not exist.

Type

Windows Event Log (Application)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ADCImportFailures

Description

Checks the PerfLib counter MSADC\Rate of Import Failures for the number of imports that have failed. If the number is 1 or 2, the policy sends a warning message to the active message browser. If the number is 3 or higher, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ADCPageFaults

Description

Checks the PerfLib counter Process\Page Faults\adc for the number of page faults for a process. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. A consistently high rate of page faults for a process usually indicates that its working set is not large enough to support the process efficiently. If the system does not have enough available memory to enlarge the working set, it cannot lower the page fault rate.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ADCPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\adc for the number of bytes allocated exclusively to the ADC process (that is, bytes that cannot be shared with other processes). If the number exceeds

15000000, the policy sends a warning message to the active message browser. If the number exceeds 18000000, the policy sends a critical message.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector r

Policy: ADSPI_ADCProcessorTime

Description

Checks the PerfLib counter Process\Processor Time\adc for the percentage of processor time Active Directory ADC is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the Active Directory server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Connector

Policy: ADSPI_ADCWorkingSet

Description

Checks the PerfLib counter Process\Working Set\adc for the current number of bytes in the working set of the ADC process. If the number exceeds 15,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 bytes, the policy sends an error message.

This policy functions only with the integration of Exchange. Without Exchange, the process adc, which the policy observes, does not exist.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy →

Connector

Domain and OU Structure Policies

Policy: ADSPI_DomainChanges

Description

Approximately every 20 minutes, checks for changes to the domain structure.

- **Name Space**
  Root\Directory\LDAP
- **Event Class**
  __InstanceOperationEvent
- **WQL Filter**
  TargetInstance ISA "ds_dnsdomain"

Successful changes in the domain structure affect the size and replication of the Active Directory database.

Deploy this policy on a domain controller only.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Domain and OU Structure

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Domain and OU Structure

Policy: ADSPI_OUChanges

Description

Checks, approximately every 20 minutes, for changes to the OU structure.

- **Name Space**
  Root\Directory\LDAP
- **Event Class**
  __InstanceOperationEvent
- **WQL Filter**
  TargetInstance ISA "ds_organizationalunit"

Successful changes in the OU structure affect the size and replication of the Active Directory database.

Deploy this policy on a domain controller only.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Domain and OU Structure

oR,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Domain and OU Structure

Global Catalog Access Policies

Policies for Windows Server 2003/2000

Policy: ADSPI_GlobalCatalogWrites

Description

Checks the counter NTDS\DS Directory Writes/sec counter, approximately every 30 minutes, for the number of writes to the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Use this policy for Windows Server 2003/2000 nodes.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_GlobalCatalogReads

Description

Checks the NTDS\DS Directory Reads/sec counter, approximately every 30 minutes, for the number of reads from the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Use this policy for Windows Server 2003/2000 nodes.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_GlobalCatalogSearches

Description

Checks the NTDS\DS Directory Searches/sec counter, approximately every 30 minutes, for the number of searches of the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Use this policy for Windows Server 2003/2000 nodes.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Global Catalog Access

Policies for Windows Server 2008

Policy: ADSPI_GlobalCatalogWrites_2k8+

Description

Checks the counter NTDS\DS Directory Writes/sec counter, approximately every 30 minutes, for the number of writes to the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Use this policy for Windows Server 2008 nodes.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_GlobalCatalogReads_2k8+

Description

Checks the NTDS\DS Directory Reads/sec counter, approximately every 30 minutes, for the number of reads from the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Use this policy for Windows Server 2008 nodes.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Global Catalog Access

Policy: ADSPI_GlobalCatalogSearches_2k8+

Description

Checks the NTDS\DS Directory Searches/sec counter, approximately every 30 minutes, for the number of searches of the Global Catalog. If the number is 10 or more, the policy sends a warning message to the active message browser. If the number is 25 or more, the policy sends an error message. If the value exceeds the upper threshold, either the existing domain controller needs additional hardware or an additional domain controller is needed. Use this policy for Windows Server 2008 nodes.

Deploy this policy to the Global Catalog server only.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008→ Manual-Deploy → Global Catalog Access

Health Monitor Policies

Policy: ADSPI_DNSServ_FwdAllInformation

Description

Monitors the DNS Server log for entries that have a severity level of Information. Forwards these entries as messages to the active message browser.

Type

Windows Event Log (DNS Server)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_DNSServ_FwdAllWarnError

Description

Monitors the DNS Server log for entries that have a severity level of Warning or Error. Forwards these entries as messages to the active message browser.

Type

Windows Event Log (DNS Server)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllInformationDS

Description

Monitors the Directory Service log for entries with a severity level of Information and forwards them as messages to the active message browser.

Type

Windows Event Log (Directory Service)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllInformationFRS

Description

Monitors the File Replication Service log for entries with a severity level of Information. Forwards them as messages to the active message browser.

Type

Windows Event Log (File Replication Service)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllWarnErrorDS

Description

Forwards all event log entries with a severity level of Warning or Error.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_FwdAllWarnErrorFRS

Description

Forwards all event log entries with a severity level of Warning or Error.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSPageFaults

Description

Checks the PerfLib counter Process\Page Faults/sec\lsass for the number of times a thread requested access to a memory page that was not in memory and therefore had to be read from disk. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the value obtained from this counter consistently generates messages, physical memory is low.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\lsass for the number of bytes allocated exclusively to the LSASS process (that is, bytes that cannot be shared with other processes). If the number exceeds 35,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 40,000,000 bytes, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSProcessorTime

Description

Checks the PerfLib counter Process\% Processor Time\lsass for the percentage of processor time the ADS LSASS process is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMLSASSWorkingSet

Description

Checks the PerfLib counter Process\Working Set\lsass for the number of memory pages recently touched by threads in the process. If the number exceeds 15,000,000 pages, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 pages, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSPageFaults

Description

Checks the PerfLib counter Process\Page Faults/sec\NTFRS for the number of times a thread requested access to a memory page that was not in memory and therefore had to be read from disk. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the value obtained from this counter consistently generates messages, physical memory is low.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSPrivateBytes

Description

Checks the PerfLib counter Process\Private Bytes\NTFRS for the number of bytes allocated exclusively to the LSASS process (that is, bytes that cannot be shared with other processes). If the number exceeds 15,000,000 bytes, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 bytes, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSProcessorTime

Description

Checks the PerfLib counter Process\% Processor Time\NTFRS for the percentage of processor time the ADS LSASS process is consuming. If the value exceeds 60%, the policy sends a warning message to the active message browser. If the value exceeds 70%, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMNTFRSWorkingSet

Description

Checks the PerfLib counter Process\Working Set\NTFRS for the number of memory pages recently touched by threads in the process. If the number exceeds 15,000,000 pages, the policy sends a warning message to the active message browser. If the number exceeds 18,000,000 pages, the policy sends an error message. If the number exceeds the upper threshold, there may be a memory leak or some other memory problems.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMThreadsInUse

Description

Checks the PerfLib counter NTDS\DS Threads in Use for the number of threads in use by the directory service. (This number is different from the number of threads in use by the directory service process.) If the number exceeds 20, the policy sends a warning message to the active message browser. If the number exceeds 25, the policy sends an error message. These threads serve client API calls, and indicate whether additional processors should be used.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Health Monitors

Policy: ADSPI_HMThreadsInUse_2k8+

Description

Checks the PerfLib counter NTDS\DS Threads in Use for the number of threads in use by the directory service. (This number is different from the number of threads in use by the directory service process.) If the number exceeds 20, the policy sends a warning message to the active message browser. If the number exceeds 25, the policy sends an error message. These threads serve client API calls, and indicate whether additional processors should be used.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 →Manual-Deploy → Health Monitors

Policy: ADSPI_KDC

Description

Checks whether the Kerberos Key Distribution Center Service and its corresponding process lsass.exe are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_NetLogon

Description

Checks whether the Net Logon service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_NTFRS

Description

Checks whether the File Replication Service and its corresponding process, ntfrs.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_SamSs

Description

Checks whether the Security Accounts Manager service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_SMTPEventLogs

Description

Monitors the System log for SMTP-specific events. Forwards them as messages to the active message browser.

Type

Windows Event Log (System)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Or,

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_SyncSchemaMissMatch

Description

Checks the PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch for the number of synchronization failures. If the number exceeds 1, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or require further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) → Windows Server 2003/2000 → Manual-Deploy → Health Monitors

Policy: ADSPI_SyncSchemaMissMatch_2k8+

Description

Checks the PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch for the number of synchronization failures. If the number exceeds 1, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or require further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) →Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_DFSR_2k8+

Description

The ADSPI_DFSR_2k8+ policy checks if the DFS Replication service and `dfsrs.exe` process are running on the Active Directory node. If they are not running, the policy sends a warning message to the active message browser. You can restart the service with the operator-initiated command. When the DFS Replication service starts running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) →Windows Server 2008 → Manual-Deploy → Health Monitors

Policy: ADSPI_NTDS_2k8+

Description

The ADSPI_NTDS_2k8+ policy checks if the Active Directory Domain service and `lsass.exe` process are running on the Active Directory node. If they are not running, the policy sends a warning message to the active message browser. You can restart the service with the operator-initiated command. When the Active Directory Domain service starts running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Default Policy Group

SPI for Microsoft Active Directory → en (or ja) →Windows Server 2008 → Manual-Deploy → Health Monitor

Index and Query Monitor Policies

Policies for Windows Server 2003/2000

Policy: ADSPI_IQKerberosAuthentications

Description

Checks the PerfLib counter NTDS\Kerberos Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPActiveThreads

Description

Checks the PerfLib counter NTDS\LDAP Active Threads for the number of LDAP Active Threads. If the number exceeds 40, the policy sends a warning message to the active message browser. If the number exceeds 50, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 →Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPBindTime

Description

Checks the PerfLib counter NTDS\LDAP Bind Time for the number of LDAP Client Sessions. If the number exceeds 100, the policy sends a warning message to the active message browser. If the number exceeds 200, the policy sends an error message. If the LDAP Bind Time exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPClientSessions

Description

Checks the PerfLib counter NTDS\LDAP Client Sessions for the number of LDAP Client Sessions. If the number exceeds 4,000 sessions, the policy sends a warning message to the active message browser. If the number exceeds 4,500 sessions, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQNTLMAuthentications

Description

Checks the PerfLib counter NTDS\NTLM Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 300, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSSearches

Description

The policy evaluates the Number of searches every second in the Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSReads

Description

The policy evaluates the Number of reads every second in the Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSWrites

Description

The policy evaluates the Number of writes every second in the Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Index and Query Monitors

Policies for Windows Server 2008

Policy: ADSPI_IQKerberosAuthentications_2k8+

Description

Checks the PerfLib counter NTDS\Kerberos Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPActiveThreads_2k8+

Description

Checks the PerfLib counter NTDS\LDAP Active Threads for the number of LDAP Active Threads. If the number exceeds 40, the policy sends a warning message to the active message browser. If the number exceeds 50, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPBindTime_2k8+

Description

Checks the PerfLib counter NTDS\LDAP Bind Time for the number of LDAP Client Sessions. If the number exceeds 100, the policy sends a warning message to the active message browser. If the number exceeds 200, the policy sends an error message. If the LDAP Bind Time exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQLDAPClientSessions_2k8+

Description

Checks the PerfLib counter NTDS\LDAP Client Sessions for the number of LDAP Client Sessions. If the number exceeds 4,000 sessions, the policy sends a warning message to the active message browser. If the number exceeds 4,500 sessions, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with LDAP queries.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_IQNTLMAuthentications_2k8+

Description

Checks the PerfLib counter NTDS\NTLM Authentications for the number of authenticating clients per second. If the number exceeds 250, the policy sends a warning message to the active message browser. If the number exceeds 300, the policy sends an error message. If the number exceeds the upper threshold, the domain controller may be overloaded with logon authentication traffic.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSSearches_2k8+

Description

The policy evaluates the Number of Searches every second in the Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSReads_2k8+

Description

The policy evaluates the Number of reads every second in the Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Policy: ADSPI_DSWrites_2k8+

Description

The policy evaluates the Number of writes every second in the Directory Service.

Type

Measurement Threshold

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Index and Query Monitors

Replication Policies

Policies for Windows Server 2003/2000

Policy: ADSPI_ADSPendingSynchronizations

Description

Checks the PerfLib counter NTDS\DRA Pending Replication Synchronizations for the number of synchronizations pending. If the number exceeds 50, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepInBoundBytesBetweenSites

Description

Checks the PerfLib counter NTDS\DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec for the number of bytes per second between sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the

Active Directory replication may need to be optimized.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepInBoundBytesWithinSites

Description

Checks the PerfLib counter NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec for the number of bytes per second within sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepInBoundObjectUpdatesRemaining

Description

Checks the PerfLib counter NTDS\DRA Inbound Object Updates Remaining in Packet for the number of objects remaining. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepNotifyQueueSize

Description

Checks the PerfLib counter NTDS\DS Notify Queue Size for the number of jobs in the queue. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication

Policies for Windows Server 2008

Policy: ADSPI_ADSPendingSynchronizations_2k8+

Description

Checks the PerfLib counter NTDS\DRA Pending Replication Synchronizations for the number of synchronizations pending. If the number exceeds 50, the policy sends a warning message to the active message browser. If the number exceeds 100, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepInBoundBytesBetweenSites_2k8+

Description

Checks the PerfLib counter NTDS\DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec for the number of bytes per second between sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepInBoundBytesWithinSites_2k8+

Description

Checks the PerfLib counter NTDS\DRA Inbound Bytes Not Compressed (Within Site)/sec for the number of bytes per second within sites. If the number exceeds 40,000 bytes per second, the policy sends a warning message to the active message browser. If the number exceeds 60,000 bytes per second, the policy sends an error message. If the Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, the Active Directory replication may need to be optimized.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+

Description

Checks the PerfLib counter NTDS\DRA Inbound Object Updates Remaining in Packet for the number of objects remaining. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the value exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Measurement)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Replication

Policy: ADSPI_ADSRepNotifyQueueSize_2k8+

Description

Checks the PerfLib counter NTDS\DS Notify Queue Size for the number of jobs in the queue. If the number exceeds 5, the policy sends a warning message to the active message browser. If the number exceeds 10, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy →

Replication

Replication Activity Policies

Policy: ADSPI_ReplicationActivities

Description

Monitors the Directory Service log for replication events.

The granularity of the raised events depends on the following registry key:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Diagnostics\5 Replication Events`

Set this value to 3 to get the following four directory replication events logged in the Directory Services log:

- 1487 Internal event: The Directory Service has been asked to begin inbound replication
- 1488 The Directory Service completed the sync request
- 1489 Internal event: The Directory Service has been asked for outbound changes
- 1490 Internal event: The Directory Service finished gathering outbound changes

Type

Windows Event Log (Directory Service)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Replication Activities

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Replication Activities

Security Policies

Policy: ADSPI_DirUserCreationDeletionModification

Description

Checks, approximately every 15 minutes, whether any accounts in Directory User Accounts have been created, deleted, or modified. If any have, the policy sends a message to the active message browser.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_DirUserCreationDeletionModification_2k8+

Description

Checks, approximately every 15 minutes, whether any accounts in Directory User Accounts have been created, deleted, or modified. If any have, the policy sends a message to the active message browser.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_KDCFailureGrantTicket

Description

Monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 676 in the Security Event Log:

676 Authentication Ticket Request Failed

Deploy this template only to servers running KDC.

Type

Windows Event Log (Security)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_KDCFailureGrantTicket_2k8+

Description

Monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 676 in the Security Event Log:

676 Authentication Ticket Request Failed

Deploy this template only to servers running KDC.

Type

Windows Event Log (Security)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_PrivilegedAccounts

Description

Monitors the Security log for entries with the following IDs (success and failure):

- 576 Special privileges assigned to new logon
- 577 Privileged Service Called
- 578 Privileged object operation

Forwards these entries as messages to the active message browser. Windows 2000 does not let you choose which rights to audit. As a result, auditing Use of User Rights will generate a very large number of audits. In most cases, the sheer volume of this information outweighs its usefulness. Do not audit Use of User Rights unless absolutely necessary for your environment. If you decide to audit Use of User Rights, you should purchase or write an event-analysis tool that can filter only the user rights of interest to your organization. If Use of User Rights is enabled, not all user rights are audited. The following user rights are never audited:

- Bypass Traverse Checking (SeChangeNotifyPrivilege)
- Generate Security Audits (SeAuditPrivilege)
- Create A Token Object (SeCreateTokenPrivilege)
- Debug Programs (SeDebugPrivilege)
- Replace A Process Level Token (SeAssignPrimaryTokenPrivilege)

The following user rights are audited only if a specific Windows Registry setting is present:

- Backup Files and Directories (SeBackupPrivilege)
- Restore Files and Directories (SeRestorePrivilege) To enable auditing of the backup and restore privileges, set the following Windows Registry value to 1:
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing (REG_DWORD)·

Type

Windows Event Log (Security)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_PrivilegedAccounts_2k8+

Description

Monitors the Security log for entries with the following IDs (success and failure):

- 576 Special privileges assigned to new logon

- 577 Privileged Service Called
- 578 Privileged object operation

Forwards these entries as messages to the active message browser. Windows 2000 does not let you choose which rights to audit. As a result, auditing Use of User Rights will generate a very large number of audits. In most cases, the sheer volume of this information outweighs its usefulness. Do not audit Use of User Rights unless absolutely necessary for your environment. If you decide to audit Use of User Rights, you should purchase or write an event-analysis tool that can filter only the user rights of interest to your organization. If Use of User Rights is enabled, not all user rights are audited. The following user rights are never audited:

- Bypass Traverse Checking (SeChangeNotifyPrivilege)
- Generate Security Audits (SeAuditPrivilege)
- Create A Token Object (SeCreateTokenPrivilege)
- Debug Programs (SeDebugPrivilege)
- Replace A Process Level Token (SeAssignPrimaryTokenPrivilege)

The following user rights are audited only if a specific Windows Registry setting is present:

- Backup Files and Directories (SeBackupPrivilege)
- Restore Files and Directories (SeRestorePrivilege) To enable auditing of the backup and restore privileges, set the following Windows Registry value to 1:
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing (REG_DWORD)·

Type

Windows Event Log (Security)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecAdminGroupChangeMonitor

Description

Monitors changes in the Enterprise and Domain Admin group.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecDirectoryServiceAccess

Description

Forwards all Security event log entries with Directory Service Access category.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecDirectoryServiceAccess_2k8+

Description

Forwards all Security event log entries with Directory Service Access category.

Type

Windows Event Log

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecErrAccessPermissions

Description

Checks the PerfLib counter Server\Errors Access Permissions for the number of attempts to access ADS elements that were denied. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. This counter warns of unauthorized access attempts that randomly seek inadequately protected files.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecErrGrantedAccess

Description

Checks the PerfLib counter Server\Errors Granted Access for the number of access attempts that opened files successfully but were allowed no further access. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number is greater than 4, the policy sends an error message. This counter warns of attempts to access files without proper authorization.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecErrorsLogon

Description

Checks the PerfLib counter Server\Errors Logon for the number of denied logon attempts to the server. If the number is between 2 and 4, the policy sends a warning message to the active message browser. If the number is greater than 4, the policy sends an error message. This counter warns of attempts to log on with a password-guessing program.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecNonTransMembEval

Description

Checks the PerfLib counter Server\SAM Non-Transitive Membership Evaluation/sec for the number of SAM nontransitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, the domain may be overloaded.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecNonTransMembEval_2k8+

Description

Checks the PerfLib counter Server\SAM Non-Transitive Membership Evaluation/sec for the number of SAM nontransitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, the domain may be overloaded.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecSDPropagatorQueue

Description

Checks the PerfLib counter NTDS\DS Security Descriptor Propagator Runtime Queue for the number of objects remaining to be examined while processing the current directory service security descriptor propagator event. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the higher threshold is exceeded, the domain controller may be overloaded.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecSDPropagatorQueue_2k8+

Description

Checks the PerfLib counter NTDS\DS Security Descriptor Propagator Runtime Queue for the number of objects remaining to be examined while processing the current directory service security descriptor propagator event. If the number exceeds 10, the policy sends a warning message to the active message browser. If the number exceeds 15, the policy sends an error message. If the higher threshold is exceeded, the domain controller may be overloaded.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_SecTransMembEval

Description

Checks the PerfLib counter NTDS\SAM Transitive Membership Evaluations for the number of SAM transitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy ends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Security

Policy: ADSPI_SecTransMembEval_2k8+

Description

Checks the PerfLib counter NTDS\SAM Transitive Membership Evaluations for the number of SAM transitive membership evaluations per second. If the number exceeds 1,000 evaluations, the policy ends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Type

Measurement Threshold (Source: Real Time Performance Management)

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Policy: ADSPI_DirComputerModif

Description

This policy sends alert messages if there is any modification to a computer in the domain.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000→ Manual-Deploy → Security

Policy: ADSPI_DirComputerModif _2k8+

Description

This policy sends alert messages if there is any modification to a computer in the domain.

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Security

Site Structure Policies

Policy: ADSPI_SiteChanges

Description

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

- **Name Space**
  Root\Directory\LDAP
- **Event Class**
  __InstanceOperationEvent
- **WQL Filter**

TargetInstance ISA "ds_site"

Successful changes in the OU structure affect the size and replication of the Active Directory database. Deploy this policy to only one node within the forest. The additional script must be executed for all sites within this domain on this node (or deployed to several nodes and execute additional scripts on these nodes).

Prerequisite: See the online Help for the Smart Plug-in for the Windows>Using Windows OS SPI policies>"Prerequisites for Windows policies."

Type

Windows Management Interface

Default Policy Group

SPI for Microsoft Active Directory → Windows Server 2003/2000 → Manual-Deploy → Site Structure

Or,

SPI for Microsoft Active Directory → Windows Server 2008 → Manual-Deploy → Site Structure

Policy: ADSPI_Logging

This policy monitors the folllowing details from various performance monitor objects:

Performance Monitor Object	Counter	Instance
Process	Page Faults/sec	LSASS
	% Processor Time	
	Working Set	
NTDS	DRA Inbound Bytes Total/sec	
	DRA Outbound Bytes Compressed (Between Sites, Before Compression)/sec	
	DS Threads in Use	
	DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec	
	DRA Outbound Bytes Total/sec	
	DRA Inbound Bytes Not Compressed (Within Site)/sec	
	DRA Outbound Bytes Not Compressed (Within Site)/sec	

The policy stores the collected data into the following columns of the ADSPI_NTDS and ADSPI_NTDSP tables:

- **ADSPI_NTDS Table**
  - DRAInboundBTS
  - DRAOutboundBCSec
  - DSThreadsinUse
  - DRAInboundBCSec
  - DRAOutboundBTS

  - DRAInboundBNCWSSec
  - DRAOutboundBNCWSSec
- **ADSPI_NTDSP Table**
  - PctProcTime
  - PageFaultsSec
  - WorkingSet

Policy group: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Manual-Deploy > Health Monitors

Related Topics:

- Descriptions of Policy Groups & Types
- Policy Group Catalog
- Discovery Policies

Components

The Microsoft Active Directory SPI installation/configuration adds components to the HPOM console tree (left pane) as follows:

Services →Systems Infrastructure ... Domains: DC:<domain_controller_name> When you select to manage a node, AD-SPI Discovery policies are deployed to that node. This adds any discovered services to the HPOM Services tree.
To view: select Services→ Systems Infrastructure→Windows→Active Directory→Domains→ DC:<dc_name>→Services.

In the right pane, the service map graphically represents the discovered DIT, DNS, operations masters/replication, and GC services running on the Active Directory domain controllers. You can view the service map by clicking any item under the Services folder.

Tools→ SPI for Active Directory:

→ **HP Operations Topology Viewer :** The Topology Viewer tool supplies information about Active Directory forests, partitions, sites, and the relationships between sites and servers in each forest. The left pane of the console display shows the hierarchy contained in one or more forests; the map in the right pane shows the selected forest topology. (The map shows only one forest at a time.)
To use the tool: at the console expand the folders **Tools →SPI for Active Directory** folder. Double-click Topology Viewer to launch the Topology Viewer window. From the File menu select **Add Forest...** and enter the fully qualified DNS name of the Domain Controller (or its IP address).
△ **Advanced Exchange Data Collection:** If you click this check box, the gathering of additional Exchange data significantly impacts the efficiency of the Active Directory display generation. You may need to wait possibly hours, depending on the size of your environment, for the process to complete.

→ **AD Trust Relationships :** This tool supplies information about trust relationships for a domain. In a Windows 2003 Server environment, it reports both two-way trusts within a forest and trusts from one forest to another for the selected nodes. In a Windows 2000 Server environment, it displays only the two-way trusts within a forest.

→**AD DC Demotion Preparation :** This tool is intended for use after you have installed the Microsoft Active Directory SPI and have begun using it. Use the tool before demoting any domain controller in your Active Directory environment to prevent the Microsoft Active Directory SPI from continuing to monitor the DC's services.

→ **Check ADS Service** : This tool connects to the ADS service of the specific node using the Microsoft Active Directory SPI.

→ **ADS Printer Information** : This tool creates a list of all printers known in the Active Directory.

→**AD Self-Healing Info** : This tool gathers error-relating data for troubleshooting operational SPI problems. See the SPI DVD Installation Guide for information about Self-Healing Services and the additional troubleshooting capabilities available through the HP Online Software Support web site.

→**Self-Healing Verification** : This tool verifies the version of the ADSPI instrumentation (executables). When launched on a managed node, the tool reports to the console if there are differences in the version of Microsoft Active Directory SPI and the Microsoft Active Directory SPI executables present on the system.

Policy groups: SPI for Active Directory — Active Directory SPI-specific policy groups are grouped for easy service discovery and policy deployment under the **Auto-Deploy** group. You need only deploy the Auto-Deploy group to all managed nodes. Then whatever Active Directory services are discovered on those nodes automatically trigger the deployment of relevant policies. The **Manual-Deploy** group is also included for you to choose from among the subgroup or individual policies for those appropriate to your Active Directory environment needs. Descriptions are available of the individual policies in Choosing a Microsoft Active Directory SPI policy .

Reports: SPI for Active Directory — Active Directory-specific reports include daily, weekly, and monthly updates. In most cases, they are updated every night. After you have installed the AD-SPI, you can view the Web-based reports the following day.

Graphs: SPI for Active Directory — Like the reports area, AD-SPI offers Active Directory-specific graphs. You can generate the graph of your choice by selecting **Graphs→SPI for Active Directory** . In the right pane right-click the graph name and selecting **Show Graph...** .

Related Topics:

- Getting Started with the Active Directory SPI
- Microsoft Active Directory SPI Policy Catalog
- Choosing a Microsoft Active Directory SPI policy

Active Directory Self Healing Info tool

The Microsoft Active Directory SPI Self-Healing Info tool is available for collecting data that can aid in troubleshooting operation of the Microsoft Active Directory SPI. When launched on a managed node, the tool gathers error message-related data, log file data related to errors, and version information for installed HP Operations products/patches.

To use the Microsoft Active Directory SPI Self-Healing Info tool:

1. At the HPOM console, select **Tools** → **SPI for Active Directory** .
2. In the details pane, right-click the **Self-Healing Info** tool and select **All Tasks** → **Launch...** .
3. In the dialog that appears, click next to the node on which you want to collect troubleshooting data. (In the message that appears, note where the compressed file will be stored.)

ⓘ **NOTE** :
Depending on a Windows setting, the file may be a hidden file on some managed nodes. If you do not see the file, open Windows Explorer and from the **Tools** menu select **Folder Options...** → **View** tabbed page. Under **Hidden files and folders** , select **Show hidden files and folders** .

In your call to HP support, send the file if the representative directs you to do so.

Related Topics:

- Getting Started with the Active Directory SPI

Self-Healing Verification tool

The Self-Healing Verification tool verifies the version of the ADSPI instrumentation (executables). When launched on a managed node, the tool reports to the console if there are differences in the version of ADSPI and the ADSPI executables present on the system.

To start the Self-Healing Verification tool:

1. At the HPOM console expand the tree to display **Operations Manager** → **Tools** → **SPI for Active Directory** → **Self-Healing Verification** .
2. Click **Launch...** .
3. As needed: In the **Edit Login** window enter User Name/Password to gain access to the system, and click **Launch...** .

Related Topics:

- Using the HP Operations Topology Viewer
- AD Trust Relationships tool
- Check ADS Services tool

AD DC Demotion Preparation tool

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 Active Directory environment. In preparation of a domain controller demotion, you use this tool to disable the Active Directory SPI from continuing to monitor the demoted DC.

To use the tool:

1. At the console in the contents (left) pane select, **Tools** → **SPI for Active Directory** .
2. In the details (right) pane, right-click **AD DC Demotion Preparation** and select **All Tasks** → **Launch Tool...** .
3. Check the box next to the node that contains the domain controller you are demoting and click **Launch...** .

ℹ **NOTE:** This tool must be used BEFORE you demote a domain controller. If you do not use the tool beforehand, you will have to manually remove the OVreplication object/user account (as described below).

To manually remove the OVReplication object (and user account) after you have demoted a domain controller:

1. Open the Active Directory Sites and Services console.
2. Select **Sites** and find the folder containing the DC that no longer exists.
3. Select the **OVReplication** folder (the OVReplication object), and delete it. (Notice that the NTDS Settings object is absent for non-existing dcs.)

To manually remove the OVReplication object user account:

1. Open the **AD User and Computer** console on any domain controller that no longer exists.
2. Open the **Users** folder.
3. Select the **OVReplication object** for the domain controller that no longer exists and delete it; for example, OVReplication-SystemTest-dc2.

Related Topics:

- Using the Topology Viewer
- Topology Viewer toolbar
- Topology Viewer menus
- Topology Viewer map connections

Check ADS Service Tool

The Check ADS Service tool connects to the ADS service of the specific node using the Microsoft Active Directory SPI.

To start the Check ADS Service tool:

1. At the HPOM console expand the tree to display **Operations Manager** → **Tools** → **SPI for Active Directory** → **Check ADS Service** .
2. Click **Launch...** .
3. As needed: In the **Edit Login** window enter User Name/Password to gain access to the system and click **Launch...** again.

Related Topics:

- Using the HP Operations Topology Viewer
- AD Trust Relationships tool
- Active Directory Printer tool

ADS Printer Information tool

The ADS Printer Information tool lists all printers known to Active Directory.
It is possible to restrict the output to specific Organizational Units (OU) by using the parameters "-ou *(name of OU)* " instead of "-all".

To start the ADS Printer Information tool:

1. At the HPOM console expand the tree to display **Operations Manager** → **Tools** → **SPI for Active Directory** → **ADS Printer Information** .
2. Click **Launch...** .
3. As needed: In the **Edit Login** window enter User Name/Password to gain access to the system, and click **Launch...** .

Related Topics:

- Using the HP Operations Topology Viewer
- AD Trust Relationships tool
- Check ADS Services tool

Delete Older ADSPI Classes tool

If you want to upgrade the Microsoft Active Directory SPI from a version lower than 5.30, you must run the Delete Older ADSPI Classes tool on all nodes during the upgrade process. The Delete Older ADSPI Classes tool removes all data tables created by the older version of the SPI from the managed node. Refer to the *Configuration Guide* for a detailed information on upgrading the Microsoft Active Directory SPI.

Do not use this tool if you upgrade the SPI from the version 5.30.

To use the Microsoft Active Directory Delete Older ADSPI Classes tool:

1. At the HPOM console, select **Tools** → **SPI for Active Directory** .
2. In the details pane, right-click the **Delete Older ADSPI Classes** tool, and then select **All Tasks** → **Launch...** .
3. In the dialog that appears, click next to the node on which you want to run the tool.

NOTE:
Use this tool only when you upgrade the Microsoft Active Directory SPI from a version lower than 5.30, as mentioned in the *Configuration Guide* . Incorrect use of the tool may lead to data loss.

Related Topics:

- Getting Started with the Microsoft Active Directory SPI

HP Operations Topology Viewer

The HP Operations Topology Viewer provides a quick means to seeing an Active Directory environment, providing a hierarchical view in a tree (left pane), and a topological view in a map (right pane). The left pane shows the partition/site/site link components, while the map in the right pane graphically represents sites/site links and server connections.

After you launch the HP Operations Topology Viewer and enter domain controller access information, the tool gathers data from the domain controller. From this information a map is created, displaying sites/servers and their replication relationships across the domain.

NOTE:
The Topology Viewer provides a view that reflects the Active Directory site/server replication information at the time you connect to a server. The view remains static until you refresh it. To update the view, select from the menu **File** → **Refresh Data** . The layout of the map is refreshed.

In the Topology Viewer window right pane, the map initially shows Active Directory site links (green lines between sites). You can display the replication links between servers and modify the display by selecting **View**→**Properties** . The Properties page allows you many options for how to display the map: you can show or hide links between sites and servers, server labels and roles, and DC and GC Exchange links (if you use the Exchange SPI as well).

Related Topics:

- Using the Operations Manager Topology Viewer
- Operations Manager Topology Viewer toolbar
- Operations Manager Topology Viewer menus
- Operations Manager Topology Viewer map connections

Using the HP Operations Topology Viewer

After you complete steps (below) to connect to an Active Directory domain controller, the Topology Viewer tool can gather information. This information is organized into a tree, showing Active Directory linked components on the left and a map graphically representing an Active Directory forest on the right.

You can modify the default display by using the **View** menu and selecting **Properties...** . The Properties page has three tabbed pages that show additional information and allow you to change the display (**Visibility** and **Colors and Lines**).

To start the Topology Viewer:

1. At the HPOM console expand the tree to display **Operations Manager** → **Tools** → **SPI for Active Directory** → **HP Operations Topology Viewer** .
2. Double-click the **HP Operations Topology Viewer** .
3. In the Topology Viewer window that appears, from the File menu select **Add Forest...** .
4. In the Add Forest dialog enter an Active Directory domain, domain controller name, or IP address; if necessary, check the Alternate Credentials check box and enter user name, password, and domain name, and click **OK** .

> ℹ **NOTE:** If the logged-in user account has proper access to the domain controller to which you are attempting to connect, no alternate credentials are necessary.

△ **Advanced Exchange Data Collection** (checkbox)**:** If you select this check box in the Connect to Forest dialog, the gathering of additional Exchange data significantly impacts the efficiency of the Active Directory display generation. You may need to wait several minutes, depending on the size of your environment, for the process to complete.

Related Topics:

- HP Operations Topology Viewer toolbar
- HP Operations Topology Viewer menus
- HP Operations Topology Viewer map

HP Operations Topology Viewer toolbar

NOTE:
See the *Smart Plug-in for Active Directory Configuration Guide* for additional information about using the HP Operations Topology Viewer.

The HP Operations Topology Viewer toolbar functions are as follows:

Starts a new file, which appears as an empty grid; you can then click the Add Forest button to populate the empty view. The "New" button allows you to transition to a new view (for example, an Add a Forest), without adding to or changing the current view if the current view has been saved.

Allows you to open a file of a previously saved view.

Saves the current view to a file.

Exports the current view and saves it to a graphic format of your choice, such as .png or .bmp. (The default format is .png.

Allows you to add a forest by opening the Add Forest dialog, where you enter server connection information.

Refreshes the data by checking information on the current connection.

Zooms out the map view to the maximum degree.

Zooms out the map view incrementally.

Resets the map view to the default.

Zooms in the map view incrementally.

Zooms in the map view to the maximum degree.

Shows the next available top-level view in the forest.

Displays the navigator, which shows a thumbnail of the entire map, surrounding the area of focus with a blue square. You can change the map focus by repositioning the blue square in the Navigator.

Displays the Topology Viewer online Help.

Related Topics:

- HP Operations Topology Viewer

- Using the Topology Viewer

HP Operations Topology Viewer menus

The HP Operations Topology Viewer menu commands are as follows:

Menu	Command	Function
File	New...	Opens a new file (empty grid); allows you to transition from the current view to a new view.
	Open...	Opens a selected, saved file that shows the layout as it was saved.
	Save	Saves the layout as the default layout.
	Save as...	Saves the layout to a file so that you can load it when desired.
	Export View...	Saves the currently displayed map in a graphical format of your choice.
	Add Forest...	Opens the Add Forest dialog, where successful connection to a server generates the replicated information within that forest and displays the information in the HP Operations Topology Viewer tree and map.
	Refresh Data	Reconnects to the server and updates the view with changes, if any, since the last connection.
View	Zoom	Allows you to zoom-in closer for greatest magnification or zoom-out farther for overall view. Minimum is at greatest degree zoomed out. Maximum is at greatest degree zoomed in.
	Next View	Shows the next view available in the right pane.
	Navigator	Shows a thumbnail of the entire map (including any area outside the current display) with a blue box indicating the current visible display.
	Legend	Displays the legend, which explains the meaning of the symbols used in the map located next to each server.
	Clear Find	When enabled, means that a server or site in the tree or the map has been right-clicked and Find in View or Find in Tree selected, resulting in selecting the corresponding item; clicking Clear Find returns the display to its default status with no elements selected.

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

Related Topics:

- Using the Topology Viewer
- Topology Viewer toolbar buttons
- HP Operations Topology Viewer map connections

HP Operations Topology Viewer map

Map connection lines labels : You can choose which connection lines to display and whether to display server and site labels by right-clicking the map, selecting **View→ Properties.** ... In the Site Topology View Properties page, select the **Colors and Lines** tabbed page. The connections are represented in default colors as follows:

Site links: Show the links between sites. These lines are the only connections initially represented. Site connections are user-defined and are the foundation on which the Active Directory is able to build connections between servers.

Server connections: Show the links between servers either in the same domain (intersite) or in different domains (intrasite). Solid lines represent connections automatically created by the KCC (Knowledge Consistency Checker); lines that display as dashes represent manually created connections (those connections created by the system administrator). You can open their display by selecting **View → Properties, Visibility** tabbed page, then select **Intersite** or **Intrasite** .

Invalid connections: Show links that once existed but are no longer valid. These previous connections are represented by a red line drawn (as solid or dashes, see above) from the center of the site where the server resided (the ghost server is represented as a red circle from which the red line originates).

Server roles/links: Check **Show Domain Controller Roles** or **Exchange Server Roles** to display icons next to those DCs and Exchange servers that have been assigned specific roles/functions. You can also choose to display various Exchange DC and global catalog links.

NOTE:
The Topology Viewer provides a view that reflects the Active Directory site/server replication information at the time you connect to a server. The view remains static until you refresh it. To update the view, select from the menu **File →Refresh Data** . The map is then updated.

Related Topics:

- Using the HP Operations Topology Viewer
- Operations Manager Topology Viewer toolbar
- HP Operations Topology Viewer menus

AD Trust Relationships Tool

The AD Trust Relationships tool generates a quick list of the trust relationships established for the selected node.

To start the HP Operations Topology Viewer:

1. At the HPOM console expand the tree to display **Operations Manager** → **Tools** → **SPI for Active Directory** → **AD Trust Relationships** .
2. Double-click the **AD Trust Relationships** .
3. In the window that appears, select the node on which to launch the tool and click **Launch...** .
4. (as needed) In the Edit Login window enter User Name/Password allowing access to the system and click Launch... again.

NOTE:
The Trust Relationships information that appears will be more extensive for Windows 2003 systems than for Windows 2000 systems.

Related Topics:

- Using the HP Operations Topology Viewer
- ADS Printer Information
- Check ADS tool
- AD DC Demotion Preparation tool
- Active Directory Self Healing Info tool

Reports

NOTE:
The Smart Plug-in for Microsoft Active Directory Configuration Guide contains information about the policies required for each report. See the section "Reporting and Graphing" for details.

After you install the Microsoft Active Directory SPI, and if HP Reporter is installed in the monitoring environment, HPOM can generate reports, using the Microsoft Active Directory SPI-collected data. The reports do not immediately appear in the HPOM console tree because they are generated every night. After HPOM runs through its first nightly schedule, on the next day you can expect to see reports. Each night from that point on HPOM, by default, re-generates reports with the updated daily data.

Reports are identified as daily, weekly, or monthly and update as follows:

- **Daily** : Updated nightly, a daily report reflects the last 24 hours' worth of data; the previous report data is deleted.
- **Weekly** : Updated nightly, a weekly report reflects the last seven days' worth of data. (Data from the previous eighth day is deleted.)
- **Monthly** : Updated after the calendar month completes, a monthly report summarizes all data collected during the last calendar month.

NOTE : The first monthly report most likely will represent a partial month's worth of data. For example, if the Active Directory SPI installation occurred on March 18, the first report would be available April 1 and would include data from March 19 to the last day in March.

Microsoft Active Directory SPI reports are located in the HPOM console under:
Reports → SPI for Microsoft Active Directory .

Related Topics:

- Microsoft Active Directory SPI Graphs

AD DC DNS Availability Report (daily/weekly)

Report Template File Name: g_ADDNSDCAvailDaily.rpt/g_ADDNSDCAvailWeekly.rpt

The report summarizes the availability of the domain controller's DNS based on a daily/weekly basis. The daily report provides a percentage of the DNS availability based on each hour over the last 24 hours, while the weekly report is based on hourly averages over the last seven-day period.

Report contents:

The report columns are as follows:

- **Computer Name -** Provides the name of each computer specified in the report criteria.
- **Availability -** Identifies the percentage of time the DNS server was available during the time specified in the report criteria.

Required Policies

For this report to work properly, deploy the following policy:

Policy name: ADSPI-DNS_DC_Response
Schedule: Every 5 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > Response Time Monitoring
Table name in the data store (CODA/HP Performance Agent): ADSPI_DNSDR
HP Reporter Table:
ADSPI_DNS_DCRESP (Mapped from the ADSPI_DNSDR table from the data store on the Active Directory node)
Columns:
RESPTIME
SYSTEMNAME
DATETIME

Related Topics:

- Microsoft Active Directory SPI Reports

AD DIT Disk Queue Length Report (weekly)

Report Template File Name: g_ADDITQueueLengthWeekly.rpt

This report summarizes the weekly queue length patterns of the disk holding the Directory Information Tree (DIT) for the domain controllers. This information helps to identify domain controllers with potential disk bottlenecks.

Report contents:

The columns of this report are defined as follows:

- **System Name -** Specifies the name of the Domain Controller.
- **Domain Name -** Name of the Domain that the Domain Controller belongs to.
- **Site Name -** Specifies the time the disk space data was collected.
- **DIT Path -** DIT Database path location.
- **Queue Length -** Disk Queue Length on DIT Disk.

Required Policies

For this report to work properly, deploy the following policies:

- ADSPI-DIT_DITQueueLength (runs with the schedule of 5 minutes)
- ADSPI-DIT_TotalDITSize (runs with the schedule of one day)

Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > DIT Monitoring
Table names in the data store (CODA/HP Performance Agent):
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_DITQUEUELENGTH
HP Reporter Tables:
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_DITQUEUELENGTH
Columns:
DOMAINVALUE
SITEVALUE

DITQLNAME
DITQLVALUE
SYSTEMNAME
DATETIME

Related Topics:

- AD DIT Disk Size Summary Report
- AD DIT Logfiles Disk Size Summary Report
- Replication Latency Graph

AD DIT Disk Size Summary Report (weekly/monthly)

Report Template File Name: g_ADDITDiskSpaceWeekly.rpt/ g_ADDITDiskSpaceMonthly.rpt

This bar chart (weekly) and line chart (monthly) report summarizes the usage patterns of the disk holding the Directory Information Tree (DIT) for the domain controllers. This information helps to identify domain controllers with potential disk bottlenecks.

Report contents:

The chart shows the average percentage DIT disk space full on each domain controller. This graph makes it possible to identify when the disk is full and take appropriate actions.

The columns of the report are defined as follows:

- **System Name** - Specifies the name of the Domain Controller.
- **Domain Name** - Name of the Domain that the Domain Controller belongs to.
- **Site Name** - Specifies the time the disk space data was collected.
- **DIT Size** - The size of the DIT Database in MB.
- **%Disk Space Full** - The percentage used space on the disk holding the DIT database.

Required Policies

For this report to work properly, deploy the following policies:

- ADSPI-DIT_DITPercentFull (runs with the schedule of 5 minutes)
- ADSPI-DIT_TotalDITSize (runs with the schedule of one day)

Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > DIT Monitoring

Table names in the data store (CODA/HP Performance Agent):
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_DITPercentFull
ADSPI_DITDBSIZE

HP Reporter Tables:
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_DITPercentFull
ADSPI_DITDatabaseSize (Mapped from the ADSPI_DITDBSIZE table from the data store on the Active Directory node)
Columns:
DOMAINVALUE
SITEVALUE
DITPTVALUE
INSTANCEVALUE
_INSTANCENAME
DATETIME

Related Topics:

- Active Directory SPI Reports
- AD Operations Master Connection Time Report (sorted by FSMO)
- Replication Latency Graph

AD DNS Server Memory Capacity Planning Report (weekly/monthly)

Report Template File Name:
g_ADDNSSrvMemCapPlanDaily.rpt/g_ADDNSSrvMemCapPlanWeekly.rpt

This report graphs the memory capacity for each specified DNS server running Active Directory services; one shows use over the last week; another shows use over the last month. The graph indicates the minimum, maximum, and average daily usage based on the Memory/Pages Per Second performance counter.

Report contents:

This report provides one graph for each specified DNS server with Active Directory Services running.

- **Average pages per second** - Average number of pages used per second.
- **Max pages per second** - Maximum number of pages used per second.
- **Min pages per second** - Minimum number of pages used per second.

Required Policies

For this report to work properly, deploy the following policy:

Policy name: ADSPI-DNS_LogDNSPagesSec
Schedule: Every 30 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > DNS Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_DNSSP
HP Reporter Table:
ADSPI_DNSSP
Columns:
SYSTEMNAME
DATETIME
PAGESPERSEC
ISDOMAINCTRL

Related Topics:

- Microsoft Active Directory SPI Reports

AD DNS Server Availability Report (daily/weekly)

Report Template File Name: g_ADDNSSrvAvailDaily.rpt/g_ADDNSSrvAvailWeekly.rpt

The DNS Server Availability report summarizes the availability of DNS servers with Active Directory services running, based on hourly and weekly data. The daily report provides a percentage of availability based on each hour over the last 24-hour period. The weekly report provides hourly percentages as well, based on each hour over the last 7-day period.

Report contents:

The report displays a pie chart indicating the percentage of availability of the DNS servers with Active Directory services running.

The report columns are as follows:

- **Response Time in miliseconds** - Provides the response time of the DNS server in miliseconds.
- **Date time** - Date and time when the data was gathered.

Required Policies

For this report to work properly, deploy the following policy:

Policy name: ADSPI-DNS_Server_Response
Schedule: Every 30 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > DNS Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_DNSSR
HP Reporter Table:
ADSPI_DNSSR
Columns:
SYSTEMNAME
DATETIME
RESPONSETIME
ISDOMAINCONTROLLER

Related Topics:

- Microsoft Active Directory SPI Reports

AD Domain Controller Availability Report

Report Template File Name: g_ADDCAvailability.rpt

This report displays the percentage of time Active Directory and the Global Catalog were successfully connected to and queried in a series of pie charts. Possible causes of falling availability are a lack of system resources, mis-configuration, or failures in Active Directory.

Report contents:

The report displays two pie charts, which are described as follows:

1. **Active Directory Availability:** The Active Directory SPI will periodically query the directory on your domain controller to determine response time and availability. This graph shows the percentage of time the directory was successfully contacted.
2. **Active Directory Global Catalog Availability:** The Active Directory Global Catalog is queried on the port 3268. The success of the attempt is used to calculate Global Catalog availability.

The report displays a table that lists the following details:

- **GC Availability** - Identifies the availability of Global Catalog, queried on the port 3268, during a particular range of time.
- **Date Time** - Date and time when the data was gathered.

Required Policies

For this report to work properly, deploy the following policy:

Policy name: ADSPI-Response_Logging
Schedule: Every 5 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > Response Time Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_RESPONSETIME
HP Reporter Table:
ADSPI_RESPONSEMON (Mapped from the ADSPI_RESPONSETIME table from the data store on the Active Directory node)
Columns:
AVAILABILITY
GCAVAILABILITY

SYSTEMNAME
DATETIME

Related Topics:

- Microsoft Active Directory SPI Reports

AD Domain and Forest Changes Report (weekly and monthly)

Report Template File Name:
g_ADDomainForestTrustMonthly.rpt/g_ADDomainForestTrustWeekly.rpt

This report presents the domain and forest trust changes in Active Directory for the selected report: either weekly or monthly. The report provides information illustrating addition, deletion and modification of trusts on Windows Server 2003 and 2008 Domain Controllers only.

Report contents:

In the report, a table displays the following details:

- **System Name** : Name of the Domain Controller
- **Trusting Domain** : Name of the Trusting Domain
- **Date Time** - Date and time when the data was gathered
- **Change Type** - Type of trust change
- **Trusted Domain** : Name of the Trusted Domain
- **Attributes** : A value that indicates the attributes of the trust relationship:
  1 is Disallow Transitivity
  2 is Uplevel clients only
  4 denotes the trust setting to another tree root in the forest
  32 denotes the trust setting to the parent in the organization tree
- **Direction** : A value that indicates the direction of Trust:
  1 is Inbound
  2 is Outbound
  3 is Bi-directional
- **Trust Status** : String description of trust status.
- **Trust Type** : A value that indicates the type of the trust relationship:
  1 is Downlevel
  2 is Uplevel
  3 is Non-Windows Kerberos Realm
  4 is DCE

Policy name: ADSPI-Trust_Mon_Modify
Schedule: Every 30 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > Trust Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_TRUST
HP Reporter Table:
ADSPI_TRUST
Columns:
DATETIME
CHANGETYPE
TRUSTEDDOMAIN
TRUSTATTRIBUTES
TRUSTDIRECTION
TRUSTSTATUSSTRING
TRUSTTYPE
TRUSTINGDOMAIN

Related Topics:

- Microsoft Active Directory SPI Reports

AD GC Replication Delay Times by DC/GC (weekly/monthly)

Report Template File Name: g_ADDCGCweekly.rpt/g_ADDCGCmonthly.rpt

This report summarizes delay times for replication from domain controllers to global catalog servers. Weekly reports show the average, maximum, and minimum replication delays occurring over the last over the last 7 days, while monthly reports show averages from the last calendar month.

This information helps to identify global catalog replication trends and potential replication problems. The report specifies a date range in which the data collection took place.

Report contents:

The report displays a bar graph showing the average replication delay per global catalog server for every domain controller.

Policy name: ADSPI-Rep_GC_Check_and_Threshold
Schedule: Every 15 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > GC Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_GCREP
HP Reporter Table:
ADSPI_REP_GC (Mapped from the ADSPI_GCREP table of the data store on the node)
Columns:
DATETIME
SYSTEMNAME
GCREPNAME
LATENCYDELTA

Related Topics:

- Microsoft Active Directory SPI Reports
- Microsoft Active Directory SPI Replication Latency Graph

AD GC Rep Delay Times By GC/DC (weekly/monthly)

Report Template File Name: g_ADGCDCweekly.rpt/g_ADGCDCmonthly.rpt

This report summarizes delay times for replication from a global catalog server to each domain controller. Weekly reports show the replication delays as they are averaged over the last 7 days. Monthly reports show replication delays as they are averaged over the last calendar month.

This information helps to identify global catalog replication trends and potential replication problems. The report specifies a date range in which the data collection took place.

Report contents:

The report displays a bar graph showing the average replication delay per domain controller for every global catalog server.

Policy name: ADSPI-Rep_GC_Check_and_Threshold
Schedule: Every 15 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > GC Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_GCREP
HP Reporter Table:
ADSPI_REP_GC (Mapped from the ADSPI_GCREP table of the data store on the node)
Columns:
DATETIME
SYSTEMNAME
DCREPNAME
LATENCYDELTA

Related Topics:

- AD GC Replication Delay Times Report DC/GC
- Microsoft Active Directory SPI Replication Latency Graph

AD GC Response Time Report (weekly/monthly)

Report Template File Name: g_ADGCResponseTimeeWeekly.rpt/g_ADGCResponseTimeMonthly.rpt

This report summarizes the average response times of global catalog servers. The information contained in this report helps identify global catalog servers with potential over-loading and bottlenecks.

The weekly report shows averages occurring over the last 7-day period, while the monthly report shows averages over the last calendar month. Each report identifies the data collection period with a start/end date range.

Response times are based on the global catalog queries and binds, which are shown in a graph. The graph shows averages for each of the global catalog servers. With this information it is possible to identify those global catalog servers that are over-loaded and take appropriate actions.

Report contents:

The report shows a chart that shows the weekly average query and bind response times (in seconds) on each global catalog server. Using this graph, you can identify the events when the global catalog server was over-loaded and take appropriate actions.

Policy name: ADSPI-Response_Logging
Schedule: Every 5 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > Response Time Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_RESPONSETIME
HP Reporter Table:
ADSPI_RESPONSEMON (Mapped from the ADSPI_RESPONSETIME table of the data store on the node)
Columns:
DATETIME
SYSTEMNAME
GCBINDTIME
GCQUERYTIME
GCPRESENT

Related Topics:

- AD Global Catalog Replication Latency Report
- Microsoft Active Directory SPI Reports

AD Log Files Disk Queue Length Report (weekly)

Report Template File Name: g_ADLogQueueLengthWeekly.rpt/ g_ADLogQueueLengthMonthly.rpt

This report summarizes the weekly queue length patterns of the disk holding the Active Directory log files for the domain controllers. This information helps to identify domain controllers with potential disk bottlenecks.

Report contents:

The columns of this report are defined as follows:

- **System Name** - Specifies the name of the domain controller.
- **Domain Name** - Name of the Domain that the domain controller belongs to.
- **Site Name** - Specifies the time the disk space data was collected.
- **Log Files Path** - Log files path location.
- **Queue Length** - Disk queue Length on the log files disk.

Required Policies

For this report to work properly, deploy the following policies:

- ADSPI-DIT_LogFilesQueueLength (runs with the schedule of 5 minutes)
- ADSPI-DIT_TotalDITSize (runs with the schedule of one day)

Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > DIT Monitoring

Table names in the data store (CODA/HP Performance Agent):
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_LOGQUEUELENGTH
HP Reporter Tables:
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_LOGQUEUELENGTH

Columns:
DOMAINVALUE
SITEVALUE
LGQLENNAME
LGQLENVALUE
SYSTEMNAME
DATETIME

Related Topics:

- Microsoft Active Directory SPI Reports

AD Log Files Disk Size Summary Report (weekly/monthly)

Report Template File Name: g_ADLogFilesDiskSpaceWeekly.rpt/ g_ADLogFilesDiskSpaceMonthly.rpt

This report summarizes the weekly and monthly usage of the disk holding the Active Directory log files for the domain controllers. This information helps to identify domain controllers with potential disk bottlenecks.

Report contents:

The columns of this report are defined as follows:

- **System Name** - Specifies the name of the domain controller.
- **Domain Name** - Name of the Domain to which the domain controller belongs.
- **Site Name** - The site in which the domain controller is located.
- **Log Files Path** - Log files path location.
- **Disk Size** - Size of the Log Files disk.
- **Disk Space** - Available disk space on the log files disk.

Required Policies

For this report to work properly, deploy the following policies:

- ADSPI-DIT_LogFilesPercentFull (runs with the schedule of one day)
- ADSPI-DIT_TotalDITSize (runs with the schedule of one day)

Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > DIT Monitoring

Table names in the data store (CODA/HP Performance Agent):
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_LOGDISKSIZE
ADSPI_LOGPERCENTFULL

HP Reporter Table:
ADSPI_DOMAIN
ADSPI_SITE
ADSPI_LOGDISKSIZE
ADSPI_LOGPERCENTFULL
Columns:
DOMAINVALUE
SITEVALUE
LGPERFULLVALUE
SYSTEMNAME
DATETIME

Related Topics:

- Microsoft Active Directory SPI Reports

Active Directory Memory Usage

Report Template File Name: g_ADMemoryUsage.rpt

This report examines the Active Directory memory-usage pattern from the logged data and displays the general patterns of memory usage between Domain Controllers.

Report contents:

The report presents two sections:

- Active Directory LSASS Page Faults Average—this section displays usage patterns for Active Directory's Page Faults in the form of a bar graph. The graph shows the average rate of occurance of page faults by the threads running in the LSASS processr. If a thread refers to a virtual-memory page, which is not available in its working set inside the main memory, the page fault occurs.
- Active Directory LSASS Working Set Average—This section displays usage patterns for Active Directory's working set in the form of a bar graph. The graph shows the average number of bytes in the working set of the LSASS process. The set of memory pages, which were touched by the threads in the process, is the working set. If the free memory on the managed node exceeds a certain threshold, pages reside in the working set of a process, even though they are not being use. If the free memory falls below the threshold, pages are removed from working sets.

Required Policies

For this report to work properly, deploy the following policy:

Policy Name: ADSPI_Logging
Schedule: Every hour
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Manual-Deploy > Health Monitors
Table names in the data store (CODA/HP Performance Agent):
ADSPI_NTDS
ADSPI_NTDSP
HP Reporter Tables :
ADSPI_NTDS
ADSPI_NTDSP
Columns:
SYSTEMNAME
DATETIME
WORKINGSET

PAGEFAULTSSEC

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

AD Operations Master Connection Time (sorted by FSMO or server)

Report Template File Name: g_ADOpMstrConTimeByFsmo.rpt/g_ADOpMstrConTimeBySvr.rpt

This report provides a graph of the ping time and bind time for Operations Masters services from a specified domain controller. 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.

This report is sorted by:

- FSMO type, and then by domain controller

  or

- Server, and then by domain controller

There is one graph by FSMO service/domain controlle.

Report contents:

The report graph displays the following Active Directory performance counters:

- Op Master Domain Naming Last Ping/Bind (seconds)
- Op Master PDC Last Ping/Bind (Seconds)
- Op Master Schema Last Ping/Bind (Seconds)
- Op Master Infrastructure Last Ping/Bind (Seconds)
- Op Master RID Last Ping/Bind (Seconds)

Policy name: ADSPI-FSMO_Logging
Schedule: Every 5 minutes
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > FSMO Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_FSMO
HP Reporter Table:
ADSPI_FSMO_MET (Mapped from the ADSPI_FSMO table of the data store on the node)
Columns:

DATETIME
SERVER
GMT
FSMO
FSMOBINDTIME
PINGTIME

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

Active Directory Processor Usage

Report Template File Name: g_ADProcessUsage.rpt

This report examines the Active Directory processor-usage pattern from the logged data. The report displays
general usage patterns between Domain Controllers.

Report contents:

The report presents two sections:

- Active Directory Average LSASS Percent Processor Time/sec—this section displays the average percentage of processor time used by all threads of the LSASS process to run instructions.
- Active Directory Average Number of Threads/sec—this section displays the average usage patterns for Active Directory's threads that are in use in the form of a bar graph. The graph shows the average number of threads *in use* by the directory service (not the number of threads in the directory service process). This is the number of threads that are serving the client API calls.

Required Policies

For this report to work properly, deploy the following policy:

Policy Name: ADSPI_Logging
Schedule: Every hour
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Manual-Deploy > Health Monitors
Table names in the data store (CODA/HP Performance Agent):
ADSPI_NTDS
ADSPI_NTDSP
HP Reporter Tables :
ADSPI_NTDS
ADSPI_NTDSP
Columns:
SYSTEMNAME
DATETIME
DSTHREADSINUSE

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

Active Directory Replication Inbound

Report Template File Name: g_ADReplicationInbound.rpt

This report examines the Active Directory replication usage pattern from the logged data. The report allocates the replication-transmission statistics of intra-site replication and replication among different sites and shows the usage pattern of inbound Active Directory replication.

Report contents:

The report presents a graph that shows the average of Inbound Bytes Replicated/sec within a site and Inbound Bytes Replicated/sec among different sites by the Active Directory Service for all monitored nodes.

Required Policies

For this report to work properly, deploy the following policy:

Policy Name: ADSPI_Logging
Schedule: Every hour
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Manual-Deploy > Health Monitors
Table names in the data store (CODA/HP Performance Agent):
ADSPI_NTDS
HP Reporter Table:
ADSPI_NTDS
Columns:
DRAINBOUNDBCSEC
DRAINBOUNDBSNCWSSEC
SYSTEMNAME
DATETIME

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

Active Directory Replication Outbound Report

Report Template File Name: g_ADReplicationOutbound.rpt

This report examines the Active Directory replication usage pattern from the logged data. The report allocates the replication-transmission statistics of intra-site replication and replication among different sites and shows the usage pattern of outbound Active Directory replication.

Report contents:

The report presents a graph that shows the average of Outbound Bytes Replicated/sec within a site and Outbound Bytes Replicated/sec among different sites by the Active Directory Service for all monitored nodes.

Required Policies

For this report to work properly, deploy the following policy:

Policy Name: ADSPI_Logging
Schedule: Every hour
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Manual-Deploy > Health Monitors
Table names in the data store (CODA/HP Performance Agent):
ADSPI_NTDS
HP Reporter Table :
ADSPI_NTDS
Columns:
DRAOUTBOUNDBCSEC
DRAOUTBOUNDBSNCWSSEC
SYSTEMNAME
DATETIME

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

Active Directory Replication Summary Report

Report Template File Name: g_ADReplicationSummary.rpt

This report examines the Active Directory replication usage pattern from the logged data. The report allocates the replication-transmission statistics intra-site replication and replication among different sites and shows an overall usage pattern of Active Directory replication.

Report contents:

The report shows the following attributes:

- Inbound Bytes Received/sec—represents the number of bytes received for replication during the monitored period
- Outbound Bytes Transmitted/sec—represents the number of bytes transmitted by the system for replication during the monitored period

The report represents the data in the form of a bar graph. With the graph, you can determine the overall replication usage pattern for all monitored systems and you can identify the systems with the highest replication load.

Required Policies

For this report to work properly, deploy the following policy:

Policy Name: ADSPI_Logging
Schedule: Every hour
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Manual-Deploy > Health Monitors
Table names in the data store (CODA/HP Performance Agent):
ADSPI_NTDS
HP Reporter Table:
ADSPI_NTDS
Columns:
DRAINBOUNDBTS
DRAOUTBOUNDBTS
SYSTEMNAME
DATETIME

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

AD Size of Sysvol Report (weekly/monthly)

Report Template File Name: g_ADSizeOfSysvolWeekly.rpt/g_ADSizeOfSysvolMonthly.rpt

This report provides a weekly summary of the Sysvol (system volume shared directory on the Domain Controller) disk space information for the specified domain controller. The columns of this report are defined as follows:

- **Domain Computer Name -** Provides the name of each computer specified in the report criteria.
- **Time of Collection -** Specifies the time the disk space data was collected.
- **Sysvol File Path -** File path to where the Sysvol exists.
- **Sysvol Drive Free Space -** Free space on the drive which contains the Sysvol.

Report contents:

The report presents a line graph indicating the percentage of occupied disk space on sysVol drives.

Policy name: ADSPI-Sysvol-PercentFull
Schedule: Once every day
Location: SPI for Active Directory > en > Windows 2003/2000 or Windows 2008 > Auto-Deploy > Sysvol Monitoring
Table name in the data store (CODA/HP Performance Agent):
ADSPI_SYSVOL_PTFULL
HP Reporter Table:
ADSPI_SYSVOL_PCT_FULL (Mapped from the ADSPI_SYSVOL_PTFULL table of the data store on the node)
Columns:
DATETIME
SYSTEMNAME
SYSPERCNAME
SYSPERCVALUE

Related Topics:

- Getting Started
- Microsoft Active Directory SPI Reports

Troubleshooting Microsoft Active Directory Reports

If the report is not being generated or if it is empty, follow these steps:

1) Check the reporter package installation.

- Make sure that the Microsoft Active Directory SPI Reporter package was installed on the HP Reporter server.
- Check for errors in the Reporter Status pane.
- If there are Reporter installation errors, report the problem.

2) Check the Reporter database.

- Check if the data is available in the HP Reporter database.
- Check the HP Reporter database on the HP Reporter server.
- Run the following SQL commands to see if data for a particular metric is being collected:
  SELECT * FROM *<Table Name>*
  where *<Table Name>* is the name of the table in the HP Reporter database that includes the data required by the report. Refer to individual help topic for reports to know *<Table Name>* .
- If there is data in the Reporter database for every metric used and the HP Reporter trace files do not reveal the cause of the problem, contact the HP Support Team. To enable Reporter trace, run **repmaint.exe -trace 9** on the HP Reporter server.
- If the data for some or all of the used metrics are missing from the Reporter database, go to the next step.

3) Check the data store.

- If there is no data in the Reporter database and the Microsoft Active Directory SPI Reporter package is installed properly, check that the data is being collected/logged on the managed node into the data store (CODA or HP Performance Agent).
- If you are using CODA:
  - Run the following CODA diagnostic command on the managed node to get the last logged record:
    - On an HTTPS-managed node: **ovcodautil -dumpds ADSPI**
    - On a DCE-managed node: **codautil -dumpds ADSPI**

  - If there is no data in the CODA database, check if the CODA agent is running.
  - You can restart CODA on the managed node by running:
    On HTTPS-managed nodes: **ovc -start coda**
    On DCE-managed nodes: **opcagt -start -id 12**
- If you are using the HP Performance Agent, refer to the HP Performance Agent documentation.

4) Have the policies been deployed?

There will be no data unless the policy is deployed. Check on the managed node to ensure the necessary policies were deployed and are enabled by running the command **opctemplate** or **ovpolicy** . Refer to individual help topics for reports to know the required policies for the report.

5) Is the agent on the managed node running?

- Check that the HP Operations agent is running. Run the following command on the managed node to get the status of the agent:
  - On the HTTPS-managed nodes: **ovc -status**
  - On the DCE-managed nodes: **opcagt -status**
- If the HP Operations agent is not running, restart with the following command:
  - On the HTTPS-managed nodes: **ovc -start**
  - On the DCE-managed nodes: **opcagt -start**

Graphs

After you install the Microsoft Active Directory SPI and data has been allowed to accumulate, you can use the HPOM graphing feature to generate graphs. Graphs offer you the ability to choose a system as well as a date/time range to view the data for a more customized perspective.

You generate a graph as follows:

1. At the console select: **Graphs** → **SPI for Active Directory** .
2. Double-click the desired graph group.
3. Right-click the graph and select **Show Graph...** .
4. In the dialog that appears enter information as required.

Related Topics:

- Active Directory GC Availability Graph
- Active Directory Replication Latency Graph
- Active Directory Replication Time by GC Graph
- Active Directory Bind Response Time Graph
- Active Directory Query Response Time Graph

Active Directory GC Availability Graph

The Microsoft Active Directory SPI includes a graph that shows the general availability of the global catalog on those systems hosting GC services.

To calculate availability of the global catalog each Active Directory node, the Active Directory global catalog service is queried on port 3268. Each successful attempt is counted and logged per collection interval.

NOTE:
To generate this graph you must deploy the ADSPI-Response_Logging policy.

The graph is available in the HPOM console under **Graphs** → **Graphs** → **SPI for Active Directory** .

Related Topics:

- Active Directory SPI Graphs
- Microsoft Active Directory SPI Reports

Active Directory Replication Latency Graph

The Microsoft Active Directory SPI includes this graph to help you establish baselines for the frequency of the replication monitoring schedules and thresholds.

NOTE:
Schedules are set in the ADSPI-Rep_ModifyObjc and ADSPI-Rep_Mon policies. Thresholds are established in the ADSPI-Rep_Mon threshold policy.

The graph is available in the HPOM console under **Graphs → SPI for Active Directory** .

This graph tracks latency replication response times as measured through the ADSPI-Rep_ModifyObj and ADSPI-Rep_Mon policies. The graph shows the results of the collected data in terms of maximum, average, and minimum response times.

Related Topics:

- Active Directory SPI Graphs
- Microsoft Active Directory SPI Reports

Active Directory Replication Time by Global Catalog

This graph shows the average replication time of Active Directory from selected global catalog domain controllers.

NOTE:
Schedules are set in the ADSPI-Rep_ModifyObjc and ADSPI-Rep_Mon policies. Thresholds are established in the ADSPI-Rep_Mon threshold policy.

The graph is available in the HPOM console under Graphs→ SPI for Active Directory. This graph tracks latency replication response times as measured through the **ADSPI-Rep_ModifyObj** and **ADSPI-Rep_Mon** policies. The graph shows the results of the collected data in terms of maximum, average, and minimum response times.

Related Topics:

- Microsoft Active Directory SPI Graphs
- Microsoft Active Directory SPI Reports

Active Directory Bind Response Time Graph

This graph shows the response times that a domain controller averages when binding to Active Directory in general and the Global Catalog in particular. The graph provides one line for Ative Directory (labeled Directory) and one for Global Catalog (labeled Catalog) binds.

To display the graph:

1. In the console left pane, select **Graphs** → **SPI for Active Directory** .
2. In the left pane select **Response Time Monitoring** .
3. In the right pane, right-click **Active Directory Bind Response Time** and select **Show Graph...** .
4. Make selections as desired for nodes/time range and click **Finish** .

Related Topics:

Microsoft Active Directory SPI Reports

Active Directory Query Response Time Graph

This graph shows the average response that a domain controller averages when querying Active Directory in general and the Global Catalog in particular. The graph provides one line for Active Directory (labeled Directory) and one for Global Catalog (labeled Catalog) queries.

To display the graph:

1. In the console left pane, select **Graphs** → **SPI for Active Directory** .
2. In the left pane select **Response Time Monitoring** .
3. In the right pane, right-click **Active Directory Query Response Time** and select **Show Graph...** .
4. Make selections as desired for nodes/time range and click **Finish** .

Related Topics:

- Microsoft Active Directory SPI Graphs
- Microsoft Active Directory SPI Reports