WFP is my new best friend

Larry Osterman [MSFT] 7 Feb 2006 12:34 PM **31**

I've mentioned our computer setup a couple of times before - Valorie's got her laptop, Daniel, Sharron and I each have our own desktop computers, and there are a couple of other machines floating around the house. Since the kids machines don't have internet access, we've got a dedicated machine sitting in our kitchen whose sole purpose is to let the kids get their email and surf the net. The theory is that if they're surfing in the kitchen, it's unlikely they'll go to bad places on the net.

It also means we can easily allow them to run as non admins when they surf but be admins on their machines (which is necessary for some of the games they play).

Ok, enough background. Yesterday night, I was surfing the web from the kitchen machine, and I noticed that the menu bar on IE had disappeared. Not only that, but I couldn't right click on any of the toolbars to enable or disable them. All the IE settings looked reasonable, IE wasn't running in full screen mode, it was just wierd.

Other than this one small behavior (no menus in either IE or other HTML applications (like the user manager and other control panel applets), the machine was working perfectly. The behavior for HTAs was wierd - there was a windows logo in the middle of the window where the menu bar should be, but that was it.

I ran an anti-spyware and virus scan and found nothing. I went to the KB to see if I could find any reason for this happening, but found nothing.

I even tried starting a chat session with PSS but it never succeeded in connecting.

I must have spent about 2 hours trying to figure out what was wrong.

The first inkling of what was actually wrong was when Daniel asked me to get up so he could read his email - he got this weird message about "Outlook Express could not be started because MSOE.DLL could not be initialized". That was somewhat helpful, and I went to the KB to look it up. The KB had lots of examples of this for Win98, but not for XP SP2. So still no luck.

And then I had my **Aha!**. I ran chkdsk /f to force a full chkdsk on the drive and rebooted.

Within a second or so on the reboot, chkdsk started finding corruptions in the hard disk. One of the files that was corrupted was one of the OE DLL's, another was something related to browsing, and there were a couple of other corrupted files.

I rebooted after running chkdsk, and now I got a message that msimn.exe was invalid or corrupt. I looked at the file, and yup, MSIMN.EXE had a 0 length. Obviously it was one of the files corrupted on the disk.

So now I had a system that almost was working, but not quite.

During my trolls through the KB, I'd run into the **SFC** command. The SFC (System File Checker) is a utility in XP and Win 2K3 that will verify that all files protected by WFP (Windows File Protection) are valid. If it finds invalid files, it restores them from the cache directory. As per the KB article, I ran SFC /SCANNOW and waited for a while. Darned if it didn't find all the files that had been corrupted and repaired them.

So Daniel got his email back, IE got its menus back, and the machine seems to be back on its feet again!

Man, I love it when stuff works the way it's supposed to.

Btw, my guess is that the data corruptions have either been there for a while and we didn't notice them, or they were introduced during a rapid series of power failures we had on Saturday and Sunday (this machine isn't currently on a UPS so...).

Comments

Dave
7 Feb 2006 1:06 PM

>> Man, I love it when stuff works the way it's supposed to.

Sure the ending was happy but the plot was too complicated. Most non-technical users would not have known to do what you did. You fessed up to two hours of troubleshooting, how much did you spend in total? In all the time you've had every television you've ever owned, have you spent anything close to that much time troubleshooting *them*?

Having just eaten some nasty dogfood, this is one of those Golden Opportunities for you to think about how to simplify things for users. Do it before the taste leaves your mouth. Does it make sense for CHKDSK to fix the drive and leave a zero-length executable file, especially one that's part of the operating system? Why didn't it offer to get a replacement for you, say from the Windows CD or the Internet?

Larry Osterman [MSFT]
7 Feb 2006 1:10 PM

Once I ran chkdsk, it was about 30 more minutes, none of which were in front of the computer (SRP took that long to run).

You're right, most people wouldn't know what to do. Heck, I got lucky, and I know it.

CHKDSK can't do any more than it does, in all honesty - it found the corrupted files and put them in a reasonable place.

It has no way of knowing that the files in question were part of the OS, it just knows they were corrupted files.

Scheduling a WRP scan after chkdsk found errors might be a good idea, but in all honesty, the challenge here was realizing that the problem was a corrupted hard disk, NOT how to recover once the hard disk was repaired.

Rob
7 Feb 2006 1:52 PM

Just out of interest, what filesystem are you running on this machine?

Larry Osterman [MSFT]
7 Feb 2006 2:08 PM

Rob, NTFS, because chkdsk verified the SDs on the files.

That's why I indicated the corruption might have been pre-existing, because I've NEVER seen NTFS corruption before. It's theoretically possible but because the FS metadata is journaled it's highly unlikely.

Jerry Pisk
7 Feb 2006 2:21 PM

Isn't NTFS transactional so it should stay consistent even through power failures?

Herb
7 Feb 2006 2:26 PM
FWIW, the sfc utility is available in W2K versions as well.

jon
7 Feb 2006 2:58 PM
Shouldn't System File Protection (or whatever it's called) have picked up automatically that those DLLs were corrupt and replaced them?

PatriotB
7 Feb 2006 2:58 PM
I've encountered the "menu bar disappears, windows flag spans the entire window width" a couple times with Windows Explorer. For me, the issue went away on its own somehow.

Jonathan
7 Feb 2006 3:26 PM
>> Man, I love it when stuff works the way it's supposed to.

I don't think files corrupting themselves are the way stuff is supposed to work. How do you know that all non-WFP-covered files are intact? If I were you, I'd check all my documents/etc are in working order, maybe compare to a recent backup or something.

C++ guy
7 Feb 2006 5:36 PM
Holy smokes. If it took you 2+ hours to figure out what was wrong and how to fix it, what chance do average joe users have?

Please lean on the good folks in the Windows group and suggest that such common failure case should be easier to detect and remedy.

Mike Dimmick
7 Feb 2006 5:51 PM
I'd ditch the disk. That's my first reaction to disk corruption: that the disk hasn't correctly recorded what the OS told it to. That often indicates that the disk is on its way out.

IDE disks tend to play fast and loose with the caching specs, caching writes that the OS told it not to.

Dean Harding
7 Feb 2006 6:14 PM
Jerry: It's journelled, not transactional. But yes, it should survive a power failure.

My guess would be that those sectors of the disk had been corrupted for a while, but just weren't being used. Perhaps Larry has the "Optimize my hard drive in the background" checkbox checked, which essentially does a defragment when the system is idle - this may have moved the exectuables to a different part of the drive - one that was corrupted.

Norman Diamond

7 Feb 2006 10:27 PM

NTFS file system corruption has been caused by the NTFS driver in Windows XP SP2, Windows 2003 SP1, Vista beta 1 32-bit, and Vista beta 1 64-bit.

Now sure, at first it looks like I have around 6 bad disk drives instead of 4 versions of a bad driver. But at second it doesn't. And at third it doesn't.

If a drive really reports a bad block, Windows records that in the event log. When the event log says the NTFS structure is uncorrectable instead of saying that the drive reported a bad block, the NTFS driver did it.

If Vista is installed in a guest machine under Microsoft Virtual PC, if the drive has a bad block, the real machine's real disk driver gets the report and the real Windows installation records it in its event log. When the guest Windows installation records an event in its log saying that the NTFS structure is uncorrectable, the guest's NTFS driver did it.

Theoretically NTFS maintains the overall integrity of the NTFS structure. If a power failure or BSOD causes writes to get lost, then a file's contents will be binary zeroes instead of the contents that you thought were there, but you won't get uncorrectable NTFS structures. If there's no power failure or BSOD then also you shouldn't get uncorrectable NTFS structures. But that's theory.

Phaeron

8 Feb 2006 1:15 AM

What I find amusing here is that if that system had been using a FAT32 filesystem instead of NTFS, odds are this would've been caught a lot earlier, because the filesystem would have been checked more often on restarts. It's like the firewall dilemma — firewalls can provide a good defense against the wilderness, but if you depend on it too much you're toast if something manages to sneak past.

Ashod Nakashian

8 Feb 2006 5:14 AM

Ahh, NTFS corruption. Finally, you are talking about one of those things that I like to find a responsible person to show what it fills like to use NTFS corrupted disk, and I have 2 of them. In total, I had 4 drives that had NTFS corruptions.

Larry, I wish you could explain why this is happening and what to do about it.

I'll try my best to explain how NTFS gets corrupted, and please, don't tell me no one else had this problem, because in 2 years period, I had 4 disks with the SAME problem. No, the drives are PERFECTLY fine, not a single bad sector. They are also working at their top speed (data transfer rate degradation is a sign of hardware problems.)

Every once in a while, I can't delete a folder because some process is using it. Explorer is a perfect example of locking-and-forgeting the folders. (A perfect example of how Micrsoft doesn't know how to inovate, they can only try to improve one thing, only to break another.) Ok, restart the machine, or KILL explorer.exe.

This is not one of those cases. I have a couple of folders that give me ACCESS DENIED when I try to delete or rename them. I can "open" the folders without a problem. I know, I have to check the security tab... but, there is NO security tab! There is only the properties tab and size is 0 bytes and all other fields are empty! I tried to reset the permissions on the parent folder (in this case the root) in vein.

I tried EVERYTHING that I know of (I'm a full-time programmer.) Check disk doesn't find ANY problems. NONE, surface-scan included. This problem occures on BOTH WinXP and 2k ALL service pack (as far as I know.) I had to format a drive because of this annoying issue. Now I have this problem on 2 different drives, 2 folders. My previous encounter with the problem was with XP service pack 1 and 2 (work and home PCs) and this time it's my home Win2k machine.

So you imagine the frustration of having a folder in the root of drive that you can't do anything with, hanging there for over a year!

Hope you have somebody has some answers.

P.S. All of these machines had a few 100K files on them, mostly source code files (i.e. small.)

Daniel Jonsson
8 Feb 2006 11:50 AM

Had a similar issue a year ago, where fonts and graphics became weird in dialogs after I woke up my work-laptop in the morning, including the logon window. I directly suspected some *dlg*.dll which was confirmed after running a chkdsk. I was in a hurry for a meeting so I went to the next cubicle and asked that guy to give me a copy of his dll on a floppy. Good idea to run SFC. I totally forgot about it and WFP, but I had less than 40 minutes to recover and wasn't thinking clear. I remember I rushed to the meeting during rebooting of windows after replacing the file.

DmitryKo
8 Feb 2006 2:25 PM

Yes NTFS can survive a power failure, but hard drives sometimes cannot.

I've personally had a case when the power cut off right in the middle of disk write and so the respective sector was permanently damaged. The disk would just cause some confusing errors on a particular file, with no automatic sector remapping that was expected to happen in this case. Scandisk/checkntfs didn't help either, so I had to back up the data and then zero all sectors using low-level disk management utility from the manufacturer (I think it was IBM DeskStar from the infamous DTLA series).

I'd guess that's what happened with Larry's harddrive.

ryanmy
8 Feb 2006 4:42 PM

When the power fails, all bets are off, no matter what filesystem you are using.

The fundamental problem is that the vast majority of hard drives lie about write completion due to cache, and even more lie about write cache flushing. Due to caching, not only can writes be rearranged, but delayed indefinitely under heavy load. A journaling filesystem can only detect the corruption, not recover the data.

If you have write caching on, expect to get data loss during a power failure. Too many drives simply lie about it, period. Get a UPS, or turn off write caching and accept the performance hit as the price of reliability. Or, use an enterprise-class RAID controllers and/or drive with a battery-backed write cache.

(FYI, the FreeBSD Handbook cites the same problem, as does the man page for Linux hdparm. This is not a Windows problem, this is across the entire storage industry.)

Skywing
9 Feb 2006 11:53 AM

The menu bar disappearing and Windows logo in the middle problem seems to be often caused by win32k running out of desktop heap; at least that's been by far the most often cause I've seen for this particularly annoying problem.

Revenant
9 Feb 2006 6:49 PM

Larry, I'd definitely put my money on the power failures. I do mainly computer repair work at the moment, and every time there's a storm or power failure we get a rash of people coming in with problems.

Every time.

We try to educate people to turn off/unplug everything during a storm or buy a UPS, but most people aren't convinced that $200 to protect that $2000 PC is a good investment... *shakes head*

Ashod Nakashian
10 Feb 2006 3:34 AM

Most decent HDDs take advantage of the few milliseconds they get before power failure to flush and park the heads. I believe that's what they do when they detect a sliding of the voltage below a certain threshold. In deed, power-supplies advertise the number of milliseconds they hold after power failure at maximum load.

Larry, I really hoped you'd give my question an answer. But, well, I guess, somethings, no one wants to get close to.

JonDR
10 Feb 2006 12:57 PM

I've also needed SFC /SCANNOW and it has saved me. My question is this: Say I have WinXP SP2 and I've kept it up-to-date with all the fixes and updates. I have a problem that is solved by running SFC (thanks to WFP!) and it gets the executable from cache or from the installation CD. Now, all the updates are logged as having been applied, but the ORIGINAL executable exists within the file system. When I go to Microsoft Update and ask for updates/fixes, does the scan that take place merely query the log files (thinking I have the updated executable) or does it properly recoginize that the old executable I am using needs to be updated because it has been replaced by a (hopefully) more secure and/or error-free version (update)?

Not that I'm paranoid about things (ok, I am, but ...).

Dean Harding
11 Feb 2006 2:37 AM

Ashod, Larry's on the audio team, not the NTFS team. Microsoft is a very big company and nobody know everything about everything. Perhaps you should ask someone on the NTFS team? Personally, I've never had this problem, and I've never known anyone else to have it either. Maybe you should do a scan for viruses or spyware. Did you try using Process Explorer or something to see who had a handle to the folder?

Brooks Moses

14 Feb 2006 5:11 PM

Dean, I've had essentially the same problem Ashod describes. (Not quite the same, because scandisk did fix it, and I got ACCESS DENIED errors trying to even open the directory.) In my case, though, I knew exactly when it happened, though I've forgotten which program I was running that did it. I seem to recall that it was repeatable, too -- apparently the program was doing something low-level with the filesystem that caused problems.

In any case, I remember that I ran both chkdsk and scandisk on the affected drive, and only one of them reported the problem (and fixed it). That may work in Ashod's case as well, if he's only run the one that doesn't fix the problem.

Akın Basdar

7 Apr 2006 10:30 PM

Ok if i had a SINGLE file corropted (sorry not a native speaker and it's 5 am in the morning) i'll just format it (if there has been a reasonable time passed since last time like 1 monts) an idea if your using only general stuff on that computer i would advice you to run linux on it damm even a linux on disc versions will be fine if you got compatible hardware so you wont have to do anything about it and you seem to have enough knowledge about comps. so you can arange it to save settings on hd. (you can find how to's everywhere) and even a 1gb hd would be enough. whatever this is what i do with the computers i got for everyones use i thought i might share...

Larry Osterman s WebLog WFP is my new best friend | Paid Surveys

30 May 2009 1:59 AM

PingBack from **http://paidsurveyshub.info/story.php?title=larry-osterman-s-weblog-wfp-is-my-new-best-friend**

Larry Osterman s WebLog WFP is my new best friend | Wood TV Stand

2 Jun 2009 7:49 PM

PingBack from **http://woodtvstand.info/story.php?id=83676**

Larry Osterman s WebLog WFP is my new best friend | Menopause Relief

9 Jun 2009 9:17 PM

PingBack from **http://menopausereliefsite.info/story.php?id=1236**

Larry Osterman s WebLog WFP is my new best friend | home lighting

19 Jun 2009 1:40 AM

PingBack from **http://homelightingconcept.info/story.php?id=3205**

Larry Osterman s WebLog WFP is my new best friend | bar stools

19 Jun 2009 3:00 AM

PingBack from **http://barstoolsite.info/story.php?id=5922**

Larry Osterman s WebLog WFP is my new best friend | storage bench

19 Jun 2009 4:16 AM

PingBack from **http://thestoragebench.info/story.php?id=5363**