## Files on Domain Controller Not at Risk of Infection.

Exclude the following files and folders from being scanned. These files are not at risk of infection and including them could cause serious performance problems due to file locking and excessive replication between domain controllers. Furthermore, they may cause Active Directory and FRS to work improperly, causing Active Directory or FRS data loss. Where a specific set of files is identified by name, exclude only those files rather than the entire folder. In some cases, the entire folder must be excluded.

Do not exclude any of these based on the file name extension (that is, do not exclude all files with a .dit extension). Microsoft has no control over other files that might choose to use the same extension as those shown here. AV software must not modify any data files in the logs, database, and/or DSA working directories specified below.

* Main NTDS database files. The location of these files is specified in:

**HKEY\_LOCAL\_MACHINE \System\CurrentControlSet\Services\NTDS\Parameters\DSA Database File**

Default location is %windir%\ntds

The file to exclude is: **NTDS.dit**

* Active Directory transaction log files. The log directory on any given server is specified in:

**HKEY\_LOCAL\_MACHINE \System\CurrentControlSet\Services\NTDS\Parameters\Database Log Files Path**
Default location is %windir%\ntds.

The specific files to exclude are:

* EDB\*.log (notice the wildcard—there can be several)
* RES1.log
* RES2.log

NTDS Working folder specified in:

**HKEY\_LOCAL\_MACHINE \System\CurrentControlSet\Services\NTDS\Parameters\DSA Working Directory**

Specific files to exclude are:

* TEMP.edb
* EDB.chk
* SYSVOL. Use the following table for folders and files to scan or exclude:

|  |  |
| --- | --- |
| Folder or File  | Scan or Exclude  |
| %systemroot%\SYSVOL | Exclude |
| %systemroot%\SYSVOL\domain | Scan |
| %systemroot%\SYSVOL\domain\DO\_NOT\_REMOVE\_NtFrs\_PreInstall\_Directory | Exclude |
| %systemroot%\SYSVOL\domain\policies | Scan |
| %systemroot%\SYSVOL\domain\scripts | Scan |
| %systemroot%\SYSVOL\staging | Exclude |
| %systemroot%\SYSVOL\staging areas | Exclude |
| %systemroot%\SYSVOL\sysvol | Exclude |

FRS Working Directory specified in:

**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\Working Directory**

Files to exclude:

* <FRS Working Directory>\jet\sys\edb.chk
* <FRS Working Directory>\jet\ntfrs.jdb
* <FRS Working Directory>\jet\log\\*.log

FRS Database Log files specified in:

**HKEY\_LOCAL\_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\DB Log File Directory**
Default location is %windir%\ntds.

Files to exclude:

* <FRS Working Directory>\jet\log\\*.log (if registry entry is not set)
* <DB Log File Directory>\log\\*.log (if registry entry is set)
* FRS Replica\_root files specified in:

**HKEY\_LOCAL\_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\Replica Sets\GUID\Replica Set Root**

* Staging directory found in:

**HKEY\_LOCAL\_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\Replica Sets\GUID\Replica Set Stage**

* FRS Preinstall directory located at:

<Replica\_root>\DO\_NOT\_REMOVE\_NtFrs\_PreInstall\_Directory.

The Preinstall directory is always open exclusively when FRS is running.