

Microsoft Windows Server 2003 Administrator's Pocket Consultant, Second Edition

William R. Stanek

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2006 by William R. Stanek

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2005939170

1 2 3 4 5 6 7 8 9 QWE 0 9 8 7 6 5

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Microsoft, Active Directory, ActiveX, FrontPage, IntelliMirror, JScript, Microsoft Press, MS-DOS, MSN, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Martin DelRe

Project Editor: Denise Bankaitis

Technical Editor: Rozanne Whalen

Copy Editor: Joseph Gustaitis

Indexer: Jack Lewis

Body Part No. X11-74977

Acknowledgments

Writing *Microsoft Windows Server 2003 Administrator's Pocket Consultant 2nd Edition* was a lot of fun—and a lot of work. As you'll see, Windows Server 2003 is very different from its predecessors, and that meant a lot of research to ensure that the book was as accurate as it could be. When all was said and done with the first edition, I ended up with a book that was nearly 1,000 pages

long, and that just isn't what a Pocket Consultant is meant to be. Pocket Consultants are meant to be portable and readable—the kind of book you use to solve problems and get the job done wherever you might be. With that in mind, I had to go back in and carefully review the text, making sure I focused on the core of Windows Server 2003 administration. Revising the book for the second edition was no less challenging. There's a wealth of changes for the latest service packs and R2, which meant a lot of research and a lot of digging into the operating system internals. The result is the book you hold in your hand, which I hope you'll agree is one of the best practical, portable guides to Windows Server 2003.

It's gratifying to see techniques I've used time and again to solve problems put into a printed book so that others may benefit from them. But, no man is an island, and this book couldn't have been written without help from some very special people. As I've stated in *Microsoft Windows XP Administrator's Pocket Consultant 2nd Edition* and in *Microsoft SQL Server 2005 Administrator's Pocket Consultant*, the team at Microsoft Press is top-notch. Throughout the writing process, Maureen Zimmerman and Denise Bankaitis were instrumental in helping me stay on track and getting the tools I needed to write this book. Both Maureen and Denise did a first-rate job managing the editorial process from the Microsoft Press side. Susan McClung headed up the editorial process for nSight, Inc. Their professionalism, thoroughness, and attention to every detail are much appreciated!

Unfortunately for the writer (but fortunately for readers), writing is only one part of the publishing process. Next came editing and author review. I must say, Microsoft Press has the most thorough editorial and technical review process I've seen anywhere—and I've written a lot of books for many publishers. Special thanks to Maureen, Denise, and Susan for helping me to meet review deadlines. Rozanne Whalen was the technical editor for the book. It was a great pleasure working with Rozanne. I'd also like to thank Joseph Gustaitis for his careful copyediting of this book. I believe Joe has been the copyeditor for every Pocket Consultant that I've written. His work is always top-notch!

I owe many thank yous to Martin DelRe and Lucinda Rowley. Thank you for believing in my work and for supporting my books. Thank you also to Linda Engelman. I truly enjoy working with all of you.

Thank you also to the many SCRB reviewers at Microsoft who reviewed the final copy and to my agents at Studio B, David Rogelberg and Neil Salkind.

Hopefully, I haven't forgotten anyone, but if I have, it was an oversight. *Honest*.;-)

About the Author

William R. Stanek (<http://www.williamstanek.com>) has more than 20 years of hands-on experience with advanced programming and development. He is a leading technology expert, an award-winning author, and a pretty darn good instructional trainer. Over the years, his practical advice has helped millions of programmers, developers, and network engineers all over the world. He has written more than 50 books. Current or forthcoming books include *Microsoft Windows Command-Line Administrator's Pocket Consultant*, *Microsoft SQL Server 2005 Administrator's Pocket Consultant*, and *Windows Server 2003 Inside Out*. He is codeveloper and series editor of the *Administrator's Pocket Consultant* series.

Mr. Stanek has been involved in the commercial Internet community since 1991. His core business and technology experience comes from more than 11 years of military service. He has substantial experience in developing server technology, encryption, and Internet solutions. He has written many technical white papers and training courses on a wide variety of topics. He is widely sought after as a subject matter expert.

Mr. Stanek has an M.S. in information systems, with distinction, and a B.S. in computer science, magna cum laude. He is proud to have served in the Persian Gulf War as a combat crew member on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including one of the United States of America's highest flying honors, the Air Force Distinguished Flying Cross. Currently, he resides in the Pacific Northwest with his wife and children.

Introduction

Microsoft Windows Server 2003 Administrator's Pocket Consultant 2nd Edition is designed to be a concise and compulsively usable resource for Microsoft Windows Server 2003 administrators. This is the readable resource guide that you'll want on your desk at all times. The book covers everything you need to perform the core administrative tasks for servers running Windows Server 2003. Not only has this book been updated to incorporate the latest service packs and changes, but it has also been updated to cover the R2 version of Windows Server 2003.

Because the focus is on giving you maximum value in a pocket-sized guide, you don't have to wade through hundreds of pages of extraneous information to find what you're looking for. Instead, you'll find exactly what you need to get the job done. In short, the book is designed to be the one resource you turn to whenever you have questions regarding Windows Server 2003 administration. To this end, the book zeroes in on daily administration procedures, frequently used tasks, documented examples, and options that are representative while not necessarily inclusive.

One of the goals is to keep the content concise so that the book remains compact and easy to navigate while at the same time ensuring that it is packed with as much information as possible—making it a valuable resource. Thus, instead of a hefty 1000-page tome or a lightweight 100-page quick reference, you get a valuable resource guide that can help you quickly and easily perform common tasks, solve problems, and implement advanced Windows technologies like Active Directory directory service, Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS), and Domain Name System (DNS).

Who Is This Book For?

Microsoft Windows Server 2003 Administrator's Pocket Consultant covers the Standard, Enterprise, Web, and Datacenter Server editions of Windows Server 2003. The book is designed for:

- Current Windows Server 2003 system administrators
- Accomplished users who have some administrator responsibilities
- Administrators upgrading to Windows Server 2003 from previous versions
- Administrators transferring from other platforms

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows Server 2003 and that Windows Server 2003 is already installed on your systems. With this in mind, I don't devote entire chapters to comprehending Windows Server 2003 architecture, installing Windows Server 2003, or understanding Windows Server 2003 startup and shutdown. I do, however, cover Windows Server 2003 configuration, Group Policy, security, auditing, data backup, system recovery, and much more.

I also assume that you're fairly familiar with Windows commands and procedures as well as the Windows user interface. If you need help learning Windows basics, you should read the Windows documentation.

How Is This Book Organized?

Microsoft Windows Server 2003 Administrator's Pocket Consultant is designed to be used in the daily administration of Windows networks, and, as such, the book is organized by job-related tasks rather than by Windows Server 2003 features. If you're reading this book, you should be aware of the relationship between Pocket Consultants and Administrator's Companions. Both types of books are designed to be a part of an administrator's library. While Pocket Consultants are the down-and-dirty, in-the-trenches books, Administrator's Companions are the comprehensive tutorials and references that cover every aspect of deploying a product or technology in the enterprise.

Speed and ease of reference are an essential part of this hands-on guide. The book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick reference features are included as well. These features include quick step-by-step instructions, lists, tables with fast facts, and extensive cross-references.

[Chapters 1 to 5](#) cover the fundamental tasks you need for Windows Server 2003 administration. [Chapter 1](#) provides an overview of Windows Server 2003 administration tools, techniques, and concepts. The chapter also introduces the security and maintenance enhancements included in Service Pack 1 and R2. [Chapter 2](#) explores the tasks you'll need to manage Windows Server 2003 systems. [Chapter 3](#) covers monitoring Windows Server 2003 services, processes, and events. [Chapter 4](#) discusses Group Policy and also explains how to automate common administrative tasks. [Chapter 5](#) details how to work with support services and remote desktop connectivity through terminal services.

[Chapters 6 to 10](#) cover the essential tasks for managing Active Directory and administering user, computer, and group accounts. [Chapter 6](#) introduces Active Directory structures and explains how to work with Active Directory domains. [Chapter 7](#) explores core Active Directory administration. You'll learn how to manage computer accounts, domain controllers, and organizational units. [Chapter 8](#) describes how to use system accounts, built-in groups, user rights, built-in capabilities, and implicit groups. You'll find extensive tables that tell you exactly when you should use certain types of accounts, rights, and capabilities. The core

administration tasks for creating user and group accounts are covered in [Chapter 9](#), with a logical follow-up for managing existing user and group accounts covered in [Chapter 10](#).

[Chapters 11 to 15](#) cover data administration. [Chapter 11](#) starts by explaining how to add hard disk drives to a system and how to partition drives. Then the chapter dives into common tasks for managing file systems and drives, such as defragmenting disks, compression, encryption, and more. In [Chapter 12](#), you'll find tasks for managing volume sets and redundant array of independent disks (RAID) arrays, as well as detailed advice on repairing damaged arrays.

[Chapter 13](#) focuses on managing files and folders and all the tasks that go along with it. You'll also find an extensive discussion of file screening, storage reporting, and combating malware. [Chapter 14](#) details how to enable file, drive, and folder sharing for remote network and Internet users and then goes on to cover Active Directory object security and auditing. The chapter also examines both NTFS file system (NTFS) disk quotas and Storage Resource Manager disk quotas. [Chapter 15](#) explores data backup and recovery. The chapter starts with a discussion of backup and recovery planning and then provides step-by-step procedures for implementing a backup plan and recovering systems.

[Chapters 16 to 20](#) cover network infrastructure and advanced administration tasks. [Chapter 16](#) provides the essentials for installing, configuring, and testing Transmission Control Protocol/Internet Protocol (TCP/IP) networking on Windows Server 2003 systems—covering everything from installing network adapter cards to actually connecting a computer to a Windows Server 2003 domain. [Chapter 17](#) begins with a troubleshooting guide for common printer problems and then goes on to cover tasks for installing and configuring local printers and network print servers. [Chapters 18, 19, and 20](#) focus on the key Windows Server 2003 services: DHCP, WINS, and DNS. DHCP is used to assign dynamic Internet Protocol (IP) addresses to network clients. WINS is used to resolve computer names to IP addresses. DNS is used to resolve host names to IP addresses.

Conventions Used in This Book

I've used a variety of elements to help keep the text clear and easy to follow. You'll find code terms and listings in monospace type, except when I tell you to actually type a command. In that case, the command appears in **bold** type. When I introduce and define a new term, I put it in *italics*.

Other conventions include:

- Note** To provide details on a point that needs emphasis
- Best Practices** To examine the best technique to use when working with advanced configuration and administration concepts
- Caution** To warn you when there are potential problems you should look out for
- More Info** To provide more information on the subject
- Real World** To provide real-world advice when discussing advanced topics.
- Tip** To offer helpful hints or additional information

I truly hope you find that *Microsoft Windows Server 2003 Administrator's Pocket Consultant* provides everything you need to perform essential administrative tasks on Windows Server 2003 systems as quickly and efficiently as possible. Your thoughts are welcome at williamstanek@aol.com or visit <http://www.williamstanek.com/>. Thank you.

Support

Every effort has been made to ensure the accuracy of this book and of the contents of the companion disc. Microsoft Press provides corrections for books through the World Wide Web at the following address:

<http://www.microsoft.com/mspress/support/default.asp>

If you have comments, questions, or ideas about this book or the companion disc, please send them to Microsoft Press using either of the following methods:

Postal Mail:

Microsoft Press
Attn: Editor, *Microsoft Windows Server 2003 Administrator's Pocket Consultant*
One Microsoft Way
Redmond, WA 98052-6399

E-mail:

mspinput@microsoft.com

Please note that product support isn't offered through the mail addresses above. For support information, visit Microsoft's Web site at <http://www.microsoft.com/support>.

Chapter 1: Overview of Microsoft Windows Server 2003 System Administration

Overview

Microsoft Windows Server 2003 is a powerful, versatile, and fully featured version of Windows Server. As a server operating system, Windows Server 2003 is fundamentally different from Windows desktop editions, such as Windows Vista and Windows XP Professional. Beginning with Service Pack 1 (SP1), Windows Server 2003 has many security and maintenance enhancements that change the way the operating system works in domains and workgroups. These security enhancements are further complemented with the introduction of Release 2 of Windows Server 2003, referred to in this book as Windows Server 2003 R2.

As with earlier versions of Windows Server 2003, Service Pack 1, Release 2, and later versions of Windows Server 2003 build on and extend the underlying technology architecture introduced with Windows 2000, including the following:

Active Directory directory service An extensible and scalable directory service that uses a namespace based on the Internet standard Domain Name System (DNS).

IntelliMirror Change and configuration management features that support mirroring of user data and environment settings, as well as central management of software installation and maintenance.

Security Architecture Architecture that provides improvements for smart cards, public and private encryption keys, and security protocols. It also features tools for analyzing system security and for applying uniform security settings to groups of systems.

Terminal Services Services that allow you to remotely log on to and manage other Windows Server 2003 systems.

Windows Script Host A scripting environment for automating common administration tasks, such as creating user accounts or generating reports from event logs.

Although Windows Server 2003 SP1 and R2 have dozens of other new features, each of the features just listed has far-reaching effects on how you perform administrative tasks. None has more effect than Active Directory technology. A sound understanding of Active Directory structures and procedures is essential to your success as a Windows Server 2003 systems administrator.

That said, the Windows Server 2003 security architecture also has a far-reaching effect on how you perform administrative tasks. Through Active Directory and administrative templates, you can apply security settings to workstations and servers throughout the organization. Thus, rather than managing security on a machine-by-machine basis, you can manage security on an enterprise-wide basis.

The focus of this book is on managing the Windows Server 2003 family of operating systems. If you want to learn more about managing Windows XP and Windows Vista, good resources are *Microsoft Windows XP Professional Administrator's Pocket Consultant 2nd Edition* (Microsoft Press, 2005) and *Microsoft Windows Vista Administrator's Pocket Consultant* (Microsoft Press, 2006).

Microsoft Windows Server 2003

The Windows Server 2003 family of operating systems consists of Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; Windows Server 2003, Datacenter Edition; and Windows Server 2003, Web Edition. Each edition has a specific purpose, as follows:

Windows Server 2003, Standard Edition Designed to provide services and resources to other systems on a network. It's a direct replacement for Windows NT 4.0 Server and Windows 2000 Server. The operating system has a rich set of features and configuration options. Windows Server 2003, Standard Edition supports two-way and four-way symmetric multiprocessing (SMP) and up to 4 gigabytes (GB) of memory on 32-bit systems and 32 GB on 64-bit systems.

Windows Server 2003, Enterprise Edition Extends the features provided in Windows Server 2003, Standard Edition to include support for Cluster Service, metadirectory services, and Services for Macintosh. It also supports 64-bit systems, hot swappable RAM, and nonuniform memory access (NUMA). Enterprise servers can have up to 32 GB of RAM on x86 and 1 terabyte (TB) of RAM on 64-bit systems and eight CPUs.

Windows Server 2003, Datacenter Edition The most robust Windows server. It has enhanced clustering features and supports very large memory configurations with up to 64 GB of RAM on x86 and 1 TB of RAM on 64-bit systems. It has a minimum CPU requirement of eight and can support up to 64 CPUs on Datacenter Itanium Edition (single partition).

Windows Server 2003, Web Edition Designed to provide Web services for deploying Web sites and Web-based applications. As such, this server edition includes the Microsoft .NET Framework, Microsoft Internet Information Services (IIS), ASP.NET, and network load-balancing features but lacks many other features, including Active Directory. In fact, the only other key Windows features in this edition are the Distributed File System (DFS), Encrypting File System (EFS), and Remote Desktop for administration. Windows Server 2003, Web Edition supports up to 2 GB of RAM and two CPUs.

Note The various server editions support the same core features and administration tools. This means you can use the techniques discussed in this book regardless of which Windows Server 2003 edition you're using. Note also that because you can't install Active Directory on the Web Edition, you can't make a server running Windows Server 2003, Web Edition a domain controller. The server can, however, be a part of an Active Directory domain.

When you install a Windows Server 2003 system, you configure the system according to its role on the network.

- Servers are generally assigned to be part of a workgroup or a domain.
- Workgroups are loose associations of computers in which each individual computer is managed separately.
- Domains are collections of computers that you can manage collectively by means of domain controllers, which are Windows Server 2003 systems that manage access to the network, to the directory database, and to shared resources.

Note In this book "Windows Server 2003" and "Windows Server 2003 family" refer to the family of four products: Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; Windows Server 2003, Datacenter Edition; and Windows Server 2003, Web Edition. The various server editions support the same core features and administration tools.

All versions of Windows Server 2003 allow you to configure different views for the Start Menu. The views for the Start Menu are:

Classic Start Menu The view used in previous versions of Windows. With this view, clicking Start displays a pop-up dialog box with direct access to common menus and menu items.

With the Classic Start Menu, you access administrative tools by clicking Start, clicking Programs, and then clicking Administrative Tools. You access the Control Panel by clicking Start, pointing to Settings, and then clicking Control Panel.

Simple Start Menu Allows you to directly access commonly used programs and directly execute common tasks. You can, for example, click Start and then click Log Off to log off the computer quickly.

With the Simple Start Menu, you access administrative tools by clicking Start and then clicking Administrative Tools. You access the Control Panel by clicking Start and then clicking Control Panel.

Domain Controllers and Member Servers

When you install Windows Server 2003 on a new system, you can configure the server to be a member server, a domain controller, or a stand-alone server. The differences between these types of servers are extremely important. Member servers are a part of a domain but don't store directory information. Domain controllers are distinguished from member servers because they store directory information and provide authentication and directory services for the domain. Stand-alone servers aren't a part of a domain and have their own user database. Because of this, stand-alone servers also authenticate logon requests themselves.

Windows 2000 and Windows Server 2003 don't designate primary or backup domain controllers. Instead, they support a multimaster replication model. In this model any domain controller can process directory changes and then replicate those changes to other domain controllers automatically. This differs from the Windows NT single master replication model in which the primary domain controller stores a master copy and backup controllers store backup copies of the master. In addition, Windows NT distributed only the Security Account Manager (SAM) database, but Windows 2000 and Windows Server 2003 distribute an entire directory of information called a *data store*. Inside the data store are sets of objects representing user, group, and computer accounts as well as shared resources, such as servers, files, and printers.

Domains that use Active Directory are referred to as *Active Directory domains*. This distinguishes them from Windows NT domains. Although Active Directory domains can function with only one domain controller, you can and should configure multiple domain controllers in the domain. This way, if one domain controller fails, you can rely on the other domain controllers to handle authentication and other critical tasks.

In an Active Directory domain, any member server can be promoted to a domain controller, and you don't need to reinstall the operating system as you had to in Windows NT. To promote a member server, all you need to do is install the Active Directory component on the server. You can also demote domain controllers to be member servers, provided that the server isn't the last domain controller on the network. You promote and demote domain controllers by using the Active Directory Installation Wizard and following these steps:

1. Click Start.
2. Select Run.
3. Type **dcpromo** in the Open field, and then click OK.

Understanding and Using Server Roles

Servers running Windows Server 2003 are configured based on the services they offer. You can add or remove services at any time by using the Configure Your Server Wizard and following these steps:

1. Click Start.
2. Select Programs or All Programs as appropriate.
3. Select Administrative Tools, and then select Configure Your Server Wizard.
4. Click Next twice. Windows Server 2003 gathers information about the server's current roles. The Server Role page displays a list of available server roles and specifies whether they're configured. Adding and removing roles is easy. Just perform the following steps:
 - If a role isn't configured and you want to add the role, click the role in the Server Role column and then click Next. Follow the prompts.
 - If a role is configured and you want to remove the role, click the role in the Server Role column and then click Next. Read any warnings displayed carefully and then follow the prompts.

Any server can support one or more of the following server roles:

Application server A server that provides Extensible Markup Language (XML) Web services, Web applications, and distributed applications. When you configure a server with this role, IIS, COM+, and the Microsoft .NET Framework are installed automatically. You also have the option of adding Microsoft FrontPage Server Extensions and enabling or disabling ASP.NET.

DHCP server A server that runs the Dynamic Host Configuration Protocol (DHCP) and can automatically assign Internet Protocol (IP) addresses to clients on the network. This option installs DHCP and starts the New Scope Wizard.

DNS server A server that runs DNS resolves computer names to IP addresses and vice versa. This option installs DNS and starts the DNS Server Wizard.

Domain controller A server that provides directory services for the domain and has a directory store. Domain controllers also manage the logon process and directory searches. This option installs DNS and Active Directory.

File server A server that serves and manages access to files. This option enables you to quickly configure disk quotas and indexing. You can also install the Web-based file administration utility, which installs IIS and enables Active Server Pages (ASP).

Mail server (POP3, SMTP) A server that provides basic Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP) mail services so that POP3 mail clients can send and receive mail in the domain. Once you install this service, you define a default domain for mail exchange and then create and manage mailboxes. These basic services are best for small offices or remote locations where e-mail exchange is needed but you don't need the power and versatility of Microsoft Exchange Server.

Print server A server that provides and manages access to network printers, print queues, and printer drivers. This option enables you to quickly configure printers and print drivers that the server should provide.

Remote access/VPN server A server that routes network traffic and manages dial-up networking or virtual private networking (VPN). This option starts the Routing and Remote Access Setup Wizard. You can configure routing and remote access to allow outgoing connections only, incoming and outgoing connections, or no outside connections at all.

Server cluster node A server that operates as part of a group of servers working together called a *cluster*. This option starts the New Server Cluster Wizard, which allows you to create a new cluster group, or the Add Nodes Wizard, which allows you to add the server to an existing cluster. (This server role is supported by the Enterprise and Datacenter versions only.)

Streaming media server A server that provides streaming media content to other systems on the network or the Internet. This option installs Windows Media Services. (This server role is supported by the Standard and Enterprise versions only.)

Terminal Server A server that processes tasks for multiple client computers running in terminal services mode. This option installs Terminal Server. You don't need to install Terminal Server to remotely manage this server. Remote Desktop is installed automatically with the operating system.

WINS server A server that runs Windows Internet Name Service (WINS), resolves NetBIOS names to IP addresses, and vice versa. This option installs WINS.

Once installed, you can manage server roles using Manage Your Server. This enhanced utility in Windows Server 2003 might just become your command and control center. As shown in [Figure 1-1](#), the current role(s) of the server are displayed in Manage Your Server. You access this tool from the Administrative Tools menu. Click Start, Program or All Programs, and then select Manage Your Server. Use the quick links provided to manage the installed server roles and related information.

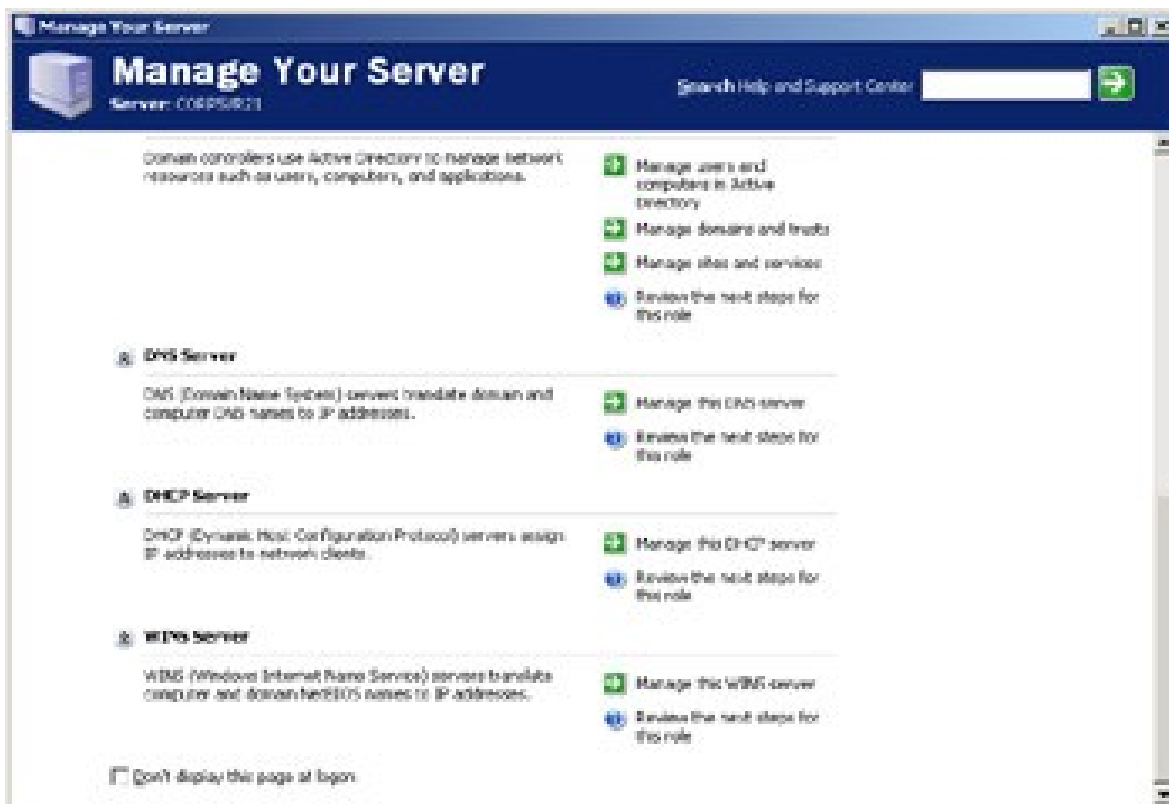


Figure 1-1: Manage Your Server provides quick access to frequently used tools and information.

Tip Use the arrow icons to the left of the role name to shrink or expand the role information provided. Don't overlook Tools And Updates and See Also. Under these headings you'll find links for quick access to Administrative Tools, Windows Update, the System Properties dialog box, Help And Support, and more. As a final note, although you might be tempted to select the Don't Display This Page At Logon check box (it's in the lower-left corner of the dialog box), I don't suggest doing it. I've found that most of the tools I routinely work with and the tasks I regularly perform can be quickly accessed from this dialog box. It really is a good command and control center.

Frequently Used Tools

Many utilities are available for administrating Windows Server 2003 systems. The tools you'll use the most include:

Control Panel A collection of tools for managing system configuration. With Classic Start Menu, you can access these tools by selecting Start, choosing Settings, and then selecting Control Panel. With Simple Start Menu, you can access these tools by selecting Start and then selecting Control Panel.

Graphical administrative tools The key tools for managing network computers and their resources. You can access these tools by selecting them individually on the Administrative Tools submenu.

Administrative wizards Tools designed to automate key administrative tasks. Unlike in Windows NT, there's no central place for accessing wizards. Instead, you access wizards by selecting the appropriate menu options in other administrative tools.

Command-line utilities You can launch most administrative utilities from the command line. In addition to these utilities, Windows Server 2003 provides others that are useful for working with Windows Server 2003 systems.

The following sections provide brief introductions to these administrative utilities. Additional details for key tools are provided throughout this book. Keep in mind that to use these utilities you might need an account with administrator privileges.

Using Control Panel Utilities

Control Panel contains utilities for working with a system's setup and configuration. You can organize the Control Panel in different ways according to the view you're using. A view is simply a way of organizing and presenting options. The key utilities you'll want to use include:

Add Hardware Starts the Add Hardware Wizard, which you can use to install and troubleshoot hardware.

Add Or Remove Programs Used to install programs and to safely uninstall programs. Also used to modify Windows Server 2003 setup components. For example, if you didn't install an add-on component, such as Certificate Services, during installation of the OS, you can use this utility to add it later.

Date And Time Used to view or set a system's date, time, and time zone. Rather than manually setting the time on individual computers in the domain, you can use the Windows Time Service to automatically synchronize time on the network.

Display Used to configure backgrounds, screen savers, video display mode, and video settings. You can also use this utility to specify desktop icons and to control visual effects, such as the menu fade effect.

Folder Options Used to set a wide variety of folder and file options, including the type of desktop used, the folder views used, whether offline files are used, and whether you need to single-click or double-click to open items.

Licensing On a workstation you use this utility to manage licenses on a local system. On a server it also allows you to change the client-licensing mode of installed products, such as Windows Server 2003 or Microsoft SQL Server.

Network Connections Used to view network identity information, to add network components, and to establish network connections. You can also use this utility to change a system's computer name and domain. See [Chapter 7](#), "Core Active Directory Administration," and [Chapter 16](#), "Managing TCP/IP Networking," for details.

Printers And Faxes Provides quick access to the Printers And Faxes folder, which you can use to manage print devices on a system. See [Chapter 17](#), "Administering Network Printers and Print Services," for more information on managing network printers.

Scheduled Tasks Allows you to view and add scheduled tasks. You can schedule tasks on a one-time or recurring basis to handle common administrative jobs. To learn more about scheduled tasks, see [Chapter 4](#), "Automating Administrative Tasks, Policies, and Procedures."

System Used to display and manage system properties, including properties for startup/shutdown, environment, hardware profiles, and user profiles. This utility is explored in [Chapter 2](#), "Managing Servers Running Microsoft Windows Server 2003."

Using Graphical Administrative Tools

Windows Server 2003 provides several types of tools for system administration. The graphical user interface (GUI)-based tools are the ones you'll use the most. Usually you can use graphical administrative tools to manage the system to which you're currently logged on, as well as systems throughout Windows Server 2003 domains. For example, in the Component Services console you specify the computer you want to work with by right-clicking the Event Viewer entry in the left panel and then choosing Connect To Another Computer. This opens the Select Computer dialog box shown in [Figure 1-2](#). You can then choose Another Computer and type the name of the computer, as shown. You can access the graphical administrative tools by selecting them on the Administrative Tools submenu or by double clicking Administrative Tools in the Control Panel.

Figure 1-2: Connecting to another computer allows you to manage remote resources.



Tools and Configuration

Which administrative tools are available on your system depends on its configuration. When you add services, the tools needed to manage those services are installed on the server. These same tools might not be available in Windows XP Professional or on another server. In this case, you might want to install the administration tools on the workstation you're using. To install Windows Server 2003 Administration Tools, complete the following steps:

1. Log on to the workstation using an account with administrator privileges.
2. Insert the Windows Server 2003 CD-ROM into the CD-ROM drive.
3. When the Autorun screen appears, click Perform Additional Tasks, and then click Browse This CD. This starts Windows Explorer.
4. Double-click I386 and then double-click Adminpak.msi. The complete set of Windows Server 2003 management tools are installed on your workstation or server.

Real World

The Windows 2000 administration tools are incompatible with Windows XP Professional and Windows Server 2003. If you upgraded to Windows XP Professional from Windows 2000 Professional, you'll find that many of the Windows 2000 administration tools won't work and you'll encounter errors frequently. You should uninstall these tools and instead install the Windows Server 2003 Administration Tools Pack (Adminpak.msi) on the Windows XP Professional systems that administrators use. The Windows Server 2003 administration tools are compatible with both Windows 2000 and Windows Server 2003.

Using Command-Line Utilities

Many command-line utilities are included with Windows Server 2003. Most of the utilities you'll work with as an administrator rely on Transmission Control Protocol/ Internet Protocol (TCP/IP). Because of this, you should install TCP/IP networking before you experiment with these tools.

Utilities to Know

As an administrator, you should familiarize yourself with the following command-line utilities:

ARP Displays and manages the IP-to-Physical address mappings used by Windows Server 2003 to send data on the TCP/ IP network.

AT Schedules programs to run automatically.

DNSCMD Displays and manages the configuration of DNS services.

FTP Starts the built-in FTP client.

HOSTNAME Displays the computer name of the local system.

IPCONFIG Displays the TCP/IP properties for network adapters installed on the system. You can also use it to renew and release DHCP information.

NBTSTAT Displays statistics and current connections for NetBIOS over TCP/IP.

NET Displays a family of useful networking commands.

NETSH Displays and manages the network configuration of local and remote computers.

NETSTAT Displays current TCP/IP connections and protocol statistics.

NSLOOKUP Checks the status of a host or IP address when used with DNS.

PATHPING Traces network paths and displays packet loss information.

PING Tests the connection to a remote host.

ROUTE Manages the routing tables on the system.

TRACERT During testing, determines the network path taken to a remote host.

To learn how to use these command-line tools, type the name at a command prompt followed by */?*. Windows Server 2003 then provides an overview of how the command is used (in most cases).

Using NET Tools

You can more easily manage most of the tasks performed with the NET commands by using graphical administrative tools and Control Panel utilities. However, some of the NET tools are very useful for performing tasks quickly or for obtaining information, especially during telnet sessions to remote systems. These commands include:

NET SEND Sends messages to users logged in to a particular system.

NET START Starts a service on the system.

NET STOP Stops a service on the system.

NET TIME Displays the current system time or synchronizes the system time with another computer.

NET USE Connects and disconnects from a shared resource.

NET VIEW Displays a list of network resources available to the system.

To learn how to use any of the NET command-line tools, type **NET HELP** followed by the command name, such as **NET HELP SEND**. Windows Server 2003 then provides an overview of how the command is used.

Introducing Security and Maintenance Enhancements

Beginning with Service Pack 1, Microsoft introduced many system security and maintenance enhancements to Windows Server 2003. Two specific changes have a major impact on how Windows Server 2003 is installed:

Post-Setup Security Update Designed to safeguard the server from malicious users and infection between the time the computer is installed and the most current security updates are applied through Windows Update. On a new installation of Windows Server 2003 with Service Pack 1 or later included, Post-Setup Security Update typically starts the first time an administrator logs on and blocks all inbound traffic to the server until updates are made or declined. After the initial log on the tool typically isn't displayed or run again.

Security Configuration Wizard Designed to reduce the attack surface of a server. This wizard can be used to guide you through the process of creating security policies based on the roles performed by a specific server. Similarly configured servers can use the same security policy, and this policy can be edited or undone (rolled back) at any time.

Unlike Post-Setup Security Update, the Security Configuration Wizard is not installed by default. To install the Security Configuration Wizard, follow these steps:

1. In Control Panel, double-click Add Or Remove Programs.
2. Start the Windows Component Wizard by clicking Add/Remove Windows Components.
3. On the Windows Components page, select Security Configuration Wizard and then click Next.
4. When prompted, insert the Windows Server 2003 with SP1 CD-ROM into the CD-ROM drive and then click OK.
5. Click Finish. Close Add Or Remove Programs.

After it's installed, you can run the Security Configuration Wizard from the Administrative Tools menu. Click Start, Programs or All Programs, Administrative Tools and then select Security Configuration Wizard. Files and other resources used by the wizard are stored under %WinDir%\Security. The wizard has a command-line counterpart which can be started by typing **scwcmd** at a command prompt.

Similar to desktops running Windows XP Professional Service Pack 2 or later, key additional features for servers running Windows Server 2003 Service Pack 1 or later include:

Windows Firewall A software-based firewall designed to help protect a server against network-based attacks and other security threats from remote systems. Windows Firewall requires the Windows Firewall/Internet Connection Sharing (ICS) service to be enabled and running. In a typical new installation of Windows Server 2003 with SP1, this service is disabled. If you want to use Windows Firewall, you can configure the service and start the firewall by completing the following steps:

1. Open Windows Firewall in Control Panel.
2. Click Yes when prompted to start the Windows Firewall/Internet Connection Sharing (ICS) service.
3. Select On and then click OK.

Data Execution Protection A set of hardware and software technologies designed to help protect against malicious code. To better safeguard computers from memory-based vulnerabilities such as buffer overruns that allow too much data to be copied into areas of a computer's memory, the core components of the operating system were recompiled for Service Pack 1. Core code was also updated to support hardware-enforced execution protection (referred to as a no execute or NX feature). Execution protection tells the CPU to mark all memory locations in an application as nonexecutable unless the location explicitly contains executable code. This prevents malicious code such as a virus from inserting itself into most areas of the memory because only specific areas of memory are marked as having executable code. Typically Data Execution Protection is enabled if supported, and you can check the status of Data Execution Protection by completing the following steps:

1. Open System in Control Panel.
2. On the Advanced tab of the System dialog box, click Settings.
3. Select the Data Execution Prevention tab in the Performance Options dialog box. See [Chapter 2](#) for more information.

Secure Browsing A set of features to enhance Internet Explorer security and lock down the local machine. The key features include Browser Information Bar, which is displayed in Internet Explorer just below the address bar whenever Information Bar messages are displayed; Add-on Manager, which allows you to view and manage currently installed add-ons for Internet Explorer; and Pop-up Blocker, which allows you to block many types of pop-up windows. [Chapter 15](#) of *Microsoft Windows XP Professional Administrator's Pocket Consultant 2nd Edition* describes these features in detail.

RPC Interface Restriction A set of changes to the Remote Procedure Call (RPC) service and the Distributed Component Object Model (DCOM) to help safeguard server systems against some types of remote attacks. The changes affect the interaction of programs across networks and also ensure that both RPC and DCOM work with the Windows Firewall.

Introducing Release 2 Enhancements

Windows Server 2003 R2 is an update release of the Windows Server 2003 operating system that is built on top of Windows Server 2003 SP1. After you install Windows Server 2003 R2, you can install additional features for manageability and reliability like other Windows components using Add Or Remove Programs in Control Panel. To install additional features, complete the following steps:

1. In Control Panel, double-click Add Or Remove Programs.
2. Click Add/Remove Windows Components.

3. On the Windows Components page, select components to install. Click Next.
4. When prompted, insert the Windows Server 2003 R2 CD-ROM into the CDROM drive and then click OK.
5. Click Finish. Close Add Or Remove Programs.

Windows Server 2003 R2 features include the following:

File Server Resource Manager Provides an improved disk quota management system that allows you to manage quotas for individual folders, sets of folders, and volumes. Quotas can be set per folder and per user, and there's an AutoQuota feature. You can also create storage reports. See [Chapter 14](#) for details.

DFS Management Provides improved management and functionality for the DFS. DFS replication enhancements improve handling of large files and large numbers of files. With Enterprise Edition and Datacenter Edition, compression features are included.

Print Management Provides a central management interface for all Windows 2000 or later print servers as well as the related printers and print queues. Printer drives, forms, and ports can also be centrally managed, and there's an automatic detection feature that can add network printers to a local print server automatically. See [Chapter 17](#) for details.

File Server Management Provides an integrated interface for File Server Resource Manager, the DFS Management console, and Storage Manager for storage area networks (SANs). Also includes extensions for shared folder, disk, and volume management. See [Chapters 11 to 15](#) for details.

Storage Manager for SANs Provides a central management interface for SAN devices. You can view storage subsystems, create and manage logical unit numbers (LUNs), and manage Internet SCSI (iSCSI) target devices. The SAN device must support Visual Disk Services in Windows Server 2003.

Other Windows Server 2003 Resources

Before we examine administration tools, let's look at other resources that make Windows Server 2003 administration easier. One of the system administrator's greatest resources is the Windows Server 2003 distribution disk. It contains all the system information you'll need whenever you make changes to a Windows Server 2003 system. Keep the disk handy whenever you modify a system's configuration. You'll probably need it.

To avoid having to access a Windows Server 2003 distribution disk whenever you make system changes, you might want to copy the \I386 directory to a network drive. When you're prompted to insert the CD-ROM and specify the source directory, you simply point to the directory on the network drive. This technique is convenient and saves time. Other resources you might want to use are examined in the sections that follow.

Windows Server 2003 Support Tools

While you're working with the distribution CD-ROM, you might want to install the Windows Server 2003 Support Tools. The support tools are a collection of utilities for handling everything from system diagnostics to network monitoring.

Installing the Support Tools To install the support tools:

1. Insert the Windows Server 2003 CD-ROM into the CD-ROM drive.
2. When the Autorun screen appears, click Perform Additional Tasks, and then click Browse This CD. This starts Windows Explorer.
3. In Windows Explorer, double-click Support and then double-click Tools.

Note Throughout this book I refer to double-clicking, which is the most common technique used for accessing folders and running programs. With a double-click, the first click selects the item and the second click opens and runs the item. In Windows Server 2003 you can also configure single-click open/run. Here, moving the mouse over the item selects it; a click opens and runs it. You can change the mouse click options with the Folder Options utility in the Control Panel. To do this, select the General Tab, and then choose Single-Click To Open An Item or Double-Click To Open An Item, as appropriate.

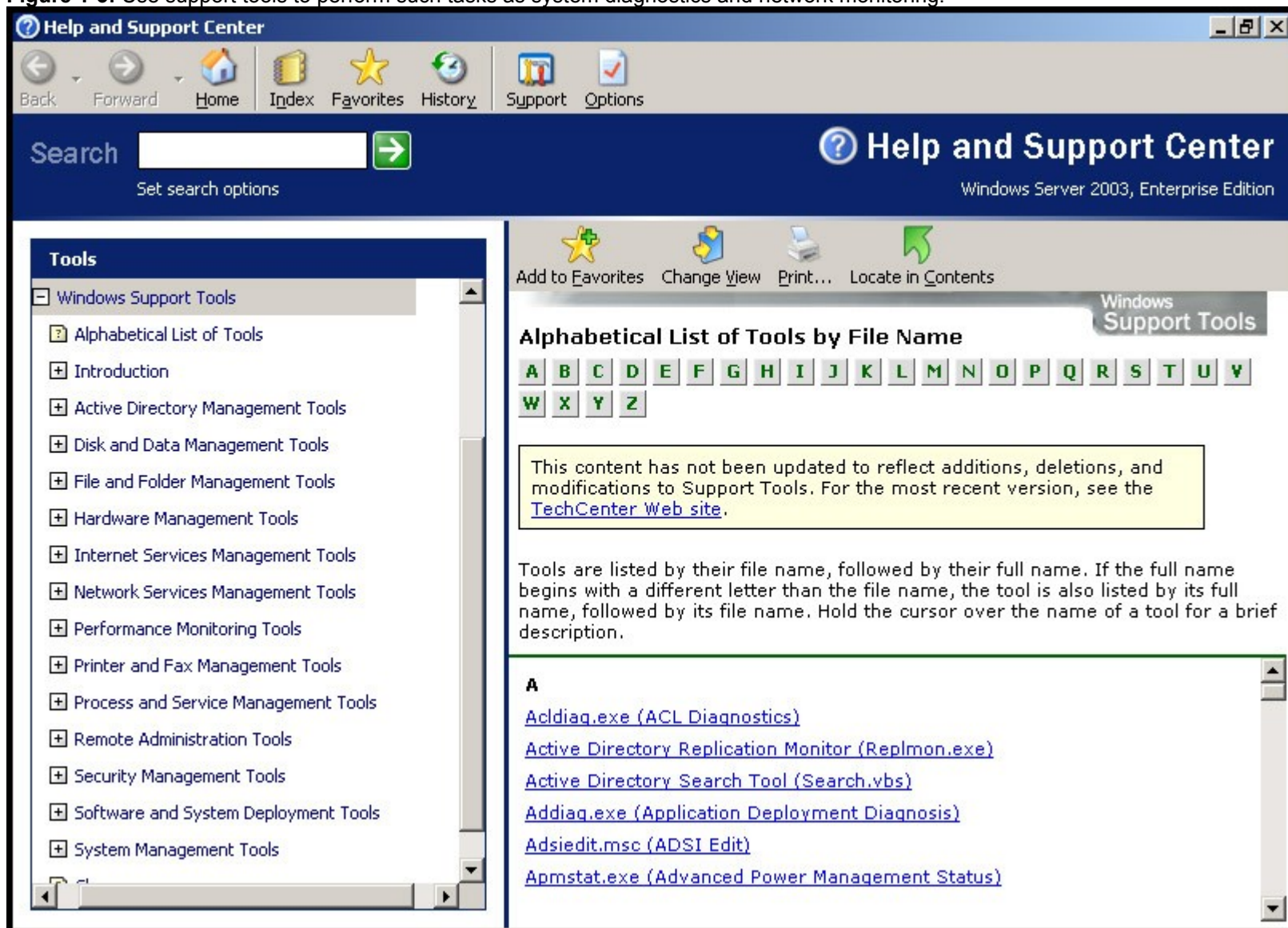
4. Double-click Suptools.msi. This starts the Windows Support Tools Setup Wizard. Click Next.
5. Read the End User License Agreement and then, if you agree and want to continue, click I Agree and then click Next.
6. Enter your user information, and then click Next.

7. Select the destination directory for the support tools. The default location is %ProgramFiles%\Support Tools. If you don't want to use the default location, type a new directory path or click Browse to search for a location. The tools use about 23 MB of disk space.
8. Click Install Now. Click Finish.

Note %ProgramFiles% refers to the ProgramFiles environment variable. The Windows operating system has many environment variables, which are used to refer to user-specific and system-specific values. Often, I'll refer to environment variables using this syntax: %VariableName%.

Using the Support Tools After installation you can access the support tools through the Tools Management Console shown in Figure 1-3. To start the console, click Start, click Programs or All Programs as appropriate, click Windows Support Tools, and then select Support Tools Help.

Figure 1-3: Use support tools to perform such tasks as system diagnostics and network monitoring.



As the figure shows, the tools are organized by file name, tool name, and category. Clicking a tool name accesses a help page that displays the online help documentation for the tool and that you can also use to run the tool.

Chapter 2: **Managing Servers Running Microsoft Windows Server 2003**

Overview

Servers are the heart of any Microsoft Windows network. One of your primary responsibilities as an administrator is to manage these resources. Your key tool is the Computer Management console, which provides a single integrated interface for handling such core system administration tasks as:

- Managing user sessions and connections to servers
- Managing file, directory, and share usage
- Setting administrative alerts
- Managing applications and network services
- Configuring hardware devices
- Viewing and configuring disk drives and removable storage devices

Although the Computer Management console is great for remote management of network resources, you also need a tool that gives you fine control over system environment settings and properties. This is where the System utility comes into the picture. You'll use this utility to:

- Configure application performance, virtual memory, and registry settings
- Manage system and user environment variables
- Set system startup and recovery options
- Manage hardware and user profiles

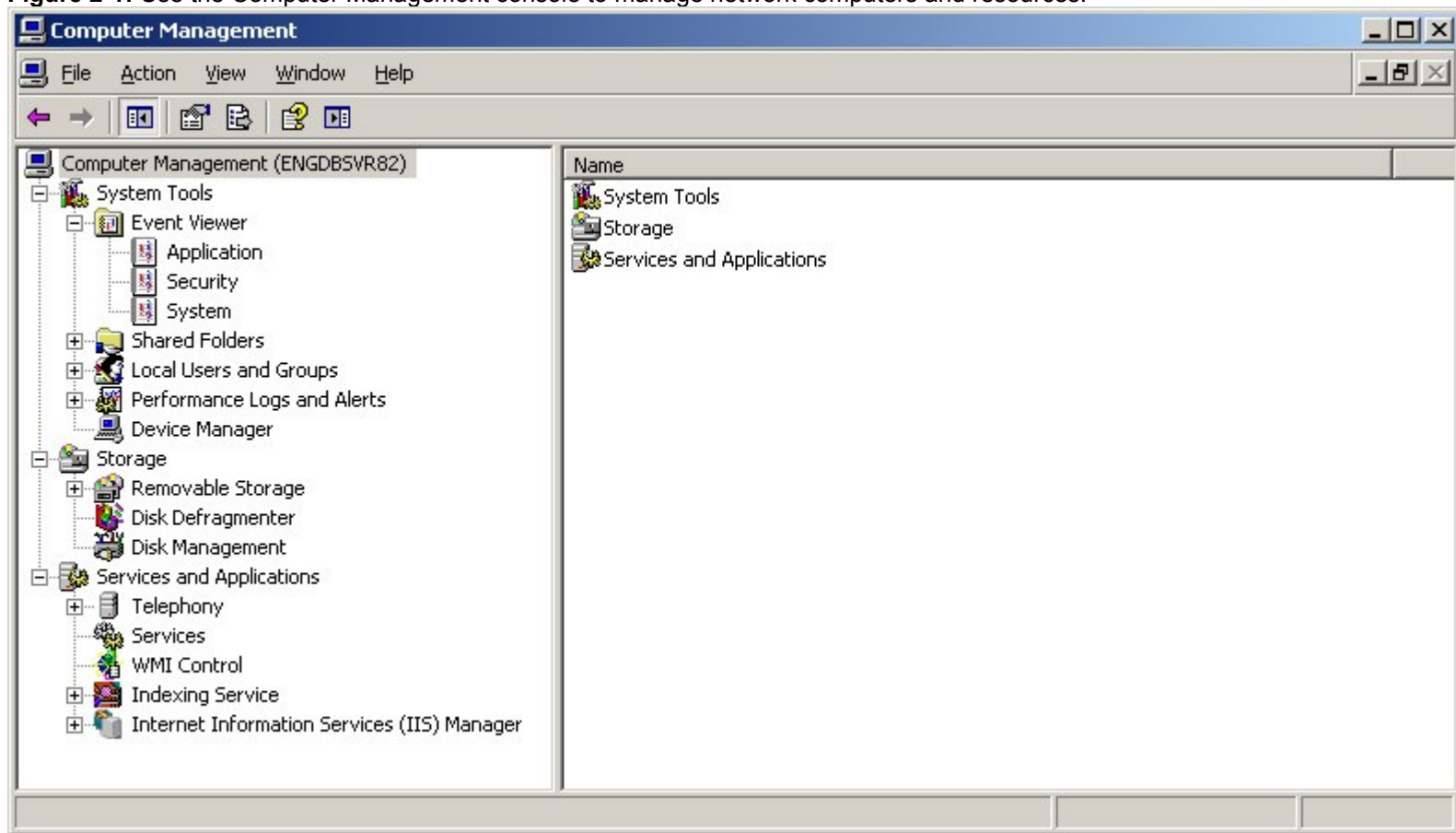
Managing Networked Systems

The Computer Management console is designed to handle core system administration tasks on local and remote systems. You'll spend a lot of time working with this tool, and you should get to know every nook and cranny. Access the Computer Management console with either of the following techniques:

- Choose Start, then Programs or All Programs as appropriate, then Administrative Tools, and finally Computer Management.
- Select Computer Management from the Administrative Tools folder.

As [Figure 2-1](#) shows, the main window has a two-pane view that's similar to Windows Explorer. You use the console tree in the left pane for navigation and tool selection. The right pane is the details pane. Tools are divided into three broad categories:

Figure 2-1: Use the Computer Management console to manage network computers and resources.



System Tools Provides access to general-purpose tools for managing systems and viewing system information

Storage Displays information on removable and logical drives and provides access to drive management tools

Services And Applications Lets you view and manage the properties of services and applications installed on the server

Tip Management consoles such as Computer Management are created using the Microsoft Management Console (MMC) framework. MMC 3.0 is included with Windows Server 2003 R2 and Windows Server 2003 SP2. MMC 3.0 offers several enhancements: a revised Add/Remove Snap-in dialog box that allows easier management of snap-ins; improved error handling, which improves error reporting in consoles; and an Action pane that lists actions that can be performed based on the currently selected item or results. The Action pane is similar to the shortcut menu that is displayed when you right-click an item. To display or close the Action pane, you need to click the Show/Hide Action Pane button on the console toolbar.

Real World The Action pane is meant to reduce confusion, because sometimes you might not see a shortcut menu when you right-click. Whether the shortcut menu appears when you right-click a menu item is controlled by the Enable Dragging And Dropping menu option. If you don't see a shortcut menu when you right-click an item, Enable Dragging And Dropping has been disabled. To enable shortcut menus, right-click Start, choose Properties, and then click Customize. If you are using the Simple Start Menu, click the Advanced tab, and then, in the Start Menu Items box, select Enable Dragging And Dropping. If you are using the Classic Start Menu, click Enable Dragging And Dropping in the Advanced Start Menu Options list.

The tools available through the console tree provide the core functionality for the Computer Management console. When Computer Management is selected in the console tree, you can easily access three important tasks:

- Connect to other computers
- View and change system properties
- Export information lists

In the following sections we'll examine these tasks, and then we'll take a detailed look at working with tools in the Computer Management console.

Connecting to Other Computers

The Computer Management console is designed to be used with local and remote systems. You can select a computer to manage by completing the following steps:

1. Right-click the Computer Management entry in the console tree and then select **Connect To Another Computer** on the shortcut menu. This opens the Select Computer dialog box.
2. Choose **Another Computer** and then type the fully qualified name of the computer you want to work with, such as **engsvr01.technology.microsoft.com**, where *engsvr01* is the computer name and *technology.microsoft.com* is the domain name. Or click **Browse** to search for the computer with which you want to work. Click **OK**.

Viewing and Changing System Properties

You can use the Computer Management console to view the system properties of the local or remote system to which you are currently connected. Essentially, this gives you access to the General, Computer Name, and Advanced tabs of the System utility for that computer. This means you can connect to a computer and access its properties to determine its operating system, service pack, processor type, total system random access memory (RAM), computer name, and more.

You view or change system properties by completing the following steps:

1. In the Computer Management console, connect to the computer with which you want to work and then right-click the Computer Management entry.
2. Choose **Properties**. This opens the dialog box shown in [Figure 2-2](#).



Figure 2-2: Use the Computer Management Properties dialog box to view system properties on the computer to which you are currently connected.

3. Click the General, Computer Name, or Advanced tab as appropriate. In the Advanced tab you can view and configure settings for processor scheduling, memory usage, virtual memory, environment variables, startup, and recovery.

Note The Advanced tab doesn't have options for viewing User Profile or Error Reporting settings. You can change these settings only by using the System utility. You can access the System utility by selecting **System** from the Control Panel menu. In addition, you must have appropriate permissions on a remote system to manage its settings.

Exporting Information Lists

The ability to export information lists is one of my favorite features of the Computer Management console, and if you maintain system information records or regularly work with Windows scripting, it'll probably be one of yours, too. The Export List feature allows you to save textual information displayed in the right pane to a tab-delimited or comma-delimited text file. You could, for example, use this feature to save detailed information on all the services running on the system by completing the following steps:

1. In the Computer Management console, click the plus sign (+) next to the Services And Applications node. This expands the node to display its contents.
2. Select and right-click Services, and then, from the shortcut menu, select Export List. This opens the Export List dialog box.
3. Use the Save In selection list to choose the save location and then enter a name for the export file in the File Name text box.
4. Use the Save As Type selection list to set the formatting of the export file. You can separate columns of information with tabs or commas and save as ASCII text or Unicode text. In most cases, you'll want to use tab-delimited ASCII text.
5. Click Save to complete the export process.

You can use a similar procedure to export lists of other information displayed in the Computer Management console.

Using Computer Management System Tools

The Computer Management system tools are designed to manage systems and view system information. The available system tools are the following:

Event Viewer View the event logs on the selected computer. Event logs are covered in “Event Logging and Viewing” in [Chapter 3](#), “Monitoring Processes, Services, and Events.”

Shared Folders Manage the properties of shared folders, user sessions, and open files. Managing user sessions, open files, and network shares is covered in [Chapter 14](#), “Data Sharing, Security, and Auditing.”

Local Users And Groups Manage local users and local user groups on the currently selected computer. Working with users and groups is covered in [Chapters 6 to 10](#), along with other types of accounts that you can manage in Active Directory directory service.

Note Local users and local user groups aren't a part of Active Directory and are managed instead through the Local Users And Groups view. Domain controllers don't have entries in the Local Users And Groups view.

Performance Logs And Alerts Monitor system performance and create logs based on performance parameters. You can also use this tool to notify or alert users of performance conditions. For more information on monitoring systems, see [Chapter 3](#).

Device Manager Use as a central location for checking the status of any device installed on a computer and for updating the associated device drivers. You can also use it to troubleshoot device problems. Managing devices is covered in the section entitled “[Managing Hardware Devices and Drivers](#),” later in this chapter.

Using Computer Management Storage Tools

The Computer Management storage tools display drive information and provide access to drive management tools. These are the storage tools available:

Removable Storage Manages removable media devices and tape libraries. Tracks work queues and operator requests related to removable media devices.

Disk Defragmenter Corrects drive fragmentation problems by locating and combining fragmented files.

Disk Management Manages hard disks, disk partitions, volume sets, and redundant array of independent disks (RAID) arrays. Replaces the Disk Administrator utility in Windows NT 4.0.

Working with files, drives, and storage devices is the subject of [Chapters 11 to 15](#).

Working with Services and Applications

You use the Computer Management services and applications tools to manage services and applications installed on the server. Any application or service-related task that can be performed in a separate tool can be performed through the Services And Applications node as well. For example, if the currently selected system has Dynamic Host Configuration Protocol (DHCP) installed, you can manage DHCP through the Server Applications And Services node. You could also use the DHCP tool in the Administrative Tools folder. You can perform the same tasks either way.

This technology is possible because the DHCP tool is an MMC snap-in. When you access the DHCP tool in the Administrative Tools folder, the snap-in is displayed in a separate console. When you access the DHCP tool through the Server Applications And Services node, the snap-in is displayed within the Computer Management console. Working with services and applications is discussed in [Chapter 3](#) and elsewhere in this book.

Managing System Environments, Profiles, and Properties

You use the System utility to manage system environments, profiles, and properties. To access the System utility, select or double-click System in the Control Panel. This displays the System Properties dialog box. Whether you must select or double-click System depends on whether Control Panel is displayed as a menu or in a separate window.

As shown in [Figure 2-3](#), the System Properties dialog box is divided into six tabs. Each of these tabs is discussed in the sections that follow. When working with remote systems, keep in mind that General, Computer Name, and Advanced tab details are accessible in Computer Management, as discussed in the section entitled “[Viewing and Changing System Properties](#),” earlier in this chapter.

Figure 2-3: Use the System utility to manage system environment variables, profiles, and properties.



The General Tab

General system information is available for any server running Windows Server 2003 through the System utility's General tab, which is shown in [Figure 2-3](#). To access the General tab, start the System utility by selecting or double-clicking the System icon in the Control Panel.

The information provided in the General tab includes: operating system version and service pack, registered owner, Windows serial number, computer type, amount of RAM installed on the computer, processor type, and total system RAM.

The Computer Name Tab

You can display and modify the computer's network identification with the System utility's Computer Name tab, shown in [Figure 2-4](#). As the figure shows, the tab displays the full computer name of the system and its domain membership. The full computer name is essentially the Domain Name System (DNS) name of the computer, which also identifies the computer's place within the Active Directory hierarchy.

Figure 2-4: Use the Computer Name tab to display and configure system identification. Notice that you can't change the



identification or access information for domain controllers.

To access the Network Identification tab, start the System utility by selecting or double-clicking the System icon in the Control Panel; then click the Computer Name tab. You can now click Change to change the system name and domain associated with the computer.

The Hardware Tab

Servers running Windows Server 2003 can use multiple hardware profiles. Hardware profiles are most useful for mobile servers, such as those configured on laptops. Using hardware profiles, you can configure one profile for when the computer is connected to the network (*docked*) and one profile for when the computer is mobile (*undocked*).

Configuring the Way Hardware Profiles Are Used

To configure hardware profiles, click the System utility's Hardware tab and then click the Hardware Profiles button. This opens the dialog box shown in [Figure 2-5](#). As with systems with multiple operating systems, Windows Server 2003 allows you to configure the way hardware profiles are used, as follows:

- Set a default profile by changing the profile's position in the Available Hardware Profiles list. The top profile is the default profile.
- Determine how long the system displays the startup hardware profile menu by setting a value using the field Select The First Profile Listed If I Don't Select A Profile In. The default value is 30 seconds.
- Have the system wait indefinitely for user input by selecting Wait Until I Select A Hardware Profile.

Figure 2-5: You can configure multiple hardware profiles for any Windows Server 2003 system.



Configuring for Docked and Undocked Profiles

To configure a computer for docked and undocked profiles, complete the following steps:

1. In the Available Hardware Profiles list, select the default profile, and then click Copy.
2. In the Copy Profile dialog box, type a name for the Docked profile in the To text box and then click OK.
3. Select the new profile, and then click the Properties button.
4. Select the This Is A Portable Computer check box, and then choose The Computer Is Docked.
5. Select the Always Include This Profile As An Option When Windows Starts check box, and then click OK.
6. Select the default profile in the Available Hardware Profiles list, and then click Copy.
7. In the Copy Profile dialog box, type a name for the Undocked profile in the To text box and then click OK.
8. Select the new profile, and then click the Properties button.
9. Select the This Is A Portable Computer check box, and then choose The Computer Is Undocked.

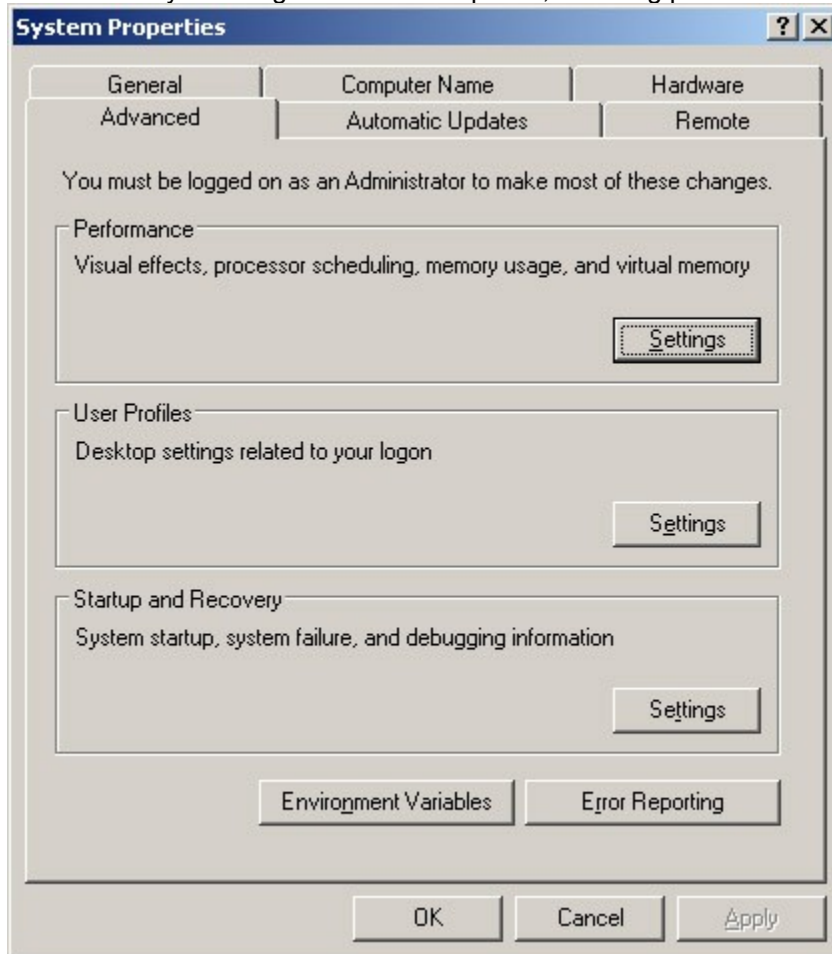
10. Select the Always Include This Profile As An Option When Windows Starts check box, and then click OK.
11. Set the default hardware profile as appropriate for the computer's current state as either docked or undocked. Click OK.

When the system is booted, the hardware profiles are displayed, and you can select the appropriate profile.

The Advanced Tab

The System utility's Advanced tab, shown in [Figure 2-6](#), controls many of the key features of the Windows operating system, including application performance, virtual memory usage, user profile, environment variables, and startup and recovery. To access the Advanced tab, start the System utility by selecting or double-clicking the System icon in the Control Panel; then click the Advanced tab.

Figure 2-6: The Advanced tab lets you configure advanced options, including performance options, environment variables, and



startup and recovery.

Setting Windows Performance

Many graphics enhancements have been added to the Windows Server 2003 interface. These enhancements include many visual effects for menus, toolbars, windows, and the taskbar. To ensure that the server performs at its best level, these options are turned off by default in an initial installation. This reduces the amount of work the server must do when administrators log on locally to perform tasks, and you usually shouldn't change this default setting. However, if you need to modify these options, you can do so by following these steps:

1. Click the Advanced tab in the System utility, and then click the Settings button in the Performance panel to display the Performance Options dialog box.
2. The Visual Effects tab should be selected by default. You have the following options for controlling visual effects:

Let Windows Choose What's Best For My Computer Allows the operating system to choose the performance options based on the hardware configuration. On a server, this typically means that Windows selects only the Use Visual Styles On Windows And Buttons option and that all other options are cleared.

Adjust For Best Appearance When you optimize Windows for best appearance, you enable all visual effects for all graphical interfaces. The menus and taskbar use transitions and shadows. Screen fonts have smooth edges. List boxes have smooth scrolling. Folders use Web views and more. On a server, this setting unnecessarily uses a lot of memory and system resources, and you should rarely use it.

Adjust For Best Performance When you optimize Windows for best performance, you turn off the resource-intensive visual effects, such as slide transitions and smooth edges for fonts, while maintaining a basic set of visual effects. In some cases this completely turns off all visual effects.

Custom You can customize the visual effects as well. To do this, select or clear the visual effects options in the Performance Options dialog box. If you clear all options, Windows doesn't use visual effects.

3. When you're finished changing visual effects, click OK and then click OK again.

Setting Application Performance

Application performance is related to the Processor Scheduling and Memory Usage options that you set for the Windows Server 2003 system. Processor Scheduling determines the responsiveness of the current active application (as opposed to background applications that might be running on the system). Memory Usage determines whether physical memory is optimized for applications or the system cache.

You control application performance by completing the following steps:

1. Access the Advanced tab in the System utility, and then display the Performance Options dialog box by clicking the Settings button in the Performance panel. Click the Advanced tab to modify the performance settings.
2. The Processor Scheduling panel has two options:
Programs To give the active application the best response time and the greatest share of available resources, select Applications. Generally, you'll want to use this option for Application, Web, and Streaming Media servers.
Background Services To give background applications a better response time than the active application, select Background Services. Generally, you'll want to use this option for Active Directory, File, Print, and Network and Communications servers.
3. The Memory Usage panel has two options:
Programs Choose this option to optimize physical memory usage for applications. Generally, you'll want to use this option for Application, Web, and Streaming Media servers.
System Cache Choose this option to optimize physical memory usage for the system cache. Generally, you'll want to use this option for Active Directory, File, Print, and Network and Communications servers.
4. Click OK.

Configuring Virtual Memory

Virtual memory allows you to use disk space to extend the amount of available RAM on a system. This feature of Intel 386 and later processors writes RAM to disks using a process called *paging*. With paging, a set amount of RAM, such as 32 megabytes (MB), is written to the disk as a paging file, where it can be accessed when needed.

An initial paging file is created automatically for the drive containing the operating system. By default, other drives don't have paging files, and you must create these paging files manually if you want them. When you create a paging file, you set an initial size and a maximum size. Paging files are written to the volume as a file called Pagefile.sys.

Best Practices Microsoft recommends that you create a paging file for each physical disk on the system. On most systems, multiple paging files can improve the performance of virtual memory. Thus, instead of a single large paging file, it's better to have several small ones. Keep in mind that removable drives don't need paging files.

You can configure virtual memory by completing the following steps:

1. Start the System utility, and then click the Advanced tab.

2. Click Setting in the Performance panel to display the Performance Options dialog box, and then click the Advanced tab. Then click Change to display the Virtual Memory dialog box shown in [Figure 2-7](#).

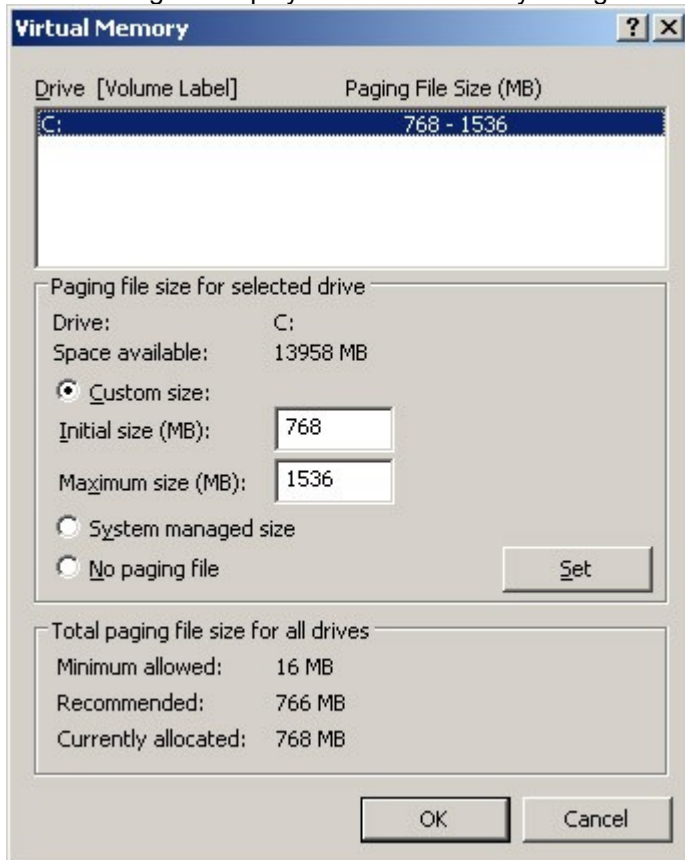


Figure 2-7: Virtual memory extends the amount of RAM on a system.

This dialog box has three key areas:

Drive [Volume Label] Shows how virtual memory is currently configured on the system. Each volume is listed with its associated paging file (if any). The paging file range shows the initial and maximum size values set for the paging file.

Paging File Size For Selected Drive Provides information on the currently selected drive and allows you to set its paging file size. Space Available tells you how much space is available on the drive.

Total Paging File Size For All Drives Provides a recommended size for virtual RAM on the system and tells you the amount currently allocated. If this is the first time you're configuring virtual RAM, you'll note that the recommended amount has already been given to the system drive (in most instances).

Best Practices

Although Windows Server 2003 can expand paging files incrementally as needed, this can result in fragmented files, which slows system performance. For optimal system performance, set the initial size and maximum size to the same value. This ensures that the paging file is consistent and can be written to a single contiguous file (if possible, given the amount of space on the volume). In most cases I recommend setting the total paging file size so that it's twice the physical RAM size on the system. For instance, on a computer with 512 MB of RAM, you would ensure that the Total Paging File Size For All Drives setting is at least 1024 MB. However, on servers with 2 GB or more of RAM, it's best to follow the hardware manufacturer's guidelines for paging file sizes.

3. In the Drive list box, select the volume with which you want to work.
4. Use the Paging File Size For Selected Drive area to configure the paging file for the drive. Select Custom Size. Then enter an initial size and a maximum size and click Set to save the changes.
5. Repeat Steps 3 and 4 for each volume you want to configure.

Note

The paging file is also used for debugging purposes when a STOP error occurs on the system. If the paging file on the system drive is smaller than the minimum amount required to write the debugging information to the paging file, this feature will be disabled. If you want to use debugging, you should set

the minimum size to the same figure as the amount of RAM on the system. For example, a system with 256 MB of RAM would need a paging file of 256 MB on the system drive.

6. On the system volume, the initial size must be as large as the current physical RAM. If it isn't, Windows won't be able to write STOP information to the system drive when fatal errors occur. Click Set to save the changes.
7. Repeat Steps 3 and 4 for each volume you want to configure.
8. Click OK, and, if prompted to overwrite an existing Pagefile.sys file, click Yes.
9. Close the System utility.

Note If you updated the settings for the paging file that's currently in use, you'll see a prompt explaining that you need to restart the server for the changes to take effect. Click OK. When you close the System utility, you'll see a prompt telling you that you need to restart the system for the changes to take effect. On a server, you should schedule this reboot outside normal business hours.

Configuring Data Execution Prevention

Data Execution Prevention (DEP) is a memory protection technology enabled with Service Pack 1 or later. DEP tells the computer's processor to mark all memory locations in an application as nonexecutable unless the location explicitly contains executable code. If code is executed from a memory page marked as nonexecutable, the processor can raise an exception and prevent it from executing. This prevents malicious code, such as a virus, from inserting itself into most areas of memory because only specific areas of memory are marked as having executable code.

Note 32-bit versions of Windows support DEP as implemented by those processors that provide the no-execute page-protection (NX) processor feature. Such processors support the related instructions and must be running in Physical Address Extension (PAE) mode. 64-bit versions of Windows also support the NX processor feature.

Tip As part of system startup, a Noexecute flag is added to the Boot.ini entry. When you change the DEP settings in the System utility, you are manually switching the type of DEP used between noexecute=optin and noexecute=optout. Two additional options are provided through noexecute=alwayson or noexecute=alwaysoff. These settings turn DEP on or off for all processes systemwide respectively, and they're more typically used with Windows XP SP2 or later than with Windows Server 2003.

You can determine whether a computer supports DEP by using the System utility. If a computer supports DEP, you can also configure it by completing the following steps:

1. Click the Advanced tab in the System utility, and then on the Performance panel click Settings to display the Performance Options dialog box.
2. The Performance Options dialog box has several tabs. Click the Data Execution Prevention tab. The text at the bottom of this tab specifies whether the computer supports execution protection.
3. If a computer supports execution protection and is configured appropriately, you can configure DEP by using the following options:

Turn On DEP For Essential Windows Programs And Services Only Enables DEP for limited system binaries as well as programs that specifically opt-in. Applications and other programs running on the server are not configured to use DEP. (Same as using /noexecute=optin in Boot.ini.)

Turn On DEP For All Programs And Services Except Those I Select Enables DEP for all programs and services running on the server. You can configure specific exceptions as necessary using the Add or Remove buttons. Click Add to specify the executable for a program or service that should run without execution protection. Selected an excepted program or service and then click Remove to remove it from the exception list. (Same as using /noexecute=optout in Boot.ini.)

4. Click OK.

Caution If you set noexecute=alwaysoff in Boot.ini, DEP options will be dimmed in the Performance Options dialog box. This appearance is the same as on systems that do not support DEP.

Real World To be compatible with this feature, applications must be able to explicitly mark memory with Execute permission. Applications that can't do this won't be compatible with the NX processor feature. If you're experiencing memory-related problems running applications, you should determine the applications that are having problems and configure them as exceptions rather than completely disabling execution protection. In this way, you still get the benefits of memory protection and can selectively disable memory protection for programs that aren't running properly with the NX processor feature.

Execution protection is applied to both user-mode and kernel-mode programs. A user-mode execution protection exception results in a STATUS_ACCESS_VIOLATION exception. In most

processes, this exception will be an unhandled exception and will result in termination of the process. This is the desired behavior because most programs violating these rules will be malicious in nature, such as a virus or worm.

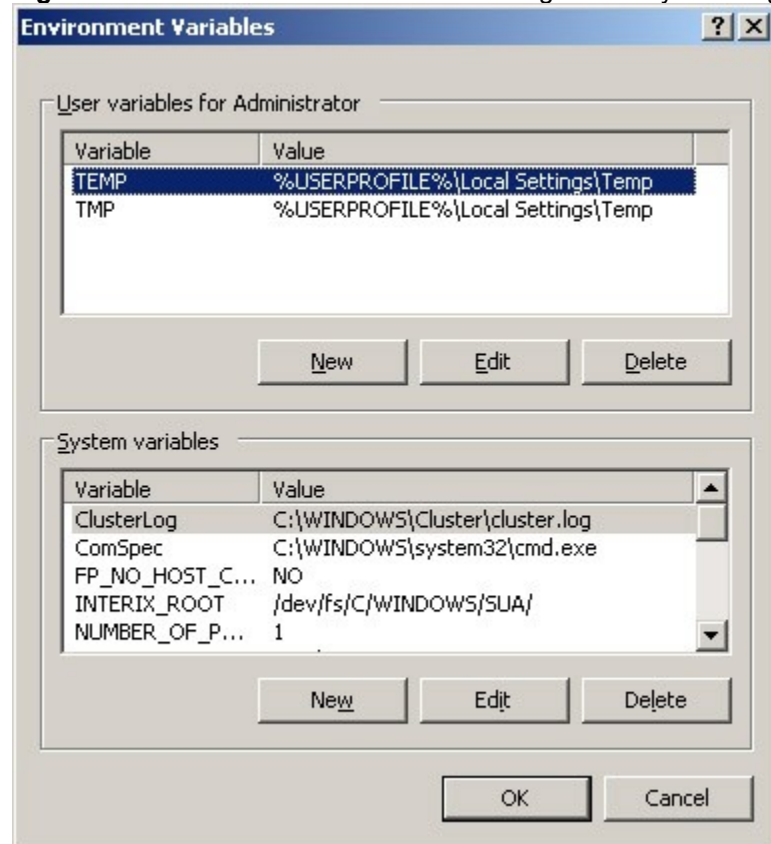
Unlike applications, execution protection for kernel-mode device drivers can't be selectively disabled or enabled. Furthermore, on compliant 32-bit systems, execution protection is applied by default to the memory stack. On compliant 64-bit systems, execution protection is applied by default to the memory stack, the paged pool, and the session pool. A kernel-mode execution protection access violation for a device driver results in an `ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY` exception.)

Configuring System and User Environment Variables

Windows tracks important strings, such as a path where files are located or the logon domain controller host name, using environment variables. Environment variables defined for use by Windows, called system environment variables, are the same no matter who is logged in to a particular computer. Environment variables defined for use by users or programs, called user environment variables, are different for each user of a particular computer.

You configure system and user environment variables by means of the Environment Variables dialog box, shown in [Figure 2-8](#). To access this dialog box, start the System utility, click the Advanced tab, and then click Environment Variables.

Figure 2-8: The Environment Variables dialog box lets you configure system and user environment variables.



Creating an Environment Variable

You can create environment variables by completing the following steps:

1. Click the New button under User Variables or System Variables, whichever is appropriate for the type of environment variable you want to create. This opens the New User Variable dialog box or the New System Variable dialog box, respectively.

2. In the Variable Name text box, type the variable name. Then, in the Variable Value text box, type the variable value. Click OK.

Editing an Environment Variable

You can edit an existing environment variable by completing the following steps:

1. Select the variable in the User Variables or System Variables list box.
2. Click the Edit button under User Variables or System Variables, whichever is appropriate for the type of environment variable you're modifying. This opens the Edit User Variable dialog box or the Edit System Variable dialog box, respectively.
3. Type a new value in the Variable Value text box. Click OK.

Deleting an Environment Variable

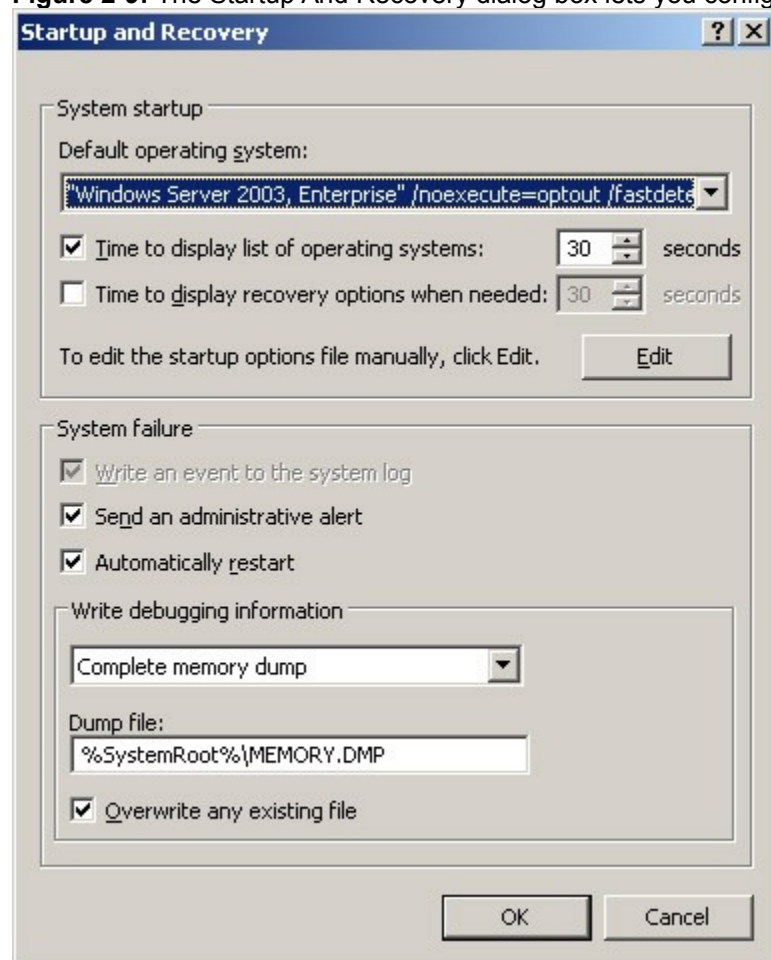
You can delete an environment variable by selecting the variable and then clicking the Delete button.

Note When you create or modify system environment variables, the changes take effect when you restart the computer. When you create or modify user environment variables, the changes take effect the next time the user logs on to the system.

Configuring System Startup and Recovery

You configure system startup and recovery properties by means of the Startup And Recovery dialog box, shown in [Figure 2-9](#). To access this dialog box, start the System utility, click the Advanced tab, and then click Settings on the Startup And Recovery panel.

Figure 2-9: The Startup And Recovery dialog box lets you configure system startup and recovery procedures.



Setting Startup Options

The System Startup panel of the Startup And Recovery dialog box controls system startup. Some of the parameters and options are used to set related Boot Loader and Operating System entries in Boot.ini. Systems with multiple startup configurations, multiple operating system versions, or both will have multiple operating system entries in Boot.ini. During startup of the operating system, Windows uses Boot.ini to identify the boot device and boot flags. Various system startup flags are set through the operating system entries in Boot.ini, including NOEXECUTE flags for Data Execution Prevention (DEP) and FASTDETECT for faster operating system detection.

On a computer with multiple operating system entries in Boot.ini, to set the default operating system, select one of the operating systems listed in the Default Operating System field. These options are obtained from the operating system section of the system's Boot.ini file.

At startup of a computer with multiple operating system entries in Boot.ini, Windows Server 2003 displays the startup configuration menu for 30 seconds by default. You can modify this by taking either of the following actions:

- Boot immediately to the default operating system by clearing the Time To Display List Of Operating Systems check box.
- Display the available options for a specific amount of time by selecting the Time

To Display List Of Operating Systems check box and then setting a time delay in seconds.

Generally, on most systems you'll want to use a value of 3–5 seconds. This is long enough to enable you to make a selection, yet short enough to expedite the system startup process.

When the system is in a recovery mode and booting, a list of recovery options might be displayed. As with the standard startup options, you can configure recovery startup options in one of two ways. You can set the computer to boot immediately using the default recovery option by clearing the Time To Display Recovery Options When Needed check box, or you can display the available options for a specific amount of time by selecting Time To Display Recovery Options When Needed and then setting a time delay in seconds.

Setting Recovery Options

The System Failure and Write Debugging Information areas of the Startup And Recovery dialog box control system recovery. Recovery options allow administrators to control precisely what happens when the system encounters a fatal system error (also known as a STOP error). The available options for the System Failure area are the following:

Write An Event To The System Log Logs the error in the system log, which allows administrators to review the error later using the Event Viewer

Send An Administrative Alert Sends an alert to the recipients specified in the Alert dialog box

Automatically Restart Check this option to have the system attempt to reboot when a fatal system error occurs

Note Configuring automatic restarts isn't always a good thing. Sometimes you might want the system to halt rather than reboot, which should ensure that the system gets proper attention. Otherwise, you can only know that the system rebooted when you view the system logs or if you happen to be in front of the system's monitor when it reboots.

The Write Debugging Information selection menu allows you to choose the type of debugging information that you want to write to a dump file. You can in turn use the dump file to diagnose system failures. The options are as follows:

None Use None if you don't want to write debugging information.

Small Memory Dump Use this option to dump the physical memory segment in which the error occurred. This dump is 64 KB in size.

Kernel Memory Dump Use this option to dump the physical memory area being used by the Windows kernel. The dump file size depends on the size of the Windows kernel.

Complete Memory Dump Use this option to dump all physical memory being used at the time of the failure. The maximum dump file size is the same as the total physical memory size.

If you elect to write a dump file, you must also set a location for the dump file. The default dump locations are %SystemRoot%\Minidump for small memory dumps and %SystemRoot%\Memory.dmp for all other memory dumps. You'll usually want to select Overwrite Any Existing File as well. This option ensures that any existing dump files are overwritten if a new STOP error occurs.

Note You can create the dump file only if the system is properly configured. The system drive must have a sufficiently large memory-paging file (as set for virtual memory with the Advanced tab), and the drive where the dump file is written must have sufficient free space as well. For example, my server has 512 MB of RAM and requires a paging file on the system drive of the same size—512 MB. Since the same drive is used for the dump file, the drive must have at least 1 gigabyte (GB) of free space to create a complete dump of debugging information correctly (that's 512 MB for the paging file and 512 MB for the dump file).

Enabling and Disabling Error Reporting

Windows Server 2003 features built-in system and program error reporting. Error reporting sends information about errors to Microsoft or to a corporate file share that administrators can monitor. Error reporting is enabled by default for all Windows Server 2003 installations, and you can configure it to monitor the following specific areas:

Windows Operating System Reports critical operating system errors that cause a blue screen crash. The error report contains all the information that's displayed on the blue screen.

Unplanned Machine Shutdowns Reports when the server is shut down and the shutdown reason is listed as unplanned. Selecting this option helps you keep track of unplanned reasons for server shutdowns, which is essential to maintaining good uptime and service records.

Programs Reports illegal program operations and internal program errors that cause a program to stop working. With program errors, you can specify which programs should be monitored for errors and which shouldn't. If you elect to report program errors, you can enable Force Queue Mode For Program Errors. In Queue mode, the last 10 errors are displayed the next time an administrator logs on and the administrator is able to choose which errors are reported. Without selecting this option, only the last error that occurs is reported, which might be misleading.

How an error is reported depends on where the error originated. When a component or program error occurs, a dialog box appears asking if you want to report the problem. If you choose to report the problem, the error report is sent over the Internet to Microsoft and a Thank You dialog box is displayed with additional information that might be helpful in resolving the problem. When an operating system error occurs, the system doesn't generate the error report until the next time you successfully boot and log on to the system.

You can enable and configure error reporting by completing the following steps:

1. Start the System utility. Click the Advanced tab and then click the Error Reporting button.
2. Select Enable Error Reporting and then select the check boxes for the areas you want to monitor.

Tip By default, all program errors are reported, regardless of who the manufacturer is. If you chose to report program errors, you can change the default configuration. To do this, select Programs, click Choose Programs in the Error Reporting dialog box, and then select All Programs In This List. You can now select programs to add to the reporting list and you can disable reporting for Programs From Microsoft and Windows Components. You can also add programs to the Do Not Report Errors list.

3. Click OK.

You can disable error reporting by completing these steps:

1. Start the System utility. Click the Advanced tab, and then click the Error Reporting button.
2. Select Disable Error Reporting, and then click OK.

Another way to configure Error Reporting is to do so through Group Policy. Because Group Policy is discussed in detail in [Chapter 4](#), "Automating Administrative Tasks, Policies, and Procedures," and in other chapters, I won't go into depth on how Group Policy works. I will tell you, however, which policies you'll want to look at to help better manage Error Reporting for the enterprise. These policies are located in Computer Configuration\Administrative Templates\System>Error Reporting and in Computer Configuration\Administrative Templates\System>Error Reporting\Advanced Error Reporting Settings.

Tip Error reporting can be distracting, but the information helps ensure that Microsoft resolves problems. To remove potential distraction, yet still help improve Windows for the future, you might want to disable Display Error Notification and enable Report Errors. When you do this, errors are automatically reported without notifying users that an error occurred.

The two most useful error reporting policies are:

Display Error Notification Determines whether users are notified when errors occur. If not configured, users can specify error notification preferences using the System utility. If disabled, users aren't notified when an error occurs (but this doesn't prevent error reporting). If enabled, users are notified when an error occurs and given the opportunity to report the error.

Report Errors Determines whether errors are reported and provides the opportunity to precisely control error reporting. If not configured, users can specify error reporting preferences using the System utility. If disabled, users won't be able to report errors but might still be notified when errors occur. If enabled, errors might be reported to Microsoft over the Internet or to a corporate file share that administrators can monitor. You can also specify whether More Information links are available, whether associated files and machine data is collected, and whether application errors are queued.

Real World Storing error reports on a file share can be helpful in resolving problems. Users might not tell you they're having problems. They might assume that a crashing program or other problems that they see are normal behavior. To be pro- active in your support, you might want to store error reports on a corporate file share. If you want to do this, create a network share and then specify the share using the Universal Naming Convention (UNC) notation, such as \\Gamma\\ErrorReports, where *Gamma* is the server name and *ErrorReports* is the network share.

Tip If you display errors and report them, you might want to customize the error reporting text with your company name. To do this, type your company name in the Replace Instances Of The Word "Microsoft" With field of the Report Errors Properties dialog box. Now your company name appears in text instead of Microsoft.

The Automatic Updates Tab

The Automatic Update tab of the System utility controls the Automatic Updates configuration on the server. This feature is discussed in the section entitled "[Understanding and Using Automatic Updates](#)" in [Chapter 5](#), "Working with Support Services and Remote Desktop."

The Remote Tab

The Remote tab of the System utility controls Remote Assistance invitations and Remote Desktop connections. These options are discussed in the section entitled "[Managing Remote Access to Servers](#)" in [Chapter 5](#).

Managing Hardware Devices and Drivers

Windows Server 2003 provides four key tools for managing hardware devices and drivers. These tools are:

- Device Manager
- Add Hardware Wizard
- Hardware Update Wizard
- Hardware Troubleshooter

You'll use these tools whenever you install, uninstall, or troubleshoot hardware devices and drivers. Before you work with device drivers, you should know the basics of signed and unsigned device drivers as well as the system settings that might prevent the use of unsigned drivers.

Working with Signed and Unsigned Device Drivers

Microsoft recommends that you use signed device drivers whenever possible. Signed device drivers have a digital signature that authenticates them as having passed rigorous testing by the Windows Hardware Quality Labs. The digital signature also means the device driver hasn't been tampered with.

Now, there are situations when you might have to use an unsigned device driver. For example, you might find that a device installed on a server doesn't have a signed device driver. Your first response should be to check the manufacturer's Web site to see if a signed driver is available. A signed driver might be available but not distributed with the device or on the Windows Server 2003 distribution disks. However, if one isn't available, you might find that you have to use an unsigned driver. You have several options:

- Install an unsigned driver; a driver that worked with Windows 2000 might work in this instance. However, the system might become unstable. The system might crash, lose data, or even fail to restart.
- Stop using the device or use a different device with supported drivers. Cost might be a factor in your decision, but it shouldn't be the only factor you consider. An unstable system costs time and money as well.

By default, Windows Server 2003 warns you if you try to install an unsigned device driver. If you don't want to see this prompt, you can change the configuration so that this warning isn't displayed. You can also specify that unsigned drivers should never be installed. One way to configure device driver settings is to use the System utility in the Control Panel:

1. Start the System utility. Click the Hardware tab and then click Driver Signing.
2. Choose the action you want Windows to take when someone tries to install an unsigned device driver. The options are:
Ignore Install the software anyway and don't ask for my approval.

Warn Prompt me each time to choose an action.

Block Never install unsigned driver software.

3. If the settings are only for the current user, clear the Make This Action The System Default check box. Otherwise, select this check box to make these settings the default for all users.
4. Click OK twice.

If you want to assign device driver settings for the enterprise, you can do this through Group Policy. In this case, Group Policy specifies the least secure setting that is allowed, and, if Group Policy is set to Block, unsigned device drivers can't be installed without overriding Group Policy.

The Code Signing For Device Drivers policy controls device driver signing settings. This policy is located in User Configuration\Administrative Templates\System. If enabled, you can specify the action to take: Ignore, Warn, or Block.

Note If you're trying to install a device and find that you can't install an unsigned driver, you should first check the System utility settings for driver signing. If you find that the settings are set to block and you can't change the setting, Code Signing For Device Drivers has been enabled and set to Block in Group Policy. You will need to override Group Policy in order to install the unsigned device driver.

Viewing and Managing Hardware Devices

You can view a detailed list of all the hardware devices installed on a system by completing the following steps:

1. Choose Start, Programs or All Programs as appropriate, Administrative Tools, and then Computer Management.
2. In the console tree, select Device Manager under System Tools. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
3. Click the plus sign (+) next to a device type to see a list of the specific instances of that device type.
4. If you right-click the device entry, you can manage the device using the shortcut menu. The options available depend on the type of device, but they include:

Disable Disables the device but doesn't uninstall it

Enable Enables a device if it's disabled

Properties Displays the Properties dialog box for the device

Uninstall Uninstalls the device and its drivers

Update Driver Updates the driver file

Tip The device list shows warning symbols if there are problems with a device. A yellow warning symbol with an exclamation point indicates a problem with a device. A red X indicates a device that's improperly installed or that has been disabled by the user or administrator for some reason.

You can use the options on the View menu in the Computer Management console to change the defaults for what types of devices are displayed and how the devices are listed. The options are as follows:

Devices By Type Displays devices by the type of device installed, such as Disk Drive or Printer. The connection name is listed below the type. This is the default view.

Devices By Connection Displays devices by connection type, such as System Board or Logical Disk Manager.

Resources By Type Displays the status of allocated resources by type of device using the resource. Resource types are direct memory access (DMA) channels, input/ output (I/O) ports, interrupt request (IRQ), and memory addresses.

Resources By Connection Displays the status of all allocated resources by connection type rather than device type.

Show Hidden Devices Displays non-Plug and Play devices as well as devices that have been physically removed from the computer but haven't had their drivers uninstalled.

Configuring Device Drivers

Device drivers are required for devices such as sound cards and display adapters to work properly. Windows Server 2003 provides comprehensive management tools for maintaining and updating device drivers. These tools allow you to track driver information, install and update driver versions, roll back to a previously installed driver, and uninstall device drivers.

Tracking Driver Information

Each driver being used on a system has a driver file associated with it. You can view the location of the driver file and related details by completing the following steps:

1. In Computer Management, select Device Manager under System Tools. You should now see a complete list of devices installed on the system identified either by type or by connection. By default, this list is organized by device type, but you can also list devices by connection using View menu options.
2. Right-click the device you want to manage and then choose Properties from the shortcut menu. This opens the Properties dialog box for the device. Click the Driver tab.
3. Display the Driver File Details dialog box by clicking Driver Details. The information displayed includes:
Driver Files Displays a list of file locations where the driver exists within %SystemRoot%

Provider The creator of the driver

File Version The version of the file

Digital Signer Indicates whether the driver is signed and by whom

Installing and Updating Drivers

To keep devices operating smoothly, it's essential that you keep their device drivers current. You can install and update drivers using the Hardware Update Wizard. By default, this wizard can search for updated device drivers in the following locations:

- On the local computer
- On a hardware installation CD
- On the Windows Update site or your organization's Windows Update server

In Group Policy, several policies control the search possibilities:

Turn Off Access To All Windows Update Features under Computer Configuration \Administrative Templates\System\Internet Communication Management Internet Communication Settings If this policy setting is enabled, all Windows Update features are blocked and not available to users. Users will also be unable to access the Windows Update Web site.

Turn Off Windows Update Device Driver Searching under Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication Settings By default, Windows Update searching is optional when installing a device. If you enable this setting, Windows Update will not be searched when a new device

is installed. If you disable this setting, Windows Update will always be searched when a new device is installed, if no local drivers are present.

Turn Off Windows Update Device Driver Search Prompt under Computer Configuration\Administrative Templates\System

If you disable or do not configure Turn Off Windows Update Device Driver Searching, this policy setting affects whether a search prompt is displayed for Windows Update of device drivers. If this policy setting is enabled, administrators aren't prompted to search Windows Update and the search will or will not take place automatically based on the Turn Off Windows Update Device Driver Searching setting. Otherwise, administrators will be prompted before Windows Update is searched.

You can install and update device drivers by completing the following steps:

1. In the Computer Management console, select Device Manager. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
2. Right-click the device you want to manage, and then select Update Driver from the shortcut menu. This starts the Hardware Update Wizard.
Tip Updated drivers can add functionality to a device, improve performance, and resolve device problems. However, you should rarely install the latest drivers on a user's computer without first testing them in a test environment. Test first, then install.
3. If the Group Policy configuration allows administrators to be prompted to determine whether Windows Update should be searched for the new driver, the first wizard page has the options shown in [Figure 2-10](#).

Figure 2-10: If allowed by Group Policy, administrators are prompted to determine whether Windows Update should be



searched.

These options are used as follows:

Yes, This Time Only Windows Update will be searched for this driver install only.

Yes, Now And Every Time I Connect A Device Windows Update will be searched automatically for driver updates. This setting applies to the installation of this driver and every time Driver Update is run.

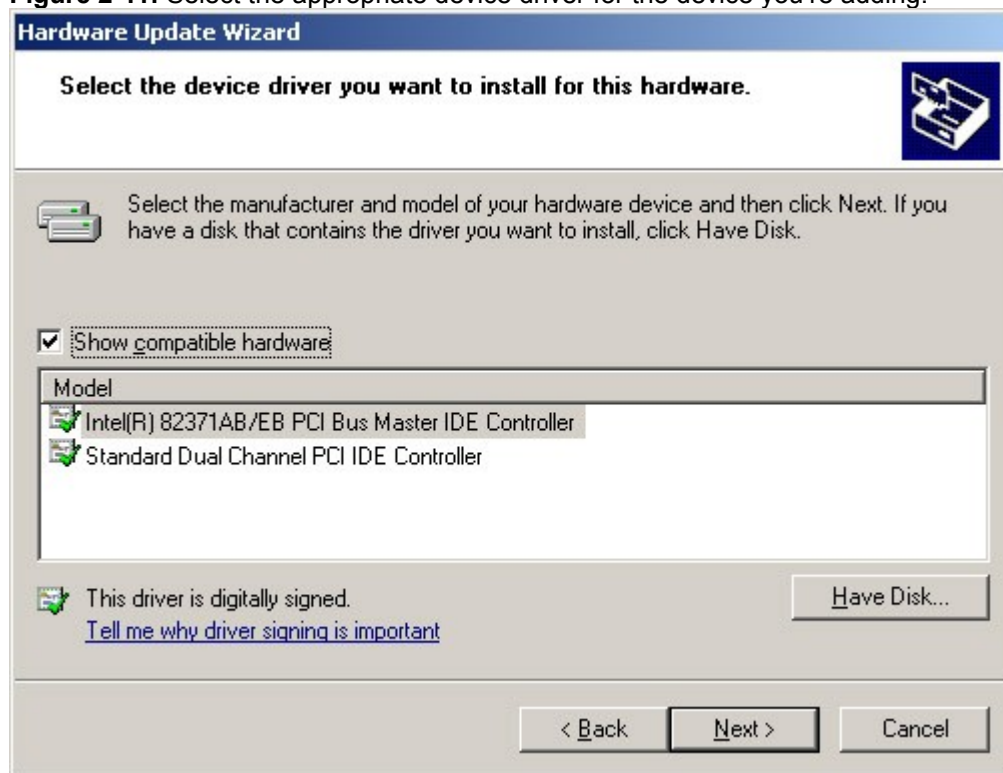
No, Not This Time Windows Update will not be searched for this install only.

4. Click Next after you make a selection. On the next page, you can specify whether you want to install the drivers automatically or manually by selecting the driver from a list or specific location.

5. If you choose to install the driver automatically, Windows Server 2003 looks for a more recent version of the device driver and, if found, installs the driver. If a more recent version of the driver is not found, Windows XP keeps the current driver. In either case, click Finish to complete the process and then skip the remaining steps.
6. If you choose to install the driver manually, you'll have the opportunity to select one of the following options:
Search For The Best Driver In These Locations If you search for drivers, the wizard checks for drivers on the driver database on the system and any of the optional locations you specify, such as a floppy disk or a CD-ROM. Any matching drivers found are displayed, and you can select a driver.

Don't Search. I Will Choose The Driver To Install If you decide to install drivers yourself, the next wizard page shows a list of compatible hardware and a recommended list of drivers for this hardware, as shown in [Figure 2-11](#). If a correct driver is listed, all you need to do is to select it. If a correct driver isn't listed, clear the Show Compatible Hardware check box. You can now view a list of manufacturers to find the manufacturer of the device. Once you find the manufacturer, select the appropriate device driver in the right pane.

Figure 2-11: Select the appropriate device driver for the device you're adding.



Note If the manufacturer or device you want to use isn't listed, insert your device driver disk into the floppy drive or CD-ROM drive, and then click Have Disk. Follow the prompts. Afterward, select the appropriate device.

7. After selecting a device driver through a search or a manual selection, continue through the installation process by clicking Next. Click Finish when the driver installation is completed. Keep in mind that in some cases you'll need to reboot the system to activate the newly installed or updated device driver.

Rolling Back Drivers

Sometimes you'll find that a device driver that you've installed causes device failure or other critical problems on a system. Don't worry; you can recover the system to the previously installed device driver. To do this, follow these steps:

1. In Computer Management, select Device Manager. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
2. Right-click the device you want to manage and then choose Properties from the shortcut menu. This opens the Properties dialog box for the device.
3. Click the Driver tab and then click Roll Back Driver. When prompted to confirm the action, click Yes. Click OK.

Note If the driver file hasn't been updated, a backup driver file won't be available. Instead of being able to roll back the driver, you'll see a prompt telling you that no driver files have been backed up for this device. If you're having problems with the device, click Yes to start the Troubleshooter. Otherwise, click No to quit.

Removing Device Drivers for Removed Devices

Usually, when you remove a device from a system, Windows Server 2003 detects the change and removes the drivers for that device automatically. Sometimes, however, when you remove a device, Windows Server 2003 doesn't detect the change and you must remove the drivers manually. You can remove device drivers manually by completing the following steps:

1. In Computer Management, select Device Manager.
2. Right-click the device you want to remove and then select Uninstall.
3. When prompted to confirm the action, click OK.

Uninstalling Device Drivers

Uninstalling a device driver uninstalls the related device. Sometimes when a device isn't working properly you can completely uninstall the device, restart the system, and then reinstall the device driver to restore normal operations. You can uninstall and then reinstall a device by completing the following steps:

1. In Computer Management, select Device Manager. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
2. Right-click the device you want to manage and then choose Uninstall from the shortcut menu.
3. When prompted to confirm the action, click OK.
4. Reboot the system. Windows should detect the presence of the device and then automatically reinstall the necessary device driver. If the device isn't automatically reinstalled, reinstall it manually as discussed in the section entitled "[Adding New Hardware](#)," later in this chapter.

Note To prevent a device from being reinstalled automatically, disable the device instead of uninstalling it. You disable a device by right-clicking it in Device Manager and then selecting Disable.

Managing Hardware

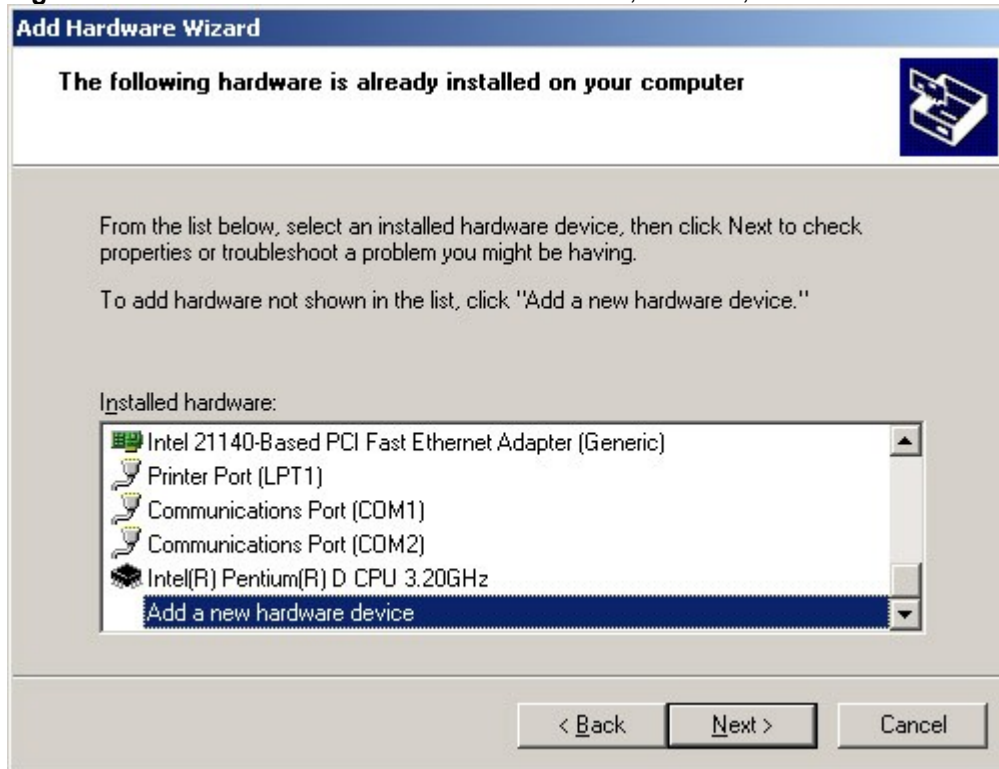
Windows Plug and Play technology does a good job of detecting and automatically configuring new hardware. However, if the hardware doesn't support Plug and Play or isn't automatically detected, you'll need to enter information about the new hardware into the Windows Server 2003 system. You do this by installing the hardware device and its related drivers on the system using the Add New Hardware Wizard. You can also use this wizard to troubleshoot problems with existing hardware.

Adding New Hardware

You can install new hardware using the Add Hardware Wizard by completing the following steps:

1. From Control Panel, select or double-click Add Hardware as appropriate. This starts the Add Hardware Wizard. Click Next.
2. At this point you have two options:
 - If you've already connected the new hardware, select Yes, I Have Already Connected The Hardware and click Next to continue. The Add Hardware Wizard screen shown in [Figure 2-12](#) should be displayed. Go on to Step 3.

Figure 2-12: Use the Add Hardware Wizard to install, uninstall, or troubleshoot hardware devices.



- If you haven't connected the hardware, click No, I Have Not Added The Hardware Yet and then click Next. The only option you have now is to click Finish. You'll need to connect the hardware (which might require shutting down the computer) and then restart the Add Hardware Wizard. Skip the remaining steps.
- 3. To add new hardware, select Add A New Hardware Device from the Installed Hardware list box and then click Next. This option is located at the very bottom of the Installed Hardware list. On the What Do You Want The Wizard To Do? page, determine whether the wizard should search for new hardware or whether you want to select the hardware from a list.
 - If you choose the search option, the wizard searches for and automatically detects new hardware. The process takes a few minutes to go through all the device types and options. When the search is completed, any new devices found are displayed, and you can select a device.
 - If you choose the manual option or if no new devices are found in the automatic search, you'll have to select the hardware type yourself. Select the type of hardware, such as Modem or Network Adapter, and then click Next. Scroll through the list of manufacturers to find the device's manufacturer, and then choose the appropriate device in the Models pane.
- 4. After you complete the selection and installation process, click Next and then click Finish. The new hardware should now be available.

Enabling and Disabling Hardware

When a device isn't working properly, sometimes you'll want to uninstall or disable it. Uninstalling a device removes the driver association for the device so that it temporarily appears that the device has been removed from the system. The next time you restart the system, Windows Server 2003 might try to reinstall the device. Typically, Windows Server 2003 reinstalls Plug and Play devices automatically, but not non-Plug and Play devices.

Disabling a device turns it off and prevents Windows Server 2003 from using it. Because a disabled device doesn't use system resources, you can be sure that it isn't causing a conflict on the system. You can uninstall or disable a device by completing the following steps:

1. In Computer Management, select Device Manager. You should now see a complete list of devices installed on the system. By default, this list is organized by device type.
2. Right-click the connection for the device you want to manage and then select one of the following options:
Enable To enable the device

Uninstall To uninstall the device

Disable To disable the device

3. If prompted to confirm the action, click Yes or OK as appropriate.

Troubleshooting Hardware

You can use the Add Hardware Wizard to troubleshoot hardware problems as well. The basic steps are as follows:

1. From Control Panel, select or double-click Add Hardware as appropriate. This starts the Add Hardware Wizard. Click Next.
2. At this point, you have two options:
 - If you've already connected the hardware that you want to examine, select Yes, I Have Already Connected the Hardware and click Next to display the Installed Hardware list box. Go on to Step 3.
 - If you haven't connected the hardware, click No, I Have Not Added the Hardware Yet and then click Next. The only option you have now is to click Finish. You'll need to connect the hardware (which might require shutting down the computer) and then restart the Add Hardware Wizard. Skip the remaining steps.
3. From the Devices list, select the hardware device that you want to troubleshoot, and then click Next. The final wizard page provides a device status. When you click Finish, the wizard does one of two things:
 - If an error code is shown with the device status, the wizard accesses the error code in the online help documentation—if it's available and installed. The help documentation should include a proposed technique to resolve the issue.
 - The wizard starts the Hardware Troubleshooter, which attempts to solve the hardware problem using your responses to the questions it asks. Follow the advice of the Hardware Troubleshooter to resolve the hardware problem.

You can also access the Hardware Troubleshooter directly. To do that, complete the following steps:

1. In the Computer Management console, select Device Manager.
2. Right-click the device you want to troubleshoot and then select Properties.
3. On the General tab, click Troubleshoot.

Managing Dynamic-Link Libraries

As an administrator, you might be asked to install or uninstall dynamic-link libraries (DLLs), particularly if you work with IT (information technology) development teams. The utility you use to work with DLLs is Regsvr32. This utility is run at the command line.

After you start a command window, you install or register a DLL by typing **regsvr32 name.dll**, for example:

```
regsvr32 mylibs.dll
```

If necessary, you can uninstall or unregister a DLL by typing **regsvr32 /u name.dll**, for example:

```
regsvr32 /u mylibs.dll
```

Note Windows File Protection prevents replacement of protected system files. You'll be able to replace only DLLs installed by the Windows Server 2003 operating system as part of a hot fix, service pack update, Windows update, or Windows upgrade. Windows File Protection is an important part of the Windows Server 2003 security architecture.

Chapter 3: **Monitoring Processes, Services, and Events**

As an administrator, it's your job to keep an eye on the network systems. The status of system resources and usage can change dramatically over time. Services might stop running. File systems might run out of space. Applications might throw exceptions, which in turn can cause system problems. Unauthorized users might try to break into the system. The techniques discussed in this chapter will help you find and resolve these and other system problems.

Managing Applications, Processes, and Performance

Any time you start an application or type a command on the command line, Microsoft Windows Server 2003 starts one or more processes to handle the related program. Generally, processes that you start in this manner are called *interactive processes*. That is, you start the processes *interactively* with the keyboard or mouse. If the application or program is active and selected, the related interactive process has control over the keyboard and mouse until you switch control by terminating the program or selecting a different one. When a process has control, it's said to be running *in the foreground*.

Processes can also run *in the background*. With processes started by users, this means that programs that aren't currently active can continue to operate—only they generally aren't given the same priority as the active process. You can also configure background processes to run independently of the user logon session; the operating system usually starts such processes. An example of this type of background process is a batch file started with an AT command. The AT command tells the system to run the file at a specified time, and, if permissions are configured correctly, the AT command can do so whether or not a user is logged on to the system.

Task Manager

The key tool you'll use to manage system processes and applications is Task Manager.

You can access Task Manager using any of the following techniques:

- Press Ctrl+Shift+Esc.
- Press Ctrl+Alt+Del and then click Task Manager.
- Type **taskmgr** into the Run utility or a command prompt.
- Right-click the taskbar and select Task Manager from the shortcut menu.

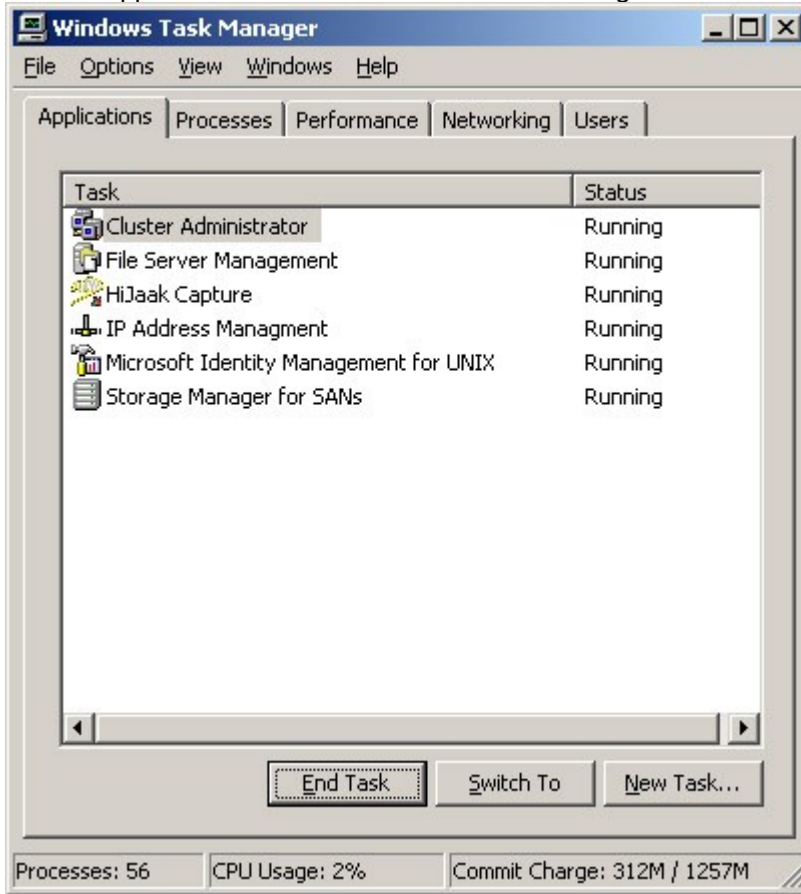
Techniques you'll use to work with Task Manager are covered in the following sections.

Administering Applications

The Applications tab of Task Manager is shown in [Figure 3-1](#). This tab shows the status of the programs that are currently running on the system. You can use the buttons on the bottom of this tab as follows:

- Stop an application by selecting the application and then clicking End Task.
- Switch to an application and make it active by selecting the application and then clicking Switch To.
- Start a new program by selecting New Task, and then enter a command to run the application. New Task functions like the Start menu's Run utility.

Figure 3-1: The Applications tab of the Windows Task Manager shows the status of programs currently running on the



system.

Tip The Status column tells you if the application is running normally or if the application has gone off into the ozone. A status of Not Responding is an indicator that an application might be frozen, and you might want to end its related task. However, some applications might not respond to the operating system during certain process-intensive tasks. Because of this, you should be certain the application is really frozen before you end its related task.

Right-clicking a Listing

Right-clicking an application's listing in the Windows Task Manager displays a shortcut menu that allows you to:

- Switch to the application and make it active.
- Bring the application to the front of the display.
- Minimize and maximize the application.
- Tile or cascade the application.
- End the application.
- Go to the related process in the Processes tab.

Note The Go To Process is very helpful when you're trying to find the primary process for a particular application. Selecting this option highlights the related process in the Processes tab.

Administering Processes

The Task Manager Processes tab is shown in [Figure 3-2](#). This tab provides detailed information about the processes that are running. By default, the Processes tab shows only processes run by the operating system, local services, network services, and the interactive user. The interactive user is the user account logged on to the local console. To see processes run by remote users, such as those connecting using a remote desktop connection, you'll need to select Show Processes From All Users.

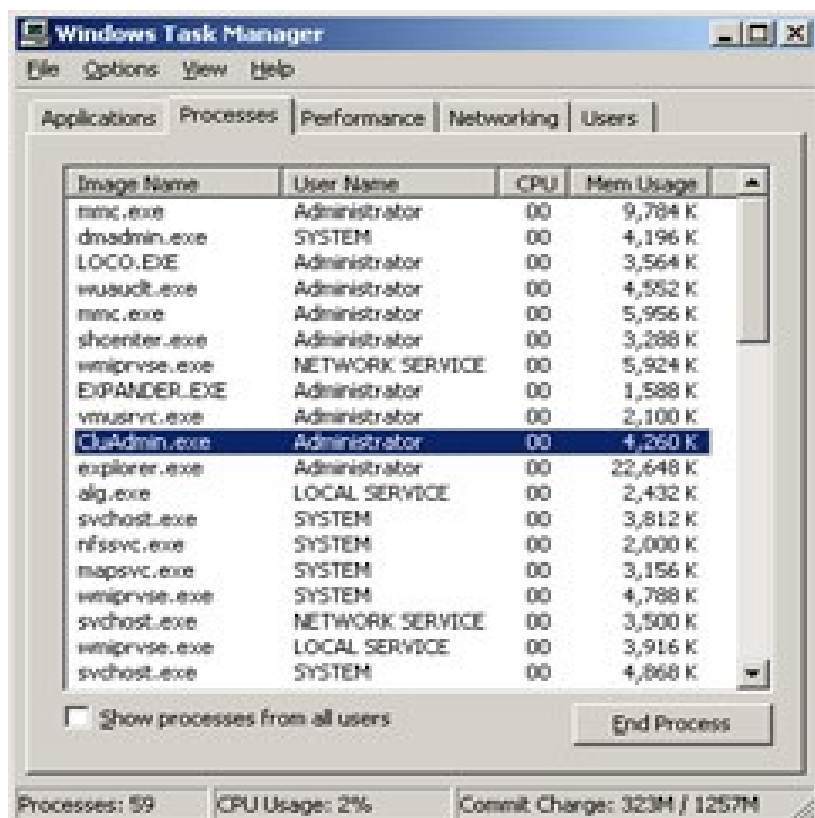
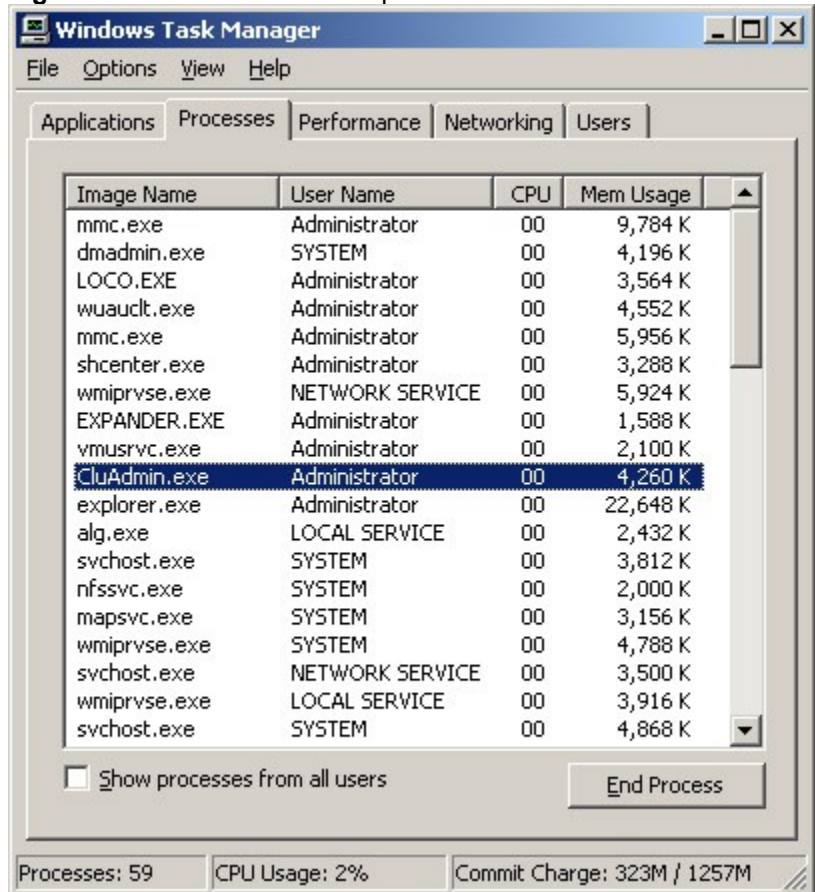


Figure 3-2: The Processes tab provides detailed information on running processes.



The fields of the Processes tab provide lots of information about running processes. You can use this information to determine which processes are hogging system resources, such as CPU time and memory. The fields displayed by default are:

Image Name The name of the process or executable running the process

User Name The name of the user or system service running the process

CPU The percentage of CPU utilization for the process

Mem Usage The amount of memory the process is currently using

If you click View and choose Select Columns, you'll see a dialog box that will let you add columns to the Processes view. When you're trying to troubleshoot system problems using process information, you might want to add these columns to the view:

Base Priority Priority determines how much of the system resources are allocated to a process. To set the priority of a process, right-click the process, choose Set Priority, and then select the new priority. Priorities are Low, Below Normal, Normal, Above Normal, High, and Real-Time. Most processes have a normal priority by default. The highest priority is given to real-time processes.

CPU Time The total amount of CPU cycle time used by the process since it was started. To quickly see the processes that are using the most CPU time, display this column and then click the column header to sort process entries by CPU Time.

Handle Count The total number of file handles maintained by the process. Use the handle count to gauge how dependent the process is on the file system. Some processes, such as those used by Microsoft Internet Information Services (IIS), have thousands of open file handles. Each file handle requires system memory to maintain.

I/O Reads, I/O Writes The total number of disk input/output (I/O) reads or writes since the process was started. Together, the number of I/O reads and writes tell you how much disk I/O activity there is. If the number of I/O reads and writes is growing disproportional to actual activity on the server, the process might not be caching files or file caching might not be properly configured. Ideally, file caching will reduce the need for I/O read and writes.

Page Faults A page fault occurs when a process requests a page in memory and the system can't find it at the requested location. If the requested page is elsewhere in memory, the fault is called a *soft page fault*. If the requested page must be retrieved from disk, the fault is called a *hard page fault*. Most processors can handle large numbers of soft faults. Hard faults, however, can cause significant delays.

Paged Pool, Non-paged Pool The *paged pool* is an area of system memory for objects that can be written to disk when they aren't used. The *non-paged pool* is an area of system memory for objects that can't be written to disk. You should note processes that require a high amount of nonpaged pool memory. If there isn't enough free memory on the server, these processes might be the reason for a high level of page faults.

Peak Memory Usage The highest amount of memory used by the process. The change or delta between current memory usage and peak memory usage is important to note as well. Applications, such as Microsoft SQL Server, that have a high delta between base memory usage and peak memory usage might need to be allocated more memory on startup so that they perform better.

Thread Count The current number of threads that the process is using. Most server applications are multithreaded. Multithreading allows concurrent execution of process requests. Some applications can dynamically control the number of concurrently executing threads to improve application performance. Too many threads, however, can actually reduce performance because the operating system has to switch thread contexts too frequently.

If you examine processes running in Task Manager, you'll note a process called System Idle Process. You can't set the priority of this process. Unlike other processes that track resource usage, System Idle Process tracks the amount of system resources that aren't used. Thus, a 99 in the CPU column for the System Idle Process means 99 percent of the system resources currently aren't being used.

As you examine processes, keep in mind that a single application might start multiple processes. Generally, these processes are dependent on a central process and from this main process a process tree containing dependent processes is formed. You can find the main process for an application by right-clicking the application in the Applications tab and selecting Go To Process. When

you terminate processes, you'll usually want to target the main application process or the application itself rather than dependent processes. This ensures that the application is stopped cleanly.

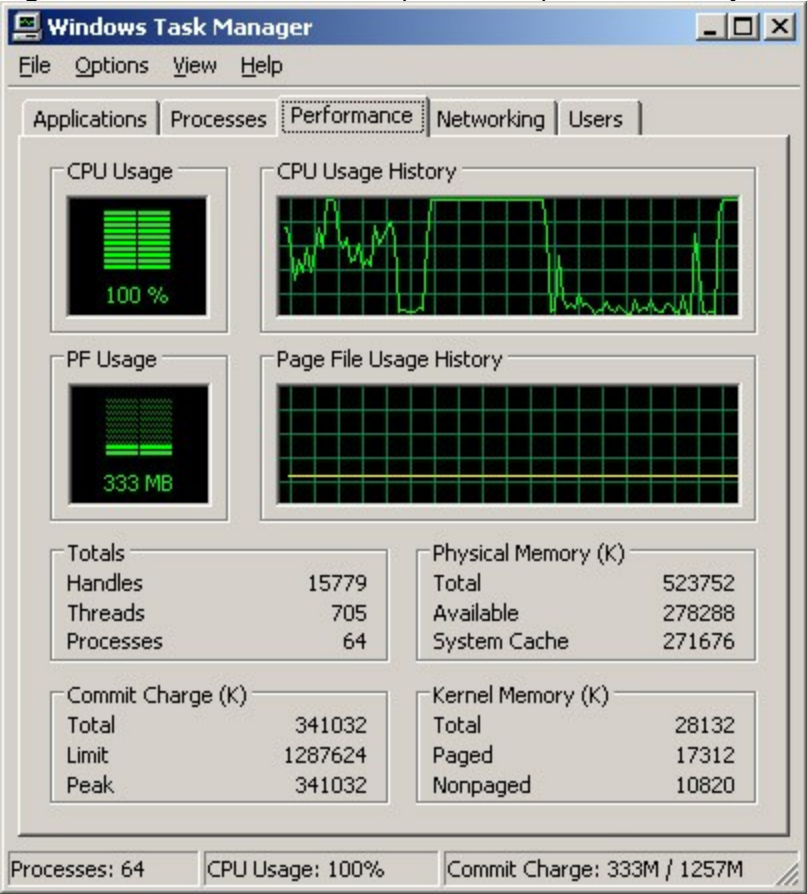
To stop the main application process and dependent processes, you have several choices. You can:

- Select the application in the Applications tab, and then click End Task.
- Right-click the main application process in the Processes tab, and then select End Process.
- Select the main or a dependent process in the Processes tab, and then select End Process Tree.

Viewing and Managing System Performance

The Task Manager Performance tab provides an overview of CPU and memory usage. As shown in [Figure 3-3](#), the tab displays graphs as well as statistics. This information gives you a quick check on system resource usage. For more detailed information, use Performance Monitor, which will be explained later in this chapter.

Figure 3-3: The Performance tab provides a quick check on system resource usage.



Graphs on the Performance Tab

The graphs on the Performance tab provide the following information:

CPU Usage The percentage of processor resources currently being used.

CPU Usage History A history graph of CPU usage plotted over time. The update speed determines how often the graph is updated.

PF Usage The amount of the paging file (or virtual memory) currently being used by the system.

Page File Usage History A history graph of paging file usage plotted over time.

Tip To view a close-up of the CPU graphs, double-click within the Performance tab. Double-clicking again returns you to normal viewing mode. If CPU usage is consistently high, even under average usage conditions, you might want to perform more detailed performance monitoring to determine the cause of the problem. Memory is often a source of performance problems, and you should rule it out before upgrading or adding CPUs. For more details, see the section entitled “[Tuning System Performance](#),” later in this chapter.

Customizing and Updating the Graph Display

To customize or update the graph display, use the following options on the View menu:

Update Speed Allows you to change the speed of graph updating as well as to pause the graph. Updates occur once every four seconds for Low, once every two seconds for Normal, and twice per second for High.

CPU History On multiprocessor systems, allows you to specify how CPU graphs are displayed. You can, for example, display one CPU in each graph or multiple CPUs in each graph.

Show Kernel Times Allows you to display the amount of CPU time used by the operating system kernel. Usage by the kernel is shown in red plotting (as opposed to green plotting, which is used otherwise).

Beneath the graphs, you'll find several lists of statistics. These statistics provide the following information:

Totals Provides information on CPU usage. *Processes* shows the number of processes in use; processes are running instances of applications or executable files. *Threads* shows the number of threads in use; threads are the basic units of execution within processes. *Handles* shows the number of I/O handles in use; I/O handles act as tokens that let programs access resources. I/O throughput and disk performance have more of an impact on a system than does a consistently high number of I/O handles.

Physical Memory Provides information on the total RAM on the system. *Total* shows the amount of physical RAM. *Available* shows the RAM not currently being used and available for use. *System Cache* shows the amount of memory used for system caching. If the server has very little physical memory available, you might need to add memory to the system. In general, you want the available memory to be no less than 5 percent of the total physical memory on the server.

Commit Charge Provides information on the total memory used by the operating system. *Total* lists all physical and virtual memory currently in use. *Limit* lists the total physical and virtual memory available. *Peak* lists the maximum memory used by the system since bootup. If the difference between the total memory used and the peak memory used is consistently large, you might want to add physical memory to the system to improve performance. If the peak memory usage is within 10 percent of the Limit value, you might want to add physical memory or increase the amount of virtual memory, or both.

Kernel Memory Provides information on the memory used by the operating system kernel. Critical portions of kernel memory must operate in RAM and can't be paged to virtual memory. This type of kernel memory is listed as *Nonpaged*. The rest of kernel memory can be paged to virtual memory and is listed as *Paged*. The total amount of memory used by the kernel is listed under *Total*.

Viewing and Managing Networking Performance

The Task Manager Networking tab provides an overview of the network adapters a system is using. You can use the information provided to quickly determine the percent utilization, link speed, and operational status usage of each network adapter configured on a system.

If a system has one network adapter, a summary graph details the network traffic on this adapter over time. If a system has multiple network adapters, the graph displays a composite index of all network connections, which represents all network traffic. By default, the graph displays only the network traffic total byte count. You can change this by clicking View, choosing Network History, and then enabling Bytes Sent, Bytes Received, or both. Bytes Sent are shown in red, Bytes Received in yellow, Bytes Total in green.

The fields of the Networking tab provide lots of information about network traffic to and from the server. You can use this information to determine how much external traffic a server is experiencing at any time. The fields displayed by default are:

Adapter Name Name of the network adapter in the Network Connections folder.

Network Utilization Percentage of network usage based on the connection speed for the interface. For example, an adapter with a link speed of 100 megabits per second (Mbps) and current traffic of 10 Mbps would have a 10 percent utilization.

Link Speed Interface connection speed as determined by the initial connection speed.

State Operational status of network adapters.

Real World	Any time you see usage consistently approaching or over 50 percent of total capacity, you'll want to start monitoring the server more closely and might also want to consider adding network adapters. Plan any upgrade carefully; there is a lot more planning required than you might think. Consider the implications not only for that server but also for the network as a whole. You might also have connectivity problems if you exceed the allotted bandwidth of your service provider—and it can often take months to obtain additional bandwidth for external connections.
-------------------	--

If you click View and choose Select Columns, you'll see a dialog box that will let you add columns to the Processes view. When you're trying to troubleshoot networking problems, you might want to add the following columns to the view:

Bytes Sent Throughput Percentage of current connection bandwidth used by traffic sent from the system

Bytes Received Throughput Percentage of current connection bandwidth used by traffic received by the system

Bytes Throughput Percentage of current connection bandwidth used for all traffic

Bytes Sent Cumulative total bytes sent on the connection to date

Bytes Received Cumulative total bytes received on the connection to date

Bytes Total Cumulative total bytes on the connection to date

Viewing and Managing Remote User Sessions

Remote users can connect to systems using Terminal Services or Remote Desktop. Terminal Services allow remote terminal connections to systems. Remote Desktop allows you to administer systems remotely as if you were sitting at the keyboard.

Remote Desktop connections are automatically enabled on Windows Server 2003 installations. One way to view and manage remote desktop connections is to use Task Manager. To do this, start Task Manager, and then click the Users tab. The Users tab shows interactive user sessions for both local and remote users.

Each user connection is listed with the user account name, session ID, status, originating client computer, and session type. A user logged on to the local system is listed with Console as the session type. Other users have a session type that indicates the connection type and protocol, such as RDP-TCP for a connection using the Remote Desktop Protocol (RDP) with Transmission Control Protocol (TCP) as the transport protocol. If you right-click user sessions, you have the following options:

Connect Connects the user session if it's inactive.

Disconnect Disconnects the user session, halting all user-started applications without saving application data.

Log Off Logs the user off, using the normal logoff process. Application data and system state information are saved as during a normal log off.

Remote Control Sets the hot keys used to end remote control sessions. The default hot keys are Ctrl+*.

Send Message Sends a console message to users logged on to remote systems.

Managing System Services

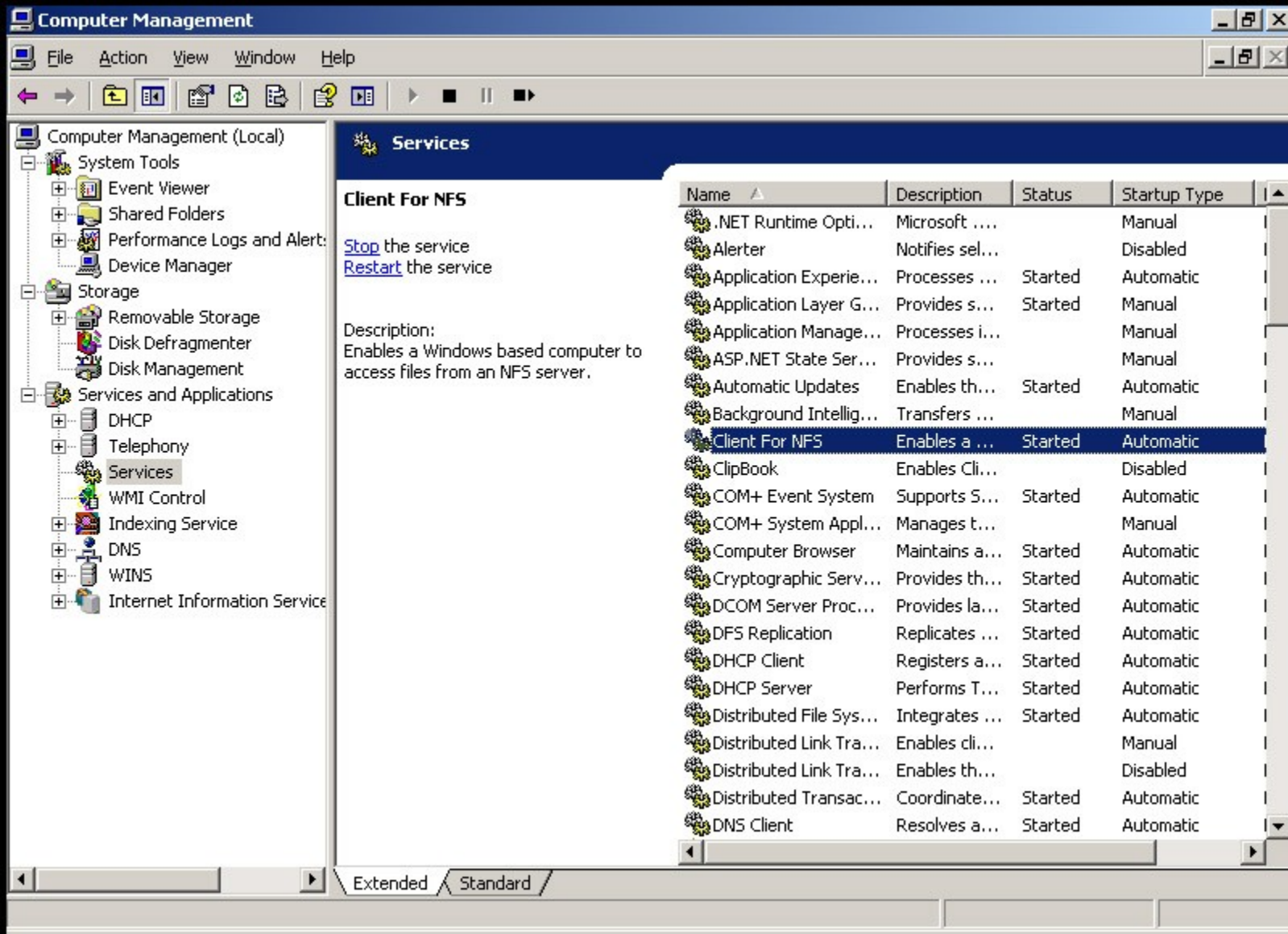
Services provide key functions to workstations and servers. To manage system services, you'll use the Services entry in the Computer Management console. You can start Computer Management and access the Services entry by completing the following steps:

- 1. Choose Start, then choose Programs or All Programs as appropriate, then Administrative Tools, and finally Computer Management. Or select Computer Management in the Administrative Tools folder.
- 2. Right-click the Computer Management entry in the console tree and select Connect To Another Computer on the shortcut menu. You can now choose the system on which you want to manage services.
- 3. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.

Note Windows Server 2003 provides several other ways to access services. For example, you can also use the Services entry in the Component Services utility.

Figure 3-4 shows the Services view in the Computer Management console. The key fields of this dialog box are used as follows:

Figure 3-4: Use the Services view to manage services on workstations and servers.



Name The name of the service. Only services installed on the system are listed here. Double-click an entry to configure its startup options. If a service you need isn't listed, you can install it by using the Network Connection Properties dialog box or the Windows Optional Networking Components Wizard. See Chapter 16, "Managing TCP/ IP Networking," for details.

Description A short description of the service and its purpose.

Status Whether the status of the service is started, paused, or stopped. (Stopped is indicated by a blank entry.)

Startup Type The startup setting for the service. Automatic services are started at bootup. Users or other services start manual services. Disabled services are turned off and can't be started while they remain disabled.

Log On As The account the service logs on as. The default in most cases is the local system account.

The Services area has two views: extended and standard. To change the view, click the tabs at the bottom of the Services area. In extended view, quick links are provided for managing services. Click Start to start a stopped service. Click Restart to stop and then start a service—essentially resetting that service. If you select a service in extended view, a service description is shown, which details the service's purpose.

Note Both the operating system and a user can disable Services. Generally, Windows Server 2003 disables services if there is a possible conflict with another service.

Starting, Stopping, and Pausing Services

As an administrator, you'll often have to start, stop, or pause Windows Server 2003 services. To start, stop, or pause a service, complete the following steps:

1. Start Computer Management and connect to the computer on which you want to manage services.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to manipulate, and then select Start, Stop, or Pause as appropriate. You can also choose Restart to have Windows stop and then start the service after a brief pause. Additionally, if you pause a service, you can use the Resume option to resume normal operation.

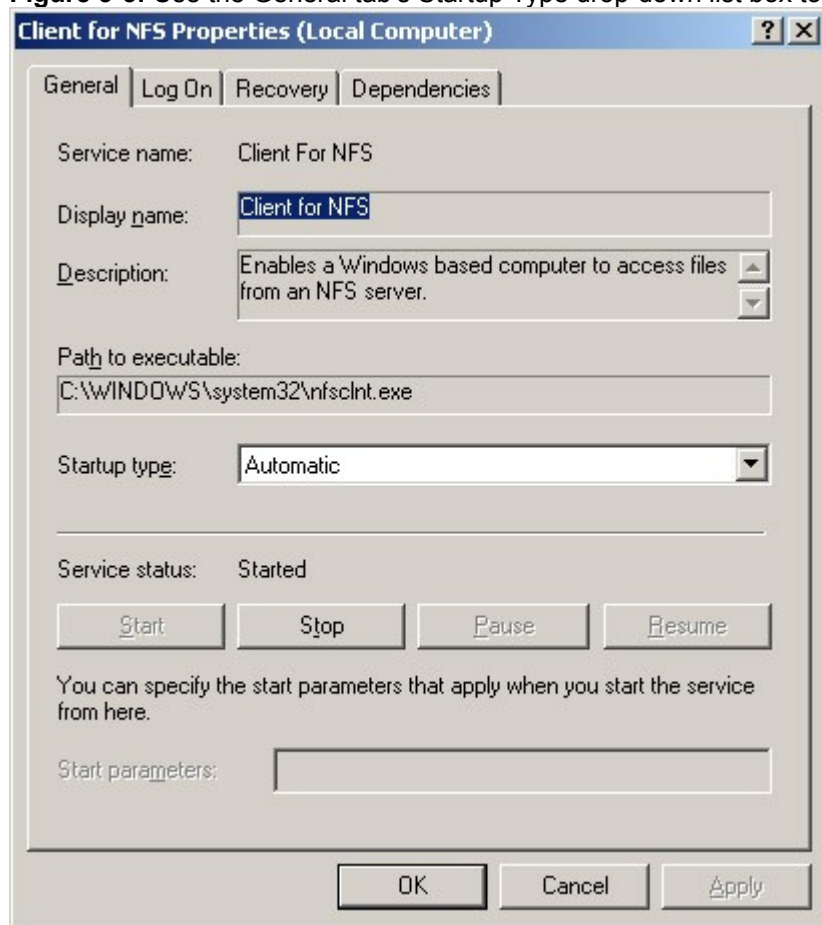
Note When services that are set to start automatically fail, the status is listed as blank and you'll usually receive notification in a pop-up dialog box. Service failures can also be logged to the system's event logs. In Windows Server 2003, you can configure actions to handle service failure automatically. For example, you could have Windows Server 2003 attempt to restart the service for you. For details, see the section entitled "[Configuring Service Recovery](#)," later in this chapter.

Configuring Service Startup

You can set Windows Server 2003 services to start manually or automatically. You can also turn them off permanently by disabling them. You configure service startup by completing the following steps:

1. In the Computer Management console, connect to the computer whose services you want to manage.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to configure, and then choose Properties.
4. In the General tab, use the Startup Type drop-down list box to choose a startup option, as shown in [Figure 3-5](#). Select Automatic to start services at bootup. Select Manual to allow the services to be started manually. Select Disabled to turn off the service. Click OK.

Figure 3-5: Use the General tab's Startup Type drop-down list box to configure service startup options.



Real World

When a server has multiple hardware profiles, you can enable or disable services for a particular profile. Before you disable services permanently, you might want to create a separate hardware profile for testing the server with these services disabled. In this way, you can use the original profile to quickly resume operations using the original service status. The profile doesn't save other service configuration options, however. To enable or disable a service by profile, use the Log On tab of the Service Properties dialog box. Select the profile that you want to work with under Hardware Profile, and then click Enable or Disable as appropriate.

Configuring Service Logon

You can configure Windows Server 2003 services to log on as a system account or as a specific user. To do either of these, complete the following steps:

1. In the Computer Management console, connect to the computer whose services you want to manage.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to configure, and then choose Properties.
4. Select the Log On tab, as shown in [Figure 3-6](#).



Figure 3-6: Use the Log On tab to configure the service logon account.

5. Select Local System Account if the service should log on using the system account (which is the default for most services). If the service provides a user interface that can be manipulated, select Allow Service To Interact With Desktop to allow users to control the service's interface.
6. Select This Account if the service should log on using a specific user account. Be sure to type an account name and password in the text boxes provided. Use the Browse button to search for a user account, if necessary. Click OK.

Security As an administrator, you should keep track of any accounts that are used with services. These accounts can be the source of huge security problems if they're not configured properly. Service accounts should have the strictest security settings and as few permissions as possible while allowing the service to perform necessary functions. Typically, accounts used with services don't need many of the permissions you would assign to a normal user account. For example, most service accounts don't need the right to log on locally. Every administrator should know what service accounts are used (so they can better track use of these accounts), and the accounts should be treated as if they were administrator accounts. This means: secure passwords, careful monitoring of account usage, careful application of account permissions and privileges, and so on.

Configuring Service Recovery

You can configure Windows Server 2003 services to take specific actions when a service fails. For example, you could attempt to restart the service or run an application. To configure recovery options for a service, complete the following steps:

1. In the Computer Management console, connect to the computer whose services you want to manage.
2. Expand the Services And Applications node by clicking the plus sign (+) next to it, and then choose Services.
3. Right-click the service you want to configure, and then choose Properties.
4. Click the Recovery tab, as shown in [Figure 3-7](#).

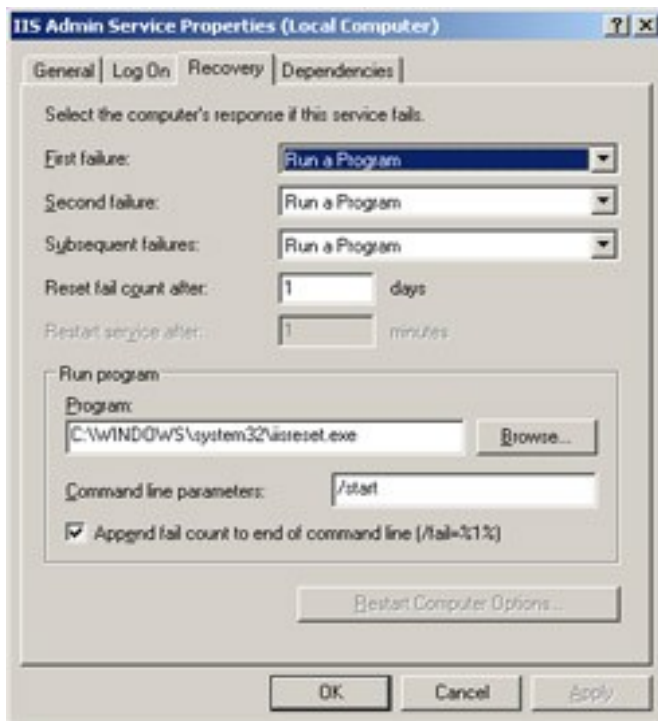


Figure 3-7: Use the Recovery tab to specify actions that should be taken in case of service failure.

Note Windows Server 2003 automatically configures recovery for some critical system services during installation. In [Figure 3-7](#), you see that the IIS Admin service is set to run a program called `lisreset.exe` if the service fails. This program is an application that corrects service problems and safely manages dependent IIS services while working to restart the service. `lisreset.exe` requires the command line parameter `/start` as well.

5. You can now configure recovery options for the first, second, and subsequent recovery attempts. The available options are:
Take No Action The operating system won't attempt recovery for this failure but might still attempt recovery of previous or subsequent failures.

Restart the Service Stops and then starts the service after a brief pause.

Run a Program Allows you to run a program or a script in case of failure. The script can be a batch program or a Windows script. If you select this option, set the full file path to the program you want to run and then set any necessary command line parameters to pass in to the program when it starts.

Restart the Computer Shuts down and then restarts the computer. Before you choose this option, double-check Startup and Recovery options as well as Hardware Profile options, as discussed in the sections entitled "[Configuring System Startup and Recovery](#)" and "[Configuring the Way Hardware Profiles Are Used](#)," respectively, in [Chapter 2](#), "Managing Servers Running Microsoft Windows Server 2003." You want the system to select defaults quickly and automatically.

Best Practices When you configure recovery options for critical services, you might want to try to restart the service on the first and second attempts and then reboot the server on the third attempt.

6. Configure other options based on your previously selected recovery options. If you elected to run a program as a recovery option, you'll need to set options in the Run Program panel. If you elected to restart the service, you'll need to specify the restart delay. After stopping the service, Windows Server 2003 waits for the specified delay before trying to start the service. In most cases, a delay of 1–2 minutes should be sufficient. Click OK.

Disabling Unnecessary Services

As an administrator, it's your job to ensure server and network security, and unnecessary services are a potential source of security problems. For example, in many organizations that I've reviewed for security problems, I've found servers running Worldwide Web Publishing Service, Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP) Publishing Service when these services weren't needed. Unfortunately, these services can make it possible for anonymous users to access servers and can also open the server to attack if not properly configured.

If you find services that aren't needed, you have several options. In the case of IIS Admin services, Domain Name System (DNS), and other services that are installed as separate Windows components, you could use the Add/Remove Programs utility in Control Panel to remove the unnecessary component and its related services. Or, you could simply disable the services that aren't being used. Typically, you'll want to start by disabling services rather than uninstalling components. This way, if you disable a service and another administrator or a user says they can't perform task X anymore, you can restore the related service, if necessary.

To disable a service, follow these steps:

1. In Computer Management, right-click the service you want to disable, and then choose Properties.
2. In the General tab, select Disabled as the option for the Startup Type drop-down list box.

Disabling a service doesn't stop a running service. It only prevents it from being started the next time the computer is booted, meaning the security risk still exists. To address this, click Stop in the Properties dialog box in the General tab, and then click OK.