

ITProTM
SERIES

Windows
& NET MAGAZINE

 **eBooks**

Windows 2003: Active Directory Administration Essentials

By Jeremy Moskowitz



netiq

mission critical software for e-business



Contents

Chapter 1 Windows Server 2003 — What's New	1
Introduction	1
A Chapter-by-Chapter Roadmap to the Book	1
Windows 2003 Editions	2
Windows 2003, Standard Edition	3
Features Common to Three Windows 2003 Editions	4
Active Directory (AD)	4
Network Load Balancing (NLB)	4
Internet Information Services (IIS) 6.0	4
Internet Connection Firewall (ICF)	4
Remote Access	5
Remote Desktop for Administration	5
Server Event Tracking	6
Manage Your Server Wizard	9
Help File	10
Volume Shadow Copy for Shares	10
IP Security (IPSec) over NAT	10
Microsoft .NET Framework	10
Windows 2003, Enterprise Edition	11
Windows 2003, Datacenter Edition	12
Windows 2003, Web Edition	13
Windows 2003 32-Bit and 64-Bit Processing	13
Windows 2003 Hardware Requirements	14
Real-World Windows 2003 Hardware Requirements	15
Keeping Your System Updated and Secure	15
Driver Signing	16
Driver Rollback	16
Automatic Updates	18
Software Updates with SUS	18
IIS Improvements	19
IIS Remote Administration Mode	20
Should You Deploy?	21
Onward — to Windows 2003 AD	22

Chapter 1

Windows Server 2003 — What's New

Introduction

If you're downloading this eBook, you probably want to know why you should care about Microsoft's latest server OS — Windows Server 2003 (Windows 2003). Inside, you'll discover which features might be important to you and why. Whether you're a Windows 2000-with-Active Directory (AD) expert or a Windows NT administrator who's been reading all the trade journals about Microsoft's new server family — this book is for you.

To get the most from this eBook, you should have a working knowledge of Win2K and some AD experience. However, if you're new to AD, you can still make good use of the information that you find here.

Windows 2003 brings much that's either new or improved to the table. I discuss the new features and improvements in some depth. In addition, I discuss key topics that many Windows texts fail to cover, such as AD backup and recovery. I occasionally compare Windows 2003 to Win2K to illustrate both the similarities and the important new differences between the two server OSs.



Note

This book differs from several currently available Windows 2003 books in that it's based on experience with the actual product — not with beta code and outdated screens. The advantage to you is that you won't be missing any "late-breaking" information.

A Chapter-by-Chapter Roadmap to the Book

To begin, let me give you a chapter-by-chapter roadmap for the book:

Chapter 1: Windows Server 2003 — What's New

Chapter 1 introduces Windows 2003's notable new non-AD-related features. You'll want to become familiar with what Windows 2003 offers in preparation for the in-depth discussions of Windows 2003 and AD. In addition, knowing these features can help you make a solid business case for deploying Windows 2003.

Chapter 2: What's New in Windows Server 2003 Active Directory

Chapter 2 covers the different AD domain and forest modes. You might be familiar with Windows 2000's Mixed and Native modes. Windows 2003 adds a new mode specific to this new server OS. In this chapter, I discuss how to prepare your existing domains for Windows 2003 with AD.

Chapter 3: What's New in Windows Server 2003 Management

Chapter 3 introduces some excellent Windows 2003 management features, including new Active Directory Users and Computers features and the Group Policy Management Console (GPMC). I

2 Windows 2003: Active Directory Administration Essentials

also review how to use AD's advanced management features to tie together your Windows 2003, Win2K, and NT domains.

Chapter 4: Inside Windows Server 2003 Forests and DNS

Chapter 4 explores Windows 2003's new cross-forest trusts – demonstrating precisely how to control resources – via the new Authentication Firewall and SIDFiltering techniques. Additionally, I cover what's new with Windows 2003 DNS: Conditional Forwarding, DNS Stub zones, and the new DNSLint tool.

Chapter 5: Windows Server 2003 Security Enhancements

Chapter 5 covers client side security with Windows 2003's new required server rules. I'll discuss the new ACL editor and explain how Windows 2003 deals with schema changes and revisions, along with other security enhancements.

Chapter 6: Backup, Restore, and Recovery for Windows Server 2003 and Active Directory

Chapter 6 discusses Windows 2003 AD backup and restore features, including the ins and outs of resurrecting objects after they've been deleted. You'll want to know how Windows 2003 addresses this situation.

Chapter 7: Command-Line, Support, and Microsoft Windows Server 2003 Resource Kit Tools

Chapter 7 introduces Windows 2003's extensive set of tools. I cover the plethora of command-line tools, support tools, and the *Microsoft Windows Server 2003 Resource Kit* tools.

Chapter 8: Windows Server 2003 Special Domain Operations

Chapter 8 reviews a new Windows 2003 domain renaming feature. You can now rename both domain controllers (DCs) and complete domains. Should your organization name change from smallcollege.edu to huge-u.edu, for example, you won't be plagued by the old name remaining in the domain.

Windows 2003 offers much that's new and even more that's improved. Over the next several months, I'll cover the key features in bite-sized chunks. So, welcome to Windows 2003 and AD. It won't be long until you're ready to go forth and deploy!

Jeremy Moskowitz
jeremym@moskowitz-inc.com

If you want to contact me with specific Windows 2003 questions, I'll take a shot at answering them or directing you to a solid specific resource. However, I might not be able to research every question in depth.

Windows 2003 Editions

Like the Win2K and NT server OSs, Windows 2003 comes in several sizes. According to Microsoft, you can find a size for every type of business. Win2K offers three servers editions and one client. Windows 2003 offers four server editions and no client — that is, the client comes in the form of Windows XP Professional. Table 1.1 presents the different versions of Win2K Server and Windows 2003 and their clients side by side.

The two most commonly deployed Windows 2003 server editions will probably be Windows 2003, Standard Edition and Windows 2003, Enterprise Edition. You might well be asked to influ-

ence a purchasing decision between the two. Knowing which features each edition offers can help you and your company make the best business decision.



Note

Windows 2003, Standard Edition might be just the ticket for most businesses' day-to-day needs. However, to weigh which server edition might be right for your business, examine the features listed in the following text.

Table 1.1

Win2K and Windows 2003 servers and clients

	Windows 2000	Windows 2003
Departmental server	Win2K Server	Windows 2003, Standard Edition
General use server	Win2K Advanced Server	Windows 2003, Enterprise Edition
Mission-critical server	Win2K Datacenter Server	Windows 2003, Datacenter Edition
One-stop-shop server for all business needs	Win2K Small Business Server	Windows 2003, Small Business Server Edition
Web server	None	Windows 2003, Web Edition
Preferred client	Win2K and Windows XP work equally well	Windows XP supports extra features and optimization.

I explore the different Windows 2003 server editions to give you an overview of each server's capabilities, beginning with Windows 2003, Standard Edition to establish a baseline. I then list the features common to Windows 2003, Standard Edition, Windows 2003, Enterprise Edition, and Windows 2003, Datacenter Server, before I continue with individual edition overviews.

Windows 2003, Standard Edition

According to Microsoft, Windows 2003, Standard Edition targets departments and small businesses with IT departments for use as a general purpose server. It performs the usual server functions of ensuring that users can access data in all forms (e.g., through file and print services), housing database systems, running complex business processes, and providing a communications gateway, such as a VPN.

Windows 2003, Standard Edition can accommodate Four-way Symmetric Multiprocessing (SMP) machines, which means that the Standard Edition servers can contain up to four processors. Windows 2003, Standard Edition can accommodate up to 4GB of memory — no matter how many processors you have in the system. You'll enjoy the room.

4 Windows 2003: Active Directory Administration Essentials



Tip

Windows 2003 introduces a new feature that – if you have enough RAM to support it – lets you eliminate your Windows swap file completely. Consider using this feature *only* if you have enough RAM to do without your swap file completely. In Task Manager, view the Performance tab. Inspect the “Commit Charge” entry to see if the peak commit is less than the physical memory. If it is, you should be able to eliminate the swap file.

Windows 2003, Standard Edition is the follow-on to Win2K Server. In theory, you can simply pop the Windows 2003, Standard Edition CD-ROM into existing Win2K servers and upgrade them “in place.” However, note the caution below.



Caution

Only upgrade your Win2K servers to Windows 2003 with a change-management plan.

Features Common to Three Windows 2003 Editions

Now that I’ve introduced Windows 2003, Standard Edition, let me briefly review features common to several of the server editions. The Windows 2003, Standard Edition, Windows 2003, Enterprise Edition, and Windows 2003, Datacenter Server Edition servers provide a gaggle of new or updated features. In the following text, I discuss some of these features. Windows 2003, Web Edition’s features are significantly different, as I point out later in this chapter. (Windows 2003, Small Business Server Edition hasn’t yet been released. The server will include many features, such as a built-in version of Exchange. However, specifications aren’t currently available.)



Note

I mention the features that Microsoft introduced in the various Win2K Server editions for comparison only.

Active Directory (AD)

Win2K Server brought us AD. Although the first iteration of AD wasn’t designated AD 1.0, it sometimes seemed to be missing features. That situation has changed in Windows 2003 with what I call “Active Directory 1.1.” As was true with Win2K, DCs still house AD components, respond to client authentication requests, and share the AD database. I discuss these basic units of AD and the newest AD features in Chapter 2, Chapter 3, and Chapter 8. Windows 2003 offers too many new AD features to list here.

Network Load Balancing (NLB)

Win2K Server didn’t support NLB. However, Windows 2003, Standard Edition supports two-node NLB. Windows 2003, Enterprise Edition and Windows 2003, Datacenter Edition support additional nodes, as you’ll see where they’re covered individually. (My research indicates that Windows 2003, Web Edition doesn’t support NLB.)

Internet Information Services (IIS) 6.0

Windows 2003 IIS 6.0 offers improved architecture and improved speed. The increased speed is impressive. The Lockdown Wizard is now included rather than being a downloadable add-on.

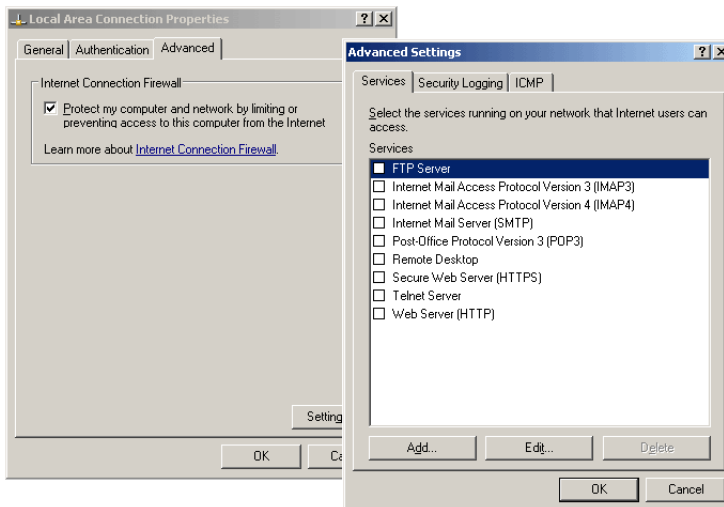
Internet Connection Firewall (ICF)

All Windows servers now have a basic stateful Internet firewall, which Figure 1.1 shows. ICF can block or permit traffic by specific traffic type or to specific ports. The “big brother” of this built-in feature is Microsoft’s Internet Security and Acceleration (ISA) Server 2000. Although ICF isn’t “industrial strength,” it performs basic security functions.

Remote Access

Microsoft has improved Windows remote access. Specifically, remote access includes a useful new feature — the Network Access Quarantine Control feature — that lets you “quarantine” users. Briefly, here’s how the feature works: If client systems don’t run software that you specify, such as a service pack or a virus scanner, those client systems are quarantined and can’t access your network.

Figure 1.1
The Internet Connection Firewall



Tip

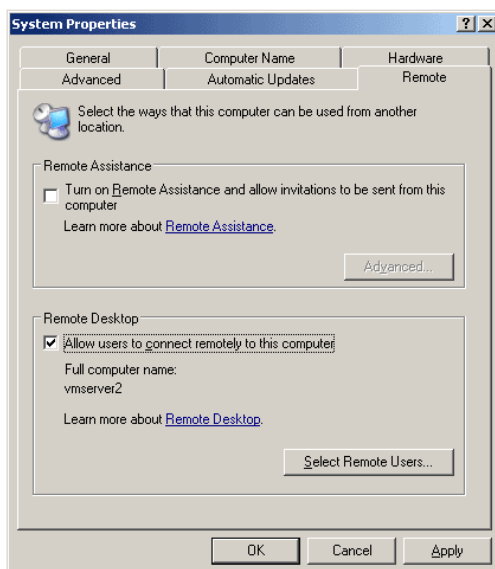
The remote access quarantine is a bit difficult to work with. You can download the complete details at the following URL:

<http://www.microsoft.com/windowsserver2003/docs/quarantine.doc>

Remote Desktop for Administration (Terminal Services in Remote Administration mode)

Win2K introduced many of us to the world of Terminal Services. You'll recall that Win2K has two modes for Terminal Services — Full Terminal Services mode (also called Application server mode) and Terminal Services — Administration Mode (also called Remote administration mode). The latter mode let two administrators remotely administer the server as if they were practically standing at the console. With Win2K, you could choose one of the two modes mentioned or choose not to select a terminal services mode. After loading Terminal Services mode, Win2K requires a reboot. In contrast, Windows 2003 by default loads the necessary files for the equivalent of Terminal Services — Administration Mode. To finish enabling Terminal Services — Administration Mode, you need only select the Remote Desktop check box on the Remote tab of the server's System Properties, which Figure 1.2 shows.

Figure 1.2
Enabling Remote Desktop



Server Event Tracking

Microsoft has tried to ensure that latest server editions are the most reliable ever. In the past, many users shut down and restarted their servers for various reasons, some of them inappropriate. With NT, for example, it might often have made sense to reboot a server on a Saturday night to clear out the memory and prevent server crashes the following week. With Windows 2003, Microsoft

intends to prove to everyone — including your management — that the servers will stay up until administrators take them down.

To that end, Microsoft has included a small reporting window into which administrators can type precisely why they choose to shut down a server. The EventcombMT tool from the *Windows Server 2003 Resource Kit* can parse the logs from all servers and highlight why administrators reboot servers.



Note

I discuss more Resource Kit tools in Chapter 7: Command-Line, Support, and Microsoft Windows Server 2003 Resource Kit Tools.

Figure 1.3 shows a Windows 2003 Event tracking Shut Down Windows screen. In the Shut-down Event Tracker Option segment of the dialog box, you can specify by category why you're shutting the server down.

Figure 1.3

Windows 2003 event-tracking Shut Down Windows screen



Figure 1.4 shows the option selected in Figure 1.3, including the comment field that lets you enter more detailed information about why you shut down the server. The record of server shut-downs might be valuable both to you and to Microsoft.

Figure 1.4
Shutdown Event Tracker comment field



You might not want to use the Shutdown Event Tracker. Figure 1.5 shows the policy you use to disable the mechanism. You can enable and disable Shutdown Event Tracker through the Group Policy Object Editor.

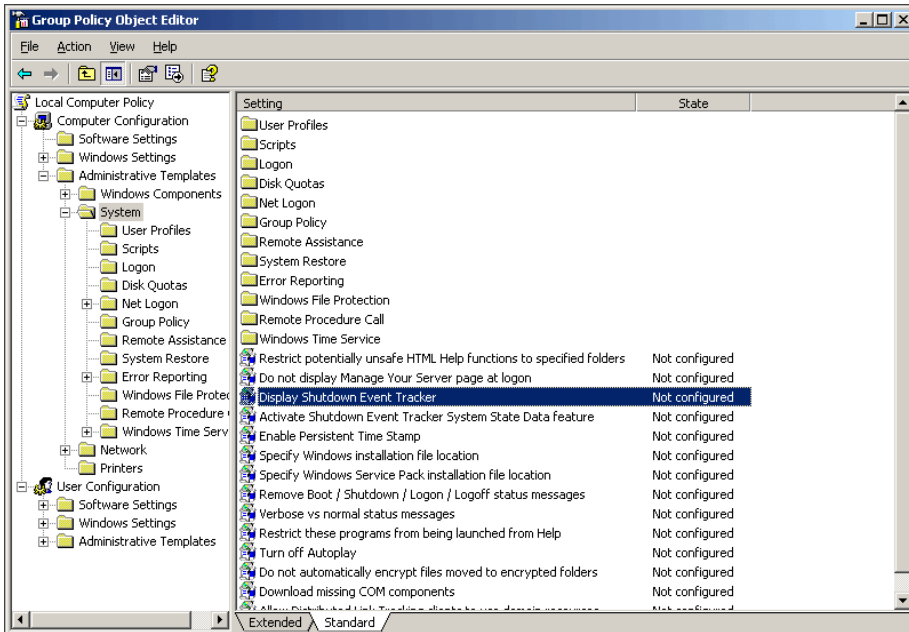


Tip

You might find the mechanism for disabling the shutdown event annoying, especially in a testing environment in which machines are rebooted all the time. You might want to turn this feature off for some servers, but certainly not for all. With that in mind, you can use these steps to turn off the Server Event Tracking on a particular server.

1. Click Start, Run, and type in GPEDIT.MSC.
2. Traverse to Computer Settings, System, Display Shutdown Event Tracker.
3. Disable the policy.

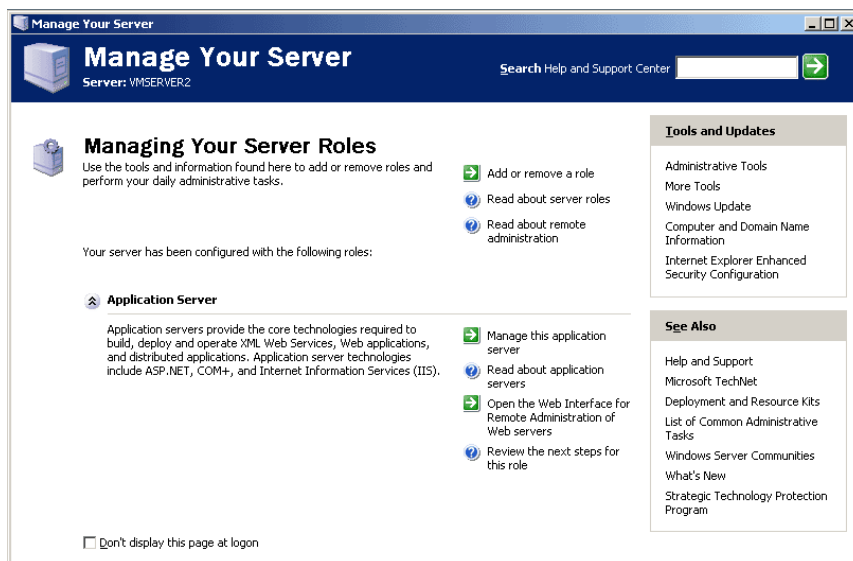
Figure 1.5
The Display Shutdown Event Tracker policy



Manage Your Server Wizard

Windows 2003 updates the Manage Your Server Wizard. Even if the Win2K wizards turned you off, give the Windows 2003 wizards a shot. You might still choose to do your day-to-day tasks manually, but know that the Windows 2003 wizards often offer a faster way to accomplish a task. For example, the Manage Your Server Wizard that Figure 1.6 shows lets you easily add or remove a server role.

Figure 1.6
The Manage Your Server Wizard



Help File

Figure 1.7 shows the Windows 2003 Help file, which you'll find highly useful. Microsoft and the entire Online Help team have outdone themselves in the level of detail provided at each turn of the virtual page. I usually click the Index button (circled in the screen shot), then track down what I need instead of relying on the (somewhat slow) Search facility.

Volume Shadow Copy for Shares

In conjunction with an XP client, this feature lets users “roll back” a data file to a particular point in time or restore a deleted file.

IP Security (IPSec) over NAT

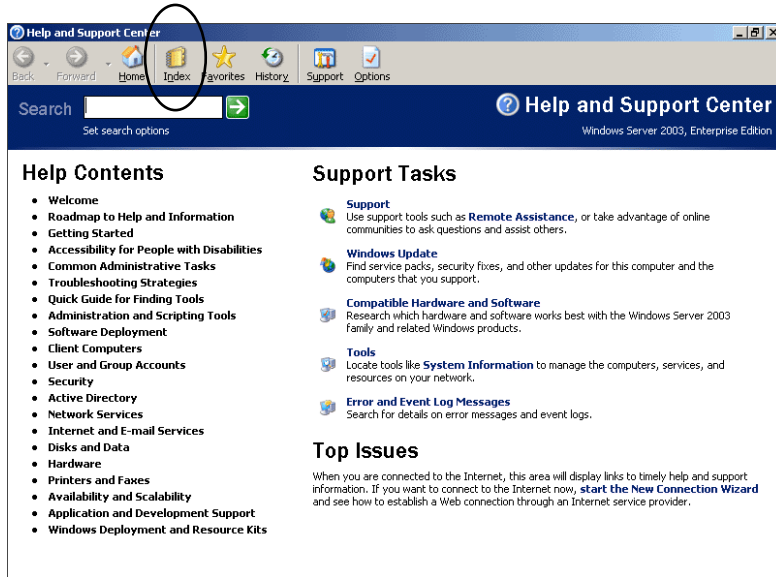
IPSec is a superior way to secure wired communications between any client and server. In the past, the problem has been that if either machine were behind a NAT or NAT-style router or fire-wall, IPSec didn't work 100 percent. Windows 2003's IPSec over NAT feature can encrypt both the header and payload parts of a packet over NAT. IPSec over NAT is an excellent new feature for servers in DMZs or in other areas that use NAT.

Microsoft .NET Framework

The .NET Framework lets programmers do new magic — and much of that new magic will take the form of Web services and IIS. System administrators and AD administrators won't need to use

or know much about the .NET Framework. Because the framework is already deployed inside the OS, it's one less thing you need to address today.

Figure 1.7
The Windows 2003 Help file



Windows 2003, Standard Edition might offer all the server firepower you need to run your business. However, as I explore Windows 2003, Enterprise Edition, you'll see that it offers considerably more.

Windows 2003, Enterprise Edition

Windows 2003, Enterprise Edition can accommodate from 1 to 8 processors and up to 32GB of memory. In addition to the general increase in hardware support, you might find support for key features that your business needs. Consider whether your business could benefit now (or might benefit soon) from one of the features listed here.



Tip

If you think you might not use all the Windows 2003, Enterprise Edition features immediately but might use them in the future, it's best to invest the dollars up front and get Enterprise Edition today, rather than deploying Windows 2003, Standard Edition. Why? Because you can't "upgrade" from Windows 2003, Standard Edition to Windows 2003, Enterprise Edition. Choosing wisely at this stage is paramount.

12 Windows 2003: Active Directory Administration Essentials

Windows 2003, Enterprise Edition offers more scalability features than either Windows 2003, Standard Edition or Win2K AS.

- Clustering has been increased from the four nodes available in Win2K AS to eight nodes.
- NLB has increased from the four nodes available in Win2K AS to eight nodes.
- Terminal Services offers a new load-balancing feature in the new Terminal Services Session Directory. The feature provides a front-end NLB that lets clients easily find an available Terminal Server in a Terminal Server farm.
- Microsoft will support the Microsoft Metadirectory Services (MMS) add-on, a centralized service meant to bridge the gap between disparate directories such as AD and iPlanet. Apparently, Microsoft is designing the Windows 2003 version of MMS for deployment upon Enterprise Edition servers only.

Still other Windows 2003, Enterprise Edition features are available only if your hardware can leverage those features. The features listed below require high-end servers.

- “Hot-add memory” lets you add memory to a server while it’s running and allocate that memory to the rest of the server.
- Non-Uniform Memory Access (NUMA) is a hardware-specific feature that returns low-level information from the hardware to NUMA-compliant applications. This returned data can fine-tune NUMA-aware applications in real time based on the system’s total stress level.

Windows 2003, Datacenter Edition

Windows 2003, Datacenter Edition is Microsoft’s “big-boy” OS. Datacenter Edition integrates OEM hardware tightly with Microsoft software to guarantee specific levels of uptime.

Because Windows 2003, Datacenter Server is available only from OEMs, it might be the least often deployed of the Windows 2003 servers. Nevertheless, when you see it deployed, you’ll recognize its tremendous power.

Windows 2003, Datacenter Edition supports up to 32 processors and up to 64GB of RAM. The clustering capability equals that of the Windows 2003, Enterprise Edition (eight nodes), which is greater than that of its Win2K Datacenter counterpart (four nodes).

The Datacenter Edition adds one special hardware hook — hyperthreading support. Hyperthreading lets certain Intel processors perform almost double duty. In fact, the Datacenter Edition server can abstract a single processor and make it appear and work as if it were really two physical processors. On some single-processor hyperthreading systems, Windows appears to be using two processors.



Note

For more information about the Windows 2003, Datacenter Edition server program, visit the URL below.

<http://www.microsoft.com/windowsserver2003/evaluation/overview/datacenter.msp>

Windows 2003, Web Edition

Windows 2003, Web Edition is totally new among the Windows server progeny. Microsoft has one short-term goal in selling this server: to compete with Linux — at least in the Web services market. Linux is popular among Web systems, and Microsoft's Windows 2003, Web Edition is meant to tackle this growing threat head on.

Like the Windows 2003, Datacenter Edition, Windows 2003, Web Edition is not for sale through retail channels. To purchase a Windows 2003, Web Edition server, you must work with specific Windows 2003, Web Edition partners (e.g., Hewlett Packard — HP, Dell, IBM, NEC, Unisys).

Windows 2003, Web Edition isn't as packed with features as other server family members. In fact, you can quickly grasp the nature of this edition by considering what it can't do. Windows 2003, Web Edition

- can't be a DC (however, it can be a domain member)
- is limited to 2GB of memory and two processors
- can't be clustered
- doesn't support NLB
- lacks services for Macintosh
- lacks Windows Media Services
- lacks Remote Installation Services (RIS)
- doesn't support 64-bit Itanium-family processors
- doesn't support Hot-Add memory
- doesn't support NUMA
- doesn't support ICF

Windows 2003, Web Edition is both the least costly and the least flexible of the server family. Its single purpose is to serve Web pages.



Tip

You can find more information about Windows 2003 at the following URL:

<http://www.microsoft.com/windowsserver2003/evaluation/overview/web.mspx>

Windows 2003 32-Bit and 64-Bit Processing

Microsoft plans to revise its Windows 2003 server line for the new 64-bit Itanium processors. In fact, some pieces of the 64-bit puzzle are available today. Clearly, 64-bit computing should jump processing muscle forward much as the change from 16-bit to 32-bit computing jumped it forward several years ago. Microsoft is betting on the Itanium-family of processors, including Itanium 1 and Itanium 2. With that in mind, Table 1.2 shows you what each 64-bit version can handle.

Table 1.2
Windows 2003 64-bit capabilities

Product	Processors	RAM
Windows 2003, Standard Edition	Won't be available in a 64-bit edition.	
Windows 2003, 64-Bit Enterprise Edition	1 — 8	64GB Maximum
Windows 2003, 64-Bit Datacenter Edition	8 — 64	512GB Maximum
Windows 2003, Web Edition	1 — 2	2GB Maximum
Windows XP Pro, 64-Bit Edition	2 (Itanium 1 or Itanium 2)	16 GB



Tip

You can find more information about XP Professional 64-bit edition at the following URL:

<http://www.microsoft.com/windowsxp/64bit/techinfo/planning/techoverview/default.asp>

Windows 2003 Hardware Requirements

Your move to a Windows 2003 installation must start with adequate hardware. Microsoft has published specifications for minimum required hardware, which Table 1.3 shows.

Table 1.3
Minimum hardware requirements for Windows 2003 installations

	Standard	Enterprise	Enterprise 64-Bit	Web	Datacenter
CPU Type	Pentium II	Pentium II	Itanium 1	Pentium II	Contact a Datacenter vendor for details.
Speed	133MHz	133MHz	733MHz	133MHz	
RAM	128MB	128MB	128MB	128MB	
Disk	1.5GB	1.5GB	2.0GB	1.5GB	



Note

Although processor speed and processor type aren't strictly enforced when you attempt to install, the amount of RAM is. For example, if you don't have 128MB of RAM, you can't load Windows 2003 on a Pentium-class system.

Real-World Windows 2003 Hardware Requirements

Minimum requirements might work well for a test machine or two, but true production systems require a bit more firepower. Table 1.4 shows my recommended minimum hardware requirements for real-world systems.

Table 1.4

Real-world minimum hardware requirements for Windows 2003 installations

	Standard	Enterprise	Enterprise 64-Bit	Web	Datacenter
CPU type	Pentium 4	Pentium 4	Itanium 1 or Itanium 2	Pentium 4	Contact a Datacenter vendor for details.
Speed	2GHz	2GHz	733MHz	2GHz	
RAM	256MB – 1GB	256MB – 1GB	256MB – 1GB	256MB – 512MB	
Disk	9GB + Storage for data	9GB + Storage for data	9GB + Storage for data	9GB + Storage for data	

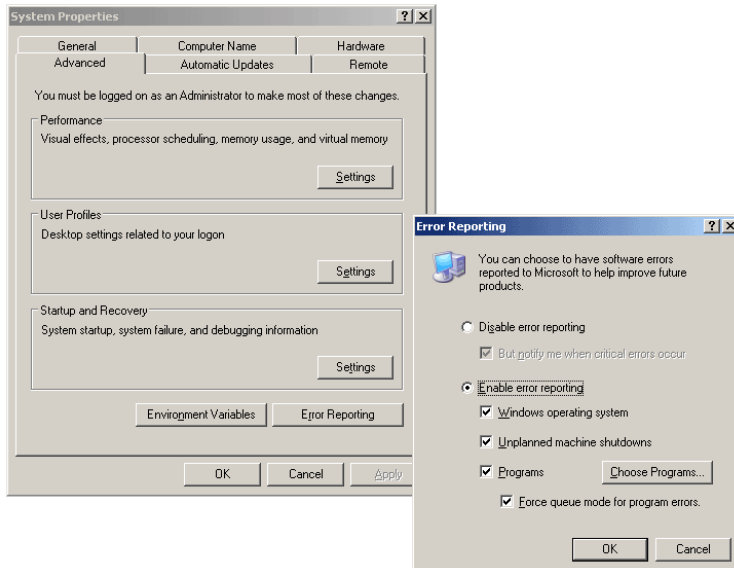
Keeping Your System Updated and Secure

Microsoft is “packing in” Windows 2003 features toward the goal of keeping the network up and running and available to user requests. Windows can go belly up — but usually it doesn't just “happen.” For example, frequently damage occurs when bad drivers are installed despite the OS's attempts to address the problem. Although loading an imperfect driver doesn't always mean curtains for the OS, it can result in the blue screen of death that Microsoft refers to as a bugcheck.

If your network experiences problems, you can send a message to Microsoft in several ways. One way is through the new error-reporting mechanism, which Figure 1.8 shows.

You can specify that an error report be sent when the Windows OS fails and when other loaded programs fail. You can select those programs through the Choose Programs button that Figure 1.8 shows. As you can see, the default selection involves all Microsoft programs and Windows components. In most environments, you might want to keep error reporting enabled. I'm not sure how Microsoft is going to evolve this feature to offer better support; however, I can see the company using it to improve the product or link your error reports with your activation ID so that Microsoft's support services can better assist you if you call for support. (Those who are paranoid can disable the error-reporting feature.)

Figure 1.8
Enabling or disabling error reporting in System Properties



Driver Signing

Driver signing isn't new with Windows 2003, but it's a highly useful feature. This feature lets you block drivers that haven't undergone Windows Hardware Quality Labs (WHQL) testing and signing. The default sets up Driver Signing to warn you when you're about to load an unsigned driver, as Figure 1.9 shows. I recommend that you consider raising the level on all your servers to *Block — Never install unsigned driver software*.

Driver Rollback

Even if a driver that shouldn't have been loaded is loaded, you have another chance to excise it from your system. You can use the Driver Rollback feature that Figure 1.10 shows to roll back the current driver to the most recent previously installed driver.



Note

The Driver Rollback feature isn't designed to keep histories of all the drivers for a device that you've ever loaded. It "remembers" only your most recent previously installed driver.

Figure 1.9
Selecting the Driver Signing level in System Properties

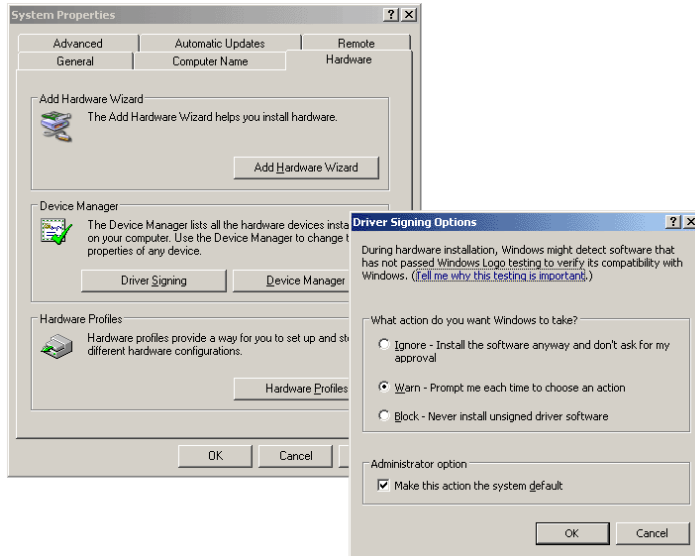
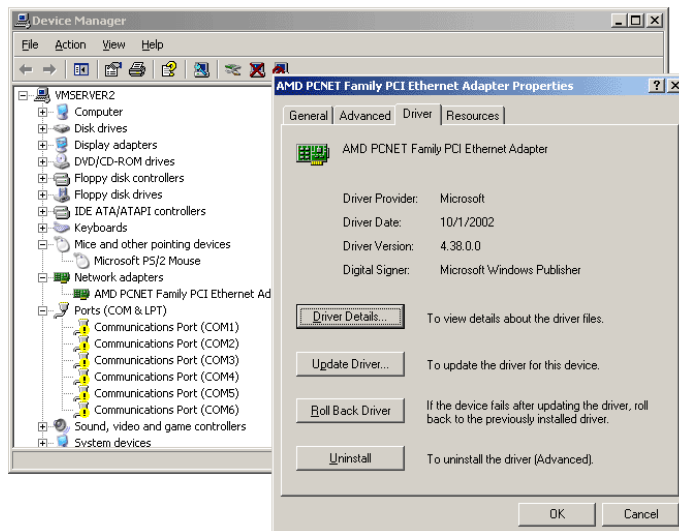


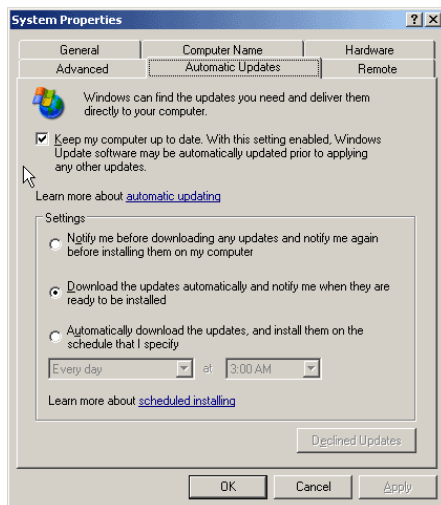
Figure 1.10
Driver Rollback feature in Device Manager



Automatic Updates

Windows 2003 now allows automatic updating when patches become available between service packs. You can choose between different modes that can help you keep your Windows 2003 servers updated, as Figure 1.11 shows.

Figure 1.11
Configuring Automatic Updates in System Properties



Software Updates with SUS

Despite the capabilities of the Automatic Update feature, the most effective way to manage Microsoft's patch updates is to disable the Automatic Update service and set up Microsoft Software Update Services (SUS), which Figure 1.12 shows. Using SUS helps ensure that new Microsoft patches are well integrated into your environment. You can test the patches you want to update in a test lab, then distribute the patches you need to your servers and clients.

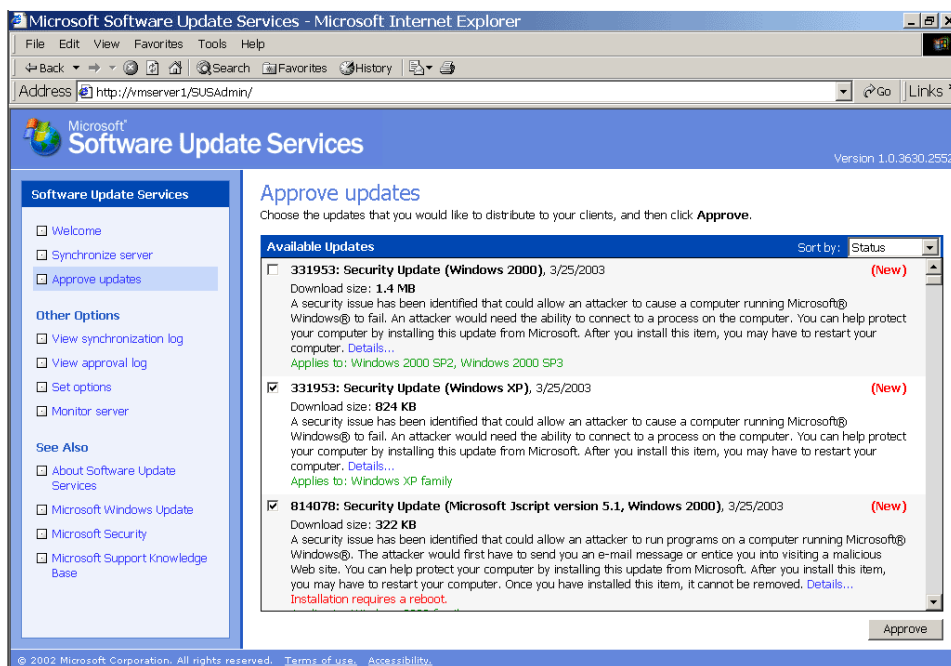
You could load SUS on a Windows 2003 or Win2K server or DC, then use group policy to distribute instructions to target machines about how to download and install the patches. For more information, see the Windows and .NET Magazine Network Security Administrator article at <http://www.secdadministrator.com/articles/index.cfm?articleid=37938> or my article at <http://www.mcpcmag.com/features/article.asp?editorialid=336>



Tip

You can leverage the power of Microsoft's free SUS to specify which patches you want to send to your systems. It's a simple task for an Administrator to test the proposed patch offline in the test lab, then select which patches will go to servers and clients. SUS is available for download from Microsoft at <http://www.microsoft.com/windowsxp/64bit/techinfo/planning/techoverview/default.asp>

Figure 1.12
Microsoft SUS



IIS Improvements

Microsoft Internet Information (IIS) Services 6.0 is a wholesale IIS overhaul. In a nutshell, IIS 6.0 is

- faster
- more secure
- easier to administer

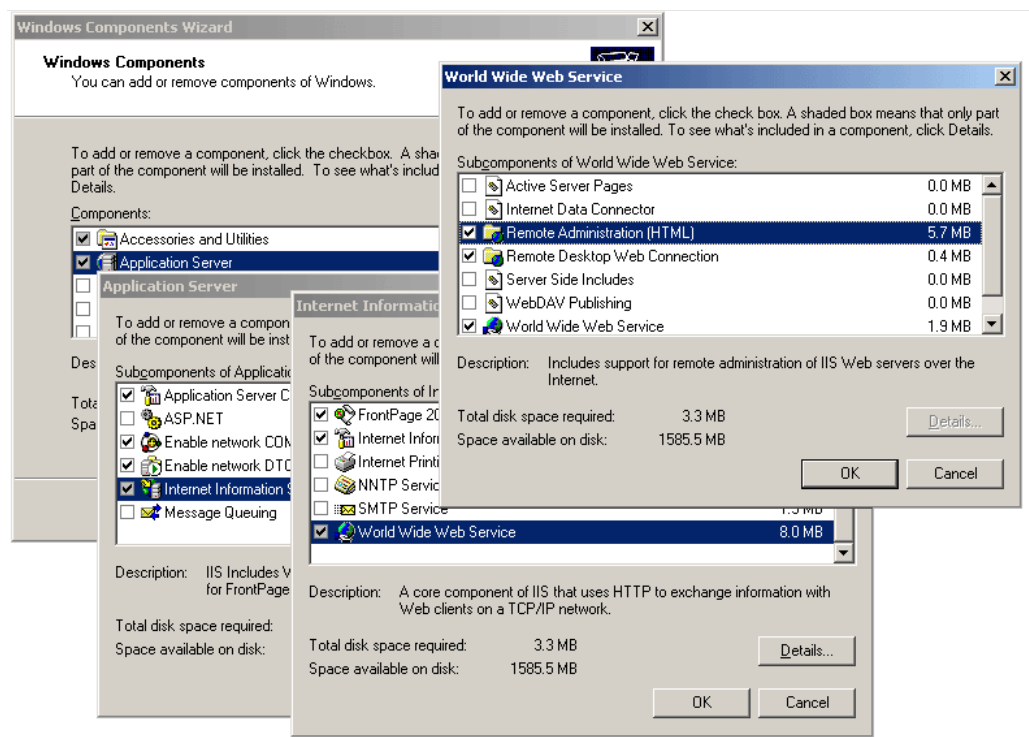
Did I mention that it's faster? IIS 6.0 is so much faster than previous IIS versions that its speed is hard to describe. Why is it faster? Microsoft has moved the HTTP processor from user mode to kernel mode, a move that makes IIS 6.0 dramatically faster.

Space constraints keep me from delving into and describing all the IIS 6.0 architecture and security changes. For an in-depth look at the changes, be sure to read Brett Hill's *Windows & .NET Magazine* article "IIS Overhauled in Version 6.0," which you'll find at the following URL:
<http://www.winnetmag.com/windowsserver2003/index.cfm?articleid=38285>

IIS Remote Administration Mode

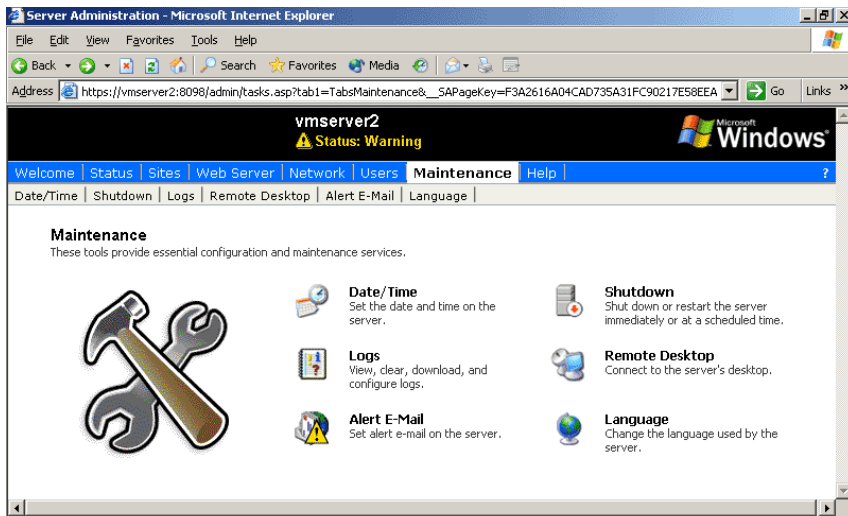
If you want to set up your servers so you can administer them remotely — from any Web browser anywhere in the world — you can do so by enabling Remote Administration Mode. You must go to Add/Remove Windows Components, then traverse to Application Server, Internet Information Services, World Wide Web Service, and Remote Administration (HTML), as Figure 1.13 shows.

Figure 1.13
Setting Up Remote Administration



When you're ready to use Remote Administration Mode, go to <http://<servername>8089>. You'll be prompted for credentials. After you're in, poke around to see what you can do from a Web browser. Figure 1.14 indicates some of what you can accomplish after you set up Remote Administration Mode.

Figure 1.14
Remote Administration Mode



Tip

You can't load Remote Administration if the target server is a DC.

Should You Deploy?

Now that Windows 2003 is generally available, it's certainly worth a look. But how can you decide whether you're ready to deploy it? You'll have to ask yourself some questions about the current state of your network to see whether, after you commit to Windows 2003, the installation will remain an uphill battle. You can begin your assessment by asking yourself these questions:

- Am I currently running on older hardware?
If yes, evaluate your hardware to make sure it won't prohibit the upgrade to Windows 2003.
- Do I have many custom applications or Web applications?
With every new OS release, application incompatibilities can be a problem. With that in mind, you'll need to test and retest each custom application if you want it to run on Windows 2003. Moreover, given the dramatic changes Microsoft has made to IIS 6.0, if you have Web applications, you need to ensure that they won't break after you upgrade to IIS 6.0.

- What will deployment cost?

Do you have a Microsoft licensing agreement that lets you upgrade to Windows 2003? If so, you'll pay only the labor costs of performing the application tests and the upgrade — not the software costs.

If you don't have a licensing agreement that lets you upgrade to Windows 2003, try to figure out how many licenses you'll need. Be especially careful after you introduce your first Windows 2003 DC. I'm not an expert on Microsoft licensing, but my understanding is that after you introduce your first Windows 2003 DC, you'll need to get current on all your Client Access Licenses (CALs). Definitely check with your Microsoft licensing representative to get the full scoop on the upgrade costs.



Tip

The article at the following URL provides some information about Microsoft licensing:
<http://www.winnetmag.com/Articles/Index.cfm?ArticleID=24033>

Onward — to Windows 2003 AD

In terms of Windows 2003 features, I've barely scratched the surface. Some of the features I've described are "skin deep" but useful. Others offer dramatic improvements over previous capabilities. Yet other features kick in when you use Windows 2003 as an AD DC, as I explore in Chapter 2: What's New in Windows Server 2003 Active Directory and Chapter 3: What's New in Windows Server 2003 Management.