Health Check Report

halgroup

delivering **beyond** expectations

SQL Server

Health Check PROD SQL_Sample

Hal Group Pty Ltd

19 January 2016

Version 5.00

Table of Contents

1 Introduction 3
2 Executive Summary 4
3 Hardware & Operating System Summary 5
Disk Sub-Systems 5
Hardware & Operating System Findings 5
4 SQL Server Configuration 9
SQL Server Configuration Findings 9
5 Databases 17
System Databases 17
User Databases 17
Database Findings 19
6 SQL Server Backup & Recovery 22
SQL Server Backup & Recovery Findings 22
7 Security 24
Security Findings 24

1 Introduction

The following report is an overview of the health of your SQL Server 2012 environment. It focuses on aspects of SQL Server that are often overlooked when it is installed or when moved from development to production environments. Any findings listed should be treated as an opportunity to improve/secure the SQL Server 2012 environment rather than as criticism of any party for not having previously implemented such changes. It is best to treat this as a positive exercise.

The following key is used to identify information provided:

Symbol Key	Description
✓	Item is within expected boundaries, **no action required**
ℹ	A recommendation is made but does not require immediate action
✗	Item **is outside** expected boundaries, **immediate action is required**

2 Executive Summary

The SQL Server hosts 12 databases utilised primarily for the applications of the sample company. The server operates during business hours and is considered to be mission critical during those times. There have been a number of application related performance issues experienced on the server, and this review has identified a number of key areas where the management of this server does not conform to a best practice approach.

The SQL Server is not solely dedicated to SQL Server and also serves as a Web-server and a File-server. SQL Server performs best when it has dedicated access to the physical resources on the windows server. Additionally SQL Server has been assigned 16,384MB of memory as its 'Maximum Server Memory'. While it is appropriate to assign an upper limit to the memory SQL Server can use, the assigned value equates to all the memory in the server, and therefore provides no benefit from the default setting which is unlimited memory. It is recommended to set the 'Max Server memory' property to a value which allows dedicated resource to the underlying operating system, and in this case also considers the memory requirements of the web and file services running on the server.

Database collation defines the way that data is stored, sorted and compared within SQL Server. In general it is recommended to have databases share the same collation settings as the SQL Server system databases as different collation sequences between servers and databases that have not been specifically coded for can adversely affect how data is transferred between databases and servers and in the worst case scenarios can cause applications not to function correctly.

Database compatibility levels affect the way that some code executed within the context of that database is handled. In general it is not recommended to leave a database in a lower compatibility level than the system databases for an extended period of time. Database compatibility is intended as a temporary workaround while code\syntax within the application or database can be addressed. It is recommended to investigate if there is a reason the databases on this server remain in the lower compatibility level, and if not to move them to the appropriate compatibility level (110).

Database Page Verification is a method used to detect corruption within a database as data is written. It is recommended to use CHECKSUM as the database page verification message in SQL 2005 and beyond. Although this can add a very small overhead, it can detect corruption issues within a database which would otherwise only be picked up with a full database consistency check.

Two databases have the auto shrink option enabled. This option is known to cause performance issues within SQL Server, both during unscheduled shrinks of the database and due to the internal and external fragmentation of databases which the constant shrinking and growing of database files leads to. It is recommended to disable this option on all databases.

A number of issues have also been identified with the potential recoverability of the SQL Server in a disaster situation. Currently SQL Server backups are taken to a local disk, and the whole server is backed up using a Veeam server level backup each night

3 Hardware & Operating System Summary

Given that SQL Server will only perform optimally on appropriate hardware and operating systems, these have been analysed against best practice and appropriateness for this SQL Server environment.

The following hardware and operating systems observations were made as part of the SQL Server Health Check process.

It is noted that this server utilises a Storage Area Network. The details of the underlying physical disk structure are detailed in the table below.

Disk Sub-Systems

Disk Sub-System RAID Level	Drive Letter	Drive Purpose	Logical Size (GB)	Free Space (GB)
3PAR 7200 VRAID 50	C	Operating System SQL Server Binaries Page File SQL Server Database Files SQL Server Log Files	60	28.01
3PAR 7200 VRAID 50	D	SQL Server Database Files SQL Server Log Files	200	94.08

Hardware & Operating System Findings

Status	Configuration	Comments
ℹ	**Virtualisation** *VMWare*	This server is running on virtualised hardware using VMWare. It is recommended to review whether the virtualisation environment is a “Server Virtualisation Validation Program (SVVP)” validated solution. It is also recommended to review the reasons why SQL Server has been virtualised, as virtualisation may not be appropriate for a high I/O SQL Server environment. Please refer to the following URL’s for further details on the support for SQL Server running in a virtualised environment: http://support.microsoft.com/kb/897615/en-us http://support.microsoft.com/?id=956893 Hal Group recommends reviewing the reasons for implementing SQL Server in a virtualised environment, and to ensure that all aspects of the virtualised environment are considered, including scalability, hardware I/O performance, shared memory resources, and Microsoft support policies.

Status	Configuration	Comments
✓	**Server Architecture** *x64*	The server is utilising 64-bit x64 hardware. The x64 architecture is based on 64-bit extensions to the industry-standard x86 instruction set. This allows a 32-bit operating system, or a 64-bit operating system, to be run natively on an x64 server.
✓	**Processor(s)** *4 Virtual Cores* *2800 MHz*	While an in-depth review of the CPU has not been completed, the processing power appears to be sufficient for a SQL Server environment of this size. It is noted that 4virtual cores are assigned to the virtual server hardware, and thus can be used by SQL Server.
✓	**RAM** *16,384 MB*	While a full analysis of the memory usage and requirements of this server has not been completed, it appears that the amount of configured RAM in this server is sufficient for this SQL Server environment.
✓	**Disk RAID Level** *See above*	The RAID level for the underlying disk sub-system is configured optimally for SQL Server performance and fault tolerance. There are multiple disk sub-systems which allow the SQL Server data and log files to be separated which is considered best practice. Currently this server utilises a Storage Area Network. The RAID levels noted in this section represent the underlying physical disk structure. RAID Level for SQL Server Data Files The SQL Server data files currently reside on a RAID 50 disk sub-system which provides for good fault tolerance. RAID Level for SQL Server Log Files The SQL Server log files currently reside on a RAID 50 disk sub-system which provides for good fault tolerance. RAID Level for Operating System The Windows Operating System currently resides on a RAID 50 disk sub-system which provides for good fault tolerance.
✗	**File Locations** *See above*	While the disk RAID level for this server is appropriate, the locations of the SQL Server data and log files are not. SQL Server data and log files should reside on separate physical disk sub-systems which will reduce the potential disk bottleneck with high data and log activity inherent with most databases. The recoverability of SQL Server data in event of a system crash is enhanced because SQL Server log files are on a separate disk sub-system to that of the SQL Server data files.
✓	**Disk Space** *See above*	At the time of the report the available disk space is sufficient on all relevant drives for the current database requirements.

Status	Configuration	Comments
✓	**Operating System** *Windows Server 2012(x64) Standard Edition*	Windows Server 2012 is installed on this server. This is appropriate and recommended. It is noted that there are no service packs for Windows Server 2012, but there are monthly ‘Update Rollups’ to apply.
✓	**Server Application Response** *Background Services*	The processor scheduling option has been set to optimise performance for background services. This is appropriate and recommended. The application response option sets CPU resources to be optimised either for foreground applications or background services currently running on the server.
✓	**Server Role** *Member Server*	The server is appropriately configured as a member server of the SampleCompanys.local domain. SQL Server performs better and more securely when installed on a server configured as a member server within a domain.
✓	**Windows Guest Account** *Disabled*	The Windows guest account is disabled. This is appropriate and recommended.
✓	**Windows Login Auditing** *Enabled*	Windows Login Auditing is enabled on this server. This is appropriate and recommended as it provides enhanced auditing and tracking of login activities occurring on this server.

Status	Configuration	Comments
✗	**Windows Event Logs**	The Windows event logs have been reviewed for errors that may impact SQL Server. Application Event Log: The following errors were found: - *(Multiple) The configuration informationof the performance library “perf-MSSQLSERVER-sqlctr11.0.2100.60.dll” for the “MSSQLSERVER service does not match the trusted performance library information stored in the registry. The functions will not be treated as trusted.* – This error should be addressed if the perf functions reference require ‘trusted’ permissions. Security Event Log: No errors of relevance were found. System Event Log: The following errors were found: - (Multiple) – This computer was not able to set up a secure session with a domain controller in domain SAMPLECOMPANY due to the following: There are currently no logon servers available to service the login request. This may lead to authentication problems. -(Multiple) The processing of Group Policy Failed. Windows could not obtain the name of a domain controller. This can be caused by a name resolution failure. Verify your Domain Name System(DNS) is configured and working correctly.

4 SQL Server Configuration

SQL Server has several configurable options. In this section these options are reviewed for their appropriateness for this particular SQL Server environment and against best practice.

SQL Server Configuration Findings

Status	Configuration	Comments
✓	**SQL Server Edition** *Standard Edition (64-bit)*	SQL Server 2012 Standard Edition is installed. Standard Edition is appropriate for the business applications using this database server. The applications do not require the extra functionality and scalability offered by Enterprise Edition. The Standard Edition of SQL Server 2012 supports up to 4 processors, 64 GB RAM limit and unlimited database sizes.
i	**SQL Server Service Pack** *Build No: 11.0.3128.0* *SP: SP1*	Microsoft recommends the latest service pack and the latest General Distribution Release (GDR) as the minimum build. As this build is in the QFE range a GDR is unable to be applied, so Microsoft recommends the latest QFE which contains a GDR, as the minimum build. The latest Service Pack is SP2 (11.0.5058.0).
✓	**Startup Parameters** *-dC:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\master.mdf* *-eC:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Log\ERRORLOG* *-lC:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\mastlog.ldf*	The SQL Server startup parameters are correctly configured with no additional non-standard trace flags configured to run on startup.
✓	**Network Protocols** *TCP/IP* *Shared Memory*	SQL Server is configured to listen on TCP/IP and shared memory. The default Named Pipes communication library has been disabled on this server. This is considered appropriate for the communication needs of this server.

Status	Configuration	Comments
ℹ	**General Endpoint Information**	The following communication endpoints are configured to be active, and are processing requests: · Dedicated Admin Connection · TSQL Local Machine · TSQL Named Pipes · TSQL Default TCP · TSQL Default VIA To ensure a secure SQL Server environment, it is recommended to review all enabled communications endpoints, and to disable any endpoints which are not required.
✗	**SQL Server Memory Settings** *Min: 16MB* *Max: 16,384MB* *Lock Pages in Memory: No*	SQL Server has had the default Maximum Memory option changed from the default to 16384. While it is appropriate to assign a maximum Server memory setting, the chosen value appears to be too high, assigning all memory to SQL Server.
✗	**Lock Pages In Memory** *Disabled*	The “lock pages in memory” security policy enables the SQL Server process to keep data pages stored in physical memory, preventing the system from paging the data to virtual memory stored on the physical disk. It is recommended to correctly configure the “Maximum Server Memory” option before enabling this security privilege.
✓	**Access Check Cache Bucket Count** *Default (0)*	This option has not been changed from the default value of 0. This enables SQL Server to dynamically control the number of hash buckets used by the access check result cache which is appropriate and recommended. This option is used in conjunction with the “Access Check Cache Quota” option and the default number of hash buckets for an x86 installation is 256. For an x64 or ia64 installation the default value number 2,048.
✓	**Access Check Cache Quota** *Default (0)*	This option has not been changed from the default value of 0. This enables SQL Server to dynamically control the number of entries stored in the access check result cache which is appropriate and recommended. This option is used in conjunction with the “Access Check Cache Bucket Count” option and the default number of hash buckets for an x86 installation is 1,024. For an x64 or ia64 installation the default is 8,192.
✓	**Ad Hoc Distributed Queries** *Default (0)*	This option has been disabled on this server, which is appropriate and recommended, as this enforces the use of linked servers for OPENROWSET and OPENDATASOURCE queries to remote data sources.

Status	Configuration	Comments
✓	**Affinity Mask** *Disabled*	This option has been disabled on this server, which is appropriate and recommended, as there are no known requirements to associate specific processors with SQL Server. This option can force SQL Server to only execute on specific processors for SMP servers. This option should only be changed for servers with more than 4 processors and furthermore, only when there is a specific need to associate SQL Server threads with specific processors in the server.
✓	**Affinity I/O Mask** *Disabled*	This option has been disabled on this server, which is appropriate and recommended. In almost all cases, leaving IO_affinity_mask at its default setting results in the best performance. In an online transaction processing (OLTP) environment, the I/O affinity mask option may provide performance enhancement in high-end, enterprise-level SQL Server environments that are running on computers with 16 or more CPUs. This option supports only SQL Server disk I/Os and does not support any hardware affinity for individual disks or disk controllers. If you specify the IO_affinity_mask switch, Microsoft suggests that you use it in conjunction with the affinity mask configuration option. Make sure not to enable a CPU for both the IO_affinity_mask switch and affinity_mask option.
✗	**Backup Compression Default** *Disabled*	Database backup compression reduces the space required to backup a database, as well as decreases the time it takes to perform a database backup. This option is available in SQL Server 2012 Standard Edition, but has not been enabled on this server. While backup compression incurs a small CPU overhead, it is recommended to enable this option on this server.

Status	Configuration	Comments
i	**FILESTREAM Access Level** *Disabled (0)*	The new SQL Server 2008 FILESTREAM function integrates the structured storage engine of SQL Server with an NTFS file system, by way of storing binary large objects as files on the file system, and then allowing TSQL statements, like insert, update, query, and backups commands to interact with the FILESTREAM data. Win32 processes can also interface with the objects to provide streaming access to the data. It is recommended that FILESTREAM be considered if any of the following scenarios exist: - Objects on average being stored are more than 1MB - Fast read access of large objects is required - The application uses middle tier logic FILESTREAM access levels can be set to only one of the following: - Disabled - Enabled for T-SQL access - Enabled for T-SQL and Win32 streaming access
✓	**Index Create Memory** *Default (0)*	This option has not been changed from the default of 0 which is appropriate and recommended. This option controls the maximum amount of memory initially allocated for creating indexes. If additional memory is required after the index creation is initialised, and there is memory available, then SQL Server will utilise it. If additional memory is not available, SQL Server will continue using the memory that has already been allocated.

Status	Configuration	Comments
✓	**Max Degree of Parallelism** *0*	This setting is the default configuration for SQL Servers, and is the recommended setting for most SQL Servers, unless there is a specific recommendation from an application provider to set the option to a setting other than the default. The maximum degree of parallelism option allows SQL Server to optimise query execution plans to execute in parallel across multiple processors, on servers which have multiple processor cores. Microsoft's general guidelines for configuring the maximum degree of parallelism states the following when considering what number to set the maximum degree of parallelism to: For servers that use more than eight processors (cores), set the maximum degree of parallelism to a maximum of 8. For servers that have eight or less processors (cores), set the maximum degree of parallelism to either 0, or to the number equal to the number of processors (cores) which are installed in the server. For servers that have NUMA (non-uniform memory access), the maximum degree of parallelism setting should not exceed the number of CPUs that are assigned to each NUMA node. For servers that have hyper-threading enabled, the maximum degree of parallelism should not exceed the number of physical processors (cores). For further information please refer to the this Microsoft Knowledge Base article: http://support.microsoft.com/kb/329204 In addition, it should be noted that the above guidelines are only general, and that some applications make a specific recommendation to disable the maximum degree of parallelism, by setting the option to one.
✓	**Lightweight Pooling** *Disabled*	This option has been disabled on this server. This is appropriate and recommended.
✓	**Locks** *0 - Dynamic*	This option has not been changed from the default value of 0. This enables SQL Server to dynamically configure locks which is appropriate and recommended.
✓	**Max Worker Threads** *0 - Default*	This option has not been changed from the default of 0, which is appropriate and recommended, unless the number of concurrent connections exceeds this default.
✓	**Min Memory Per Query** *1024 - Default*	This option has not been changed from the default of 1024 which is appropriate and recommended.

Status	Configuration	Comments
✓	**Optimize For Ad hoc Workloads** *Disabled (0)*	This option stops the storage of full compiled plans for ad-hoc, one-off queries in the plan cache. Instead SQL Server will store a compiled plan stub, which in turn reduces the memory requirements for storing the complete compiled plan which does not get used again.
ℹ	**Policy-Based Management** *No Policies*	There are no SQL Server management policies defined for this SQL Server. Policy-based management allows a system administrator to manage an instance of SQL Server by defining policies to control different entities relating to the SQL Server instance.
✓	**Priority Boost** *Disabled*	This option has been disabled on this server, which is appropriate and recommended. This option will increase the base execution priority of the SQL Server Windows process. This option is known to cause stability problems and should not be enabled unless this has been specifically recommended by Microsoft Support.
✓	**Query Wait** *-1 - Default*	This option has not been changed from the default value on this server, which is appropriate and recommended. This option will enable SQL Server to undergo a wait cycle when all the required server resources are not available in order to complete a query.
✓	**Recovery Interval** *0 - Default*	This option has not been changed from the default value on this server, which is appropriate and recommended. This option serves a number of uses. One is to set the number of minutes SQL Server requires in order to recover a database at SQL Server startup. The default value of 0 indicates typically less than 1 minute to recover each database.
✓	**User Connections** *0 - Default*	This option has been not been changed from the default value of 0. This enables SQL Server to dynamically configure connection resourcing. This is appropriate and recommended.
✓	**Default Trace** *Enabled*	The default trace option is enabled. This is appropriate as the trace information provided can be used to assist in the diagnosis of server faults.
ℹ	**SQL Server Service Account** *SAMPLE COMPANY\SQLService*	The SQL Server service is running under the specified Windows account which is not configured as an administrative level account, and which is a specific account used solely for the SQL Server service. This is appropriate.
ℹ	**SQL Server Agent Service Account** *SAMPLE COMPANY\SQLService*	The SQL Server Agent service is running under the specified Windows account which is not configured as an administrative level account. However, the account is the same account which is used for the SQL Server service, this is not appropriate.

Status	Configuration	Comments
ℹ	**SQL Server Browser** *Enabled*	This is not appropriate for a secure production SQL Server environment.
✗	**SQL Server Browser Service Account** *Local System*	The service that runs SQL Server Browser is configured to run under the local system account. This is not appropriate. The local system account is an account which has many high level privileges which are not required by the SQL Server Browser service. In addition, the local system account is a shared account, and is likely used by other services on the server. This in turn means that any service also using the local system account has the same privileges as the SQL Server Browser service. Both these issues are considered security risks.
ℹ	**E-mail** *Disabled*	Database Mail has not been configured on this server. Database Mail integrates into SQL Server and can be configured to proactively send notifications when conditions occur on the server.
ℹ	**SQL Server Alerts** *Not Used*	SQL Server alerts have not been configured on this server. It is recommended to configure the SQL Server alerts to proactively monitor the server and raise the appropriate message when certain error, performance or warning conditions are met.
✓	**SQL Server Analysis Services or Data Warehousing Tools** *Not Installed*	The SQL Server Analysis Services or other 3rd party data warehousing tools are not installed. This is appropriate as this server is not dedicated to serve the needs of a data warehouse application.
✓	**SQL Server Integration Services** *Not Installed*	SQL Server Integration Services (SSIS) is not installed. This is appropriate is no SSIS packages are to be used on this server. If at a later stage SSIS packages are required, it is recommended to install SSIS at the time it is required. This is to ensure the security foot print of SQL Server is kept to only required services.
✓	**SQL Server Reporting Services** *Not Installed*	The SQL Server Reporting Services or other 3rd party reporting tools are not installed. This is appropriate as this server is not used for reporting or is not dedicated to serve the needs of a reporting application framework.
✓	**SQL Server Notification Services** *Not Installed*	SQL Server Notification Services is not installed. This is appropriate as no Notification Services applications have been developed, and in addition Notification Services will no longer be available in SQL Server 2008.
ℹ	**Native XML Web Services**	If Native XML Web Services are being used by the business, or are being considered for us by the business, it is recommended to review the best practice recommendations.

Status	Configuration	Comments
ℹ	**Other Applications** *Web Service* *File Server*	This server is also used as a file server and web server. This is in general not recommended, SQL Server performs best when it has all resources on the server dedicated for database processing.
✓	**Server Scoped DDL and CLR Triggers** *Not Used*	At the time of writing this report, there were no server scoped DDL or CLR triggers.
✓	**Server Scoped Event Notifications** *Not Used*	At the time of writing this report, there were no Server Scoped Event Notifications.
ℹ	**Instant File Initialization** *Disabled*	Instant File Initialization is disabled on this server. This may not be appropriate.
✓	**Blocked Process Threshold** *0*	The block process threshold is set to 0, which is disabled.
✓	**Network Packet Size** *4,096*	The network packet size option has not been altered from the default of 4,096 bytes. This is appropriate.
✓	**SQL Server Data Replication** *Not Used*	SQL Server Data Replication is not installed onto this server. This server plays no role within any SQL Server Data Replication solution.
✓	**SQL Server Error Log**	The SQL Server error logs have been scanned for any errors of relevance.
✗	**SQL Server Agent Error Log**	The SQL Server Agent error logs have been scanned for any errors of relevance. The following error was found: 3/8/2014 – SQL Server Error 15404, Could not obtain information about Windows NT group/user ‘SAMPLECOMPANY\User’.
ℹ	**SQL Server Restarts** *One*	SQL Server has been shutdown 1 times in the past 30 days. The most recent shutdown occurred on 13/7/2014 at 2:03pm when the server stopped due to a system shutdown and remained down for 1 minute.
✗	**Failed Jobs** *Some*	There have been failed jobs in the last 30 days. The SQL Server maintenance plan has failed on 2 occasions due to user permissions errors.

5 Databases

System Databases

Database Name	Owner	Data File Size (MB)	Log File Size (MB)	Options
master	sa	4.9	1.8	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics
model	sa	4.1	1.0	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=FULL, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics
msdb	sa	103.4	19.6	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics, IsFullTextEnabled
tempdb	sa	8.0	0.5	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics

User Databases

Database Name	Owner	Data File Size (MB)	Log File Size (MB)	Options
ExampleAuth	SAMPLE COMPANY\Admin	5.0	1.0	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=FULL, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics, IsFullTextEnabled
ExampleSAMPLE COMPANY	SAMPLECOMPANY\User	10,294.1	1.3	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=SQL_Latin1_General_CP1_CI_AS, SQLSortOrder=52, IsAutoShrink, IsAutoCreateStatistics, IsAutoUpdateStatistics

Database Name	Owner	Data File Size (MB)	Log File Size (MB)	Options
ExampleReward	SAMPLECOMPANY\User	17.3	2.0	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics, IsFullTextEnabled
ExampleSLS	SAMPLE COMPANY\User	28.8	2.0	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsTornPageDetectionEnabled, IsAutoCreateStatistics, IsAutoUpdateStatistics
ExampleStripped	SAMPLECOMPANY\User	11.3	2.0	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsAutoCreateStatistics, IsAutoUpdateStatistics, IsFullTextEnabled
ExampleV7Demo	SAMPLECOMPANY\User	10,311.4	26.2	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=SQL_Latin1_General_CP1_CI_AS, SQLSortOrder=52, IsAutoShrink, IsAutoCreateStatistics, IsAutoUpdateStatistics
scWeb	SAMPLECOMPANY\User	39.8	1.8	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=Latin1_General_CI_AS, SQLSortOrder=0, IsTornPageDetectionEnabled, IsAutoCreateStatistics, IsAutoUpdateStatistics
WebMarshal	WebMarshal	260.1	6.3	Status=ONLINE, Updateability=READ_WRITE, UserAccess=MULTI_USER, Recovery=SIMPLE, Version=706, Collation=SQL_Latin1_General_CP1_CI_AS, SQLSortOrder=52, IsAutoCreateStatistics, IsAutoUpdateStatistics, IsFullTextEnabled

Database Findings

Status	Configuration	Comments
ℹ	**Database Owner**	Not all databases are owned by the SQL Server login “sa”. It is recommended that all databases are owned by an appropriate Windows or SQL Server account. Any databases that have a ‘Null’ owner should have their ownership changed.
✗	**Recovery Model**	Not all databases are set to use the full recovery model. This affects how the databases can be restored in the event of failure. Databases set to simple recovery model do not allow a point in time recovery. It is recommended to set all production user databases that require point-in-time recovery to the full recovery model.
✓	**Auto Close**	None of the databases have Auto Close enabled, which is appropriate and recommended.
✗	**Auto Shrink**	Several databases have Auto Shrink enabled, which is known to cause a performance overhead. This setting instructs SQL Server to periodically (typically every minute) check the database and shrink the database files as required. It is recommended to turn this option off.
✓	**Auto Create Statistics**	All databases have Auto Create Statistics enabled. This is appropriate and recommended, Not enabling this option can have a significant effect in how the SQL Server query optimiser chooses query plans to access the database table data.
✓	**Auto Update Statistics**	All user databases have the Auto Update Statistics option enabled, which is appropriate for most databases. However, it is recommended to review these settings as Auto Update Statistics can in specific cases lead to unpredictable query plans, and a high number of recompilations.
✓	**Auto Update Statistics Asynchronously**	There are no databases configured with the Auto Update Stats Async option.
✗	**Page Verify**	The following databases do not use checksum as the page verify option: - ExampleSAMPLECOMPANY is set to NONE - ExampleSLS is set to TORN_PAGE_DETECTION
ℹ	**Database Collations**	The system database collation is Latin1_General_CI_AS. The databases with collation sequences different from that of the SQL Server system databases are: - ExampleSAMPLECOMPANY(SQL_Latin1_General_CP1_CI_AS) - ExampleV7Demo (SQL_Latin1_General_CP1_CI_AS) - WebMarshal (SQL_Latin1_General_CP1_CI_AS)
✓	**Restrict Access**	None of the databases have been set to restrict access mode, which is appropriate and recommended.

Status	Configuration	Comments
✓	**Read Only**	None of the databases have been set to read only mode, which is appropriate and recommended.
✓	**Offline**	None of the databases are offline, which is appropriate and recommended. It is not recommended to leave databases in an offline status on a production server for an extended period of time.
✓	**Emergency Mode**	None of the databases have been set to read only mode, which is appropriate and recommended. Emergency mode can sometimes be used to enable read-only access to a database which has been marked suspect. The ability to do this is dependent on the severity of the corruption inside the database.
✓	**Stand-by**	None of the databases are set to the standby mode.
ℹ	**Compatibility**	The user databases that do not have a compatibility setting of 110 (SQL Server 2012) are: - ExampleSAMPLECOMPANY - ExampleRewards - ExampleSLS - ExampleStripped - ExampleV7Demo - rrWeb
✓	**Snapshot Isolation/ Read Committed Snapshot**	No databases have either Snapshot Isolation or Read Committed Snapshot enabled. These options are used for row versioning in SQL Server.
✓	**Forced Parameterization**	No databases have forced parameterization enabled.
✓	**Trustworthy + DBO**	No database which has the trustworthy option enabled also has the database owner as a member of the sysadmin fixed server role. This is appropriate and recommended.
✓	**Transaction Log Size**	All user databases transaction log sizes are deemed to be within acceptable limits requiring no transaction log resizing activity.
ℹ	**Tempdb** *Set to Auto-Grow* *No maximum size.*	The initial startup size of the tempdb database appears to be too small for this SQL Server environment. It is recommended to resize the tempdb database to either 100MB or 20% of the size of the largest actively used production database, whichever is the greater. Given these recommendations tempdb should be resized to a minimum of 2,062 MB.
✓	**Resource Database**	The Resource Database should be located in the default SQL install location.

Status	Configuration	Comments
✓	**Compressed Database Files** *Not Compressed*	The SQL Server database files are not in compressed directories, and none of the database files are compressed This is appropriate and recommended for performance and stability of SQL Server.
✓	**Database Snapshots**	At the time of writing this report there was no database snapshots present on this server.
ℹ	**Database Consistency Checks (DBCC)** *Scheduled Weekly* *Not all databases*	Database Consistency Check processes are occurring on a weekly basis. While this is appropriate and recommended it is noted that not all databases are included in the current maintenance plan.
ℹ	**Database Data Optimisations** *Scheduled Weekly* *Not all databases*	Not all user and system databases have optimisation processes occurring, however a subset of databases have full index rebuilds occurring via a maintenance plan on a weekly schedule.
ℹ	**Service Broker Enabled**	The following databases have Service Broker functionality enabled: - WebMarshal
ℹ	**Full Text Enabled**	The following databases have Full-text Search capabilities enabled: - msdb - ExampleOAuth - ExampleRewards - ExampleStripped - WebMarshal
ℹ	**Non-Production Databases** *Some*	It appears that several non-production databases exist on this server. It is recommended to move these databases to a separate non-production server and have this server dedicated to the specific needs of this production database environment.
ℹ	**Database Master Key Encryption**	To encrypt information stored in a database, a database master key must be created. There are two possible methods to encrypt this database master key, one is to use a password to encrypt, and the other method is to use the SQL Server service master key.
✗	**Orphaned Database Users**	At the time of writing this report there were a total of 8 orphaned users across all databases on the server. Please refer to the Orphaned Users Appendix for a list of the databases and associated orphaned users.

6 SQL Server Backup & Recovery

Given the increasingly critical nature of the data stored in SQL Server databases, high availability (HA), keeping a database operational in the event of a disaster, and disaster recovery DR, the ability to recover data from a database in the event of a disaster, are serious concerns for business. Due to these concerns, all databases stored on this server have been analysed for their ability to remain available, as well as their ability to be recovered, in the event of a disaster.

From the interviews conducted as part of this health check, up to 1 day data loss is tolerable. After an outage it is expected that the databases will be available again within 1 hour.

The following backup and recovery observations were made as part of the SQL Server Health Check process.

SQL Server Backup & Recovery Findings

Status	Configuration	Comments
✗	**Full Database Backups** *Partial*	Not all system and user database backups have been occurring regularly on this server. This is considered a serious issue and priority should be given to configuring these backups.
ℹ	**Transaction Log Backups** *None*	Not all user databases that are set to the Full or Bulk-Logged recovery model have transaction log backups scheduled.
✓	**Backup File Locations** *Direct to Local Disk*	The database backups are located on a local disk. This is considered appropriate and recommended.
✓	**System State Backup** *Yes*	A full System State backup is taken on the following schedule: - Nightly This is appropriate.
ℹ	**Off-site Backup Strategy** *Virtual Machine backup*	The Virtual machine backup schedule on this server is: - All servers are backed up nightly using Veeam. The Veeam backups are also taken to tape weekly. The backup process is backing up the open SQL Server database files.
✗	**Log Shipping** *Not Used*	Given that only 1 hour downtime and 1 days data loss is tolerable for the applications on this server, log shipping is deemed as a potential solution to provide the DR/HA requirements for this server.

Status	Configuration	Comments
✓	**Database Mirroring** *Not Mirrored*	This server currently does not participate in database mirroring. Given that up to 1 hour downtime is tolerable for the applications on this server, database mirroring is not deemed as required.
✓	**Clustering** *Not Clustered*	This server currently does not participate in any form of clustering. Given that up to 1 hour downtime is tolerable for the applications on this server, clustering is not deemed as required.
ℹ	**Backup and Recovery Site Documentation** *Not Available*	It is recognised that this server has no backup and recovery documentation. This is considered a risk to the business and it is recommended that this documentation be developed and kept up to date.
✗	**Backup and Recovery Test** *Never*	The backup and recovery processes have not been tested or are not regularly tested. It is recommended that the entire backup and restore process is thoroughly and regularly tested.
ℹ	**SSIS Package Backups**	SQL Services Integration Services is not installed on this server.
ℹ	**Remote Dedicated Administrators Connection** *Disabled*	The Remote Dedicated Administrators Connection (DAC) is disabled. This is not appropriate.

7 Security

Security Findings

Status	Configuration	Comments
✓	**System Administrators** *NT SERVICE\MSSQLSERVER* *NT SERVICE\SQLSERVERAGENT* *NT SERVICE\SQLWriter* *NT SERVICE\Winmgmt* *SAMPLECOMPANY\User* *SAMPLECOMPANY\SCL Admin* *SAMPLECOMPANY\SQL Services* *sa*	The members of the SQL Server System Administrator role appear to be correctly configured to contain only the SQL Server “sa” account, the account used to run SQL Server and the DBA administrators of the environment.
✓	**“sa” Password** *Set*	The SQL Server “sa” password has been set and is only known by system administrators. This is appropriate and recommended.
✓	**“sa” Users Default Database** *master*	The “sa” login is configured with the master database as its default database. This is appropriate.
ℹ	**Password Policy Enforcement**	SQL Server 2012 provides a mechanism for ensuring passwords for SQL Server standard logins adhere to the organisation password policies, as defined in either the domain group security policy, or the local Windows security policy.
✓	**Blank Passwords** *None*	All SQL Server standard users have passwords assigned and are currently blank. This is appropriate and recommended.
ℹ	**Authentication Mode** *Mixed*	The SQL Server authentication mode is set to both Windows and SQL standard authentication.
✓	**Login Auditing** *Failure*	The failed login auditing function has been enabled on this server. This is appropriate and recommended.

Status	Configuration	Comments
✓	**C2 Audit Mode** *Disabled*	This option has been disabled on this server, which is appropriate and recommended.
✓	**Common Criteria Compliance** *Not Available*	This option is only available in the SQL Server 2008 Enterprise and Developer Editions.
✓	**Cross DB Ownership Chaining** *Disabled*	This option has been disabled on this server, which is appropriate and recommended.
✓	**Scan for Startup Procedures** *Disabled*	This option has been disabled on this server, which is appropriate and recommended.
✓	**Server Connection Security Settings** *HideInstance = disabled* *ForceEncryption = disabled*	Both options have been disabled, which is appropriate and recommended.
✗	**Guest Account Access to Databases** *Has Access*	The guest account has access to user or system databases. This is not appropriate as the guest database user account is considered a security hole for SQL Server allowing anonymous database access.
✓	**File System** *NTFS*	All SQL Server files, including the database data, log and binaries are appropriately located on NTFS volumes. This is recommended from a Windows security perspective.
✗	**Anti-Virus Scanning Packages** *Not Installed*	No anti-virus software is configured to run on this server.
ℹ	**Security Policy Documentation** *Not Available*	It is recognised that the server at this stage has no form of security policy or associated supporting documentation. This is considered a risk to the business and is recommended that this documentation be developed.