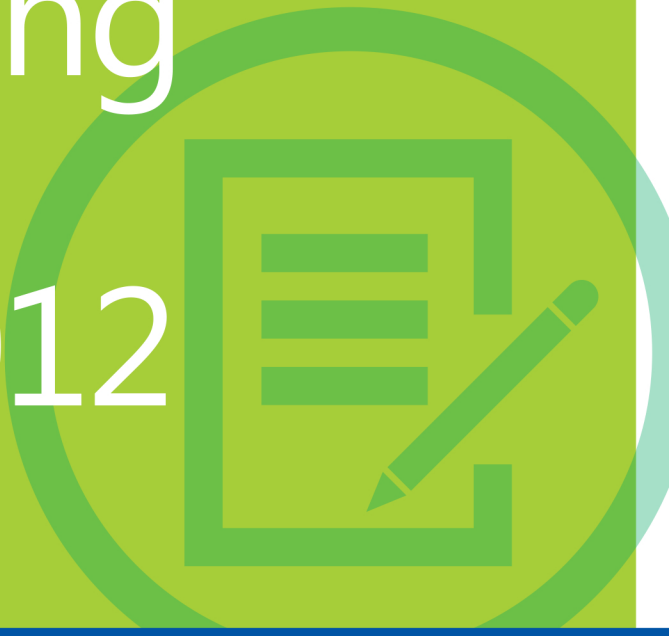
Microsoft

Installing and Configuring Windows Server® 2012



Training Guide

Mitch Tulloch

Installing and Configuring Windows Server 2012

Designed to help enterprise administrators develop real-world, job-role-specific skills—this *Training Guide* focuses on deploying and managing core infrastructure services in Windows Server 2012. Build hands-on expertise through a series of lessons, exercises, and suggested practices—and help maximize your performance on the job.

This Microsoft *Training Guide:*

- Provides in-depth, hands-on training you take at your own pace
- Focuses on job-role-specific expertise for deploying and managing Windows Server 2012 core services
- Creates a foundation of skills which, along with on-the-job experience, can be measured by Microsoft Certification exams such as 70-410

Sharpen your skills. Increase your expertise.

- Plan a migration to Windows Server 2012
- Deploy servers and domain controllers
- Administer Active Directory® and enable advanced features
- Ensure DHCP availability and implement DNSSEC
- Perform network administration
- Deploy and manage Hyper-V® hosts and virtual machines
- Deploy and manage Storage Spaces and iSCSI storage
- Deploy and manage print servers
- Plan, configure, and manage Group Policy
- Automate administrative tasks with Windows PowerShell™

About You

This *Training Guide* will be most useful to IT professionals who have at least three years of experience administering previous versions of Windows Server in midsize to large environments.

About the Author

Mitch Tulloch is a widely recognized expert on Windows administration and has been awarded Microsoft® MVP status for his contributions supporting those who deploy and use Microsoft platforms, products, and solutions. He is the author of *Introducing Windows Server 2012* and the upcoming *Windows Server 2012 Virtualization Inside Out*.

About the Practice Exercises

For most practices, we recommend using a Hyper-V virtualized environment. Some practices will require physical servers.

For *system requirements*, see the Introduction.

Preparing for Microsoft Certification?

Get the official exam-prep guide for Exam 70-410.

Exam Ref 70-410: Installing and Configuring Windows Server 2012

ISBN 9780735673168

microsoft.com/mspress

ISBN: 978-0-7356-7310-6

9 780735 673106 90000

U.S.A. $59.99
Canada $62.99
[*Recommended*]

Operating Systems/ Windows Server

Microsoft

Microsoft®

Installing and Configuring Windows Server® 2012

Training Guide

Mitch Tulloch

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

Copyright © 2012 by Mitch Tulloch

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

Library of Congress Control Number: 2012951988
ISBN: 978-0-7356-7310-6

Printed and bound in the United States of America.

Third Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Microsoft and the trademarks listed at http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

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

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

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Project Editors: Karen Szall and Carol Dillingham
Editorial Production: Waypoint Press
Technical Reviewer: Bob Dean; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Roger LeBlanc
Indexer: Christina Yeager
Cover: Twist Creative • Seattle

[LSI] [2013-08-12]

Contents at a glance

	Introduction	*xvii*
CHAPTER 1	**Preparing for Windows Server 2012**	**1**
CHAPTER 2	**Deploying servers**	**37**
CHAPTER 3	**Server remote management**	**83**
CHAPTER 4	**Deploying domain controllers**	**135**
CHAPTER 5	**Active Directory administration**	**183**
CHAPTER 6	**Network administration**	**225**
CHAPTER 7	**Hyper-V virtualization**	**291**
CHAPTER 8	**File services and storage**	**361**
CHAPTER 9	**Print and document services**	**431**
CHAPTER 10	**Implementing Group Policy**	**465**
CHAPTER 11	**Configuring Windows Firewall and IPsec**	**515**
	Index	*579*

Contents

Introduction **xvii**

System requirements xviii

Acknowledgments xxi

Errata & book support xxi

We want to hear from you xxii

Stay in touch xxii

Chapter 1 Preparing for Windows Server 2012 **1**

Before you begin. 1

Lesson 1: Planning for Windows Server 2012 2

- Migration scenarios 3
- Migration process 10
- Lesson summary 17
- Lesson review 18

Lesson 2: Assessing the readiness of your environment 19

- Manual assessment 19
- Using the MAP Toolkit 22
- Other tools and methodologies 27
- Lesson summary 28
- Lesson review 29

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

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

www.microsoft.com/learning/booksurvey/

Practice exercises 29
Exercise 1: Using the MAP Toolkit 30
Exercise 2: Performing an in-place upgrade 32
Suggested practice exercises 33
Answers. 34

Chapter 2 Deploying servers 37

Before you begin. 38
Lesson 1: Installation options 38
Understanding installation options 39
Converting between installation options 41
Lesson summary 45
Lesson review 46
Lesson 2: Preparing the build lab 47
Understanding image life-cycle management 47
Build vs. production environment 48
Setting up your build lab 48
Understanding the reference-image build process 50
Setting up the technician computer 52
Lesson summary 53
Lesson review 53
Lesson 3: Building images 54
Building reference images using MDT 2012 Update 1 54
Testing reference images 65
Lesson summary 65
Lesson review 66
Lesson 4: Deploying images 67
Preparing the deployment infrastructure 67
Using the LTI approach 68
Using the ZTI approach 69
Lesson summary 70
Lesson review 71

Practice exercises 71
Exercise 1: Converting between installation options 71
Exercise 2: Building a reference image with MDT 2012 Update 1 74
Suggested practice exercises 77
Answers. 78

Chapter 3 Server remote management 83

Before you begin. 83
Lesson 1: Server Manager 84
Navigating Server Manager 84
Configuring remote management 90
Running Server Manager on Windows 8 92
Lesson summary 93
Lesson review 94
Lesson 2: Server management tasks 95
Adding servers 95
Creating server groups 96
Restart a server 97
Collecting events 98
Monitoring services 101
Collecting performance data 103
Viewing status notifications 105
Lesson summary 106
Lesson review 107
Lesson 3: Installing roles and features 108
Prerequisites for installing roles and features 108
Installing roles and features using Server Manager 110
Installing roles and features using Windows PowerShell 114
Removing roles and features 116
Lesson summary 117
Lesson review 117

Lesson 4: Windows PowerShell automation 119
Background jobs 119
Scheduled jobs 120
Disconnected sessions 121
Resources for learning Windows PowerShell 123
Lesson summary 124
Lesson review 125
Practice exercises 126
Exercise 1: Installing roles and features 126
Exercise 2: Managing alerts with the Dashboard 127
Exercise 3: Scheduling tasks using Windows PowerShell jobs 128
Suggested practice exercises 129
Answers. 130

Chapter 4 Deploying domain controllers 135

Before you begin. 136
Lesson 1: Preparing for deploying domain controllers 136
AD DS deployment scenarios 136
New forest domain controller deployment 139
Existing forest domain controller deployment 144
Lesson summary 146
Lesson review 146
Lesson 2: Deploying domain controllers using Server Manager 147
Preparing for domain-controller deployment 148
Installing the AD DS role 150
Running the AD DS Configuration Wizard 151
Verifying the installation 157
Uninstalling AD DS 159
Lesson summary 162
Lesson review 162

Lesson 3: Deploying domain controllers using Windows PowerShell 164
Preparing for domain-controller deployment 164
Using Windows PowerShell to deploy domain controllers 167
Verifying domain-controller deployment 172
Uninstalling AD DS 174
Lesson summary 174
Lesson review 174
Practice exercises 175
Exercise 1: Installing a new forest using Server Manager 176
Exercise 2: Remotely adding an additional domain controller using Windows PowerShell 177
Suggested practice exercises 178
Answers 179

Chapter 5 Active Directory administration 183

Before you begin 183
Lesson 1: Administering Active Directory objects using ADAC 184
Overview of ADAC 184
Searching Active Directory 188
Common administration tasks 190
Lesson summary 196
Lesson review 197
Lesson 2: Enabling advanced features using ADAC 198
Enabling and using the Active Directory Recycle Bin 198
Configuring fine-grained password policies 202
Lesson summary 206
Lesson review 207

Lesson 3: Administering Active Directory using Windows PowerShell 208
Managing user accounts with Windows PowerShell 208
Finding Active Directory administration cmdlets 212
Performing an advanced Active Directory administration task 213
Lesson summary 216
Lesson review 216
Practice exercises 217
Exercise 1: Creating organizational units using Windows PowerShell 217
Exercise 2: Creating user accounts using Windows PowerShell 218
Suggested practice exercises 220
Answers. 220

Chapter 6 Network administration 225

Before you begin. 225
Lesson 1: Ensuring DHCP availability 226
Previous approaches to implementing DHCP availability 226
Understanding DHCP failover 227
Implementing DHCP failover 229
Managing DHCP failover 231
Lesson summary 233
Lesson review 233
Lesson 2: Implementing DNSSEC 234
Benefits of DNSSEC 235
DNSSEC in previous Windows Server versions 237
How DNSSEC works 237
Deploying DNSSEC 239
Lesson summary 242
Lesson review 243

Lesson 3: Managing networking using Windows PowerShell 244
Identifying networking cmdlets 244
Examples of network-administration tasks 252
Lesson summary 256
Lesson review 257
Lesson 4: Configuring IPv6/IPv4 interoperability 258
IPv6 concepts and terminology 258
IPv6 addressing 263
IPv6 address assignment 267
IPv6 transition technologies 276
ISATAP 277
Lesson summary 280
Lesson review 280
Practice exercises 281
Exercise 1: Implementing DHCP failover using Windows PowerShell 282
Exercise 2: Configuring a caching-only DNS server using Windows PowerShell 283
Suggested practice exercises 285
Answers. 286

Chapter 7 Hyper-V virtualization 291

Before you begin. 291
Lesson 1: Deploying and configuring Hyper-V hosts 292
Planning Hyper-V deployment 292
Installing the Hyper-V role 304
Configuring Hyper-V hosts 307
Lesson summary 315
Lesson review 315

Lesson 2: Deploying and configuring virtual machines 316
Planning virtual machine deployment 317
Creating virtual machines 324
Configuring virtual machines 326
Lesson summary 337
Lesson review 337
Lesson 3: Managing virtual machines 339
Optimizing workload consolidation 339
Optimizing network performance 343
Optimizing virtual disks 345
Managing snapshots 348
Monitoring virtual machines 350
Lesson summary 351
Lesson review 351
Practice exercises 352
Exercise 1: Installing and configuring Hyper-V on Server Core 353
Exercise 2: Creating and configuring virtual machines 354
Suggested practice exercises 355
Answers. 356

Chapter 8 File services and storage 361

Before you begin. 361
Lesson 1: Deploying Storage Spaces 362
Understanding Storage Spaces 362
Planning a Storage Spaces deployment 369
Implementing Storage Spaces 373
Lesson summary 375
Lesson review 375

Lesson 2: Provisioning and managing shared storage 377
Provisioning shared storage 377
Provisioning SMB shares 387
Managing shared storage 393
Lesson summary 396
Lesson review 396
Lesson 3: Configuring iSCSI storage 397
Understanding iSCSI storage 397
Configuring iSCSI Target Server 401
Using iSCSI Initiator 411
Lesson summary 418
Lesson review 419
Practice exercises 419
Exercise 1: Provisioning and managing shared storage using Server Manager 420
Exercise 2: Provisioning and managing shared storage using Windows PowerShell 423
Suggested practice exercises 424
Answers. 425

Chapter 9 Print and document services 431

Before you begin. 431
Lesson 1: Deploying and managing print servers 431
Deploying print servers 432
Managing printers using Print Management 436
Lesson summary 448
Lesson review 448
Lesson 2: Managing print servers using Windows PowerShell 450
Viewing information about printers, printer drivers, and print jobs 450
Managing printers, printer drivers, and print jobs 454
Lesson summary 457
Lesson review 457

Practice exercises 458
Exercise 1: Managing print servers using Print Management 458
Exercise 2: Managing print servers using Windows PowerShell 459
Suggested practice exercises 460
Answers. 461

Chapter 10 Implementing Group Policy 465

Before you begin. 465
Lesson 1: Planning, implementing, and managing Group Policy 466
Planning for Group Policy 466
Configuring security settings 476
Managing Group Policy 482
Lesson summary 487
Lesson review 488
Lesson 2: Managing Group Policy using Windows PowerShell 489
Creating and linking GPOs 489
Remotely refreshing Group Policy 490
Backing up and restoring GPOs 491
Lesson summary 492
Lesson review 492
Lesson 3: Implementing Group Policy preferences 493
Understanding preferences 493
Windows Settings extensions 506
Control Panel Settings extensions 506
Lesson summary 507
Lesson review 508
Practice exercises 509
Exercise 1: Designing and implementing Group Policy 509
Exercise 2: Creating and managing GPOs using Windows PowerShell 510
Suggested practice exercises 511
Answers. 511

Chapter 11 Configuring Windows Firewall and IPsec 515

Before you begin. 515

Lesson 1: Configuring Windows Firewall with Advanced Security 516

- Understanding Windows Firewall with Advanced Security 516
- Managing firewall profiles 519
- Configuring firewall rules 526
- Lesson summary 541
- Lesson review 542

Lesson 2: Configuring IPsec 543

- Understanding connection security 543
- Configuring IPsec settings 548
- Configuring connection security rules 555
- Lesson summary 569
- Lesson review 569

Practice exercises 570

- Exercise 1: Configuring firewall rules 571
- Exercise 2: Implementing IPsec 573

Suggested practice exercises 575

Answers. 575

Index 579

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

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

www.microsoft.com/learning/booksurvey/

Introduction

This training guide is intended for information technology (IT) professionals who need to upgrade their skills to support Windows Server 2012 in their workplace. The primary focus of the book is on job-role training for system administrators and IT support staff in midsize to large environments. The book contains detailed technical information and hands-on practice exercises to help you prepare for deploying, managing, and maintaining servers running Windows Server 2012. The book assumes that you have at least three years of experience administering previous versions of Windows Server, including experience with operating systems deployment, Active Directory administration, server virtualization using Hyper-V, network and storage management, file and print services, and Group Policy.

Because automation is such an essential skill for administrators who manage the modern, virtualized datacenter, much of this book focuses on learning how to administer server roles and features using Windows PowerShell. While it will be helpful if you have at least rudimentary knowledge of using Windows PowerShell to manage earlier versions of Windows Server, readers who have no prior familiarity with Windows PowerShell should still be able to learn and perform most of the exercises in this book.

This book covers some of the topics and skills that are the subject of the Microsoft certification exam 70-410. If you are using this book to complement your study materials, you might find this information useful. Note that this book is designed to help you in the job role; it might not cover all exam topics. If you are preparing for the exam, you should use additional study materials to help bolster your real-world experience. For your reference, a mapping of the topics in this book to the exam objectives is included in the back of the book.

By using this training guide, you will learn how to do the following:

- Assess the hardware and software in your current environment to plan for a migration to Windows Server 2012.
- Build customized reference images of Windows Server 2012, and deploy them using the Microsoft Deployment Toolkit.
- Perform remote server management and role installation using Server Manager and Windows PowerShell.
- Deploy domain controllers using Server Manager and Windows PowerShell.

- Administer Active Directory and enable advanced Active Directory features using the Active Directory Administrative Center and Windows PowerShell.
- Ensure DHCP availability, implement DNSSEC, configure IPv4/IPv6 interoperability, and perform network administration tasks using Windows PowerShell.
- Deploy, configure, and manage Hyper-V hosts and virtual machines using Hyper-V Manager and Windows PowerShell.
- Deploy Storage Spaces and provision and manage shared storage, including iSCSI storage, using Server Manager and Windows PowerShell.
- Deploy and manage print servers using the Print Management console and Windows PowerShell.
- Plan, configure, and manage Group Policy policies and preferences using the Group Policy Management console and Windows PowerShell.
- Configure Windows Firewall with Advanced Security and implement IPsec connection security.

System requirements

The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. To minimize the time and expense of configuring physical computers for this training guide, it's recommended that you use Hyper-V, which is a feature of Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012. Note, however, that

- The exercises in Chapter 1 recommend using a physical server instead of a virtual environment.
- The exercises in Chapters 7 and 8 require using a physical server instead of a virtual environment.

Hardware requirements

This section presents the hardware requirements for Hyper-V, the hardware requirements if you are not using virtualization software, and the software requirements.

Virtualization hardware requirements

If you choose to use virtualization software, you need only one physical computer to perform the exercises in this book. That physical host computer must meet the following minimum hardware requirements:

- x64-based processor that includes both hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection (DEP). On AMD systems, the data execution protection feature is called the No Execute or NX bit. On Intel systems, this feature is called the Execute Disable or XD bit. These features must also be enabled in the BIOS.
- 8 GB or more RAM
- 500 GB or more available hard disk space
- Integrated 1-GbE networking
- Integrated SVGA (800 x 600) or higher video
- DVD-ROM drive
- Internet connectivity

Physical hardware requirements

If you choose to use physical computers instead of virtualization software, use the following list to meet the minimum hardware requirements of the practice exercises in this book:

- Two servers, each with a 1.4-GHz or faster processor, 2 GB or more RAM, 500 GB or more available hard disk space, integrated 1-GbE networking, integrated SVGA (800 x 600) or higher video, and a DVD-ROM drive. At least one of these servers must:
  - Include hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection (DEP). On AMD systems, the data execution protection feature is called the No Execute or NX bit. On Intel systems, this feature is called the Execute Disable or XD bit. These features must also be enabled in the BIOS.
  - Have dual 1-GbE networking.
  - Have at least two additional physical disks (either internally or externally connected) of a type supported by the Storage Spaces feature (for example, SAS or SATA disks).
- One workstation with a 1-GHz or faster processor, 2 GB or more RAM, a 250 GB or greater hard disk drive, a network card, a video card, and a DVD-ROM drive.

- All three computers must be physically connected to each other and to the Internet through a Network Address Translation (NAT) router or gateway device.
- The test network that includes these computers should be isolated from your production network. (For example, your test network cannot already include a Dynamic Host Configuration Protocol [DHCP] server that automatically assigns addresses to computers.)

Software requirements

The following software is required to complete the practice exercises:

- Windows Server 2012. You can download an evaluation edition of Windows Server 2012 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/hh670538.aspx*.
- Windows 8 Enterprise. You can download an evaluation edition of Windows 8 Enterprise from the TechNet Evaluation Center at *http://technet.microsoft.com/en-US/evalcenter/hh699156.aspx*.
- Windows Server 2008 R2. You can download an evaluation edition of Windows Server 2008 R2 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/ee175713.aspx*.
- The Microsoft Assessment and Planning Toolkit 7.0 (MAP 7.0). You can download MAP 7.0 from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?&id=7826*.
- The Windows Assessment and Deployment Kit (ADK) for Windows 8. You can download the ADK for Windows 8 from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?id=30652*.
- The Microsoft Deployment Toolkit (MDT) 2012 Update 1. You can download MDT 2012 Update 1 from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?id=25175*.
- Microsoft Office 2010. You can download an evaluation edition of Office Professional Plus 2010 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-US/evalcenter/ee390818.aspx*.
- If you are not using virtualization software, you need software that allows you to handle .iso files. This software needs to perform either of the following functions:
  - Burn .iso files to CDs or DVDs. (This solution also requires CD/DVD recording hardware.)
  - Mount .iso files as virtual CD or DVD drives on your computer.

Acknowledgments

The author would like to thank the following people for their tireless work and care toward making this book a success:

- Karen Szall, Senior Content Development Manager at Microsoft Press, for helping get the project up and running and for keeping the author on the straight and narrow with her constant whip of words (just kidding).
- Carol Dillingham, Content Project Manager at Microsoft Press, who carried the project to a successful and timely conclusion to the immense relief of everyone involved, including (especially) the author.
- Steve Sagman, the owner of Waypoint Press, whose careful attention to detail ensured that the laborious production process would go smoothly.
- Roger LeBlanc, whose careful copyediting of the author's manuscript ensured that all *mays* became *mights*, all *sinces* were replaced with *becauses*, and all *whiles* were substituted by *althoughs*.
- Bob Dean, whose technical reviewing actually discovered some mistakes that the author made in the text and exercises. Golly, and I thought I was perfect!
- Neil Salkind, the author's agent at Studio B (*www.studiob.com*), who made sure the author got a good enough deal to keep him eating macaroni and cheese at least until Christmas.

Errata & book support

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://www.microsoftpressstore.com/title/9780735673106

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 1

Preparing for Windows Server 2012

Successful execution of any task always begins with planning. If your job involves the migration of your organization's IT infrastructure to Microsoft Windows Server 2012, you need to prepare both your environment and yourself for this task.

This chapter describes common infrastructure migration scenarios and outlines the steps involved in a typical server-migration process. The chapter also examines some approaches and tools you can use for assessing the readiness of your environment for migrating to Windows Server 2012.

Lessons in this chapter:

- Lesson 1: Planning for Windows Server 2012 **2**
- Lesson 2: Assessing the readiness of your environment **19**

Before you begin

To complete the practice exercises in this chapter

- You should have some familiarity with the new features and capabilities found in Windows Server 2012. If not, then before continuing take time to browse some of the following sources of information:
  - The demo videos available on the Microsoft Server And Cloud Platform page at *http://www.microsoft.com/en-us/server-cloud/new.aspx*
  - The topic "What's New in Windows Server 2012" and the subtopics linked from that page in the TechNet Library at *http://technet.microsoft.com/en-us/library/hh831769*
  - The free ebook "Introducing Windows Server 2012," which can be downloaded from *http://go.microsoft.com/FWLink/?Linkid=251464*
- You should have downloaded an evaluation copy of Windows Server 2012 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/bb291020.aspx*.

- You should have a server system available for testing purposes that meets the minimum hardware requirements for installing Windows Server 2012. This server should also meet the following additional requirements:
  - The system hardware should meet the minimum requirements for installing version 7.0 of the Microsoft Assessment and Planning (MAP) Toolkit. For more information about these requirements, see *http://www.microsoft.com/en-us/download/details.aspx?&id=7826*.
  - The server should have Windows Server 2008 R2 SP1 or Windows Server 2008 SP2 installed. If needed, you can download an evaluation copy of Windows Server 2008 R2 SP1 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/bb291020.aspx*.
  - The server should be a standalone server belonging to a workgroup.
  - The network where the server resides should have Internet connectivity, and the server should be configured with a static IP address, subnet mask, default gateway, and primary and secondary DNS servers that enable the server to access the Internet.
  - It is recommended that the server be a physical server (not a virtual machine) for the purposes of performing the exercises in this chapter. If you decide, however, to run the server as a virtual machine using Hyper-V on Windows Server 2008 R2 SP1, be sure to install the update described in *http://support.microsoft.com/kb/2526776* so that you will be able to upgrade the virtual machine's guest operating system to Windows Server 2012 as required by one of the practice exercises in this chapter.
- You will also need a client computer that has Microsoft Office 2010 or Office 365 installed for viewing the reports generated by the MAP Toolkit in one of the practice exercises in this chapter.

Lesson 1: Planning for Windows Server 2012

The success of an infrastructure-migration project depends on careful planning combined with meticulous execution. You need to start by defining the scope of the project so that you know where you want to end up. Then you need to lay out a project plan that involves pilot testing to familiarize yourself with the new platform and to identify any potential issues that might arise during the migration process. A thorough assessment of your existing environment is also necessary to ensure there are no surprises coming. A methodology needs to be developed to migrate existing servers and roles. Finally, once the migration is underway, continued testing needs to be performed to ensure everything is happening as planned.

After this lesson, you will be able to

- Describe six possible migration scenarios for organizations that want to take advantage of the new features and capabilities found in Windows Server 2012.
- Understand some of the steps involved in an infrastructure-migration process, including pilot testing, assessment, server migration, and role and feature migration.
- Explain how to install and use the Windows Server Migration Tools to migrate server roles from earlier Windows Server versions to Windows Server 2012.

Estimated lesson time: 30 minutes

Migration scenarios

Migration projects involving servers can be categorized in a number of ways, depending on whether you are deploying a new infrastructure, upgrading or consolidating an existing infrastructure, or implementing a new infrastructure model such as cloud computing. In addition, migrations can differ depending on whether or not you are migrating your entire infrastructure or only portion of it; whether you plan on re-using existing hardware or moving to new hardware; whether your environment is managed or unmanaged; whether your existing infrastructure is large or small, centralized or distributed, heterogeneous or homogeneous; and many other factors.

With so many different ways of envisioning and scoping infrastructure-migration projects, it's obvious that there is no single approach to how such projects should be planned and executed. However, there are some steps and considerations that are common to all migration projects, and being aware of such *best practices* and implementing them can help ensure the project's success.

I'll begin by describing the following six possible migration scenarios for organizations that want to take advantage of the new features and capabilities found in Windows Server 2012:

- Greenfield
- Forest upgrade
- Mixed environment
- Server consolidation
- Private cloud
- Public cloud

Note that other migration scenarios are also possible—for example, by combining two or more of the following scenarios to create hybrid scenarios.

Greenfield

In terms of infrastructure, a *greenfield* deployment is one where no infrastructure currently exists. For example, let's say that Contoso, Ltd. is a new company starting up that needs an on-premises infrastructure deployed for its rapidly growing workforce. A greenfield deployment of an infrastructure based on Windows Server 2012 might include steps like these:

- Designing, acquiring and implementing the underlying network infrastructure of switches, routers, access points, and other networking hardware.
- Designing the Active Directory environment using the guidelines and best practices found in the AD DS Design Guide at *http://technet.microsoft.com/en-us/library/cc754678(v=WS.10).aspx*.
- Purchasing system hardware that has been certified for Windows Server 2012.
- Performing a pilot deployment to determine whether the planned infrastructure will meet your business needs and to anticipate any possible problems that might arise during the rollout.
- Rolling out your production infrastructure using whatever deployment tools you've decided to use. We'll examine some of these tools later in Chapter 2, "Deploying servers."

The main advantage of a greenfield migration is that it gives you the opportunity to get it right from the start. On the other hand, businesses are always evolving and are rarely static, so even if you carefully plan for future growth you might still be faced with challenges in evolving your infrastructure to address events such as mergers, acquisitions, and spinoffs of business units. And as a reality check, most readers of this Training Guide who are looking to upgrade their job skills are likely to be working at companies that have one or more existing Active Directory forests in place and are contemplating migrating them to Windows Server 2012, which is what the next migration scenario is about.

REAL WORLD **MIGRATION FROM SCRATCH**

In one sense, it might seem strange to call a greenfield deployment a "migration." After all, how can you migrate from something that didn't previously exist? However, the underlying IT infrastructure of most new businesses generally isn't one that starts from scratch but instead evolves, rapidly or slowly, until a decision is made to settle on a specific infrastructure model and implement it using a formally agreed-upon process.

For example, the founders of Contoso, Ltd. might have started up their business in the garage of one of their homes and used free Google Apps running on Apple MacBook laptops via a neighborhood WiFi connection to do all their initial planning, accounting, and communications. Once they leased offices and hired several dozen employees, however, they might decide that it makes business sense for them to deploy an infrastructure that centralizes the management and ensures the security of their IT resources. Depending on how they foresee their business evolving, they might decide to either deploy a new Active Directory forest on-premises, implement a private cloud solution, or use a public cloud service provider.

Forest upgrade

Administrators of Active Directory environments have traditionally been cautious, or even paranoid, about performing schema upgrades using the Adprep.exe command-line utility. With the release of each new version of Windows Server comes a new schema version as well, and in the past, the task of introducing domain controllers running the new version of Windows Server into your existing Active Directory environment has required that you first prepare your forest by upgrading the schema. The reluctance that administrators have toward performing such upgrades is based largely on three concerns:

- The process of upgrading a forest schema using Adprep was often a cumbersome one on previous versions of Windows Server and involved using a variety of different credentials to log on to specific domain controllers, copy Adprep files, and run Adprep from the command line with various parameters. The more complex the process, the greater the chance is of an error occurring.
- There was the possibility that something might go wrong during the schema upgrade process, resulting in a corrupt forest that requires you to perform a forest recovery, which can be a difficult and time-consuming process.
- There was the possibility that the schema upgrade might go off well but result in side effects, such as enterprise applications that break and no longer function properly.

The recommended approach to avoiding such problems is to create a test environment that mirrors your production environment in terms of its Active Directory schema, network services, and business applications. By upgrading the schema of your test forest using Adprep, you can then better anticipate any problems that might arise when you upgrade the schema of your production forest. For information on how to mirror your production schema into a test environment so that you can perform such testing, see the article "Export, Compare, and Synchronize Active Directory Schemas" from the April 2009 issue of TechNet Magazine at *http://technet.microsoft.com/en-us/magazine/2009.04.schema.aspx*.

Clearly, these are not trivial concerns when your job as administrator is potentially at stake. So before you perform a forest upgrade, you need to be well prepared—for example:

- You need to understand the schema upgrade process and its possible impact on your environment.
- You need to have a forest recovery plan in place as a backup solution for your worst-case scenario.

With Windows Server 2012, however, Microsoft has endeavored to alleviate many of the concerns administrators often have about performing forest upgrades. For example:

- Adprep functionality is now integrated into the Active Directory Domain Services (AD DS) installation process. In most cases, this now eliminates the need to separately run Adprep prior to introducing domain controllers running the new version of Windows Server.

- The new AD DS installation process includes prerequisite validation to identify potential errors before installation begins. For example, if the installation process determines that **adprep /domainprep** needs to be run to prepare the domain, verification is done first to ensure that the user who initiated the process has sufficient rights to perform the operation.
- The Windows Server 2012 forest functional level does not add any new features to a forest and ensures only that any new domain added to the forest will automatically operate at the Windows Server 2012 domain functional level.
- The Windows Server 2012 domain functional level adds only one new feature to a domain. This new feature relates to Dynamic Access Control (DAC) and therefore is unlikely to affect any existing applications and services in your environment.

Despite these improvements to performing schema upgrades and raising forest and domain functional levels, careful planning and due care should be performed when completing these tasks. These issues will be addressed further in Chapter 4, "Deploying domain controllers," and in Chapter 5, "Active Directory administration."

IMPORTANT **FOREST UPGRADES AND FUNCTIONAL LEVELS**

After upgrading your schema, you might want to raise your forest and domain functional levels. As a best practice, follow these practices:

- **Before changing your forest functional level, take at least one domain controller offline from each domain in your forest.**
- **Before changing the domain functional level of any domain, take at least one domain controller offline from the domain.**

In both cases, you should make sure that the domain controllers you take offline do not hold any flexible single master operations (FSMO) roles in the forest or domains.

Keep the domain controllers offline for 48 to 72 hours after changing functional levels; if no issues are found, you can return the offline domain controllers to service. If issues are discovered, however, you can use your offline domain controllers as the source for rebuilding servers if a rollback to a previous functional level is required.

Mixed environment

As you saw in the previous migration scenario, existing businesses that want to take advantage of the new capabilities of Windows Server 2012 can do so without ripping out their infrastructure and replacing it with a new one. All they need to do is introduce servers running Windows Server 2012 into their environment and promote them as domain controllers. Doing this automatically upgrades the schema, and administrators can raise the forest and domain functional levels to Windows Server 2012 with minimal fear of it having a negative impact on their existing applications and services. Of course, regardless of this, you should still be sure to first test your schema upgrade and functional level changes in a test

environment that mirrors your production environment just to make sure there will be no issues that might impact your business.

But some new features of Windows Server 2012 can also be implemented into existing Active Directory environments without making significant changes to the existing forest, such as upgrading the schema or raising the forest or domain functional levels. An example where this might be done is when deploying new DHCP servers to take advantage of the new DHCP failover feature of Windows Server 2012 that ensures continuous availability of DHCP services to clients. For information on how to implement this new capability, see Chapter 6, "Network administration."

The introduction of member servers running Windows Server 2012 into an Active Directory forest based on an earlier version of Windows Server results in a mixed environment of servers running different versions of Windows. By not introducing new domain controllers in Windows Server 2012, administrators can continue to manage their environment using existing tools and processes. Although this seems like a simpler and less risky approach than upgrading your forest as described previously, there are several disadvantages to following this migration approach:

- Some new features and capabilities of Windows Server 2012 can be implemented only when your Active Directory environment includes domain controllers running Windows Server 2012. These features might not work at all, or have only limited functionality, when your Active Directory schema hasn't been upgraded to Windows Server 2012. In general, information about such limitations might be buried in the TechNet Library documentation for Windows Server 2012, which means you need to do some research before you try deploying Windows Server 2012 member servers with roles and features installed in your existing Active Directory environment.
- Some of the server administration tools built into Windows Server 2012 and included in the Remote Server Administration Tools (RSAT) for Windows 8 have limited or no functionality when managing servers running previous versions of Windows Server. Or you might have to install additional updates on servers running previous versions of Windows Server in order to manage them using the Windows Server 2012 server administration tools or RSAT for Windows 8. For more information, see KB 2693643 at *http://support.microsoft.com/kb/2693643*.

So while rolling out a few Windows Server 2012 member servers with a few roles and features installed might seem like a good idea, and less risky than performing a forest upgrade, the gains you experience from following this approach might not balance against the effort involved.

Server consolidation

Server consolidation involves using virtualization to consolidate multiple server workloads onto a single virtualization host. Although server consolidation can help an organization improve server utilization and reduce costs, it isn't generally considered a migration scenario.

With the greatly increased scalability of the Hyper-V role in Windows Server 2012, however, some businesses might be able to migrate much or even all of their existing Active Directory infrastructure based on a previous version of Windows Server and run it on a cluster of Hyper-V hosts running Windows Server 2012. In other words, they can migrate their existing physical servers into a virtual environment. For more information, see Chapter 7, "Hyper-V virtualization."

Private cloud

Cloud computing provides organizations with new options to increase efficiencies while reducing costs. The traditional data-center approach, where the organization deploys and manages its own Active Directory infrastructure on-premises, has known stability and security, but the infrastructure servers involved often run at less than 15 percent utilization. Virtualizing the data center by using server consolidation can increase utilization, reduce cost, and simplify management, but this approach lacks the elasticity to rapidly meet changing demands as your business grows or experiences market changes.

Cloud computing can simplify management and reduce cost even further while providing elasticity and the perception of infinite capacity for the IT services your business uses. Cloud resources are pooled so that they can be allocated on demand as the needs of the business grows or shrinks. If additional resources are needed, they can be provisioned without the need for extensive planning and testing beforehand.

Cloud computing can be provisioned according to three possible service models:

- **Software as a Service (SaaS)** The cloud is used to deliver an application to multiple users, regardless of their location or the type of device they are using. Compare this model with the more traditional approach of deploying separate instances of applications to each user's PC. This approach is typically used to deliver cloud-based applications that have minimal need for customization. Examples include email, Customer Relationship Management (CRM), and productivity software. The advantages of this approach are that application activities can be managed from a single central location to reduce cost and management overhead. An example of a SaaS offering from Microsoft is Office 365, which provides users with secure access from anywhere to their email, shared calendars, instant messaging (IM), video conferencing, and tools for document collaboration.
- **Platform as a Service (PaaS)** The cloud is used to deliver application execution services, such as application run time, storage, and integration for applications designed for a prespecified, cloud-based architectural framework. This allows you to develop custom cloud-based applications for your business, which you can then host in the cloud so that your users can access them from anywhere over the Internet. PaaS also lets you create multitenant applications that multiple users can access simultaneously. With support for application-level customization, PaaS allows integration with your older applications and interoperability with your current on-premises systems, although some applications might need to be recoded to work in the new

environment. An example of a PaaS offering from Microsoft is SQL Azure, which allows businesses to provision and deploy SQL databases to the cloud without having to implement and maintain an in-house Microsoft SQL Server infrastructure.

- **Infrastructure as a Service (IaaS)** The cloud is used to create pools of computer, storage, and network connectivity resources, which can then be delivered as cloud-based services billed on a per-usage basis. IaaS forms the foundation for the other two cloud service models by providing a standardized, flexible, virtualized environment that presents itself as virtualized server workloads. In this approach, the organization can self-provision these virtualized workloads and customize them fully with the processing, storage, and network resources needed and with the operating system and applications needed. The organization is relieved of the need to purchase and install hardware and can simply spin up new workloads to meet changing demand quickly.

In the context of Windows Server 2012 migration scenarios, the cloud service model under consideration here is the IaaS model, which can be implemented by using the Hyper-V role of Windows Server 2012 together with Microsoft System Center 2012 SP1. When IaaS is implemented in such a way that the customer controls the cloud, the solution is called a *private cloud*. There are several ways a private-cloud solution can be implemented by an organization:

- By having the customer build and host the private cloud in its own datacenter using Windows Server and the System Center family of products
- By having the customer purchase a dedicated private cloud appliance with Windows Server and System Center preinstalled and configured
- By having a partner company host the customer's private cloud

Migrating an organization's existing Active Directory infrastructure into a private-cloud sourcing model can be straightforward or complex, depending on a number of different factors. Because of this, it's useful to enlist a Microsoft partner to help you design and implement a solution that meets the needs of your organization. If you want to explore the private-cloud option further, there are several places you can start:

- You can download private-cloud evaluation software from Microsoft and deploy it in a test environment. At the time of this writing, this offering uses Windows Server 2008 R2 SP1 and System Center 2012, but by the time you read this, Microsoft might have upgraded the offering to Windows Server 2012 and System Center 2012 SP1. For more information, see *http://www.microsoft.com/en-us/server-cloud/private-cloud/trial.aspx*.
- You can purchase an IaaS private cloud with a prevalidated configuration from server partners in the Microsoft Private Cloud Fast Track program. These offerings combine Microsoft software, consolidated guidance, validated configurations from original equipment manufacturer (OEM) partners, and other value-added software components. For more information, see *http://www.microsoft.com/en-us/server-cloud/private-cloud/buy.aspx#tabs-2*.

- You can use the Microsoft Pinpoint site to find a partner in the Microsoft Private Cloud Service Provider Program who can host a dedicated private cloud for your organization. For more information, see *http://www.microsoft.com/en-us/server-cloud/private-cloud/buy.aspx#tabs-3*.

MORE INFO **MICROSOFT PRIVATE CLOUD**

For more information on Microsoft private-cloud solutions, see *http://www.microsoft.com/en-us/server-cloud/private-cloud/default.aspx*.

Public cloud

The private cloud is one of several cloud-sourcing models that organizations can consider. Another approach is using a public cloud, which is where a hosting provider maintains a shared cloud that provides a pool of services that can be used by multiple customers. It's important in such a model that each customer's environment be fully isolated from that of other customers to ensure security, and Windows Server 2012 includes new virtualization technology that enables secure multitenancy for hosting scenarios like this.

Public-cloud hosting providers generally focus on delivering SaaS solutions that allow them to deliver applications to customers so that the customer can focus on solving business problems instead of managing infrastructure. Because of this, any further consideration of the public-cloud sourcing model is beyond the scope of this book.

Quick check

- **Is Microsoft's cloud-based Office 365 offering an example of Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS)?**

Quick check answer

- **Office 365 is a SaaS offering in which the cloud is used to deliver an application to multiple users, regardless of their location or the type of device they are using.**

Migration process

As I said earlier, there is no single approach to how infrastructure migration projects should be planned and executed. However, there are some best practices that apply in various degrees to the different scenarios discussed earlier, and from these one can identify some of the key steps that should be involved in any migration process. I'll briefly focus on providing some guidance for the following four steps, which are common to most infrastructure migration projects:

- Pilot testing
- Assessment

- Server migration
- Role migration

Note that to help you use the information in the upcoming sections, some of it is presented in the form of a series of questions that can be used as the basis for creating worksheets for implementing your migration project.

Pilot testing

Pilot testing involves more than just installing the software and playing around with it. Instead, you should start by creating a test plan that defines the scope and objectives of the testing you want to perform. You should also define a testing methodology that describes the architecture of your test environment, your testing tools and techniques, and the type of automation you plan on using for your testing. You then need to identify the resource you need to perform your testing on, and establish a schedule for performing your various tests. Finally, you should have a process for evaluating the results of your testing to see whether the objectives you set have been achieved or not.

The following are some key questions that need to be addressed during pilot testing of Windows Server 2012:

- Why are we pilot testing Windows Server 2012?
- Who will be performing the testing?
- What training will the testers need before they can perform their testing?
- What are the specific objectives of our test process?
- What scenarios will we be using as the basis for performing our testing?
- What roles and features do we plan on testing?
- How will we test each of these roles and features?
- What hardware will we require to perform our tests?
- What additional software will we require to perform our tests?
- Will we be using any scripts or automation as part of the test process?
- Where will we set up our test environment?
- How will we ensure that our test environment will not affect our production environment?
- What is the schedule for performing our testing?
- How will we record our results for later analysis and evaluation?

Assessment

Assessment involves determining the readiness of your organization's infrastructure, hardware, applications, and personnel for migration to Windows Server 2012. Although some of this will be examined in more detail in the next lesson, here are some of the key questions that need to be addressed as part of the assessment process:

- Have you inventoried all the various hardware in your environment?
- Do you have any tools for performing an inventory of your infrastructure?
- Is your existing server hardware capable of running Windows Server 2012?
- Is your existing server hardware capable of supporting the various roles and features of Windows Server 2012 you plan to deploy in your environment?
- Will your existing storage hardware work with Windows Server 2012?
- Is your network infrastructure ready for Windows Server 2012?
- Are your various network appliances (for example, firewalls, VPN gateways, and so on) capable of interoperating with Windows Server 2012?
- If you plan on deploying DirectAccess, do your network infrastructure and appliances fully support Internet Protocol version 6 (IPv6)? And does your Internet Service Provider (ISP) support IPv6?
- Have you inventoried all the various operating systems and applications in your environment?
- Are there any operating systems or applications present in your environment that have compatibility issues with Windows Server 2012?
- Will you be virtualizing any of your existing operating systems or applications on Hyper-V hosts running Windows Server 2012?
- Have you inventoried the server roles on each of the servers of your infrastructure?
- Are there any considerations with regard to virtualizing any of the server roles currently running on your servers or migrating these roles into the cloud?
- Have you assessed your budget to ensure you have sufficient funding to purchase any hardware or software needed for your migration?
- Have you assessed the potential cost savings and return on investment (ROI) your organization can achieve by migrating to Windows Server 2012?
- Are your IT staff members ready for the migration? Do they need any additional training?

Server migration

A server migration can take several different paths, depending on the migration scenario you decide to implement. The choices you make concerning the migration process can be dictated by various factors, including cost, timeframe, the topology of your organization, the complexity of your infrastructure, and the server roles you currently have deployed in your

environment. Some of the key questions to address concerning the server-migration process include the following:

- Do you have a rollback plan in place in case something goes wrong with the migration?
- Have you performed a full system backup of the servers you'll be migrating?
- Which of the following method or methods will you be using for migrating your servers?
  - In-place upgrade, which keeps the current hardware and upgrades the current server operating system to Windows Server 2012. If you follow this approach, make sure you are aware of the supported upgrade paths for your existing server operating systems.
  - Refresh, which keeps the current hardware, saves the state information (operating system and application settings) of the current installation, wipes the hardware to remove the current operating system, performs a clean install of Windows Server 2012, and restores the state.
  - Replace, which saves the state of the current installation to a network location, retires the current hardware, performs a clean install of Windows Server 2012 on new hardware, and restores the state.
  - New computer, which involves either deploying Windows Server 2012 yourself on bare-metal hardware or purchasing preconfigured server systems from your vendor and further configuring the server as desired.
- Have you acquired and learned how to use tools such as Microsoft Deployment Toolkit (MDT) and System Center Configuration Manager (SCCM), which can be used to perform server migrations? Use of these tools is discussed in Chapter 2.
- Will you be migrating any physical servers into virtual environments? If so, you might need System Center Virtual Machine Manager (VMM) or other tools for performing the physical-to-virtual (P2V) migrations of your server workloads.
- Will you be migrating any servers running operating systems that are out-of-lifecycle, such as Windows 2000 Server, that might require special procedures such as migrating to an intermediate operating system before migrating to Windows Server 2012? For more information, see Chapter 7.
- Will you be migrating any servers across architectures? For example, migrating a server running Windows Server 2003 x86 to Windows Server 2012?
- Have you developed plans for migrating the roles on each of your servers? Role migration should be planned concurrently with server migration. See the next section for more information on this topic.
- Have you developed plans for migrating any business data stored on any of your servers? Will you be migrating your storage hardware as well as your servers? Is your business data safely backed up to prevent data loss from occurring during the migration process?

- Have you developed specific plans for migrating server applications, such as Microsoft Exchange, Microsoft SQL Server, and Microsoft SharePoint? The migration of server applications such as these requires special planning and consideration. Search the TechNet Library if you require more information on planning the migration of Microsoft server applications.
- Have you discussed your migration plans with the vendors of any third-party server applications you have deployed in your environment? Will the new operating system require a new version of these applications?
- Have you developed plans to ensure business applications and services remain available to users during the migration process?
- Have you prepared the expectations of your user population concerning any possible service interruptions or problems that might arise during the migration?
- Have you laid out a schedule for when you'll be performing your migrations and in what order you'll be migrating your servers?
- Have you assigned responsibilities to different members of your migration team?
- Have you thoroughly tested your server-migration plans in a test environment that mirrors your current production network?

Role and feature migration

A key aspect of server migration is the migration of server roles, features, operating system settings, and data. To migrate roles and features from previous versions of Windows Server to Windows Server 2012, you can use the Windows Server Migration Tools. These tools include best-practices documentation and are designed to ensure the role and feature migration process goes smoothly and without errors.

Windows Server Migration Tools can be installed on the following operating systems:

- Windows Server 2003 with Service Pack 2
- Windows Server 2003 R2
- Windows Server 2008, full installation option
- Full installation option of Windows Server 2008 R2
- Server Core installation option of Windows Server 2008 R2
- Server with a GUI installation option of Windows Server 2012
- Server Core installation option of Windows Server 2012

The source server is the server you are migrating the role or feature from, while the destination server is the server you will be migrating the role or feature to. For example, the source server might be running a Full installation option of Windows Server 2008 R2 and the destination server might be running a Server Core installation option of Windows Server 2012. The Migration Tools must be installed on both the source and destination servers, and you must be a member of the Administrators group on both servers.

The following migration paths are supported:

- Migrating between x86 and x64 architectures
- Migrating between physical machines and virtual machines
- Cross-subnet migrations

The following migration paths are not supported:

- Migrating between source and destination servers that have different system UI languages.
- Roles on the Server Core installation option of Windows Server 2008 cannot be migrated because the Microsoft .NET Framework is not available on this installation option.

The sections that follow demonstrate how role and feature migration can be performed.

Installing the Migration Tools on the destination server

The following procedure shows how to install and configure the Migration Tools on a destination server running Windows Server 2012. The goal is to be able to migrate a role such as the DHCP Server role or the Windows Server Update Services (WSUS) role from an existing server running Windows Server 2008 R2 to the new server running Windows Server 2012.

1. Open a Windows PowerShell session with elevated rights on a server running Windows Server 2012 in your environment.
2. Execute the following command to install the Windows Server Migration Tools feature on the remote server running Windows Server 2012 and named SERVER7:

   ```
   Install-WindowsFeature Migration –ComputerName SERVER7
   ```

   If the local server running Windows Server 2012 you are logged on to is a Server Core installation, type **powershell.exe** before executing the PowerShell command just shown.

   If the local server running Windows Server 2012 you are logged on to is a Full installation, you can also install the Migration Tools on the remote server by launching the Add Roles And Features Wizard from Server Manager.
3. Open an elevated command prompt by typing **cmd** in your elevated Windows PowerShell session, and change the current directory as follows:

   ```
   Cd %systemroot%\system32\ServerMigrationTools
   ```

4. Create a deployment folder on the destination by running the SmigDeploy.exe utility. This utility creates an installation package for performing the migration and places it in a new folder named C:\downloads\<*subfolder*> where <*subfolder*> depends on the operating system version and architecture of the source server. For example, if the source computer has AMD64 architecture and is running Windows Server 2008 R2, run SmigDeploy.exe using these parameters:

   ```
   SmigDeploy.exe /package /architecture amd64 /os WS08R2 /path C:\downloads
   ```

This creates a new deployment folder named C:\downloads\SMT_ws08R2_amd64 on the destination server and copies the Migration Tool files to the folder.

5. Copy the deployment folder to the local drive of the source computer running Windows Server 2008 R2 using any appropriate method.

For more information on installing and using the Windows Server Migration Tools on Windows Server 2012, see *http://technet.microsoft.com/en-us/library/jj134202*.

Installing the Migration Tools on the source server

The following procedure shows how to install and run the Migration Tools on a source server running Windows Server 2008 R2 to which you have already copied the deployment folder from the destination computer. Note that additional steps might be required for migrating certain roles, such as the Hyper-V role, the Routing And Remote Access Services role, and others.

1. Open a Windows PowerShell session with elevated rights, and execute the following command to load the Server Manager module:

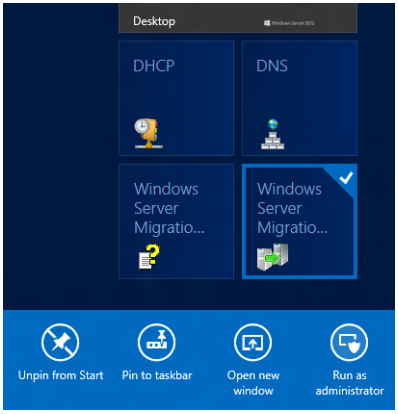
```
Import-Module ServerManager
```

2. Install the Windows Server Migration Tools feature by running this command:

```
Add-WindowsFeature Migration
```

3. Note that if your source server is running an earlier operating system such as Windows Server 2008 or Windows Server 2003, you also need to install the Microsoft .NET Framework and Windows PowerShell on the source computer and then run SmigDeploy.exe on it to register the Windows Server Migration Tools cmdlets into Windows PowerShell.

You can now launch the Migration Tools from either the destination or source server. For example, to launch them from a destination server running Windows Server 2012, right-click on the Windows Server Migration Tools tile on the Start screen and click Run As Administrator on the app bar, as shown here:



This opens a custom Windows PowerShell session from which you can run the various Windows Server Migration Tool cmdlets as shown in Figure 1-1.

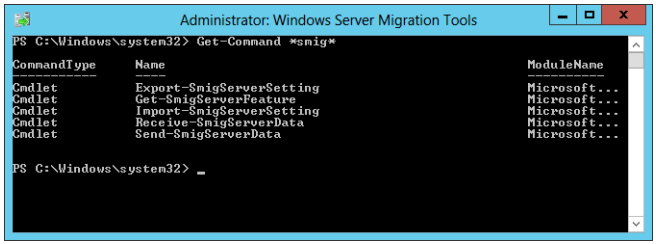


FIGURE 1-1 Displaying the list of available Windows Server Migration Tool cmdlets.

For help with the syntax of these cmdlets, use the Get-Help cmdlet. For more information on installing the Windows Server Migration Tools on Windows Server 2008 R2 and earlier, see *http://technet.microsoft.com/en-us/library/dd379545(v=WS.10).aspx*.

NOTE **GET YOUR MIGRATION QUESTIONS ANSWERED**

A good place to get help with your server migration questions is the Migration forum in the Windows Server forums on TechNet at *http://social.technet.microsoft.com/forums/en-US/winserverMigration/threads*. Be sure to start by reading the sticky post at the top of the forum titled "How to ask a question efficiently in TechNet forum" because complying with the guidelines in this post increases the chances that you'll get an answer that will help you.

Lesson summary

- Each type of infrastructure migration scenario (greenfield, forest upgrade, mixed environment, server consolidation, private cloud, public cloud) has its benefits and challenges for organizations wanting to take advantage of the new features and capabilities found in Windows Server 2012.
- Forest upgrades to Windows Server 2012 are now simpler than with previous Windows Server versions because of the integration of Adprep.exe into the AD DS role installation process.
- Four key steps for any infrastructure migration project are pilot testing, assessment, server migration, and role and feature migration.
- The Windows Server Migration Tools ease the process of migrating roles and features from previous Windows Server versions to Windows Server 2012.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following are disadvantages of the mixed-environment migration scenario? (Choose all that apply.)
   - **A.** It gives you an opportunity to get it right from the start when it comes to implementing an infrastructure based on Windows Server 2012.
   - **B.** Some new features and capabilities of Windows Server 2012 might not work at all, or have only limited functionality, when this migration scenario is implemented.
   - **C.** Server management might become more complex due to having to use separate tools for managing servers running Windows Server 2012 and those running earlier Windows Server operating system versions.
   - **D.** It can help your organization improve server utilization and reduce costs.
2. Which of the following is *not* an enhancement that Microsoft has made in Windows Server 2012 to alleviate some of the concerns administrators often have about performing forest upgrades? (Choose all that apply.)
   - **A.** Adprep functionality is now integrated into the AD DS installation process.
   - **B.** The new AD DS installation process includes prerequisite validation to identify potential errors before installation begins.
   - **C.** The Windows Server 2012 forest functional level adds several new features to a forest.
   - **D.** The Windows Server 2012 domain functional level adds only one new feature to a domain.
3. Which of the following migration paths is not supported by the Windows Server Migration Tools?
   - **A.** Migrating between x86 and x64 architectures
   - **B.** Migrating between source and destination servers that have different system UI languages
   - **C.** Migrating between physical machines and virtual machines
   - **D.** Cross-subnet migrations
4. Which Windows PowerShell cmdlet for the Windows Server Migration Tools can be used to get the set of all Windows features that can be migrated from the local server or from a migration store?
   - **A.** Export-SmigServerSetting
   - **B.** Send-SmigServerData
   - **C.** Get-SmigServerFeature
   - **D.** Import-SmigServerSetting

Lesson 2: Assessing the readiness of your environment

The assessment phase is an important step of any server migration project. During this phase, you will assess the readiness of your environment for the deployment of Windows Server 2012. A key aspect of this phase is determining whether your current server hardware, and hardware you plan to purchase, will support running Windows Server 2012 and the various server roles and features you need to deploy in your environment. As this lesson demonstrates, performing such an assessment can be done in various ways using different types of tools.

After this lesson, you will be able to

- Describe the Windows Server 2012 editions and system requirements.
- Explain how to perform a manual assessment of a server infrastructure, and describe some of the tools you would use to do this.
- Describe the capabilities of the Microsoft Assessment and Planning (MAP) Toolkit 7.0 for performing inventory, assessment, and reporting.
- Describe the six phases involved in using the MAP Toolkit to perform an assessment of your environment.
- Describe some of the wizards that the MAP Toolkit uses to collect data about your environment.
- Describe the sample reports that MAP generates.
- Describe some other tools and methodologies you can use to assess the readiness of your environment for migration to Windows Server 2012.

Estimated lesson time: 30 minutes

Manual assessment

If your current server infrastructure is very small (only a handful of servers), you can perform a manual assessment by using the documentation that came with your server hardware, viewing and recording server BIOS information, exporting system configuration information using msinfo32.exe, inventorying roles and features using the Get-WindowsFeature cmdlet of Windows PowerShell, and performing similar types of procedures. Once you have compiled such information about your servers, you can validate them against the hardware requirements for the different Windows Server 2012 editions.

Windows Server 2012 editions

Microsoft has simplified the licensing model with Windows Server 2012 by eliminating the Enterprise edition of previous versions of Windows Server. In addition, the Standard and Datacenter editions that are designed for midsized and large organizations now have feature parity, and they are both licensed by processor plus client access license (CAL). The only difference between the Standard and Datacenter editions are the virtualization rights included with the license:

- Standard edition provides full Windows Server functionality with two virtual instances.
- Datacenter edition provides full Windows Server functionality with unlimited virtual instances.

In addition to the Standard and Datacenter editions, there are also two other editions of Windows Server 2012 available that are designed for more specialized use:

- Essentials edition, which is intended for small business environments and includes a simpler interface, preconfigured connectivity to cloud-based services, a 25-user account limit, and no virtualization rights
- Foundation edition, which is an economical, general-purpose server released through OEM channels only and has a 15-user account limit and no virtualization rights

REAL WORLD **WINDOWS SERVER LICENSING**

In the past, the licensing of Windows Server editions has been a complex and confusing subject that often made it difficult for organizations to determine how much they should budget for licensing costs and whether or not they are in compliance. With Windows Server 2012, Microsoft has simplified the licensing model for Windows Server so that you can more easily determine how many licenses you need to purchase to run the number of physical and virtual instances of Windows Server 2012 you need in your environment. For more information and examples of different licensing scenarios, see the Windows Server 2012 Licensing & Pricing FAQ at *http://download.microsoft.com/download/4/D/B/4DB352D1-C610-466A-9AAF-EEF4F4CFFF27/WS2012_Licensing-Pricing_FAQ.pdf*.

System requirements

The minimum system requirements for installing the Standard and Datacenter editions of Windows Server 2012 are as follows:

- A 1.4-GHz, 64-bit processor
- 512 MB of RAM

- 32 GB of available disk space
- A network adapter card
- A graphics adapter that supports 800 by 600 or higher resolution

Bear in mind that performance depends upon hardware, and your servers will need to exceed these minimum requirements to provide acceptable performance in most scenarios. For example, if you plan on installing MAP 7.0 on your server to perform an assessment of your environment, you will need system hardware that meets the following minimum requirements:

- A dual-core, 1.5-GHz processor
- 2.0 GB of RAM
- 1 GB of available disk space
- A network adapter card
- A graphics adapter that supports 1024 by 768 or higher resolution

In addition, the inventory, assessment, and reporting performance of MAP are based primarily on the speed of the CPU and the amount of available RAM of the computer on which MAP is installed.

MORE INFO **RECOMMENDED SYSTEM REQUIREMENTS**

For more information on the recommended system requirements for Windows Server 2012, see *http://technet.microsoft.com/en-us/library/jj134246.aspx*.

Windows Server Catalog

If you plan on purchasing new system hardware and deploying Windows Server 2012 on such hardware, you can assess the readiness of the new hardware before you purchase it by using the Windows Server Catalog website shown in Figure 1-2, which identifies system and peripheral hardware from different vendors that has been certified for Windows Server 2012. For more information, see *http://www.windowsservercatalog.com*.

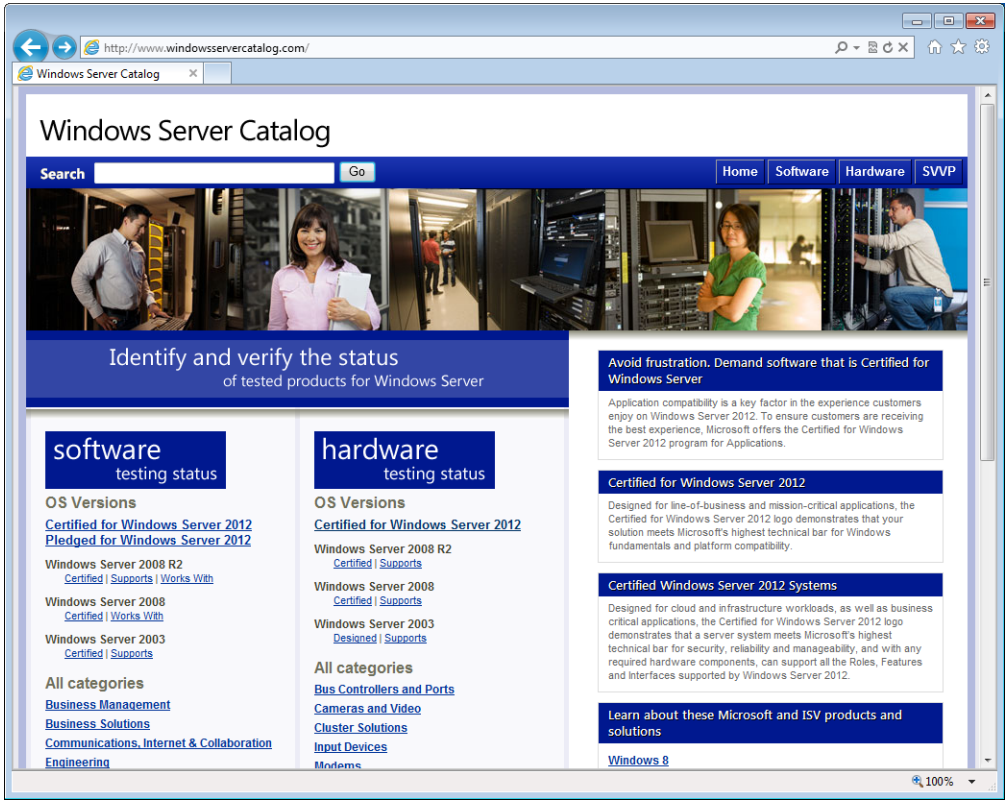


FIGURE 1-2 The Windows Server Catalog website.

Using the MAP Toolkit

Microsoft Assessment and Planning (MAP) Toolkit 7.0 is an inventory, assessment, and reporting tool you can use to assess your current IT infrastructure and determine the right Microsoft technologies for your business needs. The MAP toolkit uses Windows Management Instrumentation (WMI), Active Directory Domain Services (AD DS), SMS Provider, and other technologies to collect data from your environment and inventory hardware, software, and operating systems. MAP does this without installing any agent software on the target devices. MAP then provides you with an analysis of the collected data to help you plan for server migration, desktop refresh, server consolidation through virtualization, or cloud-capacity and migration planning.

The MAP Toolkit can simplify the planning process for migration to the following Microsoft platforms:

- Windows Server 2012
- Windows Server 2008 R2

- Hyper-V
- Hyper-V R2
- Microsoft Private Cloud Fast Track
- Windows 8
- Windows 7
- Microsoft Office 2010
- Microsoft Office 365
- Internet Explorer 9
- Windows Azure Platform
- Microsoft SQL Server 2012

Preparing to use the toolkit

As Figure 1-3 shows, there are six phases involved in using the MAP Toolkit to perform an assessment of your environment. The first four phases outline the steps you need to perform before you run the toolkit:

- **Phase 1: Choose Goals** Familiarize yourself with the different inventory, assessment, capacity-planning, and software-usage tracking scenarios supported by the MAP Toolkit. Decide which wizards to use and what selections to make in these wizards.
- **Phase 2: Gather Requirements** The MAP Toolkit uses various collection protocols to communicate with devices on your network to collect data to use in performing the various assessments. Because the communications performed by these protocols are subject to the administration and security settings of your environment, you must gather the user accounts and passwords needed to connect and successfully inventory the devices in your environment prior to running the toolkit.
- **Phase 3: Prepare Environment** The MAP Toolkit uses several different communication protocols based upon your goals and how the environment is configured. These include WMI, Active Directory Domain Services, SQL Server commands, VMware Web services, and SSH with remote shell commands. In Phase 3, you will prepare your environment to ensure that the toolkit can successfully connect and gather information from the target machines in your environment.
- **Phase 4: Install Toolkit** Download and install the toolkit using the options that best suit your environment and goals. The MAP Toolkit is available as a free download from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?&id=7826*.

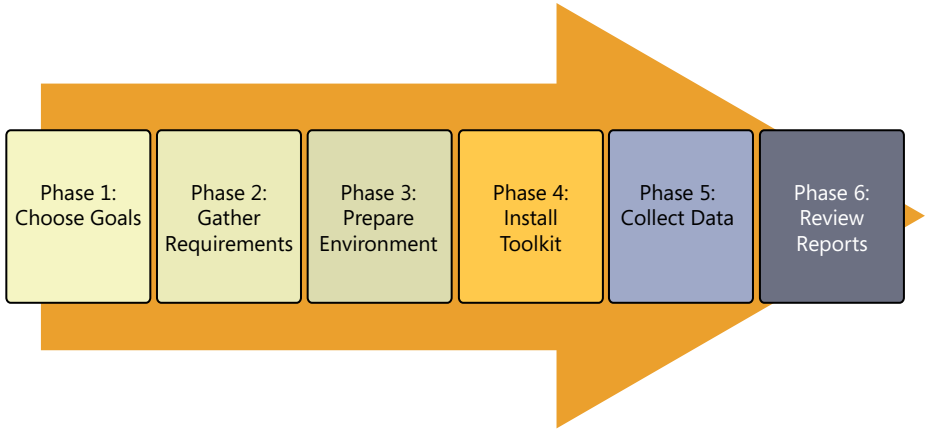


FIGURE 1-3 The six phases involved in performing an assessment using the MAP Toolkit.

Running the toolkit

The final two phases of the assessment process describe how to run the MAP Toolkit to address the goals you identified at the beginning of the process:

- **Phase 5: Collect Data** Launch the MAP Toolkit console, and click on the buttons for the first two options shown in Figure 1-4 under Steps To Complete to begin the data collection process for your environment. Selecting these options launches the following two wizards:
  - **Inventory And Assessment Wizard** Use this wizard first to select your inventory scenario, select your discovery method, and provide the credentials needed to connect and inventory the devices targeted.
  - **Performance Metrics Wizard** Use this wizard next to collect performance data such as CPU, memory, network, and disk-utilization information. The MAP Toolkit lets you collect such data for Windows servers and clients as well as for LINUX-based servers. The toolkit then uses the collected performance data for capacity planning for server consolidation, desktop virtualization, Microsoft Private Cloud Fast Track, Azure Application migration, and Microsoft Database Consolidation Appliance planning.
- **Phase 6: Review Reports** The MAP Toolkit can generate custom reports and proposals that are specific to the assessment the toolkit performed. For example, the Windows Server 2012 Hardware Assessment report package summarizes the hardware readiness of servers for a migration to Windows Server 2012 and indicates whether they are capable of running Windows Server 2012.

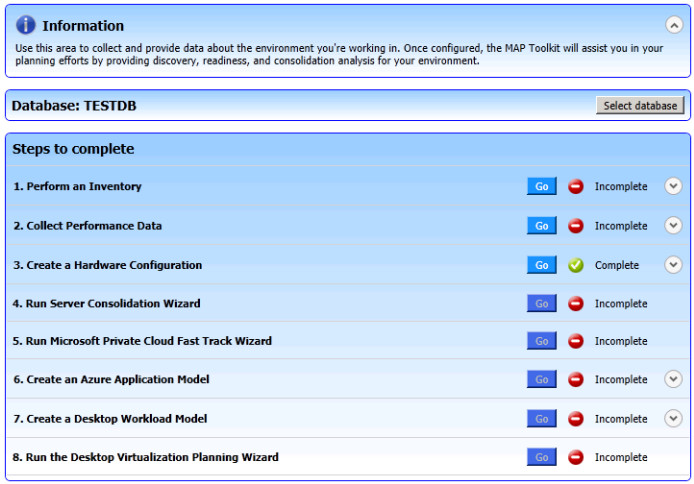
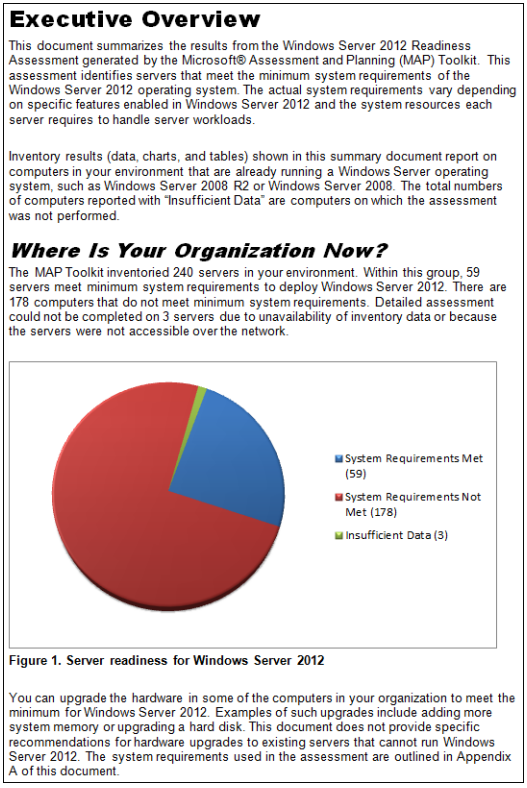


FIGURE 1-4 MAP Toolkit console options for launching wizards and performing other configuration tasks.

Sample reports

Figure 1-5 shows an excerpt from a sample Windows Server 2012 Readiness Assessment proposal generated by the MAP Toolkit. This proposal is in the form of a Microsoft Word document (.docx file) that contains the following:

- An Executive Overview section that summarizes where your organization is now and outlines some potential benefits of cloud-optimizing your IT infrastructure using Windows Server 2012.
- An Assessment Results section that summarizes your organization's Windows Server 2012 readiness and provides detailed analysis and recommendations about the servers, operating systems, and server roles inventoried.
- Appendices containing information about Windows Server 2012 system requirements and report worksheets.



Executive Overview

This document summarizes the results from the Windows Server 2012 Readiness Assessment generated by the Microsoft® Assessment and Planning (MAP) Toolkit. This assessment identifies servers that meet the minimum system requirements of the Windows Server 2012 operating system. The actual system requirements vary depending on specific features enabled in Windows Server 2012 and the system resources each server requires to handle server workloads.

Inventory results (data, charts, and tables) shown in this summary document report on computers in your environment that are already running a Windows Server operating system, such as Windows Server 2008 R2 or Windows Server 2008. The total numbers of computers reported with "Insufficient Data" are computers on which the assessment was not performed.

Where Is Your Organization Now?

The MAP Toolkit inventoried 240 servers in your environment. Within this group, 59 servers meet minimum system requirements to deploy Windows Server 2012. There are 178 computers that do not meet minimum system requirements. Detailed assessment could not be completed on 3 servers due to unavailability of inventory data or because the servers were not accessible over the network.

Figure 1. Server readiness for Windows Server 2012

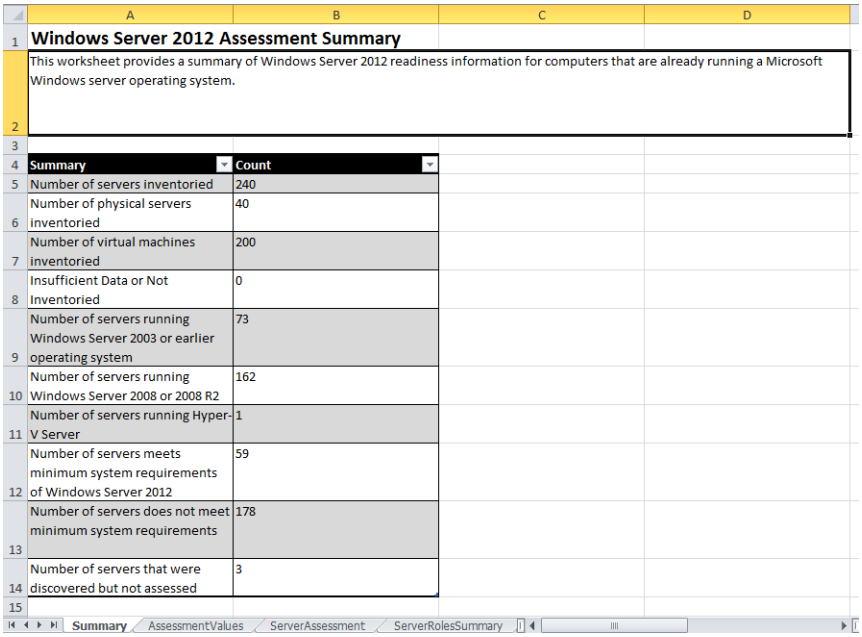
You can upgrade the hardware in some of the computers in your organization to meet the minimum for Windows Server 2012. Examples of such upgrades include adding more system memory or upgrading a hard disk. This document does not provide specific recommendations for hardware upgrades to existing servers that cannot run Windows Server 2012. The system requirements used in the assessment are outlined in Appendix A of this document.

FIGURE 1-5 A sample Windows Server 2012 Readiness Assessment proposal generated by the MAP Toolkit.

Figure 1-6 shows an excerpt from a sample Windows Server 2012 Assessment Summary generated by the MAP Toolkit. This proposal is in the form of a Microsoft Excel workbook (.xlsx file) that has four worksheets:

- **Summary** Displays the number of physical servers and virtual machines inventoried, servers running earlier versions of Windows Server, servers running Hyper-V, and servers meeting the minimum system requirements for installing Windows Server 2012
- **AssessmentValues** Displays the Windows Server 2012 system requirements used in performing the assessment along with any other requirements you specified for the assessment
- **ServerAssessment** Lists the information collected from each system inventoried, including the computer name, WMI status, machine type, IP address, subnet, current operating system, service pack level, current Windows Server 2012 readiness, and any further recommendations
- **ServerRolesSummary** Summarizes the server roles currently deployed in your environment; the operating system or systems, number of physical servers, and

number of virtual machines each role is running on; and any recommendations concerning the migration of these roles to Windows Server 2012



Windows Server 2012 Assessment Summary

This worksheet provides a summary of Windows Server 2012 readiness information for computers that are already running a Microsoft Windows server operating system.

Summary	Count
Number of servers inventoried	240
Number of physical servers inventoried	40
Number of virtual machines inventoried	200
Insufficient Data or Not Inventoried	0
Number of servers running Windows Server 2003 or earlier operating system	73
Number of servers running Windows Server 2008 or 2008 R2	162
Number of servers running Hyper-V Server	1
Number of servers meets minimum system requirements of Windows Server 2012	59
Number of servers does not meet minimum system requirements	178
Number of servers that were discovered but not assessed	3

FIGURE 1-6 A sample Windows Server 2012 Assessment Summary generated by the MAP Toolkit.

Quick check

- **Which wizard of the MAP Toolkit can be used to collect performance data for capacity planning for server consolidation, desktop virtualization, Microsoft Private Cloud Fast Track, Azure Application migration, and Microsoft Database Consolidation Appliance planning?**

Quick check answer

- **The Performance Metrics Wizard**

Other tools and methodologies

Besides using MAP, there are other tools and methodologies you can use to assess the readiness of your environment for migration to Windows Server 2012. The tools you could use include the following:

- **System Center Configuration Manager (SCCM)** System Center Configuration Manager provides a comprehensive solution for change and configuration management for the Microsoft platform. SCCM lets you deploy operating systems, software

applications, and software updates throughout your organization; monitor hardware and software inventory; monitor and remediate computers for compliance settings; and even remotely administer computers. With SCCM 2012 SP1, you can collect detailed information about the hardware of client devices in your organization, including servers managed by SCCM, and then use this information to determine Windows Server 2012 migration readiness. SCCM hardware inventory runs on devices managed by SCCM according to a schedule you specify in the client settings on the device. For more information on performing inventory using SCCM 2012, see *http://technet.microsoft.com/en-us/library/gg682202*.

- **Application Compatibility Toolkit (ACT)** This free life-cycle management tool from Microsoft helps you analyze your portfolio of applications, websites, and computers; allows you to deploy automated mitigations for known compatibility issues; and enables you to create custom shims for new compatibility issues you might identify. For more information on managing application compatibility on Windows platforms and to download the latest version of ACT, see *http://technet.microsoft.com/en-us/windows/application-compatibility.aspx*.
- **Third-party products** If you are using a third-party, systems-management product for managing the hardware and software infrastructure of your organization, you will likely be able to use the product to assess the readiness of your environment for migration to Windows Server 2012, provided that your systems-management product is up to date. There are also third-party dedicated inventory and assessment products available from different vendors that you might use if desired.
- **Engage outside help** If you feel you need help assessing the readiness of your environment for migration to Windows Server 2012, you can engage Microsoft Consulting Services (MCS) and/or Microsoft Services Premier Support to assist you with this process, and also with the migration itself if you feel this is needed. For more information, see *http://www.microsoft.com/microsoftservices/en/us/home.aspx*.

Lesson summary

- If your current server infrastructure is very small, you can perform a manual assessment of your Windows Server 2012 migration readiness.
- A manual assessment can be performed by using vendor-supplied documentation, built-in tools, information about Windows Server 2012 editions and system requirements on Microsoft's website, and the Windows Server Catalog.
- For larger environments, the MAP Toolkit helps you perform inventory, assessment, and reporting so that you can assess the readiness of your environment for migration to Windows Server 2012.
- Assessing your environment using the MAP Toolkit involves six phases: choosing goals, gathering requirements, preparing your environment, installing the toolkit, collecting data, and generating and reviewing reports.

- You can also use System Center Configuration Manager, the Application Compatibility Toolkit, third-party products, and even outside help to assess your Windows Server 2012 migration readiness.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which tool can help you ensure that new hardware you purchase will work properly with Windows Server 2012?
   - **A.** The msinfo32.exe utility
   - **B.** The Get-WindowsFeature cmdlet
   - **C.** The Application Compatibility Toolkit
   - **D.** The Windows Server Catalog
2. During which of the six phases of performing an assessment using the MAP Toolkit would you ensure that the toolkit can successfully connect and gather information from the target machines in your environment?
   - **A.** Phase 2: Gather Requirements
   - **B.** Phase 3: Prepare Environment
   - **C.** Phase 4: Install Toolkit
   - **D.** Phase 5: Collect Data
3. When you generate reports and proposals after performing a Windows Server 2012 readiness assessment using the MAP Toolkit, where can you find information about the IP address and current operating system installed on each system inventoried?
   - **A.** In the Assessment Results section of the Readiness Assessment proposal document
   - **B.** In the Summary worksheet of the Assessment Summary workbook
   - **C.** In the ServerAssessment worksheet of the Assessment Summary workbook
   - **D.** In the ServerRolesSummary worksheet of the Assessment Summary workbook

Practice exercises

The goal of this section is to provide you with hands-on practice with the following:

- Using the MAP Toolkit to perform a Windows Server 2012 readiness assessment of your test server
- Performing an in-place upgrade to Windows Server 2012, and familiarizing yourself with the new Start screen of Windows Server 2012

To perform the following exercises, you need a server system available for testing purposes that meets the minimum hardware requirements for installing Windows Server 2012. This server should also meet the following additional requirements:

- The system hardware should meet the minimum requirements for installing version 7.0 of the Microsoft Assessment and Planning (MAP) Toolkit. For more information about these requirements, see *http://www.microsoft.com/en-us/download/details.aspx?&id=7826*.
- The server should have Windows Server 2008 R2 SP1 or Windows Server 2008 SP2 installed. If needed, you can download an evaluation copy of Windows Server 2008 R2 SP1 from the TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/bb291020.aspx*.
- The server should be a standalone server belonging to a workgroup.
- The network where the server resides should have Internet connectivity, and the server should be configured with a static IP address, subnet mask, default gateway, and primary and secondary DNS servers that enable the server to access the Internet.
- It is recommended that the server be a physical server (not a virtual machine) for the purposes of performing the exercises in this chapter. If you decide, however, to run the server as a virtual machine using Hyper-V on Windows Server 2008 R2 SP1, be sure to install the update described at *http://support.microsoft.com/kb/2526776* so that you will be able to upgrade the virtual machine's guest operating system to Windows Server 2012 as required by one of the practice exercises in this chapter.

You also need a client computer that has Microsoft Office 2010 or Office 365 installed for viewing the reports generated by the MAP Toolkit in one of the practice exercises in this chapter.

Exercise 1: Using the MAP Toolkit

In this exercise, you will download and install MAP 7.0 on your test server. You will then inventory the hardware and software on your server and determine whether Windows Server 2012 can be installed on the server. For the purposes of this exercise, the name of the server is assumed to be SERVER9.

1. Install Windows Server 2008 R2 SP1 or Windows Server 2008 SP2 on your test system if you haven't done so yet. Configure the server with a static IP address, subnet mask, default gateway, and primary and secondary DNS servers so that the server has Internet access. Apply all pending software updates from Windows Update to your server so that the server is fully updated, and log on again using the local Administrator account for the server. Install one or more server roles on the server, such as the DHCP server role or Web Server (IIS) role.
2. Download MAP 7.0 to your server from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?id=7826*.

3. Open the readme.htm for MAP, and make sure your server meets all the requirements for installing MAP by adding any required features and installing any required software updates and service packs.
4. Double-click on the Microsoft_Assessment_and_Planning_Toolkit_Setup.exe file you downloaded in step 2 to launch the Setup Wizard.
5. Follow the prompts of the wizard by accepting all the defaults.
6. When Setup is finished, click Finish to close the wizard and open the Microsoft Assessment And Planning Toolkit console.
7. In the Microsoft Assessment And Planning Toolkit dialog box, type **TESTDB** in the Name field and click OK to create an inventory database for MAP.
8. After the inventory database is created, you are returned to the main Data Collection page of the Inventory And Assessment section of the MAP console.
9. In the Steps To Complete section in the middle pane of the console, click Go beside the Perform An Inventory option. This launches the Inventory And Assessment Wizard.
10. On the Inventory Scenarios page of this wizard, select Windows Computers and click Next.
11. On the Discovery Methods page, clear the Use Active Directory Domain Services (AD DS) check box, select the Scan An IP Address Range check box, and click Next.
12. On the Scan An IP Address Range page, in both the Starting Address and Ending Address fields, enter the IP address you previously assigned to your test server and then click Next.
13. On the All Computers credentials page, click Create, type **SERVER9\Administrator** in the Account Name field, type the password for the Administrator account in the Password and Confirm Password fields, and then click Save.
14. Click Next twice and then click Finish.
15. Watch the progress of the assessment in the Status dialog as it occurs, and then click Close when the assessment has completed.
16. Expand the Server node in the navigation pane, and select the Windows Server 2012 Readiness node to view whether the system requirements for installing Windows Server 2012 have been met by your server.
17. Click the Generate Report/Proposal option in the Actions pane on the right side of the console. When the proposal and workbook have been generated, click Close.
18. Open My Documents in Windows Explorer, and navigate to the TESTDB folder inside the MAP folder.
19. Copy the proposal (.docx file) and assessment (.xlsx file) reports that MAP generated to a client computer that has Microsoft Office 2010 or Office 365 installed.
20. Open the proposal and assessment reports using Word 2010 and Excel 2010 (or Word Web App and Excel Web App), and view the contents of these reports.

Exercise 2: Performing an in-place upgrade

In this exercise, you will perform an in-place upgrade of your test server from your current operating system (Windows Server 2008 R2 SP1 or Windows Server 2008 SP2) to Windows Server 2012. You will then use your Windows Server 2012 installation to familiarize yourself with the new Start screen of Windows Server 2012.

1. Start the server, and log on using the built-in Administrator account.
2. Insert your Windows Server 2012 product media into the DVD drive of your server, and run Setup.exe when prompted.
3. When the Windows Setup wizard appears, click Install Now.
4. On the Get Important Updates For Windows Setup page, click Go Online To Install Updates Now (Recommended). Follow the instructions if any updates for Setup are available for download.
5. On the Select The Operating System You Want To Install page, select the Windows Server 2012 (Server With A GUI) option.
6. On the Licensing Terms page, agree to the licensing terms after reading them.
7. On the Which Type Of Installation Do You Want? page, select the Upgrade: Install Windows And Keep Files, Settings And Applications option.
8. On the Compatibility Report page, read the information provided.
9. The Upgrading Windows page displays the progress of your in-place upgrade. The system will restart several times to complete the installation process.
10. When the installation is completed and the Windows Server 2012 logon screen is displayed, press Ctrl+Alt+Del and log on using the built-in Administrator account.
11. When the new Server Manager opens, click Local Server in the Navigation pane and view the properties of your server. You'll learn more about Server Manager in Chapter 3, "Server remote management."
12. Move the pointer to the bottom left corner of your screen and click Start.
13. Click on the tile named Desktop.
14. Click the Server Manager icon on the taskbar to maximize Server Manager.
15. Move the pointer to the top right corner of the screen until the Search, Start, and Settings charms are displayed, and then swipe the pointer downward to display the Charms Bar.
16. Press Esc to make the Charms Bar disappear.
17. Press the Windows key+C to make the Charms Bar appear again.

18. Click the Settings charm to open Settings, and then click Server Info. The System Control Panel opens while the Charms Bar disappears. View the information about your computer and then close it.
19. Press the Windows key+I to open Settings again, and then click Help. Take a moment to explore how Help works, and then close it.
20. Press the Windows key+Q to open the Search pane with the focus on Apps. Type **paint**, and press Enter to open Microsoft Paint. Close the program.
21. Move the pointer to the bottom left corner of your screen, click Start, type **paint**, and press Enter to open Microsoft Paint. Close the program.
22. Press the Windows key+Q, type **background**, press the Down Arrow key twice, and then press Enter to search for settings relating to the word "background." Change Desktop Background should be selected in your search results, so press Enter and change the background of your desktop to the solid color white.
23. Click the Windows PowerShell icon on the taskbar to open a new Windows PowerShell session.
24. Type **shutdown –s –t 0**, and press Enter to shut down your server.

Suggested practice exercises

The following additional practice exercises are designed to give you more opportunities to practice what you've learned and to help you successfully master the lessons presented in this chapter:

- **Practice 1** If you have a test environment with Active Directory deployed and with servers and clients running different versions of Windows, install the MAP Toolkit on a server or client in the environment and perform some of the other types of assessment and readiness tests supported by the toolkit.
- **Practice 2** Use the Windows Server Migration Tools to migrate several server roles from a server running Windows Server 2008 R2 SP1 to another server that has a clean installation of Windows Server 2012.
- **Practice 3** Read the "Windows 8 Survival Guide for IT Pros" in the TechNet Wiki at *http://social.technet.microsoft.com/wiki/contents/articles/7878.windows-8-survival-guide-for-it-pros.aspx*, and try out each of the options described on your Windows Server 2012 installation.

Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct answers: B and C**
   - **A.** **Incorrect**: The opportunity to get it right from the start when it comes to implementing an infrastructure based on Windows Server 2012 is an advantage of the greenfield migration scenario, not the mixed environment scenario.
   - **B.** **Correct**: Some new features and capabilities of Windows Server 2012 can be implemented only when your Active Directory environment includes domain controllers running Windows Server 2012. These features might not work at all, or have only limited functionality, when implementing a mixed-environment migration scenario because your Active Directory schema hasn't yet been upgraded to Windows Server 2012.
   - **C.** **Correct**: Some of the server administration tools built into Windows Server 2012 and included in the Remote Server Administration Tools (RSAT) for Windows 8 will have limited or no functionality when managing servers running previous versions of Windows Server. Or you might have to install additional updates on servers running previous versions of Windows Server to manage them using the Windows Server 2012 server administration tools or RSAT for Windows 8.
   - **D.** **Incorrect**: Improving server utilization and reducing costs is a benefit of the server-consolidation approach to server migration and is not relevant to a mixed-environment migration scenario.
2. **Correct answer: C**
   - **A.** **Incorrect**: In Windows Server 2012, Adprep functionality is now integrated into the AD DS installation process, which in most cases eliminates the need to separately run Adprep prior to introducing domain controllers running the new version of Windows Server.
   - **B.** **Incorrect**: The new AD DS installation process includes prerequisite validation to identify potential errors before installation begins. For example, if the installation process determines that **adprep /domainprep** needs to be run to prepare the domain, verification is done first to ensure that the user who initiated the process has sufficient rights to perform the operation.
   - **C.** **Correct**: The Windows Server 2012 forest functional level does not add any new features to a forest and ensures only that any new domain added to the forest will automatically operate at the Windows Server 2012 domain functional level.

D. **Incorrect**: The Windows Server 2012 domain functional level adds only one new feature to a domain. This new feature relates to Dynamic Access Control (DAC) and therefore is unlikely to affect any existing applications and services in your environment.

3. **Correct answer: B**

A. **Incorrect**: The Windows Server Migration Tools supports migrating between x86 and x64 architectures.

B. **Correct**: The Windows Server Migration Tools does not support migrating between source and destination servers that have different system UI languages.

C. **Incorrect**: The Windows Server Migration Tools supports migrating between physical machines and virtual machines.

D. **Incorrect**: The Windows Server Migration Tools supports cross-subnet migrations.

4. **Correct answer: C**

A. **Incorrect**: The Export-SmigServerSetting cmdlet exports selected Windows features and operating system settings from the local computer, and it stores them in a migration store.

B. **Incorrect**: The Send-SmigServerData cmdlet migrates folders, files, and associated permissions and share properties from a source server to a destination server through port 7000. The destination server must be in the same subnet as the source server, and the cmdlet Receive-SmigServerData must be run on the destination server at the same time Send-SmigServerData is running on the source server.

C. **Correct**: The Get-SmigServerFeature cmdlet gets the set of all Windows features that can be migrated from the local server or from a migration store.

D. **Incorrect**: The Import-SmigServerSetting cmdlet imports selected Windows features, and operating system settings from a migration store, and applies them to the local computer.

Lesson 2

1. **Correct answer: D**

A. **Incorrect**: The msinfo32.exe utility is useful for performing a manual assessment of existing Windows Server installations.

B. **Incorrect**: The Get-WindowsFeature cmdlet is useful for performing a manual assessment of existing Windows Server installations.

C. **Incorrect**: The Application Compatibility Toolkit is useful for assessing the compatibility of existing software with different Windows platforms.

D. **Correct**: The Windows Server Catalog identifies system and peripheral hardware from different vendors that has been certified for Windows Server 2012.

2. **Correct answer: B**

   A. **Incorrect**: During Phase 2: Gather Requirements, the toolkit uses various collection protocols to communicate with devices on your network to collect data to use in performing the various assessments. Because the communications performed by these protocols are subject to the administration and security settings of your environment, you must gather the user accounts and passwords needed to connect and successfully inventory the devices in your environment prior to running the toolkit.

   B. **Correct**: During Phase 3: Prepare Environment, the toolkit uses several different communication protocols based on your goals and how the environment is configured. These include WMI, Active Directory Domain Services, SQL Server commands, VMware Web services, and SSH with remote shell commands. During this phase, you will prepare your environment to ensure that the toolkit can successfully connect and gather information from the target machines in your environment

   C. **Incorrect**: During Phase 4: Install Toolkit, you download and install the toolkit using the options that best suit your environment and goals.

   D. **Incorrect**: During Phase 5: Collect Data, you launch the MAP Toolkit console and select wizards to begin the data-collection process for your environment.

3. **Correct answer: C**

   A. **Incorrect**: The Assessment Results section of the Readiness Assessment proposal document summarizes your organization's Windows Server 2012 readiness, and it provides a detailed analysis and recommendations about the servers, operating systems, and server roles inventoried.

   B. **Incorrect**: The Summary worksheet of the Assessment Summary workbook displays the number of physical servers and virtual machines inventoried, servers running earlier versions of Windows Server, servers running Hyper-V, and servers meeting the minimum system requirements for installing Windows Server 2012.

   C. **Correct**: The ServerAssessment worksheet of the Assessment Summary workbook displays the Windows Server 2012 system requirements used in performing the assessment along with any other requirements you specified for the assessment.

   D. **Incorrect**: The ServerRolesSummary worksheet of the Assessment Summary workbook summarizes the server roles currently deployed in your environment; the operating system or systems, number of physical servers, and number of virtual machines each role is running on; and any recommendations concerning the migration of these roles to Windows Server 2012.

CHAPTER 4

Deploying domain controllers

Active Directory Domain Services (AD DS) provides a distributed database and directory service that stores and manages information about the users, computers, groups, shares, printers, and other types of objects that comprise an organization's IT infrastructure. With AD DS, you can create the following:

- A forest that acts as the security boundary for your organization
- One or more domains that define the scope of authority of administrators in your organization
- A hierarchical collection of organizational units (OUs) to simplify delegation of authority for managing directory objects
- Sites that map to the structure of your organization's network

Domain controllers are servers that host AD DS within your infrastructure, and the process for deploying domain controllers has been enhanced in several ways in Microsoft Windows Server 2012. The Active Directory Domain Services Configuration Wizard (dcpromo.exe) used in previous Windows Server versions has been replaced with a new Active Directory Domain Services Configuration Wizard that simplifies the task of deploying new domain controllers to help reduce the possibility of error. Windows PowerShell now provides a way of scripting all aspects of domain controller deployment, making it possible to automate the mass deployment of domain controllers in data-center environments. Safeguards have also been introduced so that you can safely virtualize domain controllers, which simplifies deployment of private and public cloud solutions. This chapter describes how to prepare for the deployment of Windows Server 2012 domain controllers, how to deploy domain controllers using both Server Manager and Windows PowerShell, and how to take advantage of domain-controller virtualization.

Lessons in this chapter:

- Lesson 1: Preparing for deploying domain controllers **136**
- Lesson 2: Deploying domain controllers using Server Manager **147**
- Lesson 3: Deploying domain controllers using Windows PowerShell **164**

Before you begin

To complete the practice exercises in this chapter

- You need at least two servers that have a clean install of Windows Server 2012 and are configured as standalone servers in a workgroup. They can be either physical servers or virtual machines, and their TCP/IP settings should be configured to provide connectivity with the Internet.
- You might need additional servers to perform some of the optional exercises in the "Suggested practice exercises" section. You might also need access to installation media for earlier Windows Server versions for some of these exercises.
- You should be familiar with basic AD DS concepts such as forests, domains, organizational units (OUs), sites, domain controllers, schema, replication, and so on.
- It will be helpful if you also have at least rudimentary knowledge of using Windows PowerShell on earlier versions of Windows Server.

Lesson 1: Preparing for deploying domain controllers

Careful planning is of key importance when you roll out or make changes to an AD DS environment by adding, replacing, or upgrading domain controllers. A number of different scenarios are possible, and you should identify best practices for each scenario you need to implement for your organization. This lesson describes some common AD DS deployment scenarios and the different ways that domain controllers can be deployed for these scenarios.

After this lesson, you will be able to

- Describe some common AD DS deployment scenarios.
- Describe different ways Windows Server 2012 domain controllers can be deployed in a new forest.
- Describe different ways Windows Server 2012 domain controllers can be deployed in an existing forest running earlier versions of Windows Server.

Estimated lesson time: 30 minutes

AD DS deployment scenarios

Here are the two basic scenarios for AD DS deployment:

- Deploying a new forest based on AD DS in Windows Server 2012
- Deploying domain controllers in an existing forest based on AD DS in an earlier version of Windows Server

The sections that follow describe the high-level differences between these scenarios.

New forest deployments

If your organization has not yet deployed AD DS, you're in luck: this is your opportunity to get it right. Although deploying a new forest based on Windows Server 2012 AD DS is as simple as deploying your first domain controller (the forest root domain controller), there are numerous planning considerations you need to be aware of before you perform this task.

At a basic level, the technical requirements for deploying your forest root domain controller are straightforward:

- You must have local Administrator credentials on the server.
- You must have one or more local fixed NTFS volumes to store the directory database, log files, and SYSVOL share.
- You need to appropriately configure TCP/IP settings, including Domain Name Server (DNS) server addresses.
- You either need to use an existing DNS server infrastructure or deploy the DNS Server role together with the Active Directory Domain Services role when you make your server a domain controller.

The preceding technical requirements, however, are only a small part of the overall AD DS planning process. The key at this stage is to plan the entire directory structure of your organization so that you won't need to make drastic changes later on, like renaming domains or modifying your hierarchy of OUs. The details of such planning are well beyond the scope of this book, but for readers who are interested, the "More Info" topic in this section highlights some resources that can help you design an effective AD DS infrastructure and plan for its implementation.

After you create your forest by deploying the forest root domain controller, you can then deploy additional controllers for the following purposes:

- Deploy additional domain controllers in your forest root domain for redundancy and load-balancing purposes.
- Deploy domain controllers that create additional domains within your forest based on your organization's administrative or geographical structure.
- Deploy read-only domain controllers (RODCs) at less secure, branch-office sites within your organization.
- Deploy virtualized domain controllers to provide greater support for private and public cloud-computing environments.

MORE INFO **RESOURCES FOR AD DS PLANNING AND DESIGN**

The following resources can be helpful if you are planning an implementation of AD DS for the first time:

- **Designing and Deploying Directory and Security Services** **This section of the Windows Server 2003 Deployment Guide on Microsoft TechNet—found at *http://technet.microsoft.com/en-us/library/cc787010(v=WS.10).aspx*—is a bit dated, but it's still a good starting point to learn how to design and plan an AD DS environment. Be sure to supplement this resource, however, with the more recent resources that follow.**
- **AD DS Design Guide** **This section of the TechNet Library—found at *http://technet.microsoft.com/en-us/library/cc754678(v=ws.10)*—provides updated guidance on how to design an AD DS environment based on Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012.**
- **Windows Server 2008 Active Directory Resource Kit from Microsoft Press** **This book provides an excellent introduction to basic AD DS concepts, design, and administration. The book is available from O'Reilly Media at *http://shop.oreilly.com/product/9780735625150.do* in various formats, including APK, DAISY, ePub, Mobi, PDF, and print-on-demand.**

Finally, a good place to find answers to your AD DS questions is the Directory Services forum on TechNet at *http://social.technet.microsoft.com/Forums/en-us/winserverDS/threads*.

Best practices for new forest deployments

The actual number of domain controllers and the types needed for your environment depends on a number of factors, but here are some key best practices to keep in mind:

- Each domain should have at least two functioning writeable domain controllers to provide fault tolerance. If a domain has only one domain controller and this domain controller fails, users will not be able to log on to the domain or access any resources in the domain. And if you have only one writable domain controller in your domain and this domain controller fails, you won't be able to perform any AD DS management tasks.
- Each domain in each location should also have a sufficient number of domain controllers to service the needs of users for logging on and accessing network resources. The TechNet sections described in the earlier "More Info" topic include some recommendations on how to determine the number of domain controllers based on their hardware configuration and the number of users at the location.
- Domain controllers should be dedicated servers that are used only for hosting the AD DS and DNS Server roles and nothing else. Their full attention should be directed to performing their main job, which is authenticating users and computers for client logons and for accessing network resources.

- The simplest forest design is to have only one domain. The more domains you have, the more administrative overhead you will experience in the form of managing multiple service administrator groups, maintaining consistency among Group Policy settings that are common to different domains, maintaining consistency among access control and auditing settings that are common to different domains, and so on.
- If your organization has multiple sites, such as a head office and one or more remote branch offices, you should generally deploy at least one domain controller at each remote office to provide users with faster logon times and more efficient access to network resources. For best security, domain controllers at remote offices should be RODCs.

Existing forest deployments

Most readers of this book will likely deploy new Windows Server 2012 domain controllers in an existing Active Directory infrastructure based on Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003. There are several ways you can introduce such changes:

- Deploying new Windows Server 2012 domain controllers in an existing forest whose domain controllers are running an earlier version of Windows Server
- Upgrading domain controllers running earlier versions of Windows Server to Windows Server 2012

These scenarios will be discussed later in this lesson.

IMPORTANT **END OF SUPPORT DATE FOR WINDOWS SERVER 2003**

Windows Server 2003 exited mainstream support in July 2010 and will exit extended support in July 2015, so if you are planning to upgrade your AD DS environment to Windows Server 2012, you should do it soon.

New forest domain controller deployment

Depending on the administrative and geographical structure of your organization and the number of users to be supported, deploying a new forest based on Windows Server 2012 AD DS might involve several of the following domain-controller deployment scenarios:

- Deploying the first domain controller in a new forest (required)
- Deploying the first domain controller for a new domain (required if additional domains need to be created in the forest)
- Deploying additional domain controllers in each domain for fault tolerance and to support the number of users at each location (recommended)
- Deploying read-only domain controllers (RODCs) at remote branch office locations (recommended)

- Deploying virtualized domain controllers (not recommended for most production environments)

The sections that follow provide some additional information on each of these deployment scenarios.

First domain controller in a new forest

Installing the first domain controller in a new forest requires that you be logged on as the local Administrator of the server. This can be done using either Server Manager or Windows PowerShell, as demonstrated in Lessons 2 and 3 of this chapter.

Regardless of which method you use for deploying the first domain controller in your forest root domain, you need to provide the following information:

- **Domain name** Enter the fully qualified domain name (FQDN) for the root domain of your new forest—for example, corp.contoso.com.
- **Domain NetBIOS name** Enter the NetBIOS name for your new forest (required if the FQDN prefix name is longer than 15 characters).
- **Forest functional level** Select one of the following:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012 (the default)
- **Domain functional level** Select one of the following:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012 (set to the selected forest functional level)
- **Directory Services Restore Mode (DSRM) password** You must specify this at the time the server is promoted to a domain controller.
- **DNS Server** Indicate whether the new domain controller should also be a DNS server (recommended).
- **Database folder** Specify where the AD DS database is stored. (The default location is %windir%\NTDS.)
- **Log files folder** Specify where the AD DS log files are stored. (The default location is %windir%\NTDS.)
- **SYSVOL folder** Specify where the AD DS SYSVOL share is located. (The default is %windir%\SYSVOL.)

A new feature of deploying Windows Server 2012 domain controllers is a validation phase that is performed just prior to the promotion process. As Figure 4-1 illustrates, this validation phase invokes a series of tests that check whether all necessary prerequisites have been met to ensure that the domain controller deployment operation will succeed. This prerequisite check can be bypassed when deploying domain controllers using Windows PowerShell, but doing this is not recommended.

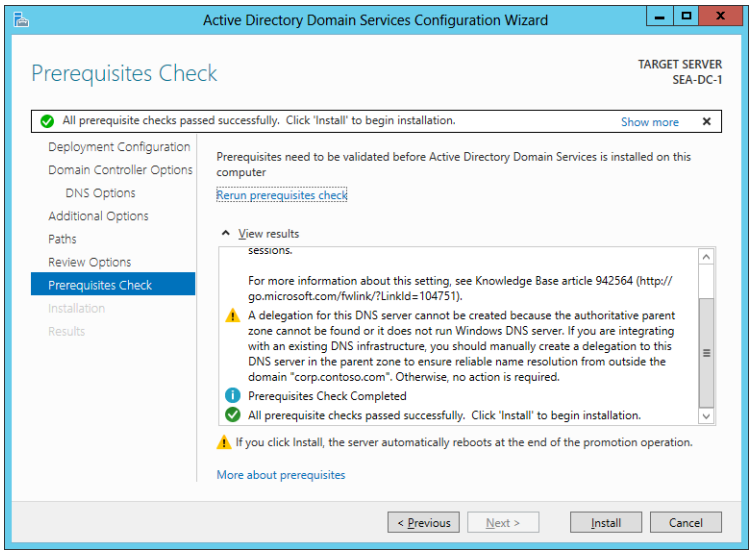


FIGURE 4-1 Example of the new validation phase that occurs during domain controller promotion using Server Manager.

REAL WORLD **DOMAIN CONTROLLERS AND DNS SERVERS**

Unless your organization uses a third-party DNS server such as BIND on your internal network, you should always have all your domain controllers also function as DNS servers to ensure high availability in distributed environments. By default, when you install the AD DS role on a server and then promote the server to a domain controller, the DNS Server role is automatically installed and configured as well.

First domain controller in a new domain

After the first domain of the forest (that is, the forest root domain) has been created, new child domains or tree domains can be created if your AD DS design warrants doing so. Installing the first domain controller for a new child domain or tree domain requires supplying the credentials of a member of the Enterprise Admins security group, which is one of two new security groups (the other is the Schema Admins group) that is created by AD DS when the forest root domain controller is deployed.

Deployment of domain controllers for new child domains or tree domains can be performed remotely using Server Manager or Windows PowerShell. The required information is similar to that listed in the previous section, with the addition of the following:

- **Domain type** Specify whether to create a new child domain or a new tree domain.
- **Parent domain name** Enter the name of the parent domain of which the new child or tree domain will be a subdomain.
- **DNS delegation** Specify whether to create a DNS delegation that references the new DNS server you are installing along with the domain controller. (The default is determined automatically based on your environment.)

Additional domain controllers in a domain

After you create a domain created by deploying its first domain controller, additional domain controllers can be deployed for fault tolerance and to support the number of users at the location. Installing additional domain controllers in a domain requires supplying the credentials of a member of the Domain Admins security group for that domain.

Deployment of additional domain controllers for a domain can be performed remotely using Server Manager or Windows PowerShell. The information you will be required to provide is similar to that listed in the previous section, with the addition of the following:

- **Site name** Specify the name of the AD DS site to which the domain controller should be added.
- **Global catalog** Specify whether the new domain controller should host the global catalog.
- **Replication source** Specify an existing domain controller to be used as the initial replication partner for replicating a copy of the directory database to the new domain controller. (The default is any available domain controller.)
- **Application partitions to replicate** Specify application partitions on existing domain controllers that should be replicated to the new domain controller.
- **Install from media path** You can choose to install the new domain controller using backed-up media by means of the Install From Media (IFM) deployment option.

REAL WORLD **DOMAIN CONTROLLERS AND THE GLOBAL CATALOG**

The global catalog contains a searchable, partial representation of every object in every domain in the forest. You can use the global catalog to quickly locate objects from any domain in the forest without having to know the name of the domain. All your domain controllers should also function as global catalog servers to ensure high availability in distributed environments. By default, when you promote a server to a domain controller, the new domain controller is automatically configured as a global catalog server.

Read-only domain controllers

Read-only domain controllers (RODCs) are additional domain controllers for a domain and are intended mainly for deployment in branch office environments that have relatively few users, few or no IT staff, and a slow wide area network (WAN) connectivity with the head office, and in environments that lack the level of physical security controls available at a typical head office.

RODCs host read-only partitions of the AD DS database. Clients can authenticate against an RODC but cannot write directory changes to it. RODCs include additional safeguards that help ensure any information on the RODC remains confidential if it is stolen or has its security compromised.

Deployment of an RODC can be performed remotely using Server Manager or Windows PowerShell. Deploying an RODC requires the following:

- Availability of credentials of a member of the Domain Admins for the domain
- A forest functional level of Windows Server 2003 or higher
- At least one writable domain controller running Windows Server 2008 or later installed in the domain

MORE INFO **DEPLOYING RODCS**

More information on how to plan the deployment of RODCs can be found in the TechNet Library at *http://technet.microsoft.com/en-us/library/cc771744(v=ws.10)*.

REAL WORLD **RODC ON SERVER CORE INSTALLATIONS**

Beginning with Windows Server 2008 R2, RODCs can be deployed on Windows Server Core installations. Doing this helps to further reduce the attack surface of your RODCs and lower their maintenance requirements. Refer back to Chapter 2, "Deploying servers," for information on how to convert a Server With A GUI installation of Windows Server 2012 to a Server Core installation.

Virtualized domain controllers

Virtualized domain controllers are domain controllers running in virtual machines on Hyper-V hosts. Windows Server 2012 includes new capabilities that help make domain controller virtualization much safer and less prone to problems than previous Windows Server versions. For more information, see the following "Real World" topic.

REAL WORLD **VIRTUALIZING DOMAIN CONTROLLERS**

Windows Server 2012 helps enable cloud computing by making virtualized domain controllers both easier to deploy and less prone to problems. For example, you can now deploy replica virtual domain controllers by cloning existing virtual domain controllers and then deploying them using Server Manager or Windows PowerShell. Virtualizing domain controllers is also much safer than it was with previous versions of Windows Server. That's because each virtual domain controller has a unique identifier called a *GenerationID* that is exposed to the hypervisor on the host machine. This helps protect the AD DS directory hosted by a virtual domain controller from unexpected rollback events caused by the accidental application of snapshots or other occurrences that caused duplicate directory objects and other issues in previous Windows Server versions.

For more information about these different improvements, see the section "Virtualization that just works" in the topic "What's New in Active Directory Domain Services (AD DS)" in the TechNet Library at *http://technet.microsoft.com/en-us/library/hh831477#BKMK_VirtualizationJustWorks*.

Quick check

- **What are the minimum credentials you need to deploy an additional domain controller in an existing domain of a forest?**

Quick check answer

- **The minimum credentials needed are those for a member of the Domain Admins security group in the target domain. You could also use the credentials of a member of the Enterprise Admins or Schema Admins group, but these credentials should generally be used only for managing the forest root domain and schema.**

Existing forest domain controller deployment

There are two basic ways of deploying Windows Server 2012 domain controllers in a forest whose domain controllers are running earlier versions of Windows Server:

- Installing additional domain controllers running Windows Server 2012
- Upgrading existing domain controllers running earlier versions of Windows Server

The sections that follow provide more details about these approaches.

REAL WORLD **UPGRADING DOMAIN CONTROLLERS**

Although performing in-place upgrades can help reduce hardware costs, the margin for error is greater. If possible, avoid performing in-place upgrades of your existing domain controllers; instead, introduce new domain controllers and then, if desired, retire your existing domain controllers.

Installing additional domain controllers

Installing additional domain controllers that are running Windows Server 2012 in a forest whose domain controllers are running an earlier version of Windows Server involves the following steps:

1. Install Windows Server 2012 on the servers that will become the new domain controllers.
2. Join the new servers to the domain.
3. Use Server Manager or Windows PowerShell to install the AD DS role on the new servers, and promote them to domain controllers.

Once deployed, the new Windows Server 2012 domain controllers can coexist with the domain controllers running earlier versions of Windows Server if you want them to. Alternatively, you can move the flexible single master operations (FSMO) roles from the earlier domain controllers that are running earlier versions of Windows Server to the new domain controllers that are running Windows Server 2012, and finally demote and retire the earlier domain controllers.

> ***NOTE*** **PREPARING THE SCHEMA**
>
> **Introducing Windows Server 2012 domain controllers into a forest whose domain controllers are running earlier versions of Windows Server automatically causes the AD DS schema to be extended to the latest version. See Lesson 2 for more information on extending the schema.**

Upgrading existing domain controllers

Upgrading all of a forest's existing domain controllers that are running an earlier version of Windows Server involves the following steps:

1. Prepare your forest and domains for an upgrade by using the Adprep.exe command-line tool to extend the schema. (See Lesson 2 for more information about Adprep.)
2. Verify that the operating system of your existing domain controllers has a supported in-place upgrade path to Windows Server 2012.
3. Verify all prerequisites for upgrading your existing domain controllers to Windows Server 2012. For example, the drive that hosts the AD DS database (NTDS.DIT) must have at least 20 percent free disk space before you begin the operating system upgrade.
4. Perform an in-place upgrade of all existing domain controllers to Windows Server 2012.

MORE INFO **PREREQUISITES FOR UPGRADING DOMAIN CONTROLLERS**

For more information about supported upgrade paths and other prerequisites for performing in-place upgrades of domain controllers running earlier versions of Windows Server to Windows Server 2012, see the topic "Upgrade Domain Controllers to Windows Server 2012" in the TechNet Library at *http://technet.microsoft.com/en-us/library/hh994618*. See also "Determine Domain Controller Upgrade Order" at *http://technet.microsoft.com/en-us/library/cc732085(WS.10).aspx*.

Lesson summary

- The two main AD DS deployment scenarios are deploying new forests using Windows Server 2012 and deploying domain controllers into existing forests running earlier versions of Windows Server.
- Be sure to gather the necessary information and credentials before deploying AD DS, and make sure you complete any other steps needed to prepare your environment before deploying domain controllers.
- The process of promoting Windows Server 2012 servers as domain controllers now includes a prerequisites check to ensure the promotion process can succeed.
- The process of promoting Windows Server 2012 servers as domain controllers now automatically run Adprep when needed to prepare a forest and domains running earlier versions of Windows Server.
- You still need to run Adprep manually if you are performing in-place upgrades of domain controllers running earlier versions of Windows Server.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following is *not* a best practice for performing new forest deployments?
   - **A.** Ensure that each domain has at least two domain controllers for fault tolerance and to ensure availability. Only one of these domain controllers needs to be writeable; the other can be an RODC.
   - **B.** Make sure that each site in your domain has a sufficient number of domain controllers to service the needs of users for logging on and accessing network resources.
   - **C.** Whenever possible, keep the design of your forest simple by having only one domain.
   - **D.** Install only the AD DS and DNS Server roles on your domain controllers and no other server roles.

2. Which of the following information should you obtain or decide upon during the planning stage of deploying the first Windows Server 2012 domain controller in a new forest? (Choose all that apply.)
   - **A.** The fully qualified domain name (FQDN) for the root domain of your new forest.
   - **B.** The forest and domain functional levels.
   - **C.** The location for the AD DS database, log files, and SYSVOL folder.
   - **D.** The credentials of a member of the Domain Admins security group.
3. Which of the following is *not* true? (Choose all that apply.)
   - **A.** Creating a DNS delegation is a required step for all AD DS deployments.
   - **B.** All domain controllers in a domain should have the DNS Server role installed and configured to ensure high availability in distributed environments.
   - **C.** All domain controllers in a domain should be configured as global catalog servers to ensure high availability in distributed environments.
   - **D.** Read-only domain controllers require that there be at least one writeable domain controller running Windows Server 2003 or later installed in the domain.

Lesson 2: Deploying domain controllers using Server Manager

Server Manager provides an easy way to deploy Windows Server 2012 domain controllers. Server Manager is mainly intended for managing small and midsized environments where the automation of domain controller deployment is not required. This lesson demonstrates how to use Server Manager to deploy domain controllers in both new and existing forests.

After this lesson, you will be able to

- Use Server Manager to prepare your Windows Server 2012 environment for domain controller deployment.
- Install the Active Directory Domain Services role using the Add Roles And Features Wizard of Server Manager.
- Promote servers to domain controllers using the Active Directory Domain Services Configuration Wizard of Server Manager.
- Verify the promotion of servers to domain controllers.
- Demote domain controllers, and remove the Active Directory Domain Services role.

Estimated lesson time: 30 minutes

Preparing for domain-controller deployment

The steps for preparing to deploy Windows Server 2012 domain controllers using Server Manager differ depending on whether you are deploying the first domain controller in a new forest, deploying additional domain controllers in the new forest, or deploying domain controllers in an existing forest whose domain controllers are running an earlier version of Windows Server.

Preparing for deploying the first domain controller in a new forest

To deploy the first Windows Server 2012 domain controller in a new forest using Server Manager, you should either log on locally to the server or connect to it using Remote Desktop. No other preparation is needed for this scenario.

Preparing for deploying additional domain controllers in the new forest

After you create a new forest by deploying your first Windows Server 2012 domain controller, you can use Server Manager to deploy additional domain controllers in an existing domain, create new child domains, or create new tree domains. These tasks can be performed remotely by using Server Manager on any Windows Server 2012 domain controller or member server, or on a Windows 8 client computer that has the Remote Server Administration Tools (RSAT) installed.

The recommended steps for preparing to use Server Manager to deploy additional domain controllers are as follows:

1. Make sure you have the appropriate credentials for the task you are going to perform. For example, if you are going to add additional domain controllers to an existing domain, make sure you have Domain Admin credentials for that domain. If you are going to create a new child domain, make sure you have Enterprise Admin credentials.
2. Add the remote servers you'll be promoting to domain controllers to the server pool so that you can manage them remotely using Server Manager.
3. Create a new server group for the remote servers you'll be promoting to domain controllers, and add the servers to the server group. Doing this makes it easier to promote multiple remote servers to domain controllers simultaneously.

Preparing for deploying domain controllers in an existing forest

Adding Windows Server 2012 domain controllers to an existing forest or domain running an earlier version of Windows Server first requires that the existing Active Directory schema be extended. In previous versions of Windows Server, Adprep.exe was used for extending the schema. Adprep is a command-line tool that was available in the \support\adprep folder of Windows Server 2008 R2 installation media or in the \sources\adprep folder of Windows Server 2008 installation media. The Adprep command uses parameters such as */forestprep* and */domainprep* to prepare an existing forest for the introduction of a domain controller running a newer version of Windows Server.

Beginning with Windows Server 2012, however, Adprep is now run automatically as needed when you deploy a new Windows Server 2012 domain controller in an existing forest or domain running an earlier version of Windows Server. This change simplifies the task of adding Windows Server 2012 domain controllers to an existing forest or domain running an earlier version of Windows Server because you no longer need to manually run Adprep before introducing the new domain controllers into your forest.

Adprep is also available as a standalone command-line tool in the \support\adprep folder of Windows Server 2012 installation media. The standalone version of Adprep is required for certain scenarios, such as performing an in-place upgrade of your first Windows Server 2012 domain controller, where you must run Adprep manually to prepare your forest and its domains before you begin upgrading your existing domain controllers to Windows Server 2012.

NOTE **ADPREP SYNTAX**

To display the syntax and usage examples for Adprep, type <*drive*>\support\adprep\adprep at a command prompt where *drive* is the letter for the drive where your Windows Server 2012 installation media can be found.

The Windows Server 2012 version of Adprep can be used to extend the schema of an existing forest whose domain controllers are running any of the following versions of Windows Server:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003

However, the following considerations apply when running the Windows Server 2012 version of Adprep:

- You must have the credentials of a member of the Enterprise Admins group to run the **Adprep /forestprep** command.
- Adprep can be run only on any server (domain controller, member server or standalone server) that is running a 64-bit version of Windows Server 2008 or later. You cannot run Adprep on a server running Windows Server 2003 or a 32-bit version of Windows Server 2008.
- The server you run Adprep on must have network connectivity to the schema master of the existing forest.
- The server you run Adprep on must have network connectivity to the infrastructure master of the existing domain where you want to add a new Windows Server 2012 domain controller.

REAL WORLD **VERIFYING ADPREP**

The Dsquery.exe command-line tool can be used to verify whether Adprep has extended your forest's schema. For example, let's say your existing forest has domain controllers running Windows Server 2008 R2. To determine the current schema level of your forest, open a command prompt on one of your domain controllers and run the following command:

```
dsquery * cn=schema,cn=configuration,dc=fabrikam,dc=com -scope base
  -attr objectVersion
```

The output from this command looks like this:

```
objectVersion
47
```

Now take a server running Windows Server 2012, join it to a domain in your forest, and use Server Manager to promote the server to a domain controller. After you finish introducing the new domain controller into your forest, re-run the preceding *dsquery* command on the domain controller you previously ran it on. The output from the command looks like this:

```
objectVersion
56
```

The version number *56* indicates that the schema of your forest has been extended to include domain controllers running Windows Server 2012.

Quick check

- **When deploying additional domain controllers in a forest using Server Manager, why should you create a server group using Server Manager for the remote servers you'll be promoting to domain controllers?**

Quick check answer

- **So that you can more easily promote them remotely as domain controllers and manage them.**

Installing the AD DS role

Before you can promote a server to domain controller, you must first install the Active Directory Domain Services role on the server. To do this using Server Manager, select Add Roles And Features from the Manage menu to launch the Add Roles And Features Wizard. On the Select Server Roles page of the wizard, select the Active Directory Domain Services role and confirm the installation of the tools for managing AD DS as shown in Figure 4-2.

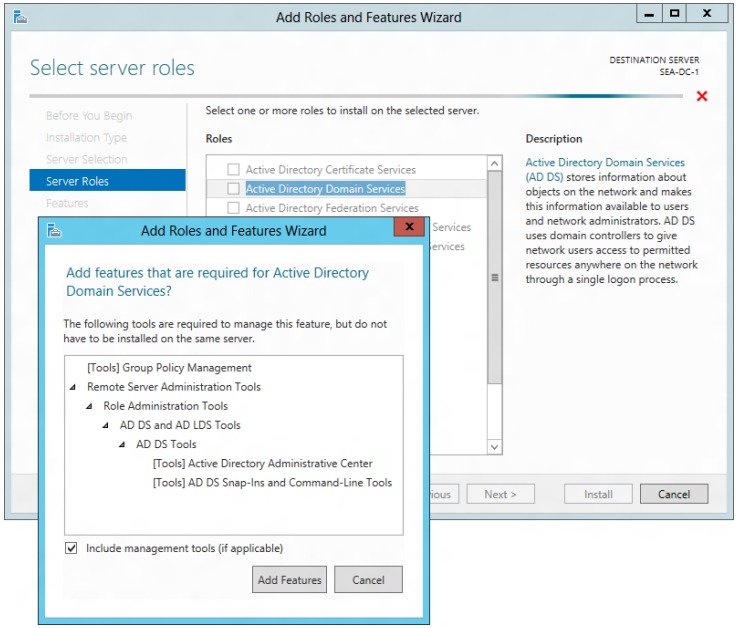


FIGURE 4-2 Installing the AD DS role together with the role-management tools.

Running the AD DS Configuration Wizard

When you complete the installation of the role, the final page of the Configuration Wizard prompts you to promote the server to a domain controller. If you close the wizard at this point, you can still access the link to promote the server from the Notifications menu of Server Manager as shown in Figure 4-3.

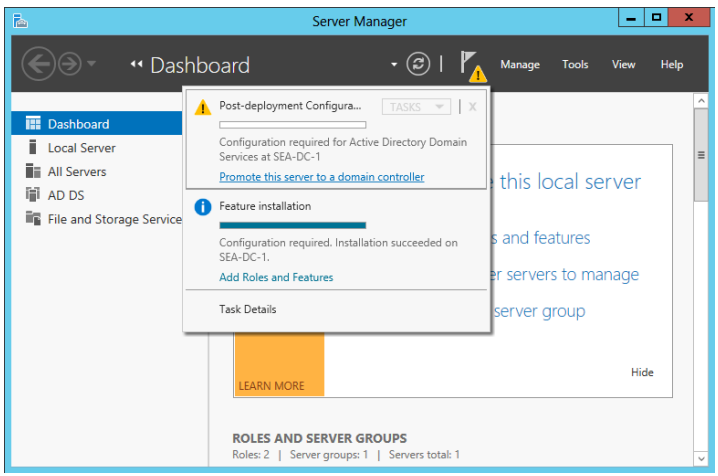


FIGURE 4-3 You can use the Notifications menu to promote the server to a domain controller.

Clicking the link to promote the server to a domain controller launches the AD DS Configuration Wizard. The steps of this wizard depend on which type of domain-controller deployment scenario you are performing. The upcoming sections cover the following scenario types:

- First domain controller in new forest
- Additional domain controller in new domain
- First Windows Server 2012 domain controller in an existing forest

First domain controller in new forest

After the AD DS role has been added to the server, using the AD DS Configuration Wizard to promote the server to the first domain controller for a new forest involves the following steps:

1. On the Deployment Configuration page of the wizard, shown in Figure 4-4, select the Add A New Forest option and specify the root domain for your new forest. Then proceed through the wizard and perform the steps that follow.

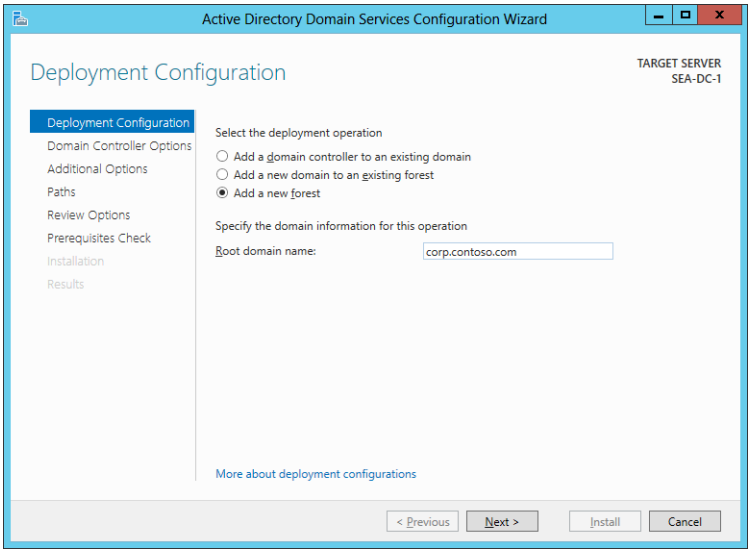


FIGURE 4-4 Deploying the first domain controller for a new forest using the AD DS Configuration Wizard.

2. On the Domain Controller Options page, specify a functional level for your new forest and root domain. The default forest and functional levels are Windows Server 2012. If you have no domain controllers running earlier versions of Windows Server in your environment, you should leave the defaults unchanged.
3. On the same page, specify whether your domain controller should also be a DNS server. Microsoft recommends that all domain controllers also be DNS servers to ensure AD DS availability.

4. On the same page, note that the first domain controller must be a global catalog server and that it cannot be an RODC.
5. On the same page, enter a password for the Directory Services Restore Mode (DSRM) administrator account.
6. On the DNS Options page, specify DNS delegation options if you are integrating AD DS with an existing DNS infrastructure. To do this, you can manually create a delegation for your new DNS server in its authoritative parent zone to ensure reliable name resolution from outside your AD DS environment. For example, if the root domain name of your new forest is corp.contoso.com as shown in Figure 4-4, you create a delegation for your DNS server in the authoritative parent zone on the DNS server that manages the public contoso.com domain for your organization.
7. On the Additional Options page, the wizard suggests a NetBIOS name for your forest root domain. You can either accept what the wizard suggests or specify a different name of up to 15 Internet-standard characters (A–Z, a–z, 0–9, and "-" but not entirely numeric).
8. On the Paths page, specify the location of the AD DS database, log files, and SYSVOL or accept the defaults.
9. The Review Options page displays the results of your selections.
10. The Prerequisites Check page verifies that all prerequisites have been met for successfully deploying the domain controller. See Figure 4-1 earlier in this chapter for an example of what this wizard page looks like.
11. Clicking Install promotes the server to a domain controller and automatically reboots the server at the end of the promotion operation.

REAL WORLD **WINDOWS POWERSHELL BEHIND THE WIZARD**

The AD DS Configuration Wizard is built entirely on Windows PowerShell. In other words, you can think of the wizard as a UI that simply runs a Windows PowerShell command whose parameters are determined by the selections you made on the different wizard pages. On the Review Options page of the wizard, you can click View Script to display the Windows PowerShell script in Notepad. For example, if you are deploying the first domain controller for a new forest whose forest root domain is corp.contoso.com, the script that performs this action looks like this:

```
#
# Windows PowerShell script for AD DS Deployment
#

Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "Win2012" `
-DomainName "corp.contoso.com" `
```

```
-DomainNetbiosName "CORP" `
-ForestMode "Win2012" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

Being able to view the script behind the wizard provides several benefits. First, it enables you to quickly learn the syntax of Windows PowerShell cmdlets for AD DS deployment. And second, you can copy these scripts, customize them, and use them to automate the deployment of other domain controllers in your environment.

MORE INFO **NAMING YOUR NEW FOREST**

For some recommendations on how to name the forest root domain of a new forest, see the topic "Selecting the Forest Root Domain" in the TechNet Library at *http://technet.microsoft.com/en-us/library/cc726016(v=WS.10).aspx*.

Additional domain controller in new domain

After you deploy the first domain controller for a new domain or forest, you should deploy at least one additional domain controller in the domain for fault tolerance. After adding the AD DS role to the server that will become the additional domain controller, you can use the AD DS Configuration Wizard to promote the server to be an additional domain controller for the domain using following steps:

1. On the Deployment Configuration page of the wizard, shown in Figure 4-5, select the Add A Domain Controller To An Existing Domain option. Specify the domain you want to add the new domain controller to, and if your current logon credentials have insufficient privileges to perform the option, click Change and specify suitable credentials.
2. On the Domain Controller Options page, specify whether your domain controller should also be a DNS server. (This option is selected by default.)
3. Also on this page, specify whether your domain controller should also be a global catalog server. (This option is selected by default.)
4. Also on this page, specify whether your domain controller should also be an RODC. You should have at least two writeable domain controllers in every domain in your forest, so do not select this option if this is the second domain controller for your domain.

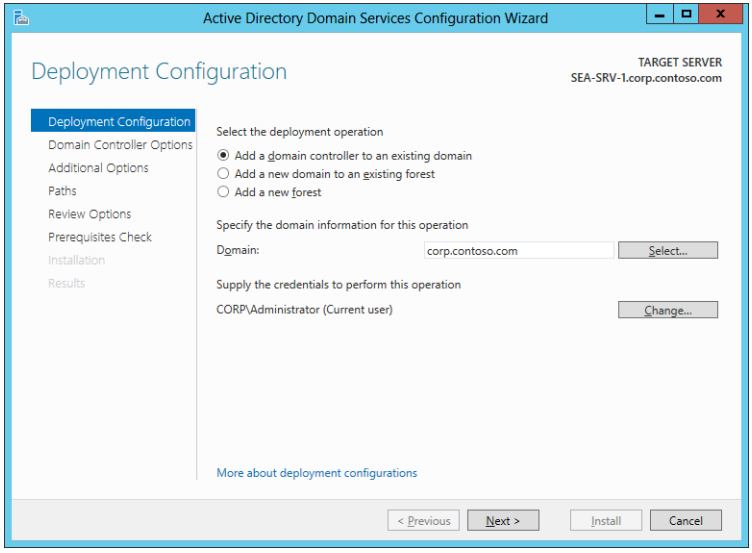


FIGURE 4-5 Deploying an additional domain controller to an existing domain.

5. Also on this page, specify the name of the existing AD DS site the new domain controller should belong to. (The default is Default-First-Site-Name.)
6. Also on this page, enter a password for the DSRM administrator account.
7. On the DNS Options page, specify DNS delegation options if you are integrating AD DS with an existing DNS infrastructure.
8. On the Additional Options page, select the Install From Media (IFM) option if you used the Ntdsutil.exe tool to create installation media for additional domain controllers that you are deploying in the domain. You can use the Install From Media (IFM) option to minimize the replication of directory data over your network, which helps make deploying additional domain controllers at remote sites more efficient. If you are deploying additional domain controllers at your organization's hub site (its headquarters or central office), however, you would generally not use the IFM option.
9. Also on this page, if you are not using the IFM option for deploying additional domain controllers, you can select which domain controller in your domain the new additional domain controller should use as an initial replication partner for pulling down a copy of the AD DS database. By default, your new domain controller replicates from any available domain controller in the domain, but you also have the option of specifying a particular domain controller as its initial replication partner.
10. Complete the remaining steps of the wizard to deploy the additional domain controller to the domain.

MORE INFO **INSTALL FROM MEDIA**

For more information about deploying domain controllers using the Install From Media (IFM) option, see the topic "Installing AD DS from Media" in the TechNet Library at *http://technet.microsoft.com/en-us/library/cc770654(v=WS.10).aspx*.

First Windows Server 2012 domain controller in an existing forest

You can also use the AD DS Configuration Wizard to deploy Windows Server 2012 domain controllers in a forest or domain whose existing domain controllers are running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003. As explained earlier in this lesson, when you use the wizard to deploy the first Windows Server 2012 domain controller in a domain of a forest whose domain controllers are running earlier Windows Server versions, the Adprep tool automatically runs to prepare the forest and domain by extending the schema to its latest version.

The procedure that follows demonstrates this scenario by deploying a Windows Server 2012 domain controller named *VAN-SRV-3* in a forest root domain named *fabrikam.com* whose existing domain controllers are all running Windows Server 2008 R2. After the AD DS role has been added to server VAN-SRV-3, using the AD DS Configuration Wizard to add the server as the first Windows Server 2012 domain controller in the fabrikam.com forest involves the following steps:

1. On the Deployment Configuration page of the wizard, shown in Figure 4-6, select the Add A Domain Controller To An Existing Domain option, specify fabrikam.com as the forest root domain, and specify suitable credentials for performing the operation.

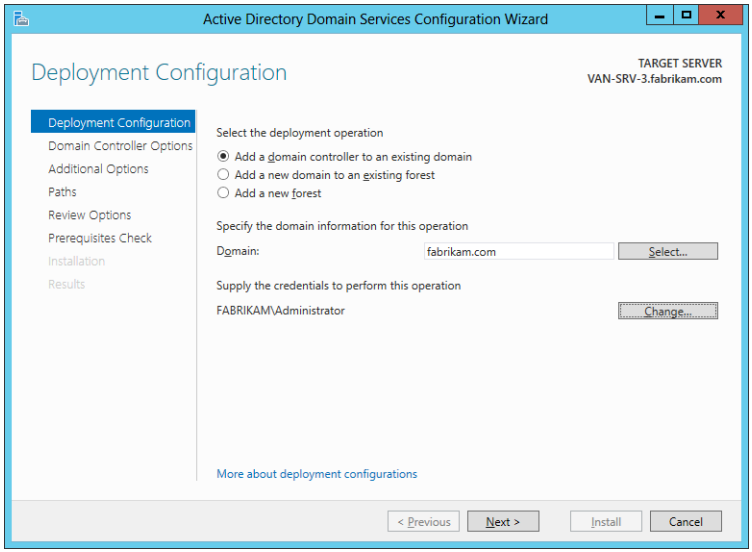


FIGURE 4-6 Promoting the server named VAN-SRV-3 to be the first Windows Server 2012 domain controller in the existing fabrikam.com forest root domain.

2. Proceed through the wizard as described in the previous section until you reach the Preparation Options page shown in Figure 4-7. This page informs you that performing this operation will prepare your forest and domain for Windows Server 2012 domain controllers by extending the schema. If you do not want to extend the schema, cancel the operation and do not deploy the new domain controller.

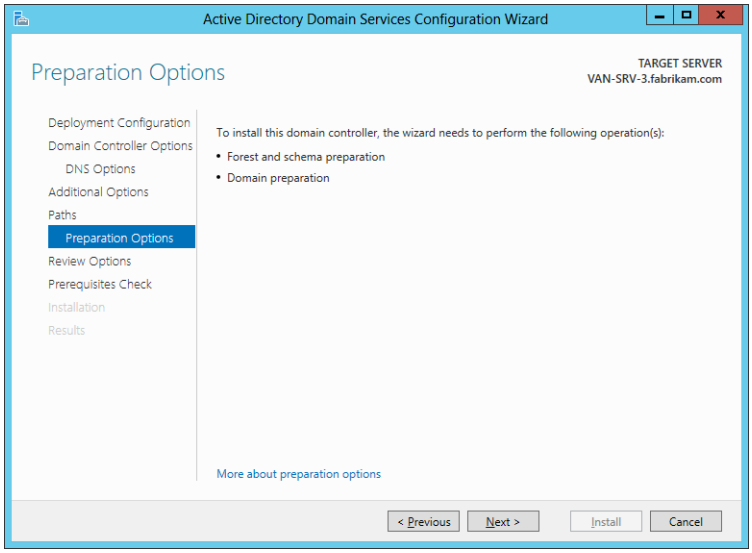


FIGURE 4-7 The wizard informs you that the forest schema will be extended if you perform this operation.

3. Complete the remaining steps of the wizard to deploy the domain controller and extend the schema. Note that you did not have to manually run Adprep to prepare your forest or domain for the domain controller running the new version of Windows Server.

Verifying the installation

After deploying a new domain controller running Windows Server 2012 using Server Manager, you should verify the installation by performing the following steps:

1. Add the new domain controller to the server pool and to any server group you created for grouping together your Windows Server 2012 domain controllers.
2. Select the new domain controller from any applicable page of Server Manager.
3. Check for any alerts raised concerning the new controller on the Notifications menu.
4. Scroll down the page to the Events tile, and review any events raised for the new domain controller. Pay special attention to any critical, error, or warning events raised, and perform any additional configuration or remedial action needed to address these events.

5. Scroll down the page to the Services tile, and review the condition of the services on the new domain controller. Make sure that all services have their startup values configured appropriately and that automatic services are running.
6. Scroll down the page, and start a Best Practices Analyzer (BPA) scan on the new domain controller by selecting Start BPA Scan from the Tasks menu of the Best Practices Analyzer tile. (See Figure 4-8.) BPAs are server management tools built into Windows Server 2012 that help you adhere to best practices by scanning installed server roles and reporting any violations discovered.

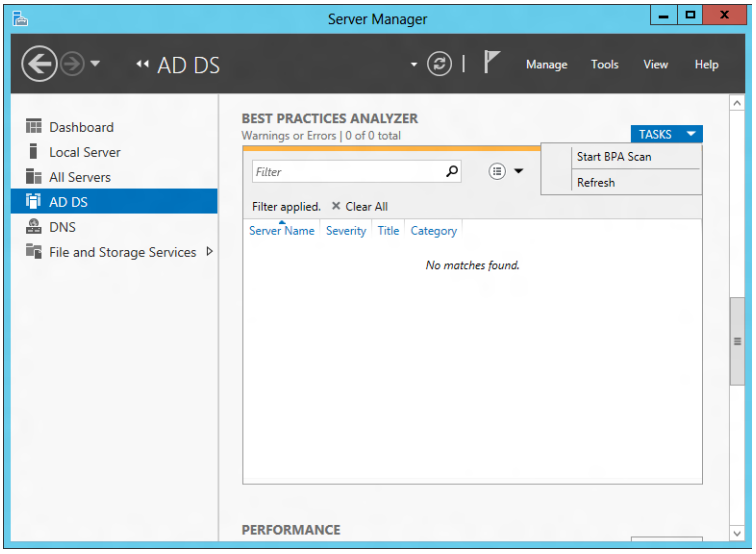


FIGURE 4-8 Starting a BPA scan on a domain controller.

As an example, Figure 4-9 shows the results of running a BPA scan on two Windows Server 2012 domain controllers deployed in a new forest. These domain controllers have been grouped together in Server Manager by creating a custom server group named Domain Controllers. The Error displayed in the Best Practices Analyzer tile indicates that domain controller SEA-DC-1 is the PDC Emulator operations master for the forest and needs to be able to synchronize its clock with a reliable time source on the Internet. After you run a BPA scan on your domain controllers, be sure to carefully review the results displayed in the tile.

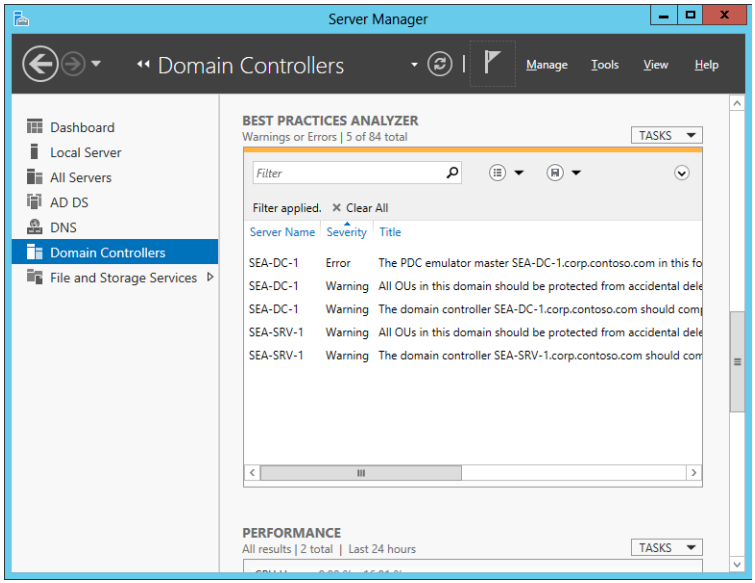


FIGURE 4-9 Reviewing the results of a BPA scan performed on newly deployed domain controllers.

Quick check

- **You used Server Manager to install the AD DS role on a remote server, but you closed the Add Roles And Features Wizard without first promoting the server to a domain controller. How can you finish the job and promote the server?**

Quick check answer

- **Access the link to promote the server from the Notifications menu of Server Manager.**

Uninstalling AD DS

If you need to retire a Windows Server 2012 domain controller from your environment—for example, to repurpose its server hardware for some other role—you can do this using Server Manager by performing the following steps:

1. Launch the Remove Roles And Features Wizard from the Manage menu, and select your server from the server pool.
2. On the Remove Server Roles page, deselect the Active Directory Domain Services check box. The Validation Results page is displayed at this point to indicate that you must first demote the domain controller before you can remove the AD DS role. (See Figure 4-10.)

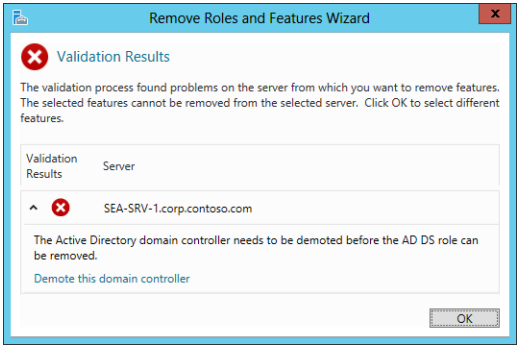


FIGURE 4-10 You must demote a domain controller before you can remove the AD DS role from it.

3. On the Validation Results page, click Demote This Domain Controller to launch the AD DS Configuration Wizard.
4. On the Credentials page of this wizard, supply the necessary credentials to perform this operation if your current logon credentials have insufficient privileges. If previous attempts to remove AD DS from this domain controller failed, select the Force The Removal Of This Domain Controller check box on this page.
5. If you are demoting the last domain controller in the domain, make sure the Last Domain Controller In The Domain check box is selected to confirm that you want to remove the domain from your forest. Note that this check box is displayed only if the server is the last domain controller in the domain.
6. On the Warnings page, make sure the Proceed With Removal check box is selected to confirm your decision to perform the demotion. Note that this page is not displayed if you chose to force the removal of AD DS in the previous step.
7. On the Removal Options page, you have the option to remove any DNS delegations created in the authoritative parent zone. Note that you need to supply appropriate credentials to perform this action.
8. If you are demoting the last domain controller in the domain, you also have the options of removing the DNS zone for the domain and also any application partitions. (See Figure 4-11.) By clicking View Partitions, you can display a list of any application partitions in AD DS.

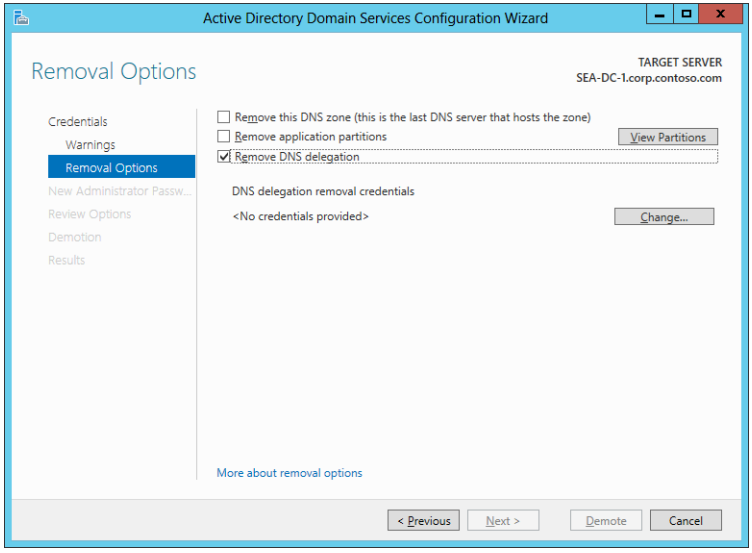


FIGURE 4-11 Options for removing the DNS zone and application partitions when demoting the last domain controller in a domain.

9. On the New Administrator Password page, enter a password for the local Administrator account for the server.
10. Complete the wizard to demote the domain controller. The server restarts, and you can log on using the local Administrator account and the new password you specified in the previous step.
11. Launch the Add Roles And Features Wizard again from the Manage menu, and select your server from the server pool.
12. On the Remove Server Roles page, deselect the Active Directory Domain Services and DNS Server check boxes. Finish running the wizard. When the server restarts, both the AD DS and DNS Server roles will have been removed.

IMPORTANT **REMOVING APPLICATION PARTITIONS**

When you demote the last domain controller in a domain using Server Manager, you have the option of removing any application partitions. At a minimum, when you do this you should see the default DNS application partitions—for example:

- **DC=DomainDNSZones,DC=corp,DC=contoso,DC=com**
- **DC=ForestDNSZones,DC=corp,DC=contoso,DC=com**

If you have other server applications deployed in your environment, you might see additional application partitions. Before removing these partitions, make sure that your deployed server applications will still be able to work properly, unless you are also retiring those server applications from your environment.

REAL WORLD **FORCING THE REMOVAL OF AD DS**

The demotion of domain controllers can fail when the domain controller you are performing this action on has no connectivity with other domain controllers in the domain. If this happens, try selecting the Force The Removal Of This Domain Controller check box on the Credentials page of the AD DS Configuration Wizard when you are attempting to demote the domain controller.

Lesson summary

- Server Manager can be used to deploy Windows Server 2012 domain controllers. This procedure is mainly intended for small and midsized environments, where automating this process is not needed.
- After you use the Add Roles And Feature Wizard to install the AD DS role on a remote server, you can use the AD DS Configuration Wizard to promote the server to a domain controller.
- After you deploy a domain controller, you can use Server Manager to verify the installation by reviewing the Event logs, reviewing the state of services, and running a Best Practices Analyzer scan on the new domain controller.
- You can use the Remove Roles And Features Wizard to uninstall the AD DS role on a remote server, but you first need to demote the server from being a domain controller.
- Adprep is still available as a standalone command-line tool in the \support\adprep folder of Windows Server 2012 installation media when you need to perform an in-place upgrade of your first Windows Server 2012 domain controller.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following procedures for deploying the first Windows Server 2012 domain controller in a new forest is correct? (Choose all that apply.)

   A. Install Windows Server 2012 on your server, and log on using the local Administrator account. Open Server Manager, and run the AD DS Configuration Wizard to promote the server as a domain controller.

   B. Install Windows Server 2012 on your server, and log on using the local Administrator account. Open Server Manager, and run the Add Roles And Features Wizard to promote the server as a domain controller.

C. Install Windows Server 2012 on your server, and log on using the local Administrator account. Open Server Manager, and run the Add Roles And Features Wizard to install the AD DS role on the server. Then run the AD DS Configuration Wizard to promote the server as a domain controller.

D. Install Windows Server 2012 on your server, and log on using the local Administrator account. Open Server Manager, and run the AD DS Configuration Wizard to install the AD DS role on the server. Then run the Add Roles And Features Wizard to promote the server as a domain controller.

2. Which of the following statements is *not* correct concerning the deployment of the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server? (Choose all that apply.)

   A. You must prepare the forest and domain and extend the schema by manually running Adprep before you use Server Manager to deploy the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server.

   B. You must select the Add A Domain Controller To An Existing Domain option on the Deployment Configuration page of the AD DS Configuration Wizard to deploy the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server.

   C. You can use the Install From Media (IFM) deployment method to deploy the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server.

   D. If your current logon credentials have insufficient privileges to deploy the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server, you can specify different credentials on the Deployment Configuration page of the AD DS Configuration Wizard.

3. Which of the following is the best syntax when using the Dsquery.exe command-line tool to verify whether Adprep has successfully extended your forest's schema?

   A. Dsquery * cn=schema,cn=configuration,dc=fabrikam,dc=com –attr objectVersion

   B. Dsquery * cn=schema,cn=configuration,dc=fabrikam,dc=com –scope base –attr sAMAccountName

   C. Dsquery * cn=schema,cn=configuration,dc=fabrikam,dc=com –scope base –attr *

   D. Dsquery * cn=schema,cn=configuration,dc=fabrikam,dc=com –scope base –attr objectVersion

Lesson 3: Deploying domain controllers using Windows PowerShell

Windows PowerShell provides a way to automate the deployment of Windows Server 2012 domain controllers. This approach to domain controller deployment can be particularly useful in large enterprise environments, data centers, and cloud-computing scenarios. This lesson demonstrates how to use Windows PowerShell to deploy domain controllers in both new and existing forests.

After this lesson, you will be able to

- Prepare your environment for domain controller deployment using Windows PowerShell.
- Use Windows PowerShell to verify the prerequisites for installing new forests, domains, and domain controllers.
- Use Windows PowerShell to install AD DS on servers and promote them as domain controllers in both new and existing forests.
- Use Windows PowerShell to demote domain controllers.

Estimated lesson time: 30 minutes

Preparing for domain-controller deployment

Similar to how domain controllers can be deployed using Server Manager as described in the previous lesson, the steps for preparing to deploy Windows Server 2012 domain controllers using Windows PowerShell differ depending on the scenario being considered.

REAL WORLD **WINDOWS POWERSHELL AND SERVER CORE INSTALLATIONS**

The Server Core installation option for Windows Server 2012 is ideal for data-center environments because of its smaller servicing footprint, disk space requirements, and attack surface. The Server Core installation option also supports installing the AD DS role, so using Windows PowerShell to deploy Server Core domain controllers is an ideal combination for a data center.

Preparing for deploying the first domain controller in a new forest

To deploy the first Windows Server 2012 domain controller in a new forest, you can run Windows PowerShell commands directly on the server by either logging on locally to the server or connecting to it using Remote Desktop. Another option, however, is to use Windows

PowerShell remoting, which lets you run Windows PowerShell commands on one or more remote computers simultaneously by using the WS-Management protocol.

As explained previously in Chapter 3, "Server remote management," the remote-management capability is enabled by default on Windows Server 2012 to make it easy to remotely manage servers using both Server Manager and Windows PowerShell. For more information, see the section "Configuring remote management" in Lesson 4 of Chapter 3.

The difficulty, however, is that Windows PowerShell remoting is primarily intended for remotely managing domain-joined computers, and if you are preparing to deploy the first domain controller in a new forest, there is no domain yet to join! In other words, the remote server that will be promoted to a domain controller is initially in a workgroup, not a domain. And the local computer you will be performing the deployment from might also be in a workgroup.

The solution is to prepare your environment by enabling the two standalone computers to talk to each other using the WS-Management protocol. If the computer you are performing the deployment from is also running Windows Server 2012, you simply need to add the name of the remote server to the *TrustedHosts list* in the local computer's WinRM configuration. Doing this enables the local computer to connect to the remote server using NTLM as the authentication mechanism instead of Kerberos, which is used in domain-based environments.

IMPORTANT **ADDING REMOTE SERVERS TO THE TRUSTEDHOSTS LIST ON YOUR COMPUTER**

When you add a remote server to the TrustedHosts list on your computer, you are allowing your credentials to be sent to the remote server without verifying the server's identity. So add remote servers to this list only if you are certain the network path from your computer to the remote server machine is completely secure.

To illustrate how to do this, consider a scenario where you have two standalone servers running Windows Server 2012: a local server named SEA-HOST-2 and a remote server named SEA-SRV-1. You want to use the Get-WindowsFeature cmdlet on the local server to display a list of installed and available roles and features on the remote server, but when you try and do this on the local server, you get the error highlighted in the following code:

```
PS C:\> Get-WindowsFeature -ComputerName SEA-SRV-1 -Credential SEA-SRV-1\Administrator

Get-WindowsFeature : The WinRM client cannot process the request. If the authentication
scheme is different from Kerberos, or if the client computer is not joined to a domain,
then HTTPS transport must be used or the destination machine must be added to the
TrustedHosts configuration setting. Use winrm.cmd to configure TrustedHosts. Note that
computers in the TrustedHosts list might not be authenticated. You can get more
information about that by running the following command: winrm help config.
```

```
At line:1 char:1
+ Get-WindowsFeature -ComputerName SEA-SRV-1 -Credential SEA-SRV-1\Administrator
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : DeviceError: (Microsoft.Manag...rDetailsHandle):CimException)
[Get-WindowsFeature], Exception + FullyQualifiedErrorId : UnSupportedTargetDevice,
Microsoft.Windows.ServerManager.Commands.GetWindowsFeatureCommand
```

The error occurs because the remote server SEA-SRV-1 is not domain-joined and therefore must first be added to the TrustedHosts list on the local server before you can manage the remote server from the local server. You can use the Set-Item cmdlet to do this:

```
PS C:\> Set-Item wsman:\localhost\Client\TrustedHosts -Value SEA-SRV-1

WinRM Security Configuration.
This command modifies the TrustedHosts list for the WinRM client. The computers
in the TrustedHosts list might not be authenticated. The client might send credential
information to these computers. Are you sure that you want to modify this list?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
```

You can then use the Get-Item cmdlet to verify the result:

```
PS C:\> Get-Item wsman:\\localhost\Client\TrustedHosts


   WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Client

Type            Name                           SourceOfValue   Value
----            ----                           -------------   -----
System.String   TrustedHosts                                   SEA-SRV-1
```

Running the Get-WindowsFeature cmdlet now no longer throws an error:

```
PS C:\> Get-WindowsFeature -ComputerName SEA-SRV-1 -Credential SEA-SRV-1\Administrator

Display Name                                            Name               Install State
------------                                            ----               -------------
[ ] Active Directory Certificate Services               AD-Certificate         Available
    [ ] Certification Authority                         ADCS-Cert-Authority    Available
    [ ] Certificate Enrollment Policy Web Service       ADCS-Enroll-Web-Pol    Available
...
```

NOTE **TIPS FOR RUNNING SET-ITEM WSMAN:\LOCALHOST\CLIENT\TRUSTEDHOSTS**

If you need to add another remote server to the TrustedHosts list on your local computer, include the *–Concatenate* parameter when you use Set-Item the second time so that you don't end up overwriting the current contents of the list. You can also suppress the Yes/No prompt with the Set-Item cmdlet by adding the *–Force* parameter to it.

Preparing for deploying additional domain controllers in the new forest

Deploying additional domain controllers in a new forest is easier because you already have a domain environment, which means Windows PowerShell remoting will work without any further configuration. By running your Windows PowerShell commands from an existing Windows Server 2012 domain controller in your forest, or from a Windows 8 client computer on which the Remote Server Administration Tools for Windows 8 have been installed, you are able to deploy additional domain controllers to existing domains, install new child domains, and install new tree domains, as long as you have the appropriate credentials for the task you are going to perform.

Preparing for deploying domain controllers in an existing forest

Deploying Windows Server 2012 domain controllers in a forest whose domain controllers are running an earlier version of Windows Server can also be done using Windows PowerShell as follows:

1. Install a Windows Server 2012 server, and join the server to an existing domain.
2. Use the Install-WindowsFeature cmdlet to install the AD DS role together with its role-management tools as follows:

   ```
   Install-WindowsFeature -name AD-Domain-Services –IncludeManagementTools
   ```

3. Run commands from the ADDSDeployment module on the server to remotely install AD DS on other domain-joined Windows Server 2012 servers.

Using Windows PowerShell to deploy domain controllers

The Windows PowerShell cmdlets for installing a forest, installing domains, deploying domain controllers, and performing similar deployment tasks are found in the ADDSDeployment module. This Windows PowerShell module is installed by default when you add the AD DS role together with its role-management tools on a server, regardless of whether the server has been promoted to a domain controller or not. To see a list of the available cmdlets in this module, use the Get-Command cmdlet as follows:

```
PS C:\> Get-Command -Module ADDSDeployment

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Add-ADDSReadOnlyDomainControllerAccount            ADDSDeployment
Cmdlet          Install-ADDSDomain                                 ADDSDeployment
Cmdlet          Install-ADDSDomainController                       ADDSDeployment
Cmdlet          Install-ADDSForest                                 ADDSDeployment
Cmdlet          Test-ADDSDomainControllerInstallation              ADDSDeployment
Cmdlet          Test-ADDSDomainControllerUninstallation            ADDSDeployment
Cmdlet          Test-ADDSDomainInstallation                        ADDSDeployment
Cmdlet          Test-ADDSForestInstallation                        ADDSDeployment
Cmdlet          Test-ADDSReadOnlyDomainControllerAccountCreation   ADDSDeployment
Cmdlet          Uninstall-ADDSDomainController                     ADDSDeployment
```

Verifying prerequisites

You can use the Test-ADDS* cmdlets to run a prerequisites check before attempting to install a new forest, install a new domain, deploy a writeable domain controller, or deploy an RODC in your environment. The output of this command will help you determine whether your environment is ready for the operation you intend to perform or whether additional configuration might be required. The example here shows some output from running the Test-ADDSForestInstallation cmdlet on a standalone Windows Server 2012 server to determine whether the server satisfies the prerequisites for becoming the first domain controller of the forest root domain of a new forest:

```
PS C:\> Test-ADDSForestInstallation -DomainName corp.adatum.com
SafeModeAdministratorPassword: ********
Confirm SafeModeAdministratorPassword: ********
WARNING: Windows Server 2012 Release Candidate domain controllers have a default for the
security setting named "Allow cryptography algorithms compatible with Windows NT 4.0"
that prevents weaker cryptography algorithms when establishing security channel
sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: This computer has at least one physical network adapter that does not have
static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled
for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both
IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es)
assignment should be done to all the physical network adapters for reliable Domain Name
System (DNS) operation.

WARNING: A delegation for this DNS server cannot be created because the authoritative
parent zone cannot be found or it  does not run Windows DNS server. If you are
integrating with an existing DNS infrastructure, you should manually create a delegation
to this DNS server in the parent zone to ensure reliable name resolution from outside
the domain "adatum.com". Otherwise, no action is required.


Message                      Context                RebootRequired    Status
-------                      -------                --------------    ------
Operation completed succes... Test.VerifyDcPromo...            False   Success
```

To determine whether a remote Windows Server 2012 server satisfies these requirements, use the Invoke-Command cmdlet to execute the Test-ADDSForestInstallation cmdlet on the remote server as follows:

```
Invoke-Command -ComputerName SEA-SRV-1 {Test-ADDSForestInstallation -DomainName
corp.adatum.com}
```

First domain controller in new forest

Deploying the first Windows Server 2012 domain controller for a new forest is equivalent to installing a new forest and involves two steps:

1. Adding the AD DS role to the server.
2. Promoting the server as a domain controller.

Using Windows PowerShell, these actions can be combined into a single script you can execute on remote servers. The following scenario uses two standalone Windows Server 2012 servers: a local server named SEA-HOST-2 and a remote server named SEA-SRV-1. The goal is to run a script on SEA-HOST-2 that will install a new forest, with SEA-SRV-1 being the first domain controller in the forest root domain. To accomplish this, you could proceed as follows:

1. Begin by logging on to a local server running Windows Server 2012 using your administrator credentials, and open an elevated Windows PowerShell prompt. (If you are logged on with the built-in Administrator account, any Windows PowerShell prompt you open will be elevated.)
2. Change the script execution policy on the local server to RemoteSigned by running the following command:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

3. This will allow you to run Windows PowerShell scripts (.ps1 files) on the local server. By using Windows PowerShell remoting, you will also be able to run scripts on the remote server.
4. Open Notepad, and type the following two commands:

   ```
   Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
   Install-ADDSForest -DomainName corp.adatum.com -InstallDNS
   ```

   The first command installs AD DS together with the role-management tools on the targeted server. The second command promotes the targeted server as the first domain controller in the forest root domain corp.adatum.com. Note that the name of the targeted server has not been specified in this script. Use Notepad to save the script with the file name script1.ps1 in the folder C:\scripts or some other suitable location on the local server.
5. Run the following command on the local server to execute your script on the remote server SEA-SRV-1:

   ```
   Invoke-Command -ComputerName SEA-SRV-1 -FilePath C:\scripts\script1.ps1
   ```

6. When the AD DS role has finished installing on SEA-SRV-1, you will be prompted to specify a Safe Mode Administrator Password. This password is needed so that you can log on to the new domain controller in Directory Services Recovery Mode when needed. After entering a password and confirming it, press Y and then ENTER to

confirm that you want to promote the server as a domain controller. The promotion process begins, as shown in Figure 4-12. Note that you can eliminate the need to press Y followed by ENTER by including the *–Force* parameter in the second line of your script.

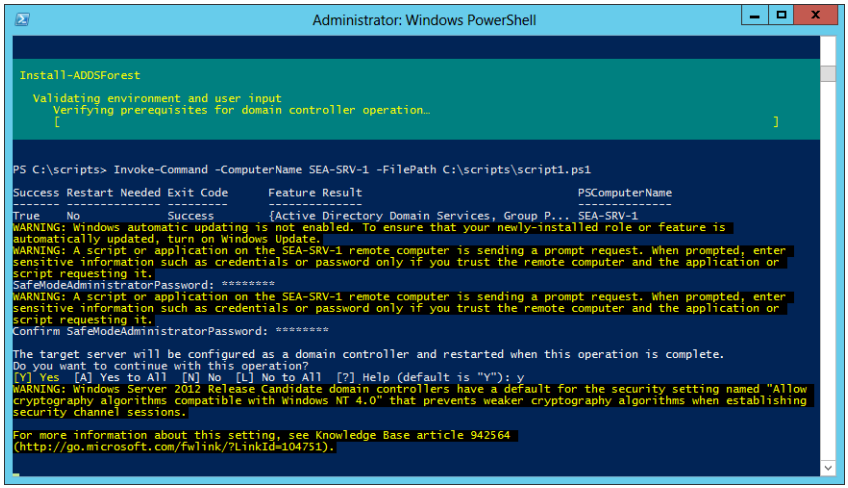


FIGURE 4-12 Remote server SEA-SRV-1 is now being promoted to be the first domain controller in a new forest.

7. Command output like the following will be displayed if the promotion process is successful:

```
PSComputerName : SEA-SRV-1
RunspaceId     : dd268942-f430-43c9-9830-7c547d1a4b73
Message        : Operation completed successfully
Context        : DCPromo.General.3
RebootRequired : False
Status         : Success
```

The server will then be restarted to complete the promotion process. If the remote server is a Server With A GUI installation, logging on to the server and launching Server Manager will confirm that the AD DS and DNS Server roles have been installed and the server is now the first domain controller in the corp.adatum.com forest.

Additional domain controller in domain

You can use the Install-ADDSDomainController cmdlet to install an additional domain controller in an existing domain. For example, the following command installs and promotes a new domain controller and DNS server in the corp.adatum.com domain using domain administrator credentials:

```
Install-ADDSDomainController -InstallDns -Credential `
(Get-Credential CORP\Administrator) -DomainName corp.adatum.com
```

You will be prompted to provide and confirm the Directory Services Restore Mode (DSRM) password during the installation process.

If you want to use local administrator credentials instead of domain administrator credentials for this process, omit the –*Credential* parameter as follows:

```
Install-ADDSDomainController -InstallDns -DomainName corp.adatum.com
```

If you want to be prompted to supply the credentials needed to install and promote the domain controller, use the following command instead:

```
Install-ADDSDomainController -InstallDns -Credential `
(Get-Credential) -DomainName corp.adatum.com
```

You can use the Invoke-Command cmdlet to install several additional domain controllers at once like this:

```
Invoke-Command -ComputerName SEA-SRV-2, SEA-SRV-3 -ScriptBlock `
{Install-ADDSDomainController -InstallDns -DomainName corp.adatum.com}
```

> ***NOTE*** **MULTIPLE LINE COMMANDS**
>
> **The backtick character is an escape character in Windows PowerShell that is appended to a line to indicate that the command continues on the next line.**

First domain controller in a child or tree domain

You can use the Install-ADDSDomain cmdlet to install a new child or tree domain in an existing forest by deploying the first domain controller for the new domain. For example, to install and promote a server to become the first domain controller of a child domain *hq* in the parent domain *corp.adatum.com*, use this command:

```
Install-ADDSDomain -Credential (Get-Credential CORP\Administrator) `
-NewDomainName hq -ParentDomainName corp.adatum.com -DomainType ChildDomain `
-InstallDNS -CreateDNSDelegation
```

For more information on the syntax for this command, use the Get-Help cmdlet.

Read-only domain controllers

You can use the Add-ADDSReadOnlyDomainControllerAccount cmdlet to create an RODC account that can be used to install an RODC in your forest. After the RODC account has been created, you can use the Install-ADDSDomainController cmdlet with the –*ReadOnlyReplica* parameter to deploy a new RODC in an existing domain. For more information on these cmdlets, use the Get-Help cmdlet.

MORE INFO **INSTALLING AND PROMOTING DOMAIN CONTROLLERS**

For additional examples and guidance concerning the deployment of domain controllers in different scenarios, see the following topics in the TechNet Library:

- **"Install Active Directory Domain Services" at *http://technet.microsoft.com/en-us/library/hh472162***
- **"AD DS Deployment Cmdlets in Windows PowerShell" at *http://technet.microsoft.com/en-us/library/hh974719***

See also Lesson 4 of Chapter 3.

Quick check

- **What do you need to do before you can use one standalone Windows Server 2012 server to remotely execute Windows PowerShell commands on another standalone Windows Server 2012 server?**

Quick check answer

- **Add the second server to the TrustedHosts list on the first server.**

Verifying domain-controller deployment

You can also use Windows PowerShell to verify the results of installing AD DS on remote servers and promoting them as domain controllers. For example, you can use the cmdlets of the BestPractices module to perform BPA scans on remote servers. To illustrate this and continue with the preceding scenario, begin by using Invoke-Command on local server SEA-HOST-2 to execute the Invoke-BPAModule cmdlet on remote server SEA-SRV-1:

```
PS C:\> Invoke-Command -ComputerName SEA-SRV-1 -ScriptBlock `
{Invoke-BpaModel -ModelId Microsoft/Windows/DirectoryServices}


ModelId           : Microsoft/Windows/DirectoryServices
SubModelId        :
Success           : True
ScanTime          : 6/20/2012 9:30:05 PM
ScanTimeUtcOffset : -07:00:00
Detail            : {SEA-SRV-1, SEA-SRV-1}
```

You can then execute the Get-BPAResult cmdlet on the remote server to display the results of the scan you performed using this command:

```
PS C:\> Invoke-Command -ComputerName SEA-SRV-1 -ScriptBlock `
{Get-BpaResult Microsoft/Windows/DirectoryServices}
```

The output from this command will be quite extensive, so you might try piping it into the Where-Object cmdlet to display only results whose severity level is Error:

```
PS C:\Users\Administrator> Invoke-Command -ComputerName SEA-SRV-1 -ScriptBlock `
{Get-BpaResult Microsoft/Windows/DirectoyServices} | Where-Object Severity -eq Error


ResultNumber   : 28
ResultId       : 513979436
ModelId        : Microsoft/Windows/DirectoryServices
SubModelId     :
RuleId         : 36
ComputerName   : SEA-SRV-1
Context        :
Source         : SEA-SRV-1
Severity       : Error
Category       : Configuration
Title          : The PDC emulator master SEA-SRV-1.corp.adatum.com in this forest should
                 be configured to correctly synchronize time from a valid time source
Problem        : The primary domain controller (PDC) emulator operations master in this
                 forest is not configured to correctly synchronize time from a valid
                 time source.
Impact         : If the PDC emulator master in this forest is not configured to
                 correctly synchronize time from a valid time source, it might use its
                 internal clock for time synchronization. If the PDC emulator master in
                 this forest fails or otherwise becomes unavailable (and if you have not
                 configured a reliable time server (GTIMESERV) in the forest root
                 domain), other member computers and domain controllers in the forest
                 will not be able to synchronize their time.
Resolution     : Set the PDC emulator master in this forest to synchronize time with a
                 reliable external time source. If you have not configured a reliable
                 time server (GTIMESERV) in the forest root domain, set the PDC emulator
                 master in this forest to synchronize time with a hardware clock that is
                 installed on the network (the recommended approach). You can also set
                 the PDC emulator master in this forest to synchronize time with an
                 external time server by running the w32tm /config /computer:SEA-SRV-
                 1.corp.adatum.com /manualpeerlist:time.windows.com
                 /syncfromflags:manual /update command. If you have configured a
                 reliable time server (GTIMESERV) in the forest root domain, set the PDC
                 emulator master in this forest to synchronize time from the forest root
                 domain hierarchy by running w32tm /config
                 /computer:SEA-SRV-1.corp.adatum.com /syncfromflags:domhier /update.
Compliance     :
Help           : http://go.microsoft.com/fwlink/?LinkId=142195
Excluded       : False
PSComputerName : SEA-SRV-1
```

MORE INFO **USING THE BESTPRACTICES MODULE**

For more information on how to use Windows PowerShell to perform BPA scans, see the topic "Run Best Practices Analyzer Scans and Manage Scan Results" in the TechNet Library at *http://technet.microsoft.com/en-us/library/hh831400.aspx*.

Uninstalling AD DS

Finally, you can use the Uninstall-ADDSDomainController cmdlet to remove the AD DS role and demote a domain controller to a member server in the domain. You will be prompted to set and confirm the local Administrator password before the completion of the removal process. For more information on using this cmdlet, use the Get-Help cmdlet.

Lesson summary

- Windows PowerShell can be used to deploy Windows Server 2012 domain controllers. This procedure is mainly intended for large enterprises, data centers, and cloud-computing environments where automation of this process is a requirement.
- You can use Windows PowerShell to install and promote a remote standalone server running Windows Server 2012 to a domain controller after taking some preparatory steps to enable Windows PowerShell remoting to work properly in a workgroup environment.
- To use Windows PowerShell to install the AD DS role on a remote server, use the Invoke-Command cmdlet to remotely execute the Install-WindowsFeature cmdlet.
- To use Windows PowerShell to promote a remote server that already has the AD DS role installed, use the Invoke-Command cmdlet to remotely execute the appropriate cmdlet from the ADDSDeployment module.
- To use Windows PowerShell to run a prerequisites check before attempting to install a new forest, install a new domain, deploy a writeable domain controller, and use the Test-ADDS* cmdlets from the ADDSDeployment module.
- To use Windows PowerShell to run a Best Practices Analyzer scan on remote servers after installing AD DS and promoting them to domain controllers, use the Invoke-Command cmdlet to remotely execute the appropriate cmdlet from the BestPractices module.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following Windows PowerShell commands adds the remote server SRV-A to the TrustedHosts list on the local server?
   - **A.** Get-Item wsman:\localhost\Client\TrustedHosts –Value SRV-A
   - **B.** Set-Item wsman:\localhost\Client\TrustedHosts –Value SRV-A
   - **C.** Get-Item wsman:\localhost\Server\TrustedHosts –Value SRV-A
   - **D.** Set-Item wsman:\localhost\Server\TrustedHosts –Value SRV-A

2. Which of the following is not a cmdlet from the ADDSDeployment module?
   - **A.** Install-ADDSDomain
   - **B.** Install-ADDSDomainController
   - **C.** Uninstall-ADDSDomainController
   - **D.** Get-ADForest
3. Which Windows PowerShell command should you use to run a prerequisites check before attempting to deploy an additional domain controller in an existing forest?
   - **A.** Install-ADDSDomainController –Prerequisites
   - **B.** Invoke-BpaModel –ModelId Microsoft/Windows/DirectoryServices
   - **C.** Test-ADDSDomainControllerInstallation
   - **D.** Install-ADDSDomainController –Whatif

Practice exercises

The goal of this section is to provide you with hands-on practice with the following:

- Deploying domain controllers using Server Manager
- Deploying domain controllers using Windows PowerShell

To perform the following exercises, you need two clean installations of Windows Server 2012: one installed using the Server With A GUI installation option, and the other installed using the Server Core installation option. The servers should be standalone servers belonging to a workgroup, have Internet connectivity, and have no additional roles or features installed. For the purposes of these exercises, the name of the first server (the Server With A GUI installation) is assumed to be SERVER1, and the name of the second server (the Server Core installation) is assumed to be SERVER2. You should be logged on interactively to SERVER1 using the built-in local Administrator account.

NOTE **SWITCHING TO SERVER CORE**

If your SERVER2 is a Server With A GUI installation, you can switch it to a Server Core installation by running the following Windows PowerShell command on it:

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra –Restart
```

Exercise 1: Installing a new forest using Server Manager

In this exercise, you will install a new forest named corp.contoso.com by using Server Manager to install AD DS on SERVER1 and promote the server as a domain controller.

1. Log on to SERVER1 using the built-in Administrator account, and open Server Manager if it doesn't open automatically.
2. Use the Dashboard to verify that SERVER1 is in a healthy state before proceeding further.
3. Use Server Manager to launch the Add Roles And Features Wizard, and install the Active Directory Domain Services role on the server, including the administration tools for this role. Close the Add Roles And Features Wizard upon completion of the role installation.
4. Use the Notification flag on the Server Manager menu to perform the post-deployment configuration task of promoting the server to a domain controller using the Active Directory Domain Services Configuration Wizard.
5. Select the Add A New Forest option on the first page of the AD DS Configuration Wizard, and create a new forest root domain named corp.contoso.com. Make appropriate selections for the remaining items in the wizard's pages.
6. On the Review Options page, click View Script and examine the Windows PowerShell script that the wizard will be executing. Make sure you understand the syntax of the command by looking up the help page for the command in the TechNet Library.
7. After reviewing the results on the Prerequisites Check page, click Install to promote SERVER1 to be the first domain controller in the new forest.
8. After the server reboots, log on using the default domain administrator account and open Server Manager if it doesn't open automatically.
9. Use the Dashboard to examine any alerts that are raised for your new domain controller.
10. Select the AD DS page of Server Manager, and review the Roles And Features tile at the bottom of the page to verify that the AD DS role has been installed on SERVER1.
11. Also on the AD DS page, review any critical, error, or warning events raised in the Events tile.
12. Also on the AD DS page, review the status of the services on SERVER1.
13. Also on the AD DS page, initiate a BPA scan of SERVER1 and review the results of this scan once it finishes.
14. Close Server Manager when you are finished.

Exercise 2: Remotely adding an additional domain controller using Windows PowerShell

In this exercise, you will join SERVER2 to the corp.contoso.com domain and then use Windows PowerShell from SERVER1 to remotely deploy SERVER2 as an additional domain controller in your domain.

1. Log on locally to SERVER2 using the built-in local Administrator account. A command prompt window should be visible.
2. Type **Sconfig** in the command prompt window, and press Enter to run the Server Configuration Tool (Sconfig.cmd).
3. Type **8** and press Enter to access the Network Adapter Settings page of the Configuration Tool. You are presented with a list of available network adapters that are attached to the server.
4. Type the index number of the adapter that you want to configure, and then press Enter. You are presented with the current configuration for the network adapter that you selected.
5. Type **2** and press Enter to configure DNS Server settings for the selected network adapter.
6. Type the IP address for SERVER1 as the new preferred DNS server, and press Enter. Then click OK in the dialog box that appears.
7. Press Enter to indicate that you will not be specifying an alternate DNS server.
8. The Configuration Tool returns you to the Network Adapter Settings page. Review the information on this page, and make sure it is correct before proceeding. Then type **4** and press Enter to return to the Main Menu page.
9. Type **1** and press Enter, and then type **D** and press Enter to indicate that you want to join SERVER2 to a domain.
10. Type **corp.contoso.com** as the name of the domain you want SERVER2 to join, and then press Enter.
11. Type **CORP\Administrator** as the name of an authorized user for performing the domain join operation and then press Enter. (If you specified a different NetBIOS name for your domain in Exercise 1, use that name instead of CORP.)
12. In the new command prompt that opens, type the password associated with the user account you specified in the previous step and press Enter.
13. In the Change Computer Name dialog box that opens, click No.
14. In the Restart dialog box that opens, click Yes.
15. After SERVER2 has restarted, log on again using the local Administrator account and run the Server Configuration Tool again to verify that the server has successfully joined the domain. Then exit the Configuration Tool and switch to using SERVER1 for the remainder of this exercise.
16. Log on to SERVER1 with the default domain administrator account, and close Server Manager if it opens automatically.

17. Open a Windows PowerShell prompt on SERVER1.
18. Use the Invoke-Command cmdlet together with the Get-WindowsFeature cmdlet to remotely review the installed roles and features on SERVER2. Verify that the AD DS role is not yet installed on SERVER2.
19. Use Invoke-Command together with Install-WindowsFeature to remotely install the AD DS role on SERVER2. Once this is done, use Get-WindowsFeature to confirm the installation.
20. Use the following command to remotely run a prerequisites check on SERVER2 to make sure the server is ready for being promoted to a domain controller:

```
Invoke-Command -ComputerName SERVER2 -ScriptBlock `
{Test-ADDSDomainControllerInstallation -DomainName corp.contoso.com `
-Credential (Get-Credential CORP\Administrator)}
```

    Review the results returned from the prerequisites check before proceeding.
21. Use the following command to remotely promote SERVER2 as an additional domain controller in the corp.contoso.com domain:

```
Invoke-Command -ComputerName SERVER2 `
{Install-ADDSDomainController -InstallDNS `
-Credential (Get-Credential CORP\Administrator) `
-DomainName corp.contoso.com}
```

22. When the promotion operation finishes, wait for SERVER2 to reboot. Then open Server Manager on SERVER1 and add SERVER2 to the server pool.
23. Use the Tools menu of Server Manager to launch the Active Directory Users And Computers console, select the Domain Controllers container under corp.contoso.com, and verify that SERVER2 is now a domain controller for this domain.

Suggested practice exercises

The following additional practice exercises are designed to give you more opportunities to practice what you've learned and to help you successfully master the lessons presented in this chapter.

- **Practice 1** Continue with the preceding exercises by first using Windows PowerShell to demote SERVER2 and remove AD DS, followed by using Server Manager to demote SERVER1 and remove AD DS to retire the forest.
- **Practice 2** Perform a clean install of Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003, add the AD DS role, and promote the server as the first domain controller in the new forest root domain adatum.com. Use the Adprep.exe tool on your Windows Server 2012 installation media to update the schema, and prepare the forest for deploying Windows Server 2012 domain controllers. Then perform an in-place upgrade of the first domain controller to Windows Server 2012.

Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct answer: A**
   - **A. Correct**: Having only one writeable domain controller in a domain is not a best practice. You should have at least two writeable domain controllers in each domain so that if one of them fails, users will still be able to log on and you will still be able to perform AD DS management tasks.
   - **B. Incorrect**: Making sure that each site in your domain has a sufficient number of domain controllers to service the needs of users for logging on and accessing network resources is a best practice.
   - **C. Incorrect**: Keeping the design of your forest simple by having only one domain is a best practice.
   - **D. Incorrect**: Installing only the AD DS and DNS Server roles on your domain controllers and no other server roles is a best practice.
2. **Correct answers: A, B, and C**
   - **A. Correct**: The fully-qualified domain name (FQDN) for the root domain of your new forest is required information when planning the deployment of the first domain controller in a new forest.
   - **B. Correct**: The forest and domain functional levels is required information when planning the deployment of the first domain controller in a new forest.
   - **C. Correct**: The location for the AD DS database, log files, and SYSVOL folder is required information when planning the deployment of the first domain controller in a new forest.
   - **D. Incorrect**: There is no Domain Admins security group if you haven't yet deployed the first domain controller in a new forest. Instead, you need the credentials of a member of the local Administrators security group on the server being promoted to a domain controller.
3. **Correct answers: A and D**
   - **A. Correct**: Creating a DNS delegation is not a required step for AD DS deployments if no external DNS servers will be used to reference the FQDN of your organization's internal forest.
   - **B. Incorrect**: A best practice is for all domain controllers in a domain to have the DNS Server role installed and configured to ensure high availability in distributed environments

C. **Incorrect**: A best practice is for all domain controllers in a domain to be configured as global catalog servers to ensure high availability in distributed environments.

D. **Correct**: Read-only domain controllers require that there be at least one writeable domain controller running Windows Server 2008 or later installed in the domain. Having only writeable domain controllers running Windows Server 2003 is insufficient.

Lesson 2

1. **Correct answer: C**

   A. **Incorrect**: You need to run the Add Roles And Features Wizard to install the AD DS role on the server before you can run the AD DS Configuration Wizard to promote the server to a domain controller.

   B. **Incorrect**: The Add Roles And Features Wizard is used to install the AD DS role on a server, not to promote the server to a domain controller.

   C. **Correct**: This is the correct procedure.

   D. **Incorrect**: The Add Roles And Features Wizard is used to install the AD DS role on a server, not to promote the server as a domain controller. And the AD DS Configuration Wizard is used to promote a server to a domain controller, not to install the AD DS role on the server.

2. **Correct answer: A and C**

   A. **Correct**: When you use the AD DS Configuration Wizard to deploy the first Windows Server 2012 domain controllers in a domain of a forest whose domain controllers are running earlier Windows Server versions, the Adprep tool automatically runs to prepare the forest and domain by extending the schema to its latest version.

   B. **Incorrect**: Add A Domain Controller To An Existing Domain is the correct option to select on the Deployment Configuration page of the AD DS Configuration Wizard to deploy the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server.

   C. **Correct**: Install From Media (IFM) does not work across different operating system versions. In other words, you must use a Windows Server 2012 domain controller to generate installation media to use for another Windows Server 2012 domain controller installation. Since this is the first Windows Server 2012 domain controller you are deploying in your environment, you cannot use IFM.

   D. **Incorrect**: You can specify different credentials on the Deployment Configuration page of the AD DS Configuration Wizard if your current logon credentials have insufficient privileges to deploy the first Windows Server 2012 domain controller in an existing forest running an earlier version of Windows Server.

3. **Correct answer: D**

   A. **Incorrect**: This command is missing the *–scope* base parameter and therefore will not return the correct result.

B. **Incorrect**: This command will return the value of the *sAMAccountName* attribute, which has nothing to do with the schema level.

C. **Incorrect**: This command will work because it will return the values of all attributes for the specified LDAP path, including the desired attribute *objectVersion*, but it is not the best syntax because it returns too much unnecessary information.

D. **Correct**: This is the correct command syntax to verify whether Adprep has successfully extended your forest's schema.

Lesson 3

1. **Correct answer: B**

   A. **Incorrect**: This command will display the contents of the TrustedHosts list on the local server.

   B. **Correct**: This is the correct command syntax.

   C. **Incorrect**: You need to use Set-Item, not Get-Item, to configure the TrustedHosts list on the local server. In addition, the wsman:\ path is incorrect in this command—it should be wsman:\localhost\Client\TrustedHosts.

   D. **Incorrect**: The wsman:\ path is incorrect in this command—it should be wsman:\localhost\Client\TrustedHosts.

2. **Correct answer: D**

   A. **Incorrect**: Install-ADDSDomain is a cmdlet from the ADDSDeployment module.

   B. **Incorrect**: Install-ADDSDomainController is a cmdlet from the ADDSDeployment module.

   C. **Incorrect**: Uninstall-ADDSDomainController is a cmdlet from the ADDSDeployment module.

   D. **Correct**: Get-ADForest is not a cmdlet from the ADDSDeployment module; it is a cmdlet from the ActiveDirectory module.

3. **Correct answer: C**

   A. **Incorrect**: The Install-ADDSDomainController cmdlet doesn't have a *–Prerequisites* parameter.

   B. **Incorrect**: This command will perform a BPA scan on the server and is intended for use after the server has been promoted as a domain controller, not before.

   C. **Correct**: This is the correct command because it runs only the prerequisites check for deploying a domain controller.

   D. **Incorrect**: This command only summarizes the changes that would occur during the deployment process; it doesn't actually test whether those changes are possible given the current environment as the Test-ADDSDomainControllerInstallation command does.

Index

Symbols

0:0:0:0:0:0:0:0 address, 267
6to4, 276
128-bit (16-byte) addresses, 263–264. *See also* IPv6

A

absent binaries. *See also* binaries
access-based enumeration, 388
access policies, central, 196
account lockout policies, 202
Accounts: Block Microsoft accounts policy, 478, 481
ACT (Application Compatibility Toolkit), 28, 29, 35
Active Directory
  ADAC, administering with, 184–197
  administering, 183–223
  administering with Windows PowerShell, 208–217
  browsing, 186
  bulk management, 190
  deleted objects, restoring, 200–201
  directory objects, states, 198–199, 207
  Dynamic Access Control, 196
  fine-grained password policies, configuring, 202–206
  Group Policy and, 469–472
  OUs, creating, 190–193
  schema upgrades, 5
  searching, 188–189
  servers, searching in, 95
  user accounts, managing, 208–211
  users, creating, 193–195
  Windows PowerShell administration cmdlets, 212–213
Active Directory Administrative Center (ADAC). *See* ADAC (Active Directory Administrative Center)
Active Directory Domains And Trusts MMC snap-in, 221
Active Directory Domain Services (AD DS). *See* AD DS (Active Directory Domain Services)
Active Directory Domain Services role, 146
  installing, 150–151, 163, 169, 176, 221
  uninstalling, 174
Active Directory environments
  domain controllers, deploying, 139
  Group Policy, planning and implementing, 466–488
  private cloud, migrating into, 9
  Windows Server 2012 features, implementing in, 7
Active Directory Sites And Services MMC console, 215
Active Directory Users And Computers snap-in, 184
active store, 575
ADAC (Active Directory Administrative Center), 184–197
  Active Directory, searching, 188–189
  Add Navigation Nodes explorer, 193
  AD Recycle Bin, enabling, 198–201
  advanced search queries, 189
  Breadcrumb bar, 185
  Column Explorer, 186, 220
  Create Organizational Unit properties page, 190–191
  Create User properties page, 193–194
  directory objects, creating, 197
  fine-grained password policies, configuring, 202–206
  list view, 186–187
  list view, customizing, 191–192
  Management list, 185
  Most Recently Used (MRU) list, 186, 197, 220–221
  navigation nodes, 220

Navigation pane, 185, 220
OUs, creating, 190–193
password settings, viewing, 205–206
Preview pane, 185
properties pages, 191
tasks allowed, 195, 197
tasks disallowed, 196, 197
Tasks pane, 185
Tree view, 187
user accounts, creating, 193–195
user-interface features, 185–186
Windows PowerShell History Viewer, 185, 193–194
Add-ADDSReadOnlyDomainControllerAccount cmdlet, 171
Add-DhcpServerv4ExclusionRange cmdlet, 254
Add-DhcpServerv4Failover cmdlet, 283
Add-DhcpServerv4Reservation cmdlet, 254
Add-DhcpServerv4Scope cmdlet, 254, 282
Add-DnsServerForwarder cmdlet, 256, 285
Add-DnsServerResourceRecordA cmdlet, 255
Add-DnsServerStubZone cmdlet, 256
Add Navigation Nodes explorer, 193
Add-Printer cmdlet, 456
Add Printer Device Wizard Printer Driver Selection page, 441
Add-PrinterDriver cmdlet, 455, 463
Add Printer Driver Wizard, 441
Add-PrinterPort cmdlet, 455, 463
Add/Remove Servers dialog box, 437
addresses, IPv6, 259
address leases, replicating, 227
Add Roles And Features Wizard, 110–113, 150–151, 161, 163, 180, 304–305, 373–374, 432
Confirm Installation Selections page, 112
Hyper-V Module For Windows PowerShell option, 305
Hyper-V server role, installing with, 306
Remove Server Roles page, 161
Select Destination Server page, 111
Select Features Page, 112
Select Installation Type page, 110
Select Server Roles page, 111–112, 402
Specify An Alternate Source Path link, 113
AD DS (Active Directory Domain Services), 135
Adprep functionality, 5, 34
database location, 140, 147, 153, 179
deployment scenarios, 136–139
directory structure, planning, 137
existing forest deployment, 144–146
log files location, 140, 147, 153, 179
new forest deployment, 139–144. *See also* new forests
planning process, 137
resources for planning and design, 138
schema, extending, 145, 148–149, 163
uninstalling, 159–162, 174
validation before installation, 5–10, 34
AD DS Configuration Wizard (dcpromo.exe), 135, 151–157
additional domain controllers, deploying, 154–156
Additional Options page, 153, 155
Adprep tool, 180
Credentials page, 162
Deployment Configuration page, 152, 154, 156
DNS Options page, 153, 155
Domain Controller Options page, 152, 154
domain controllers, forcing removal, 162
existing forest, adding domain controllers to, 156–157
first domain controller in new forest, promoting, 152–153
Install From Media (IFM) option, 155, 156
Paths page, 153
Preparation Options page, 157
Prerequisites Check page, 153
Review Options page, 153
Windows PowerShell scripting of, 153–154
ADDSDeployment module, 167, 175, 181
AD DS Design Guide, 4, 138
Add-VMHardDiskDrive cmdlet, 329
Add-VMNetworkAdapter cmdlet, 334
Add-VMStoragePath cmdlet, 357
Add-WindowsFeature cmdlet, 118
–IncludeAllSubFeature parameter, 133
ADK (Windows Assessment and Deployment Kit) for Windows 8, 52
components, choosing, 55
installing, 55
.adm files, 472
administrator scope of authority, 135
ADML format, 472
ADMX format, 472

Adprep.exe, 5, 145, 148–150, 180–181
integration with AD DS, 5
requirements for, 149
schema extension, verifying, 163–168
syntax, 149, 163
Adprep /forestprep command, 149
AD Recycle Bin
enabling, 221, 222
enabling with ADAC, 195, 198–201
enabling with Windows PowerShell, 200, 207
functionality, 198
using, 200–201
advanced SMB shares, 389, 396, 427
alerts, 86–87
configuring, 98
event alerts, 100–101
managing, 127–128
performance alerts, 104
service alerts, 102
All Servers page (Server Manager), 88–90, 107, 130
All Servers tile (Server Manager), 86
AMD NX bit, 293
AMD Virtualization (AMD-V) technologies, 293
anti-replay protection, 544
anycast IPv6 addresses, 265
APIPA (Automatic Private IP Addressing), 266
Application Compatibility Toolkit (ACT). *See* ACT (Application Compatibility Toolkit)
application partitions, removing, 161
applications, importing, 60
applications SMB shares, 389, 396, 427
AppLocker, 480, 481
Armstrong, Ben, 310, 346
ARP spoofing, 332–333
assessment of readiness for migration, 12, 19–29
with Application Compatibility Toolkit, 28
manual, 19–22
with MAP Toolkit, 22–27
with System Center Configuration Manager, 27–28
with third-party products, 28
with Windows Server Catalog, 21–22
Audit Removable Storage policy, 479–480
authenticated denial of existence, 236
Authenticated IP (AuthIP), 545
authentication, 234
authenticated bypass, 562–565
Challenge Handshake Authentication Protocol (CHAP), 407, 428
claims-based, 196
data-origin, 544
first, 546, 554
IPsec methods, 546–547, 576
IPsec settings, 552
negotiation of methods, 545
of network connections, 543
Remote Authentication Dial-In User Service (RADIUS), 412, 428
requirements, configuring, 557, 560, 570, 577
second, 546–547
authentication exemption connection security rules, 555, 577
creating, 558
Authentication Header (AH), 544
authoritative servers, 238
authority
administrator scope of, 135
of data, confirming, 236
delegation of, 135
autoconfiguration of addresses, 268, 280–281
stateful, 274
stateless, 273, 290
Automatic Private IP Addressing (APIPA), 266
automation
of deployment process, 61–62
of domain controller deployment, 135, 164–175
of server management, 119–125
of server management operational tasks, 83
availability
of Hyper-V hosts, 300–301
of storage system, 371–372

B

background jobs, 119–120, 125
managing, 133–134
scheduling, 120–121
Backup-GPO cmdlet, 491–493
backups
of GPOs, 487, 491–493, 512
of Hyper-V hosts, 302–303
bandwidth management, 69, 71, 344–345, 354–355
best practices
for infrastructure migration, 10–17
for new forest deployments, 138–139

Best Practices Analyzer (BPA), 87
domain controllers, scanning, 158, 173
binaries
removing, 38, 78
for roles and features, 108–109
source, specifying, 116
UNC path to, 113
Windows Update, downloading from, 108, 116, 118, 133
BIOS, compatibility with deployed operating system, 62, 66, 80
block storage. *See also* iSCSI storage
sharing, 397
boot disks, 375
boot media, 63
preparing, 65, 80
boot process security, 518
boot-time filters, 518
BPA Results thumbnail (Server Manager), 87
BranchCache, 388, 389
Branch Office Direct Printing, 443
breadcrumbs, 84
build labs, 37, 48
automating, 63
components, 48–50, 53
preparing, 47–53
setting up, 48–50, 53
bulk user account creation, 210–211, 216

C

caching-only DNS servers, 283–285
caching shares, 388
central store
creating, 472
functionality, verifying, 475
certificates, 546–547
Challenge Handshake Authentication Protocol (CHAP), 407, 428
change management, 27–28
change notification, enabling, 214
CHAP (Challenge Handshake Authentication Protocol), 407, 428
Checkpoint-VM cmdlet, 349
child domains, 141–142, 171
CIA triad (Confidentiality, Integrity, and Availability), 236
claims-based authentication, 196
Clear-DnsServerCache cmdlet, 256, 284
Client for NFS, 388
client-side extensions (CSEs), 493
cloud computing, 8
service models, 8–9
virtualized domain controllers, 144
cluster shared volume (CSV) shared storage, 295
Compare-VM cmdlet, 324
computer certificates, 546
computer health certificates, 547
computers
authentication, exempting from, 555, 558, 577
isolating, 555–558, 577
main mode cryptographic sets, viewing, 554, 573
confidentiality
of data, 236
of IP payload, 544
configuration
Group Policy policies and, 468
managing, 27–28
Configure Failover Wizard, 230
Configure-SMRemoting command, 91–92, 94
connection security, 543–548
connection security rules, 526, 543, 555–569, 573
authentication exemption rules, 555, 558, 577
authentication options, 570
configuring with Windows PowerShell, 561–562
custom rules, 556, 561, 570, 577
enabling, 558
isolation rules, 555–558, 561, 577
server-to-server rules, 556, 559, 570, 577
tunnel rules, 556, 559–560
types, 555–556
ConnectionSecurityVerbose operational log, 569
Connect-IscsiTarget cmdlet, 416
Connect-PSSession cmdlet, 122, 134
Connect To Target dialog box, 414
Control Panel Settings extensions for Group Policy preferences, 495, 506–507
ConvertFrom-SecureString cmdlet, 223
ConvertTo-SecureString cmdlet, 223
–Force parameter, 223
Convert-VHD cmdlet, 347
Create Organizational Unit properties page, 190–191
Create Server Group dialog box, 96
Create User properties page, 193–194

CSEs (client-side extensions), 493
CSV format, 211, 222
custom connection security rules, 556, 570, 577
  creating, 561
custom firewall rules, 529, 542, 576
  creating, 532–534
customizations, per-user vs. per-machine, 48, 50
CustomSettings.ini file, 64
  editing, 63

D

DAC (Dynamic Access Control), 6, 195–196
DAS (Direct Attached Storage), 361
  for Hyper-V hosts, 297
data archiving, 368
data centers
  traditional, 8
  virtualizing, 8
data encryption. *See* encryption
Data Execution Prevention (DEP), 293
data integrity, 544, 547–548, 576
  algorithms, 547–548
data protection
  disk-based and tape-based, 302–303
  IPsec settings, 551
dcpromo.exe, 135. *See also* AD DS Configuration Wizard (dcpromo.exe)
Default Domain Policy Group Policy Object (GPO), 202, 203
default firewall rules, 527
Delegation Signer (DS) resource records, 238
Deleted object state, 199–200, 221
DEP (Data Execution Prevention), 293
deployment
  client operating system–initiated, 70
  of domain controllers, 135–181
  greenfield, 4, 34
  of Hyper-V hosts, 292–316
  multicast, 69
  offline, 70
  of print servers, 432–435
  of servers, 37–82
  of Storage Spaces, 362–376
  unattended, 70, 71
  of virtual machines, 316–338
deployment infrastructure
  setting up, 67–68
  Windows Deployment Services in, 68
deployment shares
  applications, importing, 60
  configuration files, 61
  creating, 56–57
  device drivers, importing, 58–59
  linked, 69, 80
  Monitoring node, 57
  packages, importing, 60
  updating, 63, 66, 80
Deployment Workbench, 57
  Linked Deployment Shares feature, 69
  operating system source files, importing, 57–58
  Out-of-Box Drivers folder, 59
Desktop Experience, 41
destination servers, 14
  Migration Tools, installing, 15–16
device drivers
  availability reporting, 69, 71
  finding, 59
  importing, 58–59
DHCP availability. *See also* DHCP failover
  ensuring, 226–234
  previous approaches, 226–227, 233
DHCP console, 231
DHCP (Dynamic Host Configuration Protocol), 226
  stateful address autoconfiguration, 274
DHCP failover, 7, 227–229, 233, 286
  hot-standby mode, 228, 233–234, 286–287
  implementing, 229–231
  limitations of, 227
  load-sharing mode, 228, 233, 283, 286
  managing, 231–232
  Windows PowerShell, configuring with, 231, 282–283
DHCP Guard, 333, 338, 358
DHCP packets, 227
DHCP relay agents, 227, 228
DHCP Server role, 225
  installing, 282
DHCP servers
  Active Directory, authorizing in, 229, 282
  addresses, acquiring from, 283
  availability, 226–234
  in build lab, 49
  lease renewal requests, 226

managing, 253–255
scopes, configuring, 229–230
scopes, viewing, 254
subnets, locating in, 227
DHCPv6, 274
client software, 274
DHCPv6 servers, 280, 290
configuring, 274–276
differencing virtual hard disks, 321
merging, 346
reconnecting, 346
Diffie-Hellman Group 1 (DH Group 1), 545
Diffie-Hellman Group 2 (DH Group 2), 546, 555
Diffie-Hellman Group 14 (DH Group 14), 546, 570
Diffie-Hellman Group 24 (DH Group 24), 546
DirectAccess, 12
Direct Attached Storage (DAS), 297, 361
directory objects
creating, cmdlets for, 212
deleted, restoring, 200–201
states, 198–199, 201, 207
Directory Services Restore Mode (DSRM), 169
administrator account, 153
DisabledComponents registry value, 262–263
Disable-NetAdapterBinding cmdlet, 253, 257, 288
Disable-NetAdapter cmdlet, 253, 288
disaster recovery of Hyper-V hosts, 302–304
disconnected sessions, 121–123
Disconnect-PSSession cmdlet, 134
Discover Target Portal dialog box, 412–413
DiskPart, 376, 425
DiskRAID, 376, 425
Diskshadow.exe, 303
Distributed File System Replication, 69
Distributed Scan Server role service, 433
DNS64, 277
DNS cache poisoning, 236
DNS delegation, 142, 153, 155, 160, 179
DNS (Domain Name System)
administration tasks, cmdlets for, 256
querying, 95
DNS Public Key (DNSKEY) resource records, 238, 243
DNS resource records
adding, 255–256
removing, 256
DNSSEC (DNS Security Extensions), 234–243, 288
benefits, 235–236
deploying, 239–243
functionality, 237–239
key management, 240–241
previous versions, 237
resource records, 238
security between DNS clients and DNS servers, 242–243, 288
validation step, 238–239, 243, 287
DNS server cache
clearing, 284
contents, displaying, 284
DNS Server role, 138, 146, 147, 152, 225
installing, 141, 283
removing, 159–161
DNS servers
caching-only, configuring, 283–285
forwarders, 285
managing, 255–256
zones, viewing, 255
DnsServer Windows PowerShell module, 256
DNS zones. *See also* zones
removing, 160
signing, 239
Domain Admins security group, 142–144
domain controllers
Active Directory Domain Services role, 150. *See also* Active Directory Domain Services role
additional, 142, 145, 154–156, 167, 170–171, 177–178
Best Practices Analyzer scans, 158, 173
dedicated servers, 138
demoting, 159–161, 174
deploying, 135–181
deployment, credentials for, 144
deployment in existing forests, 144–146, 148–149, 156–157, 163, 167
deployment in new forests, 139–144, 148, 152–156, 162–166, 168–169
deployment, virtualizing, 135
deployment with Server Manager, 147–163
deployment with Windows PowerShell, 164–175
DNS delegation options, 153. *See also* DNS delegation
DNS servers, 141, 147, 152
first in new domains, 141–142, 154–156
first in new forests, 140–141, 164–166
flexible single master operations roles, 145
forcing removal, 162
forest root, 137

global catalog servers, 142, 147, 153
installation, verifying, 157–159, 172–173
Install From Media (IFM) option, 155–156
key masters, 240
listing, 214
moving between sites, 215
number of, 138, 146
purposes of, 137
read-only, 137, 143, 171, 179
at remote sites, 139
replication partners, 155
selecting, 195
SYSVOL folder, 472
upgrading, 144–146
validation phase, 141
virtualized, 137, 143–144
Windows Server 2012, 7
writable, 138, 179
domain firewall profiles, 521, 542
domain functional levels, 35
for fine-grained password policies, 204
raising, 6, 195
specifying, 140, 147, 152, 179
Domain Name System (DNS). *See* DNS (Domain Name System); DNS Server role
domain network location, 519
domains, 135
account lockout policies, 202
additional domain controllers, installing, 170–171
central store, creating, 472
child, 141–142
creating, 221
first domain controller, deploying, 141–142, 154–156
forests, removing from, 160
GPOs, linking to, 484
installing, 171
last domain controller, demoting, 160–161
number of, 139
password policies, 202
selecting, 195
sites, listing, 214
Starter GPOs folder, 473
tree, 141–142
trusts, 221
drive maps, 501–503
driver incompatibilities, 59
Dsquery.exe, 150, 163
Dynamic Access Control (DAC), 6
configuring, 195–196
dynamically expanding virtual hard disks, 320, 338
shrinking, 345
dynamic disks, and Storage Spaces, 365
Dynamic Host Configuration Protocol (DHCP), 226, 274. *See also* DHCP availability; DHCP failover; DHCP Server role
Dynamic Memory, 340
configuring, 340–342, 354

E

Elliptic Curve Diffie-Hellman P-256, 546
Elliptic Curve Diffie-Hellman P-384, 546
Enable-ADOptionalFeature cmdlet, 200, 207, 222
Enable-NetAdapter cmdlet, 253
Enable-VMResourceMetering cmdlet, 350
Encapsulating Security Protocol (ESP), 544
encapsulation, 544
encryption, 70, 543, 576
algorithms, 548
IPsec settings, 551
key exchange algorithms, 545–546
negotiating dynamically, 564
requiring, 563
for share file access, 389
Enhanced Point and Print, 447
Enterprise Admins security group, 141, 144
Enterprise Client (EC) environments, 473
enterprise deployment, 37
environment variables in Group Policy preference items, 497–499
ESP (Encapsulating Security Protocol), 544
Ethernet interfaces. *See* network interfaces
event alerts, 100–101
events
alerts for, configuring, 100–101
collecting, 98–101
for new domain controllers, 157
viewing information about, 99–100, 101
Events thumbnail (Server Manager), 86, 101
Event Viewer Windows Firewall with Advanced Security operational log, 525
executables, firewall rules for, 532
execute disable bit, 293

existing forests
domain controller deployment in, 139, 144–146, 148–149, 156–157, 163, 167
Export-SmigServerSetting cmdlet, 35
external virtual switches, 295–296

F

failover. *See* DHCP failover
Failover Clustering feature, 226, 286
for Hyper-V hosts, 301
with Storage Spaces, 369, 371–372, 376, 426
failover clusters, 295
fault tolerance, 138
feature binaries
obtaining, 42
removing, 45, 78–79
side-by-side store, 42, 78
states of, 42–43
Features On Demand, 38, 43, 108
features, server
installing, 108–118, 126–127
installing on multiple computers, 115–116
installing with Server Manager, 110–118, 126–127
installing with Windows PowerShell, 114–116, 126–127
listing, 114–115, 132
prerequisites for, 108–110
removing, 116–117, 132
Fibre Channel, 321–322, 397
for shared storage, 373
File And Storage Services, integration in Server Manager, 90
File And Storage Services page (Server Manager), 89, 400
Disks subpage, 394, 417
iSCSI subpage, 401–402, 407–408
Shares subpage, 395
Storage Pools subpage, 393, 420
Volumes subpage, 394–395
File And Storage Services role, 300
Storage Services role, 374
file server clusters, 373
File Server Resource Manager, 389
File Server role service, installing, 373–375, 420
file servers
health status, viewing, 396
managing, 89–90
reservations, adding, 254
scale-out, 298
Storage Spaces. *See* Storage Spaces
file shares. *See also* shares
provisioning, 387–392
filtering
boot-time filters, 518
security filtering GPOs, 485
Windows Management Instrumentation (WMI) filtering GPOs, 485–486
fine-grained password policies
assigning, 222
configuring, 195, 202–206, 221
creating, 204–205, 222
domain functional level and, 204
fallback policies, 203, 207, 222
implementing, 203, 207
managing with Windows PowerShell, 205
precedence values, 202
preference values, 203, 207, 222
viewing results, 205–206, 221
firewall ports, opening, 488, 490, 536
firewall profiles, 542
configuring, 522–524
configuring with Windows PowerShell, 525–526
firewall rules for, 527. *See also* firewall rules
logging, configuring, 524–525
managing, 519–526
status, viewing, 521, 575
types, 521, 542
firewall rules, 526–541
authenticated bypass, 562–565
block rules, overriding, 564
configuring, 571–572
configuring with Group Policy, 539–541
configuring with Windows PowerShell, 540–541
conflicts, 571–572
creating, 529
creating with Windows PowerShell, 535
custom firewall rules, 529, 532–534, 542, 576
default, 527, 534, 571
enabling, 530
filtering by profile, state, group, 537
Group Policy, refreshing, 536–537
IPsec and, 562–565

managing, 537–538
order of processing, 527, 542, 576
port rules, 529, 531, 576
predefined rules, 529, 531–532, 576
program rules, 529, 530, 542, 576
rule groups, 528
static, 535
types, 526–527, 529
viewing, 537–538
firewalls. *See also* Windows Firewall with Advanced Security
host-based, 516
stateful, 516–517
FirewallVerbose operational log, 525
fixed provisioning, 365, 426
fixed-size virtual hard disks, 320, 338, 347, 357
expanding, 345
flexible single master operations (FSMO) roles, 145
Folder Usage, 389
forest functional levels, 34
for AD Recycle Bin, 199
raising, 6, 195, 221, 222
rolling back, 200
specifying, 140, 147, 179
forest recovery, 5
forest root domain controllers, 137, 141
NetBIOS name, 153
prerequisites for, 137
promoting, 169–170
forests, 135
design, 139, 146
domains, installing, 171
domains, removing, 160
installing, 169
new, 137–138. *See also* new forests
forest schema, upgrading, 5
forest upgrades, 5–6
preparing for, 5
Windows Server 2012 enhancements and, 18
Format-List cmdlet, 307
Format-Volume cmdlet, 387
forums, Windows Server, 17
Full installations, 39, 78
fully qualified domain name (FQDN)
root domain, 140, 147, 179
functional level changes, 6–7

G

GenerationID identifier, 144
Get-ADComputer cmdlet, 491
Get-ADDomainController cmdlet, 214, 215
Get-ADReplicationSite cmdlet, 214
Get-ADReplicationSiteLink cmdlet, 215
Get-ADUser cmdlet, 208, 222
Get-ADUserResultantPasswordPolicy cmdlet, 206
Get-BPAResult cmdlet, 172–173
Get-ChildItem cmdlet, 491
Get-Command cmdlet, 167, 212, 217, 223
cmdlets, searching for, 245–246
dhcp option, 255
–Module command, 400
Get-DhcpServerInDC cmdlet, 282
Get-DhcpServerv4Failover cmdlet, 283
Get-DhcpServerv4Lease cmdlet, 283
Get-DhcpServerv4Scope cmdlet, 254, 282, 283
Get-Disk cmdlet, 384, 424
Get-DnsServer cmdlet, 256
Get-DnsServerForwarder cmdlet, 285
Get-DnsServerResourceRecord cmdlet, 255
Where-Object cmdlet, piping into, 255
Get-DnsServerRootHint cmdlet, 284
Get-DnsServerStatistics cmdlet, 256
Get-DnsServerZone cmdlet, 255
Get-ExecutionPolicy cmdlet, 218
Get-Help cmdlet, 17, 123–124, 217, 223
syntax, 246–247
Get-IscsiConnection cmdlet, 415, 429
Get-IscsiServerTarget cmdlet, 409, 429
Get-IscsiSession cmdlet, 415
Get-IscsiTarget cmdlet, 416, 429
Get-IscsiVirtualDisk cmdlet, 408
Get-Item cmdlet, 166
Get-Job cmdlet, 119–120
Get-NetAdapterBinding cmdlet, 253, 288
Get-NetAdapter cmdlet, 252, 270
Get-NetFirewallProfile cmdlet, 525, 538, 540, 542, 575
Get-NetFirewallRule cmdlet, 535, 538, 540
Get-NetIPAddress cmdlet, 270, 281, 289
–AddressFamily parameter, 271–272
–InterfaceAlias parameter, 249–250
Get-NetIPInterface cmdlet, 277
Get-NetIPsecMainModeCryptoSet cmdlet, 554
Get-NetIPsecMainModeSA cmdlet, 567
Get-NetIPsecPhase1AuthSet cmdlet, 554

Get-NetIPsecQuickModeSA cmdlet, 567–569
Get-NetIPsecRule cmdlet, 562
Get-PhysicalDisk cmdlet, 380, 423, 427
Get-PrintConfiguration cmdlet, 456, 462
Get-Printer cmdlet, 451, 457, 462, 463
  Get-PrintJob cmdlet, piping to, 452
Get-PrinterConfiguration cmdlet, 452–454
Get-PrinterDriver cmdlet, 454
Get-PrinterPort cmdlet, 454, 456
Get-PrinterProperty cmdlet, 453, 462
Get-PrintJob cmdlet, 452
  Where-Object cmdlet, piping to, 454
Get-PSSession cmdlet, 123
  output, piping, 123
Get-ScheduledJob cmdlet, 133
Get-SmbShare cmdlet, 392
Get-SmigServerFeature cmdlet, 35
Get-StarterGPO cmdlet, 489, 512
Get-StoragePool cmdlet, 379–381, 427
Get-StorageSubsystem cmdlet, 380, 396, 427
Get-VHD cmdlet, 329, 330
Get-VirtualDisk cmdlet, 427
Get-VM cmdlet, 327–328, 342
Get-VMHardDiskDrive cmdlet, 330
Get-VMHost cmdlet, 307–308, 357
Get-VMNetworkAdapter cmdlet, 334
Get-VMSnapshot cmdlet, 349
Get-VMSwitch cmdlet, 308
Get-Volume cmdlet, 386
Get-WindowsFeature cmdlet, 19, 35, 114–115, 117, 166, 374
  –name parameter, 114
  piping output, 132
  Where-Object filter, 114
global catalog servers, 142, 147, 153
global unicast addresses, 265–266
  assigning, 271
GPOs (Group Policy Objects)
  administrative template files, 472
  backing up, 487, 491–493, 512
  creating, 483–484, 490, 492, 510
  disabling settings of, 483
  domain, 468, 470
  inheritance, 470, 511
  linking, 474–475, 484–485, 489–490, 492, 512
  local, 468
  out of scope, 468
  policies and preferences, 467, 483. *See also* Group Policy preferences; policies, Group Policy
  precedence, 470
  preferences, configuring, 494. *See also* Group Policy preferences
  printers, associating with, 446–447
  restoring, 487, 491–492
  security filtering, 485
  Starter GPOs, 473–475, 489, 509–510
  status, viewing, 482
  Windows Management Instrumentation (WMI) filtering, 485–486
GPT disks, 384, 387
Gpupdate.exe, 475, 490
greenfield deployments, 4, 34
Group Policy, 465–514
  Active Directory design and, 469–472
  AppLocker, 480
  auditing policies, 479–480
  binaries path setting, 109, 113, 133
  central store, 472
  delegation of administration, 470–471, 488, 511
  firewall rules, configuring, 539–541
  GPOs, creating and linking, 489–490. *See also* GPOs (Group Policy Objects)
  implementation, planning, 466–476
  infrastructure status, viewing, 482
  IPv6 transition technologies settings, 279
  manageability, 470, 471
  managed settings, 467
  managing, 482–487
  managing with Windows PowerShell, 489–493
  OU hierarchy, designing, 470–471, 488, 509, 511
  policies vs. preferences, 467–469. *See also* Group Policy preferences; policies, Group Policy
  refreshing remotely, 475–477, 488, 490–491, 509–511, 536–537
  Security Options settings, 478
  security settings, 476–481
  Software Restriction Policies (SRP) settings, 481
  unmanaged settings, 467
  User Account Control (UAC) settings, 479
  User Rights Assignment settings, 477–478
  Windows Firewall with Advanced Security policies, 481
  Windows Server 2012 improvements, 465

Group Policy Management Console
<domain_name> node, 488, 512
Domain node, 512
Forest node, 512
Group Policy Objects node, 474
Resultant Set of Policy (RSoP) information, collecting, 536
root domain node, 512
Status tab, 482
Group Policy Management Editor
Computer Configuration\Policies\Windows Settings\Security Settings, 476–477
GPO policies and preferences, configuring, 483
Group Policy preferences, configuring, 494
preference items, configuring, 501–504
preference items, managing, 505
User Configuration\Policies\Windows Settings\Security Settings, 476–477
Group Policy Objects (GPOs). *See* GPOs (Group Policy Objects)
Group Policy Planning and Deployment Guide, 466
Group Policy preferences, 483, 493–508, 508
applying once only, 497
categories, 494–495
Common tab of properties sheet, 496–497, 502, 503, 508
configuring, 495–496, 508, 513
Control Panel Settings extensions, 495, 506–507
in domain GPOs, 494, 513
environment variables as, 497–499
extensions, 494, 513, 514
General tab of properties sheet, 495, 501
Item-Level Targeting, 486, 497, 500–501, 503–505
vs. policies, 467–469
preference items, configuring, 501–504
preference items, creating, 495, 513
preference items, deleting, 495
preference items, managing, 505
preference items, replacing, 495, 513
preference items, updating, 495
preference options, 496–497
priority of, 495, 513
processing, stopping, 497
removing, 497, 514
scope, 486, 500, 514
security context, 497, 514
targeting items, 500–501, 508, 513
Windows Settings extensions, 494, 506
Group Policy Remote Update Firewall Ports GPO, 536
Group Policy Remote Update Firewall Ports Starter GPO, 512
Group Policy Reporting Firewall Ports GPO, 536
Group Policy Settings Reference For Windows And Windows Server page, 469, 484
groups
creating, 221
fine-grained password policies, 202–203
guest operating systems, deploying, 322

H

hardware RAID, Storage Spaces and, 370
Holmes, Lee, 124
host-based firewalls, 516
hosts. *See also* Hyper-V hosts
IPv6, 258
ISATAP, 278
router discovery, 273
hot standby DHCP servers, 226–228, 286–287
HTTPS (Secure HTTP), 235
hub-and-spoke topology, 228, 234, 286, 304
Hyper-V
IaaS with, 9
resource metering feature, 350
Smart Paging feature, 336
update for upgrade to Windows Server 2012, 2
Hyper-V hosts, 292–316
availability, 300–301
backing up, 302–303
in build lab, 48–49
configuring, 307–314, 357
deployment, planning, 292–304
disaster-recovery planning, 302–304
domain controllers on, 143–144
File And Storage Services role, 300
hardware requirements, 293–295
Hyper-V Replica, enabling, 314
live migrations, enabling, 314
management solutions, 298–300, 315–316
media access control (MAC) address range, configuring, 313
memory, reserved, 343
mobility, 301–302
network adapters, 295
network connectivity, 313

NUMA spanning, enabling, 314
processors, planning, 294
Remote Desktop, enabling on, 316
scalability, 300
security, 300
SMB 3.0 shared storage, 301, 303
storage migrations, configuring, 314
storage options, 297–298, 304, 316
storage performance, 321
virtual machines, number of, 340
Windows Server 2012 editions, 294, 315, 356
Hyper-V Manager, 298, 315–316
Dynamic Memory, configuring, 340–341
Hyper-V hosts, configuring, 307
snapshots, managing, 349
virtual hard disks, optimizing, 347
virtual machine management settings, configuring, 335
virtual machines, configuring, 326
virtual machines, creating, 324
virtual machines, importing, 325
virtual machines, monitoring, 350
virtual switches, creating, 311–314
Hyper-V quality of service (Hyper-V QoS), 344
Hyper-V Replica, 303–304
enabling, 314
Hyper-V server role, 291
configuring, 353
installing, 304–306, 353
Hyper-V Settings dialog box, 307–314
Hyper-V virtualization, 8, 291–359. *See also* Hyper-V hosts; virtual machines
backup plans, 302
hosts, deploying and configuring, 292–316
Hyper-V server role, installing, 304–306, 353
networking, 295–297
virtual machines, configuring and deploying, 316–338
virtual machines, managing, 339–352
virtual switches, 295–296
wireless networking and, 320

I

IaaS (Infrastructure as a Service), 9
IETF (Internet Engineering Task Force), 236
IKE (Internet Key Exchange), 545
image life-cycle management, 47–48
Import-Csv cmdlet, 216, 222
Import-DnsServerRootHint cmdlet, 256
Import Drivers Wizard, 58
importing virtual machines, 323–326
Import Operating System Wizard, 58
Import-SmigServerSetting cmdlet, 35
Import-VM cmdlet, 325
inbound firewall rules, 526–527
information security CIA triad (Confidentiality, Integrity, and Availability), 236
infrastructure. *See also* virtualization infrastructure
deployment infrastructure, 67–68
evolution of, 4
Infrastructure as a Service (IaaS), 9
infrastructure migration, 1, 10–17
assessment phase, 12, 19–29
forest upgrades, 5–6
greenfield deployments, 4
hybrid scenarios, 3
mixed environments, 6–7
pilot testing, 11
private cloud solutions, 8–10
public cloud solutions, 10
scenarios, 3–10
server consolidation, 7–8
server migration, 12–17
server role and feature migration, 14–15
Initialize-Disk cmdlet, 384
–PartitionStyle parameter, 384
in-place upgrades, 13, 144, 145, 149
performing, 32–33
Install-ADDSDomain cmdlet, 171
Install-ADDSDomainController cmdlet, 170–171
–Credential parameter, 171
–ReadOnlyReplica parameter, 171
Install-ADDSForest cmdlet, 169
installation
Active Directory Domain Services role, 150–151, 163, 169
ADK for Windows 8, 55
DHCP Server role, 282
DNS Server role, 141, 283
domain controllers, 170–171
domain controllers, verifying, 157–159, 172–173
File Server role service, 373–375, 420
Hyper-V role, 304–306, 353
iSCSI Target Server, 401–403

MDT 2012 Update 1, 56
Migration Tools, 15–16
network printers, 455–456
options for server deployment, 38–46
Print And Document Services role, 436
Print And Document Services Tools, 434–435, 447
printer drivers, 441, 449, 455
printers, 455–457
Print Server role service, 432–433
server roles and features, 108–118
installation binaries. *See also* binaries
removing, 38
installation options for servers, 38–46
choosing, 39
disk footprint, 46, 78
Full installations, 39, 78
Minimal Server Interface, 40. *See also* Minimal Server Interface installations
Server Core, 39, 40. *See also* Server Core installations
Server With A GUI, 39. *See also* Server With A GUI installations
installed binaries
removing, 78
Install From Media (IFM) option for domain controllers, 155–156
Install-WindowsFeature cmdlet, 42, 45, 114–115, 118, 283, 353, 375
–IncludeManagementTools parameter, 115, 353
-Name AD-Domain-Services -IncludeManagementTools, 169
–Restart parameter, 115–116, 353
Server-Gui-Mgmt-Infra-Restart parameter, 43
Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart parameter, 43
–Source parameter, 43–44, 46, 79
–WhatIf parameter, 305–306
Integration Services, 336
integrity checking, 234
integrity of data, 236, 547–548, 576
Intel Virtualization Technology (Intel VT), 293
Intel XD bit, 293
Interactive logon: Machine account threshold policy, 478
Interactive logon: Machine inactivity limit policy, 478
interfaces, 259. *See also* network interfaces
internal virtual switches, 295
Internet Control Message Protocol (ICMP) traffic, 549
Internet Engineering Task Force (IETF), 236
Internet Key Exchange (IKE), 545
Internet Key Exchange version 2 (IKEv2), 545
Internet Printing Protocol (IPP), 433, 447
Internet Printing role service, 433, 435
Internet Protocol version 6 (IPv6), 258–281
Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, 268, 272
Internet Small Computer System Interface (iSCSI), 295, 397. *See also* iSCSI storage
Internet Storage Name Service (iSNS) servers, 412
"Introducing Windows Server 2012" ebook, 1
Invoke-BPAModule cmdlet, 172
Invoke-Command cmdlet, 115–116, 122, 168, 171
ThrottleLimit parameter, 116–117
Invoke-GPUpdate cmdlet, 490
IP addresses. *See also* Internet Protocol version 6 (IPv6)
firewall rules for, 534
IP address spoofing, 235
Ipconfig command, 269
IPP (Internet Printing Protocol), 433, 447
IPsec, 242, 243, 428, 543–570
authenticated bypass, configuring, 562–565
Authenticated IP (AuthIP), 545
Authentication Header (AH), 544
authentication methods, 546–547, 552, 576–577
communications, monitoring, 565–569
configuring, 548–555
configuring with Windows PowerShell, 553–555
connection security, 543–548
connection security rules, configuring, 555–569, 573
data encryption, 548, 576
data encryption settings, 551, 555
data integrity, 547–548, 576
data protection settings, 551
default settings, 549–552
Encapsulating Security Protocol (ESP), 544
encapsulation, 544
firewall rules and, 562–565
ICMP exemptions, 549
implementing, 573–574
Internet Key Exchange (IKE), 545
key-exchange settings, 550–551, 555, 577
security associations (SAs), 544–545
tunnel authorizations, 549, 553
on virtual network adapters, 332
Windows Firewall with Advanced Security rules, 517

IPv6, 258–281
address assignment, 267–276
addressing, 263–267
address representation, 264
address space, 263–264
address states, 273
address types, 265–267
broadcast functionality, 267
concepts and terminology, 258–259
default functionality, 261
disabling, 262–263
double-colon notation, 264
global unicast addresses, 265–266
ISATAP, 277–280
link-local addresses, 266, 268
loopback addresses, 267
manual address assignment, 268–272
migrating to, 258
multicast addresses, 267
prefixes, 264–265
stateful address autoconfiguration, 274
stateless address autoconfiguration, 273
support, 12
TCP/IP protocol networking stack, 260–261
transition addresses, 267
transition technologies, 276–290
unique local addresses, 266–267
on Windows platforms, 261
IPv6-over-IPv4 tunneling, 277
IPv6-to-IPv4 traffic translation technologies, 277
Windows computers, configuring for, 279
ISATAP, 277–280
addresses, 277–278
deployment, scope of, 280
infrastructure components, 278–279
ISATAP hosts, 278
ISATAP routers, 278, 280, 281, 290
ISATAP subnets, 278
iSCSI Initiator, 398, 411–418
configuring, 411–412
enabling, 401
IQN, 412, 428
iSNS servers and target devices, 412
RADIUS authentication, 412
targets, connecting to, 414–416
targets, discovering, 412–414
targets, favorite, 412
volumes and devices, viewing, 412
iSCSI Initiator Properties dialog box, 411–412
iSCSI Qualified Name (IQN), 399
iSCSI storage, 397–419
benefits, 397–398
concepts and terminology, 398–399
connections, 399
in heterogeneous environments, 400
initiator service, 398, 406–407
IQNs, 399, 410
iSCSI Initiator, 411–418
iSCSI Target Server, configuring, 401–410
location, 397–398
management tools, 400
sessions, 399
targets, 398, 412–416, 429
target servers, 398
uses, 398
virtual disks, 398, 400
virtual disks, creating, 403–410
volumes, creating, 417–418
iSCSI targets, 398
connecting to, 414–416
discovering, 412–414
IQN, 414
security, 429
iSCSI Target Server, 398
configuring, 401–410
installing, 401–403
iSCSI Target Storage Provider role, 402
installation location, 403
isolation connection security rules, 555, 577
creating, 556–558, 561

J

JBOD (Just a Bunch Of Disks), 361
jobs
background, 119–120
completion, verifying, 119–120
scheduled, 120–121, 125, 128–129
state, 120
triggers, 134
Joergensen, Claus, 303
Jones, Don, 124
Just a Bunch Of Disks (JBOD) enclosures, 361

K

Kerberos V5, 546
keyboard shortcuts in Server Manager, 85
key exchange, 545, 577–578
  algorithms, 545–546, 555, 570
  IPsec settings, 550–551
key management, 240–241
key masters, 240
key signing key (KSK), 240, 243

L

LBFO (load balancing and failover), 333
Learn Windows PowerShell in a Month of Lunches (Jones), 124
legacy network adapters, 330–331
Legacy Point and Print, 447
licensing Windows Server 2012, 20
life-cycle management, 28
Line Printer Daemon (LPD) Service, 433–434
Line Printer Remote (LPR) service, 433–434
link-local addresses, 266, 268
  autoconfiguration, 273
  prefix identifiers, 281, 289
  zone identifiers, 270
links, 259
Lite Touch Installation (LTI). *See* LTI (Lite Touch Installation) deployments
LiteTouchPE_arch.iso, 63
LiteTouchPE_arch.wim, 63
live migrations, 295
  enabling, 314
  Windows Server 2012 improvements, 301–302
Live object state, 198, 221
load balancing and failover (LBFO), 333
Local Server page (Server Manager), 87–88, 94
local servers. *See also* servers
  remote management capabilities, 91
Local Server tile (Server Manager), 86
logging in Windows Firewall with Advanced Security, 524–525
logical interfaces, 259
loopback addresses, 267
LTI (Lite Touch Installation) deployments, 67–69, 71, 81
  monitoring, 57

M

main mode cryptographic sets, 554, 573
Manageability thumbnail (Server Manager), 86
managed settings in Group Policy, 467. *See also* policies, Group Policy
man-in-the-middle attacks, 333
mapped drives, 467, 501–505, 508
MAP Toolkit, 2, 22–27
  console options, 25
  Inventory And Assessment Wizard, 24
  Performance Metrics Wizard, 24, 27
  performing an assessment, 24, 29, 36
  preparing to use, 23–24
  running, 24–25
  sample reports, 25–27, 29, 36
  using, 30–31
master installations, software updates, 60
MBR disks, 384, 387
MDT 2012 Update 1, 13, 52
  automating deployment, 63
  installing, 56
  reference images, building, 54–64, 74–77
  selection profiles, 59
  software prerequisites, 66, 80
  with System Center Configuration Manager, 69–70
  with Windows Deployment Services, 68–69
Measure-VM cmdlet, 351
media access control (MAC) addresses
  configuring range, 313
  of virtual network adapters, 319, 332
member servers. *See also* servers
  Windows Server 2012, 7
MemoryReserve registry value, 343
message hashes, 547
Microsoft Assessment and Planning (MAP) Toolkit. *See* MAP Toolkit
Microsoft Consulting Services (MCS), 28
Microsoft Deployment Toolkit (MDT). *See* MDT 2012 Update 1
Microsoft network server: Attempt S4U2Self to obtain claim information policy, 478
Microsoft Pinpoint site, 10
Microsoft Private Cloud Fast Track program, 9
Microsoft Private Cloud Service Provider Program, 10
Microsoft products, downloading security baselines, 473
Microsoft Server And Cloud Platform page, 1

Microsoft Services Premier Support, 28
Microsoft System Center 2012 SP1, 9
Microsoft System Center suite, 86
Microsoft Windows Server 2012. *See* Windows Server 2012
migration. *See also* infrastructure migration
  assessment of readiness, 12, 19–29
  best practices, 10–17
  paths, supported and unsupported, 15, 18, 35
  pilot testing, 11
  of print servers, 447–448
  of server applications, 14
  of servers, 12–16
Migration Tools
  cmdlets, 17, 18
  installing, 14–17
  starting, 16
Minimal Server Interface installations, 40
  converting to, 43–44, 71–74
  converting to different installation option, 41
  Hyper-V server role and, 305, 316, 356
  installed features, 78
miniports, 296
mirrored virtual disks, 367, 371, 426
mixed environment migration scenario, 6–7
  disadvantages, 18, 34
  limitations, 7
mixed environments
  AppLocker and SRP in, 481
  Hyper-V host management, 299
  iSCSI in, 400
mobility of Hyper-V hosts, 301–302
Model-Specific Drivers, 442
Monitoring node, 57
mounted virtual hard disk files, 109
mounted Windows images, 109
MPIO (MultiPath IO), 414
msinfo32.exe, 35
multicast addresses, IPv6, 265, 267
multicast deployments, 69
multihomed computers, 520–521
  network location awareness, 519
MultiPath IO (MPIO), 414
multitenancy, 10

N

name resolution, 234. *See also* DNS Server role; DNS servers
  with DNSSEC, 237–238
  optimizing, 284
  recursive, 284
  root hints, 284
Name Resolution Policy Table (NRPT), 242
NAS (Network Attached Storage), 298, 304, 361
NAT64, 277
NDIS filter drivers, 297
neighbors, 259
NetBIOS names of forest root domain controllers, 153
Netsh.exe
  netsh interface ipv6 context, 268
  Netsh interface isatap set router command, 279
NetTCPIP Windows PowerShell module, 246
network adapters
  bindings, enabling and disabling, 253, 257
  disabling, 253
  displaying, 252
  on Hyper-V hosts, 295
  virtual, 319, 330–334
  virtual switches, binding to, 296
network administration, 225–290
  DHCP availability, ensuring, 226–234
  DHCP servers, managing, 253–255
  DNSSEC, implementing, 234–243
  IPv6/IPv4 interoperability, configuring, 258–281
  network adapter bindings, enabling and disabling, 253
  network adapters, disabling, 253
  network adapters, displaying, 252
  with Windows PowerShell, 244–257
Network and Internet utility, 312
Network Attached Storage (NAS), 298, 304, 361
network communications, hijacked, 234
network connections
  creating, 312
  firewall profiles for, 521
  IPv6 default configuration, 261
  multiple, 519–520
  network location awareness, 518–519
  securing, 543–548
Network Connections folder, 251, 261, 312
  Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, 268, 272

network drives, mapping, 501, 505, 508
Network File System (NFS), 388
network-filtering applications, 517
networking
cmdlets for, 244–252
Hyper-V, 295–297
managing with Windows PowerShell, 244–257
network interfaces
addresses, assigning, 267–276
address information, displaying, 270, 281
bindings, displaying, 253
finding, 248–249
IP addresses, adding, 249–251
IP addresses, removing, 252
listing, 277
multihomed, 272
TCP/IP configuration, viewing, 249
network location awareness, 518–519
network performance, optimizing, 343–345
Network Printer Installation Wizard, 442
network printers, installing, 455–456
networks, 259
security requirements, 519
network segments, 259
network services, 225
network switches, virtual, 295–296
network traffic
encryption, negotiating dynamically, 564
filtering, 481
firewall rules, 526–527
packet filtering, 516–517
security of, 543–570
New-ADFineGrainedPasswordPolicy cmdlet, 205, 222
New-ADOrganizationalUnit cmdlet, 218
New-ADReplicationSite cmdlet, 214
New-ADReplicationSiteLink cmdlet, 214
New-ADUser cmdlet, 208, 209, 219
–Instance parameter, 219
–PassThru parameter, 210
-–PasswordNotRequired parameter, 210
–Path parameter, 209
–UserPrincipalName parameter, 210, 211
New Connection Security Rule Wizard, 555, 556
Authentication Method page, 557, 559
Connection Security Rules node, 556
Endpoints page, 559
Exempt Computers page, 558
Name page, 558
Profile And Name page, 558, 559
Profile page, 558
Protocol And Ports page, 561
Requirements page, 557, 559, 560
Rule Type page, 556
Tunnel Endpoints page, 560
Tunnel Type page, 560
New Deployment Share Wizard, 57
new forests
additional domain controllers, deploying, 142, 148, 154–156, 167, 170–171, 177–178
best practices for deployment, 138–139, 146
domain controllers, deploying, 137–144
first domain controller, deploying, 140–141, 148, 162–166, 168–169, 179
first domain controller in new domain, 141–142
first domain controller, promoting, 152–153
functional level, specifying, 152
installing, 169, 176
naming, 154
planning, 147
read-only domain controllers, 143
New-GPLink cmdlet, 490, 492, 512
New-GPO cmdlet, 490, 492, 512
New Inbound (or Outbound) Rules Wizard, 529–534
Allow The Connection If It Is Secure option, 562–564
Computers page, 563
Users page, 563
New-IscsiServerTarget cmdlet, 410
New-IscsiVirtualDisk cmdlet, 409
New iSCSI Virtual Disk Wizard, 404–408
New-Item cmdlet, 391
New-Job cmdlet, 134
New-JobTrigger cmdlet, 120, 125, 134
–DaysInterval parameter, 134
New-NetFirewallRule cmdlet, 535, 540
New-NetIPAddress cmdlet, 247–248, 268, 271
New-NetIPsecRule cmdlet, 561
New-Partition cmdlet, 386, 424
New-PSSession cmdlet, 121–123, 134
New-ScheduledJob cmdlet, 125
New Scope Wizard, 276
New Shares Wizard, 390, 396
New-SmbShare cmdlet, 391, 424
New-StoragePool cmdlet, 380, 423
New Storage Pool Wizard, 378–379, 420
New Task Sequence Wizard, 60–61
New-VHD cmdlet, 329

New-VirtualDisk cmdlet, 384, 423
New Virtual Disk Wizard, 382, 420
New Virtual Hard Disk Wizard, 328
New Virtual Machine Wizard, 324
New-VM cmdlet, 325
New-VMSwitch cmdlet, 312
New Volume Wizard, 385, 418
Next Secure (NSEC or NSEC3) resource records, 238
NFS (Network File System), 388
NIC Teaming, 333
nodes, 258
  failover, 301
no execute bit, 293
non-uniform memory architecture (NUMA) spanning, 314
Notifications flag (Server Manager), 84, 106, 113
notifications, status, 105–106
NSEC3 hash algorithm, 240
nslookup, 284
NTLMv2, 546
null encapsulation, 563
NUMA spanning, 314

O

ODX (Offloaded Data Transfer), 321
Office 365, 8, 10
offline deployments, 70
offline virtual hard disks
  installation options, converting between, 44–45
  roles and features, installing, 111
Offloaded Data Transfer (ODX), 321
operating systems. *See also* Windows 8; Windows Server 2003; Windows Server 2008/Windows Server 2008 R2; Windows Server 2012
  source files, importing, 57–58
Optimize-VHD cmdlet, 347
OUs (organizational units), 135. *See also* Group Policy
  administrative control, delegating, 221, 470
  computers in, viewing, 491
  creating with ADAC, 190–193
  creating with Windows PowerShell, 217–218
  GPOs, linking to, 484
  hierarchy, designing, 470–471, 509–510
  link order, 470
outbound firewall rules, 526–527
out-of-box drivers, importing, 58

P

PaaS (Platform as a Service), 8–9
Package Aware Point and Print, 447
packages, importing, 60
packet filtering, 516–517
parity virtual disks, 367–368, 371, 426
partitions, removing, 160
pass-through disks, 321, 337, 357
–Passthru parameter, 342
password policies
  fine-grained, 202–206
  precedence values, 202
password protection, 70
Payette, Bruce, 124
performance
  collecting data on, 103–104, 131
  hardware and, 21
  WMI filtering and, 486
performance alerts, configuring, 104, 107
Performance thumbnail (Server Manager), 87, 104
per-machine customizations, 48
permissions
  for printers, 439, 445
  for print servers, 439
persistent sessions, 121–122
persistent store, 575
per-user customizations, 48, 50
physical disks
  automatic and hot-spare allocations, 379
  boot disk, 375
  number of, 396
  quorums, 368
  storage pools, 364, 375, 377, 396, 425. *See also* storage pools
  volumes on, 375, 426–427
physical interfaces, 259
  listing, 270
  multihomed, 268
physical servers. *See also* servers
  testing on, 2
physical storage devices
  connection to servers, types, 369
  Storage Spaces-supported, 369
physical systems, 49
physical-to-virtual (P2V) conversions, 317–318
pilot testing migration, 11

planning for Windows Server 2012, 2–18
migration process, 10–17
migration scenarios, 3–10
Platform as a Service (PaaS), 8–9
policies, Group Policy, 467, 483, 494
new in Windows Server 2012 and Windows 8, 468–469
priority of, 495, 513
policy store, 575
port firewall rules, 529, 533–534, 576
creating, 531
port mirroring, 333
PortProxy, 277
ports
connection security rules for, 561
printer, 444, 445, 455
Pre-Boot Execution Environment [PXE], 331
predefined firewall rules, 529, 531–532, 576
properties, 531–532
preferences. *See* Group Policy preferences
pre-shared key authentication, 546
primordial storage pools, 364, 375, 425
physical disks in, 377–378, 425
Print And Document Services role, 94, 130, 431
installing, 436
role services, installing, 433–434
Print And Document Services Tools, installing, 434–435, 447
Printbrm.exe, 447
Print-Class Drivers, 442
printer connections, deploying, 446–447
printer drivers
driver sprawl, 442
installing, 441, 449, 455
isolation mode, 440, 449, 461–462
managing, 440–442, 450
type, determining, 453–454
updating, 441, 463
v3, 442, 449, 461
v4, 442, 449, 462
viewing, 450, 453–454
Printer Migration Wizard, 447–448
printers
advanced management, 444
configuration settings, viewing, 452
deploying with Group Policy, 446–447
errors, tracking, 451–452, 463
installation, automating, 456–458, 463
installing, 443, 455–456
managing, 442–446
ports, managing, 444, 445, 455
on print servers, listing, 451
Properties page, 444–445
settings for, 445
shared, 457
sharing and unsharing, 444, 457, 462–463
viewing, 450, 452–453
print jobs
managing, 445–446
removing, 454–455
viewing, 450–452
Print Management console, 431, 435–449
Custom Filters node, 438
Deployed Printers node, 438
Drivers node, 440–441, 449, 461
Extended View, 445–446
launching, 437–438
Printers node, 443
Print Management node, 438
Print Servers node, 438
servers, adding, 461
print permissions, 439, 445
Print Server role service, installing, 432–433
print servers
deploying, 432–435
managing, 94
managing with Print Management console, 436–449, 458–459
managing with Windows PowerShell, 450–460
migrating, 447–448
printers on, listing, 451
print permissions, 439, 445
properties, 438–439
remote management, 461
Print Services for Unix, 434
Print Services page (Server Manager), 130
Print Spooler
printer drivers, isolating from, 440, 449, 461–462
restarting, 436
private cloud solutions, 8–10
evaluation software, 9
prevalidated configurations, 9
private firewall profiles, 521
private network locations, 519
private virtual switches, 295

production environments, 48
deployment infrastructure, 67–68
reference images, deploying, 67–71
snapshots, 304, 322, 338, 348
production schema, mirroring, 5
program firewall rules, 529, 532, 542, 576
creating, 530
protocols
connection security rules for, 561
firewall rules for, 533
provisioning
fixed, 426
fixed vs. thin, 365–367
for resiliency, 371
simple, mirror, and parity disks, 368
thin, 368, 376, 426
PSSessions, 121, 125
closing, 123
creating, 122
managing, 134
public cloud migration scenarios, 10
public firewall profiles, 521
public key infrastructure (PKI) cryptography, 237
public network locations, 518
PXE (Pre-Boot Execution Environment), 331

Q

quality of service
Hyper-V, 344
policy-based, 345
quick SMB shares, 389, 396, 427
quotas, share, 389, 392

R

RADIUS authentication, 412, 428
Read-Host cmdlet, 210
read-only domain controllers (RODCs), 137, 143, 171, 179
Receive-Job cmdlet, 120
Recycled object state, 199, 201, 221
reference computers, 49, 79
deploying image to, 51
reference images
building, 54–66
build labs for, 48–53
build process, 50–52
capturing, 51, 64, 80
defined, 47
deploying in production environment, 67–71
deploying to reference computer, 51
deploying to test systems, 51
life-cycle management, 47–48
MDT 2012 Update 1, 54–64
per-user customizations, 48
technician computer for, 52
testing, 65, 79
verifying, 51
reference installations, 79
refreshes, server, 13
ReFS (Resilient File System), 371
Register-IscsiSession cmdlet, 429
Register-ScheduledJob cmdlet, 120–121, 134
registry, policy-aware section, 468
Remote Authentication Dial-In User Service (RADIUS) authentication, 412, 428
remote computers, persistent sessions, 121–122
Remote Desktop Services
infrastructure, deploying, 110
Server Manager, integration in, 90
remote print servers, 433
managing, 448–449
Remote Server Administration, installing, 115
Remote Server Administrative Tools (RSAT). *See* RSAT (Remote Server Administration Tools)
remote server management, 83–134, 165
disabling, 91
enabling, 130
Server Manager, configuring in, 90–92
verifying, 94
remote servers. *See also* servers
disconnected sessions, 121–123
performance data, collecting, 103–104
PSSessions, 121
services, monitoring, 101–102
TrustedHosts list, adding to, 165, 174
remote sessions
reconnecting to, 122
scripts, invoking, 122
remoting, 165, 169
Remove-ADFineGrainedPasswordPolicy cmdlet, 205

Remove-ADUser cmdlet, 208
Remove-DnsServerResourceRecord cmdlet, 256
Removed object state, 199, 207, 222
Remove-Job cmdlet, 134
Remove-NetIPAddress cmdlet, 252
Remove-NetIPsecRule cmdlet, 562
Remove-PrintJob cmdlet, 455
Remove-PSSession cmdlet, 123
Remove Roles And Features Wizard, 159–160
  Credentials page, 160
  New Administrator Password page, 161
  Removal Options page, 160
  Remove Server Roles page, 159–160
  Validation Results page, 159–160
  Warnings page, 160
RemoveVMSnapshot cmdlet, 349
Remove-WindowsFeature cmdlet, 117, 132
repartitioning, 70
replacement of servers, 13
replication, 69
  change notification, 214
  forcing, 232
replication partners, 155
resiliency of storage system, 371, 426
Resilient File System (ReFS), 371
Resize-VHD cmdlet, 347
resource metering, 350
resource records
  adding, 255–256
  removing, 256
Resource Record Signature (RRSIG) resource records, 238
Restore-GPO cmdlet, 491
Resultant Set of Policy (RSoP) information
  collecting, 536
Reverse CHAP, 407
roles, server
  Active Directory Domain Services role, 150. *See also* Active Directory Domain Services role
  installing, 108–118, 115, 126–129
  installing on multiple computers, 115–116
  listing, 114–115, 132
  migrating, 14–17
  prerequisites for, 108–110
  removing, 116–117
  Server Manager, installing with, 110–113, 126–127
  Server Manager page, 113
  Windows PowerShell, installing with, 114–116, 126–127
rollback plans, 13
root domain, fully qualified domain name, 147
root hints, viewing, 284
Router Advertisement messages, 273
router discovery, 273
Router Guard, 333
routers, 258–259
  address configuration, 273
  ISATAP, 278, 280, 281, 290
RSAT for Windows 8, 7, 34, 92–94, 130–131, 435, 449, 461
RSAT (Remote Server Administration Tools)
  deploying, 93
  prerequisites, 93
rules. *See* firewall rules

S

SaaS (Software as a Service), 8, 10
Safe Mode Administrator Passwords, 169
SANs (storage area networks), 297–298, 361
  for Hyper-V hosts, 297–298
SAS (Serial Attached SCSI), 364
  controller cards, 370
  enterprise-level disks, 370
SATA disks, 368–370, 376
scalability
  of Hyper-V hosts, 300
  of storage, 363
  of Storage Spaces, 372–373
scale-out file servers, 298
  implementing, 371
Scan Management snap-in, 433
scanned documents, 433
SCCM (System Center Configuration Manager). *See* System Center Configuration Manager (SCCM)
scheduled jobs, 120–121, 128–129, 299
  creating, 125
  triggering, 125
schema
  extending, 145, 148–149, 163
  upgrade testing, 6–7
  upgrading, 5
Schema Admins security group, 141, 144
scopes
  activating, 254
  adding, 254

address ranges, excluding, 254
creating, 282
default gateway addresses, configuring, 254, 257
failover relationships, configuring, 230–232
replication, forcing, 232
splitting, 226, 233, 286
viewing, 254
scripting
automating with, 39
execution policy, setting, 169
SCSI Enclosure Services (SES), 370
Secure HTTP (HTTPS), 235
Secure Sockets Layer (SSL), 235
secure strings, 223
security
of boot process, 518
Challenge Handshake Authentication Protocol (CHAP), 428
between DNS clients and DNS servers, 242, 243
for DNS protocol, 234
GPOs, security filtering, 485
Group Policy settings, 476–481
of Hyper-V hosts, 300
IPsec, 543–570
network requirements, 519
Windows Filtering Platform (WFP), 517–518
Windows Firewall with Advanced Security, 516–542
Windows service hardening, 518
security associations (SAs), 544–545
viewing, 566–567
security baselines, downloading, 473
security groups, 141, 144
user rights assigned to, 477–478
selection profiles, 59, 80
Select-Object cmdlet, 120
Send-SmigServerData cmdlet, 35
Serial Attached SCSI (SAS), 364, 370
server applications, migrating, 14
server clusters, 226–227
server consolidation, 7–8, 34
Server Core installations, 37, 39, 40
AD DS role support, 164
converting offline VHDs, 44–45
converting to, 43
converting to Minimal Server Interface, 43, 71–74
converting to Server With A GUI, 43, 71–74
disk space usage, 78
feature binaries, 42
on Hyper-V hosts, 300, 315–316, 353
read-only domain controllers, 143
switching to, 175
server deployment, 37–82
automating, 61–62
boot media, 63
customizing process, 50
driver incompatibilities, 59
installation options, 38–46
kick-starting, 63
LTI approach, 68–69, 71
strategies, 67
task sequences, 60–61
ZTI approach, 69–71
Server for NFS, 388
server groups, 107
creating, 96–97
functions of, 131–132
managing, 97
membership, 97
for remote domain controllers, 148, 150
servers, adding, 131
server management, 83
automating, 119–125
GUI-based, 90
GUI tools, 39
remote, 83–134
with Server Manager, 84–94, 95–108
in small environments, 40
with Windows PowerShell, 253–254
Server Manager, 84–94
Active Directory Domain Services role, installing, 150–151
additional domain controllers, deploying, 148
AD DS, uninstalling, 159–162
alerts, 86–87
All Servers page, 88–90, 130
console, 41
controls, 84–85
Dashboard, 85–86, 103, 127–128, 130
domain controllers, demoting, 159–161
domain controllers, deploying, 147–163
domain controller server groups, 158–159
events, collecting, 98–101
features, installing, 110–113, 126–127
features, removing, 116–117

File And Storage Services page, 89, 372, 400. *See also* File And Storage Services page (Server Manager)
first domain controller, deploying, 148
Hyper-V server role, installing, 304–305
installation options, converting between, 45
iSCSI Initiator, enabling, 401
iSCSI virtual disks, creating, 404–408
keyboard shortcuts, 85
Local Server page, 87–88
menus, 84–85
navigating, 84–90
new forest, installing, 176
notification flag, 113
Notifications menu, 151, 159
performance data, collecting, 103–104
print servers, configuring, 433
Print Services page, 130, 436
properties, 85
Quota page, 392
refresh interval, 85–86, 132
remote management, configuring, 90–92
remote management, troubleshooting, 91–92
roles, installing, 110–113, 126–127
role-specific pages, 89
roles, removing, 116–117
server groups, creating, 96–97, 107
server management tasks, 95–108
servers, adding, 95–96
servers, restarting, 97–98
services, monitoring, 101–103, 108
shared storage, provisioning and managing, 420–423
SMB shares, creating, 390–392
status notifications, viewing, 105–106
storage pools, creating, 378–379
storage pools, managing, 393
Storage Pools page, 378
Storage Spaces, implementing, 373
task prerequisites, 97
thumbnails, 86–87
tiles, 86
virtual disks, creating, 382–383
virtual disks, managing, 393–394
volumes, creating, 385–386
on Windows 8, 92–93
workgroup servers, managing remotely, 91
Server Manager cmdlets, 114
Server Message Block (SMB), 387. *See also* SMB shares
server migration, 1–19
assessment of readiness, 19–29
best practices, 12–14
destination server, installing migration tools on, 15–16
role and feature migration, 13–15
source server, installing migration tools on, 16–17
server pools, 131
server groups, 96
servers, adding, 95–96, 107, 130, 131
server roles. *See* roles, server
servers. *See also* DHCP servers; DNS servers; domain controllers; remote servers
Active Directory Domain Services role, 150–151
adding to server pool, 95–96, 107, 130, 131
destination servers, 14–16
domain-joining, 165–166
event collection, configuring, 98–101
in-place upgrades, 13
mixed environment, 7
multihomed, 520–521
performance data, collecting, 103–104, 107, 131–132
promoting to domain controllers, 151, 159
real-time monitoring, 86
refreshes, 13
remote management, 356, 461
replacement, 13
restarting, 97–98
roles and features, installing, 108–118, 126–127
roles and features, listing, 114–115
source servers, 14, 16–17
Windows Deployment Services, 49
server-to-server connection security rules, 556, 570, 577
creating, 559
server virtualization. *See* Hyper-V virtualization
Server With A GUI installations, 39
converting offline VHDs, 44–45
converting to, 71–74
converting to different installation option, 41
converting to Minimal Server Interface, 44, 78
converting to Server Core, 43–44, 175
Desktop Experience, 41
Graphical Management Tools And Infrastructure, 41
installed features, 78
Server Graphical Shell, 41

service alerts, 102
service hardening, 518
service restriction rules, 518
services
  managing, 108, 132
  monitoring, 101–103
  on new domain controllers, 158
  security context, 518
Services MMC console, 101, 132
Services thumbnail (Server Manager), 87, 102, 132
SES (SCSI Enclosure Services), 370
sessions
  disconnected, 121–123
  persistent, 121
Set-ADAccountPassword cmdlet, 223
  –AsPlainText parameter, 211
  –Force parameter, 211, 216
  –NewPassword parameter, 211
Set-ADFineGrainedPasswordPolicy cmdlet, 205
Set-ADForestMode cmdlet, 200, 222
Set-ADReplicationSiteLink cmdlet, 214
Set-ADUser cmdlet, 208
Set-DhcpServerv4OptionValue cmdlet, 254, 257
Set-DhcpServerv4Scope cmdlet, 254
Set-DnsClientServerAddress cmdlet, 268, 272
Set-DnsServerCache cmdlet, 256
Set-DnsServerScavenging cmdlet, 256
Set-Execution cmdlet, 169
Set-ExecutionPolicy cmdlet, 218
Set-GPLink cmdlet, 512
Set-Item cmdlet, 166, 174
  -Concatenate parameter, 166
  -Force parameter, 166
Set-NetFirewallProfile cmdlet, 526, 540
Set-NetIPInterface cmdlet, 252
Set-NetIPsecRule cmdlet, 562
Set-NetIsatapConfiguration cmdlet, 279
Set-PrintConfiguration cmdlet, 456, 462
Set-Printer cmdlet, 457, 463
Set-PrinterProperty cmdlet, 462
Set-Service msiscsi cmdlet, 401
Set-SmbShare cmdlet, 391, 424
Set-VM cmdlet, 328, 336, 342, 357
Set-VMHost cmdlet, 309, 310, 314, 316, 357
Set-VMNetworkAdapter cmdlet, 334, 338, 344
Set-VMSwitch cmdlet, 345
Shadow Copies of Shared Folders, 302
shared storage
  availability, 371–372
  Fibre Channel for, 373
  managing, 393–395, 420–424
  provisioning, 377–387, 420–424
  shares, managing, 395–396
  SMB shares, provisioning, 387–392
  storage pools, creating, 377–381
  storage pools, managing, 393
  virtual hard disks, creating, 381–384
  virtual hard disks, managing, 393–394
  volumes, creating, 384–387
  volumes, managing, 394–395
shares, 364. *See also* SMB shares
  access-based enumeration, 388
  caching, 388
  encrypted access, 389
  Folder Usage, 389
  Hyper-V virtual machine files, storing, 396
  managing, 395–396
  provisioning, 387–392
  quotas, 389
Show-Command cmdlet, 247–249
  asterisk (*), 257, 288
Show-DnsServerCache cmdlet, 256, 284
side-by-side store (SxS) folder
  binaries, copying from, 108
  copying, 109
simple virtual disks, 367–368, 371
single-root I/O virtualization (SR-IOV), 311, 332
site links
  cost and replication frequency, 214
  properties, viewing, 215
sites, 135, 259
  creating, 214, 221
  domain controllers, moving between, 215
  GPOs, linking to, 484
  linking, 214
  listing, 214
  verifying, 214
slabs, 367
SMAPI (Storage Management Application Programming Interface), 363, 365
Smart Paging, 336
SMB 3.0, 387–388
SMB shares. *See also* shares
  advanced, 392, 427
  BranchCache, 389

configuring, 388–389, 427
general-purpose, 390–392
provisioning, 387–392
quotas, 392
types, 389–390, 396, 427
SmigDeploy.exe, 15
SMI-S providers, 363–364
SMP (Storage Management Provider), 363
snapshots
applying, 348, 352, 359
vs. backups, 304
deleting, 348
exporting, 348, 359
managing, 348–349
performing, 322–323, 338, 348, 352, 354–355, 358, 359
renaming, 349
storage location, 336
Software as a Service (SaaS), 8, 10
Software Restriction Policies (SRP) settings in Group Policy, 481
software updates
on master installation, 60
source files
operating system, importing, 57–58
source servers, 14
Migration Tools, installing, 16–17
spaces, 364
Specialized Security Limited Functionality (SSLF) environments, 473
split scopes, 226–227, 233, 286
spoofed IP addresses, 235
spoofing, 234
SQL Azure, 9
SSL (Secure Sockets Layer), 235
standalone computers
connecting with WS-Management, 165–166, 172
Standard Client Task Sequences, 60
standard strings
converting to and from secure strings, 223
standby servers, 226–227
Start-DnsServerScavenging cmdlet, 256
Starter GPOs, 473–475
creating, 509–510
Group Policy Remote Update Firewall Ports, 536
Group Policy Reporting Firewall Ports, 536
viewing, 489
Starter GPOs folder, 473
Start-Job cmdlet, 133
Start-Service msiscsi command, 401
Start-VM cmdlet, 342
stateful address autoconfiguration, 274
stateful firewalls, 516–517
stateless address autoconfiguration, 273, 280, 281, 290
static firewall rules, 535
status notifications
brief summary, 106
viewing, 105–106
Stop-VM cmdlet
–Passthru parameter, 342–343
storage administration, 361–429
iSCSI storage, 397–419
shared storage, provisioning, 377–387
Storage Spaces, deploying, 362–376
storage area networks (SANs), 297–298, 361
Storage Management Application Programming Interface (SMAPI), 363, 365
Storage Management Initiative Specification (SMI-S) providers, 363–364
Storage Management Provider (SMP), 363
Storage Migration feature, 302
storage migrations, 314
storage pools, 364
capacity, 382
configurations, 378
creating, 377–381
managing, 393
for performance needs, 370–371, 396
primordial, 364, 375
Storage Services role, 374
Storage Spaces, 361
availability of system, 371–372
benefits, 362–363
concepts and terminology, 363–364
data storage methods, 367
deploying, 362–376
dynamic disks and, 365
with Failover Clustering, 369, 371–372, 376, 426
File Server role service, installing, 373–375
hardware RAID and, 370
hardware requirements, 369–370
health status, viewing, 380, 396, 427
highly available solutions, 369, 373
implementing, 373–375
managing, 372
performance, 370–371

resilient storage, 367–368, 371
scalability, 372–373
shared storage, provisioning and managing, 377–396
slabs, 367
USB devices and, 369
virtual hard disks, provisioing, 365–367
Storage Spaces providers, 363
storage subsystem, 363
displaying, 380, 427
storage virtualization, 362–376
subnets, 259
DCHP traffic, spanning, 227
IPv6 prefix, 265
ISATAP, 278
summarized routes, 265
Suspend-Job cmdlet, 134
synthetic network adapters, 330
system backups, 13
System Center Configuration Manager (SCCM), 13, 27–28, 86, 299
assessing environment with, 27–28
benefits of, 81
server deployment with, 69–70
System Center Data Protection Manager (DPM), 302–303
System Center Operations Manager, 86
System Center Virtual Machine Manager (VMM), 13, 299
System Preparation Tool (Sysprep), 51
system requirements for Windows Server 2012, 20–21
System Restore, 302
systems-management products, assessing readiness for migration with, 28
SYSVOL bloat, 472
SYSVOL folder, 472
central store, 472
location, 140, 147, 153, 179
SYSVOL replication, 472, 482, 488

T

target computers, opening firewall ports, 488, 490
Task Details dialog box, 105
tasks
automating, 119
status notifications, 105–106
task sequences
automating deployment with, 61–63
creating, 60–61
Install group, 81
Postinstall group, 81
Preinstall group, 81
Standard Client Task Sequence type, 65
Validate group, 66
TCP/IP protocol networking stack, 260–261, 289
Tcpip.sys, 261
TechNet
Directory Services forum, 138
domain controller deployment guidance, 172
Windows Server forums, 17
technician computers, 49, 79
deployment shares, 56–57
MDT 2012 Update 1, 54–64
setting up, 52
template accounts, 211, 218–220
Teredo, 276, 290
Test-ADDS* cmdlets, 168
Test-ADDSDomainControllerInstallation cmdlet, 175
test environments, creating, 5
testing
functional level changes, 6–7
methodology, defining, 11
reference images, 65
schema upgrades, 6–7
test plans for migration, 11
test server systems
reference images, deploying to, 51, 65
requirements, 2
thin provisioning, 365, 368, 376, 426
ThrottleLimit parameter, 116
thumbnails (Server Manager), 86–87
tiles (Server Manager), 86
traffic filtering, 481
transition addresses, 267
transport mode encapsulation, 544
tree domains, 141–142, 171
troubleshooting iSCSI target discovery, 414
trust anchors, 240–242
TrustAnchors.dns file, 242
TrustedHosts list, adding servers to, 165–166, 172, 174
tunnel connections, 549
configuring, 553
tunnel connection security rules, 556
creating, 559–560

tunneling, 276
IPv6-over-IPv4, 277
tunnel mode encapsulation, 544
type A (address) resource records, 255

U

unattended deployments, 70, 71
unicast IPv6 addresses, 265
Uninstall-ADDSDomainController cmdlet, 174
Uninstall-WindowsFeature cmdlet, 42, 45, 114, 117, 132, 175
–Remove parameter, 45, 46, 78
Server-Gui-Mgmt-Infra -Restart parameter, 44, 46
Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart parameter, 43
unique local addresses, 266–267
unmanaged settings, 467. *See also* Group Policy preferences
upgrades of existing domain controllers, 145–146
USB devices, Storage Spaces and, 369
User Account Control (UAC) settings in Group Policy, 479
user accounts
bulk creation, 210–211, 216
creating, 193–195, 209, 218–220
enabling, 210
location, 209
managing, cmdlets for, 212–213
managing with Windows PowerShell, 208–211
passwords, specifying, 210
properties, 209
retrieving, 222
template accounts, 211, 218–220
user certificates, 546
user rights assignment in Group Policy, 477–478
users
administrative control, delegating to, 470
fine-grained password policies, 202
Group Policy preferences and, 493
password settings, viewing, 205–206

V

v3 printer drivers, 442, 449, 461
v4 printer drivers, 442, 449, 462
validation of target computer, 80
VDI (virtual desktop infrastructure) environments, 291
Dynamic Memory for, 340
verification
of domain controller installation, 141, 157, 172–173
of prerequisites, 168
of schema extension, 150
VHD disk format, 321, 328
VHDX disk format, 321, 328
virtual desktop infrastructure (VDI), 291
Dynamic Memory for, 340
Virtual Disk Service (VDS), 365, 402, 425
virtual disks, iSCSI, 398, 400
creating, 403–410
virtual Fibre Channel, 321–322
virtual hard disk files location, 308–309
virtual hard disks, 320–322, 337–338, 364
adding, 328–330
automatic allocations, 368, 379
compacting, 345
converting between formats, 345
creating, 381–384
data loss, avoiding, 346
disk formats, 321, 357
expanding, 346
hot-spare allocations, 368, 379
initializing, 384, 387
managing, 393–394, 396, 427
optimizing, 345–347, 352, 359
provisioning, 365–367, 382
resiliency, 426
shrinking, 346, 359
size, specifying, 382, 383
storage capacity, 321
storage layouts, 367–368, 382, 383
virtualization, 291–359
multitenancy, 10
server consolidation, 7–8
of storage resources, 362. *See also* Storage Spaces
virtualization infrastructure, 291
Hyper-V hosts, deploying and configuring, 292–316
virtual machines, configuring and deploying, 316–338
virtual machines, managing, 339–352
virtualized domain controllers, 137, 143–144
virtual local area networks (VLANs), 311–312
Virtual Machine Import Wizard, 325
virtual machine queue (VMQ), 332

virtual machines, 337
automatic start action, 336
automatic stop action, 336
backing up, 302–304
bandwidth management, 344–345, 354–355
configuration files location, 309–310, 318
configuring, 326–336, 354–355
copying, 324, 326
creating, 324–326, 354–355
deploying, 316–338
deployment, planning, 317–324
Dynamic Memory, 319, 340–342, 354–355
guest operating systems, deploying, 322
hardware resources, 293
hardware settings, 335
Hyper-V Manager, creating with, 324
importing, 323–326
Integration Services, 336
management settings, configuring, 335–336
managing, 339–352
media access control (MAC) address range, configuring, 313
memory buffers, 341, 351–352, 358
memory, physical, 318–319
memory weight setting, 341
monitoring, 350–351
name, 336
network performance, optimizing, 343–345
number of, 293, 340
RAM, 340, 342, 351–352, 358
registering, 323
replicating, 303–304
restoring, 323
reverting, 348
settings, viewing, 327–328
Smart Paging, 336
snapshots, file location, 336
snapshots, managing, 304, 348–349
snapshots, performing, 322–323, 352, 354–355
storage, configuring, 308–310
storage controllers, 320
testing on, 2
virtual hard disks, adding, 328–330
virtual hard disks, optimizing, 345–347
virtual hard disks, planning, 320–322, 337
virtual network adapters, adding and configuring, 330–334, 357
virtual networking, 319–320
virtual processors, assigning, 319, 354–355
Windows PowerShell, creating with, 325
Windows PowerShell, managing with, 299
workload consolidation, optimizing, 339–343
virtual network adapters, 330–334, 337, 357, 358
bandwidth management, 344–345
virtual networking, 319–320
"Virtual PC Guy Blog", 310, 346
virtual processors, 319
number of, 354–355
virtual switches, 295–297, 357
backing up, 303
connection type, 311–312
creating, 311–314
extensibility features, 297
listing, 308
properties, listing, 308
Virtual Switch Manager dialog box, 311
virtual-to-virtual (V2V) conversions, 317
VLAN identification, 331
VLANs (virtual local area networks), 311–312
VMQ (virtual machine queue), 332
VMware ESX 4.1, 388
VMware virtual machines, 388
volume backups, 302–303
volumes, 364
creating, 384–387, 417–418
managing, 394–395
provisioning, 426–427
resilient, 426–427
size, specifying, 385, 386
Volume Shadow Copy Service (VSS), 302–303
VPN connections, 545
VSS for SMB File Shares, 303
VSS (Volume Shadow Copy Service), 302, 303

W

Web Server (IIS) role, 433
websites, authenticating, 235
Welcome To Server Manager tile, 86
WFP (Windows Filtering Platform), 297, 517–518
Where-Object cmdlet, 173, 223

Windows 8
administrative template files, downloading, 472
Group Policy policies, new, 468–469
Group Policy Settings Reference, 484
RSAT for, 92–94, 130–131
Server Manager, running, 92–93
Windows Firewall with Advanced Security, 515
Windows Assessment and Deployment Kit (ADK) for Windows 8, 52, 80
Windows Automated Installation Kit (Windows AIK), 80
Windows Deployment Services, 49, 68, 79
Windows Deployment Wizard, 63, 64
displaying pages, 64
Windows Filtering Platform (WFP), 297, 517–518
Windows Firewall with Advanced Security, 481, 515
cmdlets for, 526
configuring, 516–542
enabling and disabling, 522
firewall profiles, 519–526, 575
firewall rules, 526–541
inbound connections, 522–523, 575
IPsec communications, monitoring, 565–569
IPsec rules, 517
logging, configuring, 524–525
network location awareness, 518–519
notifications, 523
outbound connections, 523
packet filtering, 516–517
protected network connections, 523
rule merging, 523
unicast responses, 523
Windows Firewall with Advanced Security snap-in, 521
Connection Security Rules node, 556
firewall rules, filtering, 537
Inbound (or Outbound) node, 529
IPsec settings, configuring, 548–549
Monitoring node, 538
root node, 522
Windows images
building, 47
capturing and sysprepping, 51, 53, 80
life-cycle management, 47–48
Windows Management Instrumentation (WMI) filtering, 485–486
alternative to, 486
performance and, 486
Windows NIC Teaming, 295
Windows operating system
source files, importing, 57–58
Windows PowerShell
Active Directory administration, 208–217
Active Directory bulk management, 190, 210–211
additional domain controllers, deploying, 167, 170–171, 177–178
ADDSDeployment module, 167, 175, 181
AD Recycle Bin, enabling, 200, 207
background jobs, 119–120, 125
BPA scans, 173
caching-only DNS servers, configuring, 283–285
cmdlets, finding, 212–213, 217, 223
connection security rules, configuring, 561–562
deleted directory objects, restoring, 201
DHCP failover, configuring, 231, 282–283
DHCP servers, managing, 253–255
DNS servers, managing, 255–256
domain controller deployment, scripting, 135, 164–175
domain controller installation, verifying, 172–173
domain controllers, demoting, 174
elevated prompts, 169
escape characters, 171
existing forests, deploying domain controllers in, 167
features, installing, 126–127
fine-grained password policies, managing, 205
fine-grained password policy results, viewing, 206
firewall profiles, configuring, 525–526
firewall rules, configuring, 540–541
firewall rules, creating, 535
first domain controller in new forest, deploying, 164–166, 168–170
GPOs, creating and managing, 510
Group Policy, managing, 489–493
help, 123
help, online, 124
help, updatable, 124
Hyper-V cmdlets, 314
Hyper-V hosts, configuring, 307–308
Hyper-V module, 298–299
Hyper-V role, installing, 305–306
installation options, converting between, 42–43
IPsec communications, monitoring, 565–569
IPsec settings, configuring, 553–555
iSCSI connections, establishing, 415–416
iSCSI initiator, enabling, 401

iscsi module, 400
iscsitarget module, 400
iSCSI virtual disks, creating, 408–410
learning resources, 123–124
learning to use, 252
multiple-line commands, 171
NetSecurity module, 526, 553, 561
network adapter bindings, enabling and disabling, 253
network adapters, disabling, 253
network adapters, displaying, 252
networking cmdlets, 244–252
networking, managing with, 244–257
organizational units, creating, 217–218
–Passthru parameter, 342–343
pipeline capabilities, 329, 452, 490
prerequisites checks, 168, 175, 181
PrintManagement module, 435, 450–451
print servers, managing, 450–458
read-only domain controllers, installing, 171
Remote Server Administration, installing, 115
remoting, 164, 169
scheduled jobs, 120–121, 125, 128–129, 299
script execution policy, setting, 169
Server Core installations and, 164
server features, installing, 114–116
server features, listing, 114–115
server management, automating with, 119–125
Server Manager cmdlets, 114
server roles and features, installing on multiple computers, 115–116
server roles, installing, 114–116, 126–127
server roles, listing, 114–115
server roles, removing, 116–117
shared storage, provisioning and managing, 423–424
SMB shares, creating, 391–392
snapshots, managing, 349
Storage module, 372, 387
storage pools, creating, 379–381
Storage Spaces, implementing, 374–375
syntax, 247
user accounts, creating, 195, 218–220
user accounts, managing, 208–211
version 2.0, 119
version 3.0, 83, 119, 212
virtual disks, creating, 384
virtual hard disks, optimizing, 347
virtual machines, configuring, 336
virtual machines, creating, 325
virtual machines, importing, 325
virtual machines, monitoring, 350–351
virtual network adapters, configuring, 334
volumes, creating, 386–387
Where-Object cmdlet syntax, 115
Windows Server 2012 support for, 39
workflows, 299
Windows PowerShell Cookbook, 2nd Edition (Holmes), 124
Windows PowerShell History Viewer, 185, 193–194
copying commands from, 195
Windows PowerShell in Action, 2nd Edition (Payette), 124
Windows PowerShell Survival Guide, 124
Windows Server 2003
DNSSEC, 237
remote management and, 90
support for, 139
Windows Server 2003 Deployment Guide, 138
Windows Server 2008 Active Directory Resource Kit from Microsoft Press, 138
Windows Server 2008 R2 SP1 evaluation copy, 2
Windows Server 2008/Windows Server 2008 R2
DNSSEC, 237
Failover Clustering feature, 226, 286
remote management and, 90, 130
remote management, configuring, 92, 95
Windows Server 2012
deploying, 37–82
deprecated features, 376, 402, 425, 434
Diskshadow.exe, 303
dual IP layer TCP/IP stack, 260, 280, 289
existing Active Directory environments, implementing in, 7
Failover Clustering enhancements, 301
Fibre Channel feature, 321–322
Group Policy improvements, 465
Group Policy policies, new, 468–469
Group Policy Settings Reference, 484
installation options, 38–46
licensing model, 20, 294
live migration improvements, 301–302
planning for, 2–18
printer sharing, 447
remote Group Policy refresh capability, 475
remote server management tools, 83–134

Start screen, 32–33
Storage Spaces technology, 361–362. *See also* Storage Spaces
system requirements, 20–21
virtualization rights, 294
Windows Firewall with Advanced Security, 515
Windows PowerShell support, 39
Windows Server 2012 Datacenter edition, 20, 294, 315, 356
Windows Server 2012 domain functional level, 6
Windows Server 2012 Essentials edition, 20
Windows Server 2012 forest functional level, 6
Windows Server 2012 Foundation edition, 20
Windows Server 2012 Licensing & Pricing FAQ, 20
Windows Server 2012 Standard edition, 20, 294, 356
Windows Server Backup, 302–303
Windows Server Catalog, 21–22, 35
Windows Server forums, 17
Windows Server Migration Tools
cmdlets, 17, 18
installing, 14–17
Windows service hardening, 518
Windows services, firewall rules for, 533
Windows Settings extensions for Group Policy preferences, 494, 506
Windows Task Scheduler
job scheduling, 120–121
scheduled jobs, verifying completion, 121
Windows Update, 441
binaries, downloading, 108, 116, 118, 133
WinSxS folder
removing binaries, 45
wireless networking, Hyper-V and, 320
.wim files, 47
WMI Query Language (WQL), 485
workflows, 299
workgroup servers, remote management, 91
workloads, virtualized, 301
availability of, 301
WQL (WMI Query Language), 485
WS-Management protocol, 165

Z

Zero Touch Installation (ZTI), 67. *See also* ZTI (Zero Touch Installation) deployments
zone identifiers, 270, 281
zones
signing, 239–241, 243, 287, 288
viewing, 255
zone signing key (ZSK), 240
Zone Signing Wizard, 240
ZTI (Zero Touch Installation) deployments, 67, 69–70, 81
benefits, 71

About the author

MITCH TULLOCH is a well-known expert on Windows administration, deployment, and virtualization. He has published hundreds of articles on a wide variety of technology sites and has written more than two dozen books, including the *Windows 7 Resource Kit* (Microsoft Press, 2009), for which he was lead author; *Understanding Microsoft Virtualization Solutions*: *From the Desktop to the Datacenter* (Microsoft Press, 2010); and *Introducing Windows Server 2012* (Microsoft Press, 2012), a free ebook that has been downloaded over a quarter of a million times.

Mitch is also Senior Editor of WServerNews (*http://www.wservernews.com*), the world's largest newsletter focused on system admin and security issues for Windows servers. Published weekly, WServerNews helps keep system administrators up to date on new server and security-related issues, third-party tools, updates, upgrades, Windows compatibility matters, and related issues. With more than 100,000 subscribers worldwide, WServerNews is the largest Windows Server–focused newsletter in the world.

Mitch has been repeatedly awarded Most Valuable Professional (MVP) status by Microsoft for his outstanding contributions to supporting the global IT community. He is an eight-time MVP in the technology area of Windows Server Setup/Deployment.

Mitch also runs an IT content development business based in Winnipeg, Canada, which produces white papers and other collateral for the business decision maker (BDM) and technical decision maker (TDM) audiences. His published content ranges from white papers about Microsoft cloud technologies to reviews of third-party products designed for the Windows Server platform. Before starting his own business in 1998, Mitch worked as a Microsoft Certified Trainer (MCT) for Productivity Point.

For more information about Mitch, visit his website at *http://www.mtit.com*.

You can also follow Mitch on Twitter at *http://twitter.com/mitchtulloch* or friend him on Facebook at *http://www.facebook.com/mitchtulloch*.

Training Guide: Installing and Configuring Windows Server 2012 and Exam 70-410

This book is designed to help build and advance your job-role expertise. In addition, it covers some of the topics and skills related to Microsoft Certification Exam 70-410, and may be useful as a complementary study resource. Note: This book is not designed to cover all exam topics; see chart below. If you are preparing for the exam, use additional materials to help bolster your readiness, in conjunction with real-world experience.

EXAM OBJECTIVES/SKILLS	SEE TOPIC-RELATED COVERAGE HERE
INSTALL AND CONFIGURE SERVERS	
Install servers	Chapters 1 and 2
Configure servers	Chapters 2 and 3
Configure local storage	Chapter 8
CONFIGURE SERVER ROLES AND FEATURES	
Configure file and share access	Chapter 8
Configure print and document services	Chapter 9
Configure servers for remote management	Chapters 2, 3, and 11
CONFIGURE HYPER-V	
Create and configure virtual machine settings	Chapter 7
Create and configure virtual machine storage	Chapter 7
Create and configure virtual networks	Chapter 7
DEPLOY AND CONFIGURE CORE NETWORK SERVICES	
Configure IPv4 and IPv6 addressing	Chapter 6
Deploy and configure the Dynamic Host Configuration Protocol (DHCP) service	Chapter 6
Deploy and configure the DNS service	Chapter 6
INSTALL AND ADMINISTER ACTIVE DIRECTORY	
Install domain controllers	Chapter 4
Create and manage Active Directory users and computers	Chapter 5
Create and manage Active Directory groups and organizational units (OUs)	Chapter 5

CREATE AND MANAGE GROUP POLICY	
Create Group Policy objects (GPOs)	Chapter 10
Configure security policies	Chapter 10
Configure application restriction policies	Not covered
Configure Windows Firewall	Chapter 11

For complete information on Exam 70-410, go to *http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-410*. And for more information on Microsoft certifications, go to *http://www.microsoft.com/learning*.