Using Antivirus with SQL Server

In a perfect world, your SQL Server would be so secure that you would not need antivirus software, you would have behind layers of firewalls, nobody would ever connect with remote desktop to install anything, and it would always have all of the latest security patches… But that is not the real world.

Given that your SQL Server often times contains extremely valuable information, and that the damage that could be done by virus software, malware, and ransomware could be so great then it is strongly recommended that you run antivirus software on your SQL Server. There are some files that you will want to exclude from the virus check.

SQL Server Antivirus Exclusion List:

You will want to exclude the following files from the antivirus check list.

- SQL Server data and log files (.mdf, .ldf and .ndf files)
    - It is probably a good idea to just exclude the entire directory that holds your data or log files. The reason that I suggest this is that there are other files created in the same location as the data file when certain things run, for instance CheckDB creates temporary snapshot files in the data file directory. Excluding the data and log file directory would be the safe way to go here.
- SQL Server backup files
- Full-Text catalog files (if you are using full text search)
- Trace files (if you have traces running)
- SQL audit files (for SQL Server 2008 or later versions)
- SQL query files (.sql extension)
- The directory that holds Analysis Services data
- The directory that holds Analysis Services temporary files that are used during Analysis Services processing

The problem you run into is when someone installs antivirus on the SQL Server, without being aware of the exclusions, you can run into a number of issues such as the following:
• When the SQL Server is running, data and log files are generally locked preventing other processes from being able to change or read them. This can cause problem with the antivirus software blocking attempting to get to these files.
• If you restart the system, or restart the SQL instance, it is possible that the antivirus software could start first and open a data or log file to scan it for viruses, at which point when SQL Server starts it may not be able to access that file, therefore preventing SQL Server from starting.
• If the antivirus file finds some pattern that it suspects as a virus in your data or log file, and it

attempts to quarantine that file it could lead to extreme problems with the SQL Server.
My recommendation is to always run antivirus software on your SQL Server, but be sure to exclude the files mentioned above to avoid problems.

Related Links:

- Microsoft post on Running Antivirus on SQL Server
- Database Health Monitor