Guide to Microsoft System Center Management Pack for SQL Server 2008 and 2012

Microsoft Corporation

Published: March 2019

The Operations Manager team encourages you to provide any feedback on the management pack by sending it to sqlmpsfeedback@microsoft.com.

Copyright

Contents

Guide to Microsoft System Center Management Pack for SQL Server 2008 and 2012

This guide is based on version 7.0.15.0 of the Management Pack for Microsoft SQL Server 2008, SQL Server 2008 R2 and SQL Server 2012.

Changes History

Release Date	Changes
March 2019 (version 7.0.15.0 RTM)	• Fixed issue “Keyword not supported: ‘ApplicationIntent'” in SQL 2008 MP
February 2019 (version 7.0.13.0 CTP)	• Fixed: “Total DB Space” monitor uses MB-values instead of %-values in its conditions • Add “Unavailable Time (seconds)” parameter to “SQL Server Agent Windows Service” monitor • Increased SQL Command Timeout up to 120 seconds in order to decrease timeout errors occasionally happen to DB Space workflows on heavily loaded servers • Updated all data sources so that SQL Server connections are established with read-only application intent • Changed the root folder name to “Microsoft SQL Server (old)”
June 2018 (version 7.0.7.0 RTM)	• Fixed issue: In some environments, DB Space workflows fail when a secondary database is non-readable • Fixed issue: The "The agent is suspect. No response within last minutes" alerting rule does not catch appropriate events due to a wrong source • Fixed issue: The "DB File Space" monitor in the SQL 2008 management pack throws error events due to the unnecessary $ character in its alert configuration
June 2018 (version 7.0.5.0 CTP)	• Updated the "Max worker thread count" data source of the corresponding monitor and performance rule • Fixed issue: the "Transaction Log Free Space (%)" monitor does not work

Release Date	Changes
April 2018 (version 7.0.4.0 RTM)	• Updated the "Security Considerations" section in the operations guide • Updated the default value of SP Level in the "Service Pack Compliance" monitor for SQL Server 2012 (SP 4) • Added the actual value of free space (% and MB) in the alert description of the "Transaction Log Free Space (%)" monitor (SQL 2012 only)
March 2018 (version 7.0.3.0 CTP)	• Fixed issue: Agent tasks do not have any SQL MP Run as Profile mapped • Implemented caching of data received from WMI to reduce the number of requests to WMI • Changed ps1 data source scripts to avoid the "Pipe is being closed" error • Disabled Latency Disk Read/Write performance rules by default • Added the actual value of available disk space in DB Space monitoring alerts • Updated some of the display strings • Increased SQL Command timeout in the data source scripts up to 60 seconds (previously it was 30 seconds)
February 2018 (version 7.0.2.0 RTM)	• Fixed issue: Always On data source scripts fail as Microsoft.SqlServer.Management.PSSnapins.dll is not imported • Fixed issue: Always On monitoring scripts may fail because of "No coercion operator is defined..." error (caused by an issue in PowerShell 5.0) • Fixed Dashboards issue: "DW data early aggregation" rule crashes on SCOM 2016
November 2017 (version 7.0.0.0 RTM)	• The version of the management pack was significantly increased as the SQL Server MP product family was extended with brand new management packs for SQL Server 2017+ and SQL Server 2017+ Replication. The new management packs are designed to monitor SQL Server 2017 and the upcoming versions. • Fixed issue: Invalid encoding of SQL instance names in Always On console tasks
October 2017 (version 6.7.34.0 CTP1)	• Reimplemented Always On workflows to enable monitoring of Availability Groups hosting over 200 databases

Release Date	Changes
	• Updated alert descriptions of Availability Group monitors: added cluster name and primary replica name • Implemented 3 alerting rules for events #5105 (error with physical file access), #833 (IO request has taken longer than 15 seconds), and #41144 (AO availability group failed); they are disabled by default • Added debug information to Always On monitoring scripts • Disabled the alerting rule for event #18456 by default • Fixed issue: Invalid encoding of SQL names in Always On console tasks
June 2017 (version 6.7.31.0 RTM)	• Improved performance of DB Space monitoring workflows • Added new "Login failed" alerting rule for SQL Server event #18456 • Updated the visualization library
May 2017 (version 6.7.30.0 CTP)	• Added new "Availability Database Backup Status" monitor in Availability Group to check the existence and age of the availability database backups (this monitor is disabled by default) • "Database Backup Status" monitor has been changed to return only "Healthy" state for the databases that are Always On replicas since availability database backups are now watched by the dedicated monitor • Fixed issue: "Active Alerts" view does not show all alerts • Fixed issue: DB space monitoring scripts fail with "Cannot connect to database" error. • Fixed issue: PowerShell scripts fail with "Cannot process argument because the value of argument 'obj' is null" error • Fixed issue: Alert description of "Disk Ready Latency" and "Disk Write Latency" monitors displays the sample count instead of the performance value that was measured • Fixed issue: Different file location info from "sys.master_files" and "sysfiles" causes error when

Release Date	Changes
	Availability Group secondary database files are in different path • Fixed issue: "DB Transaction Log Free Space Total" rules return wrong data • Introduced minor updates to the display strings
March 2017 (version 6.7.20.0 RTM)	• Fixed issue: GetSQL20XXSPNState.vbs fails when the domain controller is Read-Only • Fixed issue: SQL ADODB "IsServiceRunning" function always uses localhost instead of server name
February 2017 (version 6.7.16.0 CTP)	• Implemented some enhancements to data source scripts • Fixed issue: The SQL Server 2012 Database Files and Filegroups get undiscovered upon Database discovery script failure • Fixed issue: DatabaseReplicaAlwaysOnDiscovery.ps1 connects to a cluster instance using node name instead of client access name and crashes • Fixed issue: CPUUsagePercentDataSource.ps1 crashes with “Cannot process argument because the value of argument "obj" is null” error • Fixed issue: Policy field length is restricted to 256 symbols like help_link policy • Fixed issue: Description field of custom user policy cannot be discovered • Fixed issue: SPN Status monitor throws errors for servers not joined to the domain • Fixed issue: SQL Server policy discovery does not ignore policies targeted to system databases in some cases • Increased the length restriction for some policy properties in order to make them match the policy fields) • Actualized Service Pack Compliance monitor according to the latest published Service Packs for SQL Server
December 2016 (version 6.7.15.0 RTM)	• No extra permissions on remote WMI are now required for Local System account when Always On hosts have names that are no longer than 15 symbols

Release Date	Changes
	• Fixed: Always On discovery and monitoring scripts cannot read cached values in Windows registry • Fixed: Wrong MP version number in some Always On scripts • Fixed: CPUUsage and DBDiskLatency scripts fail with the reason: "Index operation failed" • Added retry policy in some Always On workflows to make PS-scripts work more stable • Updated the visualization library • Changed behavior of Always On scripts for cases when WSFC service is stopped
October 2016 (version 6.7.7.0 RTM)	• Fixed issue: SQL Server 2012 Always On discoveries fail after stopping WSFC service • Fixed issue: “Set DB offline” task does not work when the database is in Availability Group • Fixed issue: user policy discovery script fails with “Invalid namespace "ROOT\Microsoft\SqlServer\ComputerManagement12"' error • Fixed issue: Always On console task does not work • Updated the visualization library
September 2016 (version 6.7.5.0 CTP2)	• Added support for configurations where computer hostnames are longer than 15 symbols • Added “Event ID” to descriptions of all the alerts generated by the alerting rules • Deprecated “Run As Account does not exist on the target system, or does not have enough permissions” rule • Added 2 rules for alerts generating when there are problems with execution of the monitoring workflows scripts on the following agents: “MSSQL: Monitoring failed” and “MSSQL: Monitoring warning” • Added “MSSQL 20XX: Discovery warning” rules to generate alerts when there are non-critical problems with execution of the discovery scripts (warning events in the Operations Manager log) • Changed “MSSQL 20XX: Discovery failed” rules to generate alerts for only critical errors while executing discovery scripts

Release Date	Changes
	• Improved error logging in the MP scripts • Fixed some issues in the scripts, which could lead to unstable work with WMI • Updated the visualization library
August 2016 (version 6.7.3.0 CTP1)	• Added support for databases stored on SMB Shares • Fixed error logging in a script for Blocking Sessions monitor • Removed files of SQL 2005 MP from the installer since this MP is no longer supported • Fixed issue: CPU Usage monitor & rule did not work for SQL Server cluster instance • Fixed issue: connection to an SQL Server instance was not closing when the destination was wrong • Fixed Non-Readable Replica detection (Always On) • Made detection condition stricter for DB User Policy event-based discovery: added management group name • Made detection condition stricter for Script Failed alerting rule: added management group name
June 2016 (version 6.7.2.0 RTM)	• Added rules for alerting when an Availability Replica changed its role and/or a Database Replica changed its role • Created a group for WOW64 SQL Server instances and disabled launching of some workflows for these instances • Added MP version line into MP events generated by the scripts • Fixed the display strings and Knowledge Base articles • Fixed issue: some scripts were not returning data when one of the few installed instances was stopped • Fixed issue: SPN configuration monitor used stale data • Fixed issue: mirroring monitoring scripts were failing when the instance was stopped
June 2016 (version 6.7.1.0 CTP2.1)	• Updated the visualization library

Release Date	Changes
May 2016 (version 6.7.0.0 CTP2)	• Fixed Always On Database replica discovery incorrect behavior; fixed Always On policies discovery and monitoring • Fixed Database policies discovery and monitoring • Fixed and optimized CPU Usage monitoring scripts (the issue appeared when only one core was assigned) • Added support for more than 32 processors counts in CPU Usage monitoring. • SQLPS module is now used for the tasks instead of deprecated SQLPS.EXE • Implemented FILESTREAM filegroup monitoring • Multiple Ports are now supported in SQL Server TCP/IP parameters • Fixed error occurring when no port is specified in SQL Server TCP/IP parameters • Fixed filegroup read-only state discovery • Fixed Run As profiles mapping for some workflows • Implemented support for TLS 1.2 in connection logic • Implemented support for different client drivers in connection logic • Updated connection logic error logging • Added Run As profiles for mirroring monitors, fixed mirroring discovery issues • Fixed issue: CPU usage monitor ignored SQL server limitations on CPU core count • Fixed display strings and Knowledge Base articles • Fixed error reporting in the scripts
March 2016 (version 6.6.7.6 CTP1)	• Fixed intermittent "Cannot login to database" alert with some rules • Added support for SQL Express Instances • Updated Knowledge Base articles • Microsoft SQL Server 2012 x86 on Windows 2008 R2: fixed the issue when DB filegroups cannot be discovered • Win10 support: fixed "Cannot bind argument to parameter 'Path' because it is an empty string." issue

Release Date	Changes
	• Fixed issue when SQL Configuration Manager starts snap-in of the wrong version • Fixed invalid Always On non-readable replica detection
November 2015 (version 6.6.4.0)	• Updated the visualization library
November 2015 (version 6.6.3.0)	• Updated the visualization library • Fixed the error message in SQL DB discovery script
October 2015 (version 6.6.2.0)	• Added a support for disabled TCP/IP protocol • Fixed performance metrics error that may occur on some localized versions of Windows • Fixed issues in monitor tiles on SQL Server Summary Dashboard • Fixed incorrect performance of Transaction log free space monitor • Added new type of events from failed discoveries; added a new rule that collects such events • Added overrides to prevent various scripts timeout failure • Removed some 1X1 tiles from Summary Dashboards • FILESTREAM filegroups are excluded from discovery for now • 2008/2012 Summary Dashboards tiles were reorganized
June 2015 (version 6.6.0.0)	• Replaced the Dashboards with new ones • Components of replication functionality are deprecated and disabled by default • SPN monitor now correctly handles disjointed namespaces • Added support for filegroups containing filestreams and partition schemes • Memory Consumption monitor has been fixed • Upgradeability from 6.4.1.0 version is supported • Added CPU Usage monitor and rule for SQL Server 2005 • Added ConsecutiveSamples Condition to the Buffer Cache Hit Ratio and Page Life Expectancy monitors

Release Date	Changes
	• Always On discovery was reworked • Minor fixes
December 2014 (version 6.5.4.0)	• Added Mirroring monitoring scenarios for SQL Server 2012 product • SPN monitor now has overridable ‘search scope’, which allows the end user to choose between LDAP and Global Catalog • Fixed the error with blocked discovering DBs on Windows 2003 • Fixed Timeout error in CPU utilization monitoring scenario • Monitoring SQL Server Instances on the same server with their own network interfaces and default port is now available • SQL Server instances with underscores and other allowed special symbols in names can be monitored • Minor fixes.
June 2014 (version 6.5.1.0)	• New dashboards (instance level and database level) for both SQL 2008 and SQL 2012. • Integration with Microsoft SQL Server Presentation Management Pack, the folder, and views structure has been updated. • Support of localized performance counters (CPU and Disk metrics) has been added. • Monitors have been updated to use consecutive samples instead of the average sample value. • Removed SQL Default Action Run AS from Write Actions. • None-Default port is now supported • New property - Server Role Type • Performance collection rules have been updated to use none-optimized performance collection to improve the accuracy of daily and hourly-aggregated data. • Allways On Read-Intent error fixed, Read-Intent Monitoring is not supported. • Performance counter object name changed for a number of rules.

Release Date	Changes
	• Discoveries have been disabled for Analysis Services and Reporting Services. • Icons updated for a number of classes. • Minor fixes.
October 2013 (version 6.4.1.0)	• Fixed CPU Utilization Monitor • Fixed SQL Server seed discovery for WoW64 environments • The alert severity of Average Wait Time Monitor was changed to Warning, added consecutive sampling to reduce noise, threshold was changed to 250 • The alert severity of SQL Re-Compilation monitor was changed to Warning, the threshold was changed to 25. The monitor was disabled by default. • Minor fixes

September 2013 (version 6.4.0.0)	• New Dashboard for SQL Server 2012 DB
	• New Monitors and Rules – only for SQL 2008 and SQL 2012
	  ○ Collect DB Active Connections count
	  ○ Collect DB Active Requests count
	  ○ Collect DB Active Sessions count
	  ○ Collect DB Active Transactions count
	  ○ Collect DB Engine Thread count
	  ○ Thread Count monitor
	  ○ Transaction Log Free Space (%) monitor
	  ○ Transaction Log Free Space (%) collection
	  ○ Collect DB Engine CPU Utilization (%)
	  ○ CPU Utilization (%) monitor for DB engine
	  ○ Buffer Cache Hit Ratio monitor
	  ○ Collect DB Engine Page Life Expectancy (s)
	  ○ Page Life Expectancy monitor
	  ○ Collect DB Disk Read Latency (ms)
	  ○ Collect DB Disk Write Latency (ms)
	  ○ Disk Read Latency monitor
	  ○ Disk Write Latency monitor
	  ○ Collect DB Transactions per second count

Release Date	Changes
	○ Collect DB Engine Average Wait Time (ms) ○ Average Wait Time monitor ○ Collect DB Engine Stolen Server Memory (MB) ○ Stolen Server Memory monitor ○ Collect DB Allocated Free Space (MB) ○ Collect DB Used Space (MB) ○ Collect DB Disk Free Space (MB) ○ SQL Re-Compilation monitor • SPN monitor improved • Support for special symbols in DB names. • Improved Always On seed discovery • Run As configuration changes to support Low-privilege for SQL Server 2012 Cluster • Improved performance of Always On discovery • Custom User Policy Discovery and Monitoring performance optimization • Hided AG health object from Diagram view • Minor changes
August 2012 (version 6.3.173.1)	• Fixed DB Filegroup Free Space issue
February 2012 (version 6.3.173.0)	• Added support for SQL Server 2012 • Added support for SQL Server 2012 Always On Monitoring ○ Automatically discover and monitor availability groups, availability replicas, and database replicas for hundreds of computers. ○ Health roll-up from database replicas to availability replicas. ○ Detailed knowledge with every critical health state to enable faster resolution to a problem. • Seamless integration with Policy-Based Management (PBM) ○ Auto-discover custom PBM policies targeting Always On and database components.

Release Date	Changes
	○ Rollup of the health of policy execution within the SQL management pack under extended health. ○ SQL DB PBM monitoring is supported • Added support for SQL Server 2008 Mirroring monitoring (only applicable to SQL Server 2008 and 2008 R2 version of management pack) ○ Discover mirroring databases, witness, and mirroring group. ○ Monitor database mirror state, database mirror witness state, and mirroring partners' state. ○ Custom diagram view to visually represent the primary and the mirrored databases. • Added support for SQL Server 2008 Replication monitoring ○ Approximately twenty rules to detect replication events. • Free space monitoring was improved with mount point support. • Support for SCOM 2012. • Fixed the following issues: ○ Updated display strings for SQL 2008 MPs to match the same style ○ SEED discovery introduced for SQL 2008 and SQL 2012 MPs ○ Fixed DB Free space monitoring problems reports by customers ○ Fixed issue related to false alert when Full-text search component is not installed ○ Blocking sessions monitor has been fixed, now it shows head blocker in case of long queries ○ Optimized the SQL MP SQL queries to run more efficiently ○ Monitoring of Service Principal Name ○ Created a dedicated Group for all SQL components

Release Date	Changes
	○ Introduced Database Backup Status monitoring ○ Master DB location script now scans for parameters from registry ○ Minor fixes in Knowledge Bases and display strings
May 2011 (version 6.1.400.00)	• Documented association of Run As profiles and targets for account mapping. • Made minor fixes in string resources. • Made security improvements.
July 2010 (6.1.314.35)	• Removed DMO installation requirement. • Added support for SQL Server 2008 R2 and removed support for SQL Server 2000. • Made security improvements. • Documented settings for low-privilege environments. • Introduced new rules and monitors, updated existing rules and monitors, and improved Knowledge Base information. • Populated empty alert descriptions. • Improved database consistency check monitoring and introduced detailed configuration monitoring for the 'SQL Database' object. • Reconfigured space monitoring takes into account autogrowth settings and all levels of the storage hierarchy in SQL Server (DB File, DB Log File, DB Filegroup, and Database). • Fixed the following issues: ○ Filegroup discovery fails when Databases are excluded. ○ SQL DB Engine version is incorrect ○ "Last Run Status" monitor changes the states inappropriately. ○ SQL Agent Job Discovery fails when some job properties are NULL. ○ The default interval for the rule "Logins per second" is not compliant with MPBA.

Release Date	Changes
	○ Monitor “SQL Server Windows Service” turns to red state when service is restarting. ○ “Script: Failed to login” alert is triggered if service is unavailable. ○ DB files, DB filegroups, and DB Log files discoveries are not triggered consistently. ○ Frequently changed properties of DB affect performance of the monitored system. ○ Discovery intervals for “Discover Databases for a Database Engine”, “Discover Replication Components”, and “Agent job discovery” are not compliant with MPBPA. ○ Full Text Search Service Start/Stop tasks do not work on SQL 2008 Cluster. • Disabled the following monitors and rules to cut down noise: Monitors: ○ SQL Server Full Text Search Service ○ Blocking Sessions ○ Long Running Jobs ○ Auto Close Configuration ○ Auto Create Statistics Configuration ○ Auto Shrink Configuration ○ Auto Update Statistics Configuration ○ DB Chaining Configuration ○ DB Total Space ○ DB Space Percentage Change Rules: ○ SQL Server Service Broker or Database Mirroring Transport stopped ○ SQL Server Service Broker transmitter shut down due to an exception or a lack of memory ○ SQL Server Service Broker or Database Mirroring is running in FIPS compliance mode

Release Date	Changes
	○ The SQL Server Service Broker or Database Mirroring transport is disabled or not configured ○ An SQL Server Service Broker procedure output results ○ The Service Broker or Database Mirroring Transport has started ○ Process Worker appears to be non-yielding on Scheduler ○ IO Completion Listener Worker appears to be non-yielding on Node ○ An SQL job failed to complete successfully ○ IS Service has attempted to stop a running package • Deprecated the following monitors and rules: Monitors: ○ DB Space Free (MB) ○ DB Log File Space Free (%) ○ DB Log File Space Free (MB) ○ Disk Free Space Rules: ○ Collect Database Size (MB) ○ Collect Transaction Log Free Space (MB) ○ Collect Transaction Log Free Space (%) ○ Collect Transaction Log Size (MB) ○ An exception occurred while encrypting a message in the target queue ○ Could not find column in syscolumns for object in database ○ DBCC executed found and repaired errors ○ Cannot retrieve row from page by RID because the slotid is not valid ○ Could not retrieve row from page by RID because the requested RID has a higher number than the last RID on the page

Release Date	Changes
	○ The non-clustered index indicated by the index ID is in error ○ Table error: Page is allocated to different object found in page header
October 2009 (version 6.0.6648.0)	• Fixed an issue with all versions of the SQL MP, where event based workflows were not working on clustered instances of SQL that were clustered on the Windows Server 2003 operating system. In order for this fix to work fully on Windows Server 2003 and Windows Server 2008 operating systems, all agents on clustered nodes need to be running either Operations Manager 2007 R2, or Operations Manager 2007 SP1 with the update installed from Knowledge Base article 959865, Issues that are resolved by the Operations Manager Module rollup update for System Center Operations Manager 2007 Service Pack 1. For more information, see “Rules and monitors that are based on events from the event log do not work reliably on clustered installations of SQL” in Appendix: known issues and troubleshooting.
March 2009 (6.0.6569.0)	• Fixed performance issues caused by excessive CPU utilization and script timeouts from Windows Management Instrumentation (WMI) queries in the following management pack discoveries: Discover SQL Server 2005 Database Engines (Windows Server), Discover SQL Server 2005 Reporting Services (Windows Server), Discover SQL Server 2005 Analysis Services (Windows Server), Discover SQL Server 2008 Database Engines (Windows Server), Discover SQL Server 2008 Reporting Services (Windows Server), Discover SQL Server 2008 Analysis Services (Windows Server). • Fixed an issue where SQL Server 2005 and SQL Server 2008 Analysis Services and Reporting Services discoveries were not reliably discovering these objects on instances of SQL Server that did not have the Database Engine installed. • Removed the hard-coded exception in rules and monitors that prevented the monitoring of the System, Temp, and Master databases. • Improved the means by which database discoveries recognize autogrowth enabled settings. Database discoveries now recognize both “KB” and “%” growth

Release Date	Changes
	settings; previously the database discoveries recognized only the “KB” growth setting. • Corrected typographical errors in product knowledge and improved the quality of the text.
November 2008 (version 6.0.6460.0)	• The DB discovery script casts the values that correspond to “Database Size (MB) (Numeric)” and “Log Size (MB) (Numeric)” as INT, to avoid overflows exceptions within the script itself. • The DB discovery script checks for possible overflow on the “Database Size (MB) (Numeric)” and “Log Size (MB) (Numeric)” values and prevents those overflows from occurring. • The numeric properties of the database class are limited to 2147483647 MB (~2047 terabytes). In the event that a database or log file exceeds that size, the value will be set to the maximum possible value of 2147483647 MB to prevent overflows. In these instances, the “Database Size (MB) (String)” and “Log Size (MB) (String)” will support larger values.
October 2008 (version 6.0.6441.0)	General Changes: • The management pack now includes the SQL Server 2008 discovery and monitoring management packs. SQL Server 2008 monitoring is identical to the SQL Server 2005 Management Pack, including the new functionality added in this release for SQL Server 2005 monitoring. • Addressed issues with a few performance rules attempting to collect performance counters or instances by the wrong name • Updated a number of discoveries, rules, and tasks to ensure they use the correct Run As profiles for discovery and monitoring. • Updated the criteria on a number of event-based rules to make their criteria more specific to reduce alert volumes. • SQL DB Engine discovery will now work on systems that do not have the SQL tools installed. • The SQL Server 2005 Management Pack and SQL Server 2008 Management Pack support discovery

Release Date	Changes
	and partial monitoring of 32-bit instances of SQL components installed on 64-bit operating systems. This is discussed in more detail in the “Supported Configurations” section of this guide. • All monitors are now set to public accessibility, allowing increased customization. Most notably, custom diagnostics and recoveries can now be added. • The “Database Size” and “Log Size” properties of databases are now available as a numeric property, in addition to the string form of the property that already existed. • Updated knowledge of various reports. • Database snapshots are no longer discovered and monitored as if they were a full-fledged database. • The possible states of the “Blocking SPIDs” monitor in all management packs have been changed to better align with the default override behaviors. Previously, the monitor could either be in a “Success” or “Warning” state. The “Warning” state has been replaced with “Error”. Changes to the SQL Server 2000 Management Pack: • The default thresholds for the “Job Duration” have been revised. The numbers were previously an integer corresponding to minutes when it should have been in the format of HHMMSS. The knowledge for this monitor has been updated to more clearly explain the format of the threshold. • Changed the frequency at which the SAPasswordMonitor.vbs script is run from 24 seconds to 24 hours. Changes to SQL Server 2005 Management Pack: • Added monitoring for log shipping with the “Destination Log Shipping Monitor” and “Source Log Shipping Monitor” monitors. • Fixed a few typos and formatting issues with product knowledge in various places.

Release Date	Changes
March 2008	General Changes: • The “Transaction Log Space Free (%)” monitor was made public for both SQL Server 2000 and SQL Server 2005 to allow for further customization. • Some corrections were made and additional detail provided in the “Key Monitoring Scenarios” sections of this guide. • Removed the hard-coded exception for jobs with a specific name from the “A SQL job failed to complete successfully” rules for both SQL Server 2000 and SQL Server 2005. • Fixed an issue with the scripts used to calculate database free space, which was preventing some databases from having their free space correctly monitored on SQL installations that did not have databases with contiguous IDs. • Corrected typographical errors. Changes to the SQL Server 2000 Management Pack: • Fixed an issue where incorrect free space values were being calculated for some SQL Server 2000 databases. Changes to SQL Server 2005 Management Pack: • A fix was made to address issues with collection of performance data from specific instances of Analysis Services. • Significant changes were made to the “Database Status” monitor in the SQL Server 2005 Management Pack. The monitor now has three states reflecting good, bad, and neither. The possible database states have been realigned into these categories, which will reduce “false-positive” alert volumes specifically when log shipping and database backups are occurring.
December 2007	General Changes:

Release Date	Changes

	• Corrected typographical errors, missing display strings, and localization issues in all SQL Server Management Packs
	• Fixed an issue where incorrect values were being populated for “Category” and “Owner” of discovered SQL jobs
	• Updated the “SQL Server Configuration” report in both SQL Server Management Packs to take advantage of the respective version specific SQL DB Engine class
	• Fixed issues in the SetSQL2005DBState.js, GetSQL2000DBSpace.js and SetSQL2000DBState.js scripts
	
	Changes to the SQL Server 2000 Management Pack:
	• Renamed the SQL Server 2000 instance of the “GetSQL2005AgentJobStatus.vbs” script to “GetSQL2000AgentJobStatus.vbs” and updated the script to work with SQL Server 2000
	• Set the “SQL DB Engine Service Health Rollup” and “AD Helper Health Rollup” rollup monitors to be enabled by default
	• Fixed an issue with the state of the “User Connections Baseline” and “AD Helper Service Busy” monitors
	• Made the following monitors public to allow customization:
	  ○ “Auto Close Flag”
	  ○ “Auto Create Statistics Flag”
	  ○ “Auto Shrink Flag”
	  ○ “Auto Update Flag”
	  ○ “DB Chaining Flag”
	
	Changes to SQL Server 2005 Management Pack:
	• Added optimized performance collection rules for “Lock Waits/sec” and “Lock Requests/sec”

Release Date	Changes
	• Fixed a number of issues with the SQL Server 2005 database free space scripts • Fixed a number of issues with the SQL agent job discovery for SQL Server 2005 • Fixed a script that was resulting in invalid alerts being generated from the agent job's "Job Duration" monitor • Added missing SQL Server 2005 agent tasks on actions panel for SQL Agent Job State view • Added Locks:LockWaits and Locks:LockRequests to the SQL Server Lock Analysis report • Added support for discovery of push subscriptions

Supported Configurations

SQL Server Management Pack is designed for the following versions of System Center Operations Manager:

- System Center Operations Manager 2007 R2 (Except Dashboards)
- System Center Operations Manager 2012 SP1
- System Center Operations Manager 2012 R2
- System Center Operations Manager 2016
- System Center Operations Manager 1801
- System Center Operations Manager 2019

The following table details the supported configurations for the management pack:

Configuration	Support
SQL Server 2008 SQL Server 2008 R2 SQL Server 2012	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2014 Windows Server 2016 (for SQL Server 2012) • 64-bit SQL Server on 64-bit OS • 32-bit SQL Server on 32-bit OS **Note**: 32-bit SQL Server instances are not supported on 64-bit OS
Clustered servers	Yes
Agentless monitoring	Not supported
Virtual environment	Yes

We recommend that you monitor no more than 50 databases and 150 database files per agent to avoid spikes in CPU usage that may affect the performance of the monitored computers.

Agentless monitoring is not supported. The monitoring of clustered resources is supported.

For more information and detailed instructions on setup, configuration, and monitoring of clustered SQL Server resources, see Configuration for Monitoring Clustered Resources in Other Requirements section of this guide.

The current version of Management Pack provides monitoring of Mirroring SQL Server 2008, SQL Server 2008 R2, and SQL Server 2012.

Note that neither SQL Server Express edition (SQL Server Express, SQL Server Express with Tools, SQL Server Express with Advanced Services) support SQL Server Agent, Log Shipping, Always On, OLAP Services and Data Mining, Analysis Services and Integration Services.

In addition, SQL Server Express and SQL Server Express with Tools do not support Reporting Services and Full text search. However, SQL Server Express with Advanced Services support Full text search and Reporting Services with limitations.
All SQL Server Express editions support Database mirroring as Witness and Replication as Subscriber only.

SMB fileshares are supported as a storage option. For more information, see Description of support for network database files in SQL Server article.

Get Started

SQL Server Management Pack provides both proactive and reactive monitoring of Microsoft Server 2008, SQL Server 2008 R2 and SQL Server 2012 components, such as database engine instances, databases, and SQL Server agents.

The Authoring pane of the Operations Manager console can be used to enable discovery of these components.

The monitoring provided by this management pack includes availability and configuration monitoring, performance data collection, and default thresholds. You can integrate the monitoring of SQL Server components into your service-oriented monitoring scenarios.

In addition to health monitoring capabilities, this management pack includes dashboard views, extensive knowledge with embedded inline tasks, and views that enable near real-time diagnosis and resolution of detected issues.

For more information about enabling object discovery, see Object Discoveries in Operations Manager 2007 topic in the Operations Manager Help.

You can find SQL Server Management Pack at the System Center Operations Manager catalog (http://go.microsoft.com/fwlink/?LinkId=82105). The latest version of this document is available on Microsoft TechNet http://go.microsoft.com/fwlink/?LinkId=85414.

Before You Import the Management Pack

As a best practice, you should import Windows Server Management Pack for the operating system you are using. Windows Server Management Packs monitor aspects of the operating system that influence the performance of the computers running SQL Server, such as disk capacity, disk performance, memory utilization, network adapter utilization, and processor performance.

Files in this Management Pack

The following table describes the files included in this Management Pack.

File	Display name	Description
Microsoft.SQLServer.Library.mp	Microsoft SQL Server Core Library	Contains the object types and groups that are common to SQL Server 2008, SQL Server 2008 R2 and SQL Server 2012.
Microsoft.SQLServer.Visualization.Library.mpb	Microsoft SQL Server Visualization Library	Contains basic visual components required for SQL Server dashboards.
Microsoft.SQLServer.2008.Discovery.mp	Microsoft SQL Server 2008 (Discovery)	Contains definitions for object types and groups that are specific to SQL Server 2008 and SQL Server 2008 R2. It contains the discovery logic to detect all objects of the type defined on servers running SQL Server 2008 and SQL Server 2008 R2.
Microsoft.SQLServer.2008.Monitoring.mp	Microsoft SQL Server 2008 (Monitoring)	Provides all monitoring for SQL Server 2008 and SQL Server 2008 R2. **Note:** SQL Server 2008 and SQL Server 2008 R2 will not be monitored until you import this management pack.
Microsoft.SQLServer.2008.Mirroring.Discovery.mp	Microsoft SQL Server 2008	Contains definitions for object types and groups that are

File	Display name	Description
	Mirroring (Discovery)	specific to SQL Server 2008. It contains the discovery logic to detect all objects of the type defined on servers running SQL Server 2008 and SQL Server 2008 R2, which use Mirroring.
Microsoft.SQLServer.2008.Mirroring.Monitoring.mp	Microsoft SQL Server 2008 Mirroring (Monitoring)	Provides all monitoring for Mirroring in SQL Server 2008 and SQL Server 2008 R2. **Note:** Mirroring for SQL Server 2008 and SQL Server 2008 R2 will not be monitored until you import this management pack.
Microsoft.SQLServer.2012.Discovery.mp	Microsoft SQL Server 2012 (Discovery)	Contains definitions for object types and groups that are specific to SQL Server 2012. It contains the discovery logic to detect all objects of the type defined on servers running SQL Server 2012.
Microsoft.SQLServer.2012.Monitoring.mp	Microsoft SQL Server 2012 (Monitoring)	Provides all monitoring for SQL Server 2012. **Note:** SQL Server 2012 will not be monitored until you import this management pack.

File	Display name	Description
Microsoft.SQLServer.2012.Mirroring.Discovery.mp	Microsoft SQL Server 2012 Mirroring (Discovery)	Contains definitions for object types and groups that are specific to SQL Server 2012. It contains the discovery logic to detect all objects of the type defined on servers running SQL Server 2012, which use Mirroring.
Microsoft.SQLServer.2012.Mirroring.Monitoring.mp	Microsoft SQL Server 2012 Mirroring (Monitoring)	Provides all monitoring for Mirroring in SQL Server 2012. **Note:** Mirroring for SQL Server 2008 and SQL Server 2008 R2 will not be monitored until you import this management pack.
Microsoft.SQLServer.2012.AlwaysOn.Discovery.mp	Microsoft SQL Server 2012 Always On (Discovery)	Contains definitions for object types and groups that are specific to SQL Server 2012 Always On. It contains the discovery logic to detect all objects of the type defined on servers running SQL Server 2012 Always On.
Microsoft.SQLServer.2012.AlwaysOn.Monitoring.mp	Microsoft SQL Server 2012 Always On (Monitoring)	Provides all monitoring for SQL Server 2012 Always On **Note:**

File	Display name	Description
		SQL Server 2012 Always On (Availability Groups, Availability Replicas and Database Replicas) will not be monitored until you import this management pack.
Microsoft.SQLServer.2012.Presentation.mp	Microsoft SQL Server 2012 Presentation	SQL Server 2012 Presentation management pack. This management pack adds SQL Server 2012 Summary Dashboard.
Microsoft.SQLServer.2008.Presentation.mp	Microsoft SQL Server 2008 Presentation	SQL Server 2008 Presentation management pack. This management pack adds SQL Server 2008 Summary Dashboard.
Microsoft.SQLServer.Generic.Dashboards.mp	Microsoft SQL Server Generic Dashboards	Generic Dashboards Management Pack
Microsoft.SQLServer.Generic.Presentation.mp	Microsoft SQL Server Generic Presentation	Generic Presentation management pack.

The management pack also includes Microsoft Software License Terms, Datacenter Dashboard Guide and SQL Server Management Pack Guide.

Other Requirements

To run the SQL Management Studio task and the SQL Profiler task, you must have SQL Server Management Studio and SQL Server Profiler installed on all Operations Manager computers where these tasks will be used.

If you try to run one of these tasks without the appropriate features installed, you will receive "The system cannot find the file specified" error message.

You do not need SQL Server Management Studio or SQL Server Profiler for discovery and monitoring.

Configure the Monitoring Clustered Resources

To monitor clustered resources, perform the following tasks:

- Install the Operations Manager agent on each physical node of the cluster.
- Enable the Agent Proxy option on all agents installed on servers that are members of the cluster. For instructions, see the procedure that follows this list.
- Associate the Windows Cluster Action Account Run As profile with an account that has administrator permissions for the cluster, such as the Cluster service account that is created when you configure the cluster. If the Default Action Account Run As profile for cluster nodes is associated with Local System or with another account that has administrator permissions for the cluster, then no additional associations are required. For instructions on associating an account with a profile, see How to Change the Run As Account Associated with a Run As Profile in Operations Manager 2007 article.

> **Important :**
>
> All agents on clustered nodes need to be running Operations Manager 2007 R2, or Operations Manager 2007 SP1 with the update installed from Knowledge Base article 959865, Issues that are resolved by the Operations Manager Module rollup update for System Center Operations Manager 2007 Service Pack 1. For more information, see "Rules and monitors that are based on events from the event log do not work reliably on clustered installations of SQL" in Appendix: Known Issues and Troubleshooting.

Enable the Agent Proxy Option

In order to enable the Agent Proxy option, perform the following steps:

- Open the Operations Manager console and click the **Administration** button.
- In the Administrator pane, click **Agent Managed**.
- Double-click an agent in the list.
- On the Security tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**.
- Repeat steps 3 through 4 for each agent that is installed on a clustered server.

When the discovery occurs, each physical node of the cluster is displayed in the Operations Manager console in the **Agent Managed** pane; the cluster and each named application instance are displayed in the **Agentless Managed** pane.

> **Note:**
>
> Having a SQL Server cluster resource group that contains more than one network name resource might mean that the clustered SQL Server resource is not monitored.

To ensure proper monitoring of cluster resources, when you add a resource to a cluster, do not change the name that is assigned to the resource in the Cluster Administrator user interface by default.

Import the Management Pack

For more information about importing a management pack, see How to Import an Operations Manager Management Pack article.

To start monitoring, import the management pack files for your version of SQL Server: library, discovery, and monitoring.

SQL Server 2008 and SQL Server 2008 R2	
Library	Microsoft.SQLServer.Library.mp
Generic	Microsoft.SQLServer.Generic.Presentation.mp
Generic	Microsoft.SQLServer.Generic.Dashboards.mp
Discovery	Microsoft.SQLServer.2008.Discovery.mp
Monitoring	Microsoft.SQLServer.2008.Monitoring.mp
Library	Microsoft.SQLServer.Visualization.Library.mpb
Presentation	Microsoft.SQLServer.2008.Presentation.mp
SQL Server 2008 and SQL Server 2008 R2 Mirroring	
Library	Microsoft.SQLServer.Library.mp
Generic	Microsoft.SQLServer.Generic.Presentation.mp
Generic	Microsoft.SQLServer.Generic.Dashboards.mp
Discovery	Microsoft.SQLServer.2008.Discovery.mp
Discovery	Microsoft.SQLServer.2008.Mirroring.Discovery.mp
Monitoring	Microsoft.SQLServer.2008.Mirroring.Monitoring.mp
SQL Server 2012	
Library	Microsoft.SQLServer.Library.mp
Generic	Microsoft.SQLServer.Generic.Presentation.mp
Generic	Microsoft.SQLServer.Generic.Dashboards.mp
Discovery	Microsoft.SQLServer.2012.Discovery.mp
Monitoring	Microsoft.SQLServer.2012.Monitoring.mp

Library	Microsoft.SQLServer.Visualization.Library.mpb
Presentation	Microsoft.SQLServer.2012.Presentation.mp
SQL Server 2012 Mirroring	
Library	Microsoft.SQLServer.Library.mp
Generic	Microsoft.SQLServer.Generic.Presentation.mp
Generic	Microsoft.SQLServer.Generic.Dashboards.mp
Discovery	Microsoft.SQLServer.2012.Discovery.mp
Discovery	Microsoft.SQLServer.2012.Mirroring.Discovery.mp
Monitoring	Microsoft.SQLServer.2012.Mirroring.Monitoring.mp
SQL Server 2012 Always On	
Library	Microsoft.SQLServer.Library.mp
Generic	Microsoft.SQLServer.Generic.Presentation.mp
Generic	Microsoft.SQLServer.Generic.Dashboards.mp
Discovery	Microsoft.SQLServer.2012.Discovery.mp
Monitoring	Microsoft.SQLServer.2012.Monitoring.mp
Always On Discovery	Microsoft.SQLServer.2012.AlwaysOn.Discovery.mp
Always On Monitoring	Microsoft.SQLServer.2012.AlwaysOn.Monitoring.mp

Avoid Monitoring Noise

In order to avoid receiving excessive alerts and notifications while monitoring, perform the actions described below:

1. If you are upgrading from a previous version, export and save your current management pack with any customizations so that you can roll back the installation if needed.
2. Import the library file.
3. Define Run-As accounts.
4. Import the discovery file.
5. Make sure that the required objects are discovered. In case of security alerts, adjust Run As accounts. If the list of discovered objects is not as expected, enable or disable discovery for management groups.
6. Import the monitoring file.
7. Customize the management pack.

Create a New Management Pack for Customizations

SQL Server Management Pack is sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, the Operations Manager saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

- It simplifies the process of exporting customizations created in your test and pre-production environments to your production environment. For example, instead of exporting the default management pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.
- It allows you to delete the original management pack without first needing to delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If all of your customizations are saved to the default management pack, you must delete the default management pack before you can delete an original management pack.
- It is easier to track and update customizations to individual management packs.

For more information about management pack customizations and the default management pack, see Using Management Packs article.

How to Create a New Management Pack for Customizations

1. Open the Operations Manager console, and then click the **Administration** button.
2. Right-click **Management Packs,** and then click **Create New Management Pack**.
3. Enter a name (for example, ADMP Customizations), and then click **Next**.
4. Click **Create**.

Customize SQL Server Management Pack

The following recommendations may help reduce unnecessary alerts.

- If you are monitoring instances of SQL Server 2008 that do not have the SQL Server Full Text Filter Daemon Launcher service installed, disable the monitor **SQL Server Full Text Search Service Monitor**.
- Some monitors in this management pack check the state of services. These monitors have “Alert only if service startup type is automatic” parameter that is set to **True** by default, which means that it checks services that are set to start automatically. On servers in a cluster, the startup type for the services is set to manual. If you are monitoring a SQL Server cluster, change “**Alert only if service startup type is automatic**” parameter to **false** for the following monitors:
- SQL Server Windows Service (for SQL DB Engine)

- SQL Server Reporting Services Windows Service
- SQL Server Analysis Services Windows Service
- SQL Server Integration Services Windows Service
- SQL Server Full Text Search Service Monitor
- SQL Server Agent Windows Service

Optional Configuration

After you import SQL Server Management Pack, the navigation pane of the Monitoring pane displays the object types that are discovered automatically. For more information about object types, see Objects the Management Pack Discovers section. You can modify the default discovery configuration of objects discovered by SQL Server Management Pack. You should use the overrides feature of the Operations Manager to change the configuration settings.

For an object type that is not automatically discovered, you can enable the setting for automatic discovery in the Authoring pane in the Operations Manager console.

Use an Override to Change the Setting for Automatic Discovery:

1. In the **Authoring** pane, expand **Management Pack Objects**, and then click **Object Discoveries**.
2. On the Operations Manager toolbar, click **Scope**, and filter the objects that appear in the details pane to include SQL Server objects only.
3. In the details pane, click the object type for which you want to change the setting.
4. On the Operations Manager toolbar, click **Overrides**, click **Override the Object Discovery**, and then click either **For all objects of type:** <name of object type>, **For a group**, **For a specific object of type:** <name of object type>, or **For all objects of another type**.
5. In the **Override Properties** dialog box, click the **Override** box for the **Enabled** parameter you want to change.
6. Under **Management Pack**, click **New** to create an unsealed version of the Management Pack, and then click **OK**.

After you change the override setting, the object type is automatically discovered and available in the **Monitoring** pane under **Microsoft SQL Server**.

For more information about setting the overrides, see Tuning Monitoring by Using Targeting and Overrides article.

The following monitoring scenarios might require manual configuration. For the detailed information about these requirements, see the Key Monitoring Scenarios section.

- Database configuration monitoring
- DB File monitoring
- DB Filegroup monitoring
- Excluding databases from monitoring
- Excluding DB engine instances from monitoring
- Publication component monitoring
- Service pack compliance
- Subscription component monitoring

Security Considerations

As of the October 2009 release of SQL Server Management Pack package, agentless monitoring is no longer supported. This change was made to allow full support of monitoring for clustered resources.

You may need to customize your management pack. Certain accounts cannot be run in a low-privilege environment or must have minimal permissions.

The following topics are covered in this section:

Run As Profiles

When the SQL Server Core Library Management Pack is imported for the first time, it creates three new Run As profiles:

- SQL Server Default Action Account
- SQL Server Discovery Account (this account is associated with all discoveries)
- SQL Server Monitoring Account (this account is associated with all monitors and tasks)
- Always On Discovery Account (this account is used for script-based discovery of Always On objects)
- Always On Monitoring Account (this account is used for script-based monitoring of Always On objects)

By default, all discoveries, monitors, and tasks defined in SQL Server Management Packs use the accounts defined in the “Default Action Account” Run As profile. If the default action account for a given system does not have the necessary permissions to discover or monitor the instance of SQL Server, then those systems can be bound to specific credentials in the SQL Server Run As profiles, which do have access.

For Always On monitoring, the Run As configuration is a subset of required configuration for SQL Server monitoring. Therefore, it is not required to explicitly configure Run As profiles for Always On, just perform the following steps:

- Map Always On Discovery Account profile to the same Action Account you use for SQL Server Discovery Account profile;
- Map Always On Monitoring Account profile to the same Action Account you use for SQL Server Monitoring Account profile.

How to Configure Run As Profiles

One of the Run As Profile Configuration scenarios below — where we describe how to configure and use Service Security Identifier — was first published by Kevin Holman in his blog. The original article is available here. The SQL scripts to configure the lowest-privilege access were also developed by Kevin.

To configure Run As profiles, follow one of the scenarios described below:

1. Default Agent Action Account is mapped to Local System, and you are going to use Service Security Identifier (SID) to enable SQL Server MP Workflows to access SQL Server instances. You can read more about this option in SQL Server uses a service SID to provide service isolation and How to configure SQL Server 2012 to allow for System Center Advisor monitoring articles. Follow the next steps to configure your security configuration with SID:
    a. Allow using a service SID for HealthService as it is described in How to allow a Service Security Identifier for the HealthService.
    b. If you have SQL Server Cluster instances, make sure to take the steps described in How to Configure the HealthService Service SID for Monitoring SQL Server Cluster Instances section.
    c. Create the login “NT SERVICE\HealthService” for the HealthService SID in every SQL Server and grant it with the SQL Server System Administrator rights (hereinafter—SA rights). If you cannot grant it with the SA rights for the security policy reason, then skip this step and go the next one.
    d. Take this step only if you cannot take step “c”. Use the SQL scripts provided in How to Grant the HealthService SID with the Minimal Required Rights to SQL Server section to set up the lowest privilege configuration for the account.
2. Default Agent Action Account—mapped to either Local System or a domain account—has both Local Administrator rights on the operating system and SA rights. In this case, monitoring of SQL Server instances will work out of the box, except for some configurations described below. Please follow these steps to ensure that all requirements are met:
    a. In case when servers hosting Always On Availability Replicas (at least one of them) have the machine name longer 15 symbols, make sure to take steps described in How to Configure Permissions for Always On Workflows when Servers Have Machine Names Longer than 15 Symbols section.
    b. If you store SQL Server databases on an SMB file share, make sure that Default Agent Action Account has the rights described in the corresponding Low-Privilege Configuration section.
3. Default Agent Action Account—mapped to either Local System or a domain account—cannot be granted with the SA rights, as long as the security policy prohibits granting the SA rights to the Default Agent Action Account. If the security policy permits to grant the SA rights to a separate Domain User account, which will be used for launching SQL Server MP Workflows only, perform the following steps:
    a. Create a new Domain User account and add this account to Local Administrators group on each monitored server.

b. Grant the SA rights to this account in SQL Server.
c. Create a new Action account in SCOM and map it to the Domain User account created above.
d. Map the new Action account to all SQL Server MP Run As Profiles.
e. While configuring SQL Server Always On Availability Groups for monitoring, despite granting Local Administrator rights to the new Action account, make sure this account has permissions described in How to Configure Permissions for Always On Workflows when Servers Have Machine Names Longer than 15 Symbols section.
f. If you store SQL Server databases on an SMB file share, make sure that your Domain User account has the rights described in the corresponding Low-Privilege Configuration section.

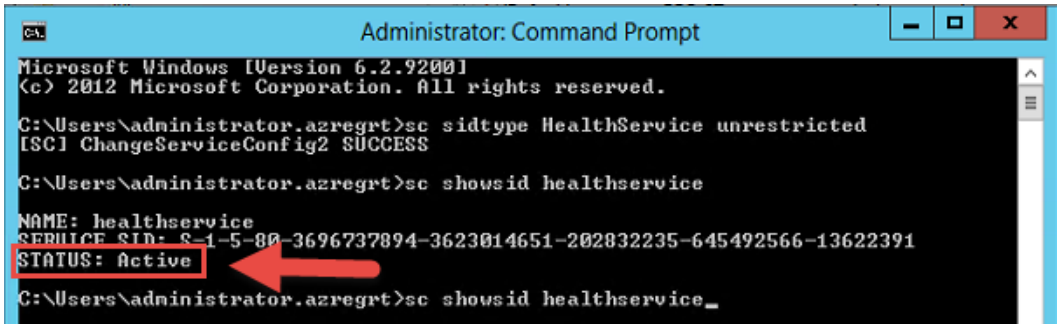
4. In case you need to run SQL Server MP Workflows with the minimal required rights, follow the instructions in Low-Privilege Environments section.

How to Allow a Service Security Identifier for the HealthService

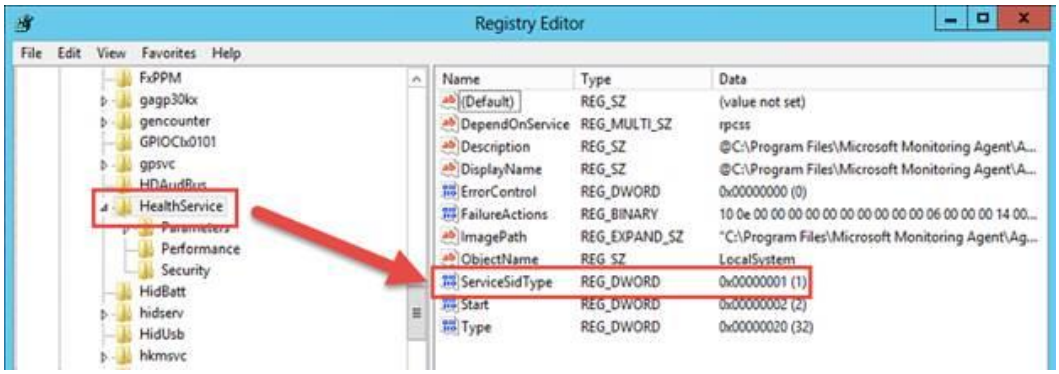
The steps below should be taken on every server hosting SQL Server to be monitored.

1. Open Command Prompt as Administrator and run "*sc sidtype HealthService unrestricted*" query; then, restart "Health Service".

2. Open Command Prompt as Administrator and run the next query: "*sc showsid HealthService*". The service "STATUS" should be "Active":



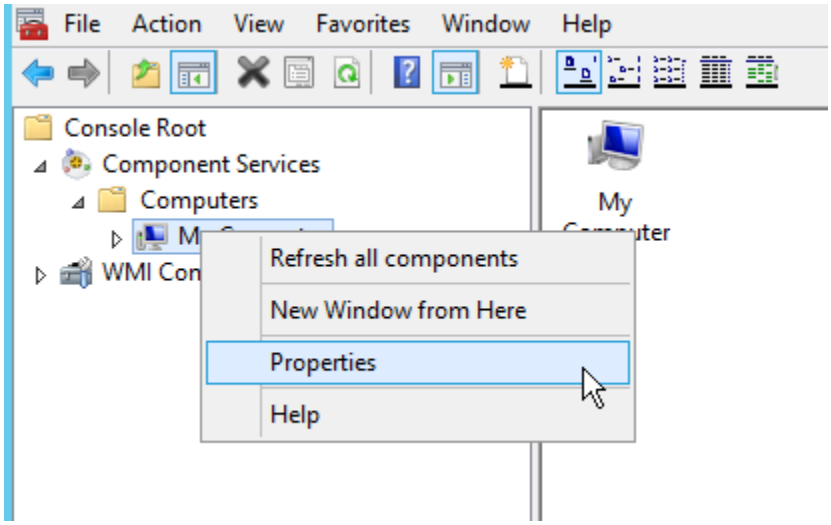
3. Open "Registry Editor". Check that "*ServiceSidType*" key has "1" value at "*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService*".



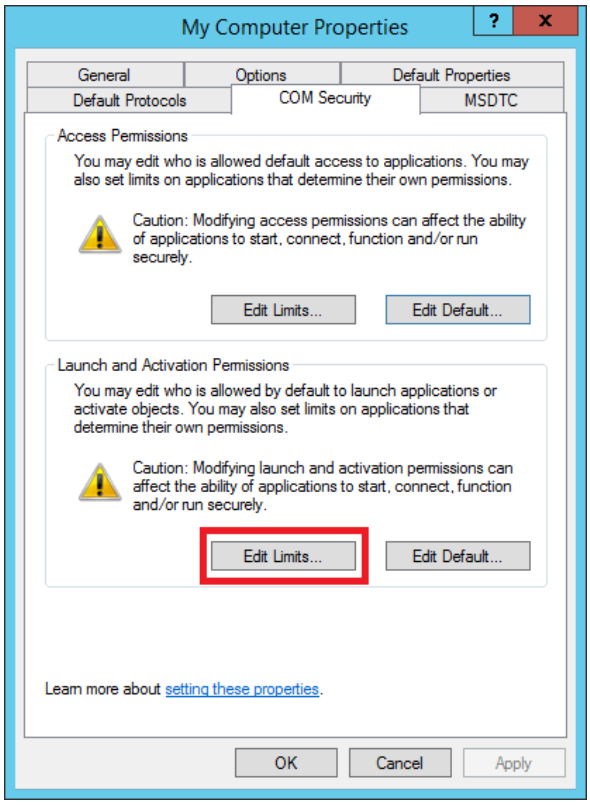
How to Configure the HealthService Service SID for Monitoring SQL Server Cluster Instances

To configure HealthService Service SID for monitoring SQL Server Failover Cluster, perform the following steps at each cluster node:

1. Launch mmc.exe and add the following two Snap-Ins:
   - **Component Services**
   - **WMI Control** (for local computer)
2. Expand **Component Services**, right-click **My Computer** and click **Properties**; the corresponding dialog menu will be displayed:

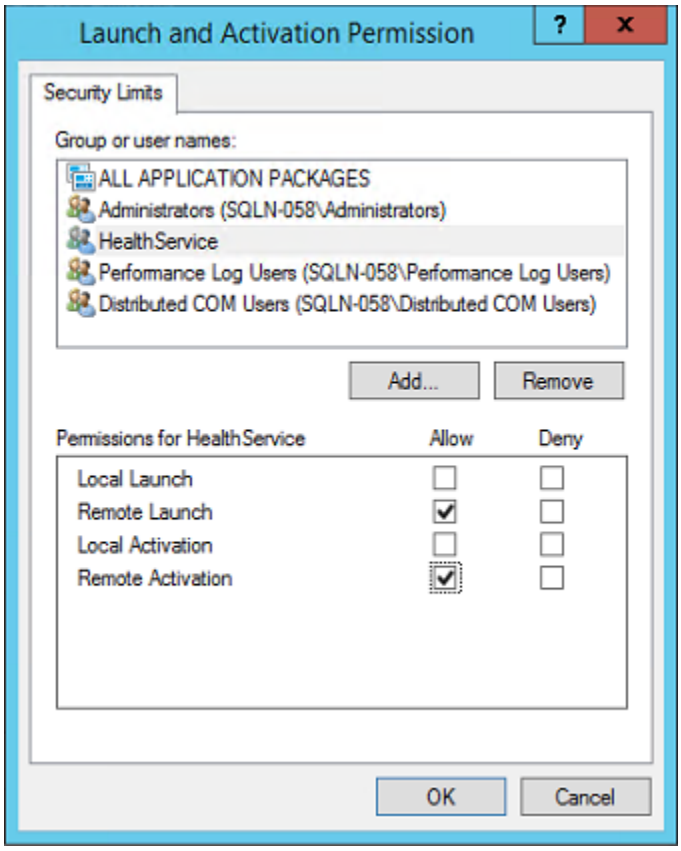


3. In this dialog menu, go to **Security** tab.
4. Click the **Edit Limits** button in **Launch and Activation Permissions** section; the corresponding dialog menu will be displayed:

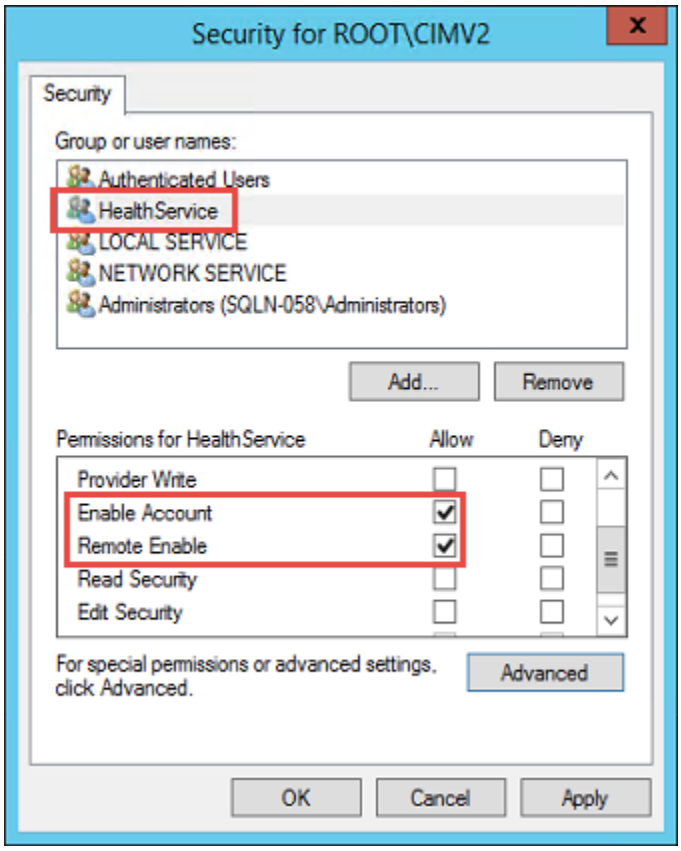


5. In this dialog menu, set the following permissions for the “NT SERVICE\HealthService” account:

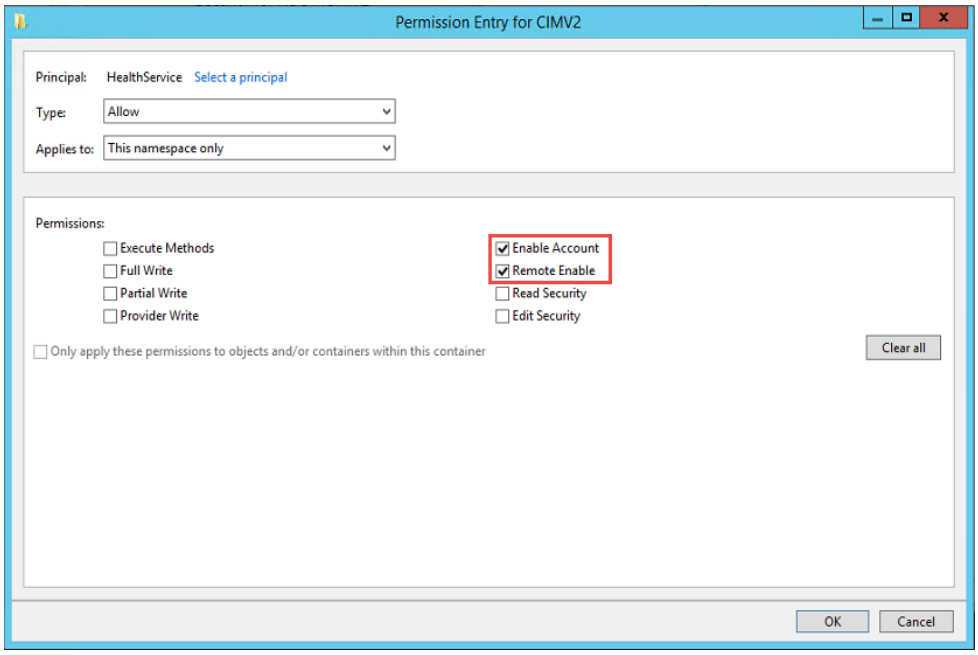
    - **Remote Launch**
    - **Remote Activation**



6. Go to **WMI Control** snap-In and call its properties; the corresponding dialog menu will be displayed.
7. In this dialog menu, go to **Security** tab, select **Root\CIMV2** namespace and click the **Security** button.
8. Add the following permissions for the “NT SERVICE\HealthService” account:
    - **Enable Account**
    - **Remote Enable**



9. Click the **Advanced** button; the corresponding dialog menu will be displayed.
10. In this dialog menu, select the “HealthService” account and click the **Edit** button.
11. In the following dialog menu, make sure that **Applies to** parameter is set to **This namespace only** value, and the following permissions are set:
    - **Enable Account**
    - **Remote Enable**



How to Grant the HealthService SID with the Minimal Required Rights to SQL Server

Run the following script in every SQL Server 2008 instance to be monitored:

```
SET NOCOUNT ON;
DECLARE @accountname nvarchar(128);
DECLARE @command1 nvarchar(MAX);
DECLARE @command2 nvarchar(MAX);
DECLARE @command3 nvarchar(MAX);
SET @accountname = 'NT SERVICE\HealthService';
SET @command1 = 'USE [master];
CREATE LOGIN ['+@accountname+']
FROM WINDOWS WITH DEFAULT_DATABASE=[master];';
SET @command2 = '';
SELECT @command2 = @command2 + 'USE ['+name+'];
CREATE USER ['+@accountname+']
FOR LOGIN ['+@accountname+'];'
FROM sys.databases db
WHERE db.database_id <> 2
AND db.user_access = 0
AND db.state = 0
AND db.is_read_only = 0;
SET @command3 = 'USE [master];
GRANT VIEW ANY DATABASE TO ['+@accountname+'];
GRANT VIEW ANY DEFINITION TO ['+@accountname+'];
GRANT VIEW SERVER STATE TO ['+@accountname+'];
GRANT SELECT on sys.database_mirroring_witnesses to ['+@accountname+'];
USE [msdb];
```

```
EXEC sp_addrolemember @rolename=''PolicyAdministratorRole'',
@membername='''+@accountname+''';
EXEC sp_addrolemember @rolename=''SQLAgentReaderRole'',
@membername='''+@accountname+''';';
EXECUTE sp_executesql @command1;
EXECUTE sp_executesql @command2;
EXECUTE sp_executesql @command3;
```

For SQL Server 2012 instances, run the script below:

```
SET NOCOUNT ON;
DECLARE @accountname nvarchar(128);
DECLARE @command1 nvarchar(MAX);
DECLARE @command2 nvarchar(MAX);
DECLARE @command3 nvarchar(MAX);
SET @accountname = 'NT SERVICE\HealthService';
SET @command1 = 'USE [master];
CREATE LOGIN ['+@accountname+']
FROM WINDOWS WITH DEFAULT_DATABASE=[master];';
SET @command2 = '';
SELECT @command2 = @command2 + 'USE ['+db.name+'];
CREATE USER ['+@accountname+']
FOR LOGIN ['+@accountname+'];'
FROM sys.databases db
left join sys.dm_hadr_availability_replica_states hadrstate
on db.replica_id = hadrstate.replica_id
WHERE db.database_id <> 2
AND db.user_access = 0
AND db.state = 0
AND db.is_read_only = 0
AND (hadrstate.role = 1 or hadrstate.role is null);
SET @command3 = 'USE [master];
GRANT VIEW ANY DATABASE TO ['+@accountname+'];
GRANT VIEW ANY DEFINITION TO ['+@accountname+'];
GRANT VIEW SERVER STATE TO ['+@accountname+'];
GRANT SELECT on sys.database_mirroring_witnesses to ['+@accountname+'];
USE [msdb];
EXEC sp_addrolemember @rolename=''PolicyAdministratorRole'',
@membername='''+@accountname+''';
EXEC sp_addrolemember @rolename=''SQLAgentReaderRole'',
@membername='''+@accountname+''';';
EXECUTE sp_executesql @command1;
EXECUTE sp_executesql @command2;
EXECUTE sp_executesql @command3;
```

How to Configure Permissions for Always On Workflows when Servers Have Machine Names Longer than 15 Symbols

Please note that regardless of the used account (Local System or a Domain User account) and the method of rights granting, you should make sure that the account has the permissions listed

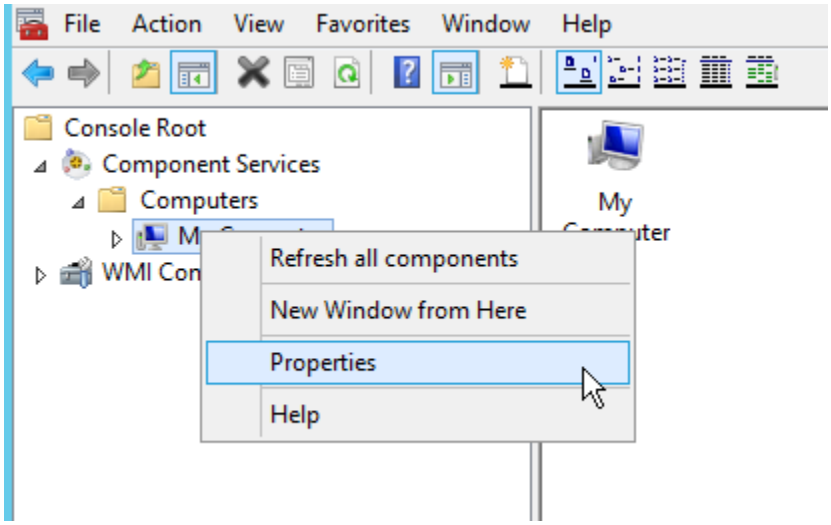
below. The process of obtaining permissions is described below as a case when Local System account is used for monitoring.

Example: You have three replicas in your Availability Group, which are hosted on the following computers: comp1, comp2 and comp3. At that, comp1 hosts the primary replica. In this case, you should configure security settings for comp1 on comp2 and comp3 computers.

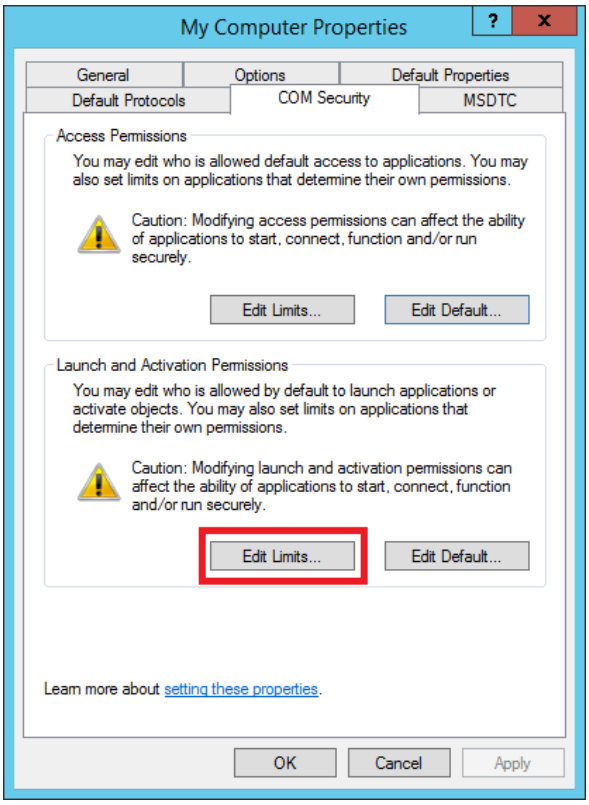
Note: If comp2 would host primary replica (after failover), other computers should also have configured WMI security for this computer. In general, you have to make sure that Local System account of each node, which can act as Primary one, have WMI permissions for the other nodes of the current Availability Group. The same is true for the Domain Action Account used for monitoring.

Therefore, below are the steps to configure security for configurations with Local System account (please note that in the provided instruction it is considered that SQLAON-020 computer hosts the primary replica).

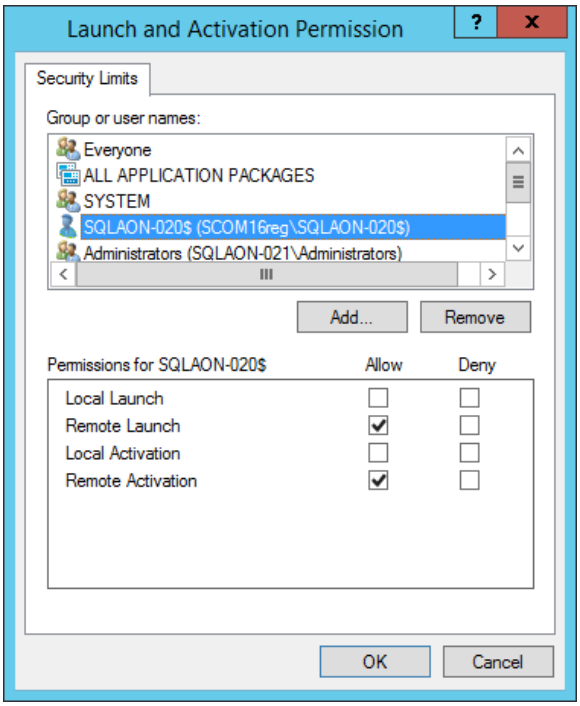
1. Launch mmc.exe and add two Snap-Ins:
    - **Component Services**
    - **WMI Control** (for local computer)
2. Expand **Component Services**, right-click **My Computer** and click **Properties**; the corresponding dialog menu will be displayed.



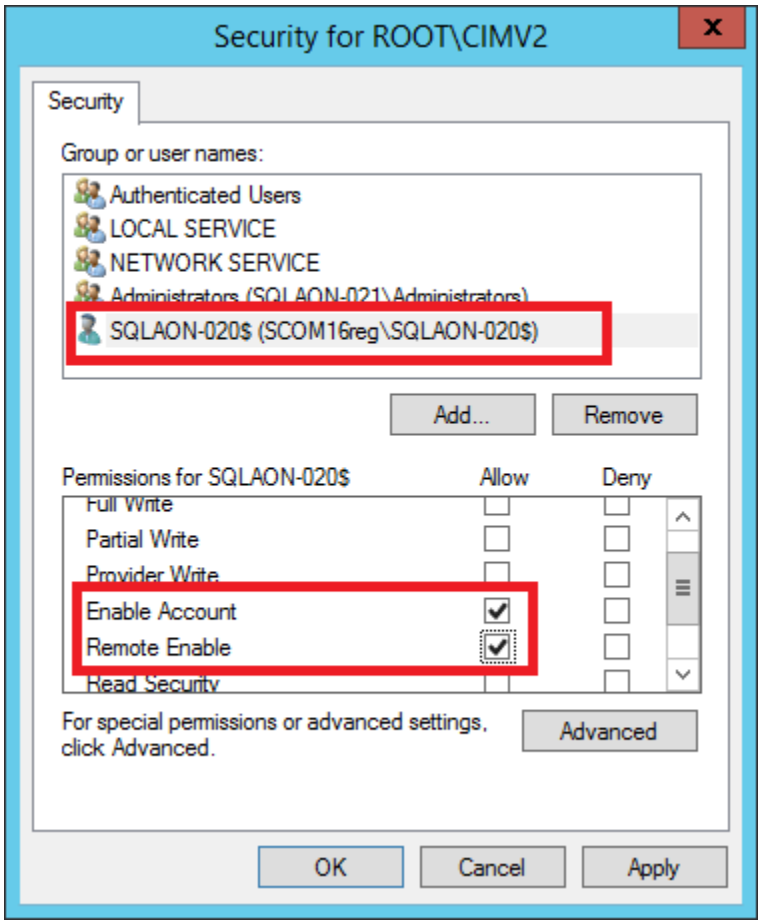
3. In this dialog menu, go to **Security** tab.
4. Click the **Edit Limits** button in **Launch and Activation Permissions** section; the corresponding dialog menu will be displayed.



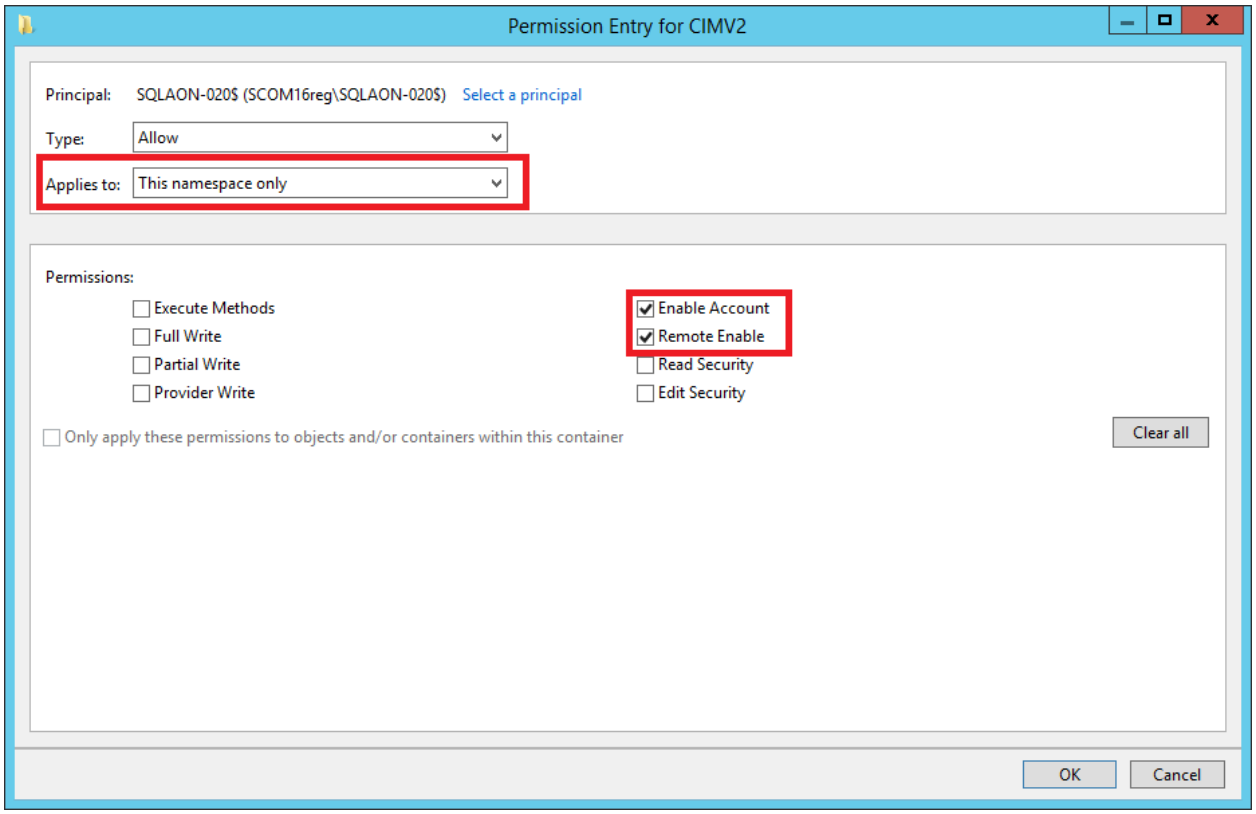
5. In this dialog menu, set the following permissions for the remote machine's account:
    - **Remote Launch**
    - **Remote Activation**



6. Go to **WMI Control** snap-In and call its properties; the corresponding dialog menu will be displayed.
7. In this dialog menu, go to **Security** tab, select **Root\CIMV2** namespace and click the **Security** button.
8. Add the following permissions for the target computer:
    - **Enable Account**
    - **Remote Enable**



9. Click the **Advanced** button; the corresponding dialog menu will be displayed.
10. In this dialog menu, select the target account and click the **Edit** button.
11. In the following dialog menu, make sure that **Applies to** parameter is set to **This namespace only** value, and the following permissions are set:
    - **Enable Account**
    - **Remote Enable**



Steps 1-11 should be performed on each replica participating in the target Availability Group.

Low-Privilege Environments

This section describes how to configure SQL Server Management Pack for low-privilege access (discovery, monitoring, and action) for both monitored SQL Server instances and the host operating system. When you follow the instructions in this section, the health service hosting SQL Server Management Pack executes all the workflows with low-privilege access to the target SQL Server instances and to the operating system where those instances are running.

For more information, see the Run As Profiles section.

> **Note:**
>
> Mirroring Monitoring is supported under low-privilege configuration. However, Mirroring Discovery works under High-Privilege only as soon as Discovery Script contains a part, which requires admin rights on Mirroring Instance.

The following procedure describes the steps needed to configure low-privilege Discovery, Monitoring, and Action for SQL Server Management Pack.

Note

This low-privilege configuration is only supported for non-clustered SQL Server environments. Clustered SQL Server instance monitoring under the low-privilege is supported for SQL Server 2012 and newer versions only.

Configure a Low-Privilege Environment in Active Directory

1. In Active Directory, create three domain users that will be commonly used for low-privilege access to all target SQL Server instances:
    a. **SQLDefaultAction**
    b. **SQLDiscovery**
    c. **SQLMonitor**
2. Create a domain group named **SQLMPLowPriv** and add the following domain users:
    a. **SQLDiscovery**
    b. **SQLMonitor**
3. Grant special permission: Read-only Domain Controllers - “Read Permission” to **SQLMPLowPriv**.

Configure a Low-Privilege Environment on the Agent Machine

1. On the agent machine, add the **SQLDefaultAction** and **SQLMonitor** domain users to the “Performance Monitor Users” local group.
2. Add the **SQLDefaultAction** and **SQLMonitor** domain users to “EventLogReaders” local group.
3. Add the **SQLDefaultAction** domain user and **SQLMPLowPriv** domain group as members to the local **Users** group.
4. Configure the “Allow log on locally” local security policy setting to allow the **SQLDefaultAction** domain user and **SQLMPLowPriv** domain group users to log on locally.
5. Grant Read permission on **HKLM:\Software\Microsoft\Microsoft SQL Server** registry path for **SQLDefaultAction** and **SQLMPLowPriv**.
6. Grant “Execute Methods”, “Enable Account”, “Remote Enable”, “Read Security” permissions for **root**, **root\cimv2**, **root\default**, **root\Microsoft\SqlServer\ComputerManagement11** WMI namespaces to **SQLDefaultAction** and **SQLMPLowPriv**.
7. Grant Read permission on **HKLM:\Software\Microsoft\Microsoft SQL Server*[InstanceID]*\MSSQLServer\Parameters** registry path for **SQLMPLowPriv** for each monitored instance.

Note:

The monitoring account user must have the following permissions to 'C:\Windows\Temp' folder:

- Modify
- Read & Execute
- List Folder Contents
- Read
- Write

Configure a Low-Privilege Environment on the Agent Machine in Cluster

1. For each node in a cluster, execute steps outlined in Configure a low-privilege environment on the agent machine section.
2. Grant “Remote Launch” and “Remote Activation” DCOM permissions to the **SQLMPLowPriv, SQLDefaultAction** using DCOMCNFG. Please note that both defaults and limits should be adjusted.
3. Allow Windows Remote Management through the Windows Firewall.
4. Grant “Read” and “Full Control” access for the cluster to the **SQLMPLowPriv** using Failover Cluster Manager.
5. Grant “Execute Methods”, “Enable Account”, “Remote Enable”, “Read Security” permissions to **SQLTaskAction** and **SQLMPLowPriv** for this WMI namespace: **root\MSCluster**.

Configure a Low-Privilege Environment on the Server, Which Hosts an SMB Share Used by SQL Server 2012 Database Engine

1. Grant share permissions by opening share properties dialog for the share, which hosts SQL Server data files or SQL Server transaction log files.
2. Grant Read permissions to **SQLMPLowPriv.**
3. Grant NTFS permissions by opening the properties dialog for the shared folder and navigate to the “Security” tab.
4. Grant Read permissions to **SQLMPLowPriv.**

Configure Instances for Monitoring in SQL Server Management Studio

1. In SQL Server Management Studio, create a login for “**SQLMPLowPriv”** on all SQL Server instances to be monitored on the agent machine, and grant the following permissions to each “**SQLMPLowPriv”** login:
    a. VIEW ANY DEFINITION
    b. VIEW SERVER STATE
    c. VIEW ANY DATABASE
2. Create an **SQLMPLowPriv** user that maps to the **SQLMPLowPriv** login in each existing user database, master, msdb, and model. By putting the user in the model database, it will automatically create an **SQLMPLowPriv** user in each future user-created database. See the code sample below. You will need to provision the user manually for the attached and restored databases.

3. Add the **SQLMPLowPriv** user on msdb to the **SQLAgentReaderRole** database role.
4. Add the **SQLMPLowPriv** user on msdb to the **PolicyAdministratorRole** database role.
5. For configuring Mirroring under low-privilege, it is necessary to execute the following code for each instance in Mirroring:
   grant select on sys.database_mirroring_witnesses to [yourdomain\SQLMPLowPriv]
   go

Configure Instances for Default Action in SQL Server Management Studio

1. In SQL Server Management Studio, create a login for **SQLDefaultAction** on all SQL Server instances to be monitored on the agent machine, and grant the following permissions to each **SQLDefaultAction** login:
   a. VIEW ANY DEFINITION
   b. VIEW SERVER STATE
   c. VIEW ANY DATABASE
   d. SELECT ON SYS.DATABASE_MIRRORING_WITNESSES
2. Create an **SQLDefaultAction** user that maps to the **SQLDefaultAction** login in each existing user database, master, msdb, and model. By putting the user into the model database, you automatically create an **SQLDefaultAction** user in each future user-created database. See code sample below. You need to manually provision the user for attached and restored databases.
3. Add an **SQLDefaultAction** user on msdb to the **SQLAgentReaderRole** database role.
4. Add the **SQLDefaultAction** user on msdb to the **PolicyAdministratorRole database** role.

 **Note:**

Some optional System Center Operations Manager tasks require a higher privilege on the agent machine and the databases where the tasks need to be executed. You should only execute the following provisioning steps on the agent machine or databases where you want the System Center Operations Manager console operator to take remedial actions.

Enable Execution of System Center Operations Manager Tasks for a Database Object

1. On the agent machine, grant the **SQLDefaultAction** user permission to start or stop an NT service if the task is about starting or stopping an NT service such as DB Engine Service, SQL Server Agent service, SQL FullText Search Service, Analysis Services, Integration Services, and Reporting Services. This involves setting a service's security descriptor. For more information, see Sc sdset.
   The basic process is to read the existing privileges for a given service (using sc sdshow) and then grant additional privileges to the SQLDefaultAction user for that server. For example, suppose the results of the SC sdshow command for SQL Server service are as follows:
   D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) In that case, the following command line confers

sufficient access to **SQLDefaultAction** for starting and stopping the SQL Server service (with appropriate substitutions for italicized values and keeping everything on a single line of text):
sc sdset SQL Server service name D:(A;;GRRPWP;;;SID for SQLDefaultAction)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

2. In SQL Server Management Studio, add "SQLDefaultAction" to db_owner database role for each database to check:
    a. "Check Catalog (DBCC)"
    b. "Check Database (DBCC)"
    c. "Check Disk (DBCC)" (invokes DBCC CHECKALLOC)
3. Grant the ALTER privilege to **SQLDefaultAction** for each database on which to set state:
    a. "Set Database Offline"
    b. "Set Database Emergency State"
4. Grant the ALTER ANY DATABASE privilege to **SQLDefaultAction** login to run the task of "Set Database Online".

Configure System Center Operations Manager

1. Import SQL Server Management Pack (if it has was not imported before).
2. Create an **SQLDefaultAction, SQLDiscovery** and **SQLMonitor** Run As accounts with "Windows" account type. For more information about how to create a Run As account, see How to Create Run As Account in Operations Manager 2012. For more information about various Run As Account types, see Managing Run As Accounts and Profiles in Operations Manager 2012.
3. On the System Center Operations Manager console, configure the Run As profiles for SQL Server Management Pack as follows:
    a. Set the "SQL Server Default Action Account" Run As profile to use the **SQLDefaultAction** Run As account.
        i. Grant CONNECT to **SQLDefaultAction** for the Operations Manager database.
        ii. Add "SQLDefaultAction" to the dbmodule_users database role.

    Note:
    When you make **SQLDefaultAction** the "SQL Server Default Action Account" on the management server, you need to grant access to the Operations Manager database.

    b. Set the "SQL Server Discovery Account" Run As profile to use the **SQLDiscovery** Run As account.
    c. Set the "SQL Server Monitoring Account" Run As profile to use the **SQLMonitor** Run As account.

The following code example shows provisioning the **SQLMPLowPriv** login on an instance:

```
use master
go
create login [yourdomain\SQLMPLowPriv] from windows
go

grant view server state to   [yourdomain\SQLMPLowPriv]
grant view any definition to [yourdomain\SQLMPLowPriv]
grant view any database to [yourdomain\SQLMPLowPriv]
grant select on sys.database_mirroring_witnesses to
[yourdomain\SQLMPLowPriv]
go
```

The next code example shows how to generate a Transact-SQL provisioning script. The generated script provisions the **SQLMPLowPriv** user in current user databases and the model database (thereby automating the provisioning in future databases).

```
SELECT 'use ' + name + ' ;'
+ char(13) + char(10)
+ 'create user [yourdomain\SQLMPLowPriv] FROM login
[yourdomain\SQLMPLowPriv];'
+ char(13) + char(10) + 'go' + char(13) + char(10)
FROM sys.databases WHERE database_id = 1 OR database_id >= 3
UNION
SELECT 'use msdb; exec sp_addrolemember
@rolename="SQLAgentReaderRole",
@membername="yourdomain\SQLMPLowPriv"'
+ char(13) + char(10) + 'go' + char(13) + char(10)
UNION
SELECT 'use msdb; exec sp_addrolemember
@rolename="PolicyAdministratorRole",
@membername="yourdomain\SQLMPLowPriv"'
+ char(13) + char(10) + 'go' + char(13) + char(10)
```

Warning!

You need to output the results of this query in text format.

Groups

The following groups are added when you import SQL Server Management Pack:

- SQL 2008 Computers
- SQL 2008 DB Engine Group
- SQL 2008 Replication Computers
- SQL 2008 Mirroring Group
- SQL 2008 R2 Computers
- SQL 2008 R2 DB Engine Group
- SQL 2008 R2 Replication Computers
- SQL 2012 Mirroring Group
- SQL 2012 Computers
- SQL 2012 DB Engine Group
- SQL Computers
- SQL Instances

TLS 1.2 Protection

Operating protection of connections in SQL Server is provided by means of TLS protocol. In order to have the ability to use TLS 1.2 protocol, your environment should meet the following prerequisites:

1. SQL Server should be updated to a version that supports TLS 1.2.
2. The following SQL Server drivers should be updated to a version that supports TLS 1.2:
    - SQL Server Native Client <version>
    - ODBC Driver 11 for Microsoft SQL Server
3. Make sure that your environment meets the prerequisites provided in the table below:

OS Version	SCOM Version	.NET Version	PowerShell version
Windows 2012 and above	Not less than minimal supported version**	From 2.0 to 4.0 with TLS 1.2 update* and from 4.0 to 4.6 with TLS 1.2 update*	3.0+
Windows 2012 and above	Not less than minimal supported version**	From 2.0 to 4.0 with TLS 1.2 update* and 4.6+	3.0+
Windows 2008 R2 and below	SCOM 2012 SP1 UR10 + SCOM 2012 R2 UR7 +	From 2.0 to 4.0 with TLS 1.2 update* and 4.6+	2.0+
Windows 2008 R2 and below	SCOM 2012 SP1 UR10 + SCOM 2012 R2 UR7 +	From 2.0 to 4.0 with TLS 1.2 update* and from 4.0 to 4.6 with TLS 1.2 update*	2.0+
Windows 2008 R2 and below	From minimal supported version** to SCOM 2012 SP1 UR9 or to SCOM 2012 R2 UR6	From 2.0 to 4.0 with TLS1.2 update*	2.0

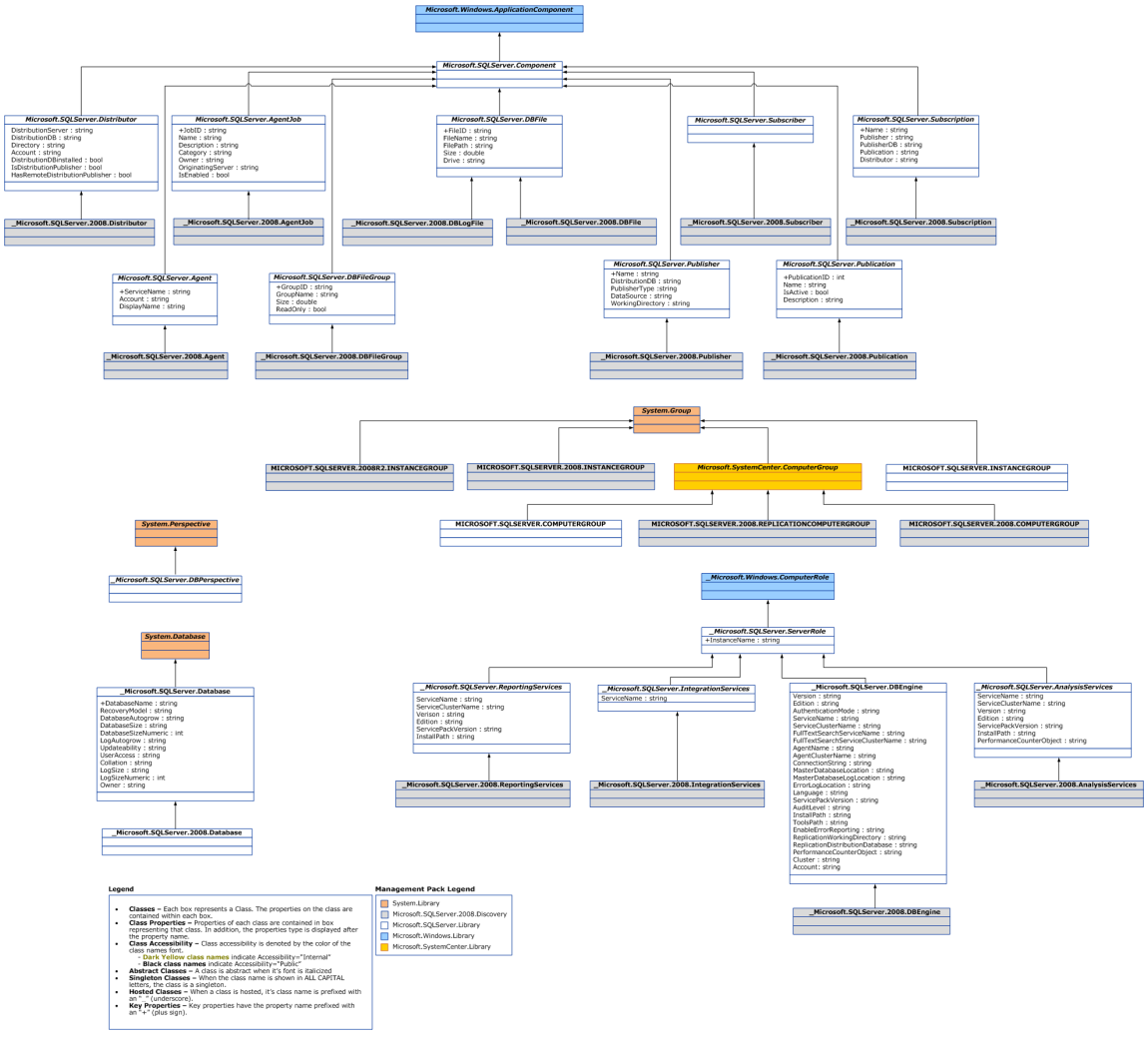
* .NET Framework TLS 1.2 updates can be downloaded from TLS 1.2 Support for Microsoft SQL Server page (**Client component downloads** section).

** Minimal supported SCOM versions are stated in Supported Configurations section.

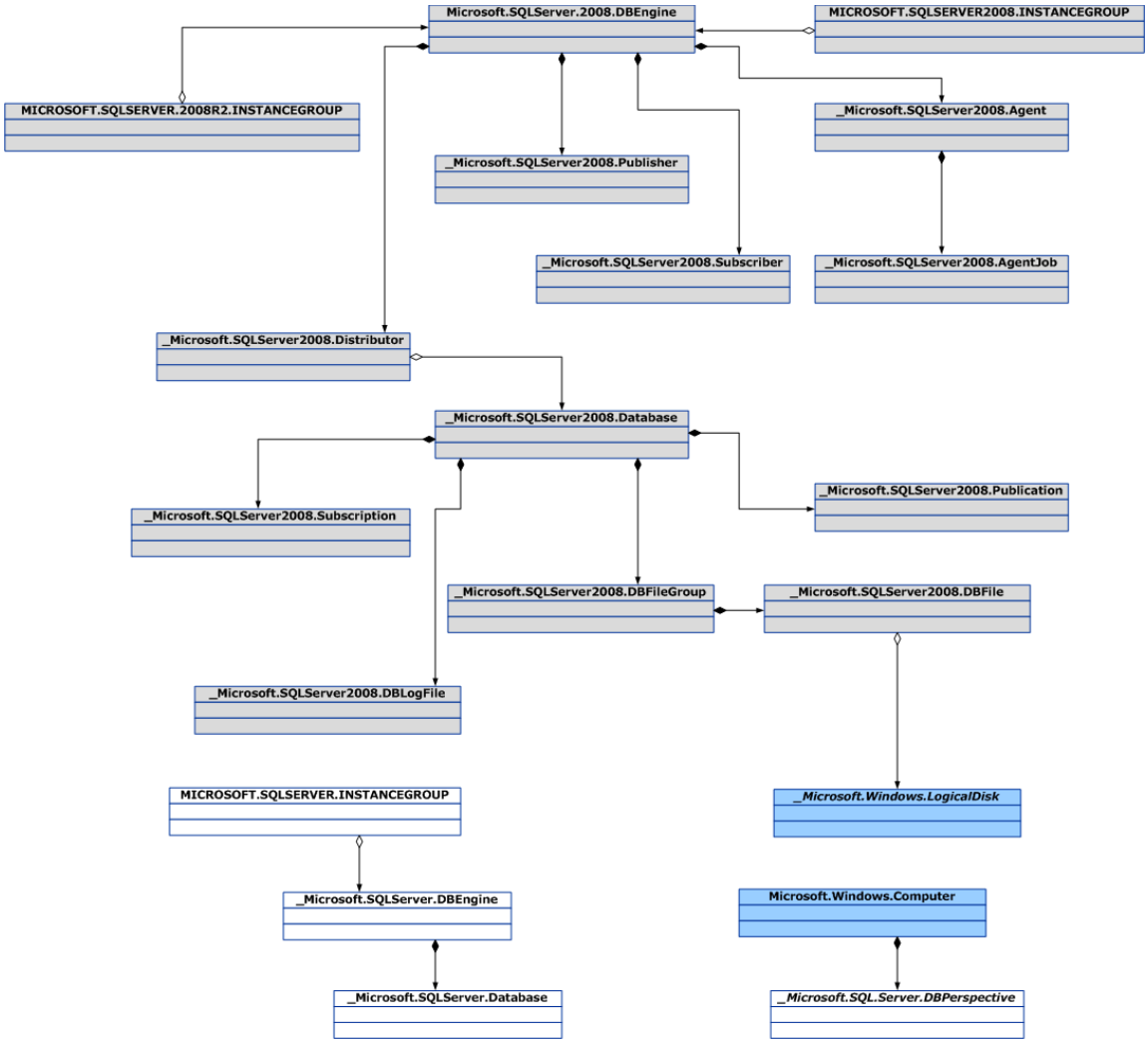
Understanding of SQL Server Management Pack

This section contains the following topics:

Inheritance Class Diagram



Relationship Class Diagram



Legend

- **Reference relationship –** Pointed arrow connectors with no diamond on the source of the relationship and the arrow pointing to the target class (i.e. [SourceClass] ⟶ [TargetClass])
- **Containment relationship –** Pointed arrow connectors where the source of the relationship is a open or white diamond and the arrow pointing to the target class (i.e. [SourceClass] ◇⟶ [TargetClass])
- **Hosting relationship –** Pointed arrow connectors where the source of the relationship is a closed or solid black diamond and the arrow pointing to the target class (i.e. [SourceClass) ◆⟶ [TargetClass])

Management Pack Legend

- Microsoft.SQLServer.2008.Discovery
- Microsoft.SQLServer.Library
- Microsoft.Windows.Library

Key Monitoring Scenarios

SQL Server Management Pack for Operations Manager includes a number of key monitoring scenarios that can be configured as follows.

Note:

The list is not intended to be a complete manifest of the management pack functionality.

Monitoring of Custom User Policies (CUP - PBM Policies Defined By User)

The new monitoring feature was added for SQL Server 2012 based on Policy-Based Management capabilities. The state of user-defined policies can be monitored if the database is used as a facet.

Note:

If the database is in the **Restoring** state, the CUP targeted to that database will np be monitored.

There are two monitors, which reflects the state of CUP:

- A two-state monitor with Error critical state used particularly for reflecting the state of Custom User Policies, which have Database as Facet and one of the predefined error categories as Policy Category.
- A two-state monitor with Warning critical state used particularly for reflecting the state of Custom User Policies, which have Database as Facet and any category except predefined error categories as Policy Category.

Separated Configuration for SQL Server 2008 and SQL Server 2008 R2

To configure different monitoring or discovery settings for SQL Server 2008 and SQL Server 2008 R2, apply overrides to the predefined computer groups:

- SQL Server 2008 DB Engine Group – includes instances of SQL Server 2008 and SQL Server 2008 SP1
- SQL Server 2008 R2 DB Engine Group – includes instances of SQL Server 2008 R2

Data File and Log File Space Monitoring

The management pack rules collect total data log and log file free space. You can use reports for reviewing this information across multiple databases and over extended periods for such functions as problem management and capacity planning. Management pack monitors provide space monitoring on three levels: data files, filegroups, and databases.

For more information, see the hierarchy of space monitors and overridable parameters in “Unit Monitors” and “Health Rolls Up Diagram” sections. The following performance counters are provided to support space monitoring:

Database Level	**Collect Database Total Free Space (in MB and in %)** The amount of space left in the database for all files in all filegroups for this database in megabytes or in percent. Also, includes space left on media hosting files with autogrowth enabled.
DB Filegroup Level	**Collect DB Filegroup Free Space (in MB and in %)** The amount of space left in all files for this filegroup in megabytes or in percent. Also, includes space left on media hosting files with autogrowth enabled.
	Collect DB Filegroup Allocated Space Left (in MB and in %) The amount of space left in all files for this filegroup in megabytes or in percent. Does not include space left on media hosting files with autogrowth enabled.
SQL DB File Level	**Collect DB File Free Space (in MB and in %)** The amount of space left in a file in megabytes or in percent. Also, includes space left on media hosting files with autogrowth enabled.
	Collect DB File Allocated Space Left (in MB and in %) The amount of space left in a file in megabytes or in percent. Does not include space left on media hosting files with autogrowth enabled.
SQL DB Log File Level	**Collect DB Log File Free Space (in MB and in %)** The amount of space left in all log files for this database in megabytes or in percent. Also, includes space left on media hosting files with autogrowth enabled.
	Collect DB Log File Allocated Space Left (in MB and in %) The amount of space left in all log files for this database in megabytes or in percent. Does not include space left on media hosting files with autogrowth enabled.

By default, space monitoring is enabled for the following levels:

- Database
- Filegroup
- File

If your environment is sensitive to any extra load, you may consider disabling monitoring on Filegroup and File level. To disable Filegroup level monitoring, you should disable the following rules:

- Collect DB Filegroup Allocated Space Left (%)
- Collect DB Filegroup Allocated Space Left (MB)
- Collect DB Filegroup Free Space (%)
- Collect DB Filegroup Free Space (MB)

To disable File level monitoring, you should disable the following rules and monitors:

Rules:

- Collect DB File Allocated Space Left (%)
- Collect DB File Allocated Space Left (MB)
- Collect DB File Free Space (%)
- Collect DB File Free Space (MB)
- Collect DB Log File Allocated Space Left (%)
- Collect DB Log File Allocated Space Left (MB)
- Collect DB Log File Free Space (%)
- Collect DB Log File Free Space (MB)

Monitors:

- DB File Space Monitor
- DB Log File Space Monitor

Many Databases on the Same Drive

Default space monitoring settings are noisy in environments where data or log files for many databases are located on the same drive and have autogrowth “On”. In such environments, an alert for each database is generated when the amount of free space on the hard drive reaches the threshold. To avoid noise, turn off the space monitors for data and log files, and use Base OS Management Pack to monitor space on the hard drive.

Long-Running SQL Server Agent Jobs

By default, this scenario is fully enabled in the management packs on a per-SQL Server Agent basis. This means that for each monitoring SQL Server Agent, maximum job duration is what is compared to the thresholds, and alerts are raised if any single job runs too long.

In addition, more detailed monitoring, which is on a per-job basis is provided in the management packs but the discoveries for SQL Server Agent jobs are disabled by default. Enable the following object discoveries:

- SQL Server 2012: Discover SQL Server 2012 Agent Jobs
- SQL Server 2008: Discover SQL Server 2008 Agent Jobs

Job Failure

To get alerts for failed jobs, enable the rule “A SQL job failed to complete successfully” and make sure that the option "Write to the Windows Application Event Log” “when the job fails” is selected for all jobs you want to monitor.

For more information, see Job Properties / New Job (Notifications Page) in the MSDN Library

Blocking Sessions

A monitor periodically queries each database engine instance for a list of active sessions (SPIDs) and checks to see if any long-running blocking is occurring. If blocking is detected and it exceeds the given threshold, then the state is changed and an alert is raised.

You can apply an override to change the time-duration value that is used to determine whether blocking is long running. The default time-duration value is one minute.

Discovery of SQL Server Database Engine Instances

The discovery of stand-alone and clustered instances of the SQL Server Database Engine role across all managed systems can be configured to exclude particular instances of the database engine.

You can apply overrides to the following discoveries to specify an “Exclude List” (in comma-delimited format) of the names of SQL Server Database Engine instances that the discovery should overlook:

- SQL Server 2012: Discover SQL Server 2012 Database Engines (Windows Server)
- SQL Server 2008: Discover SQL Server 2008 Database Engines (Windows Server)

Database Discovery and State Monitoring

For each managed database engine, the databases are discovered and monitored by means of a number of rules and monitors.

You can apply overrides to the following discoveries to specify an “Exclude List” (in comma-delimited format) of database names that the discovery should overlook.

- SQL Server 2012: Discover Databases for a Database Engine
- SQL Server 2008: Discover Databases for a Database Engine

Restart of DB Engine

The availability of DB Engine is monitored by the SQL Server Windows Service monitor for the SQL DB Engine object. This monitor does not reflect the service restart.

To be notified about each restart of DB Engine, you can enable the SQL Server <*version*> DB Engine Is Restarted rule (<*version*> can be 2012 or 2008).

SQL DB Engine CPU Monitoring

CPU utilization is monitored by the monitor, which measure actual workload of the processors working on SQL Server process threads, and raises an alert if all allocated CPUs are busy

processing SQL Server tasks. This monitoring scenario takes into account the current affinity mask of SQL DB Engine.

DB Storage Latency Monitoring

DB Storage performance is monitored by two monitors: Disk Read Latency and Disk Write Latency. In case of a significant storage performance degradation, an alert will be raised. These monitors are disabled by default. Enable these monitors only for specific databases where it is required to monitor storage performance. In addition, the latency can be viewed on the Database Dashboard.

Disabled Rules

Some rules in the management pack are disabled by default to avoid noise. Consider enabling the rules that can be valuable in your environment. The following rules are disabled by default:

- An SQL job failed to complete successfully
- An SQL Server Service Broker procedure output results
- An SNI call failed during a Service Broker/Database Mirroring transport operation
- SQL Server restarted
- SQL Server Service Broker Manager has shut down
- SQL Server Service Broker or Database Mirroring is running in FIPS compliance mode
- SQL Server Service Broker or Database Mirroring Transport stopped
- SQL Server Service Broker transmitter shut down due to an exception or a lack of memory
- SQL Server terminating because of system shutdown
- Table: Creating statistics for the following columns
- The Service Broker or Database Mirroring Transport has started
- The SQL Server Service Broker or Database Mirroring transport is disabled or not configured

Objects the Management Pack Discovers

You can use SQL Server Management Pack to monitor components of Microsoft Server 2008, SQL Server 2008 R2 and SQL Server 2012. You can use the Authoring pane of the Operations Manager console to enable discovery of components that are not automatically discovered. For more information about enabling object discovery, see Object Discoveries in Operations Manager 2007 article in the Operations Manager Help.

Note:

You can use the same procedure to override the settings for the discovery of an object.

SQL Server Management Pack discovers the object types described in the following table. Not all of the objects are automatically discovered. Use overrides to discover those that are not discovered automatically.

Category	Object type	Discovered Automatically
SQL Server Roles	SQL Server 2008 R2 DB Engine	Yes
SQL Server Roles	SQL Server 2008 DB Engine	Yes
SQL Server Roles	SQL Server 2012 DB Engine	Yes
SQL Server Roles	SQL Server 2008 R2 Analysis Services	Yes
SQL Server Roles	SQL Server 2008 Analysis Services	Yes
SQL Server Roles	SQL Server 2012 Analysis Services	Yes
SQL Server Roles	SQL Server 2008 R2 Reporting Services	Yes
SQL Server Roles	SQL Server 2008 Reporting Services	Yes
SQL Server Roles	SQL Server 2012 Reporting Services	Yes
SQL Server Roles	SQL Server 2008 R2 Integration Services	Yes
SQL Server Roles	SQL Server 2008 Integration Services	Yes
SQL Server Roles	SQL Server 2012 Integration Services	Yes
Replication Components	SQL Server 2008 R2 Distributor	No
Replication Components	SQL Server 2008 Distributor	No
Replication Components	SQL Server 2012 Distributor	No
Replication Components	SQL Server 2008 R2 Publisher	No
Replication Components	SQL Server 2008 Publisher	No

Category	Object type	Discovered Automatically
Replication Components	SQL Server 2012 Publisher	No
Replication Components	SQL Server 2008 R2 Subscriber	No
Replication Components	SQL Server 2008 Subscriber	No
Replication Components	SQL Server 2012 Subscriber	No
Replication Components	SQL Server 2008 R2 Subscription	No
Replication Components	SQL Server 2008 Subscription	No
Replication Components	SQL Server 2012 Subscription	No
Other Object Types	SQL Server 2008 R2 DB	Yes
Other Object Types	SQL Server 2008 DB	Yes
Other Object Types	SQL Server 2012 DB	Yes
Other Object Types	SQL Server 2008 Mirroring DB	Yes
Other Object Types	SQL Server 2008 Mirroring Witness	Yes
Other Object Types	SQL Server 2008 R2 Agent	Yes
Other Object Types	SQL Server 2008 Agent	Yes
Other Object Types	SQL Server 2012 Agent	Yes
Other Object Types	SQL Server 2008 R2 Agent Job	No
Other Object Types	SQL Server 2008 Agent Job	No
Other Object Types	SQL Server 2012 Agent Job	No
Other Object Types	SQL Server 2008 R2 DB Filegroup	Yes
Other Object Types	SQL Server 2008 DB Filegroup	Yes
Other Object Types	SQL Server 2012 DB Filegroup	Yes

Category	Object type	Discovered Automatically
Other Object Types	SQL Server 2012 DB FILESTREAM Filegroup	Yes
Other Object Types	SQL Server 2008 R2 DB File	Yes
Other Object Types	SQL Server 2008 DB File	Yes
Other Object Types	SQL Server 2012 DB File	Yes
Other Object Types	SQL Server 2012 DB Policy	No

Objects Discovered

Use the following procedures as an example of enabling automatic discovery for SQL Server Agent Job.

Use an Override to Change the Setting for Automatic Discovery

1. In the Authoring pane, expand **Management Pack Objects**, and then click **Object Discoveries**.
2. On the Operations Manager toolbar, click **Scope**, and then filter the objects that appear in the details pane to include only SQL Server objects.
3. In the Operations Manager toolbar, use the **Scope** button to filter the list of objects, and then click **SQL Server Agent Job**.
4. On the Operations Manager toolbar, click **Overrides**; click **Override the Object Discovery**, and then click **For all objects of type: SQL Agent**, **For a group**.
5. In the **Override Properties** dialog box, click the **Override** box for the **Enabled** parameter.
6. Under **Management Pack**, click **New** to create an unsealed version of the management pack, and then click **OK**, or select an unsealed management pack that you previously created in which to save this override. As a best practice, you should not save overrides to the Default Management Pack.

When the override setting is changed, the object type is automatically discovered and is displayed in the **Monitoring pane** under **SQL Server**.

Discovery Fail Alert Reporting

The following table contains the list of discoveries, errors of which will be collected by a special rule and displayed respectively.

Discovery Name	Error Event ID
Discover Databases for a Database Engine	**7101**
Discover Filegroups	
Discover Files	
Discover SQL Server 2008 Agent Jobs	**7102**
Discover Databases for a Database Engine	
Discover Filegroups	
Discover Files	
Discover Mirrored Databases for a Database Engine	
Discover Mirrored Databases Witnesses	

Discover SQL Server 2012 Agent Jobs	**7103**
Database Replicas Always On Discovery	
General Always On Discovery	
General Custom User Policy Discovery	
Discover Databases for a Database Engine	
SQL Server 2012 Database Custom User Policy Discovery	
Discover Filegroups	
Discover Files	
Discover Mirrored Databases for a Database Engine	
Discover Mirrored Databases Witnesses	

How Health Rolls Up

The SQL Server Management Pack categorizes the SQL Server components into a layered structure, where the health of one layer can depend on the health of the lower level.

Top Level

The top level of this model contains Windows Server. If the SQL Server application is not healthy, Windows Server is not healthy.

Second Level

The second level contains these components:	• Database Engine • Reporting Services (contains no lower-level components) • Analysis Services (contains no lower-level components) • Integration Services (contains no lower-level components) **Note:** The health of each of these components directly affects the health of Windows Server.

Database Engine

The Database Engine contains these lower-level components:	• Database (only the database has lower-level components) • Distributor • Publisher • Subscriber

Database

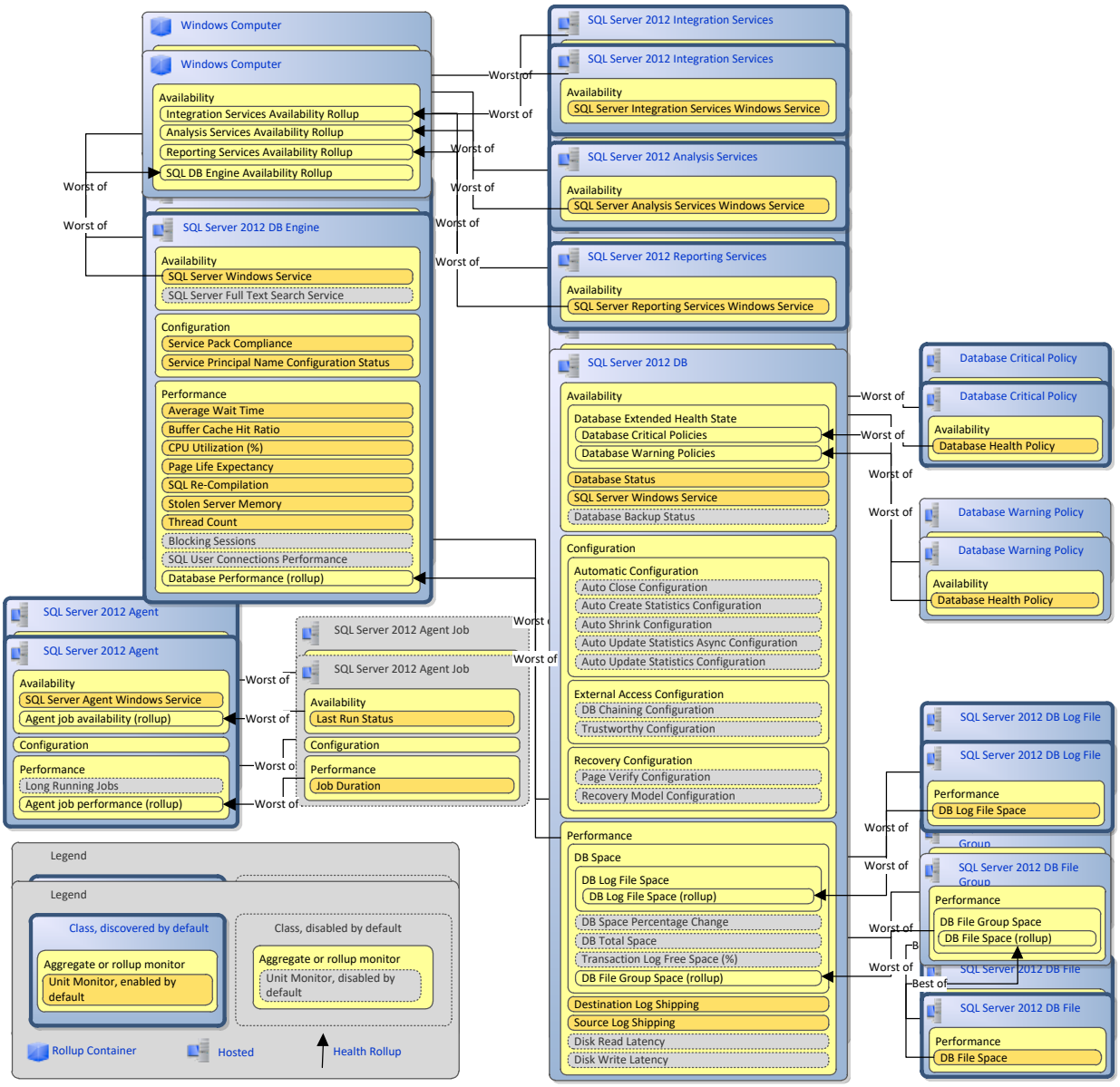
The Database contains the following lower-level components:

Database File	Affects the health of the file-group component, which in turn affects the health of the database.
SQL Server Agent	Contains one lower-level component, the SQL Server Agent Job. If the SQL Server Agent Job is not healthy, the SQL Server Agent will not be healthy, and therefore the Database Engine will not be healthy.
Publication	Rolls up to the database but has no lower-level components
Subscription	Rolls up to the database but has no lower-level components
Database Policy	Rolls up the state of Custom User Policies mapped to Database.

Health Roll Up Diagram

The following illustration shows the objects that are enabled and disabled.

Illustration of the Enabled Objects



Note:

You can create dependency monitors to customize health rollup. To view a health rollup diagram for your configuration, select an object and click **Health Explorer** in the Actions pane.

Viewing Information in the Operations Manager Console

You can see a high-level view of object types in your SQL Server deployment.

A view can contain a lengthy list of objects. To find a specific object or group of objects, you can use the **Scope**, **Search**, and **Find** buttons on the Operations Manager toolbar. For more information, see the How to Manage Monitoring Data Using Scope, Search, and Find topic in the Operations Manager Help.

These views are listed directly under the **Microsoft SQL Server** node in the **Monitoring** pane of the Operations Manager console. Details for most of the views are listed in the table below.

- Active Alerts, which displays an aggregation of all alerts that are not closed.
- Computers, which displays a state view of all the computers running SQL Server.
- Task Status, which displays a status view of all available tasks.
- Databases
- Health Monitoring
- Performance
- Replication
- Server Roles
- SQL 2008
- SQL 2008 R2
- SQL 2012
- SQL Agent

Databases Views

View Name	Description
Database Free Space	The Legend pane displays a list of counters for every monitored database. A chart illustrates the information in the Legend pane.
Database State	Displays a list of monitored databases and their current states. The Detail View pane displays the properties of the database selected above.
Transaction Log Free Space	The Legend pane displays a list of Transaction Log files.
SQL Server 2012 Databases Summary Dashboard	Displays list of SQL Server 2012 databases and their state. Provides detailed information about the selected database. Use Databases widget to select a database.

View Name	Description
	DB Alerts widget displays alerts and warnings that target the database. Free Space widget displays three series of data that represent Used, Allocated and Disk Free space if autogrowth is disabled only two series of data will be displayed (Used and Allocated). The widget has 2 scale types: Linear and Logarithmic. Hover over Y-Axis to switch between them. Red and Yellow lines represent Upper and Lower thresholds that are set for DB Total Space monitor. Performance section contains eight performance collection rules, four of them can be linked with monitors. If linked monitors are disabled, the widgets display performance collection data without health state indication. Since there are no monitors for DB Active Sessions, DB Active Requests, DB Active Connections and DB Transactions/sec they do not have health state indication. Next monitors are linked with top four performance widgets: Transaction Log Free Space (%), DB Total Space, Disk Read Latency and Disk Write Latency monitors. Personalization option allows selecting Time Range for Free Space and Performance widgets by default the value is set to 2 days.

Health Monitoring Views

View Name	Description
Agent Health	This is a dashboard view that displays the health of SQL Agents and, for each agent, the alerts that have not been closed. If you have discovered agent jobs, they are also included in this view.

View Name	Description
	The Detail View pane provides the properties of the agent selected in the SQL Agent State pane.
Database Engine Health	This is a dashboard view that displays the health of each database engine instance, including a list of the alerts that have not been closed for that database engine instance and for any objects that instance contains. The Detail View pane displays the properties of the selected database engine instance.

Performance Views

View Name	Description
All Performance Data	The Legend pane contains a list of objects for which data is collected.
Database Free Space	The Legend pane displays a list of databases.
User Connections	The Legend pane displays a list of objects governed by the SQL User Connections rule.
Transaction Log Free Space	The Legend pane displays a list of Transaction Log files.

Replication Views

View Name	Description
Distributor State	Displays the state of the replication distributor.
Publication State	Displays the state of the replication publication.
Publisher State	Displays the state of the replication publisher.
Subscription State	Displays the state of the replication subscription.

Server Roles Views

View Name	Description
Analysis Services	Displays a list of instances with SQL Server Analysis Services installed.
Database Engines	Displays a list of instances with SQL Server Database Engine installed.
Integration Services	Displays a list of instances with SQL Server Integration Services installed.
Reporting Services	Displays a list of instances with SQL Server Reporting Services installed.

SQL Server Agent Views

View Name	Description
SQL Agent Job State	The SQL Server Agent Job State panel displays a list of agent jobs. The Detail View pane contains the properties of the SQL Server Agent Job.
SQL State	Displays a list of SQL Server Agents. If agent jobs have been discovered, it also contains columns for each agent job and their respective health states. The Detail View displays the properties of the SQL Server Agent.

Dashboards

This management pack includes a set of rich dashboards, which provide detailed information about SQL Server Database Engines (Instances) and Databases.

Note:

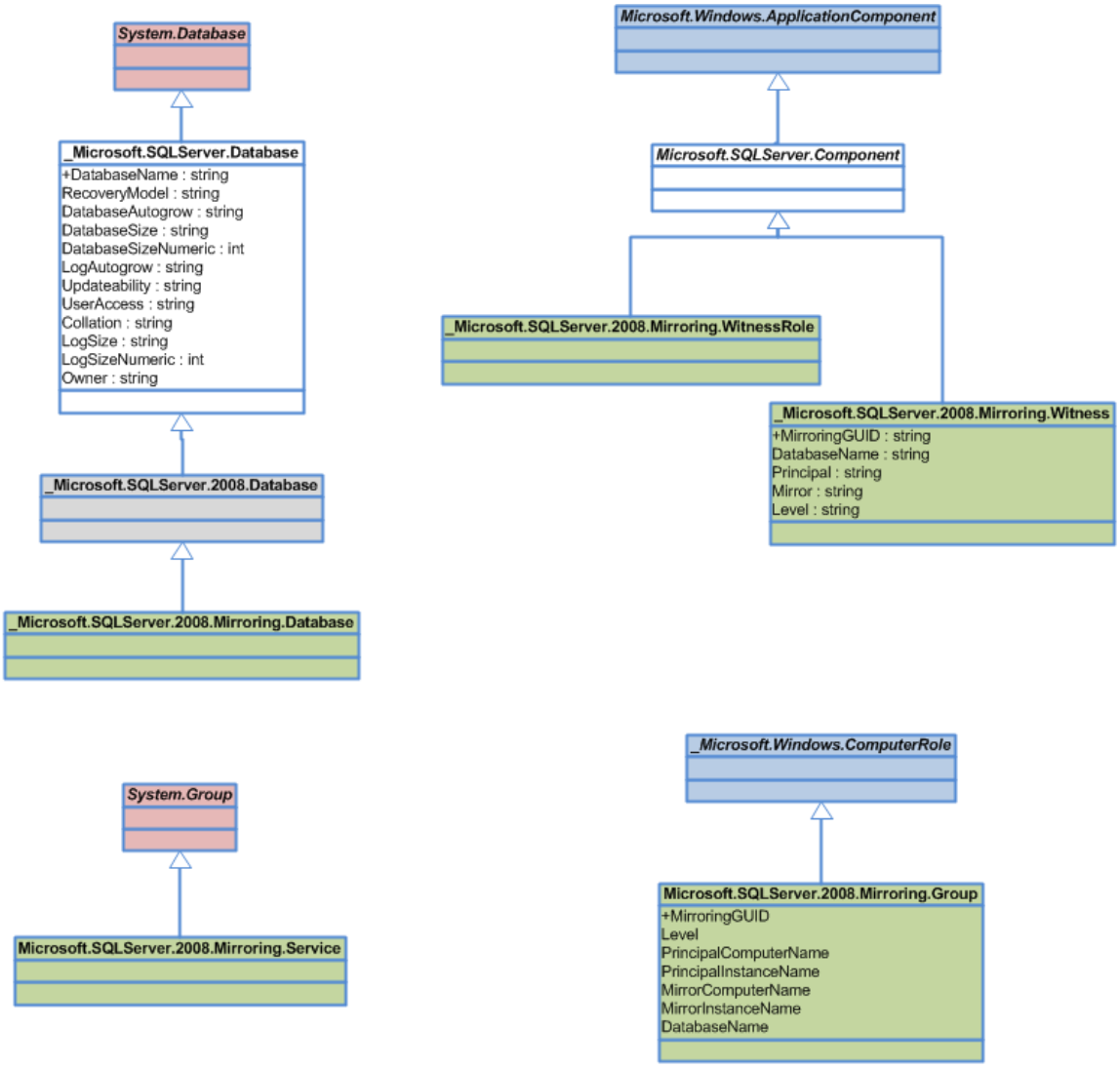
For detailed information, see SQLServerDashboardsGuide.docx.

Understanding of SQL Server 2008 and SQL Server 2012 Mirroring Management Packs

This section contains the following topics:

Inheritance Class Diagram

SQL Server 2008 Mirroring - inheritance class diagram



Legend

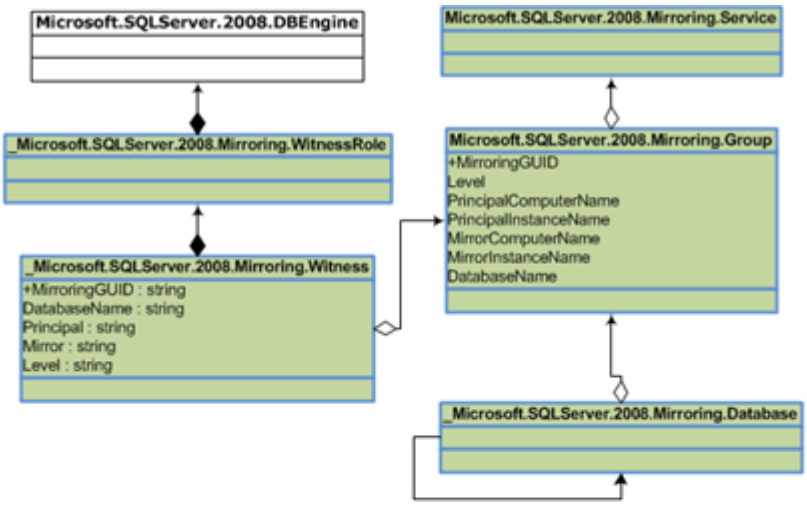
- **Classes** – Each box represents a Class. The properties on the class are contained within each box.
- **Class Properties** – Properties of each class are contained in box representing that class. In addition, the properties type is displayed after the property name.
- **Class Accessibility** – Class accessibility is denoted by the color of the class names font.
  - **Dark Yellow class names** indicate Accessibility="Internal"
  - **Black class names** indicate Accessibility="Public"
- **Abstract Classes** – A class is abstract when it's font is italicized
- **Singleton Classes** – When the class name is shown in ALL CAPITAL letters, the class is a singleton.
- **Hosted Classes** – When a class is hosted, it's class name is prefixed with an "_" (underscore).
- **Key Properties** – Key properties have the property name prefixed with an "+" (plus sign).

Management Pack Legend

- System.Library
- Microsoft.SQLServer.Library
- Microsoft.Windows.Library
- Microsoft.SystemCenter.Library
- Microsoft.SQLServer.2008
- Microsoft.SQLServer.2008.Mirroring

Relationship Class Diagram

SQL Server 2008 Mirroring - relationship class diagram



Legend

- **Reference relationship –** Pointed arrow connectors with no diamond on the source of the relationship and the arrow pointing to the target class (i.e. [SourceClass] ⟶ [TargetClass])
- **Containment relationship –** Pointed arrow connectors where the source of the relationship is a open or white diamond and the arrow pointing to the target class (i.e. [SourceClass] ◇⟶ [TargetClass])
- **Hosting relationship –** Pointed arrow connectors where the source of the relationship is a closed or solid black diamond and the arrow pointing to the target class (i.e. [SourceClass] ◆⟶ [TargetClass])

Management Pack Legend

- System.Library
- Microsoft.SQLServer.Library
- Microsoft.Windows.Library
- Microsoft.SystemCenter.Library
- Microsoft.SQLServer.2008
- Microsoft.SQLServer.2008.Mirroring

Note:

SQL Server 2012 Mirroring MP uses logically the same class structure; the only difference is naming since “2008” was updated to “2012”.

Key Monitoring Scenarios for Mirroring

The SQL Server Mirroring Management Packs for the Operations Manager include a number of key monitoring scenarios that can be configured as described below.

Note:

This list is not intended to be a complete manifest of the management pack functionality.

Discovery of Mirroring Components

The following objects are discovered for each of SQL Server instance:

- Databases enabled for Mirroring with all their properties (required for mirroring monitoring)
- Mirroring group contains the collection of databases enabled for mirroring and properties required to identify principal and mirror roles
- Witness Role and Witness
- Mirroring Session direction required to show mirroring dataflow in the diagram view. You can apply overrides to the following discoveries to specify an “Exclude List” (in comma-delimited format) of the database names that the discovery should overlook:
- SQL 2008/2012 Mirrored DB Discovery Provider

The almost all requirements to prevent performance degradation should be kept as well as for objects in SQL Server Management Pack.

Database Mirror Synchronization State Monitoring

The monitor checks the status of the database mirror reported by SQL Server. It checks the availability of mirror database as well as its SYNCHRONIZED state. This monitor also checks the following warning states:

SYNCHRONIZING - The contents of the mirror database are lagging behind the contents of the principal database. The principal server is sending log records to the mirror server, which is applying the changes to the mirror database to roll it forward. At the start of a database mirroring session, the database is in the SYNCHRONIZING state. The principal server is serving the database, and the mirror is trying to catch up.

SUSPENDED - The mirror copy of the database is not available. The principal database is running without sending any logs to the mirror server, a condition known as running exposed. This is the state after a failover. A session can also become SUSPENDED because of redo errors or if the administrator pauses the session. SUSPENDED is a persistent state that survives partner shutdowns and startups.

PENDING_FAILOVER - This state is found only on the principal server after a failover has begun, but the server has not transitioned into the mirror role. When the failover is initiated, the

principal database goes into the PENDING_FAILOVER state, quickly terminates any user connections, and takes over the mirror role soon thereafter.

Mirroring Witness State Monitoring

This monitor checks the status of the database mirroring witness reported by SQL Server. Monitor checks that connection between Mirroring Partner and Witness server is available in case if Mirroring witness is presented in Mirroring configuration.

Mirroring Partner State Monitoring

This monitor checks the status of the database mirroring session reported by SQL Server. An unhealthy state indicates that the SQL Server database mirroring session is not in the operational state.

Objects the Management Packs Discovers

You can use the SQL Server 2008 Mirroring MP and SQL Server 2012 Mirroring MP to monitor components of SQL Server 2008, SQL Server 2008 R2 and SQL Server 2012 Database Mirroring. You can use the Authoring pane of the Operations Manager console to enable discovery of components that are not automatically discovered. For more information about enabling object discovery, see Object Discoveries in Operations Manager 2007 article in the Operations Manager Help.

Note:

You can use the same procedure to override the settings for the discovery of an object.

The MPs discover the object types described in the following table. Not all of the objects are automatically discovered. Use overrides to discover those that are not discovered automatically.

Category	Object type	Discovered Automatically
SQL Server Mirroring Component	SQL Server 2008 Mirroring Database	Yes
SQL Server Mirroring Component	SQL Server 2008 Mirroring Witness	Yes
SQL Server Mirroring Component	SQL Server 2008 Witness Role	Yes
SQL Server Mirroring Component	SQL Server 2008 Mirroring Service	Yes

Category	Object type	Discovered Automatically
SQL Server Mirroring Component	SQL Server 2008 Mirroring Group	Yes

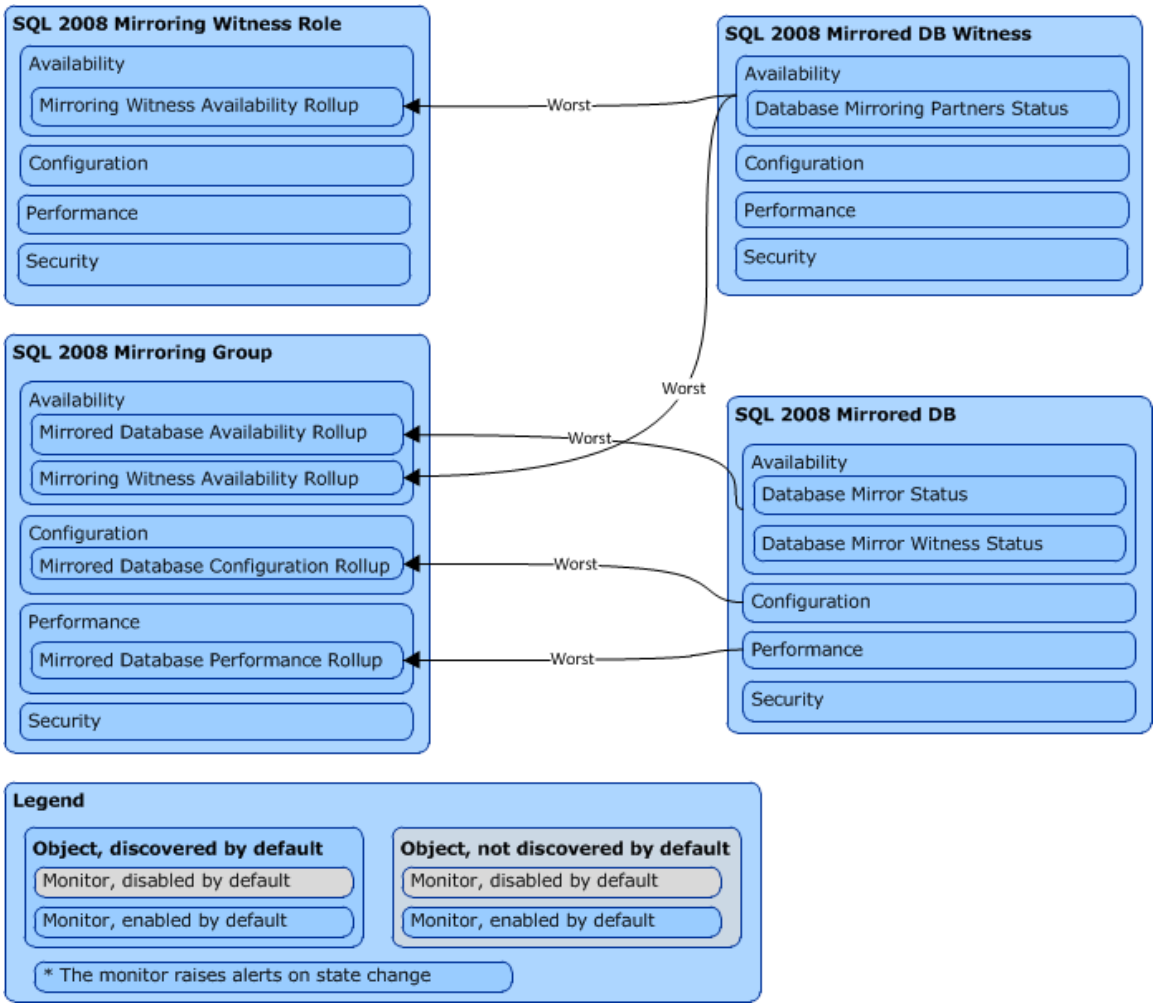
How Health Rolls Up

The SQL Server 2008/2012 Mirroring Management Packs use the layered structure of health model. SQL Server database and other related objects of SQL Server MP affect the health of the Mirroring functionality.

Health Roll Up Diagram

The following illustration shows the objects that are enabled and disabled.

Illustration of enabled objects



Note:

You can create dependency monitors to customize health rollup. To view a health rollup diagram for your configuration, select an object and click **Health Explorer** in the Actions pane.

Viewing Information in the Operations Manager Console

You can see a high-level view of object types in your SQL Server deployment.

The view can contain a lengthy list of objects. To find a specific object or group of objects, you can use the **Scope**, **Search**, and **Find** buttons on the Operations Manager toolbar. For more information, see the How to Manage Monitoring Data Using Scope, Search, and Find topic in the Operations Manager Help.

These views are listed under **Mirroring** folder of the **Microsoft SQL Server** node in the Monitoring pane of the Operations Manager console. Details for most views are listed in the following table.

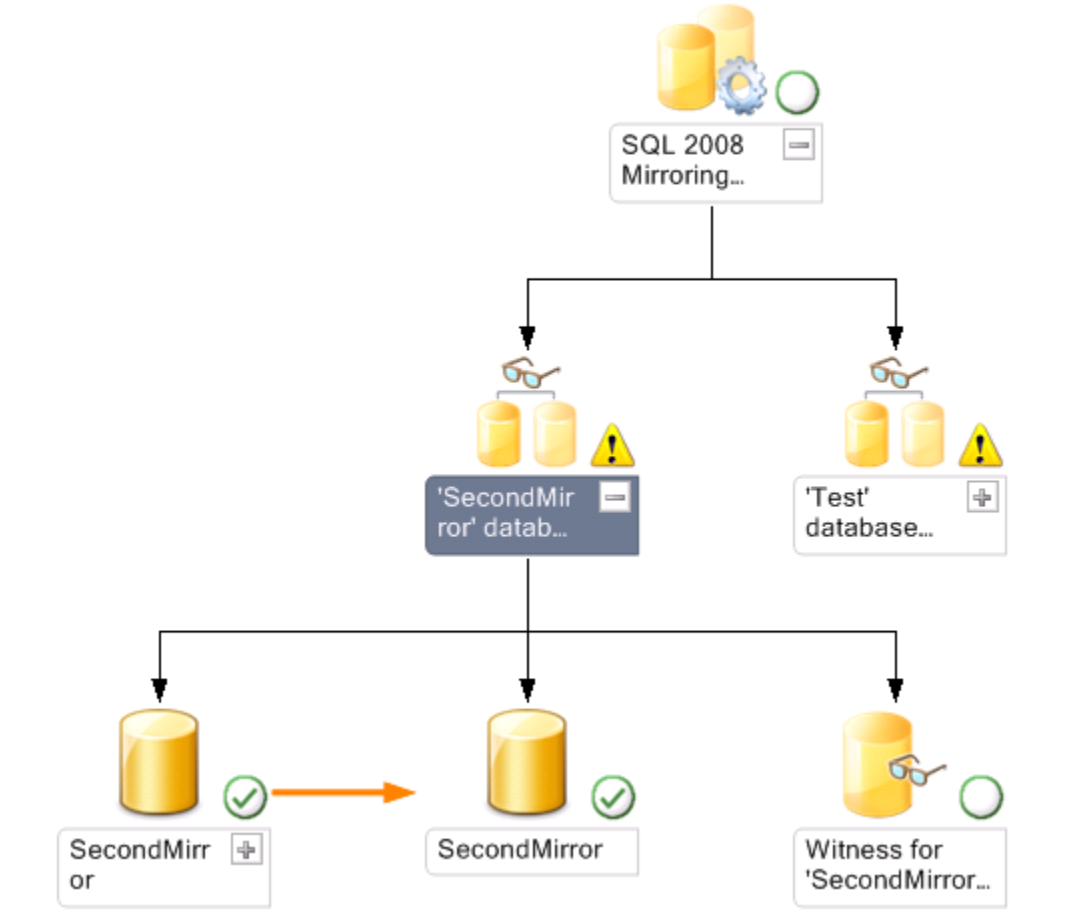
- Active Alerts, which displays an aggregation of all alerts that are not closed.
- Mirroring Diagram, which shows a diagram of mirroring components and their relationships.

Mirroring State Views

View Name	Description
Mirroring Groups	Displays all discovered Mirroring Groups with links to Mirrored Databases and Witness objects.

Mirroring Diagram

Mirroring diagram shows the main objects, which are participated in mirroring session: Mirroring database, Mirroring Group, Mirroring Service, Witness Role, and Witness. In addition, besides general relationship between components like Hosting and Containment, the mirroring diagram shows additional reference type relationship, which indicates the direction of mirroring data flow. When failover happens, that reference will be changed considering new direction, but it can take some time. To reduce the refresh time, it is possible to configure an override for the discovery of that type of relationship.


SQL 2008 Mirroring...
'SecondMir ror' datab...
'Test' database...
SecondMirr or
SecondMirror
Witness for 'SecondMirror...

Understanding of SQL Server 2012 Always On Management Pack

This section describes SQL Server 2012 Always On Management Pack

The scope of this management pack includes:

- Discovery of Always On objects (availability groups, availability replicas, and database replicas) on the SQL Server 2012 instances with enabled Always On.
- Monitoring of Always On objects' health by collecting PBM (Policy Based Management) policies' state via SQL Server PowerShell provider (part of the SQLPS module).
- Collecting of performance data for availability replicas and database replicas.
- Tasks for execution in SQL Server Management Studio and SQLPS console.

Prerequisites

SQL Server 2012 Management Studio should be installed on the machine where the Operations Manager console is installed to provide the capability to invoke SQL PowerShell tasks from the Operations Manager console.

Mandatory Configuration

To configure SQL Server 2012 Always On Management Pack, complete the following steps:

- Import prerequisite Management Packs
- Enable the Agent Proxy option on all agents that are installed on servers participating in an Always On session. For instructions, see the procedure that follows this list.

Enable the Agent Proxy Option

To enable the Agent Proxy option, complete the following steps:

1. Open the Operations Manager console and click the **Administration** button.
2. In the Administrator pane, click **Agent Managed**.
3. Double-click an agent in the list.
4. On the Security tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**.

Key Monitoring Scenarios for Always On

SQL Server 2012 Always On Management Pack for Operations Manager includes a number of key monitoring scenarios that can be configured as follows.

Discovery of Availability Groups, Availability Replicas and Database Replicas

The following objects are automatically discovered:

- Availability Group – which represents SMO Availability Group object and contains all required for identification and monitoring properties
- Availability Replica – which represents SMO Availability Replica object and contains all required for identification and monitoring properties
- Database Replica – which represents database level object of Always On and contains properties from SMO objects: Availability Database and Database Replica State
- Availability Group Health – which is hidden object used for roll-up health from agents to availability group level

Availability Groups, Availability Replicas, and Database Replicas Health Monitoring

This scenario collects health for all available Always On objects on the target SQL Server instance by using SQL Server PowerShell provider, which reads PBM policies state for each of the objects.

This management pack has two event rules for alerting when the following events appear in the Windows Application log:

- Event ID 1480: Database Replica role is changing
- Event ID 19406: Availability Replica role changed

Note that these events are disabled in SQL Server by default. To enable them, execute the next TSQL scripts:

- sp_altermessage 1480, 'with_log', 'true'
- sp_altermessage 19406, 'with_log', 'true'

Availability Groups, Availability Replicas, and Database Replicas Performance Monitoring

This scenario checks performance counters for availability replicas and database replicas on target machine and target SQL instance

Monitoring of Custom User Policies

All Always On monitors reflect their state by reader state of system policies using API provided by PBM (policy-based management). Beside system policies, Always On management pack provides the ability to monitor Custom User Policies defined by the user.

Always On management pack also extends capabilities of CUP (custom user policy) monitoring from SQL Server Management Pack where only policies with Database as Facet are monitored. Always On MP supports monitoring of policies where the following objects are facets:

- Availability Group
- Availability Replica
- Database Replica

For each of possible facets, there are two types of CUP monitors:

- A two-state monitor with Warning critical state used particularly for reflecting the state of Custom User Policies, which have <*object*> as Facet and one of the predefined warning categories as Policy Category.
- A two-state monitor with Error critical state used particularly for reflecting the state of Custom User Policies, which have <*object*> as Facet and one of the predefined error categories as Policy Category.

Low-Privilege Configuration for Always On Monitoring

For details about the low-privilege configuration for Always On monitoring, see Set Up A Low-Privilege Environment and Run As Profiles sections.

Goals of SQL Server 2012 Always On Management Pack

The goal of SQL Server 2012 Always On Management Pack is to provide discovery and monitoring for SQL Server 2012 Always On objects (availability groups, availability replicas, and database replicas) by reflecting the state of PBM policies. In addition, this management pack provides a capability to collect performance data for Always On objects and to invoke the SQL Server Management Studio and SQL PowerShell by calling console tasks.

How Health Rolls Up

The following diagram shows how the health states of objects roll up in this management pack.

Security Configuration

Run As Profile Name	Associated Rules and Monitors
Always On Discovery Account	• MSSQL 2012: General Always On Discovery • MSSQL 2012: General Custom User Policy Discovery
Always On Monitoring Account	• WSFC Cluster monitor • Availability Group Online monitor

Run As Profile Name	Associated Rules and Monitors
	• Availability Group Automatic Failover monitor • Availability Replicas Data Synchronization monitor • Synchronous Replicas Data Synchronization monitor • Availability Replicas Role monitor • Availability Replicas Connection monitor • Availability Replica Role • Availability Replica Connection • Availability Replica Data Synchronization • Availability Replica Join State • Availability Database Data Synchronization • Availability Database Join State • Availability Database Suspension State • Availability Group Health Policy • Availability Replica Health Policy • Database Replica Health Policy

Appendix: Known Issues and Troubleshooting

WMI errors may occur when SQL Server 2008/2008 R2 and SQL Server 2012 are installed on the same server

Issue: Modules can throw an error during WMI query.

Resolution: Update SQL Server 2008/2008 R2 with the latest service pack.

Database Backup Status Monitor generates false positive alerts on Always On Group secondary replicas

Issue: Database Backup Status monitor has no logic to track whether the database is a secondary replica or not. Since AOG has an advanced backup logic, which requires a backup for at least one of the databases involved, the monitor generates false positive alerts.

Resolution: The monitor is disabled by default and if the user wants to enable the monitoring scenario for his environment, it is recommended to keep the monitor disabled for all servers, which are not used for storing the database backup. A specific scenario for AON MP could be implemented in the future.

Mirroring Diagrams are version-specific

Issue: There are 3 Mirroring diagrams: SQL Mirroring 2008, 2012 and 2014. Each diagram displays object of the specified version and does not show related objects, which are hosted on other versions of SQL Server.

Resolution: If configured SQL Server Mirroring uses different versions of SQL Server, the user should monitor all views related to the chosen versions.

Error “missing performance counters” in OpsMgr event log

Issue: If required performance counters are not registered in the performance monitor, monitoring scenarios from the management pack cannot get the required information and exit with the error.

Resolution: Register the counters. More information can be found here.

Free Space widget incorrectly displays data

Issue: Free Space widget displays data provided by three performance collection rules:
1. SQL 2012 DBs Used Space (MB) performance collection rule

2. MSSQL 2012: Collect DB Allocated Free Space (MB)

3. MSSQL 2012: Collect DB Used Space (MB)

If intervals for these rules are not synchronized, the widget cannot correctly display the chart and the user sees shifted data series or overlaps in the chart.

Resolution: Make sure intervals for the rules are the same. When intervals are synchronized, the widget will start displaying chart correctly. Previously collected data will be incorrectly displayed anyway.

SQL Server 2012 Databases Summary Dashboard displays all active alerts if nothing is selected

Issue: Currently the dashboard displays all active alerts if nothing is selected. It is a standard querying mechanism of the default Alerts widget.

Resolution: Make sure that at least one DB suits the filtering options.

Widgets cannot display performance data if DB name has special symbols

Issue: Default performance widgets and SQL Server 2012 Databases Summary Dashboard will not display performance data for Databases that have a name with braces. This is a known SCOM issue. Moreover, If a database name is _**Total**, then cumulative performance metrics are collected for all databases, as long as _**Total** is a special object in a performance monitor.

Resolution: There is no known workaround at the moment.

SQL Server 2012 Databases Summary Dashboard may stop refreshing if left open for a long period

Issue: SCOM console has a memory leak that becomes noticeable if you have a dashboard with a considerable amount of widgets. Because of the memory leak, Authoring Console may consume all available memory and cause a situation when widgets stop refreshing.

Resolution:

Restart the Authoring Console.

Functions fail if instance name contains Asian characters

Issue: Functions fail to work on SQL Server 2008 if the instance name contains Asian characters. This situation is caused by the System Center Operations Manager 2007 and System Center Operations Manager 2007 SP1 known issue of the SCOM.ScriptAPI object, which is used to pass data from discovery script to Health Service at the target machine. This object incorrectly converts Variant to BSTR data type. For more information, see the Microsoft TechNet System Center Operations Manager Authoring forum.

Resolution: This issue is resolved in System Center Operations Manager 2007 R2. Users who need to monitor SQL Server with a localized instance name should update to Operations Manager 2007 R2.

10102 events from “Health Service Modules” are being generated on systems with 32-bit instances of SQL Server running on a 64-bit operating system, indicating that “PerfDataSource” could not resolve counters

Issue: On agent-managed systems that have a 32-bit instance of SQL Server installed on a 64-bit operating system, many 10102 error events will be reported into the Operations Manager log, indicating that PerfDataSource could not resolve a number of counters and that the module will be unloaded. These events are immediately followed by an 1103 event from HealthService indicating that one or more rules or one or more monitors failed and that the failed rules or monitors were unloaded.

Resolution: No resolution. Only a subset of monitoring will work for 32-bit installations of SQL Server that are monitored on a 64-bit operating system. This is because the SQL Server

processes are 32-bit, the Operations Manager agent processes are 64-bit, and there are limitations in collecting performance data across architectures. These limitations are documented in Knowledge Base article 891238.

11771 events from "Health Service Modules" are reported on systems with SQL Server 2008 Management Pack running the SQL Server Full Text Search Service Monitor

Issue: Agent-managed systems are running SQL Server Management Pack, and many 11771 events are reported. For example, see the following 11771 event.

Log	Operations Manager
Source	Health Service Modules
Event ID	11771
Level	Warning
Description	Error getting state of service Error: 0x8007007b Details: The filename, directory name, or volume label syntax is incorrect.

Resolution: The SQL Server Full Text Search Service Monitor expects to monitor the running SQL Server Full Text Search Service. If the SQL Server Full Text Search Service is not running, the management pack generates the 1171 events. To stop receiving the 11771 events, you can disable the SQL Server Full Text Search Service Monitor.

On clustered SQL Server, Management Pack discovery scripts time out for SQL Server Database Engines, SQL Server Analysis Services, and SQL Server Reporting Services

Issue: On a cluster, when there are multiple clustered SQL Server instances, management pack discovery scripts may time out for Database Engines, Analysis Services, and Reporting Services. You might see events similar to the following example.

Log Name:	Operations Manager
Source:	Health Service Modules
Date:	1/8/2009 5:33:23 PM
Event ID:	21402
Task Category:	None
Level:	Warning
Keywords:	Classic

User:	N/A
Computer:	SQL-Ex88S22.MPLAB.com
Description:	Forced to terminate the following process started at 5:28:24 PM because it ran past the configured timeout 300 seconds.
Command executed:	"C:\Windows\system32\cscript.exe" /nologo "DiscoverSQL2008DBEngineDiscovery.vbs" {32FBB1E4-C6D1-0517-2F47-3DDA67D46A3B} {D1C9D03B-AAAE-D1FF-5ECA-6AF1981FE271} SQL-Ex88S22.MPLAB.com SQL-Ex88S22.MPLAB.com SQL-Ex88S22 "Exclude:"
Working Directory:	C:\Program Files\System Center Operations Manager 2007\Health Service State\Monitoring Host Temporary Files 3\796\
Description:	One or more workflows were affected by this. Workflow name: Microsoft.SQLServer.2008.DBEngineDiscoveryRule.Server Instance name: SQL-Ex88S22.MPLAB.com Instance ID: {D1C9D03B-AAAE-D1FF-5ECA-6AF1981FE271} Management group: MOMGroup1

Resolution: Use overrides to increase the timeout value. To identify a new timeout value, use the following guidelines: (number of Database Engine instances on the physical node multiplied by 25 seconds*) plus (number of Analysis Services instances on the physical node multiplied by 25 seconds*) plus (number of Reporting Services instances on the physical node multiplied by 25 seconds*).

*This number approximates the time it takes for a script to run. The time it takes for a script to run on your system may vary.

For example, for a clustered SQL Server environment where there are 12 instances of Database Engine on each physical node, 10 instances of Analysis Services on each physical node, and 8 instances of Reporting Services on each physical node, the new timeout estimate is based on the calculation (12*25 sec)+(10*25 sec)+(8*25 sec). The default timeout value is 300 seconds. In this case, the new timeout value should be 750 seconds.

To use an override to enter a new timeout value for discovery scripts

1. Open the Operations Manager console, and then click **Authoring**.

2. In the **Authoring** pane, in the left navigation area, click **Management Pack Objects**, and then click **Object Discoveries**. The **Object Discoveries** pane displays a list of objects that the management pack discovers.

3. Right-click the discovery that you want to change, click **Overrides**, click **Override the Object Discovery**, and then click **For all objects of type: Windows Server**. The **Override Properties** dialog box is displayed.

4. Under **Override-controlled parameters**, select the **Override** box next to the **Timeout Seconds** parameter, and then increase the default number of seconds in **Override Value** by typing in a new number.

5. Under **Management Pack**, in **Select a destination management pack**, click the arrow to select a management pack from the list, or click **New** and follow the instructions in the wizard to create a new management pack for storing overrides and other customizations. For more information about creating a new management pack for customizations, see the Create a New Management Pack for Customizations section.

Data file and log file free space and free space percent collection rules and monitors might return inaccurate size values

Issue: On some agent-managed systems with databases that are two terabytes or larger, or with databases that were upgraded from SQL Server 2000, free space and free space percent collection rules and monitors might return inaccurate values for the data file and log file sizes. The following rules and monitors are reported to have been affected for SQL Server 2008 and SQL Server 2012:

Database Size Provider (Optimized)

- Collect Database Free Space (MB)
- Collect Database Free Space (%)
- Collect Database Size (MB)
- Collect Transaction Log Free Space (MB)
- Collect Transaction Log Free Space (%)
- Collect Transaction Log Size (MB)

Database / Log Free Space

- Database Space Free (%)
- Database Space Free (MB)
- Transaction Log Space Free (%)
- Transaction Log Space Free (MB)

Database Percentage Change

- Percentage Change in Database % Used Space

Resolution: If you encounter this issue, run the DBCC Update usage (Transact-SQL) command against the affected databases as described in SQL Server 2008 Books Online (February 2009).

Note:

Running this command might affect the overall performance of the database. We recommend that you schedule the command to run when it will not negatively affect the production

workload. No other workarounds exist. If the issue persists, contact customer support services or disable the affected rules or monitors.

Rules and monitors that are based on events from the event log do not work reliably on clustered installations of SQL Server

Issue: On clustered installations of SQL Server, rules and monitors that are based on events from the event log do not work reliably. The issue occurs because events for clustered installations of SQL Server are generated to event logs differently based on the version of the operating system.

Resolution: To resolve this issue, the following prerequisites must be met:

1. Ensure that the version of SQL Server Management Pack that is imported is version 6.0.6648.0 or greater.
2. Check the version of the management group:
    a. If the management group is running Operations Manager 2007, upgrade to Operations Manager 2007 SP1 and install the update from Knowledge Base article 959865, Issues that are resolved by the Operations Manager Module rollup update for System Center Operations Manager 2007 Service Pack 1.
    b. If the management group is running Operations Manager 2007 SP1, install the update from Knowledge Base article 959865, Issues that are resolved by the Operations Manager Module rollup update for System Center Operations Manager 2007 Service Pack 1.
    c. If the management group is running Operations Manager 2007 R2, no additional update is required.

“Rule/Monitor "<Rule/Monitor ID> cannot be initialized and will not be loaded” error in the event log.

Issue: Since the 6.6.7.6 version of System Center Management Pack for SQL Server has been installed, the "Microsoft.SQLServer.2012.AlwaysOn.TransactionDelay" rule failed. The issue occurs because of the “Tolerance” and “Maximum Sample Separation” were deprecated and removed. Similar issue for other monitors/rules where the Optimization used before updating System Center Management Pack for SQL Server

Log Name:	Operations Manager
Source:	HealthService
Date:	1/8/2015 10:44:20 AM
Event ID:	1102
Task Category:	Health Service
Level:	Error
Keywords:	Classic
User:	N/A
Computer:	

Description:	Rule/Monitor "Microsoft.SQLServer.2012.AlwaysOn.TransactionDelay" running for instance "xxxx" with id:"{284FC6CA-2A7F-3720-8D87-4DA0CAC6E288}" cannot be initialized and will not be loaded. Management group "SCOM 2012 Production"

Resolution: Re-create overrides for this Rule and then restart the Health Service.

SQL User Connections Performance monitor fails

Issue: In some cases, SQL Server Database Engine user connections baseline monitor can fail with an error.

Resolution: Unknown

Mirrored Databases Witnesses Discovery errors

Issue: After installation of 6.6.2.0 or higher version of the MP, the following error messages may be received:

Management Group: Script: DiscoverSQL2012MirroringWitness.vbs. Instance: xxxxx : Mirroring witness discovery script 'DiscoverSQL2012MirroringWitness.vbs' for instance 'xxxxx' failed.

Resolution: By default, local system account has no permission on sys.database_mirroring_witnesses. Accordingly, it is necessary to grant the corresponding permission for the local system account (see Set Up a Low-Privilege Environment section for details). If you do not want to change the security configuration (or you do not use mirroring at all) and want to stop getting such messages, you may disable this discovery. If you do not have mirroring and do not plan to use it, simply uninstall this discovery and the corresponding monitoring files.

SQL Configuration Manager may start snap-in of the wrong version

Issue: SQL Configuration Manager may start snap-in of the wrong version. E.g., SQL Server 2012 task starts sqlservermanager10.msc snap-in, which stands for SQL Server 2008.

Resolution: Console tasks require the installation of management tools corresponding to the target SQL Server Instance on the server where they are launched.

SQL DB Engine Service Monitor may fail if "Alert only if service startup type is automatic" override parameter is set to "FALSE"

Issue: SQL DB Engine Service Monitor may fail if "Alert only if service startup type is automatic" override parameter is manually set to "FALSE", and the string is put in uppercase.

Resolution: When overriding the abovementioned parameter, put the string to lowercase.

Some monitors may fail if a database name contains quotes.

Issue: The following monitors may fail if a database name contains two consecutive single quotation marks:

- Database Backup Status

- Auto Update Statistics Configuration
- Auto Update Statistics Async Configuration
- DB Chaining Configuration
- Recovery Model Configuration
- Page Verify Configuration
- Trustworthy Configuration
- Auto Close Configuration
- Auto Create Statistics Configuration
- Auto Shrink Configuration
- Database Status
- Database Health Policy
- Database Health Policy
- Availability Replicas Connection monitor
- Availability Group Automatic Failover monitor
- Availability Replica Connection
- Availability Replica Join State
- Synchronous Replicas Data Synchronization monitor
- WSFC Cluster monitor
- Availability Database Suspension State
- Availability Replica Role
- Availability Group Online monitor
- Availability Replica Data Synchronization
- Availability Replicas Role monitor
- Availability Replicas Data Synchronization monitor
- Availability Database Data Synchronization
- Availability Database Join State
- Availability Replica Health Policy
- Availability Replica Health Policy
- Database Replica Health Policy
- Database Replica Health Policy
- Availability Group Health Policy
- Availability Group Health Policy

Resolution: No resolution.

Some event log rules may not generate alerts for SQL deadlocks

Issue: Some event log rules may not generate alerts in the Operations Manager for certain SQL deadlocks because such events are not logged by SQL server by default in order to prevent possible surcharge on the event log and the agent.

Resolution: To switch on the logging of the events mentioned above, run the following command in SQL Server Management Studio:

Exec sp_altermessage [event ID], 'WITH_LOG', 'true'

*Select * from sys.messages where message_id=[event ID]*

Please remember that this action may lead to the overrun of the event log and the agent. Therefore, do not forget to switch off the logging of such events when you do not need it.

You can find the list of the corresponding event IDs in Appendix: Deadlocks Event Log Rules.

UNC path may not be supported while performance data collection

Issue: When the autogrowth option is switched on for a database file stored on a fileshare, the database may not be accessible for performance data collection through UNC path.

Resolution: Make sure that autogrowth option is switched off for the database.

Alerts of event-based rules are not displayed in the appropriate views

Issue: Alerts of event-based rules are displayed in the root SQL view instead of appropriate child views.

Resolution: No resolution.

Upon restart of an agent, workflows may throw WMI-related errors to the event log

Issue: Upon agent restart, workflows start working simultaneously. At that, the cached value can be outdated or non-existent and part of the workflows will get errors from WMI.

Resolution: No resolution.

SQL Policy discovery may work incorrectly

Issue: SQL Policy discovery may produce the following issues:

1. A query that gets the list of databases has the following filter: *AND name not in ('master', 'model', 'msdb', 'tempdb', 'distribution')*, while replication distribution databases can have different names.
2. The discovery assumes that the policy is targeted on all databases, while actually any target can be specified separately (for example, a database with particular name, with an ID greater than a certain value etc.).

Resolution: No resolution is available for the first issue. Resolution for the second issue is as follows: exclude policies that are not targeted on all databases.

Enabling of “Auto Close” database parameter blocks collection of the performance metrics

Issue: If “Auto Close” parameter for the database is set to “True", all performance rules return empty values.

Resolution: Set “Auto Close” database parameter back to “False”.

Double quotes in a database name may cause database console tasks failures

Issue: Database console tasks take database names enclosed in double quotes as one of their arguments. A database name may contain any symbol including double quotes. If it does, the console tasks for this database will not work.

Resolution: No resolution.

“Database Status” monitor is constantly changing its status

Issue: If “Auto Close” parameter for the database is set to “True", “Database Status” monitor is constantly changing its status from “Healthy” to “Recovering/Restoring” and vice versa according to the timeout set in the override parameters.

Resolution: In view of the monitoring operation specifics, no resolution is required.

“Out of memory” errors are received in the Operations Manager

Issue: “Out of memory” errors are regularly received in the Operations Manager while the server has plenty of memory, and the instances are part of an Availability Group.

Resolution: Isolate the SQL Server WMI provider and increase the UploadTimeout.
To isolate the provider in its own host, follow the steps below from an elevated PowerShell (the namespace *ComputerManagement11* is for SQL 2012 and *ComputerManagement10* is for 2008 & 2008 R2):

$a = [WMI]'Root\Microsoft\SqlServer\ComputerManagement11:__Win32Provider.name="MSSQL_ManagementProvider"'

$a.HostingModel = "NetworkServiceHost:SQL"

$a.put()

To revert the change:

$a = [WMI]'Root\Microsoft\SqlServer\ComputerManagement11:__Win32Provider.name="MSSQL_ManagementProvider"'

$a.HostingModel = "NetworkServiceHost"

$a.put()

To increase the unload timeout to 30 minutes, follow these steps:

- Open WBEMTEST.
- Click the “Connect” button.
- In the “Namespace”, enter *Root\Microsoft\SqlServer\ComputerManagement11*, and then click the “Connect” button.

- Click the “Query” button.
- Enter *select * from __win32provider where name = 'MSSQL_ManagementProvider',* then click the “Apply” button.
- Double-click the resulting row.
- Double-click the “UnloadTimeout” value.
- Select “Not NULL” level, enter *00000000003000.000000:000,* and then click the “Save Property” button.
- Click the “Save Object” button.
- Click the “Close” button.

“WSFC Cluster” monitor is in the unhealthy state although the WSFC Service is running with no issues

Issue: The monitor “WSFC Cluster” is in the unhealthy state, however, the WSFC Service on an appropriate Windows Cluster node is operating normally. This happens when the SQL MP monitoring account does not have permissions on sys.xp_instance_regread.

Resolution: Grant the monitoring account with the execute permission on sys.xp_instance_regread:

GRANT EXECUTE ON [sys].[xp_instance_regread] TO ['<YourMonitoringAccount>'];

Appendix: Reports

You can use the reports of SQL Server Management Pack to track trends or changes across days, weeks, or months. The following tables describe the available SQL Server reports.

Capacity Information Reports

Report	Class	Description
SQL Broker Performance	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	Displays a chart with the following performance items: • Activation stored procedures invoked per second statistics • Activation task limit reached • Activation task limit reached per second statistics • Activation tasks aborted • Messages per second placed in the queue • Transport messages per second placed in the queue • SQL RECEIVEs per second • SQL SENDs per second • Tasks started per second • Total transaction rollbacks • Transport message fragment RECEIVEs per second • Transport message fragments

Report	Class	Description
		• Transport open connection count statistics • Transport receive I/Os per second • Transport Send I/Os per second
SQL Server Database Counters	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	Displays a chart with the following performance items. • Buffer cache hit ratio • Lock timeouts per second • Number of deadlocks per second • SQL recompiles per second • Transactions per second

Operations Information Reports

Report	Class	Description
SQL Server Configuration	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	When the objects supplied are of the type SQL DB Engine, displays the following discovered properties. • Audit level • Authentication mode • Cluster • Enable error reporting • Error log location • Language • Master database location

Report	Class	Description
		• Master database log location • Service pack version • Replication distribution database • Replication working directory • Version
SQL Server Lock Analysis	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	When the objects supplied are of the type SQL DB Engine, displays a chart with the performance item, Number of deadlocks per second.
SQL Server Service pack	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	When the objects supplied are of type SQL DB Engine or ServicePackVersion, displays the following discovered properties: • Service Pack Version • Version
SQL User Activity	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	For each selected object, displays a chart with the performance item, Logins per second. Data is aggregated to days of a month.
Top 5 Deadlocked Databases	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	Displays a chart with the top five deadlocked databases and a table detailing the databases and their counter values.
User Connections by Day	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	When the objects supplied are of type SQL DB Engine, displays a chart for each selected object with the performance item, SQL user connections.

Report	Class	Description
User Connections by Peak Hours	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	When the objects supplied are of the type SQL DB Engine, displays a chart for each selected object with the performance item, SQL user connections. Data is aggregated to days of a month.

Trend Information Reports

Report	Class	Description
SQL Database Space Report	Microsoft.SQLServer.2008.DBEngine Microsoft.SQLServer.2012.DBEngine	When the objects supplied are of the type SQL Database or a type derived from SQL Database, displays a chart for each selected object with the following performance items: • Database free space in MB • Database free space in percentage • Database space in MB • Transaction log free space in MB • Transaction log free space in percentage • Transaction log space in MB Data is aggregated to days of a month.

Appendix: Deadlocks Event Log Rules

Microsoft SQL Server 2008

- Microsoft.SQLServer.2008.MSDTC_on_server__is_unavailable_1_5_Rule eventID: 8501
- Microsoft.SQLServer.2008.Could_not_create_a_statement_object_using_OLE_DB_provider_1_5_Rule eventID: 7305
- Microsoft.SQLServer.2008.Could_not_create_an_instance_of_OLE_DB_provider_1_5_Rule eventID: 7302
- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_or_Database_Mirroring_Transport_stopped_5_Rule eventID: 9691
- Microsoft.SQLServer.2008.SQL_Server_SQL_Server_Service_Broker_attempted_to_use_an_unsupported_encryption_algorithm_5_Rule eventID: 28060
- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_transmitter_shut_down_due_to_an_exception_or_a_lack_of_memory_5_Rule eventID: 28073
- Microsoft.SQLServer.2008.An_error_occurred_in_the_Service_Broker_manager_5_Rule eventID: 9645
- Microsoft.SQLServer.2008.The_Service_Broker_Database_Mirroring_Transport_could_not_listen_for_connections_due_to_an_error_5_Rule eventID: 9693
- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_or_Database_Mirroring_is_running_in_FIPS_compliance_mode_5_Rule eventID: 28077
- Microsoft.SQLServer.2008.An_error_occurred_while_processing_SQL_Server_Service_Broker_mirroring_routes_5_Rule eventID: 9789
- Microsoft.SQLServer.2008.An_SQL_Server_Service_Broker_dialog_caught_an_error_5_Rule eventID: 9736
- Microsoft.SQLServer.2008.A_SQL_Server_Service_Broker_cryptographic_operation_failed_5_Rule eventID: 9641
- Microsoft.SQLServer.2008.Cannot_start_service_broker_activation_manager_5_Rule eventID: 9701
- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_could_not_query_the_FIPS_compliance_mode_flag_from_the_registry_5_Rule eventID: 28076
- Microsoft.SQLServer.2008.Cannot_start_SQL_Server_Service_Broker_on_Database_5_Rule eventID: 9697
- Microsoft.SQLServer.2008.The_SQL_Server_Service_Broker_or_Database_Mirroring_transport_is_disabled_or_not_configured_5_Rule eventID: 9666
- Microsoft.SQLServer.2008.Cannot_start_service_broker_manager_5_Rule eventID: 9694

- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_Manager_has_shutdown_5_Rule eventID: 9689
- Microsoft.SQLServer.2008.Service_Broker_was_not_able_to_allocate_memory_for_cryptographic_operations_5_Rule eventID: 9634
- Microsoft.SQLServer.2008.An_SNI_call_failed_during_a_Service_Broker_Database_Mirroring_transport_operation_1_5_Rule eventID: 8471
- Microsoft.SQLServer.2008.Cannot_start_service_broker_manager_due_to_operating_system_error_5_Rule eventID: 28002
- Microsoft.SQLServer.2008.A_SQL_Server_Service_Broker_procedure_output_results_5_Rule eventID: 9724
- Microsoft.SQLServer.2008.An_error_occurred_in_the_SQL_Server_Service_Broker_message_transmitter_5_Rule eventID: 28072
- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_cannot_use_RC4_encryption_algorithm_when_running_in_FIPS_compliance_mode_5_Rule eventID: 28078
- Microsoft.SQLServer.2008.An_error_occurred_in_the_Service_Broker_queue_rollback_handler_5_Rule eventID: 8405
- Microsoft.SQLServer.2008.SQL_Server_cannot_start_the_Service_Broker_event_handler_5_Rule eventID: 9696
- Microsoft.SQLServer.2008.An_error_occurred_in_the_SQL_Server_Service_Broker_or_Database_Mirroring_transport_manager_5_Rule eventID: 9643
- Microsoft.SQLServer.2008.An_error_occurred_in_a_SQL_Server_Service_Broker_Database_Mirroring_transport_connection_endpoint_1_5_Rule eventID: 9642
- Microsoft.SQLServer.2008.The_Service_Broker_Database_Mirroring_transport_cannot_listen_on_port_because_it_is_in_use_5_Rule eventID: 9692
- Microsoft.SQLServer.2008.Cannot_start_service_broker_security_manager_5_Rule eventID: 9698
- Microsoft.SQLServer.2008.An_error_occurred_in_the_timer_event_cache_5_Rule eventID: 9646
- Microsoft.SQLServer.2008.SQL_Server_could_not_allocate_enough_memory_to_start_Service_Broker_task_manager_5_Rule eventID: 9695
- Microsoft.SQLServer.2008.SQL_Server_Service_Broker_or_Database_Mirror_cryptographic_call_failed_5_Rule eventID: 9650
- Microsoft.SQLServer.2008.An_error_occurred_in_the_SQL_Server_Service_Broker_message_dispatcher_5_Rule eventID: 9644
- Microsoft.SQLServer.2008.SQLServerAgent_could_not_be_started_1_5_Rule eventID: 103
- Microsoft.SQLServer.2008.Unable_to_re_open_the_local_eventlog_1_5_Rule eventID: 313

- Microsoft.SQLServer.2008.Alert_engine_stopped_due_to_unrecoverable_local_eventlog_errors_1_5_Rule eventID: 317
- Microsoft.SQLServer.2008.Step_of_a_job_caused_an_exception_in_the_subsystem_1_5_Rule eventID: 209
- Microsoft.SQLServer.2008.A_SQL_job_failed_to_complete_successfully_1_5_Rule eventID: 208
- Microsoft.SQLServer.2008.The_agent_is_suspect._No_response_within_last_minutes_1_5_Rule eventID: 20554
- Microsoft.SQLServer.2008.Job_step_cannot_be_run_because_the_subsystem_failed_to_load_1_5_Rule eventID: 212
- Microsoft.SQLServer.2008.Unable_to_connect_to_SQL_Server_1_5_Rule eventID: 207
- Microsoft.SQLServer.2008.The_configuration_file_could_not_be_loaded_5_Rule eventID: 21
- Microsoft.SQLServer.2008.RESTORE_could_not_start_database_1_5_Rule eventID: 3167
- Microsoft.SQLServer.2008.Unexpected_end_of_file_while_reading_beginning_of_backup_set_1_5_Rule eventID: 3208
- Microsoft.SQLServer.2008.Cannot_open_backup_device.__1_5_Rule eventID: 3201
- Microsoft.SQLServer.2008.Database_cannot_be_opened_due_to_inaccessible_files_or_insufficient_memory_or_disk_space._See_the_SQL_Server_errorlog_for_details_1_5_Rule eventID: 945
- Microsoft.SQLServer.2008.CREATE_DATABASE_failed._Could_not_allocate_enough_disk_space_for_a_new_database_on_the_named_disks_1_5_Rule eventID: 1803
- Microsoft.SQLServer.2008.Could_not_obtain_exclusive_lock_on_database_5_Rule eventID: 1807
- Microsoft.SQLServer.2008.Full_Text_Search___Search_on_full_text_catalog_failed_with_unknown_result_1_5_Rule eventID: 7607
- Microsoft.SQLServer.2008.Full_Text_Search___Full_Text_Search_is_not_enabled_for_the_current_database._Use_sp_fulltext_database_to_enable_Full_Text_Search_1_5_Rule eventID: 15601
- Microsoft.SQLServer.2008.Failed_to_finish_full_text_operation._The_filegroup_is_empty_read_only_or_not_online_5_Rule eventID: 9964
- Microsoft.SQLServer.2008.Full_Text_Search___An_unknown_full_text_failure_occurred_1_5_Rule eventID: 7608
- Microsoft.SQLServer.2008.Full_Text_Search___Full_text_catalog_lacks_sufficient_disk_space_to_complete_this_operation_1_5_Rule eventID: 7622
- Microsoft.SQLServer.2008.Full_Text_Search___Full_text_catalog_is_in_a_unusable_state._Drop_and_re_create_this_full_text_catalog_1_5_Rule eventID: 7624

- Microsoft.SQLServer.2008.A_default_full_text_catalog_does_not_exist_in_the_database_or_user_does_not_have_permission_to_perform_this_action_5_Rule eventID: 9967
- Microsoft.SQLServer.2008.Full_Text_Search___Could_not_find_full_text_index_for_database_1_5_Rule eventID: 7606
- Microsoft.SQLServer.2008.Transaction_was_deadlocked_on_resources_with_another_process_and_has_been_chosen_as_the_deadlock_victim._Rerun_the_transaction_1_5_Rule eventID: 1205
- Microsoft.SQLServer.2008.The_provider_reported_an_unexpected_catastrophic_failure_1_5_Rule eventID: 10001
- Microsoft.SQLServer.2008.The_query_processor_could_not_start_the_necessary_thread_resources_for_parallel_query_execution_1_5_Rule eventID: 8642
- Microsoft.SQLServer.2008.IS_Service_has_attempted_to_stop_a_running_package_5_Rule eventID: 336
- Microsoft.SQLServer.2008.IS_Service_failed_to_load_user_defined_Configuration_file_5_Rule eventID: 272
- Microsoft.SQLServer.2008.Internal_Query_Processor_Error__The_query_processor_ran_out_of_stack_space_during_query_optimization_1_5_Rule eventID: 8621
- Microsoft.SQLServer.2008.Internal_Query_Processor_Error__The_query_processor_could_not_obtain_access_to_a_required_interface_1_5_Rule eventID: 8601
- Microsoft.SQLServer.2008.Internal_Query_Processor_Error__The_query_processor_encountered_an_unexpected_error_during_execution_1_5_Rule eventID: 8630
- Microsoft.SQLServer.2008.Internal_Query_Processor_Error__The_query_processor_encountered_an_unexpected_error_during_the_processing_of_a_remote_query_phase_1_5_Rule eventID: 8680
- Microsoft.SQLServer.2008.The_query_has_been_canceled_because_the_estimated_cost_of_this_query_exceeds_the_configured_threshold._Contact_the_system_administrator_1_5_Rule eventID: 8649
- Microsoft.SQLServer.2008.Login_failed__Password_too_simple_5_Rule eventID: 18466
- Microsoft.SQLServer.2008.Login_failed__Password_too_short_5_Rule eventID: 18464
- Microsoft.SQLServer.2008.Login_failed__Error_during_validation_5_Rule eventID: 18468
- Microsoft.SQLServer.2008.Could_not_obtain_information_about_Windows_NT_group_user_1_5_Rule eventID: 15404
- Microsoft.SQLServer.2008.Cannot_open_user_default_database._Login_failed_1_5_Rule eventID: 4064
- Microsoft.SQLServer.2008.Login_failed__Password_fails_password_filter_DLL_requirements_5_Rule eventID: 18467
- Microsoft.SQLServer.2008.Cannot_determine_the_service_account_for_SQL_Server_instance_1_5_Rule eventID: 14353

- Microsoft.SQLServer.2008.Permission_denied_on_object_1_5_Rule eventID: 229
- Microsoft.SQLServer.2008.Login_failed__Password_cannot_be_used_at_this_time_5_Rule eventID: 18463
- Microsoft.SQLServer.2008.Login_failed__Password_too_long_5_Rule eventID: 18465
- Microsoft.SQLServer.2008.Table_error__Page_allocated_to_object_was_not_seen.__Page_may_be_invalid_or_have_incorrect_object_ID_information_in_its_header_1_5_Rule eventID: 2533
- Microsoft.SQLServer.2008.Table_error__B_tree_level_mismatch_page_does_not_match_level_from_parent__1_5_Rule eventID: 8931
- Microsoft.SQLServer.2008.CHECKTABLE_processing_of_object_encountered_page_twice._Possible_internal_error_or_allocation_fault_1_5_Rule eventID: 8973
- Microsoft.SQLServer.2008.Table_error___Unexpected_page_type__1_5_Rule eventID: 8938
- Microsoft.SQLServer.2008.Table_error__Extra_or_invalid_key_1_5_Rule eventID: 8952
- Microsoft.SQLServer.2008.Table_error__cross_object_chain_linkage_1_5_Rule eventID: 8930
- Microsoft.SQLServer.2008.Table_error__Wrong_PageId_in_the_page_header_1_5_Rule eventID: 8909
- Microsoft.SQLServer.2008.Table_error__page_is_out_of_the_range_of_this_database_1_5_Rule eventID: 8968
- Microsoft.SQLServer.2008.Conflict_table__does_not_exist_1_5_Rule eventID: 21286
- Microsoft.SQLServer.2008.Table_error__Cross_object_linkage_1_5_Rule eventID: 8925
- Microsoft.SQLServer.2008.CHECKTABLE_terminated._A_failure_was_detected_while_collecting_facts._Possibly_tempdb_out_of_space_or_a_system_table_is_inconsistent._Check_previous_errors_1_5_Rule eventID: 8921
- Microsoft.SQLServer.2008.Table_error__Column_is_not_a_valid_complex_column_1_5_Rule eventID: 8960
- Microsoft.SQLServer.2008.Table_error__Page_is_missing_a_reference_from_previous_page._Possible_chain_linkage_problem_1_5_Rule eventID: 8978
- Microsoft.SQLServer.2008.The_Log_Reader_Agent_for_transactional_replication_encountered_an_invalid_log_sequence_number__LSN__when_reading_the_transaction_log_5_Rule eventID: 18762
- Microsoft.SQLServer.2008.Table_error__Page_was_not_seen_in_the_scan_although_its_parent_and_previous_refer_to_it._Check_any_previous_errors_1_5_Rule eventID: 8976
- Microsoft.SQLServer.2008.Table_error__Cross_object_linkage__Parent_page_in_object_next_refer_to_page_not_in_the_same_object_1_5_Rule eventID: 8926
- Microsoft.SQLServer.2008.Table_error__B_tree_page_has_two_parent_nodes__1_5_Rule eventID: 8937

- Microsoft.SQLServer.2008.Table_error__Slot_row_extends_into_free_space__1_5_Rule eventID: 8943
- Microsoft.SQLServer.2008.Table_error__Object_index_page_Test_failed._Slot___Offset _is__invalid_1_5_Rule eventID: 8941
- Microsoft.SQLServer.2008.Could_not_find_filegroup_ID_in_sys.filegroups_for_database _5_Rule eventID: 8932
- Microsoft.SQLServer.2008.The_user_is_not_allowed_to_truncate_the_system_table_1_ 5_Rule eventID: 4709
- Microsoft.SQLServer.2008.Failed_to_drop_column__from_table__1_5_Rule eventID: 21284
- Microsoft.SQLServer.2008.Table_error__Page_is_missing_references_from_parent__un known__and_previous_nodes._Possible_bad_root_entry_in_sysindexes_1_5_Rule eventID: 8979
- Microsoft.SQLServer.2008.Table_error__Page_in_its_header_is_allocated_by_another_ object_1_5_Rule eventID: 2534
- Microsoft.SQLServer.2008.Table_error__The_text_ntext_or_image_node_at_page__is_r eferenced_by_page_not_seen_in_the_scan_1_5_Rule eventID: 8965
- Microsoft.SQLServer.2008.Table_error___Test_failed._Slot_overlaps_with_the_prior_ro w_1_5_Rule eventID: 8942
- Microsoft.SQLServer.2008.Table_error__IAM_page_is_linked_in_the_IAM_chain_for_obj ect_1_5_Rule eventID: 8959
- Microsoft.SQLServer.2008.Table_error__Extent_object_is_beyond_the_range_of_this_d atabase_1_5_Rule eventID: 2579
- Microsoft.SQLServer.2008.Table___No_columns_without_statistics_found_1_5_Rule eventID: 15013
- Microsoft.SQLServer.2008.Table_error__The_high_key_value_on_page_is_not_less_tha n_the_low_key_value_in_the_parent_slot_of_the_next_page_1_5_Rule eventID: 8934
- Microsoft.SQLServer.2008.Table_error__Allocation_page_has_invalid__page_header_v alues.__1_5_Rule eventID: 8946
- Microsoft.SQLServer.2008.Table_error__IAM_chain_linkage_error_1_5_Rule eventID: 8969
- Microsoft.SQLServer.2008.Table_error___The_next_pointer_of_refers_to_page._Neither _its_parent_were_encountered._Possible_bad_chain_linkage_1_5_Rule eventID: 8981
- Microsoft.SQLServer.2008.Table_error__The_text_ntext_or_image_node_has_wrong_ty pe_1_5_Rule eventID: 8963
- Microsoft.SQLServer.2008.Table_error__The_text_ntext_or_image_node_at_page_is_no t_referenced_1_5_Rule eventID: 8964
- Microsoft.SQLServer.2008.Table_error___Address_is_not_aligned_1_5_Rule eventID: 8940

- Microsoft.SQLServer.2008.One_or_more_indexes_are_damaged_and_must_be_repaired_or_dropped_1_5_Rule eventID: 8956
- Microsoft.SQLServer.2008.Table_error__Cross_object_linkage._Page_PGID_next_is_not_in_the_same_index_1_5_Rule eventID: 8982
- Microsoft.SQLServer.2008.Table_error__Parent_node_for_page_was_not_encountered_1_5_Rule eventID: 8977
- Microsoft.SQLServer.2008.Indexed_view_does_not_contain_all_rows_that_the_view_definition_produces.__Refer_to_Books_Online_for_more_information_on_this_error.__This_does_not_necessarily_represent_an_integrity_issue_with_th_5_Rule eventID: 8908
- Microsoft.SQLServer.2008.Table_error__Table_missing_or_invalid_key_in_index_for_the_row__1_5_Rule eventID: 8951
- Microsoft.SQLServer.2008.Unique_table_computation_failed_1_5_Rule eventID: 16959
- Microsoft.SQLServer.2008.Table__Creating_statistics_for_the_following_columns_1_5_Rule eventID: 15018
- Microsoft.SQLServer.2008.Table_error__B_tree_chain_linkage_mismatch.__1_5_Rule eventID: 8936
- Microsoft.SQLServer.2008.Failed_to_add_column__to_table__1_5_Rule eventID: 21285
- Microsoft.SQLServer.2008.Table_error__Index_node_page_refers_to_child_page_and_previous_child_but_they_were_not_encountered_1_5_Rule eventID: 8980
- Microsoft.SQLServer.2008.Table_error__The_low_key_value_on_page__is_not_the_key_value_in_the_parent_1_5_Rule eventID: 8933
- Microsoft.SQLServer.2008.Table_error__The_previous_link_on_page_does_not_match_the_previous_page_that_the_parent_slot_expects_for_this_page_1_5_Rule eventID: 8935
- Microsoft.SQLServer.2008.XML___XML_parsing_error_1_5_Rule eventID: 6603
- Microsoft.SQLServer.2008.XML___XML_document_could_not_be_created_because_server_memory_is_low._Use_sp_xml_removedocument_to_release_XML_documents_1_5_Rule eventID: 6624
- Microsoft.SQLServer.2008.XML___Size_of_data_chunk_requested_from_the_stream_exceeds_allowed_limit_5_Rule eventID: 6627
- Microsoft.SQLServer.2008.XML___Failed_to_load_Msxml2.dll_1_5_Rule eventID: 6610
- Microsoft.SQLServer.2008.XML___Failed_to_instantiate_class._Make_sure_Msxml2.dll_exists_in_the_SQL_Server_installation_1_5_Rule eventID: 6608
- Microsoft.SQLServer.2008.XML___FOR_XML_EXPLICIT_stack_overflow_occurred._Circular_parent_tag_relationships_are_not_allowed_1_5_Rule eventID: 6805
- Microsoft.SQLServer.2008.XML___XML_error_1_5_Rule eventID: 6600
- Microsoft.SQLServer.2008.Script_Failed_Database_Login eventID: 4001
- Microsoft.SQLServer.2008.ReplicationAgentFailureRule eventID: 20536

- Microsoft.SQLServer.2008.FailedToCreateSubdirectoryUnderReplicationWorkingDirectoryRule eventID: 21330
- Microsoft.SQLServer.2008.ArticleUpdateSuccessfulRule eventID: 14025
- Microsoft.SQLServer.2008.BeginLSNSpecifiedForReplicationLogscanInvalidRule eventID: 18765
- Microsoft.SQLServer.2008.CouldNotCleanUpDistributionHistoryTablesRule eventID: 20553
- Microsoft.SQLServer.2008.LoginAccountIsNotInThePublicationAccessListRule eventID: 21049
- Microsoft.SQLServer.2008.ReplicationAgentSuccessRule eventID: 20540
- Microsoft.SQLServer.2008.AnotherLogReaderIsReplicatingDatabaseRule eventID: 18752
- Microsoft.SQLServer.2008.CouldNotAllocateMemoryForReplicationRule eventID: 18755
- Microsoft.SQLServer.2008.SchemaReplicationFailedRule eventID: 21198
- Microsoft.SQLServer.2008.SystemTablesForMergeReplicationCouldNotBeDroppedSuccessfullyRule eventID: 20007
- Microsoft.SQLServer.2008.ErrorOccurredWhileWaitingOnArticleCacheAccessEventRule eventID: 18776
- Microsoft.SQLServer.2008.InitialSnapshotForPublicationIsNotYetAvailableRule eventID: 21075
- Microsoft.SQLServer.2008.SpecifiedLSNForRepldoneLogscanOccursBeforeTheCurrentStartOfReplicationInTheLogRule eventID: 18768
- Microsoft.SQLServer.2008.CouldNotGetReplicationInformationForTableRule eventID: 18756
- Microsoft.SQLServer.2008.SubscriptionStatusCouldNotBeChangedRule eventID: 14070
- Microsoft.SQLServer.2008.LogReaderAgentEncounteredUnexpectedLogRecordOfTypeWhileProcessingDMLOperationRule eventID: 18775
- Microsoft.SQLServer.2008.ArticleCouldNotBeAddedToPublicationRule eventID: 20009
- Microsoft.SQLServer.2008.CouldNotRemovePublicationFromADRule eventID: 21369

Microsoft SQL Server 2012

- Microsoft.SQLServer.2012.MSDTC_on_server__is_unavailable_1_5_Rule eventID: 8501
- Microsoft.SQLServer.2012.Could_not_create_a_statement_object_using_OLE_DB_provider_1_5_Rule eventID: 7305
- Microsoft.SQLServer.2012.Could_not_create_an_instance_of_OLE_DB_provider_1_5_Rule eventID: 7302

- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_or_Database_Mirroring_Transport_stopped_5_Rule eventID: 9691
- Microsoft.SQLServer.2012.SQL_Server_SQL_Server_Service_Broker_attempted_to_use_an_unsupported_encryption_algorithm_5_Rule eventID: 28060
- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_transmitter_shut_down_due_to_an_exception_or_a_lack_of_memory_5_Rule eventID: 28073
- Microsoft.SQLServer.2012.An_error_occurred_in_the_Service_Broker_manager_5_Rule eventID: 9645
- Microsoft.SQLServer.2012.The_Service_Broker_Database_Mirroring_Transport_could_not_listen_for_connections_due_to_an_error_5_Rule eventID: 9693
- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_or_Database_Mirroring_is_running_in_FIPS_compliance_mode_5_Rule eventID: 28077
- Microsoft.SQLServer.2012.An_error_occurred_while_processing_SQL_Server_Service_Broker_mirroring_routes_5_Rule eventID: 9789
- Microsoft.SQLServer.2012.An_SQL_Server_Service_Broker_dialog_caught_an_error_5_Rule eventID: 9736
- Microsoft.SQLServer.2012.A_SQL_Server_Service_Broker_cryptographic_operation_failed_5_Rule eventID: 9641
- Microsoft.SQLServer.2012.Cannot_start_service_broker_activation_manager_5_Rule eventID: 9701
- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_could_not_query_the_FIPS_compliance_mode_flag_from_the_registry_5_Rule eventID: 28076
- Microsoft.SQLServer.2012.Cannot_start_SQL_Server_Service_Broker_on_Database_5_Rule eventID: 9697
- Microsoft.SQLServer.2012.The_SQL_Server_Service_Broker_or_Database_Mirroring_transport_is_disabled_or_not_configured_5_Rule eventID: 9666
- Microsoft.SQLServer.2012.Cannot_start_service_broker_manager_5_Rule eventID: 9694
- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_Manager_has_shutdown_5_Rule eventID: 9689
- Microsoft.SQLServer.2012.Service_Broker_was_not_able_to_allocate_memory_for_cryptographic_operations_5_Rule eventID: 9634
- Microsoft.SQLServer.2012.An_SNI_call_failed_during_a_Service_Broker_Database_Mirroring_transport_operation_1_5_Rule eventID: 8471
- Microsoft.SQLServer.2012.Cannot_start_service_broker_manager_due_to_operating_system_error_5_Rule eventID: 28002
- Microsoft.SQLServer.2012.A_SQL_Server_Service_Broker_procedure_output_results_5_Rule eventID: 9724

- Microsoft.SQLServer.2012.An_error_occurred_in_the_SQL_Server_Service_Broker_message_transmitter_5_Rule eventID: 28072
- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_cannot_use_RC4_encryption_algorithm_when_running_in_FIPS_compliance_mode_5_Rule eventID: 28078
- Microsoft.SQLServer.2012.An_error_occurred_in_the_Service_Broker_queue_rollback_handler_5_Rule eventID: 8405
- Microsoft.SQLServer.2012.SQL_Server_cannot_start_the_Service_Broker_event_handler_5_Rule eventID: 9696
- Microsoft.SQLServer.2012.An_error_occurred_in_the_SQL_Server_Service_Broker_or_Database_Mirroring_transport_manager_5_Rule eventID: 9643
- Microsoft.SQLServer.2012.An_error_occurred_in_a_SQL_Server_Service_Broker_Database_Mirroring_transport_connection_endpoint_1_5_Rule eventID: 9642
- Microsoft.SQLServer.2012.The_Service_Broker_Database_Mirroring_transport_cannot_listen_on_port_because_it_is_in_use_5_Rule eventID: 9692
- Microsoft.SQLServer.2012.Cannot_start_service_broker_security_manager_5_Rule eventID: 9698
- Microsoft.SQLServer.2012.An_error_occurred_in_the_timer_event_cache_5_Rule eventID: 9646
- Microsoft.SQLServer.2012.SQL_Server_could_not_allocate_enough_memory_to_start_Service_Broker_task_manager_5_Rule eventID: 9695
- Microsoft.SQLServer.2012.SQL_Server_Service_Broker_or_Database_Mirror_cryptographic_call_failed_5_Rule eventID: 9650
- Microsoft.SQLServer.2012.An_error_occurred_in_the_SQL_Server_Service_Broker_message_dispatcher_5_Rule eventID: 9644
- Microsoft.SQLServer.2012.SQLServerAgent_could_not_be_started_1_5_Rule eventID: 103
- Microsoft.SQLServer.2012.Unable_to_re_open_the_local_eventlog_1_5_Rule eventID: 313
- Microsoft.SQLServer.2012.Alert_engine_stopped_due_to_unrecoverable_local_eventlog_errors_1_5_Rule eventID: 317
- Microsoft.SQLServer.2012.Step_of_a_job_caused_an_exception_in_the_subsystem_1_5_Rule eventID: 209
- Microsoft.SQLServer.2012.A_SQL_job_failed_to_complete_successfully_1_5_Rule eventID: 208
- Microsoft.SQLServer.2012.The_agent_is_suspect._No_response_within_last_minutes_1_5_Rule eventID: 20554
- Microsoft.SQLServer.2012.Job_step_cannot_be_run_because_the_subsystem_failed_to_load_1_5_Rule eventID: 212
- Microsoft.SQLServer.2012.Unable_to_connect_to_SQL_Server_1_5_Rule eventID: 207

- Microsoft.SQLServer.2012.The_configuration_file_could_not_be_loaded_5_Rule eventID: 21
- Microsoft.SQLServer.2012.RESTORE_could_not_start_database_1_5_Rule eventID: 3167
- Microsoft.SQLServer.2012.Unexpected_end_of_file_while_reading_beginning_of_backup_set_1_5_Rule eventID: 3208
- Microsoft.SQLServer.2012.Cannot_open_backup_device.__1_5_Rule eventID: 3201
- Microsoft.SQLServer.2012.Database_cannot_be_opened_due_to_inaccessible_files_or_insufficient_memory_or_disk_space._See_the_SQL_Server_errorlog_for_details_1_5_Rule eventID: 945
- Microsoft.SQLServer.2012.CREATE_DATABASE_failed._Could_not_allocate_enough_disk_space_for_a_new_database_on_the_named_disks_1_5_Rule eventID: 1803
- Microsoft.SQLServer.2012.Could_not_obtain_exclusive_lock_on_database_5_Rule eventID: 1807
- Microsoft.SQLServer.2012.Full_Text_Search___Search_on_full_text_catalog_failed_with_unknown_result_1_5_Rule eventID: 7607
- Microsoft.SQLServer.2012.Full_Text_Search___Full_Text_Search_is_not_enabled_for_the_current_database._Use_sp_fulltext_database_to_enable_Full_Text_Search_1_5_Rule eventID: 15601
- Microsoft.SQLServer.2012.Failed_to_finish_full_text_operation._The_filegroup_is_empty_read_only_or_not_online_5_Rule eventID: 9964
- Microsoft.SQLServer.2012.Full_Text_Search___An_unknown_full_text_failure_occurred_1_5_Rule eventID: 7608
- Microsoft.SQLServer.2012.Full_Text_Search___Full_text_catalog_lacks_sufficient_disk_space_to_complete_this_operation_1_5_Rule eventID: 7622
- Microsoft.SQLServer.2012.Full_Text_Search___Full_text_catalog_is_in_a_unusable_state._Drop_and_re_create_this_full_text_catalog_1_5_Rule eventID: 7624
- Microsoft.SQLServer.2012.A_default_full_text_catalog_does_not_exist_in_the_database_or_user_does_not_have_permission_to_perform_this_action_5_Rule eventID: 9967
- Microsoft.SQLServer.2012.Full_Text_Search___Could_not_find_full_text_index_for_database_1_5_Rule eventID: 7606
- Microsoft.SQLServer.2012.Transaction_was_deadlocked_on_resources_with_another_process_and_has_been_chosen_as_the_deadlock_victim._Rerun_the_transaction_1_5_Rule eventID: 1205
- Microsoft.SQLServer.2012.The_provider_reported_an_unexpected_catastrophic_failure_1_5_Rule eventID: 10001
- Microsoft.SQLServer.2012.The_query_processor_could_not_start_the_necessary_thread_resources_for_parallel_query_execution_1_5_Rule eventID: 8642

- Microsoft.SQLServer.2012.IS_Service_has_attempted_to_stop_a_running_package_5_Rule eventID: 336
- Microsoft.SQLServer.2012.IS_Service_failed_to_load_user_defined_Configuration_file_5_Rule eventID: 272
- Microsoft.SQLServer.2012.Internal_Query_Processor_Error__The_query_processor_ran_out_of_stack_space_during_query_optimization_1_5_Rule eventID: 8621
- Microsoft.SQLServer.2012.Internal_Query_Processor_Error__The_query_processor_could_not_obtain_access_to_a_required_interface_1_5_Rule eventID: 8601
- Microsoft.SQLServer.2012.Internal_Query_Processor_Error__The_query_processor_encountered_an_unexpected_error_during_execution_1_5_Rule eventID: 8630
- Microsoft.SQLServer.2012.Internal_Query_Processor_Error__The_query_processor_encountered_an_unexpected_error_during_the_processing_of_a_remote_query_phase_1_5_Rule eventID: 8680
- Microsoft.SQLServer.2012.The_query_has_been_canceled_because_the_estimated_cost_of_this_query_exceeds_the_configured_threshold._Contact_the_system_administrator_1_5_Rule eventID: 8649
- Microsoft.SQLServer.2012.Login_failed__Password_too_simple_5_Rule eventID: 18466
- Microsoft.SQLServer.2012.Login_failed__Password_too_short_5_Rule eventID: 18464
- Microsoft.SQLServer.2012.Login_failed__Error_during_validation_5_Rule eventID: 18468
- Microsoft.SQLServer.2012.Could_not_obtain_information_about_Windows_NT_group_user_1_5_Rule eventID: 15404
- Microsoft.SQLServer.2012.Cannot_open_user_default_database._Login_failed_1_5_Rule eventID: 4064
- Microsoft.SQLServer.2012.Login_failed__Password_fails_password_filter_DLL_requirements_5_Rule eventID: 18467
- Microsoft.SQLServer.2012.Cannot_determine_the_service_account_for_SQL_Server_instance_1_5_Rule eventID: 14353
- Microsoft.SQLServer.2012.Permission_denied_on_object_1_5_Rule eventID: 229
- Microsoft.SQLServer.2012.Login_failed__Password_cannot_be_used_at_this_time_5_Rule eventID: 18463
- Microsoft.SQLServer.2012.Login_failed__Password_too_long_5_Rule eventID: 18465
- Microsoft.SQLServer.2012.Table_error__Page_allocated_to_object_was_not_seen.__Page_may_be_invalid_or_have_incorrect_object_ID_information_in_its_header_1_5_Rule eventID: 2533
- Microsoft.SQLServer.2012.Table_error__B_tree_level_mismatch_page_does_not_match_level_from_parent__1_5_Rule eventID: 8931
- Microsoft.SQLServer.2012.CHECKTABLE_processing_of_object_encountered_page_twice._Possible_internal_error_or_allocation_fault_1_5_Rule eventID: 8973

- Microsoft.SQLServer.2012.Table_error___Unexpected_page_type__1_5_Rule eventID: 8938
- Microsoft.SQLServer.2012.Table_error__Extra_or_invalid_key_1_5_Rule eventID: 8952
- Microsoft.SQLServer.2012.Table_error__cross_object_chain_linkage_1_5_Rule eventID: 8930
- Microsoft.SQLServer.2012.Table_error__Wrong_PageId_in_the_page_header_1_5_Rule eventID: 8909
- Microsoft.SQLServer.2012.Table_error__page_is_out_of_the_range_of_this_database_1_5_Rule eventID: 8968
- Microsoft.SQLServer.2012.Conflict_table__does_not_exist_1_5_Rule eventID: 21286
- Microsoft.SQLServer.2012.Table_error__Cross_object_linkage_1_5_Rule eventID: 8925
- Microsoft.SQLServer.2012.CHECKTABLE_terminated._A_failure_was_detected_while_collecting_facts._Possibly_tempdb_out_of_space_or_a_system_table_is_inconsistent._Check_previous_errors_1_5_Rule eventID: 8921
- Microsoft.SQLServer.2012.Table_error__Column_is_not_a_valid_complex_column_1_5_Rule eventID: 8960
- Microsoft.SQLServer.2012.Table_error__Page_is_missing_a_reference_from_previous_page._Possible_chain_linkage_problem_1_5_Rule eventID: 8978
- Microsoft.SQLServer.2012.The_Log_Reader_Agent_for_transactional_replication_encountered_an_invalid_log_sequence_number__LSN__when_reading_the_transaction_log_5_Rule eventID: 18762
- Microsoft.SQLServer.2012.Table_error__Page_was_not_seen_in_the_scan_although_its_parent_and_previous_refer_to_it._Check_any_previous_errors_1_5_Rule eventID: 8976
- Microsoft.SQLServer.2012.Table_error__Cross_object_linkage__Parent_page_in_object_next_refer_to_page_not_in_the_same_object_1_5_Rule eventID: 8926
- Microsoft.SQLServer.2012.Table_error__B_tree_page_has_two_parent_nodes__1_5_Rule eventID: 8937
- Microsoft.SQLServer.2012.Table_error__Slot_row_extends_into_free_space__1_5_Rule eventID: 8943
- Microsoft.SQLServer.2012.Table_error__Object_index_page_Test_failed._Slot___Offset_is__invalid_1_5_Rule eventID: 8941
- Microsoft.SQLServer.2012.Could_not_find_filegroup_ID_in_sys.filegroups_for_database_5_Rule eventID: 8932
- Microsoft.SQLServer.2012.The_user_is_not_allowed_to_truncate_the_system_table_1_5_Rule eventID: 4709
- Microsoft.SQLServer.2012.Failed_to_drop_column__from_table__1_5_Rule eventID: 21284

- Microsoft.SQLServer.2012.Table_error__Page_is_missing_references_from_parent__unknown__and_previous_nodes._Possible_bad_root_entry_in_sysindexes_1_5_Rule eventID: 8979
- Microsoft.SQLServer.2012.Table_error__Page_in_its_header_is_allocated_by_another_object_1_5_Rule eventID: 2534
- Microsoft.SQLServer.2012.Table_error__The_text_ntext_or_image_node_at_page__is_referenced_by_page_not_seen_in_the_scan_1_5_Rule eventID: 8965
- Microsoft.SQLServer.2012.Table_error___Test_failed._Slot_overlaps_with_the_prior_row_1_5_Rule eventID: 8942
- Microsoft.SQLServer.2012.Table_error__IAM_page_is_linked_in_the_IAM_chain_for_object_1_5_Rule eventID: 8959
- Microsoft.SQLServer.2012.Table_error__Extent_object_is_beyond_the_range_of_this_database_1_5_Rule eventID: 2579
- Microsoft.SQLServer.2012.Table___No_columns_without_statistics_found_1_5_Rule eventID: 15013
- Microsoft.SQLServer.2012.Table_error__The_high_key_value_on_page_is_not_less_than_the_low_key_value_in_the_parent_slot_of_the_next_page_1_5_Rule eventID: 8934
- Microsoft.SQLServer.2012.Table_error__Allocation_page_has_invalid__page_header_values.__1_5_Rule eventID: 8946
- Microsoft.SQLServer.2012.Table_error__IAM_chain_linkage_error_1_5_Rule eventID: 8969
- Microsoft.SQLServer.2012.Table_error___The_next_pointer_of_refers_to_page._Neither_its_parent_were_encountered._Possible_bad_chain_linkage_1_5_Rule eventID: 8981
- Microsoft.SQLServer.2012.Table_error__The_text_ntext_or_image_node_has_wrong_type_1_5_Rule eventID: 8963
- Microsoft.SQLServer.2012.Table_error__The_text_ntext_or_image_node_at_page_is_not_referenced_1_5_Rule eventID: 8964
- Microsoft.SQLServer.2012.Table_error___Address_is_not_aligned_1_5_Rule eventID: 8940
- Microsoft.SQLServer.2012.One_or_more_indexes_are_damaged_and_must_be_repaired_or_dropped_1_5_Rule eventID: 8956
- Microsoft.SQLServer.2012.Table_error__Cross_object_linkage._Page_PGID_next_is_not_in_the_same_index_1_5_Rule eventID: 8982
- Microsoft.SQLServer.2012.Table_error__Parent_node_for_page_was_not_encountered_1_5_Rule eventID: 8977
- Microsoft.SQLServer.2012.Indexed_view_does_not_contain_all_rows_that_the_view_definition_produces.__Refer_to_Books_Online_for_more_information_on_this_error.__This_does_not_necessarily_represent_an_integrity_issue_with_th_5_Rule eventID: 8908

- Microsoft.SQLServer.2012.Table_error__Table_missing_or_invalid_key_in_index_for_the_row__1_5_Rule eventID: 8951
- Microsoft.SQLServer.2012.Unique_table_computation_failed_1_5_Rule eventID: 16959
- Microsoft.SQLServer.2012.Table__Creating_statistics_for_the_following_columns_1_5_Rule eventID: 15018
- Microsoft.SQLServer.2012.Table_error__B_tree_chain_linkage_mismatch.__1_5_Rule eventID: 8936
- Microsoft.SQLServer.2012.Failed_to_add_column__to_table__1_5_Rule eventID: 21285
- Microsoft.SQLServer.2012.Table_error__Index_node_page_refers_to_child_page_and_previous_child_but_they_were_not_encountered_1_5_Rule eventID: 8980
- Microsoft.SQLServer.2012.Table_error__The_low_key_value_on_page__is_not_the_key_value_in_the_parent_1_5_Rule eventID: 8933
- Microsoft.SQLServer.2012.Table_error__The_previous_link_on_page_does_not_match_the_previous_page_that_the_parent_slot_expects_for_this_page_1_5_Rule eventID: 8935
- Microsoft.SQLServer.2012.XML___XML_parsing_error_1_5_Rule eventID: 6603
- Microsoft.SQLServer.2012.XML___XML_document_could_not_be_created_because_server_memory_is_low._Use_sp_xml_removedocument_to_release_XML_documents_1_5_Rule eventID: 6624
- Microsoft.SQLServer.2012.XML___Size_of_data_chunk_requested_from_the_stream_exceeds_allowed_limit_5_Rule eventID: 6627
- Microsoft.SQLServer.2012.XML___Failed_to_load_Msxml2.dll_1_5_Rule eventID: 6610
- Microsoft.SQLServer.2012.XML___Failed_to_instantiate_class._Make_sure_Msxml2.dll_exists_in_the_SQL_Server_installation_1_5_Rule eventID: 6608
- Microsoft.SQLServer.2012.XML___FOR_XML_EXPLICIT_stack_overflow_occurred._Circular_parent_tag_relationships_are_not_allowed_1_5_Rule eventID: 6805
- Microsoft.SQLServer.2012.XML___XML_error_1_5_Rule eventID: 6600
- Microsoft.SQLServer.2012.Script_Failed_Database_Login eventID: 4001