Knowledge Base

Virus scanning recommendations on a Windows 2000 or on a Windows Server 2003 domain controller

PSS ID Number: 822158

Article Last Modified on 11/16/2004

The information in this article applies to:

- Microsoft Windows Server 2003, Datacenter Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

Important This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

256986 Description of the Microsoft Windows Registry

SUMMARY

This article contains recommendations that may help you protect your Windows 2000 and Windows Server 2003 domain controllers against viruses. It also contains information to help you minimize the affect of antivirus software on system and network performance.

MORE INFORMATION

Because domain controllers provide a critical service to clients, the risk of disruption of their activities as a result of malicious code from a virus must be minimized. Antivirus software is the generally accepted way to mitigate the risk of virus infection. Install and configure antivirus software so that the risk to the domain controller is reduced as much as possible and so that performance is affected as little as possible. The following list contains recommendations to help you configure and install antivirus software on a Windows 2000 or on a Windows Server 2003 domain controller:

Warning Microsoft recommends that you apply the following specified configuration to a test configuration to make sure that in your specific environment it does not introduce unexpected factors or compromise the stability of the system. The risk from too much scanning is that files are inappropriately flagged as having been changed, resulting in excessive replication on the Active Directory directory service. If testing verifies that replication is not affected by the following recommendations, you can apply the antivirus software to the production environment.

Note Specific recommendations from antivirus software vendors may supersede the recommendations in the article.

- Antivirus software must be installed on all domain controllers in the enterprise. Ideally, try to install such software on all other server and client systems that have to interact with the domain controllers. It is optimal to catch the virus at the earliest point, such as at the firewall or at the client system where the virus is first introduced. This prevents the virus from ever reaching the infrastructure systems that the clients depend on.
- Use a version of antivirus software that is designed to work with Active Directory domain controllers and that uses the correct Application Programming Interfaces (APIs) to access files on the server. Older versions of most vendor software inappropriately modify file metadata as it is scanned, causing the File Replication Service engine to recognize a file change and therefore schedule the file for replication. Newer versions prevent this problem. For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

  815263 Antivirus, backup, and disk optimization programs that are compatible with the File Replication service
- Do not use a domain controller to browse the Web or to perform any other activities that may introduce

malicious code.

- Where possible, do not use the domain controller as a file sharing server. Virus scanning software must be run against all files in those shares, and this can put an unsatisfactory load on the processor and the memory resources of the server
- Do not place Active Directory or FRS database and log files on NTFS file system compressed volumes. For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

  318116 Issues with Jet Databases on compressed drives
- Do not scan the following files and folders. These files are not at risk of infection, and if you include them, this may cause serious performance problems because of file locking. Where a specific set of files is identified by name, exclude only those files instead of the whole folder. Sometimes, the whole folder must be excluded. Do not exclude any of these based on the file-name extension; for example, do not exclude all files with a .dit extension). Microsoft has no control over other files that may use the same extension as those shown here.

  Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.
  - Active Directory and Active Directory-related files:
    - Main NTDS database files. The location of these files is specified in the following registry key:

      `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\DSA Database File`

      The default location is %windir%\ntds. Exclude the following files:

      Ntds.dit
      Ntds.pat
    - Active Directory transaction log files. The location of these files is specified in the following registry key:

      `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\Database Log Files Path`

      The default location is %windir%\ntds. Exclude the following files:

      EDB*.log (the wildcard character indicates that there may be several files)
      Res1.log
      Res2.log
      Ntds.pat
    - The NTDS Working folder that is specified in the following registry key:

      `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\DSA Working Directory`

      Exclude the following files:

      Temp.edb
      Edb.chk
  - SYSVOL files:
    - The File Replication Service (FRS) Working folder that is specified in the following registry key:

      `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\Working Directory`

      Exclude the following files:

      FRS Working Dir\jet\sys\edb.chk
      FRS Working Dir\jet\ntfrs.jdb
      FRS Working Dir\jet\log\*.log
    - The FRS Database Log files that are located in the following registry key:

      `HKEY_LOCAL_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\DB Log File Directory`

      The default location is %windir%\ntfrs. Exclude the following files:

      FRS Working Dir\jet\log\*.log (if registry key is not set)
      DB Log File Directory\log\*.log (if registry key is set)
    - The Staging folder that is specified in the following registry key and all of the Staging folder's sub-

folders:

```
HKEY_LOCAL_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\Replica
Sets\GUID\Replica Set Stage
```

The current location of the Staging folder and all of its sub-folders is the file system reparse target of the replica set staging folders. Staging defaults to the following location:

%systemroot%\sysvol\staging areas

The current location of the SYSVOL\SYSVOL folder and all of its sub-folders is the file system reparse target of the replica set root. The SYSVOL\SYSVOL folder defaults to the following location:

%systemroot%\sysvol\sysvol

- The FRS Preinstall folder that is in the following location:

  Replica_root\DO_NOT_REMOVE_NtFrs_PreInstall_Directory

  The Preinstall folder is always open when FRS is running.

In summary, the targeted and excluded list of folders for a SYSVOL tree that is placed in its default location would look similar to the following:

```
1.  %systemroot%\sysvol
2.  %systemroot%\sysvol\domain
3.  %systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory          Exc
4.  %systemroot%\sysvol\domain\Policies
5.  %systemroot%\sysvol\domain\Scripts                                           Sca
6.  %systemroot%\sysvol\staging
7.  %systemroot%\sysvol\staging areas                                            Exc
8.  %systemroot%\sysvol\sysvol
```

If any one of these folder or files have been moved or placed in a different location, scan or exclude the equivalent element.

- DFS

  The same resources that are excluded for a SYSVOL replica set must also be excluded when FRS is used to replicate shares that are mapped to the DFS root and link targets on Windows 2000 or Windows Server 2003-based member computers or domain controllers.

Additional query words: virus scan dc

Keywords: kbinfo kbprb KB822158
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch kbWinServ2003Data kbWinServ2003DataSearch kbWinServ2003Ent kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St

Send feedback to Microsoft