2

Common Windows 2000 Administrative Utilities

MICROSOFT WINDOWS 2000 INCLUDES SEVERAL UTILITIES TO aid system configuration and administration. These tools are accessed via the Start menu, in the Programs, Administrative Tools section. By default, the Administrative Tools menu is hidden in Windows 2000 Professional. In Windows 2000 Professional, these tools can be accessed from the Administrative Tools folder in Control Panel. This chapter takes a look at the Windows 2000 administrative tools, as well as several third-party tools that can make maintaining a Windows 2000 system a little easier.

What Administration Really Means

Keeping a Windows 2000 network functioning encompasses many activities. Such activities range from maintaining user accounts to configuring security, monitoring network traffic, correcting system problems, and enabling local and remote access. The size and complexity of a network is directly related to the number of tasks to be performed to keep it up and running.

The range of tasks required to sustain a network varies considerably from network to network. For example, all networks require managing user accounts, applying security controls, and backing up data. Some other networks may also require remote access management, performance monitoring, and error tracking.

Administration really means planning out the network, mapping out configurations, implementing decisions, and monitoring the activity of the network over time. As the network grows, you need to adjust various settings and configurations to support the

changes. You may find that your original decisions sustain a growing network adequately, or you may need to make adjustments unexpectedly. In either case, vigilance is your primary asset for sustaining the network.

To minimize downtime, you must anticipate problems that are likely to occur and correct problems when they occur. That's why it's so important to learn your system, understand your tools, and plan. Otherwise, you may find yourself working over the weekend or pulling an all-nighter to get things running smoothly again.

Administering a Windows 2000 System

Windows 2000 system administration is a task-based responsibility that requires you to rely upon the tools and utilities at your disposal. If you are unfamiliar with your tools, you cannot perform the required tasks.

Just as a handyman needs the right tool for a particular job, you need to know which tools can perform which functions. In the following sections, we walk through the administrative, management, monitoring, and related tools included with Windows 2000. In addition to reviewing the discussion in this chapter, you should take the time to work with the tools themselves. Hands-on experience is invaluable and cannot be substituted. Plus, you may want to review the online help documentation included in the tools, as well as materials from the *Windows 2000 Professional Resource Kit*, *Windows 2000 Server Resource Kit*, and TechNet (discussed in the following sidebar, "Microsoft Resources").

Microsoft Resources

In our experience, the resources that Microsoft provides are among the best for product documentation, troubleshooting information, and general, all-around information. Following are two items we cannot live without:

- **Microsoft Technical Information Network (TechNet).** A monthly CD-based publication that delivers numerous electronic titles on Windows products. Its offerings include all the Microsoft Resource Kits (see next bullet), product facts, technical notes, tools, utilities, the entire Microsoft Knowledge Base, as well as service packs, drivers, and patches. A single user license to TechNet costs $299 per year (TechNet Plus, which includes Beta versions of Microsoft products, costs $429), but it is well worth the price. For more details, visit **`www.microsoft.com/technet/`** and check out the information under the TechNet Subscription heading in the About TechNet menu entry.
- **Microsoft Resource Kits.** Available on nearly all major products from Microsoft. The *Microsoft Windows 2000 Server Resource Kit* and the *Microsoft Windows 2000 Professional Resource Kit* are essential references for Windows 2000 information. Both book sets come with CD-ROMs that contain useful tools. Visit **`mspress.microsoft.com`** for additional information on the Resource Kits. The *Windows 2000 Server Resource Kit* contains eight volumes and nearly 7,300 pages.

Additional resources that provide information about Windows 2000 are also available. For instance, a quick search at **`www.amazon.com`** using the phrase "Windows 2000" turns up a list of more than 440 additional references on this subject.

The Microsoft Management Console: Where Management Begins

When Microsoft released the Windows NT Option Pack version 4.0, it introduced a new tool known as the *Microsoft Management Console (MMC)*. Microsoft's vision was that this tool would become the *de facto* tool for administering anything and everything in future versions of Windows NT. This vision is a reality in Windows 2000.

What makes the MMC different from earlier versions of Windows NT administration tools is that the MMC itself does none of the administration. Instead, it is simply a shell into which administration tools can be added, modified, and removed. As you can see in Figure 2.1, when the MMC is launched (by running the MMC.EXE command), it brings up a blank window.

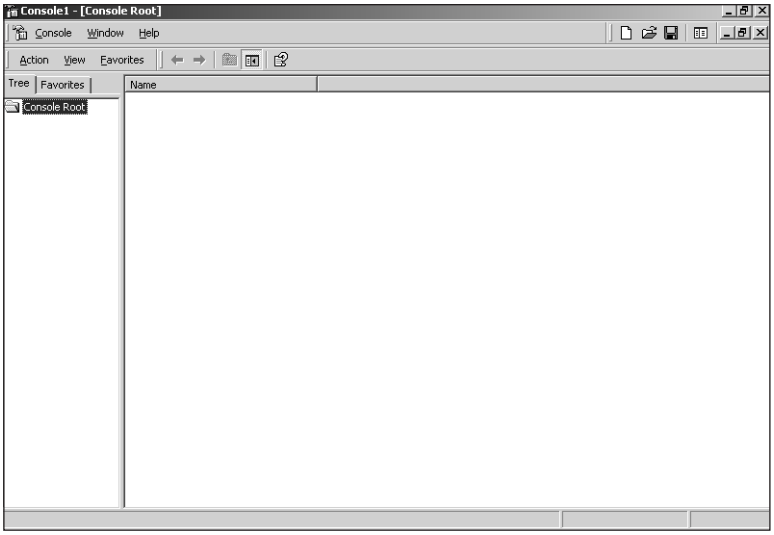

Figure 2.1 The Microsoft Management Console screen.

The administrative tools that can be added to the MMC are known as *snap-ins*. The capability to pick and choose which administrative tools a console is to have makes MMC extremely flexible, especially in an environment in which several administrators perform different tasks. Each administrator can create (or have created for him by the system administrator) an MMC that has only the tools that he requires. For example, Sue may be responsible for monitoring server performance, the Event logs, and the Domain Name Service, whereas Joe's job is to create users and groups and set security policies for each user. For example, to create Joe's MMC, follow these steps:

1. Select Start, Run, type **MMC.exe** in the field, and click OK.
2. Choose the Add/Remove Snap-In option from the Console menu and click the Add button.

3. Select the Group Policy Snap-In and click Add.
4. Select the Local Users and Groups Snap-In and click Add.
5. Click the Close button.
6. Click OK. The MMC as shown in Figure 2.2 should appear.

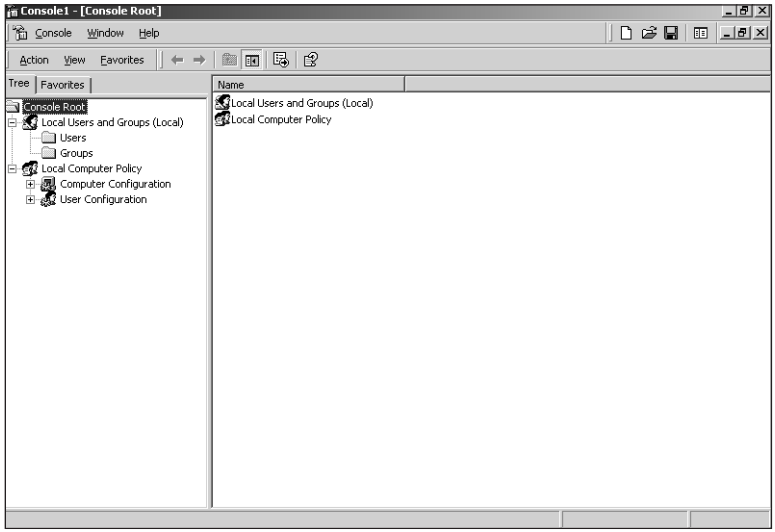

Figure 2.2 The Customized MMC.

The rest of the tools that appear in this chapter can be accessed either through their own administrative tool or by creating a custom MMC and adding their respective snap-in.

Managing Users

User management in Windows 2000 differs from that in Windows NT. With Windows NT, you used one of two tools, User Manager or User Manager for Domains. User Manager was used on either Windows NT Workstations or Windows NT standalone Servers to control user and group information, whereas User Manager for Domains was used on the domain controllers to control user and group information for the domain. The tool you use in Windows 2000 will vary depending on your configuration. In Windows NT, User Manager and User Manager for Domains were essentially the same tools, but in Windows 2000, they are radically different.

> **User Manager for Domains Under Windows 2000**
>
> Although User Manager for Domains is no longer used to create Windows 2000 users and groups, it is included with the Windows 2000 Server installations for ease of administration of Windows NT users and groups from a Windows 2000 system.

With Windows 2000, you will use either the Local Users and Groups or the Active Directory Users and Groups administrative tools. This section introduces both, but will concentrate on the Local Users and Groups tool; the Active Directory tool is discussed in detail in Chapter 5, "Active Directory Tools."

These two tools are the administration methods you can use to perform the following functions:

- Manage user accounts
- Manage groups

In Windows 2000, the Local Users and Groups administration tool is found as one of the snap-ins in the Computer Management tool (Start, Programs, Administrative Tools, Computer Management) and is shown in Figure 2.3. The tool itself is relatively simple to use and is outlined in the following sections.

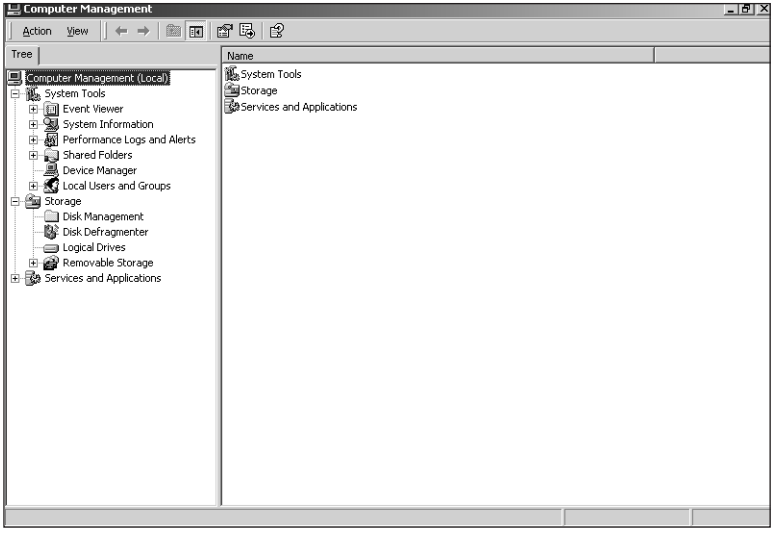

Figure 2.3 The Local Users and Groups administration tool.

Local Users and Groups is an extremely simple application. One of the nice features of this tool is the capability to create what are known as *taskpad views*. This enables you to modify the interface used by the tool to simplify configuration and creation of users. Figure 2.4 illustrates a taskpad view of the Users container. Notice that creating a user, deleting a user, renaming the user account, setting the password, and viewing the user's properties are now simple buttons.

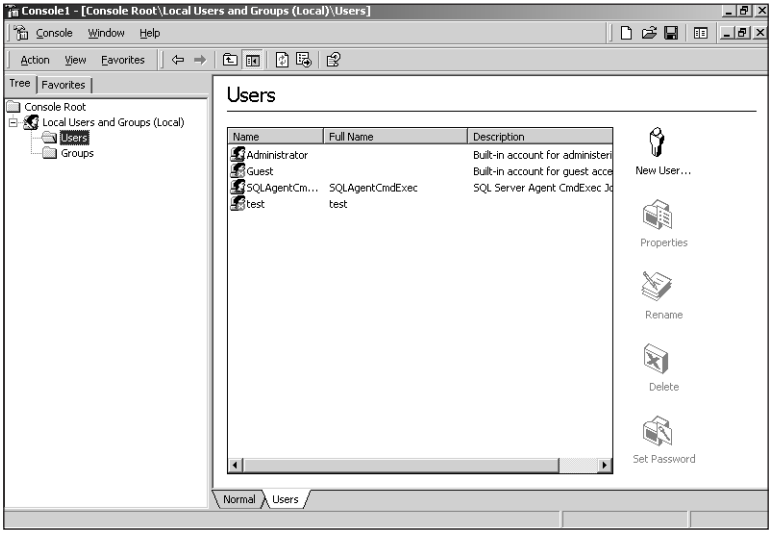

Figure 2.4 A taskpad view of the Users container.

When you are in a quandary about what to do with old user accounts, we recommend disabling rather than deleting them. Deleting a user account completely removes it from the system. This means that it never existed. Even if you created another account with the same name and permissions, it would still have a different Security ID (SID) and be considered a different account by Windows 2000.

In addition, if you need to perform a security audit or create a duplicate account, you'll be unable to do so. By disabling the account, however, you not only remove it from use, but you retain it for security audits and to be used as a template if duplicates are required.

When giving a user membership in a group, be sure to think about the results of multi-group membership. In some cases, you might overlap group purposes, which can result in granting some users too much access. Plus, if you actually use the No Access setting, you may end up blocking access to someone who legitimately needs it.

Backup Utilities

Windows 2000 now includes an advanced built-in backup tool. Instead of developing the backup program, Microsoft opted to license software from Veritas Software (formerly Seagate Software). Compared to the Windows NT backup utility, this tool is a big step forward. Although some of the inherent problems with the Windows NT version of the program have been fixed with Windows 2000, the Backup utility still has some problems:

- Remote Registry backup is not supported.
- Remote files are accessible only if a drive is mapped to a local drive letter.

Scheduling backups with the native backup utility requires the use of the *Task Scheduler service*. This service is enabled through the Services tool in the Administrative Tools menu. You'll need to set its startup parameters to Automatic. You no longer need to use the AT.EXE and WINAT.EXE utilities to schedule the backup. Instead, you simply click on the Schedule Jobs tab (see Figure 2.5) and configure the backup.

Figure 2.5 Scheduling backup jobs in Windows 2000.

Aside from its ability to back up and restore files (including the Registry), back up and restore from non-tape devices such as floppy disks, Zip disks, Jaz disks, or a file on a hard drive, and schedule these tasks, it also creates the *Emergency Repair Disk (ERD)*. In previous versions of Windows, the ERD was created using the RDISK.EXE utility. Figure 2.6 illustrates the process of creating an ERD in Windows 2000.

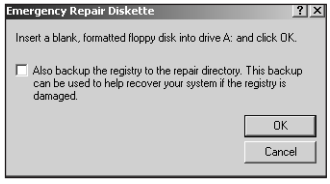

Figure 2.6 Creating an Emergency Repair Disk in Windows 2000.

Third-Party Backup Utilities

We provide pointers to a number of excellent third-party backup utilities at the end of the chapter in the "For More Information" section.

When selecting a third-party backup solution, make sure it exhibits the following features:

- Backs up to tape, disk, floppy, and other media types
- Backs up and restores local and network resources
- Backs up and restores local and remote Registries
- Includes internal automation and scheduling of backups
- Fully supports Windows 2000 security including Active Directory
- Supports backup tape locking, encryption, or other media security features

With these requirements, you are sure to find a backup product that meets your needs and can keep up with an expanding network. Note that many backup programs are rated as *enterprise solutions*. This is often a term used to indicate that the product can support a large network. You also might notice that these products have a price tag of over $1,000. This doesn't mean that you'll have to shell out that much money to obtain good backup software. You should take the time to shop around. For example, Backup Exec from Veritas has a desktop version available online for under $100.

Disk Management

Like the Local Users and Groups tool, Disk Management (see Figure 2.7) is available either in the Computer Management application or as its own snap-in. *Disk Management* is the primary tool used to manage partitions. When you add a new hard drive to your computer, use Disk Management to create primary and extended partitions and logical drives and assign drive letters. You can also use Disk Administrator to create simple volume and striped volumes (RAID). The Windows 2000 Professional version of Disk Management cannot create fault-tolerant disk configurations. Only the Server versions of Windows 2000 (Server, Advanced Server, and Datacenter Server) can create mirrored volumes, duplexed volumes, and RAID-5 volumes.

You cannot alter the boot or system partitions using the Disk Management tool. If you try to format or delete the partition where key Windows 2000 files reside, an error is displayed and the tool won't allow the operation to take place. However, there is no such protection for other partitions. Be careful not to destroy partitions that contain important data.

Windows 2000 also introduced a new type of disk, known as the *dynamic disk*. Any disk that is formatted pre-Windows 2000 is known as a basic disk. Disks can be converted from basic to dynamic and back. Dynamic disks can be moved from one system to another without the need to reconfigure them. For example, a RAID-5 volume created on one system can be imported by another without requiring a system reboot.

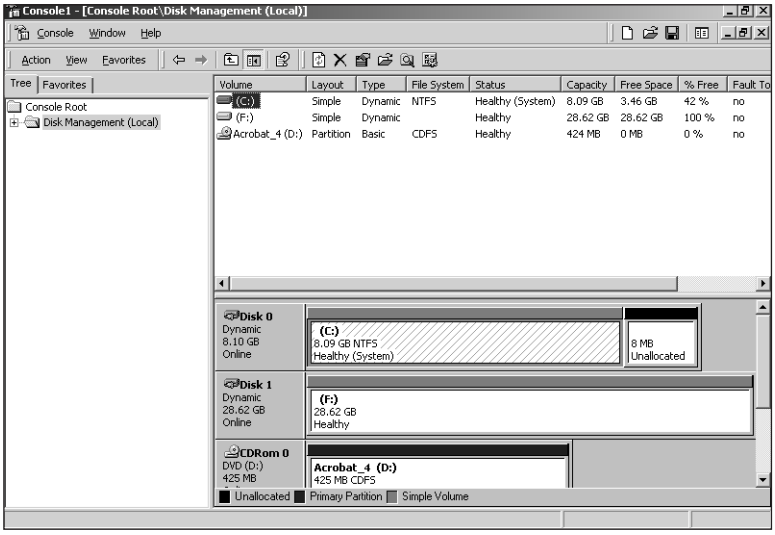

Figure 2.7 The Disk Management Utility.

According to Microsoft, NTFS partitions are not accessible from MS-DOS or non-Windows 2000 operating systems. However, several third-party utilities and file drivers are available that make such access possible. Reading data from NTFS partitions was previously restricted to Windows 2000. Now, with NTFSDOS from Systems Internals, you can read, rename, and even copy over files from an NTFS partition (providing the new file is exactly the same size) using MS-DOS. You can grab this tool from the Systems Internals Web site at **`http://www.sysinternals.com/`**.

Security Breach!

It is important to note that use of these tools opens up a potential security risk. Both tools allow you, or any other user, to bypass the security on NTFS files.

In addition to NTFSDOS, Systems Internals offers many other great tools as well. You should take the time to review this site and all the utilities available.

Event Viewer

The *Event Viewer* (see Figure 2.8) in Windows 2000 is another MMC snap-in. This Windows 2000 utility records information about various system occurrences. Windows NT was limited to three log files: System, Security, and Application. These three logs still exist in Windows 2000, but the Event Viewer has been expanded to allow other components or third-party applications to use the Event Viewer as the global location of the log files. The logs that appear in your installation of Windows 2000 will vary depending on the components that are installed. Domain Name Service, for example, maintains its own log in the Event Viewer.

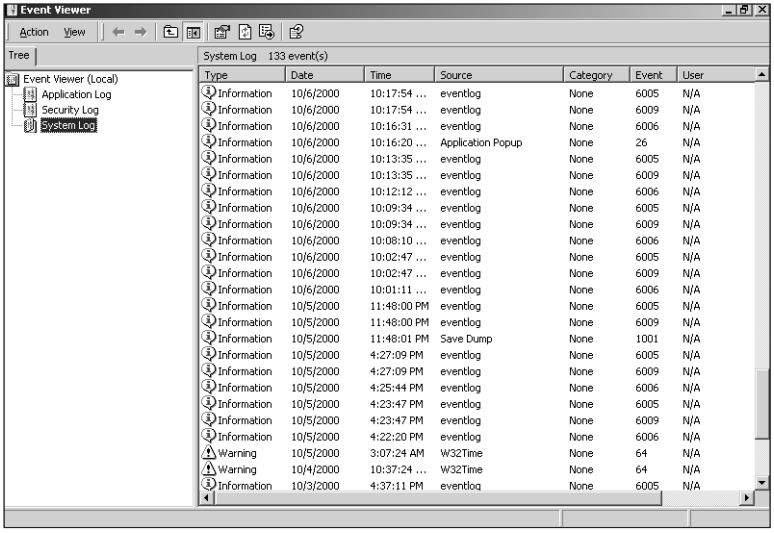

Figure 2.8 The Event Viewer.

Because all Windows 2000 systems have at the very least the three logs mentioned earlier, we will define them now:

- The *System log file* records events related to system operation, most often associated with device drivers and services.
- The *Application log file* records events related to applications, programs, and utilities, not native Windows 2000 tools.
- The *Security log file* records events related to security and auditing. The Security log will not record any information until an audit policy is enabled.

The System and Application logs can be viewed by anyone. The Security log is restricted to administrators. The viewed log file is selected from the Log menu bar command.

The default settings for the logs restrict each log file to a maximum of 512KB and a time length of seven days. When the fixed file size is reached, the log file is closed. The log file must be cleared before you can log in to that file again. Events older than the specified day length are overwritten by new events. If your log files close, you lose some information, so you need to either increase the file size or decrease the day limit. If you need to retain events for longer time periods, you should increase the file size and the day limit. You can change these options through the Log Settings menu command, accessed from the Log menu. Each log file has its own size and day limit settings.

You can view the log files from a remote system on your network using the Select Computer command from the Log menu. This feature simplifies administrative tasks by allowing you to diagnose a system remotely via Event Viewer rather than requiring you to sit at that computer's keyboard.

You can save logs to a file or use them with other applications. You can load the .EVT file type into another Event Viewer. The log's .TXT file can be in standard monospace-columned or comma-delimited format.

Use the Filter command from the View menu to quickly locate events of a certain type or pertaining to a particular source, category, user, computer, or event ID. To search through the contents of the selected log for an event by keywords, use the Find command from the View menu.

A new feature of the Windows 2000 Event Viewer is its capability to sort the logs based on the columns displayed in the utility. For example, to sort the logs based on event ID, simply click on the Event column heading.

Event Viewer can record a significant amount of useful, if not vital, information, but extracting or even locating the data within the log files can be a daunting task. You may want to invest in an Intrusion Detection solution that can automatically and semi-intelligently scan Event Viewer. These tools look for patterns of failure, intrusion, or degradation of the system and then report the findings to you in a concise format. Please look for recommendations in the "For More Information" section at the end of this chapter.

Performance Monitor

The Windows 2000 Performance Monitor is known simply as Performance on the Administrative Tools menu. This tool actually consists of two different tools: System Monitor and Performance Logs and Alerts (as shown in Figure 2.9).

This is a tool no system administrator can live without. This tool is discussed in depth in Chapter 22, "Tuning and Optimizing Windows 2000."

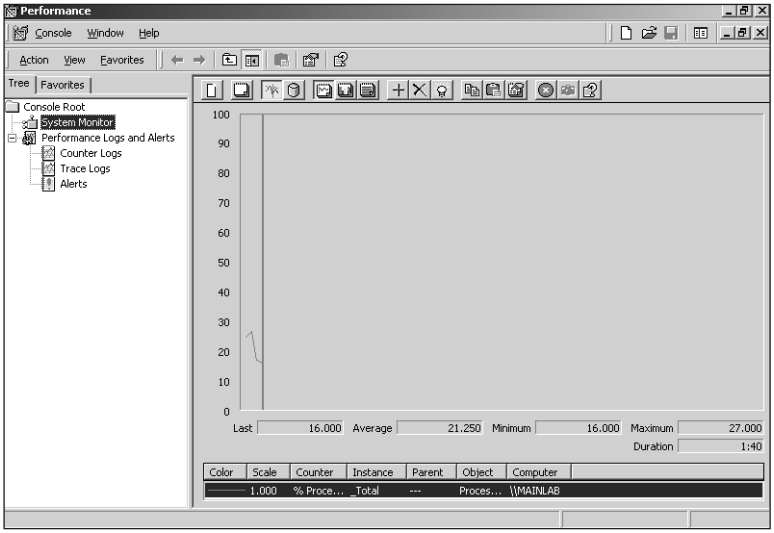

Figure 2.9 The Windows 2000 Performance tool.

System Information

The old Windows NT Diagnostics tool has been completely redesigned for Windows 2000 (actually, it was adopted from Windows 98) and is now known as the *System Information tool* (as shown in Figure 2.10). It still contains the read-only information that its counterpart did (only in much greater detail). The tool contains information about the hardware and environmental configuration of the Windows 2000 systems. This MMC snap-in contains six different sections. The sections and the details they offer are shown in Table 2.1.

Table 2.1 **System Information Sections and Details**

Tab Name	Details Provided
System Summary	Displays an overview of the system's configuration
Hardware Resources	Contains information on system IRQs, I/O ports, DMA channels, and memory
Components	Contains all the devices (hardware-wise) that are installed in the system, their configuration, and settings
Software Environment	Contains the program groups, services, drivers, tasks, and startup programs that exist on the system
Internet Explorer 5	Contains all the properties and settings for Internet Explorer 5
Applications	Contains the application-specific information stored on the system

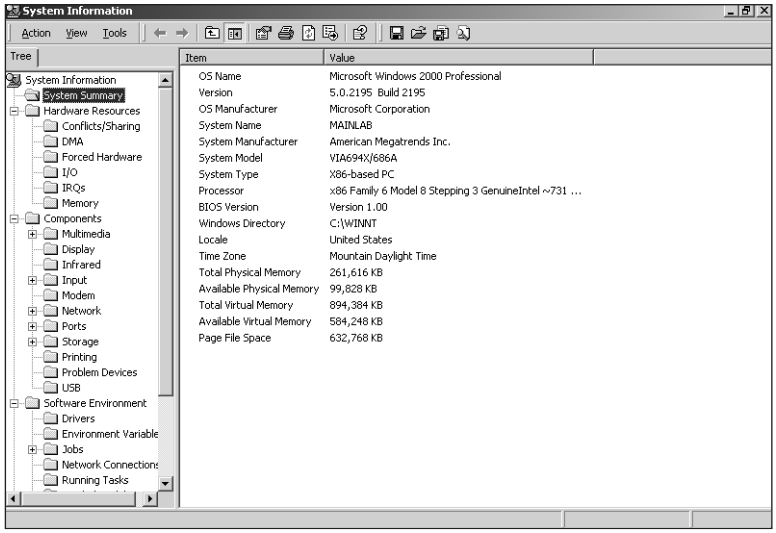

Figure 2.10 The System Information tool.

You cannot use the System Information tool to change or modify any settings it displays, but simply being able to view these items can help sidestep mistakes or quickly locate problems. This tool also includes several utilities that can be used to diagnose and troubleshoot your system. These include the following:

- **Disk Cleanup.** A utility used for removing temporary files to free up disk space.
- **Dr. Watson.** A tool for capturing the error output of failed applications.
- **DirectX Diagnostic Tool.** A tool for troubleshooting DirectX installations.
- **Hardware Wizard.** A wizard for installing, removing, or troubleshooting hardware devices.
- **Network Connections.** Displays the network connections on the system.
- **Backup.** The Windows 2000 Backup program.
- **File Signature Verification Utility.** Ensures that applications and drivers are signed as tested with Windows 2000.
- **Windows Report Tool.** A tool used to report problems with the system. This tool collects configuration information to be included with the help ticket report.

For More Information

If the information about Windows 2000 native administration tools presented in this chapter has increased your desire to learn more, here are some resources you can research to obtain more knowledge:

- *Microsoft Windows 2000 Professional Resource Kit*. Microsoft Press, 2000. ISBN: 1572318082.
- *Microsoft Windows 2000 Server Resource Kit*. Microsoft Press, 2000. ISBN: 1572318058.
- Microsoft TechNet: **http://www.microsoft.com/technet**

We recommend the following backup software:

- Veritas's Backup Exec: **www.veritas.com**
- Computer Associate's ARCserve: **www.cia.com**
- UltraBac's UltraBac: **www.ultrabac.com**

You can locate other selections by searching with the keyword `backup` at the following Web sites:

- **www.serverextras.com**
- **www.bhs.com**
- **www.sunbelt-software.com**
- **www.beyond.com**
- **www.davecentral.com**
- **www.tucows.com**

Although Windows 2000 includes a basic disk defragmentation tool, we recommend the following more advanced utilities:

- Executive Software's Diskeeper: **www.execsoft.com**
- Raxco's Perfectdisk: **www.raxco.com**
- Symantec's SpeedDisk: **www.symantec.com**

Here are several tools you can examine in the area of security auditing and intrusion detection software:

- Internet Security Systems' Web, Intranet, and Firewall scanners: **www.iss.net**
- Harris Corporation's STAT: **www.sunbelt-software.com**
- Blue Lance's LT Auditor+: **www.bluelance.com**
- Cybersafe Corporation's Entrax: **www.cybersafe.com**
- Qualys's QualysGuard: **www.sunbelt-software.com**