

# HP Operations Smart Plug-in for Microsoft® Active Directory

for the HP Operations Manager for Solaris

Software Version: 7.02

---

## Reference Guide

Document Release Date: July 2010  
Software Release Date: July 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 Notices

© Copyright 2009-2010 Hewlett-Packard Development Company, L.P.

### 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.

This guide contains SPI information for HP Operations Manager for UNIX version 9.00, HP Operations Manager for Linux version 9.01, and HP Operations Manager for Solaris version 9.02.

## Support

Visit the HP Software Support Online web site at:

**[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

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

HP Software 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 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](http://h20230.www2.hp.com/new_access_levels.jsp)**

# Contents

<b>1 Policies</b> .....	13
Policy Group Catalog .....	13
Auto Deploy Policies .....	13
Discovery Policies (Basic and Advanced) .....	14
ADSPI_Discovery .....	14
ADSPI-AutoDiscovery_Delete .....	14
ADSPI-AutoDiscovery_DIT .....	14
ADSPI-AutoDiscovery_DIT_2k8+ .....	15
ADSPI-AutoDiscovery_DNS .....	15
ADSPI-AutoDiscovery_DNS_2k8+ .....	16
ADSPI-AutoDiscovery_FSMO .....	16
ADSPI-AutoDiscovery_FSMO_2k8+ .....	17
ADSPI-AutoDiscovery_GC .....	17
ADSPI-AutoDiscovery_GC_2k8+ .....	18
ADSPI-AutoDiscovery_PBHS .....	18
ADSPI-AutoDiscovery_PBHS_2k8+ .....	19
ADSPI-AutoDiscovery_Rep .....	20
ADSPI-AutoDiscovery_Rep_2k8+ .....	21
ADSPI-AutoDiscovery_RODC_2k8+ .....	21
ADSPI-AutoDiscovery_Trust .....	22
ADSPI-AutoDiscovery_Trust_2k8+ .....	22
ADSPI-CreateDatasources .....	22
DIT Monitoring Policies .....	23
ADSPI-DIT_LogfilesQueueLength .....	23
ADSPI-DIT_LogfilesQueueLength_2k8+ .....	24
ADSPI-DIT_DITQueueLength .....	24
ADSPI-DIT_DITQueueLength_2k8+ .....	25
ADSPI-DIT_TotalDITSize .....	26
ADSPI-DIT_TotalDITSize_2k8+ .....	27
ADSPI-DIT_LogfilesPercentFull .....	27
ADSPI-DIT_LogfilesPercentFull_2k8+ .....	28
ADSPI-DIT_DITPercentFull .....	29
ADSPI-DIT_DITPercentFull_2k8+ .....	29
DNS Monitoring Policies .....	30
ADSPI-DNS_DC_A_Chk .....	30
ADSPI-DNS_DC_A_Chk_2k8+ .....	31
ADSPI-DNS_DC_CName_Chk .....	32
ADSPI-DNS_DC_CName_Chk_2k8+ .....	33
ADSPI-DNS_DC_Response .....	34

ADSPI-DNS_DC_Response_2k8+ . . . . .	35
ADSPI-DNS_Extra_GC_SRV_Chk . . . . .	36
ADSPI-DNS_Extra_GC_SRV_Chk_2k8+ . . . . .	37
ADSPI-DNS_Extra_Kerberos_SRV_Chk . . . . .	38
ADSPI-DNS_Extra_Kerberos_SRV_Chk_2k8+ . . . . .	38
ADSPI-DNS_Extra_LDAP_SRV_Chk . . . . .	39
ADSPI-DNS_Extra_LDAP_SRV_Chk_2k8+ . . . . .	39
ADSPI-DNS_GC_A_Chk . . . . .	40
ADSPI-DNS_GC_A_Chk_2k8+ . . . . .	41
ADSPI-DNS_GC_SRV_CHK . . . . .	42
ADSPI-DNS_GC_SRV_CHK_2k8+ . . . . .	43
ADSPI-DNS_GC_StrandedSite . . . . .	44
ADSPI-DNS_GC_StrandedSite_2k8+ . . . . .	46
ADSPI-DNS_Island_Server . . . . .	47
ADSPI-DNS_Island_Server_2k8+ . . . . .	48
ADSPI-DNS_LogDNSPagesSec . . . . .	49
ADSPI-DNS_LogDNSPagesSec_2k8+ . . . . .	49
ADSPI-DNS_Kerberos_SRV_Chk . . . . .	49
ADSPI-DNS_Kerberos_SRV_Chk_2k8+ . . . . .	50
ADSPI-DNS_LDAP_SRV_Chk . . . . .	52
ADSPI-DNS_LDAP_SRV_Chk_2k8+ . . . . .	53
ADSPI-DNS_Server_Response . . . . .	54
ADSPI-DNS_Server_Response_2k8+ . . . . .	54
ADSPI-DNS_Obsolete_GUIDs . . . . .	55
ADSPI-DNS_Obsolete_GUIDs_2k8+ . . . . .	56
FSMO Monitoring Polices . . . . .	57
ADSPI-FSMO_INFRA_Bind . . . . .	58
ADSPI-FSMO_INFRA_Bind_2k8+ . . . . .	58
ADSPI-FSMO_INFRA_Ping . . . . .	59
ADSPI-FSMO_INFRA_Ping_2k8+ . . . . .	60
ADSPI-FSMO_GC_Infrastructure_Check . . . . .	60
ADSPI-FSMO_GC_Infrastructure_Check_2k8+ . . . . .	61
ADSPI-FSMO_Logging . . . . .	61
ADSPI-FSMO_Logging_2k8+ . . . . .	61
ADSPI-FSMO_NAMING_Bind . . . . .	62
ADSPI-FSMO_NAMING_Bind_2k8+ . . . . .	62
ADSPI-FSMO_NAMING_Ping . . . . .	63
ADSPI-FSMO_NAMING_Ping_2k8+ . . . . .	64
ADSPI-FSMO_PDC_Bind . . . . .	64
ADSPI-FSMO_PDC_Bind_2k8+ . . . . .	65
ADSPI-FSMO_PDC_Ping . . . . .	66
ADSPI-FSMO_PDC_Ping_2k8+ . . . . .	67
ADSPI-FSMO_RID_Bind . . . . .	68
ADSPI-FSMO_RID_Bind_2k8+ . . . . .	68
ADSPI-FSMO_RID_Ping . . . . .	69
ADSPI-FSMO_RID_Ping_2k8+ . . . . .	70
ADSPI-FSMO_RoleMvmt . . . . .	70

ADSPI-FSMO_RoleMvmt_2k8+ . . . . .	71
ADSPI-FSMO_RoleMvmt_INFRA . . . . .	71
ADSPI-FSMO_RoleMvmt_INFRA_2k8+ . . . . .	72
ADSPI-FSMO_RoleMvmt_NAMING . . . . .	73
ADSPI-FSMO_RoleMvmt_NAMING_2k8+ . . . . .	73
ADSPI-FSMO_RoleMvmt_PDC . . . . .	74
ADSPI-FSMO_RoleMvmt_PDC_2k8+ . . . . .	75
ADSPI-FSMO_Consist . . . . .	75
ADSPI-FSMO_Consist_2k8+ . . . . .	76
ADSPI-FSMO_Consist_INFRA . . . . .	77
ADSPI-FSMO_Consist_INFRA_2k8+ . . . . .	77
ADSPI-FSMO_Consist_NAMING . . . . .	78
ADSPI-FSMO_Consist_NAMING_2k8+ . . . . .	79
ADSPI-FSMO_Consist_PDC . . . . .	80
ADSPI-FSMO_Consist_PDC_2k8+ . . . . .	80
ADSPI-FSMO_Consist_RID . . . . .	81
ADSPI-FSMO_Consist_RID_2k8+ . . . . .	82
ADSPI-FSMO_Consist_SCHEMA . . . . .	82
ADSPI-FSMO_Consist_SCHEMA_2k8+ . . . . .	83
GC Monitoring . . . . .	83
ADSPI-Rep_GC_Check_and_Threshold . . . . .	83
ADSPI-Rep_GC_Check_and_Threshold_2k8+ . . . . .	84
Replication Monitoring Policies . . . . .	85
Pre-requisite supporting policies . . . . .	85
The replication monitoring executable . . . . .	85
Replication Monitoring Scenarios . . . . .	85
Configuring the Replication Monitoring policies . . . . .	87
ADSPI-Rep_CheckObj . . . . .	88
ADSPI-Rep_CheckObj_2k8+ . . . . .	88
ADSPI-Rep_Delete_OvRep_Object . . . . .	89
ADSPI-Rep_Delete_OvRep_Object_2k8+ . . . . .	89
ADSPI-Rep_InboundObjs . . . . .	90
ADSPI-Rep_InboundObjs_2k8+ . . . . .	90
ADSPI-Rep_MonitorInterSiteReplication . . . . .	91
ADSPI-Rep_MonitorInterSiteReplication_2k8+ . . . . .	91
ADSPI-Rep_MonitorIntraSiteReplication . . . . .	92
ADSPI-Rep_MonitorIntraSiteReplication_2k8+ . . . . .	92
ADSPI-Rep_ISM_Chk . . . . .	93
ADSPI-Rep_ISM_Chk_2k8+ . . . . .	94
ADSPI-Rep_Modify_User_Object . . . . .	95
ADSPI-Rep_Modify_User_Object_2k8+ . . . . .	96
ADSPI-Rep_ModifyObj . . . . .	96
ADSPI-Rep_ModifyObj_2k8+ . . . . .	97
ADSPI-Rep_TimeSync . . . . .	98
ADSPI-Rep_TimeSync_2k8+ . . . . .	98
Response Time Monitoring . . . . .	99
ADSPI-ResponseTime_Bind . . . . .	99

ADSPI-ResponseTime_Bind_2k8+ . . . . .	100
ADSPI-ResponseTime_GCBind . . . . .	101
ADSPI-ResponseTime_GCBind_2k8+ . . . . .	102
ADSPI-Response_Logging. . . . .	103
ADSPI-Response_Logging_2k8+. . . . .	103
ADSPI-ResponseTime_Query . . . . .	104
ADSPI-ResponseTime_Query_2k8+. . . . .	105
ADSPI-Response Time_GCQuery. . . . .	106
ADSPI-Response Time_GCQuery_2k8+. . . . .	107
SysVol Monitoring. . . . .	107
ADSPI-Sysvol_FRS . . . . .	108
ADSPI-Sysvol_FRS_2k8+ . . . . .	108
ADSPI-Sysvol_AD_Sync . . . . .	108
ADSPI-Sysvol_AD_Sync_2k8+ . . . . .	109
ADSPI-SysVol_PercentFull. . . . .	110
ADSPI-SysVol_PercentFull_2k8+. . . . .	110
ADSPI-Sysvol_Connectivity . . . . .	111
ADSPI-Sysvol_Connectivity_2k8+ . . . . .	112
Trust Monitoring (Windows Server 2003/2008) . . . . .	112
ADSPI_Trust_Mon_Modify . . . . .	112
ADSPI_Trust_Mon_Modify_2k8+. . . . .	113
ADSPI_Trust_Mon_Add_Del . . . . .	113
ADSPI_Trust_Mon_Add_Del_2k8+ . . . . .	113
Manual Deploy Policies . . . . .	114
Auto Baseline Policies . . . . .	114
ADSPI-Rep_InboundObjects_AT . . . . .	114
ADSPI-Rep_InboundObjects_AT_2k8+ . . . . .	115
ADSPI-Rep_TimeSync_Monitor_AT. . . . .	115
ADSPI-Rep_TimeSync_Monitor_AT_2k8+. . . . .	115
ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT. . . . .	116
ADSPI-Rep_GC_Check_and_Threshold_Monitor_AT_2k8+. . . . .	116
Connector Polices . . . . .	116
ADSPI_ActiveAuthKerberos . . . . .	116
ADSPI_ActiveAuthLogon . . . . .	117
ADSPI_ActiveAuthNTLM. . . . .	117
ADSPI_ADCFwdAllWarnErrorMSADC. . . . .	117
ADSPI_ADCImportFailures . . . . .	118
ADSPI_ADCPageFaults . . . . .	118
ADSPI_ADCPrivateBytes . . . . .	118
ADSPI_ADCProcessorTime . . . . .	119
ADSPI_ADCWorkingSet . . . . .	119
Domain and OU Structures Policies . . . . .	119
ADSPI_DomainChanges . . . . .	119
ADSPI_DomainChanges_2k8+ . . . . .	120
ADSPI_OUChanges. . . . .	120
ADSPI_OUChanges_2k8+. . . . .	121
Global Catalog Access Policies . . . . .	121



ADSPI_GlobalCatalogWrites . . . . .	121
ADSPI_GlobalCatalogWrites_2k8+ . . . . .	122
ADSPI_GlobalCatalogReads . . . . .	122
ADSPI_GlobalCatalogReads_2k8+ . . . . .	122
ADSPI_GlobalCatalogSearches . . . . .	123
ADSPI_GlobalCatalogSearches_2k8+ . . . . .	123
Health Monitor Policies . . . . .	123
ADSPI_DNSServ_FwdAllInformation . . . . .	124
ADSPI_DNSServ_FwdAllInformation_2k8+ . . . . .	124
ADSPI_DNSServ_FwdAllWarnError . . . . .	124
ADSPI_DNSServ_FwdAllWarnError_2k8+ . . . . .	124
ADSPI_FwdAllInformationDS . . . . .	125
ADSPI_FwdAllInformationDS_2k8+ . . . . .	125
ADSPI_FwdAllInformationFRS . . . . .	125
ADSPI_FwdAllInformationFRS_2k8+ . . . . .	126
ADSPI_FwdAllWarnErrorDS . . . . .	126
ADSPI_FwdAllWarnErrorDS_2k8+ . . . . .	126
ADSPI_FwdAllWarnErrorFRS . . . . .	126
ADSPI_FwdAllWarnErrorFRS_2k8+ . . . . .	127
ADSPI_HMLSASSPageFaults . . . . .	127
ADSPI_HMLSASSPageFaults_2k8+ . . . . .	127
ADSPI_HMLSASSPrivateBytes . . . . .	128
ADSPI_HMLSASSPrivateBytes_2k8+ . . . . .	128
ADSPI_HMLSASSProcessorTime . . . . .	128
ADSPI_HMLSASSProcessorTime_2k8+ . . . . .	129
ADSPI_HMLSASSWorkingSet . . . . .	129
ADSPI_HMLSASSWorkingSet_2k8+ . . . . .	130
ADSPI_HMNTFRSPageFaults . . . . .	130
ADSPI_HMNTFRSPageFaults_2k8+ . . . . .	130
ADSPI_HMNTFRSPrivateBytes . . . . .	131
ADSPI_HMNTFRSPrivateBytes_2k8+ . . . . .	131
ADSPI_HMNTFRSProcessorTime . . . . .	131
ADSPI_HMNTFRSProcessorTime_2k8+ . . . . .	132
ADSPI_HMNTFRSWorkingSet . . . . .	132
ADSPI_HMNTFRSWorkingSet_2k8+ . . . . .	132
ADSPI_HMThreadsInUse . . . . .	133
ADSPI_HMThreadsInUse_2k8+ . . . . .	133
ADSPI_KDC . . . . .	133
ADSPI_KDC_2k8+ . . . . .	134
ADSPI_NetLogon . . . . .	134
ADSPI_NetLogon_2k8+ . . . . .	134
ADSPI_NTFRS . . . . .	135
ADSPI_SamSs . . . . .	135
ADSPI_SamSs_2k8+ . . . . .	135
ADSPI_SMTPEventLogs . . . . .	136
ADSPI_SMTPEventLogs_2k8+ . . . . .	136
ADSPI_SyncSchemaMismatch . . . . .	136

ADSPI_SyncSchemaMisMatch_2k8+ . . . . .	136
ADSPI_DFSR_2k8+ . . . . .	137
ADSPI_NTDS_2k8+ . . . . .	137
ADSPI_Logging . . . . .	137
ADSPI_Logging_2k8+ . . . . .	138
ADSPI_NtLmSsp . . . . .	139
Index and Query Monitor Policies . . . . .	140
ADSPI_IQKerberosAuthentications . . . . .	140
ADSPI_IQKerberosAuthentications_2k8+ . . . . .	140
ADSPI_IQLDAPActiveThreads . . . . .	141
ADSPI_IQLDAPActiveThreads_2k8+ . . . . .	141
ADSPI_IQLDAPBindTime . . . . .	141
ADSPI_IQLDAPBindTime_2k8+ . . . . .	142
ADSPI_IQLDAPClientSessions . . . . .	142
ADSPI_IQLDAPClientSessions_2k8+ . . . . .	142
ADSPI_IQNTLMAuthentications . . . . .	143
ADSPI_IQNTLMAuthentications_2k8+ . . . . .	143
ADSPI_DSSearches . . . . .	143
ADSPI_DSSearches_2k8+ . . . . .	143
ADSPI_DSReads . . . . .	144
ADSPI_DSReads_2k8+ . . . . .	144
ADSPI_DSWrites . . . . .	144
ADSPI_DSWrites_2k8+ . . . . .	145
Replication Policies . . . . .	145
ADSPI_ADSPendingSynchronizations . . . . .	145
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	145
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	145
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	146
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	146
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	147
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	147
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	147
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	148
ADSPI_ADSPendingSynchronizations_2k8+ . . . . .	148
Replication Activities Polices . . . . .	148
ADSPI_ReplicationActivities . . . . .	148
ADSPI_ReplicationActivities_2k8+ . . . . .	149
Securities Polices . . . . .	149
ADSPI_DirUserCreationDeletionModification . . . . .	150
ADSPI_DirUserCreationDeletionModification_2k8+ . . . . .	150
ADSPI_KDCFailureGrantTicket . . . . .	150
ADSPI_KDCFailureGrantTicket_2k8+ . . . . .	150
ADSPI_PrivilegedAccounts . . . . .	151
ADSPI_PrivilegedAccounts_2k8+ . . . . .	152
ADSPI_SecAdminGroupChangeMon . . . . .	152
ADSPI_SecAdminGroupChangeMon_2K8+ . . . . .	153
ADSPI_SecDirectoryServiceAccess . . . . .	153

ADSPI_SecDirectoryServiceAccess_2k8+ . . . . .	153
ADSPI_SecErrAccessPermissions . . . . .	154
ADSPI_SecErrAccessPermissions_2k8+ . . . . .	154
ADSPI_SecErrGrantedAccess. . . . .	154
ADSPI_SecErrGrantedAccess_2k8+. . . . .	155
ADSPI_SecErrorsLogon . . . . .	155
ADSPI_SecErrorsLogon_2k8+ . . . . .	155
ADSPI_SecNonTransMembEval . . . . .	156
ADSPI_SecNonTransMembEval_2k8+ . . . . .	156
ADSPI_SecSDPropagatorQueue. . . . .	156
ADSPI_SecSDPropagatorQueue_2k8+. . . . .	157
ADSPI_SecTransMembEval . . . . .	157
ADSPI_SecTransMembEval_2k8+. . . . .	157
ADSPI_DirComputerModif. . . . .	158
ADSPI_DirComputerModif_2k8+ . . . . .	158
Site-Structure Policies . . . . .	158
ADSPI_SiteChanges . . . . .	158
ADSPI_SiteChanges_2k8+ . . . . .	159
<b>2 Tools . . . . .</b>	<b>161</b>
Active Directory Self Healing Info tool . . . . .	161
Self-Healing Verification tool . . . . .	161
AD DC Demotion Preparation tool . . . . .	161
Check ADS Service Tool. . . . .	161
ADS Printer Information tool . . . . .	162
Delete Older ADSPI Classes tool . . . . .	162
HP Operations Topology Viewer . . . . .	162
HP Operations Topology Viewer map . . . . .	162
AD Trust Relationships Tool . . . . .	163
<b>3 Reports . . . . .</b>	<b>165</b>
Daily, Weekly, and Monthly Reports . . . . .	165
AD DC DNS Availability (daily/weekly) . . . . .	165
AD DIT Disk Queue Length (weekly) . . . . .	166
AD DIT Disk Size Summary (weekly/monthly) . . . . .	166
AD DNS Server Memory Capacity Planning (weekly/monthly). . . . .	167
AD DNS Server Availability (daily/weekly) . . . . .	167
AD Domain Controller Availability . . . . .	167
AD Domain and Forest Changes (weekly and monthly). . . . .	168
AD GC Replication Delay Times by DC/GC (weekly/monthly) . . . . .	169
AD GC Rep Delay Times By GC/DC (weekly/monthly) . . . . .	169
AD GC Response Time (weekly/monthly) . . . . .	169
AD Log Files Disk Queue Length (weekly) . . . . .	170
AD Log Files Disk Size Summary (weekly/monthly) . . . . .	170
Active Directory Memory Usage . . . . .	170
AD Operations Master Connection Time (sorted by FSMO or server) . . . . .	171
AD FSMO Role Holder (sorted by FSMO or Server). . . . .	171

Active Directory Processor Usage . . . . .	172
Active Directory Replication Inbound . . . . .	172
Active Directory Replication Outbound . . . . .	173
Active Directory Replication Summary . . . . .	173
AD Size of SysVol (weekly/monthly) . . . . .	173
Troubleshooting Microsoft Active Directory SPI Reports . . . . .	174
<b>4 Graphs</b> . . . . .	<b>177</b>
Microsoft Active Directory SPI Graphs . . . . .	177
Active Directory GC Availability . . . . .	177
Active Directory Replication Latency . . . . .	177
Active Directory Replication Time by Global Catalog . . . . .	178
Active Directory Bind Response Time . . . . .	178
Active Directory Query Response Time . . . . .	178
<b>A Data Store Details and Policy Mapping</b> . . . . .	<b>179</b>
<b>B Report, Report Table, Data Store, and Policy Mapping Details</b> . . . . .	<b>191</b>
<b>C Graphs, Data Store, and Policy Mapping Details</b> . . . . .	<b>203</b>
<b>D Golden Metrics</b> . . . . .	<b>205</b>
Prerequisites before Monitoring Golden Metrics . . . . .	205
<b>Index</b> . . . . .	<b>211</b>

# 1 Policies

This guide contains SPI information for HP Operations Manager for UNIX version 9.00, HP Operations Manager for Linux version 9.01, and HP Operations Manager for Solaris version 9.02.

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, and Linux as the management server. The Microsoft Active Directory SPI keeps you informed about the conditions related to Microsoft Active Directory and updates you with the following activities:

- Data consistency across the domain controllers (DCs).
- Timely replication process.
- Systems outages capability.
- Successful functioning of role masters.
- DCs 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 two levels of deployment:

- Auto deployment and
- 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 various sub-groups.

## Discovery Policies (Basic and Advanced)

The Discovery policies are used to discover all the services of the Microsoft Active Directory when either automatically deployed to newly added nodes or manually deployed 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 in:

**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 the process of removing that service from the console tree and the service map. After five verifications (taking 5 hours by default), the removal occurs.

#### Result

This policy ensures that the HPOM console's services tree and the service map are up to date if ever 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 in:

**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 in:

**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 in:

**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 policies 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 in:

**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 policies 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+ in:

**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 in:

**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 in:

**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 in:

**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 in:

**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 in:

**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 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\_2k8+ in:

**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 in:

**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 in:

**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+ in:

**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 in:

**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+ in:

**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 in:

**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  $\geq 1$
- Error: Logfile queue length  $\geq 2$

#### 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 in:

**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  $\geq 1$
- Error: Logfile queue length  $\geq 2$

### 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 in:

**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 (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

## 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 policies 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 severity level because the situation may be intentional under certain circumstances.

Critical Level: <=-1

Critical Condition: Checks also to see whether DC is registered in DNS as a GC, but not registered in 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 severity level because the situation may be intentional under certain circumstances.

Critical Level: <=-1

Critical Condition: Checks also to see whether DC is registered in DNS as a GC, but not registered in 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:

## 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:

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

## 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  $\geq 1$

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 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\_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  $\geq 1$

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  $\geq 1$

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  $\geq 1$

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  $\geq 1$

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:

## 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  $\geq 1$

(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  $\geq 1$

(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:

## 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:

## 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\_2k8+ 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.

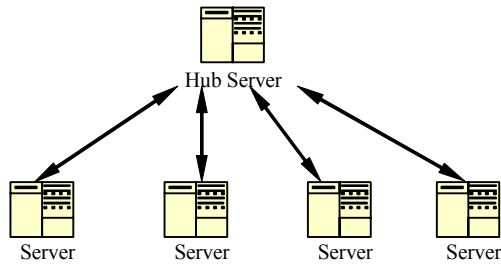
## Replication Monitoring Scenarios

You can deploy Replication Monitoring policies in the following scenarios:

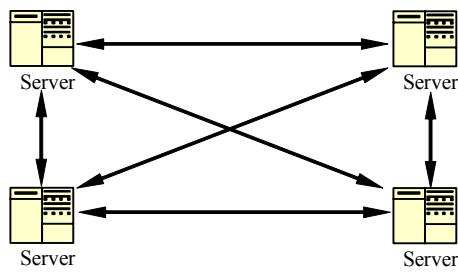
- Intra-Site Replication Monitoring: The policy [ADSPI-Rep\\_MonitorIntraSiteReplication / ADSPI-Rep\\_MonitorIntraSiteReplication\\_2k8+](#) monitors Intra-Site Replication. It checks whether replication is occurring between the DCs having connection objects in the same site.
- Inter-Site Replication 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:

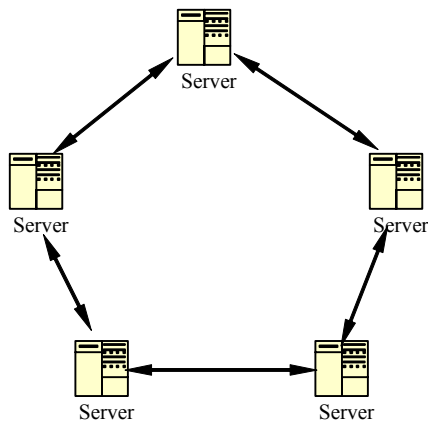
## Hub and Spoke Topology Replication Monitoring



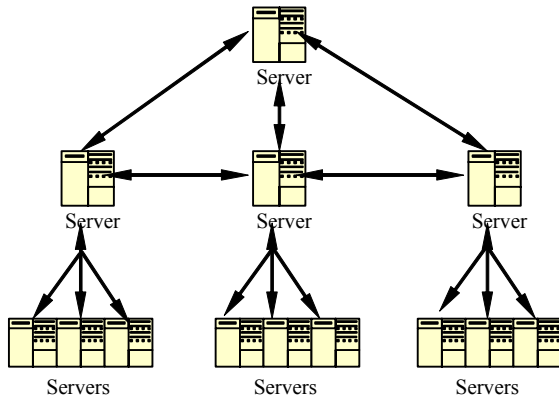
## Full Mesh Topology Replication



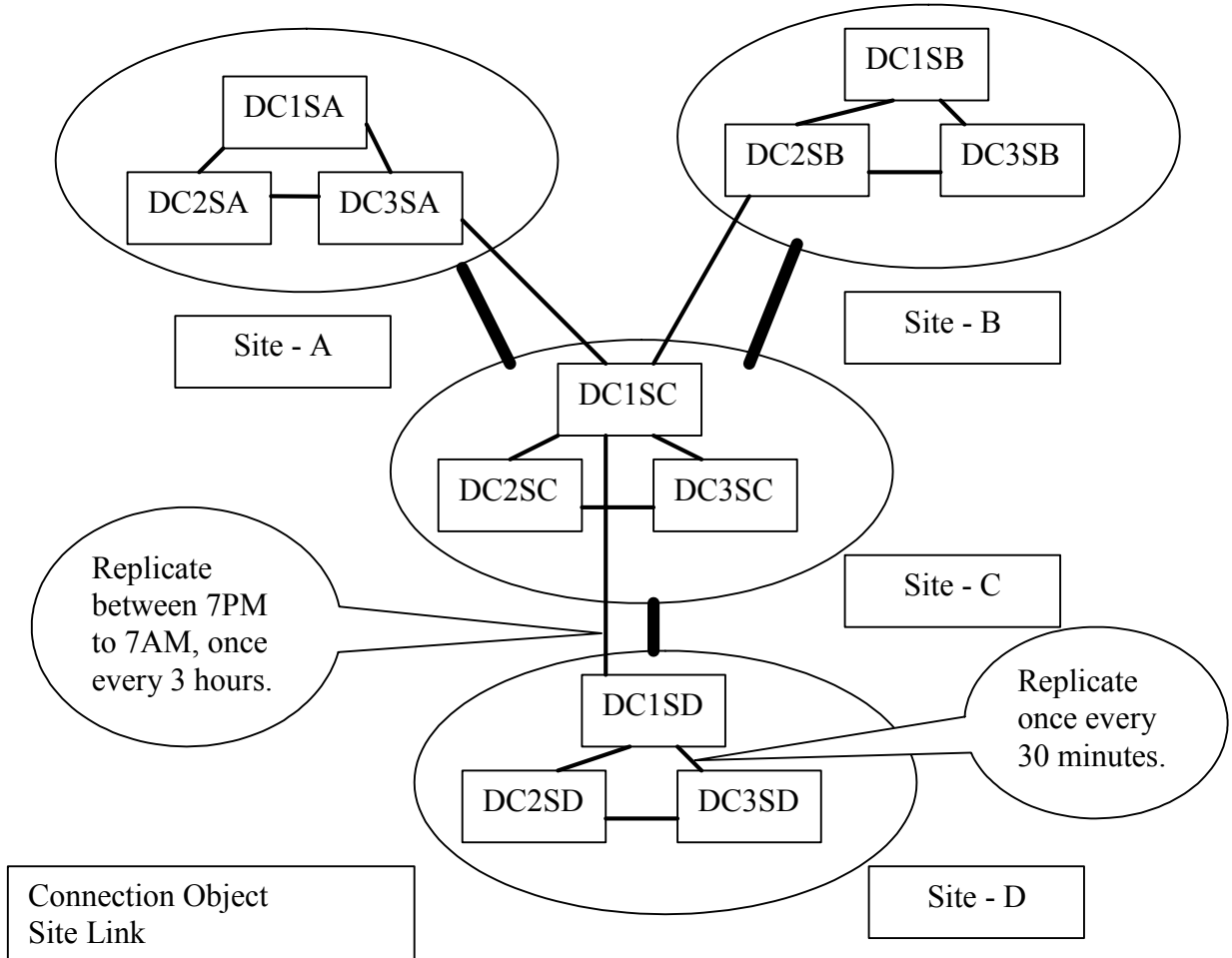
## Ring Topology Replication Monitoring



## 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:

## 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 policies 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 should 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 policies 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  $\geq 2$

Warning  $\geq 1$

### 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  $\geq 2$

Warning  $\geq 1$

### 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 Policies**

### 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 Policies**

### 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 Policies**

### 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 Policies**

## 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 should be upgraded or additional DCs should 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 should be upgraded or additional DCs should 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 should be upgraded or additional DCs should 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 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\_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 policies 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 should 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 should 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\DRS 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\DRS 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\DRS 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**

<b>Performance Monitor Object</b>	<b>Counter</b>	<b>Instance</b>
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 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**

<b>Performance Monitor Object</b>	<b>Counter</b>	<b>Instance</b>
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\_ADSSRepInBoundBytesBetweenSites

The ADSPI\_ADSSRepInBoundBytesBetweenSites 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\_ADSSRepInBoundBytesBetweenSites policy in:

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

## ADSPI\_ADSSRepInBoundBytesBetweenSites\_2k8+

The ADSPI\_ADSSRepInBoundBytesBetweenSites\_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\_ADSSRepInBoundBytesBetweenSites\_2k8+ policy in:

**Policy Bank** → **SPI for Active Directory** → **Windows Server 2008** → **Manual-Deploy** → **Replication**

## ADSPI\_ADSSRepInBoundBytesWithinSites

The ADSPI\_ADSSRepInBoundBytesWithinSites 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 should purchase or write an event-analysis tool that can filter only the user rights of interest to your organization. If Use of User Rights is enabled, not all user rights are audited. The following user rights are never audited:

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

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

- Backup Files and Directories (SeBackupPrivilege)
- Restore Files and Directories (SeRestorePrivilege) To enable auditing of the backup and restore privileges, set the following Windows Registry value to 1:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing  
(REG\_DWORD).

#### Policy Type

Windows Event Log policy

#### Policy Group

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 should purchase or write an event-analysis tool that can filter only the user rights of interest to your organization. If Use of User Rights is enabled, not all user rights are audited. The following user rights are never audited:

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

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

- Backup Files and Directories (SeBackupPrivilege)
- Restore Files and Directories (SeRestorePrivilege) To enable auditing of the backup and restore privileges, set the following Windows Registry value to 1:

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing  
(REG_DWORD)
```

### Policy Type

Windows Event Log policy

### Policy Group

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 policies 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 policies 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 sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

### Policy Type

Measurement Threshold policy

### Policy Group

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 sends a warning message to the active message browser. If the number exceeds 1,500 evaluations, the policy sends an error message. If the higher threshold is exceeded, an explicit domain trust may be necessary to reduce SAM transitive membership evaluations.

### Policy Type

Measurement Threshold policy

### Policy Group

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:

## 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 also launch tools to view the Microsoft Active Directory environment.

### Active Directory Self Healing Info tool

The Microsoft Active Directory SPI Self-Healing Info tool is available for collecting data that can aid in troubleshooting operation of the Microsoft Active Directory SPI. When launched on a managed node, the tool gathers error message-related data, log file data related to errors, and version information for installed HP Operations products/patches.

### Self-Healing Verification tool

The Self-Healing Verification tool verifies the version of the ADSPI instrumentation (executables). When launched on a managed node, the tool reports to the console if there are differences in the version of ADSPI and the ADSPI executables present on the system.

### AD DC Demotion Preparation tool

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

### 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.

It is possible to 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 from the lower versions, you must run the Delete Older ADSPI Classes tool on all nodes during the upgrade process. The Delete Older ADSPI Classes tool removes all data tables created by the older version of the SPI from the managed node. Refer to the Configuration Guide for a detailed information on upgrading the Microsoft Active Directory SPI.

## HP Operations Topology Viewer

The HP Operations Topology Viewer provides a quick means to seeing a Microsoft Active Directory environment, providing a hierarchical view in a tree (left pane), and a topological view in a map (right pane). The left pane shows the partition/site/site link components, while the map in the right pane graphically represents sites/site links and server connections.

After you launch the HP Operations Topology Viewer and enter DC access information, the tool gathers data from the domain controller. From this information a map is created, displaying sites/servers and their replication relationships across the domain.



HP Operations Topology Viewer tool

The HP Operations Topology Viewer tool operates on Windows and not on HP-UX, Solaris, and Linux. Hence ensure to 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 Chapter 5 of *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 which connection lines to display and whether to display server and site labels by right-clicking the map, selecting View Properties.... In the Site Topology View Properties page, select the Colors and Lines tabbed page. The connections are represented in default colors as follows:

- Site links: Show the links between sites. These lines are the only connections initially represented. Site connections are user-defined and are the foundation on which the Active Directory is able to build connections between servers.
- Server connections: Show the links between servers either in the same domain (intersite) or in different domains (intrasite). Solid lines represent connections automatically created by the KCC (Knowledge Consistency Checker); lines that display as dashes represent manually created connections (those connections created by the system administrator). You can open their display by selecting ViewProperties, Visibility tabbed page, then select Intersite or Intrasite.

- Invalid connections: Show links that once existed but are no longer valid. These previous connections are represented by a red line drawn (as solid or dashes, see above) from the center of the site where the server resided (the ghost server is represented as a red circle from which the red line originates).
- Server roles/links: Check Show Domain Controller Roles or Exchange Server Roles to display icons next to those DCs and Exchange servers that have been assigned specific roles/functions. You can also choose to display various Exchange DC and global catalog links.



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 with 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 cover 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. See the section "Using Reports and Graphs" for details.

After you install the Microsoft Active Directory SPI, and if HP Reporter is installed in the monitoring environment, HPOM can generate reports, using the Microsoft Active Directory SPI-collected data. The reports do not immediately appear in the HPOM console tree because they are generated every night. After HPOM runs through its first nightly schedule, on the next day you can 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' worth of data. (The previous report data is deleted.).
- Weekly: Updated nightly, a weekly report reflects the last seven days' worth of data. (Data from the previous eighth day is deleted.).
- Monthly: Updated after the calendar month completes, a monthly report summarizes all data collected during the last calendar month.

- ▶ The first monthly report most likely will represent a partial month's worth of data. For example, if the Microsoft Active Directory SPI installation occurred on March 18, the first report would be available on April 1 and would include data from March 19 to the last day in March.

#### AD DC DNS Availability (daily/weekly)

The AD DC DNS Availability report (daily/weekly) summarizes the availability of the DC's DNS based on a daily or weekly basis. The daily report provides a percentage of the DNS availability based on each hour over the last 24 hours, while the weekly report is based on hourly averages over the last seven-day period.

The Report Template File Name of this report is *g\_ADDNSDCAvailDaily.rpt* / *g\_ADDNSDCAvailWeekly.rpt*

## Report Contents

The columns of this report are defined as follows:

- *Computer Name* - Provides the name of each computer specified in the report criteria.
- *Availability* - Identifies the percentage of time the DNS server was available during the time specified in the report criteria.

## 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* - Specifies the name of the DC.
- *Domain Name* - Name of the Domain that the DC belongs to.
- *Site Name* - Specifies the time the disk space data was collected.
- *DIT Path* - DIT Database path location.
- *Queue Length* - Disk Queue Length on DIT Disk.

## AD DIT Disk Size Summary (weekly/monthly)

The AD DIT Disk Size Summary report (weekly/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 Name of this report is *g\_ADDITDiskSpaceWeekly.rpt / g\_ADDITDiskSpaceMonthly.rpt*.

## Report Contents

The chart shows the average percentage DIT disk space full on each DC. This graph makes it possible to identify when the disk is full and take appropriate actions.

The columns of the report are defined as follows:

*System Name* - Specifies the name of the DC.

*Domain Name* - Name of the Domain that the DC belongs to.

*Site Name* - Specifies the time the disk space data was collected.

*DIT Size* - The size of the DIT Database in MB.

*%Disk Space Full* - The percentage used space on the disk holding the DIT database.

## AD DNS Server Memory Capacity Planning (weekly/monthly)

The AD DNS Server Memory Capacity Planning report (weekly/monthly) graphs the memory capacity for each specified DNS server running Microsoft Active Directory services;

- One shows use over the last week
- Another shows use over the last month.

The graph indicates the minimum, maximum, and average daily usage based on the Memory/Pages Per Second performance counter.

The Report Template File Name of this report is *g\_ADDNSSrvMemCapPlanMonthly.rpt* / *g\_ADDNSSrvMemCapPlanWeekly.rpt*.

### Report Contents

This report provides one graph for each specified DNS server with Microsoft Active Directory Services running:

- Average pages per second - Average number of pages used per second.
- Max pages per second - Maximum number of pages used per second.
- Min pages per second - Minimum number of pages used per second.

## AD DNS Server Availability (daily/weekly)

The AD DNS Server Availability report (daily/weekly) summarizes the availability of DNS servers with Microsoft Active Directory services running, based on hourly and weekly data. The daily report provides a percentage of availability based on each hour over the last 24-hour period. The weekly report provides hourly percentages as well, based on each hour over the last 7-day period.

The Report Template File Name of this report is *g\_ADDNSSrvAvailDaily.rpt* / *g\_ADDNSSrvAvailWeekly.rpt*.

### Report Contents

The report displays a pie chart indicating the percentage of availability of the DNS servers with Microsoft Active Directory services running.

The columns of the report are defined as follows:

- *Response Time in milliseconds* - Provides the 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 in a series of pie charts. Possible causes of falling availability are a lack of system resources, mis-configuration, or failures in Microsoft Active Directory.

The Report Template File Name of this report is *g\_ADDCAvailability.rpt*.

## Report Contents

This report displays two pie charts, which are described as follows:

*Active Directory Availability:* The Microsoft Active Directory SPI will periodically query the directory on the DC in your environment to determine response time and availability. This graph shows the percentage of time the directory was successfully contacted.

*Active Directory Global Catalog Availability:* The Microsoft Active Directory 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* - Identifies the 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 Name for this report is *g\_ADDomainForestTrustMonthly.rpt* / *g\_ADDomainForestTrustWeekly.rpt*.

## Report Contents

In the 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/monthly)

The AD GC Replication Delay Times by DC/GC report (weekly/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, while monthly reports show averages from 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 Name of this report is *g\_ADDCGCweekly.rpt / 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/monthly)

The AD GC Rep Delay Times By GC/DC report (weekly/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 7 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 Name of this report is *g\_ADGCDCweekly.rpt / 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/monthly)

The AD GC Response Time report (weekly/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 7-day period, while the monthly report shows averages over the last calendar month. Each report identifies the data collection period with a start/end date range.

Response times are based on the GC queries and binds, which are shown in a graph. The graph shows averages for each of the GC servers. With this information it is possible to identify those GC servers that are over-loaded and take appropriate actions.

The Report Template File Name of this report is *g\_ADGCResponseTimeWeekly.rpt / g\_ADGCResponseTimeMonthly.rpt*.

## Report Contents

This report shows a chart that shows the weekly average query and bind response times (in seconds) on each 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* - Specifies the name of the DC.
- *Domain Name* - Name of the Domain that the DC belongs to.
- *Site Name* - Specifies the time the disk space data was collected.
- *Log Files Path* - Log files path location.
- *Queue Length* - Disk queue Length on the log files disk.

## AD Log Files Disk Size Summary (weekly/monthly)

The AD Log Files Disk Size Summary report (weekly/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 Name of this report is *g\_ADLogFilesDiskSpaceWeekly.rpt / g\_ADLogFilesDiskSpaceMonthly.rpt*.

### Report Contents

The columns of the report are defined as follows:

- *System Name* - Specifies the name of the DC.
- *Domain Name* - Name of the Domain to which the DC belongs.
- *Site Name* - The 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 presents 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 occurrence of page faults by the threads running in the LSASS process. 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 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\_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/sec within a site and Inbound Bytes Replicated/sec 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 that shows the average of Outbound Bytes Replicated/sec within a site and Outbound Bytes Replicated/sec among different sites by the Microsoft Active Directory Service for all monitored nodes.

## 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/monthly)

The AD Size of SysVol report (weekly/monthly) provides a weekly summary of the Sysvol (system volume shared directory on the DC) disk space information for the specified DC.

The Report Template File Name of this report is *g\_ADSizeOfSysvolWeekly.rpt / g\_ADSizeOfSysvolMonthly.rpt*.

### Report Contents

The report presents a line graph indicating the percentage of occupied disk space on sysVol drives.

The columns of this report are defined as follows:

- Domain Computer Name - Provides the name of each computer specified in the report criteria.
- Time of Collection - Specifies the time the disk space data was collected.
- Sysvol File Path - File path to where the Sysvol exists.

- Sysvol Drive Free Space - Free space on the drive which contains the Sysvol.

## Troubleshooting Microsoft Active Directory SPI Reports

If any of the report is not being 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 see 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 Make sure that the ADSPI Reporter package was installed on the HP Reporter server.
- 2 Check for errors in the Reporter Status pane.
- 3 If there are Reporter installation errors, report the problem.

### Task 3: Check the data store.

- 1 If there is no data in the Reporter database and the ADSPI Reporter package is installed properly, check that the data is being collected or logged on the managed node into the data store (CODA or HP Performance Agent).
- 2 If you are use CODA, run the following CODA diagnostic command on the managed node to get the last logged record:  
On HTTPS managed nodes: `ovcodautil -dumpds ADSPI`
- 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 that 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 have been deployed.

There will be no data unless the particular policy for each report is deployed. See [Appendix B, Report, Report Table, Data Store, and Policy Mapping Details](#) table to know the relevant policy for each report. Check on the managed node to ensure that the policy was deployed and is enabled by running the command on HTTPS nodes `ovpolicy`.

### Task 5: Check if the agent on the managed node is running

- 1 Check that the HP Operations agent is running.

- Run the following command on the managed node to get the status of the agent on the HTTPS-managed nodes:

```
ovc -status
```

- If the HP Operations agent is not running, restart with 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_DCRES
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_NTDS
AD Operations Master Connection Time	Select * from ADSPI_FSMO_MET
AD FSMO Role Holder	Select * from ADSPI_FSMO_ROLEMVT

<b>Report Name</b>	<b>SQL Command</b>
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 cover 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 has been allowed to accumulate, you can use the HPOM graphing feature to generate graphs. Graphs offer you the ability to choose a system as well as a date/time range to view the data for a more customized perspective.

#### Active Directory GC Availability

The Microsoft Active Directory SPI includes Active Directory GC Availability graph that shows the general availability of the GC on those systems hosting GC services.

To calculate availability of the GC 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 this 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.

This graph tracks latency replication response times as measured through the ADSPI-Rep\_ModifyObj and ADSPI-Rep\_Mon policies. The graph shows the results of the collected data in terms of maximum, average, and minimum response times.

## 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.

This graph tracks latency replication response times as measured through the ADSPI-Rep\_ModifyObj and ADSPI-Rep\_Mon policies. The graph shows the results of the collected data in terms of maximum, average, and minimum response times.

## Active Directory Bind Response Time

The Active Directory Bind Response Time graph shows the response times that a DC averages when binding to Microsoft Active Directory in general and the GC in particular. The graph provides 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 provides 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**

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_DITDBSIZE</b> - 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 to the DIT database file	UTF8 / Text
		InstanceValue - Size of the DIT file in MB	UINT64 / Precision 0
<b>ADSPI_DITPERCENT FULL</b> - Has 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 to the NTDS folder	UTF8 / Text
		DITPTValue - Percentage of the used space of the drive hosting DIT database	REAL64 / Precision 2
<b>ADSPI_DITQUEUE LENGTH</b> - Has 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
<b>ADSPI_DNSDR</b> - Contains the DNS response time experienced by the Domain Controller (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

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_DNSSP</b> - Contains data which 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_2k8+	IsDomainCtrl - Set to one if the DNS server is a DC and set to zero if it is not	REAL64 / Precision 2
		PagesPerSec - Value of the pages/sec counter of "memory" perfmon object	
<b>ADSPI_DOMAIN</b> - 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	
<b>ADSPI_FSMO</b> - Contains the ping and bind response times 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
<b>ADSPI_FSMO_ROLE MVMT</b> - Data is logged into this table whenever 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 has been gained and one if it has been lost by the DC	REAL64 / Precision 2

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_GCREP</b> - 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 has been replicated	UTF8 / Text
		LatencyDelta - Replication latency in seconds	REAL64 / Precision 2
<b>ADSPI_LOGDISK SIZE</b> - Has 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
<b>ADSPI_LOG PERCENTFULL</b> - Has 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
<b>ADSPI_LOGQUEUE LENGTH</b> - 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

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_NTDS</b> - Has data on the Microsoft Active Directory performance, especially replication activity.	ADSPI_Logging / ADSPI_Logging_2k8+	<b>DRAInboundBTS</b> - Total number of bytes per second received through replication. It is the sum of the number of bytes of uncompressed data and compressed data	REAL64 / Precision 2
		<b>DRAOutboundBCSec</b> - Uncompressed size in bytes of compressed replication data outbound to DCs in other sites per second	REAL64 / Precision 2
		<b>DSThreadsinUse</b> - Current number of threads in use by the directory service. This counter represents the number of threads currently servicing the clients.	UINT64 / Precision 0
		<b>DRAInboundBCSec</b> - Uncompressed size in bytes of compressed replication data inbound from DCs in other sites per second	REAL64 / Precision 2

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
		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
		DRAInboundBNC WSec - 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
		DRAOutboundBNC WSec - 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

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_NTDSPP</b> - 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



Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
<b>ADSPI_REPLA</b> <b>TENCY</b> - 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 occurred 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+	<b>LATENCYMIN</b> - Minimum latency experienced during replication from all Dcs to which a connection object exists	REAL64 / Precision 2
		<b>LATENCYMAX</b> - Maximum latency experienced during replication from all Dcs to which a connection object exists	
		<b>LATENCYAVG</b> - Average of latencies experienced during replication from all Dcs to which a connection object exists	
		<b>LASTREPDELTA MIN</b> - Minimum among time interval between current time and last replication time for all the DCs with Connection Objects	
		<b>LASTREPDELTA MAX</b> - Maximum among time interval between current time and last replication time for all the DCs with Connection Objects	
		<b>LASTREPDELTA AVG</b> - Average of time interval between current time and last replication time for all the DCs with Connection Objects	

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
		LASTREPTIME - Time elapsed, in hours, since the last change to the OvReplication object of the Source DC occurred	REAL64 / Precision 2
<b>ADSPI_RESPONSE TIME</b> - 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

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_SITE</b> - 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	
<b>ADSPI_SYSVOLPT FULL</b> - 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
<b>ADSPI_TIMESYNC</b> - 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
<b>ADSPI_TRUST</b> - 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 for Nontransitive, 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

Table in Data Store	Policy Name	Metrics in the Table and Description	Metric Data Type CODA / PA
		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
<b>ADSPI_DNSSR</b> - 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	

<b>Table in Data Store</b>	<b>Policy Name</b>	<b>Metrics in the Table and Description</b>	<b>Metric Data Type CODA / PA</b>
<b>ADSPI_INBOUNDS</b> - 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
<b>ADSPI_SCHEMA MISMATCH</b> - 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  <i>Report Content:</i> AD Domain Controller Availability  <i>Spec File:</i> ADSPI_RES_PONSETIME.spec	ADSPI_RES_PONSEMOM	SYSTEMNAME	ADSPI_RES_PONSETIME	ADSPI-Response_Logging
		AVAILABILITY		
		GCAVAILABILITY		
		DATETIME		
g_ADDCGCmonthly.rpt  <i>Report Content:</i> AD GC Rep Delay Times By DC/GC - Monthly  <i>Spec File:</i> ADSPI_GCREP.spec	ADSPI_REP_GC	SYSTEMNAME	ADSPI_GCREP	ADSPI-Rep_GC_Check_and_Threshold
		GCREPNAME		
		LATENCY DELTA		
		DATETIME		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
<b>g_ADDCGC</b> <b>weekly.rpt</b>  <i>Report Content:</i> AD GC Rep Delay Times By DC/GC - Weekly  <i>Spec File:</i> ADSPI_GCREP. spec	ADSPI_REP_GC	SYSTEMNAME	ADSPI_GCREP	ADSPI-Rep_GC_ Check_and_ Threshold
		GCREPNAME		
		LATENCY DELTA		
		DATETIME		
<b>g_ADDITDisk</b> <b>SpaceMonthly</b> <b>.rpt</b>  <i>Report Content:</i> AD DIT Disk Size Summary - Monthly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_DIT DATABASE SIZE.spec</li> <li>• ADSPI_DIT PERCENT FULL.spec</li> <li>• ADSPI_DO MAIN.spec</li> <li>• ADSPI_SITE. spec</li> </ul>	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
<b>g_ADDITDisk</b> <b>SpaceWeekly.rpt</b>  <i>Report Content:</i> AD DIT Disk Size Summary - Weekly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_DIT DATABASESIZE.spec</li> <li>• ADSPI_DIT PERCENT FULL.spec</li> <li>• ADSPI_ DOMAIN. spec</li> <li>• ADSPI_SITE. spec</li> </ul>	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_ADDITQueueLengthWeekly.rpt  <i>Report Content:</i> AD DIT Disk Queue Length - Weekly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_DO MAIN.spec</li> <li>• ADSPI_SITE.spec</li> <li>• ADSPI_DIT QUEUE LENGTH.spec</li> </ul>	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_ADDNSDCAvailDaily.rpt  <i>Report Content:</i> AD DC DNS Availability Report - Daily Summary  <i>Spec File:</i> ADSPI_DNSDR.spec	ADSPI_DNS_DCRESP	DATETIME	ADSPI_DNSDR	ADSPI-DNS_DC_Response Policy
		RESPTIME		
		SYSTEMNAME		
g_ADDNSDCAvailWeekly.rpt  <i>Report Content:</i> AD DC DNS Availability Report - Weekly Summary  <i>Spec File:</i> 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  <i>Report Content:</i> AD DNS Server availability Report - Daily Summary  <i>Spec File:</i> ADSPI_DNSSR.spec	ADSPI_DNSSR	DATETIME	ADSPI_DNSSR	ADSPI-DNS_ Server_Res ponse
		RESPONSE TIME		
		ISDOMAINCON TROLLER		
		SYSTEMNAME		
g_ADDNSSrv AvailWeekly.rpt  <i>Report Content:</i> AD DNS Availability Report - Weekly Summary  <i>Spec File:</i> ADSPI_DNSSR. spec	ADSPI_DNSSR	DATETIME	ADSPI_DNSSR	ADSPI-DNS_ Server_Res ponse
		RESPONSE TIME		
		ISDOMAINCON TROLLER		
		SYSTEMNAME		
g_ADDNSSrv MemCapPlan Monthly.rpt  <i>Report Content:</i> AD DNS Server Memory Capacity Planning Report - Monthly Summary  <i>Spec File:</i> ADSPI_DNSSP. spec	ADSPI_DNSSP	DATETIME	ADSPI_DNSSP	ADSPI-DNS_ LogDNSPages Sec
		PAGESPERSEC		
		ISDOMAIN CTRL		
		SYSTEMNAME		
g_ADDNSSrv MemCapPlan Weekly.rpt  <i>Report Content:</i> AD DNS Server Memory Capacity Planning Report - Monthly Summary  <i>Spec File:</i> ADSPI_DNSSP. spec	ADSPI_DNSSP	DATETIME	ADSPI_DNSSP	ADSPI-DNS_Lo gDNSPagesSec
		PAGESPERSEC		
		ISDOMAIN CTRL		
		SYSTEMNAME		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
<p>g_ADDomain ForestTrust Monthly.rpt</p> <p><i>Report Content:</i> AD Domain and Forest Trust Changes - Monthly</p> <p><i>Spec File:</i> ADSPI_Trust mon.spec</p>	ADSPI_TRUST	SYSTEMNAME	ADSPI_TRUST	ADSPI-Trust_Mon_Add_Del and ADSPI-Trust_Mon_Modify
		DATETIME		
		CHANGETYPE		
		TRUSTING DOMAIN		
		TRUSTED DOMAIN		
		TRUSTATTRIBUTES		
		TRUSTDIRECTION		
		TRUSTSTATUS		
		TRUSTSTATUS STRING		
		TRUSTTYPE		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
<p>g_ADDomainForestTrustWeekly.rpt</p> <p><i>Report Content:</i> AD Domain and Forest Trust Changes - Weekly</p> <p><i>Spec File:</i> ADSPI_Trustmon.spec</p>	ADSPI_TRUST	SYSTEMNAME	ADSPI_TRUST	ADSPI-Trust_Mon_Add_Del and ADSPI-Trust_Mon_Modify
		DATETIME		
		CHANGETYPE		
		TRUSTING DOMAIN		
		TRUSTED DOMAIN		
		TRUSTATTRIBUTES		
		TRUSTDIRECTION		
		TRUSTSTATUS		
		TRUSTSTATUS STRING		
TRUSTTYPE				
<p>g_ADFSMORoleHolderMovMonthly.rpt</p> <p><i>Report Content:</i> FSMO Role Holder Report - Monthly</p> <p><i>Spec File:</i> ADSPI_FSMO_RoleMvmt.spec</p>	ADSPI_FSMO_ROLEMVMТ	SYSTEMNAME	ADSPI_FSMO_ROLEMVMТ	ADSPI-FSMO_RoleMvmt
		DATETIME		
		FSMORM		
		ISROLE HOLDER		
<p>g_ADFSMORoleHolderMovWeekly.rpt</p> <p><i>Report Content:</i> FSMO Role Holder Report - Weekly</p> <p><i>Spec File:</i> ADSPI_FSMO_RoleMvmt.spec</p>	ADSPI_FSMO_ROLEMVMТ	SYSTEMNAME	ADSPI_FSMO_ROLEMVMТ	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  <i>Report Content:</i> AD GC Rep Delay Times By GC/DC - Monthly  <i>Spec File:</i> ADSPI_GCREP. spec	ADSPI_REP_GC	DATETIME	ADSPI_GCREP	ADSPI-Rep_GC_ Check_and_Thre s hold
		SYSTEMNAME		
		GCREPNAME		
		LATENCY DELTA		
g_ADGCDC weekly.rpt  <i>Report Content:</i> AD GC Rep Delay Times By GC/DC - Weekly  <i>Spec File:</i> ADSPI_GCREP. spec	ADSPI_REP_GC	DATETIME	ADSPI_GCREP	ADSPI-Rep_GC_ Check_and_ Threshold
		SYSTEMNAME		
		GCREPNAME		
		LATENCY DELTA		
g_ADGCResponseTimeMonthly. rpt  <i>Report Content:</i> AD GC Response Time - Monthly  <i>Spec File:</i> ADSPI_Respon seTime.spec	ADSPI_ RESPONSE MON	SYSTEMNAME	ADSPI_ RESPONSE TIME	ADSPI-Respon se_Logging
		DATETIME		
		GCBINDTIME		
		GCQUERY TIME		
		GCPRESENT		

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADGCResponseTimeWeekly.rpt  <i>Report Content:</i> AD GC Response Time - Weekly  <i>Spec File:</i> ADSPI_ResponseTime.spec	ADSPI_RESPONSEMON	SYSTEMNAME	ADSPI_RESPONSETIME	ADSPI-Response_Logging
		DATETIME		
		GCBINDTIME		
		GCQUERYTIME		
g_ADLogFilesDiskSpaceMonthly.rpt  <i>Report Content:</i> AD Log Files Disk Size Summary - Monthly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_LOGDISKSIZE.spec</li> <li>• ADSPI_LOGPERCENTFULL.spec</li> <li>• ADSPI_DOMAIN.spec</li> <li>• ADSPI_SITE.spec</li> </ul>	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
g_ADLogFilesDiskSpaceWeekly.rpt  <i>Report Content:</i> AD Log Files Disk Size Summary - Weekly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_LOGDISKSIZE.spec</li> <li>• ADSPI_LOGPERCENTFULL.spec</li> <li>• ADSPI_DOMAIN.spec</li> <li>• ADSPI_SITE.spec</li> </ul>	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
g_ADLogFilesDiskSpaceWeekly.rpt  <i>Report Content:</i> AD Log Files Disk Size Summary - Weekly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_LOGDISKSIZE.spec</li> <li>• ADSPI_LOGPERCENTFULL.spec</li> <li>• ADSPI_DOMAIN.spec</li> <li>• ADSPI_SITE.spec</li> </ul>	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

Report Name	Report Table	Report Table Attributes	Data Store Class Name	Policy Logging Data
g_ADLogQueueLengthWeekly.rpt  <i>Report Content:</i> AD Log Files Disk Queue Length - Weekly  <i>Spec Files:</i> <ul style="list-style-type: none"> <li>• ADSPI_DOMAIN.spec</li> <li>• ADSPI_SITE.spec</li> <li>• ADSPI_LOG_QUEUELENGTH.spec</li> </ul>	ADSPI_Domain	DATETIME	ADSPI_DOMAIN	ADSPI-DIT_TotalDitSize
		SYSTEMNAME		
		DOMAIN VALUE		
	ADSPI_Site	SITEVALUE	ADSPI_SITE	ADSPI-DIT_TotalDitSize
ADSPI_LOG_QUEUELENGTH		SYSTEMNAME	ADSPI_LOG_QUEUELENGTH	ADSPI-DIT_LogFilesQueueLength
		DATETIME		
		LGQLENNAME		
		LGQLEN VALUE		

<b>Report Name</b>	<b>Report Table</b>	<b>Report Table Attributes</b>	<b>Data Store Class Name</b>	<b>Policy Logging Data</b>
g_ADMemory Usage.rpt  <i>Report Content:</i> Active Directory Memory Usage  <i>Spec File:</i> ADSPI_NTDSP.spec	ADSPI_NTDSP	DATETIME SYSTEMNAME WORKINGSET PAGEFAULTS SEC	ADSPI_NTDSP	ADSPI_Logging
g_ADOpMstr ConTimeBy Fsmo.rpt  <i>Report Content:</i> AD Operations Master Connection Time Report by FSMO  <i>Spec File:</i> ADSPI_FSMO.spec	ADSPI_FSMO_MET	GMT DATETIME FSMO PINGTIME SERVER FSMOBIND TIME	ADSPI_FSMO	ADSPI-FSMO_Logging
g_ADOpMstr ConTimeBySvr.rpt  <i>Report Content:</i> AD Operations Master Connection Time Report by Server  <i>Spec File:</i> ADSPI_FSMO.spec	ADSPI_FSMO_MET	GMT DATETIME FSMO PINGTIME SERVER FSMOBIND TIME	ADSPI_FSMO	ADSPI-FSMO_Logging



<b>Report Name</b>	<b>Report Table</b>	<b>Report Table Attributes</b>	<b>Data Store Class Name</b>	<b>Policy Logging Data</b>
g_ADProcess Usage.rpt  <i>Report Content:</i> Active Directory Processor Usage  <i>Spec File:</i> ADSPI_NTDS.spec	ADSPI_NTDS	DATETIME	ADSPI_NTDS	ADSPI_Logging
		SYSTEMNAME		
		DSTHEADS INUSE		
g_ADReplication Inbound.rpt  <i>Report Content:</i> Active Directory Replication Inbound  <i>Spec File:</i> ADSPI_NTDS.spec	ADSPI_NTDS	DATETIME	ADSPI_NTDS	ADSPI_Logging
		SYSTEMNAME		
		DRAINBOUND BCSEC		
		DRAINBOUND BSNCWSSEC		
g_ADReplication Outbound.rpt  <i>Report Content:</i> Active Directory Replication Outbound  <i>Spec File:</i> ADSPI_NTDS.spec	ADSPI_NTDS	DATETIME	ADSPI_NTDS	ADSPI_Logging
		SYSTEMNAME		
		DRAOUT BOUNDBCSEC		
		DRAOUTBOUN DBNCWSSEC		

<b>Report Name</b>	<b>Report Table</b>	<b>Report Table Attributes</b>	<b>Data Store Class Name</b>	<b>Policy Logging Data</b>
g_ADReplication Summary.rpt  <i>Report Content:</i> Active Directory Replication Summary  <i>Spec File:</i> ADSPI_NTDS. spec	ADSPI_NTDS	DATETIME SYSTEMNAME DRAINBOUND BTS DRAOUTBOUN DBTS	ADSPI_NTDS	ADSPI_Logging
g_ADSizeOf SysvolMonthly. rpt  <i>Report Content:</i> AD Size of Sysvol Report - Monthly Summary  <i>Spec File:</i> ADSPI_SYSVOLPERCENT FULL.spec	ADSPI_SYSVOL _PCT_FULL	SYSTEMNAME DATETIME SYSPERC NAME SYSPERC VALUE	ADSPI_SYSVOL PTFULL	ADSPI-Sysvol_ PercentFull
g_ADSizeOf SysvolWeekly .rpt  <i>Report Content:</i> AD Size of Sysvol Report - Weekly Summary  <i>Spec File:</i> ADSPI_SYSVOLPERCENT FULL.spec	ADSPI_SYSVOL _PCT_FULL	SYSTEMNAME DATETIME SYSPERC NAME SYSPERC VALUE	ADSPI_SYSVOL PTFULL	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 the data-collection procedure. The data store class creator for all the reports is adspi\_ddf.bat.

**Table 6 Graphs and Policy Mapping Details**

<b>Graph Name</b>	<b>Policy Logging Data</b>	<b>Spec File</b>	<b>Data Store Data Class</b>
Active Directory Replication Latency Graph	ADSPI-Rep_MonitorIntraSiteReplication	ADSPI_Rep Latency.spec	ADSPI_Rep Latency
	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 which are basic and fundamental for monitoring the Microsoft Active Directory environment. You can deploy the policies listed in Table 9 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 occurring 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

Ensure the following requirements before you monitor the golden metrics:

- 1 SPI Data Collector Instrumentation category is deployed.
- 2 ADSPI\_CreateDataSources policy is deployed.
- 3 Basic Discovery and Advanced Discovery policies are deployed.

**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+

<b>Metric</b>	<b>Metric Description</b>	<b>Policy</b>
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+		

<b>Metric</b>	<b>Metric Description</b>	<b>Policy</b>
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+

<b>Metric</b>	<b>Metric Description</b>	<b>Policy</b>
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+



<b>Metric</b>	<b>Metric Description</b>	<b>Policy</b>
Security	Relates to the monitoring of various security aspects of the Microsoft Active Directory.	ADSPI_KDCFailureGrantTicket / ADSPI_KDCFailureGrantTicket_2k8+ <hr/> ADSPI_PrivilegedAccounts / ADSPI_PrivilegedAccounts_2k8+ <hr/> ADSPI_SecErrorsLogon / ADSPI_SecErrorsLogon_2k8+ <hr/> ADSPI_DirComputerModif / ADSPI_DirComputerModif_2k8+



# Index

## A

ADSPI\_Logging, 137  
ADSPI-AutoDiscovery\_DIT\_2k8+, 15  
ADSPI-CreateDatasources, 22  
ADSPI-DIT\_LogfilesQueueLength, 23  
Auto Baseline Polices, 114

## D

Discovery Policies, 14  
    ADSPI\_Discovery, 14  
    ADSPI-AutoDiscovery\_Delete, 14  
    ADSPI-AutoDiscovery\_DIT, 14  
    ADSPI-AutoDiscovery\_DIT\_2k8+, 15  
    ADSPI-AutoDiscovery\_DNS, 15  
    ADSPI-AutoDiscovery\_DNS\_2k8+, 16  
    ADSPI-AutoDiscovery\_FSMO, 16  
    ADSPI-AutoDiscovery\_FSMO\_2k8+, 17  
    ADSPI-AutoDiscovery\_GC, 17  
    ADSPI-AutoDiscovery\_GC\_2k8+, 18  
    ADSPI-AutoDiscovery\_PBHS, 18  
    ADSPI-AutoDiscovery\_PBHS\_2k8+, 19  
    ADSPI-AutoDiscovery\_Rep, 20  
    ADSPI-AutoDiscovery\_Rep\_2k8+, 21  
    ADSPI-AutoDiscovery\_RODC\_2k8+, 21  
    ADSPI-AutoDiscovery\_Trust, 22  
    ADSPI-AutoDiscovery\_Trust\_2k8+, 22

## H

Health Monitor Policies, 123  
HP Operations Topology Viewer Tool, 162

## M

Measurement Threshold Policy  
    ADSPI\_ActiveAuthKerberos, 116  
    ADSPI\_ActiveAuthLogon, 117  
    ADSPI\_ADCImportFailures, 118  
    ADSPI-DIT\_DITPercentFull, 29  
    ADSPI-DIT\_DITQueueLength, 24  
    ADSPI-DIT\_LogfilesPercentFull, 27  
    ADSPI-DIT\_LogfilesQueueLength, 23  
    ADSPI-DIT\_TotalDITSize, 26  
    ADSPI-DNS\_DC\_A\_Chk, 30  
    ADSPI-DNS\_DC\_CName\_Chk, 32  
    ADSPI-DNS\_DC\_Response, 34  
    ADSPI-DNS\_Extra\_GC\_SRV\_Chk, 36  
    ADSPI-DNS\_Extra\_Kerberos\_SRV\_Chk, 38  
    ADSPI-DNS\_Extra\_LDAP\_SRV\_Chk, 39  
    ADSPI-DNS\_GC\_A\_Chk, 40  
    ADSPI-DNS\_GC\_SRV\_CHK, 42  
    ADSPI-DNS\_GC\_StrandedSite, 44  
    ADSPI-DNS\_Island\_Server, 47  
    ADSPI-DNS\_Kerberos\_SRV\_Chk, 49  
    ADSPI-DNS\_LDAP\_SRV\_Chk, 52  
    ADSPI-DNS\_LogDNSPagesSec, 49  
    ADSPI-DNS\_Obsolete\_GUIDs, 55  
    ADSPI-DNS\_Server\_Response, 54  
    ADSPI-FSMO\_Consist\_INFRA, 77  
    ADSPI-FSMO\_Consist\_PDC, 80  
    ADSPI-FSMO\_GC\_Infrastructure\_Check, 60  
    ADSPI-FSMO\_INFRA\_Bind, 58  
    ADSPI-FSMO\_INFRA\_Ping, 59  
    ADSPI-FSMO\_NAMING\_Bind, 62  
    ADSPI-FSMO\_NAMING\_Ping, 63  
    ADSPI-FSMO\_PDC\_Bind, 64  
    ADSPI-FSMO\_PDC\_Ping, 66  
    ADSPI-FSMO\_RoleMvmt\_INFRA, 71  
    ADSPI-Rep\_InboundObjs, 90  
    ADSPI-Rep\_TimeSync, 98

## P

Policy Group  
    Auto Deploy Polices, 13  
    Manual Deploy, 114

## R

- Replication Monitoring Configuration, 87
- Replication Monitoring Scenarios, 85
- Response Time Monitoring, 99

## S

- Scheduled Task Policy
  - ADSPI-FSMO\_Consist, 75
  - ADSPI-FSMO\_Logging, 61
  - ADSPI-FSMO\_RoleMvmt, 70
  - ADSPI-Rep\_Delete\_OvRep\_Object, 89
  - ADSPI-Rep\_Modify\_User\_Object, 95
  - ADSPI-Rep\_ModifyObj, 96
  - ADSPI-Response\_Logging, 103

## W

- Windows Event Log Policy
  - ADSPI\_ADCFwdAllWarnErrorMSADC, 117
  - ADSPI\_DNSServ\_FwdAllWarnError, 124
  - ADSPI\_FwdAllInformationDS, 125
  - ADSPI\_FwdAllInformationFRS, 125
  - ADSPI\_FwdAllWarnErrorDS, 126
  - DSPI-Sysvol\_FRS, 108
- Windows Management Interface Policy
  - ADSPI\_DomainChange, 119
  - ADSPI\_OUChanges, 120
  - ADSPI\_Trust\_Mon\_Add\_Del, 113
  - ADSPI\_Trust\_Mon\_Modify, 112

## 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:**

