File Exclusions for SharePoint, SQL, OWA, IIS and Windows Server – Bryan Warhold

Friday, August 2, 2019 11:34 AM

Clipped from:
https://blogs.msdn.microsoft.com/bryanwarhold/2017/09/06/collection-of-file-exclusions-for-sharepoint-sql-owa-iis-and-windows-server/

Compiled a list of file exclusions based on a few different sources to have in one place.

SharePoint Server Exclusions

Note In the following sections, the placeholder Drive represents the letter of the drive on which you have your SharePoint application installed. Typically, this drive letter is C.

SharePoint Server 2016

You may have to configure your antivirus software to exclude the following folders and subfolders from antivirus scanning:

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions

If you do not want to exclude the whole Web Server Extensions folder from antivirus scanning, you can exclude only the following folders:

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16
- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\Logs
- Drive:\Program Files\Microsoft Office Servers\16.0\Data\Office Server \Applications
- Drive:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- Drive:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config
- Drive: \Users\ServiceAccount\AppData\Local\Temp\WebTempDir

Note: The WebTempDir folder is a replacement for the FrontPageTempDir folder.

- Drive:\ProgramData\Microsoft\SharePoint
- Drive:\Users\account that the search service is running as\AppData \Local\TempNote The search account creates a folder in the Gthrsvc_spsearch4 Temp folder to which it periodically must write.
- Drive:\WINDOWS\System32\LogFiles
- Drive:\Windows\Syswow64\LogFilesNote If you use a specific account for SharePoint services or application pools identities, you may also have to exclude the following folders:
- Drive:\Users\ServiceAccount\AppData\Local\Temp

- Drive:\Users\Default\AppData\Local\Temp

You should also exclude all the virtual directory folders:

- Drive:\inetpub\wwwroot\wss\VirtualDirectories and all the folders
- Drive:\inetpub\temp\IIS Temporary Compressed Files.

References:

From <https://support.microsoft.com/en-us/help/952167/certain-folders-may-have-to-be-excluded-from-antivirus-scanning-when-y>

SQL Server Exclusions

When you configure your antivirus software settings, make sure that you exclude the following files or directories (as applicable) from virus scanning. Doing this improves the performance of the files and helps make sure that the files are not locked when the SQL Server service must use them. However, if these files become infected, your antivirus software cannot detect the infection.

Note For more information about the default file locations for SQL Server, refer to the "File Locations for Default and Named Instances of SQL Server" topic for your specific version of SQL Server in SQL Server Books Online.

Files and Directory Exclusions

- SQL Server data files
    - *.mdf
    - *.ldf
    - *.ndf
- SQL Server backup files
    - *.bak
    - *.trn
- Full-Text catalog files
    - Default instance: Program Files\Microsoft SQL Server\MSSQL \FTDATA
    - Named instance: Program Files\Microsoft SQL Server\MSSQL $instancename\FTDATA
- Trace files
    - *.trc - these files can be generated either when you configure profiler tracing manually or when you enable C2 auditing for the server.
- SQL audit files (for SQL Server 2008 or later versions)
    - *.sqlaudit

- SQL query files
    - *.sql

The directory that holds Analysis Services data â€" default is C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Data. You can view and change the data directory by using Analysis Manager. To do this, follow these steps:

1. In Analysis Manager, right-click the server, and then click Properties.
2. In the Properties dialog box, click the General tab. The directory appears under Data folder.

- The directory that holds Analysis Services temporary files that are used during Analysis Services processing â€" default is C:\Program Files \Microsoft SQL Server\MSSQL.X\OLAP\Data. You can view and change the directory that holds temporary files in Analysis Manager. To do this, follow these steps:

1. In Analysis Manager, right-click the server, and then click Properties.
2. In the Properties dialog box, click the General tab.
3. On the General tab, notice the directory under Temporary file folder.

Note : Optionally, you can add a second temporary directory for Analysis Services 2000 by using the TempDirectory2 registry entry. If you use this registry entry, consider excluding from virus scanning the directory to which this registry entry points

- Analysis Services backup files â€" default is C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Backup
- The directory that holds Analysis Services log files â€" default is C: \Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Log
- Directories for any Analysis Services 2005 and later-version partitions that are not stored in the default data directory
- Note When you create the partitions, these locations are defined in the Storage location section of the Processing and Storage Locations page of the Partition Wizard.
- Filestream data files (SQL 2008 and later versions)
- Remote Blob Storage files (SQL 2008 and later versions)
- The directory that holds Reporting Services temporary files and Logs (RSTempFiles and LogFiles)

For an exhaustive list:

SQL Server 2016

https://docs.microsoft.com/sql/sql-server/install/file-locations-for-default-and-named-instances-of-sql-server

SQL Server 2014
https://msdn.microsoft.com/en-us/library/ms143547(v=sql.110).aspx

SQL Server 2012

http://msdn.microsoft.com/en-us/library/ms143547(v=sql.120).aspx

Process Exclusions

SQL Server 2012

- %ProgramFiles%\Microsoft SQL Server\MSSQL11.<Instance Name>\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSRS11.<Instance Name>\Reporting Services\ReportServer\Bin \ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSAS11.<Instance Name>\OLAP\Bin\MSMDSrv.exe

References:

From <https://blogs.technet.microsoft.com/raymond_ris/2014/01/16/windows-antivirus-exclusion-recommendations-servers-clients-and-role-specific/>

From <https://support.microsoft.com/en-us/help/309422/how-to-choose-antivirus-software-to-run-on-computers-that-are-running>

Office Web App Server/Office Online Server Exclusions

- [Prog Dir]:\Program Files\Common Files
- [Prog Dir]\Program Files\Microsoft Office Web Apps\
- %systemroot%\system32\inetsrv\
- %systemroot%\SysWOW64\inetsrv\
- %SystemDrive%\inetpub\
- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- C:\Users\Default\AppData\Local\Temp

References:

Antivirus Exception for Workflow Manager, SQL Server, Office Web App, SharePoint 2013 and SharePoint 2010

From <https://social.technet.microsoft.com/wiki/contents/articles/32683.antivirus-exception-for-workflow-manager-sql-server-office-web-app-

sharepoint-2013-and-sharepoint-2010.aspx>

Workflow Manager Server Exclusions

- C:\Program Files\Service Bus
- C:\Program Files\Workflow Manager
- C:\Program Files (x86)\Workflow Manager Tools
- C:\ProgramData\Workflow Manager
- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- %SystemDrive%\inetpub
- %systemroot%\system32\inetsrv\
- %systemroot%\SysWOW64\inetsrv\
- C: \Users\Default\AppData\Local\Temp

Antivirus Exception for Workflow Manager, SQL Server, Office Web App, SharePoint 2013 and SharePoint 2010

References:

From <https://social.technet.microsoft.com/wiki/contents/articles/32683.antivirus-exception-for-workflow-manager-sql-server-office-web-app-sharepoint-2013-and-sharepoint-2010.aspx>

Windows Server, IIS Exclusions

Exclude the IIS compression directory from the antivirus software's scan list.

The default compression directory in IIS 6.0 is %systemroot%\IIS Temporary Compressed Files. This directory may have been changed to another location. In IIS 7.0, the default location of the compressed file cache is %SystemDrive%\inetpub\temp\IIS Temporary Compressed Files.

To verify the compression directory:

1. Click Start, point to Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. In IIS Manager, right-click the Web Sites folder, and then click Properties.
3. Click the Service tab.

Under HTTP Compression, make sure that Compress static files is selected, and then locate the path to the temporary directory.

Process Exclusions

- %systemroot%\system32\inetsrv\w3wp.exe
- %systemroot%\SysWOW64\inetsrv\w3wp.exe

References:

From <https://blogs.technet.microsoft.com/raymond_ris/2014/01/16/windows-antivirus-exclusion-recommendations-servers-clients-and-role-specific/>

Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows

From <https://support.microsoft.com/en-us/help/822158/virus-scanning-recommendations-for-enterprise-computers-that-are-runni>