

# Introducing Windows Server 2008

*Mitch Tulloch with the  
Microsoft Windows Server  
Team*

[Purchase select Microsoft Press books at a discount](#)  
(available in the United States only)

To learn more about this book, visit Microsoft Learning at  
<http://www.microsoft.com/MSPress/books/11163.aspx>

9780735624214  
Publication Date: May 2007

**Microsoft®**  
Press

## Additional Resources for IT Professionals

Published and Forthcoming Titles from Microsoft Press

### → Windows Server

Microsoft® Windows Server® 2003  
*Resource Kit*

Microsoft MVPs and Partners with  
Microsoft Windows Server Team  
978-0-7356-2232-6

Microsoft Windows Server 2003  
*Administrator's Companion*  
Second Edition

Charlie Russel, Sharon Crawford,  
and Jason Gerend  
978-0-7356-2047-6

Microsoft Windows Server 2003  
*Inside Out*

William R. Stanek  
978-0-7356-2048-3

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

William R. Stanek  
978-0-7356-2245-6

### → Windows Client

Windows Vista™  
*Resource Kit*

Tulloch, Northrup, Honeycutt,  
Russel, and Wilson with the  
Microsoft Windows Vista Team  
978-0-7356-2283-8

Windows Vista  
*Administrator's Pocket Consultant*

William R. Stanek  
978-0-7356-2296-8

Microsoft Windows® XP  
Professional  
*Resource Kit*  
Third Edition

The Microsoft Windows Team with  
Charlie Russel and Sharon Crawford  
978-0-7356-2167-1

Microsoft Windows XP  
Professional  
*Administrator's Pocket Consultant*  
Second Edition

William R. Stanek  
978-0-7356-2140-4

Microsoft Windows Command-Line  
*Administrator's Pocket Consultant*

William R. Stanek  
978-0-7356-2038-4

### → SQL Server 2005

Microsoft SQL Server™ 2005  
*Administrator's Pocket Consultant*

William R. Stanek  
978-0-7356-2107-7

Microsoft SQL Server 2005  
*Administrator's Companion*

Whalen, Garcia, et al.  
978-0-7356-2198-5

Inside Microsoft SQL Server 2005:  
*The Storage Engine*

Kalen Delaney  
978-0-7356-2105-3

Inside Microsoft SQL Server 2005:  
*T-SQL Programming*

Itzik Ben-Gan, Dejan Sarka, and  
Roger Wolter  
978-0-7356-2197-8

### → Exchange Server 2007

Microsoft Exchange Server 2007  
*Administrator's Companion*  
Walter Glenn and Scott Lowe  
978-0-7356-2350-7

Microsoft Exchange Server 2007  
*Administrator's Pocket Consultant*

William R. Stanek  
978-0-7356-2348-4

### → Scripting

Microsoft Windows PowerShell™  
*Step by Step*

Ed Wilson  
978-0-7356-2395-8

Microsoft VBScript  
*Step by Step*

Ed Wilson  
978-0-7356-2297-5

Microsoft Windows  
Scripting with WMI:  
Self-Paced Learning Guide

Ed Wilson  
978-0-7356-2231-9

Advanced VBScript for Microsoft  
Windows Administrators

Don Jones and Jeffery Hicks  
978-0-7356-2244-9

#### RELATED TITLES



Microsoft Office  
SharePoint® Server  
2007 *Administrator's  
Companion*  
Bill English with the  
Microsoft SharePoint  
Community Experts  
978-0-7356-2282-1



Microsoft Windows  
Security  
*Resource Kit*  
Second Edition  
Ben Smith and Brian  
Komar with the  
Microsoft Security  
Team  
978-0-7356-2174-9



Microsoft Windows  
Small Business  
Server 2003 R2  
*Administrator's  
Companion*  
Charlie Russel and  
Sharon Crawford  
978-0-7356-2280-7



Microsoft Internet  
Security and  
Acceleration (ISA)  
Server 2004  
*Administrator's Pocket  
Consultant*  
Bud Ratliff and Jason  
Ballard with the Microsoft  
ISA Server Team  
978-0-7356-2188-6

# Resources for IT Professionals



## Administrator's Pocket Consultant

- Practical, portable guide for fast answers when you need them
- Focus on core operations and support tasks
- Organized for quick, precise reference—to get the job done



## Administrator's Companion

- Comprehensive, one-volume guide to deployment and system administration
- Real-world insights, procedures, troubleshooting tactics, and workarounds
- Fully searchable eBook on CD



## Resource Kit

- In-depth technical information and tools from those who know the technology best
- Definitive reference for deployment and operations
- Essential toolkit of resources, including eBook, on CD



## Self-Paced Training Kit

- Two products in one: official exam prep guide + practice tests
- Features lessons, exercises, and case scenarios
- Comprehensive self-tests; trial software; eBook on CD

## Available in 2008 from Microsoft Press

### Windows Server

Windows Server® 2008  
*Resource Kit*  
978-0-7356-2361-3

Windows Server 2008  
Active Directory®  
*Resource Kit*  
978-0-7356-2515-0

Windows Server 2008  
Virtualization  
*Resource Kit*  
978-0-7356-2517-4

Windows Server 2008  
Security *Resource Kit*  
978-0-7356-2504-4

Windows® Administration  
*Resource Kit: Productivity  
Solutions For IT Professionals*  
978-0-7356-2431-3

Windows Server 2008  
Networking Guide  
978-0-7356-2422-1

Windows Server 2008 TCP/IP  
Protocols and Services  
978-0-7356-2447-4

Windows Server 2008  
*Inside Out*  
978-0-7356-2438-2

Windows Server 2008  
Terminal Services  
978-0-7356-2516-7

Windows Server 2008  
*Administrator's Companion*  
978-0-7356-2505-1

Windows Server 2008  
*Administrator's Pocket Consultant*  
978-0-7356-2437-5

Windows Group Policy Guide,  
Second Edition  
978-0-7356-2514-3

Understanding IPv6,  
Second Edition  
978-0-7356-2446-7

### Internet Information Services

Internet Information  
Services (IIS) 7.0  
*Administrator's Pocket Consultant*  
978-0-7356-2364-4

Internet Information  
Services (IIS) 7.0  
*Resource Kit*  
978-0-7356-2441-2

### Scripting

Windows PowerShell™  
Scripting Guide  
978-0-7356-2279-1

Windows PowerShell  
& Command-line  
*Administrator's Pocket Consultant*  
978-0-7356-2262-3

### Certification

MCITP Self-Paced Training Kit  
(Exams 70-640, 70-642,  
70-643, 70-646): Windows Server  
Administrator Core Requirements  
978-0-7356-2508-2

MCITP Self-Paced Training Kit  
(Exam 70-640): Configuring  
Windows Server 2008  
Active Directory  
978-0-7356-2513-6

MCITP Self-Paced Training Kit  
(Exam 70-642): Configuring  
Windows Server 2008  
Network Infrastructure  
978-0-7356-2512-9

MCITP Self-Paced Training Kit  
(Exam 70-643): Configuring  
Windows Server 2008  
Applications Platform  
978-0-7356-2511-2

MCITP Self-Paced Training Kit  
(Exam 70-646): Windows Server  
2008 Administrator  
978-0-7356-2510-5

MCITP Self-Paced Training Kit  
(Exam 70-647): Windows Server  
2008 Enterprise Administrator  
978-0-7356-2509-9

See our full line of learning resources at: [microsoft.com/mspress](http://microsoft.com/mspress) and [microsoft.com/learning](http://microsoft.com/learning)

**Microsoft®**

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

Copyright © 2007 by Microsoft Corporation

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

Library of Congress Control Number: 2007924650

Printed and bound in the United States of America.

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

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

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

Chapter 4 contains the “From the Experts: WMI Remote Connection” sidebar. Copyright © 2007 by Alain Lissor.

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

Microsoft, Microsoft Press, Active Directory, ActiveX, Aero, BitLocker, ClearType, Direct3D, Excel, Internet Explorer, Microsoft Dynamics, MSDN, MS-DOS, Outlook, PowerPoint, SharePoint, SQL Server, Terminal Services RemoteApp, Visual Basic, Visual Studio, Visual Web Developer, Win32, Windows, Windows CardSpace, Windows Live, Windows Media, Windows Mobile, Windows NT, Windows PowerShell, Windows Server, Windows Server System, Windows Vista, and WinFX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

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

**Acquisitions Editor:** Martin DelRe

**Developmental Editor:** Karen Szall

**Project Editor:** Denise Bankaitis

Body Part No. X13-72717

# Table of Contents

<i>Preface</i> .....	xiii
<b>1 Introduction</b> .....	<b>1</b>
What's Between the Sheets .....	3
Acknowledgments .....	4
One Last Thing—Humor .....	7
<b>2 Usage Scenarios</b> .....	<b>9</b>
Providing an Identity and Access Infrastructure .....	10
Ensuring Security and Policy Enforcement .....	10
Easing Deployment Headaches .....	11
Making Servers Easier to Manage .....	12
Supporting the Branch Office .....	13
Providing Centralized Application Access .....	13
Deploying Web Applications and Services .....	14
Ensuring High Availability .....	14
Ensuring Secure and Reliable Storage .....	15
Leveraging Virtualization .....	16
Conclusion .....	16
<b>3 Windows Server Virtualization</b> .....	<b>17</b>
Why Enterprises Love Virtualization .....	17
Server Consolidation .....	18
Business Continuity .....	18
Testing and Development .....	19
Application Compatibility .....	19
Virtualization in the Datacenter .....	19

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

Virtualization Today .....	20
Monolithic Hypervisor .....	22
Microkernelized Hypervisor .....	22
Understanding Virtualization in Windows Server 2008 .....	24
Partition 1: Parent .....	25
Partition 2: Child with Enlightened Guest .....	26
Partition 3: Child with Legacy Guest .....	27
Partition 4: Child with Guest Running Linux .....	28
Features of Windows Server Virtualization .....	28
Managing Virtual Machines in Windows Server 2008 .....	29
System Center Virtual Machine Manager 2007 .....	36
SoftGrid Application Virtualization .....	36
Conclusion .....	37
Additional Reading .....	37
<b>4 Managing Windows Server 2008 .....</b>	<b>39</b>
Performing Initial Configuration Tasks .....	39
Using Server Manager .....	42
Managing Server Roles .....	44
ServerManagerCmd.exe .....	50
Remote Server Administration Tools .....	53
Other Management Tools .....	56
Group Policy .....	56
Windows Management Instrumentation .....	59
Windows PowerShell .....	64
Microsoft System Center .....	68
Conclusion .....	69
Additional Resources .....	69
<b>5 Managing Server Roles .....</b>	<b>71</b>
Understanding Roles, Role Services, and Features .....	71
Available Roles and Role Services .....	72
Available Features .....	83

Adding Roles and Features .....	95
Using Initial Configuration Tasks .....	97
Using Server Manager .....	104
From the Command Line .....	105
Conclusion .....	108
Additional Reading .....	108
<b>6 Windows Server Core .....</b>	<b>109</b>
What Is a Windows Server Core Installation? .....	109
Understanding Windows Server Core .....	111
The Rationale for Windows Server Core .....	115
Performing Initial Configuration of a Windows Server Core Server .....	118
Performing Initial Configuration from the Command Line .....	118
Managing a Windows Server Core Server .....	130
Local Management from the Command Line .....	130
Remote Management Using Terminal Services .....	137
Remote Management Using the Remote Server Administration Tools ....	140
Remote Administration Using Group Policy .....	141
Remote Management Using WinRM/WinRS .....	142
Windows Server Core Installation Tips and Tricks .....	143
Conclusion .....	147
Additional Resources .....	147
<b>7 Active Directory Enhancements .....</b>	<b>149</b>
Understanding Identity and Access in Windows Server 2008 .....	149
Understanding Identity and Access .....	149
Identity and Access in Windows 2000 Server .....	150
Identity and Access in Windows Server 2003 .....	151
Identity and Access in Windows Server 2003 R2 .....	152
Identity and Access in Windows Server 2008 .....	153
Active Directory Domain Services .....	158
AD DS Auditing Enhancements .....	158
Read-Only Domain Controllers .....	164
Restartable AD DS .....	168
Granular Password and Account Lockout Policies .....	169

Active Directory Lightweight Directory Services .....	172
Active Directory Certificate Services .....	176
Certificate Web Enrollment Improvements .....	176
Network Device Enrollment Service Support .....	177
Online Certificate Status Protocol Support .....	177
Enterprise PKI and CAPI2 Diagnostics .....	179
Other AD CS Enhancements .....	180
Active Directory Federation Services .....	182
Active Directory Rights Management Services .....	186
Conclusion .....	187
Additional Resources .....	187
<b>8 Terminal Services Enhancements .....</b>	<b>189</b>
Core Enhancements to Terminal Services .....	190
Remote Desktop Connection 6.0 .....	191
Single Sign-On for Domain-joined Clients .....	200
Other Core Enhancements .....	201
Installing and Managing Terminal Services .....	209
Terminal Services RemoteApp .....	216
Using TS RemoteApp .....	217
Benefits of TS RemoteApp .....	225
Terminal Services Web Access .....	226
Using TS Web Access .....	227
Benefits of TS Web Access .....	232
Terminal Services Gateway .....	232
Implementing TS Gateway .....	235
Benefits of TS Gateway .....	237
Terminal Services Licensing .....	238
Other Terminal Services Enhancements .....	243
Terminal Services WMI Provider .....	243
Windows System Resource Manager .....	246
Terminal Services Session Broker .....	247
Conclusion .....	249
Additional Resources .....	250



<b>9</b>	<b>Clustering Enhancements</b>	<b>251</b>
	Failover Clustering Enhancements	252
	Goals of Clustering Improvements	253
	Understanding the New Quorum Model	254
	Understanding Storage Enhancements	256
	Understanding Networking and Security Enhancements	259
	Other Security Improvements	261
	Validating a Clustering Solution	261
	Tips for Validating Clustering Solutions	266
	Setting Up and Managing a Cluster	267
	Creating a Highly Available File Server	269
	Performing Other Cluster Management Tasks	273
	Network Load Balancing Enhancements	278
	Conclusion	283
	Additional Resources	283
<b>10</b>	<b>Network Access Protection</b>	<b>285</b>
	The Need for Network Access Protection	286
	Understanding Network Access Protection	287
	What NAP Does	288
	NAP Enforcement Methods	289
	Understanding the NAP Architecture	297
	A Walkthrough of How NAP Works	299
	Implementing NAP	301
	Choosing Enforcement Methods	302
	Phased Implementation	303
	Configuring the Network Policy Server	307
	Configuring NAP Clients	317
	Troubleshooting NAP	319
	Conclusion	339
	Additional Resources	340

<b>11</b>	<b>Internet Information Services 7.0</b>	<b>341</b>
	Understanding IIS 7.0 Enhancements	341
	Security and Patching	342
	Administration Tools	351
	Configuration and Deployment	360
	Diagnostics	365
	Extensibility	368
	What's New in IIS 7.0 in Windows Server 2008	370
	The Application Server Role	371
	Conclusion	374
	Additional Resources	375
<b>12</b>	<b>Other Features and Enhancements</b>	<b>377</b>
	Storage Improvements	378
	File Server Role	378
	Windows Server Backup	381
	Storage Explorer	384
	SMB 2.0	386
	Multipath I/O	387
	iSCSI Initiator	390
	iSCSI Remote Boot	397
	iSNS Server	401
	Networking Improvements	402
	Security Improvements	407
	Other Improvements	414
	Conclusion	419
	Additional Resources	419
<b>13</b>	<b>Deploying Windows Server 2008</b>	<b>421</b>
	Getting Windows Server 2008	421
	Installing Windows Server 2008	422
	Manual Installation	422
	Unattended Installation	423

Using Windows Deployment Services .....	423
Multicast Deployment .....	424
TFTP Windowing .....	427
EFI x64 Network Boot Support .....	430
Solution Accelerator for Windows Server Deployment. ....	431
Understanding Volume Activation 2.0 .....	432
Conclusion .....	439
Additional Resources .....	440
<b>14 Additional Resources .....</b>	<b>441</b>
Product Home Page .....	441
Microsoft Windows Server TechCenter .....	442
Microsoft Download Center .....	442
Microsoft Connect.....	443
Microsoft TechNet.....	445
Beta Central .....	445
TechNet Events.....	446
TechNet Virtual Labs.....	448
TechNet Community Resources .....	448
TechNet Columns.....	451
TechNet Magazine.....	451
TechNet Flash Newsletter.....	451
MSDN .....	451
Blogs .....	452
Blogs by MVPs .....	453
Channel 9 .....	454
Microsoft Press Books.....	454
Conclusion .....	455
<b>Index .....</b>	<b>457</b>

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

# Managing Windows Server 2008

**In this chapter:**

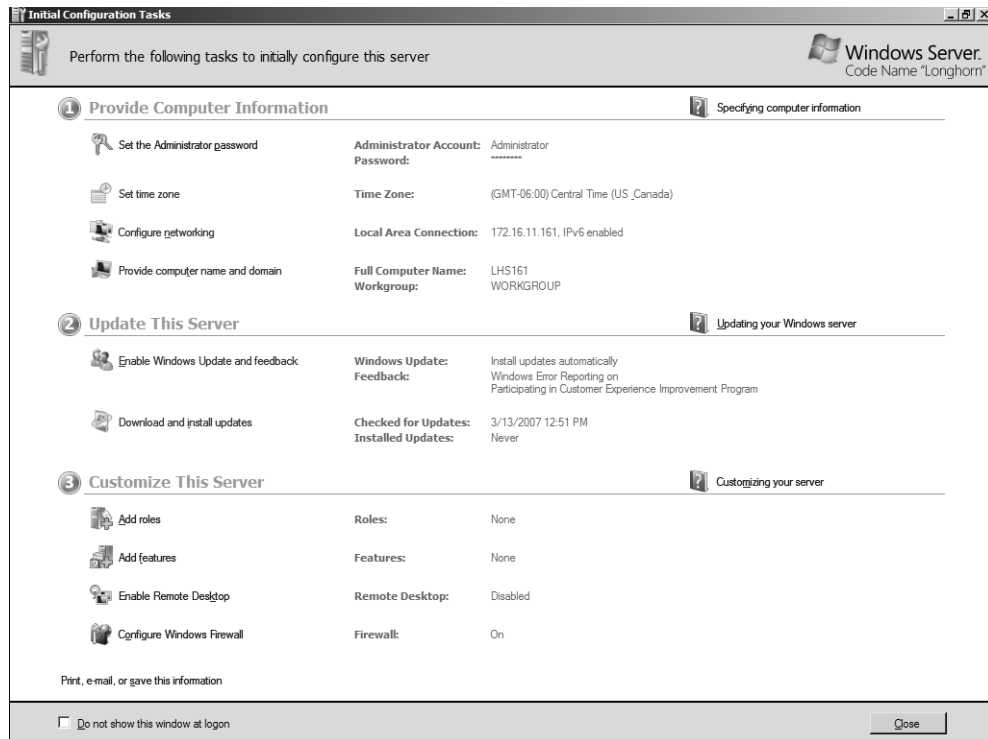
<b>Performing Initial Configuration Tasks</b> .....	<b>39</b>
<b>Using Server Manager</b> .....	<b>42</b>
<b>Other Management Tools</b> .....	<b>56</b>
<b>Conclusion</b> .....	<b>69</b>
<b>Additional Resources</b> .....	<b>69</b>

I was kidding, of course, when I said we should bring back the mainframe. After all, remember how much fun it was managing those machines? Sitting at a green screen all day long, dropping armfuls of punch cards into the hopper...what fun! At least running an IBM System/360 could be more fun than operating a PDP-11. When I was a university student years ago (decades actually), I worked one summer for the physics department, where there was a PDP-11 in the sub-sub-basement where the Cyclotron was located. I remember sitting there alone one night around 3 a.m. while an experiment was running, watching the lights blink on the PDP and flipping a switch from time to time to read a paper tape. And that was my introduction to the tools used for managing state-of-the-art computers in those days—specifically, lights, switches, and paper tape.

Computers have come a long way since then. Besides being a lot more powerful, they're also a lot easier to manage. So before we examine other new and exciting features of Microsoft Windows Server 2008, let's look at the new and enhanced tools you can use to manage the platform. These tools range from user interface (UI) tools for configuring and managing servers to a new command-line tool for installing roles and features, tools for remote administration, Windows Management Instrumentation (WMI) enhancements for improved scripted management, Group Policy enhancements, and more.

## Performing Initial Configuration Tasks

The first thing you'll notice when you install Windows Server 2008 is the Initial Configuration Tasks screen (shown in Figure 4-1).



**Figure 4-1** The Initial Configuration Tasks screen

Remember for a moment how you perform your initial configuration of a machine running Windows Server 2003 Service Pack 1 or later, where you do this in three stages:

1. During Setup, when you specify your administrator password, network settings, domain membership, and so on
2. Immediately after Setup, when a screen appears asking if you want to download the latest updates from Windows Update and turn on Automatic Updates before the server can receive inbound traffic
3. After you've allowed inbound traffic to your server, when you can use Manage Your Server to install roles on your server to make it a print server, file server, domain controller, and so on

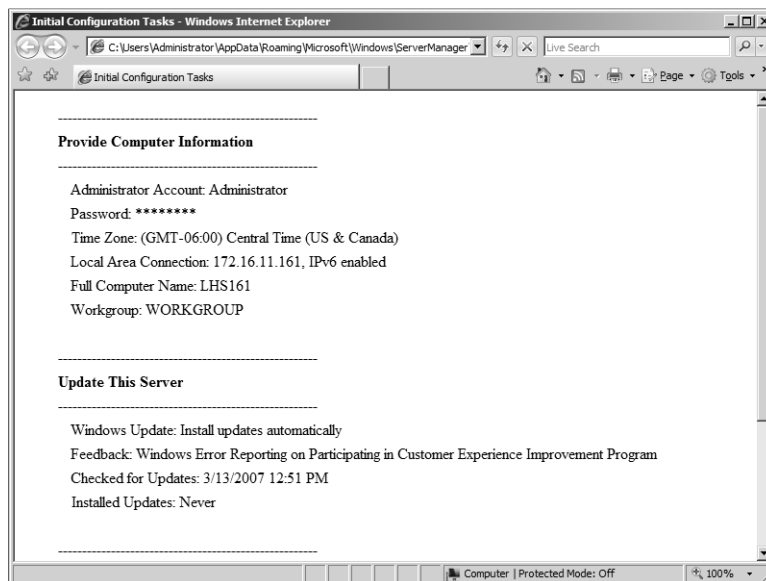
Windows Server 2008, however, consolidates these various server configuration tasks by consolidating during- and post-Setup tasks together and presenting them to you in a single screen called Initial Configuration Tasks (ICT). Using the ICT you can

- Specify key information, including the administrator password, time zone, network settings, and server name. You can also join your server to a domain. For example, clicking the Provide Computer Name And Domain link opens System Properties with the Computer Named tab selected.

- Search Windows Update for available software updates, and enable one or more of the following: Automatic Updates, Windows Error Reporting (WER), and participation in the Customer Experience Improvement Program.
- Configure Windows Firewall on your machine, and enable Remote Desktop so that the server can be remotely managed using Terminal Services.
- Add roles and features to your server—for example, to make it a DNS server or domain controller.

In addition to providing a user interface where you can perform these tasks, ICT also displays status information for each task. For example, if a task has already been performed, the link for the task changes color from blue to purple just like an ordinary hyperlink. And if WER has been turned on, the message “Windows Error Reporting on” is displayed next to the corresponding task item.

Once you’ve performed the initial configuration of your server, you can click the Print, E-mail Or Save This Information link at the bottom. This opens Internet Explorer and displays a results page showing the settings you’ve configured.



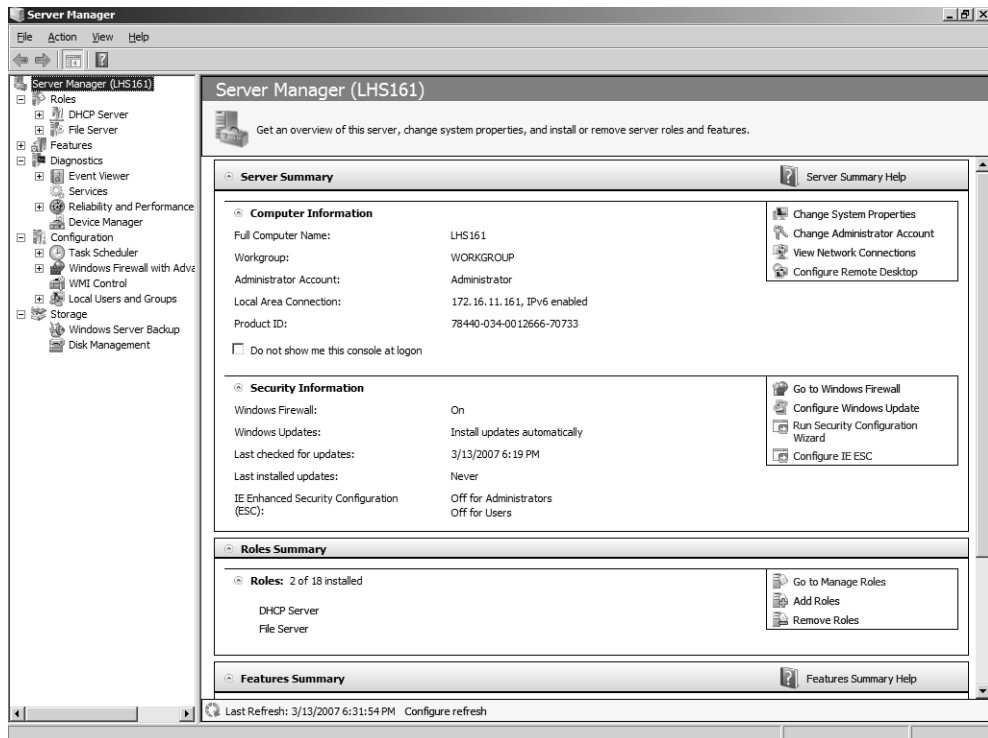
This results page can be found at %systemdrive%\users\<username>\AppData\Roaming\Microsoft\Windows\ServerManager\InitialConfigurationTasks.html, and it can be saved or e-mailed for reporting purposes.

A few more notes concerning Initial Configuration Tasks:

- Performing some tasks requires that you log off or reboot your machine. For example, by default when you install Windows Server 2008, the built-in Administrator account is enabled and has no password. If you use ICT to change the name of this account or specify a password, you must log off and then on again for this change to take effect.
- If Windows Server 2008 detects that it is deployed on a restricted network (that is, quarantined by NAP) when you first log on, the Update This Server section of the ICT displays a new link named Restore Network Access. Clicking this link allows you to review current network access restrictions and restore full network access for your server, and until you do this your server is in quarantine and has only limited network access. The reason that the other two items in this section (Enable Windows Update And Feedback and Download And Install Updates) are not displayed in this situation is that machines in quarantine cannot access Windows Update directly and must receive their updates from a remediation server. For more information about this, see Chapter 10, “Network Access Protection.”
- OEMs can customize the ICT screen so that it displays an additional section at the bottom that can include an OEM logo, a description, and task links that can launch EXEs, DLLs, and scripts provided by the OEM. Note that OEM task links cannot display status information, however.
- The ICT is not displayed if you upgrade to Windows Server 2008 from a previous version of Windows Server.
- The ICT is also not displayed if the following Group Policy setting is configured:  
Computer Configuration\Administrative Templates\System\Server Manager\Do Not Open Initial Configuration Tasks Windows At Logon

## Using Server Manager

OK, you’ve installed your server, performed the initial configuration tasks, and maybe installed a role or two—such as file server and DHCP server—on your machine as well. Now what? Once you close ICT, another new tool automatically opens—namely, Server Manager (shown in Figure 4-2). I like to think of Server Manager as “Computer Management on steroids,” as it can do everything compmgmt.msc can do plus a whole lot more. (Look at the console tree on the left in this figure and you’ll see why I said this.)



**Figure 4-2** Main page of Server Manager

The goal of Server Manager is to provide a straightforward way of installing roles and features on your server so that it can function within your business networking environment. As a tool, Server Manager is primarily targeted toward the IT generalist who works at medium-sized organizations. IT specialists who work at large enterprises might want to use additional tools to configure their newly installed servers, however—for example, by performing some initial configuration tasks during unattended setup by using Windows Deployment Services (WDS) together with unattend.xml answer files. See Chapter 13, “Deploying Windows Server 2008,” for more information on using WDS to deploy Windows Server 2008.

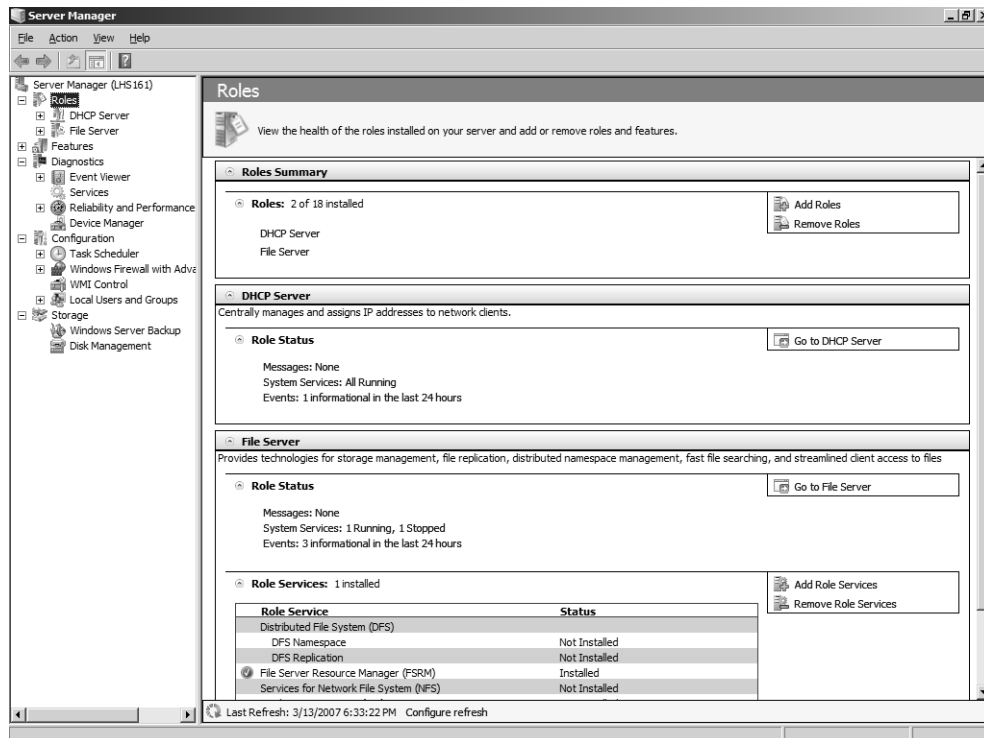
Server Manager also enables you to modify any of the settings you specified previously using the Initial Configuration Tasks screen. For example, in Figure 4-2 you can see that you can enable Remote Desktop by clicking the Configure Remote Desktop link found on the right side of the Server Summary tile. In fact, Server Manager lets you configure additional advanced settings that are not exposed in the ICT screen, such as enabling or disabling the Internet Explorer Enhanced Security Configuration (IE ESC) or running the Security Configuration Wizard (SCW) on your machine.



## Managing Server Roles

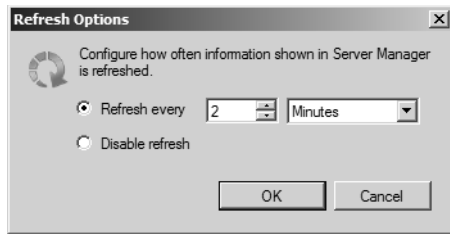
Let's dig a bit deeper into Server Manager. Near the bottom of Figure 4-2, you can see that we've already installed two roles on our server using the ICT screen. We'll learn more about the various roles, role services, and features you can install on Windows Server 2008 later in Chapter 5, "Managing Server Roles." For now, let's see what we can do with these two roles that have already been installed.

Clicking the Go To Manage Roles link changes the focus from the root node (Server Manager) to the Roles node beneath it. (See Figure 4-3.) This page displays a list of roles installed on the server and the status of each of these roles, including any role services that were installed together with them. (Role services will be explained later in Chapter 5.)



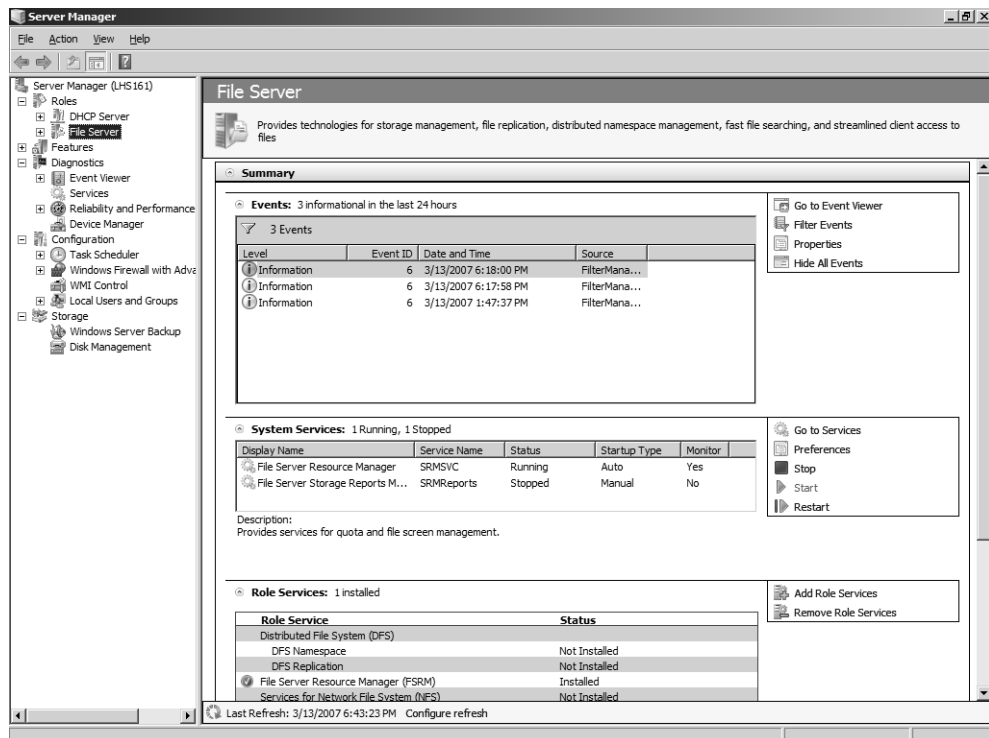
**Figure 4-3** Roles page of Server Manager

The status of this page is updated in real time at periodic intervals, and if you look carefully at these figures you'll see a link at the bottom of each page that says "Configure refresh." If you click this link, you can specify how often Server Manager refreshes the currently displayed page. By default, the refresh interval is two minutes.



Selecting the node for the File Server role in the console tree (or clicking the Go To File Server link on the Roles page) displays more information about how this role is configured on the machine (as shown in Figure 4-4). Using this page, you can manage the following aspects of your file server:

- View events relevant to this role (by double-clicking on an event to display its details).
- View system services for this role, and stop, start, pause, or resume these services.
- View role services installed for this role, and add or remove role services.
- Get help on how to perform role-related tasks.

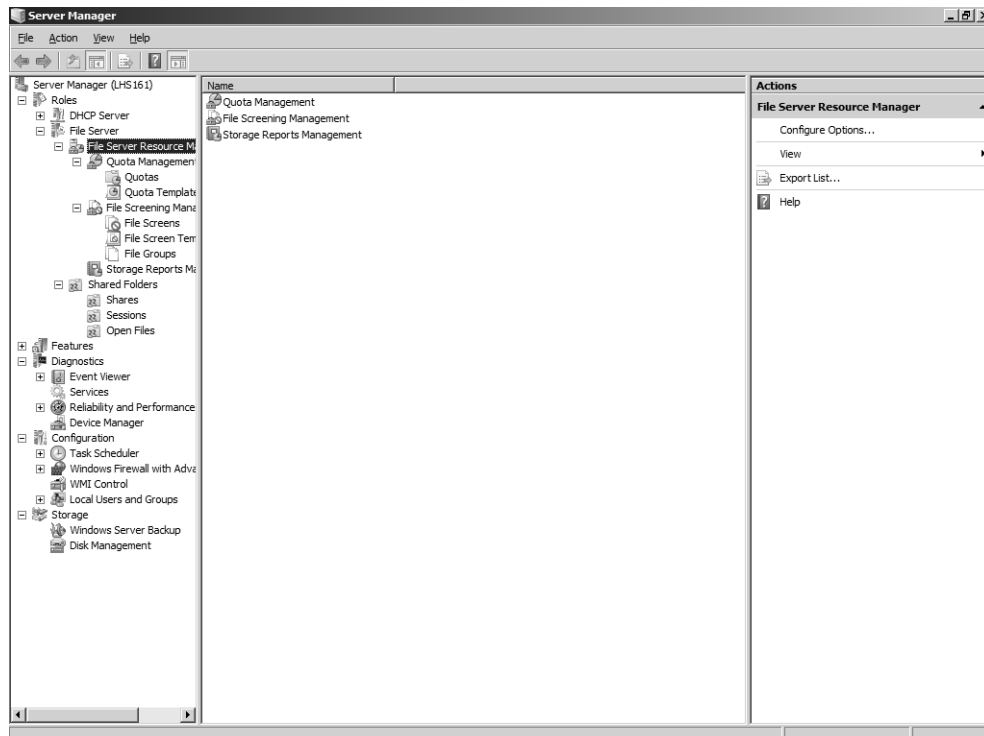


**Figure 4-4** Main page for File Server role

Note the check mark in the green circle beside File Server Resource Manager (FSRM) under Role Services. This means that FSRM, an optional component or “role service” for the File

Server role, has been installed on this server. You probably remember FSRM from Windows Server 2003 R2—it's a terrific tool for managing file servers and can be used to configure volume and folder quotas, file screens, and reporting. But in Windows Server 2003 R2, you had to launch FSRM as a separate administrative tool—not so in Windows Server 2008. What's cool about Server Manager is that it is implemented as a managed, user-mode MMC 3.0 snap-in that can host other MMC snap-ins and dynamically show or hide them inline based on whether a particular role or feature has been installed on the server.

What this means here is that we can expand our File Server node, and underneath it you'll find two other snap-ins—namely, File Server Resource Manager (which we chose to install as an additional role service when we installed the File Server role on our machine) and Shared Folders (which is installed by default whenever you add the file server role to a machine.) And underneath the FSRM node, you'll find the same subnodes you should already be familiar with in FSRM on Windows Server 2003 R2. (See Figure 4-5.) And anything you can do with FSRM in R2, you do pretty much the same way in Windows Server 2008. For example, to configure an SMTP server for sending notification e-mails when quotas are exceeded, right-click on the File Server Resource Manager node and select Properties. (In addition to hosting the FSRM snap-in within Server Manager, adding the FSRM role service also adds the FSRM console to Administrative Tools.)



**Figure 4-5** File Server role showing hosted snap-ins for File Server Resource Manager and Shared Folders

Here are a few more important things to know about Server Manager. First, Server Manager is designed to be a single, all-in-one tool for managing your server. In that light, it replaces both Manage Your Server (for adding roles) and the Add/Remove Windows Components portion of Add Or Remove Programs found on previous versions of Windows Server. In fact, if you go to Control Panel and open Programs And Features (which replaced Add Or Remove Programs in Windows Vista), you'll see a link called Turn Windows Features On And Off. If you click that link, Server Manager opens and you can use the Roles or Features node to add or remove roles, role services, and features. (See Chapter 5 for how this is done.)

Also, when Server Manager is used to install a role such as File Server on your server, it makes sure that this role is *secure by default*. (That is, the only components that are installed and ports that are opened are those that are absolutely necessary for that role to function.) In Windows Server 2003 Service Pack 1 or later, you needed to run the Security Configuration Wizard (SCW) to ensure a server role was installed securely. Windows Server 2008 still includes the SCW, but the tool is intended for use by IT specialists working in large enterprises. For medium-sized organizations, however, IT generalists can use Server Manager to install roles securely, and it's much easier to do than using SCW. In addition, while Server Manager can be used for installing new roles using *smart defaults*, SCW is mainly designed as a post-deployment tool for creating security policies that can then be applied to multiple servers to harden them by reducing their attack surface. (You can also compare policies created by SCW against the current state of a server for auditing reasons to ensure compliance with your corporate security policy.) Finally, while Server Manager can only be used to add the default Windows roles (or out-of-band roles made available later, as mentioned in the extensibility discussion a bit later), SCW can also be used for securing nondefault roles such as Exchange Server and SQL Server. But the main takeaway for this chapter concerning Server Manager vs. SCW is that when you run Server Manager to install a new role on your server, you don't need to run SCW afterward to lock down the role, as Server Manager ensures the role is already secure by default.

Server Manager relies upon something called Component Based Servicing (CBS) to discover what roles and services are installed on a machine and to install additional roles or services or remove them. For those of you who might be interested in how this works, there's a sidebar in the next section that discusses it in more detail. Server Manager is also designed to be extensible. This means when new features become available (such as Windows Server Virtualization, which we talked about in Chapter 3, "Windows Server Virtualization"), you'll be able to use Server Manager to download these roles from Microsoft and install them on your server.

Server Manager is designed to manage one server only (the local server) and cannot be used to manage multiple servers at once. If you need a tool to manage multiple servers simultaneously, use Microsoft System Center. You can find out more about System Center products and their capabilities at <http://www.microsoft.com/systemcenter/>, and it will be well worth your time to do so. In addition, the status information displayed by Server Manager is limited to

event information and whether role services are running. So if you need more detailed information concerning the status of your servers, again be sure to check out System Center, the next generation of the SMS and MOM platforms.

Unlike using Computer Management, you can't use Server Manager to remotely connect to another server and manage it. For example, if you right-click on the root node in Server Manager, the context menu that is displayed does not display a Connect To A Different Computer option. However, this is not really a significant limitation of the tool because most admins will simply enable Remote Desktop on their servers and use Terminal Services to remotely manage them. For example, you can create a Remote Desktop Connection on a Windows Vista computer, use it to connect to the console session on a Windows Server 2008 machine, and then run Server Manager within the remote console session. And speaking of Computer Management, guess what happens if you click Start, right-click on Computer, and select Manage? In previous versions of Windows, doing this opened Computer Management—what tool do you think opens if you do this in Windows Server 2008?

Finally, a few more quick points you can make note of:

- Server Manager cannot be used to manage servers running previous versions of the Windows Server operating system.
- Server Manager cannot be installed on Windows Vista or previous versions of Microsoft Windows.
- Server Manager is not available on a Windows server core installation of Windows Server 2008 because the supporting components (.NET Framework 2.0 and MMC 3.0) are not available on that platform.
- You can configure the refresh interval for Server Manager and also whether the tool is automatically opened at logon by configuring the following Group Policy settings:
  - Computer Configuration\Administrative Templates\System\Server Manager\Do Not Open Server Manager Automatically At Logon
  - Computer Configuration\Administrative Templates\System\Server Manager\Configure The Refresh Interval For Server Manager

## **From the Experts: The Security Configuration Wizard in Windows Server 2008**

The Security Configuration Wizard (SCW) reduces the attack surface of Windows Servers by asking the user a series of questions designed to identify the functional requirements of a server. Functionality not required by the roles the server is performing is then disabled. In addition to being a fundamental security best practice, SCW reduces the number of systems that need to be immediately patched when a vulnerability is exposed. Specifically, SCW:

- Disables unneeded services.
- Creates required firewall rules.
- Removes unneeded firewall rules.
- Allows further address or security restrictions for firewall rules.
- Reduces protocol exposure to server message block (SMB), LanMan, and Lightweight Directory Access Protocol (LDAP).

SCW guides you through the process of creating, editing, applying, or rolling back a security policy based on the selected roles of the server. The security policies that are created with SCW are XML files that, when applied, configure services, Windows Firewall rules, specific registry values, and audit policy. Those security policies can be applied to an individual machine or can be transformed into a group policy object and then linked to an Organizational Unit in Active Directory.

With Windows Server 2008 some important improvements have been made to SCW:

- On Windows Server 2003, SCW was an optional component that had to be manually installed by administrators. SCW is now a default component of Windows Server 2008 which means Administrators won't have to perform extra steps to install or deploy the tool to leverage it.
- Windows Server 2008 will introduce a lot of new and exciting functionality in Windows Firewall. To support that functionality, SCW has been improved to store, process, and apply firewall rules with the same degree of precision that the Windows Firewall does. This was an important requirement since on Windows Server 2008 the Windows Firewall will be on by default.
- The SCW leverages a large XML database that consists of every service, firewall rule and administration option from every feature or component available on Windows Server 2008. This database has been totally reviewed and updated for Windows Server 2008. Existing roles have been updated, new roles have been added to the database, and all firewall rules have been updated to support the new Windows Firewall.

- SCW now validates all XML files in its database files using a set of XSD files that contains the SCW XML schema. This will help administrators or developers extend the SCW database by creating new SCW roles base on their own requirements or applications. Those XSD files are available under the SCW directory.
- All SCW reports have been updated to reflect the changes made to the SCW schema regarding support for the new Window Firewall. Those reports include the Configuration Database report, the Security Policy report and the Analysis report that will compare the current configuration of Windows Server 2008 against an SCW security policy.

SCW provides an end to end solution to reduce the attack surface of Windows Server 2008 machines by providing a possible configuration of default components, roles, features, and any third-party applications that provide an SCW role.

SCW is not responsible for installing or removing any roles, features, or third-party applications from Windows Server 2008. Instead, Administrators should use Server Manager if they need to install roles and features, or use the setup provided with any third party application. The installation of roles and features via Server Manager is made based on security best practices.

While SCW complements well Server Manager, its main value is in the configuration of the core operating system and third-party applications that provide an SCW role. SCW should be used every time the configuration of a default component on Windows Server 2008 needs to be modified or when a third-party application is added or removed. In some specific scenarios, like for remote administration, running SCW after using Server Manager might provide some added value to some specific roles or features. Using SCW after modifying a role or feature through Server Manager is not a requirement, however.

—Nils Dussart

*Program Manager for the Security Configuration Wizard (SCW), Windows Core Operating System Division*

## ServerManagerCmd.exe

In addition to the Server Manager user interface, there is also a command-line version of Server Manager called ServerManagerCmd.exe that was first introduced in the IDS\_2 build of Windows Server 2008 (that is, the February CTP build). This command-line tool, which is found in the %windir%\system32 folder, can be used to perform the following tasks:

- Display a list of roles and features already installed on a machine.
- Display a list of role services and features that would be installed if you chose to install a given role.
- Add a role or feature to your server using the default settings of that role or feature.

- Add several roles/features at once by providing an XML answer file listing the roles/features to be installed.
- Remote roles or features from your server.

What `ServerManagerCmd.exe` *can't* do includes the following:

- Install a role or feature, and change its default settings.
- Reconfigure a role or feature already installed on the machine.
- Connect to a remote machine, and manage roles/features on that machine.
- Manage roles/features on machines running a Windows server core installation of Windows Server 2008.
- Manage non-OOB roles/features—such as Exchange Server or SQL Server.

Let's take a look at the `servermanagercmd -query` command, which displays the list of roles and features currently available on the computer, along with their command-line names (values that should be used to install or remove the role or feature from the command line). When you run this command, something called *discovery* runs to determine the different roles and features already installed.

```
Administrator: Command Prompt - servermanagercmd -query
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>servermanagercmd -query
Starting discovery
.....
```

After discovery completes (which may take a short period of time), the command generates output displaying installed roles/features in green and marked with “X”.

```
Administrator: Command Prompt
[ ] Application Server [Application-Server]
[ ] Application Server Core [AS-AppServer-Core]
[ ] Web Server (IIS) Support [AS-Web-Support]
[ ] COM+ Network Access [AS-Ext-Services]
[ ] TCP Port Sharing [AS-TCP-Port-Sharing]
[ ] Windows Process Activation Service Support [AS-WPAS-Support]
[ ] HTTP Activation [AS-HTTP-Activation]
[ ] Message Queuing Activation [AS-MSMQ-Activation]
[ ] TCP Activation [AS-TCP-Activation]
[ ] Named Pipes Activation [AS-Named-Pipes]
[ ] Distributed Transactions [AS-Dist-Transaction]
[ ] Incoming Remote Transactions [AS-Incoming-Trans]
[ ] Outgoing Remote Transactions [AS-Outgoing-Trans]
[ ] WS-Atomic Transactions [AS-WS-Atomic]
[X] DHCP Server [DHCP]
[ ] DNS Server [DNS]
[ ] Fax Server [Fax]
[X] File Server
[ ] Distributed File System (DFS) [FS-DFS]
[ ] DFS Namespace [FS-DFS-Namespacel]
[ ] DFS Replication [FS-DFS-Replication]
[X] File Server Resource Manager (FSRM) [FS-Resource-Manager]
[ ] Services for Network File System (NFS) [FS-NFS-Services]
[ ] Single Instance Store (SIS) [FS-Single-Instance]
[ ] Windows Search Service [FS-Search-Service]
```



You can also type **servermanagercmd -query results.xml** to send the output of this command to an XML file. This is handy if you want to save and programmatically parse the output of this command.

Let's now learn more about ServerManagerCmd.exe from one of our experts at Microsoft:

### **From the Experts: Automating Common Deployment Tasks with ServerManagerCmd.exe**

Rolling out a new internal application or service within an organization frequently means setting up roles and features on multiple servers. Some of these servers might need to be set up with exactly the same configuration, and others might reside in remote locations that are not readily accessible by full-time IT staff. For these reasons, you might want to write scripts to automate the deployment process from the command line.

One of the tools that can facilitate server deployment from the command line is ServerManagerCmd.exe. This tool is the command-line counterpart to the graphical Server Manager console, which is used to install and configure server roles and features. The graphical and command-line versions of Server Manager are built on the same synchronization platform that determines what roles and features are installed and applies user-specified configurations to the server.

ServerManagerCmd.exe provides a set of command-line switches that enable you to automate many common deployment tasks as follows:

#### **View the List of Installable Roles and Features**

You can use the **-query** command to see a list of roles and features available for installation and find out what's currently installed. You can also use **-query** to look up the command-line names of roles and features. These are listed in square brackets [] after the display name.

#### **Install and Uninstall Roles and Features**

You can use the **-install** and **-remove** commands to install and uninstall roles and features. One issue to be aware of is that ServerManagerCmd.exe enables you only to install and uninstall. Apart from a few notable exceptions for required settings, you cannot specify configuration settings as you can with the graphical Server Manager console. You need to use other role-specific tools, such as MMC snap-ins and command-line utilities, to specify configuration settings after installing roles and features using ServerManagerCmd.exe.

#### **Run in "What-If" Mode**

After you create a script to set up the server with ServerManagerCmd.exe, you might want to check that the script will perform as expected. Or you might want to see what will happen if you type a specific command with ServerManagerCmd.exe. For these scenarios, you can supply the **-whatif** switch. This switch tells you exactly what would be

installed and removed by a command or answer file, based on the current server configuration, without performing the actual operations.

### **Specify Input Parameters via an Answer File**

ServerManagerCmd.exe can operate in an interactive mode, or it can be automated using an answer file. The answer file is specified using the `-inputPath <answer.xml>` switch, where `<answer.xml>` is the name of an XML file with the list of input parameters. The schema for creating answer files can be found in the ServerManagerCmd.exe documentation.

### **Redirect Output to a Results File**

It is usually a good practice to keep a history of configuration changes to your servers in case you need to troubleshoot a problem, migrate the settings of an existing server to a new server, or recover from a disaster or failure. To assist with record keeping, you can use the `resultPath <results.xml>` switch to save the results of an installation or removal to a file, where `<results.xml>` is the name of the file where you want the output to be saved.

*—Dan Harman*

*Program Manager, Windows Server, Windows Enterprise Management Division*

You'll learn more about using ServerManagerCmd.exe for adding roles and features in Chapter 5, but for now let's move on and look at more tools for managing Windows Server 2008.

## **Remote Server Administration Tools**

What if you want to manage our file server running Windows Server 2008 remotely from another machine? We already saw one way you could do this—enable Remote Desktop on the file server, and use Terminal Services to run our management tools remotely on the server. Once we have a Remote Desktop Connection session with the remote server, we can run tools such as Server Manager or File Server Resource Manager as if we were sitting at the remote machine's console.

In Windows Server 2003, you can also manage remote servers this way. But you can also manage them another way by installing the Windows Server 2003 Administration Tools Pack (Adminpak.msi) on a different Windows Server 2003 machine, or even on an admin workstation running Windows XP Service Pack 2. And once the Tools Pack is installed, you can open any of these tools, connect to your remote server, and manage roles and features on the server (provided the roles and features are installed).

Is there an Adminpak for Windows Server 2008? Well, there's an equivalent called the Remote Server Administration Tools (RSAT), which you can use to install selected management tools on your server even when the binaries for the roles/features those tools will manage are not

installed on your server. In fact, the RSAT does Adminpak one better because Adminpak installs all the administrative tools, whereas the RSAT lets you install only those tools you need. (Actually, you can just install one tool from Adminpak if you want to, though it takes a bit of work to do this—see article 314978 in the Microsoft Knowledge Base for details.)

What features or roles can you manage using the RSAT? As of Beta 3, you can install management tools for the following roles and features using the RSAT:

■ Roles

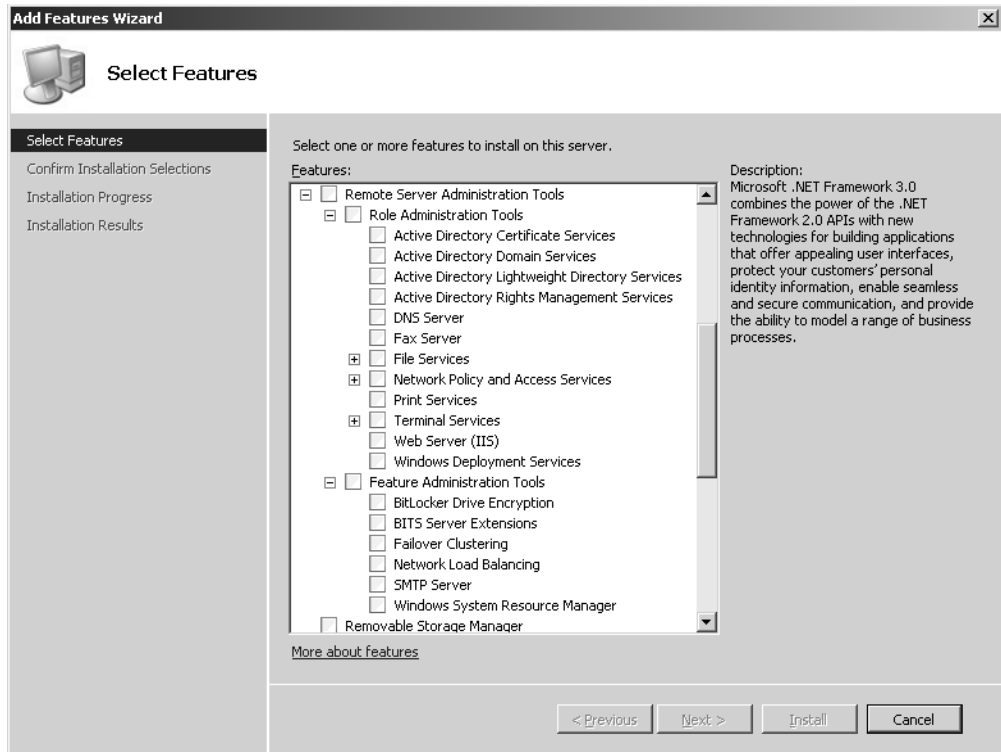
- ☐ Active Directory Domain Services
- ☐ Active Directory Certificate Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ DNS Server
- ☐ Fax Server
- ☐ File Server
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

■ Features:

- ☐ BitLocker Drive Encryption
- ☐ BITS Server Extensions
- ☐ Failover Clustering
- ☐ Network Load Balancing
- ☐ Simple SAN Management
- ☐ SMTP Server
- ☐ Windows System Resource Management (WSRM)
- ☐ WINS Server

How do you install individual management tools using the RSAT? With Windows Server 2008, it's easy—just start the Add Feature Wizard, and select the RSAT management tools you want to install, such as the Terminal Services Gateway management tool. (See Figure 4-6. Note that installing some RSAT management tools might require that you also install additional features. For example, if you choose to install the Web Server (IIS) management tool from the

RSAT, you must also install the Configuration APIs component of the Windows Process Activation Service [WPAS] feature.)



**Figure 4-6** Installing a management tool using the RSAT feature

The actual steps for installing features on Windows Server 2008 are explained in Chapter 5. For now, just note that when you install an RSAT subfeature such as TS Gateway, what this does is add a new shortcut under Administrative Tools called TS Gateway. Then if you click Start, then Administrative Tools, then TS Gateway, the TS Gateway Manager console opens. In the console, you can right-click on the root node, select Connect To TS Gateway Server, and manage a remote Windows Server 2008 terminal server with the TS Gateway role service installed on it without having to enable Remote Desktop on the terminal server.

Finally, the Windows Server 2003 Adminpak can be installed on a Windows XP SP2 workstation, which lets you administer your servers from a workstation. Can the RSAT be installed on a Windows Vista machine so that you can manage your Windows Server 2008 machines from there?

As of Beta 3, the answer is “not yet.” Plans for how RSAT will be made available for Windows Vista are uncertain at this moment, but it’s likely we can expect something that can do this around or shortly after Windows Vista Service Pack 1. We’ll just have to wait and see.

## Other Management Tools

There are other ways you can manage Windows Server 2008 besides the tools we've discussed so far. Let's examine these now. Specifically, we're going to look at the following items:

- Group Policy
- Windows Management Instrumentation (WMI)
- Windows PowerShell
- Microsoft System Center

### Group Policy

Group Policy in Windows Vista and Windows Server 2008 has been enhanced in several ways, including:

- Several new areas of policy management, including configuring Power Management settings, blocking installation of devices, assigning printers based on location, and more.
- A new format for Administrative Templates files called ADMX that is XML-based and replaces the proprietary-syntax ADM files used in previous versions of Windows.
- Network Location Awareness to enable Group Policy to better respond to changing network conditions and remove the need for relying on ICMP for policy processing.
- The ability to use local group policy objects, the capability of reducing SYSVOL bloat by placing ADMX files in a central store, and several other new features and enhancements.

A good source of information about Group Policy in Windows Vista (and therefore also in Windows Server 2008, because the platforms were designed to fit together) is Chapter 13, "Managing the Desktop Environment," in the *Windows Vista Resource Kit* from Microsoft Press. Meanwhile, while your assistant is running out to buy a couple of copies of that title (I was lead author for that title and my retirement plans are closely tied to the royalties I earn from sales, so please go buy a dozen or so copies), let's kick back and listen to one of our experts at Microsoft telling us more about post-Vista enhancements to Group Policy found in Windows Server 2008:

## **From the Experts: What's New in Group Policy in Windows Server 2008**

The following is a description of some of the Group Policy enhancements found in Windows Server 2008.

### **Server Manager Integration**

The first noticeable change in Windows Server 2008 is how the Group Policy tools are presented. In past operating systems, other than Windows Vista, an admin would have to go to the Microsoft Web site to download the Group Policy Management Console (GPMC) and install it on every administrative workstation where Group Policy management is performed. In Windows Server 2008, the installation bits are delivered with the operating system. No more downloads, no more wondering where the installation media is—it is just there.

A difference in this new environment is how optional Windows components are installed. Windows Server 2008 introduces a new management console for servers called Server Manager. This is the tool that is used to install server roles, as well as optional Windows components. If you choose to go the old-school route and add Windows components from the Add/Remove Control Panel, it will launch Server Manager.

Not only do you use Server Manager to install the optional components, but the GPMC console itself is hosted within the Server Manager console. This means all of your administrative tools are kept in one place and are easily discoverable. Of course, you will still be able to find the tools in the common locations, such as Administrative Tools.

### **Search/Filters, Comments, and Starter GPOs**

These features really enhance the administrative experience around managing and authoring policy. They are, technically, multiple features, but they work well when described as a “feature set,” as they all address the same business problem—difficulty in authoring policy. As you are probably aware, in the Windows Vista/Windows Server 2008 wave of operating systems there are hundreds of new settings to be managed. This means the total number of settings approaches 3000. That is a lot of manageable settings. Even though this provides a ton of value to the IT Professional, it increases the complexity when it comes to actually locating the setting or policy item that you are trying to manage. Microsoft has provided a “settings” spreadsheet that contains all the Group Policy settings in one relatively easy-to-use document, but it really doesn't solve the problem. Microsoft has received feedback from many IT pros that there needs to be a method within the Group Policy tool itself to make finding the right settings easier.

Now with Search and Filters, when you are authoring a policy right in the editor you have a great mechanism to locate the setting you are looking for. You will see a new Filter button in the toolbar, and if you right-click on the Administrative Templates node in the editor you will see a menu item called Filter Options. Filter Options allows you to set the

criteria that you are looking to search on. For example, you can narrow your view to only *configured* items, specific key words, or the system requirements (for example, Internet Explorer 6.0 settings). Filter Options provides a very intuitive interface and has great flexibility to help in locating the settings that you are looking for. Once you set Filter Options and turn on the Filter (global setting), the editor displays only settings that you are targeting. The Group Policy team is really excited to bring these features to you because we know it will reduce some of the administrative burden of what is otherwise a fantastic management technology.

You can also filter for settings that have Comments. This is also a new feature introduced in Windows Server 2008. You can now place a comment on any setting that you want. This means when admins are authoring policy, they can document their intentions at author time and other administrators can use that Comment as a search criteria. This feature is incredible at helping Group Policy administrators communicate to themselves, or other administrators, why specific settings are being managed and what the impact of those settings is.

The last piece of this feature set is called Starter GPOs. Starter GPOs are a starting point for administration. When a GPO is created, you can still create a blank GPO, or you can choose to create your GPO from one of the pre-existing Starter GPOs. Starter GPOs are a collection of preconfigured Administrative Template settings, complete with comments. You will see a node in the Group Policy Management Console (GPMC) called Starter GPOs. Simply right-click on this node and choose New. You will have a Starter GPO that is available to edit. There is delegation available on the Starter GPO container to ensure that only specific administrators can modify it..

This feature set—Search/Filters, Comments, and Starter GPOs—comes together to greatly enhance the authoring and management experience around Group Policy. It provides ease of authoring and discovering settings, inline documentation of Group Policy settings, and baseline configurations for starting the process.

### **ADMX/ADML**

ADMX/ADML files were introduced in Windows Vista to replace the legacy data format of the ADM files that we have become used to. ADMX files are XML files that contain the same type of information that we have become familiar with to build the administrative experience around Administrative Template settings. Using XML makes the whole process more efficient and standardized. ADML files are language-specific files that are critical in a multilanguage enterprise. In the past, all localization was done right within each ADM file. This caused some confusing version control issues when multiple administrators were managing settings in a GPO from workstations using different languages. With ADMX/ADML, all administrators work off of the same GPOs and simply call the appropriate ADML file to populate the editor.

Another value associated with ADML/ADMX files is that GPOs no longer contain the ADM files themselves. Prior to Windows Vista/Windows Server 2008, each GPO created

would contain all the ADM files. This was about 4 MB by default. This was a contributing factor in SYSVOL bloat.

Take a look at <http://www.microsoft.com/GroupPolicy> to read more on ADMX/ADML. You can also find the ADMX migration utility to help in moving to this new environment at <http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.aspx>. Just a note that ADM and ADMX can coexist; read up on it on one of the sites just referenced.

### Central Store

Related to ADMX files is the Central Store. As was previously stated, ADM files used to be stored in the GPO itself. That is no longer the case. Now the GPO contains only the data that the client needs for processing Group Policy. In Windows Vista/Windows Server 2008, the default behavior for editing is that the editor pulls the ADMX files from the local workstation. This is great for smaller environments with few administrators managing Group Policy, but in larger, more complex environments or environments that need a bit more control, a Central Store has been introduced. The Central Store provides a single instance in SYSVOL that holds all of the ADMX/ADML files that are required. Once the Central Store is set up, all administrators load the appropriate files from the Central Store instead of the local machine. Check out one of the Group Policy MVP's Central Store Creation Utility at <http://www.gpoguy.com/cssu.htm>. You can also find more information on the Central Store at <http://www.microsoft.com/grouppolicy>.

### Summary

Windows Server 2008 and Windows Vista have introduced a lot of new functionality for Group Policy. Administrators will find that these new features for management, along with the around 700 new settings to manage, will increase the ease of use of Group Policy and expand the number of areas that can be managed with policy.

—Kevin Sullivan

*Lead Program Manager for Group Policy, Windows Enterprise Management Division*

Pretty cool enhancements, eh? Sorry, that's the Canadian coming out of me, or through me, or channeling through me—whatever.

## Windows Management Instrumentation

WMI is a core Windows management technology that administrators can use to write scripts to perform administrative tasks on both local and remote computers. There are no specific enhancements to WMI in Windows Server 2008 beyond those included in Windows Vista,



but it's important to know about the Windows Vista enhancements since these apply to Windows Server 2008 also. Here are a few of the more significant changes to WMI in Windows Vista and Windows Server 2008:

- **Improved tracing and logging** The WMI service now uses Event Tracing for Windows (ETW) instead of the legacy WMI log files used on previous Windows platforms, and this makes WMI events available through Event Viewer or by using the Wevtutil.exe command-line tool.
- **Enhanced WMI namespace security** The NamespaceSecuritySDDL qualifier can now be used to secure any namespace by setting WMI namespace security in the Managed Object Format (MOF) file
- **WMI namespace security auditing** WMI now uses the namespaces system access control lists (SACL) to audit namespace activity and report events to the Security event log.
- **Get and Set security descriptor methods for securable objects** new scriptable methods to get and set security descriptors have been added to Win32\_Printer, Win32\_Service, StdRegProv, Win32\_DCOMApplicationSetting, and \_\_SystemSecurity.
- **Manipulate security descriptors using scripts** The Win32\_SecurityDescriptorHelper class now has methods that allow scripts to convert binary security descriptors on securable objects into Win32\_SecurityDescriptor objects or Security Descriptor Definition Language (SDDL) strings.
- **User Account Control** User Account Control (UAC) affects what WMI data is returned, how WMI is remotely accessed, and how scripts must be run.

What all this basically means is that WMI is more secure and more consistent in how it works in Windows Server 2008, which is good news for administrators who like to write WMI scripts to manage various aspects of their Windows-based networks.

Still, from personal experience, I know that writing WMI scripts isn't always easy, especially if you're trying to get them to run properly against remote machines. Windows Vista and Windows Server 2008 complicate things in this regard because of their numerous security improvements, including User Account Control (UAC). So it's instructive if we sit back and listen now to one of our experts at Microsoft, who will address this very issue in detail (this sidebar is worth its weight in gold):

### **From the Experts: WMI Remote Connection**

Talking about management obviously implies the need to connect remotely to the Windows systems you want to manage. Speaking about remote connection immediately implies security. Management and security are not always easy to combine. It is not rare to see situations where management represents a breach of security, or the other way around; it is not rare either to see security settings preventing the proper management of

a system. In this respect, WMI is not different from any other technologies; it provides remote management capabilities involving some security considerations.

Windows Vista and Windows Server 2008 come with a series of new security features. The most important one is called User Account Control (UAC). It is very likely that every administrator in the world will be challenged by the presence of UAC, especially if you use the Local Accounts part of the Administrator group to perform remote access. This is because any token account used in this context is automatically filtered and finally acts as a normal user in the remote system. Therefore, it is wise to consider the various security aspects to properly and securely manage your remote systems.

Before looking at the UAC aspects, let step back and look at the requirements to call WMI remotely. This applies to any Windows platform since Windows 2000. We will examine the Windows Vista and Windows Server 2008 aspects next.

To connect remotely, four conditions must be met:

1. **Firewall** Introduced with Windows XP, the Windows Firewall must be properly set up to enable connectivity for the WMI RPC traffic. Usually, you get an “RPC connection failure” if the Windows Firewall is enabled and RPC is disallowed. If you get an “access denied” message, the firewall is not the root cause of the issue. Keep in mind that the firewall is the key component to go through before anything else happens. Before Windows Vista and Windows Server 2008, RPC traffic must be enabled to allow the WMI traffic to go through. With Windows Vista and Windows Server 2008, a dedicated set of Firewall WMI rules is available to enable only WMI traffic. (This can be done with the FW.MSC MMC snap-in, Group Policies, Scripting, or NETSH.EXE.) Note that if you use WMIDiag (available on Microsoft Download Center), it will tell you which NETSH.EXE command to use to configure your firewall properly.
2. **DCOM** Once the firewall gate is passed, it is time to consider the DCOM security. The user issuing the remote call must have the right to “Launch and Activate” (which can be viewed and changed with DCOMCNFG.EXE) for both the My Computer and Windows Management and Instrumentation objects. By default, only users who are part of the Administrators group of the remote machine have the right to remotely “Launch and Activate” these DCOM objects.
3. **WMI namespace** Once the DCOM security is verified, WMI namespace security comes next. In this case, the user connecting to a remote WMI namespace must have at the minimum the Enable Remote and Enable Account rights granted for the given namespace. By default, only users who are part of the Administrators group of the remote machine have the Enable Remote right granted. (This can be updated with WMIMGMT.MSC.)

4. **Manageable entity** Last but not least, once WMI has accepted the remote request, it is actually executed against the manageable entity (which could be a Windows Service or a Terminal Server configuration setting, for instance). This last step must also succeed for the WMI operation to succeed. WMI does not add any privilege that the user does not have when issuing the WMI request. (By default, WMI impersonates the calls, which means it issues the call within the security context of the remote user.) So, depending on the WMI operation requested and the rights granted to the remote user, the call might succeed or fail at the level of the manageable entity. For instance, if you try to stop a Windows service remotely, the Service Control Manager requires the user to be an Administrator by default. If you are not, the WMI request performing this operation will fail.

This describes the behavior of WMI since Windows 2000. In the light of Windows Vista and Windows Server 2008, things can be slightly different because UAC is enabled by default on both platforms and everything depends on whether you use a local account or a domain account. If you use a local user of the remote machine who is a member of the Local Administrators group, the Administrators membership of the user is always filtered. In this context, DCOM, WMI, and the manageable entity are applying the security restrictions with respect to the filtered token presented. Therefore, with respect to the UAC behavior, the token is a user token, not an administrative token! As a consequence, the Local User is actually acting as a plain user on that remote machine even if it is part of the Local Administrators group. By default, a user does not have the rights to pass the security gates defined earlier (in step 2, 3, and 4).

Now that the scene is set, how do you manage a remote Windows Vista machine or 2008 server while respecting the Firewall, UAC, DCOM, WMI, and manageable entity security enforcements?

This challenge must be looked at in two different ways:

1. **The remote machine is part of a domain.** If the remote machine is part of a domain, it is highly recommended that you use a Domain User part of the Local Administrators group of the remote machine (and *not* a Local User part of the Local Administrators group). By doing so, you will be a plain Administrator because UAC does *not* filter users out of the Local Administrators group when the user is a Domain User. UAC only filters Local Users out of the Local Administrators group.
2. **Your machine is a workgroup machine.** If your machine is in a workgroup environment, you are forced to use a Local User part of the Local Administrators group to connect remotely. Obviously, because of the UAC behavior, that user is filtered and acts as a plain user. The first approach if you are in a large enterprise infrastructure is to consider the possibility of making this machine part of a domain to use a

Domain User. If this is not possible because you must keep the machine as part of a workgroup, from this point you have two choices:

- ❑ You decide to keep UAC active. In this case, you must adjust the security settings of DCOM and WMI to ensure that the Local User has the explicit rights to get remote access. Don't forget that a best practice is to use a dedicated Local Group and make this Local User a member of that group. In this context, the WMI requests against the manageable entity might work or not depending on the manageable entity security requirements (discussed in step 3). If the manageable entity does not allow a plain user to perform the task requested, you might be forced to change the security at the manageable entity level to explicitly grant permissions to your Local User or Group as well. Note that this is not always possible because it heavily depends on the manageable entity security requirements and security management capabilities of the manageable entity. For the Windows Services example, this can be done with the SC.EXE command via an SDDL string, the *Win32\_Service* WMI class (with the *Get/SetSecurityDescriptor* methods implemented in Windows Vista and Windows Server 2008), or Group Policies (GPEDIT.MSC). By updating the security at these three levels, you will be able to gracefully pass the DCOM and WMI security gates and stop a Windows Service as a plain user. Note that this customization represents clearly the steps for a granular delegation of the management. Only the service you changed the security for can be stopped by that dedicated user (or group). In this case, you actually define a very granular security model for a specific task. (You can watch the "Running Scripts Securely While Handling Passwords and Security Contexts Properly" webcast at <http://go.microsoft.com/fwlink/?LinkId=39643> to understand this scenario better.) Now it is possible that some manageable entities only require the user to be an Admin (typical for most devices) because there is no possibility to update the security descriptor. In such a case, for a workgroup scenario, only the second option (discussed next) becomes possible. Last but not least, keep in mind that these steps are also applicable in a domain environment to delegate some management capabilities to a group of domain users.
- ❑ You decide to disable the UAC filtering for remote access. This must be the last-resort solution. It is not an option you should consider right away if you want to maintain your workgroup system with a high level of security. So consider it only after investigating the possibility of making your system part of a domain or after reviewing the security wherever needed. If making your system part of a domain is not possible, you can consider this option. In this case, you must set the registry key in the reference shown below to ZERO on

the remote system. Note that you must be an administrator to change that registry key. So you need to do this locally once, before any remote access is made. Note that this configuration setting disables the filtering on Local Accounts only; it does not disable UAC as a whole.

```
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]"LocalAccountTokenFilterPolicy"=dword:00000001
```

Once set, the registry key is created and set to ONE, and the Local User remotely accessing the machine will be an administrator (if the user is a member of the Local Administrators group). Therefore, by default, the user will pass the security gates defined in steps 2, 3, and 4. Note that it is required to reboot the machine to get this change activated.

—Alain Lissoir

Senior Program Manager, Windows Enterprise Management Division (WEMD)

Check out Alain's Web site at <http://www.lissware.net>.

## Windows PowerShell

Another powerful tool for automating administrative tasks in Windows Server 2008 is Windows PowerShell, a command-line shell and scripting language. PowerShell includes more than 130 command-line tools (called *cmdlets*), has consistent syntax and naming conventions, and uses simplified navigation for managing data such as the registry and certificate store. PowerShell also includes an intuitive scripting language specifically designed for IT administration. As of Beta 3, PowerShell is included as an optional feature you can install on Windows Server 2008.

PowerShell can be used to efficiently perform Windows Server 2008 administration tasks, including managing services, processes, and storage. PowerShell can also be used to manage aspects of server roles, such as Internet Information Services (IIS) 7.0, Terminal Services, and Active Directory Domain Services. Some of the things you can do with PowerShell on Windows Server 2008 include

- Managing command-line services, processes, the registry, and WMI data using the *get-service*, *get-process*, and *get-wmiobject* cmdlets.
- Automating Terminal Services configuration, and comparing configurations across a Terminal Server farm.
- Deploying and configuring Internet Information Services 7.0 across a Web farm.
- Creating objects in Active Directory, and listing information about the current domain.

For example, let's look at the third item in this list—managing IIS 7.0 using PowerShell. But rather than have me explain this, why don't we listen to one of our experts at Microsoft concerning this?

### From the Experts: PowerShell Rocks!

Of all the new Microsoft technology coming down the pipe, PowerShell has got to be one of the most exciting (after IIS 7.0 of course). You might wonder why I am so excited about the new scripting shell for Windows. Even if PowerShell is better than Command Prompt on steroids, what does this have to do with my main passion, Web servers and Web applications? Check out the Channel9 video I did with Jeffrey Snover, architect of PowerShell, to get an idea of how cool PowerShell really is (see <http://channel9.msdn.com/Showpost.aspx?postid=256994>). In the video, we show off a demo we put together for Bob Muglia's keynote article in TechEd IT Forum this week, which appears to have gone very, very well. Well done, Jeffrey.

A long, long, long time ago, when I was in school and even after that, before I came to Microsoft and joined the IIS team, I used Linux and spent my days in BASH and ZSH getting work done. Until now, we sadly never really had the productive power of an interactive shell on Windows. So as a previously heavy user of shells, I have to tell you what I really like about this new shell interface on its own, and then I'll explain the many ways PowerShell can make work simpler for IIS administrators.

OK, first off, in PowerShell you input commands on objects, not text, and PowerShell returns objects and not text. So you can easily pipe commands together in one line. This allows me to input in just one line complicated commands like this one:

```
PS C:\Windows\System32> Get-ChildItem -Path G:\ -Recurse -Include  
*.mp3 | Where-Object -FilterScript {($_.LastWriteTime -gt  
"2006-10-01") -and ($_.Name -match "pearl jam")} | Copy  
-Destination C:\User\bill\l\Desktop\New_PJ_MP3s
```

which recursively looks through my entire external hard drive (G:), collects all the "Pearl Jam" mp3s that were recently added, and copies them into a folder on my desktop. Never was I given a text output listing all the mp3s, and I didn't have to use the Copy command over and over. I just piped all the items to Copy once.

Another thing I like so much about PowerShell is how consistent PowerShell commands are. In the preceding example, I used only one Get-ChildItem command, but rest assured if I wanted to get anything else, the command for that would start with Get. Similarly, if we want to stop a process or an application or anything, we always use the Stop command, not kill, not terminate, not halt, just stop.

Finally, I love that PowerShell is extensible. I love this because it means my team can produce a whole set of IIS PowerShell cmdlets to help you manage IIS 6.0, IIS 7.0, and future versions of IIS. You will also be able to submit your IIS PowerShell scriptlets to this community area (coming very soon).

Now that I've listed my favorite things about this new shell, I'd like to give you a few ways that PowerShell can and will make IIS administration simpler than ever before. The top 5...

1. IIS 7.0 has a new WMI Provider for quickly starting, stopping, creating, removing, and configuring sites and applications. Now use PowerShell to give a list of applications sorted by a particular configuration setting. Then pipe apps with the particular setting into the tasks you were performing before with the WMI Provider. My colleague Sergei Antonov wrote and just published a fantastic article, titled "Writing PowerShell Command-lets for IIS 7.0," that describes how to write PowerShell cmdlets using our WMI provider.
2. Because IIS 7.0 has a distributed file-based configuration store, you can store your application's IIS configurations in a *web.config* file in the application's directory next to its code and content. Use PowerShell to rapidly XCopy deploy the application to an entire Web farm in one step.
3. IIS 7.0's new Web.Administration API allows admins to write short programs in .NET to programmatically tackle frequent IIS 7.0 management tasks. Then, because PowerShell completely supports the .NET Framework, use it to pipe IIS objects in and out of these handy bits of code.
4. With IIS 7.0, you can use the new Runtime Status and Control API to monitor the performance of your Web applications. Use PowerShell to monitor performance information at a regular interval of every five minutes, and then have this valuable runtime information displayed to the console or sent to a log file whenever CPU is above 80%.
5. Take advantage of IIS 7.0's extensibility by writing your own custom request processing module with its own configuration and IIS Manager plug-in. Then write a PowerShell cmdlet to serve as a management interface to expose your custom IIS configuration to the command line and to power your IIS Manager plug-in.

For more information on managing IIS 7.0 using PowerShell, see "An Introduction to Windows PowerShell and IIS 7.0," found at <http://www.iis.net/default.aspx?tabid=2&subtabid=25&i=1212>.

—Bill Staples

*Product Unit Manager, IIS*

Like WMI discussed earlier, Windows PowerShell is a work in progress and is still evolving. For example, Windows PowerShell version 1.0 doesn't yet have any cmdlets for managing Active Directory, but by using the .NET Framework 2.0 together with PowerShell, you can manage Active Directory even so.

Chapter 14, "Additional Resources," has lots of pointers to where you can find more information about using PowerShell to manage Windows Server 2008. But before you flip ahead to look there, listen to what another expert at Microsoft has to say concerning the *raison d'être* behind PowerShell:

### **From the Experts: The Soul of Automation**

*"Civilization advances by extending the number of important operations which we can perform without thinking about them."*

Alfred North Whitehead, "Introduction to Mathematics" (1911)  
English mathematician & philosopher (1861 - 1947)

I really understood Whitehead's point during the great windstorm of 2006 when we lost power in my area for six days. During this time, we were without the benefits of most of the things I took for granted. I was struck by how much time it took to do things that previously I performed without thinking about them. Washing the dishes in the sink by hand took a lot more time than using the dishwasher. There were dozens of things like this. I didn't mind terribly, but I found myself resenting that I didn't have time to do as much reading as I usually do.

Whitehead's point is *not* that civilization advances by us becoming non-thinking idiots. Rather, by increasing the number of things that we don't have to think about, we free up time to think about *new* things and solve *new* problems, and then transform those things into things that we no longer have to think about. And so on and so on. Because I spent time doing dishes means that I didn't have time to read, which meant that I didn't get more educated, which would have made it easier to move the ball forward.

This is the essence of PowerShell and the soul of automation. In our world, there is no end of interesting and hard problems to think about, and the degree that our tools continue to make us think about the low-level junk is the degree to which we reduce the time that we have to think about the interesting problems. The ball gets moved forward as we adopt better and better tools that do what we want them to do without us having to tell them, and by our getting in the habit of using automation for repeating operations and sharing that automation with others.

Huge advances come from the accumulation of small deltas. In *David Copperfield*, Charles Dickens wrote, "Annual income twenty pounds, annual expenditure nineteen pounds six, result happiness. Annual income twenty pounds, annual expenditure twenty ought and size, result misery." Einstein said it this way, "The most powerful force in the universe is compound interest." So the next time you find yourself thinking about



how to do something that you've done before, you should take it as an opportunity to invest a little bit and automate the activity so that you don't have to think about it again. Give the function a good long name so that you can remember it, find it, and recognize it when you see it; then give it an alias so that you can minimize your typing (for example, `Get-FileVersionInfo` and `gfvi`).

Last but not least, SHARE. Put your script out on a blog or newsgroup or Web site so that others can benefit from your thinking. Newton might have figured out gravity, but if he didn't share his thoughts with others, he would not have moved the ball forward. OK, so your script is not in the same league as " $F=ma$ ," but share it anyway because "huge advances come from the accumulation of small deltas."

Enjoy!

—Jeffrey Snover

*Partner Architect, Windows Management*

## Microsoft System Center

Finally, the Microsoft System Center family of enterprise management solutions will be supporting management of Windows Server 2008, though at the time of this writing, the date for such support has not been made known to me. System Center is a collection of products that evolved from the earlier Microsoft Systems Management Server (SMS) and Microsoft Operations Manager (MOM) platforms. The plan for the System Center family currently includes the following products:

- System Center Operations Manager (the next generation of MOM)
- System Center Configuration Manager (the next generation of SMS)
- System Center Data Protection Manager
- System Center Essentials
- System Center Virtual Machine Manager
- System Center Capacity Planner

Keep your eye on these products as Microsoft announces its support for Windows Server 2008. You can find out more about System Center at <http://www.microsoft.com/systemcenter>.

## Conclusion

Windows Server 2008 can be managed using a number of in-box and out-of-band tools. If you only need to manage a single server, use Initial Configuration Tasks and Server Manager. If you need to do this remotely, enable Remote Desktop on your server. If you need to manage multiple servers roles on different machines, install the Remote Server Administration Tools (RSAT) and use each tool to manage multiple instances of a particular role. And if you need to automate the administration of Windows Server 2008 machines, use ServerManagerCmd.exe, WMI, Windows PowerShell, or some combination of the three.

## Additional Resources

TechNet has a level 300 webcast called “Installing, Configuring, and Managing Server Roles in Windows Server 2008” that you can download from <http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032294712&EventCategory=5&culture=en-US&CountryCode=US> (registration required).

If you have access to the Windows Server 2008 beta on Microsoft Connect (<https://connect.microsoft.com/>), you can download the following items:

- Microsoft Windows Server 2008 Server Manager Lab Companion
- Microsoft Windows Server 2008 Initial Configuration Tasks Step-By-Step Guide
- Live Meeting on Server Manager

If you don't have access to beta builds of Windows Server 2008, you can still test drive Server Manager online using the Microsoft Windows Server 2008 Server Manager Virtual Lab, available at <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032314461&EventCategory=3&culture=en-IN&CountryCode=IN>.

A good starting point for exploring the potential of using Windows PowerShell to manage Windows Server 2008 is <http://www.microsoft.com/windowsserver/2008/powershell.msp>.

Information about Group Policy enhancements in Windows Vista and Windows Server 2008 can be found at <http://technet2.microsoft.com/WindowsVista/en/library/a8366c42-6373-48cd-9d11-2510580e48171033.msp?mfr=true>.

More information about WMI enhancements in Windows Vista and Windows Server 2008 can be found on MSDN at <http://msdn2.microsoft.com/en-gb/library/aa394053.aspx>.

And if you want to find out more about Microsoft System Center, see <http://www.microsoft.com/systemcenter/>.

Finally, be sure to turn to Chapter 14 for more information on the topics in this chapter and also for webcasts, whitepapers, blogs, newsgroups, and other sources of information about all aspects of Windows Server 2008.