

TECHNICAL REFERENCE

Building

the Small Business Infrastructure

Mark Burnett
Kathy Ivens
Jeremy Moskowitz
Michael Otey
Dustin Puryear



i n v e n t



Contents

About the Authors	iii
Introduction	iv
Chapter 1 SBS 2003 Overview	1
SBS 2003 Standard Edition vs. SBS 2003 Premium Edition	1
Installation and Initial Setup	2
Administration	2
Exchange and SharePoint Services	7
Licensing	8
Meeting the Needs of Today's Small Business	9
Chapter 2 Windows Decision Point	10
Know Your Score	10
The Quiz	11
Question 1: Is Your Business Mostly NT or Mostly Win2K?	11
Question 2: How Much Do You Leverage IIS?	12
Question 3: How Much Do You Leverage Clustering?	12
Question 4: How Much Do You Leverage Exchange?	12
Question 5: Do You Have Branch Offices?	13
Question 6: Will You Use Cross-Forest Trusts?	13
Question 7: How Much Do You Leverage Terminal Services?	14
Question 8: Do You Plan to Pair Windows 2003 with XP?	15
Question 9: How Much Do You Leverage Group Policy?	15
Question 10: How Much Do You Leverage SAN/NAS Technology?	16
Tally Your Score	16
Chapter 3 Advanced Patch Management	17
Check the Signatures	17
Check the Files	18
Watch the Installation Order	18
Don't Rely Exclusively on Automatic Updates	19
Double-Check the Hotfix Checkers	19
Don't Forget Other Updates	20

Know When to Reinstall	21
Keep Up with Fixes	22
Know Where to Get Help	22
Chapter 4 Getting Started with Remote Administration	23
Installing Terminal Services in Win2K	23
Enabling Remote Desktop in Windows 2003	24
Installing the Client Software for Win2K Terminal Services	24
Installing the Client Software for Windows Server 2003 Remote Administration	25
Performing Administrative Tasks Remotely	25
Taking Over the Console Session in Windows 2003	25
Chapter 5 Powering Databases with MySQL	27
Installing MySQL on Your Server	27
Sidebar: Predefined MySQL Accounts	28
Creating and Accessing a Database	28
Connecting to MySQL from Windows Applications	31
Using MySQL from the Command Line	32
Using MySQL in a Script	33
A Patch-Management Script	33
More Flexibility, Lower Cost	35

About the Authors

Mark Burnett (mburnett@xato.net) is an independent security consultant and author who specializes in Windows security. He is an IIS MVP and the author of *Hacking the Code* (Syngress).

Kathy Ivens (kivens@winnetmag.com) is a senior contributing editor for *Windows & .NET Magazine*. She has written more than 50 books and hundreds of magazine articles about various computer subjects.

Jeremy Moskowitz (jeremym@moskowitz-inc.com) runs <http://www.gpoanswers.com>, a community forum about Group Policy. He is an MCSE and the author of *Windows 2003: Active Directory Administration Essentials* (*Windows & .NET Magazine* eBooks) and *Windows 2000: Group Policy, Profiles, and IntelliMirror* (Sybex).

Michael Otey (mikeo@teca.com) is senior technical editor for *Windows & .NET Magazine* and president of TECA, a software-development and consulting company in Portland, Oregon. He is coauthor of *ADO.NET: The Complete Reference* (Osborne/McGraw-Hill).

Dustin Puryear (dustin@puryear-it.com) is a consultant providing expertise in managing and integrating UNIX and Windows systems and services. He is the author of *Integrate Linux Solutions into Your Windows Network* (Premier Press) and *Best Practices for Managing Linux and UNIX Servers* (*Windows & .NET Magazine* eBooks).

Introduction

Every company is faced with the task of managing time, money, and assets to ensure the success of the organization. Managing these resources in a small to midsized business is especially crucial and presents several unique challenges. For instance, take the costs associated with managing a small to midsized business's IT needs. A small to midsized business's needs are different than the needs of larger organizations. Dedicated IT staffs are rare and dedicated technology specialists (e.g., someone who focuses solely on security, database administration, or messaging) are almost unheard of. Most small to midsized businesses either outsource their IT needs to a service provider or rely on a full-time employee who's unlucky enough to know something about computers and thus becomes the de factor computer guy.

So how do you keep costs down while maximizing your investment? This eBook will help you plan your IT infrastructure to get the most out of your systems while minimizing the costs involved. Chapter 1 provides an overview of Microsoft Small Business Server (SBS) 2003. You'll learn about the differences between the two versions of SBS 2003: SBS 2003 Standard Edition and SBS 2003 Premium Edition. Chapter 1 also explains how to set up and configure, administer, and license SBS 2003. In Chapter 2, you'll be able to take a Windows Decision Point quiz and tally your score to help you determine whether your organization should upgrade to Windows Server 2003 to take advantage of new computing features.

Chapter 3 describes advanced techniques that small and midsized businesses can use to keep crucial servers up to date so that you can stay on top of the latest security hotfixes. Chapter 3 also lists resources that provide free products for checking hotfixes, often-overlooked product updates, and automated patch-management solutions.

Chapter 4 teaches you how to use terminal services to remotely administer your Windows 2003 and Windows 2000 servers. You'll learn how to install and enable the client and server terminal services software, how to perform tasks remotely, and how to take over the console session so that you can interact with the remote system. In Chapter 5, you'll learn how to lower your licensing and operating costs by using a powerful, comprehensive, and free database solution called MySQL. This book will provide you with the insight you need to make the most of your IT resources to help your small or midsized business succeed.

Chapter 1:

SBS 2003 Overview

—by *Michael Otey*

According to research firm IDC, small business is currently one of the biggest growth areas for IT. In the small-business market segment, IDC predicts an 11.6 percent annual growth rate in server deployment, with a corresponding 19.3 percent annual increase in broadband usage through 2006. This growth will be fueled by the continued reduction in the price of server hardware and an increase in the availability of affordable broadband services. Microsoft's most recent Small Business Server (SBS) 2003 release targets the needs of this emerging small-business market. Designed for businesses with 75 or fewer workstations or users, SBS 2003 is the fourth generation of Microsoft's SBS product line, and it boasts simpler installation, configuration, and management than any previous SBS version.

SBS 2003 Standard Edition vs. SBS 2003 Premium Edition

Unlike earlier versions of SBS, SBS 2003 comes in two versions: SBS 2003 Standard Edition and SBS 2003 Premium Edition. Table 1-1 lists the components of each edition.

Table 1-1 SBS 2003 Standard Edition and SBS 2003 Premium Edition Comparison

Component	SBS 2003 Standard Edition	SBS 2003 Premium Edition
Windows Server 2003	X	X
Exchange Server 2003	X	X
Outlook 2003	X	X
SharePoint Services v2	X	X
FrontPage 2003		X
SQL Server 2000 (SP3)		X
ISA Server 2000		X
5 CALs	X	X

Both versions of SBS 2003 include Windows Server 2003 (with its integrated Microsoft Windows SharePoint Services feature), Microsoft Exchange Server 2003, Microsoft Office Outlook 2003, and five Client Access Licenses (CALs). To this base of core components, SBS 2003 Premium Edition adds Microsoft SQL Server 2000 Service Pack 3 (SP3), Microsoft FrontPage 2003, and Microsoft Internet Security and Acceleration (ISA) Server 2000.

The choice between the two versions essentially boils down to whether you need SQL Server. Although a firewall, such as the one that ISA Server provides, is essential, many broadband routers already incorporate firewall capabilities. SBS 2003 Standard Edition includes a basic firewall, but it isn't as full featured as most commercial firewalls. If you need SQL Server, then the bundled pricing of SQL Server 2000 as a part of SBS 2003 Premium Edition makes the premium edition a good buy.

2 Building the Small Business Infrastructure

However, if you don't need SQL Server, then SBS 2003 Standard Edition is a better choice. The budget-conscious small-business owner could also choose SBS 2003 Standard Edition and add Microsoft Access, Microsoft Data Engine (MSDE), or a freeware database such as MySQL along with a third-party firewall for functionality comparable to SBS 2003 Premium Edition for less cost. In addition, you can often gain a performance advantage by installing the database on a different server from the server that's running Exchange.

Installation and Initial Setup

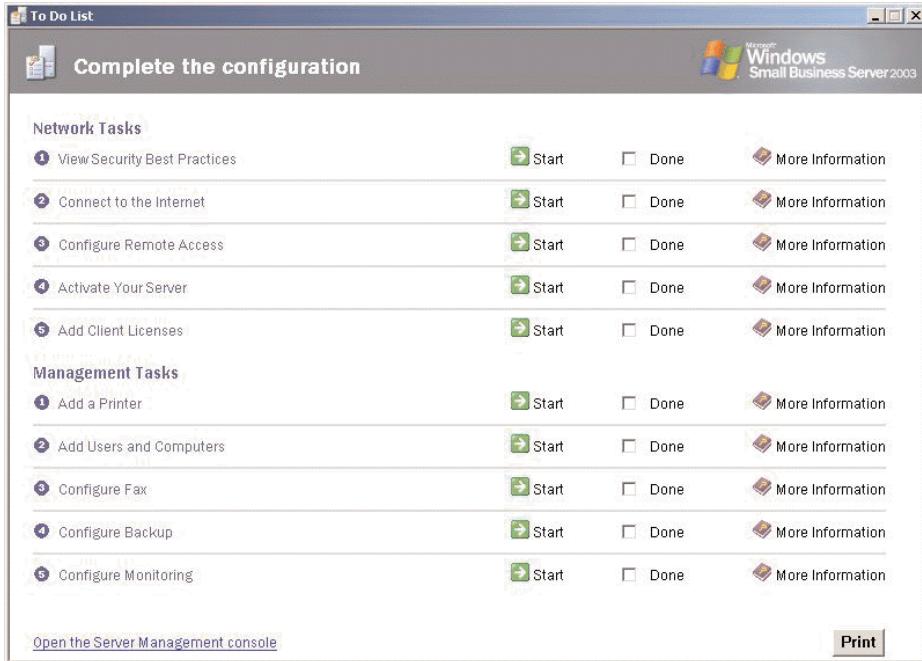
I tested SBS 2003 Standard Edition; it came OEM-installed on an HP ProLiant server with a 2.4GHz Intel Xeon processor, 256MB of RAM, and dual 18GB hard disks. Using an OEM installation meant that HP had preinstalled the setup files to a partition on the hard disk, eliminating the need to install the software from CD-ROM or DVD. The setup process began automatically as soon as I booted the server. Microsoft's goal for the OEM-installed version is to get the system running in less than 30 minutes. Although I began my installation without first locating the preinstallation checklist supplied on the installation poster included with the server, I easily managed to get the system running within the 30-minute time frame. The setup prompted me for an IP address, a gateway address, and primary and secondary DNS server addresses. In my case, my network had an existing DHCP server, so the SBS setup automatically recognized that server, which supplied several of the important network settings. Even so, you need to know your network's infrastructure to complete the setup process. All in all, the setup for SBS 2003 resulted in the fastest setup for Active Directory (AD) and Exchange that I've ever performed. I gave the system a name of WinNetMag, set the AD domain name to WinNetMag.local, and named the Exchange 2003 server WinNetMag. I didn't need to perform any extra manual steps, such as running Domainprep or Forestprep, that the typical Exchange installation requires. After setup finished, AD and Exchange were both running and ready to accept new users.

Client system setup was also a snap using the Web-based client computer deployment tool. After the server setup finished and I added some users on the client system, I pointed my Web browser to the SBS server's intranet connection URL, which on my test setup was <http://sbs2003/connectcomputer>. Connecting to the URL caused an ActiveX control to download to the client. When I clicked the *Connect to the network now* link from the client's browser, the server downloaded the preselected client components and set up various client configuration settings. The default applications included for installation on the client are Microsoft Internet Explorer (IE) 6.0, Outlook 2003, and the client OS service packs. You can add other applications to this list as well. The settings that were sent to the client included the ability to prohibit users from modifying the installed applications, as well as the tools needed to set up ActiveSync and configure Remote Desktop and printers.

Administration

After the server setup is complete, the SBS server displays the To Do List, which guides you through the required system configuration tasks, as Figure 1-1 shows.

Figure 1-1
Using the To Do List to configure the SBS server

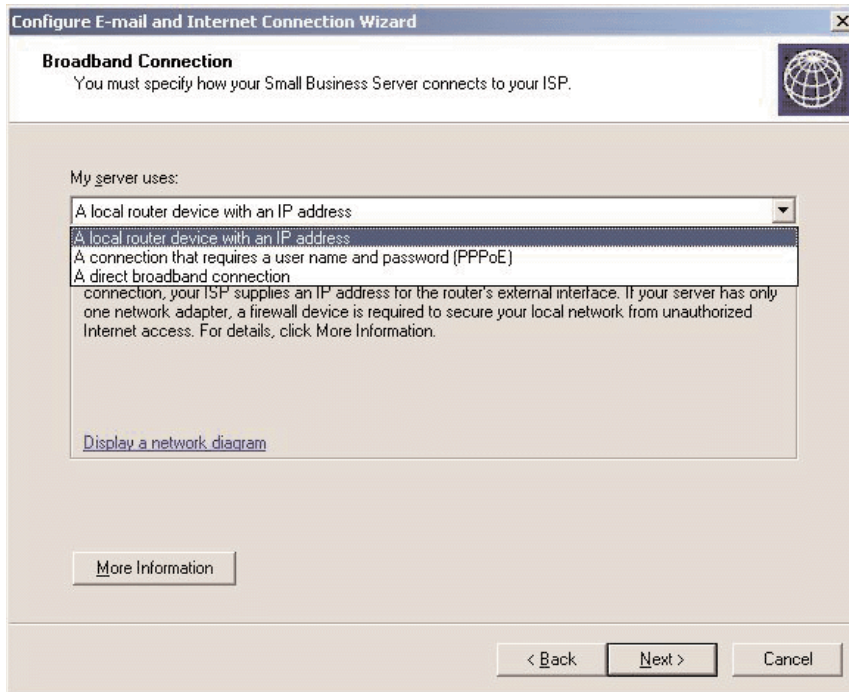


Using the To Do List, you can connect SBS to the Internet, add user and computer accounts, set up inbound and outbound mail, and configure backup and system monitoring. And, as you might notice in Figure 1-1, SBS 2003 requires you to activate the server.

I noticed when completing the items on the To Do List that the list doesn't automatically check off completed items. After I'd performed a couple of the items more than once, I realized that I needed to manually check the Done box.

The first real task you must perform on the To Do List is to set up your Internet connection and email configuration. The *Configure E-Mail and Internet Connection Wizard* guides you through the process of selecting what type of Internet connection you want SBS 2003 to use. At first, this process seems simple enough as you select between a broadband and dial-up connection; however, as the wizard progresses, it asks more complicated questions that require a fair amount of networking knowledge. For example, as Figure 1-2 shows, when you configure the DSL connection type, you need to know whether you have a local router device with an IP address, a connection that requires a username and password (Point-to-Point Protocol over Ethernet—PPPoE), or a direct broadband connection.

Figure 1-2
Selecting which Internet-connection type SBS will use



The wizard displays a network diagram link that visually describes each connection type and helps you pick the right one. The types of information that the wizard requested made it clear that the configuration, albeit simpler than any prior version, is still too complex for the typical small-business manager. All these settings are relatively easy for an experienced administrator to provide but will be a mystery for most business managers. Microsoft's real target for the SBS 2003 setup is the consultant, the Value Added Reseller (VAR), or the Value Added Provider (VAP).

After you configure the connection type, the *Configure E-mail and Internet Connection Wizard* helps you configure your SBS 2003 server's email connection. The wizard lets you configure the traditional Exchange deployment in which Exchange 2003 sends and receives SMTP mail for employees who use the company's registered domain name. You can also configure Exchange to use a POP3 connector to retrieve employee email from MSN.com or any other email service provider that supports POP3.

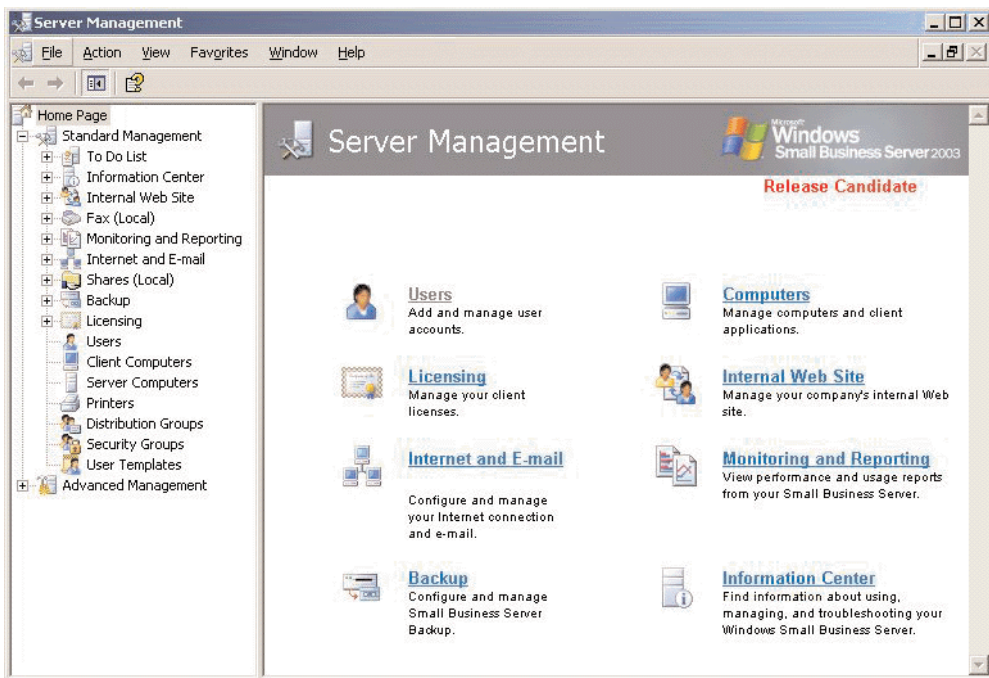
To use the direct Exchange connection, you must use an MX record to register your Exchange server in your ISP's DNS setup. The POP3 connector lets Exchange connect to an email server hosted by your ISP. In this later scenario, the POP3 server will periodically use the POP3 protocol to connect to the ISP's email server, download all the messages from one or more POP3 accounts, then automatically forward the messages to the appropriate Exchange mailboxes. After you complete the Internet and email connection configurations, SBS can begin to send and receive email.

Next, you can complete the Configure Remote Access Wizard to set up the SBS 2003 server's VPN and firewall features so that you can remotely access and administer the server. After you successfully complete the Network Tasks section of the To Do List, the system's Internet connections and email will all be working.

The Management Tasks section of the To Do List lets you perform the initial administrative-oriented tasks such as adding users and printers. However, most administrators will primarily use the Server Management console, which Figure 1-3 shows, to perform the ongoing management of the SBS 2003 system.

Figure 1-3

Managing the SBS 2003 server from the Server Management console

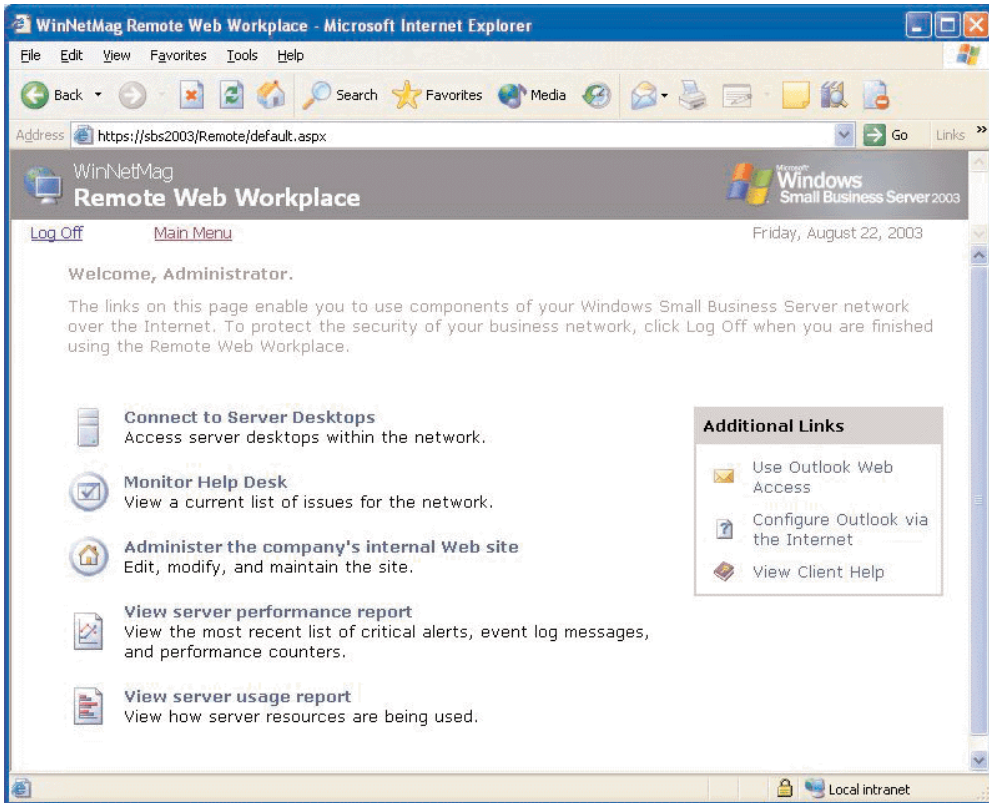


The Server Management console is automatically displayed when SBS 2003 first starts, or you can access it later by selecting the Server Management option from the Start menu.

Designed with an eye on being managed by a remote VAR or VAP, SBS 2003 includes several remote management features. One of these new features is the Remote Web Workplace, which Figure 1-4 shows.

Figure 1-4

Performing remote administration through the Remote Web Workplace



You access the Remote Web Workplace remotely by pointing a Web browser to the address http://www.registered_domain_name.com/remote. The Remote Web Workplace lets you connect to the server so that you can perform local management and connect to client desktops to perform troubleshooting. For remote desktop connections, the client desktop systems must be running Windows XP. The SBS 2003 server acts as a proxy by redirecting incoming remote connections to the locally networked client.

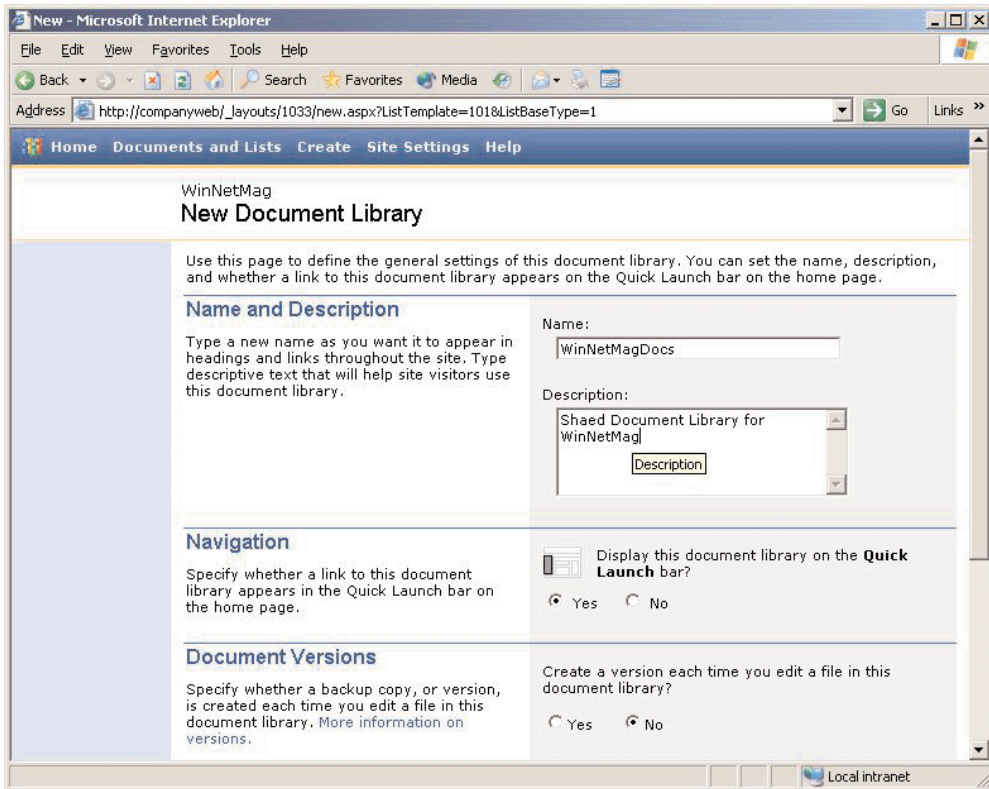
As the URL in Figure 1-4 indicates, Remote Web Workplace connections use HTTP over Secure Sockets Layer (HTTPS), which reduces the need to set up a VPN connection to create a secure remote link. The Monitor Help Desk option lets you access SBS 2003's Help Desk feature, which uses SharePoint Services. Using the Help Desk feature, you can view and respond to existing call tickets as well as generate reports and enter new items. To help the remote administrator monitor and manage the system, SBS 2003 comes with several predefined reports that list system alerts and detail server usage such as disk quotas. You can generate the reports interactively or set them to run on a

predefined schedule and be emailed to a remote administrator. The Use Outlook Web Access option shown on the right-hand side of the Remote Web Workplace screen launches Outlook Web Access (OWA) and connects the browser's HTTPS session to the SBS Exchange server.

Exchange and SharePoint Services

Two core components that are present in both SBS 2003 Standard Edition and SBS 2003 Premium Edition are Exchange 2003 and SharePoint Services. The version of Exchange 2003 included with SBS 2003 is essentially identical to the standalone product. The only difference is that Exchange in SBS 2003 is limited to 75 users and the management of the product is made simpler by the addition of SBS wizards, which can simultaneously add users to Windows as well as set up mailboxes in Exchange 2003. Likewise, the version of SharePoint Services included with SBS 2003 is essentially the same as the service that ships with Windows Server 2003. SharePoint Services lets you easily create Web-based share points. These share points can be thought of as the next generation of a Windows file system share: End users can set up share points to share documents with other users. However, their Web integration also extends the file-sharing capability. For example, with SharePoint Services share points, you can manage who checks in and checks out a document, review document usage, and run Web applications. SBS 2003's built-in Help Desk function is an example of how you can use SharePoint Services for more sophisticated Web-based collaborative applications. Although all client systems can use SharePoint Services shares, to make the most of SharePoint Services, the client systems must be using Microsoft Office 2003, which includes built-in options for using SharePoint Services share points. Figure 1-5 shows the interface for using SharePoint Services to set up a collaborative share point.

Figure 1-5
Creating a SharePoint Services share point



Licensing

The licensing cost for SBS 2003 Standard Edition is \$599, and the licensing cost for SBS 2003 Premium Edition is \$1499. The base licensing for SBS 2003 includes all the server components, and no additional licensing costs are required for the server. In addition, SBS 2003 ships with five CALs—if you plan to attach more than five clients, you must purchase additional CALs. You can attach up to 75 clients to SBS 2003. If you need to attach more than 75 client systems, you must upgrade to the standalone versions of the server components. Fortunately, Microsoft provides an upgrade path for those businesses that outgrow SBS 2003. However, upgrading to the standalone editions of all the products contained in SBS 2003 is a costly and involved move. Microsoft offers two different products that let you upgrade from SBS 2003 to one of the unrestricted versions of the product. For SBS 2003 Standard Edition, the company offers the Transition Pack Standard Edition for \$1769, and for SBS 2003 Premium Edition, the company offers the Transition Pack Premium Edition for \$3522.

Meeting the Needs of Today's Small Business

SBS 2003 makes the process of setting up the most commonly required Windows business components such as AD and Exchange easier than ever before. Even so, Microsoft has built this latest version to be installed and maintained by a consultant, VAR, or VAP. A reasonable degree of technical networking expertise is required. After the system is configured, a local business manager can perform most of the common maintenance tasks. Likewise, SharePoint Services makes the task of setting shares easy and user-friendly.

For businesses that are close to the 75-user limit or have more than 75 users, the complications of upgrading SBS 2003 to the full version of the constituent standalone products make it a poor choice. For business with fewer than 75 users and with some room to grow, Microsoft's aggressive licensing makes SBS 2003 a compelling solution.

Chapter 2:

Windows Decision Point

—by *Jeremy Moskowitz*

Windows 2000's successor has been through three names—Windows 2002, Windows .NET (Win.NET) Server, and the current Windows Server 2003. Amid the confusion of changing nomenclature and last-minute feature additions and subtractions, you might be wondering whether an upgrade to Windows 2003 is worth the effort. Some experts call Windows 2003 merely an “incremental step” forward; others call it “the next generation.” How do you know what to believe?

If you're about to begin a Win2K rollout, should you forge ahead or should you regroup and take a look at Windows 2003? In an ideal world, you would be able to determine the suitability of Windows 2003 in your environment with minimal effort. Sure, Windows 2003 is full of great features, such as support for 1 billion AD objects, tighter security, and many new command-line utilities. But what about the improvements to the OS's main features, such as Microsoft IIS, clustering support, and Terminal Services? Considering how you run your network today, will you actually use these improved features?

Know Your Score

To help you determine whether you should upgrade, let's walk through a Windows Decision Point quiz. You're going to need a pen, some paper, and a calculator or spreadsheet. To find an answer that's specific to your environment, let's start with three essential questions:

- What's the size of your business?
- Which Win2K features are you using today?
- Which Windows 2003 features can you imagine using in the near future?

After you assemble this basic information about your business, you'll have the foundation for taking this quiz, the goal of which is to determine whether you'll use enough Windows 2003 features to take a much closer look at the new OS.

The impact of Windows 2003 will be different depending on the size of your organization. So, the most important preliminary step is to examine your organization's size by placing it into one of three categories:

- small—fewer than 100 clients, with 1 to 4 servers
- midsized—100 to 599 clients, with 5 to 14 servers
- large—600 or more clients, with 15 or more servers

The Quiz

About 1000 representatives of large and small organizations have taken this quiz. I've presented it at *Windows & .NET Magazine Connections* and other industry conferences, and many people tell me that it has at least opened the doors for discussion. The quiz assigns point values to each major Windows 2003 feature or scenario. You simply add or subtract points based on your company's size and your use of the technology, then make a judgment based on your final score. Remember, this quiz is simply a guideline to help further discussions inside your organization—don't use it as a rigid gauge for whether you should upgrade.

You'll see that some questions ask whether your organization experiences light, medium, or heavy use of a specific technology. These rules certainly aren't hard and fast; you'll have to use your judgment in each scenario.

Start by giving your organization 10 points.

Question 1: Is Your Business Mostly NT or Mostly Win2K?

This first question might be the quiz's most important question. As you know, Microsoft is retiring Windows NT, and support for the OS is already waning. If you're using mostly NT, you might be aware that you can no longer get boxed NT products, NT-specific CALs, or NT through Microsoft's OEM System Builder channel. Additionally, you'll have to contend with two hard drop-dead dates that Microsoft has set: As of December 31, 2003, Microsoft stopped supporting nonsecurity-related hotfixes, except through a custom support contract, and the company will stop supporting NT Server 4.0 incident and security-related hotfixes after December 31, 2004.

If your organization is mostly NT and you have a

- **large business, add 12 points**
- **midsized business, add 8 points**
- **small business, add 4 points**

The scoring for this first scenario is vastly different for large businesses versus small businesses that run NT because small businesses typically require less Microsoft support than larger businesses do. Most small businesses can simply "set it up and forget about it." Although businesses of all sizes will need to contend with Microsoft's forthcoming NT-support deadlines, large organizations will feel more of a support ache if they don't migrate off NT in time.

If you're a mostly Win2K environment, the news is better. Win2K support is officially available for many years to come (at least through 2007). Your Win2K rollout probably resulted in quite a stable platform, and you're likely already happy with the fruits of your labor. However, Windows 2003 brings some compelling new features to the table (as you'll see), and an upgrade from Win2K to Windows 2003 is relatively painless. With these factors in mind, here's my scoring for your scenario:

If your organization is mostly Win2K and you have a

- **small business, add 2 points**
- **midsized business, add 3 points**
- **large business, add 5 points**

Question 2: How Much Do You Leverage IIS?

Windows 2003's new Internet Information Services (IIS) 6.0 is vastly improved over its predecessor. Some of the features IIS 6.0 brings to the table are kernel-mode operation, a built-in IIS Lockdown Wizard, effective bandwidth throttling, and a default-logon change from Interactive to Network. Also, IIS 6.0 is simply much faster and more secure. (For more information about IIS 6.0, see "IIS 6.0 Features," <http://www.winnetmag.com/windows/article/articleid/38496/38496.html>.) If your organization uses IIS in any capacity, you'll want to take a look at the upgrade. But for the purposes of this quiz, consider how often you use IIS.

If your current use of IIS 5.0 is

- **heavy, add 8 points**
- **medium, add 4 points**
- **light, add 2 points**
- **nonexistent, add 0 points**

Additionally, if you currently use IIS 5.0 in front of a firewall in the public address space, give yourself an additional 2 points. IIS 6.0's stronger security features are alone a worthy investment.

Question 3: How Much Do You Leverage Clustering?

Both Windows 2003, Datacenter Edition and Windows 2003, Enterprise Edition support more nodes than their Win2K counterparts do. Windows 2003 Datacenter supports eight-node clusters (increased from four), and Windows 2003 Enterprise supports eight-node clusters (increased from two). Windows 2003, Standard Edition doesn't support clustering but now includes the Network Load Balancing (NLB) feature—a welcome addition. With these improvements in mind, here's how to score:

If your business's current use of clustering/NLB is

- **heavy, add 4 points**
- **medium, add 2 points**
- **light, add 1 point**

You can use Windows 2003 NLB to perform front-end routing for Windows 2003 Terminal Services. This feature is a great way to implement inexpensive load-balanced terminal server farms. If you plan to use NLB this way, add another 2 points.

Question 4: How Much Do You Leverage Exchange?

If you have Win2K, you might also have Microsoft Exchange 2000 Server or Exchange Server 5.5. If you do, your outlook for upgrading to Windows 2003 isn't so rosy. Windows 2003's IIS 6.0 is incompatible with Exchange 2000 and Exchange 5.5. Therefore, if you plan to keep or install new Exchange 2000 or Exchange 5.5 servers within your forthcoming Windows 2003 AD implementation, you'll need to continue to put the Exchange software on Win2K or NT Server.

If you choose to upgrade to Windows 2003 in other areas of your network, you'll simply be supporting two (or perhaps more) server platforms. Ideally, you would want to support just one server platform. However, if you have Exchange 2000 or Exchange 5.5, you'll necessarily have to support more than one. For that reason, if you have Exchange 2000 or Exchange 5.5, you'll have to subtract points for the headache that you'll doubtlessly experience while maintaining multiple server infrastructures.

Windows 2003 offers improved domain controller (DC) and Global Catalog (GC) performance, including the ability to refrain from resyncing all the partial attributes. However, you'll need all Windows 2003 DCs to take advantage of this functionality.

If your business's current use of Exchange 2000 or Exchange 5.5 is

- **heavy, subtract 5 points**
- **medium, subtract 4 points**
- **light, subtract 2 points**

To read about the combinations of Windows and Exchange that Microsoft supports, see the white paper "Microsoft Exchange Server Compatibility with Microsoft Windows Server Operating Systems" (<http://www.microsoft.com/exchange/evaluation/ti/tiwin2003.doc>).

Question 5: Do You Have Branch Offices?

Windows 2003 introduces many goodies for organizations that have branch offices. The Knowledge Consistency Checker (KCC) can now gracefully handle more (many, many more) than 200 branch-office sites. Also, you can now instruct bridgehead servers not to compress data over WAN links. And you can use the new Install From Media feature to populate DCs from tape or other media, rather than over the network. This feature is quite beneficial in large domains spread across WAN links. Note that all the features (except Install From Media) listed in this category require that every DC in every domain run Windows 2003.

You'll gain the most benefit from these features if you have many branch offices. If you have no branch offices, these features won't do anything for you.

If you have

- **a large number of branch offices (e.g., 50 or more), add 6 points**
- **a moderate number of branch offices (e.g., 30 to 49), add 3 points**
- **a small number of branch offices (e.g., 1 to 30), add 2 points**
- **no branch offices, add 0 points**

Question 6: Will You Use Cross-Forest Trusts?

Windows 2003 doesn't bring the nirvana of AD "pruning and grafting" that many systems administrators have hoped for. You can't take another company's Windows 2003 or Win2K domain and "glue" it to your AD forest. However, Windows 2003 does offer one compelling feature for intracompany sharing: cross-forest trusts.

14 Building the Small Business Infrastructure

With a cross-forest trust in place, two Windows 2003 forests can more effectively share data and resources between their domains. (For more information about cross-forest trusts, see “Multiple-Forest Trusts,” <http://www.winnetmag.com/windows/article/articleid/38280/38280.html>.) This improvement can be especially helpful should your company acquire another company and want to perform a quick integration. However, all the DCs of both companies must be running Windows 2003 and the domains and forests must be switched into Windows 2003 functional levels.

Windows 2003 also adds the ability to easily rename DCs, as well as the ability to rename domains. However, the procedure for renaming domains is exceedingly painful, and you should resort to it only if absolutely necessary. Still, the capability is nice to have.

If you already have

- **more than two domains and two forests, add 5 points**
- **two domains or two forests, add 4 points**
- **one domain, add 1 point**

If you're planning an acquisition in 3 to 12 months, add another 3 points. Also, if you're planning to rename your company in the same time period, add another 3 points.

Question 7: How Much Do You Leverage Terminal Services?

Both Windows 2003 and Windows XP contain a mechanism for providing inbound connections through Terminal Services. The OSs share a new version of the RDP 5.2 Terminal Services server-side protocol. In general, the RDP 5.2 protocol is more forgiving than earlier versions if you're connecting from a computer over the Internet. Earlier versions of RDP tend to drop the session if even one packet has been lost in transit.

Additionally, Windows 2003 and XP offer a new version of the RDP client-side protocol. The RDP 5.1 protocol adds some whiz-bang features (e.g., 24-bit color, native clipboard redirection, native client printer and driver redirection, bandwidth throttling when connected through LAN versus dial-up connections, time-zone redirection, and Console Session '0') to your Terminal Services experience. You can benefit from these new features only if you use the combination of RDP 5.2 on the server and RDP 5.1 on the client. These features definitely improve the Terminal Services experience so that users feel as if they're using the same system.

If your business's current use of Terminal Services is

- **heavy, add 4 points**
- **moderate, add 3 points**
- **light, add 2 points**
- **nonexistent, add 0 points**

Question 8: Do You Plan to Pair Windows 2003 with XP?

XP brings a lot to the table when you pair it with Windows 2003. First, you can perform Universal Group caching, which lets XP clients log on to the network without a GC available. XP also permits secure wireless connections through 802.1x and supports the use of Windows 2003 certificates to validate that connection. Finally, as I stated earlier, XP features the RDP 5.1 client, which—in conjunction with the RDP 5.2 server on a Windows 2003 server (or XP client for use with Remote Desktop)—greatly enhances the Terminal Services experience.

If you'll have

- **XP fully rolled out in 1 year, add 4 points**
- **XP rolled out to half your users in 1 year, add 2 points**
- **XP rolled out to fewer than half your users in 1 year, subtract 2 points**

Question 9: How Much Do You Leverage Group Policy?

I'm a Group Policy junkie. I can't live without Group Policy settings, and I'm betting many of you can't live without them either. With its new Group Policy features, Windows 2003 increases my enthusiasm. First, the OS offers many simple Group Policy improvements, such as the ability to roll back to original default Group Policy objects; about 200 new Group Policy settings for XP, including software-restriction and wireless-networking policies; Group Policy setting support for DNS and Terminal Services; and the ability to perform Resultant Set of Policy (RSOP) calculations.

However, the biggest improvement is Group Policy Management Console (GPMC), a free downloadable tool to help you with Group Policy management. GPMC is a great tool because it adds a Group Policy—centric view to your network. Additionally, the tool permits Group Policy object backup and restore, and offers a gaggle of other great features.

However, to use the GPMC tool, you must commit to licensing at least one Windows 2003 server. Although GPMC is a free download, the product's FAQ clearly states, "You may install an unlimited number of copies of GPMC in your environment, provided you have at least one valid license for Windows Server 2003." Note that as soon as you license and install just one Windows 2003 server, you might be in for a huge uptick in the purchase of Windows 2003 CALs, so be sure that you understand the legal and cost ramifications of your choices. (For more information about the GPMC tool, see "Windows Server 2003's Group Policy Management Console," <http://www.winnetmag.com/windows/article/articleid/39190/39190.html>.)

If you

- **use Group Policy heavily, add 5 points**
- **are just starting out with Group Policy, add 2 points**
- **have no plans for using Group Policy, subtract 4 points**

If you're not using Group Policy, you're missing out on many of the benefits that AD has to offer. An understanding of how to use Group Policy will only become more important as Windows networks mature.

Question 10: How Much Do You Leverage SAN/NAS Technology?

Windows 2003 is designed to work with Storage Area Network (SAN) and Network Attached Storage (NAS) devices. With the right hardware, Windows 2003 should be able to boot off your SAN, and you should be able to use standard Windows tools to configure your LUNs. The “open” nature of Windows 2003’s SAN and NAS support will likely replace the functionality of today’s proprietary SAN and NAS solutions. The kismet between Windows 2003 and your SAN vendor might not be evident today, but be sure to stay tuned: The future is undeniably bright.

If you

- **have SAN/NAS today, add 4 points**
- **will install SAN/NAS within 1 year, add 3 points**
- **have no plans for SAN/NAS within 1 year, add 0 points**

Your current SAN or NAS implementation might not support the Windows 2003 features that I’ve mentioned. However, you should check with your hardware vendor to ensure that it’s working on compatibility with these new features.

Tally Your Score

How did you do? Using the points that you’ve accumulated, you can now make a fairly informed decision about whether to take a close look at a Windows 2003 upgrade.

You should seriously consider migrating to Windows 2003 if you are

- **a small organization that has tallied 20 points or more**
- **a midsized organization that has tallied 30 points or more**
- **a large organization that has tallied 40 points or more**

If you’re still an NT shop, you might want to consider rolling out new servers to Windows 2003. Over time, locating new hardware with NT driver support will become more and more difficult. Additionally, you need to consider the Microsoft-sanctioned deadlines that I mentioned earlier.

If you’re a mostly Win2K shop, you could feasibly skip Windows 2003. Win2K support will be available for years to come; however, you’ll be missing out on some great features. I hope this quiz has opened your eyes to whether you would find these new features beneficial.

Chapter 3:

Advanced Patch Management

—by *Mark Burnett*

In light of the endless influx of Internet-based worms, scanning scripts, and intruder attacks, patch management has become a growing concern among network administrators. A security guide, checklist, or hardening document wouldn't be complete without some recommendation to keep up with current hotfixes and service packs. But keeping up with patches isn't always as simple as visiting Windows Update and installing the recommended updates. I recommend automated patch-management solutions for updating workstations and noncrucial servers, but you might want to implement more advanced patch-management techniques to protect high-visibility or high-security servers. The strategies that I discuss in this article might not work for all organizations, but those willing to go the extra mile will benefit from the stability and security of careful patch management.

Check the Signatures

Depending on your server's security policy, when you install hotfixes you might receive a warning that the file doesn't contain a valid signature. However, Microsoft claims that it signs all its hotfixes. So why do you get the warning?

The confusion comes because two types of signatures exist: an Authenticode signature and a Windows Hardware Quality Labs (WHQL) signature. A software developer ensures a file's authenticity by appending an Authenticode signature to the file. Windows doesn't automatically check the Authenticode signature for hotfixes. You can verify the signature by right-clicking the file and selecting Properties. You can also use the Chktrust command-line tool that comes with the Microsoft Platform software development kit (SDK) to verify the Authenticode signature. Chktrust.exe will tell you whether a certificate is valid but won't tell you who owns it.

Microsoft stores the WHQL signature in a separate catalog file to show that the company has tested a driver file for Windows XP or Windows 2000 compatibility. Microsoft includes a WHQL signature for each driver file in a hotfix. The warning appears when the WHQL signature for a driver file doesn't match what's stored in the catalog file.

So if the Authenticode signature verifies the hotfix before installation and the WHQL signature verifies the driver files after you install the hotfix, why does the warning still appear? It appears because the hotfix installs new files with new WHQL signatures. Because the new WHQL signatures aren't available until the installation is finished, Windows can't verify the new signatures until the hotfix is installed. You can verify these signatures by running the Windows File Signature Verification tool (sigverif.exe) after you install the hotfix. If you check the Authenticode signature before you install the hotfix and run Sigverif to check the WHQL signatures after installation, you can safely ignore the invalid-signature warning.

Check the Files

Before you install any hotfix on a production server, you should know which files you'll be installing and which files the hotfix will update. By identifying which files will change, you can spot file-version conflicts and determine which changes a hotfix will make to your server. This step adds to the updating process, but it's worth the effort if it prevents downtime of a crucial server.

To list the files in a hotfix, you can manually extract them by using the `/x` switch. For example, the following command extracts the files from the `q123456.exe` hotfix:

```
q123456.exe /x
```

The `/x` switch also has an undocumented feature that lets you extract the files to a specific path. When combined with the `/q` switch, the file extraction requires no user interaction, which means you can use scripts to automate the file-extraction process. For example, the following command extracts the files from the `q123456.exe` hotfix to the `C:\temp` directory:

```
q123456.exe /x:c:\temp\ /q
```

After you extract the files, you can view them and their properties. To make this task easier, you can use the `hfinfo.vbs` script that I've created. Because Microsoft packages hotfixes differently in Windows Server 2003, this script will work only in Win2K. This script extracts the hotfix files and displays each file's date, time, size, and version. To use `hfinfo.vbs`, type

```
cscript.exe hfinfo.vbs <HotfixFilename>
```

where *HotfixFilename* is the name of the hotfix file. Knowing which files and file versions you're installing will make identifying potential conflicts or other problems easier. But most of all, knowing which files you're about to install on your server is simply a good idea.

Watch the Installation Order

With Windows NT 4.0, installing hotfixes in the proper chronological order is crucial. To improve the hotfix installation process, Win2K and later OSs added more thorough version checking to improve the hotfix installation process. Microsoft has also released the `Qchain` tool (available at <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=a85c9cfa-e84c-4723-9c28-f66859060f5d>), which lets you install multiple hotfixes without rebooting the system after each installation. However, situations still exist in which the hotfix installation order is important.

When a hotfix needs to install a file that's in use, the hotfix writes a registry entry that tells the OS to replace the file at the next reboot. When you install multiple hotfixes, the hotfixes might update the same file multiple times. In this situation, `qchain.exe` checks to make sure that only the most recent file version appears in the list of hotfixes to be installed. You should always run `qchain.exe` when you install multiple hotfixes.

But `qchain.exe` isn't perfect. You might still end up with an older file than expected. For example, some file types, such as `.asp` or `.chm` files, don't have version information built into the file. Also, `qchain.exe` works only with files that are in use that Windows can't replace until rebooting. Because a hotfix might replace some files immediately, `qchain.exe` will never see them.

To avoid these situations, you should install hotfixes in the proper chronological order whenever possible. However, the proper order isn't always clear. You can't just rely on the security bulletin number or the Knowledge Base article number. Although you can usually trust the hotfix release

date, the only way to be absolutely sure of the proper installation order is to check the versions and dates of each file in the hotfix.

Don't Rely Exclusively on Automatic Updates

With Win2K SP3, Microsoft introduced the Automatic Updates service, which automatically watches for, downloads, and optionally installs new Windows updates. This service is a huge step forward for Windows security, but solely relying on it does have some drawbacks.

To begin, not all security bulletins involve installing a patch. For example, Microsoft Security Bulletin MS02-064 (Windows 2000 Default Permissions Could Allow Trojan Horse Program) addresses a problem with the default NTFS permissions of the system root folder, but it doesn't provide a patch. Instead, you must manually fix these permissions on each server. The Automatic Updates service can't help you with this and other hotfixes that require manual intervention.

When you use the Automatic Updates service, neglecting to read Microsoft's security bulletins is an easy habit to get into. These bulletins contain valuable information, including best practices that can avoid or mitigate the problem, even without the patch. If you rely on automated systems to patch your servers, you need to watch the security bulletins for manual fixes.

Finally, the Automatic Updates service can't always handle the complexities of a hotfix. Some hotfixes have specific installation conditions that you must carefully review before installation. If you consider these drawbacks, you'll see that the Automatic Updates service is actually a distribution method and not a replacement for checking security bulletins.

Double-Check the Hotfix Checkers

Even when you use best practices to patch your systems, you might still need to reinstall a hotfix. For example, you might install all the Automatic Updates, then go to Windows Update only to find other fixes available. After installing all those other fixes, you might use the HFNetChk tool and discover even more fixes that you need to install. Taken a step further, you might run qfecheck.exe, which reports whether all hotfixes are installed properly, then run the Microsoft Baseline Security Analyzer (MBSA) and find that a hotfix isn't properly installed.

Why do these situations occur? Part of the problem is that Microsoft uses many different installers for hotfixes. You might notice, for example, that IE updates have different icons and file-naming conventions than Win2K hotfixes do. Some products use the Microsoft installer, Windows installer, or the Microsoft Systems Management Server (SMS) installer, whereas others, such as Microsoft Office, use yet another installer. With the release of SP3, even Win2K hotfixes switched from using the hotfix.exe installer to using the update.exe installer. Predicting how each of the many installers will behave in particular circumstances is difficult.

Installation order, file corruption, and even running the System File Checker can cause problems. (For details about System File Checker-related problems, see the Microsoft article "The SFC /SCANNOW Command May Overwrite Hotfix Files" at <http://support.microsoft.com/?kbid=814510>.) Other problems, such as service pack slipstreaming, human error, incorrect version detection, and limited product coverage, contribute to the inconsistent results.

Another part of the problem is that numerous tools exist for checking installed hotfixes, and each tool has its strengths and weaknesses. Each tool uses different combinations of methods to determine which hotfixes are installed and whether they're installed properly. To determine whether you've installed a hotfix, a tool can check the registry, the file versions, or the file signatures. But many com-

plexities can complicate file and product versioning, so the process still isn't perfect. For example, slipstreaming a service pack to a server might not record a product version in the same way as if you'd installed it after the OS.

My solution is to check my hotfixes, then double-check them again with another tool. Table 3-1 provides a list of free products that you can use to verify your hotfixes.

Table 3-1 Free Products for Checking Hotfixes

Product Name	Web Site
BigFix Consumer Edition	http://www.bigfix.com
Ecora Patch Manager Trial Version	http://www.ecora.com
Gravity Storm Software's Service Pack Manager 2000LT	http://www.securitybastion.com
MBSA	http://www.microsoft.com/downloads/details.aspx?familyid=8b7a580d-0c91-45b7-91ba-fc47f7c3d6ad&displaylang=en
Microsoft Windows Update Services (WUS) and Software Update Services (SUS)	http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
Shavlik's HFNetChk.exe	http://www.shavlik.com
Windows Update	http://windowsupdate.microsoft.com

Don't Forget Other Updates

When you install hotfixes, overlooking other updates that you need to apply to your systems is unfortunately easy to do. For example, most hotfix-checking tools tell you which hotfixes are required for your current service pack level but don't always inform you that a new service pack is available. Also, be aware that Windows Update covers only Microsoft's main products. Table 3-2 lists several updates that administrators can often overlook.

Table 3-2 Often-Overlooked Product Updates

Product Name	Web Site
COM+	Search the Microsoft Knowledge Base (http://support.microsoft.com) for the latest COM+ rollup package.
Microsoft Application Center	http://www.microsoft.com/applicationcenter
Microsoft BizTalk Server	http://www.microsoft.com/biztalk/downloads/default.asp
Microsoft Commerce Server	http://www.microsoft.com/commerceserver
Microsoft Content Management Server (CMS)	http://www.microsoft.com/cmserver
Microsoft Data Access Components (MDAC—ADO, OLE DB, ODBC, and Joint Engine Technology—JET)	http://msdn.microsoft.com/data
Microsoft Exchange Server	http://www.microsoft.com/exchange
Microsoft FrontPage 2000 Server Extensions	http://msdn.microsoft.com/library/en-us/dnservext/html/winfpe.asp
Microsoft FrontPage Server Extensions 2002	http://msdn.microsoft.com/library/en-us/dnservext/html/fpse02win.asp
Microsoft ISA Server	http://www.microsoft.com/isaserver
Microsoft SharePoint Portal Server	http://www.microsoft.com/sharepoint
Microsoft SQL Server	http://www.microsoft.com/sql
Windows Script Host (WSH)	http://msdn.microsoft.com/scripting
XML	http://msdn.microsoft.com/xml

Many third-party patch-management solutions offer much more comprehensive product coverage than the Microsoft tools do. Table 3-3 lists several such third-party patch-management offerings.

Table 3-3 Automated Patch-Management Solutions

Product Name	Web Site
Altiris's Patch Management Solution	http://www.altiris.com
Autonomic Software's ANSA	http://www.autonomic-software.com
AutoProf's Policy Maker	http://www.autoprof.com
Beadwindow's ZNQ3 SoftPatch	http://www.beadwindow.com
BigFix Patch Manager	http://www.bigfix.com
Configuresoft's Security Update Manage (SUM)	http://www.configuresoft.com
Ecora Patch Manager	http://www.ecora.com
Executive Software's Sitekeeper 3.1	http://www.executive.com
GFI Software's GFI LANguard Network Security Scanner (N.S.S.)	http://www.gfi.com
Gravity Storm's Service Pack Manager 2000	http://www.securitybastion.com
LANDesk Software's LANDesk Patch Manager	http://www.landesk.com
ManageSoft Security Patch Management	http://www.managesoft.com
Marimba's Patch and Antivirus Management	http://www.marimba.com
Novadigm's Radia OS Manager	http://www.novadigm.com
OnDemand Software's WinINSTALL 8.0	http://www.ondemandsoftware.com
PatchLink Update	http://www.patchlink.com
SecurityProfiling's SysUpdate	http://www.securityprofiling.com
Shavlik's HFNetChkPro	http://www.shavlik.com
St. Bernard Software's UpdateEXPERT	http://www.stbernard.com

Know When to Reinstall

Even if you carefully follow the guidelines in this article, you should always reinstall hotfixes in the following situations:

- after adding or removing Windows components
- after performing an emergency repair
- after recovering from a backup
- after installing a service pack

At some point before Microsoft releases a service pack, the company must freeze the code to start the testing process. During that test period, Microsoft will likely fix bugs in the service pack and release new hotfixes. Microsoft will often rerelease these hotfixes (and refer to them as post-service pack hotfixes) when releasing the service pack. After you install a new service pack, reinstalling any post-service pack hotfixes that you had previously installed is a good idea. I also suggest that you regularly check your systems with an automated patch-management system to verify that all hotfixes are current and properly installed.

Keep Up with Fixes

At one time, Microsoft recommended against installing hotfixes unless they were absolutely necessary. In fact, common practice was not to install any fix if a server was already running properly. But the proliferation of Internet-based attacks has changed that practice.

Although some exceptions exist, the new best practice is to install every hotfix and service pack relevant to your high-visibility or high-security servers. Microsoft expects users to have installed the most current service pack, and some hotfixes won't work with older service packs. Some hotfixes rely on DLLs released with service packs, and not having the right version can result in server instability. Thus, installing every update requires careful testing before full deployment.

Speed is also a concern when applying hotfixes. With some security problems, patching your servers as soon as you've tested the patch for your environment is crucial. If someone really wants to break into your Web site, all they have to do is closely monitor Microsoft's security bulletins and exploit the vulnerability before you patch your servers. The only sure way to counter such exploits is to patch your servers as quickly as possible. In the meantime, be sure to use other tools such as firewalls, Intrusion Detection Systems (IDSs), and the URLScan security tool to block known attacks.

Know Where to Get Help

Microsoft's hotfix articles used to carry a disclaimer that hotfixes weren't supported products to emphasize that the company typically didn't subject hotfixes to the same extensive testing procedures used for service packs. This situation has changed, and Microsoft now provides free support for hotfix-related problems. A complete list of ways to contact Microsoft Product Support Services (PSS) is available at <http://support.microsoft.com/common/international.aspx?rdpath=fh;en-us;contactms>.

Microsoft also provides support through newsgroups. This support option is often helpful because it not only includes feedback from Microsoft but also from the Windows community. Go to <http://www.microsoft.com/technet/community/newsgroups/security/default.msp> for a complete list of security-related newsgroups. Microsoft provides a search mechanism for these groups, but you might have better results using Google's Usenet search engine, which includes Microsoft newsgroups.

Other public forums and mailing lists are available for community support. For questions specific to patch management, check out <http://www.patchmanagement.org>. The two largest mailing lists for Microsoft-related security concerns are FOCUS-MS at <http://www.securityfocus.com/archive/88> and NTBugtraq at <http://www.ntbugtraq.com>. If you have a bad experience with a hotfix, be sure to post to all these public forums so that everyone can benefit from your experience.

As you can see, patch management still has many unresolved concerns and has some way to go before you can completely trust the automated process. The best way to deal with hotfixes is to keep up with them. You might find that an automated solution works best for your organization, or you might choose to keep your own list of fixes to install and be aware of the problems as they come up. Monitor the public forums for known concerns and properly test the fixes before deployment. If you follow all these tips, you can be sure that your crucial servers are as secure and up-to-date as you can make them.

Chapter 4:

Getting Started with Remote Administration

—by *Kathy Ivens*

I began my computer consulting career when the word “windows” meant little more to me than a semiannual household chore involving vinegar and paper towels. My clients ran UNIX or Novell NetWare networks. When a client called with a problem, I dialed in to the network. When I started installing and maintaining Windows NT networks, dialing in was a complicated affair that often failed or was too slow because of the GUI bandwidth requirements (the lack of command-line tools was a real problem). As a result, when a client with an NT network called with a problem, I had to drive in.

If you’re an administrator, you’re probably not as physically far from your servers as I was, but without remote administration tools, you must leave your workstation and go to the server, which might be down the hall, on another floor, or in a remote branch office. Life as an administrator is a lot easier when you can administer your servers remotely, from the comfort of your own office or cubicle.

Windows 2000 Server made remote administration of servers viable, thanks to better command-line tools and a completely reconfigured feature called Win2K Server Terminal Services. Microsoft built support for Terminal Services right into the kernel of all Win2K Server versions. Even better, when you install Terminal Services, you can limit the installation to Remote Administration Mode, which Microsoft designed specifically for remote administration of servers and which doesn’t require you to purchase and install Terminal Services user licenses.

Windows Server 2003 makes Terminal Services even easier and better by making Terminal Server Administration Mode part of the OS. The Windows 2003 version is called Remote Desktop, and you need only to enable the feature to begin using it to administer servers from your workstation.

Let’s discuss using terminal services for remote administration for both Windows 2003 and Win2K. Other remote administration tools exist, but I’ve found terminal services to be the easiest to use and the most reliable. (Incidentally, this component was called Terminal Server in Windows NT 4.0, became Terminal Services in Win2K, and is once again Terminal Server in Windows 2003.)

Installing Terminal Services in Win2K

If you didn’t install the Terminal Services component when you installed Win2K Server, you can run the Control Panel Add/Remove Programs applet, and move to the Windows Component section to install it. Install Terminal Services Remote Administration Mode directly on the server you want to administer. You can install the software on any server or servers in your system. The Remote Administration Mode leaves out the application-sharing components, which means the program requires very little overhead. Therefore, you can install Remote Administration Mode on servers that

are already performing important functions. In fact, Remote Administration Mode has so little impact on the server that there's no reason not to enable it on all your servers.

To install Remote Administration Mode, perform the following steps:

1. Run the Add/Remove Programs applet, then click Add/Remove Windows Components.
2. Scroll through the component list to find Terminal Services, and select it.
3. Click Details to see the Terminal Services component selection window.
4. Select both options, Client Creator Files and Enable Terminal Services, then click OK to return to the Windows Components window.
5. Click Next. Select Remote Administration Mode, then click Next again. (If your Win2K installation isn't from a network share point, you'll have to insert your Win2K CD-ROM.)
6. After the files are copied to the server, click Finish.
7. Close the Add/Remove Programs applet, then restart the server.

After the server boots up, you'll notice several additions to it. The Administrative Tools menu will have new entries for Terminal Services Client Creator, Terminal Services Configuration, and Terminal Services Manager, and you'll see a new directory, `%SystemRoot%\system32\clients\tsclient`, which contains subdirectories for Terminal Services clients.

Enabling Remote Desktop in Windows 2003

You don't have to install Terminal Server Administrative Mode in Windows 2003 because it's included with the OS. However, as I mentioned earlier, you must enable the feature on any server that you want to administer remotely. Right-click My Computer, then select Properties. On the Systems Properties dialog box, select the Remote tab, then select the option to accept remote desktop access.

Next, you must establish a list of users who have permission to access the server remotely by adding their names to the Windows 2003 local users group named Remote Desktop. Members of the domain's Administrators group are automatically granted access to the server, but you might want to add other users. To do so, click Select Remote Users to open the Remote Desktop Users dialog box. Click Add to select usernames from the domain for people who you want to let administer this server remotely.

The users you add to the Remote Desktop group don't have to have elevated privileges; you can select ordinary domain users. As a result, members of your IT staff can administer the server even if they've logged on to their workstations with an account that isn't a member of the Administrators group. However, note that any user account, including an Administrator account, that lacks a password can't access a Windows 2003 computer for remote administration. No password, no entry. In fact, this restriction applies for many features in Windows 2003.

Installing the Client Software for Win2K Terminal Services

The Terminal Services installation process creates a `%SystemRoot%\System32\clients\tsclient\net\win32` folder on your Win2K server that contains the software necessary to set up 32-bit client computers for administering Win2K servers remotely. Share that folder so that users can find it easily, then notify members of your administrative staff that they can access the folder and run `setup.exe`.

(Other subfolders exist in the \tsclient subfolder that contain files for creating disks to install the client software and for 16-bit client computers.)

Installing the Client Software for Windows Server 2003 Remote Administration

XP has the remote desktop client built in, so connecting to a Windows 2003 computer from XP is a point-and-click operation. In fact, this feature is a good reason to make sure that all the members of your administrative staff have XP machines. The program, called Remote Desktop Connection, is in the Accessories\Communications submenu. You can right-click Remote Desktop Connection and choose *Pin to Start Menu* to avoid navigating through the menus in the future. Or, you can create a shortcut on the Quick Launch toolbar.

For other Windows clients that you want to use to administer Windows 2003 servers, install the Remote Desktop Connection client software from the Windows 2003 CD-ROM or from a network share point that contains the Windows 2003 installation files:

1. Launch setup.exe (the file might run automatically if you're using the Windows 2003 CD-ROM) on the client machine.
2. Choose Perform Additional Tasks.
3. Choose Set Up Remote Desktop Connection.
4. Follow the wizard's prompts to accept the license agreement and to install the software for all users of the computer or for the current user only.
5. When the wizard finishes installing files, Remote Desktop Connection appears on the Programs menu.

The Remote Desktop Connection software on the Windows 2003 CD-ROM is version 5.2, which is a later version than the version that shipped with XP and XP SP1. Version 5.2 has an additional feature for accessing a server console session (without this version, you can only access the console session from a command line).

Performing Administrative Tasks Remotely

To connect to a server to administer it, launch the client-side software (Terminal Services Client for Win2K administration; Remote Desktop for Windows Server 2003 administration), then enter the name or IP address of the server. After you're connected, you can open and manipulate Control Panel applet settings, configure the server (including promoting it to a DC if it isn't a DC), run system tools, and generally work as if you were sitting in front of the server. If the server is a DC, you can run administrative tasks in AD, such as adding users, computers, and organizational units (OUs), in addition to setting domainwide Group Policies.

Taking Over the Console Session in Windows 2003

A Windows 2003 server that has Remote Administration enabled can support two remote sessions in addition to the console session. The Remote Desktop Connection client software can take over the console session remotely if you have some reason to work as if you were sitting in front of the

26 Building the Small Business Infrastructure

computer. The most useful application of this feature is for administering headless servers, if you've installed any. Note that if you do take over the console session, you bump off any interactive user who's logged on.

If you're running Remote Desktop Connection 5.2 (or later), you can use the GUI to take over the console session, but if you're working with version 5.1, you must use the command line. In version 5.2, simply add a space and the `/console` switch after you enter the name or IP address of the server, as in *servername* /console.

If you're running version 5.1, open a command window and enter the command

```
mstsc -v:<servername> /F -console
```

If a user is logged on to the computer, the system warns you that you'll be logging that user off.

I run two discrete Windows networks in my office—one is a Windows 2003 domain, and the other is a Win2K domain. My office is in my home, so I can use my XP laptop to manipulate my network, perform heavy-duty management tasks on the DCs, and troubleshoot servers from anywhere in the house. More important, I can do the same thing for all the servers on my clients' systems.

Chapter 5:

Powering Databases with MySQL

—by *Dustin Puryear*

The database server market is anything but small these days. Among the many players, powerful and comprehensive open-source solutions are often overlooked. Yet several such servers compete head-to-head with commercial solutions in terms of performance and reliability.

MySQL is an SQL database server that has a dual commercial and open-source license. Essentially, if you distribute any products that use MySQL and that aren't open source (i.e., governed by the GNU General Public License—GPL), you need to license MySQL. Otherwise, MySQL is free regardless of whether you're implementing a massive network management system or deploying a Web application on the Internet.

Differences between MySQL and other solutions, such as Microsoft SQL Server, include MySQL's lack of foreign key support and the absence of support for advanced SQL constructs such as subqueries. (These features are slated for support in upcoming releases that are currently in the alpha stage.) But similarities also abound. For example, MySQL supports replication; database, table, and column security; ODBC; and scalability. MySQL also supplies command-line tools that let you work with the database server from the command line or within shell scripts, in addition to GUI management tools such as the MySQL Control Center (MySQLCC).

Installing MySQL on Your Server

To install MySQL, begin by grabbing the most recent production release—version 4.0.18 as I write this article—of MySQL for Windows from the MySQL Web site (<http://www.mysql.com/downloads>). After downloading MySQL, unzip the archive and, as Administrator, run `setup.exe` to install the MySQL program files to your computer. (You can run MySQL on Windows 95 and later, but I advise using Windows 2000 or later.) By default, the setup program installs MySQL to `C:\mysql`. If you're installing MySQL on a production system, strongly consider placing your data and log files on a dedicated drive as you would if you were using SQL Server. Using a separate drive for data and log files means that you won't need to worry about database growth consuming your main drive and lets you tune the file system to increase performance and disk-usage efficiency without affecting other applications.

After the installation is complete, you need to install the MySQL service. Start the WinMySQLAdmin program from the `\mysql\bin` subdirectory. The program asks you for a username and password. If you supply them, WinMySQLAdmin stores them in `%USERPROFILE%\windows\my.ini` for later use when you log in to the MySQL server. For installation purposes, however, you can simply click Cancel, and WinMySQLAdmin will open, install and start the MySQL service, and automatically minimize to the System Tray as a traffic-light icon.

Now, download MySQLCC (<http://www.mysql.com/downloads/mysqlcc.html>). MySQLCC is similar to SQL Enterprise Manager (SEM) in that it lets you create and drop (i.e., delete) databases and tables, specify columns and indexes, and define users and ACLs. Although MySQL comes with

command-line tools, some of which you can use to manage MySQL or to dump and load databases and tables for backup purposes, administrators who are new to MySQL will find MySQLCC easier to use. (An even better tool is in the works: When MySQL Administrator becomes available, it will provide a visual interface for performing tasks such as creating databases and viewing replication status. To learn more about MySQL Administrator, go to <http://www.mysql.com/products/administrator>.)

In the `mysqlcc-0.9.4-win32.zip` distribution archive, run `setup.exe` or `mysqlcc.msi` to open the MySQL Control Center Setup Wizard. The wizard will install MySQLCC, which you can then access by clicking Start, Programs, MySQL Control Center, MySQL Control Center. When MySQLCC initially opens, it asks you to supply a name for your connection (e.g., My Connection), the host name (e.g., localhost, mysql.example.com), and login information for accessing your MySQL server. For the User Name and Password fields, specify `root` and a blank password, respectively. (The default password for the MySQL root user, which is similar to the SQL Server systems administrator account, is blank. To learn how to correct this security risk, see the sidebar “Predefined MySQL Accounts.”) Next, click Add, then double-click your new MySQL server profile to open the connection.

Predefined MySQL Accounts

MySQL ships with four predefined accounts: `root@localhost`, `root@%`, `@%`, and `@localhost`. The MySQL administrative user uses the `root@localhost` and `root@%` accounts to create new users, databases, and so forth. The `@%` and `@localhost` accounts are used for what MySQL terms *anonymous connections*. When users don't supply credentials, MySQL uses the anonymous connections to grant access. While you're learning MySQL, you might want to keep these connections active. However, they represent a security risk, so be sure you delete the anonymous connections in a production network. To delete the connections, double-click User Administration in MySQL Control Center (MySQLCC), right-click the `@%` and `@localhost` accounts, and click Delete User.

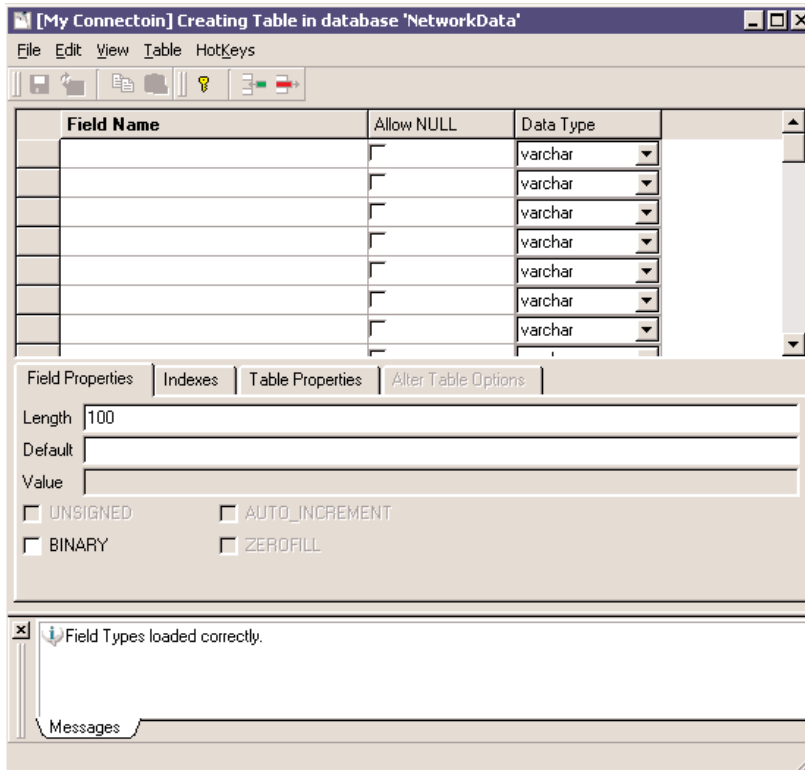
While you're in the User Administration menu, you might also want to change the root user's password, which is blank by default. To do so, right-click the `root@local host` and `root@%` accounts, click Edit User, and update the password.

Creating and Accessing a Database

Now you can do something useful: create a database. When you open your connection, you'll see MySQLCC's Console Manager window. Right-click the Databases icon, choose New Database, and enter the database name `NetworkData`. Later, I provide a script that uses this database to identify which servers need specific patches and to install the patches.

To create a table in the `NetworkData` database, double-click `NetworkData`, then right-click Tables and choose New Table. MySQLCC displays a window labeled *Creating Table in database "Network-Data."* The window contains three columns: Field Name, Allow NULL (which specifies that the field can contain a null, or empty, value), and Data Type, as Figure 5-1 shows.

Figure 5-1
Creating a MySQL Table



Because we'll use this database to track the patches that particular servers need, we'll store two values: the name of the server and of the application that it's running. Enter *Computer* in the first Field Name field and keep varchar as the Data Type. Enter *App* in the second Field Name field and again keep varchar as the Data Type. Click the Save icon, save the table as *ComputerApps*, then close the table-creation window.

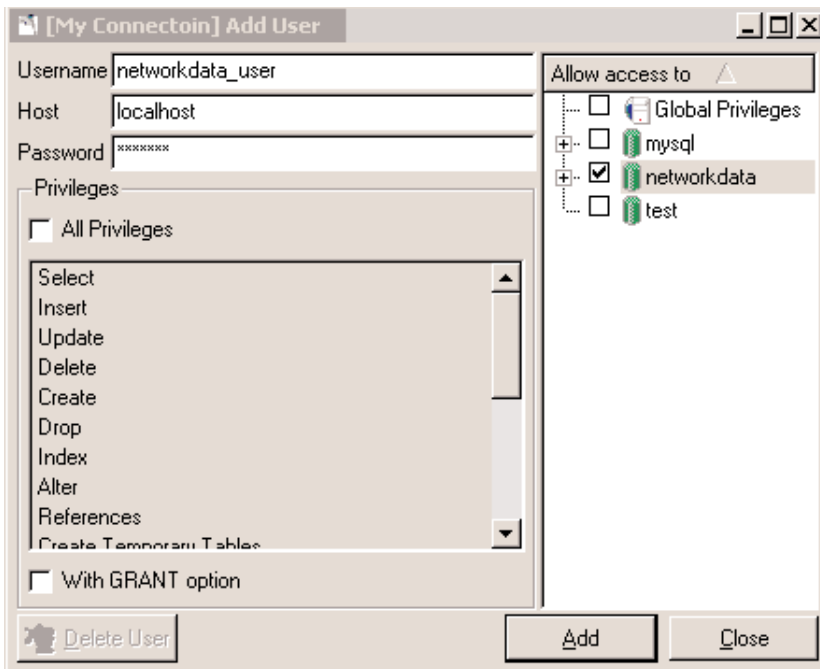
Like any multiuser relational database management system (DBMS), MySQL relies on user accounts to specify access to databases, tables, and columns. Before you create accounts, you need to decide from which computers a user will connect. For example, if you're creating an account that has administrative control over a MySQL database and you want administrators to access that account only from the MySQL server console, you must create the account with only local machine access. To allow access over a network, you must specify one account for each remote client machine address, where the address is either the client's name or TCP/IP address. Alternatively, when you specify an account, you can simply use the percent sign (%) in the Host portion of the account. The % character acts as a wildcard and allows any remote machine to access the database. For example, say that Alice needs access only from server1 and server2 and Bob needs access from anywhere. Table 5-1 shows the accounts you'd create to provide the required access.

Table 5-1 Sample MySQL Accounts

User	Account	Access
Alice	alice@server1	From server1
Alice	alice@server2	From server2
Bob	bob@%	From any remote machine
Bob	bob@localhost	From the MySQL server

For the NetworkData database, you need to allow the user access from anywhere, so you'll create two accounts: `networkdata_user@localhost` and `networkdata_user@%`. To create the accounts, right-click User Administration in the MySQLCC window and choose New User. Enter `networkdata_user` in the Username field, `localhost` in the Host field, and a password, as Figure 5-2 shows.

Figure 5-2
Creating a MySQL account



To specify that `networkdata_user` has access to the NetworkData database, select the check box next to `networkdata` in the *Allow access to* pane. Finally, click Add to create the user, then click Close. Repeat these steps to create another account with the same username, but specify % in the Host field.

Connecting to MySQL from Windows Applications

The next step is to access the NetworkData database from a Windows application, namely Microsoft Access. Being able to use multiple methods to connect to MySQL is convenient when you're building interfaces for use by people (a situation in which Access or even Visual Basic—VB—shines) or shell scripts (for which the MySQL command-line tools play an important role).

From a client machine, download Connector/ODBC (formerly known as MyODBC), the open-source ODBC driver for MySQL (<http://www.mysql.com/downloads/api-myodbc.html>). Click the link to the current production release, page down to the Windows downloads section, and download Driver Installer. (I used Connector/ODBC Driver Installer 3.51.06 for this article.) Next, run the installation program and follow the instructions.

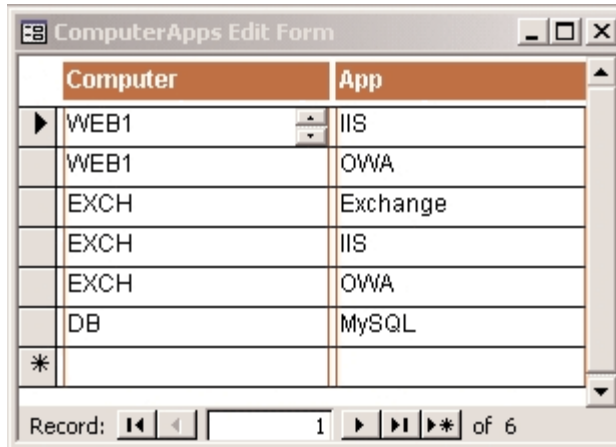
Then, configure a Data Source Name (DSN). A DSN is a way to abstract ODBC database connections from the applications that use them. For example, in Access you might use the *Database Connection* DSN to connect to a SQL Server database. Later, you might replace SQL Server with MySQL, which would require you to reconfigure the Database Connection DSN. If you retain the name Database Connection for the DSN, however, you won't need to reconfigure Access as well.

To configure a DSN, go to Administrative Tools and open the Data Sources (ODBC) tool. Choose either User DSN or System DSN. (System DSNs are systemwide, whereas User DSNs can be used only by the logged-in user who created the DSN.) Click Add, MySQL ODBC 3.51 Driver, Finish. The resulting MySQL Connector/ODBC configuration screen contains several fields that you need to complete. For Data Source Name, enter a descriptive name for the DSN, such as NetworkData. For *Host/Server Name (or IP)*, enter the MySQL server's host name or TCP/IP address. Type NetworkData in the Database Name field, and enter networkdata_user and the appropriate password in the User and Password fields, respectively. Before you continue, click Test Data Source to ensure that the connection is working.

Now you can access your NetworkData database tables in Access 2000. To do so, follow these steps:

1. Open Access.
2. Create a new, blank database.
3. In the Tables object, right-click in the Tables window and choose Link Tables.
4. For *Files of type*, choose ODBC Databases.
5. In the Select Data Source window that appears, choose Machine Data Source to specify a DSN.
6. In the Machine Data Source window, choose the NetworkData DSN.
7. When Access presents the Link Tables window, choose ComputerApps.
8. In the Select Unique Record Identifier dialog box, press and hold Shift while you select the Computer and App fields.

You can now use Access to edit the information in the ComputerApps table by building an Access form, as Figure 5-3 shows, or by double-clicking the ComputerApps icon in the Tables window.

Figure 5-3*Using an Access form to edit a MySQL table*

Tools such as Business Objects' Crystal Reports or Access's built-in reporting functionality let you build reports based on the NetworkData database as you populate its tables.

Using MySQL from the Command Line

One of the most powerful benefits of MySQL is the Mysql command-line tool, which installs by default in C:\mysql\bin and doesn't require an ODBC connection. You can use Mysql to do everything from locking database tables to inserting rows into and deleting rows from a table, all from the command line. You can use Mysql interactively or noninteractively (e.g., in a batch file), depending on how you invoke the command.

To run Mysql interactively, simply type the command in the command line and specify the host name, account information, and database that you want to use, as I did in the sample command-line session that Figure 5-4 shows.

Figure 5-4*Running Mysql interactively from the command line*

```
C:\mysql\bin>mysql -h mysqlsvr -u networkdata_user -p NetworkData
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 25 to server version: 4.0.13-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> quit
```

In the sample command, the `-h` option specifies the MySQL server's TCP/IP address or host name (e.g., `mysqlsvr`). The server defaults to `localhost`, so if you run the `Mysql` command from the MySQL server, you can omit this option. The `-u` option specifies the MySQL username, and the `-p` option indicates that you want Mysql to prompt you for a password. (For information about anonymous connections, which don't require passwords, see the sidebar "Predefined MySQL Accounts, page 28.")

Using MySQL in a Script

To use Mysql noninteractively (e.g., in a shell script), you use the `-e` option followed by the SQL statement to be executed and the `-p` option followed by the account password. The SQL statement in the following command uses the asterisk (*) wildcard to select all columns in the `NetworkData` database's `ComputerApps` table and prints the output that Figure 5-5 shows.

```
C:\mysql\bin>mysql -h mysqlsvr
-u networkdata_user
-p <password>
-e "SELECT * FROM ComputerApps"
NetworkData
```

Figure 5-5

Sample output from the Mysql SELECT statement

Computer	App
WEB1	IIS
WEB1	OWA
EX CH	Exchange
EX CH	IIS
EX CH	OWA
DB	MySQL

In shell scripts, use the `-B` and `-skip-column-names` options so that Mysql doesn't list column names and print table-like output such as Figure 5-5 shows. These options reduce Mysql's output to tab-separated fields that shell scripts can easily parse. To learn more about the available Mysql options, you can simply invoke the Mysql command and specify the `-help` parameter.

A Patch-Management Script

Imagine that you have a network of servers, each of which must be diligently patched. You've decided to deploy a custom patch-management solution using MySQL, shell scripts, and Qchain. You create the `ComputerApps` table and populate it with the OS and applications that are running on each server. Then, you use the shell script that Listing 5-1 shows to access this table.

Listing 5-1 Patch-Management Script

```
@echo off
START CALLOUT A
set SVR=mysqlsvr
set DB=NetworkData
set USER=networkdata_user
set PW=password
set OPTS= skip-column-names -B -h %SVR% -u %USER% -p%PW%
set PATCH_UNC=\\fileserver\patches
END CALLOUT A

START CALLOUT B
set SQL=SELECT App FROM ComputerApps WHERE Computer = '%COMPUTERNAME%'
END CALLOUT B

net use /d /y P: 2> NUL
net use P: %PATCH_UNC% 2> NUL
if errorlevel 1 (
    echo Could not map to patch file server, exiting..
    goto :EOF
)

BEGIN COMMENT LINE
rem Notice the use of backticks.
END COMMENT LINE
START CALLOUT C
for /F usebackq %%x in (`mysql %OPTS% -e "%SQL%" %DB%`) do (
    if "%%x" == "Win2k"    call :Win2k
    if "%%x" == "IIS"     call :IIS
)

echo Running qchain..
p:\qchain.exe
echo Patches applied. The server must now be rebooted.
goto :EOF
END CALLOUT C

:Win2k
echo Patching Win2k
echo
p:\Q123456_w2k_sp2_x86.exe -z -m
goto :EOF

:IIS
echo Patching IIS..
echo
goto :EOF
```

To match the local server name with a server name in the ComputerApps table and retrieve a list of the applications that are installed on that server, the script performs an SQL SELECT statement that contains a WHERE clause, as callout B in Listing 5-1 shows. Most of the script's logic is in the For loop, which callout C shows. This code parses the list and calls the appropriate subroutine for each application (e.g., subroutine :IIS for Microsoft IIS). The subroutine determines whether the application requires a patch and applies the appropriate patch when one is needed.

This script is a skeleton implementation that patches Win2K and IIS. You can easily adapt the script to your site and expand it to apply patches—and even hardening scripts—to other software. To adapt the script to your site, locate the code that callout A shows. Change the value of the SVR variable from mysqlsvr to your MySQL server host name, change the value of the DB variable to specify your MySQL database, set the USER variable to the username, specify the user's password for the PW variable, and replace the PATCH_UNC variable's value with the path to your patch files. After you configure the script to run in your network, you can use Scheduled Tasks to execute it automatically, or you can execute it manually during administrative downtime.

As another example of how powerful even the simple NetworkData database can be, imagine running a set of internally developed post-server-installation scripts on a newly installed Windows Server 2003 system. These scripts would determine the local server's application requirements based on the server's name and the records in NetworkData, install and configure the listed applications, then run lockdown scripts (e.g., for IIS). Automating these tasks plays directly from any disaster-recovery plan and can be a boon to harried administrators faced with day-to-day server deployments.

More Flexibility, Lower Cost

MySQL can lower your licensing and operating cost while increasing flexibility and letting you centralize vital company information. Whether you use MySQL to build an enterprisewide intranet or to provide a centralized information store for your scripts, you're well on your way to realizing the benefits of this powerful and cost-effective database server.