

HP Operations Smart Plug-in for Microsoft® SQL Server

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

Software Version: 12.04

Reference Guide

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



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2000-2006, 2008-2010 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

Pentium® is a trademark of Intel Corporation in the U.S. and other countries.

UNIX® is a registered trademark of The Open Group.

Oracle is a registered trademark of Oracle and/or its affiliates.

Documentation Updates

This guide's title page contains the following identifying information:

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

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

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

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

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

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

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

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1	Microsoft SQL Server Policies	9
	Inside Microsoft SQL Server Policies	9
	Metric Column Key	9
	Microsoft SQL Server Metric Summary	11
	Metric Specification Description	20
	Metric M001_CacheHitPct	22
	Metric M007_ReadsOutstdRate	23
	Metric M008_WritsOutstdRate	25
	Metric M009_TransactionRate	25
	Metric M209_TransactionRate	27
	Metric M011_UserConnectPct	27
	Metric M013_LocksInUsePct	29
	Metric M014_BlckdProcessCnt	29
	Metric M215_VirtDevSpUsdPct	31
	Metric M216_TransLogUsedPct	33
	Metric M017_CmdQueueLenPct	36
	Metric M218_DBSpaceUsedPct	36
	Metric M022_BufChainAvgLen	38
	Metric M023_ReadWriteErrCnt	39
	Metric M024_PacketErrorCnt	40
	Metric M025_CPUUsedPct	41
	Metric M026_ActiveConntnPct	41
	Metric M227_PhysIOByUsrPct	43
	Metric M028_SuspectDBCnt	43
	Metric M030_ServerConnect	45
	Metric M230_DBConnect	46
	Metric M032_RunableContnPct	46
	Metric M233_DatabaseBackup	48
	Metric M234_TransactionLogBackup	48
	Metric M035_LongTransaction	50
	Metric M051_FullScansRate	53
	Metric M052_IndxSearchsRate	54
	Metric M053_PgesAlloctdRate	54
	Metric M054_ExtntsAllocRate	56
	Metric M055_PageSplitsRates	57
	Metric M056_TblLckEscalRate	57
	Metric M057_ServiceMon	59
	Metric M058_ServiceMon	60
	Metric M064_DBActivTransCnt	60

Metric M264_DBActivTransCnt	62
Metric M066_DBLogGrowthsCnt	62
Metric M266_DBLogGrowthsCnt	64
Metric M067_DBLogShrinksCnt	64
Metric M267_DBLogShrinksCnt	66
Metric M068_LatchWaitsRate	66
Metric M069_AvgLatchWaitTim.	68
Metric M070_LockTimeoutRate	68
Metric M270_LockTimeoutRate	70
Metric M071_DeadlocksRate	70
Metric M271_DeadlocksRate	72
Metric M072_LocksWaitRate	72
Metric M272_LocksWaitRate	74
Metric M073_LockAvgWaitTime.	74
Metric M273_LockAvgWaitTime.	76
Metric M074_BatchReqstsRate	76
Metric M075_LockMemoryPct	78
Metric M076_CurAvgLatchWait.	78
Metric M277_CompletedJobs	80
Metric M278_FileGrpUsedSpacePct.	81
Metric M279_FileGrpSpaceFree.	82
Metric M080_FailedReports	83
Metric M280_FailedReports	84
Metric M081_RepnAgentStatus	85
Metric M082_RepnLatency	86
Metric M083_DelLatency	87
Metric M084_DBMirroring_State.	88
Metric M085_DBMirroring_UnsentLog.	88
Metric M086_DBMirroring_UnrestoredLog.	90
Metric M087_DBMirroring_LogGenRate.	90
Metric M088_DBMirroring_CurrSndRate.	92
Metric M403_DistDelLatency	92
Metric M404_MergeConflicts	94
Metric M411_LogReaderDelLatency	95
Microsoft SQL Logfile Policies.	96
MSS-Error601	96
MSS-Error 602	97
MSS-Error 604	98
MSS-Error 605	99
MSS-Error 945	99
MSS-Error 1105	100
MSS-Error 1418	101
MSS-Error 1432	101
MSS-Error 1437	102
MSS-Error 1471	102
MSS-Error 1472	102
MSS-Error 1499	103

MSS-Error 1608	104
MSS-Error 3041	104
MSS-Error 3167	105
MSS-Error 3201	105
MSS-Error 3208	105
MSS-Error 6289	106
MSS-Error 6291	106
MSS-Error 6510	106
MSS-Error 6511	107
MSS-Error 6513	107
MSS-Error 6536	108
MSS-Error 6537	108
.....	108
MSS-Error 9001	109
MSS-Error9002	110
MSS-Error9004	111
MSS-Error 9642	111
.....	111
MSS-Error 10304	112
MSS-Error14151	113
MSS-Error15457	114
MSS-Error17824	114
MSS-Error17832	118
MSS-Error 18204	123
MSS-Error 20554	123
MSS-Error 20557	123
Catch all errors in the agent file	124
SQL Server is terminating...	124
SQL Server is starting....	124
MSS-Error Message above severity19	125
MSS-Error between severity 17 and 19	125
Scheduled Task Policies	126
2 Microsoft SQL Server Tools, Reports, and Graphs	127
Tools	127
Reports	129
Graphs	132
Metrics for Graphing or Alarming or Both	132
Using Metrics for Graphing Only	132
Generic Datasource Graphing Metrics	133
Generic Datasource Format	133
A Golden Metrics	135
Index	137

1 Microsoft SQL Server Policies

This chapter provides detailed and summary listings of the HP Operations Smart Plug-in for Databases (DB SPI) policies for Microsoft SQL server explaining pertinent information about how they work, text contained in the DB SPI Microsoft SQL Server logfile policies, and DB SPI Microsoft SQL Server Scheduled task policies. The information provided here should prove valuable in understanding each metric, especially if customization is desired.

Inside Microsoft SQL Server Policies

DB SPI measurement threshold policies are designed to be efficient and easy to use. In fact, you may want to use most policies without making any modifications whatsoever. However, if you do decide to make changes, this reference document provides information for each metric, information you need to know in order to customize any monitor policy.

For easy reference, a table at the beginning of the chapter lists all Microsoft SQL Server, version 2000, 2005, and 2008 metrics in summary form. The remainder of the chapter covers each metric in a table that lists the details.

Metric Column Key

Some columns in the metric summaries contain abbreviations or values that can be interpreted as follows:

Column Heading	Column content
INTERVAL	Frequency at which a metric is collected and analyzed; m= minutes h=hour d=day
RESET	W/O reset: Without reset Cont = Continuous ##% = Reset Value (With Reset)
THRESHOLD (Default Threshold)	Any "0.5" value means that the threshold is set at "0."Because HPOM alarms occur on <= or >=, the threshold is set to 0.5.

Column Heading	Column content
TYPE)	S=Server D=Database O=Object
A or G or both	A=alarming metric G=graphing metric
RPT ACCESS	Report Access (refers to whether DB SPI-generated ASCII reports are available and how to access them): Auto=Automatic Action Opt=Operator Action Tool=Tool Bank

Microsoft SQL Server Metric Summary

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M001_CacheHitPct	% of times a data page was found in the cache.	LRUS tats	S	1 hr	Min	70%	80%	Warning	A & G	Auto, Opt & Tool	LRUS tats
M007_ReadsOutstd Rate	# of read requests issued to the operating system that have not been completed.	IOStats	S	1 hr	Max	2/min	W/O	Warning	A & G	Auto, Opt & Tool	IOStats
M008_WritesOutstd Rate	# of write requests issued to the operating system that have not completed.	IOStats	S	1 hr	Max	1/min	W/O	Warning	A & G	Auto, Opt & Tool	IOStats
M009_TransactionRate	Server transactions rate	Server	S	1 hr	Max	100/sec	Cont	Minor	A & G	Auto, Opt & Tool	Trans
M209_TransactionRate	Database transactions rate	Database	D	1 hr	Max	100/sec	Cont	Minor	A	Auto	
M011_UserConnect Pct	% of current users connected	Process	S	5 min	Max	90% 98%	W/O	Major Critical	A & G	Auto, Opt & Tool	Users
M013_LocksInUsePct	% locks in use	Server	S	5 min	Max	80%	70%	Major	A & G	Auto, Opt & Tool	Locks

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M014_BlckdProcessCnt	# of blocked processes	Server	S	5 min	Max	3 for 1 min	W/O	Warning	A & G	Auto, Opt & Tool	Server
M215_VirtDevSpUsedPct	% of space used on a specific virtual device	Space	S	1 hr	Max	90% 95% 99%	W/O	Minor Major Critical	A	Auto & Tool	
M216_TransLogUsedPct	% of transaction log space used for each database	Space	D	15 m	Max	W/O	80% 90% 99%	Minor Major Critical	N	Auto & Tool	
M017_CmdQueueLenPct	% of command queue length used	Server	S	1 hr	Max	10%	W/O	Warning	A & G	Auto, Opt & Tool	Server
M218_DBSpaceUsedPct	% database space used	Space	D	1 hr	Max	95%	W/O	Critical	A	Auto & Tool	
M022_BufChainAvgLen	Buffer chain average length.	Cache	S	1 hr	Max	4	W/O	Warning	A & G	Auto, Opt & Tool	Cache
M023_ReadWriteErrorCnt	# of SQL Server read/write errors since the last probing.	Error	S	1 hr	Max	0.5	W/O	Warning	A & G	Auto, Opt & Tool	Error
M024_PacketErrorCnt	# of packet errors while reading or writing packets.	Error	S	1 hr	Max	0.5	W/O	Warning	A & G	Auto, Opt & Tool	Error

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M025_CPUUsedPct	% CPU time used by SQL Server	Server	S	5 min	Max	95% for 15 Min	W/O	Warning	A & G	Auto, Opt & Tool	Server
M026_ActiveConnPct	% of total connections that are active vs sleeping	Server	S	1 hr	Min	20%	W/O	Warning	A & G	Auto, Opt & Tool	Users
M227_PhysIOByUserPct	% of physical I/O used by process ID	Server	S	5 min	Max	95% for 10 min	W/O	Warning	A	Auto & Tool	
M028_SuspectDBCnt	# of databases marked as suspect.	Error	S	1 hr	Max	0.5	W/O	Critical	A & G	Auto, Opt & Tool	Error
M030_ServerConnect	Ability to connect to a server.	Server	S	5 min	Max	0.5	W/O	Critical	A	N/A	
M230_DBConnect	Ability to connect to a database.	Database	D	15 min	Max	0.5	Cont	Warning	A	Auto & Tool	
M031_NumUsersConn	Number of users	Server	S						G		Users
M032_RunableConnPct	% of total connections that are runnable	Server	S	1 hr	Max	50%	W/O	Warning	A	Auto & Opt	
M233_DatabaseBackup	# of hours since last database backup.	Backup	D	1 Day	Max	87600 168 72	Cont	Major Minor Warning	A	N/A	N/A

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M234_TransLogBackup	# of hours since last database transaction log backup	Backup	D	1 Day	Max	87600 0 48 24	Cont	Major Minor Warning	A	N/A	N/A
M035_LongTransaction	Long running transaction	Databases	D	5 min	Max	60	W/O	Major	A	N/A	N/A
M051_FullScansRate	Full scans rate	Access Methods	S	1 hr	Max	20/sec	Cont	Minor	A & G	Auto, Opt & Tool	Access
M052_IdxSearchsRate	Index searches rate	Access Methods	S	1 hr	Max	1000/sec	Cont	Minor	A & G	Auto, Opt & Tool	Access
M053_PgesAllocdRate	Pages allocated rate	Access Methods	S	1 hr	Max	1000/sec	Cont	Minor	A & G	Auto, Opt & Tool	Access
M054_ExtntsAllocRate	Extents allocated rate	Access Methods	S	1 hr	Max	300/sec	Cont	Minor	A & G	Auto, Opt & Tool	Access
M055_PageSplitsRates	Page splits rate	Access Methods	S	1 hr	Max	1000/sec	W/O	Minor	A & G	Auto, Opt & Tool	Access
M056_TblLckEscalRate	Table lock escalation rate	Access Methods	S	1 hr	Max	0.5	Cont	Minor	A & G	Auto, Opt & Tool	Access
M057_ServiceMonSQLServ	Monitor SQL Server Service (M057_ServiceMonSQLServ)	Server	S	5 min	Max	4.5 2.5 0.5	W/O	Critical Minor Warning	A	N/A	N/A

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M058_ServiceMonSQLAg	Monitor SQL Agent Service (M058_ServiceMonSQLAg)	Server	S	5 min	Max	4.5 2.5 0.5	W/O	Critical Minor Warning	A	N/A	N/A
M064_DBAktivTran	# of active transactions for the entire server	Server	S	1 hr	Max	5	W/O	Warning	A & G	Auto, Opt & Tool	Server
M264_DBAktivTran	# of active transactions for each database	Databases	D	1 hr	Max	5	W/O	Warning	A	Auto	
M066_DBLogGrowthsCnt	# of transaction log expansions for server	Server	S	1 hr	Max	4	Cont	Major	A & G	Auto, Opt & Tool	Trans
M266_DBLogGrowthsCnt	# of transaction log expansions per database	Databases	D	1 hr	Max	4	Cont	Major	A	Auto	
M067_DBLogShrinksCnt	# of server transaction log shrinks for server	Server	S	1 hr	Max	4	Cont	Major	A	Auto & Tool	
M267_DBLogShrinksCnt	# of database transaction log shrinks per database	Databases	D	1 hr	Max	4	Cont	Major	A	Auto	
M068_LatchWaitsRate	Latch waits rate	Latches	S	1 hr	Max	10/sec	Cont	Minor	A & G	Auto, Opt & Tool	Latches
M069_AvgLatchWaitTim	Average latch wait time	Latches	S	1 hr	Max	500 ms	Cont	Minor	A & G	Auto, Opt & Tool	Latches

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M070_LockTimeoutRate	Lock timeout rate	Locks	S	1 hr	Max	10/sec	Cont	Minor	A & G	Auto, Opt & Tool	Locks
M270_LockTimeoutRate	Lock timeout rate for each object type: Extent, Key, Page, Table, RID, Database.	Locks	O	1 hr	Max	10/sec	Cont	Minor	A	Auto	
M071_DeadlocksRate	Deadlocks rate	Locks	S	1 hr	Max	3/sec	Cont	Major	A & G	Auto, Opt & Tool	Locks
M271_DeadlocksRate	Deadlocks rate for each object type: Extent, Key, Page, Table, RID, Database.	Locks	O	1 hr	Max	3/sec	Cont	Major	A	Auto	
M072_LocksWaitRate	Locks wait rate	Locks	S	1 hr	Max	10/sec	Cont	Minor	A & G	Auto, Opt & Tool	Locks
M272_LocksWaitRate	Locks wait rate per object type	Locks	S	1 hr	Max	10	Cont	Minor	A	Auto	N/A
M073_LockAvgWaitTime	Average lock wait time	Locks	S	1 hr	Max	500 ms	W/O	Minor	A & G	Auto, Opt & Tool	Locks

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M273_LockAvgWait Time	Average lock wait time for each object type: Extent, Key, Page, Table, RID, Database	Locks	O	1 hr	Max	500 ms	W/O	Minor	A	Auto	
M074_BatchReqsts Rate	Batch requests rate	Server	S	1 hr	Max	500/sec	W/O	Minor	A & G	Auto, Opt & Tool	Server
M075_LockMemory Pct	% of lock memory in use	Server	S	1 hr	Max	37%	Cont	Warning	A & G	Auto, Opt & Tool	Locks
M076_CurAvgLatch Wait	Current average latch wait time	Latches	S	1 hr	Max	500 ms	Cont	Minor	A & G	Auto & Opt	Latches
M277_CompletedJobs	Report on all jobs, successful, failed & canceled	Jobs	S	5 min	Max	2=Fail 3=Cancelled	Cont	Major Warning	A	Auto & Opt	N/A
M278_FileGrpUsed SpacePct	% space used per filegroup and database	Space	D	15 min	Max	90% 95% 99%	W/O	Minor Major Critical	A	Auto & Tool	N/A
M279_FileGrpSpace Free	Space free (MB) per filegroup per database	Space	D	15 min	Min	150 MB 100 MB 50 MB	W/O	Minor Major Critical	A	Auto & Tool	N/A
M080_ReportsFailed	Number of Reports (Reporting Services) Failed	Reports	D	N/A	Max	1.0	W/O	Minor	A	Auto	N/A

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M280_ReportsFailed	Number of Reports (Reporting Services) Failed (drill-down)	Reports	D	N/A	Max	1.0	W/O	Minor	A	Auto & Tool	N/A
M081_RepnAgentStatus	Replication agents status	Database	D	5 m	Max	0.5	Cont	Major	A	Auto, Opt & Tool	N/A
M082_RepnLatency	Replication Latency	Database	D	15 m	Max	60.0	Cont	Warning	A	Auto, Opt & Tool	N/A
M083_DelLatency	Delivery Latency	Database	D	15 m	Max	60.0	Cont	Warning	A	Auto, Opt & Tool	N/A
M084_DBMirroring_State	Mirroring state of the server instance (M084_DBMirroring_State)	DBMirroring	S	5 m	Max	0.5	Cont	Warning	A	Auto, & Tool	N/A
M085_DBMirroring_UnsentLog	Unsent log on the principal (M085_DBMirroring_UnsentLog)	DBMirroring	S	150 m	Max	95 90	Cont	Major Warning	A	Auto, & Tool	N/A
M086_DBMirroring_UnrestoredLog	Unrestored log on the mirror (M086_DBMirroring_UnstoredLog)	DBMirroring	S	15 m	Max	95 90	Cont	Major Warning	A	Auto, & Tool	N/A

Microsoft SQL Server Metric	Description	Area	Type	Interval	Min/Max	Threshold	Reset	Severity	A or G	Rpt Access	Graph
M087_DBMirroring_LogGenRate	Log generation rate on the principal	DBMirroring	S	15 m	Max	10	Cont	Warning	A	Auto, & Tool	N/A
M088_DBMirroring_CurrSndRate	Current send rate on the principal	DBMirroring	S	15 m	Max	10	Cont	Warning	A	Auto, & Tool	N/A
M403_DistDelLatency	Time (in milliseconds) elapsed from when transactions are delivered to the Distributor to when they are applied at the Subscriber.	Microsoft SQL Server Replication	S	15 m	Max	10000 ms 30000 ms	W/O	Major Warning	A	N/A	N/A
M404_MergeConflicts	Number of conflicts per second during Publisher or Subscriber upload and download.	Microsoft SQL Server Replication	S	15 m	Max	15	W/O	Major Warning	A	N/A	N/A
M411_LogReaderDeLlatency	Time (in milliseconds) elapsed from when transactions are applied at the Publisher to when they are delivered to the Distributor.	Microsoft SQL Server Replication	S	15 m	Max	10000 ms 30000 ms	W/O	Major Warning	A	N/A	N/A

Metric Specification Description

	Metric Specification Description (cont'd)
Metric Number	The identification number assigned to the metric. All SQL Server metrics are in the range 3000 to 3999. 3001 to 3099 : Standard Metrics 3201 to 3299 : Drill Down Metrics 3700 to 3799 : UDM Metrics
Name	The name assigned to the metric. All SQL Server metrics start with MXXX, where XXX are the last 3 digits of the metric number.
Severity	The severity of the metric (Critical, Major, Minor, Warning, Normal)
Description	What the metric means.
Alarming and/or Graphing metric	Is the metric an alarming metric (A) or a graphing metric (G) or both (A & G)? (A, G, or A & G)
Collection Interval	How often the metric is collected and analyzed. (5 min, 15 min, 1 hour, 1 time daily)
Min/Max Threshold	Designates the threshold as: Minimum or Maximum, minimum thresholds are violated when the value falls below the setting; maximum thresholds are violated when the value rises above the setting.
Threshold	The default HPOM threshold (if any). (*=Threshold value is really 0, but HPOM alarms occur at <= or >= values. Since a 0 value would trigger an alarm, the threshold is set to 0.5)
Reset (value)	Does the threshold generate a message/alarm once (without reset), again when another value is detected (with reset) or when the original, exceeded threshold value continues at every collection interval (continuous)? (Without reset, With reset, Continuous)
Message Text	The messages (if any) that may be displayed for each condition.

Instruction Text	Problem-solving information. (Probable causes, Potential impact, Suggested actions, and Reports)
Report Type	If a report is available, how it is generated. (Operator, Automatic, Tool Bank, N/A) Note: All the reports that are automatic actions or operator actions are also in the Tool Bank in HPOM. However, metrics that are Graphing only metrics (no alarms, just graphs) do not have an HPOM policy for Operator or Auto actions, so they are ONLY in the Tool Bank. N/A means that no report is planned.
Area	The logical area (if any) that the metric belongs. (Database Status, Space Management, Performance, Errors, Archive/Trace, Rollback Segments, PQO (Parallel Query Option), MTS (Multi-threaded Server), MISC)

Metric M001_CacheHitPct

Metric Number	3001
Name	CacheHitPct
Severity	Warning
Description	Percentage of times a data page was found in the cache.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Minimum
Threshold	70%
Reset (value)	Reset at 80%
Message Text	DBSPI-3001.1: Cache hit percentage <i>Value</i> too low (<i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Percentage of read requests that read information from memory rather than disk. A low value for the Cache Hit Ratio is an indication of high physical reads.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>This may mean you are starting to measure I/O when the server is starting to load cache, or it may mean that cache is not of sufficient size to contain frequently used data pages. Investigate running SQL and correct if bad SQL. If inaccurate index statistics, etc. are causing excess table scans, then remedying bad SQL will improve the cache hit ratio as well as overall server performance. The server data cache size can be automatically set by SQL Server (which is the default behavior) in which case adding RAM could be the only remedy. However, this may not be the case when SQL Server is sharing its hardware with other memory-intensive OS processes, such as other server processes, not an uncommon occurrence, or if the amount of memory configured for SQL Server to use (maximum server memory) has been set (as per the recommendations for Microsoft Full-Text Search, for example). The automatic action report for this metric will show 'Least Recently Used' statistics and which users are connected to SQL Server. The operator action for the metric generates a LRUStats graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Less Recently Used Stats (LRUStats)

Metric M007_ReadsOutstdRate

Metric Number	3007
Name	ReadsOutstdRate
Severity	Warning
Description	Number of read requests issued to the operating system that have not been completed.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	2/min
Reset (value)	Without reset
Message Text	DBSPI-3007.1: Reads outstanding rate <i>Value</i> /min too high \geq <i>Threshold</i> /min).

Metric Number	3007
Instruction Text	<p>Probable Cause(s): Number of SQL Server 'read' requests to the Windows NT I/O subsystem that have not completed.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>This will help identify I/O as a bottleneck. As I/O increases, disk speed will limit performance. If this is a problem, it may be necessary to replace disks with faster ones. It may be thought that adding RAM (presumably to increase the cache hit ratio) would be more efficient than upgrading to a faster disk I/O subsystem. This can be true, but also depends on the types of queries being issued and on how much RAM is already present in the system. If the system handles mostly DSS-type queries, which need to scan large amounts of data that are typically not held in cache, then the disk subsystem's throughput speed becomes a major factor in the overall performance of the server; increasing SQL Server's cache size typically does not benefit performance that much in these situations. Also, beyond a certain point (that is, beyond a certain total amount of RAM in the system), adding more RAM does not provide as much of a benefit, because the time required to search that much cache RAM begins to approach the time required to simply read the data from disk. The break-even point, of course, depends on the relative speed of the CPU(s) in the system versus disk I/O time, but can occur at 1GB or less of total cache memory, and thus is something to be considered. To put it in simple terms, upgrading from 512MB RAM to 1GB may have much more positive effect on performance than upgrading from 2GB to 2.5GB, so if your server is already at 2GB of RAM, you may need to look at other options. Finally, another possible cause/solution to investigate here is SQL 's background maintenance operations, which can cause extra I/O to occur; these include shrinking of databases and device files, and automatic execution of UPDATE STATISTICS on tables. These may be disabled if it is determined that they are causing performance hits on a production system. The automatic action report for this metric will show 'Input/Output' statistics and which users are connected to SQL Server. The operator action for the metric generates an IOStats graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	I/O Stats

Metric M008_WritsOutstdRate

Metric Number	3008
Name	WritsOutstdRate
Severity	Warning
Description	Number of SQL Server 'write' requests to the Windows NT I/O subsystem that have not completed.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	1/min
Reset (value)	Without reset
Message Text	DBSPI-3008.1: Writes outstanding rate <i>Value</i> /min) too high (\geq <i>Threshold</i> /min).
Instruction Text	<p>Probable Cause(s): Number of SQL Server 'write' requests to the Windows OS I/O subsystem that have not completed.</p> <p>Potential Impact:</p> <p>Suggested Action(s): You can do the following:</p> <ol style="list-style-type: none"> 1 Add more RAM 2 Install a faster IO system, 3 Review the application's transaction management. <p>The automatic action report for this metric will show 'Input/Output' statistics and which users are connected to SQL Server. The operator action for the metric generates an IOStats graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	I/O Stats

Metric M009_TransactionRate

Metric Number	3009
Name	TransactionRate
Severity	Minor
Description	Number of single page writes performed per second by logging and cache flushes.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour

Metric Number	3009
Threshold	Maximum
Threshold	100/sec
Reset (value)	Continuous
Message Text	DBSPI-3009.1: Transaction rate <i>Value</i> /sec too high \geq <i>Threshold</i> /sec.
Instruction Text	<p>Probable Cause(s): Rate of transactions for the entire server. This number increases with server modification statements.</p> <p>Potential Impact:</p> <p>Suggested Action(s): As this increases, you need to determine whether you are CPU or IO bound. If you are CPU bound, add more processors. If you are IO bound, it's time to revisit the I/O subsystem or add RAM. If this corresponds with a new release, consider optimizing queries. You can consider replication (allocate data between two or more servers.) Also check to see if the procedure cache is stressed. The automatic action report for this metric shows I/O statistics and which users are connected to SQL Server. The operator action for the metric generates a Trans graph</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M209_TransactionRate

Metric Number	3209
Name	TransactionRate
Severity	Minor
Description	Database transactions rate
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Threshold	Maximum
Threshold	100/sec
Reset (value)	Continuous
Message Text	DBSPI-3009.1: Transaction rate <i>Value/sec</i> too high \geq <i>Threshold/sec</i> .
Instruction Text	<p>Probable Cause(s): Rate of transactions for each database. This number increases with server modification statements</p> <p>Potential Impact:</p> <p>Suggested Action(s): As this increases, you need to determine whether you are CPU or IO bound. If you are CPU bound, add more processors. If you are IO bound, it's time to revisit the I/O subsystem or add RAM. If this corresponds with a new release, consider optimizing queries. You can consider replication (allocate data between two or more servers.) Also check to see if the procedure cache is stressed. The automatic action report for this metric shows I/O statistics and which users are connected to SQL Server.</p>
Report Type	Automatic.
Area	Database

Metric M011_UserConnectPct

Metric Number	3011
Name	UserConnectPct
Severity	Major Critical
Description	Percentage of the current user connections to the total number of user connections configured for SQL Server.
Alarming and/or Graphing metric	A & G
Collection Interval	5 min
Min/Max Threshold	Maximum

Metric Number	3011
Threshold	90% 98%
Reset (value)	Without reset
Message Text	DBSPI-3011.1: % of current users connected <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): The number of current user connections to the total number of user connections configured for SQL Server.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>DBA should set a 'max' threshold for this metric based on a number of user connections that is normally not exceeded, so any 'connection leaks' in applications can be found before they begin to affect server performance. This metric determines open connections, not ones that are working (processing queries, DML, etc.). See metric 3026 for percentage of connections that are active. The automatic action report for this metric will show the maximum number of user connections allowed and which users are connected to SQL Server. The operator action for the metric generates a Users graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Process

Metric M013_LocksInUsePct

Metric Number	3013
Name	LocksInUsePct
Severity	Major
Description	Percentage total locks currently held to the total number of locks configured for SQL Server.
Alarming and/or Graphing metric	A & G
Collection Interval	5 min
Min/Max Threshold	Maximum
Threshold	80%
Reset (value)	70%
Message Text	DBSPI-3013.1: % locks in use <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Percentage total locks currently held to the total number of locks configured for SQL Server.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>MS SQL Server 7.0:</p> <p>The number of locks configured is fixed at server start-up. When the number of locks is met, other processes requesting locks abort, and new users cannot connect. You should evaluate why this is occurring, then increase number of available locks (sp_configure 'locks') and reboot server for change to take effect. Note: this uses memory. The automatic action report for this metric will show all outstanding locks and which users are connected to SQL Server. The operator action for the metric generates a Locks graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M014_BlckdProcessCnt

Metric Number	3014
Name	BlckdProcessCnt
Severity	Warning
Description	Number of blocked processes
Alarming and/or Graphing metric	A & G
Collection Interval	5 min

Metric Number	3014
Min/Max Threshold	Maximum
Threshold	3 for 1 min
Reset (value)	Without reset
Message Text	DBSPI-3014.1: # of blocked processes <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of blocked processes in the server greater than the threshold for more than one collection interval (usually 5 minutes). Potential impact is performance since blocked processes will wait until block is cleared.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>Blocked processes are an indication of contention, which occurs frequently in OLTP and mixed use systems. Action depends on the situation. You may need to restructure indexes; or reschedule load processes when readers are not running, or change page lock promotion thresholds. It is also an indication of a poorly designed application process. The automatic action report for this metric will show processes that are the source of interlocking and which users are connected to SQL Server. The operator action for the metric generates a Server graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M215_VirtDevSpUsdPct

Metric Number	3215
Name	VirtDevSpUsdPct
Severity	Minor Major Critical
Description	Percentage of space used on a specific virtual device. Allocated storage is approaching total storage.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Threshold	Maximum
Threshold	90% 95% 99%
Reset (value)	Without reset
Message Text	DBSPI-3215.1: Percentage of space used <i>Value</i> on virtual device <i><virtual_device></i> too high <i>>=Threshold</i> .

Metric Number	3215
Instruction Text	<p>Probable Cause(s): Allocated storage is approaching total storage with the potential impact the inability to extend databases.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>If you are approaching the device size limit, reevaluate your initial space estimation. If you have less space, allocate more disk. Otherwise, analyze why the disk filled up unexpectedly. Autogrow is a useful feature that prevents databases from stopping dead in their tracks when the device is used up. However, most administrators will prefer a certain level of control in being able to plan for a database's next level of growth rather than letting SQL Server 'just do it.' In other words, as a DBA, when databases are going to allocate their own resources (i.e., take new disk space), you need to know about it. Besides, if the autogrow settings are becoming inadequate (causing the database to autogrow more and more often), if database usage is expected to change, or if remaining disk space changes, this alarm allows an administrator to act. For instance, if the database is about to autogrow and completely fill up a disk drive, it might be more efficient to plan on creating new file devices on which to store the database. You should always plan database systems and their device usages based on the amount of data being stored and the amount of load expected for the database, in order to plan its size and expected growth. In other words, growth should be a planned event. Since there is always the unexpected to be dealt with, autogrow becomes a great assist in preventing a potential problem (the database stopping). However, it is possible that a database can grow so fast that the log will autogrow before anyone intended it to happen. This could be the result of just an unexpected increase in usage of the database; or, it could be someone running a query that has gotten out of control (e.g., a bad ad-hoc query). In the worst case, this could cause autogrow to execute not once but repeatedly until the disk fills up. Another potential problem is that if device files get grown and shrunk many times, disk fragmentation can result, thereby slowing performance, so this is another argument in favor of preallocating databases to the desired size once, so that autogrow is only triggered rarely, if at all. So, if using autogrow on a database, this metric becomes one that would not necessarily trigger a major alarm, but would still be one you'd want to be informed of so you can keep an eye on it. The automatic action report for this metric will show all virtual devices assigned to each database and the percentage of space used.</p>
Report Type	Automatic and tool bank.
Area	Space

Metric M216_TransLogUsedPct

Metric Number	3216
Name	TransLogUsedPct
Severity	Minor Major Critical
Description	Percentage of transaction log space used for each database. Percentage of space used in database transaction log to the total log size. At 100%, all transaction processing will abort or suspend, depending on database settings.
Alarming and/or Graphing metric	A
Collection Interval	15 min
Threshold	Maximum
Threshold	80% 90% 99%
Reset (value)	Without reset
Message Text	DBSPI-3216.1: Percentage of transaction log space used (<i>Value</i>) in database <i><database_name></i> too high \geq <i>Threshold</i> .

Metric Number	3216
Instruction Text	<p>Probable Cause(s): Percentage of space used in database transaction log to the total log size. At 100%, all transaction processing will abort or suspend, depending on database settings.</p> <p>Suggested Action: You need to periodically dump (truncate) the transaction log. If you do not, the log will grow unchecked until it fills up. You can either turn on the database option (using sp_dboption) 'trunc. log on chkpt.', which is NOT recommended on a production machine, or you can dump the transaction log, which cleans out all completed transaction. You should automate cleaning out the transaction log on a periodic basis, before the threshold is reached. If you are cleaning out the transaction log, but it is not getting any smaller, you have a long-running transaction which is not complete, or you may have an aborted transaction in the database which has not been marked as complete in the log. As a last resort, you can shut down and restart the server. This will mark the incomplete transaction as complete (and rolled back). Autogrow is a useful feature that prevents databases from stopping dead in their tracks when the logfile is used up. However, most administrators will prefer a certain level of control in being able to plan for a database's next level of growth rather than letting SQL Server 'just do it.' In other words, as a DBA, when databases are going to allocate their own resources (i.e., take new log space), you need to know about it. Besides, if the autogrow settings are becoming inadequate (causing the database to autogrow more and more often), if database usage is expected to change, or if remaining disk space changes, this alarm allows an administrator to act. For instance, if the database is about to autogrow and completely fill up a disk drive, it might be more efficient to plan on creating new file devices on which to store the database. You should always plan database systems and their device usages based on the amount of data being stored and the amount of load expected for the database, in order to plan its size and expected growth. In other words, growth should be a planned event. Since there is always the unexpected to be dealt with, autogrow becomes a great assist in preventing a potential problem (the database stopping). However, it is possible that a database can grow so fast that the log will autogrow before anyone intended it to happen. In the worst case, this could cause autogrow to execute not once but repeatedly until the disk fills up. So, if using autogrow on a database, this metric becomes one that would not necessarily trigger a major alarm, but would still be one you'd want to be informed of so you can keep an eye on it. The automatic action report for this metric shows log space in MB and percent used per database and other database statistics via sp_helpdb.</p>

Metric Number	3216
Instruction Text (contd.)	<p>Use this option only on databases for which transaction log dumps are not being saved (typically development systems or systems where only full database dumps, and not DUMP TRANSACTION, will be used). If you are in a production environment and using DUMP TRANSACTION to truncate the log, time the statements close enough together so that no process ever receives the 1105 error (which indicates that the log is full). When you execute a DUMP TRANSACTION statement, transactions completed prior to the earliest outstanding transaction or the earliest transaction marked for replication but not yet moved to the distribution database are truncated from the log, unless they are on the same log page as the last outstanding transaction. All transactions since the earliest outstanding transaction are considered active and are not truncated, even if they have completed. Because the DUMP TRANSACTION statement truncates only the inactive portion of the log, you should be careful not to allow stranded (uncommitted) transactions to remain in the log for a long time. For example: if a user issues a BEGIN TRANSACTION statement but never commits the transaction. Nothing logged after the BEGIN TRANSACTION can be purged out of the log until one of the following events occurs:</p> <ul style="list-style-type: none"> * The user who began the transaction completes it. * The user process that issued the BEGIN TRANSACTION statement is forcibly stopped and the transaction is rolled back. * SQL Server is shut down and restarted Stranded transactions are usually due to application problems. <p>So, if you are cleaning out the transaction log, but it is not getting any smaller, you have a long-running transaction which is not complete, or you may have an aborted transaction in the database which has not been marked as complete in the log. As a last resort, you can shut down and restart the server. This will mark the incomplete transaction as complete (and rolled back).</p> <p>The automatic action report for this metric shows log space in MB and percent used per database and other database statistics via sp_helpdb.</p>
Report Type	Auto
Area	Space

Metric M017_CmdQueueLenPct

Metric Number	3017
Name	CmdQueueLenPct
Severity	Warning
Description	Percentage of command queue length used
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour ^c
Min/Max Threshold	Maximum
Threshold	10%
Reset (value)	Without reset
Message Text	DBSPI-3017.1: % of command queue length used <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): When SQL Server does not have a worker thread immediately available to execute a command, it place this command into Command Queue. Value of this metric running above 0 indicates that the number of user connection exceeds the max number of worker threads so that the SQL Server activated its thread pooling mechanism. Too much of thread swapping may negatively affect SQL Server performance.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Consider increasing the number of available worker threads via 'max worker threads' configuration parameter and increase memory allocated to SQL Server. However, you may wish to restrict user connections via 'user connections' configuration parameter in order to decrease the workload on the SQL Server. User connections and worker threads are counted as overhead against the SQL Server memory allocation. Thus, plan accordingly when adjusting these values. The automatic action report for this metric shows network statistics and the maximum configured worker threads. The operator action for the metric generates a Server graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M218_DBSpaceUsedPct

Metric Number	3218
Name	DBSpaceUsedPct
Severity	Critical
Description	Percentage database space used

Metric Number	3218
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	95%
Reset (value)	Without reset
Message Text	DBSPI-3218.1: % database space used <i>Value</i> in database <i><database_name></i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Percentage of space used in a database to the total database size. Database is getting filled up.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Use ALTER DATABASE to increase the size of the data segment. Drop objects from the database. Delete rows from tables in the database. The most natural action is, obviously, to add space to the database by executing ALTER DATABASE command. If there is no free space available on the existing database devices, a new device has to be created by DISK INIT command, or an existing device has to be extended by executing DISK RESIZE command. The automatic action report for this metric shows other database statistics via sp_helpdb.</p>
Report Type	Automatic and tool bank.
Area	Space

Metric M022_BufChainAvgLen

Metric Number	3022														
Name	BufChainAvgLen														
Severity	Warning														
Description	Buffer chain average length.														
Alarming and/or Graphing metric	A & G														
Collection Interval	1 hour														
Min/Max Threshold	Maximum														
Threshold	4														
Reset (value)	Without reset														
Message Text	DBSPI-3022.1: Buffer chain average length <i>Value</i> too high (\geq <i>Threshold</i>).														
Instruction Text	<p>Probable Cause(s): HASH BUCKETS are an array of pointers to linked lists of buffers pointing to pages in cache. Each page in cache has a structure used to manage it known as a 'buffer.' 'HASH BUCKETS' is configurable from 4999 to 265003 and is the actual number of entries. If chains of buffers become too long, then performance can suffer.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Below is a table of suggested values for HASH BUCKETS based on the SP_CONFIGURE MEMORY configuration value. These values are rough suggestions, and this metric should be used to make sure your system is configured correctly.</p> <table border="0"> <thead> <tr> <th>MEMORY</th> <th>HASH BUCKETS</th> </tr> </thead> <tbody> <tr> <td>=====</td> <td>=====</td> </tr> <tr> <td>25600</td> <td>8192</td> </tr> <tr> <td>51200</td> <td>15000</td> </tr> <tr> <td>102400</td> <td>25000</td> </tr> <tr> <td>204800</td> <td>40000</td> </tr> <tr> <td>409600</td> <td>75000</td> </tr> </tbody> </table> <p>Note that the actual runtime value will be the nearest prime number to the configured value. The automatic action report for this metric will show buffer chain information and which users are connected to SQL Server. The operator action for the metric generates a Cache graph</p>	MEMORY	HASH BUCKETS	=====	=====	25600	8192	51200	15000	102400	25000	204800	40000	409600	75000
MEMORY	HASH BUCKETS														
=====	=====														
25600	8192														
51200	15000														
102400	25000														
204800	40000														
409600	75000														
Report Type	Automatic, operator initiated, and tool bank.														
Area	Cache														

Metric M023_ReadWriteErrCnt

Metric Number	3023
Name	ReadWriteErrCnt
Severity	Warning
Description	Number of SQL Server read/write errors since the last probing.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Without reset
Message Text	DBSPI-3023.1: # of SQL Server read/write errors since the last probing <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	Probable Cause(s): This metric represents the number of disk I/O errors encountered by SQL Server since the last probing. Disk I/O failure. Potential Impact: Suggested Action(s): If persistent, disk hardware has to be examined. The automatic action report for this metric shows SQL Server information via the 'sp_monitor' command. The operator action for the metric generates a Error graph
Report Type	Automatic, operator initiated, and tool bank.
Area	Error



To generate reports for the metric M023, the user must have administrator privileges.

Metric M024_PacketErrorCnt

Metric Number	3024
Name	PacketErrorCnt
Severity	Warning
Description	Number of packet errors while reading or writing packets.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Without reset
Message Text	DBSPI-3024.1: <i>Value</i> packet errors while reading or writing packets.
Instruction Text	Probable Cause(s): This metric shows the number of network errors encountered by SQL Server since the last reading. This metric allows a DBA to monitor current user activity for SELECT queries. Potential Impact: Suggested Action(s): The automatic action report for this metric shows SQL Server information via the 'sp_monitor' command. The operator action for the metric generates a Error graph.
Report Type	Automatic, operator initiated, and tool bank.
Area	Error



To generate reports for the metric M024, the user must have administrator privileges.

Metric M025_CPUUsedPct

Metric Number	3025
Name	CPUUsedPct
Severity	Warning
Description	Percentage CPU time used by SQL Server. The percentage reported is the number of seconds of CPU time used by SQL Server in ratio to the total amount of elapsed time since the last probing. This percentage is aggregated for all CPUs in the system.
Alarming and/or Graphing metric	A & G
Collection Interval	5 min
Min/Max Threshold	Maximum
Threshold	95% for 15 min
Reset (value)	Without reset
Message Text	DBSPI-3025.1: % CPU time used by SQL Server <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): The percentage reported is the number of seconds of CPU time used by SQL Server in ratio to the total amount of elapsed time since the last probing.</p> <p>SQL Server CPU load running at 100% indicates a problem. Either SQL Server has excessive load or a thread is in the endless CPU loop. This percentage is aggregated for all CPUs in the system.</p> <p>Potential Impact:</p> <p>Suggested Action(s): For Excessive load: Add CPUs to the server. For Runaway process: Detect a thread causing a CPU loop and use the KILL command to kill it. If it does not help--restart SQL Server. The automatic action report for this metric shows SQL Server information via the 'sp_monitor' command and which users are connected to SQL Server. The operator action for the metric generates a Server graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M026_ActiveConntnPct

Metric Number	3026
Name	ActiveConntnPct
Severity	Warning
Description	Server percentage of total connections that are active versus sleeping. The number of current active connections as a percentage of total connections.

Metric Number	3026
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Minimum
Threshold	20%
Reset (value)	Without reset
Message Text	DBSPI-3026.1: % of total connections that are active versus sleeping <i>Value</i> too low (\leq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): The number of current active connection as a percent of total connections. If this metric's value is consistently low, SQL Server resources may be tied up by a large number of idle, 'sleeping' connections.</p> <p>Potential Impact:</p> <p>Suggested Action(s):</p> <p>If this metric is consistently low, you may want to adjust your 'front end' applications so that they do not keep idle connections for too long. Example: MSAccess keeps idle connections for 10 minutes by default. This value may be adjusted to 5 or 3 minutes. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Users graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M227 PhysIOByUsrPct

Metric Number	3227
Name	PhysIOByUsrPct
Severity	Warning
Description	Percentage of physical I/O used by process. Number of cumulative physical reads and writes by a process as a percentage of all physical reads and writes performed by all the SQL Server users.
Alarming and/or Graphing metric	A
Collection Interval	5 min
Min/Max Threshold	Maximum
Threshold	95% for 10 minutes.
Reset (value)	Without reset
Message Text	DBSPI-3227.1: % of physical I/O used by process (<i>process_id</i>). (<i>Value</i>) too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): This metric excludes SQLAgent processes. Number of cumulative physical reads and writes by a process as a percentage of all physical reads and writes performed by all the SQL Server users. If a process performs heavy I/O activities then this may cause performance problems for other users trying to run their queries.</p> <p>Potential Impact:</p> <p>Suggested Action(s): If this situation causes significant performance degradation then that process connection should be closed. The automatic action report for this metric shows which users are connected to SQL Server</p>
Report Type	Automatic and tool bank.
Area	Server

Metric M028_SuspectDBCnt

Metric Number	3028
Name	SuspectDBCnt
Severity	Critical
Description	Number of databases marked as suspect. If SQL Server cannot access a database device or recover a database at startup, it marks this database as 'suspect'. The 'suspect' status prevents users from accessing the database.
Alarming and/or Graphing metric	A & G

Metric Number	3028
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Without reset
Message Text	DBSPI-3028.1: <i>Value</i> databases marked as suspect.
Instruction Text	<p>Probable Cause(s): If SQL Server cannot access a database device or recover a database at startup, it marks this database as 'suspect'. The 'suspect' status prevents users from accessing the database. One or more databases on SQL Server have been marked as 'suspect'.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Use the sp_resetstatus stored procedure to turn off the suspect flag on a database leaving all other database options intact. Caution: Use sp_resetstatus only when directed by your primary support provider or this manual. Otherwise, you might damage your database. If the suspect database is damaged and cannot be recovered, remove the database using DBCC DBREPAIR: dbcc dbrepair(database_name,dropdb) The automatic action report for this metric shows other database statistics via sp_helpdb. The operator action for the metric generates a Error graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Error

Metric M030_ServerConnect

Metric Number	3030
Name	ServerConnect
Severity	Critical
Description	Ability to connect to a server
Alarming and/or Graphing metric	A
Collection Interval	5 minute
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Without reset
Message Text	DBSPI-3030.1: Cannot connect to MS SQL Server <\$OPTION(dbserv)>.
Instruction Text	<p>Probable Cause(s): DB SPI failed to connect to the master database of a MS SQL Server instance. This error will prevent other metrics from running. This could be caused by any of the following:</p> <ul style="list-style-type: none"> * Incorrect information in the DB SPI configuration * The user id or password that is used to connect has changed * The server is not running * The transaction log for the tempdb is full, so DB SPI cannot build temporary tables <p>Potential Impact:</p> <p>Suggested Action(s):</p> <ul style="list-style-type: none"> * If the server is just busy and the connection attempt is timing out, you can use a variable MSSQL_LOGINTIME in the dbspi defaults file (please see Appendix A of the Database SPI Configuration Guide for details about the defaults file). After you add 'MSSQL_LOGINTIME ON', the following command is run: EXEC SQL SET OPTION LOGINTIME 30 or * If the server is actually down, use the server name in the message to determine which server connection is failing. Verify that the server is running. Try to connect to the server and the master database using the configured user and password. Check the transaction log for tempdb. An automatic action report shows the configured number of open databases allowed among all users and which users are connected to SQL Server.
Report Type	N/A
Area	Server

Metric M230_DBConnect

Metric Number	3230
Name	DBConnect
Severity	Warning
Description	Ability to connect to a database.
Alarming and/or Graphing metric	A
Collection Interval	15 min
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Continuous
Message Text	DBSPI-3230.1: Cannot connect to database (<i>database_name</i>).
Instruction Text	Probable Cause(s): Unable to connect to database. The database may be corrupt, or the 'single user' database option may be turned on. Potential Impact: Suggested Action(s): Check database configuration options using sp_helpdb, and, reconfigure if that's the problem. If the database is corrupt, reload the database from a backup. The automatic action report for this metric shows other database statistics via sp_helpdb.
Report Type	Automatic and tool bank.
Area	Database

Metric M032_RunableContnPct

Metric Number	3032
Name	RunableContnPct
Severity	Warning
Description	The number of current runnable connections as a percentage of total connections.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	50%

Metric Number	3032
Reset (value)	Without reset
Message Text	DBSPI-3032.1: % of total connections that are runnable <value>% too high (>=<threshold>%).
Instruction Text	<p>Probable Cause(s): The number of current runnable connections as a percent of total connections. If the percentage of runnable connections is too high, then it means that there is too much contention for MS SQL Server resources and the overall performance of the system is negatively impacted.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Analyze the applications that are running by looking at the automatic action report and determine if the application needs to be corrected. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Users graph.</p>
Report Type	Automatic and operator initiated.
Area	Server

Metric M233_DatabaseBackup

Metric Number	3233
Name	DatabaseBackup
Severity	Major Minor Warning
Description	# of hours since last database backup.
Alarming and/or Graphing metric	A
Collection Interval	1 day
Min/Max Threshold	Maximum
Threshold	Condition 3233.1: 876000 (hours) Condition 3233.2: 168 (hours) Condition 3233.1: 72 (hours)
Reset (value)	Continuous
Message Text	DBSPI-3233.1: Database <\$OPTION(database_name)> has not been backup up for <\$VALUE> hours (>=<\$THRESHOLD> hours) for <\$OPTION(dbserv)>.
Instruction Text	Probable Cause(s): Database backup has not been done and it has exceeded the threshold time of backup. Potential Impact: Suggested Action(s): Perform a complete database backup on the indicated database.
Report Type	N/A
Area	Backup

Metric M234_TransactionLogBackup

Metric Number	3234
Name	TransLogBackup
Severity	Major Minor Warning
Description	# of hours since last database transaction log backup
Alarming and/or Graphing metric	A
Collection Interval	1 day

Metric Number	3234
Min/Max Threshold	Max
Threshold	Condition 3233.1: 876000 (hours) Condition 3233.2: 48 (hours) Condition 3233.1: 24 (hours)
Reset (value)	Continuous
Message Text	DBSPI-3234.2: The transaction log for database <\$OPTION(database_name)> has not been backup up for <\$VALUE> hours (>=<\$THRESHOLD> hours) for <\$OPTION(dbserve)>.
Instruction Text	Probable Cause(s): Database Transaction Log backup has exceeded the threshold. The Transaction log for the indicated database does not have the 'Truncate on checkpoint' option set and has exceeded the backup threshold. Potential Impact: Suggested Action(s): Perform a backup of the Transaction Log for the indicated database.
Report Type	N/A
Area	Backup

Metric M035_LongTransaction

Metric Number	3035
Name	LongTransaction
Severity	Major
Description	Longest running transaction. This metric will alarm if the longest running transaction has been running longer than the threshold (in seconds). The message text identifies the longest running transaction.
Alarming and/or Graphing metric	A
Collection Interval	5 min
Min/Max Threshold	Max
Threshold	60
Reset (value)	Without reset
Message Text	DBSPI-3032.1: % of total connections that are runnable <value>% too high (>=<threshold>%).

Metric Number	3035
Instruction Text	<p>Probable Cause(s): This metric will alarm if the longest running transaction has been running longer than the threshold (in seconds). The message text will identify the longest running transaction.</p> <p>There can be a variety of reasons for transactions taking a long time to execute, one of the most common reasons is blocking. Blocking occurs when one process (identified by SPID) holds a lock on a specific resource that a second process attempts to acquire, causing a conflicting lock type on the same resource.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Using the SPID in the message, follow the steps below to gather information about the process/transaction:</p> <ol style="list-style-type: none"> 1. Identify the SPID at the head of the blocking chain. Use the SQL Enterprise Manager as follows: <ol style="list-style-type: none"> a. Expand the server group; then expand the server. b. Expand 'Management'; then expand 'Current Activity' c. Expand 'Locks/Process ID.' In the details pane, the SPIDs, along with their blocking information, are displayed. The SPIDs that are blocking others will appear as '(Blocking).' <p>Note, however, that it is sometimes necessary to use direct queries instead of Enterprise Manager, because some types of tempdb blocking problems may prevent you from running queries through Enterprise Manager, which uses temporary table operations. Using direct queries gives you the control necessary to avoid this problem.</p> 2. Find the query that the blocking SPID is running. Use the following command to determine the command issued by a particular SPID: DBCC INPUTBUFFER(<spid>) <p>Alternately, you can use SQL Enterprise Manager as follows:</p> <ol style="list-style-type: none"> a. Expand the server group; then expand the server. b. Expand 'Management'; then expand 'Current Activity'. c. Click 'Process Info.' The SPIDs are displayed in the details pane. d. Double-click the SPID to see the last Transact-SQL command the SPID executed.

Metric Number	3035
Instruction Text (contd.)	<p>3. Find the type of locks the SPID is holding. You can determine this information by executing the sp_lock system stored procedure. Alternatively you can use Enterprise Manager as follows:</p> <ul style="list-style-type: none"> * Expand the server group; then expand the server. * Expand 'Management'; then expand 'Current Activity'. * Expand 'Locks/Process ID.' In the details pane, the SPIDs, along with the information on the locks they are holding, are displayed. <p>4. Find the transaction nesting level and process status of the blocking SPID. The transaction nesting level of a SPID is available in the @@TRANCOUNT global variable. However, it can be determined from outside the SPID by querying the sysprocesses table as follows:</p> <pre>select open_tran from sysprocesses where spid=<blocking spid number></pre> <p>The value returned is the @@TRANCOUNT value for the SPID. This value shows the transaction nesting level for the blocking SPID, which in turn can explain why it is holding locks. For example, if the value is greater than zero, the SPID is in the midst of a transaction (in which case it is expected to retain certain locks it has acquired, depending on the transaction isolation level).</p>
Report Type	N/A
Area	Databases



Microsoft SQL Server metric 3035 needs 'DBCC opentran' privilege to run.

Metric M051_FullScansRate

Metric Number	3051
Name	FullScansRate
Severity	Minor
Description	Number of unrestricted full scans per second. These can be either base-table or full-index scans
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	20/sec
Reset (value)	Continuous
Message Group	MSQL_Perf
Message Text	DBSPI-3051.1: Full scan rate <i>Value</i> /sec too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of unrestricted full scans per second. These can be either base-table or full-index scans Full Scans occur when there are no restrictions placed on queries, or when the optimizer determines that a table scan is the most efficient way to this can be a heavy performance drain. However there may be also be many small tables that don't have indexes at all. NOTE - A high scans rate does not necessarily indicate a big performance problem, since small table scans may account for most of the scans being performed. However, this metric can still be useful as an overall indicator of either an increased level of activity in the database, or a change in the types of users or the way they are using the database. So it can indicate that things are out of the ordinary with respect to the type or amount of activity going on. Also, this metric coupled with other such as #3007 (Reads Outstanding) may indicate that too many table scans on large tables are being performed, which warrants further investigation.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Find the queries or procedures that are causing the unrestricted scans. And/or build new indexes and update statistics. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates an Access graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Access Methods

Metric M052_IndxSearchsRate

Metric Number	3052
Name	IndxSearchsRate
Severity	Minor
Description	Number of index searches per second. These are used to start range scans and single index record fetches and to reposition an index.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	1000/sec
Reset (value)	Continuous
Message Text	DBSPI-3052.1: Index searches rate <i>Value</i> /sec too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of index searches per second. These are used to start range scans and single index record fetches and to reposition an index. In general the number of Index is recommended to be high. This means that more searches are being performed through the use of indexes rather than full scans. This is preferable. However on large databases where the data is constantly changing, this value may starts to decrease and the full scan value may starts to increase.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Update the statistics for the affected tables. Use Enterprise Manager to reschedule when statistics samples are updated. They may not be occurring frequently enough, or they may not be scheduled at all. In this case set 'auto update statistics' database option on all your databases. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates an Access graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Access Methods

Metric M053_PgesAlloctdRate

Metric Number	3053
Name	PgesAlloctdRate
Severity	Minor
Description	Number of pages allocated per second to database objects used for storing index or data records.

Metric Number	3053
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	1000/sec
Reset (value)	Continuous
Message Text	DBSPI-3053.1: Pages allocated rate <i>Value</i> /sec too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of pages allocated per second to database objects used for storing index or data records. A large amount of data is being added to the database, or data is being moved in an unfortunate manner causing page splitting. The relationship between this metric and #3054 (Extents allocated rate) can be informative. If existing tables are growing, then 8 pages will tend to be allocated for each extent allocated. On the other hand, if smaller tables are being created, only one or two pages may be allocated for each extent allocated. So an increase in one or both of these metrics can indicate a change in the type of activity being performed on a database.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This may be normal, but watch the trends here, as it will help you determine how busy your I/O subsystem is. Query optimization probably would not help much here, unless the problem is that temp tables are being created unnecessarily. Applying a fill factor to tables might help in the short term, if pages are being allocated due to page splits. Unfortunately, there is no known method of accurately tracking page splitting, short of analyzing the entire transaction log. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates an Access graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Access Methods

Metric M054_ExtntsAllocRate

Metric Number	3054
Name	ExtntsAllocRate
Severity	Minor
Description	Number of extents allocated per second to database objects used for storing index or data records
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	300/sec
Reset (value)	Continuous
Message Text	DBSPI-3054.1: Extents allocated rate <i>Value</i> /sec too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of extents allocated per second to database objects used for storing index or data records This should be an indication of table creation such as the creation of temporary tables. If many new rows are added to indexed database tables. The index may have more than a usual rate of Extents allocated. The relationship between this metric and #3053 (Pages allocated rate) can be informative. If existing tables are growing, then 8 pages will tend to be allocated for each extent allocated. On the other hand, if smaller tables are being created, only one or two pages may be allocated for each extent allocated. So an increase in one or both of these metrics can indicate a change in the type of activity being performed on a database.</p> <p>Potential Impact:</p> <p>Suggested Action(s): If this is an indexing problem and a regular one, the addition of new index pages may be reduced by implementing a fill factor of the indexes. If the problem is frequent and related to the creation of tables, an alternative to using temporary tables may need to be found in SQL. - Query optimization and using fill factor is one suggestion. However, query optimization might not help much here, unless the problem is that temp tables are being created unnecessarily. Applying a fill factor to tables might help in the short term, if pages are being allocated due to page splits. Unfortunately, there is no known method of accurately tracking page splitting, short of analyzing the entire transaction log. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates an Access graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Access Methods

Metric M055_PageSplitsRates

Metric Number	3055
Name	PageSplitsRates
Severity	Minor
Description	Number of page splits per second that occur as the result of overflowing index pages.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	1000/sec
Reset (value)	Without reset
Message Text	DBSPI-3055.1: Page splits rate <i>Value/sec</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of page splits per second that occur as the result of overflowing index pages. Heavy table inserts or updates that change the positions of rows. If the index pages are full, they will need to be split which produces excessive IO.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Use fillfactors on the indexes to decrease the number of Page Splits, periodically rebuild indexes to enforce the fillfactors. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates an Access graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Access Methods

Metric M056_TblLckEscalRate

Metric Number	3056
Name	TblLckEscalRate
Severity	Minor
Description	Number of times locks on a table were escalated.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum

Metric Number	3056
Threshold	0.5
Reset (value)	Continuous
Message Text	DBSPI-3056.1: Table lock escalation rate <i>Value/sec</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): Number of times locks on a table were escalated Large numbers of locks being placed by a process on a table. According to Microsoft, 'Lock escalation is the process of converting many fine-grain locks into fewer coarse-grain locks, reducing system overhead. Microsoft? SQL Server? automatically escalates row locks and page locks into table locks when a transaction exceeds its escalation threshold ?thresholds are determined dynamically by SQL Server and require no configuration.' While this is true, the major problem to be addressed is not when the table escalations occur, but that they occur at all. In other words, even if you could alter the lock escalation threshold, it would be addressing the symptoms, not the cause. Increased table locks may lead to increased blocking and/or deadlocks.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Analyze and tune queries, run UPDATE STATISTICS, make sure you have useful indexes on the table. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates an Access graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Access Methods

Metric M057_ServiceMon

Metric Number	3057
Name	ServiceMon
Severity	Critical Minor Warning
Description	Monitors SQL Server Service (M057_ServiceMon). This metric checks the status of SQL Server service.
Alarming and/or Graphing metric	A
Collection Interval	5 min
Min/Max Threshold	Maximum
Threshold	4.5 2.5 0.5
Reset (value)	Without reset
Message Text	DBSPI-3057.1: Service <MSG_OBJECT> is having Status= <OPTION(Status)>
Instruction Text	<p>Probable Cause(s): SQL Server service is not running. It can be in any of the following states: SERVICE_START_PENDING, SERVICE_CONTINUE_PENDING, SERVICE_PAUSE_PENDING, SERVICE_STOP_PENDING, SERVICE_PAUSED or SERVICE_STOPPED,ERROR</p> <p>Potential Impact: Applications, which are trying to connect to the SQL Server, will fail.</p> <p>Suggested Action(s): Verify that the SQL Server service is running. From Administrative Tools -> Services, verify that the status of the particular SQL Server service is Started. If it is not, right-click the service and then click Start or Resume, as appropriate.</p>
Report Type	N/A
Area	Server

Metric M058_ServiceMon

Metric Number	3058
Name	ServiceMon
Severity	Critical Minor Warning
Description	Monitors SQL Agent Service (M058_ServiceMon). This metric check the status of the SQL Agent service.
Alarming and/or Graphing metric	A
Collection Interval	5 min
Min/Max Threshold	Maximum
Threshold	4.5 2.5 0.5
Reset (value)	Without reset
Message Text	DBSPI-3058.1: Service <MSG_OBJECT> is having Status= <OPTION(Status)>
Instruction Text	<p>Probable Cause(s): The SQL Server Agent service is not running. It can be in any of the following states: SERVICE_START_PENDING, SERVICE_CONTINUE_PENDING, SERVICE_PAUSE_PENDING, SERVICE_STOP_PENDING, SERVICE_PAUSED or SERVICE_STOPPED,ERROR</p> <p>Potential Impact: The SQL Server actions (mostly scheduled), which depend on the SQL agent, will fail.</p> <p>Suggested Action(s): Verify that the SQL Agent service is running. From Administrative Tools -> Services, verify that the status of the particular SQL Agent service is Started. If it is not, right-click the service and then click Start or Resume, as appropriate.</p>
Report Type	N/A
Area	Server

Metric M064_DBAktivTransCnt

Metric Number	3064
Name	DBAktivTransCnt
Severity	Warning
Description	Number of active transactions for the entire server.

Metric Number	3064
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	5
Reset (value)	Without reset
Message Text	DBSPI-3064.1: # of active transactions for the entire server <Value> too high (>=Threshold).
Instruction Text	<p>Probable Cause(s): Increased server workload.</p> <p>Potential Impact:</p> <p>Suggested Action(s): If the server slows down: optimize queries, upgrade server hardware, or migrate part of the data to a separate server.</p> <p>An automatic action report shows which users are connected to SQL Server. The operator action generates a Server graph.</p>
Report Type	Auto
Area	Server

Metric M264_DBActivTransCnt

Metric Number	3264
Name	DBActivTransCnt
Severity	Warning
Description	Number of active transactions for each database in the server.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	5
Reset (value)	Without reset
Message Text	DBSPI-3264.1: # of active transactions for the database (<i>database_name</i>) Value too high (\geq Threshold).
Instruction Text	<p>Probable Cause(s): Number of active transactions for each database in the server has increased.</p> <p>Potential Impact:</p> <p>Suggested Action(s): If the server slows down: optimize queries, upgrade server hardware or migrate part of the data to a separate server.</p> <p>The automatic action report for this metric shows active transactions by database and which users are connected to SQL Server.</p>
Report Type	Automatic.
Area	Databases

Metric M066_DBLogGrowthsCnt

Metric Number	3066
Name	DBLogGrowthsCnt
Severity	Major
Description	# of transaction log expansions for server
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	4

Metric Number	3066
Reset (value)	Continuous
Message Text	DBSPI-3066.1: # of transaction log expansions for the entire server <i>Value too high (>=Threshold).</i>
Instruction Text	<p>Probable Cause(s): Number of times the transaction log has been expanded for the entire server. SQL Server has run out of space for the transaction log and expanded it, or a system administrator has expanded the log to provide more space.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This depends on whether expansion is a desirable event. If the expansion is because of increased activity on the database, they will continue. The changes may be kept or the frequency of backup tran commands may need to be increased. If the changes are due to a single unique event, an administrator may consider truncating the log and shrinking it back to its original size. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Trans graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M266_DBLogGrowthsCnt

Metric Number	3266
Name	DBLogGrowthsCnt
Severity	Major
Description	Number of times the transaction log for each database has been expanded.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	4
Reset (value)	Continuous
Message Text	DBSPI-3266.1: # of transaction log expansions for (<i>database_name</i>) <i>Value</i> too high (\geq <i>Threshold</i>) for <\$OPTION(dbserve)>.
Instruction Text	<p>Probable Cause(s): Number of times the transaction log for each database has been expanded. SQL Server has run out of space for the transaction log and expanded it. Or a system administrator has expanded the log to provide more space</p> <p>Potential Impact:</p> <p>Suggested Action(s): This depends on whether expansion is a desirable event. If the expansion is because of increased activity on the database, they will continue. The changes may be kept or the frequency of backup tran commands may need to be increased. If the changes are due to a single unique event, an administrator may consider truncating the log and shrinking back to its original size. The automatic action report for this metric shows which users are connected to SQL Server.</p>
Report Type	Automatic
Area	Databases

Metric M067_DBLogShrinksCnt

Metric Number	3067
Name	DBLogShrinksCnt
Severity	Major
Description	# of server transaction log shrinks for server
Alarming and/or Graphing metric	A
Collection Interval	1 hour

Metric Number	3067
Min/Max Threshold	Maximum
Threshold	4
Reset (value)	Continuous
Message Text	DBSPI-3067.1: # of transaction log shrinks for the entire server (<\$VALUE>) too high (>=<\$THRESHOLD>) for <\$OPTION(dbserve)>.
Instruction Text	<p>Probable Cause(s): Number of times the transaction log for each database has been shrunk.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This depends on whether expansion is a desirable event. If the shrinkage was not intended, the administrator will have to disable the automated process and expand the log back to its original size. The automatic action report for this metric shows which users are connected to SQL Server.</p>
Report Type	Automatic and tool bank.
Area	Server

Metric M267_DBlogShrinksCnt

Metric Number	3267
Name	DBLogShrinksCnt
Severity	Major
Description	# of database transaction log shrinks per database
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	4
Reset (value)	Continuous
Message Text	DBSPI-3267.1: # of transaction log shrinks for (<i>database_name</i>)> Value too high (\geq Threshold).
Instruction Text	<p>Probable Cause(s): Percentage of space available in each filegroup for each database. Database filegroup is getting filled up.</p> <p>Potential Impact:</p> <p>Suggested Action(s): The following actions can be executed to remedy the situation: Use ALTER DATABASE to increase the size of the filegroup, or add a new filegroup. Drop objects from the database. Delete rows from tables in the database. The most natural action is, obviously, to add space to the database by executing the ALTER DATABASE command. If there is no free space available on the existing database devices, a new device has to be created by the DISK INIT command, or an exiting device has to be extended by executing the DISK RESIZE command. The automatic action report for this metric will show statistics for each filegroup in the database.</p>
Report Type	Automatic
Area	Databases

Metric M068_LatchWaitsRate

Metric Number	3068
Name	LatchWaitsRate
Severity	Minor
Description	Number of latch requests that could not be granted immediately and had to wait before being granted.
Alarming and/or Graphing metric	A & G

Metric Number	3068
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	10/sec
Reset (value)	Continuous
Message Text	DBSPI-3068.1: Latch waits rate <i>Value/sec</i> too high (\geq <i>Thresholdsec</i>).
Instruction Text	<p>Probable Cause(s): Number of latch requests that could not be granted immediately and had to wait before being granted. Many users are trying to access the same row at the same time. This is a performance bottleneck.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This may require analysis of the database design, process design, and coding. The automatic action report for this metric shows which users are connected to SQL Server.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Latches

Metric M069_AvgLatchWaitTim

Metric Number	3069
Name	AvgLatchWaitTim
Severity	Minor
Description	Average latch wait time (in milliseconds) for latch requests that had to wait since the server started. See M076 for current average latch wait time.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	500 ms
Reset (value)	Continuous
Message Text	DBSPI-3069.1: Average latch wait time <i>Value</i> milliseconds too high (\geq <i>Threshold</i> milliseconds).
Instruction Text	<p>Probable Cause(s): Average latch wait time (in milliseconds) for latch requests that had to wait since the server started. See M076 for current average latch wait time. Many users are trying to access the same row at the same time. This is a performance bottleneck.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This may require analysis of the database design, process design, and coding. The automatic action report for this metric shows which users are connected to SQL Server.</p> <p>The operator action for the metric generates a Latches graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Latches

Metric M070_LockTimeoutRate

Metric Number	3070
Name	LockTimeoutRate
Severity	Minor
Description	Number of lock requests per second that timed out, including internal requests for NOWAIT locks for each object type: Extent, Key, Page, Table, RID, Database.
Alarming and/or Graphing metric	A & G

Metric Number	3070
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	10/sec
Reset (value)	Continuous
Message Text	DBSPI-3070.1: Lock timeout rate <i>Value</i> /sec too high \geq <i>Threshold</i> /sec.
Instruction Text	<p>Probable Cause(s):Number of lock requests per second that timed out, including internal requests for NOWAIT locks for all objects combined. Locks are being held too long, which usually indicates a locking contention problem. The performance impact is that processes will not complete properly and will abort.</p> <p>Potential Impact:</p> <p>Suggested Action(s): The SQL code will need to be analyzed. Look for unnecessary exclusive locks, holdlocks or overly long transactions. Often a process design problem. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Locks graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Locks

Metric M270_LockTimeoutRate

Metric Number	3270
Name	LockTimeoutRate
Severity	Minor
Description	Number of lock requests per second that timed out, including internal requests for NOWAIT locks for each object type: Extent, Key, Page, Table, RID, Database.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	10/sec
Reset (value)	Continuous
Message Text	DBSPI-3270.1: Lock timeout rate for object (<i>instance_name</i>) Value/sec too high (\geq Threshold/sec).
Instruction Text	<p>Probable Cause(s): Number of lock requests per second that timed out, including internal requests for NOWAIT locks for each object type: Extent, Key, Page, Table, RID, Database. Locks are being held too long, which usually indicates a locking contention problem. The performance impact is that processes will not complete properly and will abort.</p> <p>Potential Impact:</p> <p>Suggested Action(s): The SQL code will need to be analyzed. Look for unnecessary exclusive locks, holdlocks or overly long transactions. Often a process design problem. The automatic action report for this metric shows which users are connected to SQL Server.</p>
Report Type	Automatic
Area	Locks

Metric M071_DeadlocksRate

Metric Number	3071
Name	DeadlocksRate
Severity	Major
Description	Number of lock requests per second that resulted in a deadlock for all objects combined.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour

Metric Number	3071
Min/Max Threshold	Maximum
Threshold	3/sec
Reset (value)	Continuous
Message Text	DBSPI-3071.1: Deadlocks rate <i>Value/sec</i> too high (\geq <i>Threshold/sec</i>).
Instruction Text	<p>Probable Cause(s): Number of lock requests per second that resulted in a deadlock for all objects combined. Two or more processes are accessing data in different orders, or size of transaction is too large. In any multi-use environment, occasional lock collisions are normal. Excessive lock collisions are a performance hit. Performance will be impacted since one of the deadlocked processes will become the victim and will be terminated by the server.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Deadlocks are a performance hit for two reasons. First, because all of the work of the deadlocked process needs to be rolled back. Second, because it probably has to be done again anyway. Action depends on situation. You may need to restructure indexes; or reschedule load processes when readers are not running, or make transactions shorter/smaller. In other words: optimize queries. Also often a process design problem. The automatic action report for this metric shows which users are connected to SQL Server.</p> <p>The operator action for the metric generates a Locks graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Locks

Metric M271_DeadlocksRate

Metric Number	3271
Name	DeadlocksRate
Severity	Major
Description	Number of lock requests per second that resulted in a deadlock for each object type: Extent, Key, Page, Table, RID, Database.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	3/sec
Reset (value)	Continuous
Message Text	DBSPI-3271.1: Deadlocks rate for object (<i>instance_name</i>) Value/sec too high (\geq Threshold/sec).
Instruction Text	<p>Probable Cause(s): Number of lock requests per second that resulted in a deadlock for each object type: Extent, Key, Page, Table, RID, Database. Two or more processes are accessing data in different orders, or size of transaction is too large. In any multi-use environment, occasional lock collisions are normal. Excessive lock collisions are a performance hit. Performance will be impacted since one of the deadlocked processes will become the victim and will be terminated by the server.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Deadlocks are a performance hit for two reasons. First, all of the work of the deadlocked process needs to be rolled back. Second, because it probably has to be done again anyway. Action depends on situation. You may need to restructure indexes; or reschedule load processes when readers are not running, or make transactions shorter/smaller. In other words: optimize queries. Also often a process design problem. The automatic action report for this metric show which users are connected to SQL Server.</p>
Report Type	Automatic
Area	Locks

Metric M072_LocksWaitRate

Metric Number	3072
Name	LocksWaitRate
Severity	Minor
Description	Locks wait rate.

Metric Number	3072
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	10/sec
Reset (value)	Continuous
Message Text	DBSPI-3072.1: Locks wait rate <i>Value/sec</i> too high (\geq <i>Threshold/sec</i>).
Instruction Text	<p>Probable Cause(s): Number of lock requests per second that could not be satisfied immediately and required the caller to wait, for all object types combined: Extent, Key, Page, Table, RID, Database. Many users are trying to access the same row at the same time or there is a performance bottleneck due to increased activity.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This is normal unless you are experiencing excessive lock timeouts (as measured by user complaints). Then this becomes a very useful metric for understanding volumes. This may require analysis of the database design and coding. The automatic action report for this metric shows a lock count for each object and which users are connected to SQL Server. The operator action for the metric generates a Locks graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Locks

Metric M272_LocksWaitRate

Metric Number	3272
Name	LocksWaitRate
Severity	Minor
Description	Locks wait rate per object type.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	10/sec
Reset (value)	Continuous
Message Text	DBSPI-3272.1: Locks wait rate for object (<i>instance_name</i>) <i>Value</i> /sec too high (\geq <i>Threshold</i> /sec).
Instruction Text	<p>Probable Cause(s): Number of lock requests per second that could not be satisfied immediately and required the caller to wait for each object type: Extent, Key, Page, Table, RID, Database. Many users are trying to access the same row at the same time or there is a performance bottleneck due to increased activity.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This is normal unless you are experiencing excessive lock timeouts (as measured by user complaints). Then this becomes a very useful metric for understanding volumes. This may require analysis of the database design and coding. The automatic action report for this metric shows a lock count for each object and which users are connected to SQL Server.</p>
Report Type	Automatic.
Area	Locks

Metric M073_LockAvgWaitTime

Metric Number	3073
Name	LockAvgWaitTime
Severity	Minor
Description	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait for all objects combined.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour

Metric Number	3073
Min/Max Threshold	Maximum
Threshold	500 millisecond
Reset (value)	Without reset
Message Text	DBSPI-3073.1: Average lock wait time <i>Value</i> milliseconds too high (\geq <i>Threshold</i> milliseconds).
Instruction Text	<p>Probable Cause(s): Average amount of wait time (in milliseconds) for each lock request that resulted in a wait for all objects combined. Many users are trying to access the same row at the same time, or there is a performance bottleneck preventing latches from being released.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This may require analysis of the database design and coding for locking issues. Quick fixes include getting faster CPUs. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Locks graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Locks

Metric M273_LockAvgWaitTime

Metric Number	3273
Name	LockAvgWaitTime
Severity	Minor
Description	Average lock wait time for each object type: Extent, Key, Page, Table, RID, Database.
Alarming and/or Graphing metric	A
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	500 milliseconds
Reset (value)	Without reset
Message Text	DBSPI-3273.1: Average lock wait time for object (<i>instance_name</i>) Value milliseconds too high (\geq Threshold milliseconds).
Instruction Text	<p>Probable Cause(s): Average amount of wait time (in milliseconds) for each lock request that resulted in a wait for each object type: Extent, Key, Page, Table, RID, Database Many users are trying to access the same row at the same time, or there is a performance bottleneck preventing latches from being released.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This may require analysis of the database design and coding for locking issues. Quick fixes include getting faster CPUs. The automatic action report for this metric shows which users are connected to SQL Server.</p>
Report Type	Automatic
Area	Locks

Metric M074_BatchReqstsRate

Metric Number	3074
Name	BatchReqstsRate
Severity	Minor
Description	Batch requests rate.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour

Metric Number	3074
Min/Max Threshold	Maximum
Threshold	500/sec
Reset (value)	Without reset
Message Text	DBSPI-3074.1: Batch requests rate <i>Value/sec</i> too high (\geq <i>Threshold/sec</i>).
Instruction Text	<p>Probable Cause(s): Number of Transact-SQL command batches received per second is very high or more users are making more and more requests of the Server.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Test to see if the Server is stressed. In general the higher the number of batches the better, provided the Server can keep up. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Server graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M075_LockMemoryPct

Metric Number	3075
Name	LockMemoryPct
Severity	Warning
Description	% of lock memory in use.
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	37%
Reset (value)	Continuous
Message Text	DBSPI-3075.1: % of lock memory in use <i>Value</i> too high (\geq <i>Threshold</i>).
Instruction Text	<p>Probable Cause(s): SQL Server lock memory is approaching reconfiguration threshold.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Manually modify the 'Number of locks available' to a specified value using sp_configure. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Locks graph.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Server

Metric M076_CurAvgLatchWait

Metric Number	3076
Name	CurAvgLatchWait
Severity	Minor
Description	Current average latch wait time .
Alarming and/or Graphing metric	A & G
Collection Interval	1 hour
Min/Max Threshold	Maximum
Threshold	500 milliseconds
Reset (value)	Continuous

Metric Number	3076
Message Text	DBSPI-3076.1: Current average latch wait time <i>Value</i> milliseconds too high (\geq <i>Threshold</i> milliseconds).
Instruction Text	<p>Probable Cause(s): Average latch wait time (in milliseconds) for latch requests that had to wait during the current collection interval (default is 1 hour). See M069 for the average latch wait time since the server was started. Many users are trying to access the same row at the same time. This is a performance bottleneck.</p> <p>Potential Impact:</p> <p>Suggested Action(s): This may require analysis of the database design, process design, and coding. The automatic action report for this metric shows which users are connected to SQL Server. The operator action for the metric generates a Latches graph.</p>
Report Type	Automatic and operator initiated.
Area	Latches

Metric M277_CompletedJobs

Metric Number	3277
Name	CompletedJobs
Description	Report on all jobs, successful, failed & canceled.
Collection Interval	5 mins
Min/Max Threshold	Maximum
Thresholds	2: Fail 3: Cancelled
Reset (value)	Continuous
Message Text	DBSPI-3277.1: Job cancelled. Job name = <\$OPTION(job_name)>, Job id = <\$OPTION(job_id)>, run date = <\$OPTION(run_date)>, runtime = <\$OPTION(run_time) for <\$OPTION(dbserve)>>" AUTOACTION "dbspimjh.bat <\$OPTION(job_id)> <\$OPTION(run_date)> <\$OPTION(run_time)> <\$OPTION(dbserve)>
Instruction Text	Probable Cause(s): A job has failed or been cancelled. Potential Impact: Suggested Action(s): Check the annotations for the steps completed. If successful, all steps will have completed. If failed or cancelled, then it will show the steps completed before the failure or cancellation. The automatic action for the metric generates a report on the completed steps for this job. The operator action for this metric shows the status of all jobs running.
Condition	DBSPI-3277.1
Default Threshold	3=Cancelled
Severity	Warning
Message Text	DBSPI-3277.1:Job Canceled. Job name - <i>job_name</i> , Job id- <i>job_id</i> , run date = <i>run_date</i> , runtime = <i>run_time</i>
Condition	DBSPI-3277.2
Default Threshold	2=Fail
Message Text	DBSPI-3277.2: Job failed. Job name = <i>job_name</i> , Job id = <i>job_id</i> , run date = <i>run_date</i> , runtime = <i>run_time</i>
Severity	Major Warning
Condition	DBSPI-3277.3
Default Threshold	1=Success
Message Text	DBSPI-3277.3: Job succeeded. Job name = <i>job_name</i> , Job id = <i>job_id</i> , run date = <i>run_date</i> , runtime = <i>run_time</i>
Report Type	Automatic and operator initiated.
Area	Jobs

Metric M278_FileGrpUsedSpacePct

Metric Number	3278
Name	FileGrpUsedSpacePct
Severity	Minor Major Critical
Description	Space used per filegroup per database
Alarming and/or Graphing metric	A
Collection Interval	15 Minute
Min/Max Threshold	Maximum
Default HPOM Threshold	90% 95% 99%
Reset (value)	Without reset
Message Text	DBSPI-3278.1: Percentage filegroup space MB free (<\$VALUE> MB) for transaction log filegroup in database <\$OPTION(database_name)> too high (\\<= <\$THRESHOLD>MB) for <\$OPTION(dbserve)>. DBSPI-3278.2: Percentage filegroup space MB free (<\$VALUE>%) for filegroup <\$OPTION(filegroup_name)> in database <\$OPTION(database_name)> too high (\\<=<\$THRESHOLD>%) for <\$OPTION(dbserve)>.
Instruction Text	Probable Cause(s): Percentage of space available in each filegroup for each database. Potential Impact: Suggested Action(s): The following actions can be executed to remedy the situation: Use ALTER DATABASE to increase the size of the filegroup, or add a new filegroup. Drop objects from the database. Delete rows from tables in the database. The most natural action is, obviously, to add space to the database by executing the ALTER DATABASE command. If there is no free space available on the existing database devices, a new device has to be created by the DISK INIT command, or an existing device has to be extended by executing the DISK RESIZE command. The automatic action report for this metric will show statistics for each filegroup in the database.
Report Type	Automatic and tool bank.
Area	Space

Metric M279_FileGrpSpaceFree

Metric Number	3279
Name	FileGrpSpaceFree
Severity	Critical Major Minor
Description	Free space in MB available in each filegroup for each database.
Alarming and/or Graphing metric	A
Collection Interval	15 min
Min/Max Threshold	Min
Threshold	150MB 100MB 50MB
Reset (value)	Without reset
Message Text	DBSPI-3279.1.1: filegroup space MB free (<\$VALUE> MB) for transaction log filegroup in database <\$OPTION(database_name)> too low (\\<=<\$THRESHOLD> MB) for <\$OPTION(dbserve)>.
Instruction Text	<p>Probable Cause(s): Database filegroup is getting filled up.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Use ALTER DATABASE to increase the size of the filegroup, or add a new filegroup. Drop objects from the database. Delete rows from tables in the database. The most natural action is, obviously, to add space to the database by executing the ALTER DATABASE command. If there is no free space available on the existing database devices, a new device has to be created by the DISK INIT command, or an existing device has to be extended by executing the DISK RESIZE command. The automatic action report for this metric will show statistics for each filegroup in the database.</p>
Report Type	Automatic and tool bank.
Area	Space

Metric M080_FailedReports

Metric Number	3080
Name	Failed Reports (summary)
Description	Report executions failed (summary). To work correctly requires SQL Server 2000 Reporting Services Service Pack 1; downloadable from http://www.microsoft.com/downloads/details.aspx?familyid=580febf7-2972-40e7-bccf-6cd90ac2f464&displaylang=en
Min/Max Threshold	Max
Threshold	1.0
Reset (value)	W/O
Message Text	DBSPI-3080.1:Number of Reports Failed <\$VALUE> above <\$THRESHOLD> for <\$OPTION(dbname)>.
Instruction Text	<p>Probable Cause(s): There may be number of possible causes:</p> <ol style="list-style-type: none"> 1 DataSource is not configured properly. 2 Report took too long to execute. 3 Schedule used to trigger the report has expired. 4 The report is undeliverable (it is too big). 5 The delivery extension specified in the subscription has been uninstalled or disabled. 6 The credential settings changed from integrated to stored or prompted values. 7 Parameter name or datatype changed in the report definition and the report was republished. If the subscription includes a parameter that is no longer valid, the subscription becomes invalid. <p>Potential Impact:</p> <p>Suggested Action(s): You can do the following:</p> <ol style="list-style-type: none"> 1 Check the Application Log for errors related to Reporting Service. 2 Ensure that the subscription is active. 3 The credentials used to run the report are valid. 4 Datasource used to connect to the DB is working. <p>The operator action for the metric generates a report of failed reports</p>
Report Type	Automatic (in message details); Manual (using DatabaseSPI Reports tool)
Area	Reports

Metric M280_FailedReports

Metric Number	3280
Name	Failed Reports (drill-down)
Description	Report executions failed (drill-down). To work correctly requires SQL Server 2000 Reporting Services Service Pack 1; downloadable from http://www.microsoft.com/downloads/details.aspx?familyid=580febf7-2972-40e7-bccf-6cd90ac2f464&displaylang=en
Min/Max Threshold	Max
Threshold	1.0
Reset (value)	W/O
Message Text	DBSPI-3080.1:Number of Reports Failed <\$VALUE> above <\$THRESHOLD> for <\$OPTION(dbname)>.
Instruction Text	<p>Probable Cause(s): This could have happened because of:</p> <ol style="list-style-type: none"> 1 DataSource is not configured properly. 2 Report took too long to execute. 3 Schedule used to trigger the report has expired. 4 The report is undeliverable (it is too big). 5 The delivery extension specified in the subscription has been uninstalled or disabled. 6 The credential settings changed from integrated to stored or prompted values. 7 Parameter name or datatype changed in the report definition and the report was republished. If the subscription includes a parameter that is no longer valid, the subscription becomes invalid. <p>Potential Impact:</p> <p>Suggested Action(s): You can do the following:</p> <ol style="list-style-type: none"> 1 Check the Application Log for errors related to Reporting Service. 2 Ensure that the subscription is active. 3 The credentials used to run the report are valid. 4 Datasource used to connect to the DB is working. <p>The operator action for the metric generates a report of failed reports.</p>
Report Type	Automatic (in message details); Manual (using DatabaseSPI Reports tool)
Area	Reports

Metric M081_RepnAgentStatus

Metric Number	3081
Name	Repn Agent Status
Severity	Major
Description	<p>Replication agents status.</p> <p>This metric checks the status of the snapshot agent, logreader agent, distribution agent, and merge agent for each distribution database in a particular Microsoft SQL Server replication environment. A message is sent to the management server if any of the agents fail. This metric generates an annotation text report that contains details of all failed replication agents.</p>
Alarming and/or Graphing metric	A
Collection Interval	5 minute
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Continuous
Message Text	DBSPI-3081.1 One or more replication agents failed.
Instruction Text	<p>Probable Cause(s): One or more Replication agents failed. Server not available, deadlock, connection failure or time-out failure.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Check the agent history and job history for other issues occurred around the same time, Verify the basic connectivity is working between the computers accessed by the agent.</p> <p>The automatic action report for this metric will show the list of agents which are failed.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Database

Metric M082_RepnLatency

Metric Number	3082
Name	Replication Latency
Severity	Warning
Description	<p>Status of replication latency.</p> <p>This metric monitors the replication latency, that is, the time between transactions marked for replication being added to the log file of the publication database and being added to the log file of the distribution database, for each distribution database in a particular Microsoft SQL Server replication environment. A message is sent to the management server when a distribution database has a replication latency that is more than the threshold value. This metric generates an annotation text report that contains the replication latency details for all distribution databases.</p>
Alarming and/or Graphing metric	A
Collection Interval	15 minutes
Min/Max Threshold	Maximum
Threshold	60.0
Reset (value)	Continuous
Message Text	DBSPI-3082.1: Replication Latency <\$VALUE> for the Log Reader Agent with agent_id <\$OPTION(agent_id)> too high (>=<\$THRESHOLD>) for the publisher <\$OPTION(publisher)>
Instruction Text	<p>Probable Cause(s): Replication latency for one or more publisher is high. Delay in distribution of commands which are marked for replication. May be there are some issues for the log reader or distribution agent.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Check for the distribution of commands which are marked for replication</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Database

Metric M083_Dellatency

Metric Number	3083
Name	Delivery Latency
Severity	Warning
Description	<p>Status of replication latency.</p> <p>This metric monitors the delivery latency, that is, the time between a transaction being inserted in the distribution database and being executed against the destination database (subscriber), for each distribution database in a particular Microsoft SQL Server replication environment. A message is sent to the management server when a distribution database has a delivery latency that is more than the threshold value. This metric generates an annotation text report that contains the delivery latency details for all distribution databases.</p>
Alarming and/or Graphing metric	A
Collection Interval	15 minutes
Min/Max Threshold	Maximum
Threshold	60.0
Reset (value)	Continuous
Message Text	DBSPI-3083.1: Delivery Latency <\$VALUE> for the Distribution Agent with agent_id <\$OPTION(agent_id)> too high (>=<\$THRESHOLD>) for the publisher <\$OPTION(publisher)>
Instruction Text	<p>Probable Cause(s): Delivery latency for one or more publisher is high.Delay in distribution of commands which are marked for replication. May be there are some issues for the distribution agent.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Check for the distribution of commands which are waiting in the distribution database.</p>
Report Type	Automatic, operator initiated, and tool bank.
Area	Database

Metric M084_DBMirroring_State

Metric Number	3084
Name	DBMirroring_State
Severity	Warning
Description	Mirroring state of the Server instanc (M084_DBMirroring_State)
Alarming and/or Graphing metric	Alarming
Collection Interval	5 minutes
Min/Max Threshold	Maximum
Threshold	0.5
Reset (value)	Continuous
Message Text	DBSPI-3084.1: Mirroring is suspended for several instances <\$OPTION(dbserve)>for one or more database(s) with its mirroring partner instance <\$OPTION(mirror_instance)>
Instruction Text	Probable Cause(s): Mirroring is suspended. The principal database is available but is not sending any logs to the mirror server. If the session is paused or there are redo errors on the mirror, the principal enters the SUSPENDED state. Potential Impact: Suggested Action(s): Check for redo errors on the mirror or whether the mirroring session is paused.
Report Type	Automatic and Tool Bank
Area	DBMirroring

Metric M085_DBMirroring_UnsentLog

Metric Number	3085
Name	DBMirroring_UnsentLog
Severity	Major Warning
Description	Unsent log on the principle(M085_DBMirroring_UnsentLog)
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum

Metric Number	3085
Threshold	95 90
Reset (value)	Continuous
Message Text	DBSPI-3085.1: Size of unsent log in the send queue on the principal database <\$OPTION(database_name)> is <\$VALUE> too high (>=<\$THRESHOLD>) for <\$OPTION(dbserve)>.
Instruction Text	<p>Probable Cause(s): The amount of log waiting in the send queue (in kilobytes). During high-performance mode, a principal server can develop a backlog of unsent log records that still need to be sent from the principal server to the mirror server. However, this is also relevant for high-safety mode when mirroring is paused or suspended because the partners become disconnected.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Check mirroring is paused, suspended or partners become disconnected.</p>
Report Type	Automatic and Tool Bank
Area	DBMirroring

Metric M086_DBMirroring_UnrestoredLog

Metric Number	3086
Name	DBMirroring_UnrestoredLog
Severity	Major Warning
Description	Unrestored log on the mirror (M086_DBMirroring_UnrestoredLog)
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum
Threshold	95 90
Reset (value)	Continuous
Message Text	DBSPI-3086.1: Size of unrestored log in the redo queue on the mirror database <\$OPTION(database_name)> is <\$VALUE> too high (>=<\$THRESHOLD>) for <\$OPTION(dbserv)>.
Instruction Text	Probable Cause(s): The amount of log waiting in the redo queue (in kilobytes). In any operating mode, the mirror server can develop a backlog of unrestored log records that have been written to the log file but still need to be restored on the mirror database. Normally it happens during failover time. Potential Impact: Suggested Action(s): Check failover happened successfully.
Report Type	Automatic and Tool Bank
Area	DBMirroring

Metric M087_DBMirroring_LogGenRate

Metric Number	3087
Name	DBMirroring_LogGenRate
Severity	Warning
Description	Log generation rate on the principal (M087_DBMirroring_LogGenRate)
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum

Metric Number	3087
Threshold	10
Reset (value)	Continuous
Message Text	DBSPI-3087.1: Log generation rate on the principal database <\$OPTION(database_name)> is <\$VALUE> too high (>=<\$THRESHOLD>) for <\$OPTION(dbserve)>.
Instruction Text	<p>Probable Cause(s): Rate at which incoming transactions are being entered into the principal's log in KB per second. The amount part of the log that is generated by the application is the amount of information that is sent across the wire through the network to the mirror database, and therefore has the most significant impact on performance.</p> <p>Potential Impact:</p> <p>Suggested Action(s): As a rough guideline, the network bandwidth should be three times the maximum log generation rate.</p>
Report Type	Automatic and Tool Bank
Area	DBMirroring

Metric M088_DBMirroring_CurrSndRate

Metric Number	3088
Name	DBMirroring_CurrSndRate
Severity	Warning
Description	Current send rate on the principal (M088_DBMirroring_CurrSndRate)
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum
Threshold	10
Reset (value)	Continuous
Message Text	DBSPI-3088.1: Current send rate on the principal database <\$OPTION(database_name)> is <\$VALUE> too high (>=<\$THRESHOLD>) for <\$OPTION(dbserv)>.
Instruction Text	<p>Probable Cause(s): Rate at which transactions are being sent to the mirror server instance in kilobytes (KB) per second. It depends on the hardware, disk environment and network bandwidth.</p> <p>Potential Impact:</p> <p>Suggested Action(s): Check hardware setup and network efficiency.</p>
Report Type	Automatic and Tool Bank
Area	DBMirroring

Metric M403_DistDelLatency

Metric Number	3403
Name	Distribution Delivery Latency
Severity	Major Warning
Description	Time (in milliseconds) elapsed from when transactions are delivered to the Distributor to when they are applied at the Subscriber.
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum

Metric Number	3403
Threshold	10000ms 30000ms
Reset (value)	without reset
Message Text	DBSPI-3403.1: Distribution Delivery Latency for object <\$OPTION(instance_name)> (<\$VALUE>/sec) too high (>=<\$THRESHOLD>/sec) for <\$OPTION(dbserv)>
Instruction Text	<p>Probable Cause(s):</p> <ol style="list-style-type: none"> 1. Slow network could be an issue. Network latency has a substantial negative performance impact. 2. Delivery latency can be high if subscribing servers are overloaded. <p>Potential Impact: Performance issues at the Subscriber.</p> <p>Suggested Action(s):</p> <ol style="list-style-type: none"> 1. Check the size of Distribution database. Due to huge data load on distribution database, sometimes distribution agent face issues while reading data which in turn hit the delivery rate metric. 2. Agent values for CommitBatchSize and CommitBatchThreshold can be re-configured to increase the throughput. 3. Avoid horizontal filtering.
Report Type	NA
Area	Microsoft SQL Server Replication



This metric is valid for Microsoft SQL Server 2005 and later versions.

Metric M404_MergeConflicts

Metric Number	3404
Name	Merge Conflicts
Severity	Major Warning
Description	Number of conflicts per second during Publisher or Subscriber upload and download.
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum
Threshold	1 5
Reset (value)	without reset
Message Text	DBSPI-3404.1: Number of conflicts per second for object <\$OPTION(instance_name)> (<\$VALUE>/sec) too high (>=<\$THRESHOLD>/sec) for <\$OPTION(dbserve)>
Instruction Text	<p>Probable Cause(s): Merge replication is a two-way replication in which data changes occur on publisher and subscriber are merged at synchronization time. This value should always be zero.</p> <p>A nonzero value may require notification and appropriate action should be taken care to override the conflict.</p> <p>Change of data on both publisher and subscriber at the time of synchronization results.</p> <p>Suggested Action(s): Based on business requirement, you can specify merge replication to recognize conflicts at row-level or at column-level. In order to resolve conflict, SQL Server has few options : 1. Default Resolver: Default resolver resolves the conflict based on priority. At subscriber end, you can assign the priority values which will determine the winner in case of conflict.</p> <p>2. Custom Resolver: If your business requirements does not met with default resolver, the second option you have is custom resolver. Customer resolver are specific to table. In case of any alteration to any table, you need to modify resolver accordingly.</p> <p>3. Stored Procedure Conflict resolver: This is also one type of customer resolver which uses stored procedure in T-SQL to implement business logic at the time of conflict. These stored procedures are applicable only for publisher and will be used to resolve update conflicts only.</p>
Report Type	NA
Area	Microsoft SQL Server Replication

► This metric is valid for Microsoft SQL Server 2005 and later versions.

Metric M411_LogReaderDellatency

Metric Number	3411
Name	Log Reader Delivery Latency
Severity	Major Warning
Description	Time (in milliseconds) elapsed from when transactions are applied at the Publisher to when they are delivered to the Distributor
Alarming and/or Graphing metric	Alarming
Collection Interval	15 minutes
Min/Max Threshold	Maximum
Threshold	10000ms 30000ms
Reset (value)	without reset
Message Text	DBSPI-3411.1: LogReader Delivery Latency for object <\$OPTION(instance_name)> (<\$VALUE>/sec) too high (>=<\$THRESHOLD>/sec) for <\$OPTION(dbserve)>
Instruction Text	Probable Cause(s): 1. Slow network could be an issue. Network latency has a substantial negative performance impact. 2. Delivery latency can be high if publisher servers are overloaded. Potential Impact: Performance issues at the publisher. Suggested Action(s): 1. Monitor Log Reader delivery rate which can be found from mslogreader_history table in the distribution database. Poor log reader performance tends to be caused by network issues. 2. Check if transaction log is not growing or shrinking at the time. 3. Check if database backups are not running during your long latency period.
Report Type	NA
Area	Microsoft SQL Server Replication

► This metric is valid for Microsoft SQL Server 2005 and later versions.

Microsoft SQL Logfile Policies

This section provides detailed information about the text contained in the DB SPI SQL Server logfile policies. This information is meant to cover a range of messages for two of the errors as indicated by their titles.

MSS-Error601

Description	Error 601
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause: This error indicates that the in-memory structure used by SQL Server to access a system table has been reused. Usually, only user-table descriptors are reused; system table descriptors are always in memory.</p> <p>Suggested Action: To work around this problem, shut down and restart SQL Server. This should temporarily alleviate error 601; however, an underlying problem may still exist. To troubleshoot this problem, do the following: Examine the error logs and the parameters of sp_configure for additional information. Look for warnings indicating that open objects and open databases may be set too low. Look at the settings for memory, open objects, and open databases; increase them if they are not appropriate for the amount of physical memory, number of databases, and number of objects.</p> <p>For more information on how to determine the memory overhead for connections, objects, locks and databases, see the following article in the Microsoft Knowledge Base: Q160234 INF: Memory Overhead for Connections, Objects, Locks, and DBs Also run DBCC CHECKDB, DBCC NEWALLOC, and DBCC CHECKCATALOG to verify that there are no structural problems in the database that may have caused the error.</p> <p>For more information, use the following URL to search the Microsoft Knowledge Base for this error: http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+601</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 602

Description	Error 602
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <p>When running an application that uses FORWARD ONLY or DYNAMIC server-side cursors, you may receive error 602 in the error log: Msg 602, Level 2, State 15 Could not find row in Sysindexes for dbid '11', object '80003316', index '1'. Run DBCC CHECKTABLE on Sysindexes. The SQL Server is terminating this process.</p> <p>This does not cause problems with the execution of SQL Server, but the client is disconnected from the server as stated in the message. This problem occurs when all of the following conditions are true:</p> <ul style="list-style-type: none">* The query contains an equal join on two or more tables. * A search argument is applied to the join column on the inner table.* An ORDER BY clause is used on two or more columns.* The statement is being used as the record source for a cursor. The cursor is defined as either a DYNAMIC or FORWARD ONLY cursor. If the cursor is called by the Transact-SQL syntax (for example, a DECLARE CURSOR statement) the problem does not occur.
Help Text (contd.)	<p>Suggested Action:</p> <p>To work around the problem, modify the query to not use one of the required conditions that cause this behavior, as noted in the CAUSE section of this article. For example, use a STATIC cursor instead of a DYNAMIC cursor or apply the search argument to the outer table and not the inner table. As an additional workaround, you can do the following:</p> <ol style="list-style-type: none">1 Run showplan on the query you are basing the cursor on.2 Find the index that the query uses on the table listed in the message 602.3 Put an index hint in the query to force that index. For more information, use the following URL to search the Microsoft Knowledge Base for this error: http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+602 <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 604

Description	Error 604
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <p>Under the following conditions, error messages 602, 604 and 618 might appear in the SQL Server errorlog with a severity level of 21, which terminates the client connection: A stored procedure is run repeatedly while SET FMTONLY is enabled and disabled.</p> <p>The stored procedure creates and selects from temporary tables.</p> <p>Suggested Action:</p> <p>Minimize the use of temporary tables in stored procedures that are run on a frequent basis. Additional Information: Here is the expected text from the errorlog for the three possible error messages:</p> <p>Error 602: 2000-06-30 11:10:18.33 spid16 Error: 602, Severity: 21, State: 1 2000-06-30 11:10:18.33 spid16 Could not find row in sysindexes for database ID 2, object ID 1967346073, index ID -1. Run DBCC CHECKTABLE on sysindexes.. Error 604: 2000-06-30 11:13:30.85 spid16.</p> <p>Error 604: Severity: 21, State: 5 2000-06-30 11:13:30.85 spid16 Could not find row in sysobjects for object ID 0 in database '0'. Run DBCC CHECKTABLE on sysobjects.</p> <p>Error 618: 2000-06-30 11:11:26.71 spid10 Error: 618, Severity: 21, State: 1 2000-06-30 11:11:26.71 spid10 A varno of 666 was passed to the opentable system function. The largest valid value is 257.</p> <p>For more information, use the following URL to search the Microsoft Knowledge Base for this error:</p> <p>http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+604</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 605

Description	Error 605
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause: Either running a query with the Optimizer hint NOLOCK or setting the transaction isolation level to READ UNCOMMITTED, may generate transient 605 error messages.</p> <p>Suggested Action: Typically, access to data that is being changed by either another user or process is denied because of locks put on the data. However, the NOLOCK and READ UNCOMMITTED commands enable a query to read data that is locked by another user. This is referred to as a dirty read because you can read values that have not yet been committed and are subject to change.</p> <p>When a query that is using NOLOCK or READ UNCOMMITTED tries to read data that is being moved or changed by another user, a 605 error occurs. The severity level of 605 errors occurring during a dirty read operation is 12 versus a severity level of 21 when reading committed data. If a 605 error that has a severity level of 12 occurs, it is most likely a transient 605 error and does not indicate a database consistency problem. To verify that it is a transient 605 error, rerun the query later.</p> <p>If the error persists, remove the NOLOCK hint or set the transaction isolation level to READ COMMITTED and verify that a 605 severity level 21 does not occur. A 605 level 21 error indicates possible database corruption. If a 605 level 21 error occurs, see to SQL Server Books Online for more information and contact your primary support provider for more help.</p>

MSS-Error 945

Description	MSS-Error 945
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause: Database cannot be opened due to inaccessible files, insufficient memory or disk space.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Visit the error log file for information about memory, disk space and permission failure.2 Check for the availability of database files like .mdf and .ndf.3 Check for access permission for the account used by database engine.4 After correction, restart the database. Commands to set database is ALTER DATABASE and then set it to ONLINE.

MSS-Error 1105

Description	Error 1105
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause: The specified filegroup has run out of free space</p> <p>Suggested Action: To gain more space, you can free disk space on any disk drive containing a file in the full filegroup, allowing files in the group to grow. Or you can gain space using a data file with the specified database. Freeing disk space You can free disk space on your local drive or on another disk drive. To free disk space on another drive:</p> <ol style="list-style-type: none">1 Move the data files in the filegroup with an insufficient amount of free disk space to a different disk drive.2 Detach the database by executing <code>sp_detach_db</code>.3 Attach the database by executing <code>sp_attach_db</code>, pointing to the moved files. Using a data file Another solution is to add a data file to the specified database using the <code>ADD FILE</code> clause of the <code>ALTER DATABASE</code> statement. Or you can enlarge the data file by using the <code>MODIFY FILE</code> clause of the <code>ALTER DATABASE</code> statement, specifying the <code>SIZE</code> and <code>MAXSIZE</code> syntax. <p>A stress of multiple clients that are all querying sysprocesses with random aborts results in the following error in the error log:</p> <p>Additional Information: Error: 1105, Severity: 17, State: 3 Could not allocate space for object '(SYSTEM table id: -631257169)' in database 'tempdb' because the 'DEFAULT' filegroup is full. The error 1105 occurs even though tempdb is set for autogrow and plenty of disk space exists. The error 1105 is 'transient' because it is not a true indication of the actual amount of space available in tempdb.</p> <p>You may also see the following message in the error log as well: Ec Iterator cleaned up a reference. This message is benign and can be ignored.</p> <p>Workaround: To work around this problem, reduce the amount and frequency of concurrent queries against the sysprocesses table.</p> <p>For more information, use the following URL to search the Microsoft Knowledge Base for this error: http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+1105</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 1418

Description	Error 1418
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause: The endpoint of server network did not respond. It can be because of two reasons</p> <ol style="list-style-type: none">1 The specified server network address cannot be reached2 The specified server network address does not exist. <p>Suggested Action:</p> <ol style="list-style-type: none">1 Validate network address name.2 Validate ports for local and remote endpoints. Also make sure that mirror database is ready for mirroring. Make sure that the name and port of the mirror server instance are correct and mirror instance should not be behind any firewall.

MSS-Error 1432

Description	Error 1432
Severity	Minor
Message Group	MSS_Fault
Help Text	<p>Probable Cause: Attempt to repair physical page in database by requesting a copy from the partner could be the potential reason.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Diagnose hardware and resolve the issue (if found).2 Check application logs and SQL Server logs to detect hardware issues.

MSS-Error 1437

Description	Error 1437
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: Unable to post message from server instance because there is insufficient memory. Suggested Action: <ol style="list-style-type: none">1 Check for non-essential memory load.2 Try to increase the system memory (if possible).

MSS-Error 1471

Description	Error 1471
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: Database mirroring connection terminated due to out-of-memory during sending message. Suggested Action: Reduce non-essential memory load or increase system memory.

MSS-Error 1472

Description	Error 1472
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: Database mirroring connection terminated due to communication error during sending message. Suggested Action: Check the database connection. Still, if problem persists contact Microsoft Help Centre.

MSS-Error 1499

Description	Error 1499
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause: When a database mirroring error occurs. There are three causes - Physical, operating system, or SQL Server problems which can cause a failure in a database mirroring session. Possible causes of hard errors may be</p> <ol style="list-style-type: none">1 Operating system or process failure.2 Loss of the drive where the transaction log resides3 firewall problems etc. <p>Conditions that might cause mirroring time-outs:</p> <ol style="list-style-type: none">1 Network errors such as TCP link time -outs.2 dropped or corrupted packets, or packets that are in an incorrect order.3 Insufficient computing resources, such as a CPU or disk overload, the transaction log filling up, or the system is running out of memory or threads. <p>Potential Impact: Database Mirroring will fail.</p> <p>Suggested Action: For mirroring time outs a increase in the time-out period, reduce the workload, or change the hardware to handle the workload will help.</p>

MSS-Error 1608

Description	Error 1608
Severity	Warning
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <p>A client process exited abnormally, or a network error was encountered. Unless other errors occurred, continue processing normally. This error occurs when a client process stopped without informing SQL Server and a subsequent attempt by SQL Server to send results to this client fails.</p> <p>Error 1608 is usually not serious and may be viewed as notification that a client process no longer exists. Some of the possible reasons a client process can disappear are:</p> <ul style="list-style-type: none">* The client application was killed or ended abnormally* The client machine was powered off or rebooted* There is excessive network traffic* The network connection has been dropped or interrupted <p>Suggested Action:</p> <p>Do not be concerned if this error occurs only sporadically. However, if the error occurs frequently and continuously, or frequently for short periods of time, it may be a result of excessive network traffic or network problems. If it is suspected that there are network problems, contact the network administrator in order to run diagnostics on the network between the client and the SQL Server machines to isolate the problem.</p> <p>For more information, use the following URL to search the Microsoft Knowledge Base for this error:</p> <p>http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+1608</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 3041

Description	Error 3041
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <ol style="list-style-type: none">1 Database backup failed to complete. It happens when a valid backup sequence is not happening.2 Log backup failed to complete. <p>Suggested Action:</p> <p>Check backup sequence events. for more information on database backup sequence, contact Microsoft Help Centre.</p>

MSS-Error 3167

Description	MSS-Error 3167
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: Restore could not start database. Suggested Action: Check the connection and permissions with backup device.

MSS-Error 3201

Description	Error 3201
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: When unable to open a backup device. When the backup command executes, it fails to read the directory, since there is no directory with such a name exists. Suggested Action: Check for backup device name.

MSS-Error 3208

Description	MSS-Error 3208
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: Unexpected end of file is encountered while reading beginning of backup set. Suggested Action: Check the console error log for detail information. Also confirm that the media should contain a valid SQL server backup set.

MSS-Error 6289

Description	Error 6289
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: The computer failed to allocate memory to .NET framework CLR. Suggested Action: Check the memory availability on system and for .NET framework CLR.

MSS-Error 6291

Description	Error 6291
Severity	Major
Message Group	MSS_FAULT
Help Text	Probable Cause: When a client application failed, this error code comes. Suggested Action: AppDomain %i(%.*ls) was unloaded. This requires to look into client application. Even after restarting the problem occurs, contact Microsoft Product Support Services.

MSS-Error 6510

Description	Error 6510
Severity	Major
Message Group	MSS_Fault
Help Text	Probable Cause: CLR runtime is not installed properly Suggested Action: The CLR is required to use SQL/CLR features. CLR should be installed properly.

MSS-Error 6511

Description	Error 6511
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause: CLR failed to start due to initialization. The probable reason for this error message is because it Failed to initialize the Common Language Runtime (CLR) %ls with HRESULT 0x%x.</p> <p>Potential Impact: CLR monitoring is not possible.</p> <p>Suggested Action: The suggested action is to restart the SQL server</p>

MSS-Error 6513

Description	Error 6513
Severity	Major
Message Group	MSS_FAULT
Help Text	<p>Probable Cause: CLR failed to start due to initialization. The probable reason for this error message is that it Failed to initialize the Common Language Runtime (CLR) %ls due to memory pressure.</p> <p>Potential Impact: CLR monitoring is not possible.</p> <p>Suggested Action: Memory pressure at MemToLeave region could be the probable reason. For further troubleshooting, refer CLR integration documentation.</p>

MSS-Error 6536

Description	Error 6536
Severity	Major
Message Group	MSS_FAULT
Help Text	<p>Probable Cause: A fatal error occurs in the .NET Framework Common Language Runtime (CLR). Reason could be :</p> <ul style="list-style-type: none">a Any managed application build on .Net Framework 2.0 may stop the application process unexpectedly.b Running managed code in SQL Server may shut down the server unexpectedly. <p>Potential Impact: SQL Server will shut down</p> <p>Suggested Action: Restart the server. If the problem persists after restarting the server, contact Microsoft Product Support Services to obtain the hotfix.</p>

MSS-Error 6537

Description	Error 6537
Severity	Major
Message Group	MSS_FAULT
Help Text	<p>Probable Cause: If any user defined function shut down the .NET Framework CLR.</p> <p>Potential Impact: SQL Server will shut down</p> <p>Suggested Action: Exit the process. Do not use Exit command to exit the process. A scalar function or an output parameter should be used if the intent is to return an integer to indicate failure.</p>

MSS-Error 9001

Description	MSS-Error 9001
Severity	Minor
Message Group	MSS_Fault
Help Text	<p>Probable Cause: The log for a database is not available. This error message signifies a catastrophic failure.</p> <p>Suggested Action: Check the event log for related error messages. Resolve the errors and restart the SQL Server database instance. The event log should be checked for detailed related error messages. Resolve these errors and restart the instance of SQL Server database.</p>

MSS-Error9002

Description	Error 9002
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause: The specified transaction log file has run out of free space.</p> <p>Suggested Action: To gain more space, you can free disk space on any disk drive containing the transaction log file for the related database. Freeing disk space allows the recovery system to enlarge the log file automatically. Or you can gain space by adding or enlarging a log file for the specified database.</p> <p>Freeing disk space: You can free disk space on your local drive or on another disk drive.</p> <p>To free disk space on another drive:</p> <ol style="list-style-type: none">1. Move the transaction log files with an insufficient amount of free disk space to a different disk drive.2 Detach the database by executing <code>sp_detach_db</code>.3 Attach the database by executing <code>sp_attach_db</code>, pointing to the moved files. Adding a log file Another solution is to add a log file to the specified database using the <code>ADD FILE</code> clause of the <code>ALTER DATABASE</code> statement. Or you can enlarge the log file using the <code>MODIFY FILE</code> clause of the <code>ALTER DATABASE</code> statement, specifying the <code>SIZE</code> and <code>MAXSIZE</code> syntax. Adding an additional log file allows the existing log to grow. <p>For more information, use the following URL to search the Microsoft Knowledge Base for this error: http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+9002</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error9004

Description	Error 9004
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause: An error was encountered while processing the log during rollback, recovery, or replication. This could indicate an error detected by the operating system-or an internal consistency error detected by SQL Server.</p> <p>Suggested Action: One of the following actions will correct this error:</p> <ol style="list-style-type: none">1 Restore from a backup.2 Rebuild the log.

MSS-Error 9642

Description	Error 9642
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause: An error occurs in a Service Broker/Database Mirroring transport connection endpoint.</p> <p>Potential Impact: Database Mirroring will be suspended</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Check you TCP port and if it is disabled, Enable it on SQL Server Configuration manager.2 Telnet port between primary and secondary server.3 Check your sql authentication. Incase of windows authentication, add this user to sql login set.4 check for firewall.(if applicable).

MSS-Error 10304

Description	Error 10304
Severity	Major
Message Group	MSS_FAULT
Help Text	Probable Cause: Client application tried unsuccessfully to create a CLR AppDomain manager. PotentialImpact: CLR Monitoring will not work.

MSS-Error 14151

Description	Error 14151
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause: This error is raised for any replication agent failure. The text at the end of the message depends on the context of the failure.</p> <p>Suggested Action: This error can occur in a number of situations; use the following approaches as necessary: Restart the failed agent to see if it will now run without failures. For more information, see How to: Start and Stop a Replication Agent (SQL Server Management Studio) and Replication Agent Executables Concepts. Check the agent history and job history for other errors that occurred around the same time. For information about viewing agent status and error details in Replication Monitor, see the following topics: For the Snapshot Agent, Log Reader Agent, and Queue Reader Agent, see How to: View Information and Perform Tasks for the Agents Associated With a Publication (Replication Monitor). For the Distribution Agent and Merge Agent, see How to: View Information and Perform Tasks for the Agents Associated With a Subscription (Replication Monitor). Verify that basic connectivity is working between the computers accessed by the agent, and then connect to each computer with a utility like the sqlcmd Utility. When connecting, use the same account under which the agent makes connections. For more information about the permissions required by each agent account, see Replication Agent Security Model. If the error occurs while creating or applying a snapshot, check the files in the snapshot directory for errors. If the error continues to occur, increase the logging of the agent and specify an output file for the log. Depending on the context of the error, this could provide the steps leading up to the error and/or additional error messages. For more information, see Replication Agents (Troubleshooting).</p>

MSS-Error 15457

Description	Error 15457
Severity	Warning
Message Group	MSS_Fault
Help Text	Probable Cause: Configuration option '%ls' changed from %ld to %ld. Suggested Action: Run the RECONFIGURE statement to install.

MSS-Error 17824

Description	Error 17824
Severity	Warning
Message Group	MSS_Fault

Description	Error 17824
Help Text	<p>Probable Cause:</p> <p>Other relevant errors may follow, depending on the network library used for the connection. In case of Named Pipes connections, errors '232 The pipe is being closed' or '109 The pipe has been ended' may be logged. In case of sockets based connections (TCP/IP or IPX/SPX), errors '10054 Connection reset by peer' or '10053 Software caused connection abort' may be logged.</p> <p>These errors indicate that the connection between the client and SQL Server was broken for some reason while SQL Server was writing data to the front end. Depending on the circumstances, a certain number of these errors may be normal, and eliminating them is not always necessary. If you do not receive any end user complaints or experience general connection problems, you can ignore these errors.</p> <p>Suggested Action:</p> <p>Error 17824 'Unable to write to ListenOn connection' indicates that problems have occurred while SQL Server attempted to write to a client connection and failed. These communication problems may be caused by network problems, or if the client computer has stopped responding or been restarted.</p> <p>For more information regarding other communication errors, please refer to the following article in the Microsoft Knowledge Base: Q109787 : INF: SQL Communication Errors 17832, 17824, 1608, 232, and 109 Error 17824 does not always indicate a network problem.</p>

Description	Error 17824
Help Text (contd.)	<p>The following are the most common situations under which the error 17824 is generated, along with the corresponding troubleshooting procedures. This error may occur if the users are restarting their client computers if the application seems have stopped responding, so make sure they don't do that. It may be that the server is taking a longer time to process a long query. Once the client workstation is restarted, the connections are broken ungracefully.</p> <p>Later SQL Server tries to respond to the connection that has been dropped, and logs the message 17824. The network may be unstable; make sure it is stable. You can check this by attempting to copy large files between the computer running Windows NT Server and the client computer. If this test fails, then you are running into problems with the physical network. Because the above errors indicate a potential network issue, it is recommended that you update the server, both Windows NT Server and SQL Server, to the latest service packs.</p> <p>Please check the knowledge base articles for more information on how to obtain the latest service packs for the Windows NT Server operating system and SQL Server. It is also recommended that you update the client components such as DB-Library, the ODBC driver, and network library to the latest DLLs. In case of client computers running 16-bit Windows 3.1 or Windows for Workgroups on a Novell network, it is necessary to obtain and install the latest MS-DOS and Windows drivers from Novell.</p> <p>Error 17824 'Unable to write to ListenOn connection' may be a consequence of other errors that caused the connection to drop. Check the error logs for other errors within the same time frame as the 17824 error. If you find other errors, refer to SQL Server Books Online and the Microsoft Knowledge Base for more information on these errors. Use sp_configure or the SQL Server Enterprise Manager to check the Priority Boost and the SMP Concurrency configuration settings. Make sure that these two configuration options are set to the default settings, because deviating from the default settings may cause error 17824 under some conditions.</p>

Description	Error 17824
Help Text (contd.)	<p>For more information on why these settings may generate error 17824, please refer to the following article in the Microsoft Knowledge Base: Q111405 : INF: SQL Server and Windows NT Thread Scheduling. The error 17824 may be generated due to application problems. One major cause is running into a lock or block situation. In this case, a process holds a lock on a page or a table, and that lock is not released right away, due to an uncommitted transaction or a long query. This may cause all other processes requesting the same table to be blocked, and the client application to seem to stop responding. If the user then either uses 'End Task' to close the application or restarts the workstation, you may receive error 17824 on the server.</p> <p>To find out if the application is causing a lock or block problem on the server, use the sp_who and sp_lock stored procedures when the client computers seem to stop responding or when the error 17824 starts to appear in the SQL Server error logs. If the client workstation has stopped responding, open a command-line ISQL connection on the server itself using the local pipe, and use these stored procedures to check for a blocking situation.</p> <p>For more information on detecting and resolving blocking problems, please refer to the following article in the Microsoft Knowledge Base: Q162361 : INF: Understanding and Resolving SQL Server Blocking Problems For more information, use the following URL to search the Microsoft Knowledge Base for this error:</p> <p>http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+17824</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 17832

Description	Error 17832
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <p>This error occurs if a client starts to connect but never successfully completes the attempt because of a client operating system, application, or network failure. Wide area networks (WANs) are more susceptible than local area networks (LANs) to this type of problem, because such networks often have many routers and other network devices that can delay data packet delivery and/or cause other difficulties in the delivery of data packets due to improper packet fragmentation or misrouting.</p> <p>However, the very occurrence of these errors in the errorlog or event log does not necessarily indicate any real problems with your SQL Server connectivity.</p> <p>Even in normal operations, this error may still occur at times, due to the unreliable nature of networks, especially wide area networks. In addition, improper use of applications (such as restarting the computer in the middle of a login process) can also cause this error to occur.</p> <p>Suggested Action:</p> <p>Error 17824 'Unable to write to ListenOn connection' indicates that problems have occurred while SQL Server attempted to write to a client connection and failed. These communication problems may be caused by network problems, or if the client computer has stopped responding or been restarted.</p> <p>For more information regarding other communication errors, please refer to the following article in the Microsoft Knowledge Base: Q109787 : INF: SQL Communication Errors 17832, 17824, 1608, 232, and 109 Error 17824 does not always indicate a network problem.</p> <p>The following are the most common situations under which the error 17824 is generated, along with the corresponding troubleshooting procedures. This error may occur if the users are restarting their client computers if the application seems have stopped responding, so make sure they don't do that. It may be that the server is taking a longer time to process a long query. Once the client workstation is restarted, the connections are broken ungracefully.</p>

Description	Error 17832
Help Text (contd.)	<p>Later SQL Server tries to respond to the connection that has been dropped, and logs the message 17824. The network may be unstable; make sure it is stable. You can check this by attempting to copy large files between the computer running Windows NT Server and the client computer. If this test fails, then you are running into problems with the physical network. Because the above errors indicate a potential network issue, it is recommended that you update the server, both Windows NT Server and SQL Server, to the latest service packs.</p> <p>Please check the knowledge base articles for more information on how to obtain the latest service packs for the Windows NT Server operating system and SQL Server. It is also recommended that you update the client components such as DB-Library, the ODBC driver, and network library to the latest DLLs. In case of client computers running 16-bit Windows 3.1 or Windows for Workgroups on a Novell network, it is necessary to obtain and install the latest MS-DOS and Windows drivers from Novell.</p> <p>Error 17824 'Unable to write to ListenOn connection' may be a consequence of other errors that caused the connection to drop. Check the error logs for other errors within the same time frame as the 17824 error. If you find other errors, refer to SQL Server Books Online and the Microsoft Knowledge Base for more information on these errors. Use <code>sp_configure</code> or the SQL Server Enterprise Manager to check the Priority Boost and the SMP Concurrency configuration settings. Make sure that these two configuration options are set to the default settings, because deviating from the default settings may cause error 17824 under some conditions.</p> <p>To determine whether or not you are facing a real problem, you may want to check the following:</p> <ol style="list-style-type: none"> 1 Check with the end users to see whether they have experienced any difficulties in making connections to SQL Server. If nobody reports any connectivity problems, you can usually ignore these errors. 2 Check the frequency of this error in the errorlog. If it occurs very frequently, it indicates some potential problems, even if no one is complaining about any connectivity problems. If you have determined that you have a real problem, you may want to apply the additional troubleshooting methods described in the remainder of this article.

Description	Error 17832
Help Text (contd.)	<p>Additional Information: Errors of type 17832 can generally be classified into two categories:</p> <ol style="list-style-type: none"> 1 Frequent, repeated occurrence of these errors. If you examine the timestamps of these errors, you may find that they usually occur in regular intervals, typically one or more occurrences per second. The errorlog typically is full of these errors. This is mostly caused by client-side problems such as operating system or network software. The repeated occurrence of these errors is caused by the connection retries built into the client-side DB-Library or ODBC, which does not stop until the client application times out. 2 Intermittent, random occurrence of these errors. In the errorlog, you will find these errors occurring once in a while without any regularity. If nobody has reported any connectivity problems, you can generally ignore these errors. If someone did report connectivity problems to SQL Server, you need to use the timestamps to determine whether these reported problems correspond to the errors of type 17832 in the errorlog. Because SQL Server does not know the client's address or host name yet when the error occurs, this error message cannot provide any information about which client causes the error. Therefore, it can be very time consuming to troubleshoot this error, especially if it occurs only intermittently. If you cannot identify which client computer is likely causing the error, you may have to use network sniffing tools such as Network General's Sniffer or Microsoft's Network Monitor to capture the sniffer trace for further analysis.

Description	Error 17832
Help Text (contd.)	<p>The best approach is to check the following known issues first, and contact Microsoft SQL Server Support if none of following causes matches your case. Error 17832 can be caused by:</p> <ol style="list-style-type: none"> 1 A Windows 95 Winsock issue. A 16-bit Windows application using TCP/IP sockets may encounter this problem under Windows 95 in a slow network environment. The error is repeated numerous times in the errorlog. For more information, see the following article in the Microsoft Knowledge Base: Q164516 : INF: Error 17832 Caused by Blocking Timeout in 16-Bit Sockets 2 Some anti-virus software on named pipes clients. Typically, when you configure anti-virus software to scan all files, named pipes (which are considered files) may be affected adversely. In this case, named pipes may be opened in invalid mode, causing these errors on the server side. To correct this problem, uninstall the anti-virus software to verify that this is indeed the case, and contact the software vendor for information on how to disable the auto-scanning of named pipes. 3 The use of the 32-bit ODBC driver for 16-bit Windows application under Windows 95. The 32-bit ODBC driver for SQL Server is not supported for use with 16-bit applications under Windows 95. The error occurs repeatedly in the errorlog for the duration of client login. For more information, see the following article in the Microsoft Knowledge Base: Q140697 : INF: Win16 ODBC Applications in a Win32 Environment 4 Insufficient system resources on the client side. If a client's request for opening connections fails due to insufficient resources on the client computer, the open connection function returns with an error status, and no login packets are sent as a result, causing these errors. For more information on this known issue, see the following article in the Microsoft Knowledge Base: Q161169 : BUG: 'Too Many Open File Handles' Error Using Named Pipes

Description	Error 17832
Help Text (contd.)	<p>5 Insufficient system resources on the server side. If SQL Server, the Windows NT operating system, or network services cannot allocate enough resources to complete new connections, the connections are reset by server, thereby causing these errors to occur. For more information on this known behavior, see the following article in the Microsoft Knowledge Base: Q154628 : INF: SQL Logs 17832 With Multiple TCP\IP Connection Requests</p> <p>6 A client interruption in the middle of a login process. If a client application does not wait until the login process finishes, and either the application is stopped or the client computer is restarted, this error may occur each time such an abnormal termination happens.</p> <p>7 An ODBC application that times out. There is a small window of opportunity in the SQL Server ODBC driver that may cause these errors when the ODBC application times out. Typically this error occurs when the application's timeout setting is just a small bit longer than the actual time it takes to complete the login process.</p> <p>8. Some routers' configurations in a routed network not allowing bigger data packets to go through properly. This is often caused by incorrect router configurations, 'black hole' routers, or unreliable networks such as RAS connections. For TCP/IP networks, you can generally use the TCP/IP PING utility with the '-l' parameter to test this case, but more complex issues may require the use of network sniffing tools to analyze the bottleneck.</p>
Help Text (contd.)	<p>For more information on some relevant issues, see the following articles in the Microsoft Knowledge Base: Q159211 : Diagnoses and Treatment of Black Hole Routers Q136970 : PMTU Black Hole Detection Algorithm Change for Windows NT 3.51</p> <p>9. The Network being too slow or unreliable. In a WAN or heavily routed network, it may take many retransmissions to deliver a large data packet successfully. If such a delivery of SQL Server login packets takes more than 45 seconds, this error will occur every time. The only solution in this case is to tune or upgrade the network; otherwise, the network is too slow for any meaningful SQL Server applications.</p> <p>For more information, use the following URL to search the Microsoft Knowledge Base for this error: http://search.microsoft.com/search/results.aspx?&st=a&qp=SQL+Server&qu=Error+17832</p> <p>Disclaimer: Clicking on a URL in the above text may take the user to a non-HP site. HP does not control the content of any non-HP site.</p>

MSS-Error 18204

Description	Error 18204
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause: Backup device is failed. This error message usually occurs as a result of incorrect permissions to the network drive.</p> <p>Suggested Action: To enable backups to network drives, check for MSSQL Service. MSSQLServer service should be started under a domain account and that account should have write access to Windows NT Server share name along with its partitions underlying it.</p>

MSS-Error 20554

Description	Error 20554
Severity	Minor
Message Group	MSS_Fault
Help Text	<p>Probable Cause: There is no response from the agent for last several minutes. This may be because of an unresponsive agent or high system activity.</p> <p>Suggested Action:</p> <ol style="list-style-type: none">1 Verify records replication at destination end.2 Check connection between Subscriber, Distributor and Publisher.

MSS-Error 20557

Description	Error 20557
Severity	Minor
Message Group	MSS_Fault
Help Text	<p>Probable Cause: Agent shuts down.</p> <p>Suggested Action: For more information, see the SQL Server Agent job history for job '%s'.</p>

Catch all errors in the agent file

Description	Catch all errors in the agent file
Severity	Warning
Message Group	MSS_Fault
Help Text	Probable Cause: A message with a warning indicator '!' was detected in the SQL Server Agent logfile. Suggested Action: Examine the error and use the SQL Server reference manuals to determine the exact cause and action to take.

SQL Server is terminating...

Description	Server is terminating
Severity	Warning
Message Group	MSS_Fault
Help Text	Probable Cause: The server is terminating. This could be a normal shutdown via the Service Control Manager. Suggested Action: Look at the tail end of the MS SQL Server logfile located in the Annotations of this browser message for more details. The Annotations will contain the last 200 lines of the logfile. If this is a normal shutdown via the Service Control Manager, then this message can likely be ignored unless the shutdown is unexpected.

SQL Server is starting...

Description	Server is starting
Severity	Warning
Message Group	MSS_Admin
Help Text	Probable Cause: The server is starting. This could be a normal startup via the Service Control Manager. Suggested Action: If this is a normal startup, no action is necessary.

MSS-Error Message above severity 19

Description	MS SQL Server Error Message above severity 19
Severity	Critical
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <p>There are many messages that have severity 20 or greater that should be alarmed.</p> <p>These errors range from corrupted databases, to hardware or OS problems.</p> <p>Suggested Action:</p> <p>Look at the tail end of the MS SQL Server logfile located in the Annotations of this browser message for more details. Then see the manual or CD to look up the error message and follow the explanation to determine the cause and resolution. The Annotations will contain the last 200 lines of the logfile.</p>

MSS-Error between severity 17 and 19

Description	MS SQL Server Error Message between severity 17 and 19
Severity	Major
Message Group	MSS_Fault
Help Text	<p>Probable Cause:</p> <p>There are hundreds or thousands of messages that have severity between 17 and 19 that should be alarmed.</p> <p>Suggested Action:</p> <p>Look at the tail end of the MS SQL Server logfile located in the Annotations of this browser message for more details. Then see the manual or CD to look up the error message and follow the explanation to determine the cause and resolution.</p> <p>The Annotations will contain the last 200 lines of the logfile.</p>

Scheduled Task Policies

The Scheduled Task policy commands run on the managed nodes at a regular interval to collect metric data and send a message to the management server to indicate the success or failure of the command. Use these policies if you want to run commands on one or more managed nodes—once or according to a specific schedule.

The following table lists all the Microsoft SQL Server Scheduled Task policies:

Policy Name	Description	Metrics
DBSPI-MSS-15min-PerfMon	Runs the MSSQL DBSPI performance collector every 15 mins with performance metrics.	M403, M404, M411
DBSPI-MSS-UDM-05min	Runs the MSSQL DBSPI collector/analyzer every 05 minutes.	37XX
DBSPI-MeasureWare	DBSPI MeasureWare Data Feed (every 5 minutes)	N/A
DBSPI-MSS-05min	Runs the MS SQL Server DBSPI collector/analyzer every 5 minutes.	M011, M 13 - M014, M025, M057, M058, M227, M030, M035, M81, M84, M277
DBSPI-MSS-15min	Runs the MS SQL Server DBSPI collector/analyzer every 15 minutes	M082, M83, M85 -M088, M230, M278, M279
DBSPI-MSS-1d	Runs the MS SQL Server DBSPI collector/analyzer once per day	M233, M234
DBSPI-MSS-1h	Runs the MS SQL Server DBSPI collector/analyzer every 1 hour	M001, M007 - M009, M017, M022 - M024, M026, M028, M032, M051 - M056, M064, M066 - M076, M209, M215, M218, M264, M266 - M267, M270 - M273
DBSPI-MSS-1d-Reporter	Runs the MSSQL DBSPI collector/analyzer once per day with Reporter metrics	M240, M241, M242, M244
DBSPI-MSS-05min-Reporter	Runs the MSSQL DBSPI collector/analyzer every 5 min with Reporter metrics	M243

2 Microsoft SQL Server Tools, Reports, and Graphs

This chapter provides Microsoft SQL Server specific information on Tools, Reports, and Graphs. For information on launching tools, configuring DB SPI to generate reports and graphs, and other DB SPI common topics, see the *HP Operations Smart Plug-in for Databases Installation and Configuration Guide*.

Tools

The DB SPI includes tools that apply to all databases, and tools that apply to the specific database you are using.

The DB SPI common tools are located under:

- *Tool Bank* → *DB-SPI* → *Admin* (for UNIX nodes)
- *Tool Bank* → *DB-SPI* → *Admin Windows* (for Windows nodes)

For more information on common tools, see the *HP Operations Smart Plug-in for Databases Installation and Configuration Guide*.

Microsoft SQL Server SPI specific tools are located under **Tool Bank** → **DB-SPI** → **MS SQL**.

The Microsoft SQL Server collector command is `dbspicam`.

The following table lists Microsoft SQL Server tools. you must assign the tools to HPOM operators to enable them to run the tools:

Table 1 Microsoft SQL Server SPI tool

Tool	Description	Command
Active Jobs	Shows all jobs that are active	<code>dbspimjp.bat</code>
All Jobs	Shows all active jobs as well as those idle and suspended, and completing	<code>dbspimja.bat</code>
NT Services	Shows NT services running	<code>dbspialm ntservice</code>
Start/Stop/List Instance	Starts, stops, or lists a specified Microsoft SQL Server database instance	<code>dbspialm listi</code> <code>dbspialm startinstance</code> <code><instance name></code> <code>dbspialm stopinstance</code> <code><instance name></code>

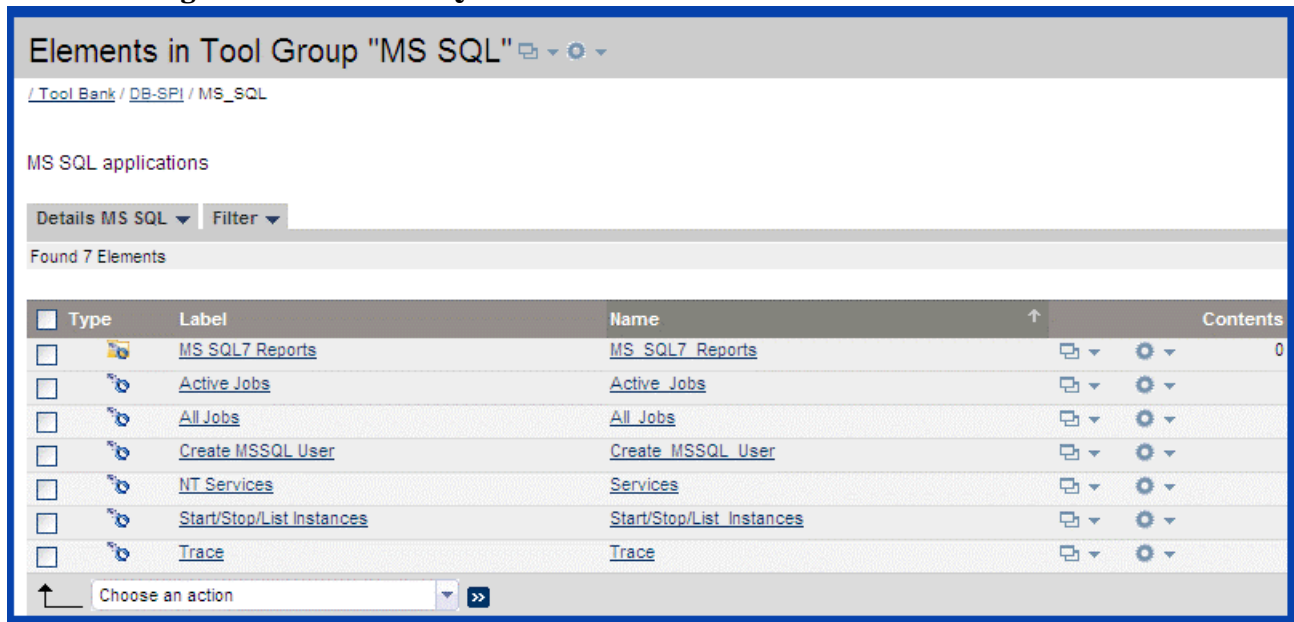
Table 1 Microsoft SQL Server SPI tool

Create MSSQL User	Allows user creation for the DB SPI to connect to the Microsoft SQL Server for monitoring purposes	dbspialm -mkusr <instance name> <username> <password>
	<p>Windows Authentication:</p> <p>dbspialm mkusr <server_name> <new_username> <new_password></p> <p>Example:</p> <p>dbspialm mkusr Sys1\INS1 test1 test1</p> <p>SQL Server Authentication:</p> <p>dbspialm mkusr <server_name> <new_username> <new_password> <SQLserver_username> <SQLServer_password></p> <p>Example:</p> <p>dbspialm mkusr Sys1\INS1 test1 test1 sa sa</p>	
Trace	Outputs the last 40 lines of the Microsoft SQL Server logfile	dbspialm trace

Microsoft SQL jobs through the "sp_help_job" command has a job status according to number of the current_execution_status column:

Value	Meaning
1	Executing
2	Waiting For Thread
3	Between Retries
4	Idle
5	Suspended
7	Performing Completion Actions

Figure 1 Microsoft SQL Server SPI Tools



Reports

HPOM generated reports cover *availability*, *size*, and *workload* of each managed nodes databases. Automatically generated every night, these web-based reports provide you with a routine means of checking the health and efficiency of specific databases.

By showing consolidated information, available otherwise only in pieces, reports provide you with a more complete view of how your database continues to perform over time.

The first reports are generated after HPOM runs through its first nightly schedule. From that point on, you can expect to see updated reports every day because HPOM, by default, re-generates reports every night with the day's data.

The following table lists DB SPI reports available from the HPOM console. The last four columns match those used by Reporter. In a few cases, a metric has different value IDs. For example, when Microsoft SQL metric M240_DBSize data is shown next to a value ID column with a number "1" in it, the data indicates "Megabytes Allocated"; data collected for the same metric next to a value ID column with a number "2" in it indicates "Megabytes Free."

Datasource name: DBSPI_MSS_REPORT

Specification file to create the datasource: dbspimosmg.sp

Database Instance name: <name of the database instance>

Table 2 Microsoft SQL Server Reports available from the HPOM Console

Report Name	Description	Reporter Table Columns			
		Metric id	Object id	Value id	Value
MS SQL Server Availability	Reports uptime information	M243	Server Instance Name		Up=5 Down=0
MS SQL Server Database Size	Database size in MB allocated and free	M240	Database Name	1	Megabytes Allocated
				2	Megabytes Free
MS SQL Server Table Size	Table size in MB allocated and free	M241	Table Name	1	Megabytes Allocated
				2	Megabytes Free
MS SQL Server Virtual Device Size	Virtual device size in MB allocated	M242	Virtual Device Name	1	Megabytes Allocated
				2	Megabytes Free
MS SQL Server Workload Sybase I/O	Number of physical reads and writes to the disk since the last collection for each tablespace.	M244	Server Instance Name		Delta of physical reads+writes since last collection
N/A, this metric is used only for data logging.		M279	File group name	1	Megabytes Allocated
				2	Megabytes Free

Table 2 Microsoft SQL Server Reports available from the HPOM Console

Report Name	Description	Reporter Table Columns			
		Metric id	Object id	Value id	Value
N/A, these metrics are used only for data logging.	Number of commands per second delivered to the Subscriber	M401	N/A, these metrics are stored in the graphing data source.		
	Number of transactions per second delivered to the Subscriber	M402			
	Number of rows per second replicated from the Publisher to the Subscriber	M405			
	Number of rows per second replicated from the Subscriber to the Publisher	M406			
	Number of commands per second delivered to the Distributor	M407			
	Number of transactions per second delivered to the Distributor	M408			
	Number of commands per second delivered to the Distributor	M409			
	Number of transactions per second delivered to the Distributor	M410			
MS SQL Server Sessions	Number of maximum number of sessions	M031	N/A, these metrics are stored in the graphing data source.		
MS SQL Server Transactions	Number of transactions	M009			

Table 2 Microsoft SQL Server Reports available from the HPOM Console

Report Name	Description	Reporter Table Columns			
		Metric id	Object id	Value id	Value
MS SQL Server Active Message Severity	Message severities for unacknowledged messages as shown over extended time period.	N/A, these are HPOM on HP-UX, Linux, and Solaris reports.			
MS SQL Server History Message Severity	Message severities for acknowledged messages as shown over extended time period.				
MS SQL Server Active Messages - Top 20	Top 20 unacknowledged messages at the time of report generation				
MS SQL Server History Messages - Top 20	Top 20 acknowledged messages at the time of report generation.				

Graphs

Graphs represent pictorial representation of the metrics. The following section provides information on Microsoft SQL Server-specific graphing metrics.

Metrics for Graphing or Alarming or Both

Some metric data may be used strictly for graphing purposes. You can determine if the metric is a graphing-only metric by viewing the [Microsoft SQL Server Metric Summary](#) on page 11, where you can find a column labeled “Graph”.

If this column contains an **A**, the metric generates a message whenever the metric value exceeds a threshold (alarm condition). If this column contains a **G**, the metrics logs the data to generate graphs.

Using Metrics for Graphing Only

You can avoid alarms or messages if you need the data only for graphing. To prevent alarms or messages from being generated, set the measurement threshold policy threshold for the metric to an extreme value (0 for Minimum metrics and 100 or higher for Maximum metrics). For example, for Microsoft SQL metric #0022, which measures cache hit ratio, you might choose to set the threshold to 0.0%. This minimum threshold setting (below which incoming data values would never drop) would allow you to receive and graph data while avoiding nuisance alarms.

Generic Datasource Graphing Metrics

The graphing data is stored in the DB SPI generic datasources. The following table lists the graphs and related metrics available in the Microsoft SQL Server SPI. For metric definitions see, [Chapter 1, Microsoft SQL Server Policies](#).

Datasource name: DBSPI_MSS_GRAPH

Specification file to create the datasource: dbspimssg.sp

Database Instance name: <name of the database instance>

Table 3 Graphs for Microsoft SQL Server Metrics

Graph Name	Metric Number
Data Access	M051, M052, M053, M054, M055, M056
Cache	M022
Errors	M023, M024, M028
IO Utilization	M003, M004, M005, M006, M007, M008, M021
Latches	M068, M069, M076
Locks and its Memory Utilization	M013, M075
Lock Requests	M070, M071, M072, M073
Least Recently Used	M001, M002
Read Ahead	M010, M012
Server Status	M017, M025, M029, M064, M074
Transactions	M009, M066
Server Status for processes and transactions	M014, M064
Users	M011, M026, M031

Generic Datasource Format

The generic datasource reserves a column for the database instance name, labeled INSTANCENAME. This column, then, contains the information that differentiates the data collected for each instance. Other columns represent the graphing metrics.

The following table is a sample of the Datasource Table. The complete list of all the graphing metrics is stored in the dbspimssg.fm file located at:

For Windows: <ovagentdir>\bin\instrumentation.

For HP-UX, Linux, and Solaris: /var/opt/OV/bin/instrumentation

Table 4 Format of Generic Datasource

INSTANCE NAME	M001_Cache HitPct	M002_CacheF reeBufPct	M003_LogLogi calIOAvg	...
<i><value></i>	<i><value></i>	<i><value></i>	<i><value></i>	<i><value></i>
<i><value></i>	<i><value></i>	<i><value></i>	<i><value></i>	<i><value></i>

A Golden Metrics

Golden metrics are a set of metrics which monitor the basic functionality of your database server. Golden metrics cover the critical areas such as database availability and details on server data access, database user statistics and database I/O utilization for which you would like to receive messages as a critical or major event happens on the database server. Implementing golden metrics and taking action against the events generated by these metrics ensure the smooth functioning of the database server.

Table 5 Golden Metrics

Metric Type	Metric
Availability	Metric M030_ServerConnect
	Metric M057_ServiceMon
	Metric M058_ServiceMon
	Metric M230_DBConnect
Server data access	Metric M051_FullScansRate
	Metric M052_IndxSearchsRate
	Metric M053_PgesAlloctdRate
	Metric M054_ExtntsAllocRate
	Metric M055_PageSplitsRates
	Metric M056_TblLckEscalRate
Database cache	Metric M022_BufChainAvgLen
Database error	Metric M023_ReadWriteErrCnt
	Metric M024_PacketErrorCnt
	Metric M028_SuspectDBCnt
Database I/O Utilization	Metric M007_ReadsOutstdRate
	Metric M008_WritsOutstdRate
Database latches	Metric M068_LatchWaitsRate
	Metric M069_AvgLatchWaitTim
	Metric M076_CurAvgLatchWait

Table 5 Golden Metrics

Metric Type	Metric
Database locks	Metric M013_LocksInUsePct
	Metric M070_LockTimeoutRate
	Metric M071_DeadlocksRate
	Metric M072_LocksWaitRate
	Metric M073_LockAvgWaitTime
	Metric M075_LockMemoryPct
General MS SQL	Metric M001_CacheHitPct
	Metric M014_BlckdProcessCnt
	Metric M017_CmdQueueLenPct
	Metric M025_CPUUsedPct
	Metric M064_DBActivTransCnt
	Metric M074_BatchReqstsRate
Database Transaction	Metric M009_TransactionRate
	Metric M209_TransactionRate
	Metric M066_DBLogGrowthsCnt
	Metric M266_DBLogGrowthsCnt
	Metric M035_LongTransaction
Database User Statistics	Metric M011_UserConnectPct
	Metric M026_ActiveConntnPet
Space	Metric M215_VirtDevSpUsdPct
	Metric M218_DBSpaceUsedPct
	Metric M278_FileGrpUsedSpacePct
	Metric M279_FileGrpSpaceFree
Jobs	Metric M277_CompletedJobs

Index

A

area, description of the logical area on which the metric focuses, 21

C

Catch all errors in the agent file, 124

collection interval, description of use in metric definitions, 20

D

description of metrics, defined, 20

G

golden metrics, 135

graphs, 132

metrics used for, not alarms/messages, 132

I

instruction text, description of, 21

L

Logfile text

SQL Server is starting..., 124

SQL Server is terminating..., 124

logfile text

MSS-Error Severity=>20, 108

M

MeasureWare, description of use in metric definitions, 20

message text, description of, 20

metric column key, 9

metrics

number ranges for SQL Server metrics, 20

those used for graphing/alarming, 132

metrics, version 7

M007_ReadsOutstdRate, 23

M008_WritesOutstdRate, 25

M011_UserConnectPct, 27

M013_LocksInUsePct, 29

M015_VirtDevSpUSdPct, 31

M017_CmdQueueLenPct, 36

M022_BufChainAvgLen, 38

M023_ReadWriteErrCnt, 39

M024_PacketErrorCnt, 40

M025_CPUUsedPct, 41

M026_ActiveConntnPct, 41

M051_FullScansRate, 53

M052_IndxSearchsRate, 54

M053_PgesAlloctdRate, 54

M054_ExtntsAllocRate, 56

M055_PageSplitsRates, 57

M056_TblLckEscalRate, 57

M064_DBActivTransCnt, 59, 60

M066_DBLogGrowthsCnt, 62

M067_DBLogShrinksCnt, 64

M068_LatchWaitsRate, 66

M069_AvgLatchWaitTim, 68

M070_LockTimeoutRatet, 68

M071_DeadlocksRate, 70

M072_LocksWaitRate, 72

M073_LockAvgWaitTime, 74

M074_BatchReqstsRate, 76

M075_LockMemoryPct, 78

M218_DBSpaceUsedPct, 36

M227_PhysIOByUsrPct, 43

M230_DBUseCnt, 46

M264_DBActivTransCnt, 62

M266_DBLogGrowthsCnt, 64

M267_DBLogShrinksCnt, 66

M270_LockTimeoutRate, 70

M271_DeadlocksRate, 72

M272_LocksWaitRate, 74

M273_LockAvgWaitTim, 76

Metric M014_BlckdProcessCnt, 29

Metric M028_SuspectDBCnt, 43, 45

Metric M032_RunableContnPct, 46

Metric M076_CurAvgLatchWait, 78

Metric M216_TransLogUsedPct, 33

Metric M233_DatabaseBackup, 48

Metric M233_TransactionLogBackup, 48

- metrics, version 7.0
 - M001_CacheHitPct, 22
- Metric Specification Description, 20
- metric summary, 11
- Microsoft SQL Server
 - reports generated by HP Reporter, 130
- MSS-Error14151, 114
- MSS-Error15457, 114
- MSS-Error 1608, 114
- MSS-Error 17-19, 123
- MSS-Error17824, 114
- MSS-Error17832, 118
- MSS-Error601, 96
- MSS-Error 602, 97
- MSS-Error 604, 98
- MSS-Error 605, 99
- MSS-Error9002, 106
- MSS-Error9004, 111
- MSS-Error Message severity>19, 108
- MSS-Error Severity=>20, 108

N

- names of metrics, description of format, 20

R

- reports, 129, 130
- report type, description of, 21

S

- scheduled task policies, 126
- severity, description of, 20
- SQL Server is starting..., 124
- SQL Server is terminating..., 124

T

- thresholds
 - description, 20
 - description of default field, 20
 - types, description of, 20
- tools, 127

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:

