



DSV

xTrack Implementation

System Health Check

Document Dated: 12/7/2020

Document Version: 1.0

Document by: Axes Software



**Document Information**

**Revision History**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| 1 | 12/07/2020 | Initial Draft |
|  |  |  |
|  |  |  |
|  |  |  |

**Reference Documents**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table of Contents

[1 Purpose 4](#_Toc58334366)

[2 Results 5](#_Toc58334367)

[2.1 Preliminary Health Check Results 5](#_Toc58334368)

[2.2 Recommendations 5](#_Toc58334369)

[2.2.1 OS and DBMS Upgrade 5](#_Toc58334370)

[2.2.2 Detailed Health Check 5](#_Toc58334371)

[2.2.3 Maintenance improvements 5](#_Toc58334372)

[2.2.4 High Availability and Disaster Recovery 5](#_Toc58334373)

[3 Methods 6](#_Toc58334374)

[3.1 Storage 6](#_Toc58334375)

[3.2 Support 6](#_Toc58334376)

[3.3 Security 7](#_Toc58334377)

[3.4 Stability 8](#_Toc58334378)

[3.5 Performance 8](#_Toc58334379)

[3.6 Disaster Recovery 9](#_Toc58334380)

[4 Additional Discussion 9](#_Toc58334381)

[4.1 Upgrading SQL Server – end of extended support 9](#_Toc58334382)

[4.1.1 Security 9](#_Toc58334383)

[4.1.2 Compliance 9](#_Toc58334384)

[4.1.3 Higher maintenance costs 10](#_Toc58334385)

[4.2 Upgrading SQL Server – end of mainstream support 10](#_Toc58334386)

[4.2.1 Security 10](#_Toc58334387)

[4.2.2 Compliance 10](#_Toc58334388)

[4.2.3 Higher maintenance costs 10](#_Toc58334389)

[4.3 Upgrade Recommendations 10](#_Toc58334390)

[4.3.1 Upgrade to Azure 10](#_Toc58334391)

[4.3.2 On-premises Upgrade scenarios 10](#_Toc58334392)

[4.3.2.1 Side-by-side – new installation 10](#_Toc58334393)

[4.3.2.2 Side-by-side – Azure 11](#_Toc58334394)

[Appendix A: Detailed Health Check 12](#_Toc58334395)

# Purpose

The purpose of this document is to provide feedback on a detailed heath check conducted on the DSV database environment.

xTrack has been identified by DSV as a critical component of their business. The health, performance and security of the database environment is key to the continued success of DSV. The following areas were included in this review:

* Support status of product versions
* High availability and disaster recovery
* Database configuration
* Storage architecture
* Security
* Minimum Database maintenance standards
* Alerts and notifications

This report will form the basis of additional work recommended to DSV that will assure ongoing stability and continued performance of the environment.

# Results

The below summarizes the results of the preliminary health check. Further detail of the results can be found in Section 3. Methods.

## Preliminary Health Check Results

|  |  |  |
| --- | --- | --- |
| Characteristic | Sub-characteristic | Pass / Fail / Not Assessed |
| Storage | Space Available | Pass |
| Storage | Disk Configuration | Pass |
| Support | OS Version | Fail |
| Support | SQL Version | Fail |
| Security | Database Ownership | Fail |
| Security | Agent Job Ownership | Fail |
| Security | Sysadmins | TBD |
| Stability | Integrity Check | Pass |
| Stability | Page Checksum | Pass |
| Performance | Index Fragmentation | Pass |
| Performance | Statististics Maintenance | Pass |
| Performance | Query Store | Fail |
| Performance | Memory Configuration | Pass |
| Disaster Recovery | Backup Plan | Pass |
| Disaster Recovery | Backup Checksum | Fail |
| Disaster Recovery | Backup Compression | Fail |
| Disaster Recovery | Recovery Point Objective | TBD |
| Disaster Recovery | Recovery Time Objective | TBD |
| Alerts and notifications | Corruption alerts | Fail |
| Alerts and notifications | Failed job alerts | Fail |

## Recommendations

For Stability, Security and ongoing support reasons the following recommendations have been made to DVS.

* + 1. OS and DBMS Upgrade
* Upgrade to Windows Server 2019 or Windows Server Core if environment will continue to be operated on-prem
* Upgrade to SQL Server 2019
* Detailed options described in Section 4. Additional Discussion
  + 1. Detailed Health Check

Deeper assessment covering over 20 data points focusing on Performance and overall system health.

Designed to maximize system efficiency and minimize risk

* + 1. Maintenance improvements

Rebuild scheduled maintenance activities to current best practices

Pro-active daily and weekly monitoring of key metrics and logs

* + 1. High Availability and Disaster Recovery

Confirm customer RTO and RPO objectives

Design solution that conforms to RTO and RPO objectives identified

# Methods

## Storage

|  |  |
| --- | --- |
| Sub-criteria | Question posed |
| **Space Available** | **Does the environment have enough storage for current and future operation?** |
| There is currently enough storage space for the database and backup needs accounting for expected growth. | |
| **Disk Configuration** | **Is the storage configured per SQL best practices?** |
| In larger environment where database growth is occurring, SQL Server should be configured to have separate physical storage locations for Data, Log and Backup files. These default locations on instance will be used to auto fill the default location for creating new databases. This is to separate the load across multiple spindles for performance as well as avoid additional risk of an outage due to database growth and storage usage by the backup routines.  Data, log and binary files were found to be on different disks. | |

## Support

|  |  |
| --- | --- |
| Sub-criteria | Question posed |
| **OS Version** | **Is the server Operating System supported?** |
| Environment is currently running Windows Server 2012 R2 which is in extended support by Microsoft until October 10, 2023. The mainstream support for this version has ended on October 9, 2018, meaning that the operating system will not receive any feature updates, but rather occasional bug fixes and security updates.  Currently supported versions of windows server with support dates are as follows:  Windows Server (Core Only)  Current Version  Windows Server 2019  Mainstream support until January 9, 2024  Extended support until January 9, 2029  Windows Server 2016  Mainstream support until January 11, 2022  Extended support until January 12, 2027  Windows Server 2012 R2  Mainstream support ended on October 9, 2018  Extended support until October 10, 2023  Windows Server 2012  Mainstream support ended on October 9, 2018  Extended support until October 10, 2023 | |
| **SQL Version** | **Is the Database Management System Supported?** |
| Environment is currently running SQL Server 2014 SP3 which is extended supported by Microsoft until July 9 2024. The mainstream support for this version has ended on July 9, 2019, meaning that it will not receive any more updates, but rather occasional bug fixes and security updates.  Currently supported versions of windows server with support dates are as follows:  SQL Server 2019  Mainstream support until January 7, 2025  Extended support until January 8, 2030  SQL Server 2017  Mainstream support until October 11, 2022  Extended support until October 12, 2027  SQL Server 2016  Mainstream support until July 13, 2021  Extended support until July 14, 2026  SQL Server 2014  Mainstream support ended on July 9, 2019  Extended support until July 9 2024 | |

## Security

|  |  |  |
| --- | --- | --- |
| Sub-criteria | Question posed | |
| **Database owners** | **Which users own the databases?** |  |
| As a best practice sa should be the owner of every database to avoid ownership problems if the user is disabled. Also based on the the principal of least priviledge, the database owner might have some additional permissions which are not required.  The following databases: xTrackEDI\_Archive, xTrackEDI\_PRD ,xTrackFIN\_PRD, xTrackTMS\_Archive, xTrackWMS\_Archive, xTrackWMS\_Security are not owned by the default user “sa”, but rather by employee’s accounts. | | |
| **Job owners** | **Which users own the jobs?** | |
| Agent jobs are usually mission critical for most businesses. If the owner of a job is disabled, or deleted the job suddenly stop running as SQL Agent is not able to verify the owner’s account.  There are jobs whose owner is an employee, meaning if their login is disabled or not available due to Active Directory problems, the job will stop working. | | |
| **Sysadmins** | **Which users are sysadmins?** | |
| According to the principal of least priviledge the users should have just enough permissions to do their work. Too many sysadmins pose a potential security risk.  We found 10 sysadmins on the server. These need to be revised. | | |

## Stability

|  |  |
| --- | --- |
| Sub-criteria | Question posed |
| **Integrity Check** | **Are there any Database Integrity issues** |
| This check should be done prior to a full backup to verify the integrity of physical and logical SQL objects within the database and to confirm that the data within the backup is usable. Failure of these checks could result in corruption and application outages. In extreme cases there may also be data loss.  DBCC CheckDB has been run successfully recently and looks to be running on a schedule. It would be best to confirm the timing as it relates to the backup schedule. | |

## Performance

|  |  |  |
| --- | --- | --- |
| Sub-criteria | Question posed | |
| **Index Fragmentation** | **Are the indexes optimized?** | |
| As data is modified in a database, the database and its indexes become fragmented. As indexes become fragmented, ordered data retrieval becomes less efficient and reduces database performance. Indexes with fragmentation less than 5 percent do not need to be defragmented because the benefit from removing such a small amount of fragmentation is almost always vastly outweighed by the CPU cost incurred to reorganize or rebuild the index.  9 indexes were found to be highly fragmented.  There is a maintenance job configured that would include index rebuilds. | | |
| **Statistics** | | **Are the execution plans using the right estimates?** |
| SQL Server statistics are essential for the query optimizer to prepare an optimized and cost-effective execution plan. These statistics provide distribution of column values to the query optimizer, and it helps SQL Server to estimate the number of rows (also known as cardinality). Improper statistics might mislead query optimizer to choose costly operators such as index scan over index seek and it might cause high CPU, memory and IO issues in SQL Server. We might also face blocking, deadlocks that eventually causes trouble to the underlying queries, resources.  Last statistics update was…. | | |
| **Query Store** | | **Is Query Store enabled?** |
| The SQL Server Query Store feature provides you with insight on query plan choice and performance. It simplifies performance troubleshooting by helping you quickly find performance differences caused by query plan changes. Query Store automatically captures a history of queries, plans, and runtime statistics, and retains these for your review.  SQL Server Query Store is not currently in use. | | |
| **Memory configuration** | | **Does SQL Server leave enough memory to the operating system?** |
| If it needs it SQL Server will use up all the memory available as per the max server memory setting. Under memory pressure SQL Server will starve the OS memory putting the whole system at risk and forcing Windows to swap out to the page file some of the SQL Server memory which will cause significant performance issues.  Max server memory values recommended: https://www.brentozar.com/blitz/max-memory/  Min server memory should be 0. | | |

## Disaster Recovery

|  |  |  |
| --- | --- | --- |
| Sub-criteria | Question posed | |
| **Backup Plan** | **Is there a backup plan?** | |
| The backup plan in place must allow the recovery to be achieved within an amount of time and to a point that is acceptable to the application. As an example, if recovery must occur within 1 hour of the disaster and get the database back to the state it was in within 1 hour of the outage then the Backup Plan and environment configuration must be designed to support this.  Backup Plan in place: Daily Full | | |
| **RPO** | | **How much data can be lost in case of system failure?** |
| Recovery Point Objective (RPO) is a measurement of time from the failure, disaster or similar loss-causing event. RPOs calculate back in time to when your data was last usable, probably the most recent backup.  RPO Objectives: Unknown  Current Recovery Point estimate: Maximum data loss assuming all backups are successful and available is 120 minutes. | | |
| **RTO** | | **How fast can the databases be back online after a system failure?** |
| Recovery Time Objective (RTO) is described as the amount of time an application can be down and not result in significant damage to a business and the time that it takes for the system to go from loss to recovery.  RTO/RPO Objectives: Unknown  Current Recovery Time estimate: Approximately 1:30 hours including reinstall of SQL, configuration, database restore and recovery. This assumes suitable equipment to run SQL is available. | | |
| **Backup checksum** | |  |
| CHECKSUM option specifies that the backup operation will verify each page for checksum and torn page, if enabled and available, and generate a checksum for the entire backup.  Checksum is disabled | | |
| **Backup compression** | |  |
| Since SQL Server 2012, backup compression is available in Standard Edition as well. The bottleneck of the backup and restore processes is the IO subsystem. By enabling compression both backups and restores will be faster.  Backup compression is not enabled. | | |

## Alerts and notifications

|  |  |  |
| --- | --- | --- |
| Sub-criteria | Question posed | |
| **Corruption alerts** | **How fast can the DBA act in case of corruption?** | |
| Corruption may lead to data loss. The sooner a DBA can take action the less data will be lost.  No alerts configured for errors 823, 824, and 825 | | |
| **Job failed alerts** | | **Is someone notified if a job fails?** |
| Agent jobs are usually mission critical for most businesses. Configuring alerts will enable the DBA to take action before the effects are seen.  No alerts are set for failed jobs. | | |

# Additional Discussion

## Upgrading SQL Server – end of extended support

Running unsupported SQL Server versions poses a severe threat to the business. The risks fall into 3 major categories: security, compliance and maintenance costs.

* + 1. Security

To protect the sensitive data, security updates should be installed as soon as they are released. Not deploying the latest security update will make the server and the applications accessing it vulnerable to cyberattacks, malware and data theft.

* + 1. Compliance

It is the legal responsibility of every organization to safeguard the sensitive data. Several regulations (HIPAA, PCI DSS, SOX, Dodd-Frank, GDPR, etc.) provide guidelines of the procedures a company needs to implement in order to protect itself from data theft. Running unsupported software might bring the company out of compliance. The legal consequences range from fines to company shutdown.

* + 1. Higher maintenance costs

Legacy software needs extra care in order to be secure, performant and compliant. More effort is required to meet the ever-increasing database maintenance challenges. Moreover, if a critical bug occurs, Microsoft will charge a significant amount of money to provide a fix.

## Upgrading SQL Server – end of mainstream support

Running unsupported SQL Server versions poses a severe threat to the business. The risks fall into 3 major categories: security, compliance and maintenance costs.

* + 1. Security

To protect the sensitive data, security updates should be installed as soon as they are released. Not deploying the latest security update will make the server and the applications accessing it vulnerable to cyberattacks, malware and data theft.

* + 1. Compliance

It is the legal responsibility of every organization to safeguard the sensitive data. Several regulations (HIPAA, PCI DSS, SOX, Dodd-Frank, GDPR, etc.) provide guidelines of the procedures a company needs to implement in order to protect itself from data theft. Running unsupported software might bring the company out of compliance. The legal consequences range from fines to company shutdown.

* + 1. Higher maintenance costs

Legacy software needs extra care in order to be secure, performant and compliant. More effort is required to meet the ever-increasing database maintenance challenges. Moreover, if a critical bug occurs, Microsoft will charge a significant amount of money to provide a fix.

## Upgrade Recommendations

* + 1. Upgrade to Azure

We strongly recommend migrating to Azure. Azure will always be safer, cheaper and fully compliant compared to any on-premises architecture. Here is a brief comparison between on-premises SQL Server and Azure SQL managed instance.

In addition, as Microsoft takes care of most of the critical DBA tasks, we see a 40% decrease in DBA resource allocation.

* + 1. On-premises Upgrade scenarios

If Azure is not an option, there are two approaches to consider when you are planning to upgrade the Database Engine from a prior release of SQL Server in order to minimize downtime and risk. You can upgrade the current SQL Server installation (in-place upgrade) or install a new upgraded instance and copy the databases across (side-by-side upgrade). Each approach comes with both advantages and disadvantages which should be carefully considered.

* + - 1. Side-by-side – new installation

A new instance is installed with the latest version of SQL Server and the databases are restored/copied. After the restore, both the old and the new server are kept in sync. Switching the applications to the new server ensures a fast failover with minimal downtime. If something goes wrong, there is always the option to failback to the old server as the databases remain in sync. The biggest disadvantage are the higher costs, as new hardware needs to be provisioned.

* + - 1. Side-by-side – Azure

To avoid the hardware costs for the previous scenario, an instance in Azure can be temporarily provisioned and kept in sync with the data on-premise. During a maintenance window, all the applications can be plugged temporarily to Azure SQL, until the on-premise server is upgraded. After the upgrade, the application can fall back to the on-premise instance. Azure helps again with the safest and most cost-effective upgrade solution, even when choosing to run SQL Server on-premises.

# Appendix A: Detailed Health Check

Below is a list of included areas in the detailed Health Check.

|  |
| --- |
| Area of Focus |
| Server Configuration Validation |
| Database Configuration Validation |
| VirusScan Configuration and Exclusions |
| Security Assessment |
| Indexing and Maintenance Strategy |
| Backup Plan |
| Performance Assessment |