Debugging a problem: Audio stops working after an XP SP2 install

Larry Osterman [MSFT] 16 Aug 2004 7:45 PM | 14

A number of people have asked for me to write up my experiences debugging a problem. The thing is that it's hard to do that explicitly without disclosing internals of functions that probably shouldn't be disclosed (because they relate to features that haven't been announced, etc). However, I debugged a problem the other day that fits the bill perfectly.

We had an internal helpdesk request come in that a user had lost audio shortly after installing XP SP2. It turns out that while I didn't have a huge impact on SP2 (mostly doing code reviews), there were a couple of things I added to the system. The biggest feature I added was the ability to stop the Windows Audio service.

And it turns out that this *could* have caused the problems the user was seeing.

So I asked for (and was granted) RDP (remote desktop) access to the machine. Looking at the machine, there were no MME (MultiMedia Extensions, our term for the waveXxx, mixerXxx, midiXxx APIs) devices enumerated. Well, it looked like I needed to break out the debugger.

Since the windows audio service runs in the same process as the networking services, and since the XP SP2 symbols are available over the network, the first thing I needed to do was to split the windows audio service into its own process. I made the necessary registry modifications to make it run in its own process (no, I'm not going to document them, nobody needs to know them), and then I stopped the windows audio service.

```
C:\>net stop “windows audio”
The requested pause or stop is not valid for this service.

More help is available by typing NET HELPMSG 2191.
```

Huh? Wait a second. Why isn't windows audio stoppable?

Time to pull the service debuggers bag-o-tricks. One of the utilities bundled with XP is a diagnostic tool known as sc.exe, it's a general purpose service control API utility. To do this, I need to use the short name for the windows audio service, audiosrv.

```
C:\>sc query audiosrv

SERVICE_NAME: audiosrv
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Hold on. I mentioned above that the biggest change I made for XP SP2 was to make the windows audio service stoppable. What's going on here?

I know that windows audio is stoppable in SP2 installations, I've verified that. The thing is that a service tells the service controller its capabilities when it first calls **SetServiceStatus**. Well, windows audio's call capabilities are hard coded, the only way that it would *not* be marked as stoppable is if something went wrong with the registration.

I wonder if somehow the DLL that holds the windows audio service didn't get updated with the SP2 installation. So I start explorer up on c:\windows\system32 and look at the windows audio DLL. It's got a file version of 6.0.4017. That's wrong; it should have a version of 5.1.2600.2180. 6.0.4017 is a *Longhorn* version number.

So I asked the person having the problem if he'd done anything that might have caused a longhorn version of audiosrv to be put on his machine. It turns out that he'd run an internal install script that copied over an interim Longhorn build of this DLL onto his machine.

And, since SP2's install didn't replace the file (because the file version on the file on his machine was newer than the SP2 version of the file), he was running a Longhorn version of the windows audio service on his XP SP2 machine.

We deleted the DLL, SFP copied back the right version and his machine had audio again!

Edit: Fixed screwy text.

Comments

Matt
16 Aug 2004 1:57 PM
Great info..There is lot to learn from the way you think..thanks for the info about these tips and tricks.

Prasanna
16 Aug 2004 4:39 PM
Hmmm... if the Longhorn version of the DLL was installed on his machine before SP2, how was his audio working before?

Larry Osterman
16 Aug 2004 4:55 PM
Good question Prasanna. The answer is that the audio service on his machine predated the SP2 changes I made. So the old longhorn audio service worked with the SP1 system (more by luck than anything else), but when the rest of SP2 was put on the machine, it broke.

Norman Diamond
16 Aug 2004 6:02 PM
1.

> I made the necessary registry modifications
> to make it run in its own process (no, I'm
> not going to document them, nobody needs to
> know them),

Well, it could be right that no one needs to know registry entries for it, but there is a big need for a capability to split separate services into separate processes. Consider the way some viruses insert their operations into existing services processes. If a user could prevent multiple services from running in one services process, and check exactly which service is running in each process, then there would be a possibility of terminating only the unwanted ones.

2.
> It turns out that he’d run an internal
> install script that copied over an interim
> Longhorn build of this DLL onto his machine.

Did he deliberately mix his OSes, or did the script mess up the wrong one? There used to be a common bug where OSes, drivers, and applications would assume that they should install some stuff on the C partition instead of the boot partition. This bug is less common than it used to be, but it still happens sometimes. When I install an OS onto a new (or newly cleaned) machine, I do not put it on C, I start by putting it on D. Whether or not I add other OSes in other partitions later, this still gives a chance of catching errant drivers or applications. If a Program Files directory or Windows directory suddenly gets created on C, I know some vendor screwed up. And there's no innocent bystander on C to get killed by it.

Now the biggest offender in recent months is, well, want to guess? Actually it started with a hotfix prior to SP2, I don't know which hotfix, but it continues after SP2 as well. The paging file (pagefile.sys) keeps getting created on C and keeps getting deleted from the boot partition. This happens on a friend's machine where I created a miniature C partition for NTLDR, NTDETECT.COM, etc., and there isn't enough room for a proper paging file, so he gets warnings all the time. I move it back to D and it sticks for about two reboots, but every third reboot or so, Windows XP keeps moving it back to C.

Among all the Knowledge Base articles that I've found about the paging file in Windows XP, only 316528 admits that Windows XP doesn't obey the user's settings. KB 316528 says that this can be fixed by downloading Intel Application Accelerator (IAA) from Intel's web site. But Intel doesn't even make IAA versions for two of the machines where this problem occurs:
(1) My friend's machine, mentioned above, has an ICH5 chipset. There's an IAA for ICH5R but none for plain ICH5.
(2) One of my machines, which I use daily, has a Crusoe CPU and ALi (Acer) chipset. Windows XP still keeps moving my pagefile.sys from D to C about every third reboot. KB 316528 says I should get a download from Intel to fix it.

Pavel Lebedinsky
16 Aug 2004 6:09 PM

Actually, svchost registry settings are documented in **http://support.microsoft.com/?id=314056**

I think this is mostly for troubleshooting purposes - changing the default configuration is probably not supported.

Iain
16 Aug 2004 10:23 PM

I'm curious. How can you say "nobody needs to know them" of the registry modifications when they made your life easier? Surely this would have been much more painful without them?

Larry Osterman
17 Aug 2004 12:29 AM

Pavel, I didn't know that they were documented anywhere. Cool :) Ok, anyone wanting to know the registry changes I made can look at the KB article that Pavel pointed to and figure them out.

Iain, the reason I didn't describe them is that nobody except someone debugging the windows audio service has a reason to split it out. I do it all the time, so I need to know that, but for customers, it's not particularly relevant stuff. And the only reason I break audiosrv out is if I want to get the symbols off the net. If the symbols are on the local machine, I usually just leave it where it is.

And if you start randomly pulling services out of svchost groups (for "diagnostic purposes"), then the system WILL start breaking. Many of these services are designed to work in the same process, and will break in subtle ways if they're pulled out. And no, once again, I'm not going to tell you which ones will break. You start messing with the registry and you're on your own.

I don't want to hear that someone called PSS to get their machine fixed up and told PSS that Larry Osterman told them how to split services out from the svchost process in which they were designed to run. As Pavel said: Changing the default configuration is NOT supported.

Btw, as a tidbit of information, no 3rd party code is allowed to run in a shared svchost process - because the svchost processes are services that are required for system reliability, we don't allow any 3rd party code in them. Please note: a SHARED svchost process. There are svchost processes that only run one service (like the spooler service).

Oh, and Norman, in this case, the user accidentally did it. He ran a script to install a component he was working on that copied a longhorn version of a DLL to his machine (actually it copied a bunch of DLLs to his machine, audiosrv.dll was the only one that caused problems). For the work he was doing, he was able to mostly get away with it (back last year when he did it), running the same script nowadays would fail (since there's now a version check).

Larry Osterman's WebLog

17 Aug 2004 1:40 PM

Norman Diamond

17 Aug 2004 5:23 PM

8/17/2004 12:29 AM Larry Osterman

> Btw, as a tidbit of information, no 3rd
> party code is allowed to run in a shared
> svchost process

This is helpful, thank you. So if a virus installs itself as a service then it will be safe to kill that process, because no genuine services will be sharing the same process.

> Oh, and Norman, in this case, the user
> accidentally did it.

OK thank you. By the way I have no complaint about the change in partition policy that came about with Windows 2000. It used to be possible for Windows NT4 to be installed into the same partition as either 95 or 98. Nonetheless, both then and now it is safer to install into separate partitions. I just wish that Windows XP would remember that, for more than two reboots after I tell it to.

Larry Osterman

17 Aug 2004 8:11 PM

Norman, once again, this is a non sequiteur.

If you find a DLL that wasn't signed by Microsoft (or other 3rd party code) running in a shared svchost instance, you can be pretty certain that someone's infected your machine.

And it's likely that you need to pave the machine because you have no idea what has happened. Run an anti-virus scan immediately.

But saying that it's safe to kill the process is silly. Some of these processes (winlogon.exe for example) are critical to the functioning of the system and will immediately cause a bluescreen.

A more accurate statement is that if you find code running in svchost.exe that wasn't signed by Microsoft you need to start looking very, very carefully at the system to ensure that someone hasn't tampered with it. But killing random processes is a recipe for disaster.

Edit: Sorry, Norman - I have a problem spelling your name for some reason. I have no idea why I have this mental blank there, sorry.

Pavel Lebedinsky
17 Aug 2004 9:03 PM

> If you find a DLL that wasn't signed by
> Microsoft (or other 3rd party code) running
> in a shared svchost instance, you can be
> pretty certain that someone's infected your
> machine.

Some of the services running in shared svchosts (like TAPI for example) can load 3rd party DLLs (TAPI service providers). This is a supported scenario.

DrPizza
18 Aug 2004 2:23 AM

"Iain, the reason I didn't describe them is that nobody except someone debugging the windows audio service has a reason to split it out."

This is utter bollocks.

Various shared services can hang. There's no way to restart them without killing the entire process. This is a big problem, because it also kills the other shared processes which is not what you want.

If a shared service has a tendency to hang, it's convenient to split it out.

Frankly, I find the shared services a pain in the butt, and can't see any real justification for it. A minute memory saving perhaps?

Larry Osterman
18 Aug 2004 9:26 AM

DrPizza, the savings is several hundred kilobytes per service - several hundred kilobytes of PHYSICAL memory, not virtual memory. That's NOT a "munute memory saving", it's significant.

And if you start splitting up shared services, then things WILL break. I can absolutely 100% guarantee it. Many of the services running in shared svchost processes have assumptions that other services are running in the same process, and will break if they're not present.

Norman Diamond

18 Aug 2004 6:14 PM

8/17/2004 8:11 PM Larry Osterman

> If you find a DLL that wasn't signed by
> Microsoft (or other 3rd party code) running
> in a shared svchost instance

But you said previously that this wasn't even possible. If a virus installs itself as a service then it must be in a non-shared instance and it is safe to kill the thing.

> And it's likely that you need to pave the
> machine

By the way I did pave one friend's machine because he got an MBR virus while Windows XP was running. Repeatedly I booted the Windows XP to the repair console, FIXMBR warned that the MBR was nonstandard but I proceeded and FIXMBR said it fixed the MBR, but it was lying. Finally had to delete all partitions including the miniature FAT32 C partition, recreate a new miniature FAT32 C partition, recreate a new NTFS D partition and continue reinstallation from there. I did some Googleing to find if it's really possible for a virus to infect an MBR while XP is running, and it seems there is one that can do it.

I haven't decided yet whether to pave another friend's machine. This one did have a ton of viruses in RUN keys in the registry and other places. I left it with no visible viruses, but guess he probably still has a few hundred less visible ones. I don't have another full day free to help him blowtorch his hard disk and start over though.