

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

What would you do if one of your core production servers crashed the next time you reboot it? More important, how much time would you need to fix the problem? For most Windows NT administrators, the thought of a mission-critical production server experiencing STOP errors (aka the blue screen of death) or any form of server outage makes them break out in a cold sweat.

A hosed NT system is never fun, but an unavailable critical server means lost productivity, lost time, lost money, and, of course, an angry boss. In this first installment of a two-part article, I discuss advanced tools and procedures that you can use to improve the availability of your network servers and to increase your chances of recovering from an NT boot failure. In addition, I delve into lesser-known techniques that you can employ right away to help you recover a downed NT system in the future. In this article, I don't address clustering solutions, and I assume that each system is a standalone, nonclustered NT system without system-level failover.

## Common Calamities

Although various circumstances can cause an NT system to crash at startup, the result of these circumstances is usually the dreaded blue screen of death, which Screen 1, page 100, exemplifies. After NT halts the system, it displays this screen to protect the system against data corruption. In addition to being blue as its name implies, a blue screen displays important information about the system's state at the time of the STOP error. The screen lists the STOP code, the location in memory where the problem occurred, and the drivers loaded in memory when the STOP took place. However, pinning down the source of a STOP error isn't always easy. In my experience, a problem usually develops from one of the following scenarios:

- You install software that corrupts the HKEY\_LOCAL\_MACHINE portion of the Registry—particularly, software that installs new services or drivers. This action usually results in a STOP error or blue screen, which indicates that the system Registry or a particular hive file failed.
- You change a system's network configuration, which causes NT to rewrite network bindings and their related Registry entries (i.e., NT corrupts or overwrites critical OS files with invalid or incompatible versions while the system is in use).
- You install a new service or driver on the system, which causes a system-level incompatibility problem that results in a STOP error when you reboot (i.e., underlying file corruption has occurred on a key system file that you loaded into memory before the corruption).

Each of these situations has a different set of underlying causes and solutions, so let's look at each scenario individually.

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

```
DSR CTS
*** STOP: 0x0000000A (0x00000000, 0x0000001a, 0x00000000, 0x00000000)
IRQL_NOT_LESS_OR_EQUAL

p4-0300 irq1:1f  SYSVER: 0xf000030e

Dll Base  DateStmp  - Name                Dll Base  DateStmp  - Name
80100000  2e53fe55  - ntoskrnl.exe        80400000  2e53eba6  - hal.dll
80010000  2e41884b  - Rhal54x.sys         80013000  2e4bc29a  - SCSIPORT.SYS
8001b000  2e4e7b6b  - Scsidisk.sys        80220000  2e53f238  - Ntfs.sys
fe420000  2e406607  - Floppy.SYS          fe430000  2e406618  - ScsiCDrm.SYS
fe440000  2e406659  - Fs Rec.SYS          fe450000  2e40660f  - Null.SYS
fe460000  2e4065f4  - Beep.SYS            fe470000  2e406634  - Sermouse.SYS
fe480000  2e42a4a4  - i8042prt.SYS        fe490000  2e40660d  - Mouclass.SYS
fe4a0000  2e40660c  - Kbdclass.SYS        fe4c0000  2e4065e2  - VIDEOPRT.SYS
fe4b0000  2e53d49d  - ati.SYS              fe4d0000  2e4065e8  - vga.sys
fe4e0000  2e406655  - Msfs.SYS             fe4f0000  2e414f30  - Npfs.SYS
fe510000  2e53f222  - NDIS.SYS             fe500000  2e40719b  - elnkii.sys
fe550000  2e406697  - TDI.SYS              fe530000  2e47c740  - nbfs.sys
fe560000  2e5279d9  - nwlknkpx.sys        fe570000  2e53a89e  - nwlknkb.sys
fe580000  2e494973  - tcpip.sys            fe5a0000  2e5256b8  - afd.sys
fe5b0000  2e5279d3  - netbt.sys            fe5d0000  2e4167f7  - netbios.sys
fe5e0000  2e4066b3  - mup.sys              fe5f0000  2e4f9f51  - rdr.sys
fe630000  2e53f24a  - srv.sys              fe660000  2ef16062  - nwlknkpx.sys

Address      dword dump Build [1057]
ff541e4c     fe5105df fe5105df 00000001 ff640128 fe4a8228 000002fe - NDIS.SYS
ff541e60     fe501368 fe501368 00000246 00040402 00000000 00000000 - elnkii.sys
ff541eb4     fe481509 fe481509 ff6688c8 ff668288 00000000 00000000 - i8042prt.SYS
ff541ee0     fe481ea8 fe481ea8 fe482078 00000000 ff541f04 8013c58a - i8042prt.SYS
ff541ee4     fe482078 fe482078 00000000 ff541f04 8013c58a ff6688c8 - i8042prt.SYS
ff541ef0     8013c58a 8013c58a ff6688c8 ff668040 80405900 00000031 - ntoskrnl.exe
ff541efc     80405900 80405900 00000031 06060606 06060606 06060606 - hal.dll

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option if this message reappears,
contact your system administrator or technical support group.
CRASHDUMP: Initializing miniport driver
CRASHDUMP: Dumping physical memory to disk: 2000
CRASHDUMP: Physical memory dump complete
```

## Registry Corruption

The system Registry is the heart of an NT installation. Thus, depending on the nature and extent of the damage, a corrupted Registry often results in a STOP error or blue screen of death at startup. Damage to the Registry can be physical or logical. Physical damage means that something (usually disk-related corruption) has scrambled the Registry hive files (e.g., the SOFTWARE or SYSTEM files in the %windir%\system32\config folder). Logical damage means that a third-party application, a user, or NT has written invalid data to the Registry, which can trigger an NT startup failure if the logically damaged Registry entry is critical.

Unfortunately, you can't always tell whether a damaged Registry is the cause of your system's STOP error. The STOP error might identify a telltale sign such as a hard Registry error or a reference to a particular damaged hive file. However, in some cases, the STOP error doesn't indicate Registry damage.

If you suspect a Registry-related problem, the first line of defense is to restore a previous known-good Registry configuration. You can use several methods to accomplish this solution.

The Last Known Good Configuration option. You access this option by pressing the space bar when the system prompts you during the NT boot process, and selecting the option to restore a previous configuration. This method is the quickest and easiest solution, if it works. Unfortunately, this solution's failures outweigh its successes in real-world applications because its scope is only a previously known-good incarnation of one portion of the Registry (i.e., a ControlSet00X Registry subtree of the HKEY\_LOCAL\_MACHINE\SYSTEM key). You have a better chance of success using the Last Known Good Configuration option if the problem is localized to this portion of the Registry

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

and an event that immediately precedes the invocation of the Last Known Good Configuration option caused the problem. However, this procedure won't cure most of your Registry-corruption ills.

NT Setup's Repair process and an Emergency Repair Disk (ERD). You can use NT Setup's Repair process to inspect and replace individual Registry hive files if the Last Known Good Configuration option fails to resolve the problem. After you insert your ERD, Setup lists the options you can select to specify which portions of the NT installation you want Setup to inspect, as Screen 2 shows. If you select Inspect registry files, Setup displays a list of Registry hive files and lets you select which files you want Setup to replace. Setup takes the replacement files from the ERD or, if you didn't provide an ERD, from the %systemroot%\repair folder. The ERD and the %systemroot%\repair folder store replacement files in compressed format, and each hive file has an underscore (\_) extension (e.g., SYSTEM\_, SOFTWARE\_).

```
As part of the repair Process, Setup will perform each of the optional
tasks shown below with an "X" in it's check box.

To perform the selected tasks, press ENTER to indicate "Continue." If you
want to select or deselect any item in the list, press the UP or DOWN arrow
key to move the highlight to the item you want to change.

Then press ENTER.

[X]   Inspect registry files.
[X]   Inspect startup environment.
[X]   Verify Windows NT system files.
[X]   Inspect Boot Sector.
      Continue <perform selected tasks>

F1=Help      F3=Exit      ESC=Cancel

ENTER=Select/Deselect
```

Using the most recent replacement files is important so that you don't lose application and service configuration information. (For information about how to update your ERD, see Michael Reilly's "The Emergency Repair Disk," January 1997.) In addition, don't restore the SAM and SECURITY hives on an NT server domain controller, unless you used the rdisk /s (or /s-) option when you ran the ERD utility (i.e., rdisk.exe). Otherwise, Setup overwrites your SAM database with the database version Setup created during the original NT installation and creates a new set of problems. In addition, ensure that you created the replacement files under the same service pack level as the files you're replacing because Service Pack 3 (SP3) and later make security-related changes to the SAM and SECURITY hives. Otherwise, you might not be able to log on after the repair is complete. Restoring the SAM and SECURITY files usually won't resolve your Registry corruption problems anyway because the SYSTEM and SOFTWARE hives usually cause Registry boot problems. Thus, start restoring previous Registry files with the SYSTEM and SOFTWARE files, and replace the SYSTEM hive first because it contains references to important system components, including drivers and services.

An alternate/parallel NT installation. Using an alternate/parallel NT installation to recover the Registry is my favorite solution. Booting an alternate NT installation lets you access NTFS-based volumes on the system that would otherwise be inaccessible, and a parallel installation gives you access to the primary installation's Registry files so that you can repair or replace them. After you boot to an alternate installation, you can perform the same actions that you can perform using NT Repair, but with more flexibility and options. Although this method isn't the solution Microsoft recommends, I think it's the best Registry repair process for advanced NT users.

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

Before you begin, make a backup copy of the Registry files. I usually back up the existing files into a subdirectory of the folder that contains the Registry files (e.g., `\%systemroot%\system32\config\backup`). After you back up the files, you can experiment with replacing individual Registry hive files. However, you can't simply copy the replacement versions, because the ERD and `\%systemroot%\repair` folder store these files in compressed format. To use the files, employ the `expand.exe` command to manually expand them. For example, to expand a compressed copy of the SYSTEM hive from an ERD or the `\%systemroot%\repair` folder, type the following command at an NT or DOS command prompt:

```
expand system._ system
```

Copy the resulting file to the `\%systemroot%\system32\config` folder of the primary installation, and reboot the system.

If you don't want to deal with compressed files, you can use the Microsoft Windows NT Server 4.0 Resource Kit `regback.exe` utility to maintain extra copies of the Registry. This handy tool makes a backup that contains all the system Registry hive files in uncompressed format. In addition, this tool automatically backs up the SAM and SECURITY hives, so you don't have to worry about using special switches. However, `regback.exe`'s uncompressed Registry copies consume a lot of space and might not fit on a 3.5" disk. The safest place to store `regback.exe`-created Registry backups is on a partition other than the NT boot partition—preferably a partition on a different physical hard disk. For maximum protection against hardware-related failures that render the Registry hive files inaccessible, store an extra copy of each server's Registry on a different system.

## Overwritten or Corrupted Files

One of NT 4.0's serious downfalls is its use of shared system files, which third-party application vendors can freely overwrite with out-of-date or otherwise incompatible support files. In addition, NT doesn't do much to protect itself against the replacement of other key system files, such as system services' files and drivers. In some cases, these conflicts are merely annoying because they cause unwanted errors or application failures. However, this type of problem can result in the inability to start NT. (Windows 2000—Win2K—removes some of this risky exposure by privatizing application DLLs and providing greater protection from overwriting critical system files.)

To repair damaged or incompatible files on an NTFS volume, you can use a parallel NT installation or NT Setup's Repair process. To repair FAT volumes, you can use a DOS or Windows 9x boot disk to access the volume.

Replacing files from a parallel installation is easier if you know which files are invalid or damaged. As a disaster-prevention measure, create an installation source on your hard disk or a CD-ROM that contains copies of the latest core NT system files for the service pack on your system. If you're running a parallel NT installation that you patched to the same service-pack level as the primary installation, you can use that installation as your source. However, if your parallel installation isn't the same service-pack level as your primary installation, create a separate directory that contains the latest versions of the primary installation's files.

To use NT Setup's Repair process to replace damaged or conflicting files, select the Verify Windows NT system files option when Setup presents you with the list of repair options. Microsoft intended this feature to let you quickly identify files that are different from the original NT installation files. However, an NT installation that you've installed a service pack on causes Setup to list most files as unoriginal because the service pack has modified them. Thus, your best bet is to instruct Setup to replace all

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

nonoriginal files by selecting the A option and reapplying the latest service pack after NT is back up and running.

Alternatively, you can replace NT system files with original versions using NT Setup's upgrade option to reinstall NT. Although some users circumvent the previous NT Setup Repair process and jump into an upgrade installation, I don't recommend this solution for several reasons. First, the upgrade process usually takes much longer than the repair process. Second, the upgrade process is more involved and poses greater risks to your system. Finally, if an upgrade installation successfully resolves your original problem, it will probably cause a tcpip.sys blue screen error (i.e., STOP error 0x00000050). When you install NT 4.0 or NT 4.0 SP1 over NT 4.0 SP2 or later, the installation doesn't replace the SP2 or later version of tcpip.sys. Thus, the driver fails the base version of NT or NT SP1.

To avoid this mess, first use the NT Setup Repair process' Verify Windows NT system files option to replace the existing files with the original versions. If NT Setup's Repair process doesn't resolve the boot problem, you can run the NT Setup upgrade option without fear of the tcpip.sys blue screen, because NT Setup's Repair process has replaced the SP2 or later version of tcpip.sys with the original version.

## An Ounce of Prevention

The difference between a quick fix and a major nightmare is often one preparatory step. Tools, such as parallel NT installations and additional backup copies of the Registry, improve your chances of resolving NT startup failures. Therefore, be sure that your servers are always prepared for the worst.

Next month, I'll discuss the third most common cause of NT startup blue screens: an autostarting service or driver that causes a STOP blue screen when it initializes. I'll teach you about some additional recovery tricks, including a method for remotely repairing the Registry of a failed installation from within a parallel NT installation. In addition, I'll show you third-party tools that can bail you out of trouble when a system won't boot.

In "Recovering from NT Startup Failures, Part 1," September 1999, I discussed common causes of Windows NT startup failures and introduced you to several techniques that you can use to prevent and quickly recover from NT boot disasters. In this second installment, I provide more prevention and recovery tips, and discuss additional NT boot failure causes and the methods and troubleshooting tools you can use to quickly recover from them.

## Be Prepared

As I concluded in part 1, the most important step in NT recovery happens long before a failure occurs—preparing for a problem before it begins. To prepare for tomorrow's worst possibilities, you need to take precautionary steps today, such as properly designing your NT systems' hardware and software setup, backing up crucial system configuration information, and developing a disaster-recovery toolkit that includes all the utilities you'll need to recover from common NT boot problems. These resources are your ace in the hole if things go awry.

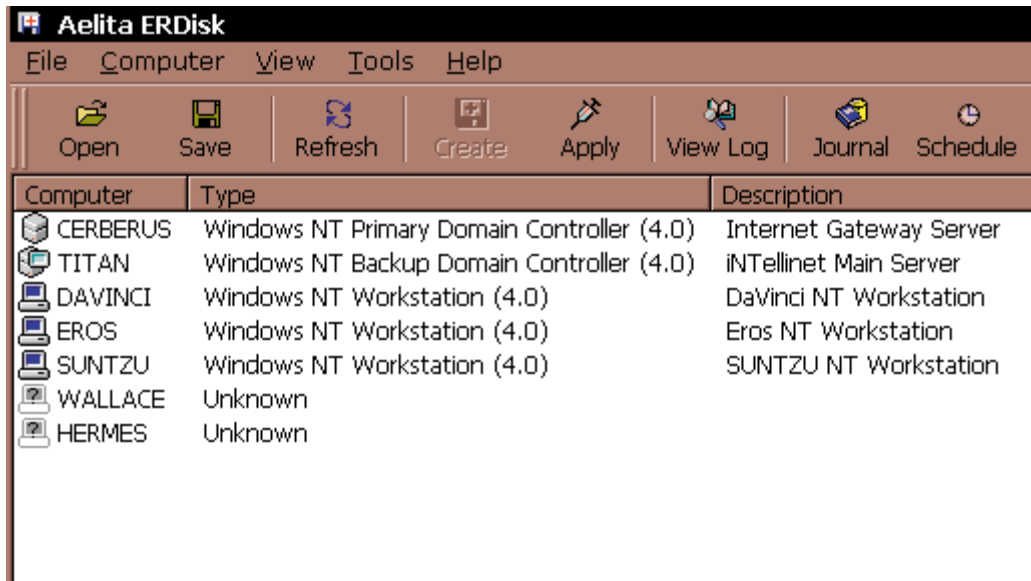
Most NT users know the importance of maintaining up-to-date copies of the Emergency Repair Disk (ERD) for NT systems. This disk contains a copy of the system Registry and provides crucial information that you need to use NT Setup's Repair process to locate and repair a damaged NT installation. Most IT shops perform regular system backups and create updates of the NT ERD for their NT servers. However, many organizations consider this process tedious and time-consuming because the process requires administrators to physically visit each server and run rdisk.exe. Thus, critical servers' ERDs aren't always as up-to-date as they need to be. If this situation sounds familiar,

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

consider an alternative method of collecting ERD information for your NT machines. Aelita Software Group's ERDisk utility, which Screen 1, page 84 shows, can perform remote, over-the-network ERD creations. In addition to storing ERD information to any drive location (local or network drive) that you specify, ERDisk can handle multiple machines' batch jobs, which you can schedule to run automatically. ERDisk can automate the ERD update process on all your networked NT systems, so you don't have an excuse for not having updated ERDs.



## Cross-Backups

You need to be vigilant about maintaining updated ERDs for each of your NT systems, but your preventive maintenance shouldn't stop there. In part 1, I discussed methods for maintaining Registry backups that are convenient when you have to perform a recovery operation. For example, the Microsoft Windows NT Server 4.0 Resource Kit regback.exe utility lets you create uncompressed copies of individual Registry hive files. These uncompressed Registry copies are convenient when you need to replace Registry hives. (For more information about regback.exe, see the sidebar "The Regback Profile Quirk," page 86.) However, common sense dictates that storing backup data on the hard disk of the system you're backing up isn't the most fault-tolerant practice. Alternatively, consider using cross-backups, in which you copy important system configuration data, such as Registry backups, from one machine to another machine on the network. The principle behind this practice is that more is always better when it comes to backups, and the best place to store a system's backup is anywhere but on that system.

If cross-backups appeal to you, consider extending this practice beyond Registry data to other types of crucial data. For example, I periodically make offline backups of my Microsoft Exchange Server databases (i.e., dir.edb, pub.edb, and priv.edb) to another server on the network. My backup software uses an Exchange agent to make online backups of Exchange Server; however, I've discovered that a recent offline backup simplifies full Exchange Server recoveries (i.e., when you have to restore Exchange Server from scratch). However, cross-backups should serve as an additional resource that complements your existing disaster-recovery plan—don't use cross-backups to replace your primary backup solution (e.g., tape backups).

If you don't want to junk up your systems with backup data, you can place this information on removable media, such as CD-Recordable (CD-R) and CD-Rewritable (CD-RW) discs, Zip and Jaz

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

cartridges, magneto-optic (MO) cartridges, or similar media. This practice is a good idea because 3.5" disks, which are the only storage media that NT's ERD utility supports, don't have the reputation of being the most reliable media type.

## Autostarting Services and Devices

In part 1, I talked about the following common causes of NT startup failures and the blue screen of death:

- Installing software that corrupts the HKEY\_LOCAL\_MACHINE portion of the Registry—particularly software that installs new services or drivers on the system.
- Changing a system's network configuration (e.g., in the Control Panel Network applet), followed by NT miswriting the configuration's network bindings in the Registry.
- Underlying file corruption that occurs on a key system file that was already in memory and working before the corruption.

In addition, I provided methods you can use to resolve these problems. The recovery methods I discussed involved wholesale replacement of Registry hive files.

This month, I highlight startup failures that result from a service or driver causing a STOP error when it initializes. Rather than completely restoring the Registry or overwriting entire Registry hives, you can edit the Registry to solve this problem. This solution might be preferable to replacing Registry hive files if you don't want to lose configuration settings or if you're not sure which service or driver is causing the problem.

In some cases, the STOP error results from a service or driver that loads before the GUI appears (i.e., when NT initializes the video display driver and shifts into graphics mode). In other cases, the error might occur after NT shifts into graphics mode; it can even happen during or after the logon process because some drivers and services might still be loading in the background after NT displays the logon prompt. This situation might be the cause if you've installed a new service or driver, or after you've reinstalled NT. Additional causes of a service/driver startup problem include software installations that install services or drivers that conflict with other services or drivers or the NT's service pack level, and changes to a system's hardware or software configuration that cause drivers or services that previously loaded successfully to become problematic. For example, physically changing the type of network card without first removing the driver causes the old driver to produce a STOP error.

Another situation that results in a STOP error is when you change a video card driver on a system with a remote control package installed (e.g., Symantec's pcANYWHERE32). Most remote control applications hook the current display driver during their installation, so problems result when you pull the original display driver out from under these applications. The originally hooked driver is no longer active, so rebooting the system results in a STOP error or blue screen. To safely change a video driver on a system with a remote control package installed, uninstall the remote control software, change the video driver, then reinstall the remote control software.

## Renaming, Moving, or Deleting Offending Files

You can employ several methods to prevent a service or driver STOP error. One method is to rename, move, or delete the file to stop the service or driver from loading. If you know the name of the

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

offending service or driver, you can try booting into DOS if the boot volume is FAT or try a parallel NT installation if the boot volume is NTFS, then rename the file to a temporary name. In many cases, this solution causes the STOP error to disappear but leaves a reference in NT's configuration to a service or driver that is no longer there. If you choose this method, be sure to reinstall the service or driver or completely uninstall it after you've booted into NT. This renaming method doesn't work and can cause problems in situations that involve multiple chained services or drivers, such as the previous remote control software example.

## Offline Registry Editing

Another method to resolve this server/driver startup problem is to edit the Registry to manually disable the service or driver. How do you edit the Registry if you can't boot NT? As long as you have an alternative method of accessing the volume that contains your original NT installation, you can edit the Registry. To gain access to Registry data from outside the original NT installation, you can boot to a parallel NT installation on the same system, or you can install a disk that contains the NT boot partition (i.e., the NT installation folder and Registry hive files) onto another NT system.

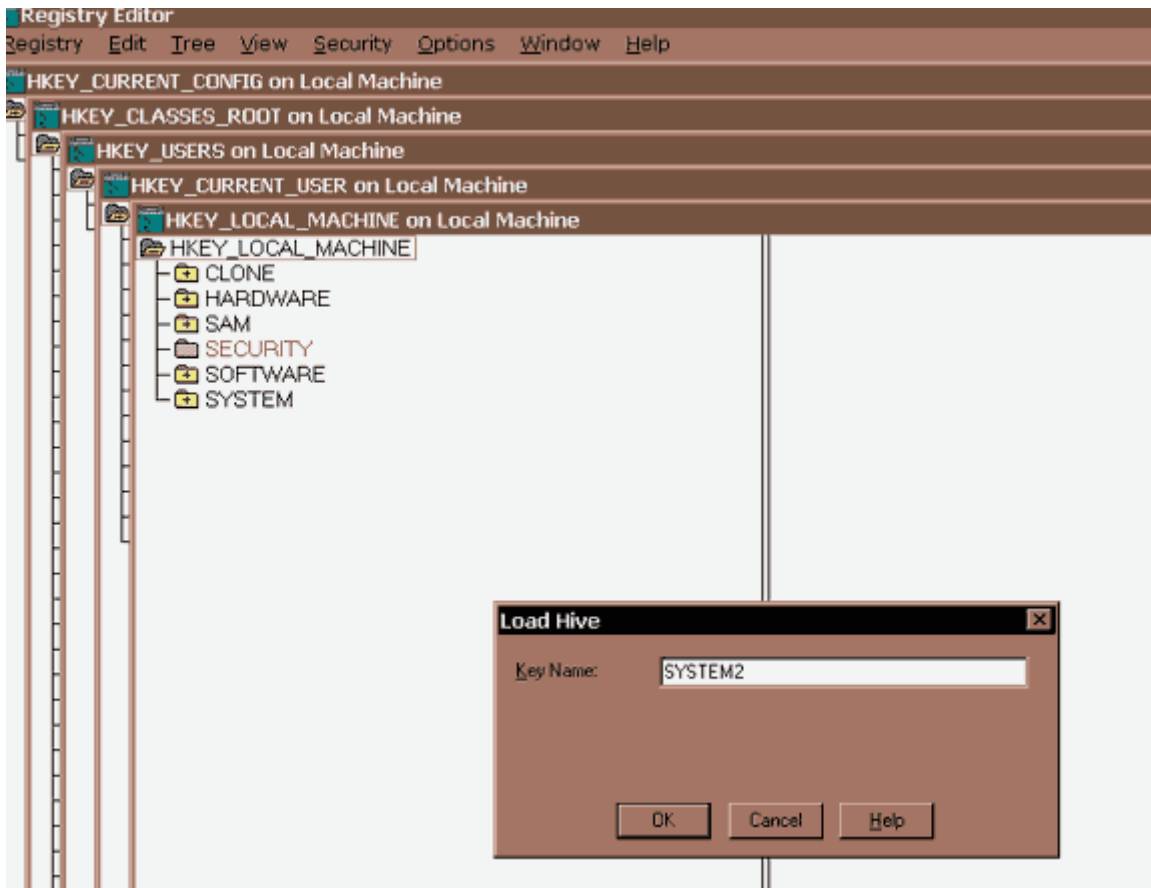
Gaining access to the Registry through a parallel NT installation on the same system is easier than using a disk because a parallel installation doesn't require physically moving disks between systems. However, whether the NT boot partition is FAT or NTFS, you must boot from NT to edit Registry data because you have to use an NT Registry editor to edit Registry data, which is impossible from outside NT. Unfortunately, no one has developed an NT Registry editor that runs under a different OS, such as DOS.

After you gain access to the original installation's Registry hive files, you're ready to begin offline editing. Although you're probably familiar with NT's Registry editors, you might not know that you can use them to open Registry hive files on other NT installations or alternate Registry sets from the same installation. To edit Registry hive files offline, open regedt32.exe (regedit.exe doesn't support loading native Registry hive files offline), highlight the HKEY\_LOCAL\_MACHINE root key, and select the Load Hive option in the Registry menu to locate the hive file you want to bring into the Registry editor. In this case, you want to change a service or driver's startup type, and NT stores this information in the SYSTEM hive. After you locate and select the file, the system will prompt you to provide a key name for the hive file contents, as Screen 2 shows. This activity doesn't modify the original hive file's name, nor does it permanently affect the Registry of the local installation you're booted under. In addition, the name you choose doesn't matter because the Registry editor will use the name only as a temporary Registry branch that contains the data of the original Registry hive file. After you provide a key name, it will appear in the HKEY\_LOCAL\_MACHINE window.

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)



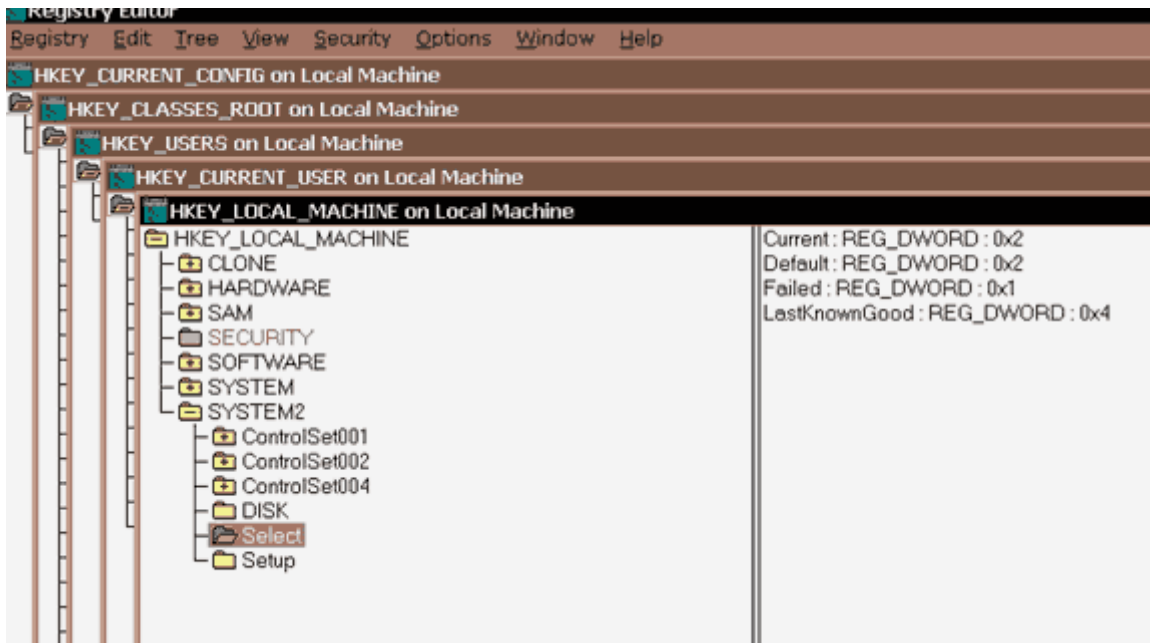
At this point, you're editing the SYSTEM hive from your original NT installation, and you can resolve your startup failure. As with any Registry editing session, back up the hive file you're working with before you edit. When you open your new key, SYSTEM2 in my example, the display is slightly different from what you usually see under the SYSTEM key. Most notably, the only ControlSet subkeys available are ControlSetxxx keys, where xxx is a number such as 001. The display doesn't exhibit the CurrentControlSet subkey that you usually see when editing the live Registry of a local machine. The display doesn't show CurrentControlSet because it's an alias for the control set that loaded when NT booted.

To ensure you're editing the correct control set and not the default control set of the parallel NT installation, choose the Select subkey under your newly created key. The right pane of the Registry editor will display several values, as Screen 3 shows. NT uses the values and their data to determine which control set is the default set loaded at startup, which value is the CurrentControlSet value, which data represents the Last Known Good configuration, and which set has failed to boot successfully. In Screen 3, the Current value tells you the last control set NT used during startup. This value represents the control set NT is using as the CurrentControlSet entry. In most cases, this value matches the default value. In my example, the data contained in Current is 0\*2, which tells you that ControlSet002 is the set you want to edit. After you locate the correct control set, you can modify your service or driver startup state.

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)



The Registry entries related to your original NT installation's services and drivers are under the HKEY\_LOCAL\_MACHINE\SYSTEM2\ControlSet00x\Services\name of suspect service or device driver Registry key. In this key, SYSTEM2 refers to the subkey in my example, ControlSet00x reflects the control set you previously determined, and name of suspect service or device driver is the name of the service or device driver that you suspect is causing your problem. Each service and driver that the Services subkey lists stores several values within its root key name, including a Start value (i.e., REG\_DWORD value). This value's number determines the current startup state of that service or device driver. Setting the Start value to 0\*4 disables a service or driver and prevents NT from attempting to start it during the boot process. Table 1, page 88, lists the possible Start key values for services and device drivers. After you finish editing your Registry offline, you must unload the imported hive file. To do so, highlight the key name you assigned to the hive and select Unload Hive from the Registry menu.

TABLE 1: Service and Device Driver Startup Values

Startup Type	Device Value (hexadecimal)	Service Value (hexadecimal)
Boot	0x0	N/A
System	0x1	N/A
Automatic	0x2	0x2
Manual	0x3	0x3
Disabled	0x4	0x4

Now that you can disable services and device drivers in your original installation, you can successfully disable the offending element that is preventing NT from booting successfully. Determining which service or driver is the culprit might take experimentation, but you can use the events that lead up to the problem and information that the STOP error screen provides to help isolate and disable the problematic component.

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

## Recovery Software

A discussion of NT system recovery isn't complete without mentioning third-party utilities that can assist you in this process. Winternals Software's ERD Commander and Remote Recover, and Systems Internals' NTRRecover are excellent products from the premier makers of NT recovery software. Although each of these utilities can help you recover a damaged NT system, they differ in their methodologies and strengths. For example, NTRRecover, Systems Internals' original NT recovery utility, lets you access the hard disk of an unstable NT system by connecting a serial cable between the damaged system and a working NT system. After they're connected, you can use NTRRecover to copy and delete files, or run Chkdsk or virus scan utilities on the remote disk. In most situations, NTRRecover provides all the functionality required to successfully recover an unbootable system.

ERD Commander is a dream come true for NT administrators who long for the days of booting DOS disks to recover wayward DOS and Windows 95 installations. This command-line-based utility boots from a 3.5" disk and can read and write to NTFS volumes. Screen 4 shows ERD Commander's interface. The Professional Edition of this utility includes several enhanced features, such as support for fault-tolerant disk sets (i.e., disk sets using NT's fdisk.sys driver), the ability to run Chkdsk, password recovery, support for FAT32 volumes, support for the Expand utility, and command-line options that let you selectively control or disable the startup state of services and drivers.

```
Microsoft (R) Windows NT (TM) Version 4.0
1 System Processor [128 MB Memory]

ERD Commander V1.0
Copyright (C) 1998 Winternals Software LLC

http://www.winternals.com

Drive letter mappings:
A: \Device\Floppy0\
C: \Device\Harddisk0\Partition1\ WINDOWS FAT 1015744 KB
D: \Device\Harddisk0\Partition2\ WINNT NTFS 205600 KB
E: \Device\Harddisk0\Partition3\ SRC FAT 870640 KB
F: \Device\Harddisk0\Partition4\ TEST NTFS 20128 KB
G: \Device\Cdrom0\ CDFS

C:\>
```

Remote Recover is the newest Winternals recovery-utility product. This utility provides a custom boot disk that includes Network driver interface specification (NDIS 2) driver support to let you remotely access an unstartable system's NTFS volumes over the network. This support lets Remote Recover remotely access the system and perform recovery functions similar to NTRRecover and ERD Commander.

## Don't Rule Out Hardware

Making assumptions about server disaster recovery is dangerous. For example, when you're dealing with a blue-screened NT installation, assuming that the problem is software-related is easy. However, defective hardware or hardware-related events (e.g., a failing hard disk or disk controller, bad main memory or cache RAM, overly aggressive BIOS performance settings) might be the culprit. By displaying STOP codes that don't indicate hardware as the problem's source, hardware-related blue screens sometimes masquerade as software-related failures.

Hardware-related problems are especially suspect if you have recently changed hardware or a power-related event has occurred (e.g., a full outage or series of voltage sags or spikes). For example, suppose you installed a new fax board in your server last week, and the fax board worked fine during

# Recovering from NT Startup Failures

Sean Daily

(Reprinted from WindowsItPro Magazine)

your testing. However, a week later, the server blue screens and the STOP error message doesn't point you to a particular service, driver, or hardware component. The malefactor might be a hardware-related problem with the fax board or the interaction with its driver that occurs only under a heavy traffic load. In a situation like this one, assuming that NT has become damaged is easy. However, if you're fighting a hardware battle with software weapons (e.g., restoring the Registry, reinstalling NT), you might end up chasing your tail for a long time.

## Be Proactive

In part 1 and in this article, I've shown you advanced techniques and utilities that you can employ in emergency situations in which an NT system refuses to boot. More important, I've discussed proactive measures that you can take now to increase your chances of performing a successful system recovery as well as reduce the amount of time that a recovery operation will take. Microsoft's documentation covers traditional recovery techniques, such as using NT Setup Repair and restoring the Last Known Good configuration, but these measures often prove insufficient. If you perform proactive disaster preparation measures, you might never have to use Microsoft's recovery techniques.