

The Recovery Console

Kathy Ivens

(Reprinted from WindowsItPro Magazine)

Finally, Microsoft has provided a useful, uncomplicated OS repair tool that actually works. The Windows 2000 Recovery Console (RC) provides a command-line interface that you can use to repair an OS installation—regardless of whether the computer is using NTFS or the FAT file system. You can launch the RC from the Win2K CD-ROM on an as-needed basis, or you can preinstall the utility as a safeguard. You can use the RC to stop and start services, read and write data on a local hard disk, copy data from a 3.5" disk or CD-ROM, and perform other command-line tasks. For example, if a system file on your hard disk has been corrupted or deleted, you can overwrite the file with a new copy from the Win2K CD-ROM.

Launching the RC

If the OS won't load on a system and you haven't preinstalled the RC on the affected computer, you can launch the tool from the Win2K CD-ROM. If the computer can't boot from a CD-ROM, you can use the Win2K setup disks. (If you can't find or didn't previously create setup disks, collect four blank formatted 3.5" disks and label them Disk1, Disk2, Disk3, and Disk4. Insert the Win2K CD-ROM into a working system's CD-ROM drive, and put Disk1 into the disk drive. Click Start, Run. In the Open box, type

```
<d>:\bootdisk\makeboot a:
```

where d is the drive letter for the CD-ROM drive. Click OK, then follow the prompts to create the setup disks.)

Insert either the bootable CD-ROM or setup Disk1, and start the affected computer. The Win2K Setup program starts. When Setup asks whether you want to continue installing Win2K, press Enter to continue. When Setup asks whether you want to install a fresh version of Win2K or repair an existing installation, press R to respond that you want to repair your current installation. Then, press C to launch the RC.

Preinstalling the RC

I recommend that you preinstall the RC on your important servers and your IT personnel's workstations. When those computers fall victim to problems, you need to get them running quickly (and the RC requires only 7MB of disk space). Preinstalling the RC means you won't need to spend time finding the Win2K CD-ROM or stepping through the RC's setup process.

To install the tool before trouble strikes, place the Win2K CD-ROM in the CD-ROM drive. (The RC won't install on a mirrored volume. If the computer on which you're preinstalling the tool has a mirrored volume, you must first break the mirror. Install the RC, then reestablish the mirrored volume.) Choose Start, Run. In the Open box, type

```
<d>:\i386\winnt32.exe /cmdcons
```

where d is the drive letter for the CD-ROM drive. Alternatively, you can use Universal Naming Convention (UNC) to install the RC from a network share point.

The system prompts you to confirm that you want to install the RC. Click Yes to start the installation procedure. You must reboot the computer after the process is complete. Thereafter, you'll see an option for the RC on the startup menu.

If necessary, you can uninstall the RC and its menu entry. (Uninstalling the RC makes sense when any of the system's users fall into that "knows-just-enough-to-be-dangerous" category that all

The Recovery Console

Kathy Ivens

(Reprinted from WindowsItPro Magazine)

administrators dread.) Simply edit boot.ini to delete the RC line, delete the \cmdcons subdirectory from the boot partition's root directory, and delete the cmlldr file from the boot partition's root directory.

Using the RC

When you use the RC, you work at a special command prompt instead of the Win2K command prompt. The RC has its own command interpreter.

Before you can enter this command interpreter, the RC prompts you to enter the Administrator password—meaning the local Administrator, not a domain Administrator. By default, Win2K doesn't assign a local Administrator password during OS installation, and most administrators don't bother to go back to each computer and specify a password. However, if you don't assign one, any user can access the RC—a scary thought. If you preinstall the RC, be sure also to assign a local Administrator password. I recommend that you create the same password on every computer, unless you have the patience to keep track of multiple passwords.

When the RC starts, it gives you the opportunity to press F6 to install a third-party SCSI or RAID driver in case you need such a driver to access the hard disk. (This prompt works the same as the prompt that appears during installation of the OS.) Move fast; the F6 message isn't onscreen for long.

The RC takes a few seconds to boot (during this time, the screen looks similar to the screen that displays during a Windows NT boot). When the RC menu appears, it displays a numbered list of the Win2K and NT 4.0 installations on the system (usually only one entry—C:\winnt—exists). Mirrored volumes appear twice, but both entries have the same drive letter. Choose either entry; the RC will mirror any changes you make during your session. You must press a number before you press Enter, even when only one entry appears. If you press Enter without entering a number, the system reboots and you get to repeat the whole process. (This time, remember to type the number.)

When you see the prompt for %systemroot% (e.g., C:\winnt), you're ready to roll. Table 1 describes the RC's available commands. Misusing these commands can be dangerous, so this tool is no place for computer newbies. (For more information about using the RC, see Sean Daily, "Mastering the Recovery Console," July 2000, and John D. Ruley, Windows 2000 Pro, "Key Recovery Console Commands," July 2000.) When you finish making your repairs, type

exit

TABLE 1: RC Commands

Command	Sample Command	Action
Attrib		Changes attributes on one file or subdirectory.
Batch	batch <inputfile> [<outputfile>]	Executes commands that you specify in the text file <i>inputfile</i> . The file <i>output file</i> holds the output of the commands. If you omit the <i>outputfile</i> parameter, output is displayed on the screen.
Cd (Chdir)		Operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
Chkdsk	chkdsk [/p] [/r]	The /p switch runs Chkdsk even if the drive isn't flagged as dirty. The /r switch locates bad sectors and recovers readable information; this switch implies /p. Chkdsk requires Autochk. Chkdsk automatically looks for autochk.exe in the

The Recovery Console

Kathy Ivens

(Reprinted from WindowsItPro Magazine)

		startup (i.e., boot) directory. If Chkdsk can't find the file in the startup directory, it looks for the Win2K Setup CD-ROM. If Chkdsk can't find the installation CD-ROM, it prompts the user for autochk.exe's location.
Cls		Clears the screen.
Copy		Copies one file to a target location. By default, the target can't be removable media and you can't use wildcards. Copying a compressed file from the Win2K Setup CD-ROM automatically decompresses the file.
Del (Delete)		Deletes one file. Operates within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources. You can't use wildcards by default.
Dir		Displays a list of all files, including hidden and system files.
Disable	disable <service_or_driver>	Disables a Windows system service or driver. The variable <i>service_or_driver</i> is the name of the service or driver you want to disable. When you use this command to disable a service, it displays the service's original startup type before changing the type to SERVICE_DISABLED. You should note the original startup type so that you can use the Enable command to restart the service.
Diskpart	diskpart [/add /delete][<device > <drive>: <partition >] [<size>]	Manages partitions on hard disk volumes. The /add option creates a new partition; the /delete option deletes an existing partition. The variable <i>device</i> is the device name for a new partition (e.g., \device\harddisk0). The variable <i>drive</i> is the drive letter for a partition you're deleting (e.g., D); <i>partition</i> is the partition-based name for a partition you're deleting (e.g., \device\harddisk0\partition1) and can be used in place of the <i>drive</i> variable. The variable <i>size</i> is the size, in megabytes, of a new partition.
Enable	enable <service_or_driver> [<start_type>]	Enables a Windows system service or driver. The variable <i>service_or_driver</i> is the name of the service or driver you want to enable, and <i>start_type</i> is the startup type for an enabled service. The startup type uses one of the following formats: <ul style="list-style-type: none"> • SERVICE_BOOT_START • SERVICE_SYSTEM_START • SERVICE_AUTO_START • SERVICE_DEMAND_START
Exit		Quits the RC and reboots the computer.
Expand	expand <source> [/f:<filespec>] [<destination>] [/y] or expand <source> [/f:<filespec>]/d	Expands a compressed file. The variable <i>source</i> is the file you want to expand; you can't use wildcard characters by default. The variable <i>destination</i> is the directory for the new file; by default, the destination can't be removable media and can't be read-only; you can use the Attrib command to remove the read-only attribute from the destination directory. The option /f:<filespec> is required if the source contains more than one file; this option permits wildcards. The /y switch disables the overwrite confirmation prompt. The /d switch specifies that the files shouldn't be expanded and displays a directory of the files in the source.
Fixboot	fixboot [<drive>:]	Writes a new boot sector on the system partition.
Fixmbr	fixmbr [<device >]	Repairs the boot partition's master boot code. The variable <i>device</i> is an optional name that specifies the device that needs a new MBR; omit this variable when the target is the boot device.
Format	format [<drive>:] [/q] [/fs:<file-system>]	Formats a disk. The /q switch performs a quick format; the /fs switch specifies the file system.

The Recovery Console

Kathy Ivens

(Reprinted from WindowsItPro Magazine)

	[drive:]	
Help	help [<command>]	If you don't use the <i>command</i> variable to specify a command, Help lists all the commands that the RC supports.
Listsvc		Displays all available services and drivers on the computer.
Logon		Displays detected installations of Win2K and requests the local Administrator password for those installations. Use this command to move to another installation or subdirectory.
Map	map [arc]	Displays currently active device mappings. Include the arc option to specify the use of Advanced RISC Computing (ARC) paths (the format for boot.ini) instead of Win2K device paths.
Md (Mkdir)		Operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
More/Type	more [<filename>] type [<filename>]	Displays the specified text file (i.e., <i>filename</i>) on screen.
Rd (Rmdir)		Operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
Ren (Rename)		Operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources. You can't specify a new drive or path as the target.
Set		Displays and sets the RC environment variables.
Systemroot		Sets the current directory to %systemroot%.

RC Rules

Several rules take effect by default while you're working in the RC:

- AllowAllPaths = FALSE prevents access to directories and subdirectories outside the system installation that you selected when you entered the RC.
- AllowRemovableMedia = FALSE prevents access to removable media as a target for copied files.
- AllowWildCards = FALSE prevents wildcard support for commands such as Copy and Del.
- NoCopyPrompt = FALSE forces prompts for confirmation when the system overwrites an existing file.

You can use the RC's Set command to display the current rules. Remember that you're working in an independent command processor, not a Win2K session's command window. Therefore, the Set command doesn't display the same information you're used to seeing when you use the command during a Windows session.

You can enable the Set command so that you can use it to reset the rules rather than simply display the current rules. I suggest that you give yourself this power on any computer on which you've preinstalled the RC. You need to take this step before trouble strikes because it requires that you

The Recovery Console

Kathy Ivens

(Reprinted from WindowsItPro Magazine)

change the computer's Group Policy—and the system must be operational for you to do so. After you enable the Set command to let you change the rules, you can change the rules at any time from within the RC.

In a Windows session, click Start, Run. In the Open box, type

```
mmc
```

to open a new Microsoft Management Console (MMC) console. In the Console1 dialog box, choose Console, Add/Remove Snap-in from the menu bar. Click Add to open an Add Standalone Snap-in dialog box. In that dialog box, select Group Policy and click Add. In the resulting Select Group Policy Object dialog box, choose Local Computer and click Finish. In the Add Standalone Snap-in dialog box, click Close. In the Add/Remove Snap-in dialog box, click OK.

In the console, expand the Local Computer Policy object and navigate to Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options. The right pane will display the local security policies. Double-click the policy Recovery Console: Allow floppy copy and access to all drives and folders. Select Enabled and click OK. Close and save the MMC console (you can then access the console from the Administrative Tools menu if you want to make changes later).

You can also set the policy to permit automatic administrative access to the RC, but doing so creates a computer that you could rename "a disaster waiting to happen." You might entrust this power to certain users on certain computers, but requiring a password instead of providing automatic access is safer.

Incidentally, if you or another administrator configure any policy for the domain, that configuration overrides any policy you set for the local computer. (Setting a domain policy for the RC would be unusual, however.)

After you change the security policy for the RC, you can change the rules when you're working in the RC. To do so, use the Set command with the following syntax:

```
set <rule> = <parameter>
```

For example, to allow access to all the directories on the computer, type

```
set AllowAllPaths = TRUE
```

A Genuine Must-Have

The RC is unbelievably useful for many reasons. First, this built-in tool replaces the third-party utilities that we needed to buy and learn to use to repair previous versions of Windows.

Second, the RC provides access to the original CD-ROM's system files. This access can help you overcome system corruption. Third, the tool's ability to repair the Master Boot Record (MBR) can help you rescue your system from viruses. You won't need to prepare special boot disks for NTFS systems. Fourth, the ability to stop and start services gives the RC far more power than any other built-in Windows repair tool. In short, the RC is an administrative necessity.