HP Operations Smart Plug-in for Microsoft® Active Directory

for HP Operations Manager for HP-UX, Linux, and Solaris

Software Version: 7.06

Reference Guide

Document Release Date: November 2010
Software Release Date: November 2010

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Policies

The Smart Plug-in for Microsoft Active Directory (Microsoft Active Directory SPI) helps you to manage the Microsoft Active Directory in your environment on HP–UX, Solaris, or Linux as the management server. The Microsoft Active Directory SPI provides information about the Microsoft Active Directory and the following:

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

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.

Policy Group Catalog

The Microsoft Active Directory SPI has the following two levels of deployment:

- Auto deployment
- Manual deployment

Auto Deploy Polices

The auto-deploy policies are deployed automatically whenever the SPI discovers an existing service in the Microsoft Active Directory. The auto-deploy polices are divided into the sub-groups.

Discovery Policies (Basic and Advanced)

The Discovery policies discover all the services of the Microsoft Active Directory when deployed automatically to newly added nodes or manually to the already managed nodes.

ADSPI_Discovery

The ADSPI_Discovery policy discovers the existing components of the Microsoft Active Directory in your environment. It makes use of `OvAdsDisc.exe` to discover the Microsoft Active Directory components.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI_Discovery policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 / Windows Server 2008 → Auto-Deploy → Discovery → Basic Discovery**

ADSPI-AutoDiscovery_Delete

The ADSPI-AutoDiscovery_Delete verifies the continued presence of an already discovered service on each domain controller (DC). Whenever a previously discovered service is detected as no longer present in the DC, this policy starts removing that service from the console tree and service map. After five verifications (taking five hours by default), the removal occurs.

Result

This policy ensures that the HPOM console's services tree and service map are up to date if a service is shifted from one DC to another.

Schedule

This policy is an event based policy.

Policy Type

Open Message Interface policy.

Policy Group

You can locate the ADSPI-AutoDiscovery_Delete at **Policy Bank → SPI for Active Directory → Windows Server 2003 / Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_DIT

The ADSPI-AutoDiscovery_DIT policy runs the auto discovery program for the directory information tree (DIT) services. The policy is deployed to all the HPOM managed nodes, where it searches for DIT services on the DC. The DIT is shown under the DC name as well as with the DC in the service map, when discovered. Use this policy for Windows Server nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_DIT policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_DIT_2k8+

The ADSPI-AutoDiscovery_DIT_2k8+ policy runs the auto discovery program for the DIT services. The policy is deployed to all the HPOM managed nodes, where it searches for DIT services on the DC. The DIT is shown under the DC name as well as with the DC in the service map, when discovered. Use this policy for Windows Server 2008 nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_DIT_2k8+ policy at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_DNS

The ADSPI-AutoDiscovery_DNS policy runs the auto discovery program for the DNS-related services. This policy is deployed to all HPOM managed nodes, where it searches for a DC and then creates a DNS service on the DC. After the DNS service is created, it is shown under the DC name as well as with the DC in the service map. Use this policy for Windows Server nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_DNS policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_DNS_2k8+

The ADSPI-AutoDiscovery_DNS_2k8+ policy runs the auto discovery program for the DNS-related services. This policy is deployed to all HPOM managed nodes, where it searches for a DC and then creates a DNS service on the DC. After the DNS service is created, it is shown under the DC name as well as with the DC in the service map. Use this policy for Windows Server 2008 nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_DNS_2k8+ at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_FSMO

The ADSPI-AutoDiscovery_FSMO policy runs the auto discovery program for monitoring FSMO-related services. The policy searches for the Microsoft Active Directory FSMO services including PDC Master (primary domain controller master), RID Master, Infrastructure Master, Schema Master, and Domain Naming Master. Use this policy for Windows Server nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_FSMO policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_FSMO_2k8+

The ADSPI-AutoDiscovery_FSMO_2k8+ policy runs the auto discovery program for monitoring FSMO-related services. The policy searches for the Microsoft Active Directory FSMO services including PDC Master, RID Master, Infrastructure Master, Schema Master, and Domain Naming Master. Use this policy for Windows Server 2008 nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_FSMO_2k8+ policy at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_GC

The ADSPI-AutoDiscovery_GC policy runs the auto discovery program for monitoring global catalog (GC)-related services. This policy searches for hosted GC services. Use this policy for Windows Server nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_GC policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_GC_2k8+

The ADSPI-AutoDiscovery_GC_2k8+ policy runs the auto discovery program for monitoring global catalog (GC)-related services. This policy searches for hosted GC services. Use this policy for Windows Server 2008 nodes.

Result

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

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_GC_2k8+ policy at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_PBHS

The ADSPI-AutoDiscovery_PBHS schedule policy runs the auto discovery program for Preferred Bridgehead Server (PBHS) monitoring within replication.

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

- Bridgehead Servers: These servers have connection objects for connections between sites. A destination bridgehead server has a connection object with a source (from) server in another site, while a source bridgehead server has a connection object with a destination (to) server.
- PBHS: You can limit the KCC's choice of servers that it can designate as bridgeheads, that is, restrict the DCs in which the KCC can create connections between sites. For this, select one or more DCs in a site as a preferred bridgehead server. The KCC will then

always consider the preferred bridgehead servers when it establishes source or destination servers from inter-site connections. PBHS are used exclusively to replicate the changes collected from the site.

Result

After the PBHS is discovered, it is identified on the DC hosting it and appears in the HPOM service tree, under Replication services, as well as in the service map as part of the Microsoft Active Directory services, illustrating the status of this service.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_PBHS policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_PBHS_2k8+

The ADSPI-AutoDiscovery_PBHS_2k8+ schedule policy runs the auto discovery program for Preferred Bridgehead Server (PBHS) monitoring within replication.

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

- Bridgehead Servers: These servers have connection objects for connections between sites. A destination bridgehead server has a connection object with a source (from) server in another site, while a source bridgehead server has a connection object with a destination (to) server.
- PBHS: You can limit the KCC's choice of servers that it can designate as bridgeheads, that is, restrict the DCs in which the KCC can create connections between sites. For this, select one or more DCs in a site as a preferred bridgehead server. The KCC then always considers the preferred bridgehead servers when it establishes source or destination servers from inter-site connections. PBHS are used exclusively to replicate the changes collected from the site.

Result

After the PBHS is discovered, it is identified on the DC hosting it and appears in the HPOM service tree, under Replication services, as well as in the service map as part of the Microsoft Active Directory services, illustrating the status of this service.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_PBHS_2k8+ at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_Rep

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

Errors which are caused due to replication failure are important to measure. For example, Sysvol, as the shared or replicated directory, stores the server copy of the domain's public files. These files are replicated among all DCs in the domain. Updates result in inbound connection objects. An increase in the number of inbound connection objects can indicate that updates are being redirected, which could mean a failed or overloaded bridgehead.

Result

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

The PBHS is also displayed as a Replication service (DC:DC_Name > Replication > Bridgehead), although another discovery policy (ADSPI-AutoDiscovery_PBHS) runs a separate program for the bridgehead discovery.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_Rep policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_Rep_2k8+

The ADSPI-AutoDiscovery_Rep_2k8+ policy runs the auto discovery program for monitoring the Microsoft Active Directory replication-related services. The policy searches for the Microsoft Active Directory replication and replication-related services including Sysvol, inbound replication objects, and time synchronization. Use this policy for Windows Server 2008 nodes.

Errors which are caused due to replication failure are important to measure. For example, Sysvol, as the shared or replicated directory, stores the server copy of the domain's public files. These files are replicated among all DCs in the domain. Updates result in inbound connection objects. An increase in the number of inbound connection objects can indicate that updates are being redirected, which could mean a failed or overloaded bridgehead.

Result

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

The PBHS is also displayed as a Replication service (DC:DC_Name > Replication > Bridgehead), although another discovery policy (ADSPI-AutoDiscovery_PBHS) runs a separate program for the bridgehead discovery.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_Rep_2k8+ policy at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_RODC_2k8+

The ADSPI-AutoDiscovery_RODC_2k8+ policy discovers the read-only DCs. Use this policy for Windows Server 2008 nodes only.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_RODC_2k8+ at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_Trust

The ADSPI-AutoDiscovery_Trust scheduled policy runs the auto discovery program for monitoring trust-related services. This policy creates the Trust service in the HPOM service map for Windows 2003 DCs. Use this policy for Windows Server nodes.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_Trust policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-AutoDiscovery_Trust_2k8+

The ADSPI-AutoDiscovery_Trust_2k8+ scheduled policy runs the auto discovery program for monitoring trust-related services. This policy creates the Trust service in the HPOM service map for Windows 2008 DCs. Use this policy for Windows Server 2008 nodes.

Schedule

This policy runs daily at 2 A.M.

Policy Type

Service Auto Discovery policy

Policy Group

You can locate the ADSPI-AutoDiscovery_Trust_2k8+ at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

ADSPI-CreateDatasources

The ADSPI-CreateDatasources policy creates the required data sources in the data store (CODA or HP Performance Agent (PA)). The Microsoft Active Directory SPI data sources enables the polices to log data.

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-CreateDataSources policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 / Windows Server 2008 → Auto-Deploy → Discovery → Advanced Discovery**

DIT Monitoring Policies

The DIT Monitoring policies are used to monitor all the Microsoft Active Directory DIT services.

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 reside is unable to handle the number of necessary updates.

Schedule

This policy runs every 5 minutes.

Threshold

This policy gives the following thresholds:

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

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start Actions: The queue length (i.e., the number of outstanding requests) on the Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME>is<$SESSION(LogFilesQueueLength)>. The log files disk drive is <$SESSION(LogFilesDrive)>.
- End Actions: The queue length on the Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME>no longer exceeds <$SESSION(CriticalThreshold)>.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_LogfilesQueueLength policy at **Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DIT Monitoring**

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 reside is unable to handle the number of necessary updates.

Schedule

This policy runs every 5 minutes.

Threshold

This policy gives the following thresholds:

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

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start Actions: The queue length (i.e., the number of outstanding requests) on the Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME>is<$SESSION(LogFilesQueueLength)>. The log files disk drive is <$SESSION(LogFilesDrive)>.
- End Actions: The queue length on the Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME>no longer exceeds <$SESSION(CriticalThreshold)>.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_LogfilesQueueLength_2k8+ policy at **Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DIT Monitoring**

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 shows 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 on which the DIT resides is unable to handle the number of necessary updates.

Result

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

Schedule

This policy runs every 5 minutes.

Threshold

This policy gives the following thresholds:

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

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start Actions: The queue length (i.e., the number of outstanding requests) on the Microsoft Active Directory database I(DIT) disk drive on <$MSG_NODE_NAME>is<$SESSION(DitQueueLength)>. The DIT disk drive is <$SESSION(DitDrive)>.
- End Actions: The queue length on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME>no longer exceeds <$SESSION(CriticalThreshold)>.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_DITQueueLength policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DIT Monitoring

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 shows 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 on which the DIT resides is unable to handle the number of necessary updates.

Result

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

Schedule

This policy runs every 5 minutes.

Threshold

This policy gives the following thresholds:

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

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start Actions: The queue length (i.e., the number of outstanding requests) on the Microsoft Active Directory database I(DIT) disk drive on <$MSG_NODE_NAME>is<$SESSION(DitQueueLength)>. The DIT disk drive is <$SESSION(DitDrive)>.
- End Actions: The queue length on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME>no longer exceeds <$SESSION(CriticalThreshold)>.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_DITQueueLength_2k8+ policy in:

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

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 files, or DIT, can cause problems when it expands over time and has gone unobserved.

Schedule

This policy runs every 24 hours.

Threshold

This policy gives the following thresholds:

- 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 warning or error message text for the start and end actions is:

- Start Actions: The freespace on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME>is only <$SESSION(DitDriveFreeSpace)>MB. It is less than the threshold value of <$SESSION(minFreeSpaceMB)>MB.
- End Actions: The freespace on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> is greater than <$SESSION(minFreeSpaceMB)>MB.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_TotalDITSize policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DIT Monitoring

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 Microsoft Active Directory database files, or DIT, can cause problems when it expands over time and has gone unobserved.

Schedule

This policy runs every 24 hours.

Threshold

This policy gives the following thresholds:

- 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 warning or error message text for the start and end actions is:

- Start Actions: The freespace on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME>is only <$SESSION(DitDriveFreeSpace)>MB. It is less than the threshold value of <$SESSION(minFreeSpaceMB)>MB.
- End Actions: The freespace on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> is greater than <$SESSION(minFreeSpaceMB)>MB.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_TotalDITSize_2k8+ policy in:

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

ADSPI-DIT_LogfilesPercentFull

The ADSPI-DIT_LogfilesPercentFull policy calculates the full percentage amount occupied by the DIT log files in proportion to the drive hosting the DIT. This policy logs the information and also checks for an unexpected 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.

Result

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

Schedule

This policy runs every 24 hours.

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: The Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME>is <$SESSION(PercentFull)>%.
- End action: The percentage full on the Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_LogfilesPercentFull policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DIT Monitoring

ADSPI-DIT_LogfilesPercentFull_2k8+

The ADSPI-DIT_LogfilesPercentFull_2k8+ policy calculates the full percentage amount occupied by the DIT log files in proportion to the drive hosting the DIT. This policy logs the information and also checks for an unexpected 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.

Result

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

Schedule

This policy runs every 24 hours.

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: The Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME>is <$SESSION(PercentFull)>%.
- End action: The percentage full on the Microsoft Active Directory log files disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_LogfilesPercentFull_2k8+ policy in:

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

ADSPI-DIT_DITPercentFull

The ADSPI-DIT_DITPercentFull policy monitors the percentage used space on the disk drive holding the Microsoft Active Directory database (DIT). It calculates the percentage full of the drive hosting the DIT.

The 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.

Schedule

This policy runs every 24 hours.

Threshold

This policy gives the following threshold:

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

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: The Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME>is <$SESSION(PercentFull)>% full.

- End action: The percentage full on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_DITPercentFull policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DIT Monitoring

ADSPI-DIT_DITPercentFull_2k8+

The ADSPI-DIT_DITPercentFull_2k8+ policy monitors the percentage used space on the disk drive holding the Microsoft Active Directory database (DIT). It calculates the percentage full of the drive hosting the DIT.

The 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.

Schedule

This policy runs every 24 hours.

Threshold

This policy gives the following threshold:

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

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: The Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME>is <$SESSION(PercentFull)>% full.
- End action: The percentage full on the Microsoft Active Directory database (DIT) disk drive on <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>%.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DIT_DITPercentFull_2k8+ policy in:

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

DNS Monitoring Policies

The DNS Monitoring polices are used to monitor the DNS-related services of the Microsoft Active Directory.

ADSPI-DNS_DC_A_Chk

The ADSPI-DNS_DC_A_Chk policy ensures that DNS contains the unexpected DNS host resource records for the LDAP service by checking for expected DNS A resource records.

There are two host records associated with each DC:

- For its fully qualified domain name
- For the domain that it services.

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

Schedule

This policy runs for every 1 hour.

Threshold

This policy has the following threshold:

Critical: >=1

Types of failures are:

“REG_RECORDS_FLAG_NOT_SET = 2”

“DNS_SERVER_PING_FAILURE = 3”

“NO_FOREST_RECOGNITION = 5”

“PROBLEM_NOT_DETECTED = 13”

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: DC<$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 **Instruction** tab for details for how to make use of this information: The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: DC<$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_DC_A_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_DC_A_Chk_2k8+

The ADSPI-DNS_DC_A_Chk_2k8+ policy ensures that DNS contains the unexpected DNS host resource records for the LDAP service by checking for expected DNS A resource records.

There are two host records associated with each DC:

- For its fully qualified domain name
- For the domain that it services.

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

Schedule

This policy runs for every 1 hour.

Threshold

This policy has the following threshold:

Critical: >=1

Types of failures are:

“REG_RECORDS_FLAG_NOT_SET = 2”

“DNS_SERVER_PING_FAILURE = 3”

“NO_FOREST_RECOGNITION = 5”

“PROBLEM_NOT_DETECTED = 13”

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: DC<$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 **Instruction** tab for details for how to make use of this information: The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: DC<$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_DC_A_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_DC_CName_Chk

The ADSPI-DNS_DC_CName_Chk policy checks for expected DNS CNAME resource records for the LDAP service.

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

Schedule

This policy runs for every 1 hour.

Threshold

This policy has the following threshold:

Error Level: Threshold limit >=1

Types of failures are:

"REG_RECORDS_FLAG_NOT_SET = 2"

"DNS_SERVER_PING_FAILURE = 3"

"NO_FOREST_RECOGNITION = 5"

"PROBLEM_NOT_DETECTED = 13"

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: DC<$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 **Instruction** tab for details for how to make use of this information: The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: DC<$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_DC_CName_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_DC_CName_Chk_2k8+

The ADSPI-DNS_DC_CName_Chk_2k8+ policy checks for expected DNS CNAME resource records for the LDAP service.

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

Schedule

This policy runs for every 1 hour.

Threshold

This policy has the following threshold:

Error Level: Threshold limit >=1

Types of failures are:

"REG_RECORDS_FLAG_NOT_SET = 2"

"DNS_SERVER_PING_FAILURE = 3"

"NO_FOREST_RECOGNITION = 5"

"PROBLEM_NOT_DETECTED = 13"

Warning/Error Message Text

The warning or error message text for the start and end actions is:

- Start action: DC<$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 **Instruction** tab for details for how to make use of this information: The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: DC<$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_DC_CName_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_DC_Response

The ADSPI-DNS_DC_Response policy monitors the response time of DNS queries made by the DC in milliseconds. Reports on whether DNS response is too long (Rule 1) or does not occur (Rule 2).

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

This policy also logs information for reporting.

Schedule

This policy runs every 30 minutes.

Threshold

This policy has the following threshold:

Warning Level: Response Time >= 1000 (Rule 1 applies)

Critical Level: Response Time >=2000 (Rule 1 applies)

Critical Level: Response Time = 0 (Rule 2 applies)

Warning/Error Message Text

The warning or error message text for the start and end actions for slow response, that is, *Rule 1*, is:

- Start action: DC<$MSG_NODE_NAME> is getting a DNS response time of <$SESSION(value)> milliseconds! It has crossed the threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.

  The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: DC<$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.

The warning or error message text for the start and end actions for no response, that is, *Rule 2*, is:

- Start action: DC<$MSG_NODE_NAME> is getting no response from DNS!

  The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: DC<$MSG_NODE_NAME> is now getting a response from DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_DC_Response policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_DC_Response_2k8+

The ADSPI-DNS_DC_Response_2k8+ policy monitors the response time of DNS queries made by the DC in milliseconds. Reports on whether DNS response is too long (Rule 1) or does not occur (Rule 2).

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

This policy also logs information for reporting.

Schedule

This policy runs every 30 minutes.

Threshold

This policy has the following threshold:

Warning Level: Response Time >= 1000 (Rule 1 applies)

Critical Level: Response Time >=2000 (Rule 1 applies)

Critical Level: Response Time = 0 (Rule 2 applies)

Warning/Error Message Text

The warning or error message text for the start and end actions for slow response, that is, *Rule 1*, is:

- Start action: DC<$MSG_NODE_NAME> is getting a DNS response time of <$SESSION(value)> milliseconds! It has crossed the threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.

  The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: DC<$MSG_NODE_NAME> is no longer exceeding the critical DNS response time threshold of <$SESSION(Critical\WarningThreshold)> milliseconds.

The warning or error message text for the start and end actions for no response, that is, *Rule 2*, is:

- Start action: DC<$MSG_NODE_NAME> is getting no response from DNS!

  The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: DC<$MSG_NODE_NAME> is now getting a response from DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_DC_Response_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_Extra_GC_SRV_Chk

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

Schedule

This policy runs for every 24 hours.

Threshold

This policy has the following threshold

Warning Level >=1

Warning condition: Generates a warning message if the DC is registered as a GC host on a site in which it does not reside. The message has only warning level serverity 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 Microsoft Active Directory as a GC.

Warning/Error Message Text

The warning or error message text for the start and end actions for *Rule 1* is:

- Start Action: DC <$MSG_NODE?_NAME> is registered as a GC for the following sites, but does not reside at hem:

  <$OPTION(extraSites)>

  The DC has been configured to use the following DNS servers:

  <$OPTION(DnsServers)>

- End Action: DC <$MSG_NODE_NAME> is no longer registered in DNS as a GC for sites that it does not reside on.

The warning or error message text for the start and end actions for *Rule 2* is:

- Start action: DC<$MSG_NODE_NAME> is not a GC host, but it is registered as one in DNS!

  The DC has been configured to use the following DNS servers:

  <$IOPTIONS(DnsServers)>

- End action: DC <$MSG_NODE_NAME> is no longer mis-registered as a GC in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Extra_GC_SRV_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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 GC.

Schedule

This policy runs for every 24 hours.

Threshold

This policy has the following threshold

Warning Level >=1

Warning condition: Generates a warning message if the DC is registered as a GC host on a site in which it does not reside. The message has only warning level serverity 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 Microsoft Active Directory as a GC.

Warning/Error Message Text

The warning or error message text for the start and end actions for *Rule 1* is:

- Start Action: DC <$MSG_NODE?_NAME> is registered as a GC for the following sites, but does not reside at hem:

  <$OPTION(extraSites)>

  The DC has been configured to use the following DNS servers:

  <$OPTION(DnsServers)>

- End Action: DC <$MSG_NODE_NAME> is no longer registered in DNS as a GC for sites that it does not reside on.

The warning or error message text for the start and end actions for *Rule 2* is:

- Start action: DC<$MSG_NODE_NAME> is not a GC host, but it is registered as one in DNS!

  The DC has been configured to use the following DNS servers:

  <$IOPTIONS(DnsServers)>

- End action: DC <$MSG_NODE_NAME> is no longer mis-registered as a GC in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Extra_GC_SRV_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

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 for every 24 hours.

Threshold

This policy has Warning Level: >=1 as threshold.

Warning/Error Message Text

The warning or error message text for the start and end action is:

- Start action: DC <$MSG_NODE_NAME> is registered as a Kerberos server for the following sites, but does not reside at them:

  <$OPTION(extraSites)>

The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: DC <$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

You can locate the ADSPI-DNS_Extra_Kerberos_SRV_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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 for every 24 hours.

Threshold

This policy has Warning Level: >=1 as threshold.

Warning/Error Message Text

The warning or error message text for the start and end action is:

- Start action: DC <$MSG_NODE_NAME> is registered as a Kerberos server for the following sites, but does not reside at them:

  <$OPTION(extraSites)>

  The DC has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: DC <$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

You can locate the ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

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

This policy has Warning Level: >=1 as the threshold.

Warning/Error Message Text

The warning or error message text for the start and end action is:

- Start action: DC<$MSG_NODE_NAME> is registered as a DC for the following sites, but does not reside at them:

  <$OPTION> (extraSites)>

  The DC has been configured to use the following DNS servers:

  <$OPTION><DnsServers)>

- End action: DC <$MSG_NODE_NAME> is no longer registered in DNS as a DC for sites that it does not reside on.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Extra_LDAP_SRV_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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

This policy has Warning Level: >=1 as the threshold.

Warning/Error Message Text

The warning or error message text for the start and end action is:

- Start action: DC<$MSG_NODE_NAME> is registered as a DC for the following sites, but does not reside at them:

  <$OPTION> (extraSites)>

  The DC has been configured to use the following DNS servers:

  <$OPTION><DnsServers)>

- End action: DC <$MSG_NODE_NAME> is no longer registered in DNS as a DC for sites that it does not reside on.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_GC_A_Chk

The ADSPI-DNS_GC_A_Chk policy ensures that the DNS contains the expected DNS A resource records for the GC. This policy checks DNS for a DC hosting GC services. It does this by looking for the DNS host record (A record) associated with a DC that hosts the GC.

Schedule

This policy runs every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers:
  <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_GC_A_Chk policy in:

ADSPI-DNS_GC_A_Chk_2k8+

The ADSPI-DNS_GC_A_Chk_2k8+ policy ensures that the DNS contains the expected DNS A resource records for the GC. This policy checks DNS for a DC hosting GC services. It does this by looking for the DNS host record (A record) associated with a DC that hosts the GC.

Schedule

This policy runs every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information: The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_GC_A_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_GC_SRV_CHK

The ADSPI-DNS_GC_SRV_CHK policy ensures that DNS contains the expected DNS SRV resource records for the GC. The Microsoft Active Directory DC 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 GC services.

This policy generates a critical message when a DC is not properly registered in DNS as a GC host. That is, it alerts you when one or more SRV records that identify it as a GC host are missing. This policy is deployed to all DCs, but only runs if the DC hosts the GC. You can then modify your Microsoft Active Directory environment without having to modify your management software.

Schedule

This policy runs every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the **Instructions** tab for details for how to make use of this information:

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_GC_SRV_CHK policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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 GC. The Microsoft Active Directory DC 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 GC services.

This policy generates a critical message when a DC is not properly registered in DNS as a GC host. That is, it alerts you when one or more SRV records that identify it as a GC host are missing. This policy is deployed to all DCs, but only runs if the DC hosts the GC. You can then modify your Microsoft Active Directory environment without having to modify your management software.

Schedule

This policy runs every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the **Instructions** tab for details for how to make use of this information:

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_GC_SRV_CHK_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_GC_StrandedSite

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

Without access to the forest's GC, 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 GC. It is dependent on inter-site connections for its GC 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 GC is registered in DNS. You are notified if DNS is showing no path to a forest's GC.

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

Result

This policy gives 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 you that the Microsoft Active Directory forest has no GC registered in DNS.

Schedule

This policy runs for every 24 hours.

Threshold

This policy gives the following threshold:

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

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

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

Warning/Error Message Text

The warning or error message text for the start and end action is:

- Start action: Site <$INSTANCE> of forest <$OPTION(forest)> has no local global catalog!

  It is using global catalogs from the following site(s):

  <$OPTION(sitesUsed)>

The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: Site <$INSTANCE> of forest <$OPTION(forest)> now has a local global catalog.

Minor Level Message Text

The warning or error message text for the start and end action at minor level is:

- Start action: Site <$INSTANCE> of forest <$OPTION(forest)> has no global catalog SRV record registered in DNS!

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: Site <$INSTANCE> of forest <$OPTION(forest)> now has a global catalog SRV record registered in DNS.

Error Level Message Text

The warning or error message text for the start and end action at error level is:

- Start action: Forest <$OPTION(forest)> has no global catalog!

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

- End action: Forest <$OPTION(forest)> now has a global catalog registered in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_GC_StrandedSite policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_GC_StrandedSite_2k8+

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

Without access to the forest's GC, 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 GC. It is dependent on inter-site connections for its GC 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 GC is registered in DNS. You are notified if DNS is showing no path to a forest's GC.

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

Result

This policy gives 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 you that the Microsoft Active Directory forest has no GC registered in DNS.

Schedule

This policy runs for every 24 hours.

Threshold

This policy gives the following threshold:

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

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

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

Warning/Error Message Text

The warning or error message text for the start and end action is:

- Start action: Site <$INSTANCE> of forest <$OPTION(forest)> has no local global catalog!

  It is using global catalogs from the following site(s):

  <$OPTION(sitesUsed)>

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>
- End action: Site <$INSTANCE> of forest <$OPTION(forest)> now has a local global catalog.

Minor Level Message Text

The warning or error message text for the start and end action at minor level is:

- Start action: Site <$INSTANCE> of forest <$OPTION(forest)> has no global catalog SRV record registered in DNS!

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>
- End action: Site <$INSTANCE> of forest <$OPTION(forest)> now has a global catalog SRV record registered in DNS.

Error Level Message Text

The warning or error message text for the start and end action at error level is:

- Start action: Forest <$OPTION(forest)> has no global catalog!

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>
- End action: Forest <$OPTION(forest)> now has a global catalog registered in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_GC_StrandedSite_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

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.

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

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

Schedule

This policy runs every 24 hours.

Threshold

This policy has the following threshold:

Warning Level: >=1

(Domain Controller uses itself as a DNS server.)

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: Domain Controller <$MSG_NODE_NAME> has been configured to use itself as a DNS server!

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>
- End action: Domain Controller <$MSG_NODE_NAME> is no longer configured to use itself as a DNS server.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Island_Server policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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.

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

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

Schedule

This policy runs every 24 hours.

Threshold

This policy has the following threshold:

Warning Level: >=1

(Domain Controller uses itself as a DNS server.)

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: Domain Controller <$MSG_NODE_NAME> has been configured to use itself as a DNS server!

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Island_Server_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_LogDNSPagesSec

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

Schedule

This is a measurement threshold policy and the default global polling interval for this policy is 10 seconds.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_LogDNSPagesSec policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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 is a measurement threshold policy and the default global polling interval for this policy is 10 seconds.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_LogDNSPagesSec_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

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.

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 also generates a critical message if the DC is registered as a Kerberos KDC on a site in which it does not reside.

Result

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

Schedule

This policy runs for every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information:

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Kerberos_SRV_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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.

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 also generates a critical message if the DC is registered as a Kerberos KDC on a site in which it does not reside.

Result

The ADSPI-DNS_Kerberos_SRV_Chk_2k8+ 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 you.

Schedule

This policy runs for every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information:

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Kerberos_SRV_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

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 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 an LDAP server. That is, it alerts you when one or more SRV records that identify it as an LDAP server are missing.

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 you that one or more SRV records that identify the DC as hosting an LDAP service are missing.

Schedule

This policy runs every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information:

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_LDAP_SRV_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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 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 an LDAP server. That is, it alerts you when one or more SRV records that identify it as an LDAP server are missing.

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 you that one or more SRV records that identify the DC as hosting an LDAP service are missing.

Schedule

This policy runs every 1 hour.

Threshold

This policy has the following 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 warning or error message text for the start and end action is:

- Start action: Domain controller <$MSG_NODE_NAME> is missing the following records in DNS:

  <$OPTION(missing)>

  The following data has been collected to diagnose the source of this problem. See the 'Instructions' tab for details for how to make use of this information:

  The domain controller has been configured to use the following DNS servers: <$OPTION(DnsServers)>

  <$SESSION(NetLogon)><$OPTION(NetLogonStatus)>

  <$SESSION(RegRecordsFlag)>

  <$SESSION(ServerPing)><$OPTION(FailingServers)>

  <$SESSION(NoForest)>

- End action: Domain controller <$MSG_NODE_NAME> is no longer missing host records in DNS.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_LDAP_SRV_Chk_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_Server_Response

The ADSPI-DNS_Server_Response policy generates messages or 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 the Microsoft Active Directory.

Result

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Server_Response policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

ADSPI-DNS_Server_Response_2k8+

The ADSPI-DNS_Server_Response_2k8+ policy generates messages or 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 the Microsoft Active Directory.

Result

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-DNS_Server_Response_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

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 DC 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 DC 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 Microsoft 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 DCs, but to minimize monitoring time, the policy runs only on a forest's Infrastructure Master.

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 DCs, it runs only on the PDC emulator for the forest's root domain to minimize monitoring time.

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

Error Message Text

The error message text for the start and end action is:

- 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 warning message text for the start and end action is:

- 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

You can locate the ADSPI-DNS_Obsolete_GUIDs policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → DNS Monitoring

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 DC 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 DC 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 Microsoft 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 DCs, but to minimize monitoring time, the policy runs only on a forest's Infrastructure Master.

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 DCs, it runs only on the PDC emulator for the forest's root domain to minimize monitoring time.

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

Error Message Text

The error message text for the start and end action is:

- 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 warning message text for the start and end action is:

- 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

You can locate the ADSPI-DNS_Obsolete_GUIDs_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → DNS Monitoring

FSMO Monitoring Polices

The FSMO monitoring policies are used to monitor flexible single masters operations (FSMO) services. These are scheduled task policies. The FSMO logging and FSMO consist policies collect the data that the other FSMO measurement threshold policies can then check for exceeded or acceptable service level objectives.

ADSPI-FSMO_INFRA_Bind

The ADSPI-FSMO_INFRA_Bind policy measures the response time length in seconds for the INFRA master. For this purpose, the 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 also 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

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: Infrastructure Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_INFRA_Bind policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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, the 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 also 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

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: Infrastructure Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_INFRA_Bind_2k8+ policy in:

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

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 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 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: Infrastructure Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_INFRA_Ping policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 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 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: Infrastructure Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_INFRA_Ping_2k8+ policy in:

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

ADSPI-FSMO_GC_Infrastructure_Check

The ADSPI-FSMO_GC_Infrastructure_Check 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.

This is a Measurement Threshold policy.

Schedule

This policy runs every 24 hours.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_GC_Infrastructure_Check policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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.

This is a Measurement Threshold policy.

Schedule

This policy runs every 24 hours.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_GC_Infrastructure_Check_2k8+ policy in:

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

ADSPI-FSMO_Logging

The ADSPI-FSMO_Logging scheduled task 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

You can locate the ADSPI-FSMO_Logging policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_Logging_2k8+

The ADSPI-FSMO_Logging_2k8+ scheduled task 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

You can locate the ADSPI-FSMO_Logging_2k8+ policy in:

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

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, the policy periodically binds to the DC that is the domain-naming master.

Threshold

This policy has the following threshold:

Warning: 1 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: 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

You can locate the ADSPI-FSMO_NAMING_Bind policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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, the policy periodically binds to the DC that is the domain-naming master.

Threshold

This policy has the following threshold:

Warning: 1 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: 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

You can locate the ADSPI-FSMO_NAMING_Bind_2k8+ policy in:

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

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 DC that is the domain-naming master.

This policy, working in conjunction with the scheduled task policy ADSPI-FSMO_Logging, measures the general responsiveness of the domain-naming master and allows thresholds on that measurement.

The domain-naming master is the DC responsible for making changes to the forest-wide domain name space. This DC is responsible for adding or removing a domain from the forest and adding or 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

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: 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

You can locate the ADSPI-FSMO_NAMING_Ping policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC that is the domain-naming master.

This policy, working in conjunction with the scheduled task policy ADSPI-FSMO_Logging, measures the general responsiveness of the domain-naming master and allows thresholds on that measurement.

The domain-naming master is the DC responsible for making changes to the forest-wide domain name space. This DC is responsible for adding or removing a domain from the forest and adding or 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

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: 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

You can locate the ADSPI-FSMO_NAMING_Ping_2k8+ policy in:

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

ADSPI-FSMO_PDC_Bind

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

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

In a Windows domain, the PDC master also performs the following functions:

- Password changes performed by other DCs in the domain are replicated preferentially to the PDC master.
- Authentication failures that occur at a given DC 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

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: PDC Emulator bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-SFSMO_PDC_Bind policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_PDC_Bind_2k8+

The ADSPI-SFSMO_PDC_Bind_2k8+ policy measures the response time length in seconds for the PDC master. For this purpose, the policy periodically binds to the DC that is the PDC master.

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

In a Windows domain, the PDC master also performs the following functions:

- Password changes performed by other DCs in the domain are replicated preferentially to the PDC master.
- Authentication failures that occur at a given DC 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

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: PDC Emulator bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-SFSMO_PDC_Bind_2k8+ policy in:

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

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 DC that is the PDC master. It also monitors the ping response time of the PDC FSMO.This policy, works in conjunction with the ADSPI-FSMO_Logging policy, measures the general responsiveness of the PDC master and allows thresholds on that measurement.

The PDC master is a Windows DC that acts as the primary DC to down-level workstations, member servers, and DCs. In a Windows domain, the PDC master also performs the following functions:

- Password changes performed by other DCs in the domain are replicated preferentially to the PDC master.
- Authentication failures that occur at a given DC 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

Warning\Error Text Message

The warning or error message text for the start action and end action is:

- Start action: 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 action: PDC Emulator ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_PDC_Ping policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC that is the PDC master. It also monitors the ping response time of the PDC FSMO.This policy, works in conjunction with the ADSPI-FSMO_Logging policy, measures the general responsiveness of the PDC master and allows thresholds on that measurement.

The PDC master is a Windows DC that acts as the primary DC to down-level workstations, member servers, and DCs. In a Windows domain, the PDC master also performs the following functions:

- Password changes performed by other DCs in the domain are replicated preferentially to the PDC master.
- Authentication failures that occur at a given DC 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

Warning\Error Text Message

The warning or error message text for the start action and end action is:

- Start action: 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 action: PDC Emulator ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_PDC_Ping_2k8+ policy in:

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

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 DC that is the RID master.

The RID master is the DC responsible for processing RID Pool requests from all DCs 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 DC is allocated a pool of RIDs. When a DC's pool falls below a threshold, that DC issues a request to the domain's RID master for a new pool. There is one RID master per domain in a forest.

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

Threshold

This policy has the following threshold:

Warning: 1 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: RID Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_RID_Bind policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC that is the RID master.

The RID master is the DC responsible for processing RID Pool requests from all DCs 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 DC is allocated a pool of RIDs. When a DC's pool falls below a threshold, that DC issues a request to the domain's RID master for a new pool. There is one RID master per domain in a forest.

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

Threshold

This policy has the following threshold:

Warning: 1 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: RID Master bind response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_RID_Bind_2k8+ policy in:

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

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 DC that is the RID master.

The RID master is the DC responsible for processing RID Pool requests from all DCs 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 RID.

This policy works in conjunction with ADSPI-FSMO_Logging policy.

Threshold

This policy has the following threshold:

Warning: 1 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: RID Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_RID_Ping policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC that is the RID master.

The RID master is the DC responsible for processing RID Pool requests from all DCs 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 RID.

This policy works in conjunction with ADSPI-FSMO_Logging policy.

Threshold

This policy has the following threshold:

Warning: 1 second

Error: 2 seconds

Warning\Error Message Text

The warning or error message text for the start and end action is:

- Start action: 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 action: RID Master ping response time on domain controller <$MSG_NODE_NAME> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-FSMO_RID_Ping_2k8+ policy in:

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

ADSPI-FSMO_RoleMvmt

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

Threshold

This scheduled task policy runs once every hour to determine if the DC it is running on has gained or lost one of the five FSMO roles. It sends the role movement information that it collects to the following policies:

- ADSPI-FSMO_RoleMvmt_INFRA
- ADSPI-FSMO_RoleMvmt_NAMING
- ADSPI-FSMO_RoleMvmt_PDC
- ADSPI-FSMO_RoleMvmt_RID
- ADSPI-FSMO_RoleMvmt_SCHEMA

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

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-FSMO_RoleMvmt policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_RoleMvmt_2k8+

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

Threshold

This scheduled task policy runs once every hour to determine if the DC it is running on has gained or lost one of the five FSMO roles. It sends the role movement information that it collects to the following policies:

- ADSPI-FSMO_RoleMvmt_INFRA
- ADSPI-FSMO_RoleMvmt_NAMING
- ADSPI-FSMO_RoleMvmt_PDC
- ADSPI-FSMO_RoleMvmt_RID
- ADSPI-FSMO_RoleMvmt_SCHEMA

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

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-FSMO_RoleMvmt_2k8+ policy in:

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

ADSPI-FSMO_RoleMvmt_INFRA

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

FSMO roles may be transferred between DCs by an administrator. In addition, a FSMO role will be automatically transferred if a DC that hosts the role is demoted. This policy sends alarms to the management server if the local DC acquires or loses ownership of the Infrastructure Master FSMO role.

Threshold

This policy has change in FSMO role assigned to DC as its threshold.

Warning\Error Message Text for Rule 1

Rule 1 is DC Acquired FSMO Role Ownership. The warning or error message text for the start action is:

Domain controller <$MSG_NODE_NAME> has acquired the Infrastructure Master FSMO role for domain <$OPTION(domain)>.

This role was formerly owned by <$OPTION(holder)>.

Warning\Error Message Text for Rule 2

Rule 2 is DC Lost FSMO Role Ownership. The warning or error message text for the start action is:

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

You can locate the ADSPI-FSMO_RoleMvmt_INFRA policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_RoleMvmt_INFRA_2k8+

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

FSMO roles may be transferred between DCs by an administrator. In addition, a FSMO role will be automatically transferred if a DC that hosts the role is demoted. This policy sends alarms to the management server if the local DC acquires or loses ownership of the Infrastructure Master FSMO role.

Threshold

This policy has change in FSMO role assigned to DC as its threshold.

Warning\Error Message Text for Rule 1

Rule 1 is DC Acquired FSMO Role Ownership. The warning or error message text for the start action is:

Domain controller <$MSG_NODE_NAME> has acquired the Infrastructure Master FSMO role for domain <$OPTION(domain)>.

This role was formerly owned by <$OPTION(holder)>.

Warning\Error Message Text for Rule 2

Rule 2 is DC Lost FSMO Role Ownership. The warning or error message text for the start action is:

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

You can locate the ADSPI-FSMO_RoleMvmt_INFRA_2k8+ policy in:

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

ADSPI-FSMO_RoleMvmt_NAMING

The ADSPI-FSMO_RoleMvmt_NAMING policy monitors the DC’s ownership of the Domain Naming Master FSMO role.

FSMO roles may be transferred between DCs by an administrator. In addition, a FSMO role will be automatically transferred if a DC that hosts the role is demoted. This measurement threshold policy sends alarms to the management server if the local DC acquires or loses ownership of the Domain Naming Master FSMO role.

Threshold

This policy has change in FSMO role assigned to DC as its threshold.

Warning\Error Message Text for Rule 1

Rule 1 DC Acquired FSMO Role Ownership. The warning or error message text for the start action is:

Domain controller <$MSG_NODE_NAME> has acquired the Domain Naming Master FSMO role forest <$OPTION(forest)>.

This role was formerly owned by <$OPTION(holder)>.

Warning\Error Message Text for Rule 2

Rule 2 is DC Lost FSMO Role Ownership. The warning or error message text for the start action is:

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

You can locate the ADSPI-FSMO_RoleMvmt_NAMING policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_RoleMvmt_NAMING_2k8+

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

FSMO roles may be transferred between DCs by an administrator. In addition, a FSMO role will be automatically transferred if a DC that hosts the role is demoted. This measurement threshold policy sends alarms to the management server if the local DC acquires or loses ownership of the Domain Naming Master FSMO role.

Threshold

This policy has change in FSMO role assigned to DC as its threshold.

Warning\Error Message Text for Rule 1

Rule 1 DC Acquired FSMO Role Ownership. The warning or error message text for the start action is:

Domain controller <$MSG_NODE_NAME> has acquired the Domain Naming Master FSMO role forest <$OPTION(forest)>.

This role was formerly owned by <$OPTION(holder)>.

Warning\Error Message Text for Rule 2

Rule 2 is DC Lost FSMO Role Ownership. The warning or error message text for the start action is:

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

You can locate the ADSPI-FSMO_RoleMvmt_NAMING_2k8+ policy in:

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

ADSPI-FSMO_RoleMvmt_PDC

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

FSMO roles may be transferred between DCs by an administrator. In addition, a FSMO role will be automatically transferred if a DC 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 DC.

Warning\Error Message Text for Rule 1

Rule 1 is Domain Controller Acquired FSMO Role Ownership| . The warning or error message text for the start action is:

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

You can locate the ADSPI-FSMO_RoleMvmt_PDC policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_RoleMvmt_PDC_2k8+

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

FSMO roles may be transferred between DCs by an administrator. In addition, a FSMO role will be automatically transferred if a DC 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 DC.

Warning\Error Message Text for Rule 1

Rule 1 is Domain Controller Acquired FSMO Role Ownership| . The warning or error message text for the start action is:

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

You can locate the ADSPI-FSMO_RoleMvmt_PDC_2k8+ policy in:

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

ADSPI-FSMO_Consist

The ADSPI-FSMO_Consist policy is a scheduled task policy that performs configuration checks. First the policy identifies the FSMO master operations running on the DC then the policy verifies that the information is also present on the DC's replication partners.

Replication problems can occur when a DC is demoted from a domain and its master operation roles are not transferred to another DC. Such a situation can happen if the DC 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.

Threshold

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. This policy shows the following states:

- 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

You can locate the ADSPI-FSMO_Consist policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC then the policy verifies that the information is also present on the DC's replication partners.

Replication problems can occur when a DC is demoted from a domain and its master operation roles are not transferred to another DC. Such a situation can happen if the DC 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.

Threshold

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. This policy shows the following states:

- 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

You can locate the ADSPI-FSMO_Consist_2k8+ policy in:

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

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 DC 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 DC 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.

Threshold

This policy has the following states as threshold:

- 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)

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: Infrastructure Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>
- End action: 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

You can locate the ADSPI-FSMO_Consist_INFRA policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC 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 DC 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.

Threshold

This policy has the following states as threshold:

- 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)

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: Infrastructure Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>
- End action: 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

You can locate the ADSPI-FSMO_Consist_INFRA_2k8+ policy in:

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

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 DC does not agree with one or more of its replication partners on which machine hosts the FSMO Naming role.

Threshold

This 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 >

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: Domain Naming Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-FSMO_Consist_NAMING policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

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 DC does not agree with one or more of its replication partners on which machine hosts the FSMO Naming role.

Threshold

This 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 >

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: Domain Naming Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-FSMO_Consist_NAMING_2k8+ policy in:

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

ADSPI-FSMO_Consist_PDC

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

Threshold

This 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

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: PDC Emulator FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-FSMO_ConsistP_PDC policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_Consist_PDC_2k8+

The ADSPI-FSMO_Consist_PDC_2k8+ policy receives information generated by the ADSPI-FSMO_Consist scheduled task policy. This policy alarms if the local DC does not agree with one or more of its replication partners on which node hosts the FSMO PDC role.

Threshold

This 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

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: PDC Emulator FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-FSMO_Consist_PDC_2k8+ policy in:

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

ADSPI-FSMO_Consist_RID

The ADSPI-FSMO_Consist_RID scheduled task 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_RID policy alarms if the local DC does not agree with one or more of its replication partners on which machine hosts the FSMO RID role.This policy is used to monitor any DC responsible for processing RID pool requests from all DCs within a given domain.

Threshold

This 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

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: RID Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-FSMO_Consist_RID policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_Consist_RID_2k8+

The ADSPI-FSMO_Consist_RID_2k8+ scheduled task 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_RID_2k8+ policy alarms if the local DC does not agree with one or more of its replication partners on which machine hosts the FSMO RID role.This policy is used to monitor any DC responsible for processing RID pool requests from all DCs within a given domain.

Threshold

This 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

Warning\Error Message Text

The warning or error message text for the start action and end action is:

- Start action: RID Master FSMO Role on domain controller <$MSG_NODE_NAME> is inconsistent with that of the replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-FSMO_Consist_RID_2k8+ in:

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

ADSPI-FSMO_Consist_SCHEMA

The ADSPI-FSMO_Consist_SCHEMA monitors the consistency of the Schema master with replication partners based on consistency state.

Policy Type

Measurement Threshold policy

Policy Group

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → FSMO Monitoring

ADSPI-FSMO_Consist_SCHEMA_2k8+

The ADSPI-FSMO_Consist_SCHEMA_2k8+ monitors the consistency of the Schema master with replication partners based on consistency state.

Policy Type

Measurement Threshold policy

Policy Group

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

GC Monitoring

The GC Monitoring policy is deployed only to Dcs hosting GC services that measures GC replication latency.

ADSPI-Rep_GC_Check_and_Threshold

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

This policy is deployed only on servers hosting GC 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 GC 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 or GC or both on which it is deployed. After it is created, the object timestamp can be modified by the ADSPI-Rep_Modify_User_Object policy. Since GC policies are deployed to every DC or GC, or both, each DC or GC has a specific object stored in the GC.

The ADSPI-Rep_GC_Check_and_Threshold policy checks the current timestamp against the timestamp of objects created by other DC or 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 or GC for more than 24 hours.

Schedule

This policy runs for every 15 minutes.

Threshold

This policy has the 24 hours as threshold.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_GC_Check_and_Threshold policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → GC Monitoring

ADSPI-Rep_GC_Check_and_Threshold_2k8+

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

This policy is deployed only on servers hosting GC services. It works in conjunction with the scheduled task policy ADSPI-Rep_Modify_User_Object_2k8+.

The ADSPI-Rep_GC_Check_and_Threshold_2k8+ policy monitors delay times of GC 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_2k8+ policy. This object, which contains a timestamp, is created specifically for the DC or GC or both on which it is deployed. After it is created, the object timestamp can be modified by the ADSPI-Rep_Modify_User_Object_2k8+ policy. Since GC policies are deployed to every DC or GC, or both, each DC or GC has a specific object stored in the GC.

The ADSPI-Rep_GC_Check_and_Threshold_2k8+ policy checks the current timestamp against the timestamp of objects created by other DC or 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 or GC for more than 24 hours.

Schedule

This policy runs for every 15 minutes.

Threshold

This policy has the 24 hours as threshold.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_GC_Check_and_Threshold_2k8+ policy in:

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

Replication Monitoring Policies

The Replication Monitoring policies are used to monitor replication latency throughout the Microsoft Active Directory forest.

Pre-requisite supporting policies

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+

The replication monitoring executable

The ADSPI_RepMonI.exe has the logic for replication monitoring.

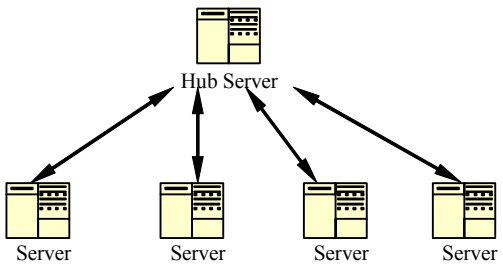
Replication Monitoring Scenarios

You can deploy Replication Monitoring polices in the following scenarios:

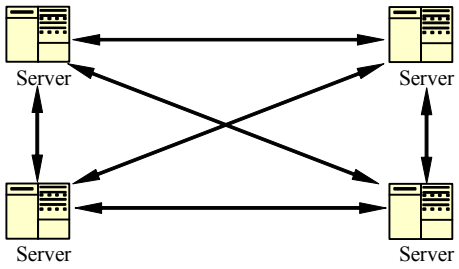
- Intra-Site Replication Monitoring: The policy ADSPI-Rep_MonitorIntraSiteReplication / ADSPI-Rep_MonitorIntraSiteReplication_2k8+ monitors Intra-Site Replication. It checks whether replication is occurring between the DCs having connection objects in the same site.
- Inter-Site Replication Monitoring: 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 occurring between the bridge-head servers of sites.
- A number of Active Directory replication topologies are supported.

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

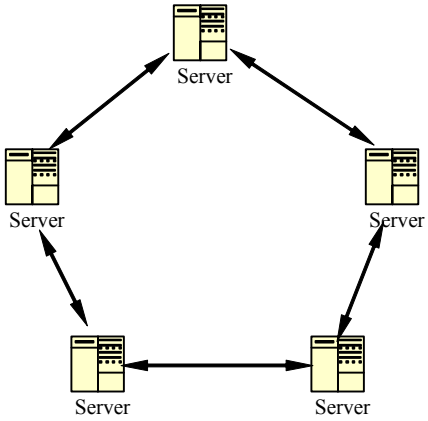
Hub and Spoke Topology Replication Monitoring



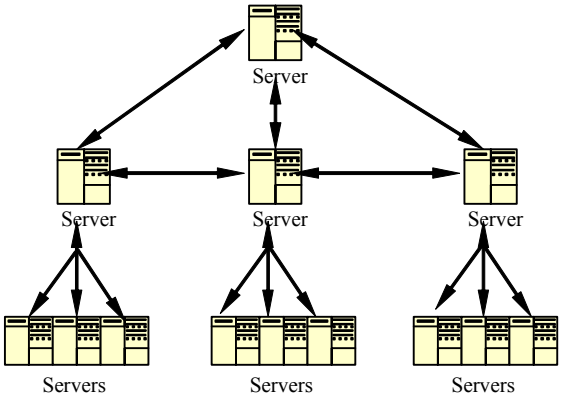
Full Mesh Topology Replication



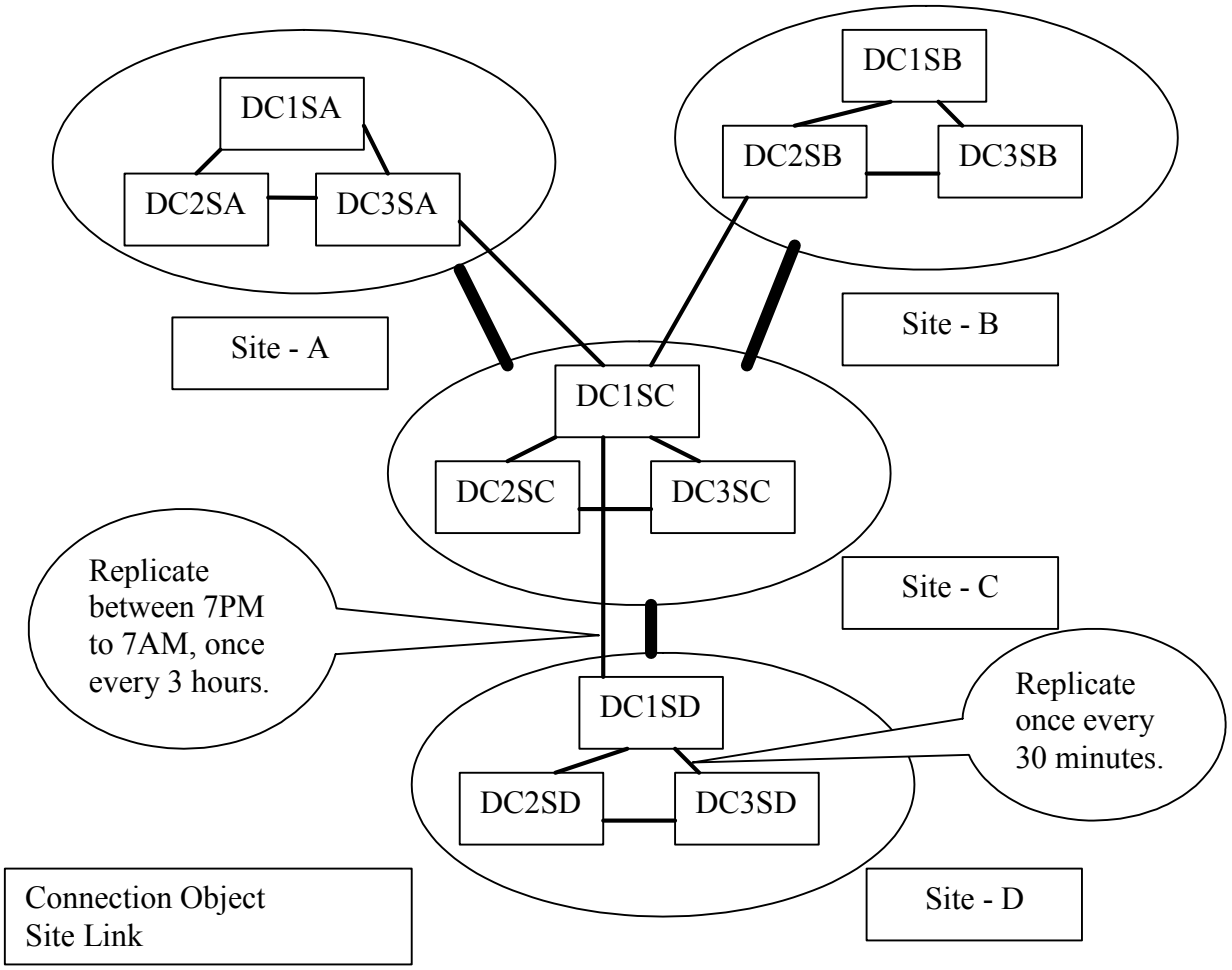
Ring Topology Replication Monitoring



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.

ADSPI-Rep_CheckObj

The ADSPI-Rep_CheckObj policy identifies DCs that do not contain the replication object and issues 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 Microsoft Active Directory forest. This policy works in conjunction with ADSPI-Rep_Modify_User_Object (creates the object to be replicated) policy.

Schedule

This policy runs every 24 hours.

Warning\Error Message Text

The warning or error message text for the start action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_CheckObj policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_CheckObj_2k8+

The ADSPI-Rep_CheckObj_2k8+ policy identifies DCs that do not contain the replication object and issues 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 Microsoft Active Directory forest. This policy works in conjunction with ADSPI-Rep_Modify_User_Object (creates the object to be replicated) policy.

Schedule

This policy runs every 24 hours.

Warning\Error Message Text

The warning or error message text for the start action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_CheckObj_2k8+ policy in:

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

ADSPI-Rep_Delete_OvRep_Object

The ADSPI-Rep_Delete_OvRep_Object policy automatically deletes the **OvReplication** and **OvReplication-<DCName>** objects from a DC 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 DC. These objects are replicated to every other DC 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 gives the following threshold:

- Warning: 24 hours
- Critical: 48 hours

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Rep_Delete_OvRep_Object policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_Delete_OvRep_Object_2k8+

The ADSPI-Rep_Delete_OvRep_Object_2k8+ policy automatically deletes the **OvReplication** and **OvReplication-<DCName>** objects from a DC 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 DC. These objects are replicated to every other DC 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 gives the following threshold:

- Warning: 24 hours
- Critical: 48 hours

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Rep_Delete_OvRep_Object_2k8+ policy in:

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

ADSPI-Rep_InboundObjs

The ADSPI-Rep_InboundObjs policy monitors the number of inbound replication objects for Windows 2003 nodes. This policy measures the DRA inbound object/sec counter.

Schedule

This policy runs every 5 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_InboundObjs policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_InboundObjs_2k8+

The ADSPI-Rep_InboundObjs_2k8+ policy monitors the number of inbound replication objects for Windows 2008 nodes. This policy measures the DRA inbound object/sec counter.

Schedule

This policy runs every 5 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_InboundObjs_2k8+ policy in:

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

ADSPI-Rep_MonitorInterSiteReplication

The ADSPI-Rep_MonitorInterSiteReplication policy monitors whether replication is happening between the bridge-head servers of sites.

Schedule

This policy runs every 4 hours.

Threshold

This policy has the following threshold values:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_MonitorInterSiteReplication policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_MonitorInterSiteReplication_2k8+

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

Schedule

This policy runs every 4 hours.

Threshold

This policy has the following threshold values:

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

Policy Type

Measurement Threshold policy

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_MonitorInterSiteReplication_2k8+ policy in:

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

ADSPI-Rep_MonitorIntraSiteReplication

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

Schedule

This policy runs every 1 hour

Threshold

This policy has the following threshold values:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_MonitorIntraSiteReplication policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

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 1 hour

Threshold

This policy has the following threshold values:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_MonitorIntraSiteReplication_2k8+ policy in:

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

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.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

- Start action: ' 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 action: None

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_ISM_Chk policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

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 cannot calculate the replication topology.

Schedule

This policy runs every 12 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

- Start action: ' 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 action: None

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_ISM_Chk_2k8+ policy in:

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

ADSPI-Rep_Modify_User_Object

The ADSPI-Rep_Modify_User_Object policy identifies DCs that do not contain this replication object and issues an alert when found. This policy updates the OvReplication object on the DCs hosting the policy. This policy is deployed to all managed DC.

This policy works in conjunction with the ADSPI-Rep_GC_Check_and_Threshold by monitoring the replication times of the GC inter-site, and intra-site replication latency.

Schedule

This policy runs every 15 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Rep_Modify_User_Object policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_Modify_User_Object_2k8+

The ADSPI-Rep_Modify_User_Object_2k8+ policy identifies DCs that do not contain this replication object and issues an alert when found. This policy updates the OvReplication object on the DCs hosting the policy. This policy is deployed to all managed DC.

This policy works in conjunction with the ADSPI-Rep_GC_Check_and_Threshold by monitoring the replication times of the GC inter-site, and intra-site replication latency.

Schedule

This policy runs every 15 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Rep_Modify_User_Object_2k8+ policy in:

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

ADSPI-Rep_ModifyObj

The ADSPI-Rep_ModifyObj 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.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Schedule

This policy runs every 30 minutes

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Rep_ModifyObj policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_ModifyObj_2k8+

The ADSPI-Rep_ModifyObj_2k8+ 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.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

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

Schedule

This policy runs every 30 minutes

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Rep_ModifyObj_2k8+ policy in:

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

ADSPI-Rep_TimeSync

The ADSPI-Rep_TimeSync policy validates time synchronization with time master in seconds.

Windows Server operating systems use 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).

The policy measures in seconds the delta between the ‘time master’ and the local host. If the delta exceeds a given threshold, the policy generates an alarm and a message appears in the HPOM message browser. If the delta is 4 minutes or more, it generates a warning; 5 minutes or more - a critical alert.

Schedule

This policy runs for every 15 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

- Start action: The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec.
- End action: The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_TimeSync policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Replication Monitoring

ADSPI-Rep_TimeSync_2k8+

The ADSPI-Rep_TimeSync_2k8+ policy validates time synchronization with time master in seconds.

Windows Server operating systems use 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).

The policy measures in seconds the delta between the 'time master' and the local host. If the delta exceeds a given threshold, the policy generates an alarm and a message appears in the HPOM message browser. If the delta is 4 minutes or more, it generates a warning; 5 minutes or more - a critical alert.

Schedule

This policy runs for every 15 minutes.

Warning\Error Message Text

The warning or error message text for the start action and the end action is:

- Start action: The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> is <$SESSION(value)>sec. It has crossed the critical threshold value of <$SESSION(CriticalThreshold)>sec.
- End action: The time delta between the domain controller <$MSG_NODE_NAME> and the time master <$INSTANCE> no longer exceeds <$SESSION(CriticalThreshold)>sec.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_TimeSync_2k8+ policy in:

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

Response Time Monitoring

The Response Time Monitoring polices are used to monitor the Microsoft Active Directory response times for purposes of checking the general responsiveness of the Microsoft Active Directory.

ADSPI-ResponseTime_Bind

The ADSPI-ResponseTime_Bind policy monitors bind response time in seconds of 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 can tolerate greater bind and query times without any problems, you can increase the warning, critical, and nwConsecLimit values in the script.

It is important to monitor the general responsiveness of Microsoft Active Directory. When the bind and query time to Microsoft Active Directory increases significantly, this is a key indicator that something needs to be investigated. A DC may have gone down and queries are being directed to another DC over a WAN link, or a DC is having resource contention. This policy periodically binds to Microsoft Active Directory and measures latency.

Threshold

This policy has the following threshold:

Warning Level: >1 second

Critical Level: >2 seconds

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-ResponseTime_Bind policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Response Time Monitoring

ADSPI-ResponseTime_Bind_2k8+

The ADSPI-ResponseTime_Bind_2k8+ policy monitors bind response time in seconds of 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 can tolerate greater bind and query times without any problems, you can increase the warning, critical, and nwConsecLimit values in the script.

It is important to monitor the general responsiveness of Microsoft Active Directory. When the bind and query time to Microsoft Active Directory increases significantly, this is a key indicator that something needs to be investigated. A DC may have gone down and queries are being directed to another DC over a WAN link, or a DC is having resource contention. This policy periodically binds to Microsoft Active Directory and measures latency.

Threshold

This policy has the following threshold:

Warning Level: >1 second

Critical Level: >2 seconds

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-ResponseTime_Bind_2k8+ policy in:

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

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 Microsoft Active Directory GC. The GC is used to quickly find an object in Microsoft Active Directory. It is a partial replica of every domain directory in the forest. The GC 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 GC. Only DCs can serve as GC servers.

Threshold

This policy has the following threshold:

Warning Level: >1 second

Critical Level: >2 seconds

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-ResponseTime_GCBind policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Response Time Monitoring

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 Microsoft Active Directory GC. The GC is used to quickly find an object in Microsoft Active Directory. It is a partial replica of every domain directory in the forest. The GC 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 GC. Only DCs can serve as GC servers.

Threshold

This policy has the following threshold:

Warning Level: >1 second

Critical Level: >2 seconds

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-ResponseTime_GCBind_2k8+ policy in:

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

ADSPI-Response_Logging

The ADSPI-Response_Logging scheduled task policy logs Microsoft Active Directory response times for GC searches. The logged response times are available for graphing purposes and aid in base-lining what the value must be for each customer.

Schedule

This policy runs for every 5 minutes.

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Response_Logging policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Response Time Monitoring

ADSPI-Response_Logging_2k8+

The ADSPI-Response_Logging_2k8+ scheduled task policy logs Microsoft Active Directory response times for GC searches. The logged response times are available for graphing

Schedule

This policy runs for every 5 minutes.

Policy Type

Scheduled Task policy

Policy Group

You can locate the ADSPI-Response_Logging_2k8+ in:

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

ADSPI-ResponseTime_Query

The ADSPI-ResponseTime_Query policy measures the general responsiveness of Microsoft Active Directory in seconds. It periodically queries Microsoft Active Directory and monitors latency.

Monitoring the general responsiveness of Microsoft 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

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-ResponseTime_Query policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Response Time Monitoring

ADSPI-ResponseTime_Query_2k8+

The ADSPI-ResponseTime_Query_2k8+ policy measures the general responsiveness of Microsoft Active Directory in seconds. It periodically queries Microsoft Active Directory and monitors latency.

Monitoring the general responsiveness of Microsoft 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

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-ResponseTime_Query_2k8+ policy in:

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

ADSPI-Response Time_GCQuery

The ADSPI-Response Time_GCQuery policy monitors bind response time in seconds of Microsoft Active Directory by measuring the time required to perform a GC search.

The GC is used to quickly find an object in Microsoft Active Directory. It is a partial replica of every domain directory in the forest. The GC 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 GC. Only DCs can serve as GC servers.

Threshold

This policy has the following threshold:

Warning Level: >1 second

Critical Level: >2 seconds

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-Response Time_GCQuery policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Response Time Monitoring

ADSPI-Response Time_GCQuery_2k8+

The ADSPI-Response Time_GCQuery_2k8+ policy monitors bind response time in seconds of Microsoft Active Directory by measuring the time required to perform a GC search.

The GC is used to quickly find an object in Microsoft Active Directory. It is a partial replica of every domain directory in the forest. The GC 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 GC. Only DCs can serve as GC servers.

Threshold

This policy has the following threshold:

Warning Level: >1 second

Critical Level: >2 seconds

Warning Message Text

The warning message text for the start action and the end action is:

- Start action: 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 action: 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

The error message text for the start action and the end action is:

- Start action: 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 action: 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

You can locate the ADSPI-Response Time_GCQuery_2k8+ policy in:

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

SysVol Monitoring

The SysVol Monitoring polices are used to monitor connectivity, space use, and replication as related to SysVol.

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 threshold:

Rule 1: Major

Rule 2: Information, Warning, Error

Warning\Error Message Text

This policy has no warning or error start and end actions.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI-Sysvol_FRS policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Sysvol Monitoring

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 threshold:

Rule 1: Major

Rule 2: Information, Warning, Error

Warning\Error Message Text

This policy has no warning or error start and end actions

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI-Sysvol_FRS_2k8+ policy in:

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

ADSPI-Sysvol_AD_Sync

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

Schedule

This policy runs for every 24 hours.

Threshold

This policy has the following threshold:

Critical >= 2

Warning >= 1

Warning\Error Message Text

This policy has no warning or error start and end actions.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Sysvol_AD_Sync policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Sysvol Monitoring

ADSPI-Sysvol_AD_Sync_2k8+

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

Schedule

This policy runs for every 24 hours.

Threshold

This policy has the following threshold:

Critical >= 2

Warning >= 1

Warning\Error Message Text

This policy has no warning or error start and end actions.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Sysvol_AD_Sync_2k8+ policy in:

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

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 threshold:

Warning Level: Disk full=80%

Critical Level: Disk full=90%

Warning\Error Message Text

The warning and error message text for the start action and the end action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-SysVol_PercentFull policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Sysvol Monitoring

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 threshold:

Warning Level: Disk full=80%

Critical Level: Disk full=90%

Warning\Error Message Text

The warning and error message text for the start action and the end action is:

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-SysVol_PercentFull_2k8+ policy in:

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

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

Warning\Error Message Text

The warning and error message text for the start action and the end action is:

- Start action: The domain controller <$MSG_NODE_NAME> was unable to connect to the Sysvol on its replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-Sysvol_Connectivity policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Sysvol Monitoring

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

Warning\Error Message Text

The warning and error message text for the start action and the end action is:

- Start action: The domain controller <$MSG_NODE_NAME> was unable to connect to the Sysvol on its replication partner <$INSTANCE>.
- End action: 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

You can locate the ADSPI-Sysvol_Connectivity_2k8+ policy in:

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

Trust Monitoring (Windows Server 2003/2008)

The Trust Monitoring policies are used to create the trust report and monitor trust relationship changes between DCs.

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

You can locate the ADSPI_Trust_Mon_Modify policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Trust Monitoring (Windows Server 2003)

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

WMI policy

Policy Group

You can locate the ADSPI_Trust_Mon_Modify_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Trust Monitoring (Windows Server 2008)

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

WMI policy

Policy Group

You can locate the ADSPI_Trust_Mon_Add_Del policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Auto-Deploy → Trust Monitoring (Windows Server 2003)

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

WMI policy

Policy Group

You can locate the ADSPI_Trust_Mon_Add_Del_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Auto-Deploy → Trust Monitoring (Windows Server 2008)

Manual Deploy Policies

The manual deploy policies are not automatically deployed through service discovery. These policies are divided into the following sub-groupings and are available for group or individual deployment.

Auto Baseline Polices

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

- Auto-baseline policies do not work on nodes configured with HP Performance Agent.
- If you have upgraded the Active Directory SPI from an older version, the auto-baseline policies will 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.

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

You can locate the ADSPI-Rep_InboundObjects_AT policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Auto Baseline Polices

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

You can locate the ADSPI-Rep_InboundObjects_AT_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Auto Baseline Polices

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

You can locate the ADSPI-Rep_TimeSync_Monitor_AT policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Auto Baseline Polices

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

You can locate the ADSPI-Rep_TimeSync_Monitor_AT_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Auto Baseline Polices

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 GC inter- and intra-site replication.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Auto Baseline Polices

ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+

This is an auto-threshold policy which monitors delay times of GC inter- and intra-site replication.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Auto Baseline Polices

Connector Polices

The Connector policies monitors the Microsoft Active Directory performance monitor counters.

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, the existing DCs must be upgraded or additional DCs must be installed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ActiveAuthKerberos policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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, the existing DCs must be upgraded or additional DCs must be installed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ActiveAuthLogon policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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, the existing DCs must be upgraded or additional DCs must be installed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ActiveAuthNTLM policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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 policy

Policy Group

You can locate the ADSPI_ADCFwdAllWarnErrorMSADC policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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

Policy Group

You can locate the ADSPI_ADCImportFailures policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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

You can locate the ADSPI_ADCPageFaults policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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

You can locate the ADSPI_ADCPrivateBytes policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

ADSPI_ADCProcessorTime

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

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

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADCProcessorTime policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

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

You can locate the ADSPI_ADCWorkingSet policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Connector

Domain and OU Structures Policies

The Domain and OU Structures policies monitors domain and organizational unit (OU) changes.

ADSPI_DomainChanges

The ADSPI_DomainChanges policy checks for changes to the domain structure approximately every 20 minutes.

It has the following details:

- 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.

Policy Type

WMI policy

Policy Group

You can locate the ADSPI_DomainChanges policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Domain and OU Structure

ADSPI_DomainChanges_2k8+

The ADSPI_DomainChanges_2k8+ policy checks for changes to the domain structure approximately every 20 minutes.

It has the following details:

- 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.

Policy Type

WMI policy

Policy Group

You can locate the ADSPI_DomainChanges_2k8+ policy in:

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

ADSPI_OUChanges

The ADSPI_OUChanges policy Checks for changes to the OU structure approximately every 20 minutes.

It has the following details:

- 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 Microsoft Active Directory database.

Deploy this policy on a DC only.

Policy Type

WMI policy

Policy Group

You can locate the ADSPI_OUChanges policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Domain and OU Structure

ADSPI_OUChanges_2k8+

The ADSPI_OUChanges_2k8+ policy Checks for changes to the OU structure approximately every 20 minutes.

It contains the following details:

- 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 Microsoft Active Directory database.

Deploy this policy on a DC only.

Policy Type

WMI policy

Policy Group

You can locate the ADSPI_OUChanges_2k8+ policy in:

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

Global Catalog Access Policies

Global Catalog Access policies monitor the performance monitor counters on GC servers. Deploy these polices to the GC server only.

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 GC. 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 needs additional hardware or an additional DC is needed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_GlobalCatalogWrites policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Global Catalog Access

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 GC. 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 needs additional hardware or an additional DC is needed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_GlobalCatalogWrites_2k8+ policy in:

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

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 GC. 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 needs additional hardware or an additional DC is needed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_GlobalCatalogReads policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Domain and OU Structure

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 GC. 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 needs additional hardware or an additional DC is needed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_GlobalCatalogReads_2k8+ policy in:

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

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 domain controller needs additional hardware or an additional domain controller is needed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_GlobalCatalogSearches policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Domain and OU Structure

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 GC. 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 needs additional hardware or an additional DC is needed.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_GlobalCatalogSearches_2k8+ policy in:

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

Health Monitor Policies

The Health Monitor policies monitor the health of DNS, Kerberos and NetLogon Services.

ADSPI_DNSServ_FwdAllInformation

The ADSPI_DNSServ_FwdAllInformation policy monitors the DNS Server log for entries that have a severity level of Information and forwards these entries as messages to the active message browser.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_DNSServ_FwdAllInformation policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

ADSPI_DNSServ_FwdAllInformation_2k8+

The ADSPI_DNSServ_FwdAllInformation_2k8+ policy monitors the DNS Server log for entries that have a severity level of Information and forwards these entries as messages to the active message browser.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_DNSServ_FwdAllInformation_2k8+ policy in:

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

ADSPI_DNSServ_FwdAllWarnError

The ADSPI_DNSServ_FwdAllWarnError policy monitors the DNS Server log for entries that have a severity level of Warning or Error and forwards these entries as messages to the active message browser.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_DNSServ_FwdAllWarnError policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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 and forwards these entries as messages to the active message browser.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_DNSServ_FwdAllWarnError_2k8+ policy in:

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

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

You can locate the ADSPI_FwdAllInformationDS policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_FwdAllInformationDS_2k8+ policy in:

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

ADSPI_FwdAllInformationFRS

The ADSPI_FwdAllInformationFRS policy monitors the File Replication 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

You can locate the ADSPI_FwdAllInformationFRS policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

ADSPI_FwdAllInformationFRS_2k8+

The ADSPI_FwdAllInformationFRS_2k8+ policy monitors the File Replication 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

You can locate the ADSPI_FwdAllInformationFRS_2k8+ policy in:

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

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

You can locate the ADSPI_FwdAllWarnErrorDS policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_FwdAllWarnErrorDS_2k8+ policy in:

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

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

You can locate the ADSPI_FwdAllWarnErrorFRS policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_FwdAllWarnErrorFRS_2k8+ policy in:

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

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

You can locate the ADSPI_HMLSASSPageFaults policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_HMLSASSPageFaults_2k8+ policy in:

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

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMLSASSPrivateBytes policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMLSASSPrivateBytes_2k8+ policy in:

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

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, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMLSASSProcessorTime in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMLSASSProcessorTime_2k8+ policy in:

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

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMLSASSWorkingSet policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMLSASSWorkingSet_2k8+ policy in:

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

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

You can locate the ADSPI_HMNTFRSPageFaults policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_HMNTFRSPageFaults_2k8+ policy in:

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

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMNTFRSPrivateBytes policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMNTFRSPrivateBytes_2k8+ policy in:

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

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, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMNTFRSProcessorTime policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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, the server may be overloaded, need a hardware upgrade, or need further tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMNTFRSProcessorTime_2k8+ policy in:

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

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMNTFRSWorkingSet policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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 may be a memory leak or some other memory problems.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMNTFRSWorkingSet_2k8+ policy in:

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

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 must be used.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMThreadsInUse policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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 must be used.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_HMThreadsInUse_2k8+ policy in:

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

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

You can locate the ADSPI_KDC policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_KDC_2k8+ policy in:

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

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

You can locate the ADSPI_NetLogon policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

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

You can locate the ADSPI_NetLogon_2k8+ policy in:

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

ADSPI_NTFRS

The ADSPI_NTFRS policy checks whether the FRS 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

You can locate the ADSPI_NTFRS policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

ADSPI_SamSs

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

Type

Measurement Threshold (Source: Program)

Policy Group

You can locate the ADSPI_SamSs policy in:

ADSPI_SamSs_2k8+

The ADSPI_SamSs_2k8+ policy checks whether the Security Accounts Manager (SAM) service and its corresponding process, lsass.exe, are running. If they are not running, the policy sends a warning message to the active message browser. The operator can restart the service using an operator-initiated command. When the service is running again, the policy acknowledges the message.

Type

Measurement Threshold (Source: Program)

Policy Group

You can locate the ADSPI_SamSs_2k8+ policy in:

ADSPI_SMTPEventLogs

The ADSPI_SMTPEventLogs policy monitors the System log for SMTP-specific events and forwards them as messages to the active message browser.

Type

Windows Event Log (System)

Policy Group

You can locate the ADSPI_SMTPEventLogs policy in:

ADSPI_SMTPEventLogs_2k8+

The ADSPI_SMTPEventLogs policy monitors the System log for SMTP-specific events and forwards them as messages to the active message browser.

Type

Windows Event Log (System)

Policy Group

You can locate the ADSPI_SMTPEventLogs policy in:

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, the server may be overloaded, need a hardware upgrade, or require further replication tuning to optimize performance.

This policy logs the value of PerfLib counter NTDS\DRA Sync Failures on Schema Mismatch.

Type

Measurement Threshold (Source: Real Time Performance Management)

Policy Group

You can locate the ADSPI_SyncSchemaMisMatch policy in:

ADSPI_SyncSchemaMisMatch_2k8+

The ADSPI_SyncSchemaMisMatch_2k8+ policy checks the PerfLib counter DirectoryServices\DRA Sync Failures on Schema Mismatch for the number of synchronization failures. If the number exceeds 1, the policy sends a warning message to the active message browser. If the number exceeds 4, the policy sends an error message. If the number exceeds the upper threshold, the server may be overloaded, need a hardware upgrade, or require further replication tuning to optimize performance.

This policy logs the value of PerfLib counter DirectoryServices\DRA Sync Failures on Schema Mismatch.

Type

Measurement Threshold (Source: Real Time Performance Management)

Policy Group

You can locate the ADSPI_SyncSchemaMisMatch_2k8+ policy in:

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

You can locate the ADSPI_DFSR_2k8+ policy in:

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

ADSPI_NTDS_2k8+

The ADSPI_NTDS_2k8+ policy checks if the Microsoft Active Directory Domain service and lsass.exe process are running on the Microsoft 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 Microsoft Active Directory Domain service starts running again, the policy acknowledges the message.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_NTDS_2k8+ policy in:

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

ADSPI_Logging

The ADSPI_Logging policy monitors the following details from various performance monitor objects as shown in the Table.

Table 1 Performance Monitor Objects of ADSPI_Logging

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	

Performance Monitor Object	Counter	Instance
	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

You can locate the ADSPI_Logging in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Health Monitors

ADSPI_Logging_2k8+

The ADSPI_Logging_2k8+ policy monitors the following details from various performance monitor objects as shown in the Table.

Table 2 Performance Monitor Objects of ADSPI_Logging

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

You can locate the ADSPI_Logging_2k8+ policy in:

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

ADSPI_NtLmSsp

The ADSPI_NtLmSsp policy checks the NT LM Security Support Provider Service.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_NtLmSsp policy in:

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

Index and Query Monitor Policies

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

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 domain controller may be overloaded with logon authentication traffic.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQKerberosAuthentications policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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 domain controller may be overloaded with logon authentication traffic.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQKerberosAuthentications_2k8+ policy in:

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

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 domain controller may be overloaded with LDAP queries.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQLDAPActiveThreads policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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 domain controller may be overloaded with LDAP queries.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQLDAPActiveThreads_2k8+ policy in:

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

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 domain controller may be overloaded with LDAP queries.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQLDAPBindTime policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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 domain controller may be overloaded with LDAP queries.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQLDAPBindTime_2k8+ policy in:

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

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 domain controller may be overloaded with LDAP queries.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQLDAPClientSessions policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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 domain controller may be overloaded with LDAP queries.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQLDAPClientSessions_2k8+ policy in:

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

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 may be overloaded with logon authentication traffic.

Policy Type

Measurement Threshold (Source: Real Time Performance Management)

Policy Group

You can locate the ADSPI_IQNTLMAuthentications policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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 may be overloaded with logon authentication traffic.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_IQNTLMAuthentications_2k8+ policy in:

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

ADSPI_DSSearches

The ADSPI_DSSearches policy evaluates the Number of searches every second in the Directory Service.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_DSSearches policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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

You can locate the ADSPI_DSSearches_2k8+ policy in:

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

ADSPI_DSReads

The ADSPI_DSReads policy evaluates the Number of reads every second in the Directory Service.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_DSReads policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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

You can locate the ADSPI_DSReads_2k8+ policy in:

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

ADSPI_DSWrites

The ADSPI_DSWrites policy evaluates the Number of writes every second in the Directory Service.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_DSWrites policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Index and Query Monitors

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

You can locate the ADSPI_DSWrites_2k8+ policy in:

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

Replication Policies

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.

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, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSPendingSynchronizations policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Replication

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, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSPendingSynchronizations_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Replication

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, the Active Directory replication may need to be optimized.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepInBoundBytesBetweenSites policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Replication

ADSPI_ADSRepInBoundBytesBetweenSites_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, the Active Directory replication may need to be optimized.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepInBoundBytesBetweenSites_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Replication

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, the Microsoft Active Directory replication may need to be optimized.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepInBoundBytesWithinSites policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Replication

ADSPI_ADSRepInBoundBytesWithinSites_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, the Microsoft Active Directory replication may need to be optimized.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepInBoundBytesWithinSites_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Replication

ADSPI_ADSRepInBoundObjectUpdatesRemaining

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, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepInBoundObjectUpdatesRemaining policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Replication

ADSPI_ADSRepInBoundObjectUpdatesRemaining_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, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepInBoundObjectUpdatesRemaining_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Replication

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, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepNotifyQueueSize policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Replication

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, the server may be overloaded, need a hardware upgrade, or need further replication tuning to optimize performance.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_ADSRepNotifyQueueSize_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Replication

Replication Activities Polices

The Replication Activities policies monitor the Directory Service log for replication events.

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

You can locate the ADSPI_ReplicationActivities policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Replication Activity

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

You can locate the ADSPI_ReplicationActivities_2k8+ policy in:

Policy Bank → SPI for Active Directory → Windows Server 2008 → Manual-Deploy → Replication Activity

Securities Polices

The Securities policies monitor:

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

ADSPI_DirUserCreationDeletionModification

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

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_DirUserCreationDeletionModification policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

ADSPI_DirUserCreationDeletionModification_2k8+

The ADSPI_DirUserCreationDeletionModification_2k8+ policy checks, approximately every 15 minutes, whether any accounts in Directory User Accounts have been created, deleted, or modified. If any have, the policy sends a message to the active message browser.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_DirUserCreationDeletionModification_2k8+ policy in:

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

ADSPI_KDCFailureGrantTicket

The ADSPI_KDCFailureGrantTicket policy monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 676 in the Security Event Log as:

672 and 676 Authentication Ticket Request Failed

Deploy this template only to servers running KDC.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_KDCFailureGrantTicket policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

ADSPI_KDCFailureGrantTicket_2k8+

The ADSPI_KDCFailureGrantTicket_2k8+ policy monitors the Security log for failures to grant authentication tickets. Failures are indicated by event 676 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

You can locate the ADSPI_KDCFailureGrantTicket_2k8+ policy in:

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

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 does not let you choose which rights to audit. As a result, auditing Use of User Rights will generate a very large number of audits. In most cases, the sheer volume of this information outweighs its usefulness. Do not audit Use of User Rights unless absolutely necessary for your environment. If you decide to audit Use of User Rights, you must 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

You can locate the ADSPI_PrivilegedAccounts policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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 must 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

You can locate the ADSPI_PrivilegedAccounts_2k8+ policy in:

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

ADSPI_SecAdminGroupChangeMon

The ADSPI_SecAdminGroupChangeMon policy monitors changes that occur in the Domain Admins group and the Enterprise Admins security group. The polices also inform about what change occurred, who changed it, and when it was changed.

Use this policy for Windows Server 2003 nodes.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_SecAdminGroupChangeMon policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

ADSPI_SecAdminGroupChangeMon_2K8+

The ADSPI_SecAdminGroupChangeMon_2k8+ policy monitors changes that occur in the Domain Admins group and the Enterprise Admins security group. The polices also inform about what change occurred, who changed it, and when it was changed.

Use this policy for Windows Server 2008 nodes.

Policy Type

Windows Event Log policy

Policy Group

You can locate the ADSPI_SecAdminGroupChangeMon_2k8+ policy in:

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

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

You can locate the ADSPI_SecDirectoryServiceAccess policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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

You can locate the ADSPI_SecDirectoryServiceAccess_2k8+ policy in:

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

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

You can locate the ADSPI_SecErrAccessPermissions policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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

You can locate the ADSPI_SecErrAccessPermissions_2k8+ policy in:

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

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

You can locate the ADSPI_SecErrGrantedAccess policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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

You can locate the ADSPI_SecErrGrantedAccess_2k8+ policy in:

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

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

You can locate the ADSPI_SecErrorsLogon policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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

You can locate the ADSPI_SecErrorsLogon_2k8+ policy in:

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

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, the domain may be overloaded.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_SecNonTransMembEval policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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, the domain may be overloaded.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_SecNonTransMembEval_2k8+ policy in:

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

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, the domain controller may be overloaded.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_SecSDPropagatorQueue policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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, the domain controller may be overloaded.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_SecSDPropagatorQueue_2k8+ policy in:

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

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 ends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_SecTransMembEval policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

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 ends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

Policy Type

Measurement Threshold policy

Policy Group

You can locate the ADSPI_SecTransMembEval_2k8+ policy in:

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

ADSPI_DirComputerModif

The ADSPI_DirComputerModif policy sends alert messages if there is any modification to a computer in the domain.

Policy Type

WMI policy

Policy Group

You can locate the ADSPI_DirComputerModif policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Security

ADSPI_DirComputerModif _2k8+

The ADSPI_DirComputerModif _2k8+ policy sends alert messages if there is any modification to a computer in the domain.

Policy Type

WMI policy

Policy Group

You can locate the ADSPI_DirComputerModif _2k8+ policy in:

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

Site-Structure Polices

The Site_Structure policies monitor the site changes.

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.

This policy has the following details:

- 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 Microsoft 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

WMI policy

Policy Group

You can locate the ADSPI_SiteChanges policy in:

Policy Bank → SPI for Active Directory → Windows Server 2003 → Manual-Deploy → Site Structure

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.

This policy has the following details:

- 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 Microsoft 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

WMI policy

Policy Group

You can locate the ADSPI_SiteChanges_2k8+ policy in:

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

2 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 launch tools to view the Microsoft Active Directory environment.

Active Directory Self Healing Info tool

The Microsoft Active Directory SPI Self-Healing Info tool collects data that aid in the troubleshooting 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 or patches.

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 Microsoft Active Directory SPI and the ADSPI executables present on the system.

AD DC Demotion Preparation tool

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

Check ADS Service Tool

The Check ADS Service tool connects to the ADS service of the specific node using the Microsoft Active Directory SPI.

ADS Printer Information tool

The ADS Printer Information tool lists all printers known to Active Directory. You can restrict the output to specific Organizational Units (OU) by using the parameters **`-ou (name of OU)`** instead of **`-all`**.

Delete Older ADSPI Classes tool

If you want to upgrade the Microsoft Active Directory SPI, you must run the Delete Older ADSPI Classes tool on all nodes during the upgrade process. The tool removes all data tables created by the older version of the SPI from the managed node. Refer to the *Installation and Configuration Guide* for a detailed information on the upgrade process.

HP Operations Topology Viewer

The HP Operations Topology Viewer displays the Microsoft Active Directory environment in a hierarchical view as a tree and a topological view in a map. The tree shows the partition, site, and site link components, and the map graphically represents sites and site links and server connections.

After launching the HP Operations Topology Viewer and entering DC access information, the tool gathers data from the DC. From this information a map is created, displaying sites and servers and their replication relationships across the domain.

The HP Operations Topology Viewer tool operates on Windows and not on HP–UX, Solaris, and Linux. So start it on a 32-bit Windows system. This tool is not listed in the **Tool Bank** under **SPI for Active Directory**. For more details on starting the tool, see *Starting HP Operations Topology Viewer Tool* in *HP Operations Smart Plug-in for Microsoft Active Directory Installation and Configuration Guide*.

HP Operations Topology Viewer map

Map connection lines labels: You can choose the connection lines to display and whether to display server and site labels by right-clicking the map and 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 existed but are no longer valid. These previous connections are represented by a red line drawn (as solid or dashes) 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.

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 FileRefresh Data. The map is then updated.

AD Trust Relationships Tool

The AD Trust Relationships tool generates a quick list of the trust relationships established for the selected node.

3 Reports

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

➤ The *HP Operations Smart Plug-in for Microsoft Active Directory Installation and Configuration Guide* contains information about the policies 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 appear immediately in the HPOM console tree as they are generated every night. After HPOM runs through its first nightly schedule, on the next day you can see reports. Each night from that point on HPOM, by default, re-generates reports with the updated daily data.

Daily, Weekly, and Monthly Reports

Reports are identified as daily, weekly, or monthly and update as follows:

- Daily: Updated nightly. A daily report reflects the last 24 hours data. (The previous report data is deleted.)
- Weekly: Updated weekly. A weekly report reflects the last seven days 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.

  ➤ The first monthly report may represent a partial month's data. For example, if the Microsoft Active Directory SPI installation occurred on March 18, the first report is available on April 1 and includes data from March 19 to the last day of March.

AD DC DNS Availability (Daily and Weekly)

The AD DC DNS Availability report (daily and weekly) summarizes the availability of the DC's DNS based on a daily and weekly basis respectively. The daily report provides a percentage of the DNS availability based on each hour over the last 24 hours, and the weekly report is based on hourly averages over the last seven-day period.

The Report Template File Names of these reports are *g_ADDNSDCAvailDaily.rpt* and *g_ADDNSDCAvailWeekly.rpt*

Report Contents

The columns of this report are defined as follows:

- *Computer Name* - Name of each computer specified in the report criteria.
- *Availability* - Percentage of time the DNS server was available during the time specified in the report criteria.

AD DIT Disk Queue Length (weekly)

The AD DIT Disk Queue Length report (weekly) summarizes the weekly queue length patterns of the disk holding the DIT for the DCs. This information helps to identify DCs with potential disk bottlenecks.

The Report Template File Name of this report is *g_ADDITQueueLengthWeekly.rpt*

Report Contents

The columns of this report are defined as follows:

- *System Name* - Name of the DC.
- *Domain Name* - Name of the domain that the DC belongs to.
- *Site Name* - Time at which the disk space data was collected.
- *DIT Path* - DIT database path location.
- *Queue Length* - Disk Queue Length on DIT Disk.

AD DIT Disk Size Summary (weekly and monthly)

The AD DIT Disk Size Summary report (weekly and monthly) shows bar chart (weekly) and line chart (monthly). This report summarizes the usage patterns of the disk holding the DIT for the DCs. This information helps to identify DCs with potential disk bottlenecks.

The Report Template File Names of these reports are *g_ADDITDiskSpaceWeekly.rpt* and *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:

System Name - Name of the DC.

Domain Name - Name of the domain that the DC belongs to.

Site Name - Time at which the disk space data was collected.

DIT Size - Size of the DIT Database in MB.

%Disk Space Full - Percentage used space on the disk holding the DIT database.

AD DNS Server Memory Capacity Planning (weekly and monthly)

The AD DNS Server Memory Capacity Planning report (weekly and monthly) graphs the memory capacity for each specified DNS server running Microsoft Active Directory services for a week and month respectively.

The graph indicates the minimum, maximum, and average daily usage based on the Memory/ Pages Per Second performance counter.

The Report Template File Names of these reports are *g_ADDNSSrvMemCapPlanMonthly.rpt* and *g_ADDNSSrvMemCapPlanWeekly.rpt*.

Report Contents

The 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.

AD DNS Server Availability (daily and weekly)

The AD DNS Server Availability report (daily and weekly) summarizes the availability of DNS servers with Microsoft Active Directory services running, based on hourly and weekly data respectively. The daily report shows a percentage of availability based on each hour over the last 24-hour period. The weekly report shows hourly percentages based on each hour over the last 7-day period.

The Report Template File Names of these reports are *g_ADDNSSrvAvailDaily.rpt* and *g_ADDNSSrvAvailWeekly.rpt*.

Report Contents

The report contains a pie chart displaying the percentage of available DNS servers with Microsoft Active Directory services running.

The columns of the report are defined as follows:

- *Response Time in milliseconds* - Response time of the DNS server in milliseconds.
- *Date time* - Date and time when the data was gathered.

AD Domain Controller Availability

The AD Domain Controller Availability report displays the percentage of time Microsoft Active Directory and the GC were successfully connected to and queried. The data is displayed in a series of pie charts. Possible causes of falling availability are lack of system resources, mis-configuration, or failures in Microsoft Active Directory.

The Report Template File Name of this report is *g_ADDCAvailability.rpt*.

Report Contents

The report displays two pie charts, which are described as follows:

Active Directory Availability: The Microsoft Active Directory SPI periodically queries the directory on the DC in your environment to determine response time and availability. This graph shows the percentage of time the directory was contacted successfully.

Active Directory Global Catalog Availability: The Microsoft Active Directory GC is queried on the port 3268. The success of the attempt is used to calculate GC availability.

The report displays a table that lists the following details:

- *GC Availability* - Availability of GC, queried on the port 3268, during a particular range of time.
- *Date Time* - Date and time when the data was gathered.

AD Domain and Forest Changes (weekly and monthly)

The AD Domain and Forest Changes report (weekly and monthly) presents the domain and forest trust changes in Microsoft Active Directory for the selected report: either weekly or monthly. The report provides information illustrating addition, deletion and modification of trusts on Windows Server 2003 and 2008 DCs only.

The Report Table File Names for these reports are *g_ADDomainForestTrustMonthly.rpt* and *g_ADDomainForestTrustWeekly.rpt*.

Report Contents

In this report, a table displays the following details:

- *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 is Disallow Transitivity
  - 2 is Uplevel clients only
  - 4 denotes the trust setting to another tree root in the forest
  - 32 denotes the trust setting to the parent in the organization tree
- *Direction*: A value that indicates the direction of Trust:
  - 1 is Inbound
  - 2 is Outbound
  - 3 is Bi-directional
- *Trust Status*: String description of trust status.
- *Trust Type*: A value that indicates the type of the trust relationship:
  - 1 is Downlevel
  - 2 is Uplevel
  - 3 is Non-Windows Kerberos Realm
  - 4 is DCE

AD GC Replication Delay Times by DC/GC (weekly and monthly)

The AD GC Replication Delay Times by DC/GC report (weekly and monthly) report summarizes delay times for replication from DC to GC servers. Weekly reports show the average, maximum, and minimum replication delays occurring over the last 7 days, and monthly reports show averages from the last calendar month.

The provided information helps to identify GC replication trends and potential replication problems. The report specifies a date range in which the data collection took place.

The Report Template File Names of these reports are *g_ADDCGCweekly.rpt* and *g_ADDCGCmonthly.rpt*.

Report Content

This report displays a bar graph showing the average replication delay per GC server for every DC.

AD GC Rep Delay Times By GC/DC (weekly and monthly)

The AD GC Rep Delay Times By GC/DC report (weekly and monthly) report summarizes delay times for replication from a GC server to each DC. Weekly reports show the replication delays as they are averaged over the last seven days. Monthly reports show replication delays as they are averaged over the last calendar month.

This information helps to identify GC replication trends and potential replication problems. The report specifies a date range in which the data collection took place.

The Report Template File Names of these reports are *g_ADGCDCweekly.rpt* and *g_ADGCDCmonthly.rpt*.

Report Contents

This report displays a bar graph showing the average replication delay per DC for every GC server.

AD GC Response Time (weekly and monthly)

The AD GC Response Time report (weekly and monthly) summarizes the average response times of GC servers. The information contained in this report helps identify GC servers with potential over-loading and bottlenecks.

The weekly report shows averages occurring over the last seven-day period, and the monthly report shows averages over the last calendar month. Each report identifies the data collection period with a start and end date range.

Response times are based on the GC queries and binds that are shown in a graph. The graph shows averages for each of the GC servers. Using this information you can identify those GC servers that are over-loaded and take appropriate actions.

The Report Template File Names of these reports are *g_ADGCResponseTimeWeekly.rpt* and *g_ADGCResponseTimeMonthly.rpt*.

Report Contents

This report shows a chart that shows the weekly average query and bind response times (in seconds) on each GC server. Using this graph, you can identify the events when the GC server was over-loaded and take appropriate actions.

AD Log Files Disk Queue Length (weekly)

The AD Log Files Disk Queue Length report (weekly) 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.

The Report Table File Name of this report is *g_ADLogQueueLengthWeekly.rpt* / *g_ADLogQueueLengthMonthly.rpt*.

Report Contents

The columns of this report are defined as follows:

- *System Name* - Name of the DC.
- *Domain Name* - Name of the Domain that the DC belongs to.
- *Site Name* - Time at which the disk space data was collected.
- *Log Files Path* - Log files path location.
- *Queue Length* - Disk Queue Length on the log files disk.

AD Log Files Disk Size Summary (weekly and monthly)

The AD Log Files Disk Size Summary report (weekly and monthly) 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.

The Report Template File Names of these reports are *g_ADLogFilesDiskSpaceWeekly.rpt* and *g_ADLogFilesDiskSpaceMonthly.rpt*.

Report Contents

The columns of the report are defined as follows:

- *System Name* - Name of the DC.
- *Domain Name* - Name of the Domain to which the DC belongs.
- *Site Name* - Site in which the DC 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.

Active Directory Memory Usage

The Active Directory 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.

The Report Template File Name of this report is *g_ADMemoryUsage.rpt*.

Report Contents

The report contains the following two sections:

- *Active Directory LSASS Page Faults Average*—This section 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 processr. If a thread refers to a virtual-memory page, which is not available in its working set inside the main memory, the page fault occurs.
- *Active Directory LSASS Working Set Average*—This section displays usage patterns for 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 use. If the free memory falls below the threshold, pages are removed from working sets.

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 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 the following:

- FSMO type, and then by DC, or
- Server, and then by DC

There is one graph by FSMO service/DC.

The Report Template File Name of this report is *g_ADOpMstrConTimeByFsmo.rpt* / *g_ADOpMstrConTimeBySvr.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)

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/DC.

The Report Template File name of this report is *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)

Active Directory Processor Usage

The Active Directory Processor Usage report examines the Microsoft Active Directory processor-usage pattern from the logged data.

The report displays general usage patterns between DCs.

The Report Template File Name of this report is *g_ADProcessUsage.rpt*.

Report Contents

The report presents two sections:

- *Active Directory Average LSASS Percent Processor Time / sec*—This section displays the average percentage of processor time used by all threads of the LSASS process to run instructions.
- *Active Directory Average Number of Threads / sec*—This section displays the average usage patterns for 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 are serving the client API calls.

Active Directory Replication Inbound

The Active Directory Replication Inbound report examines the Microsoft Active Directory replication usage pattern from the logged data. The report allocates the replication-transmission statistics of intra-site replication and replication among different sites and shows the usage pattern of inbound Microsoft Active Directory replication.

The Report Template File Name of this report is *g_ADReplicationInbound.rpt*.

Report Contents

This report presents a graph that shows the average of Inbound Bytes Replicated per second within a site and Inbound Bytes Replicated per second among different sites by the Microsoft Active Directory Service for all monitored nodes.

Active Directory Replication Outbound

The Active Directory Replication Outbound report examines the Microsoft Active Directory replication usage pattern from the logged data. The report allocates the replication-transmission statistics of intra-site replication and replication among different sites and shows the usage pattern of outbound Microsoft Active Directory replication.

The Report Template File Name of this report is *g_ADReplicationOutbound.rpt*.

Report Contents

This report presents a graph showing the average of Outbound Bytes Replicated per second within a site and Outbound Bytes Replicated per second among different sites by the Microsoft Active Directory Service for all monitored nodes.

Active Directory Replication Summary

The Active Directory Replication Summary report examines the Microsoft Active Directory replication usage pattern from the logged data. The report allocates the replication-transmission statistics intra-site replication and replication among different sites and shows an overall usage pattern of Microsoft Active Directory replication.

The Report Template File Name of this report is *g_ADReplicationSummary.rpt*.

Reports Contents

The report shows the following attributes:

- Inbound Bytes Received/sec—represents the number of bytes received for replication during the monitored period.
- Outbound Bytes Transmitted/sec—represents the number of bytes transmitted by the system for replication during the monitored period.

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.

AD Size of SysVol (weekly and monthly)

The AD Size of SysVol report (weekly and monthly) provides a weekly and monthly summary respectively, of the Sysvol (system volume shared directory on the DC) disk space information for the specified DC.

The Report Template File Names of these reports are *g_ADSizeOfSysvolWeekly.rpt* and *g_ADSizeOfSysvolMonthly.rpt*.

Report Contents

The report presents a line graph indicating the percentage of occupied disk space on sysVol drives.

The columns of this report are defined as follows:

- Domain Computer Name - Name of each computer specified in the report criteria.
- Time of Collection - 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.

Troubleshooting Microsoft Active Directory SPI Reports

If any report is not generated or if it is empty, perform the following tasks:

Task 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 check if data for a particular metric is being collected. See Table 3 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.

Task 2: Check the Reporter Package Installation

1. Check if the Microsoft Active Directory SPI Reporter package is 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.

Task 3: Check the Data store.

1. If there is no data in the Reporter database and the Microsoft Active Directory SPI Reporter package is installed properly, check that the data is being collected 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`**
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`**
4. Check if the acknowledged messages queue was acknowledged.
5. If you are using the HP Performance Agent, refer to the HP Performance Agent documentation.

Task 4: Check if the policies are deployed.

There is no data if the particular policy for each report is not deployed. See Appendix B, Report, Report Table, Data Store, and Policy Mapping Details table to know the policy for each report. Check the managed node to ensure that the policy was deployed and is enabled by running the command on HTTPS nodes **`ovpolicy.`**

Task 5: Check if the agent on the managed node is running

1. Check if HP Operations agent is running.
2. Run the following command on the managed node to get status of the agent on HTTPS-managed nodes:

   ```
   ovc -status
   ```

3. If the HP Operations agent is not running, restart using the following command on the HTTPS-managed nodes:

   ```
   ovc -start
   ```

Table 3 Report mapping to the SQL Command

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`

Report Name	SQL Command
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`

4 Graphs

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

Microsoft Active Directory SPI Graphs

After you install the Microsoft Active Directory SPI and data is accumulated, you can use the HPOM graphing feature to generate graphs. Graphs allow you to choose a system and date or time range to view customized data.

Active Directory GC Availability

The Microsoft Active Directory SPI includes the Active Directory GC Availability graph that shows the general availability of the GC on the systems hosting GC services.

To calculate availability of the GC on each Microsoft Active Directory node, the Microsoft Active Directory GC service is queried on port 3268. Each successful attempt is counted and logged per collection interval.

➤ To generate the Active Directory GC Availability graph you must deploy the ADSPI-Response_Logging policy.

Active Directory Replication Latency

The Microsoft Active Directory SPI includes the Active Directory Replication Latency graph to help you establish baselines for the frequency of the replication monitoring schedules and thresholds.

➤ Schedules are set in the ADSPI-Rep_ModifyObjc and ADSPI-Rep_Mon policies. Thresholds are established in the ADSPI-Rep_Mon threshold policy.

The Active Directory Replication Latency graph tracks latency replication response time 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.

Active Directory Replication Time by Global Catalog

The Active Directory Replication Time by Global Catalog graph shows the average replication time of Microsoft Active Directory from selected global catalog domain controllers.

Schedules are set in the ADSPI-Rep_ModifyObjc and ADSPI-Rep_Mon policies. Thresholds are established in the ADSPI-Rep_Mon threshold policy.

The Active Directory Replication Time by Global Catalog 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.

Active Directory Bind Response Time

The Active Directory Bind Response Time graph shows the response time that a DC averages when binding to Microsoft Active Directory in general and the GC in particular. The graph shows one line for Microsoft Active Directory (labeled Directory) and one for Global Catalog (labeled Catalog) binds.

Active Directory Query Response Time

The Active Directory Query Response Time graph shows the average response that a DC averages when querying Microsoft Active Directory in general and the GC in particular. The graph shows one line for Microsoft Active Directory (labeled Directory) and one for Global Catalog (labeled Catalog) queries.

A 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.

Table 4 Data Store Details and Policy Mapping

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_DITDBSIZE - Contains data on the DIT database (ntds.dit), which is the Microsoft Active Directory data store.	ADSPI-DIT_TotalDit Size / ADSPI-DIT_TotalDit Size_2k8+	Instance Name - Path of the DIT database file	UTF8 / Text
		InstanceValue - Size of the DIT file in MB	UINT64 / Precision 0
ADSPI_DITPERCENT FULL - Contains data on the drive hosting the DIT database (ntds.dit), which is the Microsoft Active Directory data store.	ADSPI-DIT_DIT PercentFull / ADSPI-DIT_DIT PercentFull_2k8+	DITPTName - Path of the NTDS folder	UTF8 / Text
		DITPTValue - Percentage of the space used of the drive hosting DIT database	REAL64 / Precision 2
ADSPI_DITQUEUE LENGTH - Contains data on the drive hosting the DIT database (ntds.dit), which is the Microsoft Active Directory data store.	ADSPI-DIT_DIT QueueLength / ADSPI-DIT_DIT QueueLength_2k8+	DITQLName - Path to the NTDS folder	UTF8/ / Text
		DITQLValue - Average disk queue length of the drive hosting DIT database	UINT64 / Precision 0
ADSPI_DNSDR - Contains the DNS response time experienced by the DC in milli seconds.	ADSPI-DNS_DC_ Response / ADSPI-DNS_DC_ Response_2k8+	RespTime - DNS response time in milliseconds, experienced by a DC	REAL64 / Precision 2
ADSPI_DNSSP - Contains data that determines whether DNS Server is a DC or not and value of pages/sec counter of memory perfmon object.	ADSPI-DNS_ LogDNSPagesSec / ADSPI-DNS_ LogDNSPagesSec_2k 8+	IsDomainCtrl - Set to one if the DNS server is a DC and to zero if it is not a DC	REAL64 / Precision 2
		PagesPerSec -Value of the pages/sec counter of memory perfmon object	
ADSPI_DOMAIN - Contains the domain name associated with the DC.	ADSPI-DIT_TotalDit Size / ADSPI-DIT_TotalDit Size_2k8+	DomainName - Always taken as the value "DomainName"	UTF8 / Text
		DomainValue - Name of the domain hosted by the DC	

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_FSMO - Contains the ping and bind response time experienced by the DC to every FSMO role owner in seconds.	ADSPI-FSMO_ Logging / ADSPI-FSMO_ Logging_2k8+	FSMO - Name of the FSMO role	UTF8 / Text
		SERVER - Name of the server hosting the role	UTF8 / Text
		PINGTIME - Ping time experienced by the DC to the server in seconds	REAL64 / Precision 2
		FSMOBINDTIME - Bind time experienced by the DC to the server in seconds	REAL64 / Precision 2
ADSPI_FSMO_ROLE MVMT - Data is logged into this table when the DC gains or loses an FSMO role.	ADSPI-FSMO_Role Mvmt / ADSPI-FSMO_Role Mvmt_2k8+	FSMORM - FSMO role name gained or lost by the DC	UTF8 / Text
		ISROLEHOLDER - Zero, if the role is gained, and one if it is lost by the DC	REAL64 / Precision 2
ADSPI_GCREP - Contains the replication latency of a Global Catalog (GC) with every other DC.	ADSPI-Rep_GC_ Check_and_ Threshold / ADSPI-Rep_GC_ Check_and_ Threshold_2k8+	GCREPName - DNS name of the DC with which the GC is replicated	UTF8 / Text
		LatencyDelta - Replication latency in seconds	REAL64 / Precision 2
ADSPI_LOGDISK SIZE - Contains data on the drive hosting the DIT log files.	ADSPI-DIT_LogFiles PercentFull / ADSPI-DIT_LogFiles PercentFull_2k8+	DISKName - DIT log file path	UTF8 / Text
		DISKValue - Size (in MB) of the drive containing DIT log files	UINT64 / Precision 0
ADSPI_LOG PERCENTFULL - Contains data on the drive hosting the DIT log files.	ADSPI-DIT_LogFiles PercentFull / ADSPI-DIT_LogFiles PercentFull_2k8+	LGPERFULLName - DIT log file path	UTF8 / Text
		LGPERFULLValue - Percentage of used space of the drive containing DIT log files	REAL64 / Precision 2
ADSPI_LOGQUEUE LENGTH - Has data on the drive hosting the DIT log files.	ADSPI-DIT_LogFiles QueueLength / ADSPI-DIT_LogFiles QueueLength_2k8+	LGQLENName - DIT log file path	UTF8 / Text
		LGQLENValue - Average disk queue length of the drive containing the DIT log files	UINT64 / Precision 0

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_NTDS - Has data on the Microsoft Active Directory performance, especially replication activity.	ADSPI_Logging / ADSPI_Logging_ 2k8+	DRAInboundBTS - Total number of bytes per second received through replication. It is the sum of number of bytes of uncompressed and compressed data	REAL64 / Precision 2
		DRAOutboundBCSec - Uncompressed size in bytes of compressed replication data outbound to DCs in other sites per second	REAL64 / Precision 2
		DSThreadsinUse - Current number of threads in use by the directory service. This counter represents the number of threads currently servicing the clients.	UINT64 / Precision 0
		DRAInboundBCSec - Uncompressed size in bytes of compressed replication data inbound from DCs in other sites per second	REAL64 / Precision 2
		DRAOutboundBTS - Total number of bytes sent per second. It is the sum of the number of bytes of uncompressed data and compressed data	REAL64 / Precision 2
		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	REAL64 / Precision 2
		DRAOutboundBNCWSSec - Uncompressed size in bytes of outbound replication data that was not compressed site - outbound to DCs in the same site per second	REAL64 / Precision 2

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_NTDSP - Has data on the LSASS process.The LSASS process is responsible for management of local security authority domain authentication and Microsoft Active Directory management.	ADSPI_Logging / ADSPI_Logging_ 2k8+	PctProcTime - Percentage of time that the processor spent executing a non-idle thread of LSASS process	REAL64 / Precision 2
		PageFaultsSec - Rate, in incidents per second, of LSASS process, at which page faults were handled by the processor	REAL64 / Precision 2
		WorkingSet - Size (in bytes) of the working set of LSASS process	UINT64 / Precision 0
ADSPI_REPLA TENCY - 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.	ADSPI-Rep_Monitor IntraSiteReplication / ADSPI-Rep_Monitor IntraSiteReplication_ 2k8+ and ADSPI-Rep_Monitor InterSiteReplication / ADSPI-Rep_Monitor InterSiteReplication_ 2k8+	LATENCYMIN - Minimum latency experienced during replication from all Dcs to which a connection object exists	REAL64 / Precision 2
		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	
		LASTREPDELTA AVG - 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	REAL64 / Precision 2

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_RESPONSE TIME - 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.	ADSPI-Response_ Logging / ADSPI-Response_ Logging_2k8+	BINDTIME - Time, in seconds, required to bind to the Microsoft Active Directory on DC	REAL64 / Precision 2
		QUERYTIME - Time, in seconds, required to query the Microsoft Active Directory on DC	REAL64 / Precision 2
		GCBINDTIME - Time required to bind to GC in seconds	REAL64 / Precision 2
		GCQUERYTIME - Time required to query GC in seconds	REAL64 / Precision 2
		GCPRESENT - Indicates one if a GC is present on the DC, else it is zero	UINT64 / Precision 0
		AVAILABILITY - Indicates one if the DC is reachable, else, it is zero	UINT64 / Precision 0
		GCAVAILABILITY - Indicates one if the GC is reachable, else, it is 0	UINT64 / Precision 0
ADSPI_SITE - Contains the name of the site in which the DC is located.	ADSPI-DIT_TotalDit Size / ADSPI-DIT_TotalDit Size_2k8+	SiteName - Always indicates the value "SiteName"	UTF8 / Text
		SiteValue - Name of the site in which the DC is located	
ADSPI_SYSVOLPT FULL - Has data on the drive hosting the SYSVOL. The SYSVOL contains the changes that have to be replicated to the other DCs. Sysvol is also the place where changes from other DCs are received.	ADSPI-Sysvol_ PercentFull / ADSPI-Sysvol_ PercentFull_2k8+	SYSPERCName - Sysvol directory path	UTF8 / Text
		SYSPERCValue - Percentage of used space of the drive hosting Sysvol	REAL64 / Precision 2
ADSPI_TIMESYNC - 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.	ADSPI-Rep_Time Sync_Monitor / ADSPI-Rep_Time Sync_Monitor_2k8+	TIMESYNC - Time difference in seconds between the time master and the DC	REAL64 / Precision 2

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_TRUST - Has data on the trust relationships between the domains in the Microsoft Active Directory forest.	ADSPI_Trust_Mon_ Modify / ADSPI_Trust_Mon_ Modify_2k8+ and ADSPI-Trust_Mon_ Add_Del / ADSPI-Trust_Mon_ Add_Del_2k8+	Changetype - Indicates zero for addition of trust, one for deletion of trust, and two for modification of a trust	UINT64 / Precision 0
		TrustingDomain - Name of the trusting domain	UTF8 / Text
		TrustedDomain - Name of trusted domain	UTF8 / Text
		Trustattributes - Can be a combination of the following values: 0x1 forNontransitive, 0x2 for Uplevel clients only, 0x40000 for Tree parent, and 0x80000 for Tree root	UINT64 / Precision 0
		TrustDirection - Indicates one for inbound, two for outbound, and three for bi-directional trust relationship	UINT64 / Precision 0
		TrustStatus - Indicates zero if there is no trust failure, else it contains the error code	UINT64 / Precision 0
		TrustString - Gives a description of the trust status	UTF8 / Text
		TrustType - Indicates one for an uplevel trust, two for downlevel trust, three for Kerberos realm trust, and four for DCE	UINT64 / Precision 0
ADSPI_DNSSR - Contains the response time of the DNS server and a metric to indicate whether the DNS server is a DC or not.	ADSPI-DNS_Server_ Response / ADSPI-DNS_Server_ Response_2k8+	IsDomainController - Set to one if the DNS server is a domain controller, and set to zero if it is not.	REAL64 / Precision 2
		ResponseTime - Response time of the DNS server in milliseconds	

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
ADSPI_INBOUNDS - Contains the number of objects received by the DC through inbound replication.	ADSPI-Rep_Inbound Objs / ADSPI-Rep_Inbound Objs_2k8+	_InstanceName - Indicates the value by default *	UINT64 / Precision 0
		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 / Precision 2
ADSPI_SCHEMA MISMATCH - This table contains data on the failure of synchronization requests made to neighboring domain controllers.	ADSPI_SyncSchema MisMatch and ADSPI_SyncSchema MisMatch_2K8+	SchemaMismatch Name - Name of the instance for which data is logged.	UTF8 / Text
		SchemaMismatch Cnt - Number of sync requests made to the neighbors that failed because their schema are out of sync.	UINT64 / Precision 0

B 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 is `adspi_ddf.bat`.

Table 5 Report and Policy Mapping Details

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADDCAvailability.rpt *Report Content:* AD Domain Controller Availability *Spec File:* ADSPI_RESPONSETIME.spec	ADSPI_RESPONSEMON	SYSTEMNAME AVAILABILITY GCAVAILABILITY DATETIME	ADSPI_RESPONSETIME	ADSPI-Response_Logging
g_ADDCGC monthly.rpt *Report Content:* AD GC Rep Delay Times By DC/GC - Monthly *Spec File:* ADSPI_GCREP.spec	ADSPI_REP_GC	SYSTEMNAME GCREPNAME LATENCY DELTA DATETIME	ADSPI_GCREP	ADSPI-Rep_GC_Check_and_Threshold

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADDCGC weekly.rpt *Report Content:* AD GC Rep Delay Times By DC/GC - Weekly *Spec File:* ADSPI_GCREP. spec	ADSPI_REP_GC	SYSTEMNAME	ADSPI_GCREP	ADSPI-Rep_GC_ Check_and_ Threshold
		GCREPNAME		
		LATENCY DELTA		
		DATETIME		
g_ADDITDisk SpaceMonthly .rpt *Report Content:* AD DIT Disk Size Summary - Monthly *Spec Files:* • ADSPI_DIT DATABASE SIZE.spec • ADSPI_DIT PERCENT FULL.spec • ADSPI_DO MAIN.spec • ADSPI_SITE. spec	ADSPI_DITData baseSize	SYSTEMNAME	ADSPI_DIT DATABASE SIZE	ADSPI-DIT_ TotalDitSize
		DATETIME		
		INSTANCE VALUE		
	ADSPI_DITPer centFull	DITPTVALUE	ADSPI_DITPER CENTFULL	ADSPI-DIT_DIT PercentFull
	ADSPI_Domain	DOMAIN VALUE	ADSPI_ DOMAIN	ADSPI-DIT_ TotalDitSize
	ADSPI_Site	SITEVALUE	ADSPI_SITE	ADSPI-DIT_Tot alDitSize
g_ADDITDisk SpaceWeekly.rpt *Report Content:* AD DIT Disk Size Summary - Weekly *Spec Files:* • ADSPI_DIT DATABASESIZE.spec • ADSPI_DIT PERCENT FULL.spec • ADSPI_ DOMAIN. spec • ADSPI_SITE. spec	ADSPI_DITData baseSize	SYSTEMNAME	ADSPI_DIT DATABASE SIZE	ADSPI-DIT_ TotalDitSize
		DATETIME		
		INSTANCE VALUE		
	ADSPI_DIT PercentFull	DITPTVALUE	ADSPI_DITPER CENTFULL	ADSPI-DIT_DIT PercentFull
	ADSPI_Domain	DOMAIN VALUE	ADSPI_ DOMAIN	ADSPI-DIT_ TotalDitSize
	ADSPI_Site	SITEVALUE	ADSPI_SITE	ADSPI-DIT_ TotalDitSize

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADDITQueue LengthWeekly. rpt *Report Content:* AD DIT Disk Queue Length - Weekly *Spec Files:* • ADSPI_DO MAIN.spec • ADSPI_SITE. spec • ADSPI_DIT QUEUE LENGTH. spec	ADSPI_Domain	SYSTEMNAME	ADSPI_ DOMAIN	ADSPI-DIT_ TotalDitSize
		DATETIME		
		DOMAIN VALUE		
	ADSPI_Site	SITEVALUE	ADSPI_SITE	ADSPI-DIT_ TotalDitSize
	ADSPI_DIT QUEUE LENGTH	SYSTEMNAME	ADSPI_DIT QUEUE LENGTH	ADSPI-DIT_DIT QueueLength
		DATETIME		
		DITQLNAME		
		DITQLVALUE		
g_ADDNSDC AvailDaily.rpt *Report Content:* AD DC DNS Availability Report - Daily Summary *Spec File:* ADSPI_DNSDR. spec	ADSPI_DNS_ DCRESP	DATETIME	ADSPI_DNSDR	ADSPI-DNS_DC _Response Policy
		RESPTIME		
		SYSTEMNAME		
g_ADDNSDC AvailWeekly.rpt *Report Content:* AD DC DNS Availability Report - Weekly Summary *Spec File:* ADSPI_DNSDR.spec	ADSPI_DNS_ DCRESP	DATETIME	ADSPI_DNSDR	ADSPI-DNS_DC _Response Policy
		RESPTIME		
		SYSTEMNAME		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADDNSSrv AvailDaily.rpt *Report Content:* AD DNS Server availability Report - Daily Summary *Spec File:* ADSPI_DNSSR.spec	ADSPI_DNSSR	DATETIME RESPONSE TIME ISDOMAINCONTROLLER SYSTEMNAME	ADSPI_DNSSR	ADSPI-DNS_Server_Response
g_ADDNSSrv AvailWeekly.rpt *Report Content:* AD DNS Availability Report - Weekly Summary *Spec File:* ADSPI_DNSSR.spec	ADSPI_DNSSR	DATETIME RESPONSE TIME ISDOMAINCONTROLLER SYSTEMNAME	ADSPI_DNSSR	ADSPI-DNS_Server_Response
g_ADDNSSrv MemCapPlan Monthly.rpt *Report Content:* AD DNS Server Memory Capacity Planning Report - Monthly Summary *Spec File:* ADSPI_DNSSP.spec	ADSPI_DNSSP	DATETIME PAGESPERSEC ISDOMAIN CTRL SYSTEMNAME	ADSPI_DNSSP	ADSPI-DNS_LogDNSPagesSec
g_ADDNSSrv MemCapPlan Weekly.rpt *Report Content:* AD DNS Server Memory Capacity Planning Report - Monthly Summary *Spec File:* ADSPI_DNSSP.spec	ADSPI_DNSSP	DATETIME PAGESPERSEC ISDOMAIN CTRL SYSTEMNAME	ADSPI_DNSSP	ADSPI-DNS_LogDNSPagesSec

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADDomain ForestTrust Monthly.rpt *Report Content:* AD Domain and Forest Trust Changes - Monthly *Spec File:* ADSPI_Trust mon.spec	ADSPI_TRUST	SYSTEMNAME	ADSPI_TRUST	ADSPI-Trust_ Mon_Add_Del and ADSPI-Trust_ Mon_Modify
		DATETIME		
		CHANGETYPE		
		TRUSTING DOMAIN		
		TRUSTED DOMAIN		
		TRUSTATTRI BUTES		
		TRUSTDIREC TION		
		TRUSTSTATUS		
		TRUSTSTATUS STRING		
		TRUSTTYPE		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADDomain ForestTrust Weekly.rpt *Report Content:* AD Domain and Forest Trust Changes - Weekly *Spec File:* ADSPI_Trust mon.spec	ADSPI_TRUST	SYSTEMNAME	ADSPI_TRUST	ADSPI-Trust_ Mon_Add_Del and ADSPI-Trust_ Mon_Modify
		DATETIME		
		CHANGETYPE		
		TRUSTING DOMAIN		
		TRUSTED DOMAIN		
		TRUSTATTRI BUTES		
		TRUSTDIREC TION		
		TRUSTSTATUS		
		TRUSTSTATUS STRING		
		TRUSTTYPE		
g_ADFSMORole HolderMov Monthly.rpt *Report Content:* FSMO Role Holder Report - Monthly *Spec File:* ADSPI_FSMO_RoleMvmt.spec	ADSPI_FSMO_ ROLEMVMT	SYSTEMNAME	ADSPI_FSMO_ ROLEMVMT	ADSPI-FSMO_ RoleMvmt
		DATETIME		
		FSMORM		
		ISROLE HOLDER		
g_ADFSMORoleHolderMov Weekly.rpt *Report Content:* FSMO Role Holder Report - Weekly *Spec File:* ADSPI_FSMO_ RoleMvmt.spec	ADSPI_FSMO_ ROLEMVMT	SYSTEMNAME	ADSPI_FSMO_ ROLEMVMT	ADSPI-FSMO_ RoleMvmt
		DATETIME		
		FSMORM		
		ISROLE HOLDER		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADGCDC monthly.rpt *Report Content:* AD GC Rep Delay Times By GC/DC - Monthly *Spec File:* ADSPI_GCREP. spec	ADSPI_REP_GC	DATETIME SYSTEMNAME GCREPNAME LATENCY DELTA	ADSPI_GCREP	ADSPI-Rep_GC_ Check_and_Thre s hold
g_ADGCDC weekly.rpt *Report Content:* AD GC Rep Delay Times By GC/DC - Weekly *Spec File:* ADSPI_GCREP. spec	ADSPI_REP_GC	DATETIME SYSTEMNAME GCREPNAME LATENCY DELTA	ADSPI_GCREP	ADSPI-Rep_GC_ Check_and_ Threshold
g_ADGCResponseTimeMonthly. rpt *Report Content:* AD GC Response Time - Monthly *Spec File:* ADSPI_Respon seTime.spec	ADSPI_ RESPONSE MON	SYSTEMNAME DATETIME GCBINDTIME GCQUERY TIME GCPRESENT	ADSPI_ RESPONSE TIME	ADSPI-Respon se_Logging

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADGCResponseTimeWeekly.rpt *Report Content:* AD GC Response Time - Weekly *Spec File:* ADSPI_ResponseTime.spec	ADSPI_RESPONSEMON	SYSTEMNAME	ADSPI_RESPONSETIME	ADSPI-Response_Logging
		DATETIME		
		GCBINDTIME		
		GCQUERYTIME		
		GCPRESENT		
g_ADLogFilesDiskSpaceMonthly.rpt *Report Content:* AD Log Files Disk Size Summary - Monthly *Spec Files:* • ADSPI_LOGDISKSIZE.spec • ADSPI_LOGPERCENTFULL.spec • ADSPI_DOMAIN.spec • ADSPI_SITE.spec	ADSPI_LogDiskSize	DATETIME	ADSPI_LOGDISKSIZE	ADSPI-DIT_LogFilesPercentFull
		SYSTEMNAME		
	ADSPI_LOGPERCENTFULL	LGPERFULLVALUE	ADSPI_LOGPERCENTFULL	ADSPI-DIT_LogFilesPercentFull
	ADSPI_DOMAIN	DOMAINVALUE	ADSPI_DOMAIN	ADSPI-DIT_TotalDitSize
	ADSPI_SITE	SITEVALUE	ADSPI_SITE	ADSPI-DIT_TotalDitSize
g_ADLogFilesDiskSpaceWeekly.rpt *Report Content:* AD Log Files Disk Size Summary - Weekly *Spec Files:* • ADSPI_LOGDISKSIZE.spec • ADSPI_LOGPERCENTFULL.spec • ADSPI_DOMAIN.spec • ADSPI_SITE.spec	ADSPI_LogDiskSize	DATETIME	ADSPI_LOGDISKSIZE	ADSPI-DIT_LogFilesPercentFull
		SYSTEMNAME		
	ADSPI_LOGPERCENTFULL	LGPERFULLVALUE	ADSPI_LOGPERCENTFULL	ADSPI-DIT_LogFilesPercentFull
	ADSPI_DOMAIN	DOMAINVALUE	ADSPI_DOMAIN	ADSPI-DIT_TotalDitSize
	ADSPI_SITE	SITEVALUE	ADSPI_SITE	ADSPI-DIT_TotalDitSize

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADLogQueueLengthWeekly .rpt *Report Content:* AD Log Files Disk Queue Length - Weekly *Spec Files:* • ADSPI_DOMAIN.spec • ADSPI_SITE. spec • ADSPI_LOG QUEUELENGTH.spec	ADSPI_Domain	DATETIME	ADSPI_ DOMAIN	ADSPI-DIT_ TotalDitSize
		SYSTEMNAME		
		DOMAIN VALUE		
	ADSPI_Site	SITEVALUE	ADSPI_SITE	ADSPI-DIT_ TotalDitSize
	ADSPI_LOG QUEUE LENGTH	SYSTEMNAME	ADSPI_LOG QUEUE LENGTH	ADSPI-DIT_Log FilesQueue Length
		DATETIME		
		LGQLENNAME		
		LGQLEN VALUE		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADMemory Usage.rpt *Report Content:* Active Directory Memory Usage *Spec File:* ADSPI_NTDSP. spec	ADSPI_NTDSP	DATETIME	ADSPI_NTDSP	ADSPI_Logging
		SYSTEMNAME		
		WORKINGSET		
		PAGEFAULTS SEC		
g_ADOpMstr ConTimeBy Fsmo.rpt *Report Content:* AD Operations Master Connection Time Report by FSMO *Spec File:* ADSPI_FSMO. spec	ADSPI_FSMO_ MET	GMT	ADSPI_FSMO	ADSPI-FSMO_ Logging
		DATETIME		
		FSMO		
		PINGTIME		
		SERVER		
		FSMOBIND TIME		
g_ADOpMstr ConTimeBySvr. rpt *Report Content:* AD Operations Master Connection Time Report by Server *Spec File:* ADSPI_FSMO. spec	ADSPI_FSMO_ MET	GMT	ADSPI_FSMO	ADSPI-FSMO_ Logging
		DATETIME		
		FSMO		
		PINGTIME		
		SERVER		
		FSMOBIND TIME		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADProcess Usage.rpt *Report Content:* Active Directory Processor Usage *Spec File:* ADSPI_NTDS. spec	ADSPI_NTDS	DATETIME	ADSPI_NTDS	ADSPI_Logging
		SYSTEMNAME		
		DSTHREADS INUSE		
g_ADReplication Inbound.rpt *Report Content:* Active Directory Replication Inbound *Spec File:* ADSPI_NTDS. spec	ADSPI_NTDS	DATETIME	ADSPI_NTDS	ADSPI_Logging
		SYSTEMNAME		
		DRAINBOUND BCSEC		
		DRAINBOUND BSNCWSSEC		
g_ADReplication Outbound.rpt *Report Content:* Active Directory Replication Outbound *Spec File:* ADSPI_NTDS. spec	ADSPI_NTDS	DATETIME	ADSPI_NTDS	ADSPI_Logging
		SYSTEMNAME		
		DRAOUT BOUNDBCSEC		
		DRAOUTBOUN DBNCWSSEC		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADReplication Summary.rpt *Report Content:* Active Directory Replication Summary *Spec File:* ADSPI_NTDS. spec	ADSPI_NTDS	DATETIME SYSTEMNAME DRAINBOUNDBTS DRAOUTBOUNDBTS	ADSPI_NTDS	ADSPI_Logging
g_ADSizeOf SysvolMonthly. rpt *Report Content:* AD Size of Sysvol Report - Monthly Summary *Spec File:* ADSPI_SYSVOLPERCENTFULL.spec	ADSPI_SYSVOL_PCT_FULL	SYSTEMNAME DATETIME SYSPERCNAME SYSPERCVALUE	ADSPI_SYSVOLPTFULL	ADSPI-Sysvol_PercentFull
g_ADSizeOf SysvolWeekly .rpt *Report Content:* AD Size of Sysvol Report - Weekly Summary *Spec File:* ADSPI_SYSVOLPERCENTFULL.spec	ADSPI_SYSVOL_PCT_FULL	SYSTEMNAME DATETIME SYSPERCNAME SYSPERCVALUE	ADSPI_SYSVOLPTFULL	ADSPI-Sysvol_PercentFull

C 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 data-collection procedure. The data store class creator for all the reports is `adspi_ddf.bat`.

Table 6 Graphs and Policy Mapping 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

D 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 Table 7 to monitor the golden metrics.

These golden metrics cover the critical areas for which you would like to receive messages as a critical or major event occuring on the Microsoft Active Directory. Monitoring golden metrics and taking action against the events generated by these metrics ensure the smooth functioning of the Microsoft Active Directory.

Prerequisites before Monitoring Golden Metrics

Make sure that you deploy the following before monitoring the golden metrics:

1. SPI Data Collector Instrumentation category
2. ADSPI_CreateDataSources policy
3. Basic Discovery and Advanced Discovery policies

Table 7 Golden Metrics

Metric	Metric Description	Policy
DIT Disk Health	Indicates the health of disk hosting DIT file	ADSPI-DIT_DITPercentFull / ADSPI-DIT_DITPercentFull_2k8+
		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+

Metric	Metric Description	Policy
DC Records on DNS	Relates to the monitoring of the availability of the DC records on DNS servers	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_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 Response Times	Relates to the monitoring of the ping and bind response times of all the FSMO roles.	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_Bind / ADSPI-FSMO_RID_Bind_2k8+
		ADSPI-FSMO_RID_Ping / ADSPI-FSMO_RID_Ping_2k8+

Metric	Metric Description	Policy
Replication Status	Relates to the monitoring of replication status on DCs.	ADSPI-Rep_ModifyObj / ADSPI-Rep_ModifyObj_2k8+
		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+
DC and GC Response Times	Relates to the monitoring of Query and Bind Response Times of DCs and GCs	ADSPI-Response Time_GCQuery / ADSPI-Response Time_GCQuery_2k8+
		ADSPI-ResponseTime_Bind / ADSPI-ResponseTime_Bind_2k8+
		ADSPI-ResponseTime_GCBind / ADSPI-ResponseTime_GCBind_2k8+
		ADSPI-ResponseTime_Query / ADSPI-ResponseTime_Query_2k8+
Sysvol Health	Relates to the monitoring of various aspects of sysvol like Sysvol Disk Health, FRS Status and Sysvol Connectivity.	ADSPI-Sysvol_Connectivity / ADSPI-Sysvol_Connectivity_2k8+
		ADSPI-Sysvol_FRS / ADSPI-Sysvol_FRS_2k8+
		ADSPI-SysVol_PercentFull / ADSPI-SysVol_PercentFull_2k8+

Metric	Metric Description	Policy
AD Processes Health	Relates to the monitoring of health of all Microsoft Active Directory processes such as LSASS, NTFRS, KDC and Netlogon.	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_KDC / ADSPI_KDC_2k8+
		ADSPI_NetLogon / ADSPI_NetLogon_2k8+
		ADSPI_NTFRS
LDAP Bind Time	Relates to the monitoring of LDAP Bind Time	ADSPI_IQLDAPBindTime / ADSPI_IQLDAPBindTime_2k8+
Replication Statistics.	Relates to the monitoring of various replication statistics such as pending synchronizations, Inbound Bytes between sites and within site, Notify Queue Size among others.	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+

Metric	Metric Description	Policy
Security	Relates to the monitoring of various security aspects of the Microsoft Active Directory.	ADSPI_KDCFailureGrantTicket / ADSPI_KDCFailureGrantTicket_2k8+
		ADSPI_PrivilegedAccounts / ADSPI_PrivilegedAccounts_2k8+
		ADSPI_SecErrorsLogon / ADSPI_SecErrorsLogon_2k8+
		ADSPI_DirComputerModif / ADSPI_DirComputerModif _2k8+

Index

R

S

W

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: