HP Operations Smart Plug-in for Microsoft Active Directory

for HP Operations Manager for Windows®

Software Version: 7.06

PDF version of the online help

This document is a PDF version of the online help that is available in the Smart Plug-in for Microsoft Active Directory. 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: June 2011
Software Release Date: January 2011

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

UNIX® is a registered trademark of The Open Group.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

TABLE OF CONTENTS

Microsoft Active Directory Smart Plug-in Overview

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

The Smart Plug-in for Microsoft Active Directory (Microsoft Active Directory SPI) helps you to manage the Microsoft Active Directory in your environment. The Microsoft Active Directory SPI keeps you informed about the conditions related to Microsoft Active Directory and updates you with the following activities:

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

Related Topics:

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

Components of Microsoft Active Directory SPI

The components of the Microsoft Active Directory SPI are:

- *Policies:* Pre-defined thresholds to keep a constant vigilance over the Microsoft Active Directory environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts are shown in service map while messages are available in message browser. Policies can be auto or manual. For more information on policies see Using Policies .
- *Tools:* Utilities to gather more Microsoft Active Directory related information. You can also launch tools to view the Microsoft Active Directory environment. For more information see Using Tools .
- *Reports:* Pictorial representation of various metrics of Microsoft Active Directory. Data collected by policies are used to generate reports. For more information on reports see Using Reports
- *Graphs:* Graphical representation of various metrics of the Microsoft Active Directory. Reports contain the data that are collected by policies. For more information on graphs, see Using Graphs .

NOTE:
Reports and graphs generated with the help of HP Reporter and HP Performance Manager provide you an overview to determine corrective actions to be taken in the long term.

Related Topics:

- Getting Started with Microsoft Active Directory SPI
- Service and Component Discovery of Microsoft Active Directory SPI

Getting Started with Microsoft Active Directory SPI

The HP Operations Smart Plug-ins DVD contains the Microsoft Active Directory SPI. Refer the *Microsoft Active Directory Installation and Configuration Guide* for complete installation, upgrade, and configuration procedures.

To verify if the Microsoft Active Directory SPI is installed properly, check the SPI under policy group. Expand **Policy Group** under **Policy Management** . The **SPI for Active Directory** in the list verifies the installation. You can further expand **SPI for Active Directory** and check for **Windows Server 2003** and **2008** polices.

NOTE:
To verify the upgrade of the Microsoft Active Directory SPI, ensure that the version of the policies and binaries is 7.650.

After you configure the Microsoft Active Directory SPI, the HP Operations Management (HPOM) console shows updates in the following areas:

- *Service Map:* Service map shows the newly added and discovered Microsoft Active Directory services displayed in both the console services tree (left) and the service map (right). Within the service map pane, the hierarchy expands to show the specific services present on each DC. Further expansion of each DC displays its components.
- *Message Browser:* Displays messages identified with the problem severity level.
- *Reports and Graphs:* Presents the information that helps you see trends to manage the Microsoft Active Directory in your environment by implementing efficient load balancing, capacity planning, and policy scheduling and threshold adjustments.
- *HP Operations Topology Viewer Tool:* Enables you to view the Microsoft Active Directory topology after it connects to a Microsoft Active Directory DC. For more information on this tool see HP Operations Topology Viewer .

Prerequisite : Install the HPOM console, management server, and agents for Microsoft Active Directory SPI programs to work.

Related Topics:

- Auto Deploying Policies for Managed and Unmanaged Nodes
- Service and Component Discovery of Microsoft Active Directory SPI

Auto Deploying Policies for Managed and Unmanaged Nodes

Policies of the Auto-Deploy group are automatically deployed. **Manual-Deploy** policies are not deployed with this procedure. You can deploy the Manual-Deploy policies, either their subgroups or individual policies, for the Microsoft Active Directory environment. See Choosing a Microsoft Active Directory SPI policy for descriptions of policies within this group.

- To deploy Auto-Deploy policies for *managed nodes* , select **Policy Groups → SPI for Active Directory → en → Windows Server 2003** (or **2008**) **→ Auto-Deploy → Discovery**
- To deploy Auto-Deploy policies on *unmanaged nodes* :
    1. Right-click **Nodes → Configure →Nodes.**
    2. Drag and drop the nodes 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. The policies can then monitor Active Directory processes, reporting on status or problems through service map alerts and messages in the HPOM browser.

Related Topics:

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

Service and Component Discovery of Microsoft Active Directory SPI

The Microsoft Active Directory SPI monitors the Microsoft Active Directory environment by discovering the existing components of the Microsoft Active Directory in your environment and maintaining thresholds set up by the policies. The Microsoft Active Directory SPI expands that discovery and adds multiple hierachical levels of details.

At a higher level, the SPI discovers forests and goes further to the lower levels to discover each domain controller (DC) with its name and further, services and components available with it including sites, the preferred PBHS connecting the sites, replication, and sysvol. In this way the SPI shows partitions in the discovered sites. The service map identifies the Microsoft Active Directory forest and the specific DC, and its services and components. With each expansion you can drill down from a service alert at the forest level to the specific service or component in a specific DC that is the root cause.

To view the Microsoft Active Directory components select:

Services → Systems Infrastructure → Active Directory → Domains → DC:<dc_name> → Services

When you select to manage a node, Microsoft Active Directory SPI Discovery policies are deployed to that node. This adds any discovered services to the HPOM Services tree.

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.

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

> For complete configuration procedure, see *Microsoft Active Directory Installation and Configuration Guide* .

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

Related Topics:

- Getting Started with the Active Directory SPI

- Using Policies

Using Policies

The Microsoft Active Directory SPI policies monitor the Microsoft Active Directory environment and run according to rules and schedule specifications. Measurement threshold policies contain the rules for interpreting Microsoft Active Directory states or conditions.

Deploying Policies

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

Policy Group

A policy group organizes policies according to the deployment method and area to be targeted for discovery or monitoring. Deployment can be auto and manual.

- *SPI for Active Directory:* All Microsoft Active Directory SPI policy subgroups are grouped under **SPI for Active Directory** . 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 operating system SPI service discovery automatically discovers the Microsoft 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 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 or 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 is sent to the HPOM message browser.

Related Topics:

- Deploying Microsoft Active Directory Policies
- Policy Groups Catalog

Deploying Microsoft Active Directory SPI Policies

Automatic deployment of Microsoft Active Directory SPI policies can occur in the following ways:

- When you add unmanaged nodes to the HPOM nodes folder.
- When you distribute the Auto-Deploy policy group to nodes already managed by HPOM.

In both the preceding scenarios, you initiate a process where Microsoft Active Directory SPI policies monitoring specific services are automatically deployed on the nodes running those services. You can, however, deploy Microsoft Active Directory SPI policies manually as described in the following procedure.

> **NOTE:**
> Before deploying Active Directory SPI policies, refer to Chapter 2 of the *Smart Plug-in for Microsoft Active Directory Installation and Configuration Guide* . The document provides detailed information on installing the product.

To deploy the individual policies:

1. In the HPOM console, select **Policy management → Policy groups → SPI for Active Directory.**
2. Select the required policy group or individual policy**.**
3. In the details pane, right-click the policy to deploy, select **All Tasks → Deploy on.**
4. Select check boxes corresponding to managed and click **OK** .

Related Topics:

- Policy Groups Catalog
- Choosing Auto-Deploy Policy Group
- Choosing Manual-Deploy Policy Group

Policy Groups Catalog

The Microsoft Active Directory SPI groups policies at the highest level according to deployment as follows:

- *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 as follows, or follow the group links to individual policy descriptions:

Auto-Deploy Policies

Discovery : to discover all Microsoft Active Directory services.

DIT Monitoring : to monitor all Directory Information Tree services.

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

FSMO Monitoring : to monitor Flexible Single Master Operations services.

Replication Monitoring : to monitor replication latency.

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

Response Time Monitoring : to monitor Active Directory response times.

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

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

Manual-Deploy Policies

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

Connector Polices : Active Directory performance monitor counters.

Domain and OU Structure Policies : monitors domain and organizational unit (OU) changes.

Global Access Catalog Policies : monitors the performance monitor counters on Global Catalog servers.

Health Monitor Policies : monitors the health of DNS, Kerberos and NetLogon Services.

Index and Query Monitor Policies : monitors the performance monitor counters associated with LDAP and Kerberos.

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

Replication Activity Polices : monitors the Directory Service log for replication events.

Security Policies : monitors the following:

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

Site Structure Policies : monitors site changes.

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

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

Related Topics:

- Choosing Auto-Deploy Policy Group
- Choosing Manual-Deploy Policy Group

Choosing Auto-Deploy Policy Group

After you deploy the Auto-Deploy group, the service discovery process starts. Service discovery starts another automatic deployment of policies relevant to the detected services on a node:

Discovery Policies

- ADSPI_Discovery :

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

- ADSPI-AutoDiscovery Delete / ADSPI-AutoDiscovery Delete_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_DIT / ADSPI-AutoDiscovery_DIT_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_DNS / ADSPI-AutoDiscovery_DNS_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_FSMO / ADSPI-AutoDiscovery_FSMO_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_GC / ADSPI-AutoDiscovery_GC_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_PBHS / ADSPI-AutoDiscovery_PBHS_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_Rep / ADSPI-AutoDiscovery_Rep_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_RODC / ADSPI-AutoDiscovery_RODC_2k8+

SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-AutoDiscovery_Trust / ADSPI-AutoDiscovery_Trust_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Discovery → Advanced Discovery

- ADSPI-CreateDataSources

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

DIT

- ADSPI-DIT LogfilesQueueLength / ADSPI-DIT LogfilesQueueLength_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → DIT Monitoring

- ADSPI-DIT_DITQueueLength / ADSPI-DIT_DITQueueLength_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → DIT Monitoring

- ADSPI-DIT Total DIT Size / ADSPI-DIT Total DIT Size_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → DIT Monitoring

- ADSPI-DIT LogfilesPercent Full / ADSPI-DIT LogfilesPercent Full_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → DIT Monitoring

- ADSPI-DITPercent Full / ADSPI-DITPercent Full_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → DIT Monitoring

GC Monitoring Policies

- ADSPI-Rep_GC Check and Threshold / ADSPI-Rep_GC Check and Threshold_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → DIT Monitoring

Replication Monitoring Policies

- ADSPI-RepMonitorInterSiteReplication / ADSPI-RepMonitorInterSiteReplication_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-RepMonitorIntraSiteReplication / ADSPI-RepMonitorIntraSiteReplication_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_Delete_OvRep_Object / ADSPI-Rep_Delete_OvRep_Object_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_CheckObj / ADSPI-Rep_CheckObj_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_InboundObjs / ADSPI-Rep_InboundObjs_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_ISM_Chk / ADSPI-Rep_ISM_Chk_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_TimeSync / ADSPI-Rep_TimeSync_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_Modify_User_Object / ADSPI-Rep_Modify_User_Object_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

- ADSPI-Rep_ModifyObj / ADSPI-Rep_ModifyObj_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Replication Monitoring

FSMO Monitoring Policies

- ADSPI-FSMO_Consist / ADSPI-FSMO_Consist_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy →

FSMO Monitoring

- ADSPI-FSMO_GC-Infrastructure_Check / ADSPI-FSMO_GC-Infrastructure_Check_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_Consist_INFRA / ADSPI-FSMO_Consist_INFRA_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_Consist_NAMING / ADSPI-FSMO_Consist_NAMING_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_Consist_PDC / ADSPI-FSMO_Consist_PDC_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_Consist_RID / ADSPI-FSMO_Consist_RID_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_Consist_SCHEMA / ADSPI-FSMO_Consist_SCHEMA_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_NAMING_Bind / ADSPI-FSMO_NAMING_Bind_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_INFRA_Ping / ADSPI-FSMO_INFRA_Ping_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RID_Ping / ADSPI-FSMO_RID_Ping_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_PDC_Bind / ADSPI-FSMO_PDC_Bind_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_PDC_Ping / ADSPI-FSMO_PDC_Ping_2k8+

SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RID_Ping / ADSPI-FSMO_RID_Ping_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RoleMvmt_SCHEMA / ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_NAMING_Ping / ADSPI-FSMO_NAMING_Ping_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_Logging / ADSPI-FSMO_Logging_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_INFRA_Bind / ADSPI-FSMO_INFRA_Bind_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RID_Bind / ADSPI-FSMO_RID_Bind_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RoleMvmt_PDC / ADSPI-FSMO_RoleMvmt_PDC_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RoleMvmt_NAMING / ADSPI-FSMO_RoleMvmt_NAMING_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_RoleMvmt / ADSPI-FSMO_RoleMvmt_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_SCHEMA_Ping / ADSPI-FSMO_SCHEMA_Ping_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

- ADSPI-FSMO_SCHEMA_Bind / ADSPI-FSMO_SCHEMA_Bind_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Auto-Deploy → FSMO Monitoring

DNS Monitoring Policies

- ADSPI-DNS_GC_StrandedSite / ADSPI-DNS_GC_StrandedSite_2k8+

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

- ADSPI DNS_Extra_GC_SRV_Chk / ADSPI DNS_Extra_GC_SRV_Chk_2k8+

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

- ADSPI-DNS_Kerberos_SRV_Chk / ADSPI-DNS_Kerberos_SRV_Chk_2k8+

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

- ADSPI-DNS_Extra_Kerberos_SRV_Chk / ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+

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

- ADSPI-DNS_LDAP_SRV_Chk / ADSPI-DNS_LDAP_SRV_Chk_2k8+

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

- ADSPI DNS_Extra_LDAP_SRV_Chk / ADSPI DNS_Extra_LDAP_SRV_Chk_2k8+

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

- ADSPI-DNS_GC_A_Chk / ADSPI-DNS_GC_A_Chk_2k8+

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

- ADSPI DNS_DC_Response / ADSPI DNS_DC_Response_2k8+

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

- ADSPI-DNS_Island_Server / ADSPI-DNS_Island_Server_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → DNS

Monitoring

- ADSPI-DNS_LogDNSPagesSec / ADSPI-DNS_LogDNSPagesSec_2k8+

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

- ADSPI DNS_DC_CNAME_Chk / ADSPI DNS_DC_CNAME_Chk_2k8+

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

- ADSPI-DNS_GC_SRV_Chk / ADSPI-DNS_GC_SRV_Chk_2k8+

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

- ADSPI-DNS_Server_Response / ADSPI-DNS_Server_Response_2k8+

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

- ADSPI-DNS_Obsolete_GUIDS / ADSPI-DNS_Obsolete_GUIDS_2k8+

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

- ADSPI-DNS_DC_A_Chk / ADSPI-DNS_DC_A_Chk_2k8+

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

- ADSPI-DNS_GC_Missing / ADSPI-DNS_GC_Missing_2k8+

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

SysVol Monitoring Policies

- ADSPI-Sysvol_AD_Sync / ADSPI-Sysvol_AD_Sync_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Sysvol Monitoring

- ADSPI-Sysvol_Connectivity / ADSPI-Sysvol_Connectivity_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Auto-Deploy → Sysvol Monitoring

- ADSPI-Sysvol_FRS / ADSPI-Sysvol_FRS_2k8+

SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Sysvol Monitoring

- ADSPI-Sysvol_PercentFull / ADSPI-Sysvol_PercentFull_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Sysvol Monitoring

Response Time Monitoring

- ADSPI-Response Time Query / ADSPI-Response Time Query_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Response Time Monitoring

- ADSPI-Response Time GCQuery / ADSPI-Response Time GCQuery_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Response Time Monitoring

- ADSPI-Response Logging / ADSPI-Response Logging_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Response Time Monitoring

- ADSPI-Response Time Bind / ADSPI-Response Time Bind_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Response Time Monitoring

- ADSPI-Response Time GC Bind / ADSPI-Response Time GC Bind_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Response Time Monitoring

Trust Monitoring

- ADSPI-Trust_Mon_Add_Del / ADSPI-Trust_Mon_Add_Del_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Trust Monitoring

- ADSPI_Trust_Mon_Modify / ADSPI_Trust_Mon_Modify_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Auto-Deploy → Trust Monitoring

Related Topics:

- Policy Groups Catalog
- Choosing Manual_Deploy Policy Group

Choosing Manual-Deploy Policy Group

You can deploy Manual-Deploy polices to suit your Microsoft Active Directory requirements:

Auto Baseline Policies

- ADSPI-Rep_InboundObjects_AT / ADSPI-Rep_InboundObjects_AT_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008→ Manual-Deploy → Auto Basline Polices

- ADSPI-Rep_TimeSync_Monitor_AT / ADSPI-Rep_TimeSync_Monitor_AT_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Auto Baseline Polices

- ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT / ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Auto Baseline Policies

Connector Policies

- ADSPI_ActiveAuthKerberos / ADSPI_ActiveAuthKerberos_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Connector

- ADSPI_ActiveAuthLogon / ADSPI_ActiveAuthLogon_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008→ Manual-Deploy → Connector

- ADSPI_ActiveAuthNTLM / ADSPI_ActiveAuthNTLM_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Connector

- ADSPI_ADCFwdAllWarnErrorMSADC / ADSPI_ADCFwdAllWarnErrorMSADC_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Connector

- ADSPI_ADCImportFailures / ADSPI_ADCImportFailures_2k8+

SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Connector

- ADSPI_ADCPageFaults / ADSPI_ADCPageFaults_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Connector

- ADSPI_ADCPrivateBytes / ADSPI_ADCPrivateBytes_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Connector

- ADSPI_ADCProcessorTime / ADSPI_ADCProcessorTime_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Connector

- ADSPI_ADCWorkingSet / ADSPI_ADCWorkingSet_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Connector

Domain and OU Structure Policies

- ADSPI_DomainChanges / ADSPI_DomainChanges_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Domain and OU Structure

- ADSPI_OUChanges / ADSPI_OUChanges_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Domain and OU Structure

Global Catalog Access Policies

- ADSPI_GlobalCatalogWrites / ADSPI_GlobalCatalogWrites_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008→ Manual-Deploy → Global Catalog Access

- ADSPI_GlobalCatalogReads / ADSPI_GlobalCatalogReads_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008→ Manual-Deploy → Global Catalog Access

- ADSPI_GlobalCatalogSearches / ADSPI_GlobalCatalogSearches_2k8+

SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Global Catalog Access

Health Monitor Policies

- ADSPI_DNSServ_FwdAllInformation / ADSPI_DNSServ_FwdAllInformation_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_DNSServ_FwdAllWarnError / ADSPI_DNSServ_FwdAllWarnError_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_FwdAllInformationDS / ADSPI_FwdAllInformationDS_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_FwdAllInformationFRS / ADSPI_FwdAllInformationFRS_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_FwdAllWarnErrorDS / ADSPI_FwdAllWarnErrorDS_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_FwdAllWarnErrorFRS / ADSPI_FwdAllWarnErrorFRS_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMLSASSPageFaults / ADSPI_HMLSASSPageFaults_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMLSASSPrivateBytes / ADSPI_HMLSASSPrivateBytes_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMLSASSProcessorTime / ADSPI_HMLSASSProcessorTime_2k8+

  SPI for Microsoft Active Directory → en → Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMLSASSWorkingSet / ADSPI_HMLSASSWorkingSet_2k8+

SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMNTFRSPageFaults / ADSPI_HMNTFRSPageFaults_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMNTFRSPrivateBytes / ADSPI_HMNTFRSPrivateBytes_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMNTFRSProcessorTime / ADSPI_HMNTFRSProcessorTime_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMNTFRSWorkingSet / ADSPI_HMNTFRSWorkingSet_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_HMThreadsInUse / ADSPI_HMThreadsInUse_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_KDC / ADSPI_KDC_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_NetLogon / ADSPI_NetLogon_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_NTFRS / ADSPI_NTFRS_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_SamSs / ADSPI_SamSs_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_SMTPEventLogs / ADSPI_SMTPEventLogs_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_SyncSchemaMissMatch / ADSPI_SyncSchemaMissMatch_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_DFSR / ADSPI_DFSR_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

- ADSPI_NTDS / ADSPI_NTDS_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008 → Manual-Deploy → Health Monitors

Index and Query Monitoring Policies

- ADSPI_IQKerberosAuthentications / ADSPI_IQKerberosAuthentications_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

- ADSPI_IQLDAPActiveThreads / ADSPI_IQLDAPActiveThreads_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

- ADSPI_IQLDAPBindTime / ADSPI_IQLDAPBindTime_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

- ADSPI_IQLDAPClientSessions / ADSPI_IQLDAPClientSessions_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

- ADSPI_IQNTLMAuthentications / ADSPI_IQNTLMAuthentications_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

- ADSPI_DSSearches / ADSPI_DSSearches_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

- ADSPI_DSReads / ADSPI_DSReads_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy →

Index and Query Monitors

- ADSPI_DSWrites / ADSPI_DSWrites_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Index and Query Monitors

Replication Policies

- ADSPI_ADSPendingSynchronizations / ADSPI_ADSPendingSynchronizations_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Replication

- ADSPI_ADSRepInBoundBytesBetweenSites / ADSPI_ADSRepInBoundBytesBetweenSites_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Replication

- ADSPI_ADSRepInBoundBytesWithinSites / ADSPI_ADSRepInBoundBytesWithinSites_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Replication

- ADSPI_ADSRepInBoundObjectUpdatesRemaining / ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Replication

- ADSPI_ADSRepNotifyQueueSize / ADSPI_ADSRepNotifyQueueSize_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Replication

Replication Activity Policies

- ADSPI_ReplicationActivities / ADSPI_ReplicationActivities_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Replication Activities

Security Policies

- ADSPI_DirUserCreationDeletionModification / ADSPI_DirUserCreationDeletionModification_2k8+

SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_KDCFailureGrantTicket / ADSPI_KDCFailureGrantTicket_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_PrivilegedAccounts / ADSPI_PrivilegedAccounts_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecAdminGroupChangeMon / ADSPI_SecAdminGroupChangeMon_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecDirectoryServiceAccess / ADSPI_SecDirectoryServiceAccess_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecErrAccessPermissions / ADSPI_SecErrAccessPermissions_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecErrGrantedAccess / ADSPI_SecErrGrantedAccess_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecErrorsLogon / ADSPI_SecErrorsLogon_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecNonTransMembEval / ADSPI_SecNonTransMembEval_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecSDPropagatorQueue / ADSPI_SecSDPropagatorQueue_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_SecTransMembEval / ADSPI_SecTransMembEval_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

- ADSPI_DirComputerModif / ADSPI_DirComputerModif_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Security

Site Structure Policies

- ADSPI_SiteChanges / ADSPI_SiteChanges_2k8+

  SPI for Microsoft Active Directory → en →Windows Server 2003/2008→ Manual-Deploy → Site Structure

Related Topics:

- Policy Groups Catalog
- Choosing Auto-Deploy Policy Group

Auto-Deploy Policies

Auto-Deploy policies are divided into the following sub-groups. They are automatically deployed through service discovery.

- Discovery Policies
- DIT Monitoring Policies
- DNS Monitoring Policies
- FSMO Monitoring Policies
- Replication Monitoring Policies
- Response Time Monitoring Policies
- GC Monitoring Policies
- SysVol Monitoring Policies
- Trust Monitoring Policies

Related Topic:

- Choosing Auto-Deploy Policy Group

Discovery Policies

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

Service discovery policies for Windows Server 2003 and 2008 nodes are as follows:

- ADSPI-Discovery
- ADSPI-CreateDataSources

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

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

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI_Discovery

The ADSPI_Discovery policy performs the discovery of the Microsoft Active Directory from **System Infrastructure** through **Domain Controller → Services** . It uses *OvAdsDisc.exe* to discover all the Microsoft Active Directory components.

Policy Type: Service Auto Discovery policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003/Windows Server 2008 → Auto Deploy → Discovery**

Related Topics:

- Discovery Policies
- Choosing Auto-Deploy Policy Group

ADSPI-CreateDataSources

The ADSPI-CreateDataSources policy creates the required data sources in the data store (CODA or HP Performance Agent). Microsoft Active Directory SPI data sources need to be created in CODA for policies to log data.

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

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003/Windows Server 2008 → Auto Deploy → Discovery**

Related Topics:

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

DIT Monitoring Policies

The DIT Monitoring policies monitor the DIT services of the Microsoft Active Directory. The polices for Windows Server 2003 and 2008 nodes are as follows:

- ADSPI-DIT LogfilesQueue Length / ADSPI-DIT LogfilesQueue Length_2k8+
- ADSPI-DIT_DITPercent Full / ADSPI-DIT_DITPercent Full_2k8+
- ADSPI-DIT_DITQueue Length / ADSPI-DIT_DITQueue Length_2k8+
- ADSPI-DIT_TotalDIT Size / ADSPI-DIT_TotalDIT Size_2k8+
- ADSPI-DIT_LogfilesPercentFull / ADSPI-DIT_LogfilesPercentFull_2k8+

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI-DIT_LogfilesQueueLength

The ADSPI-DIT_LogfilesQueueLength policy measures the disk queue length on the DIT Log files drive. This policy also logs and measures thresholds on the data.

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 resides cannot handle the number of necessary updates.

Schedule: 5 minutes

Threshold: This policy has the following thresholds:

- Warning: Logfile queue length >=1
- Error: Logfile queue length >=2

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* The queue length (that is, 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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Adspi_Dit_LogfilesQueueLength_2k8

ADSPI-DIT_LogfilesQueueLength_2k8+

The ADSPI-DIT_LogfilesQueueLength_2k8+ policy measures the disk queue length on the DIT Log files drive. This policy also logs and measures thresholds on the data.

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 resides cannot handle the number of necessary updates.

Schedule: 5 minutes

Threshold: This policy has the following thresholds:

- Warning: Logfile queue length >=1
- Error: Logfile queue length >=2

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* The queue length (that is, 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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI- DIT_LogfilesQueueLength

ADSPI-DIT_DITQueueLength

The ADSPI-DIT_DITQueueLength policy monitors the queue length on the DIT disk drive.

This policy also logs and measures thresholds on the data. 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 cannot handle the amount of updates necessary.

Schedule: 5 minutes

Threhold: This policy has the following threshold:

- Warning: DITQueueLength>=1
- Critical: DITQueueLength>=2

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

Warning/Error Message Text: The start and end actions of this policy are:

- *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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_DITQueueLength_2k8+

ADSPI-DIT_DITQueueLength_2k8+

The ADSPI-DIT_DITQueueLength_2k8+ policy monitors the queue length on the DIT disk drive.

This policy also logs and measures thresholds on the data. 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 cannot handle the amount of updates necessary.

Schedule: 5 minutes

Threhold: This policy has the following threshold:

- Warning: DITQueueLength>=1
- Critical: DITQueueLength>=2

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

Warning/Error Message Text: The start and end actions of this policy are:

- *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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_DITQueueLength

ADSPI-DIT_TotalDITSize

The ADSPI-DIT_TotalDITSize policy monitors the total amount of free space on the DIT disk drive in MB. The Microsoft Active Directory database file or DIT can cause problems when it expands over the time and this is not watched.

Schedule: 24 hours

Threshold: This policy has the following 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: The start and end actions of this policy are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_TotalDITSize_2k8+

ADSPI-DIT_TotalDITSize_2k8+

The ADSPI-DIT_TotalDITSize_2k8+ policy monitors the total amount of free space on the DIT disk drive in MB. The Active Directory database file or DIT can cause problems when it expands over time and this is not watched.

Interval: 24 hours

Threshold: This policy has the following 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: The start and end actions of this policy are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_TotalDITSize

ADSPI-DIT_LogfilesPercentFull

The ADSPI-DIT_LogfilesPercentFull 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.

Schedule: 24 hours

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

Warning/Error Message Text: The start and end actions of this policy are:

- *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)>%.

Policy Type: Measurement Threshold policy

P olicy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_LogfilesPercentFull_2k8+

ADSPI-DIT_LogfilesPercentFull_2k8+

The ADSPI-DIT_LogfilesPercentFull_2k8+ 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.

Schedule: 24 hours

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

Warning/Error Message Text: The start and end actions of this policy are:

- *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)>%.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_LogfilesPercentFull

ADSPI-DIT_DITPercentFull

The ADSPI-DIT_DITPercentFull policy monitors the percentage used space on the disk drive holding the AD database (DIT).

This policy helps to 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.

Schedule: 24 hours

Threshold: This policy has the following thresholds:

- Warning: Percentage disk full=80%
- Critical: Percentage disk full=90%

Warning/Error Message Text: The start and end actions of this policy are:

- *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)>%.

Policy Type: Measurement Threshold policy

P olicy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_DITPercentFull_2k8+

ADSPI-DIT_DITPercentFull_2k8+

The ADSPI-DIT_DITPercentFull_2k8+ policy monitors the percentage used space on the disk drive holding the AD database (DIT).

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.

Schedule: 24 hours

Threshold: This policy has the following thresholds:

- Warning: Percentage disk full=80%
- Critical: Percentage disk full=90%

Warning/Error Message Text: The start and end actions of this policy are:

- *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)>%.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DIT**

Related Topics:

- DIT Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DIT_DITPercentFull

DNS Monitoring Policies

The DNS Monitoring policies monitor the DNS services of Microsoft Active Directory. The polices for Windows Server 2003 and 2008 are as follows:

- ADSPI- DNS_DC_A_Chk / ADSPI- DNS_DC_A_Chk_2k8+
- ADSPI-DNS_DC_CNAME_Chk / ADSPI-DNS_DC_CNAME_Chk_2k8+
- ADSPI-DNS_DC_Response / ADSPI-DNS_DC_Response_2k8+
- ADSPI-DNS_Extra_GC_SRV_Chk / ADSPI-DNS_Extra_GC_SRV_Chk_2k8+
- ADSPI-DNS_Extra_Kerberos_SRV_Chk / ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+
- ADSPI-DNS_Extra_LDAP_SRV_Chk / ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+
- ADSPI-DNS_GC_A_Chk / ADSPI-DNS_GC_A_Chk_2k8+
- ADSPI-DNS_GC_StrandedSite / ADSPI-DNS_GC_StrandedSite_2k8+
- ADSPI-DNS_GC_SRV_Chk / ADSPI-DNS_GC_SRV_Chk_2k8+
- ADSPI-DNS_Kerberos_SRV_Chk / ADSPI-DNS_Kerberos_SRV_Chk_2k8+
- ADSPI-DNS_Island_Server / ADSPI-DNS_Island_Server_2k8+
- ADSPI-DNS_LDAP_SRV_Chk / ADSPI-DNS_LDAP_SRV_Chk_2k8+
- ADSPI-DNS_Obsolete_GUIDS / ADSPI-DNS_Obsolete_GUIDS_2k8+
- ADSPI-DNS_LogDNSPageSec / ADSPI-DNS_LogDNSPageSec_2k8+
- ADSPI-DNS_Server_Response / ADSPI-DNS_Server_Response_2k8+

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI-DNS_DC_A_Chk

The ADSPI-DNS_DC_A_Chk policy checks the DNS host records (A records) associated with a DC. There are two host records associated with each DC:

- For its fully qualified domain name
- For the domain that it serves

This policy generates a *critical message* if one or both records are missing.

This policy ensures that DNS contains the expected DNS host resource records for the LDAP service by checking for expected DNS A resource records.

Schedule: 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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)>
  <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_DC_A_Chk_2k8+

ADSPI-DNS_DC_A_Chk_2k8+

The ADSPI-DNS_DC_A_Chk_2k8+ policy checks the DNS host records (A records) associated with a DC. There are two host records associated with each DC: one for its fully qualified domain name, and another for the domain that it serves. This policy generates a *critical message* if one or both records are missing.

This policy ensures that DNS contains the expected DNS host resource records for the LDAP service by checking for expected DNS A resource records.

Schedule: 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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 on 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)>
  <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies

- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_DC_A_Chk

ADSPI-DNS_DC_CName_Chk

The ADSPI-DNS_DC_CName_Chk policy verifies that the DC can be located through use of its alias. This policy achieves this by verifying the DC's GUID alias, using:
< *Domain_Controller GUID* >._msdcs.<*Domain* >.

This policy checks for expected DNS CNAME resource records for the LDAP service.

Schedule: 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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
  The domain controller has been configured to use the following DNS servers:
  <$OPTION(DnsServers)>
  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>
  <$SESSION(RegRecordsFlag)>
  <$SESSION(ServerPing)><$OPTION(FailingServers)>
  <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-DNS_DC_CName_Chk_2k8+

ADSPI-DNS_DC_CName_Chk_2k8+

The ADSPI-DNS_DC_CName_Chk_2k8+ policy verifies that the DC can be located through use of its alias. This policy achieves this by verifying the DC's GUID alias, using:
< *Domain_Controller GUID* >._msdcs.<*Domain* >.

This policy checks for expected DNS CNAME resource records for the LDAP service.

Schedule: 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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
  The domain controller has been configured to use the following DNS servers:
  <$OPTION(DnsServers)>
  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>
  <$SESSION(RegRecordsFlag)>
  <$SESSION(ServerPing)><$OPTION(FailingServers)>
  <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI_DNS_DC_CName_Chk

ADSPI-DNS_DC_Response

The ADSPI-DNS_DC_Response policy alerts the user when DNS queries made by the DC 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.

This policy monitors the response time of DNS queries made by the DC in milliseconds. Reports are based on whether DNS response is too long (Rule 1) or does not occur (Rule 2). This policy also logs information for reporting. Reports can be found in **Reports → SPI for Active Directory** .

Schedule: 30 minutes

Threshold: This policy has the following threshold:

- Warning Level: ResponseTime >= 1000 (Rule 1 applies)
- Critical Level: ResponseTime >= 2000 (Rule 1 applies)
- Critical Level: Response Time = 0 (Rule 2 applies)

Warning/Error Message Text: The warning/error message text for this policy is:

- The start and end actions for Rule #1 (for slow response) are:
  - *Start Actions* (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 Actions:* Domain controller <$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.
- Start Action and end actions for Rule #2 (for no response) are:
  - *Start Actions:* 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 Actions:* Domain controller <$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_DNS_DC_Response_2k8+

ADSPI-DNS_DC_Response_2k8+

The ADSPI-DNS_DC_Response_2k8+ policy alerts the user when DNS queries made by the DC 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.

This policy monitors the response time of DNS queries made by the DC in milliseconds. Reports are based on whether DNS response is too long (Rule 1) or does not occur (Rule 2). This policy also logs information for reporting. Reports can be found in Reports→ SPI for Active Directory.

Schedule: 30 minutes

Threshold: This policy has the following threshold:

- Warning Level: ResponseTime >= 1000 (Rule 1 applies)
- Critical Level: ResponseTime >= 2000 (Rule 1 applies)
- Critical Level: Response Time = 0 (Rule 2 applies)

Warning/Error Message Text: The warning/error message text for this policy is:

- The start and end actions for Rule #1 (for slow response) are:
  - *Start Actions* (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 Actions:* Domain controller <$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.
- Start Action and end actions for Rule #2 (for no response) are:
  - *Start Actions:* 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 Actions:* Domain controller <$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_DNS_DC_Response

ADSPI-DNS_Extra_GC_SRV_Chk

The ADSPI-DNS_Extra_GC_SRV_Chk policy checks for extra DNS SRV resource records registered for the global catalog.

Schedule: This policy runs every 24 hours.

Threshold: This policy has the following 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.

Warning/Error Message Text: The warning/error message text for this policy is:

- The start and end actions for Rule #1 are:
  - *Start Actions* : 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: <$OPTION(DnsServers)>
  - *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a global catalog for sites that it does not reside on.
- Start Action and end actions for Rule #2 are:
  - *Start Actions:* 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 Actions:* Domain controller <$MSG_NODE_NAME> is no longer mis-registered as a global catalog in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI_DNS_Extra_GC_SRV_Chk_2k8+

ADSPI-DNS_Extra_GC_SRV_Chk_2k8+

The ADSPI-DNS_Extra_GC_SRV_Chk_2k8+ policy checks for extra DNS SRV resource records registered for the global catalog.

Schedule: This policy runs every 24 hours.

Threshold: This policy has the following 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.

Warning/Error Message Text: The warning/error message text for this policy is:

- The start and end actions for Rule #1 are:
  - *Start Actions* : 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: <$OPTION(DnsServers)>
  - *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a global catalog for sites that it does not reside on.
- Start Action and end actions for Rule #2 are:
  - *Start Actions:* 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 Actions:* Domain controller <$MSG_NODE_NAME> is no longer mis-registered as a global catalog in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI_DNS_Extra_GC_SRV_Chk

ADSPI-DNS_Extra_Kerberos_SRV_Chk

The ADSPI-DNS_Extra_Kerberos_SRV_Chk policy checks for records that register the DC as a Kerberos KDC on multiple sites.

Schedule: This policy runs every 24 hours.

Threshold: Warning Level: >= 1

Result: This policy generates a *warning message* if the DC 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 preferred under certain circumstances.

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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:
  <$OPTION(DnsServers)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a Kerberos server for sites that it does not reside on.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_DNS_Extra_Kerberos_SRV_Chk_2k8+

ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+

The ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+ policy checks for records that register the DC as a Kerberos KDC on multiple sites.

Schedule: This policy runs every 24 hours.

Threshold: Warning Level: >= 1

Result: This policy generates a *warning message* if the DC 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 preferred under certain circumstances.

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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: <$OPTION(DnsServers)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a Kerberos server for sites that it does not reside on.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Extra_Kerberos_SRV_Chk

ADSPI-DNS_Extra_LDAP_SRV_Chk

The ADSPI-DNS_Extra_LDAP_SRV_Chk policy checks for records that register a DC as an LDAP server on multiple sites.

Schedule: This policy runs every 24 hours.

Threshold: Warning Level: >= 1

Result: This policy generates a warning message if the DC 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 preferred situation under certain circumstances.

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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:
  <$OPTION(DnsServers)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a domain controller for sites that it does not reside on.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+

ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+

The ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+ policy checks for records that register a DC as an LDAP server on multiple sites.

Schedule: This policy runs every 24 hours

Threshold: Warning Level: >= 1

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 preferred situation under certain circumstances.

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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:
  <$OPTION(DnsServers)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer registered in DNS as a domain controller for sites that it does not reside on.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Extra_LDAP_SRV_Chk

ADSPI-DNS_GC_A_Chk

The ADSPI-DNS_GC_A_Chk policy checks DNS for a DC hosting global catalog services by detecting for the DNS host record (A record) associated with a DC that hosts the global catalog.

This policy ensures that the DNS contains the expected DNS A resource records for the global catalog.

Schedule: This policy runs every 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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)>
  <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-DNS_GC_A_Chk_2k8+

ADSPI-DNS_GC_A_Chk_2k8+

The ADSPI-DNS_GC_A_Chk_2k8+ policy checks DNS for a DC hosting global catalog services by detecting for the DNS host record (A record) associated with a DC that hosts the global catalog.

This policy ensures that the DNS contains the expected DNS A resource records for the global catalog.

Schedule: This policy runs every 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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)>
  <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-DNS_GC_A_Chk

ADSPI-DNS_GC_SRV_CHK

The ADSPI-DNS_GC_SRV_CHK policy ensures that DNS contains the expected DNS SRV resource records for the global catalog.

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

This policy generates a *critical message* when a 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 the Microsoft Active Directory environment without having to modify their management software.

Schedule: This policy runs every 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”

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_GC_SRV_CHK_2k8+

ADSPI-DNS_GC_SRV_CHK_2k8+

The ADSPI-DNS_GC_SRV_CHK_2k8+ policy ensures that DNS contains the expected DNS SRV resource records for the global catalog.

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

This policy generates a *critical message* when a 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 Microsoft Active Directory environment without having to modify their management software.

Schedule: This policy runs every 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”

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_GC_SRV_CHK

ADSPI-DNS_GC_StrandedSite

The ADSPI-DNS_GC_StrandedSite policy checks for the existence of a global catalog on every site within the forest in which the Domain Naming Master resides.

Without access to the forest's Global Catalog, a Microsoft Active Directory environment becomes unusable. This policy generates a *warning message* when a Microsoft 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 DCs, it runs only on a forest’s Domain Naming Master. This minimizes monitoring time.

Schedule: This policy runs every 24 hours.

Threshold: This policy has the following thresholds:

- *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.

Result: This policy has the following results:

- 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.
- When necessary, the policy also generates a critical message alerting the user that the Active Directory forest has no Global Catalog registered in DNS.

Warning/Error Message Text: The warning level and minor level texts are as follows:

- *Warning Level Text:* The start and end actions is as follows:
  - *Start Actions:* 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 Actions:* Site <$INSTANCE> of forest <$OPTION(forest)> now has a local global catalog.

- *Minor Level Text:* The start and end actions is as follows:
  - *Start Actions:* 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: <$OPTION(DnsServers)>
  - *End Actions:* Site <$INSTANCE> of forest <$OPTION(forest)> now has a global catalog SRV record registered in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_GC_StrandedSite_28k+

ADSPI-DNS_GC_StrandedSite_2k8+

The ADSPI-DNS_GC_StrandedSite_2k8+ policy checks for the existence of a global catalog on every site within the forest in which the Domain Naming Master resides.

Without access to the forest's Global Catalog, a Microsoft Active Directory environment becomes unusable. This policy generates a *warning message* when a Microsoft 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 DCs, it runs only on a forest's Domain Naming Master. This minimizes monitoring time.

Schedule: This policy runs every 24 hours.

Threshold: This policy has the following thresholds:

- *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.

Result: This policy has the following results:

- 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.
- When necessary, the policy also generates a critical message alerting the user that the Active Directory forest has no Global Catalog registered in DNS.

Warning/Error Message Text: The warning level and minor level texts are as follows:

- *Warning Level Text:* The start and end actions is as follows:
  - *Start Actions:* 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 Actions:* Site <$INSTANCE> of forest <$OPTION(forest)> now has a local global catalog.

- *Minor Level Text:* The start and end actions is as follows:
  - *Start Actions:* 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: <$OPTION(DnsServers)>
  - *End Actions:* Site <$INSTANCE> of forest <$OPTION(forest)> now has a global catalog SRV record registered in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_GC_StrandedSite

ADSPI-DNS_Island_Server

The ADSPI-DNS_Island_Server policy generates a *warning message* if a DC has been configured to use itself as a DNS server. This arises replication problems. When such problems occur, the DC or DNS server is referred to as an 'island' .

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

Schedule: This policy runs every 24 hours.

Threshold: Warning Level: >=1 (Domain Controller uses itself as a DNS server.)

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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 Actions:* Domain Controller <$MSG_NODE_NAME> is no longer configured to use itself as a DNS server.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Island_Server_2k8+

ADSPI-DNS_Island_Server_2k8+

The ADSPI-DNS_Island_Server_2k8+ policy generates a warning message if a DC has been configured to use itself as a DNS server. This arises replication problems. When such problems occur, the DC\DNS server is referred to as an 'island'.

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

Schedule: This policy runs every 24 hours.

Threshold: Warning Level: >=1 (Domain Controller uses itself as a DNS server.)

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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 Actions:* Domain Controller <$MSG_NODE_NAME> is no longer configured to use itself as a DNS server.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Island_Server

ADSPI-DNS_LogDNSPagesSec

The ADSPI-DNS_LogDNSPagesSec policy records pages per second that can be used to create capacity planning graphs.

Schedule: This policy runs every 5 minutes.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_LogDNSPagesSec_2k8+

ADSPI-DNS_LogDNSPagesSec_2k8+

The ADSPI-DNS_LogDNSPagesSec_2k8+ policy records pages per second that can be used to create capacity planning graphs.

Schedule: This policy runs every 5 minutes.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_LogDNSPagesSec

ADSPI-DNS_Kerberos_SRV_Chk

The ADSPI-DNS_Kerberos_SRV_Chk policy ensures that DNS contains the expected DNS Kerberos SRV resource records for the LDAP service. This 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.

The Microsoft Active Directory DCs 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. This policy checks for extra DNS SRV resource records registered for the Kerberos service. This policy generates a critical message if the DC is registered as a Kerberos KDC on a site in which it does not reside.

Schedule: This policy runs every 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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. The domain controller has been configured to use the following DNS servers:
  - <$OPTION(DnsServers)>
  - <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>
  - <$SESSION(RegRecordsFlag)>
  - <$SESSION(ServerPing)><$OPTION(FailingServers)>
  - <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy →**

DNS

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Kerberos_SRV_Chk_2k8+

ADSPI-DNS_Kerberos_SRV_Chk_2k8+

The ADSPI-DNS_Kerberos_SRV_Chk_2k8+ policy ensures that DNS contains the expected DNS Kerberos SRV resource records for the LDAP service. This 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.

The Microsoft Active Directory DCs 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. This policy checks for extra DNS SRV resource records registered for the Kerberos service. This policy generates a critical message if the DC is registered as a Kerberos KDC on a site in which it does not reside.

Schedule: This policy runs every 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”

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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. The domain controller has been configured to use the following DNS servers:
  - <$OPTION(DnsServers)>
  - <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>
  - <$SESSION(RegRecordsFlag)>
  - <$SESSION(ServerPing)><$OPTION(FailingServers)>
  - <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy →**

DNS

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Kerberos_SRV_Chk

ADSPI-DNS_LDAP_SRV_Chk

The ADSPI-DNS_LDAP_SRV_Chk policy ensures that DNS contains the expected DNS LDAP SRV resource records for the LDAP service.

The Microsoft 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 DCs that host LDAP, Kerberos, and Global Catalog services. This policy generates a *critical message* when a DC 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.

Schedule: This policy runs every 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”

Result: This policy generates a critical message when a DC 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.

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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
  The domain controller has been configured to use the following DNS servers:
  - <$OPTION(DnsServers)>
  - <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>
  - <$SESSION(RegRecordsFlag)>
  - <$SESSION(ServerPing)><$OPTION(FailingServers)>
  - <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_LDAP_SRV_Chk_2k8+

ADSPI-DNS_LDAP_SRV_Chk_2k8+

The ADSPI-DNS_LDAP_SRV_Chk_2k8+ policy ensures that DNS contains the expected DNS LDAP SRV resource records for the LDAP service.

The Microsoft 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 DCs that host LDAP, Kerberos, and Global Catalog services. This policy generates a *critical message* when a DC 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.

Schedule: This policy runs every 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”

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.

Warning/Error Message Text: The start and end actions of this policy are:

- *Start Actions:* 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
  The domain controller has been configured to use the following DNS servers:
  - <$OPTION(DnsServers)>
  - <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>
  - <$SESSION(RegRecordsFlag)>
  - <$SESSION(ServerPing)><$OPTION(FailingServers)>
  - <$SESSION(NoForest)>
- *End Actions:* Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_LDAP_SRV_Chk

ADSPI-DNS_Server_Response

The ADSPI-DNS_Server_Response 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 Microsoft Active Directory.

Result: When a threshold is exceeded, this policy generates a message/alert to the HP Operations message browser/service map. The policy also logs data for reports.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Server_Response_2k8+

ADSPI-DNS_Server_Response_2k8+

The ADSPI-DNS_Server_Response_2k8+ 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 Microsoft Active Directory.

Result: When a threshold is exceeded, this policy generates a message/alert to the HP Operations message browser/service map. The policy also logs data for reports.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- Descriptions of Policy Groups and Types
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Server_Response

ADSPI-DNS_Obsolete_GUIDs

The ADSPI-DNS_Obsolete_GUIDs policy checks for hosts that are registered under obsolete GUIDs in the forest in which the domain controller resides. This policy also alerts you to situations where no data is available.

Each DC 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.

Schedule: This policy runs every 24 hours.

Threshold: This policy has the following threshold:

- *Error Level:* Threshold limit >= 1 (maximum number obsolete GUIDs)
- *Warning Level:* Threshold limit = -1 (Unable to get Zone Transfer)

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.

Message Text: The following is message text:

- *Error Message Text:* The start and end actions are:
  - *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:* The start and end actions are:
  - *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Obsolete_GUIDs_2k8+

ADSPI-DNS_Obsolete_GUIDs_2k8+

The ADSPI-DNS_Obsolete_GUIDs_2k8+ policy checks for hosts that are registered under obsolete GUIDs in the forest in which the domain controller resides. This policy also alerts you to situations where no data is available.

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. his 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.

Schedule: This policy runs every 24 hours.

Threshold: This policy has the following threshold:

- *Error Level:* Threshold limit >= 1 (maximum number obsolete GUIDs)
- *Warning Level:* Threshold limit = -1 (Unable to get Zone Transfer)

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.

Message Text: The following is message text:

- *Error Message Text:* The start and end actions are:
  - *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:* The start and end actions are:
  - *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → DNS**

Related Topics:

- DNS Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-DNS_Obsolete_GUIDs

FSMO Monitoring Policies

The FSMO monitoring policies are used to monitor flexible single masters operations (FSMO) services. 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 polices for Windows Server 2003 and 2008 are as follows:

- ADSPI-FSMO_Logging / ADSPI-FSMO_Logging_2k8+
- ADSPI-FSMO_NAMING_Ping / ADSPI-FSMO_NAMING_Ping_2k8+
- ADSPI-FSMO_NAMING_Bind / ADSPI-FSMO_NAMING_Bind_2k8+
- ADSPI-FSMO_INFRA_Ping / ADSPI-FSMO_INFRA_Ping_2k8+
- ADSPI-FSMO_INFRA_Bind / ADSPI-FSMO_INFRA_Bind_2k8+
- ADSPI-FSMO_PDC_Ping / ADSPI-FSMO_PDC_Ping_2k8+
- ADSPI-FSMO_PDC_Bind / ADSPI-FSMO_PDC_Bind_2k8+
- ADSPI-FSMO_RID_Ping / ADSPI-FSMO_RID_Ping_2k8+
- ADSPI-FSMO_RID_Bind / ADSPI-FSMO_RID_Bind_2k8+
- ADSPI-FSMO_SCHEMA_Ping / ADSPI-FSMO_SCHEMA_Ping_2k8+
- ADSPI-FSMO_SCHEMA_Bind / ADSPI-FSMO_SCHEMA_Bind_2k8+
- ADSPI-FSMO_GC-Infrastructure_Check / ADSPI-FSMO_GC-Infrastructure_Check_2k8+
- ADSPI-FSMO Consist / ADSPI-FSMO Consist_2k8+
- ADSPI-FSMO_Consist_INFRA / ADSPI-FSMO_Consist_INFRA_2k8+
- ADSPI-FSMO_Consist_NAMING / ADSPI-FSMO_Consist_NAMING_2k8+
- ADSPI-FSMO_Consist_PDC / ADSPI-FSMO_Consist_PDC_2k8+
- ADSPI-FSMO_Consist_RID / ADSPI-FSMO_Consist_RID_2k8+
- ADSPI-FSMO_Consist_SCHEMA / ADSPI-FSMO_Consist_SCHEMA_2k8+
- ADSPI-FSMO_RoleMvmt / ADSPI-FSMO_RoleMvmt_2k8+
- ADSPI-FSMO_RoleMvmt_INFRA / ADSPI-FSMO_RoleMvmt_INFRA_2k8+
- ADSPI-FSMO_RoleMvmt_NAMING / ADSPI-FSMO_RoleMvmt_NAMING_2k8+
- ADSPI-FSMO_RoleMvmt_PDC / ADSPI-FSMO_RoleMvmt_PDC_2k8+
- ADSPI-FSMO_RoleMvmt_RID / ADSPI-FSMO_RoleMvmt_RID_2k8+

- ADSPI-FSMO_RoleMvmt_SCHEMA / ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI-FSMO_INFRA_Bind

The ADSPI-FSMO_INFRA_Bind policy measures the response time length in seconds for the INFRA master. For this purpose, this policy periodically binds to the DC that is the INFRA master.

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.

Threshold: This policy has the following threshold:

- Warning: 1
- Error: 2

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_INFRA_Bind_2k8+

ADSPI-FSMO_INFRA_Bind_2k8+

The ADSPI-FSMO_INFRA_Bind_2k8+ policy measures the response time length in seconds for the INFRA master. For this purpose, this policy periodically binds to the domain controller that is the INFRA master.

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.

Threshold: This policy has the following threshold:

- Warning: 1
- Error: 2

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_INFRA_Bind

ADSPI-FSMO_INFRA_Ping

The ADSPI-FSMO_INFRA_Ping policy 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.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Schedule: This policy runs every 24 hours.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_INFRA_Ping_2k8+

ADSPI-FSMO_INFRA_Ping_2k8+

The ADSPI-FSMO_INFRA_Ping_2k8+ policy 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.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Schedule: This policy runs every 24 hours.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_INFRA_Ping

ADSPI-FSMO_GC_Infrastructure_Check

The ADSPI-FSMO_GC_Infrastructure_Check policy checks if a DC with the Infrastructure Master role serves as a global catalog server. If the DC with the Infrastructure Master role is found to be a global catalog server, this policy sends appropriate alert messages to the HPOM console.

Schedule: This policy runs every 24 hours.

Policy type: Measurement Threshold policy

Policy group: **SPI for Microsoft Active Directory → en → Windows Server 2003 → Auto-Deploy → FSMO Monitoring**

Related Topics:

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

ADSPI-FSMO_GC_Infrastructure_Check_2k8+

The ADSPI-FSMO_GC_Infrastructure_Check_2k8+ policy checks if a DC with the Infrastructure Master role serves as a GC server. If a DC with the Infrastructure Master role is found to be a GC server, this policy helps the SPI to send appropriate alert messages to the HPOM console.

Schedule: This policy runs every 24 hours.

Policy type: Measurement Threshold policy

Policy group: **SPI for Microsoft Active Directory → en → Windows Server 2008 → Auto-Deploy → FSMO Monitoring**

Related Topics:

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

ADSPI-FSMO_Logging

The ADSPI-FSMO_Logging policy 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.

Schedule: This policy runs every 5 minutes.

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_Logging_2k8+

ADSPI-FSMO_Logging_2k8+

The ADSPI-FSMO_Logging_2k8+ policy 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.

Schedule: This policy runs for 5 minutes

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Group Policy Catalog
- ADSPI-FSMO_Logging

ADSPI-FSMO_NAMING_Bind

The ADSPI-FSMO_NAMING_Bind policy measures the response time length in seconds for the domain-naming master. For this purpose, this policy periodically binds to the domain controller that is the domain-naming master.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_NAMING_Bind_2k8+

ADSPI-FSMO_NAMING_Bind_2k8+

The ADSPI-FSMO_NAMING_Bind_2k8+ policy measures the response time length in seconds for the domain-naming master. For this purpose, this policy periodically binds to the domain controller that is the domain-naming master.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_NAMING_Bind

ADSPI-FSMO_NAMING_Ping

The ADSPI-FSMO_NAMING_Ping policy 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.

This policy works 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.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_NAMING_Ping_2k8+

ADSPI-FSMO_NAMING_Ping_2k8+

The ADSPI-FSMO_NAMING_Ping_2k8+ policy 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.

This policy works 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.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_NAMING_Ping

ADSPI-FSMO_PDC_Bind

The ADSPI-FSMO_PDC_Bind policy 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.

The PDC master is a Windows domain controller that acts as the primary domain controller to down-level workstations, member servers and domain controllers.

In a Windows 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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-FSMO_PDC_Bind_2k8+

ADSPI-FSMO_PDC_Bind_2k8+

The ADSPI-FSMO_PDC_Bind_2k8+ policy 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.

The PDC master is a Windows domain controller that acts as the primary domain controller to down-level workstations, member servers and domain controllers.

In a Windows 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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-FSMO_PDC_Bind

ADSPI-FSMO_RID_Bind

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

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 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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

ADSPI-FSMO_RID_Bind_2k8+

The ADSPI-FSMO_RID_Bind_2k8+ policy 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. This policy works in conjunction with the ADSPI-FSMO_Logging policy.

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 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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RID_Bind

ADSPI-FSMO_RID_Ping

The ADSPI-FSMO_RID_Ping policy 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. This policy works in conjunction with ADSPI-FSMO_Logging policy.

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).

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RID_Ping_2k8+

ADSPI-FSMO_RID_Ping_2k8+

The ADSPI-FSMO_RID_Ping_2k8+ policy 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. This policy works in conjunction with ADSPI-FSMO_Logging policy.

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).

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RID_Ping

ADSPI-FSMO_RoleMvmt

The ADSPI-FSMO_RoleMvmt policy determines when a FSMO role is seized or transferred from one domain controller to another.

This 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_2k8+
- ADSPI-FSMO_RoleMvmt_NAMING_2k8+
- ADSPI-FSMO_RoleMvmt_PDC_2k8+
- ADSPI-FSMO_RoleMvmt_RID_2k8+
- ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

These five policies then, as changes occur, send tailored messages back to the management server.

Schedule: This policy runs every hour

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_2k8+

ADSPI-FSMO_RoleMvmt_2k8+

The ADSPI-FSMO_RoleMvmt_2k8+ policy determines when a FSMO role is seized or transferred from one domain controller to another.

This 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_2k8+
- ADSPI-FSMO_RoleMvmt_NAMING_2k8+
- ADSPI-FSMO_RoleMvmt_PDC_2k8+
- ADSPI-FSMO_RoleMvmt_RID_2k8+
- ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

These five policies then, as changes occur, send tailored messages back to the management server.

Schedule: This policy runs every hour

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt

ADSPI-FSMO_RoleMvmt_INFRA

The ADSPI-FSMO_RoleMvmt_INFRA policy monitors the domain controller's ownership of the Infrastructure Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the Infrastructure Master FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the Infrastructure Master FSMO role for domain <$OPTION(domain)>.
    This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_INFRA_2k8+

ADSPI-FSMO_RoleMvmt_INFRA_2k8+

The ADSPI-FSMO_RoleMvmt_INFRA_2k8+ policy monitors the domain controller's ownership of the Infrastructure Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the Infrastructure Master FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the Infrastructure Master FSMO role for domain <$OPTION(domain)>.
    This role is now owned by <$OPTION(holder)>.

  Policy Type: Measurement Threshold policy

  Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

  Related Topics:

  - FSMO Monitoring Policies
  - Choosing Auto-Deploy Policy Group
  - ADSPI-FSMO_RoleMvmt_INFRA

ADSPI-FSMO_RoleMvmt_NAMING

The ADSPI-FSMO_RoleMvmt_NAMING policy monitors the domain controller's ownership of the Domain Naming Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the Domain Naming Master FSMO role forest <$OPTION(forest)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the Domain Naming Master FSMO role forest <$OPTION(forest)>. This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_NAMING_2k8+

ADSPI-FSMO_RoleMvmt_NAMING_2k8+

The ADSPI-FSMO_RoleMvmt_NAMING_2k8+ policy monitors the domain controller's ownership of the Domain Naming Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the Domain Naming Master FSMO role forest <$OPTION(forest)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the Domain Naming Master FSMO role forest <$OPTION(forest)>. This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_NAMING

ADSPI-FSMO_RoleMvmt_PDC

The ADSPI-FSMO_RoleMvmt_PDC policy monitors the domain controller's ownership of the PDC Emulator FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The start actions for Rule 1 is:

- Domain Controller Acquired FSMO Role Ownership
  - *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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_PDC_2k8+

ADSPI-FSMO_RoleMvmt_PDC_2k8+

The ADSPI-FSMO_RoleMvmt_PDC_2k8+ policy monitors the domain controller's ownership of the PDC Emulator FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The start actions for Rule 1 is:

- Domain Controller Acquired FSMO Role Ownership
  - *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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_PDC

ADSPI-FSMO_RoleMvmt_RID

The ADSPI-FSMO_RoleMvmt_RID policy monitors the domain controller's ownership of the RID Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the RID Master FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the RID Master FSMO role for domain <$OPTION(domain)>. This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_RID_2k8

ADSPI-FSMO_RoleMvmt_RID_2k8+

The ADSPI-FSMO_RoleMvmt_RID_2k8+ policy monitors the domain controller's ownership of the RID Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the RID Master FSMO role for domain <$OPTION(domain)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the RID Master FSMO role for domain <$OPTION(domain)>. This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_RID

ADSPI-FSMO_RoleMvmt_SCHEMA

The ADSPI-FSMO_RoleMvmt_SCHEMA policy monitors the domain controller's ownership of the Schema Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the Schema Master FSMO role forest <$OPTION(forest)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the Schema Master FSMO role forest <$OPTION(forest)>. This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+

The ADSPI-FSMO_RoleMvmt_SCHEMA_2k8+ policy monitors the domain controller's ownership of the Schema Master FSMO role.

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.

Threshold: Change in FSMO role assigned to domain controller.

Message Text: The message text for Rule 1 and Rule 2 are:

- *Rule 1:* Domain Controller Acquired FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> has acquired the Schema Master FSMO role forest <$OPTION(forest)>. This role was formerly owned by <$OPTION(holder)>.
- *Rule 2:* Domain Controller Lost FSMO Role Ownership
  - *Start Actions:* Domain controller <$MSG_NODE_NAME> no longer owns the Schema Master FSMO role forest <$OPTION(forest)>. This role is now owned by <$OPTION(holder)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_RoleMvmt_SCHEMA

ADSPI-FSMO_SCHEMA_Bind

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

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_SCHEMA_Bind_2k8+

ADSPI-FSMO_SCHEMA_Bind_2k8+

The ADSPI-FSMO_SCHEMA_Bind_2k8+ policy 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. This policy works in conjunction with the ADSPI-FSMO_Logging policy.

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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_SCHEMA_Bind

ADSPI-FSMO_SCHEMA_Ping

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

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_SCHEMA_Ping_2k8+

ADSPI-FSMO_SCHEMA_Ping_2k8+

The ADSPI-FSMO_SCHEMA_Ping_2k8+ policy 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. This policy works in conjunction with the ADSPI-FSMO_Logging policy. This 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.

Threshold: This policy has the following threshold:

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_SCHEMA_Ping

ADSPI-FSMO_Consist

The ADSPI-FSMO_Consist policy 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.

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.

Schedule: This policy runs every 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)

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_Consist_2k8+

ADSPI-FSMO_Consist_2k8+

The ADSPI-FSMO_Consist_2k8+ policy is 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.

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.

Schedule: This policy runs every 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)

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_Consist

ADSPI-FSMO_Consist_INFRA

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.

This 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.

Consistency State: The consistency state is as follows:

- 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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_Consist_INFRA_2k8+

ADSPI-FSMO_Consist_INFRA_2k8+

The ADSPI-FSMO_Consist_INFRA_2k8+ 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.

This 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.

Consistency State: The consistency state is as follows:

- 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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-FSMO_Consist_INFRA

ADSPI-FSMO_Consist_NAMING

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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

ADSPI-FSMO_Consist_NAMING_2k8+

The ADSPI-FSMO_Consist_NAMING_2k8+ 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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

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 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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

ADSPI-FSMO_Consist_PDC_2k8+

The ADSPI-FSMO_Consist_PDC_2k8+ 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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

ADSPI-FSMO_PDC_Ping

The ADSPI-FSMO_PDC_Ping policy 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. 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.

The PDC master is a Windows domain controller that acts as the primary domain controller to down-level workstations, member servers and domain controllers. In a Windows 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.

Threshold: This policy has the following threshold

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-FSMO_PDC_Ping_2k8+

ADSPI-FSMO_PDC_Ping_2k8+

The ADSPI-FSMO_PDC_Ping_2k8+ policy 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. 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.

The PDC master is a Windows domain controller that acts as the primary domain controller to down-level workstations, member servers and domain controllers. In a Windows 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.

Threshold: This policy has the following threshold

- Warning: 1 second
- Error: 2 seconds

Message Text: The start and end actions are:

- *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)>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group

- ADSPI-FSMO_PDC_Ping

ADSPI-FSMO_Consist_RID

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. 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.

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.

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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

ADSPI-FSMO_Consist_RID_2k8+

The ADSPI-FSMO_Consist_RID_2k8+ 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. 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.

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.

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: The start and end actions are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto Deploy → FSMO Monitoring**

Related Topics:

- FSMO Monitoring Policies
- Choosing Auto-Deploy Policy Group
- Discovery Policies

Replication Monitoring Policies

The Replication Monitoring polices monitor replication latency through the Microsoft Active Directory forest.. The policies for Windows Server 2003 and 2008 are as follows:

- ADSPI-Rep_Delete_OvRep_Object / ADSPI-Rep_Delete_OvRep_Object_2k8+
- ADSPI-Rep_InboundObjs / ADSPI-Rep_InboundObjs_2k8+
- ADSPI-Rep_OutboundObjs / ADSPI-Rep_OutboundObjs_2k8+
- ADSPI-Rep_CheckObj / ADSPI-Rep_CheckObj_2k8+
- ADSPI-REP_ModifyObj / ADSPI-REP_ModifyObj_2k8+
- ADSPI-Rep_Modify_User_Object / ADSPI-Rep_Modify_User_Object_2k8+
- ADSPI-Rep_MonitorIntraSiteReplication / ADSPI-Rep_MonitorIntraSiteReplication_2k8+
- ADSPI-Rep_MonitorInterSiteReplication / ADSPI-Rep_MonitorInterSiteReplication_2k8+
- ADSPI-Rep_ISM_Chk / ADSPI-Rep_ISM_Chk_2k8+
- ADSPI-Rep_TimeSync / ADSPI-Rep_TimeSync_2k8+

***** These scheduled task policies provide the required data for other replication-checking policies, *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.

Prerequisite Supporting Policies

Ensure to deploy the following supporting policies on all DCs where replication has to be monitored:

- ADSPI-REP_ModifyObj / ADSPI-REP_ModifyObj_2k8+
- ADSPI-Rep_Modify_User_Object / ADSPI-Rep_Modify_User_Object_2k8+
- ADSPI-Rep_Delete_OvRep_Object / ADSPI-Rep_Delete_OvRep_Object_2k8+
- ADSPI-Rep_CheckObj / ADSPI-Rep_CheckObj_2k8+

Replication Monitoring Executable

The ADSPI_RepMonI.exe has the logic for replication monitoring.

Replication Monitoring Scenarios

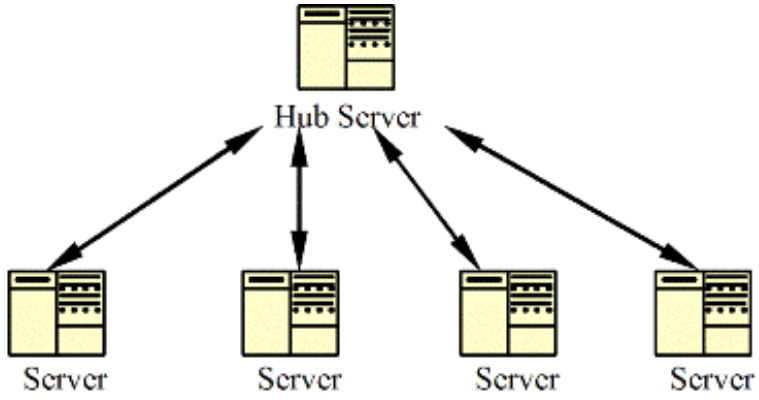
The replication monitoring scenarios are as follows:

- *Intra-Site Replication Monitoring:* The policy ADSPI-Rep_MonitorIntraSiteReplication / ADSPI-Rep_MonitorIntraSiteReplication_2k8+ monitors Intra-Site Replication. It checks whether replication is occuring between the DCs having connection objects in the same site.
- *Inter-Site Replication Monitoring:* The policy ADSPI-Rep_MonitorInterSiteReplication / ADSPI-Rep_MonitorInterSiteReplication_2k8+ monitors inter-site replication. Bridge-Servers are responsible for replication between sites. This policy checks whether replication is happening between the bridge-head servers of sites.
- A number of Microsoft Active Directory replication topologies are supported.

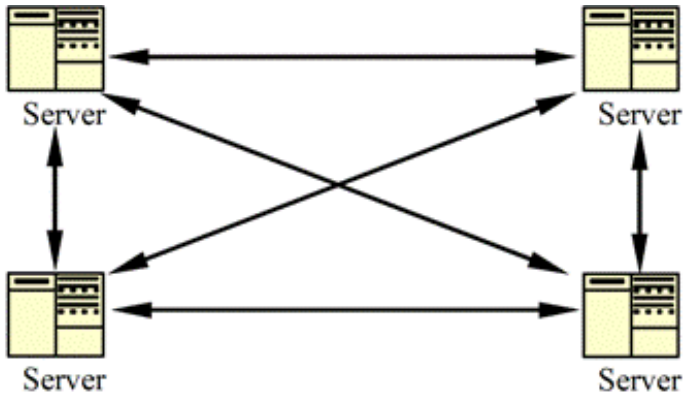
Microsoft Active Directory Replication Topologies

Microsoft Active Directory SPI can monitor the following Active Directory replication topologies.

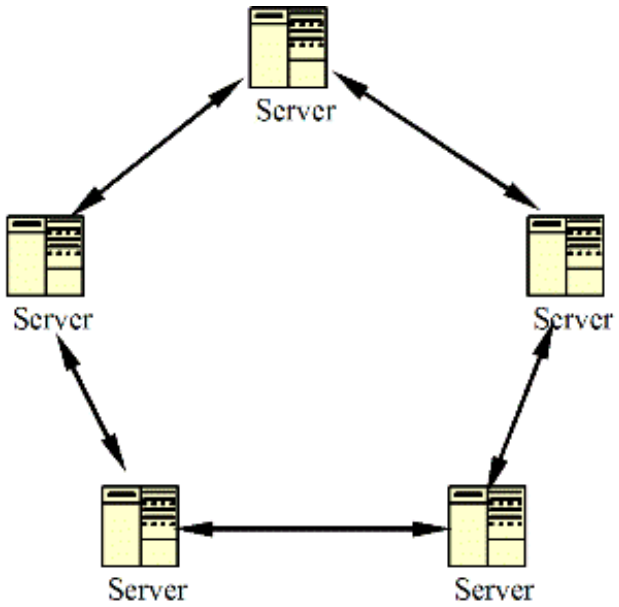
Hub and Spoke Topology Replication Monitoring



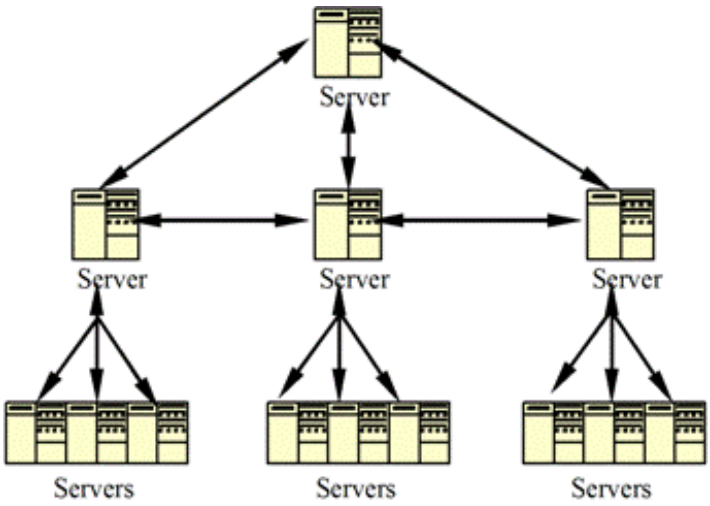
Full Mesh Topology Replication



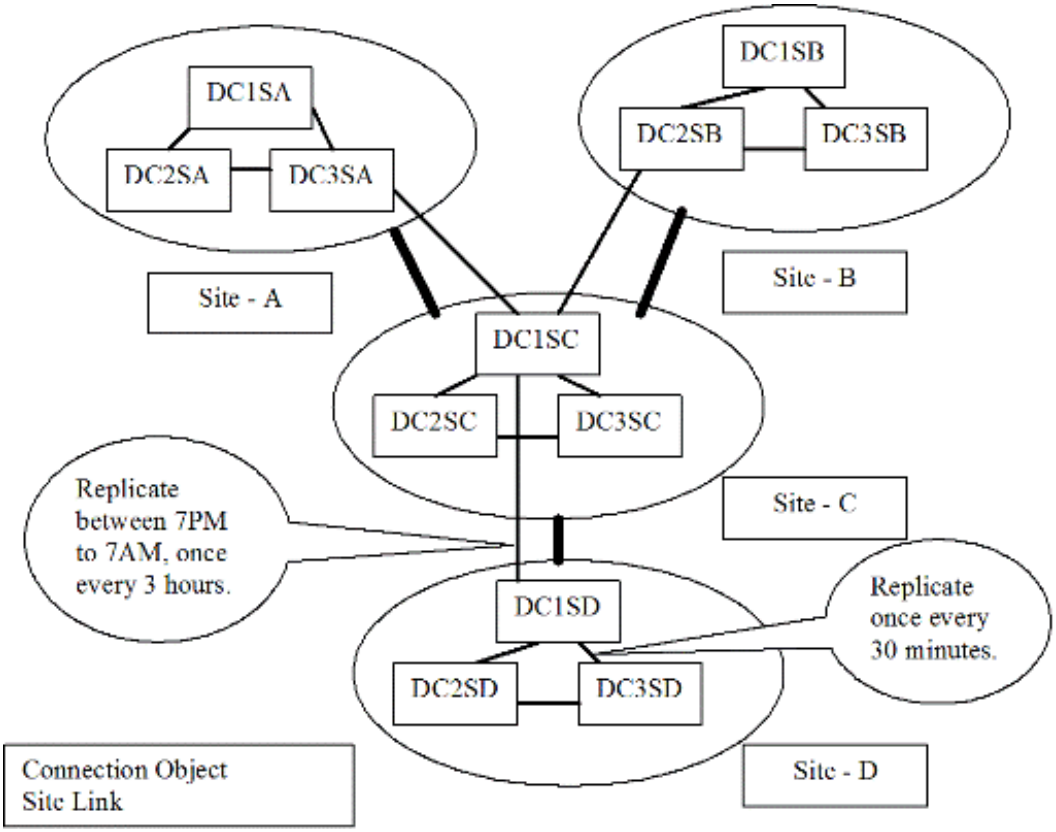
Ring Topology Replication Monitoring



Multi-tier Redundant Hub and Spoke Topology Replication Monitoring



Configuring the Replication Monitoring policies



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

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group

ADSPI-Rep_CheckObj

The ADSPI-Rep_CheckObj policy identifies DCs that do not contain the replication object and issue an alert when found. This 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.

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)

Schedule: This policy runs every 24 hours

Message Text: The start and end actions are:

- *Start Actions:* An HPOM replication object doesn't exist for domain controller(s) <$SESSION(DC)>!
- *End Actions:* None

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_CheckObj_2k8+

ADSPI-Rep_CheckObj_2k8+

The ADSPI-Rep_CheckObj_2k8+ policy identifies DCs that do not contain the replication object and issue an alert when found. This 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.

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)

Schedule: This policy runs every 24 hours

Message Text: The start and end actions are:

- *Start Actions:* An HPOM replication object doesn't exist for domain controller(s) <$SESSION(DC)>!
- *End Actions:* None

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_CheckObj

ADSPI-Rep_Delete_OvRep_Object

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.

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.

Threshold: This policy has the following threshold:

- Warning Threshold: 24 hours
- Critical Threshold: 48 hours

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_Delete_OvRep_Object_2k8+

ADSPI-Rep_Delete_OvRep_Object_2k8+

The ADSPI-Rep_Delete_OvRep_Object_2k8+ 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.

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.

Threshold: This policy has the following threshold:

- Warning Threshold: 24 hours
- Critical Threshold: 48 hours

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_Delete_OvRep_Object

ADSPI-Rep_InboundObjs

The ADSPI-Rep_InboundObjs policy measures the DRA inbound object/sec counter and monitors the number of inbound replication objects. This policy monitors the number of inbound replication objects.

Schedule: This policy runs every 5 minutes

Text Message: The start and end actions are:

- *Start Actions:* The number of inbound replication objects on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> objects. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)> objects.
- *End Actions:* The number of inbound replication objects on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)> objects.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_InboundObjs_2k8+

ADSPI-Rep_InboundObjs_2k8+

The ADSPI-Rep_InboundObjs_2k8+ policy measures the DRA inbound object/sec counter and monitors the number of inbound replication objects. This policy monitors the number of inbound replication objects.

Schedule: This policy runs every 5 minutes

Text Message: The start and end actions are:

- *Start Actions:* The number of inbound replication objects on domain controller <$MSG_NODE_NAME> is <$SESSION(value)> objects. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)> objects.
- *End Actions:* The number of inbound replication objects on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)> objects.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_InboundObjs

ADSPI-Rep_OutboundObjs

The ADSPI-Rep_OutboundObjs policy monitors the number of Outbound replication objects.

Schedule: This policy runs every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 →Auto-Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- SPI-Rep_ModifyObj_2k8+

ADSPI-Rep_OutboundObjs_2k8+

The ADSPI-Rep_OutboundObjs_2k8+ policy monitors the number of Outbound replication objects.

Schedule: This policy runs every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 →Auto-Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- SPI-Rep_ModifyObj_2k8+

ADSPI-Rep_MonitorInterSiteReplication

ADSPI-Rep_MonitorInterSiteReplication policy monitors whether replication occurs between the bridge-head servers of sites.

Schedule: This policy runs every 4 hours.

Threshold: The threshold values of this policy is as follows:

- *Critical Threshold:* 14 hours
- *Warning Threshold:* 13 hours

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto-Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_MonitorInterSiteReplication

ADSPI-Rep_MonitorInterSiteReplication_2k8+

ADSPI-Rep_MonitorInterSiteReplication_2k8+ policy monitors whether replication occurs between the bridge-head servers of sites.

Schedule: This policy runs every 4 hours.

Threshold: The threshold values of this policy is as follows:

- *Critical Threshold:* 14 hours
- *Warning Threshold:* 13 hours

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto-Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_MonitorIntraSiteReplication_2k8+

ADSPI-Rep_MonitorIntraSiteReplication

ADSPI-Rep_MonitorIntraSiteReplication policy monitors whether replication occurs between the DCs with connection objects in the same site.

Schedule: This policy runs every hour.

Threshold: The threshold value of this policy is as follows:

- *Critical Threshold:* 2 hours
- *Warning Threshold:* 1 hour

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto-Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_MonitorIntraSiteReplication_2k8+

ADSPI-Rep_MonitorIntraSiteReplication_2k8+

The ADSPI-Rep_MonitorIntraSiteReplication_2k8+ policy monitors whether replication is happening between the DCs with connection objects in the same site.

Schedule: This policy runs every hour.

Threshold: The threshold value of this policy is as follows:

- *Critical Threshold:* 2 hours
- *Warning Threshold:* 1 hour

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto-Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_MonitorIntraSiteReplication_2k8+

ADSPI-Rep_ISM_Chk

The ADSPI-Rep_ISM_Chk policy checks the intersite messaging service (ISM). 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 cannot calculate the replication topology.

Schedule: This policy runs every 12 minutes

Message Text: The start and end actions are:

- *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: '\" & 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 the corresponding process '\" _
  & Session(\"ProcessName\") & \"' is not running.\"
  Else
  Session(\"MSG\") = Left (Session(\"MSG\"), Len(Session(\"MSG\"))-1) & \" and the corresponding process '\" _
  & Session(\"ProcessName\") & \"' is running less than \" & Session(\"nProcesses\") & \" times.\"
  End If
  Policy.MsgSeverity = \"Critical\"
  End If

```
    Rule.Status = True
  End If
```

- *End Actions:* None

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_ISM_Chk_2k8+

ADSPI-Rep_ISM_Chk_2k8+

The ADSPI-Rep_ISM_Chk_2k8+ policy checks the intersite messaging service (ISM). 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.

Schedule: This policy runs every 12 minutes

Message Text: The start and end actions are:

- *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: '\" & 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 the corresponding process '\" _
         & Session(\"ProcessName\") & \"' is not running.\"
      Else
         Session(\"MSG\") = Left (Session(\"MSG\"), Len(Session(\"MSG\"))-1) & \" and the corresponding process '\" _
         & Session(\"ProcessName\") & \"' is running less than \" & Session(\"nProcesses\") & \" times.\"
      End If
      Policy.MsgSeverity = \"Critical\"
```

```
    End If
    Rule.Status = True
  End If
```

- *End Actions:* None

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_ISM_Chk

ADSPI-Rep_Modify_User_Object

The ADSPI-Rep_Modify_User_Object policy 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, this policy monitors the replication times of global catalog inter-site, and intra-site replication latency. This scheduled task policy creates and updates a user object on the DC hosting the policy. This policy is deployed to all managed DCs.

This 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.

Schedule: This policy runs every 15 minutes

Text Message: The start and end actions are:

- *Start Actions:* <$MSG_TEXT> (Command and User)
- *End Actions:* None

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_Modify_User_Object_2k8+

ADSPI-Rep_Modify_User_Object_2k8+

The ADSPI-Rep_Modify_User_Object_2k8+ policy 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, this policy monitors the replication times of global catalog inter-site, and intra-site replication latency. This scheduled task policy creates and updates a user object on the DC hosting the policy. This policy is deployed to all managed DCs.

This 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.

Schedule: This policy runs every 15 minutes

Text Message: The start and end actions are:

- *Start Actions:* <$MSG_TEXT> (Command and User)
- *End Actions:* None

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_Modify_User_Object

ADSPI-Rep_ModifyObj

The ADSPI-Rep_ModifyObj policy monitors the number of inbound replication objects. This policy creates and updates an object on the DC 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 ADSPI-Rep_MonitorInterSiteReplication policy: Verifies timely replication between DC replication partners.
- The ADSPI-Rep_MonitorIntraSiteReplication policy: Verifies the object's existence on the DC's replication partners. If the object is missing the policy generates a message.

Message Text: The start and end actions are:

- *Start Actions:* <$MSG_TEXT> (Command and User)
- *End Actions:* None

Schedule: This policy runs every 30 minutes

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 →Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- SPI-Rep_ModifyObj_2k8+

ADSPI-Rep_ModifyObj_2k8+

The ADSPI-Rep_ModifyObj_2k8+ policy monitors the number of inbound replication objects. This policy creates and updates an object on the DC hosting the policy.

This policy is deployed to all managed DCs as a means for checking replication as measured by the following policies:

- The ADSPI-Rep_MonitorInterSiteReplication policy: Verifies timely replication between DC replication partners.
- The ADSPI-Rep_MonitorIntraSiteReplication policy: Verifies the object's existence on the DC's replication partners. If the object is missing the policy generates a message.

Message Text: The start and end actions are:

- *Start Actions:* <$MSG_TEXT> (Command and User)
- *End Actions:* None

Schedule: This policy runs every 30 minutes

Policy Type: Scheduled Task policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_ModifyObj

ADSPI-Rep_TimeSync

The ADSPI-Rep_TimeSync policy validates time synchronization with time master in seconds. Windows Server operating system uses a time service, known as Windows Time Synchronization Service (Win32Time), to ensure that all Windows Servers on a network use a common time. This service is required and therefore crucial to Windows default authentication processes (which uses Kerberos protocol).

This 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.

Schedule: This policy runs every 5 minutes

Message Text: The start and end actions are:

- *Start Actions:* 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 $SESSION(CriticalThreshold)>sec.
- *End Actions:* The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_TimeSync_2k8+

ADSPI-Rep_TimeSync_2k8+

The ADSPI-Rep_TimeSync_2k8+ policy validates time synchronization with time master in seconds. Windows Server operating system uses a time service, known as Windows Time Synchronization Service (Win32Time), to ensure that all Windows Servers on a network use a common time. This service is required and therefore crucial to Windows default authentication processes (which uses Kerberos protocol).

This 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.

Schedule: This policy runs every 5 minutes

Message Text: The start and end actions are:

- *Start Actions:* 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 $SESSION(CriticalThreshold)>sec.
- *End Actions:* The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → Replication Monitoring**

Related Topics:

- Replication Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_TimeSync

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).

The polices for Windows Server 2003 and 2008 are as follows:

- ADSPI-GC_CheckStatus / ADSPI-GC_CheckStatus_2k8+
- ADSPI-Rep_GC_Check_and_Threshold / ADSPI-Rep_GC_Check_and_Threshold_2k8+

The ADSPI-Rep_Modify_User_Object / ADSPI-Rep_Modify_User_Object_2k8+ (in Replication Monitoring group) scheduled task policies are necessary for *ADSI-Rep_GC_Check_and_Threshold* (for Windows Server 2003 and 2008) to work.

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI-GC_CheckStatus

The ADSPI-GC_CheckStatus policy checks the GC Query Status in Active Directory.

Schedule: This policy runs every 1 hour.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto-Deploy → GC Monitoring**

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_2k8+

ADSPI-GC_CheckStatus_2k8+

The ADSPI-GC_CheckStatus_2k8+ policy checks the GC Query Status in Active Directory.

Schedule: This policy runs every 1 hour.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto-Deploy → GC Monitoring**

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_2k8+

ADSPI-Rep_GC_Check_and_Threshold

The ADSPI-Rep_GC_Check_and_Threshold policy calculates, stores, and sends messages/alerts when threshold hours for global catalog replication latency are exceeded. 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.

This 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.

Schedule: This policy runs every 15 minutes

Threshold: This policy has 24 hours as its threshold

Message Text: The start and end actions are:

- *Start Actions:* The global catalog server <$MSG_NODE_NAME> has not replicated from the domain controller(s) <$SESSION(DC)> for at least <$SESSION(THRESHOLD)> hours.
- *End Actions:* The replication latency between global catalog server <$MSG_NODE_NAME> and the domain controller(s) <$SESSION(DC)> no longer exceeds the critical threshold value of <$SESSION(THRESHOLD)> hours.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → GC Monitoring**

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_2k8+

ADSPI-Rep_GC_Check_and_Threshold_2k8+

The ADSPI-Rep_GC_Check_and_Threshold_2k8+ policy calculates, stores, and sends messages/alerts when threshold hours for global catalog replication latency are exceeded. 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.

This 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.

Schedule: This policy runs every 15 minutes

Threshold: This policy has 24 hours as its threshold

Message Text: The start and end actions are:

- *Start Actions:* The global catalog server <$MSG_NODE_NAME> has not replicated from the domain controller(s) <$SESSION(DC)> for at least <$SESSION(THRESHOLD)> hours.
- *End Actions:* The replication latency between global catalog server <$MSG_NODE_NAME> and the domain controller(s) <$SESSION(DC)> no longer exceeds the critical threshold value of <$SESSION(THRESHOLD)> hours.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Auto Deploy → GC Monitoring**

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold

Response Time Monitoring Policies

The Response Time Monitoring polices monitor the Microsoft Active Directory response times for purposes of checking the general responsiveness of Microsoft Active Directory. The polices for Windows Server 2003 and 2008 are as follows:

- ADSPI-LDAP_CheckStatus / ADSPI-LDAP_CheckStatus_2k8+
- ADSPI-ResponseTime_GCQuery / ADSPI-ResponseTime_GCQuery_2k8+
- ADSPI-Response_Logging / ADSPI-Response_Logging_2k8+
- ADSPI-ResponseTime_Bind / ADSPI-ResponseTime_Bind_2k8+
- ADSPI-ResponseTime_GCBind / ADSPI-ResponseTime_GCBind_2k8+
- ADSPI-ResponseTime_Query / ADSPI-ResponseTime_Query_2k8+

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI-LDAP_CheckStatus

The ADSPI-LDAP_CheckStatus policy checks the LDAP Query Status in Active Directory.

Schedule: This policy runs every 1 hour.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 → Auto-Deploy → Response Time Monitoring**

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_2k8+

ADSPI-LDAP_CheckStatus_2k8+

The ADSPI-LDAP_CheckStatus_2k8+ policy checks the LDAP Query Status in Active Directory.

Schedule: This policy runs every 1 hour.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Auto-Deploy → Response Time Monitoring**

Related Topics:

- GC Monitoring policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_2k8+

ADSPI-ResponseTime_Bind

The ADSPI-ResponseTime_Bind policy monitors bind response time in seconds of the Microsoft 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.

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 might 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.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: The start and end actions are:

- 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-ResponseTime_Bind_2k8+

ADSPI-ResponseTime_Bind_2k8+

The ADSPI-ResponseTime_Bind_2k8+ policy 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.

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 might 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.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: The start and end actions are:

- 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- AADSPI-ResponseTime_Bind

ADSPI-ResponseTime_GCBind

The ADSPI-ResponseTime_GCBind policy monitors GC bind response time in seconds of Microsoft Active Directory.

This policy measures the time required for the DC 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 DCs can serve as global catalog servers.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: The start and end actions are:

- 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-ResponseTime_GCBind_2k8+

ADSPI-ResponseTime_GCBind_2k8+

The ADSPI-ResponseTime_GCBind_2k8+ policy monitors GC bind response time in seconds of Microsoft Active Directory.

This policy measures the time required for the DC 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 DCs can serve as global catalog servers.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: The start and end actions are:

- 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Choosing Auto-Deploy Policy Group

ADSPI-Response Time_GCQuery

The ADSPI-Response Time_GCQuery policy monitors bind response time in seconds of Microsoft Active Directory global catalog queries 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 DCs can serve as global catalog servers.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: Tne start and end actions are:

- Warning 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Response Time_GCQuery_2k8+

ADSPI-Response Time_GCQuery_2k8+

The ADSPI-Response Time_GCQuery_2k8+ policy monitors bind response time in seconds of Microsoft Active Directory global catalog queries 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 DCs can serve as global catalog servers.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: Tne start and end actions are:

- Warning 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-ResponseTime_GCQuery

ADSPI-Response_Logging

The ADSPI-Response_Logging scheduled task policy logs Microsoft 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.

Schedule: This policy runs every 5 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Response_Logging_2k8+

ADSPI-Response_Logging_2k8+

The ADSPI-Response_Logging_2k8+ scheduled task policy logs Microsoft 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.

Schedule: This policy runs every 5 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Response_Logging

ADSPI-ResponseTime_Query

The ADSPI-ResponseTime_Query policy measures the general responsiveness of Microsoft Active Directory in seconds.

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 might have gone down and queries are being directed to another DC over a WAN link, or a DC is running hot. The data is also logged for graphing.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: The start and end actions are:

- 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-ResponseTime_Query_2k8+

ADSPI-ResponseTime_Query_2k8+

The ADSPI-ResponseTime_Query_2k8+ policy measures the general responsiveness of Microsoft Active Directory in seconds.

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. The data is also logged for graphing.

Threshold: This policy has the following threshold:

- Warning Level: >1 second
- Critical Level: >2 seconds

Message Text: The start and end actions are:

- 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).

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Response Time Monitoring**

Related Topics:

- Response Time Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-ResponseTime_Query

Sysvol Monitoring Policies

The SysVol Monitoring policies monitor connectivity, space use, and replication as related to SysVol. The polices for Windows Server 2003 and 2008 are as follows:

- ADSPI-Sysvol_AD_Sync / ADSPI-Sysvol_AD_Sync_2k8+
- ADSPI-Sysvol_Connectivity / ADSPI-Sysvol_Connectivity_2k8+
- ADSPI-Sysvol_FRS / ADSPI-Sysvol_FRS_2k8+
- ADSPI-Sysvol_PercentFull / ADSPI-Sysvol_PercentFull_2k8+
- ADSPI-Sysvol_DiskQueueLength / ADSPI-Sysvol_DiskQueueLength_2k8+

Related Topics:

- Trust Monitoring Policies
- Choosing Auto-Deploy Policy Group

ADSPI-Sysvol_Connectivity

The ADSPI-Sysvol_Connectivity policy connects to each replication partner's SYSVOL to validate connectivity. The ability to connect to the SysVol volume is a key indicator of the health of the Microsoft 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.

Schedule: This policy runs every 2 hours.

Threshold: This policy has the following threshold:
Error Level: Sysvol connection does not exist

Message Text: The warning and error message text for the start action and the end action are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-SysVol_PercentFull_2k8+

ADSPI-Sysvol_Connectivity_2k8+

The ADSPI-Sysvol_Connectivity_2k8+ policy connects to each replication partner's SYSVOL to validate connectivity. The ability to connect to the SysVol volume is a key indicator of the health of the Microsoft 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.

Schedule: This policy runs every 2 hours.

Threshold: This policy has the following threshold:
Error Level: Sysvol connection does not exist

Message Text: The warning and error message text for the start action and the end action are:

- *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>.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-SysVol_PercentFull_2k8+

ADSPI-Sysvol_FRS

The ADSPI-Sysvol_FRS policy checks the file replication service (FRS) event log for error or warning events.

Threshold: This policy has the following thresholds:

- Rule 1: Major
- Rule 2: Information, Warning, Error

Message Text: There is no start and end actions.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Sysvol_FRS

ADSPI-Sysvol_FRS_2k8+

The ADSPI-Sysvol_FRS_2k8+ policy checks the File Replication Service (FRS) event log for error or warning events.

Threshold: This policy has the following thresholds:

- Rule 1: Major
- Rule 2: Information, Warning, Error

Message Text: There is no start and end actions.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Sysvol_FRS

ADSPI-Sysvol_AD_Sync

The ADSPI-Sysvol_AD_Sync policy checks that the Group Policy Objects (GPO) in the Microsoft Active Directory and SysVol are in synch.

Schedule: This policy runs every 24 hours

Threshold: This policy has the following threshold:

- Critical >=2
- Warning >=1

  Policy Type: Measurement Threshold policy

  Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Sysvol Monitoring**

  Related Topics:

  - Sysvol Monitoring Policies
  - Choosing Auto-Deploy Policy Group
  - ADSPI-Sysvol_AD_Sync_2k8+

ADSPI-Sysvol_AD_Sync_2k8+

The ADSPI-Sysvol_AD_Sync_2k8+ policy checks that the Group Policy Objects (GPO) in the Microsoft Active Directory and SysVol are in synch.

Schedule: This policy runs every 24 hours

Threshold: This policy has the following threshold:

- Critical >=2
- Warning >=1

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-Sysvol_AD_Sync

ADSPI-SysVol_PercentFull

The ADSPI-SysVol_PercentFull policy monitors the amount of free space on the Sysvol disk drive in terms of percentage used. The size of the SysVol is a key indicator of the health of the Microsoft 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.

Threshold: This policy has the following thresholds:

- Warning Level: Disk full = 80 %
- Critical Level: Disk ful = 90 %

Message Text: The start and end actions are:

- *Start Actions:* The Sysvol disk drive on <$MSG_NODE_NAME> is <$SESSION(PercentFull)>% full. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>%.
- *End Actions:* The percentage full on the Sysvol disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-SysVol_PercentFull_2k8+

ADSPI-SysVol_PercentFull_2k8+

The ADSPI-SysVol_PercentFull_2k8+ policy monitors the amount of free space on the SysVol disk drive in terms of percentage used. The size of the SysVol is a key indicator of the health of the Microsoft 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.

Threshold: This policy has the following thresholds:

- Warning Level: Disk full = 80 %
- Critical Level: Disk ful = 90 %

Message Text: The start and end actions are:

- *Start Actions:* The Sysvol disk drive on <$MSG_NODE_NAME> is <$SESSION(PercentFull)>% full. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>%.
- *End Actions:* The percentage full on the Sysvol disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-SysVol_PercentFull_2k8+

ADSPI-Sysvol_DiskQueueLength

The ADSPI-Sysvol_DiskQueueLength policy monitors the queue length on the DIT log files disk drive.

Schedule: This policy runs every 5 minutes.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-SysVol_PercentFull_2k8+

ADSPI-Sysvol_DiskQueueLength_2k8+

The ADSPI-Sysvol_DiskQueueLength_2k8+ policy monitors the queue length on the DIT log files disk drive.

Schedule: This policy runs every 5 minutes.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Auto Deploy → Sysvol Monitoring**

Related Topics:

- Sysvol Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI-SysVol_PercentFull_2k8+

Trust Monitoring Policies

The Trust Monitoring polices create the trust report and monitor trust relationship changes between DCs. The polices for Windows Server 2003 and 2008 are as follows:

- ADSPI-Trust_Mon_Add_Del / ADSPI-Trust_Mon_Add_Del_2k8+
- ADSPI_Trust_Mon_Modify / ADSPI_Trust_Mon_Modify_2k8+

Related Topics:

- Discovery Policies
- Choosing Auto-Deploy Policy Group

ADSPI_Trust_Mon_Modify

The ADSPI_Trust_Mon_Modify policy monitors any modification of trusts in the Microsoft Active Directory forest.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → Auto-Deploy → Windows Server 2003 → Trust Monitoring**

Related Topics:

- Trust Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_Trust_Mon_Add_Del_2k8+

ADSPI_Trust_Mon_Modify_2k8+

The ADSPI_Trust_Mon_Modify_2k8+ policy monitors any modification of trusts in the Microsoft Active Directory forest.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → Auto-Deploy → Windows Server 2008 → Trust Monitoring**

Related Topics:

- Trust Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_Trust_Mon_Add_Del_2k8+

ADSPI_Trust_Mon_Add_Del

The ADSPI_Trust_Mon_Add_Del policy monitors additions and deletions of trusts in the Microsoft Active Directory forest.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en → Windows Server 2003 →Auto-Deploy → Trust Monitoring**

Related Topics:

- Trust Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_Trust_Mon_Add_Del

ADSPI_Trust_Mon_Add_Del_2k8+

The ADSPI_Trust_Mon_Add_Del_2k8+ policy monitors additions and deletions of trusts in the Microsoft Active Directory forest.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 →Auto-Deploy → Trust Monitoring**

Related Topics:

- Trust Monitoring Policies
- Choosing Auto-Deploy Policy Group
- ADSPI_Trust_Mon_Add_Del

Manual-Deploy Policies

Manual-Deploy 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 Policies
- Domain and OU Structure Policies
- Global Catalog Access Policies
- Health Monitors Polices
- Index and Query Monitors Policies
- Replication Policies
- Replication Activity Policies
- Security Policies
- Site Structure Policies

Related Topic

- Choosing Manual-Deploy Policy Group

Auto Baseline Polices

The Auto Baseline policies calculate appropriate adaptive threshold values for Measurement Threshold policies, based on previously collected historical data. The policies for Windows Server 2003 and 2008 are as follows:

- ADSPI-Rep_InboundObjects_AT / ADSPI-Rep_InboundObjects_AT_2k8+
- ADSPI-Rep_TimeSync_Monitor_AT / ADSPI-Rep_TimeSync_Monitor_AT_2k8+
- ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT / ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+

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

NOTE:
(1) Auto-baseline policies do not work on nodes configured with HP Performance Agent.

(2) If you have upgraded the Active Directory SPI from an older version, the auto-baseline policies cannotwill not be able to use the historical data of the previous version of the SPI.

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

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

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

1. The policy reads the historical values of the metric that it is monitoring. The historical values are stored into the data store.
2. The policy calculates the arithmetic mean of the values of the metric. Arithmetic mean = Sum of all historical values/ Number of all historical data points
3. The standard deviation of the metric is calculated with the following details:
   - Arithmetic mean of the metric
   - Historical data point

- Number of all historical data points

4. The policy sets a range of threshold values using the following calculation:
   - Maximum threshold = Arithmetic mean + Standard deviation
   - Minimum threshold = Arithmetic mean - Standard deviation
5. The policy generates an alert when the metric value does not belong to the threshold range.

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI-Rep_InboundObjects_AT

The ADSPI-Rep_InboundObjects_AT policy is an auto-threshold policy which monitors the number of inbound replication objects.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Auto Baseline Policies**

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group
- ADSPI-Rep_InboundObjects_AT_2k8+

ADSPI-Rep_InboundObjects_AT_2k8+

The ADSPI-Rep_InboundObjects_AT_2k8+ policy is an auto-threshold policy which monitors the number of inbound replication objects.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Auto Baseline Policies**

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group
- ADSPI-Rep_InboundObjects_AT

ADSPI-Rep_TimeSync_Monitor_AT

The ADSPI-Rep_TimeSync_Monitor_AT policy is an auto-threshold policy which validates time synchronization with the time master, in seconds.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy→ Auto Baseline Policies**

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group
- ADSPI-Rep_TimeSync_Monitor_AT

ADSPI-Rep_TimeSync_Monitor_AT_2k8+

The ADSPI-Rep_TimeSync_Monitor_AT_2k8+ policy is an auto-threshold policy which validates time synchronization with the time master, in seconds.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy→ Auto Baseline Policies**

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group
- ADSPI-Rep_TimeSync_Monitor_AT

ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT

The ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT policy is an auto-threshold policy which monitors delay times of global catalog inter- and intra-site replication.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Auto Baseline Policies**

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+

ADSPI-Rep_GC_Check_and _Threshold_Monitor_AT_2k8+

The ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+ policy is an auto-threshold policy which monitors delay times of global catalog inter- and intra-site replication.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Auto Baseline Policies**

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group
- ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT

Connector Policies

The Connector polices Monitors Active Directory performance monitor counters. The polices are applicable to only Windows Server 2003 are as follows:

- ADSPI_ActiveAuthKerberos
- ADSPI_ActiveAuthLogon
- ADSPI_ActiveAuthNTLM
- ADSPI_ADCFwdAllWarnErrorMSADC
- ADSPI_ADCImportFailures
- ADSPI_ADCPageFaults
- ADSPI_ADCPrivateBytes
- ADSPI_ADCProcessorTime
- ADSPI_ADCWorkingSet

Related Topics:

- Domain and OU Structure Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ActiveAuthKerberos

The ADSPI_ActiveAuthKerberos policy checks the NTDS Kerberos Authentications counter for the number of successful authentications processed by the DC. 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, ensure that the existing DCs are upgraded or the additional DCs are installed.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ActiveAuthLogon

The ADSPI_ActiveAuthLogon policy checks the Server\Logon/sec counter for the number of successful authentications processed by the DC. 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, ensure that the existing DCs are upgraded or additional DCs are installed.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ActiveAuthNTLM

The ADSPI_ActiveAuthNTLM policy checks the NTDS\NTLM Authentications counter for the number of successful authentications processed by the DC. 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, ensure that the existing DCs are upgraded or additional DCs are installed.

Policy Type: Measurement Threshold

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ADCFwdAllWarnErrorMSADC

The ADSPI_ADCFwdAllWarnErrorMSADC policy monitors the Application log for entries from MSADC that have a severity level of Warning or Error. It also forwards these entries as messages to the active message browser.
This policy functions only with the integration of Microsoft Exchange. Without Microsoft Exchange, the adc process, which the policy observes, does not exist.

Policy Type: Windows Event Log (Application)

Policy Group: **SPI for Active Directory** > **Windows Server 2003** > **Manual Deploy > Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADCFwdAllWarnErrorMSADC

ADSPI_ADCImportFailures

The ADSPI_ADCImportFailures policy 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 Microsoft Exchange. Without Microsoft Exchange, the process adc, which the policy observes, does not exist.

Policy Type: Measurement Threshold

Policy Group: **SPI for Active Directory** > **Windows Server 2003** > **Manual Deploy > Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADCImportFailures+

ADSPI_ADCPageFaults

The ADSPI_ADCPageFaults policy 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 Microsoft Exchange. Without Microsoft Exchange, the process adc, which the policy observes, does not exist.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory →Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ADCPrivateBytes

The ADSPI_ADCPrivateBytes policy 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 Microsoft Exchange. Without Microsoft Exchange, the process adc, which the policy observes, does not exist.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ADCProcessorTime

The ADSPI_ADCProcessorTime policy checks the PerfLib counter Process\Processor Time\adc for the percentage of processor time the Microsoft 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, check if the Microsoft Active Directory server is overloaded. In such a case ensure that the hardware is upgraded or tuned further to optimize performance.

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

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ADCWorkingSet

The ADSPI_ADCWorkingSet policy 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 Microsoft Exchange. Without Microsoft Exchange, the process adc, which the policy observes, does not exist.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Connector**

Related Topics:

- Connector Policies
- Choosing Manual-Deploy Policy Group

Domain and OU Structure Policies

The Domain and OU Structure Policies policies monitor Monitors domain and organizational unit (OU) changes. The policies for Windows Server 2003 and 2008 are as follows:

- ADSPI_DomainChanges / ADSPI_DomainChanges_2k8+
- ADSPI_OUChanges / ADSPI_OUChanges_2k8+

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group

ADSPI_DomainChanges

The ADSPI_DomainChanges policy checks for changes to the domain structure, approximately every 20 minutes.

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 Microsoft Active Directory database. Deploy this policy on a DC only.

Schedule: This policy runs approximately every 20 minutes.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Domain and OU Structure**

Related Topics:

- Domain and OU Structure Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DomainChanges_2k8+

ADSPI_DomainChanges_2k8+

The ADSPI_DomainChanges_2k8+ policy checks for changes to the domain structure, approximately every 20 minutes.

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 Microsoft Active Directory database. Deploy this policy on a DC only.

Schedule: This policy runs approximately every 20 minutes

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Domain and OU Structure**

Related Topics:

- Domain and OU Structure Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DomainChanges

ADSPI_OUChanges

The ADSPI_OUChanges policy 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 DC only.

Schedule: This policy runs approximately every 20 minutes

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Domain and OU Structure**

Related Topics:

- Domain and OU Structure Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_OUChanges_2k8+

ADSPI_OUChanges_2k8+

The ADSPI_OUChanges_2k8+ policy 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 DC only.

Schedule: This policy runs approximately every 20 minutes

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Domain and OU Structure**

Related Topics:

- Domain and OU Structure Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DomainChanges

Global Catalog Access Policies

The Global Catalog Access policies monitor the performance monitor counters on Global Catalog servers. The policies for Windows Server 2003 and 2008 are as follows:

- ADSPI_GlobalCatalogWrites / ADSPI_GlobalCatalogWrites_2k8+
- ADSPI_GlobalCatalogReads / ADSPI_GlobalCatalogReads_2k8+
- ADSPI_GlobalCatalogSearches /ADSPI_GlobalCatalogSearches_2k8+

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group

ADSPI_GlobalCatalogWrites

The ADSPI_GlobalCatalogWrites policy 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 DC requires an additional hardware or an additional DC is required.

Schedule: This policy runs approximately every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Global Catalog Access**

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_GlobalCatalogWrites_2k8+

ADSPI_GlobalCatalogWrites_2k8+

The ADSPI_GlobalCatalogWrites_2k8+ policy 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 DC requires an additional hardware or an additional DC is required.

Schedule: This policy runs approximately every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Global Catalog Access**

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_GlobalCatalogWrites

ADSPI_GlobalCatalogReads

The ADSPI_GlobalCatalogReads policy 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 DC requires an additional hardware or an additional DC is required.

Deploy this policy to the Global Catalog server only.

Schedule: This policy runs approximately every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Global Catalog Access**

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_GlobalCatalogReads_2k8+

ADSPI_GlobalCatalogReads_2k8+

The ADSPI_GlobalCatalogReads_2k8+ policy 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 DC requires an additional hardware or an additional DC is required.

Deploy this policy to the Global Catalog server only.

Schedule: This policy runs approximately every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Global Catalog Access**

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_GlobalCatalogReads

ADSPI_GlobalCatalogSearches

The ADSPI_GlobalCatalogSearches policy 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 DC requires an additional hardware or an additional DC is required.

Deploy this policy to the Global Catalog server only.

Schedule: This policy runs approximately every 30 minutes

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Global Catalog Access**

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_GlobalCatalogSearches_2k8+

ADSPI_GlobalCatalogSearches_2k8+

The ADSPI_GlobalCatalogSearches_2k8+ policy 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 DC requires an additional hardware or an additional DC is required.

Deploy this policy to the Global Catalog server only.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Global Catalog Access**

Related Topics:

- Global Catalog Access Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_GlobalCatalogSearches

Health Monitors

The Health Monitors policies monitor the health of DNS, Kerberos and NetLogon Services. The policies for Windows Server 2003 and 2008 are as follows:

- ADSPI_DNSServ_FwdAllInformation / ADSPI_DNSServ_FwdAllInformation_2k8+
- ADSPI_DNSServ_FwdAllWarnError / ADSPI_DNSServ_FwdAllWarnError_2k8+
- ADSPI_FwdAllInformationDS / ADSPI_FwdAllInformationDS_2k8+
- ADSPI_FwdAllInformationFRS / ADSPI_FwdAllInformationFRS_2k8+
- ADSPI_FwdAllWarnErrorDS / ADSPI_FwdAllWarnErrorDS_2k8+
- ADSPI_FwdAllWarnErrorFRS / ADSPI_FwdAllWarnErrorFRS_2k8+
- ADSPI_HMLSASSPageFaults / ADSPI_HMLSASSPageFaults_2k8+
- ADSPI_HMLSASSPrivateBytes / ADSPI_HMLSASSPrivateBytes_2k8+
- ADSPI_HMLSASSProcessorTime / ADSPI_HMLSASSProcessorTime_2k8+
- ADSPI_HMLSASSWorkingSet / ADSPI_HMLSASSWorkingSet_2k8+
- ADSPI_HMNTFRSPageFaults / ADSPI_HMNTFRSPageFaults_2k8+
- ADSPI_HMNTFRSPrivateBytes / ADSPI_HMNTFRSPrivateBytes_2k8+
- ADSPI_HMNTFRSProcessorTime / ADSPI_HMNTFRSProcessorTime_2k8+
- ADSPI_HMNTFRSWorkingSet / ADSPI_HMNTFRSWorkingSet_2k8+
- ADSPI_HMThreadsInUse /ADSPI_HMThreadsInUse_2k8+
- ADSPI_KDC / ADSPI_KDC_2k8+
- ADSPI_Logging / ADSPI_Logging_2k8+
- ADSPI_NetLogon / ADSPI_NetLogon_2k8+
- ADSPI_NTFRS / ADSPI_NTFRS_2k8+
- ADSPI_NtLmSsp
- ADSPI_SamSs / ADSPI_SamSs_2k8+
- ADSPI_SMTPEventLogs / ADSPI_SMTPEventLogs_2k8+
- ADSPI_SyncSchemaMisMatch / ADSPI_SyncSchemaMisMatch_2k8+
- ADSPI_DFSR_2k8+

- ADSPI_NTDS_2k8+

Related Topics:

- Index and Query Monitor Policies
- Choosing Manual-Deploy Policy Group

ADSPI_DNSServ_FwdAllInformation

The ADSPI_DNSServ_FwdAllInformation policy monitors the DNS Server log for entries that have a severity level of Information. This policy forwards these entries as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DNSServ_FwdAllInformation_2k8+

ADSPI_DNSServ_FwdAllInformation_2k8+

The ADSPI_DNSServ_FwdAllInformation_2k8+ policy monitors the DNS Server log for entries that have a severity level of Information. This policy forwards these entries as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DNSServ_FwdAllInformation

ADSPI_DNSServ_FwdAllWarnError

The ADSPI_DNSServ_FwdAllWarnError policy monitors the DNS Server log for entries that have a severity level of *Warning* or *Error* . This policy forwards these entries as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DNSServ_FwdAllWarnError_2k8+

ADSPI_DNSServ_FwdAllWarnError_2k8+

The ADSPI_DNSServ_FwdAllWarnError_2k8+ policy monitors the DNS Server log for entries that have a severity level of *Warning* or *Error* . This policy forwards these entries as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DNSServ_FwdAllWarnError

ADSPI_FwdAllInformationDS

The ADSPI_FwdAllInformationDS policy monitors the Directory Service log for entries with a severity level of Information and forwards them as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllInformationDS_2k8+

ADSPI_FwdAllInformationDS_2k8+

The ADSPI_FwdAllInformationDS_2k8+ policy monitors the Directory Service log for entries with a severity level of Information and forwards them as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllInformationDS

ADSPI_FwdAllInformationFRS

The ADSPI_FwdAllInformationFRS policy monitors the File Replication Service log for entries with a severity level of Information. Forwards them as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllInformationFRS_2k8+

ADSPI_FwdAllInformationFRS_2k8+

The ADSPI_FwdAllInformationFRS_2k8+ policy monitors the File Replication Service log for entries with a severity level of Information. This policy forwards them as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllInformationFRS

ADSPI_FwdAllWarnErrorDS

The ADSPI_FwdAllWarnErrorDS policy forwards all event log entries with a severity level of *Warning* or *Error* .

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllWarnErrorDS_2k8+

ADSPI_FwdAllWarnErrorDS_2k8+

The ADSPI_FwdAllWarnErrorDS_2k8+ policy forwards all event log entries with a severity level of *Warning* or *Error* .

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllWarnErrorDS

ADSPI_FwdAllWarnErrorFRS

The ADSPI_FwdAllWarnErrorFRS policy forwards all event log entries with a severity level of *Warning* or *Error* .

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllWarnErrorFRS_2k8+

ADSPI_FwdAllWarnErrorFRS_2k8+

The ADSPI_FwdAllWarnErrorFRS_2k8+ policy forwards all event log entries with a severity level of *Warning* or *Error* .

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_FwdAllWarnErrorFRS

ADSPI_HMLSASSPageFaults

The ADSPI_HMLSASSPageFaults policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Manual-Deploy → Windows Server 2003 → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSPageFaults_2k8+

ADSPI_HMLSASSPageFaults_2k8+

The ADSPI_HMLSASSPageFaults_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Manual-Deploy → Windows Server 2008 → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSPageFaults

ADSPI_HMLSASSPrivateBytes

The ADSPI_HMLSASSPrivateBytes policy 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 can be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSPrivateBytes_2k8+

ADSPI_HMLSASSPrivateBytes_2k8+

The ADSPI_HMLSASSPrivateBytes_2k8+ policy 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 can be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSPrivateBytes

ADSPI_HMLSASSProcessorTime

The ADSPI_HMLSASSProcessorTime policy 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, ensure that the server is not overloaded. Check if the server requires a hardware upgrade or further tuning to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSProcessorTime_2k8+

ADSPI_HMLSASSProcessorTime_2k8+

The ADSPI_HMLSASSProcessorTime_2k8+ policy 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, ensure that the server is not overloaded. Check if the server requires a hardware upgrade further tuning to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy→ Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSProcessorTime

ADSPI_HMLSASSWorkingSet

The ADSPI_HMLSASSWorkingSet policy 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 might be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSWorkingSet_2k8+

ADSPI_HMLSASSWorkingSet_2k8+

The ADSPI_HMLSASSWorkingSet_2k8+ policy 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 might be a memory leak or some other memory problems.

Policy Type: Measurement Threshold

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSWorkingSet

ADSPI_HMNTFRSPageFaults

The ADSPI_HMNTFRSPageFaults policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSPageFaults_2k8+

ADSPI_HMNTFRSPageFaults_2k8+

The ADSPI_HMNTFRSPageFaults_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSPageFaults

ADSPI_HMNTFRSPrivateBytes

The ADSPI_HMNTFRSPrivateBytes policy 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 might be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSPrivateBytes_2k8+

ADSPI_HMNTFRSPrivateBytes_2k8+

The ADSPI_HMNTFRSPrivateBytes_2k8+ policy 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 might be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSPrivateBytes

ADSPI_HMNTFRSProcessorTime

The ADSPI_HMNTFRSProcessorTime policy 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, ensure that the server is not overloaded. Check if the server requires a hardware upgrade or further tuning to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSProcessorTime_2k8+

ADSPI_HMNTFRSProcessorTime_2k8+

The ADSPI_HMNTFRSProcessorTime_2k8+ policy 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, ensure that the server is not overloaded. Check if the server requires a hardware upgrade or need further tuning to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSProcessorTime

ADSPI_HMNTFRSWorkingSet

The ADSPI_HMNTFRSWorkingSet policy 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 might be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSWorkingSet_2k8+

ADSPI_HMNTFRSWorkingSet_2k8+

The ADSPI_HMNTFRSWorkingSet_2k8+ policy 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 might be a memory leak or some other memory problems.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMNTFRSWorkingSet

ADSPI_HMThreadsInUse

The ADSPI_HMThreadsInUse policy 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 are to be used.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMThreadsInUse_2k8+

ADSPI_HMThreadsInUse_2k8+

The ADSPI_HMThreadsInUse_2k8+ policy 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 are to be used.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMThreadsInUse

ADSPI_KDC

The ADSPI_KDC policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy→ Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_KDC_2k8+

ADSPI_KDC_2k8+

The ADSPI_KDC_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy→ Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_KDC

ADSPI_NetLogon

The ADSPI_NetLogon policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_NetLogon_2k8+

ADSPI_NetLogon_2k8+

The ADSPI_NetLogon_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_NetLogon

ADSPI_NTFRS

The ADSPI_NTFRS policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_NTFRS_2k8+

ADSPI_NTFRS_2k8+

The ADSPI_NTFRS_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_NTFRS

ADSPI_NtLmSsp

The ADSPI_NtLmSsp policy checks the NT LM Security Support Provider Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_NTFRS

ADSPI_DFSR_2K8+

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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en → Windows Server 2008 → Manual-Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_HMLSASSPageFaults_2k8+

ADSPI_NTDS_2k8+

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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_NTDS

ADSPI_SamSs

The ADSPI_SamSs policy 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.

Policy Type: Measurement Threshold

Policy Group: **SPI for Active Directory → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_SamSs_2k8+

ADSPI_SamSs_2k8+

The ADSPI_SamSs_2k8+ policy 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.

Policy Type: Measurement Threshold

Policy Group: **SPI for Active Directory → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_SamSs

ADSPI_SMTPEventLogs

The ADSPI_SMTPEventLogs policy monitors the system log for SMTP-specific events. This policy forwards them as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (or ja) → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_SMTPEventLogs_2k8+

ADSPI_SMTPEventLogs_2k8+

The ADSPI_SMTPEventLogs_2k8+ policy monitors the system log for SMTP-specific events. This policy forwards them as messages to the active message browser.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (or ja) → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_SMTPEventLogs

ADSPI_SyncSchemaMisMatch

The ADSPI_SyncSchemaMisMatch policy 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, check if the server is overloaded. In such a case ensure that the hardware is upgraded or tuned for further replication to optimize performance.

This policy logs the value of PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (or ja) → Windows Server 2003 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_SyncSchemaMisMatch_2k8+

ADSPI_SyncSchemaMisMatch_2k8+

The ADSPI_SyncSchemaMisMatch_2k8+ policy 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, check if the server is overloaded. In such a case, ensure that the hardware is upgraded or tuned for further replication to optimize performance.

This policy logs the value of PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (or ja) → Windows Server 2008 → Manual Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_SyncSchemaMisMatch

ADSPI_Logging

ADSPI_Logging 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	

Policy Type: Measurement Threshold policy

Policy group: **SPI for Active Directory → en → Windows 2003 → Manual-Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_Logging_2k8+

ADSPI_Logging_2k8+

ADSPI_Logging_2k8+ 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	

Policy Type: Measurement Threshold policy

Policy group: **SPI for Active Directory → en → Windows 2008 → Manual-Deploy → Health Monitors**

Related Topics:

- Health Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_Logging

Index and Query Moniror Policies

The Index and Query Monitor policies monitor the performance monitor counters associated with LDAP and Kerberos. The polices of Windows Server 2003 and 2008 are as follows:

- ADSPI_IQKerberosAuthentications / ADSPI_IQKerberosAuthentications_2k8+
- ADSPI_IQLDAPActiveThreads / ADSPI_IQLDAPActiveThreads_2k8+
- ADSPI_IQLDAPBindTime / ADSPI_IQLDAPBindTime_2k8+
- ADSPI_IQLDAPClientSessions / ADSPI_IQLDAPClientSessions_2k8+
- ADSPI_IQNTLMAuthentications / ADSPI_IQNTLMAuthentications_2k8+
- ADSPI_DSSearches / ADSPI_DSSearches_2k8+
- ADSPI_DSReads / ADSPI_DSReads_2k8+
- ADSPI_DSWrites / ADSPI_DSWrites_2k8+

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group

ADSPI_IQKerberosAuthentications

The ADSPI_IQKerberosAuthentications policy 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 DC might be overloaded with logon authentication traffic.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQKerberosAuthentications_2k8+

ADSPI_IQKerberosAuthentications_2k8+

The ADSPI_IQKerberosAuthentications_2k8+ policy 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 DC might be overloaded with logon authentication traffic.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQKerberosAuthentications

ADSPI_IQLDAPActiveThreads

The ADSPI_IQLDAPActiveThreads policy 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 DC might be overloaded with LDAP queries.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en(ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQLDAPActiveThreads_2k8+

ADSPI_IQLDAPActiveThreads_2k8+

The ADSPI_IQLDAPActiveThreads_2k8+ policy 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 DC might be overloaded with LDAP queries.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en(ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQLDAPActiveThreads

ADSPI_IQLDAPBindTime

The ADSPI_IQLDAPBindTime policy 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 DC might be overloaded with LDAP queries.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en(ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQLDAPBindTime_2k8+

ADSPI_IQLDAPBindTime_2k8+

The ADSPI_IQLDAPBindTime_2k8+ policy 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 DC might be overloaded with LDAP queries.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en(ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQLDAPBindTime

ADSPI_IQLDAPClientSessions

The ADSPI_IQLDAPClientSessions policy 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 DC might be overloaded with LDAP queries.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitirs**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQLDAPClientSessions_2k8+

ADSPI_IQLDAPClientSessions_2k8+

The ADSPI_IQLDAPClientSessions_2k8+ policy 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 DC might be overloaded with LDAP queries.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQLDAPClientSessions

ADSPI_IQNTLMAuthentications

The ADSPI_IQNTLMAuthentications policy 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 DC might be overloaded with logon authentication traffic.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQNTLMAuthentications_2k8+

ADSPI_IQNTLMAuthentications_2k8+

The ADSPI_IQNTLMAuthentications_2k8+ policy 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 DC might be overloaded with logon authentication traffic.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_IQNTLMAuthentications

ADSPI_DSSearches

The ADSPI_DSSearches policy evaluates the number of searches every second in the Directory Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DSSearches_2k8+

ADSPI_DSSearches_2k8+

The ADSPI_DSSearches_2k8+ policy evaluates the number of searches every second in the Directory Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DSSearches

ADSPI_DSReads

The ADSPI_DSReads policy evaluates the number of reads every second in the Directory Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DSReads_2k8+

ADSPI_DSReads_2k8+

The ADSPI_DSReads_2k8+ policy evaluates the number of reads every second in the Directory Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DSReads

ADSPI_DSWrites

The ADSPI_DSWrites policy evaluates the number of writes every second in the Directory Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DSWrites_2k8+

ADSPI_DSWrites_2k8+

The ADSPI_DSWrites_2k8+ policy evaluates the number of writes every second in the Directory Service.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Index and Query Monitors**

Related Topics:

- Index and Query Monitors
- Choosing Manual-Deploy Policy Group
- ADSPI_DSWrites

Replication Policies

The Replication policies monitor replication through measurement of inbound objects between and within sites, verification of synchronization of replication updates, pending updates, and queue size in replication inbound objects. The policies of Windows Server 2003 and 2008 are as follows:

- ADSPI_ADSPendingSynchronizations / ADSPI_ADSPendingSynchronizations_2k8+
- ADSPI_ADSRepInBoundBytesBetweenSites / ADSPI_ADSRepInBoundBytesBetweenSites_2k8+
- ADSPI_ADSRepInBoundBytesWithinSites / ADSPI_ADSRepInBoundBytesWithinSites_2k8+
- ADSPI_ADSRepInBoundObjectUpdatesRemaining / ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+
- ADSPI_ADSRepNotifyQueueSize / ADSPI_ADSRepNotifyQueueSize_2k8+

Related Topics:

- Replication Activities Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ADSPendingSynchronizations

The ADSPI_ADSPendingSynchronizations policy 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, check if the server is overloaded. In such a case ensure that the hardware is upgraded or tuned for further replication to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSPendingSynchronizations_2k8+

ADSPI_ADSPendingSynchronizations_2k8+

The ADSPI_ADSPendingSynchronizations_2k8+ policy 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, check if the server is overloaded. In such a case ensure that the hardware is upgraded or tuned for further replication to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSPendingSynchronizations

ADSPI_ADSRepInBoundBytesBetweenSites

The ADSPI_ADSRepInBoundBytesBetweenSites policy 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 Microsoft Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, ensure that the Microsoft Active Directory replication is optimized.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepInBoundBytesBetweenSites_2k8+

ADSPI_ADSRepInBoundSites BetweenSites_2k8+

The ADSPI_ADSRepInBoundBytesBetweenSites_2k8+ policy 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 Microsoft Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, ensure that the Microsoft Active Directory replication is optimized.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepInBoundBytesBetweenSites

ADSPI_ADSRepInBoundBytesWithinSites

The ADSPI_ADSRepInBoundBytesWithinSites policy 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 Microsoft Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, ensure that the Microsoft Active Directory replication is optimized.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepInBoundBytesWithinSites_2k8+

ADSPI_ADSRepInBoundBytes WithinSites_2k8+

The ADSPI_ADSRepInBoundBytesWithinSites_2k8+ policy 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 Microsoft Active Directory replication for a server exceeds the upper threshold number of bytes per second between sites, ensure that the Microsoft Active Directory replication is optimized.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepInBoundBytesWithinSites

ADSPI_ADSRepInBoundObject UpdatesRemaining

The ADSPI_ADSRepInBoundObjectUpdatesRemaining policy 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, check if the server is overloaded. In such a case ensure the hardware is upgraded or tuned for further replication to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory →en (ja) → Windows Server 2003 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+

ADSPI_ADSRepInBoundObjectUpdates Remaining_2k8+

The ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+ policy 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, check if the server is overloaded. In such a case ensure that the hardware is upgraded or tuned for further replication to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepInBoundObjectUpdatesRemaining

ADSPI_ADSRepNotifyQueueSize

The ADSPI_ADSRepNotifyQueueSize policy 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, check if the server is overloaded. In such a case ensure that the hardware is upgraded or tuned for further replication to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepNotifyQueueSize_2k8+

ADSPI_ADSRepNotifyQueueSize_2k8+

The ADSPI_ADSRepNotifyQueueSize_2k8+ policy 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, check if the server is overloaded. In such a case ensure that the hardware is upgraded or tuned for further replication to optimize performance.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Replication**

Related Topics:

- Replication Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_ADSRepNotifyQueueSize

Replication Activity Polices

The Replication Activity policies monitor the Directory Service log for replication events. The policies of Windows Server 2003 and 2008 are as follows:

- ADSPI_ReplicationActivities / ADSPI_ReplicationActivities_2k8+

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group

ADSPI_ReplicationActivities

The ADSPI_ReplicationActivities policy 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

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Replication Activities**

Related Topics:

- Replication Activities
- Choosing Manual-Deploy Policy Group
- ADSPI_ReplicationActivities_2k8+

ADSPI_ReplicationActivities_2k8+

The ADSPI_ReplicationActivities_2k8+ policy 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

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Replication Activities**

Related Topics:

- Replication Activities
- Choosing Manual-Deploy Policy Group
- ADSPI_ReplicationActivities

Security Policies

The Security policies monitors:

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

The policies for Windows Server 2003 and 2008 are as follows:

- ADSPI_DirUserCreationDeletionModification / ADSPI_DirUserCreationDeletionModification_2k8+
- ADSPI_KDCFailureGrantTicket / ADSPI_KDCFailureGrantTicket_2k8+
- ADSPI_PrivilegedAccounts / ADSPI_PrivilegedAccounts_2k8+
- ADSPI_SecAdminGroupChangeMon / ADSPI_SecAdminGroupChangeMon_2k8+
- ADSPI_SecDirectoryServiceAccess / ADSPI_SecDirectoryServiceAccess_2k8+
- ADSPI_SecErrAccessPermissions / ADSPI_SecErrAccessPermissions_2k8+
- ADSPI_SecErrGrantedAccess / ADSPI_SecErrGrantedAccess_2k8+
- ADSPI_SecErrorsLogon / ADSPI_SecErrorsLogon_2k8+
- ADSPI_SecNonTransMembEval / ADSPI_SecNonTransMembEval_2k8+
- ADSPI_SecSDPropagatorQueue / ADSPI_SecSDPropagatorQueue_2k8+
- ADSPI_SecTransMembEval / ADSPI_SecTransMembEval_2k8+
- ADSPI_DirComputerModif / ADSPI_DirComputerModif_2k8+

Related Topics:

- Site Structure Policies
- Choosing Manual-Deploy Policy Group

ADSPI_DirUserCreationDeletionModification

The ADSPI_DirUserCreationDeletionModification policy checks whether any accounts in the Directory User Accounts have been created, deleted, or modified. If so, the policy sends a message to the active message browser.

Schedule: This policy runs approximately every 15 minutes

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DirUserCreationDeletionModification_2k8+

ADSPI_DirUserCreationDeletion Modification_2k8+

The ADSPI_DirUserCreationDeletionModification_2k8+ policy checks whether any accounts in Directory User Accounts have been created, deleted, or modified. If so, the policy sends a message to the active message browser.

Schedule: This policy runs approximately every 15 minutes

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DirUserCreationDeletionModification

ADSPI_KDCFailureGrantTicket

The ADSPI_KDCFailureGrantTicket policy monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 672 and 676 in the Security Event Log:

672 and 676 Authentication Ticket Request Failed

Deploy this template only to servers running KDC.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_KDCFailureGrantTicket_2k8+

ADSPI_KDCFailureGrantTicket_2k8+

The ADSPI_KDCFailureGrantTicket_2k8+ policy monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 4771 and 4768 in the Security Event Log:

4771 and 4768 Authentication Ticket Request Failed

Deploy this template only to servers running KDC.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_KDCFailureGrantTicket

ADSPI_PrivilegedAccounts

The ADSPI_PrivilegedAccounts policy 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

This policy forwards these entries as messages to the active message browser. Windows Server operating systems do 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)

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group

- ADSPI_PrivilegedAccounts_2k8+

ADSPI_PrivilegedAccounts_2k8+

The ADSPI_PrivilegedAccounts_2k8+ policy 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

This policy forwards these entries as messages to the active message browser. Windows Server operating systems do 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)

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group

- ADSPI_PrivilegedAccounts

ADSPI_SecAdminGroupChangeMon

The ADSPI_SecAdminGroupChangeMon policy monitors the changes that occur in the Domain Admin group and the Enterprise Admins security group. These policies also inform about what change occurred, who changed it, and when it was changed.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecAdminGroupChangeMon_2k8+

ADSPI_SecAdminGroupChangeMon_2k8+

The ADSPI_SecAdminGroupChangeMon_2k8+ policy monitors the changes that occur in the Domain Admin group and the Enterprise Admins security group. These policies also inform about what change occurred, who changed it, and when it was changed.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecAdminGroupChangeMon

ADSPI_SecDirectoryServiceAccess

The ADSPI_SecDirectoryServiceAccess policy forwards all security event log entries with Directory Service Access category.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecDirectoryServiceAccess_2k8+

ADSPI_SecDirectoryServiceAccess_2k8+

The ADSPI_SecDirectoryServiceAccess_2k8+ policy forwards all security event log entries with Directory Service Access category.

Policy Type: Windows Event Log policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecDirectoryServiceAccess

ADSPI_SecErrAccessPermissions

The ADSPI_SecErrAccessPermissions policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecErrAccessPermissions_2k8+

ADSPI_SecErrAccessPermissions_2k8+

The ADSPI_SecErrAccessPermissions_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecErrAccessPermissions

ADSPI_SecErrGrantedAccess

The ADSPI_SecErrGrantedAccess policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecErrGrantedAccess_2k8+

ADSPI_SecErrGrantedAccess_2k8+

The ADSPI_SecErrGrantedAccess_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecErrGrantedAccess

ADSPI_SecErrorsLogon

The ADSPI_SecErrorsLogon policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecErrorsLogon_2k8+

ADSPI_SecErrorsLogon_2k8+

The ADSPI_SecErrorsLogon_2k8+ policy 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.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 →Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecErrorsLogon

ADSPI_SecNonTransMembEval

The ADSPI_SecNonTransMembEval policy 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, check if the domain is overloaded.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecNonTransMembEval_2k8+

ADSPI_SecNonTransMembEval_2k8+

The ADSPI_SecNonTransMembEval_2k8+ policy 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, check if the domain is overloaded.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecNonTransMembEval

ADSPI_SecSDPropagatorQueue

The ADSPI_SecSDPropagatorQueue policy 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, check if the domain is overloaded.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecSDPropagatorQueue_2k8+

ADSPI_SecSDPropagatorQueue_2k8+

The ADSPI_SecSDPropagatorQueue_2k8+ policy 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, check if the domain is overloaded.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecSDPropagatorQueue

ADSPI_SecTransMembEval

The ADSPI_SecTransMembEval policy 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 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, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecTransMembEval_2k8+

ADSPI_SecTransMembEval_2k8+

The ADSPI_SecTransMembEval_2k8+ policy 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 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, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Policy Type: Measurement Threshold policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SecTransMembEval

ADSPI_DirComputerModif

The ADSPI_DirComputerModif policy sends alert messages if there is any modification to a computer in the domain.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DirComputerModif_2k8+

ADSPI_DirComputerModif_2k8+

The ADSPI_DirComputerModif_2k8+ policy sends alert messages if there is any modification to a computer in the domain.

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Security**

Related Topics:

- Security Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_DirComputerModif

Site Structure Policies

The Site Structure policies monitor site changes. It includes ADSPI_SiteChanges / ADSPI_SiteChanges_2k8+ policies for Windows Server 2003 and 2008.

Related Topics:

- Auto Baseline Policies
- Choosing Manual-Deploy Policy Group

ADSPI_SiteChanges

The ADSPI_SiteChanges policy monitors the Microsoft 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).

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2003 → Manual Deploy → Site Structure**

Related Topics:

- Site Structure Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SiteChanges_2k8+

ADSPI_SiteChanges_2k8+

The ADSPI_SiteChanges_2k8+ policy monitors the Microsoft 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).

Policy Type: Windows Management Interface (WMI) policy

Policy Group: **SPI for Active Directory → en (ja) → Windows Server 2008 → Manual Deploy → Site Structure**

Related Topics:

- Site Structure Policies
- Choosing Manual-Deploy Policy Group
- ADSPI_SiteChanges

Data Store Details and Policy Mapping

The Microsoft Active Directory SPI creates the following data in the data store on the node to facilitate the data-collection procedure:

Data Store Details

Table in the Data Store	Metrics in the Table and Description	Metric Data Type
ADSPI_DITDBSIZE This table contains data on the DIT database (ntds.dit) which is the Microsoft Active Directory data store. *Policy Name:* ADSPI-DIT_TotalDitSize	Instance Name - Path to the DIT database file	UTF8
	InstanceValue - Size of the DIT file in MB	REAL64
ADSPI_DITPERCENTFULL This table has data on the drive hosting the DIT database (ntds.dit) which is the Microsoft Active Directory data store. *Policy Name:* ADSPI-DIT_DITPercentFull	Instance Name - Path to the NTDS folder	UTF8
	InstanceValue - Percentage of the used space of the drive hosting DIT database	REAL64
ADSPI_DITQUEUELENGTH This table has data on the drive hosting the DIT database (ntds.dit) which is the Microsoft Active Directory data store. *Policy Name:* ADSPI-DIT_DITQueueLength	Instance Name - Path to the NTDS folder	UTF8
	InstanceValue - Average disk queue length of the drive hosting DIT database	REAL64
ADSPI_DNSDR This table contains the DNS response time experienced by the Domain Controller (DC) in milli seconds. *Policy Name:* ADSPI-DNS_DC_Response	RespTime - DNS response time in milliseconds experienced by a DC	REAL64
ADSPI_DNSSP This table contains data which determines whether DNS Server is a DC or not and value of pages/sec counter of "memory" perfmon object. *Policy Name:* ADSPI-DNS_LogDNSPagesSec	IsDomainController - Set to one if the DNS server is a DC and set to zero if it is not	REAL64
	PagesPerSec -Value of the pages/sec counter of "memory" perfmon object	
ADSPI_DOMAIN This table contains the domain	DomainName - Always taken as	UTF8

name associated with the DC. *Policy Name:* ADSPI-DIT_TotalDitSize	the value "DomainName". DomainValue is the name of the domain hosted by the DC.	
	DomainValue - Name of the domain hosted by the DC	
ADSPI_FSMO This table contains the ping and bind response times experienced by the DC to every FSMO role owner in seconds. *Policy Name:* ADSPI-FSMO_Logging	FSMO - Name of the FSMO role	UTF8
	SERVER - Name of the server hosting the role	UTF8
	PINGTIME - Ping time experienced by the DC to the server in seconds	REAL64
	BINDTIME - Bind time experienced by the DC to the server in seconds	REAL64
ADSPI_FSMO_ROLEMVMT Data is logged into this table whenever the DC gains or loses an FSMO role. *Policy Name:* ADSPI-FSMO_RoleMvmt	FSMO - FSMO role name gained or lost by the DC	UTF8
	ISROLEHOLDER - Zero if the role has been gained and one if it has been lost by the DC	REAL64
ADSPI_GCREP This table contains the replication latency of a Global Catalog (GC) with every other DC. *Policy Name:* ADSPI-Rep_GC_Check_and_Threshold	Instance Name - DNS name of the DC with which the GC has been replicated	UTF8
	LatencyDelta - Replication latency in seconds	REAL64
ADSPI_LOGDISKSIZE This table has data on the drive hosting the DIT log files. *Policy Name:* ADSPI-DIT_LogFilesPercentFull	Instance Name - DIT log file path	UTF8
	InstanceValue - Size (in MB) of the drive containing DIT log files	REAL64
ADSPI_LOGPERCENTFULL This table has data on the drive hosting the DIT log files. *Policy Name:* ADSPI-DIT_LogFilesPercentFull	Instance Name - DIT log file path	UTF8
	InstanceValue - Percentage of used space of the drive containing DIT log files	REAL64

ADSPI_LOGQUEUELENGTH This table has data on the drive hosting the DIT log files. *Policy Name:* ADSPI-DIT_LogFilesQueueLength	Instance Name - DIT log file path	UTF8
	InstanceValue - Average disk queue length of the drive containing the DIT log files	REAL64
ADSPI_NTDS This table has data on the Microsoft Active Directory performance, especially replication activity. *Policy Name:* ADSPI_Logging	DRAInboundBTS - Total number of bytes per second received through replication. It is the sum of the number of bytes of uncompressed data and compressed data	REAL64
	DRAOutboundBCSec - Uncompressed size in bytes of compressed replication data outbound to DCs in other sites per second	
	DSThreadsinUse - Current number of threads in use by the directory service. This counter represents the number of threads currently servicing the clients.	
	DRAInboundBCSec - Uncompressed size in bytes of compressed replication data inbound from DCs in other sites per second	
	DRAOutboundBTS - Total number of bytes sent per second. It is the sum of the number of bytes of uncompressed data and compressed data	
	DRAInboundBNCWSSec - Uncompressed size in bytes of replication data that was not compressed at the source - inbound from other DCs in the same site per second	
	DRAOutboundBNCWSSec -	

	Uncompressed size in bytes of outbound replication data that was not compressed site - outbound to DCs in the same site per second	
ADSPI_NTDSP This table has data on the LSASS process.The LSASS process is responsible for management of local security authority domain authentication and Microsoft Active Directory management. *Policy Name:* ADSPI_Logging	% Processor Time - Percentage of time that the processor spent executing a non-idle thread of LSASS process	REAL64
	PageFaultsSec - Rate, in incidents per second, of LSASS process, at which page faults were handled by the processor	
	WorkingSet - Size (in bytes) of the working set of LSASS process	
ADSPI_REPLATENCY This table contains replication statistics. A DC has connection objects to one or more DCs.The statistics relates to replication from all these DCs to the DC on which the policy which is running is logged. Latency is the time delay between the moment a change has occured on source DC till the change reaches the destination DC. *Policy Name:* ADSPI-Rep_MonitorIntraSiteReplication and ADSPI-Rep_MonitorInterSiteReplication	LATENCYMIN - Minimum latency experienced during replication from all Dcs to which a connection object exists	REAL64
	LATENCYMAX - Maximum latency experienced during replication from all Dcs to which a connection object exists	
	LATENCYAVG - Average of latencies experienced during replication from all Dcs to which a connection object exists	
	LASTREPDELTAMIN - Minimum among time interval between current time and last replication time for all the DCs with Connection Objects	
	LASTREPDELTAMAX - Maximum among time interval between current time and last replication time for all the DCs with Connection Objects	

	LASTREPDELTAAVG - Average of time interval between current time and last replication time for all the DCs with Connection Objects	
	LASTREPTIME - Time elapsed, in hours, since the last change to the OvReplication object of the Source DC occured	
ADSPI_RESPONSETIME This table has data on the availability, bind time, and query time of the DC. It also indicates whether a GC is present on the DC and if it is present, the bind and query times of the GC are also logged. *Policy Name:* ADSPI-Response_Logging	BINDTIME - Time, in seconds, required to bind to the Microsoft Active Directory on DC	REAL64
	QUERYTIME - Time, in seconds, required to query the Microsoft Active Directory on DC	REAL64
	GCBINDTIME - Time required to bind to GC in seconds	REAL64
	GCQUERYTIME - Time required to query GC in seconds	REAL64
	GCPRESENT - Indicates one if a GC is present on the DC, else it is zero	I32
	AVAILABILITY - Indicates one if the DC is reachable, else, it is zero	I32
	GCAVAILABILITY - Indicates one if the GC is reachable, else, it is 0	I32
ADSPI_SITE This table contains the name of the site in which the DC is located. *Policy Name:* ADSPI-DIT_TotalDitSize	SiteName - Always indicates the value "SiteName"	UTF8
	SiteValue - Name of the site in which the DC is located	
ADSPI_SYSVOLPTFULL This table has data on the drive hosting the SYSVOL. The SYSVOL contains the changes that have to be replicated to	Instance Name - Sysvol directory path	UTF8

the other DCs. Sysvol is also the place where changes from other DCs are received. *Policy Name:* ADSPI-Sysvol_PercentFull	InstanceValue - Percentage of used space of the drive hosting Sysvol	REAL64
ADSPI_TIMESYNC The table contains the time difference between the DC and the time master.The time master is usually the root pdc, but in case if the contact is not established, the domain pdc is considered to be the time master *Policy Name:* ADSPI-Rep_TimeSync_Monitor	TIMESYNC - Time difference in seconds between the time master and the DC	REAL64
ADSPI_TRUST This table has data on the trust relationships between the domains in the Microsoft Active Directory forest. *Policy Name:* ADSPI_Trust_Mon_Modify and ADSPI-Trust_Mon_Add_Del	Change Type - Indicates zero for addition of trust, one for deletion of trust, and two for modification of a trust	I32
	Trusting Domain - Name of the trusting domain	UTF8
	Trusted Domain - Name of trusted domain	UTF8
	Trust Attributes - Can be a combination of the following values: 0x1 forNontransitive, 0x2 for Uplevel clients only, 0x40000 for Tree parent, and 0x80000 for Tree root	I32
	Trust Direction - Indicates one for inbound, two for outbound, and three for bi-directional trust relationship	I32
	Trust Status - Indicates zero if there is no trust failure, else it contains the error code	I32
	Trust String - Gives a description of the trust status	UTF8
	Trust Type - Indicates one for an uplevel trust, two for downlevel trust, three for Kerberos realm trust, and four for DCE	I32

ADSPI_DNSSR This table contains the response time of the DNS server and a metric to indicate whether the DNS server is a DC or not. *Policy Name:* ADSPI-DNS_Server_Response	IsDomainController - Set to one if the DNS server is a domain controller, and set to zero if it is not.	REAL64
	ResponseTime - Response time of the DNS server in milliseconds	
ADSPI_INBOUND This table contains the number of objects received by the DC through inbound replication. *Policy Name:* ADSPI-Rep_InboundObjs *or* ADSPI-Rep_InboundObjs_2k8+ (As per node type)	_InstanceName - Indicates the value by default *	UTF8
	Objects - Shows the number of objects received from neighbors through inbound replication. A neighbor is a DC from which the local DC replicates locally	REAL64
ADSPI_SCHEMAMISMATCH This table contains data on the failure of synchronization requests made to neighboring domain controllers. *Policy Name:* ADSPI_SyncSchemaMissMatch and ADSPI_SyncSchemaMissMatch_2K8+	Instance Name - Name of the instance for which data is logged.	UTF8
	SchemaMismatchCnt - Number of sync requests made to the neighbors that failed because their schema are out of sync.	UINT32

Golden Metrics

Golden metrics are a set of metrics that are basic and fundamental for monitoring the Microsoft Active Directory environment. You can deploy the policies listed in the following table to ensure smooth functioning of the Microsoft Active Directory SPI.

The golden metrics cover the critical areas for which you want to receive messages as a critical or major event occuring on the Microsoft Active Directory. Implementing golden metrics and taking action against the events generated by these metrics ensure the smooth functioning of the Microsoft Active Directory.

Prerequisites for Implementing Golden Metrics

Ensure that the following requirements are fulfilled before you deploy the golden metrics:

1. SPI Data Collector Instrumentation category is deployed.
2. ADSPI_CreateDataSources policy is deployed
3. Basic Discovery and Advanced Discovery policies are deployed

Data Store Details

Metric Type	Policy	Metrics
DIT Monitoring	ADSPI-DIT_DITPercentFull / ADSPI-DIT_DITPercentFull_2k8+	DIT Disk Health
	ADSPI-DIT_LogfilesPercentFull / ADSPI-DIT_LogfilesPercentFull_2k8+	
	ADSPI-DIT_TotalDITSize / ADSPI-DIT_TotalDITSize_2k8+	
	ADSPI-DIT_LogfilesQueueLength / ADSPI-DIT_LogfilesQueueLength_2k8+	
	ADSPI-DIT_DITQueueLength / ADSPI-DIT_DITQueueLength_2k8+	
DNS Monitoring	ADSPI-DNS_DC_A_Chk / ADSPI-DNS_DC_A_Chk_2k8+	DC Records on DNS

	ADSPI-DNS_DC_CName_Chk / ADSPI-DNS_DC_CName_Chk_2k8+	
	ADSPI-DNS_DC_Response / ADSPI-DNS_DC_Response_2k8+	
	ADSPI-DNS_GC_A_Chk / ADSPI-DNS_GC_A_Chk_2k8+	
	ADSPI-DNS_GC_SRV_CHK / ADSPI-DNS_GC_SRV_CHK_2k8+	
	ADSPI-DNS_LDAP_SRV_Chk / ADSPI-DNS_LDAP_SRV_Chk_2k8+	
	ADSPI-DNS_Server_Response / ADSPI-DNS_Server_Response_2k8+	
FSMO Monitoring	ADSPI-FSMO_NAMING_Ping / ADSPI-FSMO_NAMING_Ping_2k8+	FSMO Response Times
	ADSPI-FSMO_NAMING_Bind / ADSPI-FSMO_NAMING_Bind_2k8+	
	ADSPI-FSMO_INFRA_Ping / ADSPI-FSMO_INFRA_Ping_2k8+	
	ADSPI-FSMO_INFRA_Bind / ADSPI-FSMO_INFRA_Bind_2k8+	
	ADSPI-FSMO_PDC_Ping / ADSPI-FSMO_PDC_Ping_2k8+	
	ADSPI-FSMO_PDC_Bind / ADSPI-FSMO_PDC_Bind_2k8+	
	ADSPI-FSMO_RID_Bind / ADSPI-FSMO_RID_Bind_2k8+	
	ADSPI-FSMO_RID_Ping / ADSPI-FSMO_RID_Ping_2k8+	
Replication Monitoring	ADSPI-Rep_ModifyObj / ADSPI-Rep_ModifyObj_2k8+	Replication Status
	ADSPI-Rep_Modify_User_Object / ADSPI-Rep_Modify_User_Object_2k8+	

	ADSPI-Rep_MonitorInterSiteReplication / ADSPI-Rep_MonitorInterSiteReplication_2k8+	
	ADSPI-Rep_MonitorIntraSiteReplication / ADSPI-Rep_MonitorIntraSiteReplication_2k8+	
	ADSPI-Rep_ISM_Chk / ADSPI-Rep_ISM_Chk_2k8+	
	ADSPI-Rep_GC_Check_and_Threshold / ADSPI-Rep_GC_Check_and_Threshold_2k8+	
Response Time Monitoring	ADSPI-Response Time_GCQuery / ADSPI-Response Time_GCQuery_2k8+	DC and GC Response Times
	ADSPI-ResponseTime_Bind / ADSPI-ResponseTime_Bind_2k8+	
	ADSPI-ResponseTime_GCBind / ADSPI-ResponseTime_GCBind_2k8+	
	ADSPI-ResponseTime_Query / ADSPI-ResponseTime_Query_2k8+	
SysVol Monitoring	ADSPI-Sysvol_Connectivity / ADSPI-Sysvol_Connectivity_2k8+	Sysvol Health
	ADSPI-Sysvol_FRS / ADSPI-Sysvol_FRS_2k8+	
	ADSPI-SysVol_PercentFull / ADSPI-SysVol_PercentFull_2k8+	
Health Monitor	ADSPI_FwdAllWarnErrorDS / ADSPI_FwdAllWarnErrorDS_2k8+	AD Processes Health
	ADSPI_FwdAllWarnErrorFRS / ADSPI_FwdAllWarnErrorFRS_2k8+	
	ADSPI_HMLSASSPageFaults / ADSPI_HMLSASSPageFaults_2k8+	
	ADSPI_HMLSASSPrivateBytes / ADSPI_HMLSASSPrivateBytes_2k8+	
	ADSPI_HMLSASSProcessorTime / ADSPI_HMLSASSProcessorTime_2k8+	
	ADSPI_HMLSASSWorkingSet / ADSPI_HMLSASSWorkingSet_2k8+	

	ADSPI_HMNTFRSPageFaults / ADSPI_HMNTFRSPageFaults_2k8+	
	ADSPI_HMNTFRSPrivateBytes / ADSPI_HMNTFRSPrivateBytes_2k8+	
	ADSPI_HMNTFRSProcessorTime / ADSPI_HMNTFRSProcessorTime_2k8+	
	ADSPI_HMNTFRSWorkingSet / ADSPI_HMNTFRSWorkingSet_2k8+	
	ADSPI_KDC / ADSPI_KDC_2k8+	
	ADSPI_NetLogon / ADSPI_NetLogon_2k8+	
	ADSPI_NTFRS	
Index and Query Monitor	ADSPI_IQLDAPBindTime / ADSPI_IQLDAPBindTime_2k8+	LDAP Bind Time
Replication	ADSPI_ADSPendingSynchronizations / ADSPI_ADSPendingSynchronizations_2k8+	Replication Statistics
	ADSPI_ADSRepInBoundBytesBetweenSites / ADSPI_ADSRepInBoundBytesBetweenSites_2k8+	
	ADSPI_ADSRepInBoundBytesWithinSites / ADSPI_ADSRepInBoundBytesWithinSites_2k8+	
	ADSPI_ADSRepInBoundObjectUpdatesRemaining /ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+	
	ADSPI_ADSRepNotifyQueueSize / ADSPI_ADSRepNotifyQueueSize_2k8+	
Securities	ADSPI_KDCFailureGrantTicket / ADSPI_KDCFailureGrantTicket_2k8+	Security
	ADSPI_PrivilegedAccounts / ADSPI_PrivilegedAccounts_2k8+	
	ADSPI_SecErrorsLogon / ADSPI_SecErrorsLogon_2k8+	
	ADSPI_DirComputerModif / ADSPI_DirComputerModif_2k8+	

Using Tools

The Microsoft Active Directory SPI uses different tools to monitor the Microsoft Active Directory environment.Tools are utilities to gather more Microsoft Active Directory related information. You can also launch tools to view the Microsoft Active Directory environment:

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.

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.

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.

Related Topics:

- Getting Started with Microsoft Active Directory SPI
- Using Reports

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 Tools

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 Tools
- Using the Operations Manager Topology Viewer
- Operations Manager Topology Viewer toolbar
- Operations Manager Topology Viewer menus
- Operations Manager Topology Viewer map connections

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:

- Using Tools
- 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 Tools
- 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 Tools
- Using the HP Operations Topology Viewer
- Operations Manager Topology Viewer toolbar
- HP Operations Topology Viewer menus

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.

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 less than 5.30, as mentioned in the *Configuration Guide* . Incorrect use of the tool may lead to data loss.

Related Topics:

- Using Tools

ADS Printer Information tool

The ADS Printer Information tool lists all printers known to the Microsoft 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 Tools

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 Tools

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...** .

NOTE: Use this tool *before* you demote a DC. If you do not use the tool beforehand, you must manually remove the OVreplication object/user account (as described below).

To manually remove the OVReplication object (and user account) after you have demoted a DC:

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 Tools

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 Tools

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 might 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:

- Using Tools

Using Reports

NOTE:
See Report, Report Table, Data Store, and Policy Mapping Details to check the policy required for each report.

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 .

The Microsoft Active Directory has the following reports:

- Active Directory Memory Usage
- Active Directory Processor Usage
- Active Directory Replication Inbound
- Active Directory Replication Outbound
- Active Directory Replication Summary
- AD Domain Controller Availability
- AD DC DNS Availability Report (daily/weekly)

- AD DIT Disk Queue Length Report (weekly)
- AD DIT Disk Size Summary Report (weekly/monthly)
- AD Log Files Disk Size Summary Report (weekly/monthly)
- AD Log Files Disk Queue Length Report (weekly)
- AD DNS Server Availability Report (daily/weekly)
- AD DNS Server Memory Capacity Planning Report (weekly/monthly)
- AD Domain and Forest Changes Report (weekly and monthly)
- AD Operations Master Connection Time (sorted by FSMO or server)
- AD FSMO Role Holder (sorted by FSMO or server)
- AD GC Rep Delay Times By GC/DC (weekly/monthly)
- AD GC Replication Delay Times by DC/GC (weekly/monthly)
- AD GC Response Time Report (weekly/monthly)
- AD Size of Sysvol Report (weekly/monthly)

Related Topics:

- Reports, Report Table, Data Store, and Policy Mapping Details

AD DC DNS Availability Report (daily/weekly)

The AD DC DNS Availability (daily/weekly) report summarizes the availability of the DC'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 7 day period.

Report Template File Name: g_ADDNSDCAvailDaily.rpt/g_ADDNSDCAvailWeekly.rpt

Report contents:

The report columns are as follows:

Column Name	Description
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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DNS_DC_Response policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- RESPTIME
- SYSTEMNAME

Reporter Table: ADSPI_DNS_DCRESP

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD DC DNS Availability report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD DIT Disk Queue Length Report (weekly)

The AD DIT Disk Queue Length Report (weekly) report summarizes the weekly queue length patterns of the disk holding the Directory Information Tree (DIT) for the DCs. This information helps to identify the DCs with potential disk bottlenecks.

Report Template File Name: g_ADDITQueueLengthWeekly.rpt

Report contents:

The columns of this report are defined as follows:

Column Name	Description
System Name	Specifies the name of the DC.
Domain Name	Name of the Domain that the DC 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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DIT_DITQueueLength policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- DATETIME
- DITQLNAME
- DITQLVALUE

Reporter Table: This report has following reporter table:

- ADSPI_Domain
- ADSPI_Site
- ADSPI_DITQUEUELENGTH

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD DIT Disk Queue Length report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD DIT Disk Size Summary Report (weekly/monthly)

This bar chart (weekly) and line chart (monthly) AD DIT Disk Size Summary report summarizes the usage patterns of the disk holding the DIT for the DCs. This information helps to identify DCs with potential disk bottlenecks.

Report Template File Name: g_ADDITDiskSpaceWeekly.rpt/ g_ADDITDiskSpaceMonthly.rpt

Report contents:

The chart shows the average percentage DIT disk space full on each DC. 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:

Column Name	Description
System Name	Specifies the name of the DC
Domain Name	Name of the Domain that the DC 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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DIT_TotalDitSize policy (for DSPI_DITDatabaseSize, ADSPI_Domain, and ADSPI_Site) and ADSPI-DIT_DITPercentFull policy (for ADSPI_DITPercentFull) policies.

Metrics: These reports use the following metrics, which are logged into the Reporter database:

- For ADSPI_DITDatabaseSize reporter table
  - SYSTEMNAME
  - DATETIME

- INSTANCEVALUE

- For ADSPI_DITPercentFull reporter table:
  - DITPTVALUE
- For ADSPI_Domain reporter table:
  - DOMAINVALUE
- For ADSPI_Site reporter table:
  - SITEVALUE

Reporter Table: These reports have the following reporter tables:

- ADSPI_DITDatabaseSize
- ADSPI_DITPercentFull
- ADSPI_Domain
- ADSPI_Site

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD DIT Disk Size Summary report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD DNS Server Memory Capacity Planning Report (weekly/monthly)

The AD DNS Server Memory Capacity Planning Report (weekly/monthly) report graphs the memory capacity for each specified DNS server running the Microsoft 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 Template File Name:
g_ADDNSSrvMemCapPlanMonthly.rpt/g_ADDNSSrvMemCapPlanWeekly.rpt

Report contents:

This report provides one graph for each specified DNS server with Microsoft 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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DNS_LogDNSPagesSec policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- PAGESPERSEC
- ISDOMAINCTRL
- SYSTEMNAME

Reporter Table: ADSPI_DNSSP

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD DNS Server Memory Capacity Planning report.

Related Topics:

- Using Reports

- Report, Report Table, Data Store, and Policy Mapping Details

AD DNS Server Availability Report (daily/weekly)

The AD DNS Server Availability report summarizes the availability of DNS servers with Microsoft 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 Template File Name: g_ADDNSSrvAvailDaily.rpt/g_ADDNSSrvAvailWeekly.rpt

Report contents:

This 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:

Column Name	Description
Response Time in miliseconds	Provides the response time of the DNS server in miliseconds.
Date time	Date and time when the data was gathered.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DNS_Server_Response policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- RESPONSETIME
- ISDOMAINCONTROLLER
- SYSTEMNAME

Reporter Table: ADSPI_DNSSR

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD DNS Server Availability report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Domain Controller Availability

AD Domain Controller Availability report displays the percentage of time Microsoft 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 Microsoft Active Directory.

Report Template File Name: g_ADDCAvailability.rpt

Report contents:

This report displays two pie charts:

- *Active Directory Availability:* The Microsoft Active Directory SPI periodically queries the directory on your DC to determine response time and availability. This graph shows the percentage of time the directory was successfully contacted.
- *Active Directory Global Catalog Availability:* The Microsoft Active Directory Global Catalog is queried on the port 3268. The success of the attempt is used to calculate Global Catalog availability.

The report columns are as follows:

Column Name	Description
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.
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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-Response_Logging policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- AVAILABILITY
- GCAVAILABILITY
- DATETIME

Reporter Table: ADSPI_RESPONSEMON

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Domain Controller Availability report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Domain and Forest Changes Report (weekly and monthly)

The AD Domain and Forest Changes Report (weekly and monthly) report presents the domain and forest trust changes in Microsoft Active Directory for the selected report: either weekly or monthly. This report provides information illustrating addition, deletion, and modification of trusts on Windows Server 2003 and 2008 Domain Controllers.

Report Template File Name:
g_ADDomainForestTrustMonthly.rpt/g_ADDomainForestTrustWeekly.rpt

Report contents:

In the report, a table displays the following details:

Column Name	Description
System Name	Name of the DC
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 - Disallow Transitivity • 2 - Uplevel clients only • 4 - The trust setting to another tree root in the forest • 32 - The trust setting to the parent in the organization tree
Direction	A value that indicates the direction of Trust: • 1 - Inbound

	• 2 - Outbound • 3 - Bi-directional
Trust Status	String description of trust status.
Trust Type	A value that indicates the type of the trust relationship: • 1 - Downlevel • 2 - Uplevel • 3 - Non-Windows Kerberos Realm • 4 - DCE

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-Trust_Mon_Add_Del and ADSPI-Trust_Mon_Modify policies.

Metrics: These reports use the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- DATETIME
- CHANGETYPE
- TRUSTINGDOMAIN
- TRUSTEDDOMAIN
- TRUSTATTRIBUTES
- TRUSTDIRECTION
- TRUSTSTATUS
- TRUSTSTATUSSTRING
- TRUSTTYPE

Reporter Table: ADSPI_TRUST

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Domain and Forest Changes report.

Related Topics:

- Using Reports

- Report, Report Table, Data Store, and Policy Mapping Details

AD GC Replication Delay Times by DC/GC (weekly/monthly)

The AD GC Replication Delay Times by DC/GC (weekly/monthly) report summarizes delay times for replication from DCs 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 Template File Name: g_ADDCGCweekly.rpt/g_ADDCGCmonthly.rpt

Report contents:

This report displays a bar graph showing the average replication delay per global catalog server for every DC.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-Rep_GC_Check_and_Threshold policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- GCREPNAME
- LATENCYDELTA
- DATETIME

Reporter Table: ADSPI_REP_GC

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD GC Replication Delay Times by DC/GC report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD GC Rep Delay Times By GC/DC (weekly/monthly)

The AD GC Rep Delay Times By GC/DC (weekly/monthly) report summarizes delay times for replication from a global catalog server to each DC. 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 Template File Name: g_ADGCDCweekly.rpt/g_ADGCDCmonthly.rpt

Report contents:

This report displays a bar graph showing the average replication delay per DC for every global catalog server.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-Rep_GC_Check_and_Threshold policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- SYSTEMNAME
- GCREPNAME
- LATENCYDELTA

Reporter Table: ADSPI_REP_GC

See Troubleshooting Microsoft Active Directory Reports for troubleshootingAD GC Rep Delay Times By GC/DC report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD GC Response Time Report (weekly/monthly)

The AD GC Response Time Report (weekly/monthly) 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 Template File Name:
g_ADGCResponseTimeWeekly.rpt/g_ADGCResponseTimeMonthly.rpt

Report Contents

This 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.

Other details of this report are:

Required Policies: For this report to work properly, deploy the ADSPI-Response_Logging policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- DATETIME
- GCBINDTIME
- GCQUERYTIME
- GCPRESENT

Reporter Table: ADSPI_RESPONSEMON

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD GC Response Time report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Log Files Disk Queue Length Report (weekly)

The AD Log Files Disk Queue Length Report (weekly) report summarizes the weekly queue length patterns of the disk holding the Microsoft Active Directory log files for the DCs. This information helps to identify DCs with potential disk bottlenecks.

Report Template File Name: g_ADLogQueueLengthWeekly.rpt/ g_ADLogQueueLengthMonthly.rpt

Report contents:

The columns of this report are defined as follows:

Column Name	Description
System Name	Specifies the name of the DC
Domain Name	Name of the Domain that the DC 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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DIT_TotalDitSize policy (for ADSPI_Domain and ADSPI_Site) and ADSPI-DIT_LogFilesQueueLength policy (for ADSPI_LOGQUEUELENGTH).

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- For ADSPI_Domain reporter table:
  - DATETIME
  - SYSTEMNAME
  - DOMAINVALUE

- For ADSPI_Site reporter table:
  - SITEVALUE
- For ADSPI_LOGQUEUELENGTH report tables:
  - SYSTEMNAME
  - DATETIME
  - LGQLENNAME
  - LGQLENVALUE

Reporter Table: This report has the following reporter tables:

- ADSPI_Domain
- ADSPI_Site
- ADSPI_LOGQUEUELENGTH

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Log Files Disk Queue Length report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Log Files Disk Size Summary Report (weekly/monthly)

The AD Log Files Disk Size Summary Report (weekly/monthly) report summarizes the weekly and monthly usage of the disk holding the Microsoft Active Directory log files for the DCs. This information helps to identify DCs with potential disk bottlenecks.

Report Template File Name: g_ADLogFilesDiskSpaceWeekly.rpt/ g_ADLogFilesDiskSpaceMonthly.rpt

Report contents:

The columns of this report are defined as follows:

Column Name	Description
System Name	Specifies the name of the DC
Domain Name	Name of the Domain that the DC belongs to.
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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-DIT_LogFilesPercentFull policy (for ADSPI_LogDiskSize and ADSPI_LOGPERCENTFULL) and ADSPI-DIT_TotalDitSize policy (for ADSPI_DOMAIN and ADSPI_SITE).

Metrics: These reports use the following metrics, which are logged into the Reporter database:

- For ADSPI_LogDiskSize reporter table:
  - DATETIME
  - SYSTEMNAME
- For ADSPI_LOGPERCENTFULL reporter table:

- LGPERFULLVALUE

- For ADSPI_DOMAIN reporter table:
  - DOMAINVALUE
  - For ADSPI_SITE reporter table:
  - SITEVALUE

Reporter Table: These reports have the following reporter tables:

- ADSPI_LogDiskSize
- ADSPI_LOGPERCENTFULL
- ADSPI_DOMAIN
- ADSPI_SITE

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Log Files Disk Size Summary report .

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Memory Usage

AD Memory Usage report examines the Microsoft Active Directory memory-usage pattern from the logged data and displays the general patterns of memory usage between DCs.

Report Template File Name: g_ADMemoryUsage.rpt

Report contents:

This report presents two sections:

- *Active Directory LSASS Page Faults Average:* Displays usage patterns for Microsoft 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 processor. 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:* Displays usage patterns for Microsoft 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 used. If the free memory falls below the threshold, pages are removed from working sets.

Other details of this report are:

Required Policies: For this report to work properly, deploy the ADSPI_Logging policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- SYSTEMNAME
- WORKINGSET
- PAGEFAULTSSEC

Reporter Table: ADSPI_NTDSP

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Memory Usage report.

Related Topics:

- Using Reports

- Report, Report Table, Data Store, and Policy Mapping Details

AD Operations Master Connection Time (sorted by FSMO or server)

The AD Operations Master Connection Time (sorted by FSMO or server) report provides a graph of the ping time and bind time for Operations Masters services from a specified DC. Ping time measures the network connection time. Bind time measures the time between the ping connection and the connection to the targeted Microsoft Active Directory service.

Report Template File Name: g_ADOpMstrConTimeByFsmo.rpt/g_ADOpMstrConTimeBySvr.rpt

This report is sorted by:

- FSMO type, and then by DC or
- Server, and then by DC

There is one graph by FSMO service/DC.

Report contents:

The report graph displays the following Microsoft 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)

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-FSMO_Logging policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- GMT
- DATETIME
- FSMO
- PINGTIME
- SERVER

- FSMOBINDTIME

Reporter Table: ADSPI_FSMO_MET

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Operations Master Connection Time report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD FSMO Role Holder (sorted by FSMO or server)

The AD FSMO Role Holder (sorted by FSMO or server) report provides a graph of the ping time and bind time for Operations Masters services from a specified DC. Ping time measures the network connection time. Bind time measures the time between the ping connection and the connection to the targeted Microsoft Active Directory service.

This report is sorted by:

- FSMO type, and then by DC or
- Server, and then by DC

There is one graph by FSMO service/domain controller.

Report Template File Name:
g_ADFSMORoleHolderMovWeekly.rpt/g_ADFSMORoleHolderMovMonthly.rpt

Report contents:

The report graph displays the following Microsoft 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)

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-FSMO_RoleMvmt policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- DATETIME
- FSMORM
- ISROLEHOLDER

Reporter Table: ADSPI_FSMO_ROLEMVMT

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD FSMO Role Holder report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Processor Usage

AD Processor Usage report examines the Microsoft Active Directory processor-usage pattern from the logged data. This report displays general usage patterns between DCs.

Report Template File Name: g_ADProcessUsage.rpt

Report contents:

This report presents two sections:

- *Active Directory Average LSASS Percent Processor Time/sec:* 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:* Displays the average usage patterns for Microsoft 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 serve the client API calls.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI_Logging policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- SYSTEMNAME
- DSTHREADSINUSE

Reporter Table: ADSPI_NTDS

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Processor Usage report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Replication Inbound

AD Replication Inbound report examines the Microsoft Active Directory replication usage pattern from the logged data. This report allocates the replication-transmission statistics of intra-site replication and replication among different sites and shows the usage pattern of inbound Microsoft Active Directory replication.

Report Template File Name: g_ADReplicationInbound.rpt

Report contents:

This 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 Microsoft Active Directory service for all monitored nodes.

Other details of this report are:

Required Policies: For this report to work properly, deploy ADSPI_Logging policy.

Metrics: This report uses the following metrics, which are logged into Reporter database:

- DATETIME
- SYSTEMNAME
- DRAINBOUNDBCSEC
- DRAINBOUNDBSNCWSSEC

Report Table: ADSPI_NTDS See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Replication Inbound report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Replication Outbound

AD Replication Outbound report examines the Microsoft Active Directory replication usage pattern from the logged data. This report allocates the replication-transmission statistics of intra-site replication and replication among different sites and shows the usage pattern of outbound Microsoft Active Directory replication.

Report Template File Name: g_ADReplicationOutbound.rpt

Report contents:

This 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 Microsoft Active Directory Service for all monitored nodes.

Other details of this report are:

Required Policies: For this report to work properly, deploy the ADSPI_Logging policy.

Metrics: This report uses the following metrics, which are logged into Reporter database:

- DATETIME
- SYSTEMNAME
- DRAOUTBOUNDBCSEC
- DRAOUTBOUNDBNCWSSEC

Reporter Table: ADSPI_NTDS See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Replication Outbound report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Replication Summary

AD Replication Summary report examines the Microsoft Active Directory replication usage pattern from the logged data. This report allocates the replication-transmission statistics intra-site replication and replication among different sites and shows an overall usage pattern of Microsoft Active Directory replication.

Report Template File Name: g_ADReplicationSummary.rpt

Report contents:

This 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.

This 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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI_Logging policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- DATETIME
- SYSTEMNAME
- DRAINBOUNDBTS
- DRAOUTBOUNDBTS

Reporter Table: ADSPI_NTDS

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Replication Summary report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

AD Size of Sysvol Report (weekly/monthly)

The AD Size of Sysvol Report (weekly/monthly) report provides a weekly summary of the Sysvol (system volume shared directory on the Domain Controller) disk space information for the specified DC.

Report Template File Name: g_ADSizeOfSysvolWeekly.rpt/g_ADSizeOfSysvolMonthly.rpt

Report contents:

The report presents a line graph indicating the percentage of occupied disk space on sysVol drives. The report columns are as follows:

Column Name	Description
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.

Other details of this report are:

Required Policies: For this report to work properly deploy ADSPI-Sysvol_PercentFull policy.

Metrics: This report uses the following metrics, which are logged into the Reporter database:

- SYSTEMNAME
- DATETIME
- SYSPERCNAME
- SYSPERCVALUE

Reporter Table: ADSPI_SYSVOL_PCT_FULL

See Troubleshooting Microsoft Active Directory Reports for troubleshooting AD Size of Sysvol report.

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

Troubleshooting Microsoft Active Directory SPI Reports

If any of the report is not being generated or if it is empty, perform the following tasks:

1. **Check the Reporter database.**
    1. Check if the data is available in the Reporter database.
    2. Check the Reporter database on the HP Reporter server.
    3. Run the respective SQL command to see if data for a particular metric is being collected. See the table below for the particular SQL command for each report.
    4. If there is data in the Reporter database for every metric listed and the Reporter trace files do not reveal the cause of the problem, contact the HP Support Team.
    5. If the data for some or all of the metrics are missing from the Reporter database, perform the next task.

2. **Check the reporter package installation.**
    1. Make sure that the ADSPI Reporter package was installed on the HP Reporter server.
    2. Check for errors in the Reporter Status pane.
    3. If there are Reporter installation errors, report the problem.

3. **Check the data store.**
    1. If there is no data in the Reporter database and the ADSPI Reporter package is installed properly, check that the data is being collected or logged on the managed node into the data store (CODA or HP Performance Agent).
    2. If you are use CODA, run the following CODA diagnostic command on the managed node to get the last logged record:
        - On HTTPS managed nodes:
          ```
          ovcodautil -dumpds ADSPI
          ```
        - On DCE managed nodes:
          ```
          codautil -dumpds ADSPI
          ```
    3. 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 the following command:
        - On HTTPS-managed nodes:

```
ovc -start -id 12
```

- On DCE-managed nodes:
```
opcagt -start -id 12
```

4. Check that the acknowledged messages queue was acknowledged.
5. If you are using the HP Performance Agent, refer to the HP Performance Agent documentation.

4. **Check if the policies have been deployed.**

   There will be no data unless the particular policy for each report is deployed. See Report, Report Table, Data Store, and Policy Mapping Details table to know the relevant policy for each report. Check on the managed node to ensure that the policy was deployed and is enabled by running the commands:

   - On DCE nodes
   ```
   opctemplate
   ```
   - On HTTPS nodes
   ```
   ovpolicy
   ```

5. **Check if the agent on the managed node is running.**
   1. Check that the HP Operations agent is running.
   2. 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
      ```
   3. 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
      ```

Report Name	SQL Command
AD DC DNS Availability Report	Select * from ADSPI_DNS_DCRESP
AD DIT Disk Queue Length Report	Select * from ADSPI_Domain
	Select * from ADSPI_Site

	Select * from ADSPI_DITQUEUELENGTH
AD DIT Disk Size Summary Report	Select * from ADSPI_DITDatabaseSize
	Select * from ADSPI_DITPercentFull
	Select * from ADSPI_Domain
	Select * from ADSPI_Site
AD DNS Server Memory Capacity Planning Report	Select * from ADSPI_DNSSP
AD DNS Server Availability Report	Select * from ADSPI_DNSSR
AD Domain Controller Availability	Select * from ADSPI_RESPONSEMON
AD Domain and Forest Changes Report	Select * from ADSPI_TRUST
AD GC Replication Delay Times by DC/GC	Select * from ADSPI_REP_GC
AD GC Rep Delay Times By GC/DC	Select * from ADSPI_REP_GC
AD GC Response Time Report	Select * from ADSPI_RESPONSEMON
AD Log Files Disk Queue Length Report	Select * from ADSPI_Domain
	Select * from ADSPI_Site
	Select * from ADSPI_LOGQUEUELENGTH
AD Log Files Disk Size Summary Report	Select * from ADSPI_LogDiskSize
	Select * from ADSPI_LOGPERCENTFULL

	Select * from ADSPI_DOMAIN
	Select * from ADSPI_SITE
AD Memory Usage	Select * from ADSPI_NTDSP
AD Operations Master Connection Time	Select * from ADSPI_FSMO_MET
AD FSMO Role Holder	Select * from ADSPI_FSMO_ROLEMVMT
AD Process Usage	Select * from ADSPI_NTDS
AD Replication Inbound	Select * from ADSPI_NTDS
AD Replication Outbound	Select * from ADSPI_NTDS
AD Replication Summary	Select * from ADSPI_NTDS
AD Size of Sysvol Report	Select * from ADSPI_SYSVOL_PCT_FULL

Related Topics:

- Using Reports
- Report, Report Table, Data Store, and Policy Mapping Details

Report, Report Table, Data Store, and Policy Mapping Details

The Microsoft Active Directory SPI creates the following data tables in the data store on the node to facilitate the data-collection procedure. The data store class creator for all the reports isadspi_ddf.bat.

Data Store and Report Details

Report Name	Report Table	Report Table Attributes	Spec File	Data Store Class Name	Policy Logging Data
g_ADDC Availability.rpt *Report Content:* AD Domain Controller Availability	ADSPI_ RESPONSE MON	SYSTEM NAME	ADSPI_ RESP ONSE TIME.spec	ADSPI_ RESPONSE TIME	ADSPI-Response _Logging
		AVAIL ABILITY			
		GC AVAIL ABILITY			
		DATETIME			
g_ADDCGC monthly.rpt *Report Content:* AD GC Rep Delay Times By DC/GC - Monthly	ADSPI_REP _GC	SYSTEM NAME	ADSPI_ GCREP .spec	ADSPI_GC REP	ADSPI-Rep_ GC_Check _and _Threshold
		GCREP NAME			
		LATENCY DELTA			
		DATETIME			
g_ADDCGC weekly.rpt *Report Content:*	ADSPI_REP _GC	SYSTEM NAME	ADSPI_ GCREP .spec	ADSPI_GC REP	ADSPI-Rep_ GC_Check _and

Report Content: AD GC Rep Delay Times By DC/GC - Weekly		GCREP NAME			_Threshold
		LATENCY DELTA			
		DATETIME			
g_ADDITDiskSpaceMonthly.rpt *Report Content:* AD DIT Disk Size Summary - Monthly	ADSPI_DIT Database Size	SYSTEM NAME	ADSPI_DIT DATA BASE SIZE.spec	ADSPI_DIT DATABASE SIZE	ADSPI-DIT_ TotalDitSize
		DATETIME			
		INSTANCE VALUE			
	ADSPI_DIT PercentFull	DITPT VALUE	ADSPI_DIT PERCENT FULL.spec	ADSPI_DIT PERCENT FULL	ADSPI-DIT_ DITPercent Full
	ADSPI_ Domain	DOMAIN VALUE	ADSPI_ DOMAIN .spec	ADSPI_ DOMAIN	ADSPI-DIT_ TotalDitSize
	ADSPI_Site	SITEVALUE	ADSPI _SITE .spec	ADSPI_SITE	ADSPI-DIT_ TotalDitSize
g_ADDITDiskSpaceWeekly.rpt *Report Content:* AD DIT Disk Size Summary - Weekly	ADSPI_DIT Database Size	SYSTEM NAME	ADSPI_DIT DATA BASE SIZE.spec	ADSPI_DIT DATABASE SIZE	ADSPI-DIT_ TotalDitSize
		DATETIME			
		INSTANCE VALUE			
	ADSPI_DIT PercentFull	DITPTVALUE	ADSPI_DIT PERCENT FULL.spec	ADSPI_DIT PERCENT FULL	ADSPI-DIT_ DITPercent Full
	ADSPI_ Domain	DOMAIN VALUE	ADSPI_ DOMAIN .spec	ADSPI_ DOMAIN	ADSPI-DIT_ TotalDitSize

	ADSPI_Site	SITEVALUE	ADSPI_SITE.spec	ADSPI_SITE	ADSPI-DIT_TotalDitSize
g_ADDITQueueLengthWeekly.rpt *Report Content:* AD DIT Disk Queue Length - Weekly	ADSPI_Domain	SYSTEMNAME	ADSPI_DOMAIN.spec	ADSPI_DOMAIN	ADSPI-DIT_TotalDitSize
		DATETIME			
		DOMAINVALUE			
	ADSPI_Site	SITEVALUE	ADSPI_SITE.spec	ADSPI_SITE	ADSPI-DIT_TotalDitSize
	ADSPI_DITQUEUELENGTH	SYSTEMNAME	ADSPI_DITQUEUELENGTH.spec	ADSPI_DITQUEUELENGTH	ADSPI-DIT_DITQueue Length
		DATETIME			
		DITQLNAME			
		DITQLVALUE			
g_ADDNSDCAvailDaily.rpt *Report Content:* AD DC DNS Availability Report - Daily Summary	ADSPI_DNS_DCRESP	DATETIME	ADSPI_DNSDR.spec	ADSPI_DNSDR	ADSPI-DNS_DC_Response Policy
		RESPTIME			
		SYSTEMNAME			
g_ADDNSDCAvailWeekly.rpt *Report Content:* AD DC DNS Availability Report - Weekly	ADSPI_DNS_DCRESP	DATETIME	ADSPI_DNSDR.spec	ADSPI_DNSDR	ADSPI-DNS_DC_Response Policy
		RESPTIME			

Summary		SYSTEM NAME			
g_ADDNSSrv AvailDaily.rpt *Report Content:* AD DNS Server availability Report - Daily Summary	ADSPI_ DNSSR	DATETIME RESPONSE TIME ISDOMAIN CONTR OLLER SYSTEM NAME	ADSPI_ DNSSR .spec	ADSPI_ DNSSR	ADSPI-DNS_ Server_ Response
g_ADDNSSrv AvailWeekly.rpt *Report Content:* AD DC DNS Availability Report - Weekly Summary	ADSPI_ DNSSR	DATETIME RESPONSE TIME ISDOMAIN CONTR OLLER SYSTEM NAME	ADSPI_ DNSSR .spec	ADSPI_ DNSSR	ADSPI-DNS_ Server_ Response
g_ADDNSSrv MemCapPlan Monthly.rpt *Report Content:* AD DNS Server Memory Capacity Planning Report - Monthly Summary	ADSPI_ DNSSP	DATETIME PAGESPER SEC ISDOMAIN CTRL SYSTEM NAME	ADSPI_ DNSSP .spec	ADSPI_ DNSSP	ADSPI-DNS_ LogDNS Pages Sec
g_ADDNSSrv MemCapPlan	ADSPI_ DNSSP	DATETIME	ADSPI_ DNSSP	ADSPI_ DNSSP	ADSPI-DNS_ LogDNS

Weekly.rpt *Report Content:* AD DNS Server Memory Capacity Planning Report - Monthly Summary			.spec		Pages Sec
		PAGESPERSEC			
		ISDOMAINCTRL			
		SYSTEMNAME			
g_ADDomainForestTrustMonthly.rpt *Report Content:* AD Domain and Forest Trust Changes- Monthly	ADSPI_TRUST	SYSTEMNAME	ADSPI_Trustmon.spec	ADSPI_TRUST	ADSPI-Trust_Mon_Add_Del and ADSPI-Trust_Mon_Modif
		DATETIME			
		CHANGETYPE			
		TRUSTINGDOMAIN			
		TRUSTEDDOMAIN			
		TRUSTATTRIBUTES			
		TRUSTDIRECTION			
		TRUSTSTATUS			
		TRUSTSTATUSSTRING			
		TRUSTTYPE			
g_ADDomainForestTrust	ADSPI_TRUST	SYSTEMNAME	ADSPI_Trustmon	ADSPI_TRUST	ADSPI-Trust_Mon_Add

Weekly.rpt *Report Content:* AD Domain and Forest Trust Changes - Weekly		DATETIME	.spec		_Del and ADSPI -Trust _Mon _Modify
		CHANGE TYPE			
		TRUSTING DOMAIN			
		TRUSTED DOMAIN			
		TRUST ATTRI BUTES			
		TRUST DIRECTION			
		TRUST STATUS			
		TRUST STATUS STRING			
		TRUST TYPE			
g_ADFSMORole HolderMov Monthly.rpt *Report Content:* FSMO Role Holder Report - Monthly	ADSPI_ FSMO _ROLE MVMT	SYSTEM NAME	ADSPI_ FSMO_ RoleMvmt .spec	ADSPI_ FSMO _ROLE MVMT	ADSPI -FSMO _RoleMvmt
		DATETIME			
		FSMORM			
		ISROLE HOLDER			
g_ADFSMORole HolderMov Weekly.rpt *Report Content:* FSMO Role	ADSPI_ FSMO _ROLE MVMT	SYSTEM NAME	ADSPI_ FSMO_ RoleMvmt .spec	ADSPI_ FSMO _ROLE MVMT	ADSPI- FSMO _RoleMvmt
		DATETIME			

Holder Report - Weekly		FSMORM			
		ISROLE HOLDER			
g_ADGCDC monthly.rpt *Report Content:* AD GC Rep Delay Times By GC/DC - Monthly	ADSPI_ REP_GC	DATETIME	ADSPI_ GCREP .spec	ADSPI_ GCREP	ADSPI-Rep_ GC_Check _and _Threshold
		SYSTEM NAME			
		GCREP NAME			
		LATENCY DELTA			
g_ADGCDC weekly.rpt *Report Content:* AD GC Rep Delay Times By GC/DC - Monthly	ADSPI_ REP_GC	DATETIME	ADSPI_ GCREP .spec	ADSPI_ GCREP	ADSPI-Rep_ GC_Check _and _Threshold
		SYSTEM NAME			
		GCREP NAME			
		LATENCY DELTA			
g_ADGC Response TimeMonthly.rpt *Report Content:* AD GC Response Time - Monthly	ADSPI_ RESPONSE MON	SYSTEM NAME	ADSPI_ Response Time.spec	ADSPI_ RESPONSE TIME	ADSPI- Response_ Logging
		DATETIME			
		GCBIND TIME			
		GCQUERY TIME			
		GCPRESENT			
g_ADGC Response	ADSPI_ RESPONSE	SYSTEM NAME	ADSPI_ Response	ADSPI_ RESPONSE	ADSPI- Response_

TimeWeekly.rpt *Report Content:* AD GC Response Time - Weekly	MON	DATETIME	Time.spec	TIME	Logging
		GCBIND TIME			
		GCQUERY TIME			
		GCPRESENT			
g_ADLogFiles DiskSpace Monthly.rpt *Report Content:* AD Log Files Disk Size Summary - Monthly	ADSPI_Log DiskSize	DATETIME	ADSPI_ LOG DISK SIZE.spec	ADSPI_LOG DISKSIZE	ADSPI-DIT_ LogFiles PercentFull
		SYSTEM NAME			
	ADSPI_LOG PERCENT FULL	LGPERFULL VALUE	ADSPI_ LOG PERCENT FULL.spec	ADSPI_LOG PERCENT FULL	ADSPI-DIT_ LogFiles PercentFull
	ADSPI_ DOMAIN	DOMAIN VALUE	ADSPI_ DOMAIN .spec	ADSPI_ DOMAIN	ADSPI-DIT _TotalDit Size
	ADSPI_SITE	SITEVALUE	ADSPI_ SITE .spec	ADSPI_SITE	ADSPI-DIT _TotalDit Size
g_ADLogFiles DiskSpace Weekly.rpt *Report Content:* AD Log Files Disk Size Summary - Weekly	ADSPI_Log DiskSize	DATETIME	ADSPI_ LOG DISKSIZE .spec	ADSPI_LOG DISKSIZE	ADSPI-DIT_ LogFiles PercentFull
		SYSTEM NAME			
	ADSPI_LOG PERCENT FULL	LGPERFULL VALUE	ADSPI_ LOG PERCENT FULL.spec	ADSPI_LOG PERCENT FULL	ADSPI-DIT_ LogFiles PercentFull
	ADSPI_ DOMAIN	DOMAIN VALUE	ADSPI_ DOMAIN .spec	ADSPI_ DOMAIN	ADSPI-DIT _TotalDit Size
	ADSPI_SITE	SITEVALUE	ADSPI _SITE .spec	ADSPI_SITE	ADSPI-DIT _TotalDit Size
g_ADLog	ADSPI_	DATETIME	ADSPI_	ADSPI_	ADSPI-DIT

Queue Length Weekly.rpt *Report Content:* AD Log Files Disk Queue Length - Weekly	Domain	SYSTEM NAME	DOMAIN .spec	DOMAIN	_TotalDit Size
		DOMAIN VALUE			
	ADSPI_Site	SITEVALUE	ADSPI _SITE .spec	ADSPI_SITE	ADSPI-DIT _TotalDit Size
	ADSPI_LOG QUEUE LENGTH	SYSTEM NAME	ADSPI _LOG QUEUE LENGTH .spec	ADSPI_LOG QUEUE LENGTH	ADSPI-DIT_ LogFiles Queue Length
		DATETIME			
		LGQLEN NAME			
		LGQLEN VALUE			
g_ADMemory Usage.rpt *Report Content:* Active Directory Memory Usage	ADSPI_NTDSP	DATETIME	ADSPI_ NTDSP .spec	ADSPI _NTDSP	ADSPI _Logging
		SYSTEM NAME			
		WORKING SET			
		PAGE FAULTS SEC			
g_ADOpMstr ConTimeBy Fsmo.rpt *Report Content:* AD Operations Master Connection Time Report by FSMO	ADSPI_FSMO _MET	GMT	ADSPI_ FSMO .spec	ADSPI _FSMO	ADSPI-FSMO _Logging
		DATETIME			
		FSMO			
		PINGTIME			
		SERVER			
		FSMO BINDTIME			
g_ADOpMstr ConTimeBy	ADSPI_FSMO _MET	GMT	ADSPI_ FSMO	ADSPI _FSMO	ADSPI-FSMO

ConTimeBy Svr.rpt *Report Content:* AD Operations Master Connection Time Report by Server	_MET	DATETIME	FSMO .spec	_FSMO	FSMO _Logging
		FSMO			
		PINGTIME			
		SERVER			
		FSMO BINDTIME			
g_ADProcess Usage.rpt *Report Content:* Active Directory Processor Usage	ADSPI_NTDS	DATETIME	ADSPI_ NTDS .spec	ADSPI _NTDS	ADSPI _Logging
		SYSTEM NAME			
		DSTHREADS INUSE			
g_AD Replication Inbound.rpt *Report Content:* Active Directory Replication Inbound	ADSPI_NTDS	DATETIME	ADSPI_ NTDS .spec	ADSPI _NTDS	ADSPI _Logging
		SYSTEM NAME			
		DRA INBOUND BCSEC			
		DRA INBOUND BSNCWS SEC			
g_AD Replication Outbound.rpt *Report Content:* Active Directory Replication Outbound	ADSPI_NTDS	DATETIME	ADSPI_ NTDS .spec	ADSPI _NTDS	ADSPI _Logging
		SYSTEM NAME			
		DRA OUTBOUND BCSEC			

		DRA OUTBOUND BNCWSSEC			
g_AD Replication Summary.rpt *Report Content:* Active Directory Replication Summary	ADSPI_NTDS	DATETIME SYSTEM NAME DRA INBOUND BTS DRAOUT BOUNDBTS	ADSPI_ NTDS .spec	ADSPI _NTDS	ADSPI _Logging
g_ADSizeOf Sysvol Monthly.rpt *Report Content:* AD Size of Sysvol Report - Monthly Summary	ADSPI_ SYSVOL _PCT_FULL	SYSTEM NAME DATETIME SYSPERC NAME SYSPERC VALUE	ADSPI_ SYSVOL PERCENT FULL.spec	ADSPI_ SYSVOL PTFULL	ADSPI- Sysvol _Percent Full
g_ADSizeOf Sysvol Weekly.rpt *Report Content:* AD Size of Sysvol Report - Weekly Summary	ADSPI_ SYSVOL _PCT_FULL	SYSTEM NAME DATETIME SYSPERC NAME SYSPERC VALUE	ADSPI_ SYSVOL PERCENT FULL.spec	ADSPI_ SYSVOL PTFULL	ADSPI- Sysvol _Percent Full

Using 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.

The Microsoft Active Directory has the following graphs:

- Active Directory GC Availability Graph
- Active Directory Replication Latency Graph
- Active Directory Replication Time by Global Catalog
- Active Directory Bind Response Time Graph
- Active Directory Query Response Time Graph

Related Topics:

- Graphs, Data Store, and Policy Mapping Details

Active Directory GC Availability Graph

Active Directory GC Availability Graph includes a graph that shows the general availability of the global catalog on those systems hosting GC services. To calculate the 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:

- Using Graphs
- Graphs, Data Store, and Policy Mapping Details

Active Directory Replication Latency Graph

The Active Directory Replication Latency Graph includes a 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.

Thise 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:

- Using Graphs
- Graphs, Data Store, and Policy Mapping Details

Active Directory Replication Time by Global Catalog

The Active Directory Replication Time by Global Catalog 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.

This 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:

- Using Graphs
- Graphs, Data Store, and Policy Mapping Details

Active Directory Bind Response Time Graph

The Active Directory Bind Response Time Graph 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:

- Using Graphs
- Graphs, Data Store, and Policy Mapping Details

Active Directory Query Response Time Graph

The Active Directory Query Response Time Graph 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:

- Using Graphs
- Graphs, Data Store, and Policy Mapping Details

Graphs, Data Store, and Policy Mapping Details

The Microsoft Active Directory SPI creates the following data in the data store on the node to facilitate the data-collection procedure. The data store class creator for all the reports is adspi_ddf.bat.

Data Store Details

Graph Name	Policy Logging Data	Spec File	Data Store Data Class
Active Directory Replication Latency Graph	ADSPI-Rep_MonitorIntraSiteReplication	ADSPI_RepLatency.spec	ADSPI_RepLatency
	ADSPI-Rep_MonitorInterSiteReplication		
Active Directory Query Response Time	ADSPI-Response_Logging	ADSPI_ResponseTime.spec	ADSPI_ResponseTime
Active Directory Bind Response Time	ADSPI-Response_Logging	ADSPI_ResponseTime.spec	ADSPI_ResponseTime
Active Directory GC Availability	ADSPI-Response_Logging	ADSPI_ResponseTime.spec	ADSPI_ResponseTime

Active Directory Replication Time by Global Catalog	ADSPI-Rep_GC_ Check_and_Threshold	ADSPI_GCREP.spec	ADSPI_GCRep

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: