

# HP Operations Smart Plug-in for Microsoft<sup>®</sup> Enterprise Servers

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

Software Version: 8.04

---

## Reference Guide

Document Release Date: July 2012  
Software Release Date: July 2012



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2010-2012 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.

## 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 user ID, go to:

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

# Contents

- 1 Introduction ..... 17
  - Components of Microsoft Enterprise Server SPI ..... 18
    - Policies ..... 18
    - Tools ..... 18
    - Reports ..... 18
    - Graphs ..... 18
  
- 2 Microsoft Enterprise Servers SPI for BizTalk Server 2006 ..... 19
  - Policies ..... 19
    - Availability Monitoring ..... 19
      - EBIZ\_BizTalkServerServices policy ..... 20
    - Performance Monitoring ..... 20
    - Windows Event Log Monitoring ..... 22
    - Database Connectivity ..... 22
    - Server Logging ..... 23
    - Discovery ..... 25
  - Reports ..... 25
    - BTS Document Process Rate (Monthly/Weekly) ..... 25
    - BTS Processes CPU Statistics ..... 25
    - BTS Processes Memory Statistics ..... 26
    - BTS Orchestration Statistics (Monthly/Weekly) ..... 26
    - BTS Transactional Rate (Monthly/Weekly) ..... 26
    - BTS Suspended Documents Report (Monthly/Weekly) ..... 27
    - BTS TDDS Statistics ..... 27
    - BTS Enterprise Single Sign-on(Monthly) ..... 27
  - Graphs ..... 27
    - Page Faults/sec ..... 28
    - Working Set ..... 28
    - Private Bytes ..... 28
  
- 3 Microsoft Enterprise Servers SPI for BizTalk Server 2010 ..... 29
  - Overview ..... 29
  - Policies ..... 29
    - SPI Metrics and Collections ..... 30
    - Availability ..... 30
      - Metrics Monitored ..... 31
        - Metric ID: 841402 ..... 31
        - Metric ID: 841403 ..... 31
        - Metric ID: 841404 ..... 31
      - Metrics Logged ..... 32

Collection ID: 840014 . . . . .	32
Event Log Policies . . . . .	32
BTS_Fwd_Application_Errors . . . . .	32
BTS_Fwd_Application_Warning . . . . .	32
Discovery . . . . .	33
BTS_Discovery . . . . .	33
BTS_Cluster_Re_Discovery . . . . .	33
Document Processing . . . . .	33
Metrics Logged . . . . .	34
Collection ID: 840012 . . . . .	34
File Receive Adapter . . . . .	34
Metrics Monitored . . . . .	35
Metric ID: 841502 . . . . .	35
Metric ID: 841503 . . . . .	35
Metrics Logged . . . . .	36
Collection ID: 840015 . . . . .	36
Message Box . . . . .	36
Metrics Monitored . . . . .	37
Metric ID: 841002 . . . . .	37
Metric ID: 845002 . . . . .	37
Metric ID: 845005 . . . . .	38
Metrics Logged . . . . .	39
Collection ID: 840001 . . . . .	39
Collection ID: 840005 . . . . .	39
Messaging . . . . .	40
Metrics Monitored . . . . .	40
Metric ID: 843002 . . . . .	40
Metric ID: 843003 . . . . .	41
Metric ID: 843004 . . . . .	41
Metric ID: 844002 . . . . .	42
Metric ID: 844003 . . . . .	42
Metric ID: 844004 . . . . .	43
Metric ID: 846002 . . . . .	43
Metric ID: 846004 . . . . .	44
Metric ID: 846005 . . . . .	44
Metric ID: 848002 . . . . .	45
Metrics Logged . . . . .	46
Collection ID: 840003 . . . . .	46
Collection ID: 840004 . . . . .	47
Collection ID: 840006 . . . . .	47
Collection ID: 840008 . . . . .	48
Orchestration Engine . . . . .	49
Metrics Monitored . . . . .	49
Metric ID: 842002 . . . . .	49
Metric ID: 842005 . . . . .	50
Metric ID: 842012 . . . . .	50
Metric ID: 842013 . . . . .	51

Metric ID: 842018.....	51
Metric ID: 842021.....	52
Metric ID: 842023.....	52
Metrics Logged.....	53
Collection ID: .....	53
Performance .....	54
Metrics Logged.....	54
Collection ID: 840009.....	54
Collection ID: 840010.....	55
Collection ID: 840011.....	55
Sharepoint Adapter .....	56
Metrics Monitored .....	56
Metric ID: 847002.....	56
Metric ID: 847003.....	57
Metric ID: 847004.....	57
Metric ID: 847005.....	58
Metric ID: 847006.....	58
Metric ID: 847007.....	59
Metric ID: 847008.....	60
Metrics Logged.....	61
Collection ID: 840007.....	61
Tracking Data Decode Services (TDDS) .....	62
Metrics Logged.....	62
Collection ID: 840013.....	62
Reports .....	63
BizTalk Server Document Processing Statistics .....	63
Tracking Date Decode Statistics (TDDS) Statistics Report .....	63
BizTalk Server Processes CPU Statistics - Application Service .....	64
BizTalk Server Processes CPU Statistics - Enterprise Single Sign On (SSO) Service .....	64
BizTalk Server Processes CPU Statistics - Rule Engine Update Service.....	64
BizTalk Server Processes Memory Statistics - Application Service .....	65
BizTalk Server Processes Memory Statistics - Enterprise Single Sign On (SSO) Service .....	65
BizTalk Server Processes Memory Statistics - Rule Engine Update Service.....	65
Graphs .....	66
BizTalk Service CPU Statistics.....	66
Enterprise SSO Service CPU Statistics.....	66
Rule Engine Update Service CPU Statistics .....	66
BizTalk Service Memory Statistics.....	66
Enterprise SSO Memory Statistics.....	66
Rule Engine Update Service Memory Statistics .....	66
Document Processing Statistics by Biztalk Server .....	66
Orchestration Statistics by Biztalk Server .....	66
BizTalk TDDS Statistics .....	66
<b>4 Microsoft Enterprise Servers SPI for Internet Security and Acceleration Server 2006.....</b>	<b>67</b>
Policies.....	67
Availability Monitoring.....	67
Performance Monitoring .....	68

Firewall Service . . . . .	68
Firewall Engine . . . . .	69
Job Scheduler . . . . .	69
Network Load Balancing . . . . .	70
Microsoft Data Engine . . . . .	70
Remote Access. . . . .	71
ISA Server Control . . . . .	71
ISA Server Storage. . . . .	72
Storage Configuration . . . . .	72
Windows Event Log Monitoring . . . . .	73
Server Logging . . . . .	73
Discovery . . . . .	74
Reports . . . . .	74
Firewall, Scheduled Cache Content Download, and ISA Server Control Process CPU Statistics . . . . .	74
Dropped Packets Statistics . . . . .	75
Firewall Statistics . . . . .	75
Firewall, Scheduled Cache Content Download, and ISA Server Control Process Memory Statistics . . . . .	75
ISA Server Cache Statistics . . . . .	75
Web Proxy Statistics . . . . .	76
Web Proxy Request Statistics . . . . .	76
Web Proxy Sites Granted and Denied Statistics. . . . .	77
Graphs . . . . .	77
<b>5 Microsoft Enterprise Servers SPI for Microsoft Office SharePoint Server 2007 . . . . .</b>	<b>79</b>
Policies . . . . .	79
Availability Monitoring . . . . .	80
Service Monitoring. . . . .	80
Application Monitoring . . . . .	81
Server Logging . . . . .	82
Discovery . . . . .	85
Reports . . . . .	85
Memory and CPU reports . . . . .	85
IIS Worker Process reports . . . . .	86
Graphs . . . . .	86
<b>6 Microsoft Enterprise Servers SPI for Microsoft SharePoint Server 2010. . . . .</b>	<b>89</b>
Policies . . . . .	89
Availability Monitoring . . . . .	89
Service Monitoring. . . . .	90
Application Monitoring . . . . .	91
Server Logging . . . . .	91
Discovery . . . . .	94
Reports . . . . .	94
Memory and CPU reports . . . . .	94
IIS Worker Process reports . . . . .	95
Graphs . . . . .	96



7 Microsoft Enterprise Servers SPI for Office Communications Server 2007 .....	99
Policies .....	99
Discovery .....	99
AccessEdgeServer .....	100
Policies deployed on OCS 2007 and OCS 2007 R2 .....	101
OCS_AccessEdgeServer_Logging .....	101
OCS_AccessEdgeServer_FlowControlledConnectionsDropped Policy .....	101
OCS_AccessEdgeServer_AddressSpaceUsage Policy .....	102
OCS_AccessEdgeService_PrivateBytes Policy .....	102
OCS_Check_AccessEdgeServiceStatus Policy .....	103
OCS_AccessEdgeServer_ActiveTLSConnections Policy .....	103
OCS_AccessEdgeServer_MsgsDroppedPerSecDueToCertMismatch Policy .....	103
OCS_AccessEdgeServer_RejectedExtEdgeServerConnectionsPerSec Policy .....	104
OCS_AccessEdgeServer_SendsTimedOut Policy .....	104
OCS_AccessEdgeServer_IncomingResponsesDroppedPerSec Policy .....	105
OCS_AccessEdgeService_WorkingSet Policy .....	105
OCS_AccessEdgeServer_MsgPerSecDroppedDueToUnknownDomain Policy .....	105
OCS_AccessEdgeServer_FlowControlledConnections Policy .....	106
OCS_AccessEdgeService_ThreadCount Policy .....	106
OCS_AccessEdgeServer_RejectedExtEdgeClientConnectionsPerSec Policy .....	107
OCS_AccessEdgeService_Logging Policy .....	107
OCS_AccessEdgeService_PageFaultsPerSec Policy .....	108
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedDomain Policy .....	108
OCS_AccessEdgeServer_MessagesInServer Policy .....	108
OCS_AccessEdgeServer_AverageIncomingMessageProcessingTime Policy .....	109
OCS_AccessEdgeService_ProcessorTime Policy .....	109
OCS_AccessEdgeServer_IncomingRequestsDroppedPerSec Policy .....	110
OCS_AccessEdgeServer_AboveLimitConnectionsDropped Policy .....	110
OCS_AccessEdgeServer_IncomingMsgHeldAboveOverloadWatermark Policy .....	110
Policies deployed only on OCS 2007 .....	111
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnresolvedDomain Policy .....	111
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain Policy .....	111
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnauthIMDomain Policy .....	112
CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain Policy .....	112
Policies deployed only on OCS 2007 R2 .....	113
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnresolvedDomain_R2 Policy .....	113
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain_R2 Policy .....	114
OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnauthIMDomain_R2 Policy .....	114
CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain_R2 Policy .....	115
Archiving CDR Server .....	115
OCS_ArchivingCDRService_Logging Policy .....	116
OCS_ArchivingCDRService_ThreadCount Policy .....	116
OCS_Check_ArchivingCDRServiceStatus Policy .....	117
OCS_ArchivingCDRServer_NumberOfMessagesNotWrittenToDB Policy .....	117
OCS_ArchivingCDRService_PageFaultsPerSec Policy .....	117
OCS_ArchivingCDRService_WorkingSet Policy .....	118
OCS_ArchivingCDRServer_NumberOfDroppedMQMessages Policy .....	118

OCS_ArchivingCDRService_ProcessorTime Policy .....	118
OCS_ArchivingCDRServer_NumberOfValidationFailedMessages Policy.....	119
OCS_ArchivingCDRService_PrivateBytes Policy.....	119
AVConfServer .....	119
OCS_AVConfService_PrivateBytes Policy .....	120
OCS_AVConfServer_NumberOfActiveConferences Policy.....	120
OCS_AVConfService_ProcessorTime Policy .....	121
OCS_AVConfService_WorkingSet Policy.....	121
OCS_Check_AVConfServiceStatus Policy.....	121
OCS_AVConfServer_MCUHealthState Policy .....	122
OCS_AVConfService_ThreadCount Policy .....	122
OCS_AVConfService_PageFaultsPerSec Policy .....	123
OCS_AVConfService_Logging Policy.....	123
AVEdgeServer .....	124
Policies deployed on OCS 2007 and OCS 2007 R2.....	124
OCS_AVEdgeServer_UDPAllocateRqstExceedingPortLimit Policy .....	124
OCS_AVAuthService_PageFaultsPerSec Policy .....	125
OCS_AVAuthService_PrivateBytes Policy .....	125
OCS_AVAuthService_ProcessorTime Policy .....	125
OCS_AVAuthService_ThreadCount Policy .....	126
OCS_AVEdgeServer_WorkingSet Policy.....	126
OCS_AVEdgeServer_LoggingPolicy .....	127
OCS_Check_AVAuthServiceStatus Policy.....	127
OCS_Check_AVEdgeServiceStatus Policy .....	128
OCS_AVEdgeService_PageFaultsPerSec Policy .....	128
OCS_AVEdgeService_PrivateBytes Policy .....	128
OCS_AVEdgeService_ProcessorTime Policy.....	129
OCS_AVEdgeService_ThreadCount Policy .....	129
OCS_AVEdgeService_WorkingSet Policy .....	130
OCS_AVEdgeServer_BadRequestsReceivedPerSec Policy.....	130
OCS_AVEdgeServer_TCPAllocRqstExceedingPortLimit Policy .....	130
OCS_AVEdgeServer_TCPAuthenticationFailuresPerSec Policy .....	131
OCS_AVEdgeServer_UDPAllocateRqstExceedingPortLimit Policy .....	131
OCS_AVEdgeServer_UDPAuthenticationFailuresPerSec Policy.....	132
Policies deployed only on OCS 2007 .....	132
OCS_AVEdgeServer_Logging Policy .....	132
OCS_AVEdgeServer_TCPPacketsDroppedPerSec Policy.....	133
OCS_AVEdgeServer_UDPActiveSessionsExceedingBandwidthLimit Policy .....	133
OCS_AVEdgeServer_UDPPacketsDroppedPerSec Policy .....	133
OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit Policy .....	134
Policies deployed only on OCS 2007 R2 .....	134
OCS_AVEdgeServer_Logging_R2 Policy.....	135
OCS_AVEdgeServer_TCPPacketsDroppedPerSec_R2 Policy .....	135
OCS_AVEdgeServer_UDPActiveSessionsExceedingBandwidthLimit_R2 Policy.....	136
OCS_AVEdgeServer_UDPPacketsDroppedPerSec_R2 Policy .....	136
OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit_R2 Policy .....	136
Configuration .....	137

CWAServer	137
OCS_CWAServer_AuthFailuresDueToLDAPErrors Policy	137
OCS_CWAServer_FailedRequests Policy	138
OCS_CWAServer_LogonsDeniedDueToServerThrottling Policy	138
OCS_CWAServer_RequestsRejectedPerSecDueToInvalidTicket Policy	139
OCS_CWAServer_RequestsToNonExistentSessions Policy	139
OCS_CWAServer_SessionsFailedToSignIn Policy	139
OCS_CWAServer_SessionsTimedOut Policy	140
OCS_CWAServer_FormsLogonFailures Policy	140
OCS_CWAServer_IWALogonFailures Policy	141
OCS_CWAServer_LDAPErrors Policy	141
FrontEnd Server	141
Policies deployed on OCS 2007 and OCS 2007 R2	142
OCS_Check_FrontEndServiceStatus Policy	142
OCS_FrontEndService_Logging Policy	142
OCS_FrontEndService_PageFaultsPerSec Policy	143
OCS_FrontEndService_PrivateBytes Policy	143
OCS_FrontEndService_ProcessorTime Policy	143
OCS_FrontEndService_ThreadCount Policy	144
OCS_FrontEndService_WorkingSet Policy	144
OCS_FrontEndServer_SendsOutstandingPolicy	145
OCS_FrontEndServer_HoldingTimeForIncMsgs Policy	145
OCS_FrontEndServer_ProcessingLatency Policy	145
OCS_FrontEndServer_QueueLatency Policy	146
Policies deployed on OCS 2007	146
OCS_FrontEndServer_Local503Responses Policy	146
OCS_FrontEndServer_Logging Policy	147
OCS_FrontEndServer_Local504Responses Policy	147
Policies deployed on OCS 2007 R2	148
OCS_FrontEndServer_Local503Responses_R2 Policy	148
OCS_FrontEndServer_Logging_R2 Policy	148
OCS_FrontEndServer_Local504Responses_R2 Policy	149
IMConfServer	149
OCS_Check_IMConfServiceStatus Policy	150
OCS_IMConfService_PageFaultsPerSec Policy	150
OCS_IMConfService_PrivateBytes Policy	150
OCS_IMConfService_ProcessorTime Policy	151
OCS_IMConfService_ThreadCount Policy	151
OCS_IMConfService_WorkingSet Policy	151
OCS_IMConfService_Logging Policy	152
Mediation Server	152
OCS_MediationService_PageFaultsPerSec Policy	153
OCS_Check_MediationServiceStatus Policy	153
OCS_MediationService_Logging Policy	153
OCS_MediationService_PrivateBytes Policy	154
OCS_MediationService_ProcessorTime Policy	154
OCS_MediationService_ThreadCount Policy	155

OCS_MediationService_WorkingSet Policy . . . . .	155
OCS_MediationServer_LoadCallFailureIndex Policy . . . . .	156
OCS_MediationServer_RejectedSIPInvitesFromGateway Policy . . . . .	156
OCS_MediationServer_RejectedSIPInvitesFromProxy Policy . . . . .	156
TelConfServer . . . . .	157
OCS_Check_TelConfServiceStatus Policy . . . . .	157
OCS_TelConfService_Logging Policy . . . . .	157
OCS_TelConfService_PageFaultsPerSec Policy . . . . .	158
OCS_TelConfService_PrivateBytes Policy . . . . .	159
OCS_TelConfService_ProcessorTime Policy . . . . .	159
OCS_TelConfService_ThreadCount Policy . . . . .	159
OCS_TelConfService_WorkingSet Policy . . . . .	160
WebCompServer . . . . .	160
Deploy the following policies on OCS 2007 . . . . .	160
OCS_WebCompServer_InvalidInputRequestsPerSec Policy . . . . .	161
OCS_WebCompServer_TimedOutSecurityDescRequestsPerSec Policy . . . . .	161
Deploy the following policies on OCS_R2 . . . . .	161
OCS_WebCompServer_InvalidInputRequestsPerSec_R2 Policy . . . . .	161
OCS_WebCompServer_TimedOutSecurityDescRequestsPerSec_R2 Policy . . . . .	162
WebConfServer . . . . .	162
OCS_Check_WebConfServiceStatus Policy . . . . .	163
OCS_WebConfServer_ComplianceErrors Policy . . . . .	163
OCS_WebConfServer_MCUHealthState Policy . . . . .	163
OCS_WebConfServer_NumberOfUnhandledApplExceptions Policy . . . . .	164
OCS_WebConfServer_ResourcesOverConfSpaceLimit Policy . . . . .	164
OCS_WebConfServer_SessionQueuesState Policy . . . . .	164
OCS_WebConfService_Logging Policy . . . . .	165
OCS_WebConfService_PrivateBytes Policy . . . . .	165
OCS_WebConfService_ProcessorTime Policy . . . . .	166
OCS_WebConfService_ThreadCount Policy . . . . .	166
OCS_WebConfService_WorkingSet Policy . . . . .	167
OCS_WebConfService_PageFaultsPerSec Policy . . . . .	167
WebEdgeServer . . . . .	167
OCS_Check_WebEdgeServiceStatus Policy . . . . .	168
OCS_WebEdgeService_PageFaultsPerSec Policy . . . . .	168
OCS_WebEdgeService_PrivateBytes Policy . . . . .	168
OCS_WebEdgeService_ProcessorTime Policy . . . . .	169
OCS_WebEdgeService_ThreadCount Policy . . . . .	169
OCS_WebEdgeService_WorkingSet Policy . . . . .	170
OCS_WebEdgeService_Logging Policy . . . . .	170
OCS_WebEdgeServer_ClientsDisconPerSecInvalidCookieData Policy . . . . .	171
OCS_WebEdgeServer_ClientsDisconPerSecInvalidCookieTimestamp Policy . . . . .	171
OCS_WebEdgeServer_SystemThrottling Policy . . . . .	171
OCS_WebEdgeServer_ThrottledServerConnections Policy . . . . .	172
Others . . . . .	172
OCS_FwdApplicationError Policy . . . . .	172
OCS_FwdApplicationInformation . . . . .	173

OCS_FwdApplicationWarning . . . . .	174
Microsoft Enterprise Servers SPI Microsoft Office Communications Server 2007 Reports . . . . .	176
Front End Service CPU Statistics . . . . .	176
IM Conferencing Service CPU Statistics . . . . .	176
Access Edge Service CPU Statistics . . . . .	176
Front End Service Memory Statistics. . . . .	176
IM Conferencing Service Memory Statistics . . . . .	176
Access Edge Service Memory Statistics . . . . .	176
SQL Back End Latency Experienced By Front End Server . . . . .	177
Average Holding Time for Incoming Messages on Front End Server. . . . .	177
Front End Server Availability and Connectivity . . . . .	177
Sends Outstanding on Front End Server . . . . .	177
Average Incoming Message Processing Time on Access Edge Server . . . . .	177
Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server . . . . .	177
Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server . . . . .	177
Data Store Table for Microsoft Enterprise Server . . . . .	178
Microsoft Enterprise Servers SPI Microsoft Office Communications Server 2007 Graphs. . . . .	179
Front End Service CPU statistics. . . . .	180
Web Conferencing Service CPU statistics . . . . .	180
IM Conferencing Service CPU statistics . . . . .	180
Telephony Conferencing Service CPU statistics . . . . .	180
Audio/Video Conferencing Service CPU statistics . . . . .	180
Access Edge Service CPU statistics . . . . .	181
Audio/Video Edge Service CPU statistics. . . . .	181
Audio/Video Authentication Service CPU statistics . . . . .	181
Web Conferencing Edge Service CPU statistics. . . . .	181
Archiving and CDR Service CPU statistics . . . . .	181
Mediation Service CPU statistics . . . . .	182
Front End Service Memory Statistics. . . . .	182
Web Conferencing Service Memory Statistics . . . . .	182
IM Conferencing Service Memory Statistics . . . . .	182
Telephony Conferencing Service Memory Statistics . . . . .	182
Audio/Video Conferencing Service Memory Statistics. . . . .	182
Access Edge Service Memory Statistics . . . . .	183
Audio/Video Edge Service Memory Statistics . . . . .	183
Audio/Video Authentication Service Memory Statistics . . . . .	183
Web Conferencing Edge Service Memory Statistics . . . . .	183
Archiving and CDR Service Memory Statistics . . . . .	183
Mediation Service Memory Statistics. . . . .	183
Authentication failures/sec on Audio/Video Edge Server . . . . .	184
SQL Back End Latency Experienced By Front End Server . . . . .	184
Average Holding Time for Incoming Messages on Front End Server. . . . .	184
Front End Server Availability and Connectivity . . . . .	184
Sends Outstanding on Front End Server . . . . .	184
Average Incoming Message Processing Time on Access Edge Server . . . . .	184
Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server . . . . .	185
Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server . . . . .	185

Data Store Table for Microsoft Enterprise Server . . . . .	185
<b>8 Microsoft Enterprise Servers SPI for Microsoft Lync Server 2010 . . . . .</b>	<b>189</b>
Policies . . . . .	189
Archiving Server . . . . .	189
General Policies . . . . .	190
GoldenMetrics . . . . .	197
AVConfServer . . . . .	198
General Policies . . . . .	198
GoldenMetrics . . . . .	205
Common. . . . .	205
Director Server . . . . .	206
General Policies . . . . .	206
GoldenMetrics . . . . .	212
Discovery . . . . .	214
Configuring LS_Discovery Policy. . . . .	215
Edge Server . . . . .	216
General Policies . . . . .	216
GoldenMetrics . . . . .	244
Front End Server . . . . .	249
General Policies . . . . .	249
GoldenMetrics . . . . .	276
Mediation Server . . . . .	283
General Policies . . . . .	283
GoldenMetrics . . . . .	290
Monitoring Server. . . . .	291
General Policies . . . . .	291
GoldenMetrics . . . . .	304
Registrar . . . . .	308
General Policies . . . . .	308
GoldenMetrics . . . . .	313
Reports . . . . .	317
LS2K10 Front End Service CPU Stat . . . . .	317
LS2K10 IM Conferencing Service CPU Stat . . . . .	317
LS2K10 Access Edge Service CPU Stat . . . . .	317
LS2K10 Front End Service Memory Stat. . . . .	317
LS2K10 IM Conferencing Service Memory Stat . . . . .	317
LS2K10 Access Edge Service Memory Stat . . . . .	317
LS2K10 SQL Back End Lat Exp by Front End Server . . . . .	317
LS2K10 Avg Hold Time for In Msg Front End Server . . . . .	318
LS2K10 Front End Server Avail and Conn . . . . .	318
LS2K10 Sends Outstanding on Front End Server. . . . .	318
LS2K10 Avg Inc Msg Proc Time Access Edge Server . . . . .	318
LS2K10 Client Request Err UDP AV Edge Server . . . . .	318
LS2K10 Client Request Err TCP AV Edge Server. . . . .	318
Graphs . . . . .	318
Front End Service CPU statistics. . . . .	319
Web Conferencing Service CPU statistics . . . . .	319

IM Conferencing Service CPU statistics . . . . .	319
Audio/Video Conferencing Service CPU statistics . . . . .	319
Access Edge Service CPU statistics . . . . .	319
Audio/Video Edge Service CPU statistics. . . . .	320
Audio/Video Authentication Service CPU statistics . . . . .	320
Web Conferencing Edge Service CPU statistics. . . . .	320
Archiving and CDR Service CPU statistics . . . . .	320
Mediation Service CPU statistics . . . . .	320
Front End Service Memory Statistics. . . . .	321
Web Conferencing Service Memory Statistics . . . . .	321
IM Conferencing Service Memory Statistics . . . . .	321
Audio/Video Conferencing Service Memory Statistics. . . . .	321
Access Edge Service Memory Statistics . . . . .	321
Audio/Video Edge Service Memory Statistics . . . . .	321
Audio/Video Authentication Service Memory Statistics . . . . .	322
Web Conferencing Edge Service Memory Statistics . . . . .	322
Archiving and CDR Service Memory Statistics . . . . .	322
Mediation Service Memory Statistics. . . . .	322
Authentication failures/sec on Audio/Video Edge Server . . . . .	322
SQL Back End Latency Experienced By Front End Server . . . . .	322
Average Holding Time for Incoming Messages on Front End Server. . . . .	323
Front End Server Availability and Connectivity . . . . .	323
Sends Outstanding on Front End Server. . . . .	323
Average Incoming Message Processing Time on Access Edge Server . . . . .	323
Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server . . . . .	323
Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server . . . . .	324
<b>9 Microsoft Enterprise Servers SPI Tools . . . . .</b>	<b>325</b>
MSES_BTS_DB_Configuration . . . . .	325
Create Datasource for ISA Server . . . . .	326
Create Datasource for BizTalk Server . . . . .	326
BTS 2010 Create Datasource . . . . .	326
Self-Healing Info . . . . .	326
Self-Healing Verification . . . . .	326
Create Datasource for SharePoint Server . . . . .	326
Create Datasource for Lync Server 2010 . . . . .	326
Configure Edge server Discovery for Lync Server 2010 . . . . .	326
BTS 2010 Cluster Config. . . . .	327
BTS 2010 Enable Trace. . . . .	327
<b>Index . . . . .</b>	<b>329</b>





# 1 Introduction

The HP Operations Smart Plug-in for Microsoft Enterprise Servers (Microsoft Enterprise Servers SPI) helps you to manage the Microsoft Enterprise Servers in your environment. The Microsoft Enterprise Servers SPI provides information about the following Microsoft Enterprise Servers:

- BizTalk Server 2006 and R2
- BizTalk Server 2010
- Internet Security and Acceleration Server 2006
- Microsoft Office SharePoint Server 2007
- Microsoft SharePoint Server 2010
- Microsoft Office Communications Server 2007 and R2
- Microsoft Lync Server 2010

Microsoft Enterprise Servers SPI for Microsoft Office Communications Server 2007 supports the following deployment configurations:

- Microsoft Office Communication Server Standard Edition
- Microsoft Office Communications Server Enterprise Edition Consolidated Configuration
- Microsoft Office Communications Server Enterprise Edition Expanded Configuration

The Microsoft Enterprise Servers SPI for Microsoft Office Communications Server does not support the following deployment configurations:

- Microsoft Office Communications Server 2007 configured with load balancing
- Microsoft Office Communications Server 2007 installed on clustered environment

The Microsoft Enterprise Servers SPI provides the following services:

- **Topology/Service Mapping:** Discovers and maps Microsoft Enterprise Servers in your network. The service map displays the servers and shows the dependencies to other systems.
- **Availability Monitoring:** Monitors the services that need to run to ensure complete availability of your Microsoft Enterprise Servers.
- **Performance Monitoring:** Monitors Windows performance counters and notifies you if thresholds exceed.
- **Event Log Monitoring:** Monitors the Windows Event Logs.
- **Reporting and Graphing:** Creates reports and graphs that show historical data and trend information based on the data logged. This can be used for capacity planning and SLA compliance.
- **Troubleshooting assistance** with the Self Healing Info tool.

# Components of Microsoft Enterprise Server SPI

The components of Microsoft Enterprise Server SPI are as follows:

## Policies

Policies are pre-defined thresholds which constantly monitor the Microsoft Enterprise Servers in the environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts appear in the service map and messages are available in the message browser. A color code indicates the severity level of each message—minor, major, or critical. The messages indicate the problem and help you to take preventive action.

## Tools

Tools are the utilities to configure and gather Microsoft Enterprise Server related information. Self Healing tools are used to troubleshoot any of the Microsoft Enterprise Servers. The *MSES\_BTS\_DB\_Configuration* and *Create Datasource for BizTalk Server* tools are used to configure the BizTalk Server. The *Create Datasource for ISA Server tool* is used to create data sources for the ISA Server of the Microsoft Enterprise Servers SPI.

## Reports

Reports represent various metrics of Microsoft Enterprise Servers. Data collected by the Microsoft Enterprise Servers SPI are used to generate reports.

## Graphs

Graphs are pictorial representations of various metrics of the Microsoft Enterprise Servers. Graphs contain the data collected by Microsoft Enterprise Servers SPI.

Reports and graphs are generated using HP Reporter and HP Performance Manager. The graphs and reports provide you an overview to determine corrective actions to be taken for problems.

## 2 Microsoft Enterprise Servers SPI for BizTalk Server 2006

Microsoft BizTalk Server provides distributed application integration services using XML as the primary messaging format. The external formats are converted to the BizTalk standards using parsers and BizTalk mapping services. Parsers and BizTalk mapping services are components of BizTalk Messaging Services.

The Biztalk Orchestration Designer defines the process that a document undergoes. In BizTalk messaging, channels convert the external formats and ports transmit the documents. The channels and ports can be configured to receive and transmit documents in a variety of formats and protocols, such as HTTP, HTTPS, SMTP, and COM. In Orchestration services, ports represent the input and output of a process. The action is defined in the XLANG schedule.

The Microsoft Enterprise Servers SPI monitors the performance of BizTalk Server 2006 with policies, tools, graphs, and reports.

You can use the MSES\_BTS\_DB\_Configuration tool to configure the Microsoft Enterprise Servers SPI for BizTalk Server 2006. For more information, see Additional Configuration Procedure for Microsoft Enterprise Servers SPI for BizTalk Server 2006 section of *HP Operations Smart Plug-in for Microsoft Enterprise Servers SPI Installation and Configuration Guide*.

### Policies

The Microsoft Enterprise Servers SPI BizTalk Server policies monitor the Microsoft BizTalk Server 2006. The policies offer the following monitoring processes:

- Availability Monitoring
- Performance Monitoring
- Windows Event Log Monitoring
- Database Connectivity
- Server Logging
- Discovery

### Availability Monitoring

The Availability Monitoring group monitors services of the Microsoft BizTalk Server. If any of the services is not running and service startup is set to Operator-initiated action, you can start the service from the operator interface. The policy also sends a console error message to indicate that the service is not running.

Monitored services of BizTalk Server include:

- BizTalk Server Application Service
- BizTalk RuleEngineUpdate Service

- Enterprise Single Sign-On

The Availability Monitoring group includes the EBIZ\_BizTalkServerServices policy.

#### EBIZ\_BizTalkServerServices policy

The EBIZ\_BizTalkServerServices policy monitors the following BizTalk Server 2006 services:

- BizTalk Server Application Service
- BizTalk RuleEngineUpdate Service
- Enterprise Single Sign-On

The following table lists the details of the EBIZ\_BizTalkServerServices policy.

Schedule	Policy Type	Policy Group
Runs every 5 minutes	Windows Management Interface policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy

## Performance Monitoring

BizTalk Server Performance Monitoring includes specific BizTalk Server performance counters and CPU process-related counters. Each policy for performance monitoring has error and warning thresholds. The Performance Monitoring policies monitor the CPU and Memory usage.

The Performance Monitoring policies are available at the following location:

**SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy**

The following table lists the policies in the Performance Monitoring group.

Policy	Description	Policy Type
EBIZ_BS-MEMUsage-BTSSvc	Measures memory usage of the Microsoft BizTalk Server Application services.	Measurement Threshold policy
EBIZ_BS-CPUUsage-BTSSvc	Measures CPU usage of the Microsoft BizTalk Server Application services.	
EBIZ_BS-MEMUsage-ENTSSO	Measures memory usage of Enterprise Single Sign-On service.	
EBIZ_BS-CPUUsage-ENTSSO	Measures CPU usage of the Enterprise Single Sign-On service.	
MSES_SendPort_Status_Monitoring	Monitors status of the SendPorts in the Microsoft BizTalk Server.	Scheduled Task policy
MSES_ReceiveLocation_Status_Monitoring	Monitors status of the ReceiveLocations of BizTalk Server.	Windows Management Interface policy
MSES_BS_DocsProcessed	Monitors the average number of documents pulled from the Work queue and sent to a port destination address per second, since the last time the BizTalk Messaging Service started.	Measurement Threshold policy

<b>Policy</b>	<b>Description</b>	<b>Policy Type</b>
MSES_BS_DocReceived	Monitors the average number of documents received per second by BizTalk Server. This includes all documents that go into the Work queue and those failed.	Measurement Threshold policy
MSES_BS_DocsSuspended	Monitors the average number of documents suspended per second in the suspended queue.	
MSES_BS_DBTransactions	Monitors the average number of database transactions performed per second since the host instance started.	
MSES_BS_ActiveAppDomains	Monitors the number of application domains currently existing for hosting orchestrations.	
MSES_BS_DehydrationThreshold	Monitors the time (in milliseconds), which determines how aggressively orchestrations are dehydrated. If the orchestration engine predicts that an instance is dehydratable (storing all the instance-specific data in the database and removing the instance from the memory), for a time period longer than the threshold value, it dehydrates the instance.	
MSES_BS_IdleOrchestrations	Monitors the number of idle orchestration instances currently hosted by the host instance. This refers to orchestrations that are not making progress but are also not dehydratable, as when the orchestration is blocked waiting for a receive, listen, or delay in an atomic transaction.	
MSES_BS_OrchestrationsCompleted	Monitors the average number of orchestration instances completed per second since the host instance started.	
MSES_BS_OrchestrationsCreated	Monitors the average number of orchestration instances per second created since the host instance started.	
MSES_BS_OrchestrationsDehydrated	Monitors the average number of orchestration instances dehydrated per second since the host instance started.	
MSES_BS_OrchestrationsDiscarded	Monitors the average number of orchestration instances discarded per second from memory since the host instance started. An orchestration can be discarded if the engine fails to persist its state.	
MSES_BS_OrchestrationsRehydrated	Monitors the average number of orchestration instances rehydrated per second (restoring the instance from the database to memory) since the host instance started.	
MSES_BS_OrchestrationsResidentInMemory	Monitors the number of orchestration instances currently hosted by the host instance.	
MSES_BS_OrchestrationsScheduledForDehydration	Monitors the number of dehydratable orchestrations having a dehydration request pending.	
MSES_BS_OrchestrationsSuspended	Monitors the average number of orchestration instances suspended per second since the host instance started.	
MSES_BS_RunningOrchestrations	Monitors the number of orchestration instances running currently.	

Policy	Description	Policy Type
MSES_Orchestration_Status_Monitoring	Monitors the status of the orchestrations.	Windows Management Interface policy
MSES_BS_PendingMessages	Monitors the number of received messages for which receipt is not yet acknowledged to the message box.	Measurement Threshold policy
MSES_BS_PendingWorkItems	Monitors the number of code execution blocks that are scheduled for execution.	Measurement Threshold policy
MSES_BS_TransactionalScopesAborted	Monitors the number of long-running or atomic scopes that were aborted since the host instance started.	Measurement Threshold policy

## Windows Event Log Monitoring

The Windows Event Log policies send alert messages to the HPOM console when errors, warnings, and entries from BizTalk Server sources are logged.

Policies monitoring events are grouped as follows:

- BizTalk Server
- XLANG Scheduler

The Windows Event Log group includes EBIZ\_BizTalkServerFwdApplicationLogEntries policy. The EBIZ\_BizTalkServerFwdApplicationLogEntries policy forwards all BizTalk Server 2006 application log entries with severity levels as follows:

- Error
- Warning

The following table lists the policies in the Windows Event Log Monitoring group.

Policy	Policy Type	Policy Group
EBIZ_BizTalkServerFwdApplicationLogEntries	Windows Event Log policy	SPI for Microsoft Enterprise Servers →en → BizTalk Server →Biztalk Server 2006→ Manual-Deploy

## Database Connectivity

The Database Connectivity attempts to connect if the databases fails. This monitoring group includes the following policies:

- MSES\_BS\_DBMonitor
- MSES\_BS\_MsgBox DBConnectionFailures
- MSES\_BizTalk\_MessageBox\_DatabaseSize
- MSES\_BizTalk\_DTA\_DatabaseSize



Before installing the MSES\_BizTalk\_DTA\_DatabaseSize and MSES\_BizTalk\_MessageBox\_DatabaseSize policies, ensure that the `SQLDMO.dll` is registered on the node. Otherwise the policy does not work properly.

## MSES\_BS\_DBMonitor

The MSES\_BS\_DBMonitor policy sends a message to the HPOM message browser if any of the following databases fail to connect. An OPC message is sent to refresh the service map with this information. The policy monitors the connections to the following BizTalk 2006 databases:

- BAMPrimaryImport - Business Activity Monitoring DB
- BAM Analysis - Business Activity Monitoring OLAP Cubes DB
- BAMStarSchema - Business Activity Monitoring DB
- BAMArchive - Archives Business Activity Monitoring DB
- BizTalkDTADb - Tracking DB
- BizTalkMgmtDB BTS - Configuration Information DB
- BizTalkMsgBoxDb - DB for storing Messages and subscriptions
- BizTalkRuleEngineDb - DB for storing Policies and Vocabularies
- SSODB - Single Sign-On DB
- BizTalkAnalysisdb - DB for storing business and health monitoring OLAP Cubes

The following table lists the details of the policies in the Database Connectivity monitoring group.

Policy	Description	Policy Type	Policy Group
MSES_BS_DBMonitor	Sends a message to the HPOM message browser if any of the following databases fail to connect.	Scheduled Task policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Auto-Deploy
MSES_BS_MsgBoxDBConnectionFailures	Monitors the number of attempted database connections that failed since the host instance started.	Measurement Threshold policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy
MSES_BizTalk_MessageBox_DatabaseSize	Monitors the percentage usage of the BizTalk MessageBox database.  Deploy this policy only on BizTalk MessageBox database nodes.	Measurement Threshold policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy
MSES_BizTalk_DTA_DatabaseSize	Monitors the the percentage usage of the BizTalk DTA database.  Deploy this policy only on BizTalk DTA database nodes.	Measurement Threshold policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy

## Server Logging

The Server Logging monitoring group collects selected performance and process-related data for CPU and memory counters. This monitoring group includes the following policies:

- MSES\_BizTalkServer\_SusDoc\_Logging

- MSES\_BizTalk\_IntervalCount\_Logging
- MSES\_BizTalkServer\_TDDS\_Logging
- MSES\_BTS\_Logging\_ApplicationService
- MSES\_BTS\_Logging\_ENTSSO
- MSES\_BTS\_Logging\_BaseEDI
- MSES\_BTS\_Logging\_RuleUpdateEngine



You must run the Create Datasource for BizTalk Server tool before deploying the other policies to create the datasource.

The following table lists the policies in the Server Logging group.

Policy	Description	Policy Type	Policy Group
MSES_BizTalkServer_SusDoc_Logging	Collects suspended document's data from the BizTalk Server database and logs it into the data source.	Scheduled Task policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Auto-Deploy
MSES_BizTalk_IntervalCount_Logging	Collects performance data for the following three BizTalk 2006 objects: <ul style="list-style-type: none"> <li>• BizTalk Messaging</li> <li>• Enterprise Single Sign On</li> <li>• XLANG/s Orchestrations</li> </ul>	Measurement Threshold policy	SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Auto-Deploy
MSES_BizTalkServer_TDDS_Logging	Collects the performance data for BizTalk TDDS (Tracking Data Decode Service), and logs it into the data source.		SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Auto-Deploy
MSES_BTS_Logging_ApplicationService	Logs the performance data for BizTalk Server 2006 Application Service.		SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy
MSES_BTS_Logging_ENTSSO	Logs the performance data for BizTalk Server 2006 ENTSSO.		SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy
MSES_BTS_Logging_BaseEDI	Logs the performance data for BizTalk Server 2006 Base EDI Service.		SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy
MSES_BTS_Logging_RuleUpdateEngine	Logs the performance data for BizTalk Server 2006 Rule Engine Update Service.		SPI for Microsoft Enterprise Servers → en → BizTalk Server → Biztalk Server 2006 → Manual-Deploy



## Discovery

The Discovery monitoring group discovers the services of the Microsoft BizTalk Server 2006. This monitoring group includes the BizTalk\_Discovery policy.



Run the MSES\_BS\_DB\_Configuration tool before deploying the BizTalk Discovery policy.

The following table lists the policies in Discovery group.

Policy	Description	Policy Type	Policy Group
BizTalk_Discovery	Discovers the BizTalk infrastructure information and adds it to the service map.	Service Auto-Discovery policy	SPI for Microsoft Enterprise Servers→ en→ BizTalk Server→ Biztalk Server 2006→ Discovery

## Reports

The Microsoft Enterprise Servers SPI offers the following reports for Microsoft Enterprise Servers (BizTalk Server 2006) SPI.

### BTS Document Process Rate (Monthly/Weekly)

The BTS Document Process Rate Monthly and Weekly reports provide summary of the following monthly and weekly statistics related to the BizTalk Documents:

- **Documents processed/sec** : Integer representing the average number of documents processed per second. The processed documents are those documents pulled from the Work queue and sent to a port destination address.
- **Documents received/sec** : Integer representing the average number of documents that are received by BizTalk Server per second. This includes all documents that go into the Work queue and those that failed.
- **Documents suspended/sec** : Integer representing the average number of items suspended in the Suspended queue per second.

### BTS Processes CPU Statistics

The BTS Process CPU Statistics report shows a summary of CPU statistics of BizTalk Server processes, compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics include the percentage of CPU time used by BizTalk Server Application Service, Enterprise SSO (Single Sign On) Service, Rule Engine Update Service and BizTalk Base EDI Service processes compared with the percentage of time the system CPU was busy.

This report has the following counters:

- Process. % Processor Time (BTSNTSvc, ENTSSO, RuleEngineUpdateService, esp\_srv)
- Process.Thread Count (BTSNTSvc, ENTSSO, RuleEngineUpdateService, esp\_srv)

## BTS Processes Memory Statistics

The BTS Processes Memory Statistics report shows summary of memory statistics of BizTalk Server processes in graphical and tabular formats. The summarized process statistics include the page faults per second, private bytes, and working set used by BizTalk Server Application Service, Enterprise SSO (Single Sign On) Service, Rule Engine Update Service and BizTalk Base EDI Service processes.

This report has the following counters:

- Process.Private Bytes (BTSNTSvc, ENTSSO, RuleEngineUpdateService, esp\_srv)
- Process.Working Set (BTSNTSvc, ENTSSO, RuleEngineUpdateService, esp\_srv)
- Process.Page Faults/sec (BTSNTSvc, ENTSSO, RuleEngineUpdateService, esp\_srv)

## BTS Orchestration Statistics (Monthly/Weekly)

The BTS Orchestration Statistics Monthly and Weekly reports provide the monthly and weekly summary of the following orchestrations statistics:

- **Orchestrations completed/sec** : Average number of orchestrations completed per second.
- **Orchestrations created/sec** : Average number of orchestrations created per second.
- **Orchestrations dehydrated/sec** : Average number of orchestrations dehydrated per second.
- **Orchestrations discarded/sec** : Average number of orchestrations discarded per second.
- **Orchestrations rehydrated/sec** : Average number of orchestrations rehydrated per second.
- **Orchestrations suspended/sec** : Average number of orchestrations suspended per second.
- **Database transactions/sec** : Average number of database transactions per second.

## BTS Transactional Rate (Monthly/Weekly)

The BTS Transactional Rate Monthly and Weekly reports provide the monthly and weekly summary of the statistics related to transactions.



A scope is a framework for grouping actions, primarily used for transactional execution and exception handling. Compensation is a process where a piece of code gets executed to undo or reverse the effects of a successfully committed transaction.

- **Transactional scopes aborted/sec** : Average number of long-running or atomic scopes aborted.
- **Transactional scopes committed/sec** : Average number of long-running or atomic scopes completed successfully.
- **Transactional scopes compensated/sec** : Average number of long-running or atomic scopes that completed compensation scopes successfully.

## BTS Suspended Documents Report (Monthly/Weekly)

The BTS Suspended Documents Report Monthly and Weekly reports provide the monthly and weekly suspended document statistics, segregated by the following attributes:

- **State:** Documents that are in resumable and non-resumable states
- **Server Name:** Processing server name
- **Priority:** Document Priority

## BTS TDDS Statistics

TDDS is also known as the BAM Event Bus Service. The BTS TDDS Statistics report provides the monthly summary of the following TDDS related statistics:

- **Events being processed:** Number of events the BAM Event Bus Service is processing.
- **Batches being processed:** Number of batches the BAM Event Bus Service is processing.
- **Events Committed:** Number of events the BAM Event Bus Service committed to SQL Server in the last second.
- **Records Committed:** Number of records the BAM Event Bus Service committed to SQL Server in the last second.
- **Batches Committed:** Number of batches the BAM Event Bus Service committed to SQL Server in the last second.

## BTS Enterprise Single Sign-on(Monthly)

The BTS Enterprise Single Sign-on(Monthly) report provide the monthly summary of the following enterprise SSO related statistics:

- **GetConfigInfo/sec:** Total number of config info accessed.
- **IssueTicket/sec:** Total number of tickets issued.
- **GetCredentials/sec:** Total number of credentials accessed.
- **RedeemTicket/sec:** Total number of tickets redeemed.
- **ValidateAndRedeemTicket/sec:** Total number of tickets validated and redeemed.

## Graphs

The Microsoft Enterprise Servers SPI offers the following pre-defined graphs for BizTalk Server:

- BizTalk Server Application Service CPU
- Enterprise Single Sign-On Service CPU
- Rule Engine Update Service CPU

These graphs represent the percentage of time spent by the processors executing threads for the BizTalk Server Application Service, Enterprise Single Sign-On Service, and Rule Engine Update Service processes. This counter can be compared to System Processor Time to determine the extent to which these processes are utilizing processor time.

- BizTalk Server Application Service Memory
- Enterprise Single Sign-On Service Memory

- Rule Engine Update Service Memory

#### Page Faults/sec

Page Faults/sec represents the rate of page faults occurring in the threads executing the BizTalk Server Application Service, Enterprise Single Sign-On Service, and Rule Engine Update process.

A page fault occurs when a thread refers to a virtual memory page not in its working set in main memory. The graph shows the average rate at which page faults occur, by the threads executing in these processes.

#### Working Set

Working Set represents number of bytes in the working set of the BizTalk Server Application Service, Enterprise Single Sign-On Service, and Rule Engine Update Service process. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a certain threshold, pages are left in the working set of a process even if they are not in use. When free memory falls below a certain threshold, pages are trimmed from working sets. If they are needed, they are then soft-faulted back into the working set before they leave main memory.

#### Private Bytes

Private Bytes is the current number of bytes the BizTalk Server Application Service, Enterprise Single Sign-On Service, and Rule Engine Update process have allocated that cannot be shared with other processes.

# 3 Microsoft Enterprise Servers SPI for BizTalk Server 2010

## Overview

Microsoft BizTalk Server 2010 provides distributed application integration services using XML as its primary messaging format. External formats are converted to the BizTalk standards through parsers and Biztalk mapping services, which are components of BizTalk Messaging Services. The BizTalk Orchestration Designer defines the process that a document undergoes. In BizTalk messaging, channels handle the conversion of external formats, and ports are responsible for transmitting documents. The channels and ports in BizTalk Messaging can be configured to receive and transmit documents in a variety of formats and protocols, such as HTTP, HTTPS, SMTP, COM. In Orchestration services, the ports represent the input and output of a process. The action is defined in the XLANG schedule.

The Microsoft Enterprise Servers SPI monitors the availability and performance of BizTalk Server 2010 using policies, tools, graphs, and reports.

The Microsoft Enterprise Servers BizTalk Server SPI requires additional configuration. You can use the MSES\_BTS\_DB\_Configuration tool to configure the Microsoft Enterprise Servers SPI for BizTalk Server 2010. For more information, see the *HP Operations Smart Plug-in for Microsoft Enterprise Servers SPI Installation and Configuration Guide*.

## Policies

The Microsoft Enterprise Servers SPI BizTalk Server 2010 policies monitor the services, availability, and performance of Microsoft BizTalk Server 2010. It comprises of the following policy groups:

- Availability
- Discovery
- Document Processing
- File Receive Adapter
- Message Box
- Messaging
- Orchestration Engine
- Performance
- Sharepoint Adapter
- Tracking Data Decode Services (TDDS)

## SPI Metrics and Collections

The metrics assess the availability and performance of BizTalk Server 2010. The main source of these metrics are performance counters. Each metric is assigned a unique Metric ID. The Microsoft Enterprise Servers SPI monitors these metrics and sends alerts if the metric value exceeds the specified threshold. For monitoring a particular Metric ID, a set of three policies are used:

- `BTS_<METRIC_ID>` - This measurement threshold policy generates alerts when the collected value exceeds the threshold.
- `BTS_SCH_<METRIC_ID>` - This schedule task policy specifies the schedule for the `BTS_<METRIC_ID>` policy.
- `BTS_CFG_<METRIC_ID>` - This is a config file policy which contains the thresholds for the `BTS_<METRIC_ID>` policy.

A collection is group of metrics from the same source. These collections are logged into an appropriate data store. Each Collection is associated with a collection ID. For collecting and logging a `<COLLECTION_ID>` the following policy is used:

`BTS_SCH_<COLLECTION_ID>` - This is a schedule task policy which identifies the schedule when the `<COLLECTION_ID>`; is to be collected and logged to the data store.



Metrics and Collections are defined in `BTS_MetricDef.xml`.

## Availability

The Availability policy group contains policies that monitor the status of BizTalk Server 2010 services. This policy group comprises of the following set of policies for monitoring and logging:

## Metrics Monitored

### Metric ID: 841402

Metric Name	ESSO_STAT
Description	This policy monitors the Enterprise Single Sign On Service.
Metric Definition	ServiceName:ENTSSO
Measurement Threshold Policy	BTS_841402
Config File Policy	BTS_CFG_841402
Scheduled Task Policy for Alerting	BTS_SCH_841402
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Availability

### Metric ID: 841403

Metric Name	BTSNT_STAT
Description	This policy monitors the status of all of the BizTalk application services.
Metric Definition	ServiceName:BTSSvc\$*
Measurement Threshold Policy	BTS_841403
Config File Policy	BTS_CFG_841403
Scheduled Task Policy for Alerting	BTS_SCH_841403
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Availability

### Metric ID: 841404

Metric Name	RULEENGINE_STAT
Description	This policy monitors the status of the Rule Engine Update Service.
Metric Definition	ServiceName:RuleEngineUpdateService
Measurement Threshold Policy	BTS_841404

Metric Name	RULEENGINE_STAT
Config File Policy	BTS_CFG_841404
Scheduled Task Policy for Alerting	BTS_SCH_841404
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Availability

## Metrics Logged

Collection ID: 840014

Collection Name	BTS_SERVSTAT
Description	This policy collects and logs the status of BizTalk services. The collected data is logged to class BTS_SERVSTAT.
Collection Definition	Performance Object: Biztalk:TDDS Service Name: ENTSSO Service Name: BTSSvc\$* Service Name: RuleEngineUpdateService Performance Instance: *
Scheduled Task Policy for Logging	BTS_SCH_840014
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Availability

## Event Log Policies

The availability policy group contains policies that monitor the BizTalk Events. This policy group comprises of the following monitoring process comprises of the following event log policies:

### [BTS\\_Fwd\\_Application\\_Errors](#)

This policy forwards all the BizTalk errors reported in the Windows event log.

### [BTS\\_Fwd\\_Application\\_Warning](#)

This policy forwards all the BizTalk warnings reported in the Windows event log.



## Discovery

The Discovery policy group contains policies which discover the BizTalk Server 2010 in the environment and updates the service map in the management console.

### BTS\_Discovery

The BTS\_Discovery policy discovers the BizTalk 2010 servers in the environment and displays it in the service map.

Policy Type	Service Auto-Discovery
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Discovery

### BTS\_Cluster\_Re\_Discovery

This policy updates the service map when a cluster failover occurs.

Policy Type	Windows Event Log
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Discovery

## Document Processing

The Document Processing policy group contains policies that collect and logs performance data related to BizTalk document processing. This policy group contains the following policies.

## Metrics Logged

Collection ID: 840012

Collection Name	BTS_DOCPROCRATE
Description	This metric collects and logs performance metrics related to Document Processing.
Collection Definition	Performance Object: Biztalk:Messaging Performance Counter: Documents processed Performance Counter: Documents processed/ sec Performance Counter: Documents received Performance Counter: Documents resubmitted PerformanceCounter: Documents received/ sec PerformanceCounter: Documents resubmitted Performance Counter: Documents suspended Performance Counter: Documents suspended/sec Performance Counter: Documents transmitted/Batch Performance Instance: *
Scheduled Task Policy for Logging	BTS_SCH_840012
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Document Processing

## File Receive Adapter

The File Receive Adapter policy group contains policies that collect and monitor the performance metrics of the File Receive Adapter. This policy group comprises of the following set of policies for monitoring and logging:

## Metrics Monitored

### Metric ID: 841502

Metric Name	BTS_RECDELRET
Description	Monitors the number of times the File Receive Adapter attempts to delete a file that is read.
Metric Definition	Performance Object: BizTalk: FILE Receive Adapter Performance Counter: Delete retries Performance Instance: *
Measurement Threshold Policy	BTS_841502
Config File Policy	BTS_CFG_841502
Scheduled Task Policy for Alerting	BTS_SCH_841502
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → File Receive Adapter

### Metric ID: 841503

Metric Name	BTS_RECLCKFAIL
Description	Monitors the number of times the File Receive Adapter failed to lock the file per second.
Metric Definition	Performance Object: BizTalk: FILE Receive Adapter Performance Counter: Lock failures/sec Performance Instance: *
Measurement Threshold Policy	BTS_841503
Config File Policy	BTS_CFG_841503
Scheduled Task Policy for Alerting	BTS_SCH_841503
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → FileReceive Adapter

## Metrics Logged

Collection ID: 840015

Collection Name	BTS_FILERECPERF
Description	This policy collects and logs performance metrics related to file receive adapter.
Collection Definition	Performance Object: BizTalk:FILE Receive Adapter Performance Counter: Delete retries Performance Counter: Lock failures/sec Performance Counter: Bytes received/sec Performance Counter: Messages received/sec Performance Counter: Time to build batch Performance Instance: *
Scheduled Task Policy for Logging	BTS_SCH_840015
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → FileReceiveAdapter

## Message Box

The Message Box policy group contains policies that collect and monitor the performance metrics of BizTalk Message Box. This policy group contains the following policies for monitoring and logging:

## Metrics Monitored

Metric ID: 841002

Metric Name	BTS_MSGSPOOLSIZE
Description	This policy monitors the Message Box Spool Size of a particular message box on the BizTalk Server. An increasing spool size indicates that the messages are being picked up at a slower rate and the throughput is down.
Metric Definition	Performance Object: BizTalk: Message Box: General Counters Performance Counter: Spool Size Performance Instance: *
Measurement Threshold Policy	BTS_841002
Config File Policy	BTS_CFG_841002
Scheduled Task Policy for Alerting	BTS_SCH_841002
Schedule	10 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Message Box

Metric ID: 845002

Metric Name	BTS_MSGSQUELEN
Description	This policy monitors the Host Queue length and checks the number of messages in the particular Host Queue. A build up in host queue length indicates that the orchestrations are not completing faster.
Metric Definition	Performance Object: BizTalk: Message Box: Host Counters Performance Counter: Host Queue - Length Performance Instance: *
Measurement Threshold Policy	BTS_845002
Config File Policy	BTS_CFG_845002

Metric Name	BTS_MSGSQULEN
Scheduled Task Policy for Alerting	BTS_SCH_845002
Schedule	10 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Message Box

Metric ID: 845005

Metric Name	BTS_MSGSUSQLEN
Description	This policy monitors the message box suspended messages length. An increase in message suspension indicates that there are problems in message processing.
Metric Definition	Performance Object: BizTalk: Message Box: Host Counters Performance Counter: Host Queue - Suspended Msgs - Length Performance Instance: *
Measurement Threshold Policy	BTS_845005
Config File Policy	BTS_CFG_845005
Scheduled Task Policy for Alerting	BTS_SCH_845005
Schedule	10 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Message Box

## Metrics Logged

### Collection ID: 840001

Collection Name	BTS_MBSTATGEN
Description	This policy collects and logs Generic Metrics related to Message Box.
Collection Definition	Performance Object: BizTalk: Message Box: General Counters Performance Counter: Spool Size Performance Counter: Tracking Data Size Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840001
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Message Box

### Collection ID: 840005

Collection Name	BTS_MBSTATHOST
Description	This policy collects and logs Host Metrics related to Message Box.
Collection Definition	Performance Object: BizTalk: Message Box: Host Counters Performance Counter: Host Queue - Length Performance Counter: Host Queue - Number of Instances Performance Counter: Host Queue - Instance State Msg Refs - Length Performance Counter: Host Queue - Suspended Msgs - Length Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840005
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Message Box

## Messaging

The Messaging policy group contains policies that collect and monitor the performance metrics of the BizTalk Messaging Engine. This policy group comprises of the following set of policies for monitoring and logging:

### Metrics Monitored

Metric ID: 843002

Metric Name	BTS_DELIVTHROTST
Description	This policy monitors the throttling state of the message delivery and generates appropriate message for each state.
Metric Definition	Performance Object: BizTalk: Message Agent Performance Counter: Message delivery throttling state Performance Instance: *
Measurement Threshold Policy	BTS_843002
Config File Policy	BTS_CFG_843002
Scheduled Task Policy for Alerting	BTS_SCH_843002
Schedule	10 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Message Box



Metric ID: 843003

Metric Name	BTS_DELIVDELAY
Description	This policy monitors the delay injected in each qualifying batch for throttling the delivery of messages.
Metric Definition	Performance Object: BizTalk: Message Agent Performance Counter: Message delivery delay (ms) Performance Instance: *
Measurement Threshold Policy	BTS_843003
Config File Policy	BTS_CFG_843003
Scheduled Task Policy for Alerting	BTS_SCH_843003
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 843004

Metric Name	BTS_DELIVTHRODUR
Description	This policy monitors the seconds spent in the current state of message delivery throttling.
Metric Definition	Performance Object: BizTalk: Message Agent Performance Counter: Message delivery throttling state duration Performance Instance: *
Measurement Threshold Policy	BTS_843004
Config File Policy	BTS_CFG_843004
Scheduled Task Policy for Alerting	BTS_SCH_843004
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 844002

Metric Name	BTS_MSGPUBDEL
Description	This policy monitors the delay injected in each qualifying batch for throttling the publishing of messages.
Metric Definition	Performance Object: BizTalk: Message Agent Performance Counter: Message publishing delay (ms) Performance Instance: *
Measurement Threshold Policy	BTS_844002
Config File Policy	BTS_CFG_844002
Scheduled Task Policy for Alerting	BTS_SCH_844002
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 844003

Metric Name	BTS_MSGPUBTHROT
Description	This policy monitors the message publishing throttling state.
Metric Definition	Performance Object: BizTalk: Message Agent Performance Counter: Message publishing throttling state Performance Instance: *
Measurement Threshold Policy	BTS_844003
Config File Policy	BTS_CFG_844003
Scheduled Task Policy for Alerting	BTS_SCH_844003
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 844004

Metric Name	BTS_MSGPUBTHROTDUR
Description	This policy monitors the seconds spent in the current state of message publishing throttling.
Metric Definition	Performance Object: BizTalk:Message Agent Performance Counter: Message publishing throttling state duration Performance Instance: *
Measurement Threshold Policy	BTS_844004
Config File Policy	BTS_CFG_844004
Scheduled Task Policy for Alerting	BTS_SCH_844004
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 846002

Metric Name	BTS_MSGOUTLAT
Description	This policy monitors the outbound latency of Biztalk Messaging Engine.
Metric Definition	Performance Object: BizTalk: Messaging Latency Performance Counter: Outbound Latency (sec) Performance Instance: *
Measurement Threshold Policy	BTS_846002
Config File Policy	BTS_CFG_846002
Scheduled Task Policy for Alerting	BTS_SCH_846002
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 846004

Metric Name	BTS_MSGINLAT
Description	This policy monitors the Inbound Messaging Latency of the BizTalk Messaging Engine.
Metric Definition	Performance Object: BizTalk: Messaging Latency Performance Counter: Inbound Latency (sec) Performance Instance: *
Measurement Threshold Policy	BTS_846004
Config File Policy	BTS_CFG_846004
Scheduled Task Policy for Alerting	BTS_SCH_846004
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 846005

Metric Name	BTS_MSGOUTAD
Description	This policy monitors the outbound adapter latency of the BizTalk Messaging Engine.
Metric Definition	Performance Object: BizTalk: Messaging Latency Performance Counter: Outbound Adapter Latency (sec) Performance Instance: *
Measurement Threshold Policy	BTS_846005
Config File Policy	BTS_CFG_846005
Scheduled Task Policy for Alerting	BTS_SCH_846005
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Metric ID: 848002

Metric Name	BTS_REQRESTO
Description	This policy monitors the request response timeout of the BizTalk Messaging Engine.
Metric Definition	Performance Object: BizTalk: Messaging Performance Counter: Request/Response timeouts Performance Instance: *
Measurement Threshold Policy	BTS_848002
Config File Policy	BTS_CFG_848002
Scheduled Task Policy for Alerting	BTS_SCH_848002
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

## Metrics Logged

Collection ID: 840003

Collection Name	BTS_MSGDELIVERY
Description	This policy collects and logs performance metrics related to Message Delivery.
Collection Definition	Performance Object: BizTalk: Message Agent Performance Counter: Message delivery throttling state Performance Counter: Message delivery delay (ms) Performance Counter: Message delivery throttling state duration Performance Counter: Message delivery incoming rate Performance Counter: Message delivery outgoing rate Performance Counter: Total messages delivered Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840003
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Collection ID: 840004

Collection Name	BTS_MSGPUBLISHING
Description	This policy collects and logs metrics related to Message Publishing.
Collection Definition	<p>Performance Object: BizTalk: Message Agent</p> <p>Performance Counter: Message publishing delay (ms)</p> <p>Performance Counter: Message publishing throttling state</p> <p>Performance Counter: Message publishing throttling state duration</p> <p>Performance Counter: Message publishing incoming rate</p> <p>Performance Counter: Message publishing outgoing rate</p> <p>Performance Counter: Total messages published</p> <p>Performance Instance: *</p>
Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Collection ID: 840006

Collection Name	BTS_MSGLATENCY
Description	This policy collects and logs metrics related to Message Latency.
Collection Definition	<p>Performance Object: BizTalk: Messaging Latency</p> <p>Performance Counter: Outbound Latency (sec)</p> <p>Performance Counter: Request-Response Latency (sec)</p> <p>Performance Counter: Inbound Latency (sec)</p> <p>Performance Counter: Outbound Adapter Latency (sec)</p> <p>Performance Instance: *</p>

Collection Name	BTS_MSGLATENCY
Schedule Task Policy for Logging	BTS_SCH_840006
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging

Collection ID: 840008

Collection Name	BTS_MSGINGPERF
Description	This policy collects and logs metrics related to Messaging Performance.
Collection Definition	Performance Object: BizTalk: Messaging Performance Counter: Request/Response timeouts Performance Counter: Active receive locations Performance Counter: Active receive threads Performance Counter: Active send messages Performance Counter: Active send threads Performance Counter: Pending receive batches Performance Counter: Pending transmitted messages Performance Counter: Throttled receive batches Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840008
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Messaging



## Orchestration Engine

This policy group comprises of the following policies.

### Metrics Monitored

Metric ID: 842002

Metric Name	BTS_BATCHFACT
Description	This metric monitors the average batch factor.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: Average batch factor Performance Instance: *
Measurement Threshold Policy	BTS_842002
Config File Policy	BTS_CFG_842002
Scheduled Task Policy for Alerting	BTS_SCH_842002
Schedule	10 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

Metric ID: 842005

Metric Name	BTS_ORCHIDLE
Description	This metric monitors the number of idle orchestrations.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: Idle orchestrations Performance Instance: *
Measurement Threshold Policy	BTS_842005
Config File Policy	BTS_CFG_842005
Scheduled Task Policy for Alerting	BTS_SCH_842005
Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

Metric ID: 842012

Metric Name	BTS_ORCHDEHYSEC
Description	This metric monitors the rate of dehydration of orchestrations.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: Orchestrations dehydrated/sec Performance Instance: *
Measurement Threshold Policy	BTS_842012
Config File Policy	BTS_CFG_842012
Scheduled Task Policy for Alerting	BTS_SCH_842012
Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

Metric ID: 842013

Metric Name	BTS_ORCHDISC
Description	This metric monitors the orchestrations discarded.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: Orchestrations discarded Performance Instance: *
Measurement Threshold Policy	BTS_842013
Config File Policy	BTS_CFG_842013
Scheduled Task Policy for Alerting	BTS_SCH_842013
Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

Metric ID: 842018

Metric Name	BTS_ORCHSUSPSEC
Description	This metric monitors the rate of orchestrations discarded.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: Orchestrations suspended/sec Performance Instance: *
Measurement Threshold Policy	BTS_842018
Config File Policy	BTS_CFG_842018
Scheduled Task Policy for Alerting	BTS_SCH_842018
Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

Metric ID: 842021

Metric Name	BTS_TRANSABORT
Description	This metric monitors the transactions aborted.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: Transactional scopes aborted/sec Performance Instance: *
Measurement Threshold Policy	BTS_842021
Config File Policy	BTS_CFG_842021
Scheduled Task Policy for Alerting	BTS_SCH_842021
Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

Metric ID: 842023

Metric Name	BTS_MSGDBCONFAIL
Description	This metric monitors the MessageBoxDB Connection Failures.
Metric Definition	Performance Object: XLANG// s Orchestrations Performance Counter: MessageBox databases connection failures Performance Instance: *
Measurement Threshold Policy	BTS_842023
Config File Policy	BTS_CFG_842023
Scheduled Task Policy for Alerting	BTS_SCH_842023
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

## Metrics Logged

Collection ID: 840002

Collection Name	BTS_ORCHPERF
Description	This policy collects and logs performance metrics related to Orchestrations
Collection Definition	Performance Object: XLANG/s Orchestrations Performance Counter: Average batch factor Performance Counter: Database transactions Performance Counter: Database transactions/sec Performance Counter: Idle orchestrations Performance Counter: Online MessageBox databases Performance Counter: Orchestrations completed Performance Counter: Orchestrations completed/sec Performance Counter: Orchestrations created Performance Counter: Orchestrations created/sec Performance Counter: Orchestrations dehydrated Performance Counter: Orchestrations dehydrated/sec Performance Counter: Orchestrations discarded Performance Counter: Orchestrations discarded/sec Performance Counter: Orchestrations rehydrated Performance Counter: Orchestrations rehydrated/sec Performance Counter: Orchestrations suspended Performance Counter: Orchestrations suspended/sec Performance Counter: Orchestrations resident in-memory Performance Counter: Running orchestrations Performance Counter: Transactional scopes aborted/sec Performance Counter: Transactional scopes committed/sec
Collection Definition	Performance Counter: Message Box databases connection failures Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840002
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Orchestration Engine

## Performance

The Performance policy group contains the following policies.

### Metrics Logged

Collection ID: 840009

Collection Name	BTS_PROCESS
Description	This policy collects and logs metrics related to BTSNTSVC Performance.
Collection Definition	Performance Object: Process Performance Counter: % Processor Time; Performance Instance: System Performance Counter: Thread Count; Performance Instance: BTSNTSVC Performance Counter: Page Faults/sec; Performance Instance: BTSNTSVC Performance Counter: Working Set; Performance Instance: BTSNTSVC Performance Counter: Private Bytes; Performance Instance: BTSNTSVC
Schedule Task Policy for Logging	BTS_SCH_840009
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Performance

Collection ID: 840010

Collection Name	BTS_PROCESS
Description	This policy collects and logs metrics related to ENTSSO Performance
Collection Definition	<p>Performance Object: Process</p> <p>Performance Counter: % Processor Time; Performance Instance: ENTSSO</p> <p>PerfCounter: % Processor Time; PerfInstance: System</p> <p>Performance Counter: Thread Count; Performance Instance: ENTSSO</p> <p>Performance Counter: Page Faults/sec; Performance Instance: ENTSSO</p> <p>Performance Counter: Working Set; Performance Instance: ENTSSO</p> <p>Performance Counter: Private Bytes; Performance Instance: ENTSSO</p>
Schedule Task Policy for Logging	BTS_SCH_840010
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Performance

Collection ID: 840011

Collection Name	BTS_PROCESS
Description	This policy collects and logs metrics related to RuleEngineUpdateService Performance.
Collection Definition	<p>Performance Object: Process</p> <p>Performance Counter: % Processor Time; Performance Instance:RuleEngineUpdateService</p> <p>Performance Counter: % Processor Time; Performance Instance: System</p> <p>Performance Counter: Thread Count; Performance Instance: RuleEngineUpdateService</p> <p>Performance Counter: Page Faults/sec PerformanceInstance: RuleEngineUpdateService</p> <p>Performance Counter: Working Set; Performance Instance: RuleEngineUpdateService</p> <p>Performance Counter: Private Bytes; Performance Instance: RuleEngineUpdateService</p>

Collection Name	BTS_PROCESS
Schedule Task Policy for Logging	BTS_SCH_840011
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Performance

## Sharepoint Adapter

The Sharepoint Adapter policy group contains the following policies.

### Metrics Monitored

Metric ID: 847002

Metric Name	BTS_RECMSGFAIL
Description	Monitors SP Adapter Message Receive Failure and checks the percentage of Windows SharePoint Services files that are not processed by Biztalk Server due to receive errors.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: % Receive Message Failures
Measurement Threshold Policy	BTS_847002
Config File Policy	BTS_CFG_847002
Scheduled Task Policy for Alerting	BTS_SCH_847002
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter



Metric ID: 847003

Metric Name	BTS_SENDMSGFAIL
Description	Monitor SP Adapter Message Send Failure and checks the percentage of Windows SharePoint Services files that are not processed by BizTalk Server due to receive errors.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: % Send Message Failures
Measurement Threshold Policy	BTS_847003
Config File Policy	BTS_CFG_847003
Scheduled Task Policy for Alerting	BTS_SCH_847003
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

Metric ID: 847004

Metric Name	BTS_WEBSVCCALLFAIL
Description	This policy monitors the SP Adapter Wsvc Call Failure and checks the percentage of Windows SharePoint Services adapter Web service calls that have failed.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: % Web Service Call Failures
Measurement Threshold Policy	BTS_847004
Config File Policy	BTS_CFG_847004
Scheduled Task Policy for Alerting	BTS_SCH_847004
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

Metric ID: 847005

Metric Name	BTS_RECCOMITFAIL
Description	This policy monitors the SP Adapter Total Receive commit Failure and checks the total number of Windows SharePoint Services errors that were raised when updating the status of the SharePoint documents.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: Total Receive Commit Failures
Measurement Threshold Policy	BTS_847005
Config File Policy	BTS_CFG_847005
Scheduled Task Policy for Alerting	BTS_SCH_847005
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

Metric ID: 847006

Metric Name	BTS_RECVMMSGFAIL
Description	This policy monitors the SP Adapter Total Receive Message Failure and checks the total number of Windows SharePoint Services files received that have not been processed by Biztalk Server due to errors.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: Total Receive Message Failures
Measurement Threshold Policy	BTS_847006
Config File Policy	BTS_CFG_847006

Metric Name	BTS_RECVMSGFAIL
Scheduled Task Policy for Alerting	BTS_SCH_847006
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

Metric ID: 847007

Metric Name	BTS_TTLSENDMSGFAIL
Description	Monitors the SP Adapter Total Send Message Failure and checks the total number of failed messages BizTalk Server attempted to send to Windows SharePoint Services.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: Total Send Message Failures
Measurement Threshold Policy	BTS_847007
Config File Policy	BTS_CFG_847007
Scheduled Task Policy for Alerting	BTS_SCH_847007
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

Metric ID: 847008

Metric Name	BTS_WEBSVCCALTOT
Description	This policy monitors the SP Adapter Total Wsvc Call Failure and checks the total number of Windows SharePoint Services adapter Web service calls that have failed.
Metric Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Instance: * Performance Counter: Total Web Service Call Failures
Measurement Threshold Policy	BTS_847008
Config File Policy	BTS_CFG_847008
Scheduled Task Policy for Alerting	BTS_SCH_847008
Schedule	5 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

## Metrics Logged

Collection ID: 840007

Collection Name	BTS_SHRPERF
Description	This policy collects and logs metrics related to Sharepoint Server
Collection Definition	Performance Object: BizTalk: Windows Sharepoint Services Adapter Performance Counter: % Receive Message Failures Performance Counter: % Send Message Failures Performance Counter: % Web Service Call Failures Performance Counter: Total Receive Commit Failures Performance Counter: Total Receive Message Failures Performance Counter: Total Send Message Failures Performance Counter: Total Web Service Call Failures Performance Counter: Total Sent Messages Performance Counter: Total Received Messages PerformanceCounter: Web Service Calls per Second Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840007
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → Sharepoint Adapter

## Tracking Data Decode Services (TDDS)

This policy group comprises of the following policies.

### Metrics Logged

Collection ID: 840013

Collection Name	BTS_TDDSSTAT
Description	This metric collects and logs performance metrics related to TDDS.
Collection Definition	Performance Object: Biztalk:TDDS Performance Counter: Total Batches Performance Counter: Total Events Performance Counter: Total Failed Batches Performance Counter: Total Failed Events Performance Counter: Total Records Performance Counter: Batches being processed Performance Counter: Events being processed Performance Counter: Records being processed Performance Counter: Batches Committed Performance Counter: Events Committed Performance Counter: Records Committed Performance Instance: *
Schedule Task Policy for Logging	BTS_SCH_840013
Collection Schedule	15 min
Policy Group	SPI for Microsoft Enterprise Servers → en → Biztalk Server → Biztalk Server 2010 → TDDS

# Reports

The Microsoft Enterprise Servers SPI provides the following reports for Microsoft Enterprise Servers (BizTalk Server 2010) SPI:

## BizTalk Server Document Processing Statistics

This is a weekly report which provides statistical summary of the documents processed by the BizTalk Server. The summarized document statistics include average number of Documents Processed, Received, Suspended, Re-Submitted and Transmitted for each day per BizTalk Server. These reports provide the summary of the following monthly and weekly statistics related to the BizTalk Documents. The following metric descriptions are displayed in this report:

- Documents processed: Represents the average number of documents processed, that is, pulled from the work queue and sent to a port destination address.
- Documents received: Represents the average number of documents that are received by the BizTalk Server. This includes all documents that are logged into the work queue and documents that have failed.
- Documents suspended: Represents the average number of documents that are suspended.
- Documents Re-submitted: Represents the average number of documents resubmitted by send adapters.
- Documents Transmitted: Represents the average number of documents transmitted per batch. The schedule for this report is defined in the following policy:

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840012

Class Name: BTS\_DOCPROCRATE

## Tracking Date Decode Statistics (TDDS) Statistics Report

This weekly report shows TDDS statistics for a BizTalk Server in graphical and tabular format. The summarization comprises of average number of TDDS Batches, Events, Failed Batches and Failed Events per day per BizTalk Server. This report provides the summary of the statistics of TDDS. Events processed

- Events failed
- Number of batches processed
- Number of batches failed

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840013

Class Name: BTS\_TDDSSTAT

## BizTalk Server Processes CPU Statistics - Application Service

The BTS Process CPU Statistics report shows a summary of CPU statistics of BizTalk Server processes, compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics include the percentage of CPU time used by BizTalk Server Application Service processes compared with the percentage of time the system CPU was busy. This report has the following counters:

- Process.% Processor Time (BTSNTSvc) - CPU time used by the BizTalk service
- Process.Thread Count (BTSNTSvc) - Thread count of the BizTalk service
- System % Processor Time - Total time the system CPU was busy

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840009

Class Name: BTS\_PROCESS

## BizTalk Server Processes CPU Statistics - Enterprise Single Sign On (SSO) Service

The BTS Process CPU Statistics report shows a summary of CPU statistics of BizTalk Server processes, compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics include the percentage of CPU time used by Enterprise SSO (Single Sign On) Service processes compared with the percentage of time the system CPU was busy. This report has the following counters:

- Process. % Processor Time (ENTSSO) - CPU time used by the BizTalk service
- Process.Thread Count (ENTSSO) - Thread count of the BizTalk service
- System % Processor Time - Total time the system CPU was busy

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840010

Class Name: BTS\_PROCESS

## BizTalk Server Processes CPU Statistics - Rule Engine Update Service

The BTS Process CPU Statistics report shows a summary of CPU statistics of BizTalk Server processes, compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics include the percentage of CPU time used by Rule Engine Update Service processes compared with the percentage of time the system CPU was busy. This report has the following counters:

- Process.% Processor Time (RuleEngineUpdateService) - CPU time used by the BizTalk service
- Process.Thread Count (RuleEngineUpdateService) - Thread count of the BizTalk service
- System % Processor Time - Total time the system CPU was busy

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840011

Class Name: BTS\_PROCESS



## BizTalk Server Processes Memory Statistics - Application Service

The BTS Processes Memory Statistics report shows summary of memory statistics of BizTalk Server processes in graphical and tabular formats. The summarized process statistics include the page faults per second, private bytes, and working set used by BizTalk Server Application Service. This report has the following counters:

- Process.Private Bytes (BTSNTSvc)
- Process.Working Set (BTSNTSvc)
- Process.Page Faults/sec (BTSNTSvc)

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840009

Class Name: BTS\_PROCESS

## BizTalk Server Processes Memory Statistics - Enterprise Single Sign On (SSO) Service

The BTS Processes Memory Statistics report shows summary of memory statistics of BizTalk Server processes in graphical and tabular formats. The summarized process statistics include the page faults per second, private bytes, and working set used by Enterprise SSO (Single Sign On) Service. This report has the following counters:

- Process.Private Bytes (ENTSSO)
- Process.Working Set (ENTSSO)
- Process.Page Faults/sec (ENTSSO)

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840010

Class Name: BTS\_PROCESS

## BizTalk Server Processes Memory Statistics - Rule Engine Update Service

The BTS Processes Memory Statistics report shows summary of memory statistics of BizTalk Server processes in graphical and tabular formats. The summarized process statistics include the page faults per second, private bytes, and working set used by Rule Engine Update Service. This report has the following counters:

- Process.Private Bytes (RuleEngineUpdateService)
- Process.Working Set (RuleEngineUpdateService)
- Process.Page Faults/sec (RuleEngineUpdateService)

The schedule for this report is defined in the following policy:

Policy Name: BTS\_SCH\_840011

Class Name: BTS\_PROCESS

# Graphs

The following pre-defined graphs are provided for BizTalk Server 2010:

## BizTalk Service CPU Statistics

This graph shows the CPU statistics of the BizTalk service compared with overall CPU statistics of the system.

## Enterprise SSO Service CPU Statistics

This graph shows the CPU statistics of Enterprise SSO service compared with overall CPU statistics of the system.

## Rule Engine Update Service CPU Statistics

This graph shows the CPU statistics of the IM conferencing service compared with overall CPU statistics of the system.

## BizTalk Service Memory Statistics

This graph shows the memory statistics of the Biztalk Service.

## Enterprise SSO Memory Statistics

This graph shows the memory statistics of the Enterprise SSO Service.

## Rule Engine Update Service Memory Statistics

This graph shows the memory statistics of the Rule Engine Update Service.

## Document Processing Statistics by Biztalk Server

This graph shows the documents processing statistics of BizTalk Server.

## Orchestration Statistics by Biztalk Server

This graph shows the issues encountered by BizTalk Orchestration.

## BizTalk TDDS Statistics

This graph shows the TDDS Statistics of BizTalk Server.

## 4 Microsoft Enterprise Servers SPI for Internet Security and Acceleration Server 2006

The Microsoft Internet Security and Acceleration (ISA) Server is a tool that integrates security (firewall) with acceleration (Web proxy cached pages). This secures your site and speeds up the web access.

The Internet Security and Acceleration Server service map displays the nodes where Internet Security and Acceleration Servers are installed. The service maps are available under both the Applications and the Systems Infrastructure areas.

### Policies

The Microsoft Enterprise Servers SPI ISA Server policies monitor the Microsoft ISA Server. The policies provide the following monitoring processes:

- Availability Monitoring
- Windows Event Log Monitoring
- Log File Monitoring
  - Performance Monitoring
  - Performance Data Logging
- Discovery

### Availability Monitoring

The Availability Monitoring group monitors the services of the Microsoft ISA Server. Services are not automatically restarted because they may have been shut down intentionally.

Monitored services of the ISA Server include the following:

- Microsoft Firewall (wspsrv)
- Microsoft ISA Server Control (mspadmin)
- Microsoft ISA Server Job Scheduler (w3prefch)
- Routing and Remote Access (svchost)
- Network Load Balancing
- Microsoft Data Engine (sqlservr)
- Microsoft ISA Server Storage (isastg)
- ISA Storage Configuration (dsadmin)

The Availability Monitoring group policies are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Availability Monitoring**

All the policies in the Availability Monitoring group of the Internet Security And Acceleration Server belong to the **Windows Management Interface** policy type.

The following table lists the details of the policies in the group.

Policy	Description
ISA2006_Availability_Config-Storage-Service	Checks if ISA Configuration Storage Server service is running. If not, it tries to restart the service.
ISA2006_Availability_DataEngine-Service	Checks if ISA Data Engine service is running. If not, it tries to restart the service.
ISA2006_Availability_Firewall-Service	Checks if Microsoft Firewall service is running. If not, it tries to restart the service.
ISA2006_Availability_JobScheduler-Service	Checks if ISA Job Scheduler service is running. If not, it tries to restart the service.
ISA2006_Availability_Network-Load-Balancing-Service	Checks if ISA Network Load Balancing service is running. If not, it tries to restart the service.
ISA2006_Availability_RemoteAccess-Service	Checks if ISA Routing and Remote Access service is running. If not, it tries to restart the service.
ISA2006_Availability_ServerControl-Service	Checks if ISA Server Control service is running. If not, it tries to restart the service.
ISA2006_Availability_Storage-Service	Checks if ISA Server Storage service is running. If not, it tries to restart the service.

## Performance Monitoring

ISA performance monitoring includes both specific ISA Server performance counters and CPU process-related counters. Each policy for performance monitoring has error and warning thresholds.

The Performance Monitoring policy group includes the following groups:

- [Firewall Service](#)
- [Firewall Engine](#)
- [Job Scheduler](#)
- [Network Load Balancing](#)
- [Microsoft Data Engine](#)
- [Remote Access](#)
- [ISA Server Control](#)
- [ISA Server Storage](#)
- [Storage Configuration](#)

### Firewall Service

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → Firewall**

All the policies in the Firewall Service group have the policy type as **Measurement Threshold**.

The following table lists the policies in the Firewall Service group.

<b>Policy</b>	<b>Description</b>
ISA2006_Firewall_PageFaults	Monitors Page Faults of Firewall process.
ISA2006_Firewall_PrivateBytes	Monitors private bytes of Firewall process.
ISA2006_Firewall_ProcessorTime	Monitors processor time of Firewall process.
ISA2006_Firewall_ThreadCount	Monitors Thread Count of Firewall process.
ISA2006_Firewall_WorkingSet	Monitors Working Set of Firewall process.

### Firewall Engine

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → Firewall Engine**

All the policies in the Firewall Service group have the policy type as **Measurement Threshold**.

The following table lists the policies in the Firewall Engine group.

<b>Policy</b>	<b>Description</b>
ISA2006_FirewallEngine_PageFaults	Monitors Page Faults of Firewall Engine.
ISA2006_FirewallEngine_PrivateBytes	Monitors Private Bytes of Firewall Engine.
ISA2006_FirewallEngine_ProcessorTime	Monitors Processor Time of Firewall Engine.
ISA2006_FirewallEngine_ThreadCount	Monitors Thread Count of Firewall Engine.
ISA2006_FirewallEngine_WorkingSet	Monitors Working Set of Firewall Engine.

### Job Scheduler

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → Job Scheduler**

All the policies in the Job Scheduler group have the policy type as **Measurement Threshold**.

The following table lists the policies in the Job Scheduler group.

<b>Policy</b>	<b>Description</b>
ISA2006_JobScheduler_PageFaults	Monitors Page Faults of Job Scheduler process.
ISA2006_JobScheduler_PrivateBytes	Monitors Private Bytes of Job Scheduler process.
ISA2006_JobScheduler_ProcessorTime	Monitors Processor Time of Job Scheduler process.
ISA2006_JobScheduler_ThreadCount	Monitors Thread Count of Job Scheduler process.
ISA2006_JobScheduler_WorkingSet	Monitors Working Set of Job Scheduler process.

### Network Load Balancing

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → Network Load Balancing**

All the policies in the Network Load Balancing group have the policy type as **Measurement Threshold**.

The following table lists the policies in the Network Load Balancing group.

<b>Policy</b>	<b>Description</b>
ISA2006_LoadBalancing_PageFaults	Monitors Page Faults of Load Balancing process.
ISA2006_LoadBalancing_PrivateBytes	Monitors Private Bytes of Load Balancing process.
ISA2006_LoadBalancing_ProcessorTime	Monitors Processor Time of Load Balancing process.
ISA2006_LoadBalancing_ThreadCount	Monitors Thread Count of Load Balancing process.
ISA2006_LoadBalancing_WorkingSet	Monitors Working Set of Load Balancing process.

### Microsoft Data Engine

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → Microsoft Data Engine**

All the policies in the Microsoft Data Engine group have the policy type as **Measurement Threshold**.

The following table lists the policies in the Microsoft Data Engine group.

<b>Policy</b>	<b>Description</b>
ISA2006_MSSQLMSFW_PageFaults	Monitors Page Faults of Microsoft Data Engine process.
ISA2006_MSSQLMSFW_PrivateBytes	Monitors Private Bytes of Microsoft Data Engine process.
ISA2006_MSSQLMSFW_ProcessorTime	Monitors Processor Time of Microsoft Data Engine process.
ISA2006_MSSQLMSFW_ThreadCount	Monitors Thread Count of Microsoft Data Engine process.
ISA2006_MSSQLMSFW_WorkingSet	Monitors Working Set of Microsoft Data Engine process.

#### Remote Access

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → Remote Access**

All the policies in the Remote Access group have the policy type as **Measurement Threshold**.

The following table lists the policies in the Remote Access group.

<b>Policy</b>	<b>Description</b>
ISA2006_RemoteAccess_PageFaults	Monitors Page Faults of Remote Access process.
ISA2006_RemoteAccess_PrivateBytes	Monitors Private Bytes of Remote Access process.
ISA2006_RemoteAccess_ProcessorTime	Monitors Processor Time of Remote Access process.
ISA2006_RemoteAccess_ThreadCount	Monitors Thread Count of Remote Access process.
ISA2006_RemoteAccess_WorkingSet	Monitors Working Set of Remote Access process.

#### ISA Server Control

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Monitoring → Service Based → ISA Server Control**

All the policies in the ISA Server Control group have the policy type as **Measurement Threshold**.

The following table lists the policies in the ISA Server Control group.

<b>Policy</b>	<b>Description</b>
ISA2006_ServerControl_PageFaults	Monitors Page Faults of Server Control process.
ISA2006_ServerControl_PrivateBytes	Monitors Private Bytes of Server Control process.
ISA2006_ServerControl_ProcessorTime	Monitors Processor Time of Server Control process.
ISA2006_ServerControl_ThreadCount	Monitors thread count of Server Control process.
ISA2006_ServerControl_WorkingSet	Monitors Working Set of Server Control process.

### ISA Server Storage

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers** → en → **Internet Security And Acceleration Server** → **Internet Security And Acceleration Server 2006** → **Log File Monitoring** → **Performance Monitoring** → **Service Based** → **ISA Server Storage**

All the policies in the ISA Server Storage group have the policy type as **Measurement Threshold**.

The following table lists the policies in the ISA Server Storage group.

<b>Policy</b>	<b>Description</b>
ISA2006_ServerStorage_PageFaults	Monitors Private Bytes of Server Storage process.
ISA2006_ServerStorage_PrivateBytes	Monitors Private Bytes of Server Storage process.
ISA2006_ServerStorage_ProcessorTime	Monitors Processor Time of Server Storage Process.
ISA2006_ServerStorage_ThreadCount	Monitors Thread Count of Server Storage Process.
ISA2006_ServerStorage_WorkingSet	Monitors Working Set of Server Storage Process.

### Storage Configuration

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers** → en → **Internet Security And Acceleration Server** → **Internet Security And Acceleration Server 2006** → **Log File Monitoring** → **Performance Monitoring** → **Service Based** → **Storage Configuration**

All the policies in the Storage Configuration group have the policy type as **Measurement Threshold**.



The following table lists the policies in the Storage Configuration group.

<b>Policy</b>	<b>Description</b>
ISA2006_StorageConfig_PageFaults	Monitors Page Faults of Storage Configuration process.
ISA2006_StorageConfig_PrivateBytes	Monitors Private Bytes of Storage Configuration process.
ISA2006_StorageConfig_ProcessorTime	Monitors Processor Time of Storage Configuration process.
ISA2006_StorageConfig_ThreadCount	Monitors Thread Count of Storage Configuration process.
ISA2006_StorageConfig_WorkingSet	Monitors Working Set of Storage Configuration process.

## Windows Event Log Monitoring

Event monitoring of the Windows 2000 and 2003 Event Log (application log) occurs for ISA Server events. Console messages are sent for all errors, warnings, and information events logged for the following sources:

- Microsoft Firewall
- Microsoft Web Proxy
- Microsoft ISA Server Control
- Microsoft Scheduled Cache Content Download

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers** → **en** → **Internet Security And Acceleration Server** → **Internet Security And Acceleration Server 2006** → **Event Log Monitoring**

All the policies in the Event monitoring group belong to the **Windows Event Log** policy type.

The following table lists the policies in the Event monitoring group.

<b>Policy</b>	<b>Description</b>
ISA2006_FwdApplicationError	Forwards all ISA Server application log entries with severity as Error.
ISA2006_FwdApplicationInformation	Forwards all ISA Server application log entries with severity as Information.
ISA2006_FwdApplicationWarning	Forwards all ISA Server application log entries with severity as Warning.

## Server Logging

In Server Logging group, selected process-related data for CPU and memory counters is logged for the ISA Server.

The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Log File Monitoring → Performance Data Logging**

All the policies in the Event monitoring group belong to the **Measurement Threshold** policy type.

The following table lists the policies of the Server Logging group.

<b>Policy</b>	<b>Description</b>
ISA2006_Logging_Firewall	Logs selected performance data for ISA Server 2006 Firewall service.
ISA2006_Logging_JobScheduler	Logs selected performance data for ISA Server 2006 Job Scheduler.
ISA2006_Logging_ServerCache	Logs selected performance data for ISA Server 2006 Cache.
ISA2006_Logging_ServerControl	Logs selected performance data for ISA Server 2006 Server Control.
ISA2006_Logging_WebProxy	Logs selected performance data for ISA Server 2006 Web Proxy service.

## Discovery

The Discovery monitoring group discovers the services of the ISA server. The policies in this group are available at the following location:

**SPI for Microsoft Enterprise Servers → en → Internet Security And Acceleration Server → Internet Security And Acceleration Server 2006 → Discovery**

The following table lists the policies in the Discovery monitoring group.

<b>Policy</b>	<b>Description</b>	<b>Policy Type</b>
ISA2006_Discovery_System	Discovers and adds infrastructure information to the service map.	Service Auto-Discovery policy
ISA2006_Discovery_Application	Discovers and adds application and dependency information to the service map.	

## Reports

Reports represent various metrics. They contain data collected by policies.

The Microsoft Enterprise Servers SPI offers a number of reports that help you monitor ISA Server activity. The following sections detail the report descriptions including listings of the performance counters used.

### Firewall, Scheduled Cache Content Download, and ISA Server Control Process CPU Statistics

The Firewall, Scheduled Cache Content Download, and ISA Server Control Process CPU Statistics report shows summary CPU statistics of ISA Server processes compared with overall CPU statistics of the system.

This report has the following counters:

- Process.% Processor Time (wspsrv, mspadmin, w3prefch, w3proxy)
- Process.Thread Count(wspsrv, mspadmin, w3prefch, w3proxy)
- Processor:% Processor Time

## Dropped Packets Statistics

The Dropped Packets Statistics report shows summary statistics of ISA Server total dropped packets resulting from packet filtering.

This report has ISA Server Firewall Packet Engine.Dropped Packets as its counter.

## Firewall Statistics

The Firewall Statistics report shows summary statistics of the ISA Server firewall, including the number of active sessions, the number of kernel mode data pumps, and the number of worker threads.

This report has the following counters:

- Active Sessions
- Active TCP Connections
- Active UDP Connections
- SecureNAT Mappings
- Worker Threads
- Available Worker Threads
- Kernel Mode Data Pumps
- Bytes Read/sec
- Bytes Written/sec

## Firewall, Scheduled Cache Content Download, and ISA Server Control Process Memory Statistics

The Firewall, Scheduled Cache Content Download, and ISA Server Control Process Memory Statistics report shows summary of memory statistics of ISA Server processes.

This report has the following counters:

- Process.Private Bytes (wspsrv, mspadmin, w3prefch, w3proxy)
- Process.Working Set (wspsrv, mspadmin, w3prefch, w3proxy)
- Process.Page Faults/sec (wspsrv, mspadmin, w3prefch, w3proxy)

## ISA Server Cache Statistics

The ISA Server Cache Statistics report shows summary statistics of the ISA Server memory and disk cache, including the memory cache usage ratio percentage, and the disk cache failure rate. This report has the following counters:

- Memory Usage Ratio Percent (%)
- Bytes Retrieved Rate from Memory Cache (KB/sec)

- Memory Cache Allocated Space (KB)
- Disk Failure Rate (Fail/sec)
- Total Disk Failures
- Bytes Retrieved Rate From Disk Cache (KB/sec)
- Disk Cache Allocated Space (KB)
- URL Commit Rate (URL/sec)
- URLs in Cache
- Max URLs Cached

## Web Proxy Statistics

The Web Proxy Statistics report shows summary statistics of the ISA Server Web Proxy, including the cache hit ratio percentage, the current number of Web proxy users, and the rate at which data bytes are sent and received by the Web proxy service to and from Web Proxy clients.

This report has the following counters:

- Cache Hit Ratio (%)
- Cache Running Hit Ratio (%)
- Total Cache Fetches
- Client Bytes Received/sec
- Client Bytes Sent/sec
- Client Bytes Total/sec
- Current Users
- Maximum Users

## Web Proxy Request Statistics

The Web Proxy Request Statistics report shows summary statistics of the ISA Server Web Proxy including the number of failing client requests per second, and the total number of successful and failing client requests that are made to the Web Proxy service.

This report has the following counters:

- Failing Requests/sec
- Requests/sec
- Total Failing Requests
- Total Successful Requests
- Total Requests
- Ftp Requests
- Http Requests

## Web Proxy Sites Granted and Denied Statistics

The Web Proxy Sites Allowed and Denied Statistics report shows summary statistics of the ISA Server Web Proxy including the number of web sites allowed access to client and the number of web sites denied access to clients.

This report has the following counters:

- Sites Denied
- Sites Allowed

## Graphs

The Microsoft Enterprise Servers SPI graphs are pictorial representations of various metrics of ISA Server. Graphs contain data that are collected by the Microsoft Enterprise Servers SPI.

The following table lists the Microsoft Enterprise Servers SPI ISA Server 2006 graphs.

<b>Graph</b>	<b>Description</b>
Cache URL Statistics	Summary statistics relating to URLs of the ISA Server cache.
Disk Cache Statistics	Summary statistics of the ISA Server disk cache.
Disk Failure Statistics	Summary statistics of the ISA Server disk cache failure rate.
Dropped Packets Statistics	Summary statistics of ISA Server total dropped packets resulting from packet filtering.
Firewall CPU	Summary CPU statistics of the ISA Server Firewall process.
Firewall Data Pump Statistics	Summary statistics of the ISA Server firewall, including the number of kernel mode data pumps.
Firewall Memory	Summary memory statistics of the ISA Server Firewall process.
Firewall Session / Connection Statistics	Summary statistics of the ISA Server firewall, including the number of active sessions.
Firewall Worker Threads Statistics	Summary statistics of the ISA Server firewall, including the number of worker threads.
ISA Server Control CPU	Summary CPU statistics of the ISA Server Control process.
ISA Server Control Memory	Summary memory statistics of the ISA Server Control process.
Memory Cache Ratio Percent	Summary statistics of the ISA Server memory cache, including the memory cache usage ratio percentage.
Memory Cache Statistics	Summary statistics of the ISA Server memory cache, including the memory bytes retrieved rate.
Scheduled Cache Content Download CPU	Summary CPU statistics of the ISA Server Scheduled Cache Content Download process.
Scheduled Cache Content Download Memory	Summary memory statistics of the ISA Server Scheduled Cache Content Download process.

<b>Graph</b>	<b>Description</b>
Sites Granted/Denied Statistics	Summary statistics of the ISA Server Web Proxy, including the number of Web sites allowed access to client and the number of Web sites denied access to clients.
Web Proxy Average Milliseconds/request	Summary statistics of the ISA Server Web Proxy, including the average milliseconds per client request that has been made to the Web Proxy service.
Web Proxy Cache Hit Ratio Statistics	Summary statistics of the ISA Server Web Proxy, including the cache hit ratio percentage.
Web Proxy Client Bytes Statistics	Summary statistics of the ISA Server Web Proxy, including the rate at which data bytes have been sent and received by the Web proxy service to and from Web Proxy clients.
Web Proxy CPU	Summary CPU statistics of the ISA Server Web Proxy process.
Web Proxy Memory	Summary memory statistics of the ISA Server Web Proxy process.
Web Proxy Requests Statistics	Summary statistics of the ISA Server Web Proxy, including the number of failing client requests per second that have been made to the Web Proxy service.
Web Proxy Users Statistics	Summary statistics of the ISA Server Web Proxy, including the current number of Web proxy users.

# 5 Microsoft Enterprise Servers SPI for Microsoft Office SharePoint Server 2007

Microsoft Office SharePoint Server 2007 (MOSS) is a document repository system accessed through both a web and native client. MOSS provides formal processes for authoring and approval, to allow simple and reliable document versioning.

MOSS enables enterprises to develop an intelligent portal that seamlessly connects users, teams, and knowledge so that people can use information and work efficiently across business processes. This is possible by the integration of information from various systems into one solution, using single sign-on and enterprise application integration capabilities, and with flexible deployment options and management tools. The portal facilitates end-to-end collaboration by enabling aggregation, organization, and search capabilities for people, teams, and information. Users can find relevant information quickly through customization and personalization of portal content and layout, and by audience targeting. Organizations can target information, programs, and updates to audiences based on their organizational role, team membership, interest, security group, or any other membership criteria that can be defined.

MOSS has the following components:

- All the systems on which Microsoft Office SharePoint Server 2007 is installed.
- All components enabled on each system.
- Microsoft Office SharePoint Server 2007 Extended Virtual Servers and the systems which they are hosted on.
- Virtual server on which any site is hosted, (allows you to see the sites affected when a virtual server is unavailable).
- Content Databases, Configuration Databases, and SMTP servers and the dependency of these services on other components like IIS and Windows Operating System.
- All WSS sites and their content sources hosted by Microsoft Office SharePoint Server 2007, and their sub web (child) sites.
- Microsoft Office SharePoint Server 2007 Portal sites and the hierarchy of their member sites.

## Policies

The Microsoft Enterprise Servers SPI policies monitor the Microsoft Office Share Point Server 2007(MOSS). The policies offer the following monitoring processes:

- Availability Monitoring
- Service Monitoring
- Application Monitoring
- Server Logging
- Discovery

## Availability Monitoring

The availability monitoring group monitors the services of the Microsoft Office SharePoint Server 2007.

All the policies in the Availability Monitoring group belongs to the **Windows Management Interface** policy type and are available at the following location:

**SPI for Microsoft Enterprise Servers** → en → **SharePoint Portal Server** → **Microsoft Office SharePoint Server 2007** → **Auto-Deploy / Manual-Deploy**

The following table lists the details of the policies in the Availability Monitoring group.

Policy	Description
MSES_MOSS_AdminService	Monitors the Microsoft Office SharePoint Server 2007 admin service. If the service is stopped it can be restarted using operator-initiated action. The policy runs every 5 minutes.
MSES_MOSS_Document Conversions Load Balancer Service	Monitors the Document Conversions Load Balancer Service process. If the service is stopped it can be restarted using operator-initiated action. The policy runs every 5 minutes.
MSES_MOSS_Document Conversions Launcher Service	Monitors Document Conversions Launcher Service process. If the service is stopped it can be restarted using operator-initiated action. The policy runs every 5 minutes.
MSES_MOSS_OfficeServerSearchService	Monitors the Office Sharepoint server search. The policy runs every 5 minutes.
MSES_MOSS_SearchService	Monitors the Microsoft SharePoint 2007 Server search service. If the service is stopped it can be restarted using operator-initiated action. The policy runs every 5 minutes.
MSES_MOSS_TimerService	Monitors the Microsoft SharePoint 2007 Server timer service. If the service is stopped it can be restarted using operator-initiated action. The policy runs every 5 minutes.
MSES_MOSS_SingleSignOnService	Monitors the Microsoft SharePoint 2007 Server single sign-on service. If the service is stopped it can be restarted using operator-initiated action. The policy runs every 5 minutes.

## Service Monitoring

The service monitoring group monitors the available services of the Microsoft Office SharePoint Server 2007.

All the policies in the Service Monitoring group are available at the following location:

**SPI for Microsoft Enterprise Servers** → en → **SharePoint Portal Server** → **Microsoft Office SharePoint Server 2007** → **Auto-Deploy / Manual-Deploy**



The following table lists the details of the policies in the Service Monitoring group.

<b>Policy</b>	<b>Description</b>	<b>Policy Type</b>
MSES_MOSS-2k7_Database_Monitoring	Checks the status of the MOSS database instances. This policy runs every 30 minutes.	Scheduled Task policy
MSES_MOSS-2k7_Logical_Services_Monitoring	Checks the status of the MOSS logical services. This policy runs every 30 minutes.	Scheduled Task policy
MSES_MOSS_HeartBeats	Monitors the Microsoft SharePoint Portal Server 2007 Gatherer/Heartbeats counters. This policy runs every 5 minutes.	Measurement Threshold policy
MSES_MOSS_Documents Delayed Retry	Monitors the Documents Delayed Retry counter. This policy runs every 20 minutes.	Measurement Threshold policy
MSES_MOSS_Active Queue Length	Monitors the Active Queue Length. This policy runs every 10 minutes.	Measurement Threshold policy
MSES_MOSS_Reason To BackOff	Monitors the ReasonToBackOff counters. This policy runs every 20 minutes.	Measurement Threshold policy
MSES_MOSS_IndexerCatalogsNumOfDocuments	Monitors the increase in the number of documents indexed. This policy runs every 12 hours.	Measurement Threshold policy

## Application Monitoring

The application monitoring group monitors the available applications of the Microsoft Office SharePoint Server 2007.

All the policies in the Application Monitoring group belong to the **Windows Event Log** policy type and are available at the following location:

**SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office SharePoint Server 2007 → Auto-Deploy / Manual-Deploy**

The following table lists the policies in the Application Monitoring group.

<b>Policy</b>	<b>Description</b>
MSES_MOSS_FwdApplicationError	Handles all error messages from all Microsoft Office SharePoint services.
MSES_MOSS_FwdApplicationInformation	Handles information from all Microsoft Office SharePoint services.
MSES_MOSS_FwdApplicationWarning	Handles the warning messages from all Microsoft Office SharePoint services.

## Server Logging

In server logging group the following metrics are collected for all the processes mentioned under logging.

Metric Name	Data Type
Instance Name	Text
Working Set	Real64
Page Faults per sec	Real64
Private Bytes	Real64
Thread Count	Real64
Processor Time (%)	Real64

The monitoring group includes the following policies:

- MSES\_MOSS-2k7\_Logging\_Process\_MOSS.Conversions.LoadBalancer
- MSES\_MOSS-2k7\_Logging\_Process\_MOSS.Conversions.Launcher
- MSES\_MOSS-2k7\_Logging\_Process\_WSSTRACING
- MSES\_MOSS-2k7\_Logging\_Process\_MSSEARCH
- MSES\_MOSS-2k7\_Logging\_Process\_OWSTIMER
- MSES\_MOSS-2k7\_Logging\_Process\_SPWRITER
- MSES\_MOSS-2k7\_Logging\_Process\_SSOSRV
- MSES\_MOSS-2k7\_Logging\_Process\_W3WP
- MSES\_MOSS-2k7\_CreateCodeDataSources
- MSES\_MOSS-2k7\_Logging\_Process\_WSSADMIN

The policies are available at the following location:

**SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office SharePoint Server 2007 → Auto-Deploy / Manual-Deploy**

**Table 1 MSES\_MOSS-2k7\_Logging\_Process\_MOSS.Conversions.LoadBalancer**

Metric	Descriptions
Policy	MSES_MOSS-2k7_Logging_Process_MOSS.Conversions.LoadBalancer
Description	Collects data for Microsoft Office Server Conversions LoadBalancer.
Service Name	Office Document Conversions Load Balancer Service
Monitored Process	Micorsoft.Office.Server.conversions.LoadBalancer.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 2 MSES\_MOSS-2k7\_Logging\_Process\_MOSS.Conversions.Launcher**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_MOSS.Conversions.Launcher
Description	Collects data for conversions.Launcher process.
Service Name	Office Document Conversions Launcher Service
Monitored Process	Microsoft.Office.Server.Conversions.Launcher.exe
Schedule	This policy runs every 5 minutes daily.
Policy Type	Measurement Threshold policy

**Table 3 MSES\_MOSS-2k7\_Logging\_Process\_WSSTRACING**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_WSSTRACING
Description	Collects data for the WSSTRACING process.
Service Name	Windows SharePoint Services Tracing
Monitored Process	wsstracing.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 4 MSES\_MOSS-2k7\_Logging\_Process\_MSSEARCH**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_MSSEARCH
Description	Collects data for the MSSEARCH process.
Service Name	Windows SharePoint Services Search
Monitored Process	mssearch.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 5 MSES\_MOSS-2k7\_Logging\_Process\_OWSTIMER**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_OWSTIMER
Description	Collects data for the OWSTIMER process.
Service Name	Windows SharePoint Services Timer

<b>Metric</b>	<b>Descriptions</b>
Monitored Process	owstimer.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 6 MSES\_MOSS-2k7\_Logging\_Process\_SPWRITER**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_SPWRITER
Description	Collects data for the SPWRITER process.
Service Name	Windows SharePoint Services VSS Writer
Monitored Process	spwriter.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 7 MSES\_MOSS-2k7\_Logging\_Process\_SSOSRV**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_SSOSRV
Description	Collects data for the SSOSRV process.
Service Name	Microsoft Single Sign-on Service
Monitored Process	ssosrv.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 8 MSES\_MOSS-2k7\_Logging\_Process\_w3wp**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_w3wp
Description	Collects data for the w3wp process.
Service Name	Windows IIS worker process
Monitored Process	w3wp.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy



Ensure that the MSES\_MOSS-2k7\_CreateCodaDataSources policy is deployed to create data sources before you deploy the Server Logging policies.

**Table 9 MSES\_MOSS-2k7\_CreateCodaDataSources**

Metric	Descriptions
Policy	MSES_MOSS-2k7_CreateCodaDataSources
Description	Creates the data source for logging data.
Schedule	This policy runs every 30 minutes
Policy Type	Scheduled Task policy

**Table 10 MSES\_MOSS-2k7\_Logging\_Process\_WSSADMIN**

Metric	Descriptions
Policy	MSES_MOSS-2k7_Logging_Process_WSSADMIN
Description	Collects data for the WSSADMIN process.
Service Name	Microsoft SharePoint Administration Service
Monitored Process	wssadmin.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

## Discovery

The Discovery group discovers the services of the Microsoft Office SharePoint Server 2007. The monitoring group includes the Microsoft Office SharePoint Server 2007 Discovery policy.

Policy	Description	Policy Type	Policy Group
Microsoft Office SharePoint Server 2007 Discovery	Discovers the services of the Microsoft Office SharePoint Server 2007	Service Auto-Discovery policy	<b>SPI for Microsoft Enterprise Servers → en → SharePoint Portal Server → Microsoft Office SharePoint Server 2007 → Discovery</b>

## Reports

Following are the reports for the Microsoft Office SharePoint Server 2007.

### Memory and CPU reports

You can use the memory and CPU reports to plan and predict capacity of the Microsoft Office SharePoint Server 2007 deployment. The reports can assist in determining whether an additional search server or Web front end server needs to be added to improve the performance.



You must deploy the MSES\_MOSS-2K7\_Logging\_Process\_MSSEARCH policy for this report to function correctly.

**Daily/Weekly CPU Usage Summary (g\_MOSS2k7CPUSummary.rpt/  
g\_MOSS2k7CPUWeeklySummary.rpt)**

The report shows summary CPU statistics of MOSS 2007 server's services installed nodes in an enterprise deployment. The displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. This reports provide the administrators an overview of which server is heavily loaded and which process is causing much load.

**Daily/Weekly Memory Usage Summary (g\_MOSS2k7MemorySummary.rpt/  
g\_MOSS2k7MemoryWeeklySummary.rpt)**

The report shows summary CPU statistics of MOSS 2007 server's services installed nodes in an enterprise deployment. The data displays for every six hours over the last 7 days, compared with overall CPU statistics of the system, in both graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the services.

**IIS Worker Process reports**

**Weekly Summary of IIS Worker Process CPU Usage  
(g\_MOSS2k7\_IIS\_CPUWeeklySummary.rpt)**

The report shows the size of each index, total free space, and total used space left on each of the SharePoint Portal Server 2003 Indexing servers. The report shows data points and charts for every 12 hours in each day over the past seven days.



You must deploy the *MSES\_MOSS-2K7\_Logging\_Process\_MSSEARCH* policy for this report to function correctly.

**Graphs**

The following predefined graphs for Microsoft Office SharePoint Server 2007 are available with the Microsoft Enterprise Servers SPI:

<b>Graph</b>	<b>Description</b>
SharePoint Server Admin service CPU usage	Shows summary CPU statistics of the SharePoint admin service process (spsadmin.exe). The data can be compared with System Processor Time to determine the extent to which the SharePoint admin service is utilizing processor time.
SharePoint Portal Server Admin service Memory usage	Shows summary memory statistics of the SharePoint admin service process (spsadmin.exe). The summarized process statistics show private bytes, and working set used by the process. <b>Counters:</b> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> </ul>
SharePoint Portal Server Search Service CPU usage	Shows summary CPU statistics of the SharePoint search service process (mssearch.exe). The data can be compared with System Processor Time to determine the extent to which the SharePoint admin service is utilizing processor time.

<b>Graph</b>	<b>Description</b>
SharePoint Portal Server Search Service Memory usages	Shows summary memory statistics of the SharePoint search service process (mssearch.exe). The summarized process statistics include the private bytes, and working set used by the process. <b>Counters:</b> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> </ul>
SharePoint Search Service Page Faults/sec	Shows summary memory statistics of the SharePoint Search service process (mssearch.exe). The summarized process statistics include the Page Faults\sec by the process. <b>Counter:</b> Process:Page Faults\sec
SharePoint Portal Server SingleSignon Service CPU usage	Shows summary CPU statistics of the SharePoint Single sign on service process (SSOSRV.exe). This data can be compared with System Processor Time to determine the extent to which the SharePoint Single sign on service is utilizing processor time.
SharePoint Portal Server SingleSignon Service Memory usage	Shows summary memory statistics of the SharePoint single sign on service process (SSOSRV.exe). The summarized process statistics include the private bytes, and working set used by the process. <b>Counters:</b> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> <li>• SharePoint Portal Server SPTimer Service CPU Usage</li> </ul>
SharePoint Portal Server SPTimer Service CPU Usage	Shows summary CPU statistics of the SharePoint SPTimer service process (OWSTIMER.exe). This data can be compared with System Processor Time to determine the extent to which the SharePoint SPTimer service is utilizing processor time.
SharePoint Portal Server SPTimer Service Memory usage	Shows summary memory statistics of the SharePoint SPTimer service process (OWSTIMER.exe). The summarized process statistics include the private bytes and working set used by the process. <b>Counters:</b> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set, Process</li> </ul>

<b>Graph</b>	<b>Description</b>
IIS Worker process CPU usage	This graph shows summary CPU statistics of the IIS worker process service (w3wp.exe). This data can be compared with System Processor Time to determine to what extent the IIS worker process service is utilizing processor time, which can be used in making decisions about whether to add additional web front end servers.
IIS Worker process Memory usage	This graph shows summary memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the private bytes and working set used by the process. <b>Counters:</b> Process.Private Bytes Process.Working Set
IIS Worker processes Page Faults	This graph shows summary memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the Page Faults \sec by the process. <b>Counters:</b> Process:Page Faults \sec



# 6 Microsoft Enterprise Servers SPI for Microsoft SharePoint Server 2010

Microsoft SharePoint 2010 is designed to replace and maintain the web requirements of your organization. It manages and provides improved functionalities like intranet and extranet portals, document and file management, and tools for social networking and business intelligence.

## Policies

The Microsoft Enterprise Servers SPI policies monitor the Microsoft SharePoint 2010 Server. The policies offer the following monitoring processes:

- Availability Monitoring
- Service Monitoring
- Application Monitoring
- Server Logging
- Discovery

### Availability Monitoring

The Availability Monitoring group monitors the services of the Microsoft SharePoint Server 2010.

All the policies in the Availability Monitoring group belongs to the **Windows Management Interface** policy type and are available at the following location:

**SPI for Microsoft Enterprise Servers** → **en** → **SharePoint Portal Server** → **SharePoint Server 2010** → **Manual-Deploy**

The following table lists the details of the policies in the Availability Monitoring group.

Policy	Description
MSES_SPS_14_AdminService	Monitors the SharePoint 2010 Administration Service. The policy runs every 5 minutes.
MSES_SPS_14_Document Conversions Load Balancer Service	Monitors the Document Conversions Load Balancer for Microsoft SharePoint Server 2010 service. The policy runs every 5 minutes.
MSES_SPS_14_Document Conversions Launcher Service	Monitors Document Conversions Launcher Service process. The policy runs every 5 minutes.

<b>Policy</b>	<b>Description</b>
MSES_SPS_14_OfficeServerSearchService	Monitors the SharePoint Server Search 14 service. The policy runs every 5 minutes.
MSES_SPS_14MOSS_SearchService	Monitors the SharePoint Foundation Search V4. The policy runs every 5 minutes.
MSES_SPS_14_TimerService	Monitors the SharePoint 2010 Timer Service. The policy runs every 5 minutes.



If any of the services are stopped it can be restarted using the operator-initiated action.

## Service Monitoring

The Service Monitoring group monitors the available services of the Microsoft SharePoint Server 2010.

All the policies in the Service Monitoring group are available at the following location:

**SPI for Microsoft Enterprise Servers** → en → **SharePoint Portal Server** → **SharePoint Server 2010** → **Manual-Deploy**

The following table lists the details of the policies in the Service Monitoring group.

<b>Policy</b>	<b>Description</b>	<b>Policy Type</b>
MSES_SPS_14_Database_Monitoring	This policy monitors the Sharepoint Server 2010 databases. This policy runs every 30 minutes.	Scheduled Task policy
MSES_SPS_14_LogicalServices_Monitoring	This policy checks the status of the SharePoint 2010 Server logical services. This policy runs every 30 minutes.	Scheduled Task policy
MSES_SPS_14_HeartBeats	This policy monitors the Sharepoint Foundation Search Gatherer/Heartbeats counter. This policy runs every 5 minutes.	Measurement Threshold policy
MSES_SPS_14_Documents Delayed Retry	This policy monitors Sharepoint Foundation Search Gatherer/Documents Delayed Retry counter. This policy runs every 20 minutes.	Measurement Threshold policy
MSES_SPS_14_Active Queue Length	This policy monitors the Sharepoint Foundation Search Gatherer/Active Queue Length counter. This policy runs every 10 minutes.	Measurement Threshold policy
MSES_SPS_14_ReasonToBackOff	This policy monitors the Sharepoint Foundation Search Gatherer/Reason To Back Off Counter counters. This policy runs every 20 minutes.	Measurement Threshold policy
MSES_SPS_14_IndexCatalogsNumofDocuments	This policy monitors the increase in the number of documents indexed. This policy runs every 12 hours.	Measurement Threshold policy

## Application Monitoring

The Application Monitoring group monitors the available applications of the Microsoft Office SharePoint Server 2010.

All the policies in the Application Monitoring group belong to the **Windows Event Log** policy type and are available at the following location:

**SPI for Microsoft Enterprise Servers** → en → **SharePoint Portal Server** → **SharePoint Server 2010** → **Manual-Deploy**

The following table lists the policies in the Application Monitoring group.

Policy	Description
MSES_SPS_14_FwdApplicationError	This policy handles all error messages from all MicrosoftSharePoint 2010 services. This policy runs every 30 minutes.
MSES_SPS_14_FwdApplicationWarning	This policy handles the warning messages from all Microsoft SharePoint 2010 services. This policy runs every 30 minutes.

## Server Logging

In Server Logging group the following metrics are collected for all the processes mentioned under logging.

Metric Name	Data Type
Instance Name	Text
Working Set	Real64
Page Faults per sec	Real64
Private Bytes	Real64
Thread Count	Real64
Processor Time (%)	Real64

The monitoring group includes the following policies:

- MSES\_SPS\_14\_Logging\_Process\_SPS.Conversions.LoadBalancer
- MSES\_SPS\_14\_Logging\_Process\_SPS.Conversions.Launcher
- MSES\_SPS\_14\_Logging\_Process\_WSSTRACING
- MSES\_SPS\_14\_Logging\_Process\_MSSEARCH
- MSES\_SPS\_14\_Logging\_Process\_OWSTIMER
- MSES\_SPS\_14\_Logging\_Process\_SPWRITER
- MSES\_SPS\_14\_Logging\_Process\_W3WP
- MSES\_SPS\_14\_Logging\_Process\_WSSADMIN

The policies are available at the following location:

**Table 11 MSES\_SPS\_14\_Logging\_Process\_SPS.Conversions.LoadBalancer**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_SPS.Conversions.LoadBalancer
Description	This policy collects data for the SPS 2010, Microsoft.Office.Server.Conversions.LoadBalancer process.
Service Name	Document Conversions Load Balancer for Microsoft SharePoint Server 2010
Monitored Process	Microsoft.Office.Server.Conversions.LoadBalancer.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 12 MSES\_SPS\_14\_Logging\_Process\_SPS.Conversions.Launcher**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_SPS.Conversions.Launcher
Description	This policy collects data for the Microsoft SharePoint Server 2010 process, Microsoft.Office.Server.Conversions.Launcher.
Service Name	Document Conversions Launcher for Microsoft SharePoint Server 2010
Monitored Process	Microsoft.Office.Server.Conversions.Launcher.exe
Schedule	This policy runs every 5 minutes daily.
Policy Type	Measurement Threshold policy

**Table 13 MSES\_SPS\_14\_Logging\_Process\_WSSTRACING**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_WSSTRACING
Description	This policy collects data for the Microsoft SharePoint Server 2010 process, WSSTRACING.
Service Name	SharePoint 2010 Tracing
Monitored Process	wsstracing.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 14 MSES\_SPS\_14\_Logging\_Process\_MSSEARCH**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_MSSEARCH
Description	This policy collects data for the Microsoft SharePoint 2010 process, MSSEARCH.
Service Name	Microsoft SharePoint Portal Server Search Service
Monitored Process	MSSEARCH.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 15 MSES\_SPS\_14\_Logging\_Process\_OWSTIMER**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_MOSS-2k7_Logging_Process_OWSTIMER
Description	This policy collects data for the Microsoft SharePoint 2010 process, OWSTIMER.
Service Name	SharePoint Foundation Timer
Monitored Process	OWSTIMER.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 16 MSES\_SPS\_14\_Logging\_Process\_SPWRITER**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_SPWRITER
Description	This policy collects data for the Microsoft SharePoint Server 2010 process, SPWRITER.
Service Name	SharePoint 2010 VSS Writer
Monitored Process	SPWRITER.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 17 MSES\_SPS\_14\_Logging\_Process\_w3wp**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_w3wp
Description	This policy collects data for the Microsoft SharePoint Server 2010 process, w3wp.
Service Name	IIS worker process

<b>Metric</b>	<b>Descriptions</b>
Monitored Process	w3wp.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

**Table 18 MSES\_SPS\_14\_Logging\_Process\_WSSADMIN**

<b>Metric</b>	<b>Descriptions</b>
Policy	MSES_SPS_14_Logging_Process_WSSADMIN
Description	This policy collects data for the Microsoft SharePoint Server 2010 process, WSSADMIN.
Service Name	SharePoint Administration Service
Monitored Process	WSSADMIN.exe
Schedule	This policy runs every 5 minutes.
Policy Type	Measurement Threshold policy

## Discovery

The Discovery group discovers the services of the Microsoft SharePoint Server 2010. The monitoring group includes the Microsoft SharePoint Server 2010 Discovery policy.

<b>Policy</b>	<b>Description</b>	<b>Policy Type</b>	<b>Policy Group</b>
Sharepoint_Discovery	Discovers the SharePoint environment.	Service Auto-Discovery policy	<b>SPI for Microsoft Enterprise Servers</b> → <b>en</b> → <b>SharePoint Portal Server</b> → <b>SharePoint Server 2010</b> → <b>Discovery</b>

## Reports

The reports for the Microsoft SharePoint Server 2010 are as listed in the following section.

### Memory and CPU reports

You can use the memory and CPU reports to plan and predict capacity of the Microsoft Office SharePoint Server 2010 deployment. .



You must deploy the MSES\_SPS\_14\_Logging\_Process\_MSSEARCH policy for the following reports to function correctly.

#### **SP2k10CPUSummary**

The SP2k10CPUSummary report shows the summary of the CPU statistics of SharePoint Server Search process compared with the overall CPU statistics of the system, in graphical and tabular format.

### **SP2k10CPUWeeklySummary**

The SP2k10CPUWeeklySummary report shows the weekly summary of the CPU statistics of SharePoint Server Search process compared with the overall CPU statistics of the system, in graphical and tabular format.

### **SP2k10MemorySummary**

The SP2k10MemorySummary report shows a summary of the memory statistics of the SharePoint Server Search process in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the mssearch process.

### **SP2k10MemoryWeeklySummary**

The SP2k10MemoryWeeklySummary report shows a weekly summary of the memory statistics of the SharePoint Portal Server processes in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the mssearch process.

## **IIS Worker Process reports**



You must deploy the MSES\_SPS\_14\_Logging\_Process\_w3wp policy for this report to function correctly.

### **SP2k10WeeklyIISCPUSummary**

The SP2k10WeeklyIISCPUSummary report shows a summary of the CPU statistics of the IIS worker processes for Front End web servers of a SharePoint Portal Server deployment. The IIS worker processes CPU utilization is compared with overall system CPU utilization.

# Graphs

The following predefined graphs for Microsoft SharePoint Server 2010 are available with the Microsoft Enterprise Servers SPI:

Graph	Description
SharePoint Server Admin Service CPU	<p>The SharePoint Server Admin Service CPU graph shows the summary CPU statistics of the SharePoint admin service process (wssadmin.exe).</p> <p>This data can be compared with System Processor Time to determine the extent to which the SharePoint admin service is utilizing processor time.</p>
SharePoint Server Admin Service Memory Usage	<p>The SharePoint Server Admin Service Memory Usage graph shows the summary of memory statistics of the SharePoint admin service process (wssadmin.exe). The summarized process statistics show private bytes, and working set used by the process.</p> <p><b>Counters:</b></p> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> </ul>
SharePoint Server Search Service CPU	<p>The SharePoint Server Search Service CPU graph shows a summary of the CPU statistics of the SharePoint search service process (mssearch.exe). This data can be compared with System Processor Time to determine the extent to which the SharePoint admin service is utilizing processor time.</p>
SharePoint Server Search Service Memory	<p>The SharePoint Server Search Service Memory graph shows a summary of the memory statistics of the SharePoint search service process (mssearch.exe). The summarized process statistics include the private bytes, and working set used by the process.</p> <p><b>Counters:</b></p> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> </ul>
SharePoint Search Service Page Faults/sec	<p>The SharePoint Search Service Page Faults/sec graph shows a summary of the memory statistics of the SharePoint Search service process (mssearch.exe). The summarized process statistics include the Page Faults/sec by the process.</p> <p><b>Counter:</b></p> <p>Process:Page Faults/sec</p>
SharePoint Server SPTimer Service CPU	<p>The SharePoint Server SPTimer Service CPU graph shows a summary of the CPU statistics of the SharePoint SPTimer service process (OWSTIMER.exe). This data can be compared with System Processor Time to determine the extent to which the SharePoint SPTimer service is utilizing processor time.</p>



<b>Graph</b>	<b>Description</b>
SharePoint Server SPTimer Service Memory	<p>The SharePoint Server SPTimer Service Memory graph shows a summary of the memory statistics of the SharePoint SPTimer service process (OWSTIMER.exe). The summarized process statistics include the private bytes and working set used by the process.</p> <p><b>Counters:</b></p> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> </ul>
IIS Worker process CPU usage	<p>The IIS Worker process CPU usage graph shows a summary of the CPU statistics of the IIS worker process service (w3wp.exe). This data can be compared with System Processor Time to determine the extent to which the IIS worker process service is utilizing processor time, which can be used in making decisions about whether to add additional web front end servers.</p>
IIS Worker process Memory usage	<p>The IIS Worker process Memory usage graph shows a summary of the memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the private bytes and working set used by the process.</p> <p><b>Counters:</b></p> <ul style="list-style-type: none"> <li>• Process.Private Bytes</li> <li>• Process.Working Set</li> </ul>
IIS Worker processes Page Faults	<p>This graph shows a summary of the memory statistics of the IIS worker process service (w3wp.exe). The summarized process statistics include the Page Faults/sec by the process.</p> <p><b>Counter:</b></p> <p>Process:Page Faults/sec.</p>



---

# 7 Microsoft Enterprise Servers SPI for Office Communications Server 2007

The Microsoft Enterprise Servers SPI monitors the Microsoft Office Communications Server 2007 and 2007 R2 and helps in unhindered flow of communications within the enterprises. The Microsoft Enterprise Servers SPI offers the following policies for process monitoring and service management, and for logging data used by Office Communications Server (OCS) 2007 reports and graphs.

## Policies

The OCS has the following policy groups:

- Discovery
- AccessEdgeServer
- Archiving CDR Server
- AVConfServer
- AVEdgeServer
- Configuration
- CWAServer
- FrontEnd Server
- IMConfServer
- Mediation Server
- TelConfServer
- WebCompServer
- WebConfServer
- WebEdgeServer
- Others

## Discovery

The Discovery policy group contains the OCS\_Discovery policy which discovers the OCS roles and services. The policy discovers the following OCS roles and services:

### Roles

- A/V edge server
- Access edge server
- Web conferencing edge server

- Instant Messaging Conferencing Server
- Telephony Conferencing Server
- Web conferencing server
- A/V conferencing server
- Communicator Web Access
- Archiving and CDR Server
- Mediation server
- Web Components Server

### Services

- Front End Service
- Audio/Video Conferencing service
- IM Conferencing service
- Telephony Conferencing Service
- Web Conferencing Service
- Archiving and CDR service
- Audio/Video Authentication service
- Audio/Video Edge service
- Access Edge service
- Web Conferencing Edge service
- Mediation service

If the node, to which the policy is deployed, is a member of an OCS pool, then the pool, pool type (standard/enterprise), and members of the pool are also discovered by the policy. If the agent is not running under the default account (Local System account) on the managed node, then you must create a user, who is a member of the RTCUniversalGuestAccessGroup, if the node is a member of the OCS pool. For Edge Servers, provide the privileges of a Local Administrator.

Edit the username and password in the policy and enter the credentials of this user. Save and close the policy and deploy the edited policy to the node.

The username format for **HTTPS** is domain\user

Policy	Description	Policy Type	Policy Group
OCS_Discovery	Discovers the OCS roles and services.	Service Auto-Discovery	<b>SPI for Microsoft Enterprise Servers → en Microsoft_Office_Communications_Server → Microsoft_Office_Communications_Server_2007 → Discovery</b>

## AccessEdgeServer

The Access Edge Server is located in the perimeter network. It validates incoming SIP traffic and forwards the IM traffic between internal and external users. In Live Communications Server 2005, it is called the Access Proxy.

The Access Edge Server and Web Edge Server can be configured on the same server. The A/V Edge Server can also be configured on the same server.

## Policies deployed on OCS 2007 and OCS 2007 R2


All the policies that can be deployed on both OCS 2007 and OCS 2007 R2 are available at **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AccessEdgeServer**

The policies belong to the **Measurement Threshold** policy type.

The following policies can be deployed on OCS 2007 and OCS 2007 R2.

### OCS\_AccessEdgeServer\_Logging

The OCS\_AccessEdgeServer\_Logging policy logs the following metrics as mentioned in the table into the data store (CODA / HP Performance Agent) for the instance **\_Total**. If a metric value is unavailable, this policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).

-  Ensure that the OCS\_CreateDataSources policy is running before you deploy the OCS\_AccessEdgeServer\_Logging policy.

<b>Policy</b>	OCS_AccessEdgeServer_Logging Policy
<b>Name</b>	OCS_AccessEdgeServer_Logging
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Counter</b>	SIP - 021 - Average Incoming Message Processing Time
<b>Data Class</b>	OCS_ACCESSEEDGE
<b>Instance</b>	_Total

### OCS\_AccessEdgeServer\_FlowControlledConnectionsDropped Policy

<b>Policy</b>	OCS_AccessEdgeServer_FlowControlledConnectionsDropped Policy
<b>Name</b>	OCS_AccessEdgeServer_FlowControlledConnectionsDropped
<b>Description</b>	Monitors the total number of connections dropped because of excessive flow-control.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter:</b>	SIP - 024 - Flow-controlled Connections Dropped

<b>Policy</b>	OCS_AccessEdgeServer_FlowControlledConnectionsDropped Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

#### OCS\_AccessEdgeServer\_AddressSpaceUsage Policy

<b>Policy</b>	OCS_AccessEdgeServer_AddressSpaceUsage Policy
<b>Name</b>	OCS_AccessEdgeServer_AddressSpaceUsage
<b>Description</b>	Monitors the percentage of available address space currently in use by the server process.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 07 - Load Management
<b>Counter</b>	SIP - 009 - Address space usage
<b>Warning</b>	65
<b>Critical</b>	75

#### OCS\_AccessEdgeService\_PrivateBytes Policy

<b>Policy</b>	OCS_AccessEdgeService_PrivateBytes Policy
<b>Name</b>	OCS_AccessEdgeService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

### OCS\_Check\_AccessEdgeServiceStatus Policy

<b>Policy</b>	OCS_Check_AccessEdgeServiceStatus Policy
<b>Name</b>	OCS_Check_AccessEdgeServiceStatus
<b>Description</b>	Checks the status of the Access Edge Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCSrv

### OCS\_AccessEdgeServer\_ActiveTLSConnections Policy

<b>Policy</b>	OCS_AccessEdgeServer_ActiveTLSConnections Policy
<b>Name</b>	OCS_AccessEdgeServer_ActiveTLSConnections
<b>Description</b>	Monitors the number of established TLS connections that are currently active. TLS Connection is considered established when peer certificate and, possibly, host name are verified for trust relationship.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:API - 00 - API Application Instance Counters
<b>Instance</b>	_TotalCounter
<b>Counter</b>	API - 026 - Transactions Pending Dispatch Completion
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 500 <b>Critical:</b> 1000

### OCS\_AccessEdgeServer\_MsgsDroppedPerSecDueToCertMismatch Policy

<b>Policy</b>	OCS_AccessEdgeServer_MsgsDroppedPerSecDueToCertMismatch Policy
<b>Name</b>	OCS_AccessEdgeServer_MsgsDroppedPerSecDueToCertMismatch
<b>Description</b>	Monitors the number of messages dropped per second because the remote peer's certificate did not contain a matching FQDN.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_AccessEdgeServer_MsgsDroppedPerSecDueToCertMismatch Policy
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Counter</b>	SIP - 011 - Messages/sec Dropped Due To Certificate Mismatch
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_AccessEdgeServer\_RejectedExtEdgeServerConnectionsPerSec Policy

<b>Policy</b>	OCS_AccessEdgeServer_RejectedExtEdgeServerConnectionsPerSec Policy
<b>Name</b>	OCS_AccessEdgeServer_RejectedExtEdgeServerConnectionsPerSec
<b>Description</b>	Monitors the number of messages dropped per second because the remote peer's certificate did not contain a matching FQDN.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 08 - Access Edge Server Connections
<b>Counter</b>	SIP - 013 - Rejected External Edge Server Connections/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_AccessEdgeServer\_SendsTimedOut Policy

<b>Policy</b>	OCS_AccessEdgeServer_SendsTimedOut Policy
<b>Name</b>	OCS_AccessEdgeServer_SendsTimedOut
<b>Description</b>	Monitors the total number of sends dropped because they stayed in the outgoing (send) queue for too long.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 018 - Sends Timed-Out
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 500 <b>Critical:</b> 1000



### OCS\_AccessEdgeServer\_IncomingResponsesDroppedPerSec Policy

<b>Policy</b>	OCS_AccessEdgeServer_IncomingResponsesDroppedPerSec Policy
<b>Name</b>	OCS_AccessEdgeServer_IncomingResponsesDroppedPerSec
<b>Description</b>	Monitors the number of incoming responses dropped per second because they could not be processed (due to bad headers, insufficient routing information, server resource allocation failure).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 02 - Protocol
<b>Counter</b>	SIP - 005 - Incoming Responses Dropped/sec
<b>Threshold</b>	Configuration recommended

### OCS\_AccessEdgeService\_WorkingSet Policy

<b>Policy</b>	OCS_AccessEdgeService_WorkingSet Policy
<b>Name</b>	OCS_AccessEdgeService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

### OCS\_AccessEdgeServer\_MsgPerSecDroppedDueToUnknownDomain Policy

<b>Policy</b>	OCS_AccessEdgeServer_MsgPerSecDroppedDueToUnknownDomain
<b>Name</b>	OCS_AccessEdgeServer_MsgPerSecDroppedDueToUnknownDomain
<b>Description</b>	Monitors the number of messages that could not be routed per second because the message domain is not in the routing table.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_AccessEdgeServer_MsgPerSecDroppedDueToUnknownDomain
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 021 - Messages/sec Dropped Due To Unknown Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_AccessEdgeServer\_FlowControlledConnections Policy

<b>Policy</b>	OCS_AccessEdgeServer_FlowControlledConnections Policy
<b>Name</b>	OCS_AccessEdgeServer_FlowControlledConnections
<b>Description</b>	Monitors the number of connections that are currently being flow-controlled (no socket receives are posted).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 023 - Flow-controlled Connections
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_AccessEdgeService\_ThreadCount Policy

<b>Policy</b>	OCS_AccessEdgeService_ThreadCount Policy
<b>Name</b>	OCS_AccessEdgeService_ThreadCount
<b>Description</b>	Monitors the number of connections that are currently being flow-controlled (no socket receives are posted).
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

### OCS\_AccessEdgeServer\_RejectedExtEdgeClientConnectionsPerSec Policy

<b>Policy</b>	OCS_AccessEdgeServer_RejectedExtEdgeClientConnectionsPerSec Policy
<b>Name</b>	OCS_AccessEdgeServer_RejectedExtEdgeClientConnectionsPerSec
<b>Description</b>	Monitors the number of client connections rejected at the external edge per second because remote user access is disabled.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 08 - Access Edge Server Connections
<b>Counter</b>	SIP - 015 - Rejected External Edge Client Connections/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_AccessEdgeService\_Logging Policy

<b>Policy</b>	OCS_AccessEdgeService_Logging Policy
<b>Name</b>	OCS_AccessEdgeService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances RTCSrv or _Total. If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS



Ensure that the OCS\_CreateDataSources policy is running before you deploy the OCS\_AccessEdgeService\_Logging policy.

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	Processor \ % Processor Time

### OCS\_AccessEdgeService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_AccessEdgeService_PageFaultsPerSec Policy
<b>Name</b>	OCS_AccessEdgeService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToBlockedDomain Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedDomain Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedDomain
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain is in the blocked list.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 027 - External Messages/sec Dropped Due To Blocked Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_AccessEdgeServer\_MessagesInServer Policy

<b>Policy</b>	OCS_AccessEdgeServer_MessagesInServer Policy
<b>Name</b>	OCS_AccessEdgeServer_MessagesInServer
<b>Description</b>	Monitors the number of messages currently being processed by the server.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_AccessEdgeServer_MessagesInServer Policy
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Counter</b>	SIP - 012 - Messages In Server
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 2500 <b>Critical:</b> 5000

#### OCS\_AccessEdgeServer\_AverageIncomingMessageProcessingTime Policy

<b>Policy</b>	OCS_AccessEdgeServer_AverageIncomingMessageProcessingTime Policy
<b>Name</b>	OCS_AccessEdgeServer_AverageIncomingMessageProcessingTime
<b>Description</b>	Monitors the average time (in seconds) it takes to process an incoming message.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Counter</b>	SIP - 021 - Average Incoming Message Processing Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 3 <b>Critical:</b> 5

#### OCS\_AccessEdgeService\_ProcessorTime Policy

<b>Policy</b>	OCS_AccessEdgeService_ProcessorTime Policy
<b>Name</b>	OCS_AccessEdgeService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

### OCS\_AccessEdgeServer\_IncomingRequestsDroppedPerSec Policy

<b>Policy</b>	OCS_AccessEdgeServer_IncomingRequestsDroppedPerSec Policy
<b>Name</b>	OCS_AccessEdgeServer_IncomingRequestsDroppedPerSec
<b>Description</b>	Monitors the number of incoming requests dropped per second because they could not be processed (due to bad headers, insufficient routing information, server resource allocation failure).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 02 - Protocol
<b>Counter</b>	SIP - 005 - Incoming Requests Dropped/sec
<b>Threshold</b>	Configuration recommended

### OCS\_AccessEdgeServer\_AboveLimitConnectionsDropped Policy

<b>Policy</b>	OCS_AccessEdgeServer_AboveLimitConnectionsDropped Policy
<b>Name</b>	OCS_AccessEdgeServer_AboveLimitConnectionsDropped
<b>Description</b>	Monitors the total number of connections that were dropped because the limit on number of incoming connections from a federated partner or clearinghouse was exceeded.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 004 - Above Limit Connections Dropped (Access Proxies only)
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 1 <b>Critical:</b> 2

### OCS\_AccessEdgeServer\_IncomingMsgHeldAboveOverloadWatermark Policy

<b>Policy</b>	OCS_AccessEdgeServer_IncomingMsgHeldAboveOverloadWatermark Policy
<b>Name</b>	OCS_AccessEdgeServer_IncomingMsgHeldAboveOverloadWatermark
<b>Description</b>	Monitors the number of incoming messages currently being held by the server for processing for more than the overload watermark time threshold.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_AccessEdgeServer_IncomingMsgHeldAboveOverloadWatermark Policy
<b>Performance Object</b>	LC:SIP - 07 - Load Management
<b>Counter</b>	SIP - 004 - Incoming Messages Held Above Overload Watermark
<b>Threshold</b>	Configuration recommended

### Policies deployed only on OCS 2007

The policies that can be deployed only on the OCS 2007 server are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AccessEdgeServer** → **OCS2007**

All the policies that can be deployed only on OCS 2007 belong to the **Measurement Threshold** policy type.

#### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToUnresolvedDomain Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnresolvedDomain Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnresolvedDomain
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain failed to resolve by DNS SRV.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 053 - External Messages/sec Dropped Due To Unresolved Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToIncompMsgDomain Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the federation type of the domain is incompatible with previous messages.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain Policy
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 061 - External Messages/sec Dropped Due To Incompatible Message Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToUnauthIMDomain Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnauthIMDomain Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnauthIMDomain
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain did not resolve by DNS SRV to the connection peer FQDN.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 057 - External Messages/sec Dropped Due To Unauthorized IM Service Provider Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### CS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToBlockedIMDomain Policy

<b>Policy</b>	CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain Policy
<b>Name</b>	CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain resolved by DNS SRV to a server that is blocked in the IM Service Providers table.
<b>Schedule</b>	This policy runs every 15 minutes.



<b>Policy</b>	CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain Policy
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 055 - External Messages/sec Dropped Due To Blocked IM Service Provider Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

### Policies deployed only on OCS 2007 R2

The policies that can be deployed only on the OCS 2007 server are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AccessEdgeServer** → **OCS2007\_R2**

All the policies that can be deployed only on OCS 2007 belong to the **Measurement Threshold** policy type.

#### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToUnresolvedDomain\_R2 Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnresolvedDomain_R2 Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnresolvedDomain_R2
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain failed to resolve by DNS SRV.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 057 - External Messages/sec Dropped Due To Unresolved Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToIncompMsgDomain\_R2 Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain_R2 Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToIncompMsgDomain_R2
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the federation type of the domain is incompatible with previous messages.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 069 - External Messages/sec Dropped Due To Incompatible Message Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToUnauthIMDomain\_R2 Policy

<b>Policy</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnauthIMDomain_R2 Policy
<b>Name</b>	OCS_AccessEdgeServer_ExtMsgPerSecDroppedDueToUnauthIMDomain_R2
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain did not resolve by DNS SRV to the connection peer FQDN.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 061 - External Messages/sec Dropped Due To Unauthorized IM Service Provider Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

## CS\_AccessEdgeServer\_ExtMsgPerSecDroppedDueToBlockedIMDomain\_R2 Policy

<b>Policy</b>	CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain_R2 Policy
<b>Name</b>	CS_AccessEdgeServer_ExtMsgPerSecDroppedDueToBlockedIMDomain_R2
<b>Description</b>	Monitors the number of messages dropped at the external edge per second because the domain resolved by DNS SRV to a server that is blocked in the IM Service Providers table.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 09 - Access Edge Server Messages
<b>Counter</b>	SIP - 059 - External Messages/sec Dropped Due To Blocked IM Service Provider Domain
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

## Archiving CDR Server

Deploy the Archiving CDR Server policy group on the Archiving and CDR server. The Archiving and CDR Server is located in the internal network. It supports archiving instant messaging (IM) conversations and group conferences, and capturing usage information related to file transfers, audio/video (A/V) conversations, application sharing, remote assistance, meetings, and conferencing servers in Call Detail Records (CDRs).

To implement archiving and CDR support, one or more Archiving and CDR servers must be deployed in the organization and the Enterprise pool or Standard Edition Server must point to the Archiving and CDR Server. The database for the Archiving and CDR Server can be deployed on the same computer as the Archiving and CDR Server or on a separate computer.

The policies in the Archiving CDR Server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **ArchivingCDRServer**

All the Archiving CDR Server group policies belong to the **Measurement Threshold** policy type.

The policy group contains the following policies.

### OCS\_ArchivingCDRService\_Logging Policy



Ensure that the OCS\_CreateDataSources policy is running before you deploy the OCS\_ArchivingCDRService\_Logging policy.

<b>Policy</b>	OCS_ArchivingCDRService_Logging Policy
<b>Name</b>	OCS_ArchivingCDRService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the counters RTCArch or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time

### OCS\_ArchivingCDRService\_ThreadCount Policy

<b>Policy</b>	OCS_ArchivingCDRService_ThreadCount Policy
<b>Name</b>	OCS_ArchivingCDRService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the Archiving and CDR service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Counter</b>	RTCArch
<b>Instance</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

### OCS\_Check\_ArchivingCDRServiceStatus Policy

<b>Policy</b>	OCS_Check_ArchivingCDRServiceStatus Policy
<b>Name</b>	OCS_Check_ArchivingCDRServiceStatus
<b>Description</b>	Checks the status of the Archiving and CDR Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCLOG

### OCS\_ArchivingCDRServer\_NumberOfMessagesNotWrittenToDB Policy

<b>Policy</b>	OCS_ArchivingCDRServer_NumberOfMessagesNotWrittenToDB Policy
<b>Name</b>	OCS_ArchivingCDRServer_NumberOfMessagesNotWrittenToDB
<b>Description</b>	Monitors the number of messages that validation failed for.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:Arch Service - 01 - READ
<b>Counter</b>	Arch Service - 002 - Messages that failed validation
<b>Threshold</b>	When the difference between two samples is greater than then <b>Critical:</b> 1

### OCS\_ArchivingCDRService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_ArchivingCDRService_PageFaultsPerSec Policy
<b>Name</b>	OCS_ArchivingCDRService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Archiving and CDR service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_ArchivingCDRService\_WorkingSet Policy

<b>Policy</b>	OCS_ArchivingCDRService_WorkingSet Policy
<b>Name</b>	OCS_ArchivingCDRService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Archiving and CDR service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

### OCS\_ArchivingCDRServer\_NumberOfDroppedMQMessages Policy

<b>Policy</b>	OCS_ArchivingCDRServer_NumberOfDroppedMQMessages Policy
<b>Name</b>	OCS_ArchivingCDRServer_NumberOfDroppedMQMessages
<b>Description</b>	Monitors the number of messages dropped from MSMQ queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:Arch Service - 01 – READ
<b>Counter</b>	Arch Service - 006 - Dropped messages from MQ
<b>Threshold</b>	When the difference between two samples is greater than then <b>Critical:</b> 1

### OCS\_ArchivingCDRService\_ProcessorTime Policy

<b>Policy</b>	OCS_ArchivingCDRService_ProcessorTime Policy
<b>Name</b>	OCS_ArchivingCDRService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Archiving and CDR service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process

<b>Policy</b>	OCS_ArchivingCDRService_ProcessorTime Policy
<b>Instance</b>	RTCArch
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_ArchivingCDRServer\_NumberOfValidationFailedMessages Policy

<b>Policy</b>	OCS_ArchivingCDRServer_NumberOfValidationFailedMessages Policy
<b>Name</b>	OCS_ArchivingCDRServer_NumberOfValidationFailedMessages
<b>Description</b>	Monitors the number of messages failed to be written to SQL database
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:Arch Service - 02 – WRITE
<b>Counter</b>	Arch Service - 002 - Messages failed to be written to DB
<b>Threshold</b>	When the difference between two samples is greater than then <b>Critical:</b> 1

#### OCS\_ArchivingCDRService\_PrivateBytes Policy

<b>Policy</b>	OCS_ArchivingCDRService_PrivateBytes Policy
<b>Name</b>	OCS_ArchivingCDRService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Archiving and CDR service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

## AVConfServer

Deploy this policy group on AV Conferencing Server. The AV Conferencing Server is located in the internal network. It enables audio and video peer-to-peer communications and audio and video conferencing. This server role is available on a Standard Edition Server.

In an Enterprise pool, it can be joined with the Front End Server and Web Conferencing Server or can be deployed on a separate server.

The policies in the AV Conferencing Server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AVConfServer**

All the Archiving CDR Server group policies belong to the **Measurement Threshold** policy type.

This policy group has the following policies.

#### [OCS\\_AVConfService\\_PrivateBytes Policy](#)

<b>Policy</b>	OCS_AVConfService_PrivateBytes Policy
<b>Name</b>	OCS_AVConfService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### [OCS\\_AVConfServer\\_NumberOfActiveConferences Policy](#)

<b>Policy</b>	OCS_AVConfServer_NumberOfActiveConferences Policy
<b>Name</b>	OCS_AVConfServer_NumberOfActiveConferences
<b>Description</b>	Monitors the number of active conferences on the A/V Conferencing Server.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	AVMCU - 00 - Operations
<b>Counter</b>	AVMCU - 000 - Number of Conferences
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 4000 <b>Critical:</b> 5000



#### OCS\_AVConfService\_ProcessorTime Policy

<b>Policy</b>	OCS_AVConfService_ProcessorTime Policy
<b>Name</b>	OCS_AVConfService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Front End service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_AVConfService\_WorkingSet Policy

<b>Policy</b>	OCS_AVConfService_WorkingSet Policy
<b>Name</b>	OCS_AVConfService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_Check\_AVConfServiceStatus Policy

<b>Policy</b>	OCS_Check_AVConfServiceStatus Policy
<b>Name</b>	OCS_Check_AVConfServiceStatus

<b>Policy</b>	OCS_Check_AVConfServiceStatus Policy
<b>Description</b>	Checks the status of the Audio/Video Conferencing Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCAVMCU

#### OCS\_AVConfServer\_MCUHealthState Policy

<b>Policy</b>	OCS_AVConfServer_MCUHealthState Policy
<b>Name</b>	OCS_AVConfServer_MCUHealthState
<b>Description</b>	Monitors the current health of the MCU. This is considered as: 0 = Normal 1 = Loaded 2 = Full 3 = Unavailable
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	AVMCU - 04 - MCU Health And Performance
<b>Counter</b>	AVMCU - 005 - MCU Health State
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1 <b>Critical:</b> 2

#### OCS\_AVConfService\_ThreadCount Policy

<b>Policy</b>	OCS_AVConfService_ThreadCount Policy
<b>Name</b>	OCS_AVConfService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process

<b>Policy</b>	OCS_AVConfService_ThreadCount Policy
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

#### OCS\_AVConfService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_AVConfService_PageFaultsPerSec Policy
<b>Name</b>	OCS_AVConfService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_AVConfService\_Logging Policy



Ensure that the OCS\_CreateDataSources policy is running before you deploy the OCS\_AVConfService\_Logging policy.

<b>Policy</b>	OCS_AVConfService_Logging Policy
<b>Name</b>	OCS_AVConfService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the counters RTCArch or _Total. If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

Instance	Performance Object
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time

## AVEdgeServer

Deploy this policy group on AV Edge server. The AV Edge Server is located in the perimeter network. It provides a single trusted point through which media traffic can traverse NATs and firewalls. It enables audio and video conferencing and audio and video peer-to-peer communications with external users equipped with the Office Communicator 2007 client.

This server role can be either configured with the Access Edge Server and Web Conferencing Edge Server, or it can reside on a separate, dedicated server.

### Policies deployed on OCS 2007 and OCS 2007 R2

The policies that can be deployed on both OCS 2007 and OCS 2007 R2 servers are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AVEdgeServer**

All the policies belong to the **Measurement Threshold** policy type.

#### OCS\_AVEdgeServer\_UDPAllocateRqstExceedingPortLimit Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPAllocateRqstExceedingPortLimit Policy
<b>Name</b>	OCS_AVEdgeServer_UDPAllocateRqstExceedingPortLimit
<b>Description</b>	Monitors the number of requests allocated over UDP that exceeded the port limit per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 006 - Allocate Requests Exceeding Port Limit/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

#### OCS\_AVAuthService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_AVAuthService_PageFaultsPerSec Policy
<b>Name</b>	OCS_AVAuthService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MRASSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_AVAuthService\_PrivateBytes Policy

<b>Policy</b>	OCS_AVAuthService_PrivateBytes Policy
<b>Name</b>	OCS_AVAuthService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MRASSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_AVAuthService\_ProcessorTime Policy

<b>Policy</b>	OCS_AVAuthService_ProcessorTime Policy
<b>Name</b>	OCS_AVAuthService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process

<b>Policy</b>	OCS_AVAuthService_ProcessorTime Policy
<b>Instance</b>	MRASSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_AVAuthService\_ThreadCount Policy

<b>Policy</b>	OCS_AVAuthService_ThreadCount Policy
<b>Name</b>	OCS_AVAuthService_ThreadCount
<b>Description</b>	Monitors the monitors the Thread Count counter of the Audio/Video Authentication service
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

#### OCS\_AVEdgeServer\_WorkingSet Policy

<b>Policy</b>	OCS_AVEdgeServer_WorkingSet Policy
<b>Name</b>	OCS_AVEdgeServer_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MRASSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

## OCS\_AVEdgeServer\_LoggingPolicy

<b>Policy</b>	OCS_AVEdgeServer_Logging Policy
<b>Name</b>	OCS_AVEdgeServer_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances MRASSvc or _Total. If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

Instance	Performance Object
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_AVEdgeServer\_Logging policy.

## OCS\_Check\_AVAuthServiceStatus Policy

<b>Policy</b>	OCS_Check_AVAuthServiceStatus Policy
<b>Name</b>	OCS_Check_AVAuthServiceStatus
<b>Description</b>	Checks the status of the Audio/Video Authentication Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMRAUTH

### OCS\_Check\_AVEdgeServiceStatus Policy

<b>Policy</b>	OCS_Check_AVEdgeServiceStatus Policy
<b>Name</b>	OCS_Check_AVEdgeServiceStatus
<b>Description</b>	Monitors checks the status of the Audio/Video Conferencing Edge Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMEDIARELAY

### OCS\_AVEdgeService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_AVEdgeService_PageFaultsPerSec Policy
<b>Name</b>	OCS_AVEdgeService_PageFaultsPerSec
<b>Description</b>	Monitors Page Faults/sec counter of the Audio/Video Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_AVEdgeService\_PrivateBytes Policy

<b>Policy</b>	OCS_AVEdgeService_PrivateBytes Policy
<b>Name</b>	OCS_AVEdgeService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process



<b>Policy</b>	OCS_AVEdgeService_PrivateBytes Policy
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_AVEdgeService\_ProcessorTime Policy

<b>Policy</b>	OCS_AccessEdgeService_ProcessorTime Policy
<b>Name</b>	OCS_AccessEdgeService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Audio/Video Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_AVEdgeService\_ThreadCount Policy

<b>Policy</b>	OCS_AVEdgeService_ThreadCount Policy
<b>Name</b>	OCS_AVEdgeService_ThreadCount
<b>Description</b>	Monitors the monitors the Thread Count counter of the Audio/Video Conferencing Edge Service
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

### OCS\_AVEdgeService\_WorkingSet Policy

<b>Policy</b>	OCS_AVEdgeService_WorkingSet Policy
<b>Name</b>	OCS_AVEdgeService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Audio/Video Conferencing Edge Service
<b>Schedule</b>	This policy runs every 5 minutes
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

### OCS\_AVEdgeServer\_BadRequestsReceivedPerSec Policy

Policy	OCS_AVEdgeServer_BadRequestsReceivedPerSec Policy
Name	OCS_AVEdgeServer_BadRequestsReceivedPerSec
Description	Monitors the number of invalid requests received per second
<b>Schedule</b>	This policy runs every 15 minutes.
Performance Object	A/V Auth - 00 – Requests
Counter	- 003 - Bad Requests Received/sec
Threshold	This policy has the following threshold: <b>Warning:</b> 20 <b>Critical:</b> 30

### OCS\_AVEdgeServer\_TCPAllocRqstExceedingPortLimit Policy

<b>Policy</b>	OCS_AVEdgeServer_TCPAllocRqstExceedingPortLimit Policy
<b>Name</b>	OCS_AVEdgeServer_TCPAllocRqstExceedingPortLimit
<b>Description</b>	Monitors the number of allocated requests over TCP per second that exceeded the port limit.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 01 - TCP Counters

<b>Policy</b>	OCS_AVEdgeServer_TCPAllocRqstExceedingPortLimit Policy
<b>Instance</b>	_Total
<b>Counter</b>	- 006 - Allocate Requests Exceeding Port Limit/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

OCS\_AVEdgeServer\_TCPAuthenticationFailuresPerSec Policy

<b>Policy</b>	OCS_AVEdgeServer_TCPAuthenticationFailuresPerSec Policy
<b>Name</b>	OCS_AVEdgeServer_TCPAuthenticationFailuresPerSec
<b>Description</b>	Monitors the failed attempts to authenticate with the relay over TCP per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 004 - Authentication Failures/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

OCS\_AVEdgeServer\_UDPAllocateRqstExceedingPortLimit Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPAllocateRqstExceedingPortLimit Policy
<b>Name</b>	OCS_AVEdgeServer_UDPAllocateRqstExceedingPortLimit
<b>Description</b>	Monitors the number of requests allocated over UDP that exceeded the port limit per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 006 - Allocate Requests Exceeding Port Limit/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

### OCS\_AVEdgeServer\_UDPAuthenticationFailuresPerSec Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPAuthenticationFailuresPerSec Policy
<b>Name</b>	OCS_AVEdgeServer_UDPAuthenticationFailuresPerSec
<b>Description</b>	Monitors the number of failed attempts to authenticate with the relay over UDP per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 004 - Authentication Failures/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

### Policies deployed only on OCS 2007

The policies that can be deployed only on the OCS 2007 server are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AVEdgeServer** → **OCS2007**

All the policies belong to the **Measurement Threshold** policy type.

### OCS\_AVEdgeServer\_Logging Policy

<b>Policy</b>	OCS_AVEdgeServer_Logging Policy
<b>Name</b>	OCS_AVEdgeServer_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances MediaRelaySvc or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_AVEdgeServer\_Logging policy.

#### OCS\_AVEdgeServer\_TCIPacketsDroppedPerSec Policy

<b>Policy</b>	OCS_AVEdgeServer_TCIPacketsDroppedPerSec Policy
<b>Name</b>	OCS_AVEdgeServer_TCIPacketsDroppedPerSec
<b>Description</b>	Monitors the number of packets over TCP dropped by the relay per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 023 - Packets Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 200 <b>Critical:</b> 300

#### OCS\_AVEdgeServer\_UDPActiveSessionsExceedingBandwidthLimit Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPActiveSessionsExceedingBandwidthLimit Policy
<b>Name</b>	OCS_AVEdgeServer_UDPActiveSessionsExceedingBandwidthLimit
<b>Description</b>	Monitors the number of active relay sessions over UDP that are exceeding bandwidth limit.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 007 - Active Sessions Exceeding Bandwidth Limit
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

#### OCS\_AVEdgeServer\_UDPPacketsDroppedPerSec Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPPacketsDroppedPerSec Policy
<b>Name</b>	OCS_AVEdgeServer_UDPPacketsDroppedPerSec
<b>Description</b>	Monitors packets over UDP dropped by the relay per second rate
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_AVEdgeServer_UDPPacketsDroppedPerSec Policy
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 022 - Packets Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 200 <b>Critical:</b> 300

#### OCS\_AVEdgeServer\_TCPActiveSessionsExceedingBandwidthLimit Policy

<b>Policy</b>	OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit Policy
<b>Name</b>	OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit
<b>Description</b>	Monitors monitors the number of active relay sessions over TCP per second that are exceeding bandwidth limit
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 007 - Active Sessions Exceeding Bandwidth Limit
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

#### Policies deployed only on OCS 2007 R2

The policies that can be deployed only on the OCS 2007 R2 server are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **AVEdgeServer** → **OCS2007\_R2**

All the policies belong to the **Measurement Threshold** policy type.

### OCS\_AVEdgeServer\_Logging\_R2 Policy

<b>Policy</b>	OCS_AVEdgeServer_Logging_R2 Policy
<b>Name</b>	OCS_AVEdgeServer_Logging_R2
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances MediaRelaySvc or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

Instance	Performance Object
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_AVEdgeServer\_Logging\_R2 policy.

### OCS\_AVEdgeServer\_TCPKetsDroppedPerSec\_R2 Policy

<b>Policy</b>	OCS_AVEdgeServer_TCPKetsDroppedPerSec_R2 Policy
<b>Name</b>	OCS_AVEdgeServer_TCPKetsDroppedPerSec_R2
<b>Description</b>	Monitors the number of packets over TCP dropped by the relay per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 022 - Packets Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

### OCS\_AVEdgeServer\_UDPActiveSessionsExceedingBandwidthLimit\_R2 Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPActiveSessionsExceedingBandwidthLimit_R2 Policy
<b>Name</b>	OCS_AVEdgeServer_UDPActiveSessionsExceedingBandwidthLimit_R2
<b>Description</b>	Monitors the number of active relay sessions over UDP that are exceeding bandwidth limit.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 026 - Active Sessions Exceeding Avg Bandwidth Limit (R2)
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

### OCS\_AVEdgeServer\_UDPPacketsDroppedPerSec\_R2 Policy

<b>Policy</b>	OCS_AVEdgeServer_UDPPacketsDroppedPerSec_R2 Policy
<b>Name</b>	OCS_AVEdgeServer_UDPPacketsDroppedPerSec_R2
<b>Description</b>	Monitors packets over UDP dropped by the relay per second rate.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	- 021 - Packets Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 200 <b>Critical:</b> 300

### OCS\_AVEdgeServer\_TCPActiveSessionsExceedingBandwidthLimit\_R2 Policy

<b>Policy</b>	OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit_R2 Policy
<b>Name</b>	OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit_R2
<b>Description</b>	Monitors the number of active relay sessions over TCP per second that are exceeding bandwidth limit.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	A/V Edge - 01 - TCP Counters



<b>Policy</b>	OCS_AVEdgeServer_TCPActiveSessionsExceedingBandwidthLimit_R2 Policy
<b>Instance</b>	_Total
<b>Counter</b>	- 025- Active Sessions Exceeding AvgBandwidth Limit
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 10 <b>Critical:</b> 20

## Configuration

This policy group can be deployed on all Microsoft Office Communications Server 2007 server roles. The policy group includes OCS\_CreateDataSources policy.

<b>Policy</b>	OCS_CreateDataSources Policy
<b>Name</b>	OCS_CreateDataSources
<b>Description</b>	Creates the OCS data source (CODA or HP Performance Agent) into which OCS SPI logging policies log data. Ensure to run this policy on the node before you deploy any logging policy.
<b>Policy Type</b>	Scheduled Task policy
<b>Policy Group</b>	SPI for Microsoft Enterprise Servers → en → Microsoft_Office_Communications_Server → Microsoft_Office_Communications_Server_2007 → Configuration

## CWAServer

Deploy this policy group on Communicator Web Access (CWA) server. The CWA server enables browser-based client access to Microsoft Office Communications Server 2007.

The policies are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **CWAServer**

All the policies belong to the **Measurement Threshold** policy type.

The policy group has the following policies.

### OCS\_CWAServer\_AuthFailuresDueToLDAPErrors Policy

<b>Policy</b>	OCS_CWAServer_AuthFailuresDueToLDAPErrors Policy
<b>Name</b>	OCS_CWAServer_AuthFailuresDueToLDAPErrors
<b>Description</b>	Monitors the total number of authorizations that have failed due to LDAP errors during binds and searches since the Communicator Web Access virtual server was started.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_CWAServer_AuthFailuresDueToLDAPErrors Policy
<b>Performance Object</b>	CWA - 01 - Authentication Module
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 012 - LDAP error total
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 300 <b>Critical:</b> 500

#### OCS\_CWAServer\_FailedRequests Policy

<b>Policy</b>	OCS_CWAServer_FailedRequests Policy
<b>Name</b>	OCS_CWAServer_FailedRequests
<b>Description</b>	Monitors the total number of requests that failed to process since the Communicator Web Access virtual server was started.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 03 - User session Service
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 018 - Total requests failed
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 250 <b>Critical:</b> 500

#### OCS\_CWAServer\_LogonsDeniedDueToServerThrottling Policy

<b>Policy</b>	OCS_CWAServer_LogonsDeniedDueToServerThrottling Policy
<b>Name</b>	OCS_CWAServer_LogonsDeniedDueToServerThrottling
<b>Description</b>	Monitors total number of logon attempts that were not allowed due to server throttling under heavy resource consumption.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 01 - Authentication Module
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 014 - Logons denied due to server throttling
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 10 <b>Critical:</b> 15

#### OCS\_CWAServer\_RequestsRejectedPerSecDueToInvalidTicket Policy

<b>Policy</b>	OCS_CWAServer_RequestsRejectedPerSecDueToInvalidTicket Policy
<b>Name</b>	OCS_CWAServer_RequestsRejectedPerSecDueToInvalidTicket
<b>Description</b>	Monitors the number of requests rejected per second due to an invalid ticket in the request. This problem occurs occasionally under normal circumstances, but spikes can be symptomatic of a denial of service attack or hacking attempt.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 02 – Security
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 001 - Requests rejected due to invalid ticket / sec
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_CWAServer\_RequestsToNonExistentSessions Policy

<b>Policy</b>	OCS_CWAServer_RequestsToNonExistentSessionss Policy
<b>Name</b>	OCS_CWAServer_RequestsToNonExistentSessionss
<b>Description</b>	Monitors the total number of requests targeting nonexistent sessions since the Communicator Web Access virtual server was started.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 03 - User session Service
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 016 - Requests to nonexistent sessions
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 250 <b>Critical:</b> 500

#### OCS\_CWAServer\_SessionsFailedToSignIn Policy

<b>Policy</b>	OCS_CWAServer_SessionsFailedToSignIn Policy
<b>Name</b>	OCS_CWAServer_SessionsFailedToSignIn
<b>Description</b>	Monitors the total number of user sessions that failed to sign in to Office Communications Server since the Communicator Web Access virtual server was started.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_CWAServer_SessionsFailedToSignIn Policy
<b>Performance Object</b>	CWA - 03 - User session Service
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 004 - Sessions failed to sign in
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 50 <b>Critical:</b> 75

#### OCS\_CWAServer\_SessionsTimedOut Policy

<b>Policy</b>	OCS_CWAServer_SessionsTimedOut Policy
<b>Name</b>	OCS_CWAServer_SessionsTimedOut
<b>Description</b>	Monitors the total number of Communicator Web Access user sessions that timed out due to communication failure with clients.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 03 - User session Service
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 007 - Total sessions timed out
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 250 <b>Critical:</b> 500

#### OCS\_CWAServer\_FormsLogonFailures Policy

<b>Policy</b>	OCS_CWAServer_FormsLogonFailures Policy
<b>Name</b>	OCS_CWAServer_FormsLogonFailures
<b>Description</b>	Monitors total number of forms logon attempts that have failed since the Communicator Web Access virtual server was started
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 01 - Authentication Module
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 003 - Forms auth logon failures
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 300 <b>Critical:</b> 500

## OCS\_CWAServer\_IWALogonFailures Policy

<b>Policy</b>	OCS_CWAServer_IWALogonFailures Policy
<b>Name</b>	OCS_CWAServer_IWALogonFailures
<b>Description</b>	Monitors the total number of failed logons that used IIS authentication since the Communicator Web Access virtual server was started. The IIS authentication types used are NTLM, Kerberos, or single sign on (SSO) authentication if the Communicator Web Access server is in SSO mode.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 01 - Authentication Module
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 007 - IWA auth logon failures
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 300 <b>Critical:</b> 500

## OCS\_CWAServer\_LDAPErrors Policy

<b>Policy</b>	OCS_CWAServer_LDAPErrors Policy
<b>Name</b>	OCS_CWAServer_LDAPErrors
<b>Description</b>	Monitors total number of LDAP errors that have occurred during Communicator Web Access directory search operations.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	CWA - 00 - Directory Search
<b>Instance</b>	_Total
<b>Counter</b>	CWA - 003 - LDAP errors
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 2 <b>Critical:</b> 5

## FrontEnd Server

Deploy this policy group on a FrontEnd server. The FrontEnd Server is located in the internal network that hosts the IM Conferencing service, Address Book service, and Telephony Conferencing service to support registration, presence, IM, and conferencing.

This server role is available on a Standard Edition Server. In an Enterprise pool, it can either be configured with the Web Conferencing Server and A/V Conferencing Server, or can be deployed on a separate server.

## Policies deployed on OCS 2007 and OCS 2007 R2

The policies deployed on both OCS 2007 and OCS 2007 R2 servers are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **FrontEndServer**

The policies belong to the **Measurement Threshold** policy type.

### OCS\_Check\_FrontEndServiceStatus Policy

<b>Policy</b>	OCS_Check_FrontEndServiceStatus Policy
<b>Name</b>	OCS_Check_FrontEndServiceStatus
<b>Description</b>	Checks the status of the Front-End Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCSrv

### OCS\_FrontEndService\_Logging Policy

<b>Policy</b>	OCS_FrontEndService_Logging Policy
<b>Name</b>	OCS_FrontEndService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances RTCSrv or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before you deploy the OCS\_FrontEndService\_Logging policy.

#### OCS\_FrontEndService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_FrontEndService_PageFaultsPerSecs Policy
<b>Name</b>	OCS_FrontEndService_PageFaultsPerSecs
<b>Description</b>	Monitors the Page Faults/sec counter of the Front End service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_FrontEndService\_PrivateBytes Policy

<b>Policy</b>	OCS_FrontEndService_PrivateBytes Policy
<b>Name</b>	OCS_FrontEndService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Front End service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_FrontEndService\_ProcessorTime Policy

<b>Policy</b>	OCS_FrontEndService_ProcessorTime Policy
<b>Name</b>	OCS_FrontEndService_ProcessorTime
<b>Description</b>	Monitors tthe the % Processor Time counter of the Front End service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process

<b>Policy</b>	OCS_FrontEndService_ProcessorTime Policy
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_FrontEndService\_ThreadCount Policy

<b>Policy</b>	OCS_FrontEndService_ThreadCount Policy
<b>Name</b>	OCS_FrontEndService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the Front End service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

#### OCS\_FrontEndService\_WorkingSet Policy

<b>Policy</b>	OCS_FrontEndService_WorkingSet Policy
<b>Name</b>	OCS_FrontEndService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Front End service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007



#### OCS\_FrontEndServer\_SendsOutstandingPolicy

<b>Policy</b>	OCS_FrontEndServer_SendsOutstanding Policy
<b>Name</b>	OCS_FrontEndServer_SendsOutstanding
<b>Description</b>	Monitors the number of requests and responses that are queued outbound.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP – 01 – Peers
<b>Counter</b>	SIP – 017 – Sends Outstanding
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 200

#### OCS\_FrontEndServer\_HoldingTimeForIncMsgs Policy

<b>Policy</b>	OCS_FrontEndServer_HoldingTimeForIncMsgs Policy
<b>Name</b>	OCS_FrontEndServer_HoldingTimeForIncMsgs
<b>Description</b>	Monitors the average amount of time taken by the server to process a request.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP – 07 - Load Management
<b>Counter</b>	SIP – 000 - Average Holding Time For Incoming Messages
<b>Threshold</b>	This policy has the following threshold: Warning: 4 Critical: 5

#### OCS\_FrontEndServer\_ProcessingLatency Policy

<b>Policy</b>	OCS_FrontEndServer_ProcessingLatency Policy
<b>Name</b>	OCS_FrontEndServer_ProcessingLatency
<b>Description</b>	Monitors the amount of time (in milliseconds) that the back end spent in processing a request.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_FrontEndServer_ProcessingLatency Policy
<b>Performance Object</b>	LC:USrv - 00 - DBStore
<b>Counter</b>	Usvr - 004- Sproc Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 4000 <b>Critical:</b> 6000

#### OCS\_FrontEndServer\_QueueLatency Policy

<b>Policy</b>	OCS_FrontEndServer_QueueLatency Policy
<b>Name</b>	OCS_FrontEndServer_QueueLatency
<b>Description</b>	Monitors the amount of time( in milliseconds) that a request is spent in the back end queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:USrv - 00 - DBStore
<b>Counter</b>	Usvr - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 4000 <b>Critical:</b> 6000

### Policies deployed on OCS 2007

The policies to be deployed on OCS 2007 are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **FrontEndServer** → **OCS2007**

The policies belong to the **Measurement Threshold** Policy type.

#### OCS\_FrontEndServer\_Local503Responses Policy

<b>Policy</b>	OCS_FrontEndServer_Local503Responses Policy
<b>Name</b>	OCS_FrontEndServer_Local503Responses
<b>Description</b>	Monitors the number of 503 responses per second. The 503 code indicates that the server is unavailable.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_FrontEndServer_Local503Responses Policy
<b>Performance Object</b>	LC:SIP – 04 - Responses
<b>Counter</b>	SIP – 051 - Local 503 Responses/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 2 <b>Critical:</b> 5

#### OCS\_FrontEndServer\_Logging Policy

<b>Policy</b>	OCS_FrontEndServer_Logging Policy
<b>Name</b>	OCS_FrontEndServer_Logging
<b>Description</b>	logs the following metrics into the data store (CODA or HP Performance Agent) for the instances msec or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_FRONTEND

<b>Instance</b>	<b>Performance Object</b>
msec	LC:USrv - 00 – DBStore\Usrv - 002 - Queue Latency
	LC:USrv - 00 – DBStore\Usrv - 004- Sproc Latency
_Total	LC:SIP - 07 - Load Management\SIP - 000 - Average Holding Time For Incoming Messages
	LC:SIP - 04 – Responses\SIP - 051 - Local 503 Responses/sec
	LC:SIP - 04 – Responses\SIP - 053 - Local 504 Responses/sec
	LC:SIP - 01 – Peers\SIP - 017 - Sends Outstanding



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_FrontEndServer\_Logging policy.

#### OCS\_FrontEndServer\_Local504Responses Policy

<b>Policy</b>	OCS_FrontEndServer_Local504Responses Policy
<b>Name</b>	OCS_FrontEndServer_Local504Responses
<b>Description</b>	Monitors the number of 504 responses per second. The 504 code indicates connectivity problems with other servers.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_FrontEndServer_Local504Responses Policy
<b>Performance Object</b>	LC:SIP – 04 - Responses
<b>Counter</b>	SIP – 053 - Local 504 Responses/sec
<b>Threshold</b>	This policy has the following threshold: Warning: 2 Critical: 5

## Policies deployed on OCS 2007 R2

The policies to be deployed on OCS 2007 R2 are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **FrontEndServer** → **OCS2007\_R2**

The policies belong to the **Measurement Threshold** Policy type.

### OCS\_FrontEndServer\_Local503Responses\_R2 Policy

<b>Policy</b>	OCS_FrontEndServer_Local503Responses_R2 Policy
<b>Name</b>	OCS_FrontEndServer_Local503Responses_R2
<b>Description</b>	Monitors the number of 503 responses per second. The 503 code indicates that the server is unavailable.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP – 04 - Responses
<b>Counter</b>	SIP – 055 - Local 503 Responses/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning: 2</b> <b>Critical: 5</b>

### OCS\_FrontEndServer\_Logging\_R2 Policy

<b>Policy</b>	OCS_FrontEndServer_Logging_R2 Policy
<b>Name</b>	OCS_FrontEndServer_Logging_R2
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances msec or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_FRONTEND

Instance	Performance Object
msec	LC:USrv - 00 – DBStore\Usvr - 002 - Queue Latency
	LC:USrv - 00 – DBStore\Usvr - 004- Sproc Latency
_Total	LC:SIP - 07 - Load Management\SIP - 000 - Average Holding Time For Incoming Messages
	LC:SIP - 04 – Responses\SIP - 051 - Local 503 Responses/sec
	LC:SIP - 04 – Responses\SIP - 053 - Local 504 Responses/sec
	LC:SIP - 01 – Peers\SIP - 017 - Sends Outstanding



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_FrontEndService\_Logging policy.

#### OCS\_FrontEndServer\_Local504Responses\_R2 Policy

<b>Policy</b>	OCS_FrontEndServer_Local504Responses_R2 Policy
<b>Name</b>	OCS_FrontEndServer_Local504Responses_R2
<b>Description</b>	Monitors the number of 504 responses per second. The 504 code indicates connectivity problems with other servers.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP – 04 - Responses
<b>Counter</b>	SIP – 057 - Local 504 Responses/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 2 <b>Critical:</b> 5

## IMConfServer

Deploy this policy group on the IM Conferencing Server. The IM Conferencing Server is an instant messaging server and it is the conferencing server of OCS 2007.

It provides server-managed group IM and runs as a separate process on the Standard Edition Server or Enterprise pool Front End Server.

The policies in the IM Conferencing Server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **IMConfServer**

The policies belong to the **Measurement Threshold** Policy type.

This policy group includes the following policies.

### OCS\_Check\_IMConfServiceStatus Policy

<b>Policy</b>	OCS_Check_IMConfServiceStatus Policy
<b>Name</b>	OCS_Check_IMConfServiceStatus
<b>Description</b>	Checks the status of the IM Conferencing Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	IMMCU

### OCS\_IMConfService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_IMConfService_PageFaultsPerSec Policy
<b>Name</b>	OCS_IMConfService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_IMConfService\_PrivateBytes Policy

<b>Policy</b>	OCS_IMConfService_PrivateBytes Policy
<b>Name</b>	OCS_IMConfService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_IMConfService\_ProcessorTime Policy

<b>Policy</b>	OCS_IMConfService_ProcessorTime Policy
<b>Name</b>	OCS_IMConfService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_IMConfService\_ThreadCount Policy

<b>Policy</b>	OCS_IMConfService_ThreadCount Policy
<b>Name</b>	OCS_IMConfService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

#### OCS\_IMConfService\_WorkingSet Policy

<b>Policy</b>	OCS_IMConfService_WorkingSet Policy
<b>Name</b>	OCS_IMConfService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process

<b>Policy</b>	OCS_IMConfService_WorkingSet Policy
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_IMConfService\_Logging Policy

<b>Policy</b>	OCS_IMConfService_Logging Policy
<b>Name</b>	OCS_IMConfService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances IMMCUSvc or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_IMConfService\_Logging policy.

## Mediation Server

Deploy this policy group on the Mediation Server. The Mediation Server is located in the internal network that mediates signaling and media between the Enterprise Voice infrastructure (such as a Director or home server) and another gateway (such as a Basic Media Gateway).

A Mediation Server is also used to link Office Communications Server and a PBX in both departmental deployment and PBX integration topologies. The server is deployed on a separate, dedicated server.



The policies in the Mediation Server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **MediationServer**

The policies belong to the **Measurement Threshold** Policy type.

This policy group includes the following policies.

#### OCS\_MediationService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_MediationService_PageFaultsPerSec Policy
<b>Name</b>	OCS_MediationService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Mediation service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_Check\_MediationServiceStatus Policy

<b>Policy</b>	OCS_Check_MediationServiceStatus Policy
<b>Name</b>	OCS_Check_MediationServiceStatus
<b>Description</b>	Checks the status of the Mediation Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMEDSRV

#### OCS\_MediationService\_Logging Policy

<b>Policy</b>	OCS_MediationService_Logging Policy
<b>Name</b>	OCS_MediationService_Logging

<b>Policy</b>	OCS_MediationService_Logging Policy
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances MediationServerSvc or _Total. If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

Instance	Performance Object
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_MediationService\_Logging policy.

#### OCS\_MediationService\_PrivateBytes Policy

<b>Policy</b>	OCS_MediationService_PrivateBytes Policy
<b>Name</b>	OCS_MediationService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Mediation service
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_MediationService\_ProcessorTime Policy

<b>Policy</b>	OCS_MediationService_ProcessorTime Policy
<b>Name</b>	OCS_MediationService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Mediation service.
<b>Schedule</b>	This policy runs every 5 minutes.

<b>Policy</b>	OCS_MediationService_ProcessorTime Policy
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_MediationService\_ThreadCount Policy

<b>Policy</b>	OCS_MediationService_ThreadCount Policy
<b>Name</b>	OCS_MediationService_ThreadCount
<b>Description</b>	Monitors the Page Faults/sec counter of the Mediation service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

#### OCS\_MediationService\_WorkingSet Policy

<b>Policy</b>	OCS_MediationService_WorkingSet Policy
<b>Name</b>	OCS_MediationService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Mediation service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_MediationServer\_LoadCallFailureIndex Policy

<b>Policy</b>	OCS_MediationServer_LoadCallFailureIndex Policy
<b>Name</b>	OCS_MediationServer_LoadCallFailureIndex
<b>Description</b>	Monitors scaled index between zero and 100 that is related to all call failures due to heavy load.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	MediationServer - 03 - Health Indices
<b>Instance</b>	000 - Load Call Failure Index
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_MediationServer\_RejectedSIPInvitesFromGateway Policy

<b>Policy</b>	OCS_MediationServer_RejectedSIPInvitesFromGateway Policy
<b>Name</b>	OCS_MediationServer_RejectedSIPInvitesFromGateway
<b>Description</b>	Monitors the number of SIP INVITEs from gateway which were rejected immediately because of server load.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	MediationServer - 01 - Inbound Calls
<b>Instance</b>	003 - Total rejected
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 5 <b>Critical:</b> 10

#### OCS\_MediationServer\_RejectedSIPInvitesFromProxy Policy

<b>Policy</b>	OCS_MediationServer_RejectedSIPInvitesFromProxy Policy
<b>Name</b>	OCS_MediationServer_RejectedSIPInvitesFromProxy
<b>Description</b>	Monitors the number of SIP INVITEs from proxy which were rejected immediately because of server load.
<b>Schedule</b>	This policy runs every 5 minutes.

<b>Policy</b>	OCS_MediationServer_RejectedSIPInvitesFromProxy Policy
<b>Performance Object</b>	MediationServer - 00 - Outbound Calls
<b>Instance</b>	003 - Total rejected
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

## TelConfServer

Deploy this policy group on the Telephony Conferencing server. The Telephony Conferencing Server is a conferencing server. It enables audio conference integration with audio conferencing providers (ACPs). This server runs as a separate process on the Standard Edition Server or Enterprise pool Front End Server.

The policies in the Telephony Conferencing server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **TelConfServer**

The policies belong to the **Measurement Threshold** Policy type.

This policy group includes the following policies.

### OCS\_Check\_TelConfServiceStatus Policy

<b>Policy</b>	OCS_Check_TelConfServiceStatus Policy
<b>Name</b>	OCS_Check_TelConfServiceStatus
<b>Description</b>	Checks the status of the Telephony Conferencing Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCACPMCU

### OCS\_TelConfService\_Logging Policy

<b>Policy</b>	OCS_TelConfService_Logging policy Policy
<b>Name</b>	OCS_TelConfService_Logging policy

<b>Policy</b>	OCS_TelConfService_Logging policy Policy
<b>Description</b>	The OCS_TelConfService_Logging policy logs the following metrics into the data store (CODA or HP Performance Agent) for the instances AcpMcuSvc or _Total. If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_TelConfService\_Logging policy.

#### OCS\_TelConfService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_TelConfService_PageFaultsPerSec Policy
<b>Name</b>	OCS_TelConfService_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Telephony Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AcpMcuSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

#### OCS\_TelConfService\_PrivateBytes Policy

<b>Policy</b>	OCS_TelConfService_PrivateBytes Policy
<b>Name</b>	OCS_TelConfService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Telephony Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AcpMcuSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_TelConfService\_ProcessorTime Policy

<b>Policy</b>	OCS_TelConfService_ProcessorTime Policy
<b>Name</b>	OCS_TelConfService_ProcessorTime
<b>Description</b>	Monitors the Percentage Processor Time counter of the Telephony Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AcpMcuSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_TelConfService\_ThreadCount Policy

<b>Policy</b>	OCS_TelConfService_ThreadCount Policy
<b>Name</b>	OCS_TelConfService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the Telephony Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process

<b>Policy</b>	OCS_TelConfService_ThreadCount Policy
<b>Instance</b>	AcpMcuSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

#### OCS\_TelConfService\_WorkingSet Policy

<b>Policy</b>	OCS_TelConfService_WorkingSet Policy
<b>Name</b>	OCS_TelConfService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Telephony Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	AcpMcuSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

## WebCompServer

Deploy this policy group on Web Components Server. The Web Components Server is located in the internal network. It provides IIS-based Web components that support Office Communications Server 2007.

These Web components include IIS Virtual Directory setup to support Address Book Server, the Web Conferencing Server (downloading of meeting content), and the IM Conferencing group expansion Web service. The Web Components Server runs on each Standard Edition Server and, for Enterprise pools, either on the Front End Server (in a consolidated configuration) or on a dedicated IIS server (in an expanded configuration).

The policies of this group must be deployed on OCS 2007 or OCS 2007\_R2.

### Deploy the following policies on OCS 2007

The policies to be deployed on the OCS 2007 server are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **WebCompServer** → **OCS2007**

The policies belong to the **Measurement Threshold** Policy type.



### OCS\_WebCompServer\_InvalidInputRequestsPerSec Policy

<b>Policy</b>	OCS_WebCompServer_InvalidInputRequestsPerSec Policy
<b>Name</b>	OCS_WebCompServer_InvalidInputRequestsPerSec
<b>Description</b>	Monitors the number of invalid input requests per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DLX - 00 - Distribution List Expansion
<b>Counter</b>	DLX - 016 - Invalid input requests/sec
<b>Threshold</b>	When a sample is greater than: <b>Warning:</b> 1 <b>Critical:</b> 5

### OCS\_WebCompServer\_TimedOutSecurityDescRequestsPerSec Policy

<b>Policy</b>	OCS_WebCompServer_InvalidInputRequestsPerSec Policy
<b>Name</b>	OCS_WebCompServer_InvalidInputRequestsPerSec
<b>Description</b>	Monitors the number of invalid input requests per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DLX - 00 - Distribution List Expansion
<b>Counter</b>	DLX - 018 - Timed out Requests that fetch Security Descriptors/sec
<b>Threshold</b>	When a sample is greater than: <b>Warning:</b> 1 <b>Critical:</b> 5

### Deploy the following policies on OCS\_R2

The policies to be deployed on the OCS 2007 R2 server are available at the following location:

**SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **WebCompServer** → **OCS2007\_R2**

The policies belong to the **Measurement Threshold** Policy type.

### OCS\_WebCompServer\_InvalidInputRequestsPerSec\_R2 Policy

<b>Policy</b>	OCS_WebCompServer_InvalidInputRequestsPerSec_R2 Policy
<b>Name</b>	OCS_WebCompServer_InvalidInputRequestsPerSec_R2
<b>Description</b>	Monitors the number of invalid input requests per second.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_WebCompServer_InvalidInputRequestsPerSec_R2 Policy
<b>Performance Object</b>	LC:DLX - 00 - Distribution List Expansion
<b>Counter</b>	DLX - 016 - Invalid input requests/sec
<b>Threshold</b>	When a sample is greater than: <b>Warning: 1</b> <b>Critical: 5</b>

OCS\_WebCompServer\_TimedOutSecurityDescRequestsPerSec\_R2 Policy

<b>Policy</b>	OCS_WebCompServer_InvalidInputRequestsPerSec_R2 Policy
<b>Name</b>	OCS_WebCompServer_InvalidInputRequestsPerSec_R2
<b>Description</b>	Monitors the number of invalid input requests per second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DLX - 00 - Address Book and Distribution List Expansion
<b>Counter</b>	DLX - 018 - Timed out Requests that fetch Security Descriptors/sec
<b>Threshold</b>	When a sample is greater than: <b>Warning: 1</b> <b>Critical: 5</b>

## WebConfServer

Deploy this policy group on Web Conferencing server. The Web Conferencing Server is located in the internal network that enables multi-party data collaboration. This server role is available on a Standard Edition Server.

In an Enterprise pool, it can be either configured with the Front End Server and A/V Conferencing Server, or can be deployed on a separate server.

The policies in the Web Conferencing server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **WebConfServer**

The policies belong to the **Measurement Threshold** Policy type.

This policy group includes the following policies.

### OCS\_Check\_WebConfServiceStatus Policy

<b>Policy</b>	OCS_Check_WebConfServiceStatus Policy
<b>Name</b>	OCS_Check_WebConfServiceStatus
<b>Description</b>	Checks the status of the Web Conferencing Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Monitored Service</b>	RTC DATAMCU

### OCS\_WebConfServer\_ComplianceErrors Policy

<b>Policy</b>	OCS_WebConfServer_ComplianceErrors Policy
<b>Name</b>	OCS_WebConfServer_ComplianceErrors
<b>Description</b>	Monitors the number of errors reported by the compliance module.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAMCU - 00 - DataMCU Conferences
<b>Counter</b>	DATAMCU - 026 - Compliance errors
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_WebConfServer\_MCUHealthState Policy

<b>Policy</b>	OCS_WebConfServer_MCUHealthState Policy
<b>Name</b>	OCS_WebConfServer_MCUHealthState
<b>Description</b>	Monitors the the current health of the MCU. It indicates 0 as Normal, 1 as Loaded, 2 as Full, and 3 as Unavailable.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAMCU - 02 - MCU Health And Performance
<b>Counter</b>	DATAMCU - 005 - MCU Health State
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 1 <b>Critical:</b> 2

### OCS\_WebConfServer\_NumberOfUnhandledApplExceptions Policy

<b>Policy</b>	OCS_WebConfServer_NumberOfUnhandledApplExceptions Policy
<b>Name</b>	OCS_WebConfServer_NumberOfUnhandledApplExceptions
<b>Description</b>	Monitors the number of unhandled application exceptions.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAMCU - 00 - DataMCU Conferences
<b>Counter</b>	DATAMCU - 038 - Number of Unhandled Application Exception
<b>Interval</b>	15 min
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_WebConfServer\_ResourcesOverConfSpaceLimit Policy

<b>Policy</b>	OCS_WebConfServer_ResourcesOverConfSpaceLimit Policy
<b>Name</b>	OCS_WebConfServer_ResourcesOverConfSpaceLimit
<b>Description</b>	Monitors the number of resource failed to be created because the Data MCU has reached the space limit for one or more conferences.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAMCU - 00 - DataMCU Conferences
<b>Counter</b>	DATAMCU - 031 - Resources over conference space limit
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 5 <b>Critical:</b> 10

### OCS\_WebConfServer\_SessionQueuesState Policy

<b>Policy</b>	OCS_WebConfServer_SessionQueuesState Policy
<b>Name</b>	OCS_WebConfServer_SessionQueuesState
<b>Description</b>	Monitors the state of the session queues.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAMCU - 00 - DataMCU Conferences

<b>Policy</b>	OCS_WebConfServer_SessionQueuesState Policy
<b>Counter</b>	DATAMCU - 041 - Session queues state
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 1 <b>Critical:</b> 2
<b>Warning/Error Instruction Text</b>	<b>Probable Cause(s):</b> When the Data MCU cannot handle the load capacity. <b>Suggested Action(s):</b> This should be a temporary condition. If this condition persists, increase the load capacity of the Data MCU by provisioning more Data MCU machines.

#### OCS\_WebConfService\_Logging Policy

<b>Policy</b>	OCS_WebConfService_Logging Policy
<b>Name</b>	OCS_WebConfService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the counters DataMCUSvc or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

Instance	Performance Object
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_WebConfService\_Logging policy.

#### OCS\_WebConfService\_PrivateBytes Policy

<b>Policy</b>	OCS_WebConfService_PrivateBytes Policy
<b>Name</b>	OCS_WebConfService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every 15 minutes.

<b>Policy</b>	OCS_WebConfService_PrivateBytes Policy
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

#### OCS\_WebConfService\_ProcessorTime Policy

<b>Policy</b>	OCS_WebConfService_ProcessorTime Policy
<b>Name</b>	OCS_WebConfService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_WebConfService\_ThreadCount Policy

<b>Policy</b>	OCS_WebConfService_ThreadCount Policy
<b>Name</b>	OCS_WebConfService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 100 <b>Critical:</b> 150

### OCS\_WebConfService\_WorkingSet Policy

<b>Policy</b>	OCS_WebConfService_WorkingSet Policy
<b>Name</b>	OCS_WebConfService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+007

### OCS\_WebConfService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_WebConfServer_PageFaultsPerSec Policy
<b>Name</b>	OCS_WebConfServer_PageFaultsPerSec
<b>Description</b>	Monitors the Page Faults/sec counter of the Web Conferencing service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Warning:</b> 50 <b>Critical:</b> 100

## WebEdgeServer

Deploy this policy group on WebEdge server. The WebEdge Server is located in the perimeter network. It enables data collaboration with external users.

This server role is collocated with the Access Edge Server, except in remote offices, where the Web Conferencing Edge Server is deployed separately because no Access Edge Servers are deployed in the remote office.

The policies in the WebEdge server group are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft Office Communications Server** → **Microsoft Office Communications Server\_2007** → **WebEdgeServer**

The policies belong to the **Measurement Threshold** Policy type.

This policy group has the following policies.

### OCS\_Check\_WebEdgeServiceStatus Policy

<b>Policy</b>	OCS_Check_WebEdgeServiceStatus Policy
<b>Name</b>	OCS_Check_WebEdgeServiceStatus
<b>Description</b>	Checks the status of the Web Conferencing Edge Service and sends a critical message if the service is not running. When you receive the critical message, click the message, and then click the Commands tab in Message Properties box. Click Start in the Operator Initiated box to restart the service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCDATAPROXY

### OCS\_WebEdgeService\_PageFaultsPerSec Policy

<b>Policy</b>	OCS_WebEdgeService_PageFaultsPerSec Policy
<b>Name</b>	OCS_WebEdgeService_PageFaultsPerSec
<b>Description</b>	Monitors the Thread Count counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_WebEdgeService\_PrivateBytes Policy

<b>Policy</b>	OCS_WebEdgeService_PrivateBytes Policy
<b>Name</b>	OCS_WebEdgeService_PrivateBytes
<b>Description</b>	Monitors the Private Bytes counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process



<b>Policy</b>	OCS_WebEdgeService_PrivateBytes Policy
<b>Instance</b>	DataProxy
<b>Counter</b>	Private Bytes
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+0070

#### OCS\_WebEdgeService\_ProcessorTime Policy

<b>Policy</b>	OCS_WebEdgeService_ProcessorTime Policy
<b>Name</b>	OCS_WebEdgeService_ProcessorTime
<b>Description</b>	Monitors the % Processor Time counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	% Processor Time
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 80 <b>Critical:</b> 90

#### OCS\_WebEdgeService\_ThreadCount Policy

<b>Policy</b>	OCS_WebEdgeService_ThreadCount Policy
<b>Name</b>	OCS_WebEdgeService_ThreadCount
<b>Description</b>	Monitors the Thread Count counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Thread Count
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 100 <b>Critical:</b> 150

### OCS\_WebEdgeService\_WorkingSet Policy

<b>Policy</b>	OCS_WebEdgeService_WorkingSet Policy
<b>Name</b>	OCS_WebEdgeService_WorkingSet
<b>Description</b>	Monitors the Working Set counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Working Set
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 1.5e+007 <b>Critical:</b> 2e+0070

### OCS\_WebEdgeService\_Logging Policy

<b>Policy</b>	OCS_WebEdgeService_Logging Policy
<b>Name</b>	OCS_WebEdgeService_Logging
<b>Description</b>	Logs the following metrics into the data store (CODA or HP Performance Agent) for the instances DataProxy or _Total.  If a metric value is unavailable, the policy logs zero (for real or integer metrics) or an empty string (for string-valued metrics).
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	OCS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process \ Working Set
	Process \ Page Faults/sec
	Process \ Private Bytes
	Process \ Thread Count
	Process \ % Processor Time
_Total Processor	\% Processor Time



Ensure that the OCS\_CreateDataSources policy is running before deploying the OCS\_WebEdgeService\_Logging policy.

### OCS\_WebEdgeServer\_ClientsDisconPerSecInvalidCookieData Policy

<b>Policy</b>	OCS_WebEdgeServer_ClientsDisconPerSecInvalidCookieData Policy
<b>Name</b>	OCS_WebEdgeServer_ClientsDisconPerSecInvalidCookieData
<b>Description</b>	Monitors the number of clients disconnected per second due to invalid cookie data.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAPROXY - 01 - Client Connections
<b>Counter</b>	DATAPROXY - 012 - Clients disconnected per second due to invalid cookie data
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_WebEdgeServer\_ClientsDisconPerSecInvalidCookieTimestamp Policy

<b>Policy</b>	OCS_WebEdgeServer_ClientsDisconPerSecInvalidCookieTimestamp Policy
<b>Name</b>	OCS_WebEdgeServer_ClientsDisconPerSecInvalidCookieTimestamp
<b>Description</b>	Monitors the number of clients rejected per second due to invalid timestamps.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAPROXY - 01 - Client Connections
<b>Counter</b>	DATAPROXY -008 - Clients disconnected per second due to invalid cookie timestamp
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning:</b> 50 <b>Critical:</b> 100

### OCS\_WebEdgeServer\_SystemThrottling Policy

<b>Policy</b>	OCS_WebEdgeServer_SystemThrottling Policy
<b>Name</b>	OCS_WebEdgeServer_SystemThrottling
<b>Description</b>	Indicates that system wide throttling is on.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAPROXY - 00 - Server Connections

<b>Policy</b>	OCS_WebEdgeServer_SystemThrottling Policy
<b>Instance</b>	_Total
<b>Counter</b>	DATAPROXY - 041 - System is throttling
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning: 1</b> <b>Critical: 2</b>

#### OCS\_WebEdgeServer\_ThrottledServerConnections Policy

<b>Policy</b>	OCS_WebEdgeServer_ThrottledServerConnections Policy
<b>Name</b>	OCS_WebEdgeServer_ThrottledServerConnections
<b>Description</b>	Monitors the number of server connections currently that are throttled.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:DATAPROXY - 00 - Server Connections
<b>Instance</b>	_Total
<b>Counter</b>	DATAPROXY - 034 - Current count of server connections that are throttled
<b>Threshold</b>	When the difference between two samples is greater than: <b>Warning: 1</b> <b>Critical: 2</b>

## Others

The policies in the Others group can be deployed on all Microsoft Office Communications Server 2007 server roles.

This policy group includes the following policies:

- OCS\_FwdApplicationError
- OCS\_FwdApplicationInformation
- OCS\_FwdApplicationWarning

All the three policies belong to the **Windows Event Log** policy type and are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Office\_Communications\_Server\_2007** → **Others**

#### OCS\_FwdApplicationError Policy

The OCS\_FwdApplicationError policy forwards all error messages logged in Windows Event Log using the following sources to the management console:

- OCS Server
- OCS Audio-Video Conferencing Server

- OCS Communicator Web Access Session Service
- OCS Data MCU
- OCS IM MCU
- OCS Intelligent IM Filter
- OCS MCU Infrastructure
- OCS Mediation Server
- OCS Protocol Stack
- OCS QoE Monitoring Server
- OCS User Replication
- OCS User Services
- OCS WMI Event Provider
- OCS ACP MCU
- OCS Address Book Server
- OCS Applications Module
- OCS AppDomain Host Process
- OCS Archiving Agent
- OCS Certificate Manager
- OCS Exchange Unified Message Routing
- OCS Inbound Routing
- OCS MCU Factory
- OCS MCU Infrastructure
- OCS Outbound Routing
- OCS Translation Service
- OCS User Replicator
- OCS User Services
- OCS WMI Consumer
- OCS WMI Provider
- OCS Archiving Server
- OCS Distribution List Expansion Web Service
- OCS Web Conferencing Edge Server
- OCS LDM

#### [OCS\\_FwdApplicationInformation](#)

The OCS\_FwdApplicationInformation policy forwards all informational messages logged in Windows Event Log using the following sources to the management console:

- OCS Server
- OCS Audio-Video Conferencing Server
- OCS Communicator Web Access Session Service

- OCS Data MCU
- OCS IM MCU
- OCS Intelligent IM Filter
- OCS MCU Infrastructure
- OCS Mediation Server
- OCS Protocol Stack
- OCS QoE Monitoring Server
- OCS User Replication
- OCS User Services
- OCS WMI Event Provider
- OCS ACP MCU
- OCS Address Book Server
- OCS Applications Module
- OCS AppDomain Host Process
- OCS Archiving Agent
- OCS Certificate Manager
- OCS Exchange Unified Message Routing
- OCS Inbound Routing
- OCS MCU Factory
- OCS MCU Infrastructure
- OCS Outbound Routing
- OCS Translation Service
- OCS User Replicator
- OCS User Services
- OCS WMI Consumer
- OCS WMI Provider
- OCS Archiving Server
- OCS Distribution List Expansion Web Service
- OCS Web Conferencing Edge Server
- OCS LDM

#### [OCS\\_FwdApplicationWarning](#)

The `OCS_FwdApplicationWarning` policy forwards all warning messages logged in Windows Event Log using the following sources to the management console:

- OCS Server
- OCS Audio-Video Conferencing Server
- OCS Communicator Web Access Session Service
- OCS Data MCU

- OCS IM MCU
- OCS Intelligent IM Filter
- OCS MCU Infrastructure
- OCS Mediation Server
- OCS Protocol Stack
- OCS QoE Monitoring Server
- OCS User Replication
- OCS User Services
- OCS WMI Event Provider
- OCS ACP MCU
- OCS Address Book Server
- OCS Applications Module
- OCS AppDomain Host Process
- OCS Archiving Agent
- OCS Certificate Manager
- OCS Exchange Unified Message Routing
- OCS Inbound Routing
- OCS MCU Factory
- OCS MCU Infrastructure
- OCS Outbound Routing
- OCS Translation Service
- OCS User Replicator
- OCS User Services
- OCS WMI Consumer
- OCS WMI Provider
- OCS Archiving Server
- OCS Distribution List Expansion Web Service
- OCS Web Conferencing Edge Server
- OCS LDM

# Microsoft Enterprise Servers SPI Microsoft Office Communications Server 2007 Reports

The following sections describe the Microsoft Enterprise Servers SPI Microsoft Office Communications Server 2007 reports.

## Front End Service CPU Statistics

The Front End Service CPU Statistics report shows CPU statistics of the front end service compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics includes the percentage of CPU time used by the front end service compared with the percentage of time the system's CPU was busy.

## IM Conferencing Service CPU Statistics

The IM Conferencing Service CPU Statistics report shows CPU statistics of the IM conferencing service compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics includes the percentage of CPU time used by the IM conferencing compared with the percentage of time the system's CPU was busy.

## Access Edge Service CPU Statistics

The Access Edge Service CPU Statistics report shows CPU statistics of the access edge service compared with overall CPU statistics of the system, in graphical and tabular formats. The summarized process statistics includes the percentage of CPU time used by the access edge compared with the percentage of time the system's CPU was busy.

## Front End Service Memory Statistics

The Front End Service Memory Statistics report shows summary memory statistics of the front end service in graphical and tabular formats. The summarized process statistics includes the page faults per second, private bytes, and working set used by the front end service.

## IM Conferencing Service Memory Statistics

The IM Conferencing Service Memory Statistics report shows summary memory statistics of the IM conferencing service, in graphical and tabular formats. The summarized process statistics includes the page faults per second, private bytes, and working set used by the IM conferencing service.

## Access Edge Service Memory Statistics

The Access Edge Service Memory Statistics report shows summary memory statistics of the access edge service, in graphical and tabular formats. The summarized process statistics includes the page faults per second, private bytes, and working set used by the access edge service.



## SQL Back End Latency Experienced By Front End Server

The SQL Back End Latency Experienced By Front End Server report shows the time that a request spent in the queue to the SQL back end and the time taken by the back end to process. The report is shown in graphical (line graph) and tabular formats. If either the queue latency or processing latency is high, the front end will start throttling requests to the back end.

## Average Holding Time for Incoming Messages on Front End Server

The Average Holding Time for Incoming Messages on Front End Server report shows the average holding time for incoming messages on the front end server, in graphical (line graph) and tabular formats. A high value indicates that the front end server is overloaded and unable to process the requests on time.

## Front End Server Availability and Connectivity

The Front End Server Availability and Connectivity report shows the Local 503 Responses/sec and the Local 504 Responses/sec on the front end server, in graphical (line graph) and tabular formats. The 503 code indicates that the server is unavailable while the 504 code indicates that there are connectivity problems with other servers.

## Sends Outstanding on Front End Server

The Sends Outstanding on Front End Server report shows the Sends Outstanding on the front end server, in graphical (line graph) and tabular formats. A high value means that a large number of requests and responses are queued outbound and this could be due to network latency issues or a problem with a remote server.

## Average Incoming Message Processing Time on Access Edge Server

The Average Incoming Message Processing Time on Access Edge Server report needs to depict the average incoming message processing time on the access edge server, in graphical (line graph) and tabular formats. High values indicate that the access edge server is overloaded and unable to process the requests on time.

## Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server

The Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server report shows the client request errors/sec, client send request errors/sec and the idle sessions timed-out/sec over UDP on the Audio/Video Edge Server, in graphical and tabular formats. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you may need to increase the session idle timeout parameter.

## Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server

The Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server report shows the client requests errors/sec, client send request errors/sec and the idle sessions timed-out/sec over TCP on the Audio/Video Edge Server in graphical and tabular format. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you may need to increase the session idle timeout parameter.

## Data Store Table for Microsoft Enterprise Server

The Microsoft Enterprise SPI creates the following data tables for Microsoft Office Communication Server 2007 metrics in the data store on the node to facilitate the data-collection procedure.

Report Name	Report Table	Report Table Attributes	Data Store Data Class
g_Front End Service CPU Statistics.rpt  Policy logging data: OCS_FrontEndService_Logging	OCS_PROCESS	<ul style="list-style-type: none"> <li>• PCTPROCESSORTIME</li> <li>• THREADCOUNT</li> <li>• SYSPCTPROCESSOR TIME</li> </ul>	OCS_PROCESS
g_IM Conferencing Service CPU Statistics.rpt  Policy logging data: OCS_IMConfService_Logging	OCS_PROCESS	<ul style="list-style-type: none"> <li>• PCTPROCESSORTIME</li> <li>• THREADCOUNT</li> <li>• SYSPCTPROCESSOR TIME</li> </ul>	OCS_PROCESS
g_Access Edge Service CPU Statistics.rpt  Policy logging data: OCS_AccessEdgeService_Logging	OCS_PROCESS	<ul style="list-style-type: none"> <li>• PCTPROCESSORTIME</li> <li>• THREADCOUNT</li> <li>• SYSPCTPROCESSOR TIME</li> </ul>	OCS_PROCESS
g_Front End Service Memory Statistics.rpt  Policy logging data: OCS_FrontEndService_Logging	OCS_PROCESS	<ul style="list-style-type: none"> <li>• PAGEFAULTS</li> <li>• WORKINGSET</li> <li>• PRIVATEBYTES</li> </ul>	OCS_PROCESS
g_IM Conferencing Service Memory Statistics.rpt  Policy logging data: OCS_IMConfService_Logging	OCS_PROCESS	<ul style="list-style-type: none"> <li>• PAGEFAULTS</li> <li>• WORKINGSET</li> <li>• PRIVATEBYTES</li> </ul>	OCS_PROCESS
g_Access Edge Service Memory Statistics.rpt  Policy logging data: OCS_AccessEdgeService_Logging	OCS_PROCESS	<ul style="list-style-type: none"> <li>• PAGEFAULTS</li> <li>• WORKINGSET</li> <li>• PRIVATEBYTES</li> </ul>	OCS_PROCESS
g_SQL Back End Latency.rpt  Policy logging data: OCS_FrontEndServer_Logging	OCS_FRONTEND	<ul style="list-style-type: none"> <li>• QUEUELATENCY</li> <li>• SPROCLATENCY</li> </ul>	OCS_FRONTEND

<b>Report Name</b>	<b>Report Table</b>	<b>Report Table Attributes</b>	<b>Data Store Data Class</b>
g_Average Holding Time for Incoming Messages on Front End Server.rpt  Policy logging data: OCS_FrontEndServer_Logging	OCS_FRONTEND	HOLDINGTIMEFORINCM SG	OCS_FRONTEND
g_Front End Server Availability and Connectivity.rpt  Policy logging data: OCS_FrontEndServer_Logging	OCS_FRONTEND	<ul style="list-style-type: none"> <li>• LOCAL503RESPONSES</li> <li>• LOCAL504RESPONSES</li> </ul>	OCS_FRONTEND
g_Sends Outstanding on Front End Server.rpt  Policy logging data: OCS_FrontEndServer_Logging	OCS_FRONTEND	SENDSOUTSTANDING	OCS_FRONTEND
g_Average Incoming Message Processing Time on Access Edge Server.rpt  Policy logging data: OCS_AccessEdgeServer_Logging	OCS_ACCESS EDGE	AVINCMMSGPROCTIME	OCS_ACCESS EDGE
g_UDP Client Request Errors and Timed Out Sessions on Audio/Video Edge Server.rpt	OCS_AVEDGE	<ul style="list-style-type: none"> <li>• UDPCLIENTREQERR</li> <li>• UDPCLIENTSENDERR</li> <li>• UDPSESSIONTIME OUTS</li> </ul>	OCS_AVEDGE
g_TCP Client Request Errors and Timed Out Sessions on Audio/Video Edge Server.rpt  Policy logging data: OCS_AVEEdgeServer_Logging	OCS_AVEDGE	<ul style="list-style-type: none"> <li>• TCPCLIENTREQERR</li> <li>• TCPCLIENTSENDERR</li> <li>• TCPSESSIONTIME OUTS</li> </ul>	OCS_AVEDGE

## Microsoft Enterprise Servers SPI Microsoft Office Communications Server 2007 Graphs

Graphs are pictorial representations of various metrics and contain data collected by policies. The following sections describe the Microsoft Office Communications Server 2007 SPI graphs.

## Front End Service CPU statistics

The Front End Service CPU statistics graph shows the CPU statistics of the Front End service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the Front End service is utilizing the processor time.

This graph uses the data collected by the `OCS_FrontEndService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Web Conferencing Service CPU statistics

The Web Conferencing Service CPU statistics graph shows the CPU statistics of the web conferencing service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the web conferencing service is utilizing the processor time.

This graph uses the data collected by the `OCS_WebConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## IM Conferencing Service CPU statistics

The IM Conferencing Service CPU statistics graph shows the CPU statistics of the IM conferencing service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the IM conferencing service is utilizing the processor time.

This graph uses the data collected by the `OCS_IMConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Telephony Conferencing Service CPU statistics

The Telephony Conferencing Service CPU statistics graph shows the CPU statistics of the telephony conferencing service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the telephony conferencing service is utilizing the processor time.

This graph uses the data collected by the `OCS_TelConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Audio/Video Conferencing Service CPU statistics

The Audio/Video Conferencing Service CPU statistics graph shows the CPU statistics of the audio/video conferencing service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the audio/video conferencing service is utilizing the processor time.

This graph uses the data collected by the `OCS_AVConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Access Edge Service CPU statistics

The Access Edge Service CPU statistics graph shows the CPU statistics of the access edge service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the access edge service is utilizing the processor time.

This graph uses the data collected by the OCS\_AccessEdgeService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Audio/Video Edge Service CPU statistics

The Audio/Video Edge Service CPU statistics graph shows the CPU statistics of the audio/video edge service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the audio/video edge service is utilizing the processor time.

This graph uses the data collected by the OCS\_AVEdgeService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Audio/Video Authentication Service CPU statistics

The Audio/Video Authentication Service CPU statistics graph shows the CPU statistics of the audio/video authentication service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the audio/video authentication service is utilizing the processor time.

This graph uses the data collected by the OCS\_AVAAuthService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Web Conferencing Edge Service CPU statistics

The Web Conferencing Edge Service CPU statistics graph shows the CPU statistics of the web conferencing edge service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the web conferencing edge service is utilizing the processor time.

This graph uses the data collected by the OCS\_WebEdgeService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Archiving and CDR Service CPU statistics

The Archiving and CDR Service CPU statistics graph shows the CPU statistics of the Archiving and CDR service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the Archiving and CDR service is utilizing the processor time.

This graph uses the data collected by the OCS\_ArchivingCDRService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Mediation Service CPU statistics

The Mediation Service CPU statistics graph shows the CPU statistics of the mediation service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the mediation service is utilizing the processor time.

This graph uses the data collected by the `OCS_MediationService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Front End Service Memory Statistics

The Front End Service Memory Statistics graph shows the memory statistics of the front end service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the front end service.

This graph uses the data collected by the `OCS_FrontEndService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Web Conferencing Service Memory Statistics

The Web Conferencing Service Memory Statistics graph shows the memory statistics of the web conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the web conferencing service.

This graph uses the data collected by the `OCS_WebConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## IM Conferencing Service Memory Statistics

The IM Conferencing Service Memory Statistics graph shows the memory statistics of the IM conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the web conferencing service.

This graph uses the data collected by the `OCS_IMConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Telephony Conferencing Service Memory Statistics

The Telephony Conferencing Service Memory Statistics graph shows the memory statistics of the telephony conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the telephony conferencing service.

This graph uses the data collected by the `OCS_TelConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Audio/Video Conferencing Service Memory Statistics

The Audio/Video Conferencing Service Memory Statistics graph shows the memory statistics of the audio/video conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the audio/video conferencing service.

This graph uses the data collected by the `OCS_AVConfService_Logging` policy. In the data store of the node, the `OCS_PROCESS` table is used to construct this graph.

## Access Edge Service Memory Statistics

The Access Edge Service Memory Statistics graph shows the memory statistics of the access edge service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the access edge service.

This graph uses the data collected by the OCS\_AccessEdgeService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Audio/Video Edge Service Memory Statistics

The Audio/Video Edge Service Memory Statistics graph shows the memory statistics of the audio/video edge service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the audio/video edge service.

This graph uses the data collected by the OCS\_AVEdgeService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Audio/Video Authentication Service Memory Statistics

The Audio/Video Authentication Service Memory Statistics graph shows the memory statistics of the audio/video authentication service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the audio/video authentication service.

This graph uses the data collected by the OCS\_AVAuthService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Web Conferencing Edge Service Memory Statistics

The Web Conferencing Edge Service Memory Statistics graph shows the memory statistics of the web conferencing edge service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the web conferencing edge service.

This graph uses the data collected by the OCS\_WebEdgeService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Archiving and CDR Service Memory Statistics

The Archiving and CDR Service Memory Statistics graph shows the memory statistics of the Archiving and CDR service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the Archiving and CDR service.

This graph uses the data collected by the OCS\_ArchivingCDRService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.

## Mediation Service Memory Statistics

The Mediation Service Memory Statistics graph shows the memory statistics of the mediation service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the mediation service.

This graph uses the data collected by the OCS\_MediationService\_Logging policy. In the data store of the node, the OCS\_PROCESS table is used to construct this graph.



## Authentication failures/sec on Audio/Video Edge Server

The Authentication failures/sec on Audio/Video Edge Server graph shows the authentication failures per sec over UDP and TCP on the A/V Edge Server

This graph uses the data collected by the OCS\_AVEdgeServer\_Logging policy. In the data store of the node, the OCS\_AVEDGE table is used to construct this graph.

## SQL Back End Latency Experienced By Front End Server

The SQL Back End Latency Experienced By Front End Server graph shows the amount of time that a request spent in the queue to the SQL back end and the time taken by the SQL backend to process a request. If either the queue latency or processing latency is high, the front end will start throttling requests to the back end.

This graph uses the data collected by the OCS\_FrontEndServer\_Logging policy. In the data store of the node, the OCS\_FRONTEND table is used to construct this graph.

## Average Holding Time for Incoming Messages on Front End Server

The Average Holding Time for Incoming Messages on Front End Server graph shows the average holding time for incoming messages on the front end server. A high value indicates that the front end server is overloaded and unable to process the requests on time.

This graph uses the data collected by the OCS\_FrontEndServer\_Logging policy. In the data store of the node, the OCS\_FRONTEND table is used to construct this graph.

## Front End Server Availability and Connectivity

The Front End Server Availability and Connectivity graph shows the Local 503 Responses/sec on the front end server. The 503 code indicates that the server is unavailable while the 504 code indicates connectivity problems with other servers.

This graph uses the data collected by the OCS\_FrontEndServer\_Logging policy. In the data store of the node, the OCS\_FRONTEND table is used to construct this graph.

## Sends Outstanding on Front End Server

The Sends Outstanding on Front End Server graph shows the Sends Outstanding on the front end server. A high value means that a large number of requests and responses are queued outbound and could be due to network latency issues or a problem with a remote server.

This graph uses the data collected by the OCS\_FrontEndServer\_Logging policy. In the data store of the node, the OCS\_FRONTEND table is used to construct this graph.

## Average Incoming Message Processing Time on Access Edge Server

The Average Incoming Message Processing Time on Access Edge Server graph shows the Average Incoming Message Processing Time on the Access Edge Server . High values indicate that the Access Edge Server is overloaded and unable to process the requests on time.

This graph uses the data collected by the OCS\_AccessEdgeServer\_Logging policy. In the data store of the node, the OCS\_ACCESSEEDGE table is used to construct this graph.



## Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server

The Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server graph shows the client requests errors/sec, client send request errors/sec and the idle sessions timed-out/sec over UDP on the Audio/Video Edge Server. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you can increase the session idle timeout parameter.

This graph uses the data collected by the OCS\_AVEdgeServer\_Logging policy. In the data store of the node, the OCS\_AVEDGE table is used to construct this graph.

## Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server

The Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server graph shows the client requests errors/sec, client send request errors/sec and the idle sessions timed-out/sec over TCP on the Audio/Video Edge Server. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you can increase the session idle timeout parameter.

This graph uses the data collected by the OCS\_AVEdgeServer\_Logging policy. In the data store of the node, the OCS\_AVEDGE table is used to construct this graph.

## Data Store Table for Microsoft Enterprise Server

The Microsoft Enterprise SPI creates the following data tables for Microsoft Office Communication Server 2007 metrics in the data store on the node to facilitate the data-collection procedure.

<b>Graph Name</b>	<b>Policy Logging Data</b>	<b>Spec File</b>	<b>Data Store Data Class</b>
Front End Service CPU Statistics	OCS_FrontEndService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Web Conferencing Service CPU Statistics	OCS_WebConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
IM Conferencing Service CPU Statistics	OCS_IMConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Telephony Conferencing Service CPU statistics	OCS_TelConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Audio/Video Conferencing Service CPU statistics	OCS_AVConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Access Edge Service CPU statistics	OCS_AccessEdgeService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Audio/Video Edge Service CPU statistics	OCS_AVEdgeService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Audio/Video Authentication Service CPU statistics	OCS_AVAuthService_Logging	OCS_PROCESS.spec	OCS_PROCESS

<b>Graph Name</b>	<b>Policy Logging Data</b>	<b>Spec File</b>	<b>Data Store Data Class</b>
Web Conferencing Edge Service CPU statistics	OCS_WebEdgeService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Archiving and CDR Service CPU statistics	OCS_ArchivingCDRService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Mediation Service CPU statistics	OCS_MediationService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Front End Service Memory Statistics	OCS_FrontEndService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Web Conferencing Service Memory Statistics	OCS_WebConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
IM Conferencing Service Memory Statistics	OCS_IMConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Telephony Conferencing Service Memory Statistics	OCS_TelConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Audio/Video Conferencing Service Memory Statistics	OCS_AVConfService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Access Edge Service Memory Statistics	OCS_AccessEdgeService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Audio/Video Edge Service Memory Statistics	OCS_AVEdgeService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Audio/Video Authentication Service Memory Statistics	OCS_AVAuthService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Web Conferencing Edge Service Memory Statistics	OCS_WebEdgeService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Archiving and CDR Service Memory Statistics	OCS_ArchivingCDRService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Mediation Service Memory Statistics	OCS_MediationService_Logging	OCS_PROCESS.spec	OCS_PROCESS
Authentication Failures/sec on Audio/Video Edge Server	OCS_AVEdgeServer_Logging	OCS_AVEDGE.spec	OCS_AVEDGE
SQL Back End Latency Experienced By Front End Server	OCS_FrontEndServer_Logging	OCS_FRONTEND.spec	OCS_FRONTEND
Average Holding Time for Incoming Messages on Front End Server	OCS_FrontEndServer_Logging	OCS_FRONTEND.spec	OCS_FRONTEND

<b>Graph Name</b>	<b>Policy Logging Data</b>	<b>Spec File</b>	<b>Data Store Data Class</b>
Front End Server Availability and Connectivity	OCS_FrontEndServer_Logging	OCS_FRONTEND.spec	OCS_FRONTEND
Sends Outstanding on Front End Server	OCS_FrontEndServer_Logging	OCS_FRONTEND.spec	OCS_FRONTEND
Average Incoming Message Processing Time on Access Edge Server	OCS_AccessEdgeServer_Logging	OCS_ACCESEEDGE.spec	OCS_ACCESSEDGE
Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server	OCS_AVEdgeServer_Logging	OCS_AVEDGE.spec	OCS_AVEDGE
Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server	OCS_AVEdgeServer_Logging	OCS_AVEDGE.spec	OCS_AVEDGE



# 8 Microsoft Enterprise Servers SPI for Microsoft Lync Server 2010

The Microsoft Lync Server 2010 integrates various forms of communication tools and provides a single platform that enables users to connect and access these tools, irrespective of their physical location. Microsoft Lync Server 2010 uses a secure channel for user access that simplifies communication management and deployment. In addition, Lync 2010 supports data sharing, audio/video conferencing, instant messaging, telephony by integrating with Microsoft architecture such as Office, Exchange and SharePoint.

The Microsoft Enterprise Servers SPI monitors the Microsoft Lync Server 2010 and enables seamless flow of communications within the enterprise. The Microsoft Enterprise Servers SPI offers the following policies for process monitoring, service management, and data logging. The logged data is used to generate the Lync Server 2010 reports and graphs.

## Policies

The Microsoft SharePoint 2010 server has the following policy groups:

- Archiving Server
- AVConfServer
- Director Server
- Discovery
- Edge Server
- Front End Server
- Mediation Server
- Monitoring Server
- Registrar

## Archiving Server

The Archiving Server archives instant messages (IM) content received by the Lync Server 2010. This server role includes the Archiving service and the Archiving database. All IM conversations and group conferences are stored in a SQL database, also called the Archiving database.

To implement archiving support, you must deploy more Archiving Servers in the organization such that the Enterprise pool or Standard Edition Server communicates with the Archiving Server. You can deploy the database for the Archiving Server on the same computer as the Archiving Server or on a separate computer.

## General Policies

The General policy group contains all the policies that monitor the processes and services of the Archiving Server.

### LS\_Archiving\_AvgNoOfBlkedClientThreads

<b>Policy Name</b>	LS_Archiving_AvgNoOfBlkedClientThreads Policy
<b>Description</b>	This policy monitors the average number of client threads that are blocked and waiting for the decrease in the queue depth.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:Arch Service - 00 - DBArch
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 024 - Flow-controlled Connections Dropped
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	0
<b>Critical</b>	100

### LS\_Archiving\_AvgTimeRequestHeldInDB

<b>Policy Name</b>	LS_Archiving_AvgTimeRequestHeldInDB Policy
<b>Description</b>	This policy monitors the average time (in milliseconds) spent by a request in the database queue before it is processed.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:Arch Service - 00 - DBArch
<b>Instance</b>	All instances
<b>Counter</b>	Arch Service - 002 - Queue Latency (msec)
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	0
<b>Critical</b>	100

### LS\_Archiving\_Logging

<b>Policy Name</b>	LS_Archiving_Logging Policy
<b>Description</b>	This policy logs the following metrics into the data store (CODA or HP Performance Agent) for the counters RTCArch or _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCArch	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	\% Processor Time

### LS\_Archiving\_NumOfDroppedMQMessages

<b>Policy Name</b>	LS_Archiving_NumOfDroppedMQMessages Policy
<b>Description</b>	This policy monitors MSMQ for the number of messages getting dropped.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:Arch Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	Arch Service - 006 - Dropped messages from MQ
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	0
<b>Critical</b>	1

**LS\_Archiving\_NumberOfMessagesNotWrittenToDB**

<b>Policy Name</b>	LS_Archiving_NumberOfMessagesNotWrittenToDB Policy
<b>Description</b>	This policy monitors the rate of failure in numbers when the messages are written in to the SQL database.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:Arch Service - 02 - WRITE
<b>Instance</b>	All instances
<b>Counter</b>	Arch Service - 002 - Messages failed to be written to DB
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	0
<b>Critical</b>	1

**LS\_Archiving\_NumberOfValidationFailedMessages**

<b>Policy Name</b>	LS_Archiving_NumberOfValidationFailedMessages Policy
<b>Description</b>	This policy monitors the number of messages for which the validation has failed.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:Arch Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	Arch Service - 002 - Messages that failed validation
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	0
<b>Critical</b>	1

**LS\_Archiving\_PageFaultsPerSec**

<b>Policy Name</b>	LS_Archiving_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter of the Archiving Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process



<b>Policy Name</b>	LS_Archiving_PageFaultsPerSec Policy
<b>Instance</b>	RTCArch
<b>Counter</b>	PageFaults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_Archiving\_PrivateBytes

<b>Policy Name</b>	LS_Archiving_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Archiving and CDR service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_Archiving\_ProcessorTime

<b>Policy Name</b>	LS_Archiving_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Archiving and CDR service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Archiving\_ThreadCount

<b>Policy Name</b>	LS_Archiving_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available in the Archiving and CDR service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_Archiving\_WorkingSet

<b>Policy Name</b>	LS_Archiving_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter available in the Archiving and CDR service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCArch
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Check\_Arch\_ADStatus

<b>Policy Name</b>	LS_Check_Arch_ADStatus Policy
<b>Description</b>	This policy checks the connectivity status of the Active Directory with the Archiving Server and sends a critical alert message if the Active Directory is not accessible from the Archiving Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Check\_Arch\_ReplicaStatus

<b>Policy Name</b>	LS_Check_Arch_ReplicaStatus Policy
<b>Description</b>	This policy checks the Central Management Store replication status at the Archiving Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	REPLICA

### LS\_Check\_ArchivingServiceStatus

<b>Policy Name</b>	LS_Check_ArchivingServiceStatus Policy
<b>Description</b>	This policy checks the status of the Archiving Service and returns values that correspond to different states of the 'RTCLOG'. This policy sends a critical alert message if the Archiving Service is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCLOG

### LS\_Check\_ReplicaServiceStatus\_Arch

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Arch Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Archiving Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

### LS\_Replica\_PageFaultsPerSec

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

#### LS\_Replica\_PrivateBytes

<b>Policy Name</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

#### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_Replica\_ThreadCount

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_Replica\_WorkingSet

<b>Policy Name</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set Counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

## GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the Archiving Server.

### LS\_Check\_ArchivingServiceStatus

<b>Policy</b>	LS_Check_ArchivingServiceStatus Policy
<b>Description</b>	This policy checks the status of the Archiving Service and returns values that correspond to different states of the 'RTCLOG'. This policy sends a critical alert message if the Archiving Service is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCLOG

## LS\_Check\_ReplicaServiceStatus\_Arch

<b>Policy</b>	LS_Check_ReplicaServiceStatus_Arch Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Archiving Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

## AVConfServer

The A/V Conferencing Server is a server role that controls and integrates the audio/video inputs from various sources required during multiparty audio/video conferences.

The AV Conferencing Server is located in the internal network. It enables audio and video peer-to-peer communications and audio and video conferencing. This server role is available on a Standard Edition Server.

In an Enterprise pool, you can either join it with the Front End Server and the Web Conferencing Server or can deploy it on a separate server.

## General Policies

The General policy group contains all policies that monitor the processes and services of the A/V Conferencing Server.

### LS\_Replica\_PageFaultsPerSec

<b>Policy</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_AVConf\_ETAToProcessItemsInHttpStack

<b>Policy</b>	LS_AVConf_ETAToProcessItemsInHttpStack Policy
<b>Description</b>	This policy monitors the time taken in HTTP stack to process all pending transactions. It is measured in milliseconds.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:AVMCU - 04 - MCU Health And Performance
<b>Instance</b>	All instances
<b>Counter</b>	AVMCU - 000 - HTTP Stack load
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	30000
<b>Critical</b>	120000

### LS\_AVConf\_Logging

<b>Policy</b>	LS_AVConf_Logging Policy
<b>Description</b>	This policy collects data for the Audio/Video Conferencing Service and logs the following metrics into the data store (CODA or HP Performance Agent) for the instances AVMCUSvc or _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
AVMCUSvc	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	\% Processor Time

**LS\_AVConf\_MCUHealthState**

<b>Policy</b>	LS_AVConf_MCUHealthState Policy
<b>Description</b>	This policy monitors the current health of the AVMCU. If the value is 0, it indicates that the MCU is normal, 1 indicates loaded, 2 indicates full and 3 indicates unavailable.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:AVMCU - 04 - MCU Health And Performance
<b>Instance</b>	All instances
<b>Counter</b>	AVMCU - 005 - MCU Health State
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	1
<b>Critical</b>	2

**LS\_AVConf\_NoOfAddConfFailed**

<b>Policy</b>	LS_AVConf_NoOfAddConfFailed Policy
<b>Description</b>	This policy monitors number of failed responses returned by add-conference.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:AVMCU - 03 - CCCP Processing
<b>Instance</b>	All instances
<b>Counter</b>	AVMCU - 029 - Number of add conference requests failed
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

**LS\_AVConf\_NumberOfActiveConferences**

<b>Policy</b>	LS_AVConf_NumberOfActiveConferences Policy
<b>Description</b>	This policy monitors the number of active conferences on the A/V Conferencing Server.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:AVMCU - 00 - Operations
<b>Instance</b>	All instances
<b>Counter</b>	AVMCU - 000 - Number of Conferences



<b>Policy</b>	LS_AVConf_NumberOfActiveConferences Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	4000
<b>Critical</b>	5000

#### LS\_AVConf\_PageFaultsPersec

<b>Policy</b>	LS_AVConf_PageFaultsPersec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Audio/Video Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

#### LS\_AVConf\_PrivateBytes

<b>Policy</b>	LS_AVConf_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

#### LS\_AVConf\_ProcessorTime

<b>Policy</b>	LS_AVConf_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy</b>	LS_AVConf_ProcessorTime Policy
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

#### LS\_AVConf\_ThreadCount

<b>Policy</b>	LS_AVConf_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available in the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 150</b>

#### LS\_AVConf\_WorkingSet

<b>Policy</b>	LS_AVConf_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter available in the Audio/Video Conferencing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	AVMCUSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_Check\_AVConfServiceStatus

<b>Policy</b>	LS_Check_AVConfServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of the 'RTCAVMCU'. This policy checks the status of the Audio/Video Conferencing Service and sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCAVMCU

### LS\_Check\_AVConf\_ADStatus

<b>Policy</b>	LS_Check_AVConf_ADStatus Policy
<b>Description</b>	This policy checks the connectivity status of the Active Directory with the AV Conferencing Server and sends a critical alert message if the Active Directory is not accessible from the AV Conferencing Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Check\_AVConf\_ReplicaStatus

<b>Policy</b>	LS_Check_AVConf_ReplicaStatus Policy
<b>Description</b>	This policy checks the Central Management Store replication status at the A/V Conferencing Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	REPLICA

### LS\_Check\_ReplicaServiceStatus\_AVConf

<b>Policy</b>	LS_Check_ReplicaServiceStatus_AVConf Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the A/V Conferencing Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

### LS\_Replica\_PrivateBytes

<b>Policy</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Replica\_ProcessorTime

<b>Policy</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Replica\_ThreadCount

<b>Policy</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_Replica\_WorkingSet

<b>Policy</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set Counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the AVConfServer.

### LS\_Check\_AVConfServiceStatus

<b>Policy</b>	LS_Check_AVConfServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of the 'RTCAYMCU'. This policy checks the status of the Audio/Video Conferencing Service and sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCAYMCU

### LS\_Check\_ReplicaServiceStatus\_AVConf

<b>Policy</b>	LS_Check_ReplicaServiceStatus_AVConf Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the A/V Conferencing Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

### Common

The Common policy group contains a set of policies that can be deployed on all the Microsoft Lync Server 2010 server roles.

This policy group includes the following policies:

- LS\_FwdApplicationError
- LS\_FwdApplicationInformation
- LS\_FwdApplicationWarning

All the three policies belong to the **Windows Event Log** policy type and are available at the following location: **SPI for Microsoft Enterprise Servers** → **en** → **Microsoft\_Office\_Communications\_Server** → **Microsoft\_Lync\_Server\_2010** → **Common**

## Director Server

The Director is a server role that validates the internal and external users and directs traffic between the Edge Servers and the internal Office Communications Server deployment. The Director server role is supported only in an internal trusted network.

### General Policies

The General policy group contains all the policies that monitor the processes and services of the Director Server.

#### LS\_Check\_FrontEndServiceStatus

<b>Policy Name</b>	LS_Check_FrontEndServiceStatus Policy
<b>Description</b>	This policy returns the values that correspond to different states of the 'RTCSrv'. This policy sends a critical alert message if the FrontEnd Service is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCSRVR

#### LS\_Check\_Director\_ADStatus

<b>Policy Name</b>	LS_Check_Director_ADStatus Policy
<b>Description</b>	This policy checks the connectivity status of the Active Directory with the Director Server and sends a critical alert message if the Active Directory is not accessible from the Director Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Check\_Director\_ReplicaStatus

<b>Policy Name</b>	LS_Check_Director_ReplicaStatus Policy
<b>Description</b>	This policy checks the Central Management Store replication status at the Director Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	REPLICA

### LS\_Check\_ReplicaServiceStatus\_Director

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Director Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Director Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Check\_DirectorServiceStatus

<b>Policy Name</b>	LS_Check_DirectorServiceStatus Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Director Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Director\_NoOfLDAPErrorsPerSec

<b>Policy Name</b>	LS_Director_NoOfLDAPErrorsPerSec Policy
<b>Description</b>	This policy monitors the total number of outstanding searches on this LDAP session in the Directory Search component of the Communications Server User Servers Module associated with a GC.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 000 - Number of outstanding searches
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Director\_NoOfOutStandingSearches

<b>Policy Name</b>	LS_Director_NoOfOutStandingSearches Policy
<b>Description</b>	This policy monitors the number of outstanding searches on the LDAP session, per second, in the Directory Search component of Communications Server User Servers module associated with a GC.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 004 - Number of LDAP errors / sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Director\_SearchLatency

<b>Policy Name</b>	LS_Director_SearchLatency Policy
<b>Description</b>	This policy monitors the average time (in seconds) it takes to perform the actual LDAP search.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 005 - Search Latency (ms)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Director\_SprocLatency

<b>Policy Name</b>	LS_Director_SprocLatency Policy
<b>Description</b>	This policy monitors the average time taken in processing a RTCAuthorizeDelegate sproc call.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 31 - Authorize delegate sproc
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 001 - Sproc Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>



### LS\_FrontEnd\_PageFaultsPerSec

<b>Policy Name</b>	LS_FrontEnd_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

### LS\_FrontEnd\_PrivateBytes

<b>Policy Name</b>	LS_FrontEnd_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_FrontEnd\_ProcessorTime

<b>Policy Name</b>	LS_FrontEnd_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_FrontEnd\_ThreadCount

<b>Policy Name</b>	LS_FrontEnd_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available in the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 150</b>

### LS\_FrontEnd\_WorkingSet

<b>Policy Name</b>	LS_FrontEnd_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter available in the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_Replica\_PageFaultsPerSec

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

### LS\_Replica\_PrivateBytes

<b>Policy Name</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_Replica\_ThreadCount

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 150</b>

### LS\_Replica\_WorkingSet

<b>Policy Name</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter available in the Lync Server Replica Replicator Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the Director Server.

### LS\_Check\_FrontEndServiceStatus

<b>Policy Name</b>	LS_Check_FrontEndServiceStatus Policy
<b>Description</b>	This policy returns the values that correspond to different states of the 'RTCSrv'. It sends a critical alert message if the FrontEnd Service is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCSRV

### LS\_Check\_ReplicaServiceStatus\_Director

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Director Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Director Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Director\_NoOfLDAPErrorsPerSec

<b>Policy Name</b>	LS_Director_NoOfLDAPErrorsPerSec Policy
<b>Description</b>	This policy monitors the total number of outstanding searches on this LDAP session in the Directory Search component of the Communications Server User Servers Module associated with a GC.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	Counter USrv - 000 - Number of outstanding searches
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Director\_SearchLatency

<b>Policy Name</b>	LS_Director_SearchLatency Policy
<b>Description</b>	This policy monitors the average time (in seconds) it takes to perform the actual LDAP search.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 005 - Search Latency (ms)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Director\_SprocLatency

<b>Policy Name</b>	LS_Director_SprocLatency Policy
<b>Description</b>	This policy monitors the average time taken in processing a RTCAuthorizeDelegate sproc call.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 31 - Authorize delegate sproc
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 001 - Sproc Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

## Discovery

The Discovery policy group contains the LS\_Discovery policy which discovers the LS roles and services. The LS\_Discovery policy discovers the roles and services of the Microsoft Lync Server 2010, along with sites, pools, and pool members, and displays them in the service tree on the management server console.

Microsoft Lync Server 2010 Discovery policy discovers the following roles and services:

- **Roles**
  - Archiving Server
  - Audio/Video Conferencing server
  - Director Server
  - Edge Server
  - Front End Server
  - Mediation Server
  - Monitoring Sever
  - Registrar Server
- **Services**
  - Lync Server Replica Replicator Agent
  - Lync Server Front-End (Registrar and other)
  - Lync Server IM Conferencing
  - Lync Server Audio Test Service
  - Lync Server Bandwidth Policy Service (Core)
  - Lync Server Bandwidth Policy Service (Authentication)
  - Lync Server Audio/Video Conferencing
  - Lync Server Application Sharing
  - Lync Server Web Conferencing
  - Lync Server Web Conferencing Compatibility
  - Lync Server Master Replicator Agent
  - Lync Server File Transfer Agent
  - Lync Server Conferencing Attendant
  - Lync Server Conferencing Announcement
  - Lync Server Response Group
  - Lync Server Call Park
  - Lync Server Mediation
  - Lync Server Front-End
  - Lync Server Registrar and other
  - Lync Server Mediation
  - Lync Server Access Edge

- Lync Server Audio/Video Edge
- Lync Server Audio/Video Authentication
- Lync Server Web Conferencing Edge
- Lync Server Audio/Video Conferencing
- Lync Server Mediation
- Lync Server Archiving
- Lync Server QoE Monitoring Service
- Lync Server Call Detail Recording

If the node, to which the policy is deployed, is a member of an LS pool, then the pool, pool type (standard/enterprise), and members of the pool are also discovered by the policy. If the agent is not running under the default account (Local System account) on the managed node, then you must create a user, who is a member of the RTCUniversalReadOnlyAdmins, if the node is a member of the LS pool. For Edge Servers, provide the privileges of a CSViewOnlyAdministrator.

Edit the username and password in the policy and enter the credentials of this user. Save and close the policy and deploy the edited policy to the node.

The username format for **HTTPS** is domain\user.

### LS\_Discovery

The LS\_Discovery policy discovers the roles and services of the Microsoft Lync Server 2010, along with sites, pools, and pool members, and displays them in the service tree on the management server console.

<b>Policy Name</b>	LS_Discovery Policy
<b>Description</b>	This policy Discovers the LS roles and services.
<b>Policy Type</b>	Service Auto-Discovery
<b>Policy Group</b>	<b>SPI for Microsoft Enterprise Servers</b> → en → <b>Microsoft_Office_Communications_Server</b> → <b>Microsoft_Lync_Server_2010</b> → <b>Discovery</b>

### Configuring LS\_Discovery Policy

The LS\_Discovery policy discovers the Microsoft Lync Server 2010 roles and services and displays them on the service tree on the console of the management server.

To run the LS\_Discovery policy on all servers, except the Edge Server, follow these steps:

- 1 Create a domain user to run the discovery policy with the following user privileges:
  - CSViewOnlyAdministrator
  - RTCUniversalReadOnlyAdmins
  - Execute permission to the %OvAgentDir%\bin\instrumentation folder on the managed node.
- 2 Open the LS\_Discovery policy.
- 3 Edit the username and password in the policy and enter the user credentials - CSViewOnlyAdministrator and RTCUniversalReadOnlyAdmins.

4 Deploy the policy on all Lync servers, except the Edge Server.

To run the LS\_Discovery policy on the Edge Server, follow these steps:

- 1 Create a user under the CSViewOnlyAdministrator account.
- 2 Open the Edge Server configuration tool **Configure Edge server Discovery for Lync Server 2010**.
- 3 In the console tree, expand **Tools** → **SPI for Microsoft Enterprise Servers Lync Server 2010**.
- 4 Double-click the **Configure Edge server Discovery for Lync Server 2010** tool in the details pane.
- 5 Right-click **All Tasks** → **Launch Tool**.
- 6 Select **Edge Sever**.
- 7 Click **Launch**.
- 8 Fill in details Edge Server details, such as:
  - Domain: <Lync Server domain name>
  - User Name: <CSViewOnlyAdministrator
  - Password: <Password>
- 9 Click **OK**.
- 10 Run the tool. Information related to the Lync Server is deployed on the Edge Server.
- 11 Create another user on the Edge Server with the user privilege 'Local Administrator' for the Edge Server .
- 12 Open the LS\_Discovery policy.
- 13 Edit the username and password in the policy and enter the user credentials of the 'Local Administrator' created on the Edge Server.
- 14 Deploy the LS\_Discovery Policy on the Edge Servers.
  - The Edge Server must be able to access all the Front End and Directors servers. Publish the SRV records or update the %SystemRoot%\System32\drivers\etc\hosts to resolve Front End and Director server FQDN to their IP.
  - Run this tool only once for every deployment on the Edge Server. If you change the CSViewOnlyAdministrator credential of the user, run the tool again with the latest user credentials.



## Edge Server

The Edge Server is a server role in the network perimeter. It provides access to external users such as remote, federated and anonymous users. The Edge Server supports connectivity with public IM service providers.

The Edge Server runs the Access Edge Service, A/V Edge Service, and Web Conferencing Edge service. These three services are automatically installed with the Edge Server.

### General Policies

The General policy group contains all the policies that monitor the processes and services of the EdgeServer.



### LS\_Replica\_PageFaultsPerSec

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

### LS\_AccessEdge\_AboveLimitConnectionsDropped

<b>Policy Name</b>	LS_AccessEdge_AboveLimitConnectionsDropped Policy
<b>Description</b>	This policy monitors total number of connections that were dropped because the limit on number of incoming connections from a federated partner or clearing house was exceeded.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 004 - Above Limit Connections Dropped (Access Proxies only)
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	1
<b>Critical</b>	2

### LS\_AccessEdge\_ActiveTLSConnections

<b>Policy Name</b>	LS_AccessEdge_ActiveTLSConnections Policy
<b>Description</b>	This policy monitors the number of established TLS connections currently active. TLS Connection is considered established when peer certificate and, possibly, host name are verified for trust relationship.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:API - 00 - API Application Instance Counters(*)
<b>Instance</b>	_Total
<b>Counter</b>	API - 026 - Transactions Pending Dispatch Completion

<b>Policy Name</b>	LS_AccessEdge_ActiveTLSConnections Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	500
<b>Critical</b>	100

#### LS\_AccessEdge\_AddressSpaceUsage

<b>Policy Name</b>	LS_AccessEdge_AddressSpaceUsage Policy
<b>Description</b>	This policy monitors the percentage of available address space currently in use by the server process.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 07 - Load Management
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 009 - Address space usage
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	65
<b>Critical</b>	75

#### LS\_AccessEdge\_AvgIncomingMsgProcessingTime

<b>Policy Name</b>	LS_AccessEdge_AvgIncomingMsgProcessingTime Policy
<b>Description</b>	This policy monitors the average processing time of an incoming message in seconds.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 021 - Average Incoming Message Processing Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

### LS\_AccessEdge\_DataLogging

<b>Policy Name</b>	LS_AccessEdge_DataLogging Policy
<b>Description</b>	This policy monitors the SIP - 017 - Sends Outstanding counter.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 021 - Average Incoming Message Processing Time

### LS\_AccessEdge\_DNSResolutionFailures

<b>Policy Name</b>	LS_AccessEdge_DNSResolutionFailures Policy
<b>Description</b>	This policy monitors the total number of DNS resolution failures.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SipEps - 02 - SipEps Connections
<b>Instance</b>	_Total
<b>Counter</b>	SipEps - 010 - NumberOfDNSResolutionFailures
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

### LS\_AccessEdge\_EventsQueueLength

<b>Policy Name</b>	LS_AccessEdge_EventsQueueLength Policy
<b>Description</b>	This policy monitors the current Queue Length of events indicated by the core manager thread.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SipEps - 00 - Sip Dialogs
<b>Instance</b>	_Total
<b>Counter</b>	SipEps - 003 - CoreManagerQueueLength
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

### LS\_AccessEdge\_ExtMsgDropDueToUnresolvedDomain

<b>Policy Name</b>	LS_AccessEdge_ExtMsgDropDueToUnresolvedDomain Policy
<b>Description</b>	This policy monitors the rate at which the number of messages are dropped at the external edge, as DNS SRV failed to resolve the domain.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 09 - Access Edge Server Messages
<b>Instance</b>	All instances.
<b>Counter</b>	SIP - 063 - External Messages/sec Dropped Due To Unresolved Domain
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

### LS\_AccessEdge\_ExtMsgDroppedDueToBlkedIMDomain

<b>Policy Name</b>	LS_AccessEdge_ExtMsgDroppedDueToBlkedIMDomain Policy
<b>Description</b>	This policy monitors the rate of messages dropped at the external edge, in a second, because of DNS SRV resolving the domain to a server blocked in the IM Service Providers table.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 09 - Access Edge Server Messages
<b>Instance</b>	All instances.
<b>Counter</b>	SIP - 065 - External Messages/sec Dropped Due To Blocked IM Service Provider Domain
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

### LS\_AccessEdge\_ExtMsgDroppedDueToIncompMsgDomain

<b>Policy Name</b>	LS_AccessEdge_ExtMsgDroppedDueToIncompMsgDomain Policy
<b>Description</b>	This policy monitors the rate at which the messages are dropped, per second, at the external edge, as the previous messages are not compatible with the federation type of domain.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 09 - Access Edge Server Messages
<b>Instance</b>	All instances.
<b>Counter</b>	SIP - 077 - External Messages/sec Dropped Due To Incompatible Message Domain
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

### LS\_AccessEdge\_ExtMsgPerSecDropDueToBlckdDomain

<b>Policy Name</b>	LS_AccessEdge_ExtMsgPerSecDropDueToBlckdDomain Policy
<b>Description</b>	This policy monitors the number of messages which are dropped at the external edge as their domain is in the blocked list, in one second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 09 - Access Edge Server Messages
<b>Instance</b>	All instances.
<b>Counter</b>	SIP - 033 - External Messages/sec Dropped Due To Blocked Domain
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

### LS\_AccessEdge\_FlowControlledConnections

<b>Policy Name</b>	LS_AccessEdge_FlowControlledConnections Policy
<b>Description</b>	This policy monitors the number of connections that are currently being flowcontrolled (no socket receives are posted).
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 023 - Flow-controlled Connections
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

### LS\_AccessEdge\_FlowControlledConnectionsDropped

<b>Policy Name</b>	LS_AccessEdge_FlowControlledConnectionsDropped Policy
<b>Description</b>	This policy monitors the total number of connections dropped because of excessive flow-control.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 024 - Flow-controlled Connections Dropped

<b>Policy Name</b>	LS_AccessEdge_FlowControlledConnectionsDropped Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

#### **LS\_AccessEdge\_IncomingMsgHeldAboveOverloadWatermark**

<b>Policy Name</b>	LS_AccessEdge_IncomingMsgHeldAboveOverloadWatermark Policy
<b>Description</b>	This policy monitors the number of incoming messages which are currently held by the server for processing more than the overload watermark time threshold.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 07 - Load Management
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 005 - Incoming Messages Held Above Overload Watermark
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

#### **LS\_AccessEdge\_IncomingRequestsDroppedPerSec**

<b>Policy Name</b>	LS_AccessEdge_IncomingRequestsDroppedPerSec Policy
<b>Description</b>	This policy monitors the rate at which the incoming requests are dropped, as they could not be processed due to bad headers, insufficient routing information, and severe resource allocation failure.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 02 - Protocol
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 005 - Incoming Requests Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 10</b>

### LS\_AccessEdge\_IncomingResponsesDroppedPerSec

<b>Policy Name</b>	LS_AccessEdge_IncomingResponsesDroppedPerSec Policy
<b>Description</b>	This policy monitors the rate at which the incoming responses are dropped per second as they could not be processed.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 02 - Protocol
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 009 - Incoming Responses Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 10</b>

### LS\_AccessEdge\_Logging

<b>Policy Name</b>	LS_AccessEdge_Logging Policy
<b>Description</b>	This policy collects data for the Access Edge Service. The LS_AccessEdge_Logging policy logs the following metrics as mentioned in the table into the data store (CODA / HP Performance Agent) for the instance _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_ACCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	Processor\% Processor Time

### LS\_AccessEdge\_MessagesInServer

<b>Policy Name</b>	LS_AccessEdge_MessagesInServer Policy
<b>Description</b>	This policy monitors the number of messages currently being processed by the server.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 02 - Protocol
<b>Instance</b>	All instances

<b>Policy Name</b>	LS_AccessEdge_MessagesInServer Policy
<b>Counter</b>	SIP - 012 - Messages In Server
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	2500
<b>Critical</b>	5000

#### LS\_AccessEdge\_MsgPerSecDroppedDueToUnknownDomain

<b>Policy Name</b>	LS_AccessEdge_MsgPerSecDroppedDueToUnknownDomain Policy
<b>Description</b>	This policy monitors the number of messages that are not routed in a second, as the message domain is not in the routing table.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 09 - Access Edge Server Messages
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 025 - Messages/sec Dropped Due To Unknown Domain
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

#### LS\_AccessEdge\_MsgsDroppedPerSecDueToCertMismatch

<b>Policy Name</b>	LS_AccessEdge_MsgsDroppedPerSecDueToCertMismatch Policy
<b>Description</b>	This policy monitors the rate at which the messages are dropped per second as they did not have an FQDN that matched the remote peer's certificate.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 02 - Protocol
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 011 - Messages/sec Dropped Due To Certificate Mismatch
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>



**LS\_AccessEdge\_NoOfMsgsDropDueToInternalSrvError**

<b>Policy Name</b>	LS_AccessEdge_NoOfMsgsDropDueToInternalSrvError Policy
<b>Description</b>	This policy monitors the number of messages dropped due to an internal server error.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS: SIP – 05 – Routing
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 022 - Messages Dropped Due To Internal Error
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	10
<b>Critical</b>	20

**LS\_AccessEdge\_NoOfMsgsDropDueToRoutingFailure**

<b>Policy Name</b>	LS_AccessEdge_NoOfMsgsDropDueToRoutingFailure Policy
<b>Description</b>	This policy monitors the total number of messages dropped due to a routing failure not covered by other counters.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS: SIP – 05 – Routing
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 021 - Messages Dropped Due To Other Routing Failure
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	10
<b>Critical</b>	20

**LS\_AccessEdge\_NoOfSrvCnxDisDueToThrottling**

<b>Policy Name</b>	LS_AccessEdge_NoOfSrvCnxDisDueToThrottling Policy
<b>Description</b>	This policy monitors the total number of server connections disconnected due to throttling.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 00 - Server Connections
<b>Instance</b>	_Total
<b>Counter</b>	DATAPROXY - 035 - Server connections disconnected due to throttling

<b>Policy Name</b>	LS_AccessEdge_NoOfSrvCnxDisDueToThrottling Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

#### LS\_AccessEdge\_PageFaultsPerSec

<b>Policy Name</b>	LS_AccessEdge_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter of Access Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_AccessEdge\_PrivateBytes

<b>Policy Name</b>	LS_AccessEdge_PrivateBytes Policy
<b>Description</b>	This policy monitors Private Bytes counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_AccessEdge\_ProcessorTime

<b>Policy Name</b>	LS_AccessEdge_ProcessorTime Policy
<b>Description</b>	This policy monitors % Processor Time counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_AccessEdge_ProcessorTime Policy
<b>Instance</b>	RTCSrv
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

#### LS\_AccessEdge\_RateOfCnxDropDueToPeer

<b>Policy Name</b>	LS_AccessEdge_RateOfCnxDropDueToPeer Policy
<b>Description</b>	This policy monitors the rate of the connections dropped, in a second, as the peer failed to exchange valid data with the server within establishing timeout.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS: SIP – 00 – Networking
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 005 - Connections Failed To Establish/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_AccessEdge\_RateOfCnxRefusedDueToSrvOverload

<b>Policy Name</b>	LS_AccessEdge_RateOfCnxRefusedDueToSrvOverload Policy
<b>Description</b>	This policy monitors the rate of the connections refused, in a second, with a Service Unavailable response because the server was overloaded.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS: SIP – 00 – Networking
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 007 - Connections Refused Due To Server Overload/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_AccessEdge\_RejExtEdgeClientConnectionsPerSec

<b>Policy Name</b>	LS_AccessEdge_RejExtEdgeClientConnectionsPerSec Policy
<b>Description</b>	This policy monitors the rate at which the number of client connections is rejected, in a second, at the external edge as the remote user access is disabled.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 08 - Access Edge Server Connections
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 015 - Rejected External Edge Client Connections/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 10</b>

### LS\_AccessEdge\_RejExtEdgeServerConnectionsPerSec

<b>Policy Name</b>	LS_AccessEdge_RejExtEdgeServerConnectionsPerSec Policy
<b>Description</b>	This policy monitors the rate of server connections rejected at the external edge in a second because all federation are disabled.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 08 - Access Edge Server Connections
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 013 - Rejected External Edge Server Connections/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 10</b>

### LS\_AccessEdge\_SendsTimedOut

<b>Policy Name</b>	LS_AccessEdge_SendsTimedOut Policy
<b>Description</b>	This policy monitors the number of sends that were dropped as they stayed in the outgoing (send) queue for a long time.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 01 - Peers
<b>Instance</b>	_Total
<b>Counter</b>	SIP - 018 - Sends Timed-Out
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	500
<b>Critical</b>	1000

### LS\_AccessEdge\_ThreadCount

<b>Policy Name</b>	LS_AccessEdge_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter of the Access Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_AccessEdge\_Throttling

<b>Policy Name</b>	LS_AccessEdge_Throttling Policy
<b>Description</b>	This policy monitors the system wide throttling.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 00 - Server Connections
<b>Instance</b>	_Total
<b>Counter</b>	DATAPROXY - 041 - System is throttling
<b>Threshold</b>	When the difference between two samples is greater than Warning and Critical values.
<b>Warning</b>	10
<b>Critical</b>	20

### LS\_AccessEdge\_TimedOutTransactions

<b>Policy Name</b>	LS_AccessEdge_TimedOutTransactions Policy
<b>Description</b>	This policy monitors the total number of transactions that have timed out.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SipEps - 01 - SipEps Transactions
<b>Instance</b>	All instances
<b>Counter</b>	SipEps - 008 - Transactions Timed Out/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 20

### LS\_AccessEdge\_WorkingSet

<b>Policy Name</b>	LS_AccessEdge_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter available in the Access Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv'
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_AVAuth\_Logging

<b>Policy Name</b>	LS_AVAuth_Logging Policy
<b>Description</b>	This policy logs the following metrics into the data store (CODA or HP Performance Agent) for the instances MRASSvc or _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_Process

Instance	Performance Object
MRASSvc	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	Processor\% Processor Time

### LS\_AVAuth\_PageFaultsPerSec

<b>Policy Name</b>	LS_AVAuth_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_AVAuth_PageFaultsPerSec Policy
<b>Instance</b>	MRASSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

#### LS\_AVAuth\_PrivateBytes

<b>Policy Name</b>	LS_AVAuth_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MRASSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

#### LS\_AVAuth\_ProcessorTime

<b>Policy Name</b>	LS_AVAuth_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MRASSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

#### LS\_AVAuth\_ThreadCount

<b>Policy Name</b>	LS_AVAuth_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_AVAuth_ThreadCount Policy
<b>Instance</b>	MRASSvc
<b>Counter</b>	ThreadCount
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

#### LS\_AVAuth\_WorkingSet

<b>Policy Name</b>	LS_AVAuth_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter of the Audio/Video Authentication service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MRASSvc
<b>Counter</b>	WorkingSet
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_AVEdge\_BadRequestsReceivedPerSec

<b>Policy Name</b>	LS_AVEdge_BadRequestsReceivedPerSec Policy
<b>Description</b>	This policy monitors the number of bad requests received in a second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Auth - 00 - Requests
<b>Instance</b>	All instances
<b>Counter</b>	- 003 - Bad Requests Received/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 20

#### LS\_AVEdge\_DataLogging

<b>Policy Name</b>	LS_AVEdge_DataLogging Policy
<b>Description</b>	This policy collects data for the LS A/V Edge Server. The LS_AVEdge_DataLogging policy logs the data into the data store (CODA / HP Performance Agent) for the instance _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_PROCESS



Instance	Performance Object
_Total	LS:A/V Edge - 00 - UDP Counters\A/V Edge - 008 - Authentication Failures/sec
	LS:A/V Edge - 01 - TCP Counters\A/V Edge - 008 - Authentication Failures/sec
	LS:A/V Edge - 00 - UDP Counters\A/V Edge - 014 - Client Request Errors/sec (4xx Responses/sec)
	LS:A/V Edge - 00 - UDP Counters\A/V Edge - 016 - Client Send Request Errors/sec
	LS:A/V Edge - 00 - UDP Counters\A/V Edge - 019 - Session Idle Timeouts/sec
	LS:A/V Edge - 01 - TCP Counters\A/V Edge - 015 - Client Request Errors/sec (4xx Responses/sec)
	LS:A/V Edge - 01 - TCP Counters\A/V Edge - 017 - Client Send Request Errors/sec
	LS:A/V Edge - 01 - TCP Counters\A/V Edge - 020 - Session Idle Timeouts/sec

### LS\_AVEdge\_Logging

<b>Policy Name</b>	LS_AVEdge_Logging Policy
<b>Description</b>	This policy collects data for the Audio/Video Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS_PROCESS

Instance	Performance Object
MediaRelaySvc	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	Process\% Processor Time

### LS\_AVEdge\_PageFaultsPerSec

<b>Policy Name</b>	LS_AVEdge_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Audio/Video Edge service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_AVEdge_PageFaultsPerSec Policy
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_AVEdge\_PrivateBytes

<b>Policy Name</b>	LS_AVEdge_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter available in the Audio/Video Edge service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_AVEdge\_ProcessorTime

<b>Policy Name</b>	LS_AVEdge_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the Audio/Video Edge service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

#### LS\_AVEdge\_TCPActiveSessionsExceedingBWLmt

<b>Policy Name</b>	LS_AVEdge_TCPActiveSessionsExceedingBWLmt Policy
<b>Description</b>	This policy monitors the number of active relay sessions over TCP, which are exceeding the bandwidth limit.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 01 - TCP Counters

<b>Policy Name</b>	LS_AVEdge_TCPActiveSessionsExceedingBWLmt Policy
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 035 - Active Sessions Exceeding Avg Bandwidth Limit
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	10
<b>Critical</b>	20

#### LS\_AVEdge\_TCPAuthenticationFailuresPerSec

<b>Policy Name</b>	LS_AVEdge_TCPAuthenticationFailuresPerSec Policy
<b>Description</b>	This policy monitors the number of failed authentication attempts with the relay over TCP in one second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 008 - Authentication Failures/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_AVEdge\_TCPPacketsDroppedPerSec

<b>Policy Name</b>	LS_AVEdge_TCPPacketsDroppedPerSec Policy
<b>Description</b>	This policy monitors the rate at which the packets over TCP are dropped by the relay, in a second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 030 - Packets Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 300</b>

**LS\_AVEdge\_ThreadCount**

<b>Policy Name</b>	LS_AVEdge_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter available in the Audio/Video Edge service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 150</b>

**LS\_AVEdge\_UDPActiveSessionsExceedingBWLmt**

<b>Policy Name</b>	LS_AVEdge_UDPActiveSessionsExceedingBWLmt Policy
<b>Description</b>	This policy monitors the number of active relay sessions over UDP, which are exceeding the bandwidth limit.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 034 - Active Sessions Exceeding Avg Bandwidth Limit
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

**LS\_AVEdge\_UDPAllocateRqstExeedingPortLimit**

<b>Policy Name</b>	LS_AVEdge_UDPAllocateRqstExeedingPortLimit Policy
<b>Description</b>	This policy monitors the number of allocated requests over UDP that exceed the port limit, in one second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 010 - Allocate Requests Exceeding Port Limit/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_AVEdge\_UDPAAuthenticationFailuresPerSec

<b>Policy Name</b>	LS_AVEdge_UDPAAuthenticationFailuresPerSec Policy
<b>Description</b>	This policy monitors the rate of failed authentication attempts with the relay over UDP in one second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 008 - Authentication Failures/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_AVEdge\_UDPPacketsDroppedPerSec

<b>Policy Name</b>	LS_AVEdge_UDPPacketsDroppedPerSec Policy
<b>Description</b>	This policy monitors the rate of packets over UDP that are dropped by the relay in one second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 029 - Packets Dropped/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 300</b>

### LS\_AVEdge\_WorkingSet

<b>Policy Name</b>	LS_AVEdge_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter available in the Audio/Video Edge service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediaRelaySvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_Check\_AccessEdgeServiceStatus

<b>Policy Name</b>	LS_Check_AccessEdgeServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of 'RTCSRVR'. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCSRVR

### LS\_Check\_AVAuthServiceStatus

<b>Policy Name</b>	LS_Check_AVAuthServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of the 'RTCMRAUTH' service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMRAUTH

### LS\_Check\_AVEdgeServiceStatus

<b>Policy Name</b>	LS_Check_AVEdgeServiceStatus Policy
<b>Description</b>	This policy checks the status of the Audio/Video Conferencing Edge Service and returns values that correspond to different states of the 'RTCMEDIARELAY'. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMEDIARELAY

### LS\_Check\_ReplicaServiceStatus\_Edge

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Edge Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Edge Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

### LS\_Check\_WebEdgeServiceStatus

<b>Policy Name</b>	LS_Check_WebEdgeServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of the 'RTCDATAPROXY'. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCDATAPROXY

### LS\_Replica\_PrivateBytes

<b>Policy Name</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter of the Replica Service.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Replica\_ThreadCount

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

#### LS\_Replica\_WorkingSet

<b>Policy Name</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_WebEdge\_ClientsDisconPerSecInvalidCookieData

<b>Policy Name</b>	LS_WebEdge_ClientsDisconPerSecInvalidCookieData Policy
<b>Description</b>	This policy monitors the number of clients disconnected in a second because of invalid cookie data.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 01 - Client Connections
<b>Instance</b>	All instances
<b>Counter</b>	DATAPROXY - 012 - Clients disconnected per second due to invalid cookie data
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_WebEdge\_ClientsDisconPerSecInvalidCookieTm

<b>Policy Name</b>	LS_WebEdge_ClientsDisconPerSecInvalidCookieTm Policy
<b>Description</b>	This policy monitors the number of clients rejected in a second because of invalid timestamps.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 01 - Client Connections



<b>Policy Name</b>	LS_WebEdge_ClientsDisconPerSecInvalidCookieTm Policy
<b>Instance</b>	All instances
<b>Counter</b>	DATAPROXY - 008 - Clients disconnected per second due to invalid cookie timestamp
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_WebEdge\_Logging

<b>Policy Name</b>	LS_WebEdge_Logging Policy
<b>Description</b>	This policy collects data for the LS Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Monitored Service</b>	LS_PROCESS

Instance	Performance Object
DataProxy	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	Process\% Processor Time

### LS\_WebEdge\_PageFaultsPerSec

<b>Policy Name</b>	LS_WebEdge_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_WebEdge\_PrivateBytes

<b>Policy Name</b>	LS_WebEdge_PrivateBytes Policy
<b>Description</b>	This policy monitors the Private Bytes counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_WebEdge\_ProcessorTime

<b>Policy Name</b>	LS_WebEdge_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_WebEdge\_SystemThrottling

<b>Policy Name</b>	LS_WebEdge_SystemThrottling Policy
<b>Description</b>	The policy monitors the system wide throttling.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 00 - Server Connections
<b>Instance</b>	_Total
<b>Counter</b>	DATAPROXY - 041 - System is throttling
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	1
<b>Critical</b>	2

### LS\_WebEdge\_ThreadCount

<b>Policy Name</b>	LS_WebEdge_ThreadCount Policy
<b>Description</b>	This policy monitors the Thread Count counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_WebEdge\_ThrottledServerConnections

<b>Policy Name</b>	LS_WebEdge_ThrottledServerConnections Policy
<b>Description</b>	This policy monitors the total number of throttled server connections.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 00 - Server Connections
<b>Instance</b>	_Total
<b>Counter</b>	DATAPROXY - 034 - Current count of server connections that are throttled
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	1
<b>Critical</b>	2

### LS\_WebEdge\_WorkingSet

<b>Policy Name</b>	LS_WebEdge_WorkingSet Policy
<b>Description</b>	This policy monitors the Working Set counter of the Web Conferencing Edge Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataProxy
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

## GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the Edge Server.

### LS\_AccessEdge\_AvgIncomingMsgProcessingTime

<b>Policy Name</b>	LS_AccessEdge_AvgIncomingMsgProcessingTime Policy
<b>Description</b>	This policy monitors the average processing time of an incoming message in seconds.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LC:SIP - 02 – Protocol
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 021 - Average Incoming Message Processing Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

### LS\_AccessEdge\_ExtMsgDroppedDueToBlkedIMDomain

<b>Policy Name</b>	LS_AccessEdge_ExtMsgDroppedDueToBlkedIMDomain Policy
<b>Description</b>	This policy monitors the rate of messages dropped at the external edge, in a second, because of DNS SRV resolving the domain to a server blocked in the IM Service Providers table.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 09 - Access Edge Server Messages
<b>Instance</b>	All instances.
<b>Counter</b>	SIP - 065 - External Messages/sec Dropped Due To Blocked IM Service Provider Domain
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 40</b>

### LS\_AccessEdge\_RateOfCnxDropDueToPeer

<b>Policy Name</b>	LS_AccessEdge_RateOfCnxDropDueToPeer Policy
<b>Description</b>	This policy monitors the rate of the connections dropped, in a second, as the peer failed to exchange valid data with the server within establishing timeout.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS: SIP – 00 – Networking

<b>Policy Name</b>	LS_AccessEdge_RateOfCnxDropDueToPeer Policy
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 005 - Connections Failed To Establish/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_AccessEdge\_RateOfCnxRefusedDueToSrvOverload

<b>Policy Name</b>	LS_AccessEdge_RateOfCnxRefusedDueToSrvOverload Policy
<b>Description</b>	This policy monitors the rate of the connections refused, in a second, with a Service Unavailable response because the server was overloaded.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS: SIP – 00 – Networking
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 007 - Connections Refused Due To Server Overload/Sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_AVEdge\_BadRequestsReceivedPerSec

<b>Policy Name</b>	LS_AVEdge_BadRequestsReceivedPerSec Policy
<b>Description</b>	This policy monitors the number of bad requests which are received in a second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Auth - 00 - Requests
<b>Instance</b>	All instances
<b>Counter</b>	- 003 - Bad Requests Received/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_AVEdge\_TCPActiveSessionsExceedingBWLmt

<b>Policy Name</b>	LS_AVEdge_TCPActiveSessionsExceedingBWLmt Policy
<b>Description</b>	This policy monitors the number of active relay sessions over TCP, which are exceeding the bandwidth limit.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 01 - TCP Counters

<b>Policy Name</b>	LS_AVEdge_TCPActiveSessionsExceedingBWLmt Policy
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 035 - Active Sessions Exceeding Avg Bandwidth Limit
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	10
<b>Critical</b>	20

#### LS\_AVEdge\_TCPAuthenticationFailuresPerSec

<b>Policy Name</b>	LS_AVEdge_TCPAuthenticationFailuresPerSec Policy
<b>Description</b>	This policy monitors the number of failed authentication attempts with the relay over TCP in one second.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:A/V Edge - 01 - TCP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 008 - Authentication Failures/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_AVEdge\_UDPActiveSessionsExceedingBWLmt

<b>Policy Name</b>	LS_AVEdge_UDPActiveSessionsExceedingBWLmt Policy
<b>Description</b>	This policy monitors the number of active relay sessions over UDP, which are exceeding the bandwidth limit.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 034 - Active Sessions Exceeding Avg Bandwidth Limit
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

**LS\_AVEdge\_UDPAllocateRqstExceedingPortLimit**

<b>Policy Name</b>	LS_AVEdge_UDPAllocateRqstExceedingPortLimit Policy
<b>Description</b>	This policy monitors the number of allocated requests over UDP that exceed the port limit, in one second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 010 - Allocate Requests Exceeding Port Limit/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

**LS\_AVEdge\_UDPAuthenticationFailuresPerSec**

<b>Policy Name</b>	LS_AVEdge_UDPAuthenticationFailuresPerSec Policy
<b>Description</b>	This policy monitors the rate of failed authentication attempts with the relay over UDP in one second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:A/V Edge - 00 - UDP Counters
<b>Instance</b>	_Total
<b>Counter</b>	A/V Edge - 008 - Authentication Failures/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

**LS\_Check\_AccessEdgeServiceStatus**

<b>Policy Name</b>	LS_Check_AccessEdgeServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of 'RTCSRVR'. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCSRVR

**LS\_Check\_AVAuthServiceStatus**

<b>Policy Name</b>	LS_Check_AVAuthServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of the 'RTCMRAUTH' service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMRAUTH

**LS\_Check\_AVEdgeServiceStatus**

<b>Policy Name</b>	LS_Check_AVEdgeServiceStatus Policy
<b>Description</b>	This policy checks the status of the Audio/Video Conferencing Edge Service and returns values that correspond to different states of the 'RTCMEDIARELAY'. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCMEDIARELAY

**LS\_Check\_ReplicaServiceStatus\_Edge**

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Edge Policy
<b>Description</b>	This policy checks the status of the Replica Replicator Agent Service at the Edge Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

**LS\_Check\_WebEdgeServiceStatus**

<b>Policy Name</b>	LS_Check_WebEdgeServiceStatus Policy
<b>Description</b>	This policy returns values that correspond to different states of the 'RTCDATAPROXY'. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCDATAPROXY



### LS\_WebEdge\_ClientsDisconPerSecInvalidCookieData

<b>Policy Name</b>	LS_WebEdge_ClientsDisconPerSecInvalidCookieData Policy
<b>Description</b>	This policy monitors the number of clients disconnected in a second because of invalid cookie data.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 01 - Client Connections
<b>Instance</b>	All instances
<b>Counter</b>	DATAPROXY - 012 - Clients disconnected per second due to invalid cookie data
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

### LS\_WebEdge\_ClientsDisconPerSecInvalidCookieTm

<b>Policy Name</b>	LS_WebEdge_ClientsDisconPerSecInvalidCookieTm Policy
<b>Description</b>	This policy monitors the number of clients rejected in a second because of invalid timestamps.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAPROXY - 01 - Client Connections
<b>Instance</b>	All instances
<b>Counter</b>	DATAPROXY - 008 - Clients disconnected per second due to invalid cookie timestamp
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

## Front End Server

The FrontEnd Server is located in the internal network that hosts the IM Conferencing service, Address Book service, and Telephony Conferencing service to support registration, presence, IM, and conferencing.

This server role is available on a Standard Edition Server. In an Enterprise pool, it can either be configured with the Web Conferencing Server and A/V Conferencing Server, or can be deployed on a separate server.

## General Policies

The General policy group contains all the policies that monitor the processes and services of the FrontEnd Server.

### LS\_AppSharing\_PageFaultsPerSec

<b>Policy Name</b>	LS_AppSharing_PageFaultsPerSec Policy
<b>Description</b>	This policy monitors the Page Faults/sec counter available in the Lync Server Application Sharing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ASMCUSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_FileTransferAgent\_PageFaultsPerSec

<b>Policy Name</b>	LS_FileTransferAgent_PageFaultsPerSec Policy
<b>Description</b>	The LS_FileTransferAgent_PageFaultsPerSec policy monitors the Page Faults/sec counter of the File Transfer Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	FileTransferAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_Replica\_PageFaultsPerSec

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	The LS_Replica_PageFaultsPerSec monitors the Page Faults/sec counter of the Replica Service
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_AppSharing\_ProcessorTime

<b>Policy Name</b>	LS_AppSharing_ProcessorTime Policy
<b>Description</b>	The LS_AppSharing_ProcessorTime policy monitors the % Processor Time counter of the Application Sharing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ASMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_AppSharing\_ThreadCount

<b>Policy Name</b>	LS_AppSharing_ThreadCount Policy
<b>Description</b>	The LS_AppSharing_ThreadCount policy monitors the Thread Count counter of the Application Sharing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ASMCUSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_AppSharing\_WorkingSet

<b>Policy Name</b>	LS_AppSharing_WorkingSet Policy
<b>Description</b>	The LS_AppSharing_WorkingSet policy monitors the Working Set counter of the Application Sharing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ASMCUSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Check\_AppSharingServiceStatus

<b>Policy Name</b>	LS_Check_AppSharingServiceStatus Policy
<b>Description</b>	The LS_Check_AppSharingServiceStatus policy checks the status of the Application Sharing Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCASMCU

### LS\_Check\_AudioTestServiceStatus

<b>Policy Name</b>	LS_Check_AudioTestServiceStatus Policy
<b>Description</b>	The LS_Check_AudioTestServiceStatus policy checks the status of the Audio Test Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCATS

### LS\_Check\_BandwidthAuthServiceStatus

<b>Policy Name</b>	LS_Check_BandwidthAuthServiceStatus Policy
<b>Description</b>	The LS_Check_BandwidthAuthServiceStatus policy checks the status of the Bandwidth Policy (Authorization) Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCPDPAUTH

### LS\_Check\_BandwidthCoreServiceStatus

<b>Policy Name</b>	LS_Check_BandwidthCoreServiceStatus Policy
<b>Description</b>	The LS_Check_BandwidthCoreServiceStatus policy checks status of the Bandwidth Policy (Core) Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCPDPCORE

**LS\_Check\_CallParkServiceStatus**

<b>Policy Name</b>	LS_Check_CallParkServiceStatus Policy
<b>Description</b>	LS_Check_CallParkServiceStatus policy checks the status of the Call Park Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCCPS

**LS\_Check\_ConfAnnouncementServiceStatus**

<b>Policy Name</b>	LS_Check_ConfAnnouncementServiceStatus Policy
<b>Description</b>	The LS_Check_ConfAnnouncementServiceStatus policy checks the status of the Conferencing Announcement Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCCAS

**LS\_Check\_ConfAttendantServiceStatus**

<b>Policy Name</b>	LS_Check_ConfAttendantServiceStatus Policy
<b>Description</b>	The LS_Check_ConfAttendantServiceStatus policy checks the status of the ConfAttendant Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCCAA

**LS\_Check\_FileTransferAgentServiceStatus**

<b>Policy Name</b>	LS_Check_FileTransferAgentServiceStatus Policy
<b>Description</b>	The LS_Check_FileTransferAgentServiceStatus policy checks the status of the File Transfer Agent Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	FTA

**LS\_Check\_FrontEnd\_ADStatus**

<b>Policy Name</b>	LS_Check_FrontEnd_ADStatus Policy
<b>Description</b>	The policy LS_Check_FrontEnd_ADStatus checks the connectivity status of the Active Directory with the Front End Server. It sends a critical alert message if the Active Directory is not accessible from the Front End Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

**LS\_Check\_FrontEnd\_ReplicaStatus**

<b>Policy Name</b>	LS_Check_FrontEnd_ReplicaStatus Policy
<b>Description</b>	The policy LS_Check_FrontEnd_ReplicaStatus checks the Central Management Store replication status at the Front End Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	REPLICA

**LS\_Check\_FrontEndServiceStatus**

<b>Policy Name</b>	LS_Check_FrontEndServiceStatus Policy
<b>Description</b>	The LS_Check_FrontEndServiceStatus policy checks the status of the Front-End Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCSRVS

**LS\_Check\_IMConfServiceStatus**

<b>Policy Name</b>	LS_Check_IMConfServiceStatus Policy
<b>Description</b>	The LS_Check_IMConfServiceStatus policy checks the status of the IM Conferencing Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCIMMCU

**LS\_Check\_MasterReplicatorAgentServiceStatus**

<b>Policy Name</b>	LS_Check_MasterReplicatorAgentServiceStatus Policy
<b>Description</b>	The LS_Check_MasterReplicatorAgentServiceStatus policy checks the status of the Master Replicator Agent Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	MASTER

**LS\_Check\_ReplicaServiceStatus\_FrontEnd**

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_FrontEnd Policy
<b>Description</b>	The policy LS_Check_ReplicaServiceStatus_FrontEnd checks the status of the Replica Replicator Agent Service at the Front End Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	Replica Replicator Agent

**LS\_Check\_ResponseGroupServiceStatus**

<b>Policy Name</b>	LS_Check_ResponseGroupServiceStatus Policy
<b>Description</b>	The LS_Check_ResponseGroupServiceStatus policy checks the status of the Response Group Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCGRS

**LS\_Check\_WebConfCompatibilityServiceStatus**

<b>Policy Name</b>	LS_Check_WebConfCompatibilityServiceStatus Policy
<b>Description</b>	The LS_Check_WebConfCompatibilityServiceStatus policy checks the status of the Web Conferencing Compatibility Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCMEETINGMCU

### LS\_Check\_WebConfServiceStatus

<b>Policy Name</b>	LS_Check_WebConfServiceStatus Policy
<b>Description</b>	The LS_Check_WebConfServiceStatus policy checks the status of the Web Conferencing Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCDATAMCU

### LS\_FileTransferAgent\_PrivateBytes

<b>Policy Name</b>	LS_FileTransferAgent_PrivateBytes Policy
<b>Description</b>	The LS_FileTransferAgent_PrivateBytes policy monitors the Private Bytes counter of the File Transfer Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	FileTransferAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_FileTransferAgent\_ProcessorTime

<b>Policy Name</b>	LS_FileTransferAgent_ProcessorTime Policy
<b>Description</b>	The LS_FileTransferAgent_ProcessorTime policy monitors the % Processor Time counter of the File Transfer Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	FileTransferAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90



### LS\_FileTransferAgent\_ThreadCount

<b>Policy Name</b>	LS_FileTransferAgent_ThreadCount Policy
<b>Description</b>	The LS_FileTransferAgent_ThreadCount policy monitors the Thread Count counter of the File Transfer Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	FileTransferAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_FileTransferAgent\_WorkingSet

<b>Policy Name</b>	LS_FileTransferAgent_WorkingSet Policy
<b>Description</b>	The LS_FileTransferAgent_WorkingSet policy monitors the Working Set counter of the File Transfer Agent service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	FileTransferAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_FrontEnd\_AvgNoOfBlkedClientThreads

<b>Policy Name</b>	LS_FrontEnd_AvgNoOfBlkedClientThreads Policy
<b>Description</b>	This policy monitors the average number of client threads that are blocked in the queue, waiting for the queue depth to decrease.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 01 - DBStore
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 011 - Blocked Client Threads

<b>Policy Name</b>	LS_FrontEnd_AvgNoOfBlkedClientThreads Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	4000
<b>Critical</b>	6000

#### **LS\_FrontEnd\_AvgTimeRequestHeldInDB**

<b>Policy Name</b>	LS_FrontEnd_AvgTimeRequestHeldInDB Policy
<b>Description</b>	This policy monitors the average time (in milliseconds) a request is held in the database queue.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances
<b>Counter</b>	Usvr - 002 - Queue Latency (msec)
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	4000
<b>Critical</b>	6000

#### **LS\_FrontEnd\_AvgTimeToFetchProperties**

<b>Policy Name</b>	LS_FrontEnd_AvgTimeToFetchProperties Policy
<b>Description</b>	This policy monitors the average fetch time of member properties in milliseconds.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:WEB - 00 - Distribution List Expansion
<b>Instance</b>	All instances
<b>Counter</b>	WEB - 008 - Average member properties fetch time in milliseconds
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	10000
<b>Critical</b>	30000

### LS\_FrontEnd\_DataLogging

<b>Policy Name</b>	LS_FrontEnd_DataLogging Policy
<b>Description</b>	This policy collects data for the LS Front End Server.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_PROCESS

<b>Instance</b>	Performance Object
<b>All instances</b>	LS:USrv - 00 - REGDBStore\Usrv -002 - Queue Latency (msec)
	LS:USrv - 00 - REGDBStore\Usrv -004 - Sproc Latency (msec)
	LS:SIP - 07 - LoadManagement\SIP - 000 - AverageHolding Time ForIncoming Messages
	LS:SIP - 04 - Responses\SIP - 055 -Local 503 Responses/sec
	LS:SIP - 04 - Responses\SIP - 057 -Local 504 Responses/sec
	LS:SIP - 01 - Peers\SIP - 017 -Sends Outstanding

### LS\_FrontEnd\_HoldingTimeForIncMsgs

<b>Policy Name</b>	LS_FrontEnd_HoldingTimeForIncMsgs Policy
<b>Description</b>	This policy monitors the average processing time taken by the server for one request.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 07 - Load Management
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 000 - Average Holding Time For Incoming Messages
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

### LS\_FrontEnd\_Local503Responses

<b>Policy Name</b>	LS_FrontEnd_Local503Responses Policy
<b>Description</b>	This policy monitors the number of 503 responses received in a second. Code 503 means that the server is unavailable.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 04 - Responses

<b>Policy Name</b>	LS_FrontEnd_Local503Responses Policy
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 055 - Local 503 Responses/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

#### LS\_FrontEnd\_Local504Responses

<b>Policy Name</b>	LS_FrontEnd_Local504Responses Policy
<b>Description</b>	This policy monitors the number of 504 responses received in a second. Code 504 implies that there are problems connecting to other servers.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 04 - Responses
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 057 - Local 504 Responses/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

#### LS\_FrontEnd\_Logging

<b>Policy Name</b>	LS_FrontEnd_Logging Policy
<b>Description</b>	The LS_FrontEnd_Logging policy logs the following metrics into the data store (CODA or HP Performance Agent) for the instances RTCSrv or _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_PROCESS

Instance	Performance Object
RTCSrv	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	Processor\% Processor Time

### LS\_FrontEnd\_NoOfRequestsWaitingOnAD

<b>Policy Name</b>	LS_FrontEnd_NoOfRequestsWaitingOnAD Policy
<b>Description</b>	This policy monitors the number of request waiting currently for Active Directory responses.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:WEB - 00 - Distribution List Expansion
<b>Instance</b>	_Total
<b>Counter</b>	WEB - 004 - Pending Active Directory Requests
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

### LS\_FrontEnd\_PageFaultsPerSec

<b>Policy Name</b>	LS_FrontEnd_PageFaultsPerSec Policy
<b>Description</b>	The LS_FrontEnd_PageFaultsPerSec policy monitors the Page Faults/sec counter of the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_FrontEnd\_PrivateBytes

<b>Policy Name</b>	LS_FrontEnd_PrivateBytes Policy
<b>Description</b>	The LS_FrontEnd_PrivateBytes policy monitors the Private Bytes counter of the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_FrontEnd\_ProcessingLatency

<b>Policy Name</b>	LS_FrontEnd_ProcessingLatency Policy
<b>Description</b>	This policy monitors the processing time taken by the back end for one request.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 01 - DBStore
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 004 - Sproc Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 6000

### LS\_FrontEnd\_SearchLatency

<b>Policy Name</b>	LS_FrontEnd_SearchLatency Policy
<b>Description</b>	The policy LS_FrontEnd_SearchLatency monitors the average time (in milliseconds) it takes to perform the LDAP search.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 005 - Search Latency (ms)
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 20

### LS\_FrontEnd\_ProcessorTime

<b>Policy Name</b>	LS_FrontEnd_ProcessorTime Policy
<b>Description</b>	The LS_FrontEnd_ProcessorTime policy monitors the % Processor Time counter of the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_FrontEnd\_QueueLatency

<b>Policy Name</b>	LS_FrontEnd_QueueLatency Policy
<b>Description</b>	This policy monitors the time period that a request takes in the back end queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 01 - DBStore
<b>Instance</b>	All instances
<b>Counter</b>	Usvr - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 6000</b>

### LS\_FrontEnd\_RateOfSoapExceptions

<b>Policy Name</b>	LS_FrontEnd_RateOfSoapExceptions Policy
<b>Description</b>	This policy monitors the SOAP exceptions generated per second.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:WEB - 00 - Distribution List Expansion
<b>Instance</b>	_Total
<b>Counter</b>	WEB - 015 - Soap exceptions/sec

<b>Policy Name</b>	LS_FrontEnd_RateOfSoapExceptions Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	50
<b>Critical</b>	100

#### LS\_FrontEnd\_SendsOutstanding

<b>Policy Name</b>	LS_FrontEnd_SendsOutstanding Policy
<b>Description</b>	This policy monitors the number of outbound requests and responses that are queued.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP – 01 – Peers
<b>Instance</b>	All instances
<b>Counter</b>	SIP – 017 – Sends Outstanding
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 200

#### LS\_FrontEnd\_ThreadCount

<b>Policy Name</b>	LS_FrontEnd_ThreadCount Policy
<b>Description</b>	The LS_FrontEnd_ThreadCount policy monitors the Thread Count of the front end service
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150



### LS\_FrontEnd\_WorkingSet

<b>Policy Name</b>	LS_FrontEnd_WorkingSet Policy
<b>Description</b>	The LS_FrontEnd_WorkingSet policy monitors the Working Set counter of the Front End service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RTCSrv
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_IMConf\_Logging

<b>Policy Name</b>	LS_IMConf_Logging Policy
<b>Description</b>	This policy collects data for the LS IM Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	\% Processor Time

### LS\_IMConf\_PageFaultsPerSec

<b>Policy Name</b>	LS_IMConf_PageFaultsPerSec Policy
<b>Description</b>	The LS_IMConf_PageFaultsPerSec policy the monitors the Page Faults/sec counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_IMConf_PageFaultsPerSec Policy
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

#### LS\_IMConf\_PrivateBytes

<b>Policy Name</b>	LS_IMConf_PrivateBytes Policy
<b>Description</b>	The LS_IMConf_PrivateBytes policy monitors the Private Bytes counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

#### LS\_IMConf\_ProcessorTime

<b>Policy Name</b>	LS_IMConf_ProcessorTime Policy
<b>Description</b>	This policy monitors the % Processor Time counter available in the IM Conferencing service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_IMConf\_ThreadCount

<b>Policy Name</b>	LS_IMConf_ThreadCount Policy
<b>Description</b>	The LS_IMConf_ThreadCount policy monitors the Thread Count counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_IMConf\_WorkingSet

<b>Policy Name</b>	LS_IMConf_WorkingSet Policy
<b>Description</b>	The LS_IMConf_WorkingSet policy monitors the Working Set counter of the IM Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	IMMcuSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_MasterReplicatorAgent\_PageFaultsPerSec

<b>Policy Name</b>	LS_MasterReplicatorAgent_PageFaultsPerSec Policy
<b>Description</b>	The LS_MasterReplicatorAgent_PageFaultsPerSec policy monitors the Page Faults/sec counter of the MasterReplicatorAgent Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MasterReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_MasterReplicatorAgent\_PrivateBytes

<b>Policy Name</b>	LS_MasterReplicatorAgent_PrivateBytes Policy
<b>Description</b>	The LS_MasterReplicatorAgent_PrivateBytes policy monitors the Private Bytes counter of the MasterReplicatorAgent Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MasterReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_MasterReplicatorAgent\_ProcessorTime

<b>Policy Name</b>	LS_MasterReplicatorAgent_ProcessorTime Policy
<b>Description</b>	The LS_MasterReplicatorAgent_ProcessorTime policy monitors the % Processor Time counter of the MasterReplicatorAgentService.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MasterReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_MasterReplicatorAgent\_ThreadCount

<b>Policy Name</b>	LS_MasterReplicatorAgent_ThreadCount Policy
<b>Description</b>	The LS_MasterReplicatorAgent_ThreadCount policy monitors the Thread Count counter of the MasterReplicatorAgent Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MasterReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_MasterReplicatorAgent\_WorkingSet

<b>Policy Name</b>	LS_MasterReplicatorAgent_WorkingSet Policy
<b>Description</b>	The LS_MasterReplicatorAgent_WorkingSet policy monitors the Working Set counter of the MasterReplicatorAgent Service.
<b>Schedule</b>	This policy runs every one hour.s
<b>Performance Object</b>	Process
<b>Instance</b>	MasterReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Replica\_PrivateBytes

<b>Policy Name</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	The LS_Replica_PrivateBytes policy monitors the Private Bytes counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	The LS_Replica_ProcessorTime policy monitors the '% Processor Time' counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Replica\_ThreadCount

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	The LS_Replica_ThreadCount policy monitors the Thread Count counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_Replica\_WorkingSet

<b>Policy Name</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	The LS_Replica_WorkingSet policy monitors the Working Set counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_WebConf\_Logging

<b>Policy Name</b>	LS_WebConf_Logging Policy
<b>Description</b>	This policy collects data for the Web Conferencing Service.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Data Class</b>	LS_PROCESS

<b>Instance</b>	<b>Performance Object</b>
RTCSrv	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	\% Processor Time

### LS\_WebConf\_MCUHealthState

<b>Policy Name</b>	LS_WebConf_MCUHealthState Policy
<b>Description</b>	This policy monitors the current health of DATAMCU. The value 0 signifies that the DATAMCU is normal, 1 signifies that it is loaded, 2 signifies that it is full, and 3 signifies that the MCU is unavailable.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAMCU - 04 - MCU Health And Performance
<b>Instance</b>	All instances.
<b>Counter</b>	DATAMCU - 005 - MCU Health State
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	1
<b>Critical</b>	2

### LS\_WebConf\_NumberOfUnhandledAppExceptions

<b>Policy Name</b>	LS_WebConf_NumberOfUnhandledAppExceptions Policy
<b>Description</b>	The number of unhandled exceptions in application is monitored by this policy.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAMCU - 00 - DataMCU Conferences
<b>Instance</b>	All instances.
<b>Counter</b>	DATAMCU - 005 - Number of Unhandled Application Exception

<b>Policy Name</b>	LS_WebConf_NumberOfUnhandledApplExceptions Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

#### LS\_WebConf\_PageFaultsPerSec

<b>Policy Name</b>	LS_WebConf_PageFaultsPerSec Policy
<b>Description</b>	The LS_WebConf_PageFaultsPerSec policy monitors the Page Faults/sec counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_WebConf\_PrivateBytes

<b>Policy Name</b>	LS_WebConf_PrivateBytes Policy
<b>Description</b>	The LS_WebConf_PrivateBytes policy monitors the Private Bytes counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007



### LS\_WebConf\_ProcessorTime

<b>Policy Name</b>	LS_WebConf_ProcessorTime Policy
<b>Description</b>	The LS_WebConf_ProcessorTime policy monitors the % Processor Time counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_WebConf\_SessionQueuesState

<b>Policy Name</b>	LS_WebConf_SessionQueuesState Policy
<b>Description</b>	This policy monitors the state of session queues.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:DATAMCU - 00 - DataMCU Conferences
<b>Instance</b>	All instances
<b>Counter</b>	DATAMCU - 008 - Session queues state
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	1
<b>Critical</b>	2

### LS\_WebConf\_ThreadCount

<b>Policy Name</b>	LS_WebConf_ThreadCount Policy
<b>Description</b>	The LS_WebConf_ThreadCount policy monitors the Thread Count counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_WebConf_ThreadCount Policy
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

#### LS\_WebConf\_WorkingSet

<b>Policy Name</b>	LS_WebConf_WorkingSet Policy
<b>Description</b>	The LS_WebConf_WorkingSet policy monitors the Working Set counter of the Web Conferencing Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	DataMCUSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_WebConfCompatibility\_PageFaultsPerSec

<b>Policy Name</b>	LS_WebConfCompatibility_PageFaultsPerSec Policy
<b>Description</b>	The Page Faults / sec of Web Conference compatibility process is monitored by the LS_WebConfCompatibility_PageFaultsPerSec policy.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MeetingMCUSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

### LS\_WebConfCompatibility\_PrivateBytes

<b>Policy Name</b>	LS_WebConfCompatibility_PrivateBytes Policy
<b>Description</b>	The private bytes of Web conference compatibility process is monitored by the LS_WebConfCompatibility_PrivateBytes policy.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MeetingMCUSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_WebConfCompatibility\_ProcessorTime

<b>Policy Name</b>	LS_WebConfCompatibility_ProcessorTime Policy
<b>Description</b>	The % processor time of web conference compatibility process is monitored by the policy LS_WebConfCompatibility_ProcessorTime policy.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MeetingMCUSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_WebConfCompatibility\_ThreadCount

<b>Policy Name</b>	LS_WebConfCompatibility_ThreadCount Policy
<b>Description</b>	The thread count of web conference compatibility process is monitored by the LS_WebConfCompatibility_ThreadCount policy.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MeetingMCUSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_WebConfCompatibility\_WorkingSet

<b>Policy Name</b>	LS_WebConfCompatibility_WorkingSet Policy
<b>Description</b>	The Working Set bytes of web conference compatibility process is monitored by the policy LS_WebConfCompatibility_WorkingSet.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MeetingMCUSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the FrontEnd Server.

### LS\_Check\_AppSharingServiceStatus

<b>Policy Name</b>	LS_Check_AppSharingServiceStatus Policy
<b>Description</b>	The LS_Check_AppSharingServiceStatus policy checks the status of the Application Sharing Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCASMCU

### LS\_Check\_AudioTestServiceStatus

<b>Policy Name</b>	LS_Check_AudioTestServiceStatus Policy
<b>Description</b>	The LS_Check_AudioTestServiceStatus policy checks the status of the Audio Test Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCATS

### LS\_Check\_BandwidthAuthServiceStatus

<b>Policy Name</b>	LS_Check_BandwidthAuthServiceStatus Policy
<b>Description</b>	The LS_Check_BandwidthAuthServiceStatus policy checks the status of the Bandwidth Policy (Authorization) Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCPDPAUTH

### LS\_Check\_BandwidthCoreServiceStatus

<b>Policy Name</b>	LS_Check_BandwidthCoreServiceStatus Policy
<b>Description</b>	The LS_Check_BandwidthCoreServiceStatus policy checks status of the Bandwidth Policy (Core) Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCPDPCORE

### LS\_Check\_CallParkServiceStatus

<b>Policy Name</b>	LS_Check_CallParkServiceStatus Policy
<b>Description</b>	LS_Check_CallParkServiceStatus policy checks the status of the Call Park Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCCPS

### LS\_Check\_ConfAnnouncementServiceStatus

<b>Policy Name</b>	LS_Check_ConfAnnouncementServiceStatus Policy
<b>Description</b>	The LS_Check_ConfAnnouncementServiceStatus policy checks the status of the Conferencing Announcement Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCCAS

### LS\_Check\_ConfAttendantServiceStatus

<b>Policy Name</b>	LS_Check_ConfAttendantServiceStatus Policy
<b>Description</b>	The LS_Check_ConfAttendantServiceStatus policy checks the status of the ConfAttendant Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCCAA

### LS\_Check\_FileTransferAgentServiceStatus

<b>Policy Name</b>	LS_Check_FileTransferAgentServiceStatus Policy
<b>Description</b>	The LS_Check_FileTransferAgentServiceStatus policy checks the status of the File Transfer Agent Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	FTA

### LS\_Check\_FrontEnd\_ADStatus

<b>Policy Name</b>	LS_Check_FrontEnd_ADStatus Policy
<b>Description</b>	The policy LS_Check_FrontEnd_ADStatus checks the connectivity status of the Active Directory with the Front End Server. It sends a critical alert message if the Active Directory is not accessible from the Front End Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Check\_FrontEnd\_ReplicaStatus

<b>Policy Name</b>	LS_Check_FrontEnd_ReplicaStatus Policy
<b>Description</b>	The policy LS_Check_FrontEnd_ReplicaStatus checks the Central Management Store replication status at the Front End Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	REPLICA

### LS\_Check\_FrontEndServiceStatus

<b>Policy Name</b>	LS_Check_FrontEndServiceStatus Policy
<b>Description</b>	The LS_Check_FrontEndServiceStatus policy checks the status of the Front-End Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCSRV

### LS\_Check\_IMConfServiceStatus

<b>Policy Name</b>	LS_Check_IMConfServiceStatus Policy
<b>Description</b>	The LS_Check_IMConfServiceStatus policy checks the status of the IM Conferencing Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCIMMCU

### LS\_Check\_MasterReplicatorAgentServiceStatus

<b>Policy Name</b>	LS_Check_MasterReplicatorAgentServiceStatus Policy
<b>Description</b>	The LS_Check_MasterReplicatorAgentServiceStatus policy checks the status of the Master Replicator Agent Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	MASTER

### LS\_Check\_ReplicaServiceStatus\_FrontEnd

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_FrontEnd Policy
<b>Description</b>	The policy LS_Check_ReplicaServiceStatus_FrontEnd checks the status of the Replica Replicator Agent Service at the Front End Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	Replica Replicator Agent

**LS\_Check\_ResponseGroupServiceStatus**

<b>Policy Name</b>	LS_Check_ResponseGroupServiceStatus Policy
<b>Description</b>	The LS_Check_ResponseGroupServiceStatus policy checks the status of the Response Group Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCRGS

**LS\_Check\_WebConfCompatibilityServiceStatus**

<b>Policy Name</b>	LS_Check_WebConfCompatibilityServiceStatus Policy
<b>Description</b>	The LS_Check_WebConfCompatibilityServiceStatus policy checks the status of the Web Conferencing Compatibility Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCMEETINGMCU

**LS\_Check\_WebConfServiceStatus**

<b>Policy Name</b>	LS_Check_WebConfServiceStatus Policy
<b>Description</b>	The LS_Check_WebConfServiceStatus policy checks the status of the Web Conferencing Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCDATAMCU

**LS\_FrontEnd\_HoldingTimeForIncMsgs**

<b>Policy Name</b>	LS_FrontEnd_HoldingTimeForIncMsgs Policy
<b>Description</b>	This policy monitors the average processing time taken by the server for one request.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 07 - Load Management



<b>Policy Name</b>	LS_FrontEnd_HoldingTimeForIncMsgs Policy
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 000 - Average Holding Time For Incoming Messages
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

#### LS\_FrontEnd\_Local503Responses

<b>Policy Name</b>	LS_FrontEnd_Local503Responses Policy
<b>Description</b>	This policy monitors the number of 503 responses received in a second. Code 503 means that the server is unavailable.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 04 - Responses
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 055 - Local 503 Responses/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 5</b>

#### LS\_FrontEnd\_ProcessingLatency

<b>Policy Name</b>	LS_FrontEnd_ProcessingLatency Policy
<b>Description</b>	This policy monitors the processing time taken by the back end for one request.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 01 - DBStore
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 004 - Sproc Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 6000</b>

### LS\_FrontEnd\_SearchLatency

<b>Policy Name</b>	LS_FrontEnd_SearchLatency Policy
<b>Description</b>	The policy LS_FrontEnd_SearchLatency monitors the average time (in milliseconds) it takes to perform the LDAP search.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 19 - Directory Search
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 005 - Search Latency (ms)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_FrontEnd\_QueueLatency

<b>Policy Name</b>	LS_FrontEnd_QueueLatency Policy
<b>Description</b>	This policy monitors the time period that a request takes in the back end queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 01 - DBStore
<b>Instance</b>	All instances
<b>Counter</b>	Usvr - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 6000</b>

### LS\_FrontEnd\_SendsOutstanding

<b>Policy Name</b>	LS_FrontEnd_SendsOutstanding Policy
<b>Description</b>	This policy monitors the number of outbound requests and responses that are queued.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:SIP - 01 - Peers
<b>Instance</b>	All instances
<b>Counter</b>	SIP - 017 - Sends Outstanding
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 200</b>

## Mediation Server

The Mediation Server is located in the internal network that mediates signaling and media between the Enterprise Voice infrastructure (such as a Director or home server) and another gateway (such as a Basic Media Gateway).

A Mediation Server is also used to link Office Communications Server and a PBX in both departmental deployment and PBX integration topologies. The Mediation Server is deployed on a separate and dedicated server.

### General Policies

The General policy group contains all the policies that monitor the processes and services of the Mediation Server.

#### LS\_Mediation\_PageFaultsPerSec

<b>Policy Name</b>	LS_Mediation_PageFaultsPerSec Policy
<b>Description</b>	The LS_Mediation_PageFaultsPerSec policy monitors the Page Faults/sec counter of the Mediation service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_Check\_MediationServiceStatus

<b>Policy Name</b>	LS_Check_MediationServiceStatus Policy
<b>Description</b>	The LS_Check_MediationServiceStatus policy checks the status of the Mediation Service. This policy sends a critical alert message if the service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored service</b>	RTCMEDSRV

**LS\_Check\_Mediation\_ADStatus**

<b>Policy Name</b>	LS_Check_Mediation_ADStatus Policy
<b>Description</b>	The policy LS_Check_Mediation_ADStatus checks the connectivity status of the Active Directory with the Mediation Server and sends a critical alert message if the Active Directory is not accessible from the Mediation Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every five minutes.

**LS\_Check\_Mediation\_ReplicaStatus**

<b>Policy Name</b>	LS_Check_Mediation_ReplicaStatus Policy
<b>Description</b>	The policy LS_Check_Arch_ReplicaStatus checks the Central Management Store replication status at the Mediation Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every five minutes.
<b>Monitored service</b>	REPLICA

**LS\_Check\_ReplicaServiceStatus\_Mediation**

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Mediation Policy
<b>Description</b>	The policy LS_Check_ReplicaServiceStatus_Mediation checks the status of the Replica Replicator Agent Service at the Mediation Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every five minutes.
<b>Monitored service</b>	Replica Replicator Agent

**LS\_Mediation\_LoadCallFailureIndex**

<b>Policy Name</b>	LS_Mediation_LoadCallFailureIndex Policy
<b>Description</b>	This policy monitors the index of call failures due to heavy load. The index is scaled between 0 and 100.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:MediationServer - 03 - Health Indices
<b>Instance</b>	All instances

<b>Policy Name</b>	LS_Mediation_LoadCallFailureIndex Policy
<b>Counter</b>	- 000 - Load Call Failure Index
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

#### LS\_Mediation\_Logging

<b>Policy Name</b>	LS_Mediation_Logging Policy
<b>Description</b>	This policy collects data for the ls Mediation Service. The LS_Mediation_Logging policy logs the following metrics into the data store (CODA or HP Performance Agent) for the instances MediationServerSvc or _Total.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS_PROCESS

Instance	Performance Object
MediationServerSvc	Process\Working Set
	Process\Page Faults/sec
	Process\Private Bytes
	Process\Thread Count
	Process\% Processor Time
_Total	\% Processor Time

#### LS\_Mediation\_NoOfCallsFailedFromProxy

<b>Policy Name</b>	LS_Mediation_NoOfCallsFailedFromProxy Policy
<b>Description</b>	This policy monitors the number of call failures due to unexpected interaction with the proxy.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:MediationServer - 05 - Global Per Gateway Counters
<b>Instance</b>	All instances
<b>Counter</b>	- 000 - Total failed calls caused by unexpected interaction from a gateway

<b>Policy Name</b>	LS_Mediation_NoOfCallsFailedFromProxy Policy
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

#### **LS\_Mediation\_NoOfMediaCnxCheckFailures**

<b>Policy Name</b>	LS_Mediation_NoOfMediaCnxCheckFailures Policy
<b>Description</b>	This policy monitors the number of failures in the media connectivity check.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:MediationServer - 02 - Media Relay
<b>Instance</b>	All instances
<b>Counter</b>	- 001 - Media Connectivity Check Failure
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

#### **LS\_Mediation\_PrivateBytes**

<b>Policy Name</b>	LS_Mediation_PrivateBytes Policy
<b>Description</b>	The LS_Mediation_PrivateBytes policy monitors the Private Bytes counter of the Mediation service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Mediation\_ProcessorTime

<b>Policy Name</b>	LS_Mediation_ProcessorTime Policy
<b>Description</b>	The LS_Mediation_ProcessorTime policy monitors the % Processor Time counter of the Mediation service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Mediation\_RejectedSIPInvitesFromProxy

<b>Policy Name</b>	LS_Mediation_RejectedSIPInvitesFromProxy Policy
<b>Description</b>	The policy monitors the number of SIP INVITEs from proxy which were rejected immediately because of the server load.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:MediationServer - 00 - Outbound Calls
<b>Instance</b>	All instances
<b>Counter</b>	- 003 - Total rejected due to load
<b>Threshold</b>	When the difference between two samples is greater than the Warning and Critical values.
<b>Warning</b>	5
<b>Critical</b>	10

### LS\_Mediation\_ThreadCount

<b>Policy Name</b>	LS_Mediation_ThreadCount Policy
<b>Description</b>	The LS_Mediation_ThreadCount policy monitors the Thread Count counter of the Mediation service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_Mediation_ThreadCount Policy
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

#### LS\_Mediation\_WorkingSet

<b>Policy Name</b>	LS_Mediation_WorkingSet Policy
<b>Description</b>	The LS_Mediation_WorkingSet policy monitors the Working Set counter of the Mediation service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	MediationServerSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

#### LS\_Replica\_PageFaultsPerSec

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	The LS_ReplicaService_PageFaultsPerSec policy monitors the Page Faults/sec counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100



### LS\_Replica\_PrivateBytes

<b>Policy Name</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	The LS_Replica_PrivateBytes policy the Private Bytes counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007.

### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	The LS_Replica_ProcessorTime policy monitors the '% Processor Time' counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Replica\_ThreadCount

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	The LS_ReplicaService_ThreadCount policy monitors the Thread Count counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_Replica\_WorkingSet

<b>Policy Name</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	The LS_Replica_WorkingSet policy monitors the Working Set counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the Mediation Server.

### LS\_Check\_Mediation\_ReplicaStatus

<b>Policy Name</b>	LS_Check_Mediation_ReplicaStatus Policy
<b>Description</b>	The policy LS_Check_Arch_ReplicaStatus checks the Central Management Store replication status at the Mediation Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every five minutes.
<b>Monitored service</b>	REPLICA

### LS\_Check\_ReplicaServiceStatus\_Mediation

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Mediation Policy
<b>Description</b>	The policy LS_Check_ReplicaServiceStatus_Mediation checks the status of the Replica Replicator Agent Service at the Mediation Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every five minutes.
<b>Monitored service</b>	Replica Replicator Agent

## Monitoring Server

The Monitoring Server is a server role in the internal network that gathers all records information about the call details and quality of experience (QoE).

### General Policies

The General policy group contains all the policies that monitor the processes and services of the Monitoring Server.

#### LS\_CallDetailRecording\_DroppedMessagesFromMQ

<b>Policy Name</b>	LS_CallDetailRecording_DroppedMessagesFromMQ Policy
<b>Description</b>	This policy monitors the number of messages that are dropped from the MSMQ queue.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 006 - Dropped messages from MQ
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_CallDetailRecording\_MessagesFailedValidation

<b>Policy Name</b>	LS_CallDetailRecording_MessagesFailedValidation Policy
<b>Description</b>	This policy monitors the number of messages that failed the validation process.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 002 - Messages that failed validation
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_MessagesFailedWrittenDB

<b>Policy Name</b>	LS_CallDetailRecording_MessagesFailedWrittenDB Policy
<b>Description</b>	This policy monitors the number of messages that failed to get written to the SQL database.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 02 - WRITE
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 002 - Messages failed to be written to DB
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_NoOfFailuresDueToInternalLks

<b>Policy Name</b>	LS_CallDetailRecording_NoOfFailuresDueToInternalLks Policy
<b>Description</b>	This policy monitors the number of error report failures that occurred because of internal locks.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 03 - Report Error
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 001 - Number of failures due to internal locks
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_NumberOfThrottledErrorReports

<b>Policy Name</b>	LS_CallDetailRecording_NumberOfThrottledErrorReports Policy
<b>Description</b>	This policy monitors the number of error reports throttled because of the limit on maximum reports in a minute.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 03 - Report Error
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 002 - Number of throttled error reports due to max report per minute limit
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_NumberOfUnknownFailures

<b>Policy Name</b>	LS_CallDetailRecording_NumberOfUnknownFailures Policy
<b>Description</b>	This policy monitors the number of unknown error report failures.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 03 - Report Error
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 000 - Number of unknown failures
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_PageFaultsPerSec

<b>Policy Name</b>	LS_CallDetailRecording_PageFaultsPerSec Policy
<b>Description</b>	The LS_CallDetailRecording_PageFaultsPerSec policy monitors the Page Faults/sec counter of the CallDetailRecording Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RtcCdr
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

### LS\_CallDetailRecording\_PrivateBytes

<b>Policy Name</b>	LS_CallDetailRecording_PrivateBytes Policy
<b>Description</b>	The LS_CallDetailRecording_PrivateBytes policy monitors the private bytes counter.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RtcCdr
<b>Counter</b>	PrivateBytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_CallDetailRecording\_ProcessorTime

<b>Policy Name</b>	LS_CallDetailRecording_ProcessorTime Policy.
<b>Description</b>	The LS_CallDetailRecording_ProcessorTime policy monitors the '% Processor Time' counter of the CallDetailRecording Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RtcCdr
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

### LS\_CallDetailRecording\_QueueLatency

<b>Policy Name</b>	LS_CallDetailRecording_QueueLatency Policy
<b>Description</b>	This policy monitors the average time (in milliseconds) the database holds a request in queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_ThreadCount

<b>Policy Name</b>	LS_CallDetailRecording_ThreadCount Policy
<b>Description</b>	The LS_CallDetailRecording_ThreadCount policy monitors the thread count counter of the CallDetailRecording Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RtcCdr
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 150</b>

### LS\_CallDetailRecording\_TotalDeadLks

<b>Policy Name</b>	LS_CallDetailRecording_TotalDeadLks Policy
<b>Description</b>	This policy monitors the total number of deadlocks that have occurred since the start of the server.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 013 - Total Deadlocks
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TotalFatalSQLErrors

<b>Policy Name</b>	LS_CallDetailRecording_TotalFatalSQLErrors Policy
<b>Description</b>	This policy monitors the number of fatal SQL errors that have taken place since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 019 - Total fatal SQL errors
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TotalODBCFailures

<b>Policy Name</b>	LS_CallDetailRecording_TotalODBCFailures Policy
<b>Description</b>	This policy monitors the number of ODBC timeout failures that have taken place since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 017 - Total ODBC Timeout Failures
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TotalSevereSQLErrors

<b>Policy Name</b>	LS_CallDetailRecording_TotalSevereSQLErrors Policy
<b>Description</b>	This policy monitors the number of severe SQL errors that occurred since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 018 - Total severe SQL errors
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TotalThrottledRequests

<b>Policy Name</b>	LS_CallDetailRecording_TotalThrottledRequests Policy
<b>Description</b>	This policy monitors the number of requests that were rejected with a retry-after due to high database queue latency.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 021 - Total throttled requests
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TransactionsAborted

<b>Policy Name</b>	LS_CallDetailRecording_TransactionsAborted Policy
<b>Description</b>	This policy monitors the number of transactions that are aborted.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 010 - Transactions aborted
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>



### LS\_CallDetailRecording\_WorkingSet

<b>Policy Name</b>	LS_CallDetailRecording_WorkingSet Policy
<b>Description</b>	The LS_CallDetailRecording_WorkingSet policy monitors the Working Set counter of the CallDetailRecording Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	RtcCdr
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_Check\_CallDetailRecordingServiceStatus\_

<b>Policy Name</b>	LS_Check_CallDetailRecordingServiceStatus Policy
<b>Description</b>	The LS_Check_CallDetailRecordingServiceStatus checks the status of the Call Detail Recording Service. This policy sends a critical alert message if the service is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCCDR

### LS\_Check\_Monitor\_ADStatus

<b>Policy Name</b>	LS_Check_Monitor_ADStatus Policy
<b>Description</b>	The policy LS_Check_Monitor_ADStatus checks the connectivity status of the Active Directory with the Monitoring Server and sends a critical alert message if the Active Directory is not accessible from the Monitoring Server. After the connectivity is obtained, the policy sends a normal message and acknowledges the critical alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.

### LS\_Check\_Monitor\_ReplicaStatus

<b>Policy Name</b>	LS_Check_Monitor_ReplicaStatus Policy
<b>Description</b>	The policy LS_Check_Monitor_ReplicaStatus checks the Central Management Store replication status at the Monitoring Server. This policy sends out a critical alert message if the Central Management Store data is not updated. After the Central Management Store data is updated, the policy sends a normal message and acknowledges the critical error message sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	REPLICA

### LS\_Check\_QualityMonitoringServiceStatus

<b>Policy Name</b>	LS_Check_QualityMonitoringServiceStatus Policy
<b>Description</b>	The LS_Check_QualityMonitoringServiceStatus checks the status of the QoE Monitoring Service. This policy sends a critical alert message if the QualityMonitoringService is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCQMS

### LS\_Check\_ReplicaServiceStatus\_Monitor

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Monitor Policy
<b>Description</b>	The policy LS_Check_ReplicaServiceStatus_Monitor checks the status of the Replica Replicator Agent Service at the Monitoring Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

### LS\_QualityMonitoring\_NoIncorrectMSMQMsgsReceive

<b>Policy Name</b>	LS_QualityMonitoring_NoIncorrectMSMQMsgsReceive Policy
<b>Description</b>	This policy monitors the number of discarded MSMQ messages that are not of the expected type or version.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:QMS - 00 - QoEMonitoringServer

<b>Policy Name</b>	LS_QualityMonitoring_NoIncorrectMSMQMsgsReceive Policy
<b>Instance</b>	All instances.
<b>Counter</b>	QMS - 004 - Number of MSMQ messages received with an incorrect type or version
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 20

#### LS\_QualityMonitoring\_PageFaultsPerSec

<b>Policy Name</b>	LS_QualityMonitoring_PageFaultsPerSec Policy
<b>Description</b>	The LS_QualityMonitoring_PageFaultsPerSec policy monitors the Page Faults/sec counter of the QualityMonitoring Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	QmsSvc
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 100

#### LS\_QualityMonitoring\_PrivateBytes

<b>Policy Name</b>	LS_QualityMonitoring_PrivateBytes Policy
<b>Description</b>	The LS_QualityMonitoring_PrivateBytes policy monitors the Private Bytes counter of the QualityMonitoring Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	QmsSvc
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_QualityMonitoring\_ProcessorTime

<b>Policy Name</b>	LS_QualityMonitoring_ProcessorTime Policy
<b>Description</b>	The LS_QualityMonitoring_ProcessorTime policy monitors the '% Processor Time' counter of the QualityMonitoring Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	QmsSvc
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_QualityMonitoring\_ThreadCount

<b>Policy Name</b>	LS_QualityMonitoring_ThreadCount Policy
<b>Description</b>	The LS_QualityMonitoring_ThreadCount policy monitors the Thread Count counter of the QualityMonitoring Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	QmsSvc
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_QualityMonitoring\_WorkingSet

<b>Policy Name</b>	LS_QualityMonitoring_WorkingSet Policy
<b>Description</b>	The LS_QualityMonitoring_WorkingSet policy monitors the working set counter of the QualityMonitoring Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	QmsSvc
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

### LS\_QualityMonitoring\_NoRptssDropDueToDBFailure

<b>Policy Name</b>	LS_QualityMonitoring_NoRptssDropDueToDBFailure Policy
<b>Description</b>	This policy monitors the number of reports dropped because of database insertion failure. The transaction was committed prematurely because of an unrecoverable database error.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:QMS - 00 - QoEMonitoringServer
<b>Instance</b>	All instances.
<b>Counter</b>	QMS - 003 - Total number of reports that were dropped due to database insertion failure.
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_QualityMonitoring\_NoRptssDropDueToDBFailure

<b>Policy Name</b>	LS_QualityMonitoring_NoRptssDropDueToDBFailure Policy
<b>Description</b>	This policy monitors the number of reports dropped because of database insertion failure. The transaction was committed prematurely because of an unrecoverable database error.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:QMS - 00 - QoEMonitoringServer
<b>Instance</b>	All instances.
<b>Counter</b>	QMS - 003 - Total number of reports that were dropped due to database insertion failure.
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Replica\_PageFaultsPerSec

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Description</b>	The LS_ReplicaService_PageFaultsPerSec policy monitors the Page Faults/sec counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process

<b>Policy Name</b>	LS_Replica_PageFaultsPerSec Policy
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Page Faults/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 100</b>

#### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	The LS_Replica_ProcessorTime policy monitors the % Processor Time counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 90</b>

#### LS\_Replica\_PrivateBytes

<b>Policy Name</b>	LS_Replica_PrivateBytes Policy
<b>Description</b>	The LS_Replica_PrivateBytes policy the Private Bytes counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process.
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Private Bytes
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 2e+007</b>

### LS\_Replica\_ProcessorTime

<b>Policy Name</b>	LS_Replica_ProcessorTime Policy
<b>Description</b>	The LS_Replica_ProcessorTime policy monitors the '% Processor Time' counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	% Processor Time
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 90

### LS\_Replica\_ThreadCount

<b>Policy Name</b>	LS_Replica_ThreadCount Policy
<b>Description</b>	The LS_ReplicaService_ThreadCount policy monitors the Thread Count counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Thread Count
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 150

### LS\_Replica\_WorkingSet

<b>Policy Name</b>	LS_Replica_WorkingSet Policy
<b>Description</b>	The LS_Replica_WorkingSet policy monitors the Working Set counter of the Replica Service.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	Process
<b>Instance</b>	ReplicaReplicatorAgent
<b>Counter</b>	Working Set
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 2e+007

## GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the Monitoring Server.

### LS\_CallDetailRecording\_MessagesFailedValidation

<b>Policy Name</b>	LS_CallDetailRecording_MessagesFailedValidation Policy
<b>Description</b>	This policy monitors the number of messages that failed the validation process.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 002 - Messages that failed validation
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_MessagesFailedWrittenDB

<b>Policy Name</b>	LS_CallDetailRecording_MessagesFailedWrittenDB Policy
<b>Description</b>	This policy monitors the number of messages that failed to get written to the SQL database.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 02 - WRITE
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 002 - Messages failed to be written to DB
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_QueueLatency

<b>Policy Name</b>	LS_CallDetailRecording_QueueLatency Policy
<b>Description</b>	This policy monitors the average time (in milliseconds) the database holds a request in queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr



<b>Policy Name</b>	LS_CallDetailRecording_QueueLatency Policy
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### **LS\_CallDetailRecording\_TotalDeadLks**

<b>Policy Name</b>	LS_CallDetailRecording_TotalDeadLks Policy
<b>Description</b>	This policy monitors the total number of deadlocks that have occurred since the start of the server.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 013 - Total Deadlocks
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### **LS\_CallDetailRecording\_TotalFatalSQLErrors**

<b>Policy Name</b>	LS_CallDetailRecording_TotalFatalSQLErrors Policy
<b>Description</b>	This policy monitors the number of fatal SQL errors that have taken place since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances.
<b>Counter</b>	CDR Service - 019 - Total fatal SQL errors
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TotalThrottledRequests

<b>Policy Name</b>	LS_CallDetailRecording_TotalThrottledRequests Policy
<b>Description</b>	This policy monitors the number of requests that were rejected with a retry-after due to high database queue latency.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 00 - DBCdr
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 021 - Total throttled requests
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_CallDetailRecording\_TransactionsAborted

<b>Policy Name</b>	LS_CallDetailRecording_TransactionsAborted Policy
<b>Description</b>	This policy monitors the number of transactions that are aborted.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:CDR Service - 01 - READ
<b>Instance</b>	All instances
<b>Counter</b>	CDR Service - 010 - Transactions aborted
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Check\_CallDetailRecordingServiceStatus

<b>Policy Name</b>	LS_Check_CallDetailRecordingServiceStatus Policy
<b>Description</b>	The LS_Check_CallDetailRecordingServiceStatus checks the status of the Call Detail Recording Service. This policy sends a critical alert message if the service is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCCDR

### LS\_Check\_QualityMonitoringServiceStatus

<b>Policy Name</b>	LS_Check_QualityMonitoringServiceStatus Policy
<b>Description</b>	The LS_Check_QualityMonitoringServiceStatus checks the status of the QoE Monitoring Service. This policy sends a critical alert message if the QualityMonitoringService is not running. After the service starts the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	RTCQMS

### LS\_Check\_ReplicaServiceStatus\_Monitor

<b>Policy Name</b>	LS_Check_ReplicaServiceStatus_Monitor Policy
<b>Description</b>	The policy LS_Check_ReplicaServiceStatus_Monitor checks the status of the Replica Replicator Agent Service at the Monitoring Server and returns values that correspond to different states of the service. This policy sends a critical alert message if the Replica Replicator Agent Service is not running. After the service starts, the policy acknowledges the alert sent previously.
<b>Schedule</b>	This policy runs every 5 minutes.
<b>Monitored Service</b>	Replica Replicator Agent

### LS\_QualityMonitoring\_NoIncorrectMSMQMsgsReceive

<b>Policy Name</b>	LS_QualityMonitoring_NoIncorrectMSMQMsgsReceive Policy
<b>Description</b>	This policy monitors the number of discarded MSMQ messages that are not of the expected type or version.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:QMS - 00 - QoEMonitoringServer
<b>Instance</b>	All instances.
<b>Counter</b>	QMS - 004 - Number of MSMQ messages received with an incorrect type or version
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_QualityMonitoring\_NoRptssDropDueToDBFailure

<b>Policy Name</b>	LS_QualityMonitoring_NoRptssDropDueToDBFailure Policy
<b>Description</b>	This policy monitors the number of reports dropped because of database insertion failure. The transaction was committed prematurely because of an unrecoverable database error.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:QMS - 00 - QoEMonitoringServer
<b>Instance</b>	All instances.
<b>Counter</b>	QMS - 003 - Total number of reports that were dropped due to database insertion failure.
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

## Registrar

The registrar server is a component that accepts register requests from users and is located along with a Director or a Front End server.

### General Policies

The General policy group contains all the policies that monitor the processes and services of the Registrar Server.

#### LS\_Registrar\_EndpointsDisconnected

<b>Policy Name</b>	LS_Registrar_EndpointsDisconnected Policy
<b>Description</b>	This policy monitors the number of endpoints that are disconnected because of missed keep-alives.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 12 - Register
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 011 - Endpoints Disconnected
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_IndirectEndpointsDisconnected

<b>Policy Name</b>	LS_Registrar_IndirectEndpointsDisconnected Policy
<b>Description</b>	This policy monitors the number of indirect endpoints that are disconnected because of error responses.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 12 - Register
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 012 - Indirectly Connected Endpoints Disconnected
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_LegacyRegistersRejected

<b>Policy Name</b>	LS_Registrar_LegacyRegistersRejected Policy
<b>Description</b>	This policy monitors the number of legacy registers that are rejected because the publisher is in rich mode.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 12 - Register
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 005 - Legacy REGISTERS rejected (421 Response)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_QueueDepth

<b>Policy Name</b>	LS_Registrar_QueueDepth Policy
<b>Description</b>	This policy monitors the average number of database requests to execute.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 000 - Queue Depth
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_QueueLatency

<b>Policy Name</b>	LS_Registrar_QueueLatency Policy
<b>Description</b>	This policy monitors the average time (in milliseconds) a request is held in database queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_RegistrationNotificationSent

<b>Policy Name</b>	LS_Registrar_RegistrationNotificationSent Policy
<b>Description</b>	This policy monitors the number of deregistered notifications that are sent to the contacts. These notifications are sent when the server decides that the contacts are invalid.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 12 - Register
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 006 - Registration Notifications Sent
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_ThrottledRequests

<b>Policy Name</b>	LS_Registrar_ThrottledRequests Policy
<b>Description</b>	This policy monitors the number of requests rejected in a second with a message to retry later because of the high database latency.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 020 - Throttled requests/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20.</b>

### LS\_Registrar\_TotalDeadlkFailure

<b>Policy Name</b>	LS_Registrar_TotalDeadlkFailures Policy
<b>Description</b>	This policy monitors the number of deadlock failures occurred since the server was started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 015 - Total Deadlock Failures
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalDeadLks

<b>Policy Name</b>	LS_Registrar_TotalDeadLks Policy
<b>Description</b>	This policy monitors the number of deadlocks occurred since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 013 - Total Deadlocks
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalDroppedRequests

<b>Policy Name</b>	LS_Registrar_TotalDroppedRequests Policy
<b>Description</b>	This policy monitors the number of requests dropped by the database layer as they will time out.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 014 - Total Dropped Requests
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalFatalSQLErrors

<b>Policy Name</b>	LS_Registrar_TotalFatalSQLErrors Policy
<b>Description</b>	This policy monitors the number of fatal SQL errors occurred since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 019 - Total fatal SQL errors
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalODBCTimeoutFailures

<b>Policy Name</b>	LS_Registrar_TotalODBCTimeoutFailures Policy
<b>Description</b>	This policy monitors the number of ODBC timeout failures occurred since the server was started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 017 - Total ODBC Timeout Failures
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalSevereSQLErrors

<b>Policy Name</b>	LS_Registrar_TotalSevereSQLErrors Policy
<b>Description</b>	This policy monitors the number of severe SQL errors occurred since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 018 - Total severe SQL errors
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>



### LS\_Registrar\_TotalThrottledRequests

<b>Policy Name</b>	LS_Registrar_TotalThrottledRequests Policy
<b>Description</b>	This policy monitors the number of requests rejected with a message to retry after some time because of high database queue latency.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 021 - Total throttled requests
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### GoldenMetrics

The GoldenMetrics policy group is a sub set of the General policy group. This sub-group contains policies mandatory for monitoring the Microsoft Lync Server 2010. You must deploy these policies on the Registrar Server.

### LS\_Registrar\_EndpointsDisconnected

<b>Policy Name</b>	LS_Registrar_EndpointsDisconnected Policy
<b>Description</b>	This policy monitors the number of endpoints that are disconnected because of missed keep-alives.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 12 - Register
<b>Instance</b>	All instances
<b>Counter</b>	USrv - 011 - Endpoints Disconnected
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_IndirectEndpointsDisconnected

<b>Policy Name</b>	LS_Registrar_IndirectEndpointsDisconnected Policy
<b>Description</b>	This policy monitors the number of indirect endpoints that are disconnected because of error responses.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 12 - Register

<b>Policy Name</b>	LS_Registrar_IndirectEndpointsDisconnected Policy
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 012 - Indirectly Connected Endpoints Disconnected
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_Registrar\_QueueDepth

<b>Policy Name</b>	LS_Registrar_QueueDepth Policy
<b>Description</b>	This policy monitors the average number of database requests to execute.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 000 - Queue Depth
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

#### LS\_Registrar\_QueueLatency

<b>Policy Name</b>	LS_Registrar_QueueLatency Policy
<b>Description</b>	This policy monitors the average time (in milliseconds) a request is held in database queue.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 002 - Queue Latency (msec)
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_ThrottledRequests

<b>Policy Name</b>	LS_Registrar_ThrottledRequests Policy
<b>Description</b>	This policy monitors the number of requests rejected in a second with a message to retry later because of the high database latency.
<b>Schedule</b>	This policy runs every 15 minutes.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 020 - Throttled requests/sec
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 20.

### LS\_Registrar\_TotalDeadlkFailures

<b>Policy Name</b>	LS_Registrar_TotalDeadlkFailures Policy
<b>Description</b>	This policy monitors the number of deadlock failures occurred since the server was started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 015 - Total Deadlock Failures
<b>Threshold</b>	This policy has the following threshold: <b>Critical:</b> 20

### LS\_Registrar\_TotalDeadLks

<b>Policy Name</b>	LS_Registrar_TotalDeadLks Policy
<b>Description</b>	This policy monitors the number of deadlocks occurred since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 013 - Total Deadlocks
<b>Threshold</b>	This policy has the following threshold: Critical: 20

### LS\_Registrar\_TotalDroppedRequests

<b>Policy Name</b>	LS_Registrar_TotalDroppedRequests Policy
<b>Description</b>	This policy monitors the number of requests dropped by the database layer as they will time out.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 014 - Total Dropped Requests
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalFatalSQLErrors

<b>Policy Name</b>	LS_Registrar_TotalFatalSQLErrors Policy
<b>Description</b>	This policy monitors the number of fatal SQL errors occurred since the server started.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 019 - Total fatal SQL errors
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

### LS\_Registrar\_TotalThrottledRequests

<b>Policy Name</b>	LS_Registrar_TotalThrottledRequests Policy
<b>Description</b>	This policy monitors the number of requests rejected with a message to retry after some time because of high database queue latency.
<b>Schedule</b>	This policy runs every one hour.
<b>Performance Object</b>	LS:USrv - 00 - REGDBStore
<b>Instance</b>	All instances.
<b>Counter</b>	USrv - 021 - Total throttled requests
<b>Threshold</b>	This policy has the following threshold: <b>Critical: 20</b>

# Reports

The Microsoft Enterprise Servers SPI for Microsoft Lync Server 2010 has the following reports:

## LS2K10 Front End Service CPU Stat

The LS2K10 Front End Service CPU Stat report shows CPU statistics of the front end service compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the front end service compared with the percentage of time the system's CPU was busy.

## LS2K10 IM Conferencing Service CPU Stat

The LS2K10 IM Conferencing Service CPU Stat report shows CPU statistics of the IM conferencing service compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the IM conferencing compared with the percentage of time the system's CPU was busy.

## LS2K10 Access Edge Service CPU Stat

The LS2K10 Access Edge Service CPU Stat report shows CPU statistics of the access edge service compared with overall CPU statistics of the system, in graphical and tabular format. The summarized process statistics include the percentage of CPU time used by the access edge compared with the percentage of time the system's CPU was busy.

## LS2K10 Front End Service Memory Stat

The LS2K10 Front End Service Memory Stat report shows summary memory statistics of the front end service in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the front end service.

## LS2K10 IM Conferencing Service Memory Stat

The LS2K10 IM Conferencing Service Memory Stat report shows summary memory statistics of the IM conferencing service in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the IM conferencing service.

## LS2K10 Access Edge Service Memory Stat

The LS2K10 Access Edge Service Memory Stat report shows summary memory statistics of the access edge service in graphical and tabular format. The summarized process statistics include the page faults per second, private bytes, and working set used by the access edge service.

## LS2K10 SQL Back End Lat Exp by Front End Server

The LS2K10 SQL Back End Lat Exp by Front End Server report shows the amount of time that a request spent in the queue to the SQL back end and the amount of time taken by the back end to process in graphical (line graph) and tabular format. If either the queue latency or processing latency is high, the front end will start throttling requests to the back end.

## LS2K10 Avg Hold Time for In Msg Front End Server

The LS2K10 Avg Hold Time for In Msg Front End Server report shows the average holding time for incoming messages on the front end server in graphical (line graph) and tabular format. A high value indicates that the front end server is overloaded and unable to process the requests on time.

## LS2K10 Front End Server Avail and Conn

The LS2K10 Front End Server Avail and Conn report shows the Local 503 Responses/sec and the Local 504 Responses/sec on the front end server in graphical (line graph) and tabular format. The 503 code indicates that the server is unavailable while the 504 code indicates that there are connectivity problems with other servers.

## LS2K10 Sends Outstanding on Front End Server

The LS2K10 Sends Outstanding on Front End Server report shows the Sends Outstanding on the front end server in graphical (line graph) and tabular format. A high value means that a large number of requests and responses are queued outbound and this could be due to network latency issues or a problem with a remote server.

## LS2K10 Avg Inc Msg Proc Time Access Edge Server

The LS2K10 Avg Inc Msg Proc Time Access Edge Server report needs to depict the average incoming message processing time on the access edge server in graphical (line graph) and tabular format. High values indicate that the access edge server is overloaded and unable to process the requests on time.

## LS2K10 Client Request Err UDP AV Edge Server

The LS2K10 Client Request Err UDP AV Edge Server report shows the client request errors/sec, client send request errors/sec and the idle sessions timed-out/sec over UDP on the Audio/Video Edge Server in graphical and tabular format. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you may need to increase the session idle timeout parameter.

## LS2K10 Client Request Err TCP AV Edge Server

The LS2K10 Client Request Err TCP AV Edge Server report shows the client requests errors/sec, client send request errors/sec and the idle sessions timed-out/sec over TCP on the Audio/Video Edge Server in graphical and tabular format. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you may need to increase the session idle timeout parameter.

# Graphs

The graphs are pictorial representation of the various metrics. Graphs contain data that are collected by policies. The Microsoft Lync Server 2010 SPI graphs are as follows:

## Front End Service CPU statistics

The Front End Service CPU statistics graph shows the CPU statistics of the Front End service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the Front End service is utilizing the processor time. This graph uses the data collected by the LS\_FrontEndService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Web Conferencing Service CPU statistics

The Web Conferencing Service CPU statistics graph shows the CPU statistics of the web conferencing service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the web conferencing service is utilizing the processor time.

This graph uses the data collected by the LS\_WebConfService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## IM Conferencing Service CPU statistics

The IM Conferencing Service CPU statistics graph shows the CPU statistics of the IM conferencing service compared with overall CPU statistics of the system. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the IM conferencing service is utilizing the processor time. This graph uses the data collected by the LS\_IMConfService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Audio/Video Conferencing Service CPU statistics

The Audio/Video Conferencing Service CPU statistics graph shows the CPU statistics of the audio/video conferencing service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the audio/video conferencing service is utilizing the processor time.

This graph uses the data collected by the LS\_AVConfService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Access Edge Service CPU statistics

The Access Edge Service CPU statistics graph shows the CPU statistics of the access edge service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the access edge service is utilizing the processor time.

This graph uses the data collected by the LS\_AccessEdgeService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Audio/Video Edge Service CPU statistics

The Audio/Video Edge Service CPU statistics graph shows the CPU statistics of the audio/video edge service compared with overall CPU statistics of the system, in graphical format.

The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the audio/video edge service is utilizing the processor time.

This graph uses the data collected by the LS\_AVEdgeService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Audio/Video Authentication Service CPU statistics

The Audio/Video Authentication Service CPU statistics graph shows the CPU statistics of the audio/video authentication service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the audio/video authentication service is utilizing the processor time. This graph uses the data collected by the LS\_AVAuthService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Web Conferencing Edge Service CPU statistics

The Web Conferencing Edge Service CPU statistics graph shows the CPU statistics of the web conferencing edge service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the web conferencing edge service is utilizing the processor time.

This graph uses the data collected by the LS\_WebEdgeService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Archiving and CDR Service CPU statistics

The Archiving and CDR Service CPU statistics graph shows the CPU statistics of the Archiving and CDR service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the Archiving and CDR service is utilizing the processor time.

This graph uses the data collected by the LS\_ArchivingCDRService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Mediation Service CPU statistics

The Mediation Service CPU statistics graph shows the CPU statistics of the mediation service compared with overall CPU statistics of the system, in graphical format. The summarized process statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the mediation service is utilizing the processor time.

This graph uses the data collected by the LS\_MediationService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.



## Front End Service Memory Statistics

The Front End Service Memory Statistics graph shows the memory statistics of the front end service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the front end service.

This graph uses the data collected by the LS\_FrontEndService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Web Conferencing Service Memory Statistics

The Web Conferencing Service Memory Statistics graph shows the memory statistics of the web conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the web conferencing service.

This graph uses the data collected by the LS\_WebConfService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## IM Conferencing Service Memory Statistics

The IM Conferencing Service Memory Statistics graph shows the memory statistics of the IM conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the web conferencing service.

This graph uses the data collected by the LS\_IMConfService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Audio/Video Conferencing Service Memory Statistics

The Audio/Video Conferencing Service Memory Statistics graph shows the memory statistics of the audio/video conferencing service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the audio/video conferencing service.

This graph uses the data collected by the LS\_AVConfService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Access Edge Service Memory Statistics

The Access Edge Service Memory Statistics graph shows the memory statistics of the access edge service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the access edge service.

This graph uses the data collected by the LS\_AccessEdgeService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph. The statistics include the percentage of CPU time used by the service compared with the percentage of time the system's CPU was busy. The graph helps you to determine to what extent the mediation service is utilizing the processor time.

This graph uses the data collected by the LS\_MediationService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

## Audio/Video Edge Service Memory Statistics

The Audio/Video Edge Service Memory Statistics graph shows the memory statistics of the audio/video edge service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the audio/video edge service.

This graph uses the data collected by the LS\_AVEdgeService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

### Audio/Video Authentication Service Memory Statistics

The Audio/Video Authentication Service Memory Statistics graph shows the memory statistics of the audio/video authentication service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the audio/video authentication service.

This graph uses the data collected by the LS\_AVAuthService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

### Web Conferencing Edge Service Memory Statistics

The Web Conferencing Edge Service Memory Statistics graph shows the memory statistics of the web conferencing edge service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the web conferencing edge service.

This graph uses the data collected by the LS\_WebEdgeService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

### Archiving and CDR Service Memory Statistics

The Archiving and CDR Service Memory Statistics graph shows the memory statistics of the Archiving and CDR service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the Archiving and CDR service.

This graph uses the data collected by the LS\_ArchivingCDRService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

### Mediation Service Memory Statistics

The Mediation Service Memory Statistics graph shows the memory statistics of the mediation service in graphical format. The summarized process statistics include the page faults per second, private bytes, and working set used by the mediation service.

This graph uses the data collected by the LS\_MediationService\_Logging policy. In the data store of the node, the LS\_PROCESS table is used to construct this graph.

### Authentication failures/sec on Audio/Video Edge Server

The Authentication failures/sec on Audio/Video Edge Server graph shows the authentication failures per sec over UDP and TCP on the A/V Edge Server. This graph uses the data collected by the LS\_AVEdgeServer\_Logging policy. In the data store of the node, the LS\_AVEDGE table is used to construct this graph.

### SQL Back End Latency Experienced By Front End Server

The SQL Back End Latency Experienced By Front End Server graph shows the amount of time that a request spent in the queue to the SQL back end and the time taken by the SQL backend to process a request. . If either the queue latency or processing latency is high, the front end will start throttling requests to the back end.

This graph uses the data collected by the LS\_FrontEndServer\_Logging policy. In the data store of the node, the LS\_FRONTEND table is used to construct this graph.

### Average Holding Time for Incoming Messages on Front End Server

The Average Holding Time for Incoming Messages on Front End Server graph shows the average holding time for incoming messages on the front end server. A high value indicates that the front end server is overloaded and unable to process the requests on time.

This graph uses the data collected by the LS\_FrontEndServer\_Logging policy. In the data store of the node, the LS\_FRONTEND table is used to construct this graph.

### Front End Server Availability and Connectivity

The Front End Server Availability and Connectivity graph shows the Local 503 Responses/sec on the front end server. The 503 code indicates that the server is unavailable while the 504 code indicates connectivity problems with other servers.

This graph uses the data collected by the LS\_FrontEndServer\_Logging policy. In the data store of the node, the LS\_FRONTEND table is used to construct this graph.

### Sends Outstanding on Front End Server

The Sends Outstanding on Front End Server graph shows the Sends Outstanding on the front end server. A high value means that a large number of requests and responses are queued outbound and could be due to network latency issues or a problem with a remote server.

This graph uses the data collected by the LS\_FrontEndServer\_Logging policy. In the data store of the node, the LS\_FRONTEND table is used to construct this graph.

### Average Incoming Message Processing Time on Access Edge Server

The Average Incoming Message Processing Time on Access Edge Server graph shows the Average Incoming Message Processing Time on the Access Edge Server. High values indicate that the Access Edge Server is overloaded and unable to process the requests on time.

This graph uses the data collected by the LS\_AccessEdgeServer\_Logging policy. In the data store of the node, the LS\_ACCESEEDGE table is used to construct this graph.

### Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server

The Client Request Errors and Timed Out Sessions over UDP on Audio/Video Edge Server graph shows the client requests errors/sec, client send request errors/sec and the idle sessions timed-out/sec over UDP on the Audio/Video Edge Server. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you can increase the session idle timeout parameter.

This graph uses the data collected by the LS\_AVEdgeServer\_Logging policy. In the data store of the node, the LS\_AVEDGE table is used to construct this graph.

## Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server

The Client Request Errors and Timed Out Sessions over TCP on Audio/Video Edge Server graph shows the client requests errors/sec, client send request errors/sec and the idle sessions timed-out/sec over TCP on the Audio/Video Edge Server. High values of client request errors/sec and client send request errors/sec can indicate network latency issues. If a large number of sessions time out per second, then you can increase the session idle timeout parameter.

This graph uses the data collected by the LS\_AVEdgeServer\_Logging policy. In the data store of the node, the LS\_AVEDGE table is used to construct this graph.

## 9 Microsoft Enterprise Servers SPI Tools

The Microsoft Enterprise Servers SPI has the following tools:

- MSES\_BTS\_DB\_Configuration
- Create Datasource for ISA Server
- Create Datasource for BizTalk Server
- BTS 2010 Create Datasource
- Self-Healing Info
- Self-Healing Verification
- Create Datasource for SharePoint Server
- Create Datasource for Lync Server 2010
- Configure Edge server Discovery for Lync Server 2010
- BTS 2010 Cluster Config
- BTS 2010 Enable Trace

### MSES\_BTS\_DB\_Configuration

The MSES\_BTS\_DB\_Configuration tool is used to configure the Microsoft BizTalk Server.

The BizTalk Server 2006 stores data in SQL server instead of the WMI CIMV2 database. The Microsoft Enterprise Servers SPI connects to the BizTalk Server's SQL database to collect the data.

Before running Discovery, the HPOM administrator must configure the SQL database for all nodes with BizTalk Server installed. Windows integrated security (SSPI mode) does not work if the SQL authentication mode is set for SQL server. If SQL authentication is "users /", the HPOM console needs to know the SQL user name and password. To connect to SQL server, if you choose to customize one or more policies after deploying them, ensure that you redeploy the policies after customizing them. Even when in SQL authentication mode, the HPOM administrator can use the MSES\_BTS\_DB\_Configuration tool to store the corresponding SQL server name, and SQL user name and password. If this configuration is not done for BizTalk Server 2006 nodes, the default SQL user name and password is considered.



To enable the X-Windows Server display, run the following command from the command line interface of the Management Server: `export DISPLAY=<system IP>:0.0`

Set the xterm path on the HPOM server before you run the MSES\_BTS\_DB\_Configuration tool.

For more details on the MSES\_BTS\_DB\_Configuration tool, see *Additional Configuration Procedure section of HP Operations Smart Plug-in for Microsoft Enterprise Servers Installation and Configuration Guide*.

## Create Datasource for ISA Server

The Create Datasource for ISA Server tool is launched to configure datasources for data logging in the ISA server. The name of the datasource configured using this tool is *ISAServer2006*.

## Create Datasource for BizTalk Server

The Create Datasource for BizTalk Server tool is launched to configure data sources for data logging in the BizTalk Server. The name of the data source configured using this tool is *MSES\_BIZTALKSERVER\_INTERVAL*.

## BTS 2010 Create Datasource

This tool configures the datasource for BizTalk Server 2010. The name of the datasource is *BTS\_Data*. By default, the datasource is created by CODA.

## Self-Healing Info

The Self-Healing Info tool runs the Microsoft Enterprise Servers SPI data collector on the selected nodes.

## Self-Healing Verification

The Self-Healing Verification tool verifies the versions of the Microsoft Enterprise Servers SPI components.

## Create Datasource for SharePoint Server

The Create Datasource for SharePoint Server tool is launched to configure data sources for data logging in the SharePoint Server 2010. The name of data source configured using this tool is *SharePoint\_Server*.

## Create Datasource for Lync Server 2010

The Create Datasource for Lync Server 2010 tool creates databases into the HP Operations agent data store (embedded performance component also known as CODA).

If you use Performance Agent as the data store, data source creation and data logging happens in Performance Agent, by default. There is no additional configuration required. If you do not have the HP Performance Agent installed in your environment, the tool creates databases into CODA.

## Configure Edge server Discovery for Lync Server 2010

The Configure Edge server Discovery for Lync Server 2010 tool stores user information required to run the *LS\_Discovery* policy on the Edge Server in an encrypted format. The SPI Discovery instrumentation reads the user information that is stored on the Edge Server.

## BTS 2010 Cluster Config

This tool generates the apminfo.xml file. This file provides necessary information to enable the Microsoft Enterprise SPI to identify and monitor BizTalk Server 2010 cluster nodes in the environment.

## BTS 2010 Enable Trace

This tool can be used to enable tracing for the BizTalk SPI data collector. By enabling tracing, you can collect the troubleshooting information. This tool can be run on all BizTalk Server 2010 nodes. This tool sets the trace level on the managed node. You must pass the following parameters as the trace level:

\$Trace Level - An integer value between 0 to 4, with 0 being the minimum and 4 being the maximum

The possible trace levels are as follows:

- 0 - No errors are logged. If no trace levels are passed, this is the default value.
- 1 - Warnings. All errors and warnings are logged.
- 3 - Debug. Apart from all other information, all debug trace statements are also logged.
- 4 - Verbose. All trace statements are logged

The log files are created in the %OvDataDir%\bin\BTS\log folder. Separate log files are created for each collection. All trace files have the prefix BTS.





# Index

## A

AccessEdgeServer 102  
Application Monitoring 83, 93  
Archiving CDR Server 117  
Availability Monitoring 17, 69, 82  
AVConfServer 121

## B

BizTalk Messaging Services 17  
Biztalk Orchestration Designer 17  
BizTalk Server  
    Graphs 25  
    Policies 17  
    Reports 23

## C

Configuration 139  
Create Datasource for ISA Server 328  
CWAServer 139

## D

Database Connectivity 20  
databases fail 20  
Data Store 180, 187  
Discovery 23, 76, 87, 97, 101

## F

FrontEnd Server 143

## H

HP Performance Manager 16  
HP Reporter 16

## I

IMConfServer 151

ISA Server  
    Graphs 79  
    Policies 69  
    Reports 76

## M

MediationServer 155  
Microsoft Enterprise Servers 15  
Microsoft Enterprise Server SPI Components 16  
Microsoft Office Communications Server  
    Graphs 181  
    Policies 91, 101, 191  
    Reports 177  
Microsoft Office SharePoint Server  
    Graphs 88  
    Policies 81  
    Reports 87, 97  
monitoring processes 17  
MSES\_BTS\_DB\_Configuration Tool 327

## O

Others 174

## P

Performance Monitoring 18, 70  
Policies 16

## S

Self-Healing Info 328  
Self-Healing Verification 328  
Server Logging 21, 75, 84  
Service Monitoring 82  
Services 15

## T

TelConfServer 159

## W

WebCompServer 162

WebConfServer 164  
WebEdgeServer 169

Windows Event Log Monitoring 20, 75

## 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:**



## 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:**

