Windows Server 2008
Server Core

Mitch Tulloch, MVP
with the Windows Server Core Team at Microsoft

Administrator's Pocket Consultant
Contents at a Glance

1  Examining Server Core ................................................. 1
2  Deploying Server Core ............................................. 17
3  Initial Configuration .................................................. 47
4  Installing Roles and Features ..................................... 77
5  Local Management ...................................................... 95
6  Remote Management ................................................... 117
7  Active Directory Domain Services Role ....................... 143
8  DHCP Server Role ....................................................... 189
9  DNS Server Role ......................................................... 213
10 File and Print Services Roles ..................................... 245
11 Web Server Role ......................................................... 295
12 Hyper-V and Other Roles .......................................... 321
13 Maintaining Server Core ............................................ 357
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 survey, please visit:

www.microsoft.com/learning/booksurvey
Table of Contents

Deploying Server Core Using the Windows AIK .......................... 21
Types of Unattended Installs ............................................. 21
Installing the Windows AIK .................................................. 22
Creating a Basic Answer File for Unattended Installs ............... 23
Performing an Unattended Install from a DVD ....................... 31
Performing an Install from a Configuration Set ....................... 32
Performing an Install from Image ....................................... 37
Deploying Server Core Using Windows Deployment Services 40
Deploying Server Core Using Microsoft Deployment ....... 44

3 Initial Configuration ......................................................... 47
Methods for Performing Initial Configuration ....................... 47
Setting the Local Administrator Password .......................... 47
Managing Local Users and Groups ..................................... 49
Changing the Computer Name ........................................... 51
Configuring TCP/IP Networking Settings ............................. 53
Configuring Date and Time Settings ................................... 58
Configuring Regional and Language Settings ........................ 59
Configuring Automatic Updates ......................................... 60
Configuring Windows Error Reporting ................................. 62
Participating in the Customer Experience Improvement Program . 64
Activating Windows .......................................................... 65
Enabling Remote Desktop .................................................. 67
Enabling Remote Administration of Windows Firewall ............ 69
Joining a Domain ............................................................. 71
Other Initial Configuration Tasks ......................................... 72

4 Installing Roles and Features ............................................. 77
Understanding Roles and Features ....................................... 77
Tools for Installing Roles and Features ................................ 78
Understanding Packages .................................................... 79
Understanding Package Names .......................................... 80
Understanding Package Dependencies ................................ 82
Enumerating Installed Roles and Features ............................. 83
Enumerating Installed Roles and Features Using Oclist .......... 84
Using Find to Simplify the Output of Oclist ......................... 84
Enumerating Installed Roles and Features Using WMI ............. 85
## Table of Contents

- Installing and Uninstalling Roles and Features Using Ocsetup ............... 86
- Installing a Role or Feature Using Ocsetup ........................................ 86
- Installing the DHCP Server Role ......................................................... 86
- Verifying Installation of the Role ......................................................... 86
- Uninstalling the DHCP Server Role ...................................................... 86
- Installing the Web Server (IIS) Role ...................................................... 87
- Adding HTTP Logging to the Web Server (IIS) Role ................................. 87
- Installing Roles and Features That Have Dependencies ......................... 87
- Removing Roles and Features That Have Dependencies .......................... 88
- Installing Multiple Roles and Features Using Ocsetup with an Answer File ........................................................................ 88
- Unattended Installation of Roles and Features ........................................ 89
- Sysprep Support for Server Roles ........................................................... 92
- Permanently Removing Unneeded Roles and Features ............................ 93

### 5 Local Management ........................................................................... 95

- Using the Command Prompt ................................................................. 95
- Starting the Command Prompt ............................................................... 95
- Customizing the Command Prompt ....................................................... 100
- Running Multiple Commands ............................................................... 103
- Command Redirection ........................................................................... 103
- Working with Environment Variables .................................................. 104
- Commands for Common Tasks ............................................................ 107

- Using Scripts ......................................................................................... 110
  - WMI Support in Server Core ............................................................... 111
  - Using WMIC ...................................................................................... 116

### 6 Remote Management ......................................................................... 117

- Using Remote Desktop ........................................................................... 117
  - Enabling Remote Desktop Using Scregedit.wsf .................................. 117
  - Enabling Remote Desktop Using an Answer File .................................. 118
  - Using Scregedit.wsf to Require Network Level Authentication for Remote Desktop .......................................................... 119
  - Using an Answer File to Require Network Level Authentication for Remote Desktop .......................................................... 119
  - Using Remote Desktop to Administer Server Core ............................... 120
  - Using TS Remote App for Publishing Cmd to Administer Server Core .......................................................... 122
  - Managing Terminal Services on Server Core ...................................... 124
Table of Contents

Using WinRS ................................................................. 125
Configuring WinRM on Server Core ................................. 125
Using WinRS to Administer Server Core in a Domain .......... 126
Using WinRS to Administer Server Core in a Workgroup .... 126
Requirements for Using WinRS ........................................ 127
Configuring WinRM and WinRS Using Group Policy .......... 128

Using MMC Snap-ins and RSAT .......................... 128
Using MMC Consoles to Administer Server Core
in a Domain ................................................................. 128
Using MMC Snap-ins to Administer Server Core
in a Workgroup .......................................................... 132
Using RSAT to Administer Server Core in a Domain ....... 133
Installing RSAT on a Full Installation of Windows
Server 2008 ................................................................. 134
Installing RSAT on Windows Vista SP1 ....................... 134
Using RSAT to Administer Server Core Remotely
in a Domain ................................................................. 135
Using RSAT to Administer Server Core Remotely
in a Workgroup .......................................................... 136

Using Other GUI Tools .................................................. 136
Using Windows Explorer Remotely ....................... 137
Using Task Scheduler Remotely .................................. 137
Using Registry Editor Remotely .................................. 138

Using Group Policy ...................................................... 138
Group Policy Tools on Server Core ....................... 138
Using WMI Filters to Administer Server Core with
Group Policy .............................................................. 138
Managing Local Group Policy on Server Core .............. 140

Using Windows PowerShell ............................................ 141

7 Active Directory Domain Services Role .................. 143
Installing AD DS on Server Core ......................... 143
Creating a New Forest Using Unattended Dcpromo ...... 144
Creating a New Domain Tree Using Unattended Dcpromo . 158
Creating a New Child Domain Using Unattended
Dcpromo ................................................................. 159
Installing a Replica Domain Controller into an
Existing Domain Using Unattended Dcpromo ............. 160
Removing a Domain Controller Using Unattended
Dcpromo ................................................................. 165
Preparing an Existing Active Directory Environment
for Windows Server 2008 Domain Controllers ............ 169
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Table of Contents</strong></td>
<td>ix</td>
</tr>
<tr>
<td></td>
<td>Managing Server Core Domain Controllers</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>Managing Server Core Domain Controllers Using MMC Consoles</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>Managing Server Core Domain Controllers Using Command-Line Utilities</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>Performing Common Active Directory Management Tasks</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td>Working with Server Core Read-Only Domain Controllers</td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>Additional Limitations of RODCs</td>
<td>183</td>
</tr>
<tr>
<td></td>
<td>Preparing a Forest for RODCs</td>
<td>184</td>
</tr>
<tr>
<td></td>
<td>Installing an RODC on Server Core</td>
<td>185</td>
</tr>
<tr>
<td></td>
<td>Configuring the Password Replication Policy for an RODC</td>
<td>186</td>
</tr>
<tr>
<td>8</td>
<td><strong>DHCP Server Role</strong></td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Installing the DHCP Server Role on Server Core</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Installing the DHCP Server Role from the Command Prompt</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Installing the DHCP Server Role Using an Answer File</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Starting the DHCP Server Service</td>
<td>190</td>
</tr>
<tr>
<td></td>
<td>Removing the DHCP Server Role</td>
<td>191</td>
</tr>
<tr>
<td></td>
<td>Managing a Server Core DHCP Server</td>
<td>192</td>
</tr>
<tr>
<td></td>
<td>Managing DHCP Servers</td>
<td>192</td>
</tr>
<tr>
<td></td>
<td>Viewing and Modifying DHCP Server Configuration</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>Creating and Managing Scopes</td>
<td>199</td>
</tr>
<tr>
<td></td>
<td>Maintaining DHCP Servers</td>
<td>207</td>
</tr>
<tr>
<td>9</td>
<td><strong>DNS Server Role</strong></td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>Installing the DNS Server Role on Server Core</td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>Installing the DNS Server Role on a Domain Controller</td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>Installing the DNS Server Role from the Command Prompt</td>
<td>216</td>
</tr>
<tr>
<td></td>
<td>Installing the DNS Server Role Using an Answer File</td>
<td>217</td>
</tr>
<tr>
<td></td>
<td>Removing the DNS Server Role</td>
<td>218</td>
</tr>
<tr>
<td></td>
<td>Managing a Server Core DNS Server</td>
<td>218</td>
</tr>
<tr>
<td></td>
<td>Managing DNS Servers</td>
<td>218</td>
</tr>
<tr>
<td></td>
<td>Configuring DNS Servers</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>Creating and Managing Zones</td>
<td>222</td>
</tr>
<tr>
<td></td>
<td>Creating and Managing Resource Records</td>
<td>227</td>
</tr>
<tr>
<td></td>
<td>Performing Other DNS Management Tasks</td>
<td>234</td>
</tr>
<tr>
<td></td>
<td>Maintaining DNS Servers</td>
<td>240</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>10</td>
<td>File and Print Services Roles</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Installing and Managing the File Services Role on Server Core</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Installing File Services Role Services from the Command Line</td>
<td>245</td>
</tr>
<tr>
<td></td>
<td>Installing File Services Role Services Using an Answer File</td>
<td>246</td>
</tr>
<tr>
<td></td>
<td>Managing Disks and File Systems</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Managing Shared Folders</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td>Implementing DFS</td>
<td>272</td>
</tr>
<tr>
<td></td>
<td>Installing and Managing the Print Services Role on Server Core</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>Managing Server Core Print Servers Using Print Management</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>Managing Server Core Print Servers from the Command Line</td>
<td>284</td>
</tr>
<tr>
<td>11</td>
<td>Web Server Role</td>
<td>295</td>
</tr>
<tr>
<td></td>
<td>Understanding the Web Server Role</td>
<td>295</td>
</tr>
<tr>
<td></td>
<td>Understanding IIS 7.0 Components and Their Dependencies</td>
<td>295</td>
</tr>
<tr>
<td></td>
<td>Understanding the Limitations of IIS 7.0 on Server Core</td>
<td>303</td>
</tr>
<tr>
<td></td>
<td>Installing the Web Server Role</td>
<td>303</td>
</tr>
<tr>
<td></td>
<td>Installing a Default Web Server</td>
<td>304</td>
</tr>
<tr>
<td></td>
<td>Installing a Classic ASP Web Server</td>
<td>305</td>
</tr>
<tr>
<td></td>
<td>Installing All IIS 7.0 Components</td>
<td>306</td>
</tr>
<tr>
<td></td>
<td>Installing PHP on Server Core</td>
<td>306</td>
</tr>
<tr>
<td></td>
<td>Installing the Web Server Role Using an Answer File</td>
<td>307</td>
</tr>
<tr>
<td></td>
<td>Managing the Web Server Role</td>
<td>308</td>
</tr>
<tr>
<td></td>
<td>Using Appcmd.exe</td>
<td>308</td>
</tr>
<tr>
<td></td>
<td>Common Management Tasks</td>
<td>310</td>
</tr>
<tr>
<td>12</td>
<td>Hyper-V and Other Roles</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>Installing and Managing the Hyper-V Role on Server Core</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>Hyper-V Terminology</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>Installing the Hyper-V Role</td>
<td>324</td>
</tr>
<tr>
<td></td>
<td>Managing the Hyper-V Role</td>
<td>327</td>
</tr>
<tr>
<td></td>
<td>Installing and Managing the AD LDS Role on Server Core</td>
<td>348</td>
</tr>
<tr>
<td></td>
<td>Installing the AD LDS Role</td>
<td>349</td>
</tr>
<tr>
<td></td>
<td>Managing the AD LDS Role</td>
<td>349</td>
</tr>
</tbody>
</table>
# Table of Contents

## Installing and Managing the Streaming Media Services Role on Server Core
- Installing the Streaming Media Services Role ................................................. 353
- Managing the Streaming Media Services Role .............................................. 354

## Maintaining Server Core ................................................................. 357
- Managing Services .................................................................................. 357
  - Managing Services from the Command Line ........................................... 357
  - Managing Services Using the Services Snap-in ....................................... 363
- Managing Devices and Device Drivers ....................................................... 364
  - Managing Devices from the Command Line ............................................ 364
  - Managing Devices Using the Device Manager Snap-in ............................ 369
- Managing Processes .................................................................................. 371
  - Displaying Processes and Process Details .............................................. 372
  - Stopping a Process .............................................................................. 374
  - Starting a Process ............................................................................... 376
- Managing Scheduled Tasks ....................................................................... 376
  - Managing Scheduled Tasks from the Command Line ............................... 376
  - Managing Scheduled Tasks Using the Task Scheduler Snap-in .................... 380
- Event Logging .......................................................................................... 382
  - Viewing Events from the Command Line .............................................. 383
  - Viewing Events Using Event Viewer ..................................................... 390
  - Configuring Event Subscriptions ............................................................ 391
- Performance Monitoring .......................................................................... 397
  - Collecting and Analyzing Performance Data Using the Reliability and Performance Monitor 397
  - Collecting and Analyzing Performance Data from the Command Line .......... 398
- Backup and Recovery ............................................................................... 403
  - Installing the Windows Server Backup Feature ....................................... 404
  - Performing Backup and Recovery Using the Windows Server Backup Snap-in ... 405
  - Performing Backup and Recovery from the Command Line ....................... 410
- Installing Software Updates ...................................................................... 416
  - Installing Updates Manually .................................................................. 417
  - Viewing Installed Updates ..................................................................... 418
  - Uninstalling Updates ............................................................................ 419
Table of Contents

Installing Applications ............................................. 421
Supported Types of Applications ................................. 421
Installing and Uninstalling Applications ...................... 422

Index ................................................................. 425

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 survey, please visit:

www.microsoft.com/learning/booksurvey
Acknowledgments

Huge thanks first of all to Andrew Mason, Principal Program Manager for the Server Core program at Microsoft, for reviewing all my chapters for technical accuracy and for patiently responding to my numerous questions.

Much thanks as well to the following individuals: to my friend and colleague Jason Miller, MVP, who assisted me in developing and testing the Hyper-V content for this book; to James O’Neill, IT Pro Evangelist at Microsoft UK, who reviewed the Hyper-V content and provided helpful advice; and to Bob Dean, the technical reviewer for this project, who went above and beyond the call of duty in helping ensure the content is accurate. Special thanks also to Bill Noonan, Mark Kitris, and the members of the CSS Global Technical Readiness Team (GTR) at Microsoft for the invaluable assistance they provided on this project.

Thanks also to Karen Szall, the development editor at Microsoft Press for this book, and Carol Vu, the project editor at Microsoft Press, both of whom I’ve enjoyed working with on this project and hope to do so again in the future. Thanks also to Martin DelRe, who first approached me about being involved in this project.

Thanks as well to my friend and agent, Neil Salkind of Salkind Literary Agency, which is part of Studio B Productions, Inc.

And finally, thanks to my wife, Ingrid, for her encouragement and support during this project.
As Windows Server has continued to evolve, increasing functionality with each release, it became apparent that there was a need for additional deployment flexibility. Windows Server is a general-purpose operating system, but it is frequently deployed to provide a fixed function on a network, such as a DNS Server, File Server, Active Directory Domain Services domain controller, and so on. In these deployments, more functionality than necessary is often installed for a single server role to run, and a common customer request has been to allow the installation of just what is needed. The result of this is the new Server Core installation option in Windows Server 2008.

Server Core is an exciting and big step forward that allows customers more flexibility in how they deploy, manage, maintain, and secure a Windows Server installation. You may have heard that Server Core is a minimal, GUI-less interface, or even that it is a Windows without windows installation of Windows Server. As you will see as you go through this book, Server Core is much more than just the removal of the Windows shell. The way I like to describe Server Core is that it is a slice off the bottom of the operating system, providing a subset of the full functionality. To that end, customers are finding a variety of ways to take advantage of the many benefits Server Core provides. Some of the benefits you will find include a reduction in the number of software updates required to maintain the operating system (OS), a smaller attack surface, its relative simplicity (there’s less to configure, so there’s less to misconfigure), and the fact that it can be used to extend the life of older hardware.

As you delve into Server Core in this book, you may wonder why some functionality was included while other functionality was left out of Server Core. The best way to explain that in the limited space I have is to state the goal we had in designing Server Core: to provide customers with a minimal installation option that reduces management, maintenance, and the security attack surface while running the network infrastructure server roles and still being manageable with the same set of tools. To achieve this, a lot of time was spent on the management side to ensure Server Core is manageable and fits seamlessly in with the management infrastructures that customers are already using with Windows Server. We included functionalities such as Windows Installer, so that the Microsoft Windows Installer (.msi) packages for management agents can be used to install the agents the same way they are on a full Windows Server installation. However, including functionality in Server Core while trying to maintain these goals is very much a tightrope walk that requires some hard decisions and some omissions until dependencies can be changed.
This book will be an invaluable resource for administrators wanting to understand how to install, configure, and manage a Server Core installation. It is a resource that you can refer to for end-to-end deployments of Server Core, as well as for guidance on using specific server roles and useful tips for working with Server Core.

The Server Core team is very proud of what we were able to accomplish and hope you will take advantage of its benefits in your environment.
Introduction

Welcome to the Windows Server 2008 Server Core Administrator’s Pocket Consultant. Server Core is a new installation option available for Windows Server 2008 that has a reduced servicing footprint and is designed for running a specific set of server roles for dedicated use. Enterprises have been asking for a book like this for a while, because Server Core can help branch offices, data centers, and other environments significantly reduce the cost involved with deploying and managing servers running Microsoft Windows. I hope you find that this book meets your needs and answers any questions you may have about Server Core; feel free to use my personal contact info found later in this Introduction to send me questions.

Who Is This Book For?

The target audience for the Windows Server 2008 Server Core Administrator’s Pocket Consultant is administrators and staff of enterprise IT departments who need to learn how to deploy, configure, manage, and maintain Server Core computers in various roles, including domain controllers, infrastructure servers, Web servers, and other supported roles. The book assumes that you have at least a couple of years’ experience managing servers running Windows in various roles, that you are familiar with most of the administrative tools used to manage servers running Windows, and that you have at least some experience trying to administer such servers from the command line.

Because most administrators who work with servers running Windows tend to be comfortable using administrative tools like Microsoft Management Console (MMC) consoles for managing their servers, this book focuses to a large extent on showing how you can perform many administrative tasks from the command line. This choice of focus was obvious for two reasons. First, when you log on to Server Core, all you see is a command prompt—there’s no desktop! That means no MMC consoles either, but of course, you can use most MMC consoles remotely to manage Server Core from another computer, and that’s covered too. But second, I didn’t want to reinvent the wheel because über-author William Stanek has already published an excellent book called the Windows Server 2008 Administrator’s Pocket Consultant, which explains in detail how to use these various MMC consoles to manage different roles and features on servers running Windows Server 2008. The result is that this present book is intended to complement Stanek’s book instead of supplant it, and I encourage you to buy both books and use them together as a comprehensive quick reference for administering all aspects of the Windows Server 2008 platform.
How This Book Is Organized

Although this book is intended mainly as a quick lookup reference of how to perform administrative tasks, you can also read the book from cover to cover and gain a good understanding of the capabilities, features, and occasional quirks of Server Core. Whatever way you use it—as a task reference or for learning purposes—you’ll benefit from using the most comprehensive resource available on administering Server Core.

The overall flow of this book looks like this:

- Chapter 1 provides a brief introduction to the platform and should be read in its entirety if you are new to Server Core.
- Chapters 2 and 3 cover manual and unattended deployment methods and various post-deployment configuration tasks that you may need to perform.
- Chapter 4 looks at the various roles and features that you can install on Server Core and explains how to deploy them both manually and during unattended installation.
- Chapters 5 and 6 explain the various tools and methods that you can use to administer Server Core, including using the local command line, Remote Desktop, the Windows Remote Shell, MMC consoles, Group Policy, and, to a limited extent, Windows PowerShell.
- Chapters 7 through 12 examine in detail each of the server roles that you can install on Server Core and how to install, configure, and manage each role using the tools and methods described in Chapters 5 and 6.
- Finally, Chapter 13 describes how to maintain various aspects of Server Core, including managing services, devices, processes, scheduled tasks, event logs, software updates, and management agents.

Conventions Used in This Book

Many elements have been used in this book to help keep the text clear and easy to follow. Commands within text that you can type to perform different tasks are styled in **bold** type. Commands with their command output are styled in **monospace** type to make them more visible, and I’ve included typical output of many commands so you can know what to expect when you use them. And new terms being introduced are styled in *italic* type.

I’ve also included the following elements where they can be helpful:

- **Note** Provides additional detail or a sidelight on the topic under discussion
- **Caution** Informs you of things to be aware of so you can avoid potential pitfalls
- **Tip** Gives you some pointers that you’ll probably want to know because it will make your job easier
Best Practices  Offers advice that you should follow to maintain supportability for your configuration

More Info  Directs you to where you can get more information about the subject being discussed

Other Server Core Resources

While this book is intended as a comprehensive resource on administering Server Core, there are several other resources out there that you can use if this book doesn’t provide you with all the information you need. I’ve already mentioned the Windows Server 2008 Administrator’s Pocket Consultant, which complements this book—Stanek’s book focuses on GUI administration, while this book concentrates on how you can do things from the command line. Another book you may find useful is the Windows Command-Line Administrator’s Pocket Consultant, Second Edition, also by William Stanek, which explains the syntax of different Windows commands. Both these books are published by Microsoft Press and are available from booksellers everywhere.


There are also several blogs that contain some excellent posts on administering Server Core. The two I’ve found most useful are Andrew Mason’s “Server Core” blog on TechNet (http://blogs.technet.com/server_core/) and the Server Core posts on Sander Berkouwer’s “The Things That Are Better Left Unspoken” blog (http://blogs.dirteam.com/blogs/sanderberkouwer/).

Finally, if you want to interact with other administrators who are working with Server Core, the best place to do so is the Server Core forum on TechNet at http://forums.technet.microsoft.com/en-US/winservercore/threads/. Feel free to post your questions and comments there, or better yet, answer questions posted by others.

Contact the Author

You may feel free to contact me if you have comments, questions, or suggestions regarding anything in this book. While I respond to all queries from readers and will do my best to answer your question to your satisfaction, I cannot provide readers with technical support. Please send your questions to the alias sc@mtit.com, where they will be queued for my attention; expect a reply within one or two days. You can also check my Web site http://www.mtit.com for links to numerous articles and tips I’ve written. Please check these out because the answer to your question or problem may already be published in one of these.
Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address: http://www.microsoft.com/mspress/support.

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

Postal mail:
Microsoft Press
Attn: Windows Server 2008 Server Core Administrator’s Pocket Consultant Editor
One Microsoft Way
Redmond, WA 98052-6399

E-mail:
mspininput@microsoft.com

Please note that product support isn’t offered through the mail addresses. For support information, visit Microsoft’s Web site at http://support.microsoft.com/.
Chapter 6

Remote Management

Server Core can be managed remotely using a variety of approaches, including using Remote Desktop or TS Remote App, using Microsoft Management Console (MMC) snap-ins and the Remote Server Administration Tools (RSAT), using Windows Remote Shell (WinRS), using Group Policy, and, to some extent, using Windows PowerShell. This chapter examines each of these remote administration methods and demonstrates how to set them up and use them to manage Server Core.

Using Remote Desktop

You can use Remote Desktop (also known as Terminal Services for Administration) to administer a Server Core installation remotely in exactly the same way you would administer it from the local console of the server. By default, Remote Desktop is disabled on Server Core, so before you can use Remote Desktop to manage a Server Core installation remotely, you must first enable Remote Desktop on the server. This can be done in several ways, as the next sections illustrate.

Enabling Remote Desktop Using Scregedit.wsf

You can use the Scregedit.wsf script to enable Remote Desktop on your Server Core installation by logging on locally to your server and doing the following:

```
C:\Users\Administrator> cscript %windir%\system32\scregedit.wsf /ar 0
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
Registry has been updated.
```

To verify that the registry change has been made, do this:

```
C:\Users\Administrator> cscript %windir%\system32\scregedit.wsf /ar /v
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
System\CurrentControlSet\Control\Terminal Server fDenyTSConnections
View registry setting.
0
```

A value of 0 for the fDenyTSConnections registry value means that Remote Desktop is enabled on the system, while a value of 1 means that Remote Desktop is disabled. If you later decide you want to disable Remote Desktop on your Server Core installation, type `cscript %windir%\system32\scregedit.wsf /ar 1` at a command prompt.
Tip If your current directory is C:\Windows\System32, you can shorten these commands by omitting the %Windir%\System32\ portion of them.

Enabling Remote Desktop using Scrgedit.wsf also automatically enables the Remote Desktop rule group in Windows Firewall.

Enabling Remote Desktop Using an Answer File

You can use an answer file to enable Remote Desktop during an unattended install of Server Core. You do this as follows:

1. Add the following component to the specialize configuration pass of your answer file:
   
   Microsoft-Windows-TerminalServices-LocalSessionManager

2. In the Properties pane, click the box to the right of the fDenyTSConnections setting; a drop-down arrow appears. Click the drop-down arrow and select False, as shown here.

3. Add the following component to the oobeSystem configuration pass of your answer file:
   
   Microsoft-Windows-Shell-Setup\FirstLogonCommands\SynchronousCommand

4. In the Properties pane, type C:\Windows\system32\netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes in the box beside CommandLine and type 1 (or another number if you are running multiple FirstLogonCommands) in the box beside Order.

Tip You can also use WinRS to enable Remote Desktop remotely on a Server Core installation. See the section “Using WinRS to Administer Server Core in a Domain,” later in this chapter, for more information.
Using Scrededit.wsf to Require Network Level Authentication for Remote Desktop

By default, when Remote Desktop is enabled on Server Core, computers running versions of Microsoft Windows earlier than Windows Vista are allowed to connect. You can use the Scrededit.wsf script to prevent computers running versions earlier than Windows Vista from connecting to Server Core using Remote Desktop by logging on locally to your server and doing the following:

C:\Users\Administrator>\cscript %windir%\system32\scrededit.wsf /cs 1
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
Registry has been updated.

Doing this increases the security of your Server Core installation by requiring that the client you are using to administer Server Core uses Network Level Authentication. For more information, see the section “Configuring Remote Desktop to Require Network Level Authentication,” in Chapter 3, “Initial Configuration.”

Using an Answer File to Require Network Level Authentication for Remote Desktop

You can use an answer file to require that Network Level Authentication be used for Remote Desktop connections. You do this as follows:

1. Add the following component to the specialize configuration pass of your answer file:

   Microsoft-Windows-TerminalServices-RDP-WinStationExtensions

2. In the Properties pane, click the box to the right of the UserAuthentication setting and type 1 to require Network Level Authentication, as shown here.

   ![Diagram showing answer file settings](image)
You can also configure the SecurityLayer setting to specify how your server and Remote Desktop clients authenticate each other prior to a Remote Desktop connection being established. The possible values for this setting are shown in Table 6-1.

### Table 6-1 The SecurityLayer Setting Values

<table>
<thead>
<tr>
<th>SecurityLayer</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Remote Desktop Protocol (RDP) is used by the server and the client for authentication prior to a Remote Desktop connection being established. Use this setting if you are working in a heterogeneous network environment.</td>
</tr>
<tr>
<td>1</td>
<td>The server and the client negotiate the method for authentication prior to a Remote Desktop connection being established (this is the default value). Use this setting if all your client computers are running Windows.</td>
</tr>
<tr>
<td>2</td>
<td>Transport Layer Security (TLS) is used by the server and the client for authentication prior to a Remote Desktop connection being established. Use this setting for maximum security.</td>
</tr>
</tbody>
</table>

### Using Remote Desktop to Administer Server Core

To use Remote Desktop to administer a Server Core installation, log on to a computer running Windows Vista or Windows Server 2008 and do the following:

1. Press the Windows key+R to open the Run text box.
2. Type `mstsc` and press Enter to open Remote Desktop Connection.
3. Type the name, either NetBIOS or Fully Qualified Domain Name (FQDN), or the Internet Protocol (IP) address of your Server Core installation in the Computer text box.
4. Click Options and type the name of a user account that has administrative privileges on the Server Core installation. Be sure to type this user name in the form `servername\username` (if the server belongs to a workgroup) or `domainname\username` (if the server belongs to a domain), as shown here.
5. Click Connect. When the Windows Security dialog box appears, type the password for the user account you are using to administer Server Core, as shown here.

6. Select Remember My Credentials if you want Credential Manager to save the credentials for this user.
7. Click OK. After a few moments, Remote Desktop Connection should connect to your remote Server Core installation (as shown here), and you then can administer your server using the same methods described in Chapter 5, “Local Management.”

8. When you are finished administering your server, type `logoff` to end the Terminal Services session with the remote server.

**Note**  Like the Full installation option of Windows Server 2008, the Server Core installation option supports two simultaneous Terminal Services connections for remote administration.

**Using TS Remote App for Publishing Cmd to Administer Server Core**

You don’t have to use the full version of Remote Desktop to administer Server Core remotely. Instead, you can use Terminal Services RemoteApp to publish the Server Core command interpreter (Cmd) so that it can be started on another computer. That way, the command prompt running on Server Core programs can be accessed remotely using Terminal Services and appear as if it is running on your local
To use TS RemoteApp to publish Cmd running on Server Core, do the following:

1. On the Server Core installation you want to manage, enable Remote Desktop using one of the methods described earlier in this chapter. Then enable the Remote Administration rule group in Windows Firewall by typing the following command:

   ```
   netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
   ```


3. On your terminal server (or on your Terminal Services management station), click Start, Administrative Tools, Terminal Services, and finally TS RemoteApp Manager to open the TS RemoteApp console on your terminal server.

4. Click Connect To Computer in the right Actions pane to open a Select Computer dialog box. Select the Another Computer option and type or browse to the name of your Server Core computer. Click OK. Your TS RemoteApp Manager console is now connected to the Server Core computer.

5. In the Actions pane, click Add RemoteApp Programs, Next, and Browse to open the Choose A Program dialog box. Browse the local file system of the Server Core computer using the connection to the C$ administrative share on that computer until you find and select the C$\Windows\System32\Cmd.exe file. Click Open, Next, and finally Finish.

6. In the RemoteApp Programs list, right-click Cmd.exe and select Create .rdp File from the drop-down menu to start the RemoteApp Wizard. Click Next twice and then click Finish. The folder C:\Program Files\Packaged Programs opens on your Server Core computer, displaying the .rdp file for Cmd.

7. Double-click the .rdp file and click Connect. The Windows Security dialog box appears. Type credentials that have administrative privileges on the remote Server Core installation and then click OK.

8. Click Run to run Cmd.exe on the remote Server Core installation and display the remote command interpreter as a command-prompt window on your desktop. You can also copy the .rdp file to any computer using the RDC 6.0 client or later and use it to connect to your Server Core installation and open the command prompt on the Server Core computer.
Managing Terminal Services on Server Core

You can use the following two MMC snap-ins for remotely managing Terminal Services (Remote Desktop for Administration) on Server Core:

- Terminal Services Manager
- Terminal Services Configuration

You can use these snap-ins on a Full installation of Windows Server 2008 that has the Terminal Services role installed, or you can use them on a computer running Windows Vista or Windows Server 2008 that has the RSAT installed.

You can also manage Terminal Services (Remote Desktop for Administration) from the command prompt on a Server Core installation. Table 6-2 lists the commands that you can use to manage Terminal Services locally on Server Core.

**Table 6-2 Commands Available for Locally Managing Terminal Services on Server Core**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change logon</td>
<td>Enables or disables logons to a terminal server</td>
</tr>
<tr>
<td>Logoff</td>
<td>Logs a user off a session and deletes the session</td>
</tr>
<tr>
<td>Msg</td>
<td>Sends a message to a user or group of users</td>
</tr>
<tr>
<td>Query process</td>
<td>Displays information about processes running on a terminal server</td>
</tr>
<tr>
<td>Query session</td>
<td>Displays information about sessions on a terminal server</td>
</tr>
<tr>
<td>Query user</td>
<td>Displays information about user sessions on a terminal server</td>
</tr>
<tr>
<td>Tscon</td>
<td>Connects to another existing terminal server session</td>
</tr>
<tr>
<td>Tsdiscon</td>
<td>Disconnects a client from a terminal server session</td>
</tr>
<tr>
<td>Tskill</td>
<td>Ends a process</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down a terminal server</td>
</tr>
</tbody>
</table>

For example, to display all Terminal Services sessions on a Server Core installation named SEA-SC2, do this:

```bash
C:\Users\tallen> query session /server:SEA-SC2
```

<table>
<thead>
<tr>
<th>SESSIONNAME</th>
<th>USERNAME</th>
<th>ID</th>
<th>STATE</th>
<th>TYPE</th>
<th>DEVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>services</td>
<td>tallen</td>
<td>0</td>
<td>Disc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>console</td>
<td>tallen</td>
<td>1</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdp-tcp#0</td>
<td>Administrator</td>
<td>2</td>
<td>Active</td>
<td>rdpwd</td>
<td></td>
</tr>
<tr>
<td>rdp-tcp</td>
<td></td>
<td>65536</td>
<td>Listen</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The output of the Query Session command shows that administrator Tony Allen (tallen@contoso.com) is logged on locally to the Server Core installation, while the default Administrator account (either a built-in local or a domain account) is logged on remotely using a Remote Desktop session.
To log the remote Administrator off of the Server Core installation forcibly, log off session 2 as follows:

C:\Users\tallen> logoff 2 /server:SEA-SC2

Verify the result:

C:\Users\tallen> query session /server:SEA-SC2

<table>
<thead>
<tr>
<th>SESSIONNAME</th>
<th>USERNAME</th>
<th>ID</th>
<th>STATE</th>
<th>TYPE</th>
<th>DEVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>services</td>
<td></td>
<td>0</td>
<td>Disc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>console</td>
<td>tallen</td>
<td>1</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdp-tcp</td>
<td></td>
<td>65536</td>
<td>Listen</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using WinRS

You can use WinRS to administer a Server Core installation remotely from the command line. WinRS is a command-line tool included in both Windows Vista and the Full installation of Windows Server 2008, which relies on Windows Remote Management (WinRM) to execute remote commands, especially for headless servers. WinRM is Microsoft’s implementation of the WS-Management protocol, a standard Simple Object Access Protocol (SOAP)–based, firewall-friendly protocol that enables hardware and operating systems from different vendors to interoperate. You can think of WinRM as the server side and WinRS the client side of WS-Management.

Configuring WinRM on Server Core

To enable WinRM on a Server Core installation, you need to run a configuration command that creates a “listener” that can respond to WinRS commands issued from other computers. The configuration command also opens an exception for WinRM in Windows Firewall. To enable WinRM, do the following:

C:\Users\tallen> winrm quickconfig

WinRM is not set up to allow remote access to this machine for management. The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
WinRM firewall exception enabled.
Note: For more information on configuring WinRM, type `winrm help config` at a command prompt.

Using WinRS to Administer Server Core in a Domain

The basic syntax for WinRS commands is as follows:

```
winrs -r:target command
```

where `target` is the name (NetBIOS or FQDN) of the Server Core installation that has had WinRM enabled on it, and `command` is any command string that you want to execute on the Server Core installation. For example, to use WinRS to enable Remote Desktop remotely on a Server Core installation named SEA-SC2, type the following command on any computer running Windows Vista or on a Full installation of Windows Server 2008:

```
winrs -r:SEA-SC2 cscript %WINDIR%\system32\scregedit.wsf /ar 0
```

When you type this command on a computer running Windows Vista, for example, the command is executed remotely on the targeted Server Core installation and the command output is piped back to the command shell on your computer running Windows Vista:

```
C:\Users\Administrator>winrs -r:SEA-SC2 cscript %windir%\system32\scregedit.wsf /ar 0
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
Registry has been updated.
```

You can do anything using WinRS that you can do at the local command prompt on Server Core. For example, you can perform the initial configuration of your Server Core installation, install and uninstall roles and features on your server, and perform other tasks.

Note: For more information on the syntax of WinRS commands, type `winrs /?` at a command prompt.

Using WinRS to Administer Server Core in a Workgroup

You can use WinRS to administer a Server Core installation that belongs to a workgroup. Before you can do this, however, you must add the name of your computer to the TrustedHosts table of WinRM on your Server Core installation. For example, to enable a computer running Windows Vista named SEA-DESK155 to execute
commands remotely on your Server Core installation using WinRM, type the following on your Server Core computer:

C:\Users\Administrator>winrm set winrm/config/client @{TrustedHosts="SEA-DESK155"}

Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = false
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
    DefaultPorts
        HTTP = 80
        HTTPS = 443
    TrustedHosts = SEA-DESK155

Requirements for Using WinRS

To use WinRS to administer a Server Core installation remotely, each of the following must be true:

■ Your local computer must be running either Windows Vista or a Full installation of Windows Server 2008.

■ You must enable a WinRM listener on the Server Core installation, and you must open the WinRM exception in Windows Firewall on the Server Core installation; the Winrm quickconfig command can be used to do this.

■ You must execute your WinRS commands using administrator credentials on the Server Core installation. If you are not currently logged on to your computer using such credentials, you can use the Net use command to connect to the Server Core computer using such credentials. For example, to connect to a Server Core installation named SEA_SC2 using the credentials of administrator Tony Allen (tallen@contoso.com), type net use \SEA-SC2\IPC$ /u:CONTOSO\tallen at a command prompt. Type Tony’s password when prompted to do so, and then you can execute commands remotely on the Server Core installation using WinRS.

■ Commands or scripts that are executed using WinRS must have no user interface dependencies. This means that you cannot execute commands that prompt you to Press Any Key when they are typed at the local console or require any other interactive response.
Configuring WinRM and WinRS Using Group Policy

You can use Group Policy to configure security for both WinRM and WinRS. The relevant policy settings are found in the following locations:

- Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)
- Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell

Using MMC Snap-ins and RSAT

You can use Microsoft Management Console (MMC) snap-ins to administer a Server Core installation remotely from a Full installation of Windows Server 2008. You can also install RSAT on either Windows Vista or a Full installation of Windows Server 2008 and use these tools to administer Server Core. The advantage of using RSAT is that it gives you the full complement of MMC consoles; by comparison, on a Full installation of Windows Server 2008, you may be missing some consoles because of certain roles and features not being installed on your server. Using MMC snap-ins or RSAT allows you to administer a Server Core installation—the same way that you administer a Full installation—without the need of learning the syntax of many command-line utilities.

Using MMC Consoles to Administer Server Core in a Domain

When you install a server role on a Server Core installation, the appropriate firewall ports needed to manage that role remotely using MMC snap-ins are opened automatically. This means that when you type `start /w ocsetup DNS-Server-Core-Role` at a command prompt on a Server Core installation, the command installs the DNS Server role and enables the Windows Management Instrumentation (WMI) and DNS Service rule groups to allow the DNS snap-in running on another computer to connect to Server Core.

For example, to use the DNS console found under Administrative Tools on a domain controller named FULL161 to administer a Server Core DNS server named SEA-SC2, perform the following steps:

1. On the domain controller, click Start, Administrative Tools, and then DNS to open the DNS Manager console.
2. Right-click the root node of the console and select Connect To DNS Server.
3. In the Connect To DNS Server dialog box, select The Following Computer and type `SEA-SC2` in the text box. Click OK.
4. The DNS Manager console connects to DNS server SEA-SC2. Expand the console tree to display the configuration of DNS server SEA-SC2, as shown here.

Changing the Focus of an MMC Console

Most (but not all) MMC consoles found under Administrative Tools can have their focus changed to administer a different computer than the local one on which they are being used. Examples of consoles that can have their focus changed include Active Directory Users And Computers, Computer Management, DHCP, DNS, and Event Viewer. Examples of consoles whose focus cannot be changed include Server Manager, Windows Firewall With Advanced Security, and Windows Server Backup.

Using MMC Snap-ins to Administer Server Core

You can also add MMC snap-ins to a new MMC console to administer Server Core remotely. For example, to use the Windows Firewall With Advanced Security snap-in to manage the firewall remotely on a Server Core installation named SEA-SC2, do the following:

1. Press the Windows key+R, type mmc, and click OK to open an empty MMC console.
2. Click File, and then click Add/Remove Snap-in. Scroll down the list of snap-ins and double-click Windows Firewall With Advanced Security to select it. When the Select Computer dialog box appears, choose Another Computer and type SEA-SC2 in the text box, as shown here.

![Image of DNS Manager console with Add a New Zone dialogue box for SEA-SC2]
3. Click Finish, and then click OK to add the snap-in to the console. Expand the console tree to view the configuration of Windows Firewall on your Server Core installation.

Some MMC snap-ins require that you also open ports in the firewall on Server Core to use these snap-ins to administer Server Core remotely. For example, for the previous procedure to work, you must first enable the Windows Firewall Remote Management rule group in the firewall on your Server Core installation. This can be done by typing the following command at your Server Core command prompt:

```
netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes
```

Table 6-3 lists some of the more commonly used MMC snap-ins and the firewall rule group that must be enabled to use these snap-ins to manage Server Core remotely. The general syntax for enabling a rule group in Windows Firewall is as follows:

```
netsh advfirewall firewall set rule group="Name of rule group" new enable=yes
```

Table 6-3 Rule Groups You Must Enable in Windows Firewall to Allow Remote Management by an MMC Snap-in

<table>
<thead>
<tr>
<th>MMC Snap-in</th>
<th>Rule Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Viewer</td>
<td>Remote Event Log Management</td>
</tr>
<tr>
<td>Services</td>
<td>Remote Service Management</td>
</tr>
<tr>
<td>Shared Folders</td>
<td>File And Printer Sharing</td>
</tr>
<tr>
<td>Task Scheduler</td>
<td>Remote Scheduled Tasks Management</td>
</tr>
<tr>
<td>Reliability And Performance</td>
<td>Performance Logs And Alerts</td>
</tr>
<tr>
<td></td>
<td>File And Printer Sharing</td>
</tr>
<tr>
<td>Windows Firewall With Advanced Security</td>
<td>Windows Firewall Remote Management</td>
</tr>
</tbody>
</table>
Best Practices  The simplest way to configure Windows Firewall on Server Core is to enable remote management of Windows Firewall and then use the Windows Firewall With Advanced Security snap-in on a computer running Windows Vista to make further configuration changes to your firewall. You can also use Group Policy to configure Windows Firewall once the Windows Firewall Remote Management rule group is enabled on your Server Core installation. For more information on using the Windows Firewall With Advanced Security snap-in, see http://technet.microsoft.com/en-us/network/bb545423.aspx.

Some MMC snap-ins require further configuration of your Server Core installation before you can use them to administer your server. The following sections describe several of these snap-ins and the additional configuration that they require on the server before they will work remotely against it.

Using the Device Manager Snap-in

To allow the Device Manager snap-in to administer Server Core remotely, perform the following steps:

1. On your Server Core computer, enable the Remote Administration rule group in Windows Firewall.

2. On a Full installation of Windows Server 2008, open a new MMC console by pressing the Windows key+R, typing mmc, and clicking OK.

3. Click File, and then Add/Remove Snap-in to open the Add Or Remove Snap-ins dialog box.

4. Double-click Group Policy Object Editor to display the Group Policy Wizard.

5. Click Browse, select Another Computer, and type or browse to the name of your Server Core computer. Then click OK, Finish, and finally OK again. The Group Policy Object Editor is now connected to your Server Core computer.

6. Browse the console tree to find and enable the following policy setting:
   Computer Configuration\Policies\Administrative Templates\System\Device Installation\Allow Remote Access To The PnP Interface.

7. Close the Group Policy Object Editor. Then, on your Server Core computer, type shutdown -r -t 0 at the command prompt to restart the server.

Note  Device Manager can operate only in “view only” mode when run from a remote computer as described here.
Using the Disk Management Snap-in

To allow the Disk Management snap-in to administer Server Core remotely, perform the following steps:

1. Enable the Remote Volume Management rule group in Windows Firewall on your Server Core installation.

2. Start the Virtual Disk Service (VDS) by typing `sc start vds` at the command prompt. You can also type `sc config vds start= auto` to configure the service to start automatically each time the computer boots.

Using the IP Security Policy Management Snap-in

To allow the IP Security Policies snap-in to administer Server Core remotely, type the following command at the command prompt of your Server Core installation:

```
cscript %windir%\system32\scregedit /im 1
```

Using the Reliability And Performance Snap-in

No additional configuration is needed to use the Reliability And Performance snap-in, but it can monitor only performance data, not reliability data, on a remote Server Core installation.

Enabling Any MMC Snap-in to Administer Server Core

You can allow any MMC snap-in to administer Server Core remotely by enabling the Remote Administration rule group in Windows Firewall on your Server Core installation. To do this, type the following command:

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
```

As described in the section “Using MMC Consoles to Administer Server Core in a Domain,” earlier in this chapter, some snap-ins require additional configuration to get them to work properly for remotely administering Server Core.

Using MMC Snap-ins to Administer Server Core in a Workgroup

To use MMC snap-ins to administer a Server Core installation that belongs to a workgroup, you need to perform the following actions on your Server Core installation:

1. Enable the required rule groups in Windows Firewall (see the previous section for details).

2. Use Cmdkey to specify different credentials for MMC connections.
For example, to use the Services snap-in on a computer running Windows Vista to administer the services on a Server Core installation named SEA-SC1 that belongs to a workgroup, perform the following steps:

1. On your Server Core installation, type the following command to enable the Remote Service Management rule group in Windows Firewall:
   
   ```
   netsh advfirewall firewall set rule group="Remote Service Management" new enable=yes
   ```

2. Open a command prompt on your computer running Windows Vista and type the following command:
   
   ```
   cmdkey /add:SEA-SC1 /user:Administrator /pass:Pa$$w0rd
   ```
   
   In this command, the local Administrator account on SEA-SC1 has the password Pa$$w0rd.

3. Open the Services console under Administrative Tools (or add the Services snap-in to an empty MMC console), right-click the root node, and select Connect To Another Computer. Type **SEA-SC1** in the dialog box and then click OK.

You can now manage services remotely on your stand-alone Server Core installation from either a stand-alone or domain-joined computer running Windows Vista or Windows Server 2008.

**Note**  
Cmdkey is not needed for certain consoles, including Event Viewer and Scheduled Tasks.

### Using RSAT to Administer Server Core in a Domain

Windows Server 2003 included the Administration Tools Pack (Adminpak.msi), which provided server management tools that allowed administrators to manage Windows 2000 Server and Windows Server 2003 family servers remotely. The Administration Tools Pack could be installed on workstations running Windows XP to provide administrators with a full set of MMC consoles on their workstations for administering servers across their network.

With Windows Server 2008, however, the Administration Tools Pack has been replaced with the Remote Server Administration Tools (RSAT), which enables administrators to manage Windows Server 2008 roles and features remotely from a computer running Windows Vista with Service Pack 1 (SP1). RSAT is included as an optional feature on all editions of Windows Server 2008, and versions of RSAT for installing on 32-bit and 64-bit versions of Windows Vista SP1 Business, Enterprise, and Ultimate editions are available for download from the Microsoft Download Center at
For detailed information concerning the downloadable version of RSAT and the administrative tools it includes, see http://support.microsoft.com/kb/941314.

Using RSAT on either Windows Vista or a Full installation of Windows Server 2008, you can administer roles and features remotely on a Server Core installation the same way that you would administer them on a Full installation of Windows Server 2008.

**Note** RSAT cannot be installed on Server Core.

### Installing RSAT on a Full Installation of Windows Server 2008

To install RSAT on a Full installation of Windows Server 2008, perform the following steps:

1. Start the Add Features Wizard from either Server Manager or Initial Configuration Tasks.

2. Expand the Remote Server Administration Tools check box and select the check boxes under it for the specific role and feature administration tools that you want to install on your server. Alternatively, you can select the Remote Server Administration Tools check box to install all the role and feature administration tools on your server.

### Installing RSAT on Windows Vista SP1

To install RSAT on Windows Vista with Service Pack 1, perform the following steps:

1. Download the appropriate Windows Installer (.msi) package (either 32-bit or 64-bit) by using the links found at http://support.microsoft.com/kb/941314.

2. Double-click the downloaded Windows Update Standalone Installer package (Windows6.0-KB941314-x86.msu or Windows6.0-KB941314-x64.msu) to start the Setup wizard. Follow the prompts to complete the installation.

3. Open Control Panel and click Programs.

4. Under Programs And Features, click Turn Windows Features On Or Off. Respond to the User Account Control prompt as required.

5. In the Windows Features dialog box, scroll down and expand the Remote Server Administration Tools check box, then select the check boxes under it to install the remote administration snap-ins and tools that you want to install. You can also install all role and feature administration tools by selecting the Remote Server Administration Tools check box. Click OK when finished.
6. Configure your Start menu to display the Administration Tools shortcut by right-clicking Start and clicking Properties. Then on the Start Menu tab, click Customize, scroll down to System Administrative Tools, and select Display On The All Programs Menu And The Start Menu. Click OK when finished.

**Note** Installing RSAT also provides additional snap-ins that you can add to a blank MMC console.

**Using RSAT to Administer Server Core Remotely in a Domain**

You can use the RSAT tools to administer roles and features remotely on a Server Core installation that belongs to the same domain as your management workstation. As described in the section “Using MMC Snap-ins to Administer Server Core,” earlier in this chapter, you may need to configure Windows Firewall on your remote Server Core installation for some RSAT tools to be able to connect.

For example, to use RSAT on a computer running Windows Vista in the contoso.com domain to manage the DNS Server role on a Server Core installation named SEA-SC2 that belongs to the same domain, follow these steps:

1. On your Server Core installation, begin by enabling the necessary rule groups in Windows Firewall to allow remote administration of roles and features on the server. To allow remote administration of all roles and features on the server, type the following command:

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
```

As described in the section “Using MMC Consoles to Administer Server Core in a Domain,” earlier in this chapter, some snap-ins require additional configuration to get them to work properly for remotely administering Server Core.

2. Click Start, Administrative Tools, and then DNS to open the DNS Manager console. Before the console opens, a Connect To DNS Server dialog box appears. Select the The Following Computer option, type **SEA-SC1**, and click OK. DNS Manager opens and lets you remotely manage your Server Core DNS server.

**Tip** When you install RSAT using the procedures outlined earlier in this section, some MMC consoles found under Administrative Tools (such as the Windows Firewall With Advanced Security) cannot have their focus changed. To administer Windows Firewall remotely on a Server Core installation, you can open a blank MMC, add the Windows Firewall With Advanced Security snap-in, and change the focus of the snap-in so you can manage Windows Firewall on the remote Server Core installation.
Using RSAT to Administer Server Core Remotely in a Workgroup

You can use the RSAT tools to administer roles and features remotely on a Server Core installation that belongs to a workgroup. As described in the section “Using MMC Snap-ins to Administer Server Core,” earlier in this chapter, you may need to configure Windows Firewall on your remote Server Core installation for some RSAT tools to be able to connect.

For example, to use RSAT on a computer running Windows Vista to manage the DNS Server role on a stand-alone Server Core installation named SEA-SC1, do this:

1. On your Server Core installation, begin by enabling the necessary rule groups in Windows Firewall to allow remote administration of roles and features on the server. To allow remote administration of all roles and features on the server, type the following command:

   ```bash
   netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
   ```

   As described in the section “Using MMC Consoles to Administer Server Core in a Domain,” earlier in this chapter, some snap-ins require additional configuration to get them to work properly for remotely administering Server Core.

2. Open a command prompt on your Windows Vista computer and type the following command:

   ```bash
   cmdkey /add:SEA-SC1 /user:Administrator /pass:Pa$$w0rd
   ```

   In the previous command, the local Administrator account on SEA-SC1 has the password Pa$$w0rd.

3. Click Start, Administrative Tools, and then DNS to open the DNS Manager console. Before the console opens, a Connect To DNS Server dialog box appears. Select the The Following Computer option, type `SEA-SC1`, and click OK. DNS Manager opens and lets you remotely manage your Server Core DNS server.

Using Other GUI Tools

You can use other graphical user interface (GUI) tools besides MMC snap-ins to manage certain aspects of Server Core remotely. These tools include the following:

- Windows Explorer
- Task Scheduler
- Registry Editor

The following procedures assume that your remote Server Core installation belongs to the same domain as your Windows Vista management workstation. If your Server Core installation belongs to a workgroup, type the command `cmdkey /add:servername`
/user:username /pass:password to provide administrator credentials (that is, username and password) for these tools to be able to manage your Server Core installation (servername) remotely.

Using Windows Explorer Remotely

You can use Windows Explorer on a computer running Windows Vista or a computer running a Full installation of Windows Server 2008 to manage the file system remotely on a Server Core installation. To do this, follow these steps:

1. On the Server Core installation, enable the Remote Administration rule group in Windows Firewall by typing the following command:

   netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes

2. On the computer from which you want to manage your Server Core installation’s file system remotely, press the Windows key+R, type \servername\C$ (where servername is the name of your Server Core installation), and click OK. Specify credentials that have administrative privileges on the Server Core installation if you are prompted to do so.

3. Windows Explorer opens a new window focused on the root of the system drive on your Server Core installation. You now can browse the system drive on your remote server, create or delete files and folders, and perform other operations depending upon your level of privileges.

You can use the previous procedure with any share, whether administrative or user-created. You can also use the Net use command to map persistent network drives to shares on your remote Server Core installation. For example, you can type net use Z: \servername\C$ /persistent:yes at the command prompt, where servername is the name of your remote Server Core installation.

Using Task Scheduler Remotely

You can use Task Scheduler on a computer running Windows Vista or a computer running a Full installation of Windows Server 2008 to create, delete, configure, and manage tasks remotely on a Server Core installation. To do this, follow these steps:

1. Click Start, All Programs, Accessories, and then System Tools, and open Task Manager on your computer running Windows Vista.

2. Right-click the root node in Task Scheduler and select Connect To Another Computer.

3. Type the name of the remote Server Core installation and click OK.
Using Registry Editor Remotely
You can use Registry Editor on a computer running Windows Vista or a computer running a Full installation of Windows Server 2008 to edit the registry on a Server Core installation remotely. To do this, follow these steps:

1. Press the Windows key+R, type `regedit`, and click OK to open Registry Editor on your computer running Windows Vista.
2. Select File, and then Connect Network Registry.
3. Type the name of the remote Server Core installation and click OK.

Using Group Policy
You can use Group Policy to manage Server Core remotely the same way that you manage any other computer running Windows. You cannot install Group Policy MMC consoles on Server Core; you must manage Server Core remotely using Group Policy MMC consoles on another computer, such as a Full installation of Windows Server 2008 or a computer running Windows Vista with RSAT installed.


Group Policy Tools on Server Core
Server Core does include two command-line Group Policy tools:


- **Gpresult** Used to display Resultant Set of Policy (RSoP) information. Detailed syntax for using this command can be found in the Windows Server 2008 Command Reference (available from the Microsoft Download Center, as cited earlier in this chapter) or by typing `gpresult /?` at a command prompt.

Using WMI Filters to Administer Server Core with Group Policy
You can use WMI filters to ensure that the policy settings contained in a particular Group Policy Object (GPO) are applied only to Server Core installations. WMI filters are used to determine the scope of Group Policy based on computer attributes such as operating system and free hard disk space.
To create a WMI filter that will cause the Seattle SC GPO to be applied only to Server Core computers, perform the following steps:

1. On your domain controller, open Group Policy Management from Administrative Tools.

2. Right-click the WMI Filters node in the console tree and select New.

3. Click Add and type the information in the screenshot shown here to create a WMI Query Language (WQL) query that uses the OperatingSystemSKU property of the Win32_OperatingSystem WMI class to determine whether a given computer is running Server Core Standard (13), Enterprise (14), or Datacenter (15) edition.

4. Click OK to add the WQL query to your WMI filter and type a name and description for your filter, as shown here.

5. Click Save to save your WMI filter.

6. Under Group Policy Objects, select Seattle SC GPO.
7. On the Scope tab, under WMI Filtering, select Server Core ONLY and click Yes when the dialog box appears, as shown here. The WMI filter is now linked to the GPO.

When Group Policy is processed by a computer targeted by the GPO, the WQL query contained in the WMI filter is evaluated against the WMI repository on the targeted computer. If the query evaluates as True, the GPO is applied; if the query evaluates as False, the GPO is not applied.

Note GPOs can have only one WMI filter, but you can link a single WMI filter to multiple GPOs.

Managing Local Group Policy on Server Core

You can manage local Group Policy on Server Core by using the Group Policy Object Editor running on a Full installation of Windows Server 2008 or on a computer running Windows Vista SP1. To do this, follow these steps:

1. Open a new MMC console by pressing the Windows key+R, typing `mmc`, and clicking OK.
2. Click File, and then Add/Remove Snap-in to open the Add Or Remove Snap-ins dialog box.
3. Double-click Group Policy Object Editor to display the Group Policy Wizard.
4. Click Browse, select Another Computer, and type or browse to the name of the remote Server Core computer.

5. Click OK, Finish, and finally OK again. Group Policy Object Editor is now connected to your remote Server Core computer, and you can browse local policy on the computer and configure it as desired.

**Using Windows PowerShell**

You can use Windows PowerShell to administer Server Core remotely, but only if you use WMI in your PowerShell commands. PowerShell WMI commands typically take the following form:

```
Get-WMIObject WMIclass -computername servername
```

where `WMIclass` is the WMI class you want to access and `servername` is the name of the remote Server Core installation.

**Tip** To display a list of all WMI classes supported on a remote Server Core installation, type `Get-WMIObject –list –computername servername` at the PowerShell command prompt.

Here is an example of using PowerShell (running on a computer running Windows Vista on which PowerShell 1.0 has been installed) to display a list of services installed on a Server Core installation named SEA-SC2 that belongs to the same domain. Perform the following steps:

1. On the Server Core installation, enable the Windows Management Instrumentation (WMI) rule group in Windows Firewall by typing the following command:

   ```
   netsh advfirewall firewall set rule group=“Windows Management Instrumentation (WMI)” new enable=yes
   ```

2. On the computer running Windows Vista, open the PowerShell command prompt by clicking Start, All Programs, Windows PowerShell 1.0, and finally Windows PowerShell.

3. Use the command shown here to display a list of services installed on SEA-SC2:

   ```
   PS C:\Users\tallen> Get-WMIObject Win32_Service -computername SEA-SC2
   ```

   ExitCode : 0
   Name : AeLookupSvc
   ProcessId : 964
   StartMode : Auto
   State : Running
   Status : OK
   
   ExitCode : 1077
Name : AppMgmt
ProcessId : 0
StartMode : Manual
State : Stopped
Status : OK
...

Note You cannot install Windows PowerShell 1.0 locally on Server Core.

Index

Symbols
% (percent sign), 106
& (ampersand), 103
&& (double ampersand), 103
() parentheses, 103
* (asterisks), 53
| (bar), 104
|| (double bar), 103

A
A resource record, 222, 227
AAAA resource record, 227
access control lists (ACLs), 237, 259–263
ACLs (access control lists), 237, 259–263
Active Directory Application Mode (ADAM), 349
Active Directory Domains And Trusts, 171, 174
Active Directory Installation Wizard, 158
Active Directory Sites And Services, 174
Active Directory Users And Computers
  additional information, 71
  changing focus, 129
  configuring password replication, 186
  managing domain controllers, 174
AD CS (Active Directory Certificate Services), 6
AD DS (Active Directory Domain Services)
  creating child domains, 159–160
  creating domain trees, 158–159
  creating forests, 144–158
  DFSN support, 272
  DNS support, 213
  installing, 143
  installing replica domain controllers, 160–165
  managing domain controllers, 172–175
  package names, 80
  performing common management tasks, 175–182
  preparing environment for domain controllers, 169–172
  removing domain controllers, 165–169
  RODC support, 182–188
  role support, 77, 92
  Server Core installation option, 3, 6, 15
AD DS-integrated primary DNS server, 220
AD DS-integrated primary zone, 225
AD DS-integrated zone, 222, 226
AD FS (Active Directory Federation Services), 6
AD LDS (Active Directory Lightweight Directory Services)
  installing, 348–352
  role support, 77, 80, 92
  Server Core installation option, 6, 15
AD LDS instance, 349–352
AD RMS (Active Directory Rights Management Services), 6
ADAM (Active Directory Application Mode), 349
AdamInstall.exe command, 349
Add Features Wizard, 134
Add Or Remove Snap-ins dialog box, 140
Add Printer Wizard, 288
Add Roles Wizard, 83
admin role separation, 184
Adprep command
  functionality, 144
  preparing environment, 169–172
  preparing forests for RODCs, 184
  viewing debug logs, 170
Advanced Encryption Standard (AES) encryption, 172
AeLookupSvc (Application Experience), 11
AES (Advanced Encryption Standard) encryption, 172
ALLUSERSPROFILE environment variable, 104
ampersand (&), 103
answer files
  activating Windows, 67
  additional information, 29–30, 47
  configuring Automatic Updates, 61–62
  configuring CEIP settings, 65
  configuring date/time settings, 58–59
  configuring regional/language settings, 60
  configuring TCP/IP settings, 53, 56–57
  configuring Windows Error Reporting, 64
  creating child domains, 159–160
  creating domain trees, 158–159
  creating for unattended installs, 23–30
  creating new forests, 144–158
  defined, 24
  deploying Server Core, 17
  enabling Remote Desktop, 69, 118
  enabling Windows Firewall remote administration, 70
  installing backup feature, 404–405
  installing DHCP server role, 189–190
  installing DNS servers, 213–218
  installing File Services, 246–247
  installing replica domain controllers, 160–165
  installing RODCs, 185–186
  installing roles/features, 78
  joining domains, 72
  manipulating roles/features, 88–89
  Network Level Authentication, 119–120
removing domain controllers, 165–169
setting local administrator password, 48–49
specifying computer names, 53
validating, 36
Windows SIM support, 21
APIPA (Automatic Private IP Addressing), 54
APIs (application programming interfaces), 5, 83
Appcmd.exe, 308–310
APPDATA environment variable, 104
Application Event log, 256
Application Experience (AeLookupSvc), 11
Application Management (Appmgmt), 11
application pools, 317–318
application programming interfaces (APIs), 5, 83
Application Server, 6
applications, 109, 316–320, 421–423
Applications And Services logs, 383
Appmgmt (Application Management), 11
archiving event logs, 389–390
ASP.NET, 7
asterisks (*), 53
At tool, 108
authentication
Kerberos, 172, 183–184, 214
Remote Desktop support, 68, 119–120
RODC considerations, 183–184
authorization, DHCP server role, 191, 196–197
Autochk tool, 256
automated installs, 28–30
Automatic Private IP Addressing (APIPA), 54
Automatic Updates
configuring using answer files, 61–62
configuring using command prompt, 60–61
Scregedit.wsf script, 60–61
B
background, command prompt, 102–103
Backup feature
changing focus, 129
executing, 405–406
installing, 404–405
package names, 81
Server Core installation option, 78
Backup Scheduling Wizard, 407–408
backups
configuring types, 408
DHCP server database, 208–209
full server recovery, 409–410
manual, 406–407, 412–413
overview, 403
performing data recovery, 409
restoring database from, 209–210
scheduling, 407–408, 410–412
system state, 415–416
viewing status, 413
bar (|), 103–104
Base Filtering Engine (BFE), 11
BAT file extension, 110
batch mode, 195, 203
BDD 2007, 44
BFE (Base Filtering Engine), 11
bindings, 312
BitLocker Drive Encryption
Remote Administration Tool, 81
supported optional features, 7, 9, 78, 81
BITS (Background Intelligence Transfer Service), 11, 360
BITS Server Extensions, 7
boot image, 26, 43
bridgehead servers, 184
Browser service (Computer Browser), 11
BugcheckOnCorrupt option, 258
C
caching, 184
caching-only DNS servers, 220–221
Calcs tool, 109
Calculator accessory, 5
capture image, 42
case sensitivity, 80, 86
Catalog file, 24
CD environment variable, 104
CEIP (Customer Experience Improvement Program)
additional information, 64
configuring with answer files, 65
configuring with command prompt, 64–65
participating in, 64–65
Certificate Propagation (CertPropSvc), 11
certificates, managing, 109
CertPropSvc (Certificate Propagation), 11
Certreq tool, 109
Certutil tool, 109
Change logon command, 124
Change tool, 110
child domains, 159–160
child partition, 322, 324
Chkdsk tool, 247, 256–257
Choose A Recover Tool dialog box, 410
Choose How to Restore The Backup dialog box, 410
Choose How to Restore The Backup dialog box, 410
classes
defined, 114
ListClasses.vbs script, 115–116
WMI support, 114–115
classic ASP Web server, 305
Cmd.exe. see command prompt (Cmd.exe)
CMDCMDLINE environment variable, 104
CMDEXTVERSION environment variable, 104
cmdkey command, 132–133, 268
CNAME resource record, 227
CNG Key Isolation (KeyIso), 12
COM (Component Object Model), 111
COM+ Event System (EventSystem), 12
COM+ System Application (COMSysApp), 11
command prompt (Cmd.exe)
  activating Windows, 65–66
  changing computer names, 52
  closing, 100
  collecting/analyzing performance data, 398–403
  command redirection, 103–104
  commands for common tasks, 107–110
  configuring Automatic Updates, 60–61
  configuring CEIP settings, 64–65
  configuring date/time settings, 58
  configuring regional/language settings, 59
  configuring TCP/IP settings, 53–56
  configuring Windows Error Reporting, 63
  customizing background, 102–103
  enablingRemote Desktop, 67–68
  enabling Windows Firewall remote administration, 69–70
  environment variables, 104–107
  increasing history buffer, 101
  increasing screen buffer, 101–102
  initial configuration, 47
  installing Backup feature, 404
  installing DHCP server role, 189
  installing DNS servers, 216–217
  installing File Services, 245–246
  joining domains, 71
  managing devices, 364–369
  managing DNS servers, 219–220
  managing local users/groups, 50–51
  managing Print Services, 284–285
  managing services, 357–363
  minimizing, 99
  nested, 97
  overview, 95
  parameter support, 98–99
  Remote Desktop support, 122–123
  running multiple command, 103
  scheduled backups, 410–412
  Server Core GUI support, 5
  setting local administrator password, 49
  simplifying cut-and-paste, 101
  starting, 95–99
  starting additional windows, 97
  viewing events from, 383–390
Compact tool, 109
Component Object Model (COM), 111
computer accounts
  deleting, 188
  managing, 178–179
Computer Browser (Browser service), 11
Computer Management, 129
computer names
  changing domain-joined computers, 52
  changing from command prompt, 52
  manipulating, 108
  restrictions, 51
  specifying in answer files, 53
COMPUTERNAME environment variable, 104
COMSPEC environment variable, 105
COMSysApp (COM+ System Application), 11
conditional forwarders, 235–236
configuration pass (Windows Setup)
  defined, 25
  phases, 25
configuration sets
  installs using network shares, 37
  unattended installs from, 32–37
Connection Manager Administration Kit, 7
Convert tool, 109
core servers, 184
Cross-File Replication, 7
Cryptographic Services (CryptSvc), 11
CryptSvc (Cryptographic Services), 11
Cscript.exe, 65
current directory, 95
Customer Experience Improvement Program (CEIP)
  additional information, 64
  configuring with answer files, 65
  configuring with command prompt, 64–65
  participating in, 64–65
cut-and-paste operation, 101

D
DAEMON tools, 22
Data Execution Protection (DEP), 324
data image, 34
data recovery
  performing, 409
  performing using Wbadmin tool, 413–415
  restoring database from backups, 209–210
Date And Time (Timedate.cpl)
  configuring settings, 58
  Server Core support, 5
date and time settings, 58
DATE environment variable, 105
Davis, Joseph, 57
dcdiag utility, 147–149, 174
dcomLaunch (DCOM Server Process Launcher), 11
dcpromo utility
  AdministratorPassword option, 166
  AllowDomainControllerReinstall option, 150
  AllowDomainReinstall option, 150
  ApplicationPartitionsToReplicate option, 150
  ChildName option, 150
  ConfirmGc option, 150
  CreateDNSDelegation option, 151
creating child domains, 159–160
creating domain trees, 158–159
creating forests, 144–158
CriticalReplicationOnly option, 151
DatabasePath option, 151
DelegatedAdmin option, 151
DemoteFSMO option, 166
dnsDelegationPassword option, 151, 166
dnsDelegationUserName option, 152, 166
dnsOnNetwork option, 152
DomainLevel option, 152
DomainNetBiosName option, 152
ForestLevel option, 153
functionality, 80
IgnoreIsLastDcInDomainMismatch option, 167
IgnoreIsLastDNSServerForZone option, 167
InstallDNS option, 153
installing AD DS, 143
installing DNS servers, 213–216
installing replica domain controllers, 160–165
installing RODCs, 185–186
IsLastDCInDomain option, 167
LogPath option, 153
NewDomain option, 154
NewDomainDNSName option, 154
ParentDomainDNSName option, 154
Password option, 154, 167
PasswordReplicationAllowed option, 154
PasswordReplicationDenied option, 155
RebootOnCompletion option, 155, 167
RebootOnSuccess option, 155, 168
RemoveApplicationPartitions option, 168
RemoveDNSDelegation option, 168
removing domain controllers, 165–169
ReplicaDomainDNSName option, 155
ReplicaOrNewDomain option, 155
ReplicationSourceDC option, 156
ReplicationSourcePath option, 156
RetainDCMetadata option, 168
SafeModeAdminPassword option, 156
SiteName option, 156
Syskey option, 157
SysVolPath option, 157
TransferIMRoleIfNeeded option, 157
UserDomain option, 157, 168
UserName option, 158, 168
debug logs, 170, 242
defrag tool, 109, 247, 258–259
delegation, 220
deployment from images, 37–40
deploying Windows AIK, 22–23
deployment from images, 37–40
installing from images, 37–40
manual installation, 18–20
Microsoft Development support, 44–45
unattended installs, 21–22
unattended installs from configuration sets, 32–37
unattended installs from DVDs, 31–32
Windows Deployment Services, 40–44
Deployment Workbench, 44–45
Desktop Experience, 7
device drivers. see drivers
Device Manager snap-in, 131, 369–371
devices
managing from command prompt, 364–369
managing with Device Manager snap-in, 369–371
DFS (Distributed File System)
functionality, 272
management tools, 272
role services supported, 272
Server Core installation option, 7
DFS Management console, 274, 276, 279
DFS namespaces
defined, 272
role support, 80
testing, 281
dlscmd tool, 4, 272, 276
dfsdiag tool, 272, 281
dfsr (DFS Replication), 7, 172, 272
dfsadmin command, 279
dfsutil tool
adding folder targets, 278
adding namespace servers, 275
creating domain-based namespace, 273–274
creating folders, 276–277
functionality, 272
DHCP (Dynamic Host Configuration Protocol)
changing focus, 129
configuring options, 201–203
configuring TCP/IP networking settings, 53
DNS dynamic update, 236–237
functionality, 189
reconciling scope, 211
resource records and, 220
Server Core installation option, 3, 15
DHCP Administrators group, 195
DHCP Client, 11
DHCP server role
authorizing, 191, 196–197
backing up database, 208–209
dumping configuration, 211
exporting configuration, 210
granting user privileges, 195–196
importing configuration, 210
installing, 86, 189–191
installing from answer files, 189–190
installing from command prompt, 189
loading configuration, 211
maintaining, 207–212
managing in batch mode, 195
managing scope, 199–207
managing using Netsh, 194
managing using RSAT, 192–194
modifying configuration, 197–199
monitoring, 211–212
removing, 191
restoring database, 209–210
role support, 77, 80, 92
Server Core installation option, 6
starting service, 190–191
troubleshooting, 211–212
uninstalling, 86
verifying installation, 86
viewing activity, 207
viewing scope statistics, 208
DHCP Users group, 195
Diagnostic Policy Service (DPS), 11
Diagnostic System Host (WdiSystemHost), 13–14
Dir command, 254, 263
dirty bit, 256
Disk Management snap-in, 132, 248
Diskpart tool
defined, 109, 247
managing disks/volumes, 248–252
managing RAID, 264
scripting commands, 253
Diskraid tool, 109, 247, 264–266
disks
managing, 248–252
tools for managing, 247
display settings, configuring, 73–74
Distributed File System (DFS), 7
Distributed Transaction Coordinator (MSDTC), 12
distribution shares, 34
DNS (Domain Name System)
AD DS support, 213
changing focus, 129
calendar name conventions, 51
DNS dynamic update, 236–237
RODC considerations, 184
Server Core installations, 6, 15
domain functional level
debugging logging, 242
displaying list of zones, 223–224
GNZ and, 239–240
installing from answer files, 217–218
installing from command prompt, 216–217
installing on domain controllers, 213–216
integrating WINS, 238–239
joining domains and, 71
maintaining, 240–242
managing from command prompt, 219–220
managing using RSAT, 218–219
master, 220, 236
monitoring, 241
Nslookup support, 243
primary, 220–221
removing, 218
role support, 77, 80, 92
secondary, 220, 222
Server Core installation considerations, 6, 15
specifying secondary, 55
troubleshooting, 241
DNS Client (Dnscache), 11
Dnscmd command
aging resource records, 238
configuring conditional forwarders, 235–236
configuring DNS servers, 220
configuring forwarders, 234–235
configuring GNZ, 239–240
configuring zone transfers, 236–237
creating resource records, 231–232
displaying list of resource records, 228–229
displaying list of zones, 223–224
displaying resource records for nodes, 231
DNS dynamic updates, 237
exporting resource record information, 229–230
functionality, 4
managing DNS servers, 218–220
modifying resource records, 232
scavenging resource records, 238, 241
Domain Admins group, 170–171, 177, 219
domain controllers. see also RODCs (Read-Only Domain Controllers)
demoting, 166–168
forced removals, 169
installing DNS servers, 213–216
installing replica, 160–165
invocation ID, 179
managing, 172–182
managing replication, 180–182
managing using command-line utilities, 174–175
managing using MMC, 172–174
preparing environment, 169–172
promoting, 146–158
removing, 165–169
verifying SRV resource records, 214–215
domain functional level, 172, 273
Domain Name System. see DNS (Domain Name System)
domain trees, 158–159
domain-based namespace, 273, 275

domains
  child, 159–160
  joining, 71–72, 108
  preparing existing, 171
  removing last domain controllers, 169
  removing replica domain controllers, 165–166
  RSAT support, 133–135
  Server Core installations, 128–132
  WinRS support, 126

DPS (Diagnostic Policy Service), 11
Driverquery tool, 109, 364–366
drivers
  displaying list, 365–366
  installing manually with Pnputil, 367–368
  managing, 109, 364
  obtaining for devices, 368–369
dsacls utility, 174
dsaddd utility
  functionality, 174
  managing computer accounts, 179
  managing organizational units, 180
  managing user accounts, 177
dsget utility, 175, 179
dsmgmt utility, 175
dsmod utility, 175, 178, 195
dsmove utility, 175, 180
Dsnccmd.exe command, 3
dsquery utility
  functionality, 175
  managing computer accounts, 178–179
  managing FSMO roles, 176
  managing organizational units, 180
dsrn utility, 175
DTC (Distributed Transaction Coordinator), 12
dynamic addressing, 56
Dynamic Host Configuration Protocol. see DHCP
  (Dynamic Host Configuration Protocol)

E
efficiency, 323–324
End User Licensing Agreement (EULA), 19, 26
  enlightened guest, 323
  enlightenments, 323
  Enterprise Admins group, 170–171
  Enterprise Virtual Array (EVA), 264
enumrating
  event log names, 383
  roles/features, 83–85
environment variables
  defined, 104
  defining new, 106
  displaying, 106
initialization considerations, 62
local, 104
predefined, 104–106
system, 104
usage considerations, 106–107
ERRORLEVEL environment variable, 105
EULA (End User Licensing Agreement), 19, 26
EVA (Enterprise Virtual Array), 264
event logs
  archiving, 389–390
  clearing, 389–390
  configuring event subscriptions, 391–397
  displaying status, 384
  DNS support, 241
  enumerating names, 383
  exporting, 389–390
  installation considerations, 12
  location, 382
  managing, 109
  querying for specific events, 385–389
  Sysprep tool support, 21
  viewing configuration, 384–385
  viewing events, 390
Event Viewer
  changing focus, 129
  enabling rule groups, 130
  event logging, 382
  viewing events, 390
EventSystem (COM+ Event System), 12
exFAT file system, 263
Explorer.exe (Windows Explorer desktop shell), 5
exporting
  DHCP server configuration, 210
  event logs, 389–390
  resource record information, 229–230
F
Failover Clustering
  package names, 81
  supported optional features, 7, 9, 78
Fast User Switching (FUS), 50
Fax Server, 6
Fc command, 358
FCRegSvc (Microsoft Fibre Channel Platform Registration Service), 12
features
  defined, 77
  enumerating, 83–85
  enumerating using Oclist.exe, 84–85
  enumerating using WMI, 85
  installing, 78–79, 109
  installing with dependencies, 87–88
  manipulating with Ocsetup, 86, 88–89
  overview, 77–78
  packages modifying, 79
  removing unneeded, 93–94
  unattended installation, 78, 89–92
Fibre Channel Platform Registration Service (FCRegSvc), 12
File Replication Service (FRS), 172, 246
File Services
  installing from answer files, 246–247
  installing from command prompt, 245–246
  role support, 77, 80, 92
  Server Core installation option, 6–7, 15
file systems
  creating symbolic links, 263
  displaying detailed information, 253
  displaying filters, 255–256
  formatting using exFAT, 263
  managing, 109
  tools for managing, 247
files
  managing, 109
  modifying ACLs, 259–263
  searching volumes for, 254–255
Filter Manager (Fltmc.exe), 247, 255
filters, file system, 255–256
Find command, 84–85
Flexible Single Master Operation roles. see FSMO (Flexible Single Master Operation) roles
Fltmc.exe (Filter Manager), 247, 255
folders
  adding targets, 278
  creating, 276–278
  modifying ACLs, 259–263
  replicating, 279–281
  searching volumes for, 254–255
  shared, 266–271
forest functional level, 172, 185
forests
  creating, 144–158
  preparing existing, 170
  preparing for RODCs, 184–185
  removing last domain controllers, 169
Format tool, 247, 264
forward lookup zones
  creating, 224–226
  defined, 222
  types, 223
Forwarded Events log, 383
forwarders
  conditional, 235–236
  configuring, 234–235
  defined, 221, 234
FQDN (fully qualified domain name), 196, 222, 313
FRS (File Replication Service), 172, 246
FSMO (Flexible Single Master Operation) roles
  functionality, 169
  managing, 176
  RODC limitations, 183–184
Fsutil tool
  checking for bugs, 258
  correcting volume corruption, 257–258
  displaying detailed file system information, 253
  displaying free space on volumes, 253
  functionality, 109, 247
  setting dirty bit on volume, 256
Full installation option
  architecture overview, 9
  driver support, 10–11
  overview, 3
  performance considerations, 14
  RSAT support, 134
  service footprint, 11–14
  supported optional features, 7–9
  supported server roles, 6–7
  upgrade constraints, 18
  WinRS requirements, 127
full server recovery, 409–410
fully qualified domain name (FQDN), 196, 222, 313
FUS (Fast User Switching), 50
G
global catalogs
  installing DNS servers, 214
  RODC considerations, 184–185
  globally unique identifier (GUID), 71, 179
  GlobalNames zone (GNZ), 239–240
  Gpresult tool, 109, 138
  gpsvc (Group Policy Client), 12
  Gpupdate tool, 109, 138
  graphical user interface. see GUI (graphical user interface)
  Group Policy
    additional information, 138
    configuring WER on domain-joined computers, 63
    configuring Windows Firewall, 131
    configuring WinRM, 128
    configuring WinRS, 128
    remote management support, 138–141
    supported optional features, 8
    tools supported, 109
    WMI filters and, 138–140
  Group Policy Client (gpsvc), 12
  guest operating systems, 337–338
  GUI (graphical user interface)
    DSN servers, 3
    remote management support, 136–138
    Server Core support, 3–6, 11
  GUID (globally unique identifier), 71, 179
H
hardware requirements, 17–18
Health Key and Certificate Management (hkmsvc), 12
HID (Human Interface Device), 323
hidserv (Human Interface Device Access), 12
history buffer, 101
hkmsvc (Health Key and Certificate Management), 12
HOMEDRIVE environment variable, 105
HOMEPATH environment variable, 105
HOMESHARE environment variable, 105
host header, 313
Hostname command, 52, 108
Howard, John, 327
HTML (Hypertext Markup Language), 5
HTML Help, 5
HTTP Logging role service
adding to server role, 87
installing, 87
Human Interface Device (HID), 323
Human Interface Device Access (hidserv), 12
Hyper-V
AD DS support, 348–352
creating snapshots, 342–344
creating virtual machines, 332–335
defined, 321
installing Integration Services, 341–342
installing role, 324–327
installing update package, 325–326
managing role, 327–344
managing virtual machines, 339–341, 344–347
role support, 77, 80, 92–93
Server Core installation option, 6–7, 15–16
Streaming Media Services support, 353–356
terminology, 321–324
troubleshooting role installation, 326–327
verifying role installation, 326
virtual network support, 331–332
Hyper-V Management console, 328–331
Hypertext Markup Language (HTML), 5
hypervisor, 322
Icacls tool, 109, 247, 259–263, 267
IIS (Internet Information Services). see also Web Server (IIS) role
limitations, 303
package dependencies, 82–83
IIS 7.0 components, 295, 304–305
IIS-ApplicationDevelopment package, 298
IIS-ASP package, 299
IIS-ASPNET package, 299
IIS-BasicAuthentication package, 300
IIS-CGI package, 299
IIS-ClientCertificateMappingAuthentication package, 301
IIS-CommonHttpFeatures package, 298
IIS-CustomLogging package, 300
IIS-DefaultDocument package, 299
IIS-Digest Authentication package, 301
IIS-DirectoryBrowsing package, 299
IIS-FTPManagement package, 302–303
IIS-FTPPublishingService package, 298
IIS-FTPServer package, 302
IIS-HealthAndDiagnostics package, 298
IIS-HttpCompressionDynamic package, 301
IIS-HttpCompressionStatic package, 301
IIS-HttpErrors package, 299
IIS-HttpRedirect package, 299
IIS-HttpTracing package, 300
IIS-IIS6ManagementCompatibility package, 302
IIS-IISCertificateMappingAuthentication package, 301
IIS-IPSecurity package, 301
IIS-ISAPIExtensions package, 300
IIS-ISAPIFilter package, 302
IIS-LegacyScripts package, 302
IIS-LegacySnapIn package, 302–303
IIS-LoggingLibraries package, 300
IIS-ManagementConsole package, 301, 303
IIS-ManagementScriptingTools package, 302
IIS-ManagementService package, 302–303
IIS-Metabase package, 302
IIS-NetFxExtensibility package, 299, 303
IIS-ODBCLogging package, 300
IIS-Performance package, 298
IIS-RequestFiltering package, 301
IIS-RequestMonitor package, 300
IIS-Security package, 298
IIS-ServerSideIncludes package, 300
IIS-StaticContent package, 299
IIS-URLAuthorization package, 301
IIS-WebServerManagementTools package, 298
IIS-WebServerRole package, 297
IIS-WindowsAuthentication package, 300
IIS-WMICompatibility package, 302
IISHTTPLogging package, 300
IKEEXT, 12
image groups, 42
images
installing from, 37–40
servicing, 79
ImageX, 21, 37–40
importing, DHCP server configuration, 210
initial configuration
activating Windows, 65–67
changing computer name, 51–53
configuring Automatic Updates, 60–62
configuring date/time settings, 58
configuring display settings, 73–74
configuring paging file, 72–73
configuring proxy server settings, 75–76
configuring regional/language settings, 59–60
configuring screen save timeout, 74–75
configuring TCP/IP networking settings, 53–57
configuring Windows Error Reporting, 62–64
date and time settings, 58
enabling Remote Desktop, 67–69
enabling Windows Firewall remote administration, 69–70
joining domains, 71–72
managing local users/groups, 49–51
participating in CEIP, 64–65
setting local administrator password, 47–49
Initial Configuration Tasks page, 78
initiate reconcile command, 211
install image, 26

K
Kerberos authentication
AED support, 172
installing DNS servers, 214
RODC considerations, 184
TGT support, 183
Key Management Service (KMS), 19
KeyIso (CNG Key Isolation), 12
KMS (Key Management Service), 19
KtmRm (KtmRm for Distributed Transaction Coordinator), 12

L
LanmanServer, 12
LanmanWorkstation, 12
LDAP (Lightweight Directory Access Protocol) AD LDS support, 348
installing DNS servers, 214
RODC considerations, 184
ldifde utility, 175
lease duration, configuring, 204–206
Lightweight Directory Access Protocol. see LDAP
Line Printer Daemon (LPD) service, 282
Link-Layer Topology Discovery Mapper (lltSvc), 12
ListClasses.vbs script, 115–116
ListNamespaces.vbs script, 113–114
ListProviders.vbs script, 111–112
lltSvc (Link-Layer Topology Discovery Mapper), 12
lmhosts (TCP/IP NetBIOS Helper), 12
local Administrator account, 47–49
local Administrator group, 50–51
Local Area Connection interface, 54
local environment variables, 104
local Group Policy, 140–141
local user account adding, 50
displaying, 50
managing from command prompt, 50–51
managing with answer files, 51
removing, 50
logical unit numbers (LUNs), 265
Logman tool, 108, 398
clogoff command, 108, 110, 124–125
LOGONSERVER environment variable, 105
lookup zone forward, 222–224
reverse, 222–223
LPD (Line Printer Daemon) service, 282
Lpq tool, 285
LPR Port Monitor, 8
Lpr tool, 285
LUNs (logical unit numbers), 265

M
MAC (media access control) address, 200
MAK (Multiple Activation Key), 19, 66
management information base (MIB), 207
manual backups, 406–407, 412–413
manual installations, 18–20
master DNS server, 220, 236
MDT (Microsoft Deployment Tool), 44–45
media access control (MAC) address, 200
Message Queuing, 8
MIB (management information base), 207
Microsoft Deployment Tool (MDT), 44–45
Microsoft Fibre Channel Platform Registration Service (FCRegSvc), 12
Microsoft iSCSI Initiator Service (MSiSCSI), 12
Microsoft Management Console. see MMC
Microsoft Software Shadow Copy Provider (swprv), 13
Microsoft Support Diagnostic Tool (Msdt.exe), 5
Microsoft System Installer, 79
Microsoft Update Standalone Package, 7
Microsoft Volume Licensing, 19
Mklink tool, 247, 263
MMC (Microsoft Management Console). see also specific snap-ins
  Active Directory Users and Computers, 71
  adding snap-ins, 129–131
  additional information, 176
  administering Server Core in domains, 128–132
  administering Server Core in workgroups, 132–133
  changing focus, 129
  enabling rule groups, 132
  managing domain controllers, 172–174
  Server Core interface element and, 5
  Server Manager console, 78
  Windows Deployment Services support, 40
monitoring. see performance monitoring
  monitors, configuring display settings, 73–74
More command, 85
Mountvol tool, 109
MpsSvc. see Windows Firewall (MpsSvc)
MSDTC (Distributed Transaction Coordinator), 12
Msg tool, 110, 124
msiexec.exe (Windows Installer)
  functionality, 109
  installation considerations, 12
  manipulating applications, 422
  manipulating packages, 79
  Server Core GUI support, 5
  uninstalling applications, 423
Msinfo32.exe (System Information), 5, 108
MSiSCSI (Microsoft iSCSI Initiator Service), 12
msiserver (Windows Installer), 12
Msstd.exe (Microsoft Support Diagnostic Tool), 5
Mstsc tool, 110
MSU file extension, 7, 353
Multipath IO
  package names, 81
  supported optional features, 8–9, 78
Multiple Activation Key (MAK), 19, 66
MX resource record, 227

N
namespace roots, 273
namespace servers, 275–276
Namespaces role service, 245
naming conventions
  additional information, 52
  case sensitivity, 80, 86
  computer names, 51
  package names, 80
napagent (Network Access Protection), 12
net accounts command, 97
net continue command, 108
net group command, 108
net localgroup command, 51, 108
net pause command, 108
net print command, 285, 294
net share command, 109, 266–269
net start command
  DHCP Server role, 191
  functionality, 108
  managing services, 357–359
net stop command, 108, 240, 357
net user command
  additional information, 51
  displaying local user accounts, 50
  functionality, 108
  managing user accounts, 178
  setting local administrator password, 49
netdom command
  joining domains, 71–72
  managing computer accounts, 179
  managing domain controllers, 175, 177
netdom join command, 108
netdom rename command, 52
netdom renamecomputer command, 52, 108
Netlogon, 12
netprofm (Network List Service), 12
netsh advfirewall command, 108, 123, 191
netsh command
  activating scope, 206
  adding IP address range to scope, 199–200
  backing up DHCP server database, 208–209
  configuring DHCP options, 201–203
  configuring lease duration, 204–206
  configuring proxy server settings, 75
  configuring scope using batch file, 203
  configuring TCP/IP networking settings, 53, 57
  creating new scope, 199
  creating reservations, 201
  deleting scope, 206–207
  DHCP server role, 191, 194–199
  dumping/loading DHCP configuration, 211
  enabling Windows Firewall remote administration, 69–70
  exporting/importing DHCP configuration, 210
  functionality, 4
  reconciling scope, 211
  restoring database from backups, 209–210
  viewing DHCP server activity, 207
  viewing scope statistics, 208
netsh interface command, 53, 108
netsh ipsec command, 108
netsh routing command, 108
Network Access Protection (napagent), 12
network adapters, 10
Network File System (NFS), 246, 271
network ID, 200
Network Level Authentication (NLA), 68, 119–120
Network List Service (netprofm), 12
Network Load Balancing
package names, 81
supported optional features, 8–9, 78
Network Location Awareness (NlaSvc), 12
Network Policy and Access Services, 6
network shares, 37
Network Store Interface Service (nsi), 12
New Folder dialog box, 276
New Virtual Machine Wizard, 333
NFS (Network File System), 246, 271
NLA (Network Level Authentication), 68, 119–120
NlaSvc (Network Location Awareness), 12
nodes, 231
Notepad (Notepad.exe), 5
NS resource record, 222, 227
nsi (Network Store Interface Service), 12
Nslookup command, 216, 241, 243
Ntbackup tool, 409
NTDS, 184
ntdsutil utility, 175–176
NTFS, Self-Healing, 257–258
NTLM authentication, 184
null string, 53
NUMBER_OF_PROCESSORS environment variable, 105

O
Oclist.exe
enumerating roles/features, 84
environment variable support, 107
functionality, 78, 83, 109
simplifying output with Find command, 84–85
verifying service installation, 282
Ocsetup.exe
additional information, 78, 80, 89
DHCP server role, 86
DNS servers, 216–217
functionality, 109
installing role services, 246
manipulating packages, 79
manipulating roles/features, 86, 88–89
overview, 78
removing roles/features, 93
OEM (Original Equipment Manufacturer), 19
Openfiles tool, 109
operating systems, guest, 337–338
Optimize Backup Performance dialog box, 408
organizational units, managing, 180
Original Equipment Manufacturer (OEM), 19
OS environment variable, 105
Out-of-Box Drivers folder, 35

P
Package Manager (Pkgmgr.exe)
functionality, 79, 109
installing IIS 7.0 components, 304
passing packages to, 79
removing roles/features, 93–94
uninstalling updates, 419
package names, 80
packages
defined, 79
dependency considerations, 82–83
installing, 79
overview, 79–80
removing, 79
Packages folder, 35
paging file, configuring, 72–73
Paint accessory, 5
parameters, command prompt, 98–99
parent partition, 322
parentheses (), 103
partitions, 322
pass-through disk, 333
passwords
local administrator, 49
replicating, 183, 186–188
resetting, 183
PATH environment variable, 105
PATHEXT environment variable, 105
PDC Emulator, 216
Peer Name Resolution Protocol, 8
percent sign (%), 106
Performance Logs & Alerts (pla), 12, 241
performance monitoring
analyzing data, 108
command prompt and, 398–403
DHCP server role, 211–212
DNS servers, 241
Reliability and Performance Monitor, 397–398
permissions
managing, 109
scheduled tasks and, 376
shared folders, 266, 268–269
PHP (PHP Hypertext Preprocessor), 306–307
pipe (|), 103
Pkgmgr.exe (Package Manager)
functionality, 79, 109
passing packages to, 79
removing roles/features, 93–94
pla (Performance Logs & Alerts), 12, 241
planning for installation
system requirements, 17–18
upgrade constraints, 18
PnP (Plug and Play) subsystem, 12
driver support, 10–11, 364
Pnputil tool, 109, 367–368
PolicyAgent (IPsec Policy Agent), 12
port numbers, 313
PowerShell Provider for IIS 7.0, 308
primary DNS servers
   AD DS-integrated, 220
   configuring, 221
   defined, 220
   standard, 220
primary zones, 222, 225
PrinBrm.exe tool, 285
print command, 285
print jobs, 294
Print Management console, 282–284, 289, 364
print queues, 294
Print Services
   configuring properties, 288
   installation requirements, 88
   managing from command prompt, 284–285
   managing from Print Management console, 282–284
   role support, 77, 80, 92
   Server Core installation option, 6, 15
printer drivers, 292–293
printers
   configuring properties, 291
   default, 292
   deleting, 289
   displaying settings, 291
   installing, 288
   viewing properties, 291
PrintUI.dll, 286–288
priority, 215
privileges, 195–196
Prncnfg.vbs script, 110, 285
Prndrvr.vbs script, 285
Prnjobs.vbs script, 285
Prnmngr.vbs script, 110, 285, 290
Prnport.vbs script, 285
Prnqctl.vbs script, 285
Process Explorer tool, 110
Process Monitor tool, 110
processes
   displaying, 372–374
   managing, 108, 371–376
   starting, 376
   stopping, 374–375
PROCESSOR_ARCHITECTURE environment variable, 105
PROCESSOR_IDENTIFIER environment variable, 105
PROCESSOR_LEVEL environment variable, 105
PROCESSOR_REVISION environment variable, 105
product keys
   additional information, 29
   installing, 19, 66
ProfSvc (User Profile Service), 13
PROMPT environment variable, 105
Protected Storage service, 13
Provision Storage Wizard, 271
proxy servers, 66, 75–76
PTE resource record, 227
Pubprn.vbs script, 285
Puputil command, 364
PXE server, 40
Q
Qappsrv tool, 110
Qprocess tool, 110
Query process command, 124
Query session command, 124
Query tool, 110
Query user command, 124
QWAVE (Quality Windows Audio Visual Experience), 8, 78, 81
Qwinsta tool, 110
R
RAID, managing, 264–266
RANDOM environment variable, 105
RDC (Remote Desktop Connection)
   additional information, 68
   authentication considerations, 68
   enabling Remote Desktop, 68
RDP (Remote Desktop Protocol), 120
Read-Only Domain Controllers. see RODCs
   (Read-Only Domain Controllers)
Recovery Wizard, 409
recursive queries, 234
redirection operators, 103–104
reg add command, 75
Reg Query command, 304
Regedt32.exe. see Registry Editor (Regedt32.exe)
Regional And Language Options (Intl.cpl), 5, 59–60
Registry Editor (Regedt32.exe)
   configuring display settings, 73–74
   DefaultSettings.BitsPerPel, 74
   DefaultSettings.VRefresh, 74
   DefaultSettings.XResolution, 73
   DefaultSettings.YResolution, 73
   functionality, 109
   KB322756 article, 73
   remote management support, 138
   ScreenSaveActive, 75
   ScreenSaverIsSecure, 75
   ScreenSaveTimeOut, 75
   SCRNSAVE.EXE, 75
   Server Core support, 5
Reliability and Performance Monitor
   collecting/analyzing data, 397–398
   enabling rule groups, 130
   functionality, 132
Relog tool, 108, 398
Remote Assistance, 8
Remote Desktop
  administering Server Core, 120–122
  authentication considerations, 68, 119–120
  enabling from answer files, 69, 118
  enabling from command prompt, 67–68
  enabling with Scregedit.wsf, 117–118
  functionality, 117
  installing DHCP server role, 189
  managing, 110
  publishing command interpreter, 122–123
  Scregedit.wsf script, 67–68
Remote Desktop Connection. see RDC (Remote Desktop Connection)
Remote Desktop Protocol (RDP), 120
Remote Differential Compression, 8
Remote Installation Services (RIS), 40
remote management. see also Remote Desktop;
  WinRS (Windows Remote Shell)
    administering Server Core in workgroups, 132–133
    Group Policy support, 138–141
    GUI tool support, 136–138
    MMC support, 128–132
    RSAT support, 133–136
    Windows PowerShell support, 141–142
Remote Procedure Call (RPC), 13
Remote Registry service, 13
Remote Server Administration Tools, 8
Removable Storage Manager
  package names, 81
  supported optional features, 8–9, 78
Repadmin command
  functionality, 164, 175
  managing computer accounts, 179
  managing replication, 180–182
replication
  folder, 279–281
  managing, 180–182
  password, 183, 186–188
  RODC considerations, 184
Replication role service, 246
reservations, 200–201
reset session command, 110
resource records. see also specific types of resource records
  aging, 238
  common types, 227–228
  creating, 231–232
  defined, 220
  displaying for nodes, 231
  displaying lists of, 228–229
  exporting information, 229–230
  information in, 227
  modifying, 232
  scavenging, 238, 241
  restoring database from backups, 209–210
Resultant Set of Policy Provider (RSoPProv), 13
reverse lookup zones
  creating, 226
  defined, 222
  types, 223
RIS (Remote Installation Services), 40
RO Partial Attributes Set (RO-PAS), 184
RO-PAS (RO Partial Attributes Set), 184
Robocopy command, 209, 247
RODCs (Read-Only Domain Controllers)
  additional information, 170, 172, 188
  defined, 182
  group membership caching, 184
  installing on Server Core, 185–186
  limitations, 183–184
  password replication, 183, 186–188
  preparing forests, 184–185
  resetting passwords, 183
roles
  corresponding package names, 80
  defined, 77
  enumerating, 83–85
  enumerating using Oclist.exe, 84–85
  enumerating using WMI, 85
  installing, 78–79, 109
  installing with dependencies, 87–88
  manipulating with Ocsetup, 86, 88–89
  overview, 77
  packages modifying, 79
  removing unneeded, 93–94
  Sysprep support, 92
  unattended installation, 78, 89–92
root hints, 221
root partition, 322
route command, 108
Routing and Remote Access Service (RRAS), 3
RPC (Remote Procedure Call), 13
RPC Over HTTP Proxy, 8
RpcsSs service (Remote Procedure Call), 13
RRAS (Routing and Remote Access Service), 3
RSAT (Remote Server Administration Tools)
  administering Server Core in domains, 133–135
  administering Server Core in workgroups, 136
  advantages in using, 128
  DHCP server role, 191–194
  DNS servers, 218–219, 221
  managing DNS servers, 218
  managing domain controllers, 173
  Share And Storage Management snap-in, 269
  Windows Server 2008 support, 134
  Windows Vista support, 134–135
RSoPProv (Resultant Set of Policy Provider), 13
Run registry key, 96
Rundll32.exe, 286–288, 291
Runcornce registry keys, 96
Rwinsta tool, 110
sacsvr (Special Administration Console Helper), 13
SamSs (Security Accounts Manager), 13
Sc tool
  configuring start mode for services, 362–363
  DHCP Server role, 190–191
  displaying service configuration information, 360–362
  functionality, 108–109
  managing devices, 364
  managing services, 357
SCardSvr (Smart Card), 13
scavenging resource records, 238, 241
Schedule service (Task Scheduler), 13
scheduled tasks
  creating new, 379
  managing, 380–382
  viewing, 377–378
scheduling backups, 407–408, 410–412
Schema Admins group, 170
Schtasks tool
  creating new tasks, 379
  deleting tasks, 380
  ending tasks, 380
  functionality, 108, 259
  managing tasks from command prompt, 376
  modifying tasks, 380
  running tasks, 380
  viewing scheduled tasks, 377–378
SCOM (Service Center Operations Manager), 382
scope
  activating, 206
  adding exclusions, 200
  adding IP address range, 199–200
  configuring DHCP options, 201–203
  configuring lease duration, 204–206
  creating new, 199
  creating reservations, 200–201
  creating using batch file, 203
  defined, 199
  deleting, 206–207
  network ID, 200
  reconciling, 211
  viewing, 206
  viewing statistics, 208
Scope Options dialog box, 204
SCPolicySvc (Smart Card Removal Policy), 13
screen buffer, command prompt, 101–102
screen savers, 74–75
Scrededit.wsf script
  configuring Automatic Updates, 60–61
  enabling Remote Desktop, 67–68, 117–118
  functionality, 108–110
  network level authentication support, 119
  SRV resource records, 215
scripts
  Diskpart commands, 253
  functionality, 110–111
  managing DHCP servers, 195
  WMI support, 111–116
  WMIC support, 116
  writing custom, 110
Secedit command, 48, 109
seclogn (Secondary Logon), 13
secondary DNS server, 220, 222
Secondary Logon (seclogn), 13
secondary zones, 222, 225
secure dynamic update, 220
Security Accounts Manager (SamSs), 13
security identifiers (SIDs), 21
SecurityLayer setting, 120
Select An Image dialog box, 26
Self-Healing NTFS, 257–258
SENS (System Event Notification Service), 13
Server Core installation
  activating, 20, 65–67
  architecture overview, 9
  benefits, 14–15
  driver support, 10–11
  Full installation option vs., 3
  GUI overview, 3–5
  installation options, 1–3
  interface elements and, 5
  MMC consoles in domains, 128–132
  non-usage scenarios, 16
  overview, 1
  possible usage scenarios, 15–16
  roles/features, 78
Server Manager console, 78, 129
Server Message Block (SMB), 271
Server Operators group, 219
ServerCEIPOptin.exe utility, 64
ServerManagerCmd.exe, 78
ServerWEROptin.exe utility, 63
Service Center Operations Manager (SCOM), 382
services. see also specific types of services
  configuring start mode, 362–363
  displaying configuration information, 360–362
  managing, 108
  managing from command prompt, 357–363
  Services snap-in, 363–364
  stopping/starting, 359–360
  Services snap-in, 130, 363–364
  servicing images, 79
SessionEnv (Terminal Services Configuration), 13
Set command, 108
Setup log, 383
Setx command, 107
Shadow tool, 110
Share And Storage Management snap-in, 269–271
shared folders
  configuring permissions, 268–269
  creating, 266–267
  managing, 269–271
  viewing, 267
Shared Folders snap-in, 130
shares
  deleting, 269
  managing, 109
show config command, 53
shutdown command, 52, 71, 108, 124
SIDs (security identifiers), 21
Sigverif tool, 109
Simple Network Management Protocol. see SNMP
(Simple Network Management Protocol)
slsvc (Software Licensing), 13
Smart Card
  SCardSvr service, 13
  SCPolicySvc service, 13
SMTP Server, 8
snapshots, 323, 342–344
SNMP (Simple Network Management Protocol)
  package names, 81
  supported optional features, 78
  viewing DHCP server activity, 207
SNMP Services, 8
SNMPTTRAP service, 13
SOA resource record, 222, 228, 233–234
SOEMS folder, 34
Software Shadow Copy Provider (swprv), 13
software updates
  installing, 416–420
  uninstalling, 419–420
  viewing, 418–419
Special Administration Console Helper (sacsvr), 13
SRV resource records, 214–216, 228
standalone namespace, 273
standard primary DNS server, 220
standard zones
  creating, 224–225
  defined, 222
Stanek, William R., 5, 107, 176, 218, 221, 357
Start command, 86
static addressing, 56, 71
Storage Manager for SANs, 8, 266
Streaming Media Services
  installing roles, 353–354
  managing, 354–356
  role support, 77, 80, 92
  Server Core installation option, 6–7, 15
  stub zone, 222, 225–226
SUA (Subsystem for Unix-based Applications), 8, 78, 81
subscriptions, 391, 396–397
Subsystem for Unix-based Applications. see SUA
(Subsystem for Unix-based Applications)
swprv (Microsoft Software Shadow Copy Provider), 13
symbolic links, 263
synthetic devices, 323
Sysinternals tools, 110, 201, 371
Sysprep (System Preparation Tool), 21, 92
system environment variables, 104
System Event log, 258
System Event Notification Service (SENS), 13
System Information (Msinfo32.exe), 5, 108
System Preparation Tool (Sysprep), 21
System Recovery Options dialog box, 410
system state, backing up, 415–416
SYSTEMDRIVE environment variable, 105
Systeminfo tool, 108–109
SYSTEMROOT environment variable, 105

T
Takeown tool, 109
Task Manager (Taskmgr.exe), 5, 108
Task Scheduler (Schedule)
  enabling rule groups, 130
  managing scheduled tasks, 380–382
  remote management support, 137
  Server Core installation option, 13
Taskkill tool, 108
Tasklist tool, 108, 372–374
tasks. see also scheduled tasks
  creating new, 379
  deleting, 380
  ending, 380
  managing, 108, 376–382
  running immediately, 380
TBS (TPM Base Services), 13
TCP/IP (Transmission Control Protocol/Internet Protocol)
  configuring settings from answer files, 56–57
  configuring settings from command prompt, 53–56
TCP/IP NetBIOS Helper (lmhosts), 12
Telnet client, 8, 78, 81
Telnet server, 8
TEMP environment variable, 105
Terminal Services
  displaying all sessions, 124
  managing, 110, 124–125
  Remote Desktop support, 122–123
  Server Core installation option, 6, 13
  SessionEnv service, 13
  UmRdpService service, 13
Terminal Services Configuration snap-in, 124
Terminal Services for Administration. see Remote Desktop
Terminal Services Manager snap-in, 124
testing DFS namespace, 281
TFTP (Trivial File Transfer Protocol), 43
TFTP Client, 8
TGT (ticket-granting-ticket), 183
ticket-granting-ticket (TGT), 183
TIME environment variable, 105
timeout.cpl (Date And Time), 5, 58
TLS (Transport Layer Security), 120
TMP environment variable, 105
TPM Base Services (TBS), 13
Tracerpt tool, 398
Transmission Control Protocol/Internet Protocol (TCP/IP), 53
Transport Layer Security (TLS), 120
Trivial File Transfer Protocol (TFTP), 43
troubleshooting
   DHCP server role, 211–212
   DNS servers, 241
   Hyper-V role installation, 326–327
TrustedInstaller (Windows Modules Installer), 13
Tscn tool, 110, 124
Tsdiscon tool, 110, 124
Tskill tool, 110, 124
Type command, 263
Typeperf tool, 108, 398

U
UAC (User Account Control), 174
UDDI Services, 6
UmRdpService (Terminal Services UserMode Port Redirector), 13
unattend files. see answer files
Unattend.chm (Unattended Windows Setup Reference Help file), 47
unattended installs
   creating answer files, 23–30, 47
   for roles/features, 78, 89–92
   from configuration sets, 32–37
   from DVDs, 31–32
   initial configuration, 47
   types, 21–22
Unattended Windows Setup Reference Help file (Unattend.chm), 47
UNC (Universal Naming Convention), 406
Understanding IPv6 (Davies), 57
undo disks, 323
Universal Naming Convention (UNC), 406
upgrade considerations, Server Core constraints, 18
USB flash drives, 263
User Account Control (UAC), 174
user accounts, 177–178
User Profile Service (ProfSvc), 13
User State Migration Tool, 45
USERDOMAIN environment variable, 106
UserMode Port Redirector (UmRdpService), 13
USERNAME environment variable, 106
USERPROFILE environment variable, 106
V
validating answer files, 36
VBS file extension, 36
VBS file extension, 36
VBScript, 110
vds (Virtual Disk), 13
VDS hardware providers, 264
VGA (Video Graphics Array), 10
virtual directories, 315
Virtual Disk (vds), 13
virtual hard disk, 333
virtual machines
   configuring settings, 335–337
   creating, 332–335
   defined, 321–322, 324
   managing, 339–341
   managing using PowerShell, 347
   managing using WMI, 344–347
virtual networks, 331–332
virtualization, 321
VLSC (Volume Licensing Service Center), 19
Volodarsky, Mike, 308
Volume Activation, 20
Volume Licensing Service Center (VLSC), 19
Volume Shadow Copy (VSS), 13, 109
volumes
   checking for corruption, 256–257
   correcting corruption, 257–258
   defragmenting, 258–259
   displaying free space, 253
   managing, 248–252, 269–271
   searching for files/folders, 254–255
   setting dirty bit, 256
VSS (Volume Shadow Copy), 13, 109
Vssadmin tool, 109

W
W32Time (Windows Time), 13
Waik.chm (Windows AIK User’s Guide), 20–21
WAS (Windows Activation Service)
   installing roles/features, 87–89
   Web Server role and, 297–298
   WAS-ConfigurationAPI package, 302–303
   WAS-NetFxEnvironment package, 302–303
   WAS-ProcessModel package, 302
Wbadmin command
   backing up system state, 415–416
   managing scheduled backups, 410–412
   performing manual backups, 412–413
   performing recovery, 413–415
   scheduling backups, 408
   viewing status of backup operations, 413
WcsPlugInService (Windows Color System), 13
WdServiceHost (Diagnostic Service Host), 13
WdSystemHost (Diagnostic System Host), 14
WDSUTIL utility, 40–41
Web applications, 109, 316–320, 421–423
Web Server (IIS) role
component categories, 297–298
components and dependencies, 295–297
creating application pools, 317–318
creating virtual directories, 315
creating Web applications, 316–317
creating Web sites, 312–314
defined, 295
installing, 87, 303–307
installing from answer file, 307
isolating applications, 318
managing, 308
managing application pools, 319–320
role support, 77, 80, 92
Server Core installation option, 6–7, 15
starting/stopping Web sites, 314–315
verifying default Web sites, 310–312
Web sites
creating, 312–314
starting/stopping, 314–315
verifying default, 310–312
Wecsvc (Windows Event Collector), 14
Wcutil command, 396–397
weight, 215
WER (Windows Error Reporting)
configuring on domain-joined computers, 63
configuring with answer files, 64
configuring with command prompt, 63
functionality, 62–63
Wevtutil tool
functionality, 109
viewing event logs, 382
viewing events from command prompt, 383–390
enumerating event log names, 383
Whoami tool, 108
WIM file extension, 24, 43
WINDIR environment variable, 106
Windows Activation Service. see WAS (Windows Activation Service)
Windows AIK
Deployment Workbench support, 45
installing, 22–23
unattended installs, 21–22
Windows Deployment Services support, 40
Windows AIK User’s Guide. see Waik.chm
(Windows AIK User’s Guide)
Windows Color System (WcsPlugInService), 13
Windows Command Reference, 51, 107
Windows Command-Line Administrator’s Pocket Consultant (Stanek), 5, 107, 176
Windows Deployment Services
additional information, 44
deploying Server Core, 40–44
Server Core installation option, 6
Windows Error Reporting (WER)
configuring with command prompt, 63
functionality, 62–63
Windows Event Collector (Wecsvc), 14
Windows Explorer desktop shell (Explorer.exe)
managing file systems, 248
remote management support, 137
Server Core GUI support, 5
Windows Firewall (MpsSvc)
administering remotely, 118, 123
configuring, 108, 131
installation considerations, 12
WinRM requirements, 127
Windows Firewall with Advanced Security snap-in
administering remotely, 69–70, 129–131, 135
changing focus, 129
enabling rule groups, 130
Windows Imaging files, 24
Windows Installer. see msiexec.exe (Windows Installer)
Windows Internal Database, 8
Windows Mail, 5
Windows Management Instrumentation. see WMI
(Windows Management Instrumentation)
Windows Management Instrumentation
Command-line. see WMIC (Windows Management Instrumentation Command-line)
Windows Media Audio (WMA), 353
Windows Media Player, 5
Windows Media Services
applying update package, 353–355
Remote Server Administration Tools snap-in, 355–356
starting, 354
Windows Modules Installer (TrustedInstaller), 13
Windows PE (Preinstallation Environment)
additional information, 20
manual installation and, 20
overview, 21
Windows Deployment Services support, 40
Windows PowerShell
additional information, 142
managing virtual machines, 347
remote management support, 141–142
restrictions, 111
Server Core GUI support, 6
supported optional features, 8
Windows Preinstallation Environment. see
Windows PE (Preinstallation Environment)
Windows Product Activation Service, 8
Windows Remote Management (WinRM), 14
Windows Remote Shell. see WinRS (Windows Remote Shell)
Windows Server 2008
Bluetooth technology and, 289
domain functional level, 172
forest functional level, 172
RSAT support, 134
verifying Hyper-V support, 325
Windows Server 2008 Administrator’s Pocket Consultant (Stanek), 218, 221, 357
Windows Server 2008 Product Roadmap, 18
Windows Server 2008 Technical Library, 5
Windows Server Backup Features, 8
Windows Setup, 25
Windows Side-by-Side (WinSxS) directory, 17
Windows SIM (Windows System Image Manager) activating Windows, 67
additional information, 47
Answer File pane, 23
automating prompts, 44
configuring CEIP settings, 65
configuring screen saver settings, 75
configuring TCP/IP settings, 56–57
creating answer files, 23–24
Distribution Share pane, 23
installing DHCP server role, 189
installing DNS servers, 217
installing File Services, 246
installing roles/features, 89
joining domains, 72
Messages pane, 23
overview, 21
Properties pane, 23
Windows Image pane, 23
Windows System Resource Manager, 8
Windows Time (W32Time), 13
Windows Update (wuauserv), 14
Windows Vista, 134–135
WinHttp Web Proxy Auto-Discovery Service (WinHttpAutoProxySvc), 14
WinHttpAutoProxySvc (WinHttp Web Proxy Auto-Discovery Service), 14
Winmgmt (Windows Management Instrumentation), 14
WinRE, 409
WinRM (Windows Remote Management) additional information, 126
configuring, 125–126
configuring with Group Policy, 128
domain controller support, 175
Server Core installation option, 14
usage requirements, 127
WinRS (Windows Remote Shell) additional information, 126
administering in domains, 126
administering in workgroups, 126–127
configuring WinRM, 125–126
configuring with Group Policy, 128
creating reservations, 201
enabling Remote Desktop, 118
functionality, 125
managing domain controllers, 174
usage requirements, 127
WINS Server
integrating DNS servers, 238–239
package names, 81
supported optional features, 8, 78
WinSxS (Windows Side-by-Side) directory, 17
Wireless LAN Service, 8
WMA (Windows Media Audio), 353
WMI (Windows Management Instrumentation) administering Server Core with Group Policy, 138–140
configuring roles/features, 85
managing virtual machines, 344–347
script support, 110–116
Server Core GUI support, 6
Server Core installations, 128
Windows PowerShell support, 141
Winmgmt service, 14
WMI namespace, 113–114
WMI Performance Adapter (wmiApSrv), 14
WMI providers, 111–112
WMI Query Language (WQL), 139
wmiApSrv (WMI Performance Adapter), 14
WMIC (Windows Management Instrumentation Command-line)
configuring paging file, 72
script support, 116
viewing installed applications, 422
viewing installed updates, 418–419
Wordpad, 5
workgroups
administering Server Core, 132–133, 136
WinRS support, 126–127
WQL (WMI Query Language), 139
WS-Management, 14, 125
WSF file extension, 110
Wuaclt tool, 109, 416
wuauserv (Windows Update), 14
Wusa tool, 109

Z
zone files, 220
zone transfers
configuring, 236–237
defined, 220
zones, see also specific types of zones defined, 220
deleting, 226–227
displaying list of resource records, 228–229
displaying list on DNS servers, 223–224
exporting resource record information, 229–230
pausing/resuming, 241