Resolving network file speed & lockup problems

Network / file problems can take many forms but most often it's a network configuration problem issue. The biggest potential problem area is Opportunistic Locking (oplocks)

Opportunistic locking (oplocks) and performance

Improperly configured Windows networks can lead to data corruption in any file system database, including the database file system that ENERCALC uses. Two Windows networking behaviors, opportunistic locking (on Windows servers) and read caching (on Windows clients) are sources for speed and corruption issues. Here we discuss these behaviors, their effects and what can be done to minimize the chances of data corruption on Windows networks when running ENERCALC.

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. It is supposed to provide performance benefits when sharing small document files. 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) which ENERCLAC uses.

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" 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) for backward compatibility.

Recommendations

The ENERCALC project file 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.

Disabling oplocks may have a performance impact 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)

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 a project file 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, your project file is located on another server than the one running WTS/Citrix, oplocks between the WTS/Citrix 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 (dword) 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 (dword) 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 (dword) 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.

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 files in question. Send them to ENERCALC for this process.

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.

Other sources of Network problems

Drivers up to date? Windows networking is subject to a number of problems, MANY of which can be solved simply by installing updated driver software from the manufacturer or (more often) Microsoft. The link below will go to a web page that describes just ONE of the problems in Windows peer-to-peer networking, yet there are several other problems referenced at the bottom of that page. In particular, anyone on Windows 95 needs to get their network drivers and "requestor" updated.

http://support.microsoft.com/support/kb/articles/q174/3/71.asp
and
http://support.microsoft.com/support/kb/articles/q148/3/67.asp
in particular note some problems that can burn you.

Windows NT users - Are you on service pack 6 instead of service pack 6a or another service pack? If so, expect lots of problems. Microsoft has acknowledged that service pack 6 broke a lot of things network-wise. You can get service pack 6a at their site or you can go back to service pack 5, either of which is stable. In addition, do NOT mix service packs on different NT machines on your network. In other words, run all your NT machines on service pack 5 or on service pack 6a, but not a mix of both service packs.

Test your network using TestLock
Download this program : http://www.rescuemarketing.com/testlock.zip

Follow the instructions. Note: We didn’t write it and can’t support it. I just follow the directions and use it.

Is your network slow when using a mapped drive letter?
The reason is this: The computer has both TCP/IP and NetBEUI (network protocols, similar to different spoken languages). TCP/IP for the Internet and NetBEUI for the local network. TCP/IP is the default protocol. When connecting to a mapped drive after some idle time, the computer tries to connect first over TCP/IP and times out. Then and only then it tries the NetBEUI connection. Go to the Control Panel > Networks > Bindings. Make NetBEUI as the default protocol.

Is your network slow when using a mapped drive letter? (part 2)
Is the drive mapped to the main computer's drive or to a folder?
If it is mapped to a folder, you will likely see a decrease in performance, often a quite noticeable decrease. We are not sure why this happens, but mapping directly to the drive has been proven time and time again to be faster. We have not discovered the reason for this, despite extended searches of Microsoft's tech database (http://msdn.microsoft.com).

Is your network slow?
Recently, we have noticed that the "Windows Indexing Service" has a seriously negative effect on network performance. Turn it off. The indexing service scans your hard disk and indexes the files so that the next time you do a file search, Windows can find the files more quickly. Turn it off. Think about how often you do searches vs. how much time you waste waiting on your

network. Do a search and do other work while waiting for it. It’s just not worth waiting 99% of the time to speed up 1% of your work.

Do some or all computers on your network randomly "die", "go to sleep" or "hang"?
Usually, this is caused by power management being active on the workstation and possibly the server. Power management is a fancy computer geek word for "*Windows has settings that turns stuff off when it hasn't been used in a while*". Power management is a bad thing on a network. It's great on a laptop at 37,000 feet with 3 hours remaining of your flight, but it's far more trouble than it is worth otherwise. Bottom line issue: You don’t want network cards turning off because you haven't moved your mouse for 20 minutes. You don’t want your server's hard drive turning off because no one has touched the server keyboard in the last 30 minutes (this might make your workstations just a little bit cranky when they are trying to read stuff on that server's drive). This is exactly what Power Management is supposed to do, but you don't want this to happen when using a networked database. To investigate, go to Start, settings, control panel (XP in "ugly mode" or Windows 2000) or Start, Control Panel (XP in "pretty mode") and double click the Network Connections icon (if that doesn’t exist on your computer, you need to find the place where you can change settings on your network cards). Find your network adapter on this screen. Usually it will say something like "Local Area Connection" or "Wireless Connection 1" (if you are ignoring our advice and using wireless). Right click that icon, click properties. When the screen opens, you'll see the name of the network card up near the top, just below the tabs. To the right of that, there is a Configure button. Click it. When the next screen opens, there will almost certainly be a Power Management tab. On that tab, chances are you will see a checkbox that says something like "Allow the computer to turn off this device to save power". Uncheck the box and click OK until you don’t have to look at all these network settings anymore. Reboot your PC, hope for the best.

Windows 98 networking
Here is Microsoft's "best place to start" page for dealing with Windows98 issues, including networking issues. http://support.microsoft.com/highlights/w98.asp

Windows 2000 networking
Here is Microsoft's "best place to start" page for dealing with Windows 2000 issues, including networking issues.
http://support.microsoft.com/highlights/Win2000.asp

Windows XP networking
Here is Microsoft's "best place to start" page for dealing with Windows XP issues, including networking issues.
http://support.microsoft.com/highlights/winxp.asp

Windows 2003 Server networking
http://support.microsoft.com/default.aspx?scid=fh;EN-US;winsvr2003

Workstation drive letters "getting the red X" (disconnecting from the main computer)
You can disable this by issuing this command from the DOS command line: net config server /autodisconnect:-1
Before using this command, we suggest you read the Microsoft article that discusses

autodisconnect. You can find it here: http://support.microsoft.com/default.aspx?scid=kb;en-us;138365

Windows 2000 or Windows XP mapped drives disconnecting for no apparent reason?
(showing the red X over the drive in explorer)
http://support.microsoft.com/default.aspx?scid=kb;en-us;138365

Novell Netware problems?
The problem could be your Novell Opportunistic Locking setting. Contact your network person for further details. How to turn it off? Goto Control Panel -> Networks -> Novell Client Properties -> Advanced Settings Tab -> Opportunistic Locking and make sure this is switched off on all client Machines - ALSO Make sure True Commit is ON at each client PC (This should help stop data corruption)

Performance issues are often caused by network protocol "bindings"
Check the following Network protocols basics:

- Make sure that your default network protocol has no bindings to a virtual device (dialup.....).
- If you are using TCP/IP and you have dialup on this workstation, try NetBEUI.
- Try to avoid using IPX and NetBEUI together. IPX gets confused when you have a "chatty" NetBEUI. Removing IPX (if you can) is strongly advised.
- If you need to examine the network further, check out http://www.sysinternals.com/Utilities/TdiMon.html to get a bird's eye view of what's going on.

Does the system work on some machines but seems to "think about it" and then do nothing on others?
Sometimes your Windows doesn't have enough "files" set in your config.sys. Try 100 or 125. If this isn't descriptive enough, you need to have your consultant do this for you. Sometimes having full-time virus scanning turned on does this. Ask your virus software vendor how to work around this OR exclude our program from your scanner if you can. Power management - Do you have Energy Star features on your computers? Probably so. Power management and networking DO NOT MIX. You can have your computers' power management features turn off and/or dim the monitor, but DO NOT have them turn off the hard drive, network cards etc. This will definitely cause you grief when computers are networked. Grief = lost data

Database corruptions, timeouts and other troubles
Another issue is the various ways that Windows9x and NT try to improve performance, often at the price of stability. Sometimes these things work, other times they cause network timeouts because they force additional file operations behind the scenes and those file operations time out (fail). One way to turn one of these items off is to turn off "Synchronous buffer commits". To do this, click Control Panel, System, Performance, File System, Troubleshooting and check the "Disable synchronous buffer commits" checkbox.

Database corruptions, timeouts and other troubles, part II
Further, Windows NT users face issues caused by some performance improvements that NT tries to implement with network applications by 'faking' multiple use of files. Unfortunately, some users experience file corruption because of this. This article is a bit of nerd-speak, but your

network person should take a look at it if you are seeing "Access denied" errors on network files when they *know* that the network permissions are set properly. http://support.microsoft.com/support/kb/articles/Q129/2/02.asp The topic of this article can also be the cause of database corruption and network timeouts (drive not available messages and the like).

Windows 2000 and Windows XP users - Turn off write caching

You need to disable the "write-behind cache". When the program asks to save the data, the data is kept in cache on the local machine [until the cache is flushed] instead of being on the server.
Right Click MY Computer > Properties > Hardware > Device Manager
Right Click Disk Drive > Properties
Disable: Write Cache Enabled
Restart the computer