Managing Antivirus Software on Active Directory Domain Controllers

Updated: January 15, 2009

Because domain controllers provide critical services to their clients, it is crucial to minimize the risk of any disruption of these services that may be caused by malicious code.

You can generally use antivirus software to mitigate the risk of malicious code. However, installing antivirus software (from any vendor) on a domain controller and configuring it to scan everything is not a reliable or recommended solution because the antivirus software may interfere with domain controller performance. Specifically, the scanning procedures that most antivirus applications use require exclusive locks on files. In many cases, these locks can interfere with the real-time data replication that domain controllers use to stay synchronized with the rest of the network.

The antivirus software that you use must be compatible with Windows operating systems in general and domain controllers in particular. Antivirus software must be installed in a manner that protects against attacks as much as possible while not interfering with domain controller performance. For example, antivirus software must be able to scan Distributed File System (DFS) files that are replicated by File Replication Service (FRS) or DFS Replication in a way that does not initiate full synchronization of files and folders in SYSVOL or of DFS roots and links. Any antivirus vendor should provide specific instructions to correctly configure their product to work with domain controllers that are running versions of Windows Server and that have Active Directory Domain Services (AD DS) installed.

We cannot guarantee the interoperability of any antivirus software with DFS Replication, including any tests recommended in this guide. The need for extensive testing can be avoided completely by asking their antivirus software vendor to disclose their tested interoperability with DFS Replication. Vendors that have tested their software are happy to stand by their products. For a list of antivirus software vendors, see article 49500 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=22381).

**Guidelines for managing antivirus software on Active Directory domain controllers**

Follow the guidelines from your antivirus software vendor. Verify that the antivirus software you select is confirmed to be compatible with your domain controllers. Test your chosen antivirus software solution thoroughly in a lab environment to ensure that the software does not compromise the stability of your system.

Antivirus software has been known to cause blue screens on domain controllers. Before you install antivirus software or any update to that software on domain controllers in a domain, test lab domain controllers for the following issues:

 Stability issues

 Memory leaks

 High CPU usage

 Interruptions or failure of inbound and outbound replication

The following recommendations are general and should not be construed as more important than the specific recommendations of your antivirus software vendor. These guidelines must be followed for correct Active Directory file replication operation:

 Antivirus software must be installed on all domain controllers in the enterprise. Ideally, such software should also be installed on all other server and client computers that have to interact with the domain controllers. Catching the virus at the earliest point—at the firewall or at the client computer on which the virus is first introduced—is the best way to prevent the virus from ever reaching the infrastructure systems on which all client computers depend.

 Use a version of antivirus software that is confirmed to work with AD DS and that uses the correct application programming interfaces (APIs) for accessing files on the server. Some versions of antivirus software inappropriately modify file metadata as it is scanned, causing the FRS replication engine to perceive a file as having changed and to schedule it for replication. Some newer versions of antivirus software prevent this problem. For more information about antivirus software versions and FRS, see article 815263 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=120540) and see the vendor-specific sites for compliant versions.

Verify antivirus compatibility with DFS Replication, as described in Testing Antivirus Application Interoperability with DFS Replication (http://go.microsoft.com/fwlink/?LinkId=122787).

**Note**

If you are using ForeFront Client Security, see article 956123 in the Microsoft

Knowledge Base for a hotfix (http://go.microsoft.com/fwlink/?LinkId=131409).

 Prevent the use of domain controller systems as general workstations. Users should not use a domain controller to surf the Web or to perform any other activities that can allow the introduction of malicious code. Allow browsing of known safe sites only for the purpose of supporting server operation and maintenance.

 When possible, do not use a domain controller as a file sharing server. Virus scanning software must be run against all files in the shared folders, and it can place a large resource load on the processor and memory resources of the server. For the same reason, the SYSVOL and Netlogon shares that are automatically created on domain controllers should not be used to distribute software or for to store data.



**Files to exclude from scanning**

Exclude the following files and folders from your antivirus scanning operations. These files are not at risk of infection, and including them can cause serious performance problems or loss of functionality as a result of file locking and excessive replication between domain controllers. Furthermore, scanning these files may cause AD DS, FRS, and DFS Replication to work improperly, possibly causing data loss. Where a specific set of files is identified by name, exclude only those files rather than the entire folder. In some cases, you must exclude the entire folder.

Do not exclude any files that you think are not at risk based only on the file name extension. (For example, do not exclude all files with a .dit extension.) Microsoft has no control over other files that might use the same file name extension as the files shown here. Antivirus software must not modify any data files in the logs, database, or directory service working directories that are specified below.

**Active Directory and related files to exclude**

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

**HKLM\System\CurrentControlSet\Services\NTDS\Parameters\DSA Database File**

The default location is %systemroot%\ntds.

File to exclude:

o **Ntds.dit**

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

**HKLM\System\CurrentControlSet\Services\NTDS\Parameters\Database Log Files Path**

The default location is %systemroot%\ntds.

Files to exclude:

1. o EDB\*.log (Notice the wildcard symbol; there can be several log files.)
2. o Edbres00001.jrs
3. o Edbres00001.jrs

 The NTDS Working folder that is specified in:

**HKLM\System\CurrentControlSet\Services\NTDS\Parameters\DSA Working Directory**

Files to exclude:

1. o TEMP.edb
2. o EDB.chk

**SYSVOL files to exclude**

The list in the following table shows the default locations of files and folders to be excluded or scanned for the SYSVOL directory and subdirectories when you use FRS to replicate SYSVOL.

**Important**

If you have placed SYSVOL in another location, then exclude the appropriate path for your installation.

**Scan or Folder or File Exclud e**

%systemroot%\SYSVOL Exclude %systemroot%\SYSVOL\domain Scan %systemroot%\SYSVOL\domain\DO\_NOT\_REMOVE\_NtFrs\_PreInstall\_Direc

Exclude

tory %systemroot%\SYSVOL\domain\policies Scan %systemroot%\SYSVOL\domain\scripts Scan %systemroot%\SYSVOL\staging Exclude %systemroot%\SYSVOL\staging areas Exclude %systemroot%\SYSVOL\sysvol Exclude

**FRS and related files to exclude**

 The FRS working directory that is specified in:

**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\NtFrs\Par ameters\Working Directory**

Files to exclude:

1. o <FRS working directory>\jet\sys\edb.chk
2. o <FRS working directory>\jet\ntfrs.jdb

o <FRS Working Directory>\jet\log\\*.log  The FRS database log files that are specified in:

**HKEY\_LOCAL\_MACHINE\system\currentcontrolset\services\NtFrs\Param eters\DB Log File Directory**

The default location is %systemroot%\ntds.

Files to exclude:

o <FRS working directory>\jet\log\\*.log (if the registry entry is not set)

o <Database log file directory>\log\\*.log (if the registry entry is set)  FRS Replica\_root files that are specified in:

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

 The staging directory in:

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

 The FRS Preinstall directory at: **<Replica\_root>\DO\_NOT\_REMOVE\_NtFrs\_PreInstall\_Directory**. The Preinstall directory is always open when FRS is running.

**DFS Replication and related files to exclude**

 System Volume Information\DFSR folders and their contents (includes DFSR.DB). This system-protected directory contains working files for the DFS Replication service. It should not be scanned because these files are always in use by the service.

 <Replicated folder path>\dfsrprivate folders and their contents