

# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

In Windows 2000, Microsoft introduces an enormous number of long-overdue features and capabilities. However, regardless of the new benefits available to administrators and users, the introduction of a new OS version inevitably presents at least one major disadvantage: It renders obsolete many of the skills, techniques, and tools that network administrators have developed for day-to-day OS maintenance.

Consider system recovery. I won't even ponder the mass deployment of a new OS on my network until I've mastered the basics of fixing the system when things go wrong. My reasons for this approach are simple. First, no OS is crash-proof or corruption-proof (not yet, anyway). Second, a large-scale deployment of any OS necessarily translates to a commensurately large-scale dependence on the availability of that system—particularly in the case of servers.

If your organization depends on Win2K, you need to know how to fix your Win2K systems when they break. Although Microsoft has greatly improved system reliability and recoverability in Win2K, things still can and do go wrong. When they do, you don't want to be unprepared. In Win2K, Microsoft offers new tools to help you in your efforts.

## New Recovery Tools

In terms of performance, reliability, and scalability, Windows NT has maintained a long-standing superiority over the Windows 9x and Windows 3.x branch of the Microsoft family tree. However, Win9x has always dominated NT in at least one area: ease of recoverability. Anyone who has spent time as an administrator on Win9x systems has probably longed for the good old days of booting to MS-DOS (or MS-DOS mode) to repair system problems such as overwritten or corrupted system files.

NT 4.0 lets you approximate some of these conveniences through techniques such as using the FAT file system on boot partitions, using third-party utilities that provide access to NTFS outside of NT (e.g., Winternals Software's NTFSDOS, ERD Commander), and using parallel OS installations. However, these methods are either logistically inconvenient or require additional setup time or expense, which can be unappealing if you're dealing with dozens, hundreds, or thousands of systems.

In Win2K, Microsoft has finally leveled the recoverability playing field by providing features that put Win2K on par with its Win9x counterparts. In addition to the internal reliability enhancements that make Win2K less prone to crashes, Microsoft has introduced several new system-recovery features that make repairing an unbootable Win2K system easier. (For more information about Win2K reliability enhancements, see Mark Russinovich, NT Internals "Inside Win2K Reliability Enhancements," parts 1 through 3, August through October 1999.) For example, Win2K lets you boot into safe modes of operation in a manner similar to that of Win9x. And, like Win9x, Win2K offers additional boot-time choices that let you disable certain OS features so that you can successfully boot the system. To access most of these choices, you press F8 on the Win2K Boot Loader menu at startup. Pressing F8 displays a menu, which Figure 1 shows, of the following alternative safe-boot options:

- Safe Mode boots with the minimal set of drivers and services necessary to start Win2K.
- Safe Mode with Networking is similar to Safe Mode but adds drivers and services necessary to enable networking.
- Safe Mode with Command Prompt is similar to Safe Mode, but the system starts with a Command Prompt window instead of Windows Explorer.

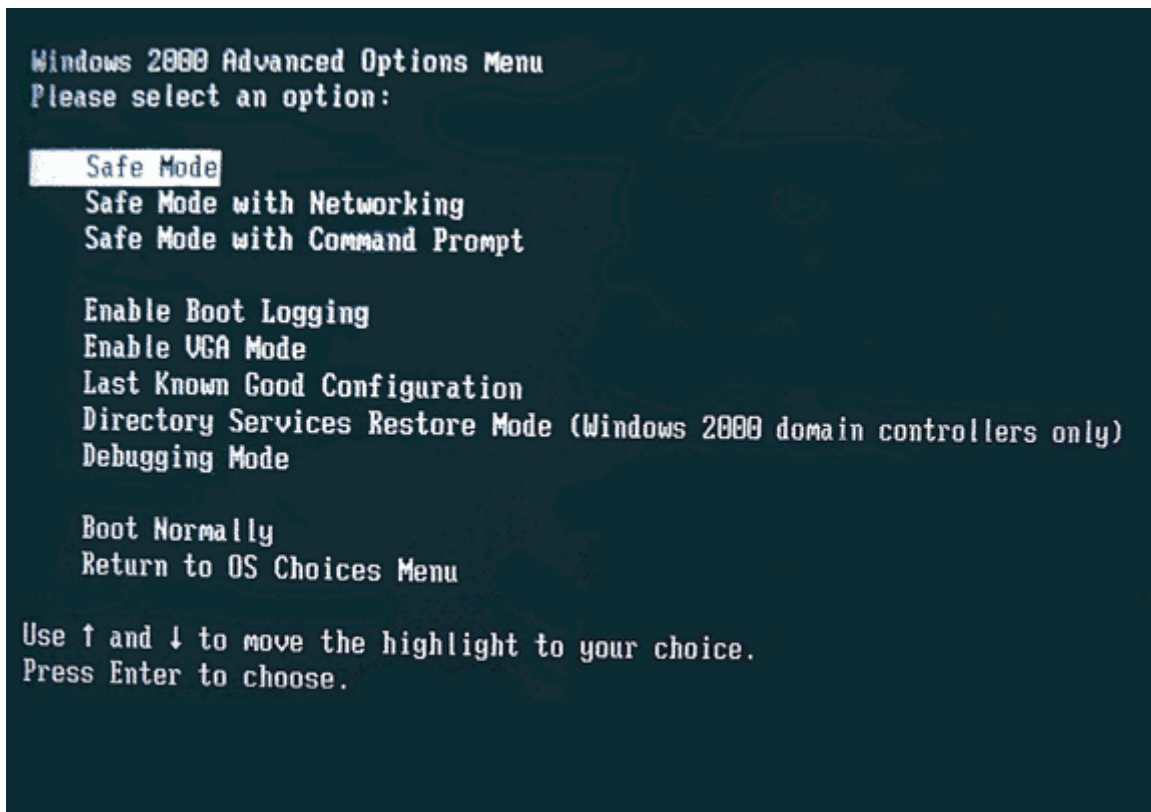
# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

- Enable Boot Logging creates an extended log file of success events and failure events for the initialization of system components as they load during system boot. (This behavior is the default for all safe-boot options except for the Last Known Good Configuration boot.) The log file is named ntbtdlog.txt and resides in the %windir% folder (e.g., C:\winnt).
- Enable VGA Mode starts Win2K in VGA mode by using the vga.sys driver instead of the regular video driver.
- Last Known Good Configuration starts Win2K by using a previous version of the SYSTEM Registry hive. (The Last Known Good Configuration is the most recent session in which a successful startup—one without any service or driver-initialization failures—and logon to the computer occurred.)
- Directory Services Restore Mode recovers the Active Directory (AD) database. This option is valid only for Win2K domain controllers.
- Debugging Mode enables a startup mode in which the system sends debugging information across a serial cable to another computer running a debugger. (The mode uses COM2 as the debugging port.)

One of these options might be appropriate at any given time, depending on the type of problem you're experiencing with a system. However, although Win2K's new safe-boot options enhance your ability to diagnose and recover a malfunctioning system, you won't find Win2K's most versatile boot option on this menu.



# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

## RC to the Rescue

Microsoft has introduced in Win2K a new startup mode called the Recovery Console (RC). For every NT administrator who has wanted to boot to a command prompt to perform system-recovery operations on NTFS-based computers, the RC is the answer. After you install the RC, you can boot to a special slimmed-down Win2K console session that provides access to all FAT16, FAT32, and NTFS disk partitions on the system, as well as a basic set of commands and utilities for performing system-recovery operations. (If you're familiar with NTFSDOS and ERD Commander—as well as Winternals Software's NTRecover and Remote Recover—you might recognize these capabilities because these products provide similar functionality for NT 4.0.)

To use the RC on a Win2K system, you must first install it by rerunning Win2K Setup (i.e., winnt32.exe) on the system with a /cmdcons switch (e.g., D:\i386\winnt32 /cmdcons). Win2K informs you that this action will install the RC and asks you whether you want to continue, as Figure 2 shows. After you click OK, the system copies the necessary files (typically, less than 6MB of data) to a hidden folder named \cmdcons, which resides off the root of your system's boot drive (e.g., C:\cmdcons). The next time you boot, your Win2K Boot Loader menu will contain a new Microsoft Windows 2000 Recovery Console option.



When you select this boot option, Win2K gives you a brief opportunity to press F6 to load a third-party SCSI or RAID driver. (This option is necessary if the RC can't properly detect your disk controller configuration.) Next, the system enters a text-based mode and prompts you for a Win2K installation to log on to, as Figure 3 shows. This feature lets the RC support the recovery of multiple OS installations on a multiboot system. After you select the Win2K installation you want to access, the system prompts you for that installation's administrative password. (This password is the local administrator account password for that installation, not the do-main administrator account password—assuming a domain membership exists.)

# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

```
Microsoft Windows 2000(TM) Recovery Console.  
The Recovery Console provides system repair and recovery functionality.  
Type EXIT to quit the Recovery Console and restart the computer.  
  
1: C:\WINNT  
  
Which Windows 2000 installation would you like to log onto  
(To cancel, press ENTER)? 1  
Type the Administrator password: *****  
C:\WINNT>
```

Although you'll probably want to install a hard-disk-based copy of the RC on each of your crucial systems, you can also start the RC from Win2K Setup's Repair menu. Thus, you can also access RC after you run Win2K Setup from CD-ROM or 3.5" disks. This capability is helpful if you're having problems with a Win2K system that has a damaged RC installation—or never had one to begin with.

## Recovery Feats

The RC is extremely handy when Win2K won't boot and you need quick access to the file system so that you can diagnose and repair the problem. Because the RC provides direct access to the file system and a host of low-level commands and utilities, it lets you perform some amazing recovery feats. The RC simplifies many of the NT recovery procedures I discussed in "Recovering from NT Startup Failures," parts 1 and 2, September and November 1999.

Although most users won't look forward to an opportunity to use the RC, it's an important tool to understand. Identifying likely causes of system startup problems before they happen—and understanding the steps necessary to correct them—is also important. Therefore, I've compiled a list of the most common software-related causes of Win2K and NT startup failures, based on my experiences recovering failed Win2K and NT systems:

- Corruption or deletion of a crucial system file (e.g., Registry hive files, ntoskrnl.exe, ntdetect.com, hal.dll, boot.ini)
- Installation of an incompatible or faulty service or driver, or the corruption or deletion of a crucial service or driver
- Disk or file-system damage or corruption, including damage to directory structures, the Master Boot Record (MBR), and the Win2K or NT boot sector

# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

- Invalid Registry data (e.g., the Registry is physically intact but contains logically erroneous data, such as out-of-range data in a service- or driver-related Registry value)
- Incorrect or overly restrictive permissions on the `%systemroot%` (e.g., `C:\winnt`) folder

Although this list is by no means comprehensive, it covers the majority of situations that cause Win2K and NT 4.0 startup failures. Using the RC or a Safe Mode boot, you can correct the majority of these problems. Table 1 lists the most common system startup problems and recommended methods for tackling them in Win2K.

TABLE 1: Recovery Procedures for Common Win2K Problems	
Symptom	Potential Recovery Procedures
Invalid or deleted boot.ini file	Use the RC's Copy command or the Win2K Setup Repair menu's Inspect Startup Environment option to replace with a healthy version of boot.ini.
Overwritten or damaged MBR	Use the RC's Fixmbr command.
Overwritten or damaged Win2K boot sector	Use the RC's Fixboot command or the Win2K Setup Repair menu's Inspect Startup Environment option.
Boot failure caused by damaged files or invalid file versions	Use the RC's Ren, Del, and Copy commands to restore working copies of files, or use the Win2K Setup Repair menu's Verify Windows 2000 System Files option.
Boot failure caused by damaged or invalid Registry settings	First, try the Safe Mode boot option. Second, try the Last Known Good Configuration boot option. Third, try the Win2K Setup Fast or Manual Repair options. Fourth, use the RC's Copy command to restore known-good Registry files to the <code>%systemroot%\system32\config</code> folder. (Note: If the problem is related to the settings for a specific service or driver, you might also be able to use the RC's Disable command to disable the offending service or driver.)
Boot failure caused by video display driver problem	Use the Safe Mode or Enable VGA Mode boot option, and repair or replace the driver.
Boot failure caused by service or driver initialization	First, use the Safe Mode boot option. Second, use the RC's Listsvc and Disable commands to identify and disable the offending service or driver. Third, use the Last Known Good Configuration boot option. Fourth, use the Win2K Setup Repair option or the RC's Copy command to restore a working copy of the Registry.
Boot failure caused by invalid file attributes set on system files or folders	Use the RC's Attrib command to restore the correct attributes.
Boot failure caused by disk or file-system corruption	Use the RC's Chkdsk command to repair the disk. (Note: Additional action might be necessary to fully recover the system.)
Boot failure caused by unknown system startup event	Use the Safe Mode or Enable Boot Logging boot option and the RC's Type command on the resulting log file to identify the failed initialization event.

# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

To demonstrate the potential usefulness of the RC in these situations, imagine a scenario in which one or more Registry hive files have become corrupted on a computer that uses an NTFS-formatted system volume. In my articles about startup failure recovery, I discussed several alternative methods for dealing with such a situation in NT. For example, you can copy a known-good set of Registry hive files by using a third-party utility (e.g., ERD Commander for NT 4.0) that allows write access to NTFS volumes, or you can use a parallel installation of Win2K or NT. (The Win2K Setup Repair process is also an option, although it doesn't offer the flexibility of the other methods.) In Win2K, you can easily boot to an RC console and copy and replace Registry hive files (or other crucial system files) that have become damaged or overwritten. In my scenario, you would simply log on to the desired Win2K installation and use the RC's Copy command to copy the necessary files.

You can also use the RC to resolve problems that underlying disk or file-system corruption causes. The RC includes several commands that can help you repair a damaged disk outside of Win2K. One such command is the Chkdsk command, which is similar to the Win9x and DOS command of the same name. Two other helpful disk-repair commands are Fixmbr and Fixboot. Like Win9x's Fdisk /mbr command, Fixmbr replaces the primary system disk's MBR with a clean copy—a feature that can resolve problems in which the MBR has become damaged or infected with a virus. The equally useful Fixboot command lets you repair the Win2K boot sector if it becomes damaged or overwritten during the installation of another OS (a situation resulting in the loss of the Win2K Boot Loader at startup).

Another nice inclusion in the RC is Diskpart, a disk-management utility similar to the one that Win2K Setup provides. You can use Diskpart to perform basic disk-management tasks such as adding and deleting partitions.

The RC console provides several other potentially useful commands. For example, Listsvc, Disable, and Enable let you list, disable, and enable (respectively) system services and drivers. These commands are invaluable if a faulty service or driver is at the heart of a system startup problem. Using an RC session, you can simply disable the offending service or driver, then reboot the system—no Registry editing or restores are necessary.

Because the RC exposes both Win2K and NT installation folders on dual-boot systems, users of such systems might find it useful as a recovery tool for failed NT installations. Although several Microsoft articles warn against this usage, they offer no explanations to justify this warning. When I've used the RC to run various commands on NT 4.0 installations, I've experienced no problems. Most of the RC's commands are file-system-related and therefore work fine on an NTFS5 volume shared between Win2K and NT. (You must install Service Pack 4—SP4—or later on NT to support NTFS5.) However, if you use the Win2K RC to recover an NT installation, you'll be on your own as far as Microsoft is concerned.

## Can You Toss Your Old Tools?

Considering the RC's features and capabilities, you might be wondering whether you can toss out your NT 4.0 system-recovery tools and techniques. After all, with such a powerful tool at your disposal, are third-party utilities and parallel recovery installations still necessary? Before you start trashing disks and changing your disaster-preparedness procedures, you need to understand the RC's limitations.

First, the RC can solve the majority of, but not all, system startup failures. In some situations, the RC alone might not be enough to recover a failed system—for example, when overly restrictive permissions settings on the Win2K installation folder cause a startup failure. Because the RC doesn't provide a command that lets you edit file or folder permissions on a volume, you'll need to reset the

# Mastering the Recovery Console

Sean Daily

(Reprinted from WindowsItPro Magazine)

permissions manually under a parallel Win2K installation or with a third-party utility. At least one third-party tool, ERD Commander, includes a permissions-reset feature.

Also, because the RC provides only a limited command-line-based environment, it won't let you run your GUI-based backup application to access and restore data. If you're unable to boot your primary Win2K installation and you need to restore data (e.g., from a tape backup) to complete the recovery process, you'll still want to have a parallel installation available that lets you restore the system's previous state.

Finally, you might encounter circumstances in which the RC becomes inaccessible. For example, if damage preventing the primary Win2K installation from booting also affects the RC installation, you might need to use one of the aforementioned alternative methods to access and recover the primary installation.

Another practice that you shouldn't ignore is regularly updating the Emergency Repair Disk (ERD) for each of your Win2K systems. Even under Win2K, ERDs are a valuable system-recovery tool. Like an NT ERD, a Win2K ERD can help the Setup Repair process locate a Win2K installation folder and provides a known-good backup copy of the Registry. If you don't like the idea of using Win2K's backup utility (the new tool for creating and updating ERDs) to manually update ERDs on all your systems, you might want to consider using a utility such as Aelita Software Group's ERDisk 5.0. This tool lets you create remote Win2K ERD backups across the network for multiple machines and also provides remote-recovery features.

You need to be aware of a few RC bugs and gotchas. One nasty limitation is that you can't install the RC on a software-based mirror/RAID1 volume (i.e., a volume that you created with NT's Disk Administrator or Win2K's logical disk manager, not a hardware RAID controller). In terms of partition-configuration requirements, the RC installation uses rules similar to Win2K's setup rules. As with regular OS installations, you can work around this problem by breaking the mirror, installing the RC, then reestablishing the mirror.

However, another gotcha presents itself: Win2K won't let you establish mirrored volumes on basic disks—only on dynamic disks. Therefore, if you have a basic disk mirror volume and want to install the RC, you'll need to convert the disk from basic to dynamic. Another ugly glitch is that, as of this writing, the RC fails to run if you convert its host FAT16 or FAT32 volume to NTFS. This situation's solution is to reinstall the RC, using the same procedure you used initially to install it.

## Prepare for the Worst

Microsoft's introduction of safe-mode booting, the RC, and other Win2K system-recovery features is an important and necessary step in NT's evolution. The RC, in particular, is a powerful yet simple built-in tool that lets you resolve most of the problems that cause system boot failures. For more information about these recovery tools, see "Win2K Recovery Resources."

Remember that you can prepare your system for disaster by installing the RC on each of your important Win2K systems and performing frequent ERD updates. By doing so, you'll significantly improve your chances of achieving a quick and painless recovery in the event of a disaster.