Internet Information Services (IIS) 7.0

William R. Stanek
Author and Series Editor

Administrator's Pocket Consultant
Internet Information Services (IIS) 7.0 Administrator’s Pocket Consultant

William R. Stanek
To my wife and children for their love, their support, and their extraordinary ability to put up with the clackety-clackety of my keyboard.
Contents at a Glance

1  IIS 7.0 Administration Overview ................................................. 1
2  Deploying IIS 7.0 in the Enterprise ........................................... 23
3  Core IIS 7.0 Administration ..................................................... 59
4  Managing IIS 7.0 from the Command Line ................................. 85
5  Managing Global IIS Configuration ............................................ 107
6  Configuring Web Sites and Directories ....................................... 135
7  Customizing Web Server Content .............................................. 173
8  Running IIS Applications ........................................................... 209
9  Managing Applications, Application Pools, and Worker Processes. ......................................................... 251
10 Managing Web Server Security .................................................... 291
11 Managing Active Directory Certificate Services and SSL ............. 323
12 Performance Tuning, Monitoring, and Tracing ............................ 349
13 Tracking User Access and Logging .......................................... 385
14 IIS Backup and Recovery .......................................................... 411
Appendix  Comprehensive IIS 7.0 Module and Schema Reference ...... 429
# Table of Contents

*Introduction* ............................................. xxii

Who Is This Book For? ................................. xxiii

How This Book Is Organized .......................... xxiv

Conventions Used in This Book ...................... xxv

Other Resources ........................................ xxi

Support ................................................... xxiv

1  IIS 7.0 Administration Overview .................... 1

   Working with IIS 7.0: What You Need to Know Right Now .... 1

   Introducing IIS 7.0 Configuration Architecture .............. 4

      IIS 7.0 Configuration Schema .......................... 4

      IIS 7.0 Global Configuration System ..................... 8

   IIS 7.0 and Your Hardware ............................ 13

   IIS 7.0 Editions and Windows .......................... 15

   Web Administration Tools and Techniques .................... 16

      Managing Resources by Using Key Administration Tools .... 16

      Web Administration Techniques ........................ 17

2 Deploying IIS 7.0 in the Enterprise .................... 23

   IIS 7.0 Protocols ..................................... 23

      HTTP and SSL ........................................ 23

      FTP .................................................. 24

      SMTP ................................................. 26

   IIS 7.0 Roles .......................................... 26

   Navigating the IIS 7.0 Role Services and Features .......... 32

      Role Services for Application Servers .................... 33

      Role Services for Windows Desktops and Web Servers .... 36

      Role Services for Servers Running SharePoint Services ... 46

   Setting Up IIS 7.0 .................................... 47

   Installing Application Servers .......................... 47

   Installing Web Servers .................................. 49

---

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](http://www.microsoft.com/learning/booksurvey)
## Table of Contents

### Core IIS 7.0 Administration

- Installing Windows SharePoint Services .................................. 51
- Adding or Removing Web Server Features on Windows Vista .......... 53
- Managing Installed Roles and Role Services ............................. 54
- Viewing Configured Roles and Role Services .............................. 54
- Adding or Removing Roles on Servers .................................... 56
- Viewing and Modifying Role Services on Servers ......................... 57

### 3 Core IIS 7.0 Administration

- Working with IIS and URLs .................................................. 59
- Understanding the Core IIS Architecture ................................ 62
- Working with Web Sites ...................................................... 62
- Working with Web Applications and Virtual Directories ................. 62
- Controlling Access to Servers, Sites, and Applications ................. 63
- Understanding the Services and Processing Architecture ............... 64
- Essential IIS Services and Processes .................................... 65
- IIS Worker Process Isolation Mode ....................................... 65
- Understanding and Using IIS Applications ............................... 68
- Understanding and Using ASP.NET Applications ........................ 69
- Managing IIS Servers: The Essentials .................................... 72
- Using Internet Information Services (IIS) Manager ....................... 72
- Enabling and Configuring Remote Administration ......................... 74
- Starting, Stopping, and Restarting All Internet Services ............... 76
- Managing Individual Resources in IIS Manager ......................... 78
- Rebooting IIS Servers ...................................................... 79

### 4 Managing IIS 7.0 from the Command Line

- Using the Windows PowerShell ............................................. 85
- Introducing the Windows PowerShell ...................................... 85
- Running and Using Windows PowerShell .................................. 86
- Running and Using Cmdlets ................................................. 87
- Running and Using Other Commands and Utilities ....................... 89
- Working with Cmdlets ....................................................... 89
- Using Windows PowerShell Cmdlets ...................................... 89
- Using Cmdlet Parameters ................................................... 91
- Understanding Cmdlet Errors .............................................. 91
Using Cmdlet Aliases ........................................ 92
Using Cmdlets with IIS ..................................... 93
Using the IIS Command-Line Administration Tool .......... 95
  Running and Using the IIS Command Line Administration Tool ........................................ 95
  Working with the IIS Command Line Administration Tool ........................................ 97
Working with IIS Commands .................................. 98
  Using Configuration Management Commands ................. 98
  Using Module Management Commands ...................... 100
  Using Site Management Commands ......................... 101
  Using Application Pool Management Commands .......... 102
  Using Application Management Commands .................. 103
  Using Virtual Directory Management Commands .......... 104
  Using Utility Commands .................................. 105

5 Managing Global IIS Configuration ..................... 107
  Understanding Configuration Levels and Global Configuration ........................................ 107
  Managing Configuration Sections ............................ 112
    Working with Configuration Sections ......................... 112
    Determining Settings for a Configuration Section ........ 113
    Modifying Settings for a Configuration Section ............ 115
    Locking and Unlocking Configuration Sections .............. 116
    Clearing and Resetting Configuration Sections ............. 116
  Extending IIS with Modules ................................ 117
    Controlling Native Modules through the Configuration Files ........................................ 118
    Controlling Managed Modules through the Configuration Files ........................................ 119
    Controlling Managed Handlers through the Configuration Files ....................................... 120
    Using the Configuration and Schema Files to Install Non-Standard Extension Modules ......... 122
  Managing Modules ........................................... 124
    Viewing Installed Native and Managed Modules ............. 124
    Installing Native Modules .................................. 125
    Enabling Native Modules ................................... 126
    Enabling Managed Modules ................................ 128
    Editing Native and Managed Module Configurations ......... 129
    Disabling Native and Managed Modules ..................... 130
    Uninstalling Native Modules ............................... 131
Table of Contents

Sharing Global Configuration ........................................... 131
Working with Shared Configurations .............................. 132
Exporting and Sharing Global Configuration ................. 132

6 Configuring Web Sites and Directories ......................... 135
Web Site Naming and Identification ............................ 135
Understanding IP Addresses and Name Resolution .......... 135
Understanding Web Site Identifiers ............................. 136
Hosting Multiple Sites on a Single Server ...................... 137
Checking the Computer Name and IP Address of Servers .... 140
Examining Site Configuration ..................................... 141
Creating Web Sites ..................................................... 143
Creating a Web Site: The Essentials ......................... 144
Creating an Unsecured Web Site ................................ 145
Creating a Secured Web Site ...................................... 147
Managing Web Sites and Their Properties ....................... 149
Working with Sites in IIS Manager ............................. 149
Configuring a Site's Application Pool and Home Directory ......................................................... 151
Configuring Ports, IP Addresses, and Host Names Used by Web Sites ........................................................... 153
Restricting Incoming Connections and Setting Time-Out Values ................................................................. 155
Configuring HTTP Keep-Alives .................................... 158
Configuring Access Permissions in IIS Manager .............. 159
Managing a Site's Numeric Identifier and AutoStart State ................................................................. 160
Deleting Sites .............................................................. 162
Creating Directories ....................................................... 162
Understanding Physical and Virtual Directory Structures 163
Examining Virtual Directory Configuration .................... 163
Creating Physical Directories ...................................... 165
Creating Virtual Directories ........................................ 165
Managing Directories and Their Properties ..................... 167
Enabling or Disabling Directory Browsing ...................... 167
Modifying Directory Properties .................................. 169
Renaming Directories ................................................ 169
Changing Virtual Directory Paths, Logon Methods, and More .............................................................. 170
Deleting Directories ..................................................... 171
# Customizing Web Server Content

- Managing Web Content
- Opening and Browsing Files
- Modifying the IIS Properties of Files
- Renaming Files
- Deleting Files
- Redirecting Browser Requests
- Redirecting Requests to Other Directories or Web Sites
- Redirecting All Requests to Another Web Site
- Redirecting Requests to Applications
- Customizing Browser Redirection
- Configuring Default Documents
- Configuring Document Footers
- Configuring Included Files
- Using Content Expiration and Preventing Browser Caching
- Using Custom HTTP Headers
- Using Content Ratings and Privacy Policies
- Improving Performance with Compression
- Configuring Content Compression for an Entire Server
- Enabling or Disabling Content Compression for Sites and Directories
- Customizing Web Server Error Messages
- Understanding Status Codes and Error Messages
- Managing Custom Error Settings
- Using MIME and Configuring Custom File Types
- Understanding MIME
- Viewing and Configuring MIME Types
- Additional Customization Tips
- Using Update Sites to Manage Outages
- Using Jump Pages for Advertising
- Handling 404 Errors and Preventing Dead Ends

# Running IIS Applications

- Managing ISAPI and CGI Application Settings
- Understanding ISAPI Applications
- Configuring ISAPI and CGI Restrictions
- Configuring ISAPI Filters
- Configuring CGI Settings
Table of Contents

Managing ASP Settings .................................................. 215
  Controlling ASP Behavior ........................................... 216
  Customizing Request Handling for ASP ............................ 218
  Optimizing Caching for ASP ......................................... 220
  Customizing COM+ Execution for ASP ............................... 221
  Configuring Session State for ASP ................................. 223
  Configuring Debugging and Error Handling for ASP .......... 224
Managing ASP.NET Settings .............................................. 226
  Configuring Session State Settings for ASP.NET .............. 227
  Configuring SMTP E-Mail Settings ................................. 231
  Configuring Key/Value Pairs for ASP.NET Applications ........ 233
  Configuring Settings for ASP.NET Pages and Controls ....... 234
  Connecting to Data Sources ...................................... 237
Managing .NET Framework Settings ................................... 240
  Configuring .NET Providers ......................................... 240
  Configuring .NET Trust Levels ..................................... 243
  Configuring .NET Profiles .......................................... 244
  Configuring .NET Roles ............................................... 245
  Configuring .NET Users .............................................. 246
  Configuring .NET Compilation ...................................... 247
  Configuring .NET Globalization .................................... 249

9 Managing Applications, Application Pools, and Worker Processes .............................................. 251
  Defining Custom Applications ....................................... 251
Managing Custom IIS Applications .................................... 253
  Viewing Applications ................................................... 253
  Configuring Default Settings for New Applications ........... 254
Creating Applications .................................................... 256
Converting Existing Directories to Applications ................. 258
Changing Application Settings ........................................ 258
Configuring Output Caching for Applications ..................... 259
Deleting IIS Applications ................................................ 263
Managing ASP.NET and the .NET Framework ......................... 264
  Installing ASP.NET and the .NET Framework ..................... 264
Deploying ASP.NET Applications ...................................... 266
Uninstalling .NET Versions ............................................. 266
Working with Application Pools ...................................... 267
Viewing Application Pools ............................................. 267
Configuring Default Settings for New Application Pools ...... 269
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Application Pools</td>
<td>273</td>
</tr>
<tr>
<td>Changing Application Pool Settings</td>
<td>275</td>
</tr>
<tr>
<td>Assigning Applications to Application Pools</td>
<td>276</td>
</tr>
<tr>
<td>Configuring Application Pool Identities</td>
<td>277</td>
</tr>
<tr>
<td>Starting, Stopping, and Recycling Worker Processes Manually</td>
<td>277</td>
</tr>
<tr>
<td>Configuring Multiple Worker Processes for Application Pools</td>
<td>281</td>
</tr>
<tr>
<td>Configuring Worker Process Recycling</td>
<td>282</td>
</tr>
<tr>
<td>Recycling Automatically by Time and Number of Requests</td>
<td>283</td>
</tr>
<tr>
<td>Recycling Automatically by Memory Usage</td>
<td>284</td>
</tr>
<tr>
<td>Maintaining Application Health and Performance</td>
<td>284</td>
</tr>
<tr>
<td>Configuring CPU Monitoring</td>
<td>285</td>
</tr>
<tr>
<td>Configuring Failure Detection and Recovery</td>
<td>286</td>
</tr>
<tr>
<td>Shutting Down Idle Worker Processes</td>
<td>287</td>
</tr>
<tr>
<td>Limiting Request Queues</td>
<td>288</td>
</tr>
<tr>
<td>Deleting IIS Application Pools</td>
<td>289</td>
</tr>
<tr>
<td>10 Managing Web Server Security</td>
<td>291</td>
</tr>
<tr>
<td>Managing Windows Security</td>
<td>291</td>
</tr>
<tr>
<td>Working with User and Group Accounts</td>
<td>292</td>
</tr>
<tr>
<td>IIS User and Group Essentials</td>
<td>292</td>
</tr>
<tr>
<td>Managing the IIS Service Logon Accounts</td>
<td>293</td>
</tr>
<tr>
<td>Managing the Internet Guest Account</td>
<td>295</td>
</tr>
<tr>
<td>Working with File and Folder Permissions</td>
<td>295</td>
</tr>
<tr>
<td>Working with Group Policies</td>
<td>299</td>
</tr>
<tr>
<td>Managing IIS Security</td>
<td>305</td>
</tr>
<tr>
<td>Configuring Handler Mappings for Applications</td>
<td>305</td>
</tr>
<tr>
<td>Setting Authentication Modes</td>
<td>309</td>
</tr>
<tr>
<td>Setting Authorization Rules for Application Access</td>
<td>313</td>
</tr>
<tr>
<td>Configuring IPv4 Address and Domain Name Restrictions</td>
<td>315</td>
</tr>
<tr>
<td>Managing Feature Delegation and Remote Administration</td>
<td>318</td>
</tr>
<tr>
<td>11 Managing Active Directory Certificate Services and SSL</td>
<td>323</td>
</tr>
<tr>
<td>Understanding SSL</td>
<td>323</td>
</tr>
<tr>
<td>Using SSL Encryption</td>
<td>323</td>
</tr>
<tr>
<td>Using SSL Certificates</td>
<td>325</td>
</tr>
<tr>
<td>Understanding SSL Encryption Strength</td>
<td>326</td>
</tr>
</tbody>
</table>
### Table of Contents

12 Performance Tuning, Monitoring, and Tracing ................................................. 349

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working with Active Directory Certificate Services</td>
<td>327</td>
</tr>
<tr>
<td>Understanding Active Directory Certificate Services</td>
<td>327</td>
</tr>
<tr>
<td>Installing Active Directory Certificate Services</td>
<td>329</td>
</tr>
<tr>
<td>Accessing Certificate Services in a Browser</td>
<td>330</td>
</tr>
<tr>
<td>Starting and Stopping Certificate Services</td>
<td>331</td>
</tr>
<tr>
<td>Backing Up and Restoring the CA</td>
<td>332</td>
</tr>
<tr>
<td>Configuring Certificate Request Processing</td>
<td>334</td>
</tr>
<tr>
<td>Approving and Declining Pending Certificate Requests</td>
<td>335</td>
</tr>
<tr>
<td>Generating Certificates Manually in the Certification Authority Snap-In</td>
<td>336</td>
</tr>
<tr>
<td>Revoking Certificates</td>
<td>336</td>
</tr>
<tr>
<td>Reviewing and Renewing the Root CA Certificate</td>
<td>337</td>
</tr>
<tr>
<td>Creating and Installing Certificates</td>
<td>338</td>
</tr>
<tr>
<td>Creating Certificate Requests</td>
<td>338</td>
</tr>
<tr>
<td>Submitting Certificate Requests to Third-Party Authorities</td>
<td>340</td>
</tr>
<tr>
<td>Submitting Certificate Requests to Certificate Services</td>
<td>342</td>
</tr>
<tr>
<td>Processing Pending Requests and Installing Site Certificates</td>
<td>343</td>
</tr>
<tr>
<td>Working with SSL</td>
<td>343</td>
</tr>
<tr>
<td>Configuring SSL Ports</td>
<td>343</td>
</tr>
<tr>
<td>Adding the CA Certificate to the Client Browser's Root Store</td>
<td>344</td>
</tr>
<tr>
<td>Confirming that SSL is Correctly Enabled</td>
<td>345</td>
</tr>
<tr>
<td>Resolving SSL Problems</td>
<td>346</td>
</tr>
<tr>
<td>Ignoring, Accepting, and Requiring Client Certificates</td>
<td>346</td>
</tr>
<tr>
<td>Requiring SSL for All Communications</td>
<td>347</td>
</tr>
<tr>
<td>Monitoring IIS Performance and Activity</td>
<td>349</td>
</tr>
<tr>
<td>Why Monitor IIS?</td>
<td>349</td>
</tr>
<tr>
<td>Getting Ready to Monitor</td>
<td>350</td>
</tr>
<tr>
<td>Detecting and Resolving IIS Errors</td>
<td>351</td>
</tr>
<tr>
<td>Examining the Access Logs</td>
<td>351</td>
</tr>
<tr>
<td>Examining the Windows Event Logs</td>
<td>353</td>
</tr>
<tr>
<td>Examining the Trace Logs</td>
<td>357</td>
</tr>
<tr>
<td>Monitoring IIS Performance and Reliability</td>
<td>365</td>
</tr>
<tr>
<td>Using the Reliability And Performance Console</td>
<td>365</td>
</tr>
<tr>
<td>Choosing Counters to Monitor</td>
<td>369</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>xv</td>
</tr>
<tr>
<td>-------------------</td>
<td>----</td>
</tr>
<tr>
<td>Tuning Web Server Performance</td>
<td>371</td>
</tr>
<tr>
<td>Monitoring and Tuning Memory Usage</td>
<td>371</td>
</tr>
<tr>
<td>Monitoring and Tuning Processor Usage</td>
<td>374</td>
</tr>
<tr>
<td>Monitoring and Tuning Disk I/O</td>
<td>375</td>
</tr>
<tr>
<td>Monitoring and Tuning Network Bandwidth and Connectivity</td>
<td>376</td>
</tr>
<tr>
<td>Strategies for Improving IIS Performance</td>
<td>379</td>
</tr>
<tr>
<td>Removing Unnecessary Applications and Services</td>
<td>379</td>
</tr>
<tr>
<td>Optimizing Content Usage</td>
<td>379</td>
</tr>
<tr>
<td>Optimizing ISAPI, ASP, and ASP.NET Applications</td>
<td>381</td>
</tr>
<tr>
<td>Optimizing IIS Caching, Queuing, and Pooling</td>
<td>382</td>
</tr>
<tr>
<td>13 Tracking User Access and Logging</td>
<td>385</td>
</tr>
<tr>
<td>Tracking Statistics: The Big Picture</td>
<td>385</td>
</tr>
<tr>
<td>Working with the NCSA Common Log File Format</td>
<td>387</td>
</tr>
<tr>
<td>Working with the Microsoft IIS Log File Format</td>
<td>391</td>
</tr>
<tr>
<td>Working with the W3C Extended Log File Format</td>
<td>393</td>
</tr>
<tr>
<td>Working with ODBC Logging</td>
<td>396</td>
</tr>
<tr>
<td>Working with Centralized Binary Logging</td>
<td>397</td>
</tr>
<tr>
<td>Understanding Logging</td>
<td>398</td>
</tr>
<tr>
<td>Configuring Logging</td>
<td>400</td>
</tr>
<tr>
<td>Configuring Per-Server or Per-Site Logging</td>
<td>400</td>
</tr>
<tr>
<td>Configuring the NCSA Common Log File Format</td>
<td>401</td>
</tr>
<tr>
<td>Configuring Microsoft IIS Log File Format</td>
<td>402</td>
</tr>
<tr>
<td>Configuring W3C Extended Log File Format</td>
<td>403</td>
</tr>
<tr>
<td>Configuring ODBC Logging</td>
<td>405</td>
</tr>
<tr>
<td>Configuring Centralized Binary Logging</td>
<td>409</td>
</tr>
<tr>
<td>Disabling Logging</td>
<td>410</td>
</tr>
<tr>
<td>14 IIS Backup and Recovery</td>
<td>411</td>
</tr>
<tr>
<td>Backing Up the IIS Configuration</td>
<td>411</td>
</tr>
<tr>
<td>Understanding IIS Configuration Backups</td>
<td>411</td>
</tr>
<tr>
<td>Managing the IIS Configuration History</td>
<td>415</td>
</tr>
<tr>
<td>Viewing IIS Configuration Backups</td>
<td>416</td>
</tr>
<tr>
<td>Creating IIS Configuration Backups</td>
<td>416</td>
</tr>
<tr>
<td>Removing IIS Configuration Backups</td>
<td>417</td>
</tr>
<tr>
<td>Restoring IIS Server Configurations</td>
<td>417</td>
</tr>
<tr>
<td>Rebuilding Corrupted IIS Installations</td>
<td>418</td>
</tr>
<tr>
<td>Backing Up and Recovering Server Files</td>
<td>419</td>
</tr>
<tr>
<td>Turning on the Backup Feature</td>
<td>419</td>
</tr>
<tr>
<td>Working with Windows Server Backup</td>
<td>420</td>
</tr>
</tbody>
</table>
Table of Contents

Setting Basic Performance Options .............. 421
Scheduling Server Backups .................... 422
Backing up a Server ........................... 424
Protecting a Server Against Failure ............ 425
Recovering Files and Folders .................. 427

Appendix  Comprehensive IIS 7.0 Module and Schema Reference ...... 429

Working with IIS 7.0 Modules .................... 429
Introducing the Native Modules ................. 430
Introducing the Managed Modules ............... 433

IIS 7.0 Native Module Reference ................ 434
AnonymousAuthenticationModule ............... 434
BasicAuthenticationModule .................... 436
CertificateMappingAuthenticationModule ...... 437
CgiModule ..................................... 437
ConfigurationValidationModule ................. 439
CustomErrorModule ............................ 440
CustomLoggingModule ......................... 441
DefaultDocumentModule ....................... 442
DigestAuthenticationModule ................... 443
DirectoryListingModule ....................... 444
DynamicCompressionModule ................... 445
FailedRequestsTracingModule ................. 448
FastCgiModule .................................. 453
FileCacheModule ................................ 454
HttpCacheModule ................................ 455
HttpLoggingModule ............................. 458
HttpRedirectionModule ....................... 460
IISCertificateMappingAuthenticationModule .... 462
IpRestrictionModule ................. 464
IsapiFilterModule ............................ 466
IsapiModule .................................... 467
ManagedEngine .................................. 468
ProtocolSupportModule ...................... 469
RequestFilteringModule ...................... 470
RequestMonitorModule ....................... 472
ServerSideIncludeModule ..................... 472
StaticCompressionModule ..................... 473
Table of Contents

StaticFileModule ........................................ 474
TokenCacheModule ...................................... 474
TracingModule .......................................... 475
UriCacheModule ......................................... 475
UrlAuthorizationModule ................................ 476
WindowsAuthenticationModule ....................... 477

IIS 7.0 Managed Module Reference .................. 478
AnonymousIdentificationModule ...................... 478
DefaultAuthenticationModule ......................... 479
FileAuthorizationModule ................................ 479
FormsAuthenticationModule ............................ 480
OutputCacheModule .................................... 482
ProfileModule ........................................... 482
RoleManagerModule .................................... 482
SessionStateModule .................................... 483
UrlAuthorizationModule ................................ 484
UrlMappingsModule ..................................... 484
WindowsAuthenticationModule ....................... 485

Index ....................................................... 487

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

Writing *Internet Information Services (IIS) 7.0 Administrator’s Pocket Consultant* was a lot of fun—and a lot of work. As I set out to write this book, my first goal was to determine what had changed between IIS 6 and IIS 7.0 and what new administration options were available. With any product, and especially with IIS 7.0, this meant doing a great deal of research to determine exactly how things work and a lot of digging into the configuration internals. Thankfully I’d already written many books on IIS, Web technologies, and Web publishing, so I had a starting point of reference for my research—but it was by no means a complete one.

When you start working with IIS 7.0, you’ll see at once that this release is different from previous releases. What won’t be readily apparent, however, is just how different IIS 7.0 is from its predecessors—and that’s because many of the most significant changes to the product are under the surface. These changes affect the underlying architecture and not just the interfaces—and these changes were some of the hardest for me to research and write about.

Because pocket consultants are meant to be portable and readable—the kind of book you use to solve problems quickly and easily and get the job done wherever you might be—I had to carefully review my research to make sure I focused on the core of IIS 7.0 administration. The result is the book you hold in your hand, which I hope you’ll agree is one of the best practical, portable guides to IIS 7.0.

It is gratifying to see techniques I’ve used time and again to solve problems put into a printed book so that others may benefit from them. But no man is an island, and this book couldn’t have been written without help from some very special people. As I’ve stated in all my previous books with Microsoft Press, the team at Microsoft Press is top-notch. Throughout the writing process, Maureen Zimmerman was instrumental in helping me stay on track and getting the tools I needed to write this book. Maureen did a top-notch job managing the editorial process. Thanks also to Martin DelRe for believing in my work and shepherding it through production.

Unfortunately for the writer (but fortunately for readers), writing is only one part of the publishing process. Next came editing and author review. I must say, Microsoft Press has the most thorough editorial and technical review process I’ve seen anywhere—and I’ve written a lot of books for many different publishers. Bob Hogan was the technical editor for the book. Joel Rosenthal was the copy editor for the book. I want to thank both of them for their careful reviews. Bob and Joel are great to work with!

I also want to thank Lucinda, Jack, Karen, Denise, and everyone else at Microsoft who has helped me during this project. Hopefully, I haven’t forgotten anyone but if I have, it was an oversight. Honest,;-)
Introduction

Welcome to Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant. As the author of over 65 books, I’ve been writing professionally about Web publishing and Web servers since 1994. Over the years, I’ve written about many different Web server technologies and products, but my favorite has always been Internet Information Services (IIS). IIS provides the core services for hosting Web servers, Web applications, and Microsoft Windows SharePoint services. From top to bottom, IIS 7.0 is substantially different from earlier versions of IIS. For starters, the underlying configuration architecture for IIS has been completely reconstructed—IIS configuration architecture is now based entirely on Extensible Markup Language (XML) and XML schema.

Having written many top-selling Web publishing and XML books, I was able to bring a unique perspective to this book—the kind of perspective you can gain only after working with technologies for many years. You see, long before IIS 7.0 architecture was built on XML and related technologies, I was working with, researching, and writing about these technologies. The advantage for you, the reader, is that my solid understanding of these technologies allowed me to dig into the IIS configuration architecture and to provide a comprehensive roadmap to this architecture and the hundreds of related configuration settings in this book.

In addition, as you’ve probably noticed, there’s more than enough information about IIS 7.0 on the Web and in other printed books. There are tutorials, reference sites, discussion groups, and more to help make it easier to use IIS 7.0. However, the advantage to reading this book instead is that all the information you need to learn IIS 7.0 is organized in one place and presented in a straightforward and orderly fashion. This book has everything you need to customize IIS installations, master IIS configuration, and maintain IIS servers.

In this book, I teach you how features work, why they work the way they work, and how to customize them to meet your needs. You’ll also learn why you may want to use certain features and when to use other features to resolve any issues you are having. In addition, this book provides tips, best practices, and examples of how to optimize IIS 7.0 to meet your needs. This book won’t just teach you how to configure IIS—it’ll teach you how to squeeze every last bit of power out of the application and how to make the most of the features and options included in IIS 7.0.

Also, unlike many other books on the subject, this book doesn’t focus on a specific user level. This isn’t a lightweight, beginners-only book. Regardless of whether you are a novice administrator or a seasoned professional, many of the concepts in this book will be valuable to you. And you’ll be able to apply them to your IIS server installations.
Who Is This Book For?

*Internet Information Services (IIS) 7.0 Administrator’s Pocket Consultant* covers core services for hosting Web servers, Web applications, and Windows SharePoint services. The book is designed for:

- Current Microsoft Web administrators and developers
- Administrators and developers of intranets and extranets
- Administrators and developers migrating to Microsoft Web-based solutions
- Programmers, engineers, and quality assurance personnel who manage internal or test servers running any of these services

To pack in as much information as possible, I assume that you already have basic networking skills and a basic understanding of Web servers. With this in mind, I don’t devote entire chapters to understanding the World Wide Web, Web services, or Web servers. I do, however, cover configuration, enterprise-wide server management, performance tuning, optimization, automation, and much more.

I also assume that you’re fairly familiar with the standard Windows user interface and that if you plan to use the scripting techniques outlined in the book, you know scripting. If you need help learning Windows or scripting, you should read other resources (many of which are available from Microsoft Press and the Microsoft Web site as well).

How This Book Is Organized

Rome wasn’t built in a day, and this book wasn’t intended to be read in a day, a week, or even 21 days. Ideally, you’ll read this book at your own pace, a little each day, as you work your way through all the features IIS has to offer. This book is organized into four parts with 14 chapters and a comprehensive reference in an appendix. The chapters are arranged in a logical order, taking you from planning and deployment tasks to configuration and maintenance tasks.

Speed and ease of reference are essential parts of this hands-on guide. This book has an expanded table of contents and an extensive index to help you find answers to problems quickly. Many other quick reference features have been added to the book as well, including quick step-by-step instructions, lists, tables with fast facts, and extensive cross-references.

As with all the books in the Pocket Consultant series, *Internet Information Services (IIS) 7.0 Administrator’s Pocket Consultant* is designed to be a concise and easy-to-use resource for managing Web servers running IIS. This book is the readable resource guide that you’ll want on your desktop at all times, as it covers everything you’ll need to perform core Web administration tasks. Because the focus is on giving you maximum value in a pocket-sized guide, you don’t have to wade through hundreds of pages of
extraneous information to find what you’re looking for. Instead, you’ll find exactly what you need to get the job done.

In short, this book is designed to be the one resource you can turn to whenever you have questions regarding Web server administration. To this end, the book zeroes in on daily administration procedures, frequently used tasks, documented examples, and options that are representative while not necessarily inclusive. One of the key goals I had when writing this book is to keep the content so concise that the book remains compact and easy to navigate, while ensuring that it is packed with as much information as possible. Thus, rather than a hefty 1,000-page tome or a lightweight 100-page quick reference, you get a valuable resource guide that can help you quickly and easily perform common tasks, solve problems, and implement advanced IIS techniques, such as failed request tracing, handler mapping, customized Hypertext Transfer Protocol (HTTP) redirection, and integrated request processing.

**Conventions Used in This Book**

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

Other conventions include:

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

I truly hope you find that *Internet Information Services (IIS) 7.0 Administrator’s Pocket Consultant* provides everything you need to perform the essential administrative tasks on IIS servers as quickly and efficiently as possible. You are welcome to send your thoughts to me at williamstanek@aol.com.

**Other Resources**

No single magic bullet exists for learning everything you’ll ever need to know about IIS. While some books claim to be all-in-one guides, there’s simply no way one
book can do it all. With this in mind, I hope you’ll use this book as it is intended to be used: as a concise and easy-to-use resource.

Your current knowledge will largely determine your success with this or any other IIS resource or book. As you encounter new topics, take the time to practice what you’ve learned and read about. Seek out further information as necessary to get the practical hands-on know-how and knowledge you need.

Throughout your studies, I recommend that you regularly visit Microsoft’s IIS site (http://www.iis.net) and Microsoft’s support site (http://support.microsoft.com) to stay current with the latest changes in the software. To help you get the most out of this book, there’s a corresponding Web site at http://www.williamstanek.com/iis which contains information about IIS, updates to the book, and updated information about IIS.

**Support**

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for its books 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
Atttn: Internet Information Services (IIS) 7.0 Administrator’s Pocket Consultant Editor
One Microsoft Way
Redmond, WA 98052-6399

E-mail:

MSPINPUT@MICROSOFT.COM
Chapter 1

IIS 7.0 Administration Overview

Let’s start with the bad news right up front: Internet Information Services (IIS) 7.0 isn’t what you think it is. Although IIS 7.0 is the latest release of Internet Information Services, it isn’t what it seems. IIS does look a lot like its predecessors, but this is deceiving because under the surface, the architecture is completely different. So much has changed, in fact, that perhaps it might have been better if Microsoft had given IIS 7.0 a new product name. That way you’d know that IIS 7.0 was completely different from its predecessors, allowing you to start with a fresh perspective and a reasonable expectation of having to learn a whole new bag of tricks. Seasoned IIS pros also are going to have to unlearn some old tricks; and that’s not only going to be difficult, it might be the single biggest obstacle to mastering IIS 7.0.

IIS 7.0 provides the core services for hosting Web servers, Web applications, and Microsoft Windows SharePoint Services. Throughout this book, I’ll refer to administration of IIS, Web applications, and Windows SharePoint Services as Microsoft Web administration or simply Web administration. As you get started with Microsoft Web administration, you should concentrate on these key areas:

- What’s new or changed in IIS 7.0
- How IIS 7.0 configuration schema and global configuration architecture are used
- How IIS 7.0 works with your hardware
- How IIS works with Windows-based operating systems
- Which administration tools are available
- Which administration techniques you can use to manage and maintain IIS

Working with IIS 7.0: What You Need to Know Right Now

Microsoft fully integrated Microsoft ASP.NET and the Microsoft .NET Framework into IIS 7.0. Unlike IIS 6, IIS 7.0 takes ASP.NET and the .NET Framework to the next level by integrating the ASP.NET runtime extensibility model with the core server architecture, allowing developers to fully extend the core server architecture by using ASP.NET and the .NET Framework. This tighter integration makes it possible to use existing ASP.NET features such as .NET Roles, Session Management, Output Caching, and Forms Authentication with all types of content.
IIS 7.0 has generalized the Hypertext Transfer Protocol (HTTP) process activation model that IIS 6 introduced with application pools and made it available for all protocols through an independent service called the Windows Process Activation Service, and developers can use Windows Communication Foundation (WCF) protocol adapters to take advantage of the capabilities of this service. You also should know up front that IIS 7.0 includes a metabase compatibility component that allows your existing scripts and applications to continue running but does not use a metabase to store configuration information. Instead of a metabase, IIS 7.0 uses a distributed configuration system with global and application-specific configuration files that are based on a customizable set of Extensible Markup Language (XML) schema files. These XML schema files define the configuration elements and attributes in addition to valid values for those elements and attributes, providing you precise control over exactly how you can configure and use IIS.

Microsoft built the configuration system around the concept of modules. Modules are standalone components that provide the core feature set of an IIS server. Microsoft ships more than 40 independent modules with IIS 7.0. Either these modules are IIS 7.0–native modules that use a Win32 DLL or IIS 7.0–managed modules that use a .NET Framework Class Library contained within an assembly. Because all server features are contained within modules, you can modify the available features easily by adding, removing, or replacing a server’s modules. Further, by optimizing the installed modules based on the way an IIS server is used, you can enhance security by reducing the attack surface area and improve performance by reducing the resources required to run the core services.

Note Because modules are such an important part of IIS 7.0, you’ll find much discussion about them and how they are used in this book. Chapter 2, “Deploying IIS 7.0 in the Enterprise,” introduces all the available native and managed modules. Chapter 5, “Managing Global IIS Configuration,” details how to install and manage modules. The appendix, “Comprehensive IIS 7.0 Module and Schema Reference,” provides a complete guide to using modules and schemas.

IIS 7.0 is more secure than IIS 6 because of built-in request filtering and rules-based Uniform Resource Locator (URL) authorization support. You can configure request filtering to reject suspicious requests by scanning URLs sent to a server and filtering out unwanted requests. You can configure URL authorization rules to require logon and allow or deny access to specific URLs based on user names, .NET roles, and HTTP request methods. To make it easier to resolve problems with the server and Web applications, IIS 7.0 includes new features for diagnostics, real-time request reviewing, and error reporting. These features allow you to:

- View the current running state of the server.
- Trace failed requests through the core server architecture.
- Obtain detailed error information to pinpoint the source of a problem.
IIS 7.0 has many other new and enhanced features, but few are as important as the new set of administration tools, including new graphical, command-line, and scripting administration tools. The new graphical administration tool uses a browser-like interface and adds features for delegated administration, remote administration over Secure HTTP (HTTPS), and extensibility through custom user interface components. The new command-line administration tool makes it possible to perform most configuration tasks with a single line of command text. With ASP.NET, you can manage IIS configuration through the .NET Framework by using the Microsoft.Web.Administrators application programming interface (API). With scripting, you can manage IIS configuration through the IIS 7.0 Windows Management Instrumentation (WMI) provider.

Because of the many changes, much of what you know about IIS is obsolete or irrelevant. But there’s a light at the end of the tunnel—well, it’s more like a freight train coming right at you—but it’s there. The changes in IIS 7.0 are well worth the time and effort you’ll spend learning the new architecture and the new techniques required to manage Web servers. Our dependence on ASP.NET and the .NET Framework will only grow over time, and the more you learn about the heart of the .NET architecture—IIS 7.0—the better prepared you’ll be for now and for the future.

With IIS 7.0, key components that were a part of previous IIS releases are no longer available or work in different ways than they did before. Because IIS 7.0 does not use a metabase, applications designed for IIS 6 will not run on IIS 7.0 without special actions being taken. To run IIS 6 applications, you must install the IIS 6 compatibility and metabase feature. To manage IIS 6 applications and features, you must install IIS 6 Manager, IIS 6 scripting tools, and IIS 6 WMI compatibility. Additionally, IIS 7.0 does not include Post Office Protocol version 3 (POP3) or Simple Mail Transfer Protocol (SMTP) services. With IIS 7.0, you can send e-mail messages from a Web application by using the SMTP E-mail component of ASP.NET.

IIS Manager is the graphical user interface (GUI) for managing both local and remote installations of IIS 7.0. To use IIS Manager to manage an IIS server remotely, Web Management Service (WMSVC) must be installed and started on the IIS server you want to manage remotely. WMSVC is also required when IIS site or application administrators want to manage features over which they’ve been delegated control.

The Web Management Service provides a hostable Web core that acts as a standalone Web server for remote administration. After you install and start WMSVC on an IIS server, it listens on port 8172 on all unassigned IP addresses for four specific types of requests:

- **Login Requests**  
  IIS Manager sends login requests to WMSVC to initiate connections. On the hostable Web core, login requests are handled by Login.axd. The authentication type is either NT LAN Manager (NTLM) or Basic, depending on what you select when you are prompted to provide credentials in the connection dialog box.
Code Download Requests  If login is successful, WMSVC returns a list of user interface (UI) modules for the connection. Each IIS Manager page corresponds to a specific UI module. If there's a module that IIS Manager doesn't have, it will request to download the module binaries. Code download requests are handled by Download.axd.

Management Service Requests  After a connection is established, your interactions with IIS Manager cause management service requests. Management service requests direct module services in WMSVC to read or write configuration data, runtime state, and providers on the server. Management service requests are handled by Service.axd.

Ping Requests  Ping requests are made from within the WMSVC service to the hostable Web core. Ping requests are made by Ping.axd to ensure that the hostable Web core continues to be responsive.

The Web Management Service stores a limited set of editable configuration values in the registry. Each time the service is started, the Web configuration files are regenerated in the following directory: %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\Temp\WMSvc. To enhance security, WMSVC requires SSL (HTTPS) for all connections. This ensures that data passed between the remote IIS Manager client and WMSVC is secure. Additionally, WMSVC runs as Local Service with a reduced permission set and a locked down configuration. This ensures that only the minimal set of required modules are loaded when the hostable Web core starts. See Chapter 3, “Core IIS 7.0 Administration,” for more information.

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

Introducing IIS 7.0 Configuration Architecture

You can use IIS 7.0 to publish information on intranets, extranets, and the Internet. Because today’s Web sites use related features, such as ISAPI filters, ASP, ASP.NET, CGI, and the .NET Framework, IIS bundles these features as part of a comprehensive offering. What you need to know right now about IIS 7.0 is how IIS 7.0 uses the configuration schema and its global configuration system. In Chapter 2, you’ll learn about the available setup features and the related configuration modules.

IIS 7.0 Configuration Schema

Unlike IIS 6, in which the main configuration information is stored in metabase files, IIS 7.0 has a unified configuration system for storing server, site, and application settings. You can manage these settings by using an included set of managed code, scripting APIs, and management tools. You can also manage these settings by directly
editing the configuration files themselves. Direct editing of configuration files is possible because the files use XML and are written in plain-language text files based on a predefined set of XML schema files.

**Note**  IIS 7.0 always takes the master state for configuration from the configuration files. This is a dramatic change from IIS 6, in which the master state was taken from the in-memory configuration database, which was flushed periodically to disk.

Using the XML schema to specify the configuration settings ensures that the related configuration files are well-structured XML, which is easy to modify and maintain. Because configuration values are stored using easy-to-understand text strings and values, they are easy to work with. By examining the schema itself, you can determine the exact set of acceptable values for any configuration option. IIS shares the same schema with ASP.NET configuration, ensuring that configuration settings for ASP.NET applications are just as easy to manage and maintain.

On an IIS server, schema files are stored in the `%SystemRoot%\System32\Inetsrv\Config\Schema` directory. The four standard schema files are:

- **IIS_schema.xml**  This file provides the IIS configuration schema.
- **ASPNET_schema.xml**  This file provides the ASP.NET configuration schema.
- **FX_schema.xml**  This file provides the .NET Framework configuration schema (providing features beyond what the ASP.NET schema offers).
- **rscaext.xml**  This file provides the Runtime Status and Control API (RSCA) configuration schema, providing dynamic properties for obtaining detailed runtime data.

IIS reads in the schema files automatically during startup of the application pools. The IIS schema file is the master schema file. Within the IIS schema file, you'll find configuration sections for each major feature of IIS, from application pooling to failed request tracing. The ASP.NET schema file builds on and extends the master schema with specific configuration sections for ASP.NET. Within the ASP.NET schema file, you'll find configuration sections for everything from anonymous identification to output cache settings. The FX schema file builds on and extends the ASP.NET schema file. Within the FX schema file, you'll find configuration settings for application settings, connection strings, date-time serialization, and more.

Whereas configuration sections are also grouped together for easier management, section groups do not have schema definitions. If you want to extend the configuration features and options available in IIS, you can do this by extending the XML schema.

You extend the schema by following these basic steps:

1. Specify the desired configuration properties and the necessary section container in an XML schema file.
2. Place the schema file in the `%SystemRoot%\System32\Inetsrv\Config\Schema` directory.
3. Reference the new section in IIS 7.0’s global configuration file.
The basic syntax for a schema file is as follows:

```xml
<configSchema>
  <sectionSchema name="configSection1"/>
  <sectionSchema name="configSection2"/>
  <sectionSchema name="configSection3"/>
</configSchema>
```

As an administrator or developer, you don’t necessarily need to be able to read and interpret XML schemas to succeed. However, because having a basic understanding of schemas is helpful, I’ll introduce the essentials. Within schema files, configuration settings are organized into sets of related features called schema sections. The schema for a configuration section is defined in a `<sectionSchema>` XML element. For example, the features related to the HTTP listener in IIS are defined with a schema section named `system.applicationHost/listenerAdapters`. In the IIS_schema.xml file, this section is defined as follows:

```xml
<sectionSchema name="system.applicationHost/listenerAdapters">
  <collection addElement="add">
    <attribute name="name" type="string" required="true" isUniqueKey="true" />
    <attribute name="identity" type="string" />
    <attribute name="protocolManagerDll" type="string" />
    <attribute name="protocolManagerDllInitFunction" type="string" />
  </collection>
</sectionSchema>
```

This schema definition states that the `system.applicationHost/listenerAdapters` element can contain a collection of `add` elements with the following attributes:

- **name**  A unique string that is a required part of the `add` element.
- **identity**  An identity string that is an optional part of the `add` element.
- **protocolManagerDll**  A string that identifies the protocol manager DLL.
- **protocolManagerDllInitFunction**  A string that identifies the initialization function for the protocol manager DLL.

An attribute of an element is either optional or required. If the attribute definition states `required="true"` as with the name attribute, the attribute is required and must be provided when you are using the related element. Otherwise, the attribute is considered
optional and does not need to be provided when you are using the related element. In addition to being required, attributes can have other enforced conditions, including:

- **isUniqueKey** If set to true, the related value must be unique.
- **encrypted** If set to true, the related value is expected to be encrypted.

With some attributes, you'll see default values and possibly an enumerated list of the acceptable string values and their related internal values. In the following example, the `identityType` attribute has a default value of `NetworkService` and a list of other possible values:

```xml
<attribute name="identityType" type="enum" defaultValue="NetworkService">
    <enum name="LocalSystem" value="0"/>
    <enum name="LocalService" value="1"/>
    <enum name="NetworkService" value="2"/>
    <enum name="SpecificUser" value="3"/>
</attribute>
```

The friendly name of a value is provided to make the value easier to work with. The actual value used by IIS is provided in the related value definition. For example, if you set `identityType` to `LocalService`, the actual configuration value used internally by IIS is 2.

As a standard rule, you cannot use enumerated values in combination with each other. Because of this, the `identityType` attribute can have only one possible value. In contrast, attributes can have flags, which can be used together to form combinations of values. In the following example, the `logEventOnRecycle` attribute uses flags and has a default set of flags that are used in combination with each other:

```xml
<attribute name="logEventOnRecycle" type="flags" defaultValue="Time, Memory, PrivateMemory">
    <flag name="Time" value="1"/>
    <flag name="Requests" value="2"/>
    <flag name="Schedule" value="4"/>
    <flag name="Memory" value="8"/>
    <flag name="IsapiUnhealthy" value="16"/>
    <flag name="OnDemand" value="32"/>
    <flag name="ConfigChange" value="64"/>
    <flag name="PrivateMemory" value="128"/>
</attribute>
```

Again, the friendly name is provided to make the value easier to work with. The actual value used by IIS is the sum of the combined flag values. With a setting of “Time, Requests, Schedule,” the `logEventOnRecycle` attribute is set to 7 (1+2+4=7).

Attribute values can also have validation. IIS performs validation of attribute values when parsing the XML and when calling the related API. Table 1-1 provides an overview of the validators you'll see in schemas.
IIS 7.0 Administrator's Pocket Consultant

Table 1-1 Summary of Attribute Validation Types in an IIS XML Schema

<table>
<thead>
<tr>
<th>Validation Type</th>
<th>Validation Parameter</th>
<th>Validation Fails If...</th>
</tr>
</thead>
<tbody>
<tr>
<td>validationType= &quot;applicationPoolName&quot;</td>
<td>validationParameter=&quot;&quot;</td>
<td>A validated value contains these characters: [&lt;&gt;&quot;</td>
</tr>
<tr>
<td>validationType= &quot;integerRange&quot;</td>
<td>validationParameter= &quot;&lt;minimum&gt;, &lt;maximum&gt;[exclude]&quot;</td>
<td>A validated value is outside [inside] range, in integers.</td>
</tr>
<tr>
<td>validationType= &quot;nonEmptyString&quot;</td>
<td>validationParameter=&quot;&quot;</td>
<td>A validated value has a string value that is not set.</td>
</tr>
<tr>
<td>validationType= &quot;siteName&quot;</td>
<td>validationParameter=&quot;&quot;</td>
<td>A validated value contains these characters: /.?</td>
</tr>
<tr>
<td>validationType= &quot;timeSpanRange&quot;</td>
<td>validationParameter= &quot;&lt;minimum&gt;, &lt;maximum&gt;, &lt;granularity&gt; [exclude]&quot;</td>
<td>A validated value is outside [inside] range, in seconds.</td>
</tr>
<tr>
<td>validationType= &quot;requireTrimmedString&quot;</td>
<td>validationParameter=&quot;&quot;</td>
<td>A validated value has white space at start or end of value.</td>
</tr>
</tbody>
</table>

IIS 7.0 Global Configuration System

IIS uses a global configuration system that is difficult to understand at first but gets easier and easier to understand once you’ve worked with it awhile. Because there’s no sense trying to ease into this, I’ll dive right in. If you’ll hang with me for a few pages, I’ll get you through the roughest parts and zero in on exactly what you need to know—I promise.

IIS configuration settings are stored in configuration files that together set the running configuration of IIS and related components. One way to think of a configuration file is as a container for the settings you apply and their related values. You can apply multiple configuration files to a single server and the applications it is running. Generally, you manage configuration files at the .NET Framework root level, the server root level, and the various levels of a server’s Web content directories. A server’s Web content directories include the root directory of the server itself, the root directories of configured Web sites, and any subdirectories within Web sites. The root levels and the various levels of a server’s Web content directories can be described as containers for the settings you apply and their values. If you know a bit about object-oriented programming, you might expect the concepts of parent-child relationship and inheritance to apply—and you’d be right.

Through inheritance, a setting applied at a parent level becomes the default for other levels of the configuration hierarchy. Essentially, this means that a setting applied at a parent level is passed down to a child level by default. For example, if you apply a
setting at the server root level, the setting is inherited by all Web sites on the server and by all the content directories within those sites.

The order of inheritance is as follows:

.NET Framework root ➔ server root ➔ Web Site root ➔
top-level directory ➔ subdirectory

This means that the settings for the current .NET Framework root are passed down to IIS, the settings for IIS are passed down to Web sites, and the settings for Web sites are passed down to content directories and subdirectories. As you might expect, you can override inheritance. To do this, you specifically assign a setting for a child level that contradicts a setting for a parent. As long as overriding a setting is allowed (that is, overriding isn’t blocked), the child level’s setting will be applied appropriately. To learn more about overriding and blocking, see Chapter 5.

When working with the configuration files, keep the following in mind:

■ The .NET Framework root IIS applies depends on the current running version of ASP.NET and the .NET Framework. The default configuration files for the .NET Framework root are Machine.config and Web.config, which are stored in the %SystemRoot%\Microsoft.net\Framework\Version\Config\Machine.config directory. Machine.config sets the global defaults for the .NET Framework settings in addition to some ASP.NET settings. Web.config sets the rest of the global defaults for ASP.NET. See Chapter 8, “Running IIS Applications,” and Chapter 9, “Managing Applications, Application Pools, and Worker Processes,” for more information about configuring the .NET Framework and ASP.NET.

■ The default configuration file for the server root is ApplicationHost.config, which is stored in the %SystemRoot%\System32\Inetsrv\Config directory. This file controls the global configuration of IIS. See Chapter 5 for more information about configuring IIS servers.

■ The default configuration file for a Web site root is Web.config. This file is stored in the root directory of the Web site to which it applies and controls the behavior for the Web site. See Chapters 8 and 9 for more information about configuring IIS applications.

■ The default configuration file for a top-level content directory or a content subdirectory is Web.config. This file is stored in the content directory to which it applies and controls the behavior of that level of the content hierarchy and downwards. See Chapter 6 for more information about configuring content directories.

In some cases, you may want a .config file to include some other .config file. This can be done by using the configSource attribute to refer to the .config file containing the settings you want to use. Currently, the referenced .config file must reside in the same
directory as the original .config file. Note that this behavior may change to allow .config files in other directories to be used. To see how this works, consider the following example from the ApplicationHost.config file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <httpErrors>
      <error statusCode="401" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="401.htm" />
      <error statusCode="403" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="403.htm" />
      <error statusCode="404" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="404.htm" />
      <error statusCode="405" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="405.htm" />
      <error statusCode="406" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="406.htm" />
      <error statusCode="412" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="412.htm" />
      <error statusCode="500" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="500.htm" />
      <error statusCode="501" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="501.htm" />
      <error statusCode="502" prefixLanguageFilePath="%SystemDrive%\inetpub\custerr" path="502.htm" />
    </httpErrors>
  </system.webServer>
</configuration>
```

In this example, error elements specify how certain types of HTTP error status codes should be handled. If you wanted to customize the error handling for a server, you might want to extend or modify the default values in a separate .config file and then reference the .config file in ApplicationHost.config. To do this, you would update the ApplicationHost.config file to point to the additional .config file. An example follows.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <httpErrors configSource=errorMode.config />
  </system.webServer>
</configuration>
```

You would then create the errorMode.config file and store it in the same directory as the ApplicationHost.config file. The following is an example of the contents of the errorMode.config file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- errorMode.config -->
```
Chapter 1  IIS 7.0 Administration Overview

When you make these or other types of changes in configuration files, you don’t need to worry about restarting IIS or related services. IIS automatically picks up the changes and uses them. In these examples, you’ll note that we’re working with the system.webServer section of the configuration file. As per the schema definition files, all settings are defined within specific configuration sections. Although sections cannot be nested, a section can exist within a section group, and that section group can in turn be contained in a parent section group. A section group is simply a container of logically related sections.

In ApplicationHost.config, section groups and individual sections are defined in the configSections element. The configSections element controls the registration of sections. Every section belongs to one section group. By default, ApplicationHost.config contains these section groups:

- **system.applicationHost**  Defines the following sections: applicationPools, configHistory, customMetadata, listenerAdapters, log, sites, and webLimits.

IIS 7.0 Administrator’s Pocket Consultant

- **system.webServer.security**  A subgroup of system.webServer that defines the following sections: access, applicationDependencies, authorization, ipSecurity, isapiCgiRestriction, and requestFiltering. Includes the authentication subgroup.

- **system.webServer.security.authentication**  A subgroup of system.webServer .security that defines the following sections: anonymousAuthentication, basicAuthentication, clientCertificateMappingAuthentication, digestAuthentication, iisClientCertificateMappingAuthentication, and windowsAuthentication.

- **system.webServer.security.tracing**  A subgroup of system.webServer.security that defines the traceFailedRequests and traceProviderDefinitions sections.

In ApplicationHost.config, section groups and individual sections are defined as follows:

```xml
<configSections>
  <sectionGroup name="system.applicationHost">
    <section name="applicationPools" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="configHistory" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="customMetadata" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="listenerAdapters" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="log" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="sites" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="webLimits" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
  </sectionGroup>
  <sectionGroup name="system.webServer">
    ...
  </sectionGroup>
</configSections>
```

In Machine.config, you’ll also find definitions for section groups and individual sections. These are similar to those used in ApplicationHost.config but are used for configuring the .NET Framework and some ASP.NET settings. When working with either .config file, keep in mind that a section is the basic unit of deployment, locking, searching, and containment for configuration settings. Every section has a name attribute and optional allowDefinition and overrideModeDefault attributes. The name attribute sets the unique section name. The allowDefinition attribute specifies the level at which the section can be set:

- **Everywhere**  The section can be set in any configuration file including directories mapped to virtual directories that are not application roots, and their subdirectories. Because this is the default setting, a section that doesn’t have an allowDefinition attribute uses this setting automatically.

- **MachineOnly**  The section can be set only in ApplicationHost.config or Machine.config.
Chapter 1  IIS 7.0 Administration Overview  13

- **MachineToWebRoot**  The section can be set only in the .NET Framework root’s Machine.config or Web.config file, or in ApplicationHost.config.

- **MachineToApplication**  The section can be set only in the .NET Framework root’s Machine.config or Web.config file, in ApplicationHost.config, or in Web.config files for application root directories.

- **AppHostOnly**  The section can be set only in Web.config files for application root directories.

The OverrideModeDefault attribute sets the default lockdown state of a section. Essentially, this means that it controls whether a section is locked down to the level in which it is defined or can be overridden by lower levels of the configuration hierarchy. If this attribute is not set, the default value is Allow. With Allow, lower level configuration files can override the settings of the related section. With Deny, lower level configuration files cannot override the settings of the related section. As discussed in Chapter 5, you’ll typically use location tags to lock or unlock sections for specific Web sites or applications.

Because the complete configuration settings of a server and its related sites and applications are stored in the configuration files, you easily can back up or duplicate a server’s configuration. Backing up a server’s configuration is a simple matter of creating a copy of the configuration files. Similarly, duplicating a server’s configuration on another server is a simple matter of copying the source configuration files to the correct locations on another server.

### IIS 7.0 and Your Hardware

Before you deploy IIS 7.0, you should carefully plan the server architecture. As part of your planning, you need to look closely at pre-installation requirements and the hardware you will use. IIS 7.0 is no longer the simple solution for hosting Web sites that it once was. It now provides the core infrastructure for hosting Web servers, Web applications, and Windows SharePoint Services.

Guidelines for choosing hardware for Internet servers are much different from those for choosing other types of servers. A Web hosting provider might host multiple sites on the same computer and might also have service level agreements that determine the level of availability and performance required. On the other hand, a busy e-commerce site might have a dedicated Web server or even multiple load-balanced servers. Given that Internet servers are used in a wide variety of circumstances and might be either shared or dedicated, here are some guidelines for choosing server hardware:

- **Memory**  The amount of random access memory (RAM) that’s required depends on many factors, including the requirements of other services, the size of frequently accessed content files, and the RAM requirements of the Web applications. In most installations, I recommend that you use at least 1 gigabyte (GB) of RAM. High-volume servers should have a minimum of 2 to 4 GB of RAM.
RAM will allow more files to be cached, reducing disk requests. For all IIS installations, the operating system paging file size should at least equal the amount of RAM on the server.

**Note** Don't forget that as you add physical memory, virtual paging to disk grows as well. With this in mind, you might want to ensure that the Pagefile.sys file is on the appropriate disk drive, one that has adequate space for the page file to grow, along with providing optimal input/output (I/O) performance.

**More Info** For detailed information on memory management and performance tuning, see Chapter 12, “Performance Tuning, Monitoring, and Tracing.”

**CPU** The CPU processes the instructions received by the computer. The clock speed of the CPU and the size of the data bus determine how quickly information moves among the CPU, RAM, and system buses. Static content, such as HTML and images, place very little burden on the processor, and standard recommended configurations should suffice. Faster clock speeds and multiple processors increase the performance scalability of a Web server, particularly for sites that rely on dynamic content. 32-bit versions of Windows run on Intel x86 or compatible hardware. 64-bit versions of Windows run on the x64 family of processors from AMD and Intel, including AMD64 and Intel Extended Memory 64 Technology (Intel EM64T). IIS provides solid benchmark performance on Intel Xeon, AMD Opteron, and AMD Athlon processors. Any of these CPUs provide good starting points for the typical IIS server. You can achieve significant performance improvements with a large processor cache. Look closely at the L1, L2, and L3 cache options available—a larger cache can yield much better performance overall.

**SMP** IIS supports symmetric multiprocessors (SMPs) and can use additional processors to improve performance. If the system is running only IIS and doesn’t handle dynamic content or encryption, a single processor might suffice. You should always use multiple processors if IIS is running alongside other services, such as Microsoft SQL Server or Microsoft Exchange Server.

**Disk drives** The amount of data storage capacity you need depends entirely on the size of content files and the number of sites supported. You need enough disk space to store all your data plus workspace, system files, and virtual memory. I/O throughput is just as important as drive capacity. However, disk I/O is rarely a bottleneck for Web sites on the public Internet—generally, bandwidth limits throughput. High-bandwidth sites should consider hardware-based redundant array of independent disks (RAID) solutions using copper or fiber channel–based small computer system interface (SCSI) devices.
Data protection  Unless you can tolerate hours of downtime, you should add protection against unexpected drive failures by using RAID. Hardware RAID implementations are always preferred over software RAID implementations. RAID 0 (disk striping without parity) offers optimal read/write performance, but if a drive fails, IIS won’t be able to continue operation until the drive is replaced and its contents are restored from backup. Because of this, RAID 0 isn’t the recommended choice. RAID 1 (disk mirroring) creates duplicate copies of data on separate physical drives, allowing the server to remain operational when a drive fails, and even while the RAID controller rebuilds a replacement drive in a failed mirror. RAID 5 (disk striping with parity) offers good protection against single-drive failure but has poor write performance. Keep in mind that if you’ve configured redundant load-balanced servers, you might not need RAID. With load balancing, the additional servers might offer the necessary fault tolerance.

UPS  Sudden power loss and power spikes can seriously damage hardware. To prevent this, get an uninterruptible power supply (UPS). A properly configured UPS system allows the operating system to automatically shut down the server gracefully in the event of a power outage, and it’s also important in maintaining system integrity when the server uses write-back caching controllers that do not have on-board battery backups. Professional hosting providers often offer UPS systems that can maintain power indefinitely during extended power outages.

If you follow these hardware guidelines, you’ll be well on your way to success with IIS.

IIS 7.0 Editions and Windows

IIS 7.0 is available for both desktop and server editions of Windows. On Windows Vista, IIS 7.0 offers Web administrators and Web developers a complete platform for building and testing dynamic Web sites and Web applications. IIS 7.0 running on Windows Vista also enables process activation, process management, and the necessary HTTP infrastructure for creating WCF–based applications.

As discussed further in Chapter 2, the way IIS 7.0 works on Windows Vista depends on the edition of Windows Vista you are using. On Windows Vista Starter and Home Basic editions, IIS 7.0 cannot be used to host Web sites, Web applications, or Windows SharePoint Services. On these editions, a limited set of IIS features are available, such as Windows Activation Service components that are used to enable WCF-based applications. Users who install WCF-based applications will not need to install these components. The necessary components are installed automatically by WCF. With these editions, the simultaneous request execution limit for IIS is three, meaning that an application or a group of running applications could make up to three simultaneous requests for Web content through the installed IIS components.
On Windows Vista Home Premium, most of the IIS 7.0 features required for Web site development are available. The available features should allow most casual or hobbyist administrators and developers to build and test dynamic Web sites and Web applications. Many advanced features are missing, however, including advanced authentication components, advanced logging components, and FTP server components. As with Starter and Home Basic editions of Windows Vista, the simultaneous request execution limit for IIS is three for Windows Vista Home Premium, meaning you or running applications could make up to three simultaneous requests for Web content through the installed IIS components.

For Windows Vista Business, Enterprise, and Ultimate editions, all IIS 7.0 features are available. This means that professional Web administrators and Web developers have everything necessary to design, build, and test Web sites and Web applications. The simultaneous request execution limit is ten for these editions of Windows Vista, meaning you or running applications could make up to ten simultaneous requests for Web content through the installed IIS components.

With server editions of Windows, you can use IIS to host Web servers, Web applications, and Windows SharePoint Services. All features of IIS 7.0 are available on all editions of Windows Server 2008. On Windows Server operating systems, IIS 7.0 has no request execution limit. This means that an unlimited number of simultaneous requests can be made to the IIS 7.0 server core.

### Web Administration Tools and Techniques

Web administrators will find that there are many ways to manage Web and application servers. The key administration tools and techniques are covered in the following sections.

### Managing Resources by Using Key Administration Tools

Many tools are available for managing Web resources. Key tools you’ll use are shown in Table 1-2. Most of these tools are available on the Administrative Tools menu. Click Start and choose All Programs, Administrative Tools, and then the tool you want to use. You can use all the tools listed in the table to manage local and remote resources.

For example, if you connect to a new computer in IIS Manager, you can manage all its sites and services remotely from your system.

<table>
<thead>
<tr>
<th>Administration Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Users and Computers</td>
<td>Manages domain user, group, and computer accounts.</td>
</tr>
<tr>
<td>Computer Management</td>
<td>Manages services, storage, and applications. The Services And Applications node provides quick access to Indexing Service catalogs and IIS sites and servers.</td>
</tr>
</tbody>
</table>
When you add services to a server, the tools needed to manage those services are automatically installed. If you want to manage these servers remotely, you might not have these tools installed on your workstation. In that case, you need to install the administration tools on the workstation you’re using.

Web Administration Techniques

Web administrators have many options for managing IIS. The key administration tools are:

- IIS Manager (InetMgr.exe)
- IIS Administration objects made available through the IIS 7.0 WMI provider
- IIS command-line administration tool (AppCmd.exe)

IIS Manager provides the standard administration interface for IIS. To start IIS Manager, click Start and choose All Programs, Administrative Tools, and then Internet Information Services (IIS) Manager. When started, IIS Manager displays the Start page

<table>
<thead>
<tr>
<th>Administration Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Sources (ODBC)</td>
<td>Configures and manages Open Database Connectivity (ODBC) data sources and drivers. Data sources link Web front ends with database back ends.</td>
</tr>
<tr>
<td>DNS</td>
<td>Public Internet sites must have fully qualified domain names (FQDNs) to resolve properly in browsers. Use the Domain Name System (DNS) administrative snap-in to manage the DNS configuration of your Windows DNS servers.</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Allows you to view and manages events and system logs. If you keep track of system events, you’ll know when problems occur.</td>
</tr>
<tr>
<td>Internet Information Services (IIS) 6.0 Manager</td>
<td>Manages Web and application server resources that were designed for IIS 6. This tool is included for backward compatibility only.</td>
</tr>
<tr>
<td>Internet Information Services (IIS) Manager</td>
<td>Manages Web and application server resources that were designed for IIS 7.0.</td>
</tr>
<tr>
<td>Web Management Service (WMSVC)</td>
<td>Allows you to use the IIS Manager to manage Web and application server resources on remote servers.</td>
</tr>
<tr>
<td>Reliability and Performance Monitor</td>
<td>Tracks system reliability and performance allowing you to pinpoint performance problems.</td>
</tr>
<tr>
<td>Services</td>
<td>Views service information, starts and stops system services, and configures service logons and automated recoveries.</td>
</tr>
</tbody>
</table>
shown in Figure 1-1 and automatically connects to the local IIS installation, if it’s available. On the Start page, you have the following options:

- **Connect to localhost**  Connects you to the IIS installation on the local computer
- **Connect to a server**  Allows you to connect to a remote server
- **Connect to a site**  Allows you to connect to a specific Web site on a designated Web server
- **Connect to an application**  Allows you to connect to a specific Web application on a designated site and server

![Internet Information Services (IIS) Manager](image)

**Figure 1-1**  You can access servers, sites, and applications by using IIS Manager.

As discussed previously, remote access to an IIS server is controlled by the WMSVC. When you install and start WMSVC on an IIS server, it listens on port 8172 on all unassigned IP addresses and allows remote connections from authorized user accounts. You can connect to a remote server by following these steps:

1. In Internet Information Services (IIS) Manager, click Start Page in the console tree and then click Connect To A Server. This starts the Connect To A Server wizard.

2. Type or select the server name in the Server Name box. For a server on the Internet, type the FQDN of the server, such as www.adatum.com. For a server on the local network, type the computer name, such as WEBSVR87. Port 80 is the default port for connections. As necessary, you can provide the port to which you
want to connect. For example, if you want to connect to the server on port 8080, you would follow the server name by :8080, such as WEBSVR87:8080.

3. After you type the server name (and optionally the port number), click Next. IIS Manager will then try to use your current user credentials to log on to the server. If this fails, you’ll need to provide the appropriate credentials on the presented Provide Credentials page before clicking Next to continue. Click Finish to complete the connection.

Tip If IIS Manager displays a connection error stating that the remote server is not accepting connections, you’ll need to log on locally or through remote desktop. Once logged on, check to ensure the Management Service is started and configured properly. For more information, see the “Enabling and Configuring Remote Administration” section of Chapter 3.

You can connect to a specific Web site on a designated server by following these steps:

1. In Internet Information Services (IIS) Manager, click Start Page in the console tree and then click Connect To A Site. This starts the Connect To A Site Wizard.
2. Type or select the server name in the Server Name box, such as TESTSVR22. In the Site Name box, type or select the name of the Web site to which you want to connect, such as Default Web Site.
3. Click Next. IIS Manager will then try to use your current user credentials to log on to the server. If this fails, you’ll need to provide the appropriate credentials on the presented Provide Credentials page before clicking Next to continue. Click Finish to complete the connection.

You can connect to a specific application on a designated site and server by following these steps:

1. In Internet Information Services (IIS) Manager, click Start Page in the console tree and then click Connect To An Application. This starts the Connect To An Application Wizard.
2. Type or select the server name in the Server Name box, such as TESTSVR22. In the Site Name box, type or select the name of the Web site to which you want to connect, such as Default Web Site.
3. In the Application Name box, type or select the relative path of the Web application to which you want to connect, such as /MyApplication or /Apps/Myapp.
4. Click Next. IIS Manager will then try to use your current user credentials to log on to the server. If this fails, you’ll need to provide the appropriate credentials on the presented Provide Credentials page before clicking Next to continue. Click Finish to complete the connection.
As Figure 1-2 shows, IIS Manager has been completely redesigned for IIS 7.0. Instead of being a snap-in for the Microsoft Management Console, IIS Manager is now a stand-alone application with a browser-like interface. Once you connect to a server, site, or application, IIS Manager automatically connects to these installations upon startup. You can change this behavior by disconnecting from the remote server while in IIS Manager. See Chapter 3 for more information on using IIS Manager.

IIS 7.0 introduces the concept of delegated administration. With delegated administration, a machine administrator can delegate administrative control safely and securely. Delegated administration allows different levels of the configuration hierarchy to be managed by other users, such as site administrators or application developers. In a standard configuration, the default delegation state limits write access to most configuration settings to machine administrators only, and you must explicitly modify the delegation settings to grant write access to others. You’ll learn more about IIS security and delegation in Chapter 10, “Managing Web Server Security.”

IIS Manager and other graphical tools provide just about everything you need to work with IIS 7.0. Still, there are times when you might want to work from the command line, especially if you want to automate installation or administration tasks. To help you with all your command-line needs, IIS 7.0 includes the IIS command-line administration tool (AppCmd.exe). AppCmd.exe is located in the %SystemRoot%\System32\Inetsrv directory. By default, this directory is not in your command path. Because of this, you’ll need either to add this directory to the default path or change to this directory each time you want to use this tool. Add this directory temporarily to your default path by typing the following at an elevated command prompt:

```
path %PATH%;%SystemRoot%\System32\Inetsrv
```
Then add this directory permanently to your default path by typing the following at an elevated command prompt:

```bash
setx PATH %PATH%;%SystemRoot%\System32\inetsrv
```

**Note**  You use Path to temporarily update the command path for the current window. You use SETX PATH to permanently update the command path for future command windows.

Table 1-3 provides a summary of the core set of administration objects for the IIS command-line administration tool.

**Table 1-3  Administration Objects for the IIS Command-Line Administration Tool**

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Description</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP</td>
<td>Allows you to create and manage Web application settings by using related list, set, add, and delete commands</td>
<td>list, set, add, and delete</td>
</tr>
<tr>
<td>APPPOOL</td>
<td>Allows you to create and manage application pools by using related list, set, add, delete, start, stop, and recycle commands</td>
<td>list, set, add, delete, start, stop, and recycle</td>
</tr>
<tr>
<td>BACKUP</td>
<td>Allows you to create and manage backups of your server configuration by using list, add, delete, and restore commands</td>
<td>list, add, delete, and restore</td>
</tr>
<tr>
<td>CONFIG</td>
<td>Allows you to manage general configuration settings by using related list, set, search, lock, unlock, clear, reset, and migrate commands</td>
<td>list, set, search, lock, unlock, clear, reset, and migrate</td>
</tr>
<tr>
<td>MODULE</td>
<td>Allows you to manage IIS modules by using related list, set, add, delete, install, and uninstall commands</td>
<td>list, set, add, delete, install, and uninstall</td>
</tr>
<tr>
<td>REQUEST</td>
<td>Allows you to list current HTTP requests by using a related list command</td>
<td>list</td>
</tr>
<tr>
<td>SITE</td>
<td>Allows you to create and manage virtual sites by using related list, set, add, delete, start, and stop commands</td>
<td>list, set, add, delete, start, and stop</td>
</tr>
<tr>
<td>TRACE</td>
<td>Allows you to manage failed request tracing by using related list, configure, and inspect commands</td>
<td>list, configure, and inspect</td>
</tr>
<tr>
<td>VDIR</td>
<td>Allows you to create and manage virtual directory settings by using related list, set, add, and delete commands</td>
<td>list, set, add, and delete</td>
</tr>
<tr>
<td>WP</td>
<td>Allows you to list running worker processes by using a related list command</td>
<td>list</td>
</tr>
</tbody>
</table>
The basics of working with the IIS command-line administration tool are straightforward. Most administration objects support these basic commands:

- **ADD** Creates a new object with the properties you specify.
- **DELETE** Deletes the object you specify.
- **LIST** Displays a list of related objects. Optionally, you can specify a unique object to list, or you can type one or more parameters to match against object properties.
- **SET** Sets parameters on the object specified.

Some objects support other commands, including:

- **RECYCLE** Recycles the object you specify by deleting it and then re-creating it
- **START** Starts the object you specify if it is stopped
- **STOP** Stops the object you specify if it is started or otherwise active

To type commands, use the following basic syntax:

```
appcmd Command <Object-type>
```

where `Command` is the action to perform, such as list, add, or delete, and `Object-type` is the object on which you want to perform the action, such as app, site, or vdir. Following this, if you wanted to list the configured sites on a server, you could type the following command at an elevated command prompt:

```
appcmd list site
```

Because the IIS command-line administration tool will also accept plural forms of object names, such as apps, sites, or vdirs, you could also use:

```
appcmd list sites
```

In either case, the resulting output is a list of all configured sites on the server with their related properties, such as:

```
SITE "Default Web Site" (id:1,bindings:http/*:80:,state:Started)
```

You’ll find a comprehensive discussion of using the IIS command-line administration tool in Chapter 4, “Managing IIS 7.0 from the Command Line.” In addition, you will see examples of using this tool throughout the book.
Chapter 2

Deploying IIS 7.0 in the Enterprise

Before you deploy Internet Information Services (IIS) 7.0, you should carefully plan the machine and administration architecture. As part of your planning, you need to look closely at the protocols and roles IIS will use and modify both server hardware and technology infrastructure accordingly to meet the requirements of these roles on a per-machine basis. Your early success with IIS 7.0 will largely depend on your understanding of the ways you can use the software and in your ability to deploy it to support these roles.

IIS 7.0 Protocols

TCP/IP is a protocol suite consisting of Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP/IP is required for internetwork communications and for accessing the Internet. Whereas TCP operates at the transport layer and is a connection-oriented protocol designed for reliable end-to-end communications, IP operates at the network layer and is an internetworking protocol used to route packets of data over a network.

IIS 7.0 uses protocols that build on TCP/IP, including:

- Hypertext Transfer Protocol (HTTP)
- Secure Sockets Layer (SSL)
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)

HTTP and SSL

As you probably already know, HTTP is an application-layer protocol that makes it possible to publish static and dynamic content on a server so that it can be viewed in client applications, such as Microsoft Windows Internet Explorer. Publishing a Web document is a simple matter of making the document available in the appropriate directory on an HTTP server and assigning the appropriate permissions so that an HTTP client application can access the document. An HTTP session works like this:

1. The HTTP client application uses TCP to establish a connection to the HTTP server. The default (well-known) port used for HTTP connections is TCP port 80. You can configure servers to use other ports as well. For example, TCP port 8080 is a popular alternative to TCP port 80 for sites that are meant to have limited access.
2. After connecting to the server, the HTTP client application requests a Web page or other resource from the server. In the client application, users specify the pages or resources they want to access by using a Web address, otherwise known as a Uniform Resource Locator (URL).

3. The server responds to the request by sending the client the request resource and any other related files, such as images, that you've inserted into the requested resource. If you've enabled the HTTP Keep-Alive feature on the server, the TCP connection between the client and server remains open to speed up the transfer process for subsequent client requests. Otherwise, the TCP connection between the client and server is closed and the client must establish a new connection for subsequent transfer requests.

That in a nutshell is essentially how HTTP works. The protocol is meant to be simple yet dynamic, and it is the basis upon which the World Wide Web is built.

With HTTP, you can configure access to documents so that anyone can access a document or so that documents can be accessed only by authorized individuals. To allow anyone to access a document, you configure the document security so that clients can use Anonymous authentication. With Anonymous authentication, the HTTP server logs on the user automatically using a guest account, such as IUSR. To require authorization to access a document, configure the document security to require authentication using one of the available authentication mechanisms, such as Basic authentication, which requires a user to type a user name and password.

You can use Secure Sockets Layer (SSL) to enable Hypertext Transfer Protocol Secure (HTTPS) transfers. SSL is an Internet protocol used to encrypt authentication information and data transfers passed between HTTP clients and HTTP servers. With SSL, HTTP clients connect to Web pages using URLs that begin with https://. The https prefix tells the HTTP client to try to establish a connection using SSL. The default port used with secure connections is TCP port 443 rather than TCP port 80. See Chapter 10, “Managing Web Server Security,” for more information on SSL.

FTP

FTP is an application-layer protocol that makes it possible for client applications to retrieve files from or transfer files to remote servers. FTP predates HTTP, and its usage is in decline as compared to HTTP. With FTP, you can publish a file so that a client can download it by making the file available in the appropriate directory on an FTP server and assigning the appropriate permissions so that an FTP client application can access the document. To upload a file to an FTP server, you must grant an FTP client application permission to log on to the server and access directories used for uploading files.
An FTP session works like this:

1. The FTP client application uses TCP to establish a connection to the FTP server. The default (well-known) port used for FTP connections is TCP port 21. FTP servers listen on this port for client connection requests. After the client and server establish a connection, the server randomly assigns the client a TCP port number above 1023. This initial TCP connection (with port 21 for the server and a random port for the client) is then used for transmission of FTP control information, such as commands sent from the client to the server and response codes returned by the server to the client.

2. The client then issues an FTP command to the server on TCP port 21. Standard FTP commands include GET for downloading a file, CD for changing directories, PUT for uploading files, and BIN for switching to binary mode.

3. When the client initiates a data transfer with the server, the server opens a second TCP connection with the client for the data transfer. This connection uses TCP port 20 on the server and a randomly assigned TCP port above 1023 on the client. After the data transfer is complete, the second connection goes in a wait state until the client initiates another data transfer or the connection times out.

That in a nutshell is how FTP works. As you can see, FTP is a bit clunkier than HTTP, but it is still fairly simple.

Real World   What sets FTP and HTTP apart is primarily the way you transfer files. FTP transfers files as either standard text or encoded binaries. HTTP has the capability to communicate the file format to the client, and this capability allows the client to determine how to handle the file. If the client can handle the file format directly, it renders the file for display. If the client has a configured helper application, such as with PDF documents, the client can call the helper application and let it render the file for display within the client window. The component that makes it possible for HTTP clients and servers to determine file format is their support for the Multipurpose Internet Mail Extensions (MIME) protocol. Using the MIME protocol, an HTTP server identifies each file with its corresponding MIME type. For example, an HTML document has the MIME type text/html, and a GIF image has the MIME type image/gif.

With FTP, you can allow anonymous downloads and uploads in addition to restricted downloads and uploads. To allow anyone to access a file, configure directory security so that clients can use Anonymous authentication. With Anonymous authentication, the FTP server logs the user on automatically using a guest account and allows the anonymous user to download or upload files as appropriate. To require authorization to log on and access a directory, configure directory security to require authentication using one of the available authentication mechanisms, such as Basic authentication, which requires a user to type a user name and password prior to logging on and downloading or uploading files.
SMTP

SMTP is an application-layer protocol that makes it possible for client applications to send e-mail messages to servers and for servers to send e-mail messages to other servers. A related protocol for retrieving messages from a server is Post Office Protocol version 3 (POP3). In IIS 6, full implementations of Simple Mail Transfer Protocol (SMTP) and Post Office Protocol version 3 (POP3) are included. IIS 7.0 does not include SMTP or POP3 services.

With IIS 7.0, a Web application can send e-mail on behalf of a user by using the SMTP E-mail component of Microsoft ASP.NET. An SMTP session initiated by a Web application works like this:

1. The Web application generates an e-mail message in response to something a user has done.
2. The System.Net.Mail API (a component of ASP.NET) delivers the email to an online SMTP server or stores the message on disk where it is stored for later delivery.
3. When sending mail to an SMTP server, the IIS server uses TCP port 25 to establish the connection. SMTP can be running on the local machine or on a different machine.

That is essentially how SMTP is used by Web applications. Microsoft doesn’t provide other e-mail features as a part of IIS. However, a separate SMTP Server component is included as an optional feature that you can install on a computer running a Windows Server operating system.

IIS 7.0 Roles

You can deploy IIS on both desktop and server platforms. On desktop platforms, you can use IIS 7.0 for designing, building, and testing dynamic Web sites and Web applications. On server platforms, IIS 7.0 can have several different roles:

- **Application server** Application servers host distributed applications built using ASP.NET, Enterprise Services Network Support, and Microsoft .NET Framework 3.0. You can deploy application servers with or without Web Server (IIS) support. When you deploy an application server without Web Server (IIS) support, you configure application services through the application server core APIs and by adding or removing role services. Because the server lacks IIS configuration and administration components, you won’t have any of the common IIS features and won’t be able to configure the server by using IIS 7.0 modules, and you can’t manage the server by using IIS 7.0 administration tools. To avoid these limitations, you should install the application server with Web Server (IIS) support. You’ll then be able to use IIS features to better manage the application server installation.
Web server  Web servers use the services bundled in IIS 7.0 to host Web sites and Web applications. Web sites hosted on a Web server can have both static content and dynamic content. You can build Web applications hosted on a Web server by using ASP.NET and .NET Framework 3.0. When you deploy a Web Server, you can manage the server configuration by using IIS 7.0 modules and administration tools.

Microsoft Windows SharePoint Services server  Computers running Windows SharePoint Services enable team collaboration by connecting people and information. A SharePoint Services server is essentially a Web server running a full installation of IIS and using managed applications that provide the necessary collaboration functionality. When you deploy SharePoint Services, you can manage the server by using IIS 7.0 modules and administration tools in addition to several SharePoint-specific tools, including SharePoint Central Administration and the SharePoint Products and Technologies Configuration Wizard.

Table 2-1 organizes the 75 configuration features available for the three server roles into 14 general categories. Each entry for a particular configuration feature has one of the following values:

- **Available**  Indicates a feature that is available for selection during installation. You can add available features as necessary to optimize the configuration of your server.

- **Default**  Indicates a feature that is selected for installation by default. Although you may be able to deselect default features during setup, you should not do this in most cases because it could adversely affect the server performance or necessary core functionality.

- **Included**  Indicates an included but unlisted feature that is part of the IIS server core. With application servers, these features are included only when you choose to install Web Server (IIS) support. With Web Server and SharePoint Services Server, these features are included automatically.

- **Not Installed**  Indicates an available feature that is not installed as part of the standard setup. With Web and SharePoint Services servers, you can configure these features after installation by enabling the related modules. With application servers, these features are configurable after installation only when you choose to install Web Server (IIS) support or modify the role services associated with an installed Web server role.

- **Required**  Indicates a feature that is required in order to install the server role. Setup selects required features automatically during installation.

- **N/A**  Indicates a feature that is not applicable or available for a particular server role.
Web Common  Indicates a feature installed by default as part of the common
Web Server (IIS) features of an application server.

WPASS Required  Indicates an application server feature required for Windows
Process Activation Service Support.

Table 2-1  Configuration Features for Application and Web Servers and Computers
Running SharePoint Services

<table>
<thead>
<tr>
<th>Feature</th>
<th>Application Server</th>
<th>Web Server</th>
<th>SharePoint Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>.NET Framework 3.0</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.NET Framework 3.0</td>
<td>Required</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Application Server Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Server Foundation</td>
<td>Default</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>COM+ Network Access</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>TCP Port Sharing</td>
<td>WPASS Required</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Web Server (IIS) Support</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Application Development Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.NET Extensibility</td>
<td>Web Common; WPASS Required</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>ASP</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>ASPNET</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>CGI</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>ISAPI Extensions</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>ISAPI Filters</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>Server-Side Includes</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td><strong>Common HTTP Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Document</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>Directory Browsing</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>HTTP Errors</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>HTTP Redirection</td>
<td>Web Common</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Static Content</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
</tbody>
</table>
Table 2-1  Configuration Features for Application and Web Servers and Computers Running SharePoint Services

<table>
<thead>
<tr>
<th></th>
<th>Application Server</th>
<th>Web Server</th>
<th>SharePoint Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Distributed Transaction Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incoming Remote Transaction Support</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Outgoing Remote Transaction Support</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>WS-Atomic Transaction Support</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Extended Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Cache</td>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Managed Engine</td>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Token Cache</td>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>HTTP Trace</td>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td>URI Cache</td>
<td>Not Installed</td>
<td>Not Installed</td>
<td>Not Installed</td>
</tr>
<tr>
<td><strong>FTP Publishing Service</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP Management Console</td>
<td>Not Installed</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Not Installed</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
<tr>
<td><strong>Health and Diagnostics Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Logging</td>
<td>Not Installed</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
<tr>
<td>HTTP Logging</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>Logging Tools</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>ODBC Logging</td>
<td>Not Installed</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
<tr>
<td>Request Monitor</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>Tracing</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td><strong>IIS Server Core</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous Authentication</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Configuration Validation</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>HTTP Cache</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Protocol Support</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
</tbody>
</table>
Table 2-1  Configuration Features for Application and Web Servers and Computers Running SharePoint Services

<table>
<thead>
<tr>
<th>Feature</th>
<th>Application Server</th>
<th>Web Server</th>
<th>SharePoint Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Content Compression</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>Static Content Compression</td>
<td>Web Common</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>Client Certificate Mapping</td>
<td>Web Common</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digest Authentication</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>IIS Client Certificate Mapping</td>
<td>Web Common</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP and Domain Restrictions</td>
<td>Web Common</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Request Filtering</td>
<td>Web Common; WPASS Required</td>
<td>Default</td>
<td>Available</td>
</tr>
<tr>
<td>URL Authorization</td>
<td>Web Common</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Windows Authentication</td>
<td>Web Common</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Web Management Tools</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS Management Console</td>
<td>Default</td>
<td>Default</td>
<td>Required</td>
</tr>
<tr>
<td>IIS Management Scripts and Tools</td>
<td>Web Common</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
<tr>
<td>IIS Management Service</td>
<td>Web Common</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
<tr>
<td>IIS 6 Management Compatibility</td>
<td>Not Installed</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>IIS Metabase Compatibility</td>
<td>Not Installed</td>
<td>Available</td>
<td>Required</td>
</tr>
<tr>
<td>IIS 6 WMI Compatibility</td>
<td>Not Installed</td>
<td>Available</td>
<td>Not Installed</td>
</tr>
</tbody>
</table>
When configuring application servers, Web servers, and SharePoint Services, it is important to understand exactly what comprises the .NET Framework 3.0. The Microsoft .NET Framework 3.0 is a managed code programming model for Windows. It combines the power of the .NET Framework 2.0 with four new technologies:

- **Windows CardSpace (WCS)** A suite of .NET technologies for managing digital identities. Windows CardSpace supports any digital identity system and gives users consistent control of their digital identities. A digital identity can be as simple as an e-mail address and password used to log on to a Web site, or it can include a user’s full contact and logon information. Client applications display each digital identity as an information card. Each card contains information about a particular digital identity, including what provider to contact to acquire...
a security token for the identity. By selecting a card and sending it to a provider such as Amazon or Yahoo!, users can validate their identity and log on to the service offered by the site.

- **Windows Communication Foundation (WCF)** A suite of .NET technologies for building and running connected systems. WCF supports a broad array of distributed systems capabilities to provide secure, reliable, and transactional messaging along with interoperability. Servers establish distributed communications through service endpoints. Service endpoints have an endpoint address, a binding that specifies how the endpoint can communicate, and a contract description that details what an endpoint communicates.

- **Windows Presentation Foundation (WPF)** A suite of .NET technologies for building applications with attractive and effective user interfaces. WPF supports tight integration of application user interfaces, documents, and media content, allowing developers to create a unified interface for all types of documents and media. This means that applications can use the same interface for displaying forms, controls, fixed-format documents, on-screen documents, 2D images, 3D images, video, and audio.

- **Windows Workflow Foundation (WF)** A suite of .NET technologies for building workflow-enabled applications on Windows. WF provides a rules engine that allows for the declarative modeling of units of application logic within the scope of an overall business process. What this means is that developers can use WF to model and implement the necessary programming logic for a business process from start to finish.

To support applications written for IIS 6, you can deploy IIS 7.0 with IIS 6 compatibility enabled. If you have existing IIS 6 server installations, you can also install the IIS 6 Management Compatibility tools to support remote administration of these server installations. You also can deploy IIS 7.0 to support remote administration. You can use both desktop and server platforms for remote administration of other IIS servers in addition to the sites and applications configured on these servers. For remote administration of an IIS server, you must enable the Web Management Service (WMSVC) on the server you want to manage remotely. Then install the Web management tools on the machine you want to use for remote administration.

### Navigating the IIS 7.0 Role Services and Features

As discussed previously, you can deploy IIS 7.0 running on a computer running Windows Server 2008 to support three specific roles: application server, Web server, and Windows SharePoint Services server. You can deploy IIS 7.0 running on a Windows desktop to support designing, building, and testing sites and applications. The components used to support these roles are referred to as either role services or
features, depending on which user interface you are working with. In the sections that follow, I discuss each of the server roles and the related role services.

**Role Services for Application Servers**

You use application servers running on Windows Server 2008 editions to host distributed applications built by using ASP.NET, Enterprise Services, and WCF. Figure 2-1 provides an overview of the related services for application servers.

![Figure 2-1 Role services for application servers.](image)

When you install an application server, only the Application Server Core and Enterprise Services Network Access services are included as standard core features. In addition to the standard core features, you must install the .NET Framework 3.0 components and the Windows Activation Service components. Other components are optional and should be installed based on the specific requirements of the distributed applications you are hosting.

Application servers can use the following general-purpose role services:

- **Application Server Foundation** Provides the core application server functionality through these .NET Framework 3.0 technologies: Windows CardSpace, WCF, WPF, and WF. These technologies allow you to deliver managed-code applications that model business processes.
COM+ Network Access Enables application servers to invoke applications remotely over the network. Applications being invoked must have been built using Enterprise Services and provide support for hosting COM+ components.

TCP Port Sharing Allows multiple applications to share a single TCP port. By using this feature, many Web applications can coexist on the same server in separate, isolated processes while sharing the network infrastructure required for sending and receiving data over TCP ports.

Web Server (IIS) Support Allows the application server to host Web sites with both static and dynamic content. The Web sites support the standard IIS server extensions and allow you to create Web pages containing dynamic content. This allows an application server to host an internal or external Web site or provide an environment for developers to create Web applications. See Table 2-2 for a complete list of IIS features installed by default when you select this feature.

The Windows Process Activation Service supports distributed Web-based applications that use different protocols to transfer information. You can use the following related components:

- .NET Environment Installs the .NET Environment for use with managed code activation.
- Configuration APIs Installs the managed code APIs that allow you to configure the process model.
- Process Model Installs a process model for developing and running applications.

Windows Process Activation Service Support enables the application server to invoke applications remotely over a network by using protocols such as HTTP, Microsoft Message Queueing (MSMQ), named pipes, and TCP. This allows applications to start and stop dynamically in response to incoming requests, resulting in improved performance and enhanced manageability. To specify which protocols an application server can use with Windows Process Activation, you can use the following related role services:

- HTTP Activation Supports process activation over HTTP. This is the standard activation method used by most Web applications. Applications that support HTTP Activation can start and stop dynamically in response to requests that arrive via HTTP. With HTTP, the application and the computers with which it communicates need to be online to pass active communications back and forth without the need for queuing requests.
- Message Queuing Activation Supports process activation over Microsoft Message Queue (MSMQ). This activation method is used when the application server runs distributed messaging applications. Applications that support MSMQ Activation and message queuing can start and stop dynamically in
response to requests that arrive via MSMQ. With message queuing, source applications send messages to queues, where they are stored temporarily until target applications retrieve them. This queuing technique allows applications to communicate across different types of networks and with computers that may be offline.

- **Named Pipes Activation**  Supports process activation over named pipes. Applications that support Named Pipes Activation can start and stop dynamically in response to requests that arrive via named pipes. You use this activation method when Web applications communicate with older versions of the Windows operating system. A *named pipe* is a portion of memory that one process can use to pass information to another process such that the output from one process is the input of the other process. Named pipes have standard network addresses such as `\\\Pipe\Sql\Query`, which a process can reference on a local machine or a remote machine. The Named Pipes protocol is used primarily for local or remote connections by applications written for Microsoft Windows NT, Windows 98, and earlier versions of Windows.

- **TCP Activation**  Supports process activation over TCP. Applications that support TCP Activation can start and stop dynamically in response to requests that arrive via TCP. With TCP, the application and the computers with which it communicates need to be online so they can pass active communications back and forth without the need for queuing requests.

When using Windows Process Activation Support, these additional roles services may be required:

- **Non-HTTP Activation**  Provides non-HTTP activation support using any of the following: MSMQ, named pipes, and TCP. IIS installs this feature as a WCF Activation component.

- **Message Queuing Server**  Provides the necessary server functions for message queuing.

**Tip**  Each of the Windows Process Activation Support features has a related set of required role services. With HTTP Activation, all the features listed as Web Common in Table 2-1 are required. With Message Queuing Activation, Message Queuing Server and Non-HTTP Activation are required. With TCP Activation and Named Pipes Activation, Non-HTTP Activation is required.

When applications communicate with each other, they may need to perform various types of transactions, such as queries to retrieve data stored in a database or a data submission to update data stored in a database. When the application server hosts the database or needs to query a single database to complete a transaction, transactions are fairly straightforward. Things get complex fast, though, when you are working with multiple databases hosted on multiple computers. A transaction that involves multiple
databases hosted on multiple computers is referred to as a distributed transaction. With distributed transactions, you need a way to guarantee that all the data you need is either retrieved or submitted as appropriate, and this is where Distributed Transactions support comes into the picture. Distributed Transactions support provides services that help ensure that distributed transactions are successfully completed.

To enable Distributed Transactions support on an application server, you can use the following related role services:

- **Incoming Remote Transactions** Provides distributed transaction support to help ensure that incoming remote transactions are successfully completed.
- **Outgoing Remote Transactions** Provides distributed transaction support to help ensure that outgoing remote transactions are successfully completed.
- **WS-Atomic Transactions** Provides distributed transaction support for applications that use two-phase commit transactions with Simple Object Access Protocol (SOAP)-based exchanges. SOAP-based exchanges contain text-based commands that are formatted with XML. If you plan to use SOAP for two-phase commit transactions, you’ll also need to set and configure HTTP endpoints.

**Real World** WS-Atomic Transactions use SSL to encrypt network traffic when communicating with clients. To use SSL, you must install a server authentication certificate suitable for SSL encryption on the WS-AT site in IIS. If you obtain a certificate from a certificate authority (CA), you can import the certificate as part of the setup process. For small-scale and test environments, you also have the option of creating a self-signed certificate during setup. The drawback of this type of certificate is that you must install it manually on clients.

In your deployment planning, there is a distinct advantage to deploying an application server with Web Server support. When you deploy an application server with Web Server support, you can configure application services using the APIs provided by ASP.NET and the .NET Framework. Because the server includes IIS configuration and administration components, you’ll have all of the common IIS features available and will be able to configure the server by using the IIS 7.0 modules and the IIS 7.0 administration tools.

**Role Services for Windows Desktops and Web Servers**

Web servers running on Windows Vista desktop editions or on Windows Server 2008 editions can host Web sites and Web applications. Figure 2-2 provides an overview of the related role services for Web servers.
As summarized in Table 2-1, when you install a Web server, several configuration features are installed automatically as part of the server core, and other features are installed by default (if applicable for the operating system version you are using). These features represent core internal components in addition to the recommended minimum and required components for managing a Web server and publishing a Web site. In most installations of IIS 7.0, you will want to install additional features based on the specific requirements of the Web sites and Web applications the server is hosting.
As discussed in Chapter 1, “IIS 7.0 Administration Overview,” Windows Server editions and Windows Vista editions have different sets of supported features. Table 2-2 provides a feature comparison based on Windows version and edition. The table also lists the related request limitations of Windows versions and editions. Because Windows Server editions have no request limitations, you can use them in live production environments. Because Windows Vista editions have severe request limitations, they are best suited for individual administrator or developer use and use in test and development environments.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IIS Server Core</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous Authentication</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Validation</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP Cache</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol Support</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Common HTTP Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Document</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Directory Browsing</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP Errors</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>HTTP Redirection</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Static Content</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Application Development Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.NET Extensibility</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>ASP</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>ASP.NET</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>CGI</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>ISAPI Extensions</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>ISAPI Filters</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Table 2-2  Feature Comparison Based on Windows Version and Edition

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server-Side Includes</strong></td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Health and Diagnostics Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Logging</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP Logging</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Logging Tools</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>ODBC Logging</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Request Monitor</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Tracing</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>Client Certificate Mapping Authentication</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Digest Authentication</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>IIS Client Certificate Mapping Authentication</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>IP and Domain Restrictions</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Request Filtering</td>
<td>Default</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>URL Authorization</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Windows Authentication</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Performance Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static Content Compression</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Table 2-2  Feature Comparison Based on Windows Version and Edition

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Content Compression</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td><strong>Web Management Tools</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS Management Console</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>IIS Management Scripts and Tools</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>IIS Management Service</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>IIS 6 Management Compatibility</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>IIS Metabase compatibility</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>IIS 6 WMI Compatibility</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>IIS 6 Scripting Tools</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td>IIS 6 Management Console</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>FTP Publishing Service</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP Management Console</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>FTP Server</td>
<td>Available</td>
<td>Available</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Windows Activation Service</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.NET Environment</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Configuration APIs</td>
<td>Default</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Process Model</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td><strong>Limitations</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Execution Limit</td>
<td>Unlimited</td>
<td>10</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
As the table shows, many different features are available with Web servers. I’ll discuss each of the features I haven’t previously discussed in this section, and you’ll also find detailed information on these features in appropriate chapters throughout this book. In the appendix, “Comprehensive IIS 7.0 Module and Schema Reference,” you’ll also find a detailed description of features with related configuration modules.

The IIS Server Core features provide the foundation functions for IIS. You can use these features as follows:

- **Anonymous Authentication**  
  Supports anonymous access to a server. With anonymous access, any user can access content without having to provide credentials. Each server has to have at least one authentication mechanism configured, and this is the default mechanism.

- **Configuration Validation**  
  Validates the configuration of a server and its applications. If someone improperly configures a server or application, IIS 7.0 generates errors that can help detect and diagnose the problem.

- **HTTP Cache**  
  Improves performance by returning a processed copy of a requested Web page from cache, resulting in reduced overhead on the server and faster response times. IIS 7.0 supports several levels of caching including output caching in user mode and output caching in kernel mode. When you enable kernel-mode caching, cached responses are served from the kernel rather than from IIS user mode, giving IIS an extra boost in performance and increasing the number of requests IIS can process.

- **Protocol Support**  
  Provides support for common protocols used by Web servers, including HTTP keep-alives, custom headers, and redirect headers. **HTTP keep-alives** allows clients to maintain open connections with servers, which speeds up the request process once a client has established a connection with a server. **Custom headers** and **redirect headers** allow you to optimize the way IIS works to support advanced features of the HTTP 1.1 specification.

The Common HTTP features install the common services required for serving Web content. You can use these features as follows:

- **Default Document**  
  Supports displaying of default documents. When you’ve enabled this feature and a user enters a request with a trailing ‘/’, such as http://www.adatum.com/, IIS can redirect the request to the default document for the Web server or directory. For best performance, you should list the default document you use the most first and reduce the overall list of default documents to only those necessary.

- **Directory Browsing**  
  Supports directory browsing functionality. When you’ve enabled default documents but there is no current default document, IIS can use this feature to generate a listing of the contents of the specified directory. If you haven’t enabled the default document or directory browsing features, and a client requests a directory-level URL, IIS returns an empty response.
HTTP Errors  Supports custom error and detailed error notification. When you enable this feature and the server encounters an error, the server can return a customer error page to all clients regardless of location, a detailed error message to all clients regardless of location, or a detailed error for local clients and a custom error page for remote clients. IIS displays a custom error page based on the type of HTTP error that occurred.

HTTP Redirection  Supports redirection of HTTP requests to send users from an old site to a new site. In the default configuration for redirection, all requests for files in the old location are mapped automatically to files in the new location you specify. You can customize this behavior in several ways.

Static Content  Supports static Web content, such as HTML documents and GIF or JPEG images. The staticContent/mimeMap configuration collection in the applicationHost.config file determines the list of file extensions supported.

Note  Each of these common features has a related IIS 7.0 native module that Setup installs and activates when you select the feature. For the exact mapping of common features to their corresponding native modules, see the appendix. You'll learn more about working with these features in Chapter 5, “Managing Global IIS Configuration.”

The Application Development features install the features required for developing and hosting Web applications. You can use these features as follows:

.NET Extensibility  Enables a Web server to host .NET Framework applications and provides the necessary functionality for IIS integration with ASP.NET and the .NET Framework. When you are working with managed modules, you must also enable the Managed Engine. The Managed Engine is the actual server component that performs the integration functions.

ASP  Enables a Web server to host classic Active Server Pages (ASP) applications. Web pages that use ASP are considered to be dynamic because IIS generates them at request time. To use ASP, you must also use ISAPI Extensions.

ASP.NET  Enables a Web server to host ASP.NET applications. Web pages that use ASP.NET are considered to be dynamic because they are generated at request time. To use ASP.NET, you must also use .NET Extensibility, ISAPI Extensions and ISAPI Filters.

CGI  Enables a Web server to host Common Gateway Interface (CGI) executables. CGI describes how executables specified in Web addresses, also known as gateway scripts, pass information to Web servers. By default, IIS handles all files with the .exe extension as CGI scripts.

ISAPI Extensions  Allows ISAPI Extensions to handle client requests. In the IIS server core, several components rely on handlers that are based on ISAPI Extensions, including ASP and ASP.NET. By default, IIS handles all files with the .dll extension as ISAPI Extensions.
ISAPI Filters  Allows ISAPI Filters to modify Web server behavior. IIS uses ISAPI Filters to provide additional functionality. When you select ASP.NET as part of the initial setup, Setup configures an ASP.NET filter to provide this functionality. In applicationHost.config, each version of ASP.NET installed on the Web server must have a filter definition that identifies the version and path to the related filter.

Server-Side Includes  Allows a Web server to parse files with Server-Side Includes (SSI). SSI is a technology that allows IIS to insert data into a document when a client requests it. When this feature is enabled, files with the .stm, .shtm, and .shtml extension are parsed to see if they have includes that should be substituted for actual values. If this feature is disabled, IIS handles .stm, .shtm, and .shtml files as static content, resulting in the actual include command being returned in the request.

Health and Diagnostics features enable you to monitor your servers, sites, and applications and to diagnose problems if they occur. You can use these features as follows:

Custom Logging  Enables support for custom logging. Typically, custom logging uses the ILogPlugin interface of the Component Object Model (COM). Rather than using this feature, Microsoft recommends that you create a managed module and subscribe to the RQ_LOG_REQUEST notification.

HTTP Logging  Enables support for logging Web site activity. You can configure IIS 7.0 to use one log file per server or one log file per site. Use per-server logging when you want all Web sites running on a server to write log data to a single log file. Use per-site logging when you want to track access separately for each site on a server.

Logging Tools  Allows you to manage server activity logs and automate common logging tasks using scripts.

ODBC Logging  Enables support for logging Web site activity to ODBC-compliant databases. In IIS 7.0, ODBC logging is implemented as a type of custom logging.

Request Monitor  Allows you to view details on currently executing requests, the run state of a Web site or the currently executing application domains, and more.

Tracing  Supports tracing of failed requests. Another type of tracing that you can enable after configuration is HTTP tracing, which allows you to trace events and warnings to their sources through the IIS server core.

Security features make it possible to control access to a server and its content. You can use these features as follows:

Basic Authentication  Requires a user to provide a valid user name and password to access content. All browsers support this authentication mechanism,
but they transmit the password without encryption, making it possible for a malicious individual to intercept the password as the browser is transmitting it. If you want to require Basic Authentication for a site or directory, you should disable Anonymous Authentication for the site or directory.

- **Client Certificate Mapping Authentication**  Maps client certificates to Active Directory accounts for the purposes of authentication. When you enable certificate mapping, this feature performs the necessary Active Directory certificate mapping for authentication of authorized clients.

- **Digest Authentication**  Uses a Windows domain controller to authenticate user requests for content. Digest Authentication can be used through firewalls and proxies.

- **IIS Client Certificate Mapping Authentication**  Maps SSL client certificates to a Windows account for authentication. With this method of authentication, user credentials and mapping rules are stored within the IIS configuration store.

- **IP and Domain Restrictions**  Allows you to grant or deny access to a server by IP address, network ID, or domain. Granting access allows a computer to make requests for resources but doesn’t necessarily allow users to work with resources. If you require authentication, users still need to authenticate themselves. Denying access to resources prevents a computer from accessing those resources, meaning that denied users can’t access resources even if they could have authenticated themselves.

- **Request Filtering**  Allows you to reject suspicious requests by scanning URLs sent to a server and filtering out unwanted requests. By default, IIS blocks requests for file extensions that could be misused and also blocks browsing of critical code segments.

- **URL Authorization**  Supports authorization based on configuration rules. This allows you to require logon and to allow or deny access to specific URLs based on user names, .NET roles, and HTTP request method.

- **Windows Authentication**  Supports Windows-based authentication using NTLM, Kerberos, or both. You’ll use Windows Authentication primarily in internal networks.

For enhancing performance, IIS supports both static compression and dynamic compression. With static compression, IIS performs an in-memory compression of static content upon first request and then saves the compressed results to disk for subsequent use. With dynamic content, IIS performs in-memory compression every time a client requests dynamic content. IIS must compress dynamic content every time it is requested because dynamic content changes.
When you are trying to improve server performance and interoperability, don’t overlook the value of these extended features:

- **File Cache** Caches file handles for files opened by the server engine and related server modules. If IIS does not cache file handles, IIS has to open the files for every request, which can result in performance loss.

- **Managed Engine** Enables IIS integration with the ASP.NET runtime engine. When you do not configure this feature, ASP.NET integration also is disabled, and no managed modules or ASP.NET handlers will be called when pooled applications run in Integrated mode.

- **Token Cache** Caches Windows security tokens for password based authentication schemes, including Anonymous Authentication, Basic Authentication, and Digest Authentication. Once IIS has cached a user’s security token, IIS can use the cached security token for subsequent requests by that user. If you disable or remove this feature, a user must be logged on for every request, which can result in multiple logon user calls that could substantially reduce overall performance.

- **HTTP Trace** Supports request tracing for whenever a client requests one of the traced URLs. The way IIS handles tracing for a particular file is determined by the trace rules that you create.

- **URI Cache** Caches the Uniform Resource Identifier (URI)–specific server state, such as configuration details. When you enable this feature, the server will read configuration information only for the first request for a particular URI. For subsequent requests, the server will use the cached information if the configuration does not change.

You use Web management tools for administration and can divide the available tools into two general categories: those required for managing IIS 7.0 and those required for backward compatibility with IIS 6. You can use the related setup features as follows:

- **IIS Management Console** Installs the Internet Information Services (IIS) Manager, the primary management tool for working with IIS 7.0.

- **IIS Management Scripts and Tools** Installs the IIS command line administration tool and related features for managing Web servers from the command prompt.

- **IIS Management Service** Installs the Web Management Service (WMSVC), which provides a hostable Web core that acts as a standalone Web server for remote administration.

- **IIS Metabase Compatibility** Provides the necessary functionality for backward compatibility with servers running IIS 6 Web sites by installing a component that translates IIS 6 metabase changes to the IIS 7.0 configuration store.
IIS 6 WMI Compatibility  Provides the necessary functionality for scripting servers running IIS 6 Web sites by installing the IIS 6 Windows Management Instrumentation (WMI) scripting interfaces.

IIS 6 Scripting Tools  Provides the necessary functionality for scripting servers running IIS 6 Web sites by installing the IIS 6 Scripting Tools.

IIS 6 Management Console  Installs the Internet Information Services (IIS) 6.0 Manager, which is required to remotely manage servers running IIS 6 sites and to manage FTP servers for IIS 6.

Role Services for Servers Running SharePoint Services

You use servers running Windows SharePoint Services to enable team collaboration by connecting people and information. A server running SharePoint Services is essentially a Web server running a full installation of IIS and using managed applications that provide the necessary collaboration functionality. When you deploy SharePoint Services on a server, you can manage the server by using IIS 7.0 modules and administration tools and several SharePoint-specific tools, including SharePoint Central Administration and the SharePoint Products And Technologies Configuration Wizard. After installation, both management tools will be available on the Administrative Tools menu.

On a SharePoint site, you can host lists and libraries. A list is a collection of information on a site that you share with team members, including announcements, contacts, discussion boards, tasks, and team calendars. A library is a location on a site where you can create, store, and manage the files used by a team. SharePoint sites can host Web pages in addition to lists and libraries, and your Web pages can use static content, dynamic content, or both.

In your deployment planning for servers running SharePoint Services, you must consider several additional issues including the additional security and connectivity requirements that may be necessary for team collaboration. You’ll want to ensure that you carefully protect access to a server running SharePoint Services. You’ll also want to ensure that team members can access the server from remote locations as appropriate for the potential sensitivity of the information they are sharing.

As part of your planning, you’ll need to consider the additional workload produced by SharePoint applications running on the server in addition to resources used by user connections. Windows SharePoint Services has a number of standard applications that run on a server running SharePoint Services, and these applications place an additional burden on the server’s physical resources. Each user connection to a server will place an additional workload on the server, as will the requests and modifications users make.
Setting Up IIS 7.0

The way you set up IIS 7.0 depends on the role and operating system you are using. As discussed previously, you can configure IIS 7.0 to support one of three server roles: application server, Web server, and server running SharePoint Services. You can also configure IIS 7.0 as part of a desktop installation. I discuss deploying IIS 7.0 in each of these situations in the sections that follow.

Installing Application Servers

You can install an application server with or without Web server support by following these steps:

1. Start Server Manager by clicking the Server Manager icon on the Quick Launch toolbar or by clicking Start, Administrative Tools, Server Manager.

2. In Server Manager, select the Roles node in the left pane, and then, under Roles Summary, click Add Roles. This starts the Add Roles Wizard. If the wizard displays the Before You Begin page, read the Welcome page, and then click Next. You can avoid seeing the Welcome page the next time you start this wizard by selecting the Do Not Show Me This Page Again check box before clicking Next.

3. On the Select Server Roles page, select the Application Server role. You’ll then see the Add Features Required For Application Server dialog box. This dialog box lists the features that are required in order to install an application server. Click Add Required Features to close the dialog box and add the .NET Framework 3.0 components and the Windows Process Activation Service components to the application server installation.

4. When you are deploying an application server with Web Server support, you can elect to accept the default common Web features or configure the exact features you’d like to use. If you have not installed Web Server (IIS) components previously and want to select the Web server (IIS) components for installation, select Web Server (IIS), and then click Next twice. Otherwise, just click Next twice to continue.

5. You should now see the Select Role Services page. If not previously installed, select Web Server (IIS) Support to install the application server with Web server support in the standard default configuration. You’ll then see a dialog box listing the additional required roles. After you review the required roles, click Add Required Role Services to close the dialog box.

Note  The required roles are the same as those listed in Table 2-1 as Web Common. I recommend selecting Web Server (IIS) Support if the application server will host Web sites or Web services. This will ensure that Setup selects the required Web Common features by default, and this will be helpful later in the setup process.
6. Select other role services to install as appropriate, and then click Next. If you select a role service with additional required features, you’ll see a dialog box listing the additional required roles. After you review the required roles, click Add Required Role Services to close the dialog box.

7. If you selected the WS-Atomic Transactions feature, you’ll see the Choose A Certificate For SSL Encryption page next. You have the following options:

- **Choose An Existing Certificate For SSL Encryption** Select this option if you previously obtained a certificate from a certification authority (CA) and want to install it for use with the WS-AT site that Setup will configure on the server. If you’ve previously imported certificates using the Certificate snap-in or the Import Certificate Wizard, you’ll see a list of available certificates, and you can click the certificate you want to use. Otherwise, click Import to start the Certificate Import Wizard, and then follow the prompts to import the certificate.

- **Create A Self-Signed Certificate For SSL Encryption** Select this option if you are using WS-Atomic transactions with a limited number of clients or for testing/development purposes and want to create and then automatically install a self-signing certificate for use with the WS-AT site that Setup will configure on the server. You will need to install the same certificate manually on all clients that need to be able to authenticate with the server.

- **Choose A Certificate For SSL Encryption Later** Select this option if you haven’t obtained a certificate from a CA yet but plan to later. When you choose this option, IIS disables SSL on the WS-AT site until you import the certificate, as discussed in Chapter 10.

8. If you selected Web Server (IIS) on the Select Server Roles page, as discussed in Step 5, click Next twice to display the Select Role Services page for Web server features. You can then select the Web server features to install. In most cases, you’ll want to select additional features rather than trying to remove features. When selecting or clearing role services, keep the following in mind before you click Next to continue:

- If you select a role service with additional required features, you’ll see a dialog box listing the additional required roles. After you review the required roles, click Add Required Role Services to accept the additions and close the dialog box. If you click Cancel instead, Setup clears the feature you previously selected.

- If you try to remove a role service that is required based on a previous selection, you’ll see a warning prompt about dependent services that Setup must also remove. In most cases, you’ll want to click Cancel to preserve the previous selection. If you click Remove Dependent Role Services, Setup
Chapter 2  Deploying IIS 7.0 in the Enterprise

will remove the previously selected dependent services, which could cause
the Web server to not function as expected.

9. Click Next. On the Confirm Installation Selections page, click the Print, E-mail,
Or Save This Information link to generate an installation report and display it
in Windows Internet Explorer. You can then use standard Windows Internet
Explorer features to print or save the report. After you’ve reviewed the installa-
tion options and saved them as necessary, click Install to begin the installation
process.

10. When Setup finishes installing the application server with the features you’ve
selected, you’ll see the Installation Results page. Review the installation details to
ensure that all phases of the installation completed successfully. If any portion of
the installation failed, note the reason for the failure, and then use these trouble-
shtooting techniques:

a. Click the Print, E-mail, Or Save The Installation Report link to create or
update the installation report and display it in Windows Internet Explorer.

b. Scroll down to the bottom of the installation report in Windows Internet
Explorer, and then click Full Log (For Troubleshooting Only) to display
the Server Manager log in Notepad.

c. In Notepad, press Ctrl+F, type the current date in the appropriate format
for your language settings, such as 2007-08-30, and then click Find
Next. Notepad will then move through the log to the first Setup entry from
the current date.

d. Review the Server Manager entries for installation problems, and take cor-
rective actions as appropriate.

Installing Web Servers

You can install a Web server by following these steps:

1. Start the Server Manager by clicking the Server Manager icon on the Quick
Launch toolbar or by clicking Start, Administrative Tools, Server Manager.

2. In Server Manager, select the Roles node in the left pane and then, under Roles
Summary, click Add Roles. This starts the Add Roles Wizard. If the wizard dis-
plays the Before You Begin page, read the Welcome page, and then click Next.
You can avoid seeing the Welcome page the next time you start this wizard by
selecting the Do Not Show Me This Page Again check box before clicking Next.

3. On the Select Server Roles page, select the Web Server (IIS) role. You’ll then see
the Add Features Required For Web Server dialog box. This dialog box lists the
features that are required to install a Web server. Click Add Required Features to
close the dialog box and add the Windows Activation Service components to the
Web server installation. Click Next twice to continue.
4. On the Select Role Services page, Setup selects the core set of standard features by default. When selecting or clearing role services, keep the following in mind before you click Next to continue:

- If you select a role service with additional required features, you’ll see a dialog box listing the additional required roles. After you review the required roles, click Add Required Role Services to accept the additions and close the dialog box. If you click Cancel instead, Setup will clear the feature you previously selected.

- If you try to remove a role service that is required based on a previous selection, you’ll see a warning prompt about dependent services that Setup must also remove. In most cases, you’ll want to click Cancel to preserve the previous selection. If you click Remove Dependent Role Services, Setup will also remove the previously selected dependent services, which could cause the Web server to not function as expected.

5. Click Next. On the Confirm Installation Options page, click the Print, E-mail, Or Save This Information link to generate an installation report and display it in Windows Internet Explorer. You can then use standard Windows Internet Explorer features to print or save the report. After you’ve reviewed the installation options and saved them as necessary, click Install to begin the installation process.

6. When Setup finishes installing the application server with the features you’ve selected, you’ll see the Installation Results page. Review the installation details to ensure that all phases of the installation completed successfully. If any portion of the installation failed, note the reason for the failure and then use these troubleshooting techniques:

   a. Click the Print, E-mail, Or Save The Installation Report link to create or update the installation report and display it in Windows Internet Explorer.

   b. Scroll down to the bottom of the installation report in Windows Internet Explorer and then click Full Log (For Troubleshooting Only) to display the Server Manager log in Notepad.

   c. In Notepad, press Ctrl+F, type the current date in the appropriate format for your language settings, such as 2007-08-30, and then click Find Next. Notepad will then move through the log to the first Setup entry from the current date.

   d. Review the Server Manager entries for installation problems and take corrective actions as appropriate.
Installing Windows SharePoint Services

Windows SharePoint Services uses one of two distinctly different configurations: independent server configuration and dependent load-balanced configuration. With an independent server configuration, you install Windows SharePoint Services on a single server that has its own database for storing application and user information. With a dependent load-balanced configuration, you install SharePoint Services on a computer as part of a Web farm where all servers share a Microsoft SQL Server 2000 or SQL Server 2005 database. Although both types of installations are configured using a similar initial setup process, if you want to connect to the SQL Server database and use load balancing, you must configure a server that is part of a Web farm.

Note  Windows SharePoint Services 2008 is a supplement to the Windows Server 2008 operating system. As such, Windows SharePoint Services 2008 is not included in Windows Server 2008 and must be installed separately. Once you’ve downloaded the installer packages from Microsoft and double-clicked each one to install it, you can configure this role using Server Manager, as discussed in this section. However, because SharePoint is a supplement, the wizard pages and related setup options may be different.

You can install Windows SharePoint Services on a computer by following these steps:

1. Start Server Manager by clicking the Server Manager icon on the Quick Launch toolbar or by clicking Start, Administrative Tools, Server Manager.

2. In Server Manager, select the Roles node in the left pane, and then, under Roles Summary, click Add Roles. This starts the Add Roles Wizard. If Setup displays the Before You Begin page, read the Welcome page and then click Next. You can avoid seeing the Welcome page the next time you start this wizard by selecting the Do Not Show Me This Page Again check box before clicking Next.

3. On the Select Server Roles page, select the Windows SharePoint Services role. You’ll then see the Add Role Services And Features Required For Windows SharePoint Services dialog box. As listed previously in Table 2-1, this dialog box lists the features that are required in order to install SharePoint Services. Click Add Required Features to close the dialog box and add the Web Server (IIS), Windows Activation Service, and .NET Framework 3.0 components to the SharePoint installation. Click Next.

4. Read the introduction to Windows SharePoint Services. As necessary, click the links provided to learn more about the features offered with Windows SharePoint Services. Click Next when you are ready to continue.

5. On the Select Configuration Type page, choose the type of installation. If you are deploying a single-server solution, select Install Only On This Server and then click Next. If you are deploying a server that is part of a Web farm, select Install As Part Of A Server Farm, and then click Next.
6. Although individual SharePoint sites can use different languages, the administration site for Windows SharePoint Services can use only the language chosen during Setup, and you cannot change this language later. On the Select The Language For The Administration Site page, use the selection drop-down list provided to choose the desired language for the administration site, such as English, German, or Korean, and then click Next.

7. If you are installing a single-server configuration of Windows SharePoint Services, on the Specify E-mail Settings page, configure the default e-mail settings that SharePoint will use to send e-mail notifications to administrators. You can use the options provided as follows:

   - **Outbound SMTP Server**: Sets the fully qualified domain name of the e-mail server that will send notifications to administrators, such as mail.adatum.com.

   - **From E-mail Address**: Sets the e-mail address that will appear in the From field of notification messages, such as wss-admin@adatum.com.

   - **Reply-To E-mail Address**: Sets the reply-to e-mail address for notification messages, such as wss-incoming@adatum.com.

8. If you have not previously installed Web Server (IIS), click Next twice to display the Select Role Services page for Web server features. You can then select the Web server features to install. In most cases, you’ll want to select additional features rather than trying to remove features. When selecting or clearing role services, keep the following in mind before you click Next to continue:

   - If you select a role service with additional required features, you’ll see a dialog box listing the additional required roles. After you review the required roles, click Add Required Role Services to accept the additions and close the dialog box. If you click Cancel instead, Setup will clear the feature you previously selected.

   - If you try to remove a role service that is required based on a previous selection, you’ll see a warning prompt about dependent services that Setup must also remove. In most cases, you’ll want to click Cancel to preserve the previous selection. If you click Remove Dependent Role Services, Setup will also remove the previously selected dependent services, which could cause the Web server to not function as expected.

9. On the Confirm Installation Selections page, click the Print, E-mail, Or Save This Information link to generate an installation report and display it in Windows Internet Explorer. You can then use standard Windows Internet Explorer features to print or save the report. After you’ve reviewed the installation options and saved them as necessary, click Install to begin the installation process.
Chapter 2  Deploying IIS 7.0 in the Enterprise

10. If you are setting up a server that is part of a Web farm, you must configure a connection to the shared SQL Server database and perform other preliminary setup tasks by using the Windows SharePoint Services Central Administration tool.

11. When Setup finishes installing the application server with the features you’ve selected, you’ll see the Installation Results page. Review the installation details to ensure that all phases of the installation completed successfully. If any portion of the installation failed, note the reason for the failure and then use these troubleshooting techniques:
   
a. Click the Print, E-mail, Or Save The Installation Report link to create or update the installation report and display it in Windows Internet Explorer.

b. Scroll down to the bottom of the installation report in Windows Internet Explorer and then click Full Log (For Troubleshooting Only) to display the Server Manager log in Notepad.

c. In Notepad, press Ctrl+F, type the current date in the appropriate format for your language settings, such as 2007-08-30, and then click Find Next. Notepad will then move through the log to the first Setup entry from the current date.

d. Review the Server Manager entries for installation problems and take corrective actions as appropriate.

Adding or Removing Web Server Features on Windows Vista

In earlier versions of Windows, you use Add/Remove Windows Components in the Add or Remove Programs application to add or remove operating system components. In Windows Vista, you configure operating system components as Windows features that you can turn on or off rather than add or remove.

You can configure Web server features on a computer running Windows Vista by completing these steps:

1. Click Start, and then click Control Panel.

2. In Control Panel, click Programs.

3. Under Programs And Features, click Turn Windows Features On Or Off. This displays the Windows Features dialog box.

4. You’ll find Windows features for Web servers under the following nodes:

   - **Internet Information Services/FTP Publishing Service**  Includes the FTP Management Console and the FTP Server

   - **Internet Information Services/Web Management Tools**  Includes the IIS 6 Management and IIS 7.0 Management components
IIS 7.0 Administrator’s Pocket Consultant

- **Internet Information Services/World Wide Web Services**  Includes the Application Development, Common HTTP, Health and Diagnostics, Performance, and Security features

- **Microsoft .NET Framework 3.0**  Includes the XPS View and the HTTP Activation and Non-HTTP Activation components for WCF

- **Microsoft Message Queue (MSMQ) Server**  Includes the MSMQ Core server components in addition to support and integration components for message queuing

- **Windows Process Activation Service**  Includes the .NET Environment, Configuration APIs, and Process Model

To turn features on, select feature check boxes. To turn features off, clear feature check boxes. As you select features, Windows Vista selects any required related features automatically without a warning prompt.

5. When you click OK, Windows Vista reconfigures components as appropriate for any changes you’ve made. You may need your original installation media.

**Managing Installed Roles and Role Services**

When you are working with Web and application servers and servers running SharePoint Services, Server Manager is the primary tool you’ll use to manage roles and role services. Not only can you use Server Manager to add or remove roles and role services, you can also use Server Manager to view the configuration details and status for roles and roles services.

**Viewing Configured Roles and Role Services**

On Windows Server, Server Manager lists roles you’ve installed when you select the Roles node in the left pane. As Figure 2-3 shows, the main view of the Roles node displays a Roles Summary section that lists the number of roles and the names of the roles installed. When there are error-related events for a particular server role, Server Manager displays a warning icon to the left of the role name.

In the Roles window, the name of the role is a clickable link that accesses the related role details. The role details provide the following:

- Summary information about the status of related system services. If applicable, Server Manager lists the number of related services that are running or stopped, such as “System Services: 3 Running, 2 Stopped.”

- Summary information about events the related services and components have generated in the last 24 hours, including details on whether any errors have occurred, such as “Events: 1 error(s), 6 warning(s), 2 informational in the last 24 hours.”
Summary information about the role services installed including the number of role services installed and the installed or not installed status of each individual role service that you can use with the role.

**Figure 2-3** View the status details for installed roles.

**Tip** By default, Server Manager refreshes the details once an hour. You can refresh the details manually by selecting Refresh on the Action menu. If you want to set a different default refresh interval, click Configure Refresh at the bottom of the Summary window, use the options provided to set a new refresh interval, and then click OK.

In Server Manager's main window, if you click a role under Roles Summary or click the Go To Manage Roles link under Roles Summary section or click a role under Roles Summary, Server Manager displays expanded summary details on the events and services for the related role. As shown in Figure 2-4, Server Manager lists all events in the last 24 hours. If you click an event and then click View Event Properties, you can get detailed information about the event. Additionally, Server Manager provides details regarding the system services used by the role and their status. You can manage a service by clicking it and then clicking the related Stop, Start, or Restart links provided. In many cases, if a service isn’t running as you think it should, you can click Restart to resolve the issue by stopping and then starting the service.
Adding or Removing Roles on Servers

When you select the Roles node in Server Manager, the Roles Summary pane section details on the current roles that you’ve installed. In the Roles Summary section, you’ll find options for adding and removing roles. You can add a role as discussed previously in the “Setting Up IIS 7.0” section of this chapter. The roles you can remove depend on the type of server. The roles are as follows:

- On application servers, you can remove the application server role, the Web server role, or both.
- On a Web server, you can remove the Web server role.
- On a server computer running SharePoint Services, you can remove the Windows SharePoint Services role or both the Windows SharePoint Services role and the Web server role.

You can remove a server role by completing the following steps:

1. Start Server Manager by clicking the Server Manager icon on the Quick Launch toolbar or by clicking Start, Administrative Tools, Server Manager.
2. In Server Manager, select the Roles node in the left pane, and then click Remove Roles. This starts the Remove Roles Wizard. If Setup displays the Before You
Begin page. read the Welcome page and then click Next. You can avoid seeing the Welcome page the next time you start this wizard by selecting the Do Not Show Me This Page Again check box before clicking Next.

3. On the Remove Server Roles page, clear the check box for the role you want to remove, and then click Next. If you try to remove a role that another role depends on, you’ll see a warning prompt stating that you cannot remove the role unless you also remove the other role as well. If you click Remove Dependent Role Services, Setup will remove both roles.

4. On the Confirm Removal Selections page, review the related role services that Setup will remove based on your previous selections, and then click Remove.

5. When Setup finishes modifying the server configuration, you’ll see the Removal Results page. Review the modification details to ensure that all phases of the removal process completed successfully. If any portion of the removal process failed, note the reason for the failure and then use the previously discussed troubleshooting techniques to help resolve the problem.

Viewing and Modifying Role Services on Servers

In Server Manager, you can view the role services configured for a role by selecting Roles in the left pane and then scrolling down to the Role Services section for the role you want to work with. In the details section, you’ll find a list of role services that you can install in addition to their current Installed or Not Installed status. You can manage role services for application servers and Web servers by using the Add Role Services and Remove Role Services functions provided for the related role details entry. The Windows SharePoint Services role, however, does not have individual role services that you can manage in this way. With a server computer running SharePoint Services, you can modify the Web server role or remove only the Windows SharePoint Services role.

You can add role services by completing the following steps:

1. Start Server Manager by clicking the Server Manager icon on the Quick Launch toolbar or by clicking Start, Administrative Tools, Server Manager.

2. In Server Manager, select the Roles node in the left pane, and then scroll down until you see the Roles Services section for the role you want to manage. In the Roles Services section for the role, click Add Role Services. This starts the Add Role Services Wizard.

3. On the Select Role Services page, Setup makes the currently selected roles unavailable so that you cannot select them. To add a role, select it in the Role Services list. When you are finished selecting roles to add, click Next, and then click Install.
You can remove role services by completing the following steps:

1. Start Server Manager by clicking the Server Manager icon on the Quick Launch toolbar or by clicking Start, Administrative Tools, Server Manager.

2. In Server Manager, select the Roles node in the left pane and then scroll down until you see the Roles Services section for the role you want to manage. In the Roles Services section for the role, click Remove Role Services. This starts the Remove Role Services Wizard.

3. On the Select Role Services page, Setup selects the currently installed roles. To remove a role, clear the related check box. When you are finished selecting roles to remove, click Next, and then click Remove.
Index

Symbols
& (ampersand), in URL, 61
* (asterisk)
    in cmdlets, 91
    in URL, 60
@ (at symbol)
    in e-mail addresses, 231
    in URL, 61
{ } (braces), in URL, 61
[ ] (brackets)
    in set site command, 154
    in URL, 61
^ (caret), in URL, 61
: (colon)
    preceding cmdlet parameter, 91
    in URL, 60
$ (dollar sign)
    preceding redirect variables, 178
    in URL, 60
= (equal sign), in URL, 61
! (exclamation point)
    redirect variable, 178
    in URL, 60
- (hyphen)
    preceding cmdlet parameter, 91
    in URL, 60
#include directive, 183
( ) (parentheses), in URL, 60
% (percent sign), in URL, 61
. (period)
    in URL, 59, 60
+ (plus sign), in URL, 60, 61
? (question mark), in URL, 61
‘ (single quote), in URL, 60
/ (slash), in URL, 61
// (double slash), in URL, 59, 61
˜ (tilde), in URL, 61
_ (underscore), in URL, 60
A
access control, 63–64. See also
    authentication
    based on domain name. See domain
    restrictions
    based on IP address. See IP restrictions
access logs, 351–352, 385–387
analyzing, tracking software for, 385
centralized binary logging, 386, 397
    configuring, 409
    naming conventions for, 399
centralized W3C extended log file
    format, 386
    configuring, 400–401
disabling, 410
    enabling, 400
format of
    changing, 400
    choosing, 385
    list of, 386–387
IIS log file format, 386, 391–392,
    402–403, 458
    configuring, 402–403
    naming conventions for, 398
    location of, 352, 399
NCSA common log file format. See NCSA
    common log file format
ODBC logging. See ODBC logging
per-server logging, 386, 400
per-site logging, 386, 400
searching, 352
text encoding for, 352, 387, 400
uses of, 385
W3C extended log file format, 387,
    393–396, 458
    configuring, 403–404
    naming conventions for, 399
access permissions, 64, 173, 296. See also
    group policies
    assigning, guidelines for, 297
    inherited, 298
    list of, 296
    module for, 434, 479
    setting, 298–299
    special permissions, 296
    users and groups allowed to
        configure, 296
        viewing, 297
access policy, managed handlers, 121–122, 159, 308
accessPolicy attribute, 121
account lockout policies, 302, 303
account policies, 302, 303–304
accounts
group accounts, 292
domain-level accounts, 292
IIS_IUSRS group, 293, 297
local-level accounts, 292
IIS Manager user accounts, 318–319
user accounts, 292
access permissions configured by, 297
anonymous user account, 295
domain-level accounts, 292
for IIS, 292, 293
IIS Manager user accounts, 318–319
local-level accounts, 292
Active Directory Certificate Services, 323, 326, 327–329
starting and stopping, 331–332
submitting certificate requests to, 341–342
Web-based ASP application for, 328, 330–331
when to use, 324
Active Directory Client Certificate authentication, 309
Active Directory Group Policy, 300. See also group policies
Active Directory Users and Computers, 16
Active Server Pages. See entries at ASP
add app command, AppCmd, 104, 257
add apppool command, AppCmd, 102, 275
add backup command, AppCmd, 105, 416
ADD command, 22
add module command, AppCmd, 100
add site command, AppCmd, 101, 147, 148
add vdir command, AppCmd, 104, 167, 257
administration tools
command-line administration tool. See AppCmd
Computer Management console, 16, 80–84
graphical administration tool. See IIS Manager
list of, 3, 16
Reliability and Performance Monitor, 17, 365–369
services. See also services
Web administration, 1
account privileges for, 59
tools for, list of, 16–17
Windows PowerShell. See Windows PowerShell
WMSVC (Web Management Service), 3, 17
configuration values stored by, 4
remote management using, 66, 74–76
requests listened for, types of, 3
administration.config file, 412
administrators
access permissions configured by, 296
configuration performed by, based on role, 64
roles of, 62
advertising, jump pages for, 207
allowDefinition attribute, 12, 111
American Registry for Internet Numbers (ARIN), 136
ampersand (&), in URL, 61
anonymous authentication, 309, 310
availability of, by server role, 29, 38
enabling, 295
enabling and disabling, 311
module for, 432, 434–435
with Web servers, 41
anonymous identification, ASP.NET, 478
anonymous user account, 295
anonymous user identity, 292, 295
AnonymousAuthenticationModule module, 432, 434–435
APP administration object, 21
App management object, 96
AppCmd (Command-line Administration Tool), 3, 20–22, 95, 158
application management commands, 103–104
application pool management commands, 102–103
application pools
changing settings, 276
configuring, 270
creating, 275
deleting, 289
starting and stopping, 278
viewing, 268
applications
  changing settings, 259
  creating, 257
  default settings for, 255
  deleting, 264
  viewing, 254
ASP behaviors, configuring, 218
ASP caching, optimizing, 221
ASP COM+ execution, configuring, 222
ASP debugging and error handling, configuring, 226
ASP request handling, configuring, 220
ASP session state, configuring, 224
AutoStart state, configuring, 161
browser redirection with redirect variables, 179
CGI restrictions, configuring, 213
CGI settings, configuring, 215
commands for, list of, 22
compression, configuring, 191
configuration management commands, 98–100
configuration settings, determining, 113–115
content expiration, configuring, 185, 186
custom HTTP headers, configuring, 187
default documents, configuring, 180–182
directories
  browsing, enabling or disabling, 168
deleting, 172
footers, configuring, 182
help on, 97
HTTP errors, configuring, 198
installation of, 85
ISAPI restrictions, configuring, 213
location of, 20, 95
management objects available to, 95–96
management objects, viewing, 97
migrating applications, 71
MIME types, configuring, 205
module management commands, 100–101
modules
  configuring, 129
disabling, 130
installed, viewing, 125
managed, enabling, 128
native, enabling, 127
native, uninstalling, 131
numeric ID, configuring, 161
objects for, list of, 21
output caching, configuring, 259
parameters for, 97–98
requests currently running, listing, 269
running, 95
site management commands, 101–102
utility commands, 105–106
virtual directories
  creating, 167
  listing, 164
  properties of, modifying, 171
virtual directory management commands, 104–105
Web site limits, setting, 157
Web sites
  bindings for, 154
deleting, 162
managing, 151
secured, creating, 148
on server, listing, 142–143
unsecured, creating, 147
Appcmd.xml file, 96
Apphostsvc (Application Host Helper Service), 66
application buffering, 381
application development, modules for, 430, 432
Application Host Helper Service (Apphostsvc), 66
application logs, 353
application pools, 252, 267. See also worker processes
AppCmd commands for, 102–103
assigning applications to, 276
configuring, 151–153, 255, 256, 269–273
CPU settings, 270
creating, 273–275
default, 67, 255
deleting, 289
feature changes to, 2
identity for, configuring, 277
managing, 74
name of, 270, 274
.NET Framework version used by, 270, 274
for new Web site, 144
optimizing performance of, 382–384
pipeline modes for, 270, 274
configuration levels of, 108
configuring, 254–255
site-wide applications, 251, 252
starting point for, 251
viewing, 253
virtual directory for, 257, 259
Web applications. See Web applications
APPOOOL administration object, 21
Apppool management object, 96
architecture of IIS, 62
access control, 63–64
Web applications. See Web applications
Web sites, 62
architecture of services and processing,
64–72
IIS applications, 68
services, list of, 65
Worker Process isolation mode, 65–68
ARIN (American Registry for Internet
Numbers), 136
ASP (Active Server Pages), 215. See also
applications
automatic restarts for, 217
availability of, by server role, 28, 38
behaviors, configuring, 216–218
buffering for, 216
caching, optimizing performance of,
220–221
chunked transfer encoding for, 217
code page for, default, 217
COM+ execution for, 221–222
configuration levels of, 108
debugging for, 224–226
error handling for, 224–226
HTML fallback file for, 217
locale identifier (LCID) for, 217
module for, 432
objects used by, 215
parent paths for, 217
performance counters for, 369, 375
performance of, optimizing, 380, 381–382
request handling for, 218–220
resource files for, 215
response buffer limit for, 219
script timeout for, 219
scripting languages for, 215, 217
session state for, 223–224
threads per processor limit for, 219
with Web servers, 42
.asp file extension, 215
ASP Script Engine Cache, 384
Asp section, 218, 220, 221, 222, 224, 226
ASP template cache, 384
ASP.DLL extension, 211
ASP.NET, 226. See also .NET Framework;
applications
availability of, by server role, 28, 38
batch compilations of, 108, 247–248
configuration file for, 5
connection strings for, 237–240
deploying applications, 266
globalization for, 108, 249
installing, 264–265
integration into IIS 7.0, 1, 433, 468
key/value pairs stored by, 233–234
module for, 432
multiple versions of
configuration for, 265
default version of, 264
installing, 264
monitoring performance of, 265
side-by-side execution of, 264
performance counters for, 369
performance of, optimizing, 380, 381–382
pipeline modes for, 69–72
profiles for, 108, 241, 244–245
providers for, 110, 240–243
request validation for, 237
server-level configuration for, 227
session state for, 223–224, 227–231, 236
SMTP e-mail settings for, 231–233
trust levels for, 108, 243–244
uninstalling older versions of, 266
user roles for, 108, 240, 245
users for, 108, 241, 246
with Web servers, 42
ASP.NET controls
base type for, 235
compilation mode for, 236
registering, 234
response buffering for, 235
ASP.NET Forms-based authentication, 310, 312
ASP.NET IIS Registration tool, 265
ASP.NET impersonation, 309, 312
ASP.NET pages
base type for, 235
compilation mode for, 236
configuration levels of, 110
master page path for, 236
namespaces for, 236
response buffering for, 235
theme for, 237
view state for
authenticated, 236
enabling, 236
maximum field length, 236
ASP.NET State Service (aspnet_state), 66
aspnet_filter.dll file, 69, 213, 265
aspnet_isapi.dll file, 211, 265
AspNetMembershipProvider provider, 241
aspnet_regiis tool, 265, 267
ASPNET_schema.xml file, 5, 429
AspNetSqlProfileProvider provider, 241
AspNetSqlRoleProvider provider, 241
aspnet_state (ASP.NET State Service), 66
AspNetWindowsTokenRoleProvider provider, 241
assemblies, ASP.NET, 226
asterisk (*),
in cmdlets, 91
in URL, 60
at symbol (@),
in e-mail addresses, 231
in URL, 61
attributes in XML schema
defining, 6
encrypted, 7
flags for combinations of values, 7
friendly-name of, 7
required, 6
unique, 7
validation for, 7
auditing policies, 303, 304–305
authentication
Active Directory Client Certificate authentication, 309
anonymous authentication, 309, 310
availability of, by server role, 29, 38
enabling, 295
enabling and disabling, 311
module for, 432, 434–435
with Web servers, 41
ASP.NET Forms-based authentication, 310, 312
availability of, by server role, 29, 39
492 authentication modes

basic authentication, 309
  availability of, by server role, 30, 39
  combining with integrated or digest Authentication, 310
  enabling and disabling, effects of, 311
  module for, 432, 436
  realm for, specifying, 312
  with Web servers, 43
Client Certificate Mapping Authentication, 44
  availability of, by server role, 30, 39
  module for, 433, 436
configuration levels of, 108
default, module for, 434, 479
digest authentication, 309
  availability of, by server role, 30, 39
  combining with basic Authentication, 310
  module for, 433, 443–444
  realm for, specifying, 312
  reversible password encryption requirements, 310
  with Web servers, 44
IIS Client Certificate Mapping Authentication, 44, 310
  availability of, by server role, 30, 39
  module for, 433, 462–464
for new Web site, 144
  passport authentication, 313
  with Web servers, 43
authentication modes, 309
  combining, 310
  enabling and disabling, 311–313
  global authentication, 310
  list of, 309–310
  local authentication, 310
authorization rules for URLs, 2, 44, 313.
  See also .NET roles
  availability of, by server role, 30, 39
  configuration levels of, 108, 313
  modifying, 315
  module for, 433, 434, 476–477, 484
  removing, 315

B
BACKUP administration object, 21
Backup management object, 96
backups of CAs (certificate authorities), 332–334
backups of IIS, 411
  configuration backups, 411–414
    for content configuration, 413–414
    creating, 105, 416
    deleting, 105
    enabling, 413
    frequency of, 412
    listing, 105
    managing, 415
    rebuilding corrupt installation from, 418–419
    removing, 417
    restoring, 106, 417
    for server configuration, 412–413
    uses of, 414
    viewing, 416
recovery from, 411
server backups
  configuring, 421
  enabling, 419
  full backups, 420
  incremental backups, 420
  performing, 424–425
  recovery from, 427–428
  scheduling, 422–423
  Windows Server Backup for, 419, 420
bandwidth throttling, 378
banner advertisements, jump pages for, 207
basic authentication, 309
  availability of, by server role, 30, 39
  combining with integrated or digest authentication, 310
  enabling and disabling, effects of, 311
  module for, 432, 436
  realm for, specifying, 312
  with Web servers, 43
BasicAuthenticationModule module, 432, 436
Batch logon type, 252
bindings for Web sites, 62, 153–155
Bitness precondition, managed handlers, 121
braces { }, in URL, 61
brackets [ ], in URL, 61
browser redirection. See redirection of browser requests
Bytes Received field, IIS log file format, 392
Bytes Received field type, W3C extended log file form, 395
Bytes Sent field, IIS log file format, 386
Bytes Sent field type, W3C extended log file format, 395
BytesRecvd field, ODBC logging, 397
BytesSent field, ODBC logging, 397

C

c prefix, W3C extended log file format, 394
C#, Windows PowerShell based on, 85
CA (certificate authority), 325–326
backing up, 332–334
certificate servers configured as, 327
restoring from backup, 332, 334
Cache-Control HTTP header field, 186
caching
for ASP, optimizing performance of, 220–221, 384
file cache
availability of, by server role, 29
module for, 433, 454
with Web servers, 45
HTTP cache
availability of, by server role, 29, 38
module for, 435–457
with Web servers, 41
output cache
configuration levels of, 110
configuring, 259–263
module for, 372, 434, 482
performance counters for, 373
performance of
optimizing, 382–384
problems caused by, 371
token cache
availability of, by server role, 29
module for, 372, 433, 474
with Web servers, 45
of type libraries, 381
URL cache
availability of, by server role, 29
module for, 372, 433, 475
with Web servers, 45
caching section, 259
caret (^), in URL, 61
cat cmdlet alias, 92
cd cmdlet alias, 93
centralized binary logging, 386, 397
configuring, 409
naming conventions for, 399
centralized W3C extended log file format, 386
CertEnroll virtual directory, 331
certificate authority. See CA
Certificate Authority snap-in, 328–329
approving certificate requests, 335
backing up CAs, 332–334
configuring certificate request processing, 334
declining certificate requests, 335
generating certificates manually, 335
renewing root certificate, 337
revoking certificates, 336
starting and stopping Certificate Services, 331–332
viewing root certificate, 337
Certificate Revocation List (CRL), 336
certificate servers, 327
Certificate Services. See Active Directory Certificate Services
CertificateMappingAuthenticationModule module, 433, 437
certificates, SSL, 325–326
approving, 335
autoenrollment of, 334
client certificates, 346
certificate requests, configuring, 334
configuration levels of, 110
creating requests, 338–339
declining, 335
denying, 328
failed (declined), viewing, 328
generating manually, 335
installing, 343
issued, viewing, 328
pending, viewing and approving, 328
request processing, configuring, 334
requesting
from Certificate Services, 341–342
from third-party authority, 339
revoked, viewing, 328
revoking, 336
root certificate
installing in browser authorities
store, 344
renewing, 337
CertSrv virtual directory

types of, 327
templates for, 329
CertSrv virtual directory, 330
certutil command, 331
CGI (Common Gateway Interface), 68, 209
access permissions for, 297
availability of, by server role, 28, 38
configuration levels of, 108
context for, 214
handler mappings for CGI scripts, 306
module for, 432, 437–439
multithreaded (Fast CGI), 380
performance of, 380
restrictions, configuring, 109, 210–213
separate console window for, 214
settings for, configuring, 214–215
time-out for, 214
with Web servers, 42
Cgi section, 215
CgiModule module, 68, 432, 437–439
chdir cmdlet alias, 93
classic pipeline mode, for ASP.NET
applications, 69–72
clear cmdlet alias, 92
clear config command, AppCmd, 99, 116
Clear-Host cmdlet, 92
ClearText logon type, 252
Client Certificate Mapping
Authentication, 44
availability of, by server role, 30, 39
module for, 433, 437
client certificates, 346
Client IP Address field type, W3C extended
log file format, 395
Client IP field, IIS log file format, 392
ClientHost field, ODBC logging, 397
cls cmdlet alias, 92
cmdlets, Windows PowerShell. See
Windows PowerShell, cmdlets
code download requests, 4
colon (:), in URL, 59, 60, 61
.com domain, 59, 389
COM+ execution for ASP, 221–222
COM+ network access
with application servers, 34
availability of, by server role, 28
Command-line Administration Tool. See
AppCmd (Command-line
Administration Tool)
command-line tools. See AppCmd
(Command-line Administration
Tool); Windows PowerShell
-command parameter, powershell
command, 88
Common Gateway Interface. See CGI
Compare-Object cmdlet, 92
Component Object Model. COM+
compression of Web content. See content
compression
Computer Management console,
16, 80–84
Computer Name field, IIS log file
format, 392
CONFIG administration object, 21
Config management object, 96
configSource attribute, 9
configuration. See also global configuration
system; set config command,
AppCmd
AppCmd commands for, 98–100
backups of. See backups of IIS,
configuration backups
feature changes to, 2, 429
of managed handlers, 120–122
of managed modules, 119
of native modules, 118, 129–130
WMSVC storing values for, 4
XML schema for, 2, 4–8
extending the schema, 5
list of files, 5
location of files, 5
managing, 4
configuration APIs
with application servers, 34
availability of, by server role, 31, 40
configuration sections, 112. See also specific
section names
clearing and resetting, 116–117
levels allowed for, locking, 112–113
levels allowed for, specifying, 111
locking and unlocking, 116
settings for
determining, 113–115
modifying, 115
configuration validation
availability of, by server role, 29, 38
module for, 432, 439–440
with Web servers, 41
for HTTP (Hypertext Transfer Protocol), 369
instances of, 370
list of categories of, 369
for memory-related problems, 372
for memory usage, 372
for requests, 369
selecting for monitoring, 370
for services, 369
for thread queuing, 374
for URL (Uniform Resource Locator), 369
for Web service, 370
cp cmdlet alias, 92
CPU monitoring, 285–286
CPU requirements, 14
CPU settings, application pools, 270
CPU usage, monitoring, 366, 374
creator owner, access permissions configured by, 296
credential objects, getting based on password, 90
credentials. See logon credentials
CRL (Certificate Revocation List), 336
cs prefix, W3C extended log file format, 394
culture, for .NET globalization, 249
custom controls, ASP.NET, 234
custom headers, HTTP, 186–188, 469–470
custom logging, 398
availability of, by server role, 29, 39
module for, 432, 441–442
with Web servers, 43
CustomErrorModule module, 432, 440–441
CustomLoggingModule module, 432, 441–442

D
Data Collector Sets and Reports, 369
data protection requirements, 15
Data Source Name (DSN), 396, 405, 407–408
date
current, 90
setting, 90
Date directive, W3C extended log file format, 394
Date field, IIS log file format, 392
Date field type, W3C extended log file format, 395
-Debug parameter, cmdlet, 91
disabling, to improve performance, 381
SSL, troubleshooting, 345
default documents, 179
availability of, 28, 38
configuration levels of, 108
configuring, 179–182
module for, 432, 442–443
performance affected by, 180
viewing settings for, 180
with Web servers, 41
DefaultAppPool pool, 67
DefaultAuthenticationModule module, 434, 479
defaultDocument section, 180
DefaultDocumentModule module, 432, 442–443
del cmdlet alias, 93
delegated administration, 20
delegation state, 318, 320–322
delete app command, AppCmd, 104, 264
delete apppool command, AppCmd, 103, 289
delete backup command, AppCmd, 105, 417
DELETE command, 22
delete module command, AppCmd, 100
DELETE request, with ISAPI extensions, 210
delete site command, AppCmd, 102, 162
delete vdir command, AppCmd, 105, 172
desktop
deploying IIS 7.0 on, 26
role services for, 36–46
device profile, 230
diagnostics, 2. See also logging; monitoring
availability of, by server role, 29
modules for, 430, 432
Diff cmdlet alias, 92
digest authentication, 309
availability of, by server role, 30, 39
combining with basic authentication, 310
module for, 433, 443–444
realm for, specifying, 312
reversible password encryption
requirements, 310
with Web servers, 44
DigestAuthenticationModule module, 433, 443–444
dir cmdlet alias, 92
directories
access permissions for. See access permissions
alternate pass-through credentials for, 152
browsing
availability of, 28, 38
configuration levels of, 109
enabling or disabling, 167–169
module for, 432, 444–445
with Web servers, 41
converting to applications, 258
deleting, 171
home directory for Web site, 151–153
organization of, 297
physical directories, 163
properties of, modifying, 169
redirecting browser requests to, 175
renaming, 169
virtual directories. See virtual directories
Directory Browsing module, 167
directory-wide applications, 252
directoryBrowse section, 168
DirectoryListingModule module, 432, 444–445
disk drives
defragmenting, 380
organization of, 380
requirements for, 14
disk usage
monitoring, 366, 375–376
performance counters for, 375
diskperf command, 376
distributed transactions
with application servers, 36
availability of, by server role, 29
DNS (Domain Name System), 17
for Internet, 136
for intranets, 136
for new Web site, 144
documents. See default documents; files;
Web content
dollar sign ($)
preceding redirect variables, 178
in URL, 60
domain classes, 389
domain-level accounts, 292
Domain Name System (DNS), 17, 136
domain restrictions, 315
  availability of, by server role, 30, 39
  configuration levels of, 109
  configuring, 317–318
  module for, 433, 464–466
  viewing current restrictions, 316
  with Web servers, 44
domains, in URL, 59
double slash (//), in URL, 59, 61
drives. See disk drives
DSN (Data Source Name), 396, 405, 407–408
dynamic content compression
  availability of, by server role, 30, 40
  module for, 433, 445–448
  with Web servers, 44
dynamic content, performance of, 379
DynamicCompressionModule module, 433, 445–448

E
E-mail
  ASP.NET settings for, 231–233
  protocol for. See SMTP (Simple Mail Transfer Protocol)
  for Windows SharePoint Services servers, 52
echo cmdlet alias, 93
.edu domain, 59, 389
Elapsed Time field, IIS log file format, 392
encrypted command prompt, 352
encrypted attribute, 7
encryption, 323. See also Active Directory Certificate Services; SSL (Secure Sockets Layer)
End-Date directive, W3C extended log file format, 394
enterprise root CA, 327
enterprise subordinate CA, 327
environment variables, 4
Epal cmdlet alias, 92
Epcsv cmdlet alias, 92
equal sign (=), in URL, 61
erase cmdlet alias, 93
error handling. See also HTTP errors
  for ASP applications, 224–226
logs containing recorded errors. See access logs; failed request trace logs;
  Windows event logs
  nonblocking error state, inability to detect, 287
  request viewing, in real time, 2
  services started automatically, failure of, 81
  STOP error, 425
  Windows PowerShell cmdlets, 91
-ErrorAction parameter, cmdlet, 91
-ErrorVariable parameter, cmdlet, 91
escape codes, in URL, 61
event logs, Windows. See Windows event logs
Event Viewer, 17
exclamation point (!)
  redirect variable, 178
  in URL, 60
execution policy
  getting, 90
  setting, 87, 90
-executionpolicy parameter, powershell command, 87
expiration for Web content, 184–186
Export-Alias cmdlet, 92
Export-Csv cmdlet, 92
Extensible Markup Language (XML) schema files. See XML schema files

F
failed request trace logs, 357–360
  area of managed modules to trace, 359
  area of server to trace, 359
  configuring, 360–361
  enabling, 360
  module for, 432, 448–453
  naming of, 357
  trace rules for, 357, 361–365
  verbosity of, 359
FailedRequestsTracingModule module, 432, 448–453
Fast CGI, 380
FastCGIModule module, 68, 432, 453–454
feature delegation, 109, 318, 320–322
Fields directive, W3C extended log file format, 394
file cache
  availability of, by server role, 29
  module for, 433, 454
  with Web servers, 45
file encoding, for .NET globalization, 249
file not found (404) errors, 208, 352
File Transfer Protocol. See FTP
file types, 201. See also MIME types
File URI field, IIS log file format, 386
FileAuthorizationModule module, 434, 479
FileCacheModule module, 372, 433, 454
files. See also default documents
access permissions for. See access
permissions
browsing, 174
deleting, 173, 175
downloading and uploading. See FTP (File Transfer Protocol)
opening, 174
organization of, 297
properties of
inheritance for, 173
modifying, 174
renaming, 173, 174
size of, reducing, 380
find config command, AppCmd, 99
firewalls, affecting connections to server, 72
503 (service unavailable) errors,
278, 287, 288
Fixed-length records, centralized binary
logging, 397
fl cmdlet alias, 92
footers, configuring, 182
foreach cmdlet alias, 92
ForEach-Object cmdlet, 92
Format-List cmdlet, 92
Format-Table cmdlet, 92
Format-Wide cmdlet, 92
FormsAuthenticationModule module, 434, 480–481
404 (file not found) errors, 208, 352
ft cmdlet alias, 92
FTP (File Transfer Protocol), 24
anonymous downloads and uploads, 25
compared to HTTP, 25
default port for, 25
restricted downloads and uploads, 25
URLs for, 60
FTP Management Console, 29, 40
FTP Publishing Service (MSFTPSVC), 66
FTP server, 29, 40
FTP sites, managing, 74
Full Control permission, 296
fw cmdlet alias, 92
FX_schema.xml file, 5, 429
G
gal cmdlet alias, 92
gateway scripts, 68
gcm cmdlet alias, 92
Get-Alias cmdlet, 90, 92
Get-AuthenticodeSignature cmdlet, 90
Get-ChildItem cmdlet, 92
cmdlet verb, 88
Get-Command cmdlet, 92
Get-Content cmdlet, 92
Get-Credential cmdlet, 90
Get-Date cmdlet, 90
Get-EventLog cmdlet, 90
Get-ExecutionPolicy cmdlet, 90
Get-History cmdlet, 92
Get-Host cmdlet, 90
Get-Location cmdlet, 90, 92
Get-Process cmdlet, 92
Get-PSDrive cmdlet, 90
GET request, with ISAPI extensions, 210
Get-Service cmdlet, 90, 92
Get-Variable cmdlet, 92
gl cmdlet alias, 92
global configuration system, 8–13, 107.
See also configuration
changes to, automatically incorporated,
11, 107
configuration sections for. See
configuration sections
exporting, 132
inheritance for, 8, 107
levels of
list of features by, 107–110
specifying for configuration sections, 111
list of configuration files, 9
locking values of
compared to location locking, 112
inheritance of, 107
limitations of, 113
specifying, 111, 112–113
nesting (including) configuration files, 9–11
restricted values of, inheritance of, 107
sharing, 131–134
globalization, .NET, 249
globalModules section, 118
gov domain, 59, 389
gpedit.msc tool, 302
GPO (Group Policy Object), 300. See also group policies
gps cmdlet alias, 92
graphical administration tool, 3
group accounts, 292
domain-level accounts, 292
IIS_IUSRS group, 293, 297
local-level accounts, 292
group cmdlet alias, 92
Group-Object cmdlet, 92
group policies, 299
account lockout policies, 302, 303
account policies, 303–304
auditing policies, 303, 304–305
for computers, when applied, 300
for domains, 300, 303
for domains in a forest, 301–302
Kerberos policies, 303
for local computer, 302
multiple, order of application, 299
for organizational units (OUs), 300, 303
password policies, 302, 303
for sites, 300, 303
for sites in a forest, 301–302
for users, when applied, 300
Group Policy Management Console, 300, 301–302
Group Policy Object Editor, 300, 302
Group Policy Object (GPO), 300. See also group policies
gsv cmdlet alias, 92
gv cmdlet alias, 92

H
h cmdlet alias, 92
handler mappings, 120, 305
access policy for, 308
configuration levels of, 109
creating, 307–308
editing, 308
entry type for, 306
for executables, 306
handler for, 306
for IIS modules, 306, 307
for managed handlers, 306, 307
name of, 305, 307
path for, 305
path type for, 306
removing, 308
renaming, 308
request types handled by, 308
for scripts, 306, 307
state of, 305
viewing, 305
handlers. See managed handlers
handlers section, 121
hard page faults, 373
hardware requirements, 13–15
HEAD request, with ISAPI extensions, 210
headers, custom, 186–188
health monitoring, 43. See also logging;
monitoring; tracing
features for, availability of, 29, 39
modules for, 430, 432
help command, 89
history cmdlet alias, 92
home directory for Web site, 151–153, 173
host
goinget information about, 90
reading input line from console, 90
Host field, NCSA common log file format, 388
host headers, 62, 138–140, 324
host name, in URL, 59, 153–155
HTTP activation
with application servers, 34
availability of, by server role, 31
HTTP cache
availability of, by server role, 29, 38
module for, 455–457
with Web servers, 41
HTTP compression. See content compression
HTTP errors, 193
404 (file not found) errors, handling,
208, 352
503 (service unavailable) errors, handling,
278, 287, 288
.asp or .aspx files for, 196
availability of, by server role, 28, 38
customizing, 109, 196–201, 432, 440–441
default information sent for, 194
detailed errors, 194–195
executing URL for, 200
localized, 198
non-localized, 200
redirection for, 200
sent to client
HTTP headers, custom

- replaced by Internet Explorer messages, 194
- security regarding, 194, 195
- static file content, inserting into, 200
- status codes for, 193–194
- terse errors, 195
- with Web servers, 42
- HTTP headers, custom, 186–188, 469–470
- HTTP (Hypertext Transfer Protocol), 23
  - compared to FTP, 25
  - custom headers, 469–470
  - default document, 179
    - availability of, 28, 38
    - configuration levels of, 108
    - configuring, 179–182
    - module for, 432, 442–443
    - performance affected by, 180
    - viewing settings for, 180
    - with Web servers, 41
  - default port for, 23
  - directory browsing
    - availability of, 28, 38
    - configuration levels of, 109
    - enabling or disabling, 167–169
    - module for, 432, 444–445
    - with Web servers, 41
  - keep-alive support, 158–159, 469–470
  - modules for, 430, 432, 469–470
  - performance counters for, 369
  - redirect headers, 469–470
  - static content
    - availability of, 28, 38
    - module for, 432, 474
    - performance of, 379
    - with Web servers, 42
- HTTP logging, 398
  - availability of, by server role, 29, 39
  - module for, 432, 458–460
  - with Web servers, 43
- HTTP process activation model, 2
- HTTP redirection. See redirection of browser requests
- HTTP Request field, NCSA common log file format, 390
- HTTP response headers. See response headers
- HTTP trace
  - availability of, by server role, 29
  - module for, 432, 475
  - with Web servers, 45
- HttpCacheModule module, 372, 455–457
- httpCompression section, 192
- httpErrors section, 198
- HttpLoggingModule module, 432, 458–460
- httpProtocol section, 158, 187
- httpRedirect section, 179
- HttpRedirectModule module, 432, 460–462
- HTTPS (Hypertext Transfer Protocol Secure), 24, 324
- https prefix, 24, 324
- Hypertext Transfer Protocol. See entries at HTTP
- Hypertext Transfer Protocol Secure (HTTPS), 24, 324
- hyphen (-)
  - preceding cmdlet parameter, 91
  - in URL, 60

I
- Identification field, NCSA common log file format, 389
- identity attribute, 6
- identityType attribute, 7
- IIS 6 Management Compatibility, 30, 32, 40
- IIS 6 Management Console
  - availability of, by server role, 31, 40
  - with Web servers, 46
- IIS 6 Manager, 3, 17
- IIS 6 Scripting Tools, 3
  - availability of, by server role, 31, 40
  - with Web servers, 46
- IIS 6 WMI compatibility, 3
  - availability of, by server role, 30, 40
  - with Web servers, 46
- IIS Admin Service (IISADMIN), 66
- IIS applications. See applications
- IIS Client Certificate Mapping
  - Authentication, 44, 310
  - availability of, by server role, 30, 39
  - module for, 433, 462–464
- IIS (Internet Information Services) 6.0. See also metabase
  - applications, managing on IIS 7.0, 3, 32
  - applications, running on IIS 7.0, 3
  - configuration for, 429
- IIS (Internet Information Services) 7.0
administration of. See Web administration architecture of. See architecture of IIS
changes in, 1–4
deploying
  on desktop platforms, 26
  planning for, 23
  on server platforms, 26–27
features of, by server role, 27–31
hardware requirements, 13–15
installation of. See installation learning curve needed for, 1, 3
setting up, 47–54
Windows editions supported, 15
IIS log file format, 386, 391–392, 458
configuring, 402–403
naming conventions for, 398
IIS Management Console
  availability of, by server role, 30, 40
  with Web servers, 45
IIS Management Scripts and Tools
  availability of, by server role, 30, 40
  with Web servers, 45
IIS Management Service
  availability of, by server role, 30, 40
  with Web servers, 45
IIS Manager, 3, 17, 72–74
  access permissions, configuring, 159
  application pools
    configuring, 269
    creating, 274
    deleting, 289
    identity, configuring, 277
    managing, 152
    multiple worker processes for, 281
    settings, changing, 275
    starting and stopping, 278
    viewing, 267
  applications
    assigning to application pools, 276
    creating, 253, 256
    default settings for, 254
    deleting, 263
    settings, changing, 258–259
    viewing, 253
  ASP behaviors, configuring, 218
  ASP caching, optimizing, 221
  ASP COM+ execution, configuring, 222
  ASP debugging and error handling,
    configuring, 225
  ASP pages and controls, configuring, 237
  ASP request handling, configuring, 219
  ASP session state, configuring, 223
  ASP.NET key/value pairs, configuring, 233
  ASP.NET session state, configuring,
    227–231
  AutoStart state, configuring, 160
  browsing files, 174
certificate requests, creating, 338–339
certificates, installing, 343
CGI restrictions, configuring, 212
CGI settings, configuring, 214
compression, configuring, 190, 192
connection strings, creating, 238, 239
content expiration, configuring, 184, 186
Content View, 174
CPU monitoring
  configuring, 285
  disabling, 286
custom controls, adding, 234
custom HTTP headers, configuring, 187
default documents, configuring, 180
delegation state, configuring, 321
directories
  converting to applications, 258
  deleting, 172
  properties of, modifying, 169
  renaming, 169
directory browsing, enabling and
  disabling, 168
global configuration level, accessing, 110
handler mappings, creating, 307–308
health monitoring, configuring, 286
home directory, managing, 151
HTTP errors, configuring, 196
HTTP keep-alives, configuring, 158
idle worker processes, shutting down, 288
IIS Manager user accounts
  creating, 318
  granting permissions to, 319
interface of, redesigned, 20
ISAPI filters, configuring, 213
ISAPI restrictions, configuring, 212
logging, disabling, 410
MIME types, configuring, 203
modules
  configuring, 129
IIS Manager user accounts

Iisreset.exe command-line utility
- rebooting a server, 79
- starting and stopping services, 77–78

IIS_schema.xml file, 5, 429
Import-Alias cmdlet, 90, 92
Import-Csv cmdlet, 92
.inc file extension, 183
#include directive, 183
included files. See Server-Side Includes (SSI)

Index records, centralized binary logging, 397

Inetinfo.exe process, 76
Inetmgr.exe process, 65
inspect trace command, AppCmd, 106
install module command, AppCmd, 101

installation
- Active Directory Certificate Services, 329–330
- application servers, 47–49
- ASP.NET, 264–265
- certificates, SSL, 343
- IIS
  - on application servers, 47–49
  - default Web site created by, 62
  - on Web servers, 49–50
  - on Windows SharePoint Services servers, 51–53
- native modules, 117, 125–126, 430
- .NET Framework, 264–265
- non-standard modules, 122–123
- Web servers, 49–50
- Windows PowerShell, 85, 86
- Windows SharePoint Services servers, 51–53
- integrated pipeline mode, for ASP.NET applications, 70–72
- integrated Windows authentication, 310
- Interactive logon type, 252
- Internet Guest account, 295
- Internet Information Services. See IIS 6.0; IIS 7.0
- Internet Server Application Programming Interface. See entries at ISAPI
- intranets, 136
- Invoke-History cmdlet, 92
- IP addresses, 135–136
  - configuring, 153–155
  - multiple, assigned to one server, 137
multiple host headers for, 138–140
multiple port numbers for, 138
naming conventions for, 136
for private networks, 135
for public networks, 136
for server, determining, 140
types of, 135
IP restrictions
availability of, by server role, 30, 39
configuration levels of, 109
module for, 433, 464–466
with Web servers, 44
ipal cmdlet alias, 92
ipcsv cmdlet alias, 92
IpRestrictionModule module, 433, 464–466
IPv4 address restrictions, 315–318
ISAPI applications, 69, 209–210, 380, 381–382
ISAPI extensions, 210
availability of, by server role, 28, 38
HTTP request types used with, 210
module for, 432, 467–468
restrictions, configuring, 109, 210–213
with Web servers, 42
ISAPI filters, 209, 213
availability of, by server role, 28, 38
for compression (in previous versions), 189
configuration levels of, 109
configuring, 213–214
global filters, 210
local (site) filters, 210
module for, 432, 466–467
with Web servers, 43
when to use, 210
IsapiCgiRestriction section, 213
IsapiFilterModule module, 69, 432, 466–467
IsapiModule module, 69, 432, 467–468
isUniqueKey attribute, 7
IUSR_ComputerName account, 292, 295
J
jump pages, 207
K
keep-alive support, HTTP, 158–159, 469–470
Kerberos policies, 303
key/value pairs stored by ASP.NET, 233–234
keys, SSL encryption, 323
kill cmdlet alias, 93
L
latency, 376
libraries, on SharePoint sites, 46
list app command, AppCmd, 103, 254
list apppool command, AppCmd, 102, 268
list backup command, AppCmd, 105, 416
LIST command, 22
list config command, AppCmd, 98, 113–114
List Folder Contents permission, 296
list module command, AppCmd, 100
list request command, AppCmd, 105, 269
list site command, AppCmd, 101, 142–151
list trace command, AppCmd, 106
list vdir command, AppCmd, 104, 164
list wp command, AppCmd, 105, 269
lists, on SharePoint sites, 46
local-level accounts, 292
local service account, 292
local service domain, 232
local system account, 292, 293, 296
location
getting, 90
pushing to stack, 90
setting, 90
location locking, 112
lock config command, AppCmd, 99, 116
locking, location, 112
locking of configuration values
compared to location locking, 112
inheritance of, 107
limitations of, 113
overriding, 111, 112–113
specifying, 99, 116
unlocking, 99, 116
logEventOnRecycle attribute, 7
logging, 398–399
access logs. See access logs
availability of, by server role, 29, 39
configuration levels of, 109
custom, 398
availability of, by server role, 29, 39
module for, 432, 441–442
with Web servers, 43
data from Windows log files, getting, 90
login requests

failed request trace logs. See failed request trace logs
naming conventions for, 398
reducing, to improve performance, 381
storing logs on separate disks, 381
with Web servers, 43
Windows event logs. See Windows event logs
login requests, 3
logon account for services, 293–294
logon credentials, 142
 alternate pass-through credentials, 152
 for applications, 252, 255, 257
 for virtual directories, 166, 170, 171
Logtemp.sql script, 396
LogTime field, ODBC logging, 397
ls cmdlet alias, 92

M
Machine field, ODBC logging, 397
machine key, 109
Machine.config file, 9, 12
managed engine
 availability of, by server role, 29
 with Web servers, 45
managed handlers, 119
 configuration, editing, 129
 configuration files controlling, 120–122
 handler mappings for, 306, 307
managed modules, 2, 433
 configuration, editing, 129–130
 configuration files controlling, 119
 disabling, 119, 130
 enabling, 128–129
 installed, viewing, 124–125
 list of, 433
 managed handlers for, 119
 reference for, 478–485
 running for all requests, 119
managed pipelines, for application pools, 270
ManagedEngine module, 433, 468
management objects, 95–96
management service, 40, 110
management service requests, 4
Mbschema.xml file, 412
memory paging, 374
memory requirements, 13
memory usage
monitoring, 366, 371–374
performance counters for, 372
worker processes, recycling automatically based on, 284
message queuing
 activation of, 34
 availability of, 31
 server functions for, 35
metabase
 compatibility with, 30, 40, 45
 feature changes to, 2, 3, 429
Metabase.xml file, 412
Method Used field, IIS log file format, 386
Method Used field type, W3C extended log file format, 395
Microsoft Management Console (MMC), 302
Microsoft Message Queuing (MSMQ)
 activation, 31, 34, 54
Microsoft SQL Server. See SQL Server
Microsoft SQL Server 2005 Administrator’s Pocket Consultant, 396, 405
Microsoft Web administration. See Web administration
Microsoft Windows PowerShell Step By Step, 88
Microsoft Windows security, 291
 access permissions. See access permissions
group accounts. See group accounts
group policies. See group policies
Internet Guest account, 295
 user accounts. See user accounts
Microsoft Windows SharePoint Services. See entries at Windows SharePoint Services
migrate config command, AppCmd, 100
migrating applications, 71
.mil domain, 59, 389
MIME (Multipurpose Internet Mail Extensions) protocol, 25
MIME types, 201
categories of, 202
configuration levels of, 110
configuring, 203–205
list of, 201–203
subtypes of, 202
MMC (Microsoft Management Console), 302
Mode precondition, managed handlers, 120
Modify permission, 296
MODULE administration object, 21
Module management object, 96
module maps, 306, 307
modules, 2, 117. See also managed modules;
native modules
AppCmd commands for, 100–101
configuration levels of, 110, 124
features enabled or disabled by, 2
non-standard, installing, 122–123
types of, 2
modules section, 118, 119
monitoring, 349–351
access logs. See access logs
Data Collector Sets and Reports, 369
Performance Monitor, 351, 366
planning for, 350
reasons for, 349
Reliability and Performance Monitor,
365–369
Reliability Monitor, 351, 367
tools for, list of, 349, 351
Windows event logs. See Windows
event logs
mount cmdlet alias, 93
MSFTPSVC (FTP Publishing Service), 66
MSMQ (Microsoft Message Queuing)
activation, 31, 34, 54
MSW3PRT.DLL extension, 211
Multipurpose Internet Mail Extensions
(MIME), 25
multithreaded CGI. See Fast CGI

N
name attribute, 6, 12
named pipes activation
with application servers, 35
availability of, by server role, 31
native modules, 2
categories of, 430
configuring, 118, 129–130
disabling, 118, 130
enabling, 126–127
installed, viewing, 124–125
installing, 117, 125–126, 430
list of, 430–433
reference for, 434–478
uninstalling, 118, 131
NCSA common log file format, 386,
387–388, 458
configuring, 401–402
Host field, 388
HTTP Request field, 390
Identification field, 389
naming conventions for, 399
Status Code field, 390
Time Stamp field, 390
Transfer Volume field, 391
User Authentication field, 389
.NET compilation, 108, 247–248
.net domain, 59, 389
.NET environment
with application servers, 34
availability of, by server role, 31, 40
.NET extensibility
availability of, by server role, 28, 38
enabling default ASP.NET version, 264
module for, 432, 467–468
with Web servers, 42
.NET Framework, 240
availability of, by server role, 28
configuration file for, 5, 9
installing, 264–265
integration into IIS 7.0, 1, 433, 468
new features of, 31
Windows PowerShell based on, 85
.NET globalization, 108, 249
.NET profiles, 108, 241, 244–245
.NET providers, 110, 240–243
.NET roles, 108, 240, 245
.NET security, 291
.NET trust levels, 108, 243–244
.NET users, 108, 241, 246
NetBIOS naming convention, 136
Network logon type, 252
network service account, 292
network usage, monitoring, 366, 376–379
New-Alias cmdlet, 90
new- cmdlet verb, 88
New-Item cmdlet, 93
New-PSDrive cmdlet, 93
New-Service cmdlet, 90
New-Variable cmdlet, 93
ni cmdlet alias, 93
-nologo parameter, powershell command,
86, 88
non-HTTP activation
nonblocking error state, inability to detect

with application servers, 35
availability of, by server role, 31
nonblocking error state, inability to detect, 287
-noprofile parameter, powershell command, 87, 88
nv cmdlet alias, 93

O
object-based scripting environment. See ASP (Active Server Pages)
objects, writing to pipeline, 90
OCSPISAPI.DLL extension, 211
ODBC data sources, 17
ODBC logging, 387, 396–397, 398
availability of, by server role, 29, 39
configuring, 405–408
DSN (Data Source Name) for, 396, 405, 407–408
enabling, 408
logging database for, 406
module for, 432
with Web servers, 43
operating system security. See Microsoft Windows security
Operation field, ODBC logging, 397
OPTIONS request, with ISAPI extensions, 210
.org domain, 59, 389
outages, update sites for, 205–207
-OutBuffer parameter, cmdlet, 91
outgoing remote transactions, 29, 36
output cache
configuration levels of, 110
configuring, 259–263
module for, 372, 434, 482
OutputCacheModule module, 372, 434, 482
-OutVariable parameter, cmdlet, 91
overrideModeDefault attribute, 12, 13, 111, 112–113

P
$P redirect variable, 178
P3P (Platform for Privacy Preferences Project), 188
page faults, 373
pages. See ASP (Active Server Pages);
ASP.NET pages; jump pages
paging, 374
Parameters field, ODBC logging, 397
parentheses ( ), in URL, 60
passport authentication, 313
password encryption, reversible, 310
password, in URL, 60
password policies, 302, 303
path (directory), in URL, 60
PATH environment variable, 89
per-server logging, 386, 400
per-site logging, 386, 400
percent sign (%), in URL, 61
performance
applications, removing, 379
of ASP cache, 220–221
of ASP, optimizing, 380, 381–382
of ASP.NET
monitoring for multiple versions, 265
optimizing, 380, 381–382
baseline metrics for, 350
of caching
optimizing, 382–384
problems caused by, 371
of CGI, 380
content compression improving, 30, 39, 44, 189
content usage, optimizing, 379–381
CPU usage, monitoring, 366, 374
debugging, disabling, 381
default documents affecting, 180
disk usage, monitoring, 366, 371–374
features for, availability of, 39
of ISAPI applications, optimizing, 380, 381–382
logging, reducing, 381
memory usage
monitoring, 366, 371–374
recycling worker processes based on, 284
modules for, 430, 433
monitoring as tool for, 349
multiple worker processes affecting, 282
network usage, monitoring, 366, 376–379
of pooling, optimizing, 382–384
of queuing, optimizing, 382–384
Reliability and Performance Monitor for, 365–369
services, removing, 379
tuning, methods for, 349
performance counters. See counters
Performance Monitor, 351, 366
period (.), in URL, 59, 60
permissions for files and directories. See access permissions
permissions for remote administration, 319–320
PHP (PHP Hypertext Preprocessor), 68
physical directories, 163
  creating, 163, 165
  icon representing, 163
  managing, 167
ping requests, 4
pinging of processes, 286
pipeline modes
  for application pools, 270, 274
  for ASP.NET applications, 69–72
pipeline, writing objects to, 90
piping, 85
Platform for Privacy Preferences Project (P3P), 188
plus sign (+), in URL, 60, 61
policies. See also group policies
  access policy, managed handlers, 121–122, 308
  account policies, 302, 303–304
  auditing policies, 303, 304–305
  execution policy
    getting, 90
    setting, 87, 90
    Kerberos policies, 303
    password policies, 302, 303
    privacy policy, 188–189
pooling. See application pools
POP3 (Post Office Protocol version 3), 3, 26
port number, in URL, 60, 137
  configuring, 153–155
  multiple, assigned to one IP address, 138
Post Office Protocol version 3 (POP3), 3, 26
POST request, with ISAPI extensions, 210
PowerShell. See Windows PowerShell
powershell command
  -command parameter, 88
  -executionpolicy parameter, 87
  -nologo parameter, 86, 88
  -noprofile parameter, 87, 88
privacy policy, 188–189
private key, 324
problems, resolving, 2. See also error handling; health monitoring
process model
  application pool settings for, 271
  with application servers, 34
  availability of, by server role, 31, 40
process orphaning settings, application pools, 272
process pinging, 286
processes, architecture of, 64–72
ProcessingTime field, ODBC logging, 397
processor (CPU) usage, monitoring, 366, 374
ProfileModule module, 434, 482
profiles
  device profile, 230
  module for, 434, 482
  .NET profiles, 108, 241, 244–245
  system profiles
    not running, 87
    run by Windows PowerShell, 87
Protocol Status field type, W3C extended log file format, 395
Protocol Substatus field type, W3C extended log file format, 395
protocol support, 41
  availability of, by server role, 29, 38
  module for, 432, 469–470
Protocol Version field type, W3C extended log file format, 395
protocolManagerDll attribute, 6
protocolManagerDllInitFunction attribute, 6
protocols. See also FTP (File Transfer Protocol); HTTP (Hypertext Transfer Protocol); SMTP (Simple Mail Transfer Protocol); SSL (Secure Sockets Layer)
HTTPS (Hypertext Transfer Protocol Secure), 24, 324
MIME (Multipurpose Internet Mail Extensions) protocol, 25
TCP/IP, 23
  in URLs, 59
ProtocolSupportModule module, 432, 469–470
providers, .NET, 110, 240–243
proxy servers, affecting connections to server, 72
ps cmdlet alias, 92
PS drive, 90
.psl file extension, 88
public key, 324
public key encryption, 323
Push-Location cmdlet, 90
PUT request, with ISAPI extensions, 210
pwd cmdlet alias, 92

$Q redirect variable, 178
query string, in URL, 61
question mark (?), in URL, 61
queuing
message queuing
activation of, 34
availability of, 31
server functions for, 35
request queues
limiting, 270, 288–289, 382
optimizing performance of, 382–384
thread queuing, performance counters for, 374

R
r cmdlet alias, 92
r prefix, W3C extended log file format, 394
RAID, 15
RAM (random access memory) requirements, 13
rapid-fail protection, 273, 278, 287
ratings for Web content, 188
rd cmdlet alias, 93
Read and Execute permission, 296
Read-Host cmdlet, 90
Read permission, 296, 297
real-time request viewing, 2
recovery disks, 426
recovery of IIS from backup, 411
recycle apppool command, AppCmd, 103
RECYCLE command, 22
recycling settings, application pools, 272
redirect headers, HTTP, 469–470
redirection of browser requests, 175
of all requests to another Web site, 176
to applications, 177
availability of, by server role, 28, 38
configuration levels of, 109
module for, 432, 460–462
not including subdirectories, 178
to one specific file, 177
with redirect variables, 178–179
of specific requests to other directories or Web sites, 175
status codes for, 178
with Web servers, 42
Redirection.config file, 412
Referrer field, IIS log file format, 386
Referrer field type, W3C extended log file format, 395
Reliability and Performance Monitor, 17, 365–369
Reliability Monitor, 351, 367
Remark directive, W3C extended log file format, 394
remote administration, 318
IIS Manager permissions, 319–320
IIS Manager user accounts, 318–319
remote management of IIS, 18–19
requirements for, 3
with WMSVC, 66, 74–76
remote service domain, 232
remote transactions
with application servers, 36
availability of, by server role, 29
remove- cmdlet verb, 88
Remove-item cmdlet, 93
Remove-Variable cmdlet, 93
REQUEST administration object, 21
request filtering, 2
availability of, by server role, 30, 39
module for, 433, 470–472
with Web servers, 44
Request management object, 96
request monitor
availability of, by server role, 29, 39
module for, 432, 472
with Web servers, 43
request queues
limiting, 270, 288–289, 382
optimizing performance of, 382–384
RequestFilteringModule module, 433, 470–472
RequestMonitorModule module, 432, 472
requests
code download requests, 4
currently running, listing, 105
encoding, for .NET globalization, 249
execution limit for, 40
failed. See failed request trace logs; tracing
login requests, 3
management service requests, 4
performance counters for, 369
ping requests, 4
redirecting. See redirection of browser requests
running, listing, 269
viewing in real time, 2
WMSVC listening for, types of, 3
worker processes, recycling automatically based on, 283
requireAccess attribute, 121
reset config command, AppCmd, 99, 117
response headers
configuration levels of, 109
custom, 186–188, 469–470
encoding, for .NET globalization, 249
HEAD request for, 210
responses, encoding for .NET globalization, 249
Restart-Service cmdlet, 90
restore backup command, AppCmd, 106, 417
Resume-Service cmdlet, 90
reversible password encryption, 310
rm cmdlet alias, 93
rmdir cmdlet alias, 93
role management, module for, 434, 482
role services
for application servers, 33–36, 47
for desktop, 36–46
managing, 54–58
modifying, 57
viewing, 54, 57
for Web servers, 36–46
for Windows SharePoint Services servers, 46
RoleManagerModule module, 434, 482
roles, .NET, 108, 240, 245
roles of server. See server roles
root certificate, SSL
installing in browser authorities store, 344
renewing, 337
types of, 327
root virtual directory, 63
round-robin load balancing technique, 281
rs prefix, W3C extended log file format, 394
Rscaext.xml file, 5
Runtime Version precondition, managed handlers, 120
rv cmdlet alias, 93
S
s prefix, W3C extended log file format, 394
$s redirect variable, 178
sal cmdlet alias, 93
sasv cmdlet alias, 93
sc prefix, W3C extended log file format, 394
schema files, 429
Script Engine Cache, ASP, 384
script maps, 306, 307
scripting administration tool, 3
scripts, server-side. See ASP (Active Server Pages)
scripts, Windows PowerShell. See Windows PowerShell, scripts
search config command, AppCmd, 114–115
Secure HTTP (HTTPS), 24, 324
Secure Sockets Layer. See SSL
secured Web sites, 147–148
security, 291, 305
access permissions. See access permissions
authentication. See authentication authorization rules. See authorization rules for URLs
domain restrictions. See domain restrictions
enhancements to, 2
feature delegation, 109, 318, 320–322
features for, availability of, 30, 39
handler mappings. See handler mappings
of HTTP errors sent to client, 194, 195
Internet Guest account, 295
IPv4 address restrictions, 315–318
Microsoft Windows security. See Microsoft Windows security
modules affecting, 2
modules for, 430, 432
.NET security, 291
remote administration. See remote administration
request filtering, 2
with SQL Server, 239
with Web servers, 43
Web sites, secured, 147–148
server

for Windows SharePoint Services servers, 46
for WMSVC connections, 4
server. See also application servers; Web servers; Windows SharePoint Services servers
access to, 63–64
administrator for, 63
computer name for, determining, 140
connecting to firewalls affecting, 72
proxy servers affecting, 72
deploying IIS 7.0 on, 26–27
failure of, protecting against, 425–427
IP address for, determining, 140
managing. See IIS Manager; WMSVC (Web Management Service)
multiple sites hosted on, 137–140
rebooting, 79
recovery disks for, 426
role services for. See role services
roles of. See server roles
starting and stopping all services, 76–78
startup and recovery options for, 425–426
server backups. See backups of IIS, server backups
Server IP field, IIS log file format, 392
Server IP field type, W3C extended log file format, 395
Server Manager, 80
adding or removing roles, 56
modifying role services, 57
viewing roles and services, 54, 57
Server Name field type, W3C extended log file format, 395
Server Port field type, W3C extended log file format, 395
server roles, 26
adding or removing, 56
features available for, 27–31, 38–41
managing, 54–58
viewing, 54
server root, configuration file for. See ApplicationHost.config file
Server-Side Includes (SSI)
access permissions for, 297
availability of, by server role, 28, 39
configuring, 182–183
module for, 432, 472–473
with Web servers, 43
server-side scripts. See ASP (Active Server Pages)
ServerIP field, ODBC logging, 397
ServerSidelIncludeModule module, 432, 472–473
Service field
IIS log file format, 392
ODBC logging, 397
Service Host processes, 65
service logs, 353
Service Name and Instance Number field type, W3C extended log file format, 395
service unavailable (503) errors, 278, 287, 288
services
adding, management for, 17
architecture of, 64–72
creating, 90
list of, getting, 90
logon account for, 293–294
managing. See also Server Manager
with Computer Management console, 80–84
pausing, 81
performance counters for, 369
properties of, configuring, 82
removing, to improve performance, 379
restarting after stopping, 90
resuming after suspending, 90
started automatically, failure of, 81
starting, 81, 90
starting and stopping all services for server, 76–78
startup for, configuring, 82
stopping, 81, 90
suspending, 90
Services tool, 17
ServiceStatus field, ODBC logging, 397
session key, 324, 326
Session object, 223
session state
for ASP, 223–224
for ASP.NET, 227–231
configuration levels of, 110
module for, 434, 483
SessionStateModule module, 434, 483
Set-Alias cmdlet, 90, 93
set app command, AppCmd, 103, 224, 259
set apppool command, AppCmd, 102, 270, 276
Set-AuthenticodeSignature cmdlet, 90
set cmdlet alias, 93
set cmdlet verb, 88
SET command, 22
set config command, AppCmd, 99, 115
application pools, configuring, 270
applications, default settings for, 255
ASP behaviors, configuring, 218
ASP caching, optimizing, 221
ASP COM+ execution, configuring, 222
ASP debugging and error handling, configuring, 226
ASP request handling, configuring, 220
browser redirection, configuring, 179
CGI restrictions, configuring, 213
CGI settings, configuring, 215
compression, configuring, 191
content expiration, configuring, 185, 186
custom HTTP headers, configuring, 187
default documents, configuring, 180
directory browsing, enabling and disabling, 168
document footers, configuring, 182
HTTP errors, configuring, 198
HTTP keep-alives, configuring, 158
ISAPI restrictions, configuring, 213
MIME types, configuring, 205
output caching, configuring, 259
Set-Date cmdlet, 90
Set-ExecutionPolicy cmdlet, 90
Set-Location cmdlet, 90, 93
set module command, AppCmd, 100
Set-Service cmdlet, 90
set site command, AppCmd, 101, 154, 157, 161
Set-Variable cmdlet, 93
set vdir command, AppCmd, 104, 171
shared servers, 132
SharePoint. See entries at Windows SharePoint Services
sharing global configurations, 131–134
shell, suspending, 90
side-by-side execution of ASP.NET, 264

SSL (Secure Sockets Layer)  511

signature objects
  getting for file, 90
  setting for script or file, 90
Simple Mail Transfer Protocol. See SMTP
Simple Object Access Protocol (SOAP), with
  WS-atomic transactions, 36
single quote (‘), in URL, 60
SITE administration object, 21
Site management object, 96
site-wide applications, 251, 252, 253
sl cmdlet alias, 93
slash, double (//), in URL, 59, 61
slash (/), in URL, 61
sleep cmdlet alias, 93
SMP (symmetric multiprocessor)
  requirements, 14
SMTP (Simple Mail Transfer Protocol), 26
  ASP.NET settings for, 231–233
  configuration levels of, 110
  services not included for, 3
  using from ASP.NET, 3, 26
SOAP (Simple Object Access Protocol), with
  WS-atomic transactions, 36
soft page faults, 373
Software directive, W3C extended log file
  format, 394
sort cmdlet alias, 93
Sort-Object cmdlet, 93
spps cmdlet alias, 93
spsv cmdlet alias, 93
SQL Server
  book about, 396, 405
  connection strings for, 238, 239
  integrated security with, 239
  out-of-process state management using,
    227, 229
sr prefix, W3C extended log file
  format, 394
SSI (Server-Side Includes)
  availability of, by server role, 28, 39
  configuring, 182–183
  with Web servers, 43
SSL (Secure Sockets Layer), 24, 323–325
  certificates for, 325–326
  configuration levels of, 110
  managing. See Active Directory
    Certificate Services
  configuration levels of, 110
  confirming SSL is enabled, 345
encryption level of, 326, 345
host headers not available with, 324
ports for
  configuring, 343
  default port, 324
requiring for all communications, 346
secured Web sites, creating, 147–148
when to use, 324
with WS-atomic transactions, 36, 48
stand-alone root CA, 327
stand-alone subordinate CA, 327
start apppool command, AppCmd, 103, 278
START command, 22
Start-Date directive, W3C extended log file
  format, 394
Start-Service cmdlet, 90, 93
start site command, AppCmd, 102, 151
Start-Sleep cmdlet, 90, 93
starting point for applications, 251
startup and recovery options, 425–426
static content
  availability of, 28, 38
  module for, 432, 474
  performance of, 379
  with Web servers, 42
static content compression
  availability of, by server role, 30, 39
  module for, 433, 473
  with Web servers, 44
StaticCompressionModule module, 433, 473
staticContent section, 182, 185, 186, 205
StaticFileModule module, 432, 474
Status Code field
  IIS log file format, 385
  NCSA common log file format, 390
status codes
  for HTTP errors, 193–194
  for redirection, 178
stop apppool command, AppCmd, 103, 278
STOP command, 22
STOP error, 425
Stop-Process cmdlet, 93
Stop-Service cmdlet, 90, 93
stop site command, AppCmd, 102, 151
subnet, 135
Suspend-Service cmdlet, 90
sv cmdlet alias, 93
symmetric multiprocessor (SMP)
  requirements, 14
system profiles
  not running, 87
  run by Windows PowerShell, 87
T
  Target field, ODBC logging, 397
TCP activation
  with application servers, 35
  availability of, by server role, 31
TCP/IP, 23
TCP port sharing
  with application servers, 34
  availability of, by server role, 28
thread queuing, performance counters for,
  374
tilde (~), in URL, 61
time
  current, 90
  setting, 90
Time field, IIS log file format, 392
Time field type, W3C extended log file
  format, 395
Time Stamp field, NCSA common log file
  format, 390
Time Taken field type, W3C extended log
  file format, 395
token cache
  availability of, by server role, 29
  module for, 372, 433, 474
  with Web servers, 45
TokenCacheModule module, 372, 433, 474
TRACE administration object, 21
trace logs for failed requests. See failed
  request trace logs
Trace management object, 96
TRACE request, with ISAPI extensions, 210
tracing, 349
  availability of, by server role, 29, 39
  events logged by, displaying, 106
  failed requests
    configuration levels of, 109
    configuring, 106
    listing, 106
    with Web servers, 43
TracingModule module, 432, 475
tracking software, 385
transactions, distributed, 29
Transfer Volume field, NCSA common log
  file format, 391
troubleshooting. See debugging
trusted third-party CA, 326, 339
TTL (Time to Live) value, 383  

type cmdlet alias, 92  
type libraries, caching, 381  

U  
UI culture, for .NET globalization, 249  
UNC (Universal Naming Convention), 137  
underscore (_), in URL, 60  
Uniform Resource Locator (URL). See entries at URL  
uninstall module command, AppCmd, 101  
uninterruptible power supply (UPS) requirements, 15  
Universal Naming Convention (UNC), 137  
unlock config command, AppCmd, 99, 116  
unsecured Web sites, 145–147  
update sites, 205–207  
UPS (uninterruptible power supply) requirements, 15  
URI cache  
availability of, by server role, 29  
module for, 372, 433, 475  
with Web servers, 45  
URI Query field type, W3C extended log file format, 395  
URI Stem field type, W3C extended log file format, 395  
UriCacheModule module, 372, 433, 475  
URL authorization. See authorization rules for URLs  
URL mapping, 434, 484  
URL (Uniform Resource Locator), 59–62, 137  
characters allowed in, 60  
domain name in, 59  
escape codes in, 61  
host name in, 59  
path (directory) in, 60  
performance counters for, 369  
port number in, 60  
protocol name in, 59  
query string in, 61  
(reserved) characters not allowed in, 61  
for SSL, 324  
user name and password in, 60  
UrlAuthorizationModule module, 433, 434, 476–477, 484  

W3C extended log file format  
urlCompression section, 191  
UrlMappingsModule module, 434, 484  
user accounts, 292  
access permissions configured by, 297  
amonymous user account, 295  
domain-level accounts, 292  
for IIS, 292, 293  
IIS Manager user accounts, 318–319  
local-level accounts, 292  
User Agent field type, W3C extended log file format, 395  
User Authentication field, NCSA common log file format, 389  
User Name field, IIS log file format, 392  
User Name field type, W3C extended log file format, 395  
user name, in URL, 60  
Username field, ODBC logging, 397  
users, .NET, 108, 241, 246  

V  
SV redirect variable, 178  
VDIR administration object, 21  
Vdir management object, 96  
-Verbose parameter, cmdlet, 91  
Version directive, W3C extended log file format, 394  
virtual directories, 163  
access to, 64  
AppCmd commands for, 104–105  
for application, created automatically, 257  
for application, managing, 259  
configuring, 163  
creating, 165  
directory-wide applications, 252  
icon representing, 163  
logon credentials for, 166, 170, 171  
logon type for, 170  
physical path for, 170  
virtual directory, root, 63  
virtual memory usage, 372  
virtualDirectoryDefaults section, 255  

W  
W3C extended log file format, 387, 393–396, 458  
configuring, 403–404  
naming conventions for, 399
W3C (World Wide Web Consortium), Platform for Privacy Preferences Project (P3P), 188
W3SVC (World Wide Web Publishing Service), 65, 66
WAS (Windows Process Activation Service), 31, 40
WCF (Windows Communication Foundation), 32
WCS (Windows CardSpace), 31
Web administration, 1
  account privileges for, 59
  tools for, list of, 16–17
Web application administrator, 64
Web applications, 62
  access to, 63–64
  administration of. See Web administration root virtual directory for, 63
Web content. See also default documents, files compression of
  configuring for server, 190–192
  enabling for Web sites and directories, 192
  performance improved by, 189
content ratings, 188
customizing, features for, 173
expiration for, configuring, 184–186
footers, configuring, 182
jump pages, 207
managing, 173–175
privacy policy for, 188–189
update sites, 205–207
Web garden, worker processes for, 68, 281–282
Web Management Service. See WMSVC
Web server administrator, 63
Web server content. See Web content
Web server (IIS) support
  with application servers, 34, 48
  availability of, by server role, 28
Web servers, 27
  features available for, 27–31
  installing, 49–50
  role services for, 36–46, 54–58
Web service, performance counters for, 370
Web site administrator, 64
Web site root, configuration file for, 9
Web sites, 62
  access permissions for, 159
  access to, 63–64
  AppCmd commands for, 101–102
  application pools for, 144, 151–153
  authentication for, 144
  AutoStart state for, 160–162
  bandwidth limits, 155
  bindings for, 62, 153–155
  browsing, 149, 151
  configuring, 149
  creating, 143
    secured, 147–148
    unsecured, 145–147
  default, after IIS installation, 62, 144
  deleting, 162
  directories for, 144
  DNS record for, 144
  editing, 149
  home directory for, 151–153, 173
  host headers for, 62
  HTTP keep-alives, 158–159, 469–470
  identifiers for, 136–137
  incoming connections, restricting, 155–157
  IP address for. See IP addresses
    list of, on server, 141–143
  managing, 149–151
  multiple, hosting on one server, 137–140, 153
  numeric ID for, 160–162
  redirecting browser requests to, 175, 176
  restarting, 150
  starting, 78, 151
  stopping, 78, 151
  time-out values for, setting, 155–157
  update sites, 205–207
Web.config file, 429
  ASP.NET key/value pairs stored in, 233
  backups of, 413–414
  for .NET Framework root, 9
  for server-level ASP.NET configuration, 227
  for top-level content directory, 9
  for Web site root, 9
well-known ports, 60
WF (Windows Workflow Foundation), 32
  -WhatIf parameter, cmdlet, 91
Win32 Status field type, W3C extended log file format, 395
Win32Status field, ODBC logging, 397
Windows authentication, 310
availability of, by server role, 30, 39
integrated Windows authentication, 310
module for, 433, 434, 477–478, 485
with Web servers, 44
Windows CardSpace (WCS), 31
Windows Communication Foundation (WCF), 32
Windows event logs, 351, 353–356
accessing, 353
event sources listed in, 354, 355
filtering by event, 355
information in, analyzing, 354–355
Windows logs, 353
Windows Performance Monitor, 351, 366
Windows PowerShell, 85
cmdlets, 87–89
alias names for, 90, 92–93
debugging, 91
deploying IIS using, 94–95
errors in, 91
help on, 89
list of, 90
managing IIS using, 93
output buffer for, 91
parameters for, 91
running at prompt, 88
running from scripts, 88
verbs for, 88
wildcards used with, 91
command prompt for, 87
installing, 85, 86
location of, 86
running, 86
running without profiles, 87
scripting language of, 85, 88
scripts
enabling, 87
execution policy for, 87, 90
running from current directory, 89
suspending, 90
system profiles run by, 87
Windows commands, running from, 89
Windows Presentation Foundation (WPF), 32
Windows Process Activation Service Support (WPASS), 2, 66
adding or removing on Windows Vista, 54
with application servers, 34
availability of, by server role, 31

Worker Process isolation mode
protocols for, specifying, 34
Windows Process Activation Service (WAS), 31, 40
Windows Reliability Monitor, 351, 367
Windows security. See Microsoft Windows security
Windows Server 2008 Administrator's Pocket Consultant, 294, 296, 419
Windows Server 2008 Inside Out, 419
Windows Server Backup, 419, 420
enabling, 419
full backups, 420
incremental backups, 420
performance options for, 421
performing backups, 424–425
recovery of files and folders, 427–428
scheduling backups, 422–423
Windows server editions, support for, 16
Windows SharePoint Management Tools, 31
Windows SharePoint Services applications
availability of, by server role, 31
libraries in, 46
lists in, 46
workload produced by, 46
Windows SharePoint Services servers, 27
dependent load-balanced configuration
for, 51
e-mail settings for, 52
features available for, 27–31
independent server configuration for, 51
installing, 51–53
role services for, 46
security for, 46
Windows Status Code field, IIS log file format, 385
Windows Vista
support for, 15
Web server features for, turning on or off, 53
Windows Workflow Foundation (WF), 32
WindowsAuthenticationModule module, 433, 434, 477–478, 485
WMSVC (Web Management Service), 3, 17
configuration values stored by, 4
remote management using, 66, 74–76
requests listened for, types of, 3
Worker Process isolation mode, 65–68
worker processes, 68, 267
  configuration levels of, 110
  currently running, listing, 105
  failure detection and recovery, 286–287
  idle, shutting down, 287
  listing, 269
  maximum number of, 383
  multiple (Web gardens), 68, 281–282
  pinging of, 286
  recycling automatically, 282–283, 284
  recycling manually, 279
  starting and stopping manually, 277–279
  startup and shutdown limits for, 280–281
World Wide Web Consortium. See entries at W3C
World Wide Web Publishing Service (W3SVC), 65, 66
WP administration object, 21
Wp management object, 96
WPASS. See Windows Process Activation Service Support

WPF (Windows Presentation Foundation), 32
write cmdlet alias, 93
Write-Output cmdlet, 90, 93
Write permission, 296
WS-atomic transactions
  with application servers, 36
  availability of, by server role, 29
  SSL certificate for, 48

X
  x prefix, W3C extended log file format, 394
X.509 standard, 325
XML (Extensible Markup Language)
  schema files, 2, 4–8
  extending the schema, 5
  list of files, 5
  location of files, 5
  managing, 4
  syntax for schema, 6–8
About the Author

William R. Stanek (http://www.williamstanek.com/) has over 20 years of hands-on experience with advanced programming and development. He is a leading technology expert, an award-winning author, and an excellent and popular instructional trainer. Over the years, his practical advice has helped millions of technical professionals all over the world. He has written more than 65 books, including Microsoft Exchange Server 2007 Administrator’s Pocket Consultant, Windows Vista Administrator’s Pocket Consultant, Windows Server 2008 Administrator’s Pocket Consultant, and Windows Server 2008 Inside Out.

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

Stanek has an MS degree with distinction in information systems and a BS degree (magna cum laude) in computer science. He is proud to have served in the Persian Gulf War as a combat crewmember on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including the Air Force Distinguished Flying Cross, one of the highest flying honors one can receive in the U.S. military. Currently, he resides in the Pacific Northwest with his wife and children.
What do you think of this book?

We want to hear from you!

Do you have a few minutes to participate in a brief online survey?

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you.

To participate in our survey, please visit:

www.microsoft.com/learning/booksurvey/

...and enter this book’s ISBN-10 number or ISBN-13 number (located above barcode on back cover*). As a thank-you to survey participants in the United States and Canada, each month we’ll randomly select five respondents to win one of five $100 gift certificates from a leading online merchant. At the conclusion of the survey, you can enter the drawing by providing your e-mail address, which will be used for prize notification only.

Thanks in advance for your input. Your opinion counts!

*Where to find the ISBN on back cover

Example only. Each book has unique ISBN.

No purchase necessary. Void where prohibited. Open only to residents of the 50 United States (includes District of Columbia) and Canada (void in Quebec). For official rules and entry dates see:

www.microsoft.com/learning/booksurvey/