TechRepublic
Real World. Real Time. Real IT.

Click for Tips to Maximize Microsoft Office:
Recover data from Corrupt Office files | Publish databases with FrontPage 2000 | Edit a custom dictionary in Word
Use Word's label feature | Debug Excel formulas | Create handy Access forms

What events can cause Windows 2000 to crash?

Dec 4, 2001
Brien M. Posey MCSE
© 2001 TechRepublic, Inc.

If you've worked with computers for any length of time, you've no doubt encountered situations in which a crash was so severe that it took a full day (or longer) to restore the system to working order. Meanwhile, your workload continued to pile up, and users were kept waiting for less significant repairs while you tackled the big one.

Unfortunately, there's no foolproof method of preventing a massive crash. You can significantly reduce the amount of time required to recover from a really big crash, though, if you know what caused it in the first place. This knowledge can also help you prevent crashes.

Let's take a look at the root causes of Win2K crashes. One note before we get started: Although people have different ideas of what constitutes a major crash, for the purposes of this article, I'll define a major crash as one that prevents the Windows 2000 operating system from booting.

Incorrect device drivers
One of the most frequent causes of a system failing to boot is an incorrect driver. An incorrect driver can be one of the easiest problems to track down and fix. If you change a driver and suddenly the system fails to boot, it's pretty obvious that the driver is probably what's causing the problem. What makes this problem even easier to track down is that most of the time, only a handful of device drivers have the potential to cause a boot failure.

If you suspect an incorrect device driver, the device with the incorrect driver is most often a video adapter, network card, sound card, or some other high-profile hardware component that's used during the boot process. A modem driver or a printer driver, even if incorrect, usually won't cause a boot failure because modems and printers usually aren't initialized during the boot sequence.

The incorrect device driver also probably won't have anything to do with lower-level system components such as hard drives, CD-ROM drives, USB, LPT, or serial ports because these items typically rely on generic device drivers that work for just about any system. The exception to this is SCSI devices, which rely on specific device drivers. An incorrect SCSI device driver can and usually will cause a boot failure.

Bad device drivers
A bad device driver is one that has been loaded appropriately but is malfunctioning. Sometimes drivers go bad when a registry entry or file that's associated with the driver is accidentally modified, deleted, or corrupted. Many of the rules that apply to incorrect device drivers apply to bad device drivers. A bad device driver will cause a boot failure only if the device that's associated with the bad driver is used during the boot process.

Hard disk corruption or failure
Another major cause of major system crashes is a hard disk failure or hard disk corruption. Obviously, if the hard disk that contains the boot or system partitions (or both) were to fail, booting the operating system would be impossible. Likewise, even if the hard disk doesn't physically fail, if some or all of the information contained on the system or boot partitions becomes corrupted, the boot process may also be impossible.

If the hard drive physically fails, the only real solution is to replace the drive and reload the operating system, restore a backup, or both. If the drive is still working but some corruption has occurred, things quickly become much more interesting. Getting the system back up and running becomes a question of what was on the failed drive or partition.

For example, if the failed drive or partition contained only the Windows 2000 operating system, the quickest and easiest solution might be to reformat the drive and restore a backup or reload the operating system. If, on the other hand, the affected drive or partition contained data, you'd probably be better off trying to salvage the drive or partition rather than simply reformatting it.

User tampering (security)

Another cause of massive failures is user tampering. I've seen more situations than I can count in which a user crashed a workstation. One example is the user who was running out of hard disk space and "corrected" the problem by erasing every file he didn't recognize (COMMAND.COM, WIN.COM, etc.).

User tampering isn't nearly as big an issue in Windows 2000 as it was in Windows 9x because of the integrated security. I have seen it happen, though. For example, in one situation, Windows 2000 workstations used the FAT file system instead of NTFS, and there was nothing preventing users from making changes to system files.

An even uglier situation involved the Windows 2000 security system. Windows 2000 is designed so that you can log in to either a domain or the local machine. Each individual workstation contains its own Administrator account that can be used to make changes to the individual machine's configuration.

A help desk technician logged in to a workstation to perform some routine maintenance. During the course of this maintenance, the technician received a phone call. The machine's user knew just enough about Windows 2000 to be dangerous and changed the local administrator's password. After the technician got off the phone, he finished the job, unaware of the password change. The rogue user then made a few changes and crashed the system. The technician was unable to get back into the system to fix the problem because the password had been changed.

As you can see, even a fairly secure operating system like Windows 2000 can be subject to user tampering if security policies and procedures are lax. It's impossible for me to tell you that if a user tampers with a system, you can follow a specified procedure to fix the problem. The user can do almost anything to the system. Fortunately, just about any type of tampering that's severe enough to crash the system falls into one of the other categories discussed here.

Incorrect version of files or missing files

Incorrect or missing system files can cause a crash. This can happen when files are accidentally deleted, when a buggy service pack is installed, or when a technician attempts to copy a missing file from another machine.

Viruses

All the e-mail viruses that have been going around lately have created an increased awareness of this threat. Although this type of virus usually can't prevent a system from booting, there are some that can, such as boot sector viruses and file viruses.

CPU failure

It may seem obvious that if a CPU fails, the system may not boot. Unfortunately, there are many types of CPU failures. For example, rather than the CPU completely going bad, one particular memory block may go bad.

Registry

One of the trickiest problems to fix is a bad registry entry. There's a very real chance that registry corruption can lead to a major crash.

Summary
Major systems crashes can be extremely disruptive to both users and the IT desk staff. When a major crash occurs, your goal is usually to recover as quickly as possible with minimal data loss. The first step in recovering from a really big crash, whether on a server or a workstation, is to understand the factors that could have led to that crash. Only then can you effectively begin the troubleshooting process.

Try TechProGuild free!

If you found this article helpful, check out our TechProGuild premium subscription product, which offers in-depth technical articles covering a variety of IT topics, including Windows NT/2000, Linux, IT troubleshooting, and NetWare. With a TechProGuild account, you can also read the complete text of popular IT industry books online. Sign up now for a FREE 30-day TechProGuild trial.

Copyright © 1999-2001 TechRepublic, Inc.
Visit us at www.TechRepublic.com