http://www.dsug.eu/forum/index.php?page=Thread&threadID=235

Foxpro- DBF-Geschwindigkeitsproblem

Das klingt extrem nach dem altbekannten Oplock Caching Phänomen. „Opportunistic Locking“ wird von allen modernen Server-Betriebssystemen gemacht, egal ob Windows, Samba oder Novell. Vereinfacht gesagt: Der Netzwerk- Server behandelt Dateien, die im Multiuser/Shared-Mode geöffnet werden ausnahmsweise als SingleUser-Mode Dateien, solange nur ein Client die Datei offen hat. In diesem Pseudo-Exclusive-Mode wird die Datei im Client zwischengepuffert, und somit hat der erste (bzw ein einzelner) User das Gefühl wie wenn er lokal mit der Datei arbeiten würde. Sobald allerdings ein weiterer User sich auf die Datei aufschaltet, muss das lokale Caching bei Client1 schlagartig beendet werden und alle Änderungen vom Client1 auf den Netzserver zurückgeschrieben werden. Ab dem Zeitpunkt sind dann wieder normale Netzwerk-Geschwindigkeiten, wie sie eben im Shared-Modus üblich sind.

Das Ganze ist vielfach im Internet beschrieben, und wurde auch x-mal im dFPUG Forum etc durchgekaut. Betrifft wie gesagt alle Netzwerkserver und alle file-basierten Datenbanken, also auch Access, Paradox, Filemaker, Superbase, ADS etc. Daher findet man auch auf diversen anderen Herstellerseiten ganze Romane dazu (siehe Links am Ende).

Dieses „Opportunistic Locking“ kann man abschalten, dann ist zwar der Geschwindigkeits-Vorteil beim Einzeluser weg, dafür ist die Fehlerfreiheit der Dateien um den Faktor 100000 besser. OpLocks sind bekannt dafür, dass sie beim Umschalten von Single- auf Multiuser Mode die Indices und teilweise auch die DBFs zermantschen…
Daher wird generell empfohlen, beim Einsatz von DBFs (oder MDBs etc) dieses Verfahren abzuschalten.

Hier die weiterführenden Links:

http://www.eduadmin.com/oplock.htm
http://www.dataaccess.com/whitepapers/op…eadcaching.html
http://www.superbase.com/services_tech_support_oplocks.htm
http://devzone.advantagedatabase.com/dz/…fNo=090707-2191
http://www.samba.org/samba/docs/man/Samb…on/locking.html

http://support.microsoft.com/kb/296264

http://www.sysprobs.com/windows-7-network-slow
http://www.networksteve.com/forum/topic….Id=5025&Posts=4

Hier gibt’s nen Installer, der alle Registry-Keys korrekt setzt:
http://www.alaska-software.com/fixes/smb2/overview.shtm (s.auch weiter unten)

http://www.hexcentral.com/articles/troubleshoot.htm

Trouble-shooting a Visual FoxPro application

If you're having problems with a VFP application, these solutions might just be what you need.

By Dan Macleod

I recently received an anxious phone call from a local office supply firm. The company uses a large Visual FoxPro (VFP) application to control its business. Or rather, it's trying to. Unfortunately, the application is plagued with bugs, poor performance and frequent crashes, almost to the point where it's unusable. Could I help?

My first reaction was to ask if they had contacted the people who wrote the application. Yes, they had spent long hours discussing the issues with the vendor's help desk. At first, the people there were supportive and helpful, but they eventually said that none of the problems were of their making. The fault, they claimed, lay somewhere in the users' environment, and they were unable to give any more help. That's when the company called me.

Naturally, I accepted the assignment. Now, after several days of observation, diagnosis and research, I've solved all the major issues. I offer my findings here in the hope they will be of benefit to others. If you are seeing any of these same problems, I can't guarantee that these solutions will work for you, but they should at least give you something to think about.

Problem #1: Application goes to sleep for a while, then wakes up

Symptoms: The application was frequently freezing for a short period, ranging from about ten seconds to a couple of minutes. This always happened on system startup, and often when opening a form or launching a report. The application would then resume normally.

Diagnosis: This is a classic symptom of an over-zealous anti-virus (AV) program. The program scans the many files that make up the application's Visual FoxPro database whenever any of the files is opened. Because some of the files are very large, and because they are typically opened and closed many times during a session, the scanning time can quickly become unacceptable.

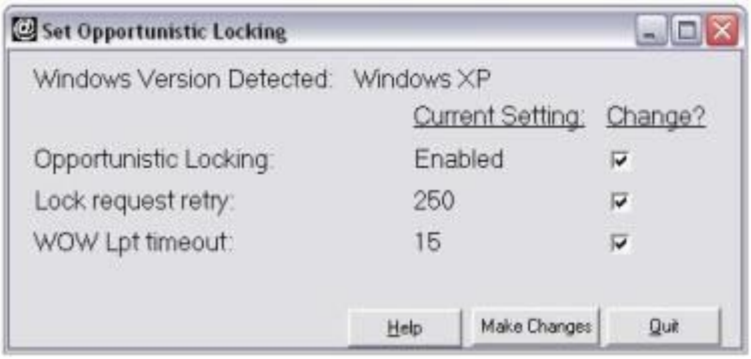
The silly thing is that none of the FoxPro database files need to be scanned, as they can't contain executable code.

Solution: Tell the AV program to refrain from checking the following file types: DBF, CDX, FPT, DBC, DBX and DBT.

Problem #2: "File access is denied" error

Symptoms: The application occasionally crashed with this error, usually on system startup. On monitoring the file usage, I could see that it usually happened part of the way through opening a series of abut 25 files, but not always at the same point. Despite what the wording of the message suggests, none of the files was being opened exclusively.

Diagnosis: This is opportunistic locking rearing its ugly head. In brief, opportunistic locking (also known as oplocks) is a Windows feature designed to improve the performance of client-server systems. When a workstation asks to open a file in shared mode, the file is in fact opened in exclusive mode, which is faster. If another workstation then needs to open the same file, the system is supposed to release the exclusive lock that was given to the first workstation. But with simple file-based databases like Visual FoxPro, this sometimes fails to happen, hence the "access denied" error. (For more information, see this Microsoft Knowledge Base article.)



Windows Version Detected: Windows XP

	Current Setting:	Change?
Opportunistic Locking:	Enabled	☑
Lock request retry:	250	☑
WOW Lpt timeout:	15	☑

Figure 1: Use Addsum OpLockSet to control opportunistic locking.

Solution: Disable opportunistic locking. This needs to be done for all workstations and servers on the network. You can do it by editing certain registry keys (described in the article mentioned above). Or you can purchase the low-cost Addsum OpLockSet Utility which does the job for you through a user-friendly interface (Figure 1).

If you adopt this solution, I strongly recommend that you do it in a carefully controlled trial. And be prepared to reverse the action if necessary. Disabling oplocks could adversely affect the performance of the network as a whole, especially if you are also running a true client-server databases such as SQL Server.

Problem #3: "Class definition xxx.yyy is not found" error

Symptoms: This error frequently occurred at a certain point in the application, but only on a few workstations, and not consistently (xxx.yyy in the above heading is the name of the class definition that was not found).

Diagnosis: In general, a class definition whose name is in this form (two or more elements each separated by a dot) is an external component, such as a DLL, COM server or ActiveX control. The error is triggered by Visual FoxPro's CREATEOBJECT() function when it fails to find the component in question. This can happen either because the component is not physically present, or it is present but not properly registered.

But that didn't explain why the error was only occurring intermittently. You'd think that either the component was all present and correct, or it wasn't.

It turned out that - for a reason I never discovered - the person who installed the application did so by using Remote Desktop to log into the server. So the component was properly installed, but it was registered on the server, not the workstation. What's more, the user sometimes used Remote Desktop to actually run the application (again, I don't know why). On those occasions, it ran normally. It only failed when they launched the application from the workstation.

Solution: Always install a Visual FoxPro application from the workstation. If you want to place the executable directory on a server, that's fine. But navigate to the server from the workstation, not by using Remote Desktop.

Problem #4: Program crashes after producing a PDF

Symptoms: Whenever users output a report to a PDF file, the application would crash, typically with a "File xxx does not exist" message (where xxx stands for a filename). The crash sometimes happened immediately after generating the report, and sometimes when the user next opened a form.

Diagnosis: This is caused by a somewhat strange interaction between Visual FoxPro and the PDF driver. It happens when the following sequence of events occurs: the VFP code starts a report; the user chooses a PDF driver as the destination printer; and the driver prompts the user for a filename and directory for the output file. When that happens, the driver changes the default directory, as seen by VFP, to the one selected by the user - and fails to change it back when it has finished. Later, VFP tries to open a file in what it thinks is the default directory, and naturally can't find it. (This isn't a bug in a particular PDF driver. I've seen exactly the same behavior with several different drivers.)

Solution: This is one for FoxPro developers to fix. Before producing any report, save the path to the current default directory to a variable, and restore it after the report has finished. You need to always do this with all reports, because you never know when the user is going to choose a PDF driver as the destination printer.

Problem #5: Printed output goes to the wrong printer

Symptoms: When a user tried to print a report, the output would always go to the same printer, regardless of which printer the user specified. This happened consistently with certain reports, but never with others.

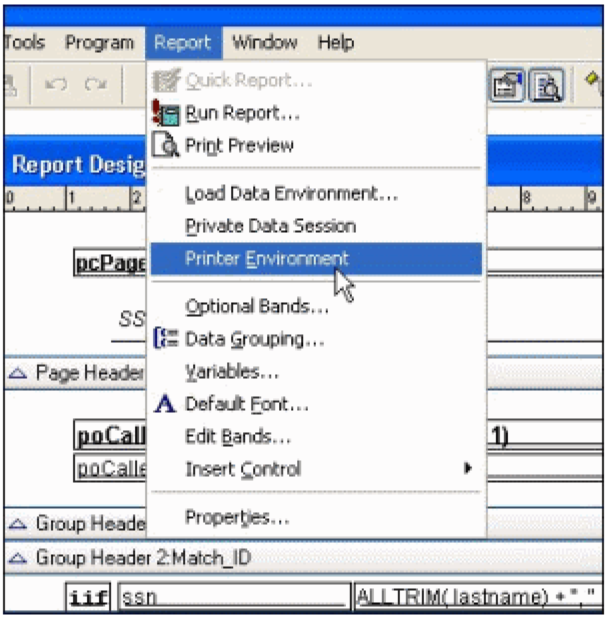


Figure 2: Uncheck this option in the report designer.

Diagnosis: This was an easy one to solve, mainly because it's such a common VFP problem.

The FoxPro report designer has an unfortunate tendency to store the so-called printer environment within the report. The printer environment covers such items as the paper size, orientation, paper source, and - crucially - the destination printer. These parameters then get applied to the report whenever it's printed - regardless of what settings the user makes in the Printer dialog.

Solution: Again, this is one for developers to fix. You need to ensure that the report designer does not store the printer environment with the report, and to remove it from any reports where it's already stored.

For programmers using Visual Foxpro 9.0, that's simply a matter of unchecking the Printer Environment option on the Report menu (Figure 2). You can also change the default setting of this option from the Reports page in the Options dialog. But if you're using an earlier version, you will have to resort to hacking the actual report file (the FRX file). Several articles are available that will tell you how do that; see for example Controlling report settings at run time.

Summing up

I was able to solve these problems, mainly because I had seen them all before - although some are more common than others. If you are running a Visual FoxPro application, you might come across some of these same issues. As I said at the outset, I can't be sure that my solutions will work for you as well. But I hope the information I have given here will at least help you in your own trouble-shooting efforts.

January 2012

https://groups.google.com/forum/?hl=de&fromgroups=#!topic/microsoft.public.de.fox/tKm5kz3ACl0

Geschwindigkeitsprobleme

Generell wird empfohlen, das "Opportunistic Locking" ABzuschalten! Ein eingeschaltetes OppLock führt zwar zur Beschleunigung immer dann wenn nur 1 User die Datei in Verwendung hat, verursacht aber auch gleichzeitig Probleme bei normalem Multiuser-Betrieb. Dies ist KEIN "NurFoxPro"-Problem, es betrifft durchgängig alle dateibasierten Datenbank-Produkte. Daher findest du beim netsprechenden Googlen überall das passende Wehklagen...

Wenn die Netzwerkgeschwindigkeit für "normale User unerträglich" ist, dann ist schlicht ein Netzwerk-Problem da. Man konnte selbst zu Zeiten von Arcnet oder den 10Mbit Ring-Leitungen problemlos im Netzwerk arbeiten, auch mit 100 Usern gleichzeitig.

Ob nun ein Steckdosen-Netzwerk tatsächlich die selbe Übertragungsrate und Antwortverhalten wie ein normales Netzwerk hat, weiss ich nicht. Aber, wie schon gesagt: Selbst mit simplen Tests kannst du ausprobieren, ob zumindest die Datenrate mithalten kann.

--

Jürgen Wondzinski

Microsoft Visual FoxPro Technologieberater
Microsoft Most Valuable Professional seit 1996
"*´¨)
¸.•´¸.•*´¨) ¸.•*¨)
(¸.•´. (¸.•` *
.•`.Visual FoxPro: It's magic !
(¸.•``••*

Nein, es wird immer wieder nur empfohlen diese Form von Vorgaukelung exklusiven Zugriffs nicht zu nutzen, weil nur ein einzeln auf einer Tabelle arbeitender User davon profitiert, sobald ein zweiter dieselbe Tabelle nutzt gibt es dabei sogar den Overhead, daß erstmal die Änderungen des 1. Benutzers wirklich zurück zum Server müssen, bevor der 2. auch nur überhaupt lesen kann, sonst würde der ja etwas veraltetes vom Server kriegen.

Es ist besser das von vornherein gar nicht zu aktivieren.

Tschüß, Olaf.

Microsoft Knowledge Base Article

http://kbalertz.com/296264/Configuring-Opportunistic-Locking-Windows.aspx

Configuring opportunistic locking in Windows

Article ID: 296264 - View products that this article applies to.

This article was previously published under Q296264

Expand all | Collapse all

SUMMARY

By default, opportunistic locking is enabled for server message block (SMB) clients that run one of the Windows operating systems that is listed in the "Applies to" section. Opportunistic locking lets clients lock files and locally cache information without the risk of another user changing the file. This increases performance for many file operations but may decrease performance in other operations because the server that grants the opportunistic lock must manage the breaking of that lock when another user requests access to the file.

Notes for Windows Vista

- The opportunistic locking registry keys are valid only for traditional SMB (SMB1). You cannot turn off opportunistic locking for SMB2. SMB2 was introduced in Windows Vista to enable faster communication between computer that are running Windows Vista and Windows Server 2008 or Windows Server 2008 R2.
- If you disable opportunistic locking, the offline files feature in Windows Vista fails.

MORE INFORMATION

Important This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756

(http://kbalertz.com/Feedback.aspx?kbNumber=322756/)

How to back up and restore the registry in Windows

The location of the client registry entry for opportunistic locking has changed from the location in Microsoft Windows NT. In later versions of Windows, you can disable opportunistic locking by setting the following registry entry to 1:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters\

OplocksDisabled REG_DWORD 0 or 1
Default: 0 (not disabled)

Note The OplocksDisabled entry configures Windows clients to request or not to request opportunistic locks on a remote file.

You can also deny the granting of opportunistic locks by setting the following registry entry to 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

EnableOplocks REG_DWORD 0 or 1
Default: 1 (enabled)

Note The EnableOplocks entry configures Windows-based servers to allow or to deny opportunistic locks on local files. These servers include workstations that share files.

In addition, you can use the following values to tune opportunistic locking for Windows-based computers that have granted opportunistic locks.

The following value specifies the minimum link throughput that the server allows before it disables raw and opportunistic locks for this connection:

MinLinkThroughput REG_DWORD 0 to infinite bytes per second
Default: 0

The following value specifies the maximum time that is allowed for a link delay. If delays exceed this number, the server disables raw I/O and opportunistic locking for this connection.

MaxLinkDelay REG_DWORD 0 to 100,000 seconds
Default: 60

The following value specifies the time that the server waits for a client to respond to an oplock break request. Smaller values allow detection of crashed clients more quickly, but might potentially cause loss of cached data.

OplockBreakWait REG_DWORD 10 to 180 seconds
Default: 35

Note You must restart the computer for these registry changes to take effect.

PROPERTIES

Article ID: 296264 - Last Review: April 4, 2011 - Revision: 11.0

APPLIES TO

- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows XP Professional

- Microsoft Windows XP Tablet PC Edition
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional Edition
- Microsoft Windows Small Business Server 2003 Premium Edition
- Microsoft Windows Small Business Server 2003 Standard Edition
- Windows Server 2008 Datacenter without Hyper-V
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 for Itanium-Based Systems
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Web Server 2008
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Standard
- Windows Web Server 2008 R2
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Enterprise
- Windows 7 Professional
- Windows 7 Ultimate

http://www.dataaccess.com/whitepapers/opportunlockingreadcaching.html

Opportunistic Locking and Read Caching on Microsoft Windows Networks

A Data Access Worldwide White Paper

by Dennis Piccioni

May 14, 2002
Last Edited: September 6, 2011

Summary

Improperly configured Windows networks can lead to data corruption in any **file system database**, including the **embedded (DataFlex) database**. Two Windows networking behaviors, **opportunistic locking** (on Windows servers) and **read caching** (on Windows clients) are sources for corruption potential. This paper is provided for Data Access Worldwide (DAW) customers to discuss these behaviors, their effects and what can be done to minimize the chances of data corruption on Windows networks when running Visual DataFlex (VDF) and/or DataFlex applications, and to centralize this information in one convenient place.

The information in this paper is compiled from the latest available information regarding these issues from Microsoft, our own in-house testing and customer reports. We are attempting to combine the limited information provided my Microsoft on these topics in one place. Please revisit this white paper from time to time to check for updated information. The Last Edited date at the top of the paper will reflect when the latest edits were made.

The information in this white paper only deals with operating systems that we currently support. You can view information about supported products & environments in the Data Access Worldwide Supported Products List.

Contents

What is Opportunistic Locking?

Opportunistic locking (oplocks) is a Windows-specific mechanism for client/server databases to allow multiple processes to lock the same file while allowing for local (client) data caching to improve performance over Windows networks. Unfortunately, the default setting of the oplocks mechanism that enhances the performance of one type of database (client/server) also introduces data integrity issues for other database types (file system/ISAM).

Microsoft's documentation states "An *opportunistic lock* (also called an oplock) is a lock placed by a client on a file residing on a server. In most cases, a client requests an oplock so it can cache data locally, thus reducing network traffic and improving apparent response time. Oplocks are used by network redirectors on clients with remote servers, as well as by client applications on local servers" and "Oplocks are requests from the client to the server. From the point of view of the client, they are opportunistic. In other words, the server grants such locks whenever other factors make the locks possible.".

You can read more about oplocks in Microsoft's documentation. Please see the Resources section for more information.

What is Read Caching?

Read caching, sometimes referred to as read-ahead caching, is a feature of oplocks. It is a technique used to speed network access to data files. It involves caching data on clients rather than on servers when possible.

The effect of local caching is that it allows multiple write operations on the same region of a file to be combined into one write operation across the network. Local caching reduces network traffic because the data is written once. Such caching improves the apparent response time of applications because the applications do not wait for the data to be sent across the network to the server.

Problems with read caching usually occur if something unforeseen happens, such as a workstation crash, where data is not properly flushed from the workstation, which can lead to data corruption.

Microsoft's documentation states that 'Under extreme conditions, some multiuser database applications that use a common data store over a network connection on a file server may experience transactional integrity issues or corruption of the database files and/or indexes stored on the server. This typically applies to some so-called "ISAM style", or "record oriented" multiuser database applications, not to a client/server relational system like SQL Server' and 'A hazard of local caching is that written data only has as much integrity as the client itself for as long as the data is cached on the client. In general, locally cached data should be flushed to the server as soon as possible.'

You can read more about read caching in Microsoft's documentation.

What Is SMB2?

SMB2 is the second generation of server message block (SMB) communication on Windows networks. SMB2 was introduced in Windows Vista and Windows Server 2008 to enable faster communication between computers that are running Windows Vista and Windows Server 2008. Previous Windows versions used SMB1, also called "traditional" SMB. SMB1 is still supported in current Windows versions (Vista, Server 2008, 7) for backward compatibility.

Data Access Worldwide Recommendations

The embedded (DataFlex) database is an ISAM database and thus susceptible to the effects of the default Windows oplocks settings. **Using the embedded database on Windows networks without disabling oplocks is not recommended or supported** and has a high likelihood of data corruption.

The best data integrity, security and performance is available by using a client/server database, such as IBM DB2, Microsoft SQL Server or Pervasive.SQL with your Visual DataFlex and DataFlex applications. Data Access Worldwide has direct drivers (Connectivity Kits) available for IBM DB2, Microsoft SQL Server and Pervasive.SQL, as well as an ODBC Connectivity Kit for access to any ODBC-compliant databases. All of these drivers are loaded at runtime and require no coding changes to be used with existing VDF, DataFlex or WebApp Server applications.

Reliable database operation on Windows Networks can be achieved using the embedded database, provided that the network is properly configured. You can use the information in this paper to set up your Windows network's oplocks parameters. One downside to using this method are maintenance issues: you must continually ensure that each and every server and client using an application accessing the embedded database has oplocks disabled and are always maintained in that state.

One method to ensure that oplocks are disabled on client PCs is to add code to applications that checks those settings on application startup. The folks at VDF-Guidance.com have created an open source project named RegCheck for this purpose.

Disabling oplocks may have a performance impact on Windows networks.

Oplocks do not apply to client-server databases. DAW makes no specific recommendation on oplocks if you use a client server database and no embedded database tables.

This paper will tell you how to disable oplocks, but due to the reasons stated above, **Data Access Worldwide recommends using a client-server database for multi-user DataFlex applications on Windows networks.**

What Operating Systems are Affected?

All computers running Windows operating systems that host or access embedded database tables accessed by other Windows PCs need to have oplocks disabled in order to minimize the chances of database corruption.

Oplocks can be disabled on either (or both) of these:

- the client side (a Windows PC that accesses an embedded database table hosted on another PC)
- the server side (a Windows PC that hosts an embedded database table accessed from another PC)

The Windows operating system list that we currently support for our products includes Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003 and Windows Server 2008.

What Environments Are Not Affected?

There are some environments and scenarios that we support that may not be affected by oplocks, even if using the embedded database:

- **Local database access**

In general, whenever an embedded database table is accessed on the same PC where that table is located, oplocks do not apply.

- **Windows Terminal Services and Citrix**

Under normal use for these environments, users log onto a Windows server and run applications locally on that server. If, however, an embedded database is located on another server than the one running WTS/Citrix, oplocks between the WTS/Citrix server and the database server must be disabled.

- **Web Application Server Applications/Web Services**

In web applications users access a web browser which requests data from a web application and/or data is requested via a web service. In both cases, the web application on a web server accesses the database, the client does not. If the data is located on the same server, oplocks do not come into play. If, however, an embedded database is located on another server than the one running the web application, oplocks between the web server and the database server must be disabled.

Making Windows Registry Changes

The topics below discuss changing editing the Windows Registry.

Caution: The following warning appears in every Microsoft article that discusses editing the Windows Registry:

WARNING : You can edit the registry by using Registry Editor (Regedit.exe or Regedt32.exe). If you use Registry Editor incorrectly, you can cause serious problems that may require you to reinstall your operating system. Microsoft does not guarantee that problems that you cause by using Registry Editor incorrectly can be resolved. Use Registry Editor at your own risk.

If you change any of the Registry values discussed below, you will have to reboot the PC on which the value was changed to ensure that the new setting goes into effect.

The Registry changes are listed in the format MainRegistryKey\SubKey\SubKey RegistryValue = RequiredValue

where:

- MainRegistryKey is one of the main Windows Registry keys (e.g. HKey_Local_Machine)
- SubKey is any subkey of a main Registry key
- RegistryValue is a Registry value to change or add in the specified Registry key
- RequiredValue is the value RegistryValue must be set to cause the effect described

If any subkeys or values described do not exist in your Registry, you will have to add them. Please check carefully before doing so.

Disabling Oplocks on Windows Client PCs

To disable oplocks on a Windows client PC (a Windows PC that accesses an embedded database table hosted on another PC), change or add the following Registry values:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters **OplocksDisabled = 1**

Disabling Oplocks on Windows Servers

To disable oplocks on a Windows server (a Windows PC that hosts an embedded database table accessed from another PC), change or add the following Registry values:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters **EnableOplocks = 0**

Disabling Oplocks on SMB2

Oplocks **cannot** be turned off for SMB2. You can apparently disable SMB2 itself, but how to do so is not documented by Microsoft and was only mentioned in a Microsoft support forum post as a workaround for a bug.

According to that post, SMB2 can be disabled on Windows operating systems that support it (Vista, Server 2008).

To disable SMB2 on a Windows Server 2008 or Windows Vista PC hosting embedded database tables, change or add the following Registry value:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters **SMB2 = 0**

Once SMB2 is disabled, SMB1 will be used again and the methods described above applied to disable oplocks for SMB1.

Do Coding Practices Affect These Issues?

- If your application code uses DataDictionaries and/or Data_Sets, there should be no data integrity problems after oplocks have been disabled.

  Customers have reported that with application code that does not use Data Dictionaries and/or Data Sets (for example, in a Find loop using the record buffer for finding), data in records that is new or edited since the data was first accessed will still not be retrieved properly, even with oplocks disabled. Workarounds for this condition are to do the Find in a locked state or issuing a Reread command after each record is found (remember to issue an unlock command after the reread as a reread performs a lock as part of its functionality). We will publish any additional information we obtain about how to get around this Microsoft operating system problem when it becomes available.

- We have tried using the Win32 FlushFileBuffers Windows API function that Microsoft recommends in their documentation in the Visual DataFlex/DataFlex runtime when the DF_HIGH_DATA_INTEGRITY attribute was turned on. However, application performance degraded to the point that it was virtually unusable when doing so, because this Windows API function is a very generic call that flushes all buffers on a client PC instead of just those used by one application.

Persistent Data Corruption

If you have applied all of the settings discussed in this paper but data corruption problems and other symptoms persist, here is some additional information:

- We have credible reports from developers that faulty network hardware, such as a single faulty network card, can cause symptoms similar to data corruption.
- If you see persistent data corruption even after repeated reindexing, you may have to rebuild the tables in question. This involves creating a new table with the same definition as the table to be rebuilt and transferring the data from the old table to the new one. There are several known methods for doing this that can be found in our Knowledge Base.

Terms

- **ISAM**
  Indexed Sequential Access Method is a file management system developed at IBM

that allows records to be accessed either sequentially (in the order they were entered) or randomly (with an index).

- **SMB**
  The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol. If you wish to learn more about SMB, consult Microsoft's documentation.

You may want to check for an updated version of this white paper from time to time. Many of our white papers are updated as information changes. For those papers, the **Last Edited** date is always at the top of the paper.

Resources

- **Opportunistic Locks**, Microsoft Developer Network (MSDN)

- Microsoft Knowledge Base Article Q296264 Configuring Opportunistic Locking in Windows

- Microsoft Knowledge Base Article Q224992 Maintaining Transactional Integrity with OPLOCKS

- Microsoft Knowledge Base Article Q129202 PC Ext: Explanation of Opportunistic Locking on Windows NT

- Microsoft Knowledge Base Article Windows registry information for advanced users.

- **RegCheck**
  One of the best ways to ensure that oplocks are disabled on client PCs is to add code to applications that checks those settings on startup. The folks at VDF-Guidance.com have created an open source project named RegCheckfor this purpose. Note that the code in this project is not verified or maintained by DAW.

- **Data Access Worldwide Support**
  Visit the DAW Support Home page for information about all of our support offerings, including the list of supported products, bug report forms and free support offerings, such as the Knowledge Base, White Papers and Peer Support Forums.

- **DAW Knowledge Base**
  Visit the Data Access Worldwide Knowledge Base, a great resource for the latest technical information about all Data Access Worldwide products.

- **Data Access Worldwide Forums**
  Visit the DAW Forums for sharing information about Data Access Worldwide products with other developers and users.

http://www.caseware.com/support/caseknowledge/kb-271

Potential file corruption when using WindowsVista/Windows7 or Windows Server 2008/Windows Server 2008R2 with SMB2

October 20, 2011

This article has been updated to reflect Microsoft's release of the new KB2618096 hotfix for SMB2.

Microsoft has acknowledged that the Server Message Block version 2 (SMB2) protocol may cause stability problems with applications such as CaseWare® Working Papers that require real-time file information on files accessed over a network. Error messages in Working Papers such as 'Error -310: Not a correct index file' and 'Inconsistent Database Indices Detected' may be due to data corruption caused by SMB2.

Any laptops, workstations, Terminal servers, or Citrix servers running CaseWare Working Papers accessing client files over a network with the following operating systems can be affected by this issue:

- Windows 7
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2

Different solutions are available from Microsoft depending on the version of Windows that you are running. One set of fixes should be applied to Windows Vista and Server 2008 while another set are applicable to Windows 7 and Server 2008 R2. The table at the end of this article specifies the fixes to apply for the version of Windows that you are running.

On all computers running Working Papers on Windows 7 or Server 2008 R2:

1. **Install Microsoft KB2028965 SMB2 hotfix**

   Microsoft has included the hotfix in their recent updates. Check the table below to determine if you need to install the hotfix. For instructions on installing, see http://support.microsoft.com/kb/2028965

   AND

2. **Install Microsoft KB2618096 SMB2 hotfix**

   Microsoft has provided a new hotfix for SMB2 issues. Check the table below to determine if you need to install the hotfix. For instructions on installing, see http://support.microsoft.com/kb/2618096

On all computers running Working Papers on Windows Vista or Server 2008:

The following 2 steps will eliminate the possibility of file corruption resulting from this issue.

1. **Configure the following registry key**

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
- Create a DWORD value named **DirectoryCacheLifetime** and give it a binary or hexidecimal value of **0**.

For more information on configuring this registry key, see http://support.microsoft.com/kb/2461645

Note: The instructions in this article involve making changes to the Windows Registry. It is highly recommended that these changes be made by someone who is very comfortable using REGEDIT.

AND

2. **Install Microsoft KB2028965 SMB2 hotfix**

Microsoft has included the hotfix in their recent updates. Check the table below to determine if you need to install the hotfix. For instructions on installing, see http://support.microsoft.com/kb/2028965

It is possible to automate both these steps. Contact your IT department if you need assistance.

If you require assistance implementing the recommendations above, please contact our support department atsupport@caseware.com.

Actions required by operating system

Operating Systems	**Registry Keys**	**KB2028965 Hotfix**	**KB2618096 Hotfix**
Windows 7	N/A	install	install
Windows 7 SP1	N/A	included	install
Windows Vista SP1	modify	install	N/A
Windows Vista SP2	modify	install	N/A
Windows Server 2008	modify	install	N/A
Windows Server 2008 SP2	modify	install	N/A
Windows Server 2008 R2	N/A	install	install
Windows Server 2008 R2 SP1	N/A	included	install
Small Business Server 2008	modify	install	N/A
Small Business Server 2011	N/A	install	install
Small Business Server 2011 SP1	N/A	included	install

Note: The KB2618096 hotfix must be downloaded on the machine it is being installed on. This is due to the fact that Microsoft only presents applicable hotfixes based on the architecture that you are running (e.g. x86 vs x64). Alternatively, you can click the "Show hotfixes for all platforms and languages" link, and then download the appropriate hotfix.

SMB2 Workstation Cache Configuration

http://www.alaska-software.com/fixes/smb2/overview.shtm#download

Description

To avoid data loss or data corruption when using Windows Vista or Windows 7 clients in a network where data is stored on a Windows Server 2008 or higher, the SMB2 file meta data cache needs to be reconfigured. The proper configuration is automatically applied by the MSI package **available here.**

Details

With the advent of Windows Vista and Windows 7, Microsoft introduced a new network protocol (SMB2) to optimize file sharing for WAN and low bandwidth and high latency scenarios. To optimize these types of file access scenarios, Microsoft performed design decisions which lead to the inability of the new SMB2 protocol to handle cache coherency of file meta information such as the file size, the last update time and whether the file actually exists on the server ("file not found" status).

As a result of this design decision made by Microsoft, the SMB2 protocol with its default configuration breaks any application relying on shared, concurrent data access. It is therefore absolutely required to reconfigure the SMB2 cache of the local workstation to not cache file meta information.

Alaska Software provides to its customers and their end-users an MSI installation package which reconfigures the SMB2 cache accordingly. This MSI package needs to be executed on any Vista and Windows 7 workstation in a network to ensure that no data loss or data corruption occurs when accessing files concurrently.

- Applicable to Vista and higher
- Installation is denied on other machines
- Package does not work on Win95/Win98/WinMe

This package creates and modifies values under following registry key:

- HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\LanmanWorkstation\Parameters

The following registry values are created and set to zero:

- FileInfoCacheLifetime
- FileNotFoundCacheLifetime
- DirectoryCacheLifetime

Download/Run

To execute: **Click here** and push the "Run" button.
To download: Press **right mouse button and choose: "Save target as"** to store the MSI package on your local harddisk. It may be executed later on on the same or another computer by double-clicking the MSI file in Windows Explorer.

Deinstallation

To deinstall the package, go to Control Panel -> Programs -> Uninstall Program. Choose Uninstall for the "Alaska Software SMB2 cache configuration" entry. The deinstallation process will remove the added entries from the registry. Therefore, the original default settings of 10 respectively 5 seconds cache lifetime are used by the workstation thereafter.