Knowledge Base

Antivirus programs may modify security descriptors and cause excessive replication of FRS data in SYSVOL and DFS

PSS ID Number: 284947

Article Last Modified on 1/26/2005

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

This article was previously published under Q284947

SUMMARY

The File Replication service (FRS) is a multi-threaded, multi-master replication engine that replaces the Lmrepl service in the 3.*x* and 4.0 versions of Microsoft Windows NT. Microsoft Windows 2000-based domain controllers and servers use FRS to replicate system policy and logon scripts that reside in the System Volume (SYSVOL) for Windows 2000-based clients and earlier.

FRS can also replicate files and directories between Windows 2000-based servers that are members of the same fault-tolerant Distributed File System (DFS) root or link replicas.

FRS initiates replication on "closed" files in directory trees in which replication has been enabled. Events that can trigger replication include the creation or deletion of a file, a version change to an existing file, or the resetting of permissions on a file or directory. This article describes the symptoms that occur when some antivirus programs that are not FRS-compliant perform virus scans on directories that host FRS-replicated files. Additional symptoms include:

- Files in SYSVOL and DFS shares are replicated excessively with no apparent change to the files in those replica sets.
- Files may replicate at off-peak hours, or at regularly occurring times if virus scans are scheduled to occur at specific times, or during periods of low server utilization.
- The number of files in the staging directory constantly grows, perhaps emptying sometime after the virus scan program completes, or after the FRS schedule opens to allow replication.
- The number of files in the staging directory constantly grows but never empties if changes to downstream partners cannot be replicated either because of network connectivity or an inability to process the number of modified files needing replication.
- Network traffic between replication partners is consuming excessive network bandwidth and FRS is determined to be the responsible service.

One program that is known to reset security descriptors during virus scan is Norton AntiVirus (NAV) versions 7.0 and 7.5. Other virus checking programs that modify security descriptors during virus scans will result in the same symptoms.

MORE INFORMATION

The File Replication Service (FRS) monitors the NTFS file system USN journals for changes to files and directories that occur in FRS-replicated Sysvol and DFS trees. Some antivirus utilities modify the security descriptor during virus scans. A security descriptor is an attribute in the file system of NTFS-formatted drives that defines who and what type of access users and groups have to files and directories.

FRS properly records the modification to the file and the directory in the NTFS USN journal and then queues the change in its staging directory for replication to all direct and transitive downstream partners. Downstream partners are those computers in a DFS or SYSVOL replica set that have inbound connection objects from a computer that is sending changes for modified files.

Virus scans against large FRS-replicated directories may result in the replication of hundreds of megabytes or even gigabytes worth of files every time a scan takes place. The number and rate of modified files needing replication often become unsustainable, particularly when virus scans are taking place on more than one member of a SYSVOL or DFS replica set.

Representatives from Symantec describe NAV's modification of the security descriptor in the following way:

> During a scan, NAV will save various attributes of the file (file attributes, the security descriptor GetFileSecurity, last access timestamp, and so forth) before the scan so that the file can be restored to its original condition. Several of these attributes including the security descriptors (SetFileSecurity) are restored.
>
> In the case of FRS replication, calling the Windows API SetFileSecurity to restore the security descriptor triggers replication. The same effect can be duplicated from the **Security** tab of Windows Explorer by granting a user file permissions to access to a file, and then immediately removing the access right.
>
> This problem does not occur on all files, but rather on container files, including those with .exe, .doc, .ppt, .xls, .zip, .arc, and .cab extensions.

Displaying USN Change Reasons on FRS-Replicated Files

The FRS debug log files and the outbound log files of the FRS database record the type of change that initiated replication of a file or directory. Use the following method to determine if virus scan programs are causing excessive FRS replication traffic in your environment.

NOTE: The examples in this article illustrate how to search the debug logs for change reason.

1. Increase FRS log verbosity and endurance. To do this, start Registry Editor, and then in the following registry key

   HLKM\SYSTEM\CCS\Services\NTFRS\Parameters

   set the following values:

   - "Debug Maximum Log Messages (REG_DWORD)" to 20000 decimal (no comma in registry entry)
   - "Debug Log Files (REG_DWORD)" between 20 to 50 decimal

     The default log verbosity for the Windows 2000 2195 build and Service Pack 1 (SP1) release of FRS is level 4. The default log verbosity for the SP2 and SP2 hotfix version of FRS is level 2. To see the "ContentCmd" string in the FRS debug logs, set the "Debug Log Severity (REG_DWORD)" value to "4".
2. Restart the service, and then let it run for a sufficient period of time. If you do not set the log verbosity high enough, you may be able to filter on the "UsnReason" string in the debug logs to locate the type of modification that took place.
3. From a command prompt, type the following command line:

   ```
   cd /d %systemroot%\debug"
   ```

   HINT: Use the **Layout** tab of the command property sheet to set window size, width, and height to accommodate **findstr** output. Use approximately 110 characters for width and 45 characters or more for height on a screen resolution of 1024 X 768 display.
4. Use **findstr** to locate all instances of the "ContentCmd" string in the debug log files:

   ```
   c:\>findstr /i "ContentCmd" %systemroot%\debug\ntfrs_00??.log
   ```

   The type of change that took place on the NTFS-formatted partition is displayed by the "ContentCmd" string in the debug log. Files that were modified by antivirus programs list "Security" as the change reason. Similarly, security templates that were applied manually or by group policy, as well as administrators setting permissions in Windows Explorer, also show "Security" as the change reason.

   The following sample illustrates output of a FRS debug logs filtered with the **frsstr** command:

   ```
   <ChgOrdRetryWorker: ... S4:  hh:mm:ss>  ContentCmd:  80008800  Flags  [Close Info Security
   <ChgOrdDispatch:    ... S4:  hh:mm:ss>  ContentCmd:  80008800  Flags  [Close Info Security
   <ChgOrdAccept:      ... S4:  hh:mm:ss>  ContentCmd:  80008800  Flags  [Close Info Security
   <ChgOrdRetryWorker: ... S4:  hh:mm:ss>  ContentCmd:  80008800  Flags  [Close Info Security
   <ChgOrdRetryWorker: ... S4:  hh:mm:ss>  ContentCmd:  80008800  Flags  [Close Info Security
   <ChgOrdAccept:      ... S4:  00:24:37>  ContentCmd:  00008800  Flags  [Info Security ]
   <ChgOrdAccept:      ... S4:  00:24:37>  ContentCmd:  00008800  Flags  [Info Security ]
   <DbsWriteTableRecord:   S1:  00:24:37>  ContentCmd:  00008800  Flags  [Info Security ]
   <ChgOrdAccept:      ... S4:  00:24:37>  ContentCmd:  00008800  Flags  [Info Security ]
   ```

5. If excessive replication is suspected, proceed to the "Recovering from Excessive Replication" section in this article.

FRS Change Reasons in the FRS Debug and Outbound Logs

Flags that are set in the NTFRS debug log describe modifications to FRS-replicated files. FRS replication is predicated on closed files residing on NTFS 5.0-formatted partitions in FRS-replicated directories. The reasons for changes in FRS-replicated directories are displayed in the following table:

```
Close  - Change log close record
Create - File or dir was created
Delete - File or dir was deleted
RenNew - File or dir was renamed
DatOvrWrt       - Main file data stream was overwritten
DatExt - Main file data stream was extended
DatTrunc        - Main file data stream was truncated
Info            - Basic info change (attrib, last write time, and so forth)
Oid             - Object Id change
StreamNam       - Alternate data stream name change
StrmOvrWrt      - Alternate data stream was overwritten
StrmExt         - Alternate data stream was extended
StrmTrunc       - Alternate data stream was truncated
EAChg  - Extended file attribute was changed
Security        - File access permissions changes
IndexableChg    - File change requires re-indexing.
HLink  - Hardlink change
CompressChg     - File compression attribute changed
EncryptChg      - File encryption changed
Reparse         - Reparse point changed
```

Avoiding Excessive Replication by Antivirus Utilities

You can use the following steps to prevent antivirus programs from causing excessive replication of FRS-monitored directories:

1. Exclude FRS-replicated directories from being scanned by antivirus programs that cause excessive replication.
2. Obtain the updated versions of NAV that avoid changing the security descriptor of files.
3. Configure the list of folders that are targeted and excluded by antivirus programs as defined in the following Knowledge Base article:

   822158 Virus scanning recommendations on a Windows 2000 or on a Windows Server 2003 domain controller

Recovering from Excessive Replication

If excessive replication as a result of an antivirus program resetting security descriptors is discovered, consider the following action plan:

1. Stop the FRS service on members of FRS replica sets generating excessive changes to prevent the backlog from increasing
2. Stop any programs, services, or administrative processes that are modifying files and directories in FRS-replicated directories. Potential sources of replication include:
   a. Microsoft Systems Management Server client installed on Windows 2000 domain controllers.
   b. Security templates containing file system policy that are applied manually or by Group Policy to the Organizational Units or parent containers that are hosting Windows 2000 domain controllers or DFS-replicated directories.
   c. Diskeeper scans against FRS-replicated content.
   d. Antivirus scans against FRS-replicated content.
   e. Virus programs creating files in FRS-replicated directories.
3. Identify the servers that have large backlogs of changes

   Use the output of the **ntfrsutl sets** command-line utility that is parsed with the CONNSTAT PERL script to view downstream partners that have large backlogs of change orders.
4. Remove or disable the connections to downstream partners.

The FRS service builds staging files and stores change orders in its outbound log for all modified files that need to be sent to downstream partners. Upstream partners maintain staging files and change orders in the outbound log until all downstream partners receive a given change.

The FRS service deletes files in the staging directory and its outbound log when the connection object to the downstream partner is deleted or its connection is disabled; "enabledConnection" is an attribute on Active Directory, SYSVOL, and DFS connection objects that can be set to =true|false and that can be set in LDP, or ADSIEDIT.

Deleting connection objects for Active Directory and SYSVOL is an easy task as they are easily identified and can be re-created in the Active Directory Sites and Services snap-in.

5. Stagger the creation and/or enabling of connection objects.

Keywords: kb3rdparty kbinfo KB284947
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch kbWinServ2003Data kbWinServ2003DataSearch kbWinServ2003Ent kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St

---