Inside The Windows 2000 Registry

As the Registry grows in size and importance, administrators and support personal are discovering that it pays to have more than a passing knowledge of the subject.

By Dave Cook

All operating systems need a method for keeping track of hardware and software parameters and initialisation files. In the days of 16-bit Windows, third-party software developers and even Microsoft itself stored important configuration information in .INI files. Microsoft used WIN.INI and SYSTEM.INI to hold specific information, while third-party vendors often created their own .INI files, either in the Windows directory or in the application's home directory.

Sensibly, Microsoft changed this in later versions of Windows when the information was rounded up and kept together more or less in one place. Thus, the Registry was born. While the Registry has been a major part of Windows since Windows 95, it has expanded considerably in Windows 2000. Even so, some programs continue to use .INI files in which to save settings. Windows 2000 supports these files to maintain backward compatibility with older applications.

The Windows 2000 Registry contains a mass of settings and configurations, including profiles for each user of the computer, information about system hardware, programs, and property settings. Consequently, a computer equipped with a full set of peripherals and only an average amount of software could easily sport a Registry of 15 MB or more in size.

Discovering the size of a Windows 2000 Registry is easy. Choose Start, Settings, Control Panel, and click System. Click the Advanced Tab in the System Properties dialog box, and then select Performance Options. In the Virtual Memory section, click Change. The current size of the Registry can be seen in the lower portion of the Virtual Memory dialog box (Figure 1). Note that it is also possible to set a Maximum Registry value setting from here.

Hives

Like the Windows NT Registry, the Windows 2000 Registry is not simply one large file but a set of discrete files that are known as hives. Each hive contains a Registry tree, with a key that serves a root of the tree. Subkeys and their values reside beneath the root. Most hives are stored in the c:\winnt\System32\Config folder, while for each user profile there is also a hive in the c:\winnt\Profiles\username folder with the name Ntuser.dat. A hive that corresponds to a particular segment of the Registry also consists of a number of associated files, each sharing the same main filename but with a different file extension.

The majority of hives are keys made up of permanent components of the Registry. However, some hives are volatile and do not have associated files. The system creates these volatile hives every time it boots. A typical example of a volatile hive is the HKEY_LOCAL_MACHINE\Hardware hive, which stores information relating to the computer's hardware and device assigned resources. Making this hive volatile makes sense because hardware detection and resource assignment naturally take place each time the system boots.

When it comes to storing the various credentials for users, groups and computers, standalone Windows 2000 machines store information in three Registry-based security databases: Builtin, Security Accounts Manager (SAM), and LSA. Note that Windows 2000 domain controllers store security information in the Active Directory.

The Builtin database is part of the SAM Registry hive in the HKEY_LOCAL_MA-

CHINE subtree. It contains the two default user accounts, Administrator and Guest, along with various default groups. The SAM database is contained in the SAM Registry hive, and contains classic NT user and group accounts created after the initial installation of Windows 2000. Finally, the LSA database contains system policies, password rules, and trust accounts for the computer. It is stored in the Security Registry hive, also under the HKEY_LOCAL_MACHINE subtree.

The Registry consists of five subtrees, each beginning with the word HKEY. When viewed from one of Microsoft's purpose-built Registry editors (Figure 2), subtrees are displayed in the left pane window along with a brief description of their use. The five subtrees are as follows:

- HKEY_LOCAL_MACHINE holds information about the local computer, such as hardware settings, operating system features and startup control data.
- HKEY_USERS contains all of the actively loaded user profiles including those found in HKEY_CURRENT_USER and the default Admins profile.
- HKEY_CURRENT_CONFIG contains information about the hardware profile used by the local computer at system startup.
- HKEY_CLASSES_ROOT contains the associations between applications and file types. It is a subkey of HKEY_LOCAL_MACHINE\Software. The information stored here ensures that the correct program opens when users open a file with Windows Explorer.
- Finally, HKEY_CURRENT_USER stores the user profile for the user currently logged on, as well as environmental variables, application preferences, desktop settings and so on.

Each of the five subtrees accommodates individual keys, with each key responsible for holding certain kinds of information. Some keys hold data, while others hold subkeys. Subkeys can also hold additional subkeys. When using a Registry editor, users can expand and navigate the left pane of Registry window much like they would expand and navigate folders in Windows Explorer. The contents of a key, otherwise known as value entries, are displayed to the right in the details pane. A value entry has three parts: name, data type, and value. Name defines the values contained by a key. Data Type tetermines the type of data allowed in a value and could be in one of three forms: string value (text), binary value (hexadecimal), and the DWORD value (consisting of four 8-bit bytes). Value is the data associated with a name.

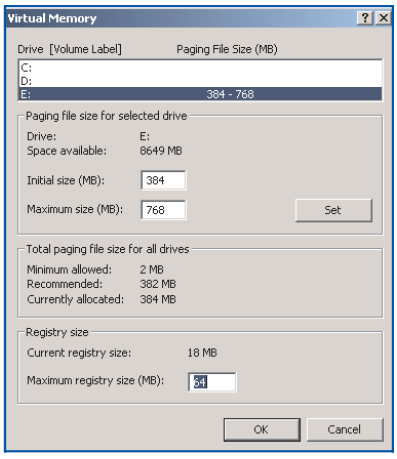

Figure 1 - The Virtual Memory dialog box, showing the current size of the Registry.

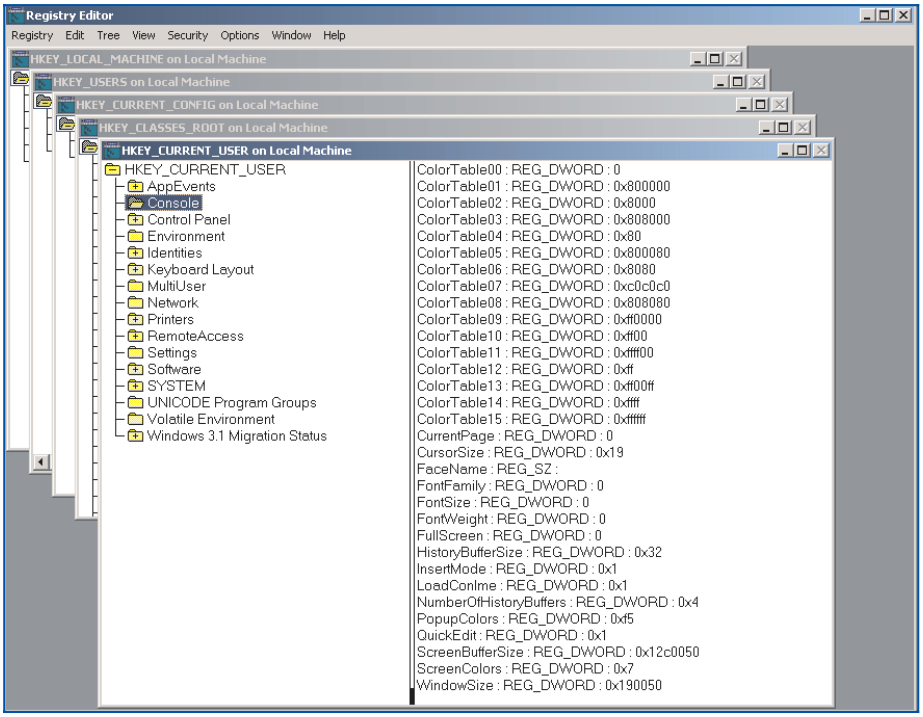

Figure 2 - The five subtrees as seen from Regedt32.exe, with the HKEY_CURRENT_USER\Console key selected.

Editors

Windows 2000 provides two editors for editing the Registry: Regedit.exe and Regedt32.exe. Regedit.exe (Figure 3) is included primarily for its search capability and is automatically installed in the (WINNT) Systemroot folder. While Regedit.exe can be used to make changes in the Registry, its big brother, Regedt32.exe, should be regarded as the preferred editor since it supports several features that Regedit.exe does not. Most of these features can be found on the Security menu under Permissions, Auditing, and Ownership. Regedt32.exe is automatically installed in the Systemroot\System32 folder.

To open Regedt32.exe, click Start, and then Run. In the Open text box, type REGEDT32.EXE and click OK. This opens the 32-bit Windows 2000 Registry editor. Users not familiar with the workings of the Registry should at first view the Registry in read-only mode, thereby avoiding any inadvertent changes. To place the editor in read-only mode, open the editor and click the Options menu, then select Read Only Mode.

Moving around the Registry is fairly straightforward, if a little laborious. Note that Regedt32.exe uses a different set of conventions to Regedit.exe. The former provides a multiple document interface that permits users to see more than one window at a time. A variety of tools are provided to help users unload hives, restore keys and suchlike. There is also a handy Bookmark feature that enables users to return quickly to a key that has been bookmarked via the Favorites menu. Regedit.exe provides a less cluttered view than Regedt32.exe, but it is not as powerful. It is, however, particularly useful when searching for keys, values and data.

Permissions

The ability to make changes to the Registry using Regedit.exe or Regedt32.exe depends on a user's access permissions. For example, users belonging to the Administrators group can view the Registry of remote computers by using the Select Computer option on the Registry menu. In general, users can make the same kinds of changes with the editors as their permissions allow for other administrative tools.

So administrators - or the owner - of a Registry key can specify which users and groups have access to open that particular key, while retaining the right to add or remove users or groups from the authorised list at any time. Administrators can also use Group Policy to restrict the use of the editors for users who do not need access to the Registry. This is usually a much better solution than simply removing Regedit.exe and Regedt32.exe from the computer.

To assign permissions to a Registry key, first select the key. Then on the Security menu, click Permissions, and highlight the user or group in the Security window. Access levels can be assigned to the selected key as follows:

- To grant the user permission to read the key contents but not to save any changes made to the file, select Read in the Allow check box.
- To grant the user permission to open, edit, and take ownership of the selected key, select Full Control in the Allow check box.
- To grant the user special permission in the selected key, click Advanced.

In cases where it is a requirement that inheritable permissions assigned to the parent key must also apply to the subkey, select the "Allow inheritable permissions from parent to propagate to this object" check box, found in the lower left portion of the Access Control Settings dialog box (Figure 4).

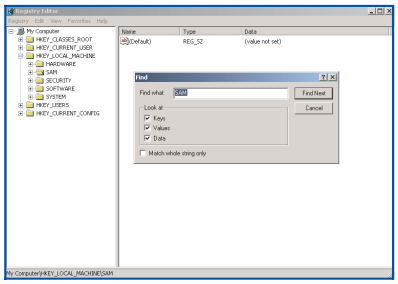

Figure 3 - Regedit.exe is used primarily for its search capabilities.

Last Known Good

Back in the early days, many administrators thought that grappling with the Windows Registry was akin to learning the black arts. But with so many third-party software developers now using the Registry to store preferences and settings, it is growing increasingly common for administrators and support users to find themselves delving into the Registry to fine-tune the system, to generally keep it running smoothly and free from errors. This is hardly surprising. The simple fact is that the Registry provides users with a tremendous amount of power in configuring the system.

On occasions, though, and despite the best efforts of everyone concerned, it is all too easy to end up with a corrupted Registry. This can be an unnerving experience, but it need not be the end of the world. As in Windows NT, Windows 2000 anticipates this event and maintains a backup copy of a portion of the system hive called the Control Set. This backup copy is named the Last Known Good Configuration. If a computer fails to boot and displays a message that the Registry has become corrupted, the Last Known Good Configuration will more often than not get the computer back up and running.

The Last Known Good Configuration can be accessed from Safe Mode. To gain access to Safe Mode, wait for the "Please select the Operating System to start" message after a reboot, then press the F8 key. Use the arrow keys to curser down and select the following choice: "Last Known Good Configuration". Next, press Enter and follow the onscreen prompts to restore the Registry back to a recoverable state. Note that when the Last Known Good Configuration is enabled, Windows 2000 restores the information held in Registry key HKLM\System\CurrentControlSet only. So any changes that have been made to other registry keys will remain.

Registry Console Tools

While the Last Known Good Configuration can be tremendously useful, backup administrators should never rely on it entirely to restore the Registry back to a recoverable state. Indeed, regular backups of the Registry are as important as any other type of backup. One way to make a copy of the Registry is to use the Windows 2000 Backup utility to back up the system state, but this will back up many other things as well. This is where the Windows 2000 Resource Kit comes in useful. The Resource Kit contains a number of management and support tools, including some useful Registry utilities.

These additional utilities are available from the Registry Console Tool (Reg.exe). This is a powerful command line tool, and made available to users upon installation of the Resource Kit. Note that the Windows 2000 version of Reg.exe has been substantially updated. Therefore, users using Reg.exe commands in existing batch files are advised to check the syntax in the batch file against new usage.

Be aware that the Windows 2000 Resource Kit is not installed during a default Windows installation. To install the Resource Kit, insert the Windows 2000 CD and navigate to the \Support\Tools\ folder, then run SETUP.EXE and follow the installation instructions. Once installed, backup copies of the Registry can be made while maintaining the ability to restore these files as and when necessary. This is accomplished using two command line tools: Reg Save, for creating Registry backups; and Reg Restore, for restoring Registry backups. Both tools work on individual Registry subtrees, and can backup and restore Registry files even when they are open.

Other Useful Tools

For the most part, editing with Regedit.exe and particularly Regedt32.exe will be sufficient for the needs of most users. It should be remembered, however, that the results of an incorrect edit are unpredictable and could easily impair or disable the operating system. To make matters worse, neither Regedit.exe nor Regedt32.exe is capable of spotting syntax errors or other mistakes. Again, this is where the Registry Console Tool comes in useful, because it provides users with a number of command line tools to ensure edits made to the Registry are valid. Registries can also be compared and searched for values.

A detailed listing of the commands available from the Registry Console Tool, complete with syntax and examples, can be found in the Windows 2000 Support Tools help file. The help file is installed automatically during installation of the Windows 2000 Resource Kit.

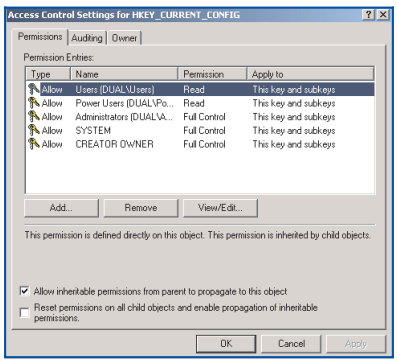

Figure 4 - Assigning inheritable permissions from the Access Control Settings dialog box.

PCSA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.