CSS SQL Server Engineers

This is the official team Web Log for Microsoft Customer Service and Support (CSS) SQL Support. Posts are provided by the CSS SQL Escalation Services

The Case of Anti-Virus filter drive interference with File Stream Restore

psssql 29 Mar 2013 2:47 PM 1

"Denzil and I were working on this issue for a customer and Denzil has been gracious enough to write-up a blog for all of us." – Bob Dorr

From Denzil:

I recently worked with a customer on a Database restore issue where the database being restored had 2TB of File stream data. The restore in this case would just not complete successfully and would fail with the error below.

10 percent processed.

20 percent processed.

30 percent processed.

40 percent processed.

Msg 3634, Level 16, State 1, Line 1

The operating system returned the error '32(The process cannot access the file because it is being used by another process.)' while attempting 'OpenFile' on 'F:\SQLData11\DataFiles\535cc368-de43-4f03-9a64-f5506a3f532e\547fc3ed-da9f-44e0-9044-12babdb7cde8\00013562-0006edbb-0037'.

Msg 3013, Level 16, State 1, Line 1

RESTORE DATABASE is terminating abnormally.

Subsequent restore attempts would fail with the same error though on "different" files and at a different point in the restore cycle.

Given that this was "not" the same file or the same point of the restore on various attempts my thoughts immediately went to some filter driver under the covers wreaking some havoc. I ran an a command to see what filter drivers were loaded (trimmed output below.)

C:\>fltmc instances

```
Filter Volume Name Altitude Instance Name

------------------- ---------------------- ------------ ---------------------- -----

BHDrvx64             F:\SQLData11             365100           BHDrvx64                      0

eeCtrl               F:\SQLData11              329010           eeCtrl                         0

SRTSP                F:\SQLData11              329000           SRTSP                          0

SymEFA                 F:\SQLData11              260600           SymEFA                           0

RsFx0105               \Device\Mup               41001.05         RsFx0105 MiniFilter Instance  0
```

SymEFA = Symantec extended file attributes driver
SRTSP = Symantec Endpoint protection
RsFx0105 = SQL Server File Stream filter driver.

In discussing this with the customer, Anti-virus exclusions were controlled by GPO so he had put in a request to exclude the respective folders, yet the issue still continued.

In order to do my due diligence, the other question was whether we "released" the file handle after we created it, and whether someone else grabbed it? So we (Venu, Bob and I) did take a look at the code and this can be the case. On SQL Server 2008 R2 when we call the **CreateFile** API and we hardcode the ***shareAccess*** parameter to 0 which is exclusive access while we have it open to prevent secondary access.

http://msdn.microsoft.com/en-us/library/windows/desktop/aa363858(v=vs.85).aspx

*If this parameter is zero and **CreateFile** succeeds, the file or device cannot be shared and cannot be opened again until the handle to the file or device is*

closed. For more information, see the Remarks section.

Once the file is created, we release the EX latch and can close the file handle, on the file, but sqlservr.exe continues to hold the lock on the file itself during the restore process. Once the restore operation is completed, we no longer hold an exclusive lock to the file.

We can reopen file handles during the Recovery process so the other thought was perhaps it was a transaction affected by recovery and GC and potentially some race condition but in this case we know that the restore was failing prior to that as it didn't reach 100% so that could be ruled out as well.

Getting a dump at the failure time showed me the same Restore Stack but different dumps showed multiple different files in question so it wasn't a particular Log record sequence per say causing this.

```
sqlservr!ex_raise
sqlservr!HandleOSError

sqlservr!FileHandleCache::OpenFile
sqlservr!FileHandleCache::ProbeForFileHandle
sqlservr!FileHandleCache::GetFileHandle
sqlservr!RestoreCopyContext::RestoreFilesystemData
BackupIoRequest::StartDatabaseScatteredWrite
```

Given now that it was unlikely it was SQL Server, I concentrated more on the Filter driver theory. I tried to capture Process monitor, but given the time it took and amount of files touched, Process monitor was not all that useful. I couldn't filter on a specific folder as it failed on different folders and there were 10 + mount points involved.

However from Process monitor while the restore was going on, I looked at the stack for some I/O operations (not ones that failed by any means) and I still saw fltmgr.sys sitting there for an OpenFile Call on a file in the filestream directory

```
fltmgr.sys + 0x2765                    0xfffffa6001009765  C:\Windows\system32\drivers\fltmgr.sys

fltmgr.sys + 0x424c                    0xfffffa600100b24c  C:\Windows\system32\drivers\fltmgr.sys

fltmgr.sys + 0x1f256                   0xfffffa6001026256  C:\Windows\system32\drivers\fltmgr.sys

ntoskrnl.exe + 0x2c8949                0xfffff80002918949  C:\Windows\system32\ntoskrnl.exe

ntoskrnl.exe + 0x2c0e42                0xfffff80002910e42  C:\Windows\system32\ntoskrnl.exe

ntoskrnl.exe + 0x2c19d5                0xfffff800029119d5  C:\Windows\system32\ntoskrnl.exe

ntoskrnl.exe + 0x2c6fb7                0xfffff80002916fb7  C:\Windows\system32\ntoskrnl.exe


ntoskrnl.exe + 0x2b61a8                0xfffff800029061a8  C:\Windows\system32\ntoskrnl.exe

ntoskrnl.exe + 0x57573                 0xfffff800026a7573  C:\Windows\system32\ntoskrnl.exe

ntdll.dll + 0x471aa                    0x77b371aa          C:\Windows\System32\ntdll.dll   □  ZwOpenFile

kernel32.dll + 0x10d48                 0x779d0d48          C:\Windows\system32\kernel32.dll

kernel32.dll + 0x10a7c                 0x779d0a7c          GetVolumeNameForRoot

_____SQL_____Process_____Available
+ 0x695c7e                             0x1a080fe           GetVolumeDeviceNameAndMountPoint

_____SQL_____Process_____Available
+ 0x6d6898                             0x1a48d18             • ParseContainerPath

_____SQL_____Process_____Available
```

```
+ 0x6d714a                    0x1a495ca          sqlservr!CFsaShareFilter::RsFxControlContainerOwnership
```

Also looking at some other Symantec related issues, I found an article not necessarily to do with any SQL restores but the fact that this was a possibility – again this has to do with a specific issue on a specific build, but am illustrating that Filter drivers can cause some unexpected behaviors.

As far as Anti-virus exclusions go, we actually have guidance in the article below: http://support.microsoft.com/kb/309422

And also in our File stream best practices article: http://msdn.microsoft.com/en-us/library/dd206979(v=SQL.105).aspx

> *When you set up FILESTREAM storage volumes, consider the following guidelines:*
>
> *•Turn off short file names on FILESTREAM computer systems. Short file names take significantly longer to create. To disable short file names, use the Windows fsutil utility.*
>
> *•Regularly defragment FILESTREAM computer systems.*
>
> *•Use 64-KB NTFS clusters. Compressed volumes must be set to 4-KB NTFS clusters.*
>
> *•Disable indexing on FILESTREAM volumes and set disablelastaccess to set disablelastaccess, use the Windows fsutil utility.*
>
> *•**Disable antivirus scanning of FILESTREAM volumes when it is not unnecessary**. If antivirus scanning is necessary, avoid setting policies that will automatically delete offending files.*
>
> *•Set up and tune the RAID level for fault tolerance and the performance that is required by an application.*

Looking at another run of "***fltmc instances***" command output and still saw the Anti-virus components on the list for those mount points. Given we "thought" we had put an exclusion in for the whole drive, and it was showing up, it was time to look at this closer

1. Excluded the drives where the data was being stored – Restore still failed
2. Stopped the AV Services - Restore still failed
3. Uninstalled Anti-virus – Restore now succeeded

Voila once we uninstalled AV on this machine, the restore succeeded. The customer is broaching this this with the AV vendor to figure out more of the root cause.

Denzil Ribeiro – Senior PFE

Comments

2 Apr 2013 12:00 PM

Kenneth Brian Kelley

We've also seen issues with AV network filter drivers. This is true even when the source and destination were on the same server. Recommendation that we ultimately got from Premier Support was to pull the AV install and scan from remote.

Recent Posts

How It Works: Behavior of a 1 Trillion Row Index Build (Gather Streams from SORT)
Posted 7 days ago by psssql

How to grab multiple parent/child elements from XML Data Source
Posted 7 days ago by Adam W. Saxton

SharePoint Adventures : Using Claims with Reporting Services
Posted 8 days ago by Adam W. Saxton

Version 9.04.0013 of the RML Utilities for x86 and x64 has been released to the download center
Posted 12 days ago by psssql

RS, SharePoint and Forefront UAG Series – Intro
Posted 13 days ago by Adam W. Saxton