

Simplified SQL Server Health Checklist

1. Make sure the instance name and server name are aligned

This is to help reduce confusion on the administrative and configuration side.

2. Make sure instant file initialization is enabled

This is a boost to performance, this can be a security issue [but is a net benefit](#).

3. Make sure as many jobs and databases are owned by sa as possible

If a user leaves the company, or has their account disabled for any reason it can cause jobs to fail. For databases we would recommend making the owner sa and giving the previous owner 'db_owner', if necessary.

4. Make TempDB have the number of files equal to the CPU up to 8, make sure they are sized the same.

This provides a small performance benefit

5. Check for server configurations

1. Backup checksum default to 1 (this is for corruption verification)
2. Backup compression default to 1 (this is to conserve disk space)
3. Max degree of parallelism to $\frac{1}{2}$ the number of CPUs up to 8 (this is to reduce the risk of one query using all of the server's processing power)
4. Cost threshold for parallelism to 50 (this is to increase the threshold for parallelism so that less simple queries are going parallel)
5. Optimize for ad-hoc to 1 (this increases performance if you have any one-off queries being run with any frequency)
6. Remote admin connections to 1 (this is helpful in case of SQL Server being locked up; [more explanation here](#))
7. Max memory (we recommend following [Jonathan Kehayias's recommendation](#) for most environments)

6. Alerts 3226 enabled, and 1117 and 1118 for pre-2016 environments.

3226 cleans up the error log by suppressing successful log backup messages. 1117 and 1118 are corruption-related and are built-in 2016 onward.

7. We recommend enabling errors 16-25 and 823-825

These are considered advanced errors and help with corruption detection and remediation. We recommend finding an expert immediately to help if you start getting these errors.

8. Maintenance (come up with a plan that works for your business, but this is our default.)

1. Are full backups being taken for user databases weekly? a. +c+d The full weekly, diff daily, and log every 15 minutes combined with Ola's 2-week cleanup times provides an easy point in time recovery.
2. Are full backups being taken for system databases daily? b. System databases can fail or be corrupted, having a backup makes an already painful system database restore a bit easier to manage because you won't be starting from scratch.
3. Are diff backups being taken for user databases in full recovery daily? See above.
4. Are log backups being taken for user databases in full recovery every 15 minutes? See above.
5. Are indexes being rebuilt and stats being updated weekly? e. Index and statistics maintenance ensures performance for existing indexes and data does not degrade over time as data is inserted and deleted.
6. Are integrity checks being run weekly (for user and system databases)? f. Integrity checks are an important part of corruption detection and remediation. Combined with a strong backup and recovery plan this minimize the impact corruption could have.

9. Update tools (Dbatools, Ola, and Brent Ozar's First Responder toolkit, whoisactive)

These tools are used across the industry. Updating them helps bring in new functionality.

10. Verify that database file autogrowth is not set to %

% autogrowth can cause performance and availability issues, especially with larger databases. We recommend a fixed autogrowth amount based on database size.

11. Make sure no databases have auto-shrink or auto-close enabled

Auto shrink can cause fragmentation problems, and auto close can also cause performance issues.

12. Make sure page verify is set to CHECKSUM for all databases.

Page-verification is a corruption checking tool, checksum is the best of the three options (none and torn-page being the other two).

13. Make sure recovery target interval is set to 60 for 2016 onward.

The new industry standard for 2016 onwards is that the recovery target should be set to 60 seconds.

14. As much as possible, make sure C:\ is not being used and that data, log, tempdb, and backups are all going to different drives.

Seeing environments where everything is on the C:\ drive, or TempDB shares a disk with data or log and backups can be concerning. The adage of not putting all of your eggs into one basket applies here. Not to mention that performance would increase if these loads were separated.