



# Configuring Advanced Windows Server 2012 Services

## Training Guide

Orin Thomas

# Configuring Advanced Windows Server 2012 Services



Designed to help enterprise administrators develop real-world, job-role-specific skills—this *Training Guide* focuses on advanced configuration of services necessary to deploy, manage, and maintain a Windows Server 2012 infrastructure. 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 advanced infrastructure services in Windows Server 2012
- Creates a foundation of skills which, along with on-the-job experience, can be measured by Microsoft Certification exams such as 70-412

## Sharpen your skills. Increase your expertise.

- Configure full forest and domain trust relationships
- Configure Active Directory (AD) sites and manage AD replication
- Implement advanced DNS and DHCP solutions
- Install, configure, and manage AD Certificate Services
- Manage backups and recover servers
- Optimize storage and configure advanced file services
- Manage failover clustering and Network Load Balancing
- Move virtual machines from one Hyper-V server to another
- Implement Dynamic Access Control and Active Directory RMS
- Implement Active Directory Federation Services

[microsoft.com/mspress](http://microsoft.com/mspress)

ISBN: 978-0-7356-7425-7



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

Windows

## 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

**Orin Thomas** is a consultant, writer, and Microsoft MVP whose books include *Microsoft Press Training Kits for Exams 70-646, 70-647, 70-662, and 70-680*. He is also a contributing editor for *Windows IT Pro* magazine.

## About the Practices

For most practices, we recommend using a Hyper-V virtualized environment.

For *system requirements*, see the Introduction.

## Preparing for Microsoft Certification?

Get the official exam-prep guide for Exam 70-412.

*Exam Ref 70-412: Configuring Advanced Windows Server 2012 Services*  
ISBN 9780735673618

Microsoft Press

Celebrating 30 years!

# Training Guide: Configuring Advanced Windows Server 2012 Services

Orin Thomas

Copyright © 2013 by Orin Thomas

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.

ISBN: 978-0-7356-7425-7

1 2 3 4 5 6 7 8 9 LSI 8 7 6 5 4 3

Printed and bound in the United States of America.

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](mailto: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 and Developmental Editor:** Michael Bolinger

**Production Editor:** Christopher Hearse

**Editorial Production:** Box Twelve Communications

**Technical Reviewer:** Randall Galloway

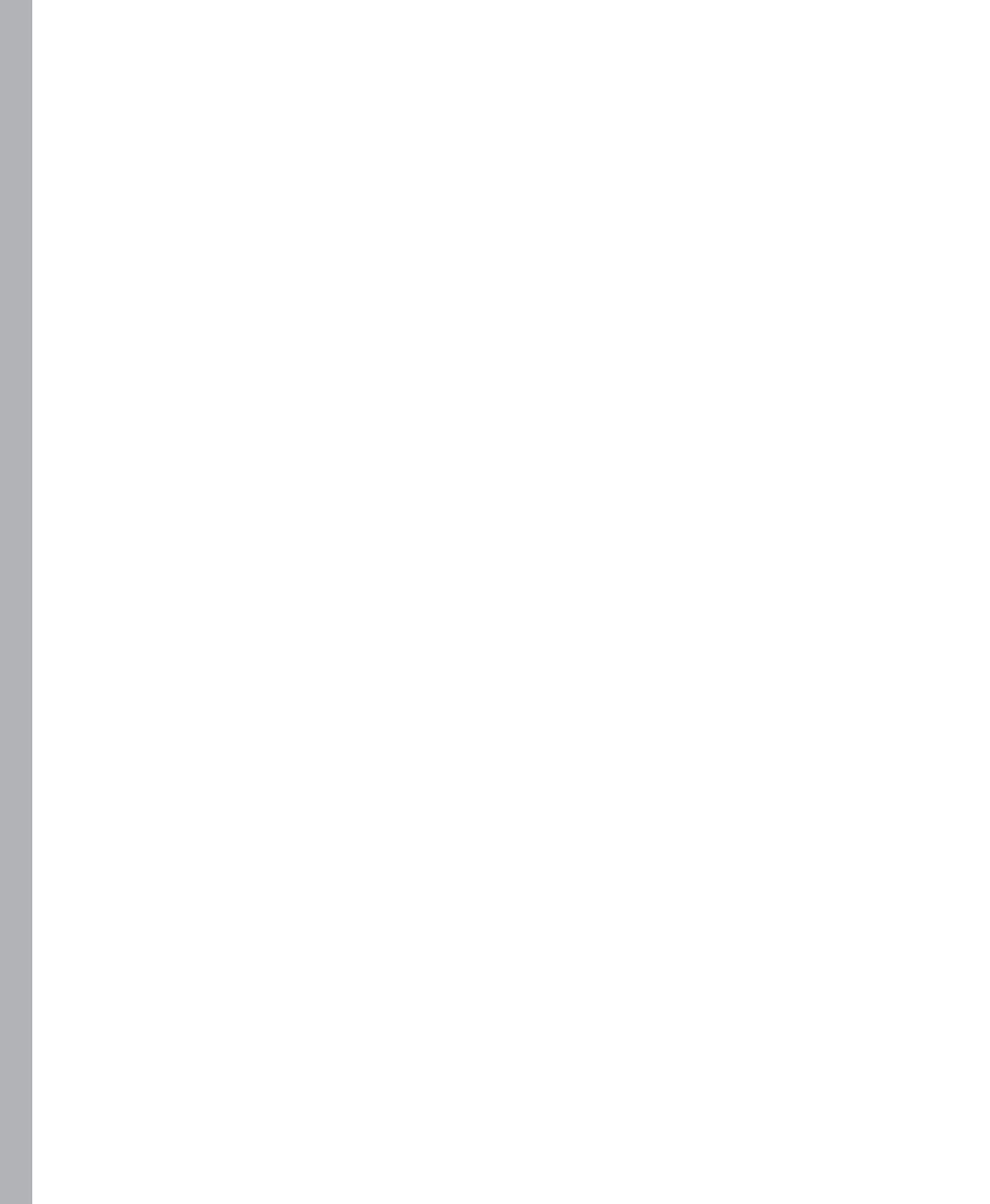
**Cover Design:** Twist Creative • Seattle

**Cover Composition:** Randy Comer

**Illustrator:** Rebecca Demarest

# Contents at a glance

	<i>Introduction</i>	<i>xix</i>
CHAPTER 1	Advanced Active Directory infrastructure	1
CHAPTER 2	Active Directory sites and replication	59
CHAPTER 3	Advanced DHCP and DNS	121
CHAPTER 4	Active Directory Certificate Services	209
CHAPTER 5	Backup and recovery	311
CHAPTER 6	Advanced file services and storage	399
CHAPTER 7	High availability	477
CHAPTER 8	Virtual machine and site resilience	551
CHAPTER 9	DAC and AD RMS	621
CHAPTER 10	Active Directory Federation Services	721
	<i>Index</i>	<i>781</i>
	<i>About the author</i>	<i>807</i>



# Contents

<b>Introduction</b>	<b>xix</b>
<b>Chapter 1 Advanced Active Directory infrastructure</b>	<b>1</b>
Before you begin.....	1
Lesson 1: Configuring domains and forests .....	1
Multidomain Active Directory environments	2
Multiforest Active Directory environments	8
Upgrading existing domains and forests	9
User Principal Name (UPN) suffixes	10
Lesson summary	11
Lesson review	12
Lesson 2: Configuring trusts .....	13
Trusts	13
SID filtering	22
Name suffix routing	23
Lesson summary	24
Lesson review	24
Practice exercises .....	26
Exercise 1: Prepare a domain controller to host a child domain with a contiguous namespace	26
Exercise 2: Create a child domain with a noncontiguous namespace	28
Exercise 3: Prepare domain controller to host the wing-tiptoys.com tree in the contoso.com forest	31
Exercise 4: Promote domain controller for new tree in contoso.com forest	31
Exercise 5: Prepare a domain controller to host a new forest	33

---

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

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

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

Exercise 6: Create new forest	34
Exercise 7: Prepare to configure a forest trust relationship	35
Exercise 8: Begin creating a forest trust relationship	38
Exercise 9: Complete the creation of the forest trust relationship between contoso.com and margiestravel.com	41
Exercise 10: Configure name suffix routing	44
Exercise 11: Configure selective authentication	46
Exercise 12: Configure additional UPN suffixes	51
Exercise 13: Configure a shortcut trust	51
Suggested practice exercises	55
Answers	56
Lesson 1	56
Lesson 2	57
<b>Chapter 2 Active Directory sites and replication</b>	<b>59</b>
Before you begin	59
Lesson 1: Configuring sites	59
Configure sites and subnets	60
Manage SRV record registration	68
Moving domain controllers	70
Lesson summary	71
Lesson review	72
Lesson 2: Active Directory replication	73
Active directory partitions	73
Understanding multi-master replication	74
RODC replication	77
Configure RODC password replication	78
Monitor and manage replication	81
Readmin	83
Upgrade SYSVOL replication	85
Lesson summary	86
Lesson review	87
Practice exercises	89
Exercise 1: Create Active Directory sites	89
Exercise 2: Create Active Directory subnets	91

Exercise 3: Create site links	94
Exercise 4: Modify site link cost and replication schedule	95
Exercise 5: Configure MEL-DC as an additional domain controller	97
Exercise 6: Verify site placement and trigger replication	101
Exercise 7: Configure ADL-DC as an RODC	102
Exercise 8: Configure RODC replication	106
Exercise 9: View account passwords replicated to ADL-DC	108
Exercise 10: Monitor replication with repadmin	111
Exercise 11: Remove the RODC and reset accounts	114
Suggested practice exercises	115
Answers	116
Lesson 1	116
Lesson 2	117

### **Chapter 3 Advanced DHCP and DNS 121**

Before you begin	121
Lesson 1: Implement an advanced DNS solution	121
DNSSEC	122
DNS event logs	124
GlobalNames Zones	126
Advanced DNS options	128
Delegated administration	131
Lesson summary	132
Lesson review	133
Lesson 2: Implement an advanced DHCP solution	134
Superscopes	135
Multicast scopes	136
Split scopes	137
Name Protection	137
DHCP failover	138
Lesson summary	140
Lesson review	141
Lesson 3: Deploy and manage IPAM	142
Introduction to IPAM	143

Deploy IPAM	143
Configure server discovery	144
Managing the IP address space	147
IP address tracking	149
IPAM administration	151
Lesson summary	152
Lesson review	152
Practice exercises	153
Exercise 1: Configure MEL-DC	154
Exercise 2: Configure DNSSEC	155
Exercise 3: Configure the name resolution policy	158
Exercise 4: Increase the size of the DNS socket pool	161
Exercise 5: Modify DNS Cache Locking	161
Exercise 6: Create and manage a GlobalNames Zone	163
Exercise 7: Configure and view the DNS Event Log	166
Exercise 8: Verify netmask ordering and disable recursion	168
Exercise 9: Install and activate the DHCP role	169
Exercise 10: Create a DHCP superscope	175
Exercise 11: Create a split scope	179
Exercise 12: Configure DHCP Name Protection	182
Exercise 13: Create new multicast scopes	185
Exercise 14: Configure DHCP failover	186
Exercise 15: Install the IPAM feature	189
Exercise 16: Configure IPAM GPOs and server discovery	190
Exercise 17: Configure servers to be managed by IPAM	192
Exercise 18: Manage servers using IPAM	198
Exercise 19: Use IPAM to create a DHCP scope	200
Exercise 20: Use IPAM to manage IP addresses	201
Suggested practice exercises	203
Answers	204
Lesson 1	204
Lesson 2	206
Lesson 3	207

## **Chapter 4 Active Directory Certificate Services 209**

Before you begin. . . . .	209
Lesson 1: Install and configure Active Directory Certificate Services . . .	209
Installing certificate authorities	210
CRL Distribution Points	217
Online responders	218
Administrative role separation	219
CA backup and recovery	221
Lesson summary	223
Lesson review	224
Lesson 2: Manage certificates. . . . .	226
Certificate templates	226
Certificate revocation	227
Certificate renewal	230
Autoenrollment	231
Key archiving and recovery	233
Lesson summary	236
Lesson review	236
Practice exercises . . . . .	238
Exercise 1: Deploy and configure an enterprise root CA	239
Exercise 2: Deploy an enterprise subordinate CA	247
Exercise 3: Install a standalone subordinate CA	253
Exercise 4: Configure a standalone CA	257
Exercise 5: Configure a CRL Distribution Point	260
Exercise 6: Configure an online responder	265
Exercise 7: Configure administrative role separation	272
Exercise 8: Configure a key recovery agent certificate template	276
Exercise 9: Request a key recovery agent certificate	282
Exercise 10: Configure Key Recovery	285
Exercise 11: Configure a certificate template for autoenrollment and key recovery	287
Exercise 12: Configure group policy to support autoenrollment, credential roaming, and automatic renewal	292
Exercise 13: Configure a certificate template to support private key archival and recovery and reenroll all certifi-	

cate holders	295
Exercise 14: Perform certificate revocation	297
Exercise 15: Perform certificate recovery	300
Suggested practice exercises	305
Answers	306
Lesson 1	306
Lesson 2	308
<b>Chapter 5 Backup and recovery</b>	<b>311</b>
Before you begin	311
Lesson 1: Configure and manage backups	311
Windows Server Backup	312
Windows Azure Backup	317
Role- and application-specific backups	322
Vssadmin	324
System restore points	327
Data Protection Manager	328
Lesson summary	329
Lesson review	329
Lesson 2: Recover servers	330
Restore from backups	330
Recover servers using Windows Recovery Environment	333
Safe Mode and Last Known Good Configuration	335
Configure the Boot Configuration Data store	336
Lesson summary	337
Lesson review	338
Practice exercises	338
Exercise 1: Prepare MEL-DC and CBR-DC for exercises	339
Exercise 2: Install Windows Server Backup	340
Exercise 3: Configure CBR-DC for local backup	344
Exercise 4: Perform a backup to a local volume	350
Exercise 5: Perform a backup over the network	352
Exercise 6: Use Vssadmin	356
Exercise 7: Perform a full volume recovery using Win-	



Exercise 1: Prepare MEL-DC and ADL-DC	426
Exercise 2: Deploy FSRM	427
Exercise 3: Configure quota templates and quotas	428
Exercise 4: Create file groups, file screen templates, apply file screens, and apply file screen exceptions	435
Exercise 5: Configure file classification	440
Exercise 6: Verify the classification	442
Exercise 7: Configure file access auditing	444
Exercise 8: Create and assign an iSCSI target	448
Exercise 9: Connect to an iSCSI target	454
Exercise 10: Create a new storage pool and thin provisioned virtual disk	456
Exercise 11: Install the iSNS server and register the initiator	460
Exercise 12: Remove feature files	463
Exercise 13: Configure BranchCache policies	466
Exercise 14: Deploy BranchCache on Windows Server 2012	470
Suggested practice exercises	473
Answers	474
Lesson 1	474
Lesson 2	475

## **Chapter 7 High availability 477**

Before you begin	477
Lesson 1: Configure and manage failover clustering	477
Failover clustering	478
Cluster Quorum Modes	479
Cluster storage and cluster shared volumes	481
Cluster-Aware Updating	484
Migrating and upgrading clusters	486
Failover and preference settings	487
Continuously available shares	489
Lesson summary	490
Lesson review	491
Lesson 2: Network Load Balancing	492
Network Load Balancing	492

Network Load Balancing prerequisites	494
NLB cluster operation modes	495
Managing cluster hosts	496
Port rules	498
Filtering and affinity	499
Upgrading an NLB cluster	500
New NLB PowerShell cmdlets	501
Lesson summary	502
Lesson review	502
Practice exercises	504
Exercise 1: Prepare ADL-DC, MEL-DC, and CBR-DC for exercises	504
Exercise 2: Install the Network Load Balancing feature on ADL-DC, CBR-DC, and MEL-DC	506
Exercise 3: Create a three-node NLB cluster	507
Exercise 4: Configure port rules and affinity	511
Exercise 5: Remove an NLB cluster	513
Exercise 6: Create shared storage for failover clustering	515
Exercise 7: Connect potential cluster nodes to shared storage	517
Exercise 8: Install failover cluster features	523
Exercise 9: Validate cluster configuration	524
Exercise 10: Create a two-node failover cluster	525
Exercise 11: Add a cluster node	527
Exercise 12: Change the quorum configuration	529
Exercise 13: Install and configure a highly available file server	531
Exercise 14: Configure a highly available file share	533
Exercise 15: Configure failover settings, failback settings, and move node	536
Exercise 16: Simulate unplanned failure	539
Exercise 17: Cluster-Aware Updating	540
Suggested practice exercises	547
Answers	548
Lesson 1	548
Lesson 2	549

<b>Chapter 8</b>	<b>Virtual machine and site resilience</b>	<b>551</b>
	Before you begin.....	551
	Lesson 1: Virtual machine movement.....	551
	Virtual machine failover clustering	552
	Shared Nothing Hyper-V Live Migration	556
	Storage Migration	559
	Virtual machine import and export	562
	Lesson summary	564
	Lesson review	564
	Lesson 2: Site-level fault tolerance.....	565
	Hyper-V Replica	566
	Multisite clustering	575
	Lesson summary	576
	Lesson review	577
	Practice exercises.....	578
	Exercise 1: Install the Hyper-V role on MEL-HV-1 and MEL-HV-2	580
	Exercise 2: Configure identical virtual switches on MEL-HV-1 and MEL-HV-2	586
	Exercise 3: Prepare servers for live migration	589
	Exercise 4: Prepare servers for replication	591
	Exercise 5: Create two virtual machines on MEL-HV-1	595
	Exercise 6: Configure TEST-ONE for replication	599
	Exercise 7: View replication health and perform planned failover of TEST-ONE to MEL-HV-2	603
	Exercise 8: Configure Hyper-V to support live migration	605
	Exercise 9: Perform live migration of TEST-TWO	606
	Exercise 10: vPerform storage migration	609
	Exercise 11: Perform a virtual machine export	611
	Exercise 12: Import a copy of a virtual machine	612
	Exercise 13: Perform an unplanned failover	613
	Exercise 14: Enable reverse replication	614
	Suggested practice exercises.....	616
	Answers.....	617
	Lesson 1	617
	Lesson 2	618

<b>Chapter 9 DAC and AD RMS</b>	<b>621</b>
Before you begin.....	621
Lesson 1: Implement Dynamic Access Control (DAC).....	621
Introduction to Dynamic Access Control	622
Configuring group policy to support DAC	623
Configuring user and device claims	623
Configuring resource properties	625
Central access rules	628
Central access policies	630
Staging	632
Access Denied Assistance	633
Lesson summary	634
Lesson review	635
Lesson 2: Install and configure Active Directory Rights Man- agement Services (AD RMS) .....	636
Installing AD RMS	636
AD RMS certificates and licenses	638
AD RMS templates	639
AD RMS Administrators and Super Users	642
Trusted user and publishing domains	644
Exclusion policies	645
Apply AD RMS templates automatically	646
Lesson summary	647
Lesson review	648
Practice exercises .....	649
Exercise 1: Prepare MEL-DC and ADL-DC	649
Exercise 2: Enable group policy support for DAC	651
Exercise 3: Create users and groups	653
Exercise 4: Configure user and device claims	658
Exercise 5: Configure Resource Properties	664
Exercise 6: Prepare server for file classification	666
Exercise 7: Create a file classification rule	668
Exercise 8: Run and verify the file classification	677
Exercise 9: Create central access rules	679

Exercise 10: Create a central access policy	683
Exercise 11: Configure Access Denied Assistance	686
Exercise 12: Configure staging	688
Exercise 13: Prepare infrastructure for an AD RMS deployment	691
Exercise 14: Install and configure the AD RMS server role	695
Exercise 15: Create the AD RMS Super Users group	703
Exercise 16: Create AD RMS templates	705
Exercise 17: Configure template distribution	710
Exercise 18: Configure application exclusions	712
Exercise 19: Apply RMS templates using file classification	712
Suggested practice exercises	716
Answers	717
Lesson 1	717
Lesson 2	718

## **Chapter 10 Active Directory Federation Services 721**

Before you begin	721
Lesson 1: Implement Active Directory Federation Services	721
AD FS Components	722
Claims, claim rules, and attribute stores	722
Claims provider	723
Relying party	724
Relying party trust	724
Claims provider trust	725
Configuring certificate relationship	726
Attribute stores	727
Claims rules	728
Configure AD FS proxy	730
Lesson summary	730
Lesson review	731
Practice exercises	732
Exercise 1: Prepare separate forests	732
Exercise 2: Configure DNS forwarding	734
Exercise 3: Deploy AD CS in each forest	737

Exercise 4: Prepare SYD-DC for certificate publication	740
Exercise 5: Prepare MEL-DC for certificate publication	745
Exercise 6: Configure CA trust in each forest	750
Exercise 7: Acquire certificates for each server.	752
Exercise 8: Deploy AD FS in each forest	756
Exercise 9: Configure relying party trust	766
Exercise 10: Configure Claims Provider Trust	768
Exercise 11: Prepare claim data	769
Exercise 12: Configure Claim Rules	771
Suggested practice exercises . . . . .	779
Answers. . . . .	780
Lesson 1	780
 <i>Index</i>	 781

---

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

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

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



# Introduction

---

When Microsoft puts together exam objectives for an exam, it doesn't randomly select pages from TechNet. Instead, in conjunction with subject matter experts and representatives of the product team, it puts together a list of tasks and areas of knowledge that represents what someone in a specific job role would do and need to know on a day-to-day, a weekly, or even a monthly basis.

Each exam maps to a different job role. The objectives for the 70-412 exam are a list of tasks and areas of knowledge that describe what an advanced administrator of the Windows Server 2012 operating system with several years of on-the-job experience (managing other server operating systems as well as Windows Server 2012) does and understands. These topics include some that experienced administrators may not have encountered before or have limited experience with, such as Active Directory Rights Management Services and Active Directory Federation Services.

This book covers the majority of the topics and skills that are the subject of the Microsoft certification exam 70-412. The idea behind this book is that by reading it and by performing the extensive practice exercises at the end of each chapter in your own lab, you can learn how to perform tasks with the technologies addressed by the exam. By performing the tasks yourself in a test environment, you'll learn enough about how these technologies work that you'll be able to leverage that knowledge in your real-world role as a Windows Server 2012 administrator. Reading and performing the lab exercises in this book will assist you in preparing for the exam, but it's not a complete exam preparation solution. If you are preparing for the exam, you should use additional study materials, such as practice tests and the forthcoming *Exam Ref 70-412: Configuring Advanced Windows Server 2012 Services* to help bolster your real-world experience.

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

- Configure and manage high availability
- Configure file and storage solutions
- Implement business continuity and disaster recovery
- Configure network services
- Configure the Active Directory infrastructure
- Configure identity and access solutions

## System requirements

---

The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. This book is designed assuming you will be using Hyper-V—either the client version available with some editions of Windows 8 or the version available in Windows Server 2012. You can use other virtualization software instead, such as VirtualBox or VMWare Workstation, but the practice setup instructions later in this introduction assume that you are using Hyper-V.

## Hardware and software requirements

This section presents the hardware requirements for Hyper-V 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, except for in Chapter 8, which requires two identical computers.

The 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. (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. (Note: You can run Windows Virtual PC without Intel-VT or AMD-V.) If you want to use Hyper-V on Windows 8, you need a processor that supports Second Layer Address Translation (SLAT).
- 8 gigabytes (GB) of RAM (more is recommended).
- 250 GB of available hard disk space.
- Internet connectivity.

### Software requirements

The following software is required to complete the practice exercises:

- Windows Server 2012 evaluation. You can download an evaluation edition of Windows Server 2012 in ISO format from the Windows Server and Cloud Platform website at <http://www.microsoft.com/server>.

# Virtual machine setup instructions

---

This set of exercises contains abbreviated instructions for setting up the SYD-DC, MEL-DC, ADL-DC, and CBR-DC computers used in the practice exercises in all chapters of this training kit. To perform these exercises, first install Windows Server 2012 Standard edition using the default configuration, setting the administrator password to Pa\$\$w0rd.

## **EXERCISE 1** SYD-DC to function as a Windows Server 2012 domain controller

1. Log on to the first computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa\$\$w0rd.

2. Open an elevated PowerShell prompt and issue the following command:

```
cmd
```

3. Enter the following command:

```
Netsh interface ipv4 set address "Ethernet" static 10.10.10.10
```

4. Enter the following command:

```
netdom renamecomputer %computename% /newname:SYD-DC
```

5. Restart the computer and log back on using the Administrator account.

6. Open an elevated PowerShell prompt and issue the following command:

```
Add-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

7. Open the Server Manager console. Click the Refresh icon.

8. Click on the Notifications icon and then click Promote This Server to Domain Controller.

9. On the Deployment Configuration page, choose Add a New Forest. Enter **Contoso.com** as the root domain name and then click Next.

10. On the Domain Controller Options page, configure the following settings and then click Next:

- Forest Functional Level: Windows Server 2012
- Domain Functional Level: Windows Server 2012
- Specify Domain Controller Capabilities:
  - Domain Name System (DNS) Server
  - Global Catalog
- DSRM Password: Pa\$\$w0rd

11. On the DNS Options page, click Next.
12. On the Additional Options page, click Next.
13. Accept the default settings for the Database, Log Files, and SYSVOL locations and click Next.
14. On the Review Options page, click Next.
15. On the Prerequisites Check page, click Install.
16. The computer will restart automatically.

### **EXERCISE 2 Prepare Active Directory Domain Server (AD DS)**

1. Log on to server SYD-DC using the Administrator account.
2. Using Active Directory Users and Computers, create a user account named don\_funk in the Users container and assign the account the password Pa\$\$w0rd. Configure the password to never expire. Add this user account to the Enterprise Admins, Domain Admins, and Schema Admins groups.
3. Open the DNS console and create a primary IPv4 Reverse Lookup Zone for the subnet 10.10.10.x. Ensure that the zone is stored within AD DS and is replicated to all DNS servers running on domain controllers in the forest and allows only secure dynamic updates.

### **EXERCISE 3 Prepare ADL-DC**

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the second computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa\$\$w0rd.
3. Open an elevated PowerShell prompt and issue the following commands:

```
cmd
```

```
Netsh interface ipv4 set address "Ethernet" static 10.10.10.20
```

```
Netsh interface ipv4 set dnsservers "Ethernet" static 10.10.10.10 primary
```

4. Enter the following command:

```
netdom renamecomputer %computername% /newname:ADL-DC
```

5. Restart the computer and then log on again using the Administrator account.
6. Shut down the computer.

#### **EXERCISE 4 Prepare CBR-DC**

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the third computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa\$\$w0rd.
3. Open an elevated PowerShell prompt and issue the following commands:

```
cmd
```

```
Netsh interface ipv4 set address "Ethernet" static 10.10.10.30
```

```
Netsh interface ipv4 set dnsservers "Ethernet" static 10.10.10.10 primary
```

4. Enter the following command:

```
netdom renamecomputer %computername% /newname:CBR-DC
```

5. Restart the computer and then log on again using the Administrator account.
6. Shut down the computer.

#### **EXERCISE 5 Prepare MEL-DC**

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the third computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa\$\$w0rd.
3. Open an elevated PowerShell prompt and issue the following commands:

```
cmd
```

```
Netsh interface ipv4 set address "Ethernet" static 10.10.10.40
```

```
Netsh interface ipv4 set dnsservers "Ethernet" static 10.10.10.10 primary
```

4. Enter the following command:

```
netdom renamecomputer %computername% /newname:MEL-DC
```

5. Restart the computer and then log on again using the Administrator account.
6. Shut down the computer.

### **EXERCISE 6** Snapshot all virtual machines

1. Snapshot all virtual machines. This is the state that they need to be in prior to performing exercises.

## **Acknowledgments**

---

I'd like to thank the following people for their dedication and help in getting this book written: Troy Mott, Randall Galloway, Christopher Hearse, Michael Bolinger, and Charlotte Kughen. I'd also like to thank Oksana and Rooslan for their patience with me during the writing process.

## **Errata & book support**

---

We 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 at:

*<http://aka.ms/TGCA2012S/errata>*

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, send an email to Microsoft Press Book Support at [mspinput@microsoft.com](mailto:mspinput@microsoft.com).

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

## **We want to hear from you**

---

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

*<http://aka.ms/tellpress>*

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>.



# Advanced Active Directory infrastructure

If you are the administrator of a medium to large organization, it is likely that you are responsible for managing multiple domains, perhaps even multiple forests, rather than managing a single domain forest. In this chapter you discover how and why you would configure forests with multiple domain trees and the benefits of each functional level. You also find out how to configure and manage different types of trust relationships to ensure users in one forest or domain are granted appropriate access to resources in another forest, domain, or Kerberos realm.

## Lessons in this chapter:

- Lesson 1: Configure domains and forests
- Lesson 2: Configure trusts

## Before you begin

---

To complete the practice exercises in this chapter, you need to have deployed computers SYD-DC, MEL-DC, CBR-DC, and ADL-DC as described in the Introduction, using the evaluation edition of Windows Server 2012.

## Lesson 1: Configuring domains and forests

---

As an experienced administrator you're probably quite familiar with the configuration of single domain Active Directory forests. In this lesson, you find out more about multidomain and multiforest environments. You discover how to upgrade an existing domain and forest so that it uses only Windows Server 2012 domain controllers, and you find out how to configure UPN suffixes.

### After this lesson, you will be able to

- Understand multidomain Active Directory environments
- Understand multiforest Active Directory environments
- Upgrade existing domains and forests
- Configure multiple user principal name (UPN) suffixes

Estimated lesson time: 45 minutes

## Multidomain Active Directory environments

The majority of current Active Directory deployments in small- and medium-sized enterprises have a single domain. This hasn't always been the case because earlier versions of the Windows Server operating system, such as Windows NT4, supported far fewer user accounts. Supporting a smaller number of accounts often necessitated the use of multiple domains, and it wasn't unusual to see medium-sized organizations that used complicated domain structures.

Each Windows Server 2012 domain controller can create approximately 2.15 billion objects during its lifetime, and each domain supports the creation of up to approximately 2.15 billion relative identifiers (*RIDs*). Given these statistics, few administrators implement multiple domain forests because they need to support a large number of users. Of course, in very large organizations, the replication load between sites might make a domain with several hundred thousand user accounts problematic, but site and replication considerations are covered in Chapter 2, "Active Directory sites and replication."

There are many reasons why organizations implement multidomain forests. These can include but are not limited to:

- **Historical domain structure** Even though newer versions of the Windows Server operating system handle large numbers of objects more efficiently, some organizations have retained the forest structure that was established when the organization first adopted Active Directory.
- **Organizational or political reasons** Some organizations are conglomerates, and they might be composed of separate companies that share a common administrative and management core. An example of this is a university faculty in Europe or Australia, such as a Faculty of Science, that is composed of different departments or schools,

such as the school of physics and the department of botany. For political or organizational reasons it might have been decided that each department or school should have its own domain that is a part of the overall faculty forest. Active Directory gives organizations the ability to create domain namespaces that meet their needs, even if those needs might not directly map to the most efficient way of accomplishing a goal from a strict technical perspective.

- **Security reasons** Domains enable you to create security boundaries so that you can have one set of administrators who are able to manage computers and users in their own domain, but who are not able to manage computers and users in a separate domain. Although it's possible to accomplish a similar goal by delegating privileges, many organizations prefer to use separate domains to accomplish this goal.

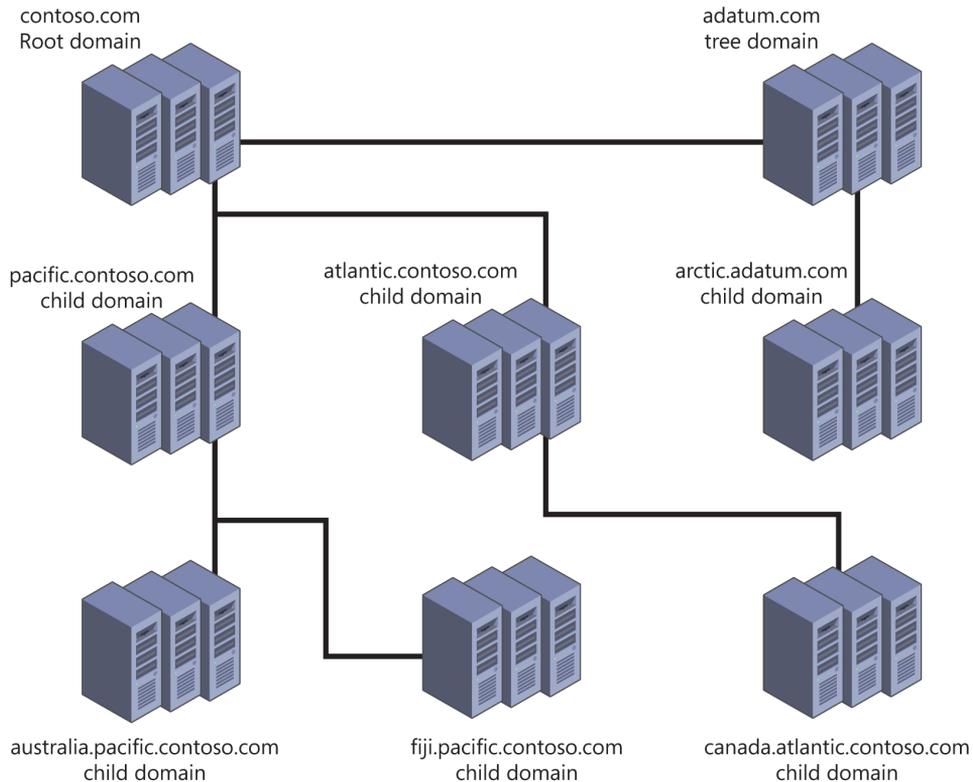
#### **REAL WORLD POLITICS TRUMPS TECHNOLOGY**

It is very important to understand that geeks often see technology as something completely separate from organizational politics, with the most efficient technical solution being the best, but everyone else doesn't necessarily share this perception. When I worked as a systems administrator at an Australian University, there was a shared room in one building that hosted two different printers used by different departments, even though the departments were part of the same faculty. People in each department felt strongly that the printer should be labeled with a departmental identity on the network and that users from one department should, under no circumstances, be able to print to the printer owned by the other department. Although the machinations of interdepartmental politics are usually of little interest to the geeks in the information technology (IT) department, administrators who ignore unclearly defined boundaries do so at their own peril.

## Domain trees



A domain tree is a set of names that share a common *root domain* name. For example contoso.com can have pacific.contoso.com and atlantic.contoso.com as child domains, and these domains can have child domains themselves. A forest can have multiple *domain trees*. When you create a new tree in a forest, the root of the new tree is a *child domain* of the original root domain. In Figure 1-1, adatum.com is the root of new domain tree in the contoso.com forest.



**FIGURE 1-1** Contoso.com as the root domain in a two-tree forest

The depth of a domain tree is limited by a maximum fully qualified domain name (FQDN) length for a host of 64 characters. This means that the host name and the domain name combined cannot exceed 64 characters, including the periods that separate each component of the name. For example, the name `3rd-floor-printer` could not be used in the `melbourne.victoria.australia.pacific.contoso.com` domain because it cannot be used as a hostname in an Active Directory forest as the hostname exceeds the 64-character limit.

## Intra-forest authentication

All domains within the same forest automatically trust one another. This means that in the environment shown in Figure 1-1, you can assign a user in the `Australia.pacific.contoso.com` permissions to a resource in the `arctic.adatum.com` domain without performing any extra configuration.



Because of the built-in automatic *trust relationships*, a single forest implementation is not appropriate for separate organizations, even when they are in partnership with one another. A single forest makes it possible for one or more users to have administrative control. Most organizations aren't comfortable even with trusted partners having administrative control over their IT environments. When you do need to allow users from partner organizations to

have access to resources, you can configure trust relationships or federation. You read more about trust relationships in Lesson 2 of this chapter and more about federation in Chapter 10, “Active Directory Federation Services.”

## Domain functional levels



Domain functional levels determine the Active Directory functionality and features that are available. The higher the *domain functional level* is, the more functionality and features are available. You can use Windows Server 2012 domain controllers with the following domain functional levels:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

The limiting factor on a domain functional level is the domain controllers used to host Active Directory. If your organization has Windows Server 2003 domain controllers, you aren’t able to raise the functional level until you replace or upgrade those domain controllers to a more recent version of the Windows Server operating system.

You can alter the domain functional level using the Active Directory Users and Computers console, the Active Directory Domains and Trusts console as shown in Figure 1-2, or the Set-ADDomainMode Windows PowerShell cmdlet. Your account needs to be a member of the Domain Admins or Enterprise Admins groups to perform this operation.



**FIGURE 1-2** Raise or verify the domain functional level

### WINDOWS SERVER 2003 FUNCTIONAL LEVEL

The Windows Server 2003 domain functional level is the lowest level at which you can introduce domain controllers running the Windows Server 2012 operating system. You can set this functional level if you have domain controllers running the Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 operating systems. The Windows Server 2003 domain functional level includes the following features, which are also available at higher domain functional levels:



- The LastLogonTimestamp attribute records a user's last domain logon.
- *Constrained Delegation* enables applications to securely delegate user credentials.
- *Selective authentication* enables you to configure specific resources in the forest so that only certain users and groups can authenticate. The default is to allow all users in the forest to authenticate before permissions to those resources are checked.
- Support for storing DNS zones in custom application partitions enables you to selectively replicate DNS zones to specific domain controllers that are enrolled in the custom partitions, rather than requiring that you configure replication to all domain controllers in the domain or the forest.
- Attribute-level replication for group and other multivalued attributes. Rather than replicating the whole Active Directory object, only altered attributes will be replicated.

### WINDOWS SERVER 2008 FUNCTIONAL LEVEL

The Windows Server 2008 domain functional level requires that all domain controllers be running the Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 operating systems. The Windows Server 2008 domain functional level includes all the features available at the Windows Server 2003 functional level as well as the following:

- Improvements in Distributed File System (DFS) replication that make it possible for replication to occur more efficiently
- Support for fine-grained password policies, which enables you to apply multiple separate password policies within the same domain
- Support for Personal Virtual Desktops through RemoteApp and Remote Desktop when used with Hyper-V
- AES (Advanced Encryption Services) 128 and 256 Kerberos support

### WINDOWS SERVER 2008 R2 FUNCTIONAL LEVEL

The Windows Server 2008 R2 domain functional level requires that all domain controllers are running the Windows Server 2008 R2 or Windows Server 2012 operating systems. This functional level supports the features of the Windows Server 2003 and Windows Server 2008 domain functional levels as well as:

- Managed service account support, which enables you to automatically manage service account passwords rather than manually managing them
- Support for command-line-based Active Directory Recycle Bin if the forest functional level is raised to Windows Server 2008 R2

### WINDOWS SERVER 2012 FUNCTIONAL LEVEL

The Windows Server 2012 domain functional level requires that all domain controllers be running the Windows Server 2012 operating system. This functional level supports the features of all the lower functional levels as well as:

- Group managed service accounts, which enable you to install a single managed service account on multiple computers.
- Fine-Grained Password Policies through the Active Directory Administrative Center rather than by editing them using ADSI Edit.
- Active Directory Recycle Bin through Active Directory Administrative Center rather than through command-line utilities if the forest is configured at the Windows Server 2012 forest functional level.
- If the Key Distribution Center (KDC) support for claims, compound authentication, and Kerberos armoring is set to Always Provide Claims or Fail Unarmored Authentication Requests, these options aren't available unless the domain is raised to the Windows Server 2012 functional level.

## Forest functional levels

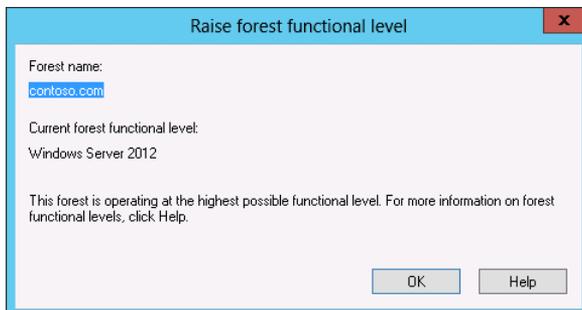


A forest can host domains running at different domain functional levels. *Forest functional level* is dependent on the minimum domain functional level of any domain in your forest. For example, if your organization has one domain running at the Windows Server 2008 functional level and all other domains running at the Windows Server 2012 functional level, you can't raise the forest functional level beyond Windows Server 2008. After you raise that one domain from the Windows Server 2008 functional level to the Windows Server 2012 domain functional level, you're also able to raise the forest functional level to Windows Server 2012.

### **MORE INFO FUNCTIONAL LEVELS**

To learn more about functional levels, consult the following link: [http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx).

You can raise the forest functional level using the Active Directory Domains and Trusts console, as shown in Figure 1-3, or using the Set-ADForestMode Windows PowerShell cmdlet. You need to use a user account that is a member of the Enterprise Admins group to perform this task. In general you can't lower the forest functional level after you've raised it. The exception to this rule is that you can lower the forest functional level from Windows Server 2012 to Windows Server 2008 R2 if you haven't enabled Active Directory Recycle Bin.



**FIGURE 1-3** Raise the forest functional level

Although Active Directory Recycle Bin becomes available at the Windows Server 2008 R2 forest functional level, you need to have configured your organization's forest to run at the Windows Server 2012 forest functional level to be able to use the Active Directory Administrative Center interface as opposed to the command-line interface. Setting the Windows Server 2012 forest functional level does not introduce other features, but it limits the forest to using only domain controllers running Windows Server 2012 or more recent versions of the Windows Server operating system.



#### **Quick check**

- What is the minimum forest functional level that enables you to implement Active Directory Recycle Bin?

#### **Quick check answer**

- You can implement Active Directory Recycle Bin at the Windows Server 2008 R2 forest functional level.

## Multiforest Active Directory environments

Not only do many organizations have more than one domain in their forest, but some organizations have multiple Active Directory forests. Multiple forests often result when organizations merge, during the period before the acquiring organization has subsumed the acquired organization's infrastructure.

Other reasons for having multiple Active Directory forests within a single organization include:

- **Security requirements** You can ensure that administrators of one part of the organization have no rights over another part of the organization by having each part of the organization in a separate forest.
- **Incompatible schemas** All domains in a forest share a schema. If two separate schemas are required for two different parts of the organization, it is necessary to implement multiple forests.
- **Political requirements** Multinational organizations might have to deal with different jurisdictional requirements. It might be simpler to meet these requirements by hav-

ing separate forests with trust relationships than it is to attempt to configure domains within the same forest to meet these different compliance benchmarks.

## Upgrading existing domains and forests

You can use one of two strategies when upgrading an existing domain so that you can configure it at the Windows Server 2012 functional level:

- The first strategy is to upgrade the operating systems on each domain controller to Windows Server 2012. This method can be problematic because many organizations are running Windows Server 2003 on domain controllers, and you can't directly upgrade Windows Server 2003 to Windows Server 2012. It's also likely that existing domain controllers are running an x86 version of a Windows Server operating system. Windows operating systems never support direct upgrades from x86 versions to x64 versions.
- You can introduce Windows Server 2012 domain controllers into an existing domain and then decommission existing domain controllers running earlier versions of the Windows Server operating system. This method is less complex than performing a direct upgrade. If the hardware supports it, you can repurpose the existing hardware so that the decommissioned domain controllers have a new purpose as Windows Server 2012 domain controllers (although an increasing number of organizations have domain controllers run on virtual machines).

Unlike previous domain controller upgrades, you don't need to run `adprep.exe` directly to prepare Active Directory for the introduction of domain controllers running Windows Server 2012. Instead, if you promote the first Windows Server 2012 domain controller using an account that is a member of the Schema Admins and Enterprise Admins group, the schema upgrade occurs automatically. You need to run `adprep.exe` separately only if you are performing an in-place upgrade of a domain controller running an x64 version of Windows Server 2008 or Windows Server 2008 R2 and if this upgraded domain controller will be the first Windows Server 2012 domain controller in the domain.

### **NOTE** ACTIVE DIRECTORY MIGRATION TOOL

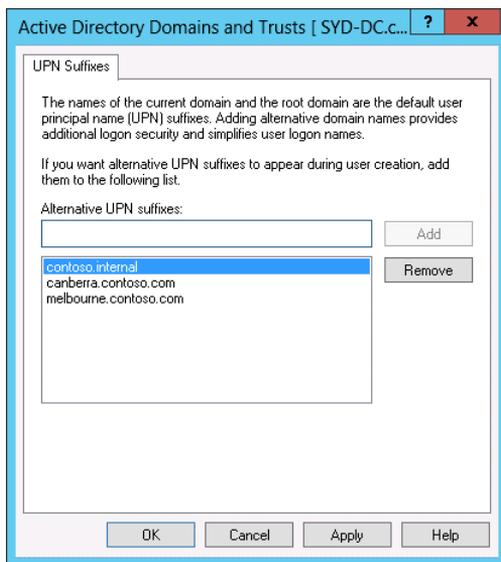
The Active Directory Migration Tool can assist you in migrating from an existing Active Directory environment rather than upgrading an existing environment. Version 3.2 of the Active Directory Migration Tool isn't supported on Windows Server 2012.



## User Principal Name (UPN) suffixes

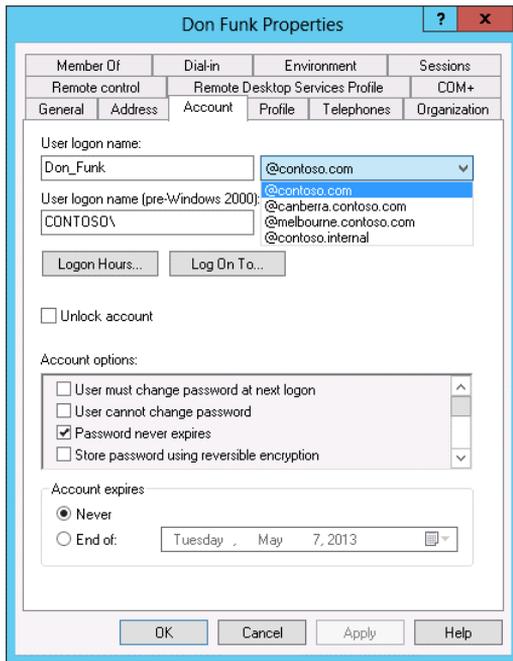
*User Principal Name (UPN) suffixes* are the part of a user's UPN that trails the @ symbol. For example, in the UPN don\_funk@contoso.com, the UPN suffix is the domain name contoso.com. UPN suffixes enable users to sign on using an account name that includes the name of their domains. Because UPN suffixes look like email addresses, users find them easy to remember. This is useful in complex environments where users might be logging on to computers that are members of domains that are different from the domains that host their accounts. For example, Kim Aker's user account might be located in the accounts.contoso.com domain, but she needs to sign on to a computer that is a member of the computers.contoso.com domain. Rather than having to sign on as accounts\kim\_akers as her user name, or selecting the accounts domain from a list, she can instead sign on using the UPN of kim\_akers@contoso.com.

By default, all users use the UPN suffix that is the name of the root domain, even if their accounts are in a child domain. This is why Kim is able to sign on as kim\_akers@contoso.com as contoso.com is the UPN suffix of the root domain. You configure UPN suffixes using the Active Directory Domains and Trusts console as shown in Figure 1-4.



**FIGURE 1-4** Configure alternative UPN suffixes

You can configure the UPN suffix associated with a specific user account on the Account tab of the user account's properties through the Active Directory Users and Computers console as shown in Figure 1-5. When you are configuring forest trusts, you can block or allow user authentication based on UPN suffix.



**FIGURE 1-5** Configure a specific UPN suffix

#### **MORE INFO UPN SUFFIXES**

To learn more about UPN suffixes, consult the following link <http://technet.microsoft.com/en-us/library/cc772007.aspx>.

## Lesson summary

- A forest can contain multiple domains. Domain trees build on the same namespace. A forest can contain multiple domain trees.
- No hostname in an Active Directory forest can exceed 64 characters.
- The domain functional level is dependent on the earliest version of the Windows Server operating system used on a domain controller in a domain.
- A domain functional level defines the minimum version of the Windows Server operating system that can be used on domain controllers.
- Each domain in a forest can have a different functional level. The forest functional level depends on the lowest domain functional level in the forest.
- You can configure custom UPN suffixes to simplify the sign-on process for users in multidomain and multiforest environments.

## 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 each answer choice in the “Answers” section at the end of this chapter.

- 1.** You are in the process of designing a new Active Directory implementation for your organization. Two different departments in your organization will be adopting applications that have separate and mutually exclusive Active Directory schema requirements. Which of the following Active Directory structures should you use in your design to accommodate these requirements?

  - A.** A single forest with a single domain tree
  - B.** A single forest with multiple domain trees
  - C.** Multiple forests
  - D.** A single domain forest
- 2.** You are the systems administrator for Tailspin Toys and its subsidiary company Wingtip Toys. You are in the process of designing a new Active Directory structure. You’ve been asked to ensure that employees who work in the Tailspin Toys part of the organization log into a domain named tailspintoys.com and that employees who work in the Wingtip Toys part of the organization log into a domain named wingtip toys.com. You want to do this in the simplest way possible and minimize the creation of trust relationships. Which of the following Active Directory structures should you use in your design to accommodate these requirements?

  - A.** A single domain forest
  - B.** Multiple forests
  - C.** A single forest with multiple domain trees
  - D.** A single forest with a single domain tree
- 3.** You want to deploy several domain controllers running the Windows Server 2012 operating system. You will eventually decommission existing domain controllers and bring the domain up to the Windows Server 2012 domain functional level. What is the minimum domain functional level required to support the introduction of domain controllers running the Windows Server 2012 operating system?

  - A.** Windows Server 2003 domain functional level
  - B.** Windows Server 2008 domain functional level
  - C.** Windows Server 2008 R2 domain functional level
  - D.** Windows Server 2012 domain functional level
- 4.** At which forest functional levels is the Active Directory Recycle Bin available? (Choose all that apply.)

- A. Windows Server 2012 forest functional level
- B. Windows Server 2008 R2 forest functional level
- C. Windows Server 2008 forest functional level
- D. Windows Server 2003 forest functional level

## Lesson 2: Configuring trusts

---

From time to time it's necessary to connect two different domains so that users who have accounts in one domain are able to access resources in another domain. If those domains are owned by the same organization, the simplest way of doing this is by configuring a trust. In this lesson you find out how to configure trusts between two different forests, between two separate domains in different forests, and between a domain and a Kerberos realm.

### After this lesson, you will be able to:

- Configure external, forest, shortcut, and realm trusts
- Configure trust authentication
- Configure SID filtering
- Configure name suffix routing

**Estimated lesson time: 45 minutes**

## Trusts

Trusts make it possible for users in one domain to be authenticated by domain controllers in a separate domain. For example, if there is a bidirectional trust relationship between the domains `contoso.local` and `adatum.remote`, users with accounts in the `contoso.local` domain are able to authenticate in the `adatum.remote` domain. By configuring a trust relationship, it's possible to allow users in one domain to access resources in another, such as being able to use shared folders and printers or being able to sign on locally to machines that are members of a different domain than the one that holds the user's account.

 Some trusts are created automatically. For example, domains in the same forest automatically trust each other. Other trusts, such as *external trusts*, *realm trusts*, *shortcut trusts*, and *forest trusts* must be created manually. Trusts use the Kerberos V5 authentication protocol by default, and they revert to NTLM if Kerberos V5 is not supported. You configure and manage trusts using the Active Directory Domains and Trusts console or the `netdom.exe` command-line utility with the trust switch.

### **REAL WORLD UNDERSTANDING TRUSTS**

Although trusts themselves are relatively easy to come to terms with, the terminology around trusts tends to confuse many people. It's important that you understand the difference between a trusting and a trusted domain and how trust direction, incoming or outgoing, relates to which security principals are able to authenticate.

To understand trusts, you need to understand the difference between a trusting domain or forest and a trusted domain or forest. The trusting domain or forest contains the resources to which you want to grant security principals from the trusted domain or forest access. The trusted domain or forest hosts the security principals that you want to allow to access resources in the trusting forest. For example, if you want to grant users in the adatum.remote domain access to resources in the contoso.local domain, the adatum.remote domain is the trusted domain and the contoso.local domain is the trusting domain. In by-directional trust relationships a domain or forest is both trusting and trusted.

### **MORE INFO TRUSTS**

To learn more about the basics of trusts consult the following link: <http://technet.microsoft.com/en-us/library/cc731335.aspx>.

## **Trust transitivity**



A *transitive trust* is one that extends beyond the original trusting domains. For example, if you have a trust between two domain forests and that trust is transitive, all the domains in each of the forests trust each other. Forest trusts are transitive by default. External trusts are not transitive by default. When you create a trust, keep in mind that there may be domains beyond the one you are establishing the relationship with that may be included. You might trust the administrator of adatum.remote not to allow access by nefarious users, but do you trust the administrator of subdomain.adatum.remote?

### **MORE INFO TRUST TRANSITIVITY**

To learn more about trust transitivity, consult the following link: <http://technet.microsoft.com/en-us/library/cc754612.aspx>.

## **Trust direction**

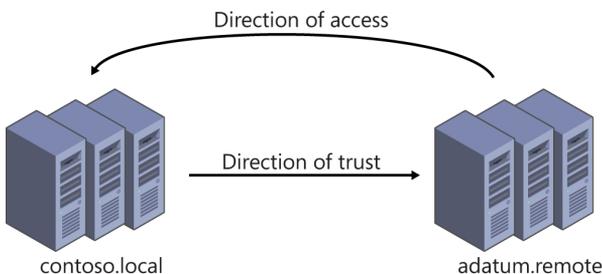
When you create a new trust, you specify a trust direction as shown in Figure 1-6. You can choose a two-way (or bidirectional) trust or a unidirectional trust, which is either one-way incoming or one-way outgoing.



**FIGURE 1-6** Specify the trust direction

When you configure a one-way incoming trust, users in the local are authenticated in the remote domain, realm, or forest. Remember that if you are configuring a one-way incoming trust between the single domain forests contoso.local and adatum.remote, users with accounts in contoso.local are able to access resources in adatum.remote. Similarly if you are configuring a one-way outgoing trust between the single domain forests contoso.local and adatum.remote, users with accounts in adatum.remote are able to access resources hosted in contoso.local.

The terminology around trusts can be a little confusing. The key thing to remember is that the direction of trust is the opposite of the direction of access, as shown in Figure 1-7. An outgoing trust allows incoming access, and an incoming trust allows outgoing access.



**FIGURE 1-7** The direction of trust and direction of access

#### **MORE INFO TRUST DIRECTION**

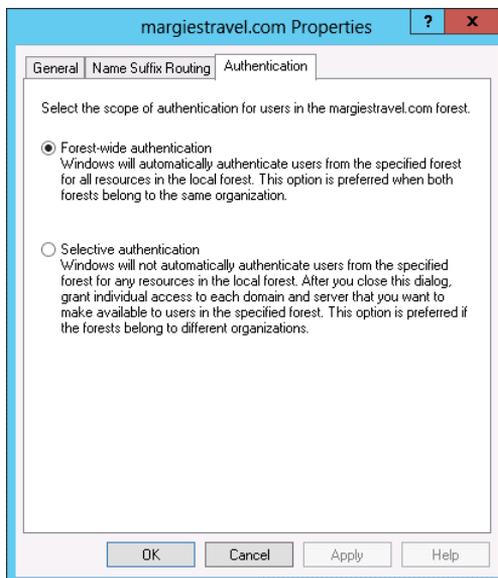
To learn more about trust direction, consult the following link: <http://technet.microsoft.com/en-us/library/cc731404.aspx>.

## Forest trusts

When you configure a forest trust, one Active Directory forest trusts the other one. Forest trusts are transitive. When you configure a forest trust, you can allow any domain in the trusting forest to be accessible to any security principal in the trusted forest. Forest trusts require that each forest be configured to run at the Windows Server 2003 forest functional level or higher. Forest trusts can be bi- or unidirectional. You are most likely to configure forest trusts if your organization has two or more Active Directory forests.

You can configure one of two authentication scopes when you configure a forest trust. The type of authentication scope that you configure depends on your security requirements. The options are:

- **Forest-wide authentication** When you choose forest-wide authentication, users from the trusted forest are automatically authenticated for all resources in the local forest. You should use this option when both the trusted and trusting forest are part of the same organization. Figure 1-8 shows a forest trust configured with this type of authentication.
- **Selective authentication** When you configure this option, Windows does not automatically authenticate users from the trusted forest. You can then configure specific servers and domains within the forest to allow users from the trusted forest to authenticate. Use this option when the two forests are from different organizations, or you have more stringent security requirements.



**FIGURE 1-8** Configure the authentication type

## Configuring selective authentication

Configuring *selective authentication* means granting specific security principals in the trusted forest the Allowed to authenticate (allow) permission on the computer that hosts the resource to which you want to grant access. For example, assume you had configured a forest trust with selective authentication. You want to grant users in the Research universal group from the trusted forest access to a Remote Desktop Services (RDS) server in the trusting forest. To accomplish this goal, you can configure the properties of the RDS server's computer account in Active Directory Users and Computers and grant the Research universal group from the trusted forest the Allowed to authenticate permission as shown in Figure 1-9. Doing this only allows users from this group to authenticate; you still have to grant them access to RDS by adding them to the appropriate local group on the RDS server.

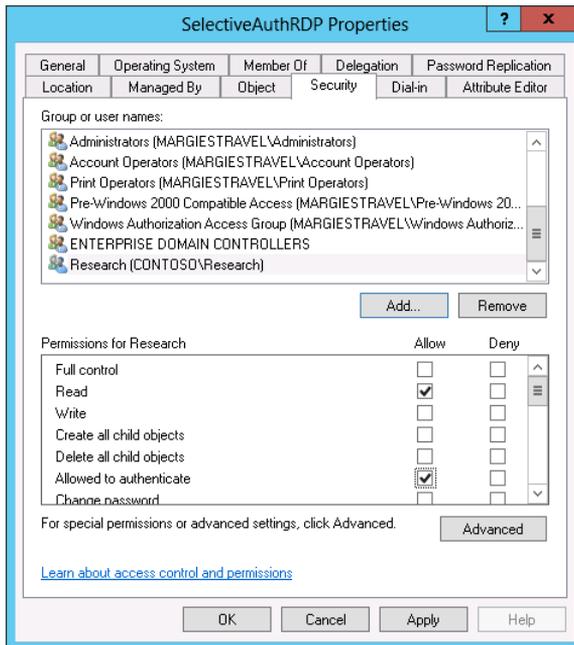


FIGURE 1-9 Configure the Allowed to Authenticate permission

## External Trusts

External trusts enable you to configure one domain in one forest to trust a domain in another forest without enabling a transitive trust. For example, you configure an external trust if you want to allow the auckland.fabrikam.com domain to have a trust relationship with the wellington.adatum.com domain without allowing any other domains in the fabrikam.com or adatum.com forests to have a security relationship with one another.

### **MORE INFO EXTERNAL TRUSTS**

To learn more about external trusts, consult the following link: <http://technet.microsoft.com/en-us/library/cc732859.aspx>.

You can use External Trusts to configure trust relationships with domains running unsupported Windows Server operating systems, such as Windows 2000 Server and Windows NT 4.0, because these operating systems do not support Forest Trusts. Even though these operating systems are well beyond their supported lifespan, there are still organizations out there with servers, and even domains, running these operating systems. It's possible, however unlikely, that you might need to configure a trust relationship between a domain running these operating systems and one running Windows Server 2012 domain controllers.

#### **Quick check**

- You are the administrator of the single domain `contoso.local` forest. Users in the `adatum.remote` single domain forest need to access resources in the `contoso.local` domain. Users in `contoso.local` should not have access to resources in `adatum.remote`. You are configuring an external trust between these two single domain forests from the `contoso.local` domain. Which trust direction should you configure to support this configuration?

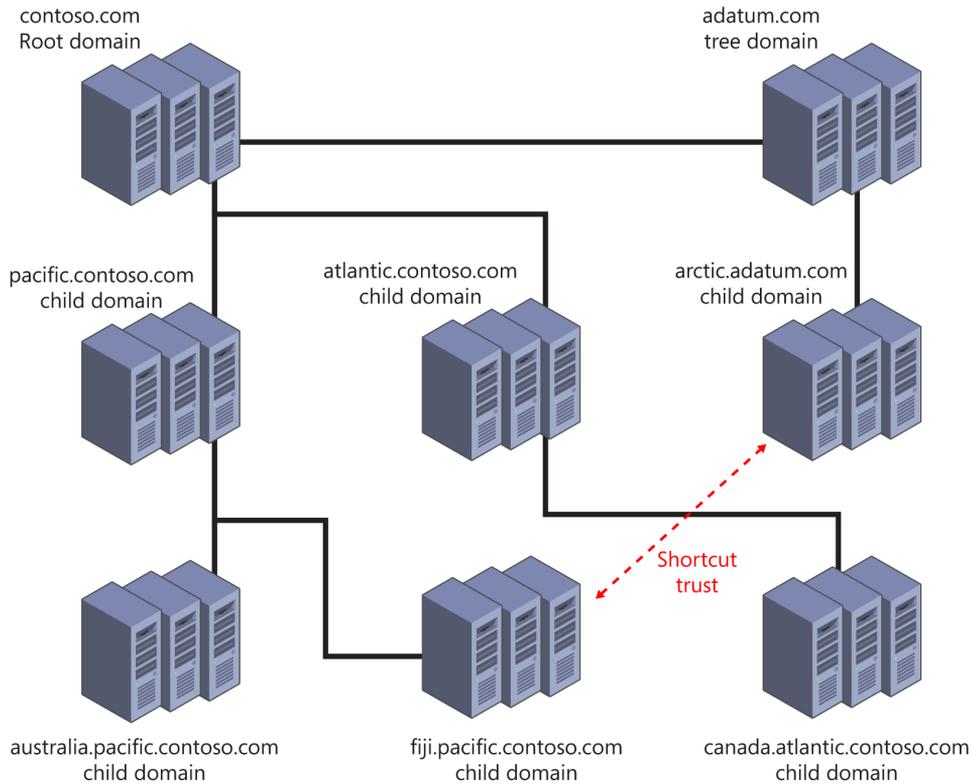
#### **Quick check answer**

- One-way outgoing. Remember that the direction of trust is opposite to the direction of authentication. To have incoming users authenticated, you configure an outgoing trust.

## **Shortcut trusts**

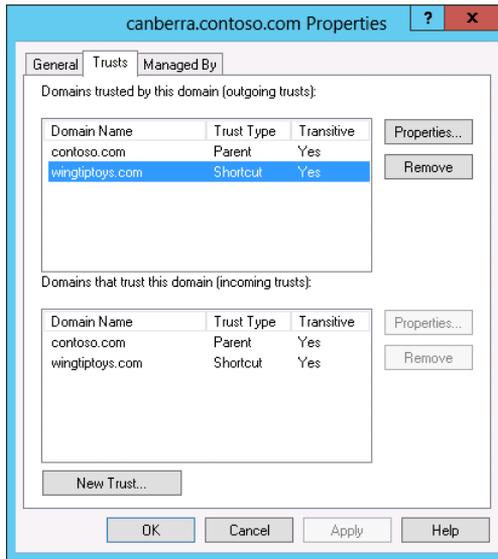


*Shortcut trusts* enable you to speed up authentication between domains in a forest that might be in separate branches or even separate trees. For example, in the hypothetical forest shown in Figure 1-10, if a user in the `fiji.pacific.contoso.com` domain wants to access a resource in the `arctic.adatum.com` domain, authentication needs to travel up through the `pacific.contoso.com` and `contoso.com` domains before passing across to the `adatum.com` domain and finally back to the `arctic.adatum.com`. If you implement a shortcut trust between the `fiji.pacific.contoso.com` and `arctic.adatum.com` domains, authentication traffic instead travels directly between these two domains without having to traverse the two domain trees in the forest.



**FIGURE 1-10** Shortcut trust

You configure a shortcut trust using the Active Directory Domains and Trusts console by editing the properties of one domain and triggering the New Trust Wizard on the Trusts tab. When the trust is created, it is listed as a shortcut trust as shown in Figure 1-11. Shortcut trusts can be uni- or bidirectional. As is the case with the creation of other trusts, ensure that you have name resolution working properly between the trusting and the trusted domains either by having the Domain Name System (DNS) zones propagate through the forest, by configuring conditional forwarders, or by configuring stub zones.



**FIGURE 1-11** A shortcut trust

## Realm trusts

You use a realm trust to create a relationship between an Active Directory Services domain and a Kerberos V5 realm that uses a third-party directory service. Realm trusts can be transitive or nontransitive. They can also be uni- or bidirectional. You're most likely to configure a realm trust when you need to allow users who use a UNIX directory service to access resources in an Active Directory domain or users in an Active Directory domain to access resources in a UNIX Kerberos V5 realm.

You can configure a realm trust from the Active Directory Domains and Trust console. You do this by selecting the Realm trust option as shown in Figure 1-12. When configuring a realm trust, you specify a realm trust password that you use when configuring the other side of the trust in the Kerberos V5 realm.

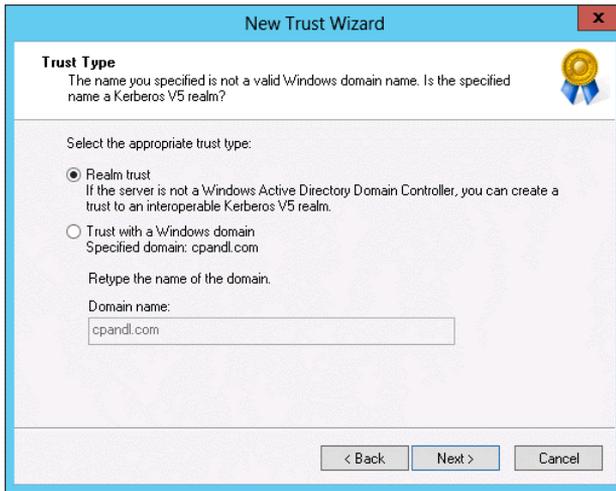


FIGURE 1-12 Configure the realm trust

### MORE INFO REALM TRUSTS

To learn more about realm trusts, consult the following link: <http://technet.microsoft.com/en-us/library/cc731297.aspx>.

## Netdom.exe

You use netdom.exe with the /trust switch to create and manage trusts from the command line. When using netdom.exe, you specify the trusting domain name and the trusted domain name. You can use netdom.exe with the /trust switch to create and manage forest, shortcut, realm, and external trusts.

The syntax of the netdom.exe command with the trust switch is shown in Figure 1-13.

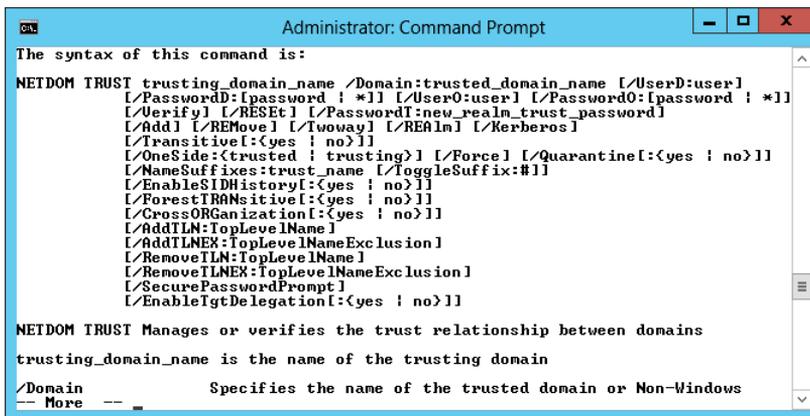


FIGURE 1-13 The command syntax for netdom.exe

At release, Windows PowerShell in Windows Server 2012 does not include much in the way of cmdlets for creating and managing trust relationships beyond the Get-ADTrust cmdlet.

## SID filtering

In a trusted domain, it's possible, though extremely difficult, for you to configure an account in your domain to have SIDs that are identical to those used by privileged accounts in a trusting domain. If you use this configuration then the accounts from trusted domains gain the privileges of the accounts in the trusting domain. For example, you can configure the SIDs of an account in a trusted domain so that it has domain administrator privileges in the trusting domain.



To block this type of configuration, Windows Server 2012 enables *SID filtering*, also known as *domain quarantine*, on all external trusts. SID filtering blocks users in a trusted forest or domain from being able to grant themselves elevated user rights in the trusting forest domain by discarding all SIDs that do not have the domain SID of the trusting domain.

It's possible to verify SID filtering settings on a trust using the Get-ADTrust cmdlet in a Windows PowerShell session run by a user with administrative privileges. For example, to verify that SID filtering is enabled on the trust with the margiestravel.com forest, issue the command:

```
Get-ADTrust margiestravel.com | fl *SID*
```

To disable SID filtering for the trusting forest, use the netdom trust command with the following option:

```
/enablesidhistory:Yes
```

Enabling SID history allows SIDs that don't have the domain SID of the trusting domain. You enable or disable SID filtering on the trusting side of the trust. For example, if you are an administrator in the contoso.com domain and you want to disable SID filtering, you can issue the following command from an elevated command prompt:

```
Netdom trust contoso.com /domain:margiestravel.com /enablesidhistory:Yes
```

In the same scenario, if you want to re-enable SID filtering, you can issue the following command:

```
Netdom trust contoso.com /domain:margiestravel.com /enablesidhistory:No
```

The default configuration, where SID filtering is enforced by default on trusts, is something that you should probably leave as it is. In the past it was necessary to allow SID history when trusts were created with forests running Windows 2000 Server domain controllers. As Windows 2000 is no longer supported by Microsoft, and SID history is not necessary for trust relationships with Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 domain controllers, you probably won't need to disable it.

### MORE INFO SID FILTER QUARANTINING ON EXTERNAL TRUSTS

To learn more about SID filtering, consult the following link: [http://technet.microsoft.com/en-us/library/cc794757\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc794757(v=ws.10).aspx).

## Name suffix routing

*Name suffix routing* enables you to configure how authentication requests are routed when you configure a forest trust between two Active Directory forests. When you create a forest trust, all unique name suffixes are routed. Name suffix routing assists when users sign on with a UPN, such as don\_funk@contoso.com. Depending upon the UPNs that are configured, you might want to allow or disallow the use of specific UPN suffixes. You do this by configuring name suffix routing on the Name Suffix Routing tab of the trust's properties as shown in Figure 1-14.

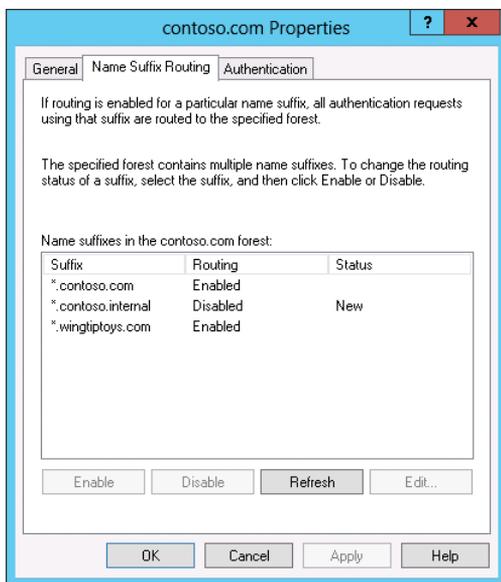


FIGURE 1-14 Configure name suffix routing

### MORE INFO NAME SUFFIX ROUTING

To learn more about name suffix routing, consult the following link: <http://technet.microsoft.com/en-us/library/cc731648.aspx>.

## Lesson summary

- Trusts can be uni- or bidirectional. A one-way outgoing trust allows users in the remote domain to access resources in the local domain. A one-way incoming trust allows users in the local domain to access resources in the remote domain.
- Trust transitivity allows access to resources in child domains of the trusting domain.
- A forest trust allows one forest to trust another forest. This means that all domains in the first forest have a trust relationship with all domains in the second forest.
- Selective authentication in a forest trust enables you to limit which users and groups from the trusted domain are able to authenticate.
- An external trust is a trust between domains in different forests. External trusts are not transitive. You can configure external trusts to connect to Windows 2000 Server and Windows NT 4 domains.
- You use a realm trust when you want to configure a trust between an Active Directory domain and a Kerberos V5 realm.
- You can use a shortcut trust between domains in the same forest to speed the authentication process.
- SID filtering is enabled by default on all new external and forest trusts.
- You can configure name suffix routing to configure which users are able to authenticate in a forest.

## 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 each answer choice in the “Answers” section at the end of this chapter.

1. You have a 30-domain Active Directory forest that has contoso.com as its root domain. This forest has five separate domain trees. Users in the melbourne.australia.pacific.contoso.com domain report that there are substantial authentication delays when they try to access resources in the auckland.newzealand.adatum.com domain. Both domains are located in the same forest. Which of the following trust types would you configure to resolve this problem?
  - A. Forest trust
  - B. External trust
  - C. Realm trust
  - D. Shortcut trust

2. You are a systems administrator at a local university. The university has a deployment of Linux servers and workstations that are members of a Kerberos V5 realm. You want to allow users of the Linux workstations to have access to several file shares hosted in one of your organization's Active Directory domains. Which of the following trust types would you implement to accomplish this goal?

  - A. Shortcut trust
  - B. Realm trust
  - C. Forest trust
  - D. External trust
3. Your organization recently acquired a subsidiary company. Your organization currently has a 10-domain Active Directory forest running at the Windows Server 2012 functional level. The subsidiary company has a five-domain Active Directory forest running at the Windows Server 2008 functional level. The subsidiary company has implemented a number of schema modifications to support a custom application. You want to allow users in the subsidiary company to be able to access resources hosted in your organization's forest. Users in your organization's forest should also be able to access resources in the subsidiary company's forest. Which of the following trust relationships should you configure to accomplish this goal?

  - A. External trust
  - B. Forest trust
  - C. Realm trust
  - D. Shortcut trust
4. You are the senior systems administrator of the contoso.com forest. Users in the australia.pacific.contoso.com domain need access to resources hosted in one domain of a partner organization's Active Directory forest. These users shouldn't have access to any other domain in the partner organization's forest. Users from other domains in your organization's forest should also not have access to resources in the partner organization's forest. Which of the following trust types would you configure in this scenario?

  - A. External trust
  - B. Realm trust
  - C. Shortcut trust
  - D. Forest trust

# Practice exercises

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

- Creating a forest trust
- Configuring name suffix routing
- Configuring selective authentication
- Configuring UPN suffixes
- Configuring a shortcut trust

To perform the exercises in this section, you need access to an evaluation version of Windows Server 2012. You should also have access to virtual machines SYD-DC, MEL-DC, CBR-DC, and ADL-DC, the setup instructions for which are as described in the Introduction. You should ensure that you have a snapshot of these virtual machines that you can revert to at the end of the practice exercises.

## Exercise 1: Prepare a domain controller to host a child domain with a contiguous namespace

In this exercise, you prepare CBR-DC to function as a domain controller for a child domain of the contoso.com domain. To complete this exercise, perform the following steps:

1. Power on SYD-DC and log in as contoso\don\_funk with the password Pa\$\$w0rd.
2. Click the Tools menu in the Server Manager console, and click DNS.
3. In the DNS Manager console, expand SYD-DC and Forward Lookup Zones.
4. Verify that the following lookup zones are present as shown in Figure 1-15:
  - `_msdcs.contoso.com`
  - `contoso.com`

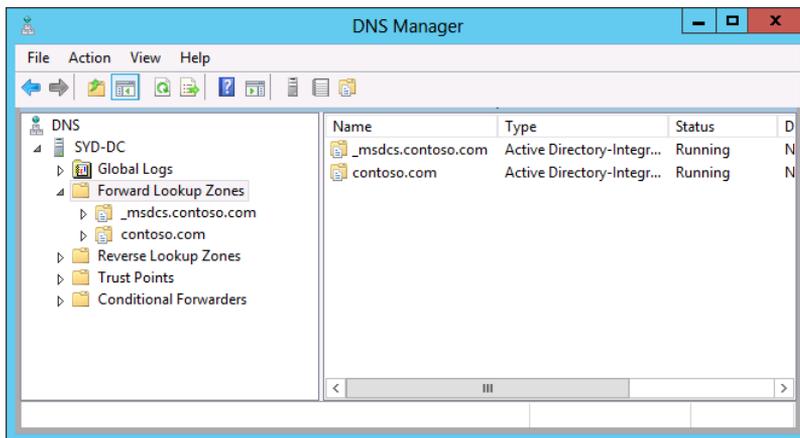
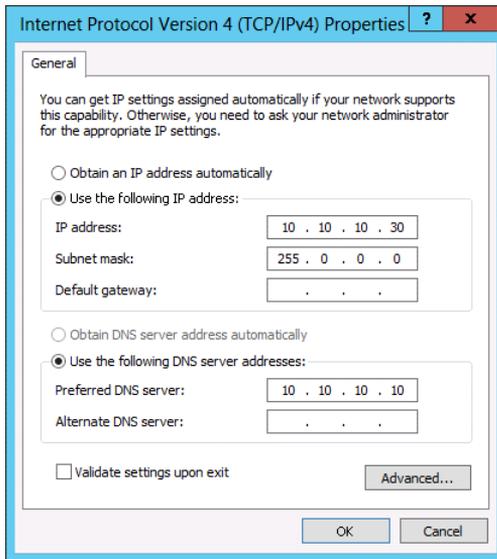


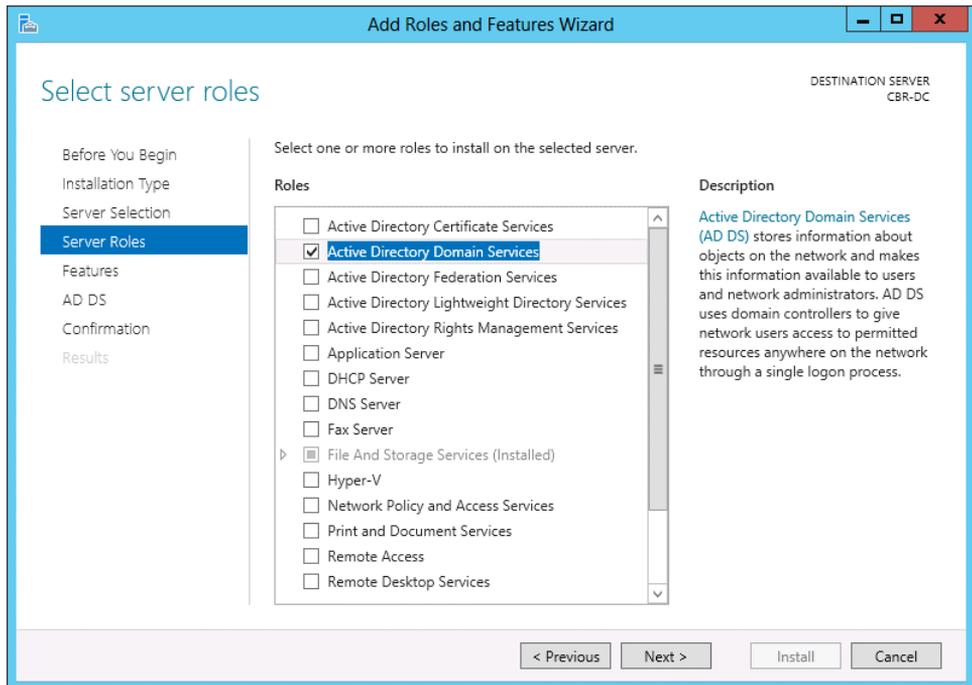
FIGURE 1-15 Verify the DNS configuration

5. Power on CBR-DC and sign on as Administrator with the password Pa\$\$w0rd.
6. In Server Manager, click the Local Server node.
7. In the Properties area, click 10.10.10.30 next to Ethernet.
8. In the Network Connections window, right-click Ethernet and click Properties.
9. In the Ethernet Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
10. Verify that the Preferred DNS Server is set to 10.10.10.10, as shown in Figure 1-16, click OK, and then click Close.



**FIGURE 1-16** Verify the Internet Protocol (IP) address configuration

11. In the Server Manager console, click Manage and then click Add Roles and Features.
12. On the Before You Begin page of the Add Roles and Features Wizard, click Next three times.
13. On the Select Server Roles page, click the Active Directory Domain Services check box as shown in Figure 1-17.
14. On the Add Roles and Features Wizard, click Add Features.



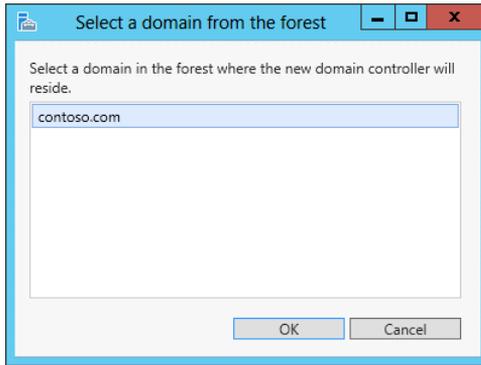
**FIGURE 1-17** Add the AD DS role

15. On the Select Server Roles page, click Next three times and click Install. When the installation completes, click Close.

## Exercise 2: Create a child domain with a noncontiguous namespace

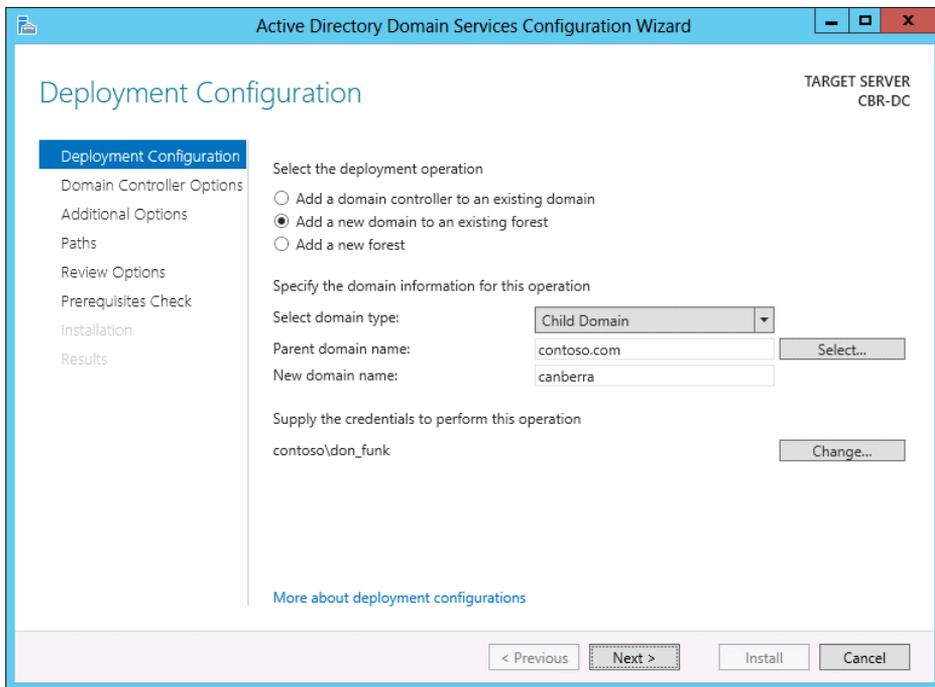
In this exercise, you configure CBR-DC to host the Canberra.contoso.com child domain. To complete this exercise, perform the following steps:

1. In the Server Manager console on CBR-DC, click the Notifications item and then click Promote This Server to a Domain Controller.
2. On the Deployment Configuration page, click Add a New Domain to an Existing Forest.
3. On the Select Domain Type drop-down menu, select Child Domain.
4. Click Select next to Parent Domain Name.
5. In the Windows Security dialog box, enter the user name contoso\don\_funk, enter the password Pa\$\$w0rd, and click OK.
6. In the Select a Domain from the Forest dialog box, click contoso.com as shown in Figure 1-18 and then click OK.



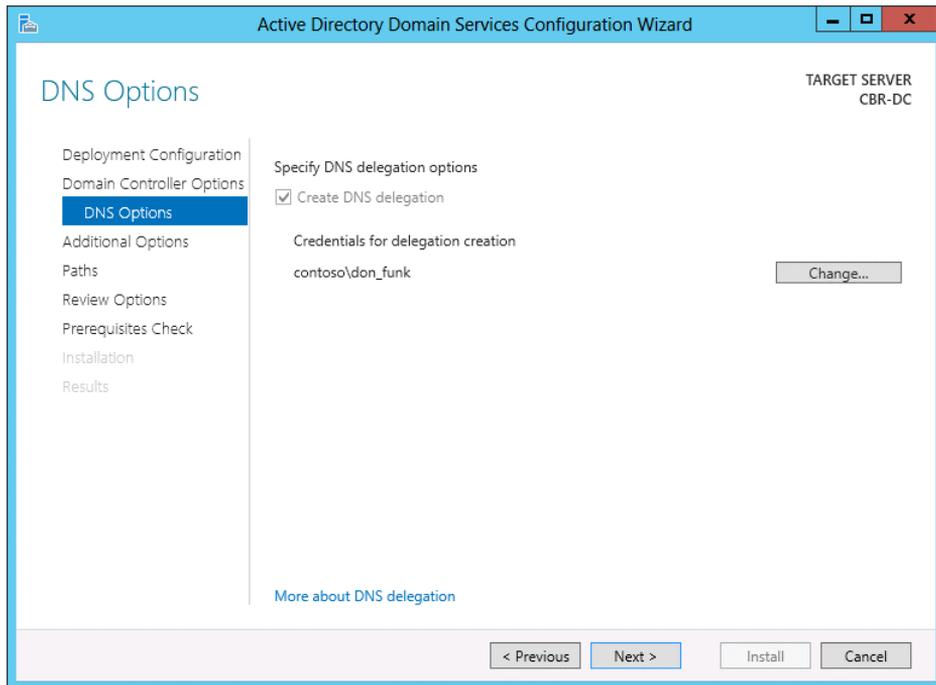
**FIGURE 1-18** Select the domain in the forest

7. In the New Domain Name text box enter the name Canberra as shown in Figure 1-19 and then click Next.



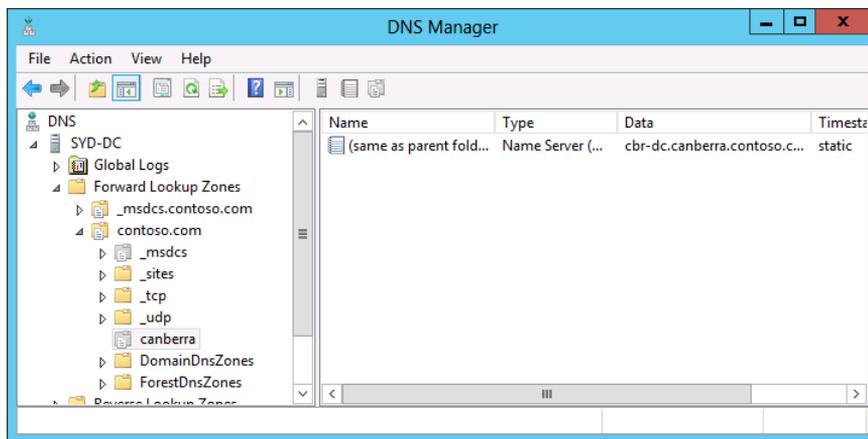
**FIGURE 1-19** Configure the child domain

8. On the Domain Controller Options page, set the DSRM password as Pa\$\$w0rd in both the Password and Confirm Password dialog boxes and click Next.
9. On the DNS Options page, ensure that the settings match those in Figure 1-20 and click Next.



**FIGURE 1-20** Configure the delegation credentials

- 10.** On the additional options page, verify that the NetBIOS domain name is set to CANBERRA, click Next three times, and click Install.
- 11.** After CBR-DC restarts, sign on as Canberra\Administrator with the password Pa\$\$w0rd.
- 12.** Switch to SYD-DC. In the DNS console, expand the contoso.com zone and verify the presence of the canberra.contoso.com zone as shown in Figure 1-21.



**FIGURE 1-21** Verify the DNS zone

## Exercise 3: Prepare domain controller to host the wingtiptoy.com tree in the contoso.com forest

In this exercise, you prepare computer ADL-DC so that it can be promoted to a domain controller. To complete this exercise, perform the following steps:

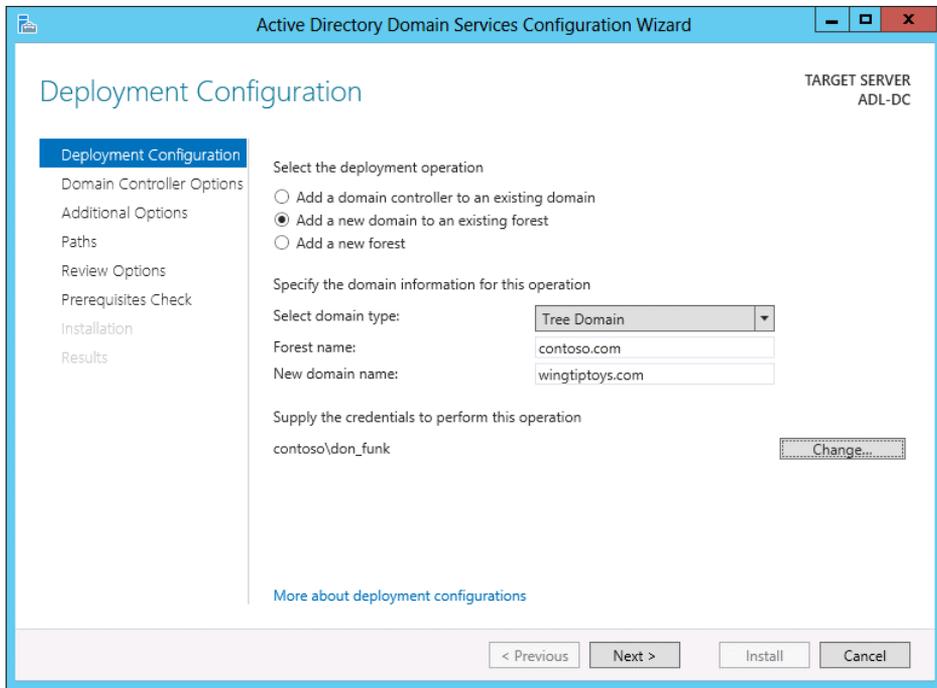
1. Sign on to ADL-DC as Administrator with the password Pa\$\$w0rd.
2. In Server Manager, click the Local Server node.
3. In the Properties area, click 10.10.10.20 next to Ethernet.
4. In the Network Connections window, right-click Ethernet and click Properties.
5. In the Ethernet Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
6. Verify that the Preferred DNS server is set to 10.10.10.10 and then click OK. Click Close.
7. In the Server Manager console, click Manage and then click Add Roles and Features.
8. On the Before You Begin page of the Add Roles and Features Wizard, click Next three times.
9. On the Select Server Roles page, click the Active Directory Domain Services check box.
10. On the Add Roles and Features Wizard, click Add Features.
11. On the Select Server Roles page, click Next three times and click Install. When the installation completes, click Close.

## Exercise 4: Promote domain controller for new tree in contoso.com forest

In this exercise, you promote ADL-DC to domain controller of a new domain tree in an existing Active Directory forest. To complete this exercise, perform the following steps:

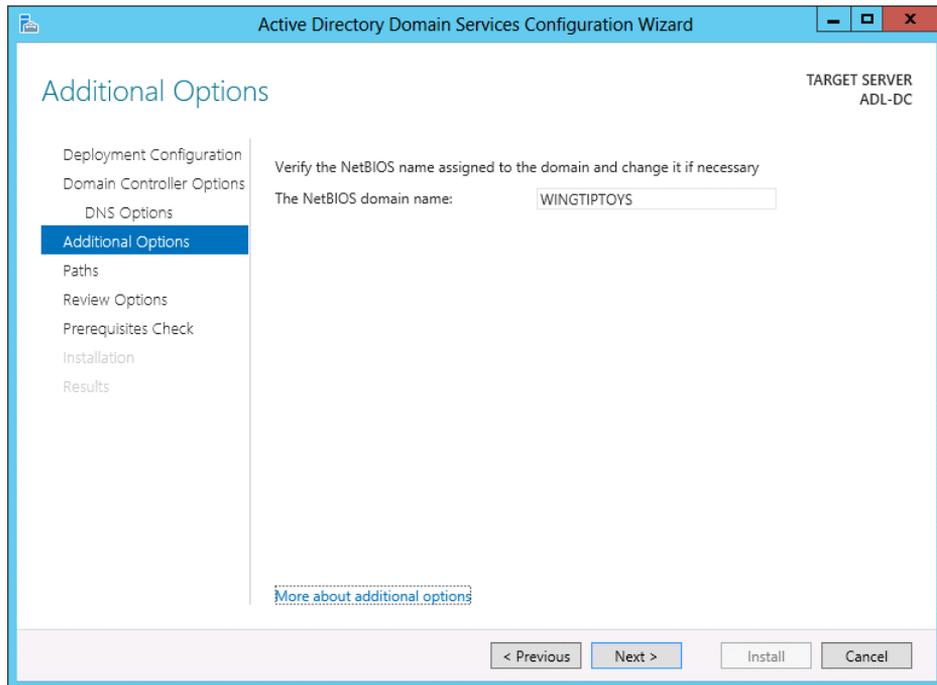
1. In the Server Manager console on ADL-DC, click the Notifications item and then click Promote This Server to a Domain Controller.
2. On the Deployment Configuration page, click Add a New Domain to an Existing Forest.
3. On the Select Domain Type drop-down menu, click Tree Domain.
4. In the Forest Name text box, type contoso.com.
5. In the New Domain Name text box, type wingtiptoy.com.
6. Next to <No Credentials Provided>, click Change.
7. On the Windows Security dialog box, enter the user name as contoso\don\_funk, enter the password as Pa\$\$w0rd, and click OK.

8. Verify that the Deployment Configuration page matches Figure 1-22 and then click Next.



**FIGURE 1-22** Add a domain tree

9. On the Domain Controller Options page, enter the DSRM password Pa\$\$w0rd in both the Password and Confirm Password text boxes and then click Next.
10. On the DNS Options page, review the warning and click Next.
11. On the Additional Options page, verify that the NetBIOS name is set to WINGTIPTOYS as shown in Figure 1-23. Click Next three times and then click Install.



**FIGURE 1-23** Verify the NetBIOS name

12. After the computer restarts, sign in as WINGTIPTOYS\Administrator with the password Pa\$\$w0rd.

## Exercise 5: Prepare a domain controller to host a new forest

In this exercise, you configure MEL-DC so that it is able to host the new forest margiestravel.com. To complete this exercise, perform the following steps:

1. Sign on to MEL-DC as Administrator with the password Pa\$\$w0rd.
2. In Server Manager, click the Local Server node.
3. In the Properties area, click 10.10.10.40 next to Ethernet.
4. In the Network Connections window, right-click Ethernet and click Properties.
5. In the Ethernet Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
6. Verify that the Preferred DNS server is set to 10.10.10.10, click OK, and then click Close.
7. In the Server Manager console, click Manage and then click Add Roles and Features.

8. On the Before You Begin page of the Add Roles and Features Wizard, click Next three times.
9. On the Select Server Roles page, click the Active Directory Domain Services check box.
10. On the Add Roles and Features Wizard, click Add Features.
11. On the Select Server Roles page, click Next three times and then click Install. When the installation completes, click Close.

## Exercise 6: Create new forest

In this exercise, you configure MEL-DC as the first domain controller in a new forest. To complete this exercise, perform the following steps:

1. In the Server Manager console on MEL-DC, click the Notifications item and then click Promote This Server to a Domain Controller.
2. On the Deployment Configuration page, click Add a new forest.
3. In the Root Domain Name textbox, type margiestravel.com as shown in Figure 1-24 and click Next.

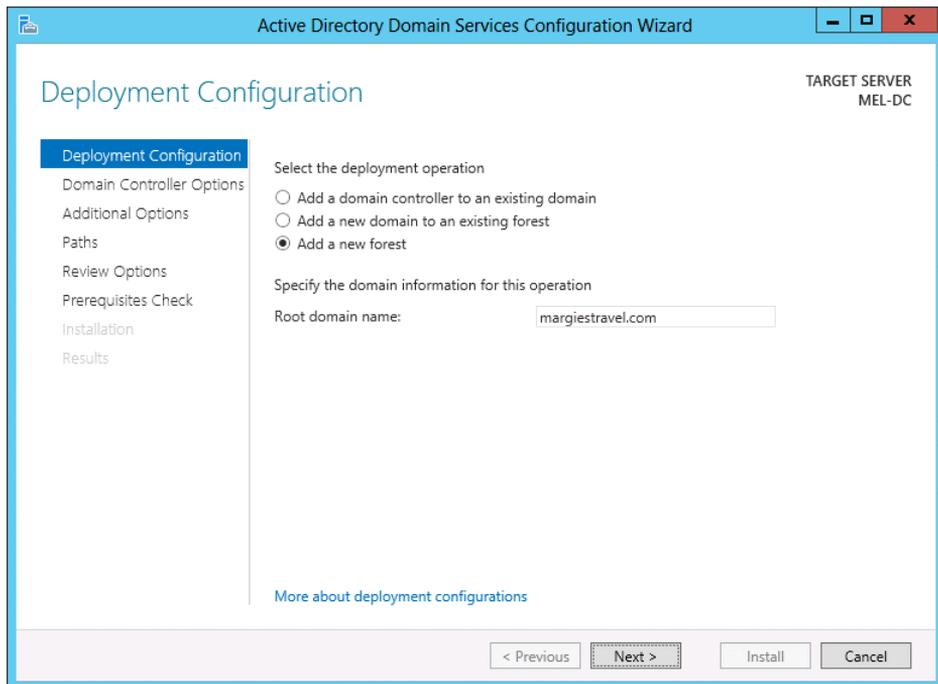
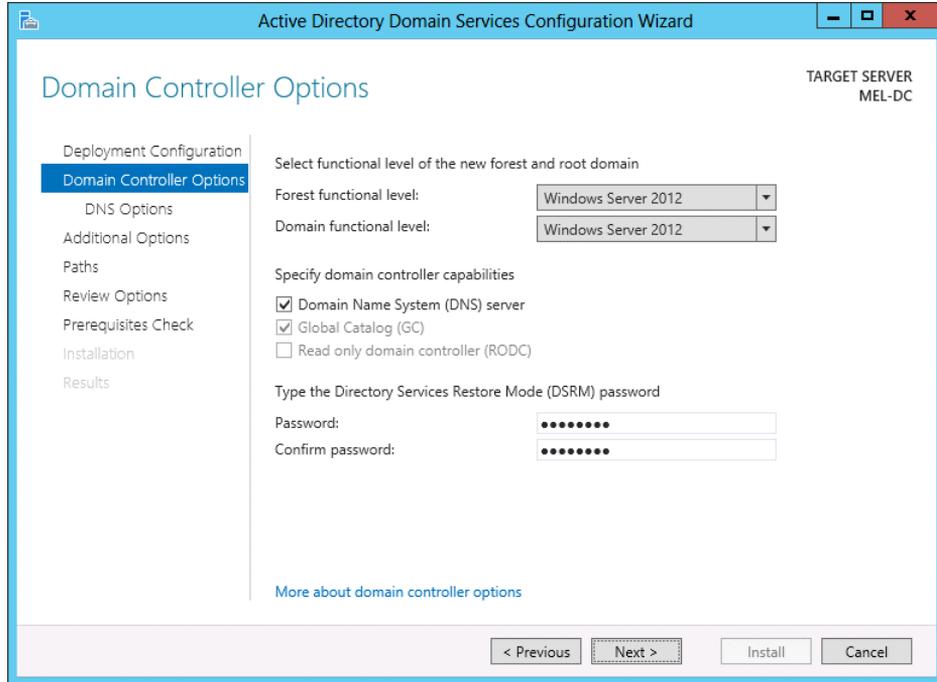


FIGURE 1-24 Add a new forest

4. On the Domain Controller Options page, ensure that Domain Name System (DNS) server is selected and that you enter the DSRM password of Pa\$\$word twice as shown in Figure 1-25. Click Next twice.



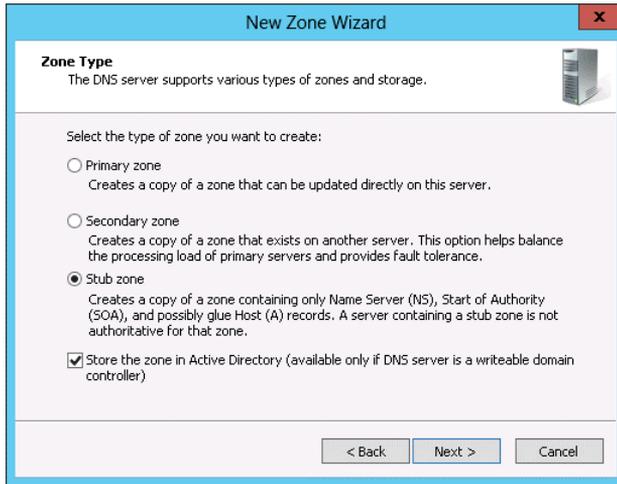
**FIGURE 1-25** The Domain Controller options page

5. On the Additional Options page, verify that the NetBIOS domain name is set to MARGIESTRAVEL, click Next three times, and then click Install.
6. After the server restarts, sign on as MARGIESTRAVEL\Administrator with the password Pa\$\$w0rd.

## Exercise 7: Prepare to configure a forest trust relationship

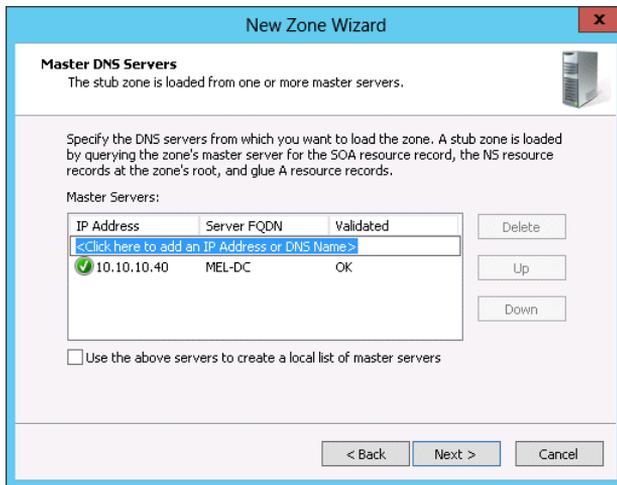
In this exercise, you configure a forest trust relationship between the contoso.com forest and the margiestravel.com forest. To complete this exercise, perform the following steps:

1. While logged onto SYD-DC as contoso\don\_funk, open the DNS Manager console from the Tools menu in the Server Manager console.
2. Right-click on Forward Lookup Zones and click New Zone.
3. On the Welcome to the New Zone Wizard page, click Next.
4. On the Zone Type page, click Stub Zone and ensure that the Store the Zone in Active Directory check box is selected as shown in Figure 1-26. Click Next.



**FIGURE 1-26** Configure the zone type

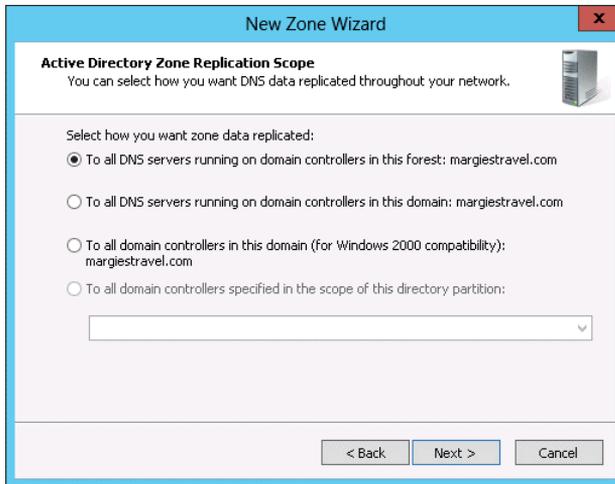
5. On the Active Directory Zone Replication Scope page, click To All DNS Servers Running on Domain Controllers in this Forest: contoso.com and click Next.
6. In the Zone Name text box, enter margiestravel.com and click Next.
7. On the Master DNS Servers page, type the IP address 10.10.10.40 in the list of master servers as shown in Figure 1-27, click Next, and then click Finish.



**FIGURE 1-27** Configure the stub zone master servers

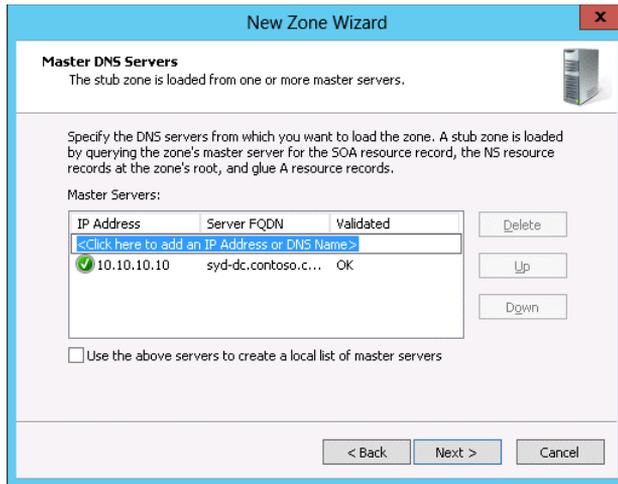
8. On MEL-DC, ensure that you are signed in as MARGIESTRAVEL\Administrator with the password Pa\$\$w0rd.
9. Open the DNS Manager console from the Tools menu in the Server Manager console.

10. In the DNS Manager console, right-click Forward Lookup Zones and click New Zone.
11. On the Welcome to the New Zone Wizard page, click Next.
12. On the Zone Type page, click Stub Zone and ensure that the Store the Zone in Active Directory check box is selected. Click Next.
13. On the Active Directory Zone Replication Scope page, click To All DNS Servers Running on Domain Controllers in This Forest: margiestravel.com as shown in Figure 1-28. Click Next.



**FIGURE 1-28** Configure the zone replication scope

14. On the Zone Name page, enter the name contoso.com in the Zone Name text box and click Next.
15. On the Master DNS Servers page, enter the IP address 10.10.10.10 in the Master Servers list as shown in Figure 1-29, click Next, and click Finish.

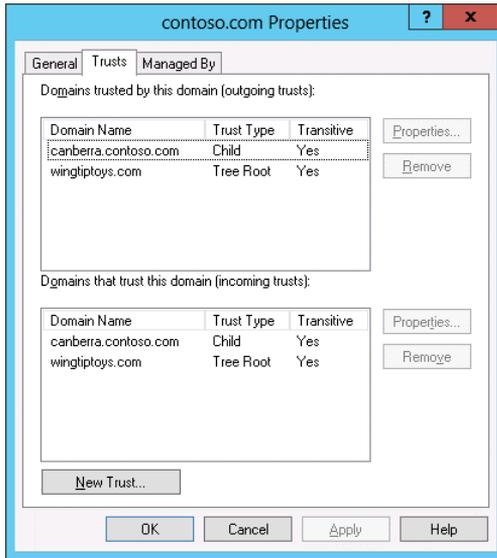


**FIGURE 1-29** Configure the master DNS servers

## Exercise 8: Begin creating a forest trust relationship

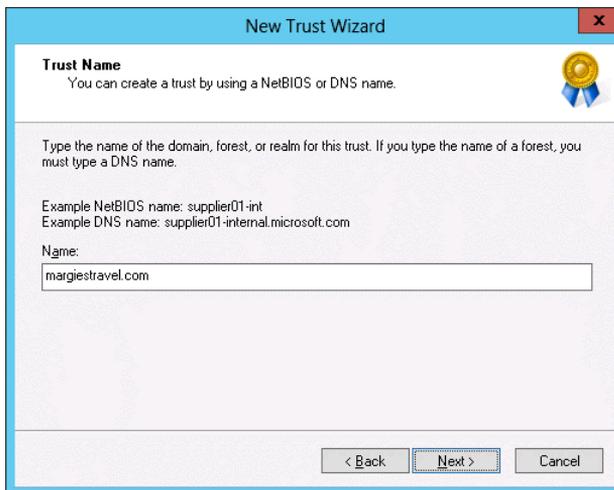
In this exercise, you configure the contoso.com side of a forest trust relationship between the contoso.com and margiestravel.com forests. To complete this exercise, perform the following steps:

1. On the Tools menu of the Server Manager console on SYD-DC, click Active Directory Domains and Trusts.
2. In the Active Directory Domains and Trusts console, right-click contoso.com and click Properties.
3. On the Trusts tab of the contoso.com Properties dialog box, shown in Figure 1-30, click New Trust.



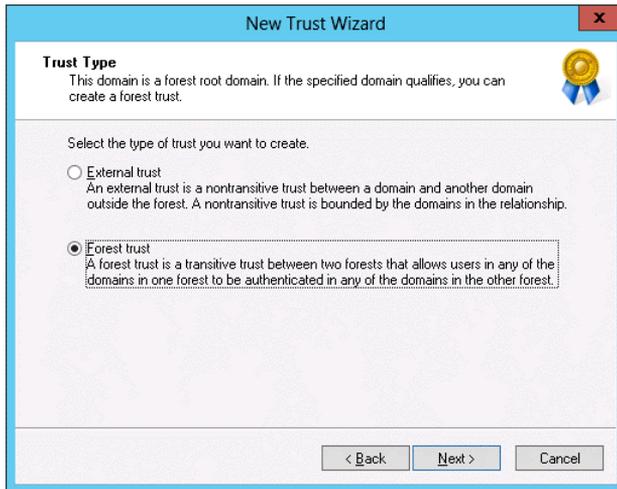
**FIGURE 1-30** Create the new trust

4. On the Welcome to the New Trust Wizard page, click Next.
5. On the Trust Name page, type margiestravel.com as shown in Figure 1-31, and click Next.



**FIGURE 1-31** Set the trust name

6. On the Trust Type page, click Forest Trust as shown in Figure 1-32 and click Next.



**FIGURE 1-32** Configure the trust type

7. On the Direction Of Trust page, click Two-Way and click Next.
8. On the Sides Of Trust page, click This Domain Only and then click Next.
9. On the Outgoing Trust Authentication Level page, click Forest-Wide Authentication as shown in Figure 1-33 and click Next.



**FIGURE 1-33** Configure the trust authentication level

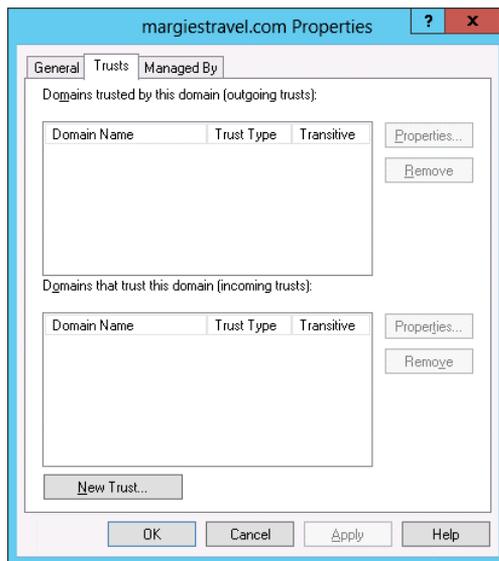
10. On the Trust Password page, type Pa\$\$w0rd in the Trust Password and Confirm Trust Password text boxes. Click Next three times.

11. On the Confirm Outgoing Trust page, click No, Do Not Confirm the Outgoing Trust and click Next.
12. On the Confirm Incoming Trust page, click No, Do Not Confirm the Incoming Trust, click Next, and click Finish.

## Exercise 9: Complete the creation of the forest trust relationship between contoso.com and margiestravel.com

In this exercise, you configure the margiestravel.com side of a forest trust relationship between the contoso.com and margiestravel.com forests. To complete this exercise, perform the following steps:

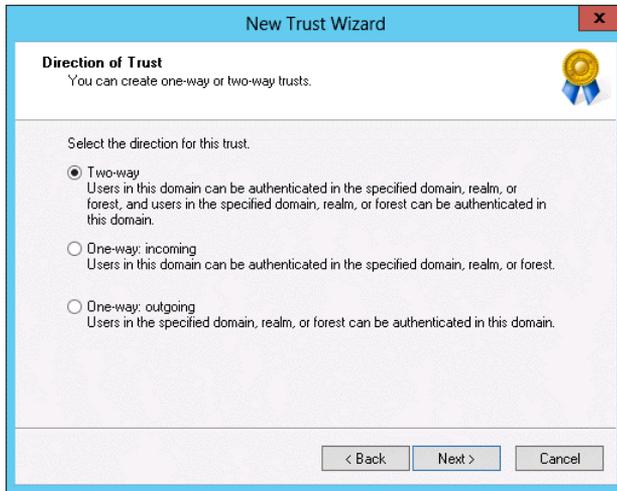
1. In the Tools menu of the Server Manager console on MEL-DC, click Active Directory Domains and Trusts.
2. In the Active Directory Domains and Trusts console, right-click Margiestravel.com and click Properties.
3. On the Trusts tab of the margiestravel.com Properties dialog box, shown in Figure 1-34, click New Trust.



**FIGURE 1-34** View the current trusts

4. On the Welcome to the New Trust Wizard page, click Next.
5. On the Trust Name page of the New Trust Wizard, type contoso.com in the Name text box and click Next.
6. On the Trust Type page, click Forest Trust and click Next.

7. On the Direction of Trust page, click Two-way as shown in Figure 1-35 and click Next.



**FIGURE 1-35** Configure the direction of the trust

8. On the Sides of Trust page, click This Domain Only and click Next.
9. On the Outgoing Trust Authentication Level page, click Forest-Wide Authentication and click Next.
10. On the Trust Password page, enter Pa\$\$w0rd in the Trust Password and Confirm Trust Password text boxes. Click Next three times.
11. On the Confirm Outgoing Trust page, click Yes, Confirm the Outgoing Trust as shown in Figure 1-36, and click Next.



**FIGURE 1-36** Confirm the outgoing trust

12. On the Confirm Incoming Trust page, click Yes, Confirm the Incoming Trust. In the User Name text box, type contoso\don\_funk and in the Password text box type Pa\$\$w0rd as shown in Figure 1-37. Click Next.



FIGURE 1-37 Confirm the incoming trust

13. On the Completing the New Trust Wizard page verify that the trust is successfully created as shown in Figure 1-38 and click Finish. Click OK to close the margiestravel.com properties dialog box.



FIGURE 1-38 Confirm the trust creation

## Exercise 10: Configure name suffix routing

In this exercise, you configure the forest trust between the margiestravel.com forest and the contoso.com forest so that name suffix routing is supported for the wingtiptoys.com domain tree. To complete this exercise, perform the following steps:

1. In the Active Directory Domains and Trusts console on MEL-DC, right-click margiestravel.com and click Properties.
2. On the Trusts tab of the margiestravel.com Properties dialog box click contoso.com in the Domains Trusted by This Domain (Outgoing Trusts) area, as shown in Figure 1-39, and then click Properties.

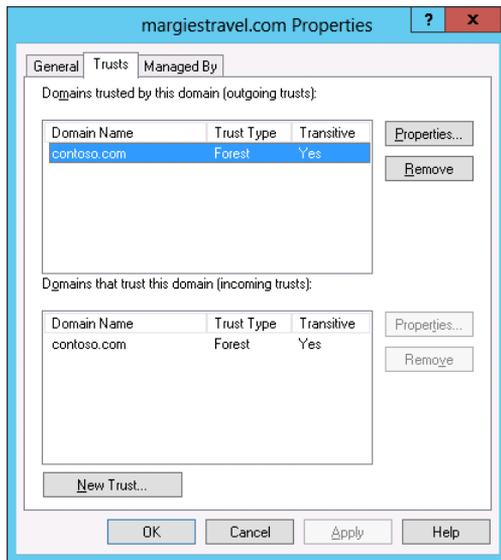
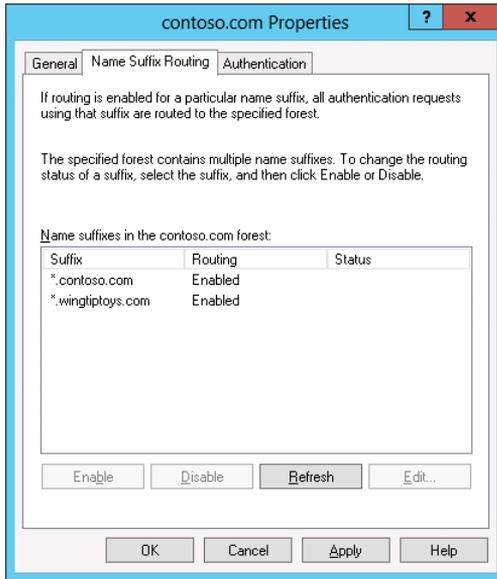


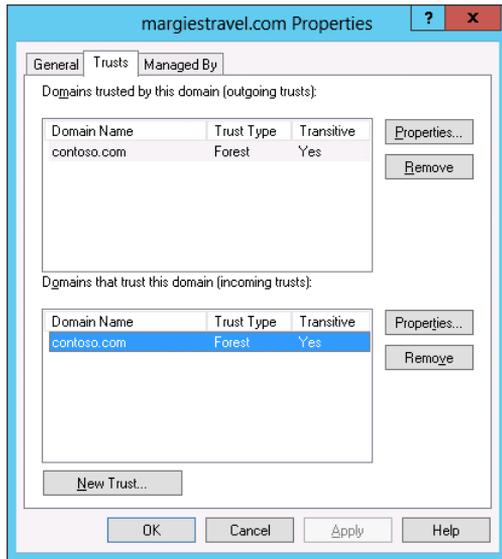
FIGURE 1-39 Editing the properties of trusts

3. On the Name Suffix Routing tab of the contoso.com Properties dialog box, click \*.wingtiptoys.com and then click Enable as shown in Figure 1-40.



**FIGURE 1-40** Configure name suffix routing

4. On the General tab of the contoso.com Properties dialog box, click Validate.
5. On the Active Directory Domain Services dialog box, click Yes, Validate the Incoming Trust by entering the user name contoso\don\_funk and the password Pa\$\$w0rd, and click OK.
6. Click OK on the Active Directory Domain Services dialog box and then click Yes on the second Active Directory Domain Services dialog box.
7. Click OK to close the contoso.com Properties dialog box.
8. Click contoso.com on the list of Domains That Trust This Domain (Incoming Trusts) dialog box as shown in Figure 1-41 and then click Properties.



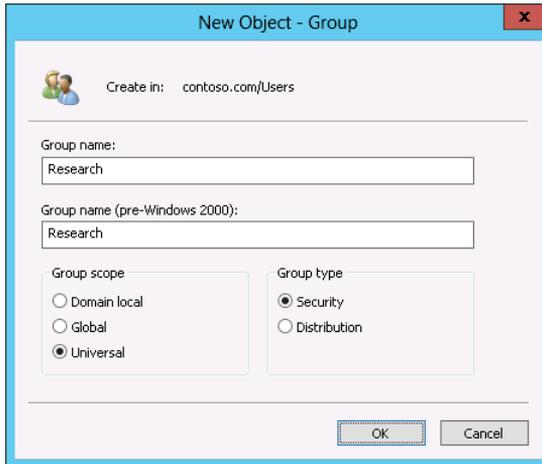
**FIGURE 1-41** Trusts for the margiestravel.com domain

9. On the Name Suffix Routing tab of the contoso.com Properties dialog box verify that both \*.contoso.com and \*.wingtiptoy.com are enabled and then click OK.
10. Click OK to close the margiestravel.com Properties dialog box.

## Exercise 11: Configure selective authentication

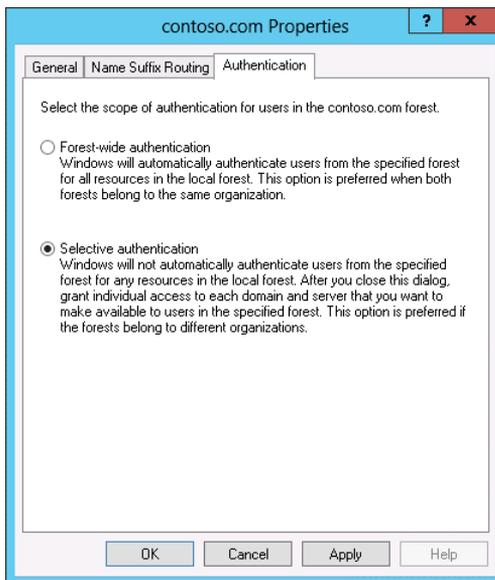
In this exercise, you configure selective authentication. You configure the trust to use selective authentication, create a user group in one forest, and create a computer account in the other forest. You then configure the computer account so that members of the user group in the trusted forest can authenticate when connecting to that computer. To complete this exercise, perform the following steps:

1. When signed on to SYD-DC as contoso\don\_funk, click Active Directory Users and Computers on the Tools menu of the Server Manager console.
2. In Active Directory Users and Computers, right-click the Users container, click New, and click Group.
3. On the New Object – Group dialog box, enter the group name as Research, set the group scope to Universal as shown in Figure 1-42, and click OK.



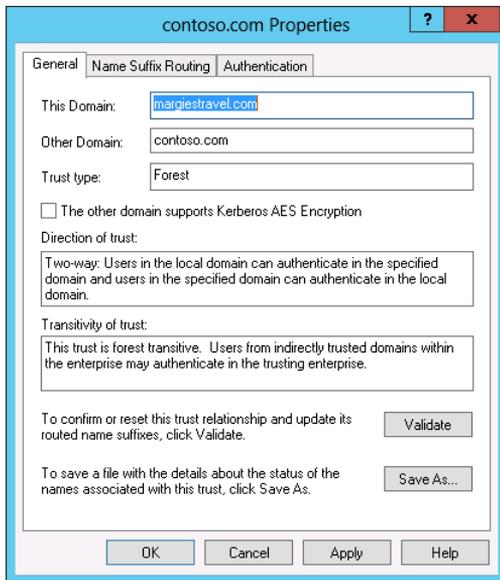
**FIGURE 1-42** Create a new universal group

4. On MEL-DC, right-click margiestravel.com in the Active Directory Domains and Trust console and click Properties.
5. On the Trusts tab of the margiestravel.com Properties dialog box, click contoso.com in the Domains That Trust This Domain (Incoming Trusts) list and click Properties.
6. On the Authentication tab of the contoso.com Properties dialog box, click Selective Authentication as shown in Figure 1-43.



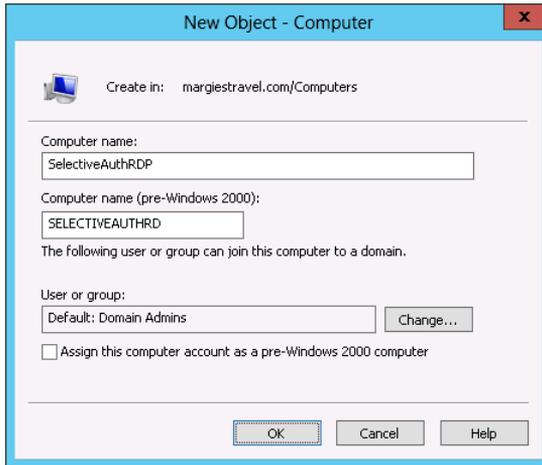
**FIGURE 1-43** Configure selective authentication

7. On the General tab of the contoso.com Properties dialog box, shown in Figure 1-44, click Validate.



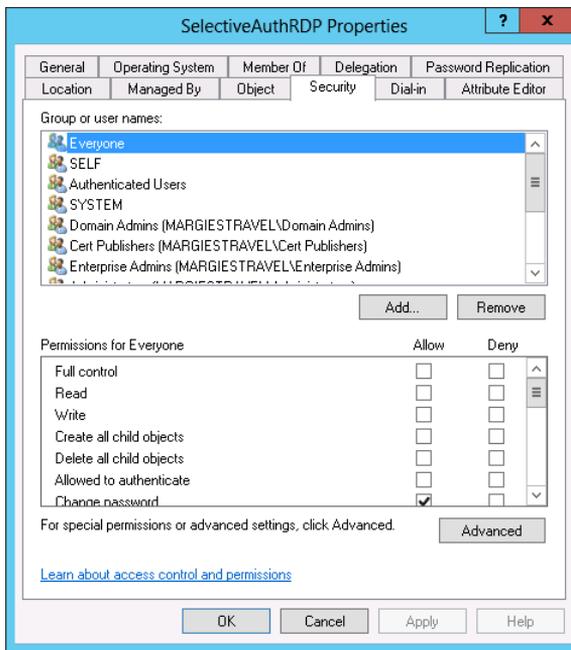
**FIGURE 1-44** Validate authentication

8. On the Active Directory Domain Services dialog box, click Yes, validate the incoming trust. Enter the user name as contoso\don\_funk, enter the password as Pa\$\$w0rd, and then click OK twice.
9. Click Yes on the Active Directory Domain Services dialog box and then click OK twice to close the contoso.com Properties and margiestravel.com Properties dialog boxes.
10. Click Active Directory Users and Computers in the Tools menu of the Server Manager console.
11. Right-click the Computers node and click New and then click Computer.
12. In the New Object – Computer dialog box, enter the name SelectiveAuthRDP as shown in Figure 1-45 and click OK.



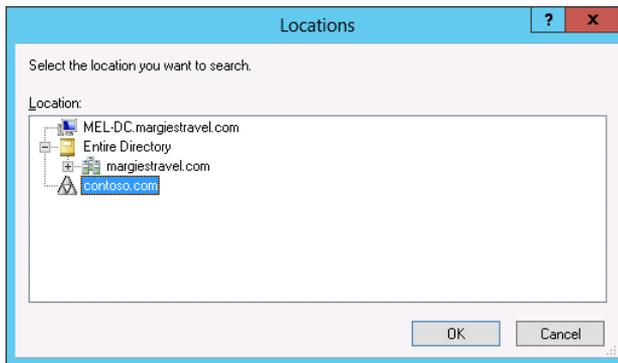
**FIGURE 1-45** Create new computer object

- 13.** Enabled Advanced Features on the View menu of the Active Directory Users and Computers console.
- 14.** Right-click the SelectiveAuthRDP computer object and click Properties.
- 15.** On the Security tab of the SelectiveAuthRDP Properties dialog box, shown in Figure 1-46, click Add.



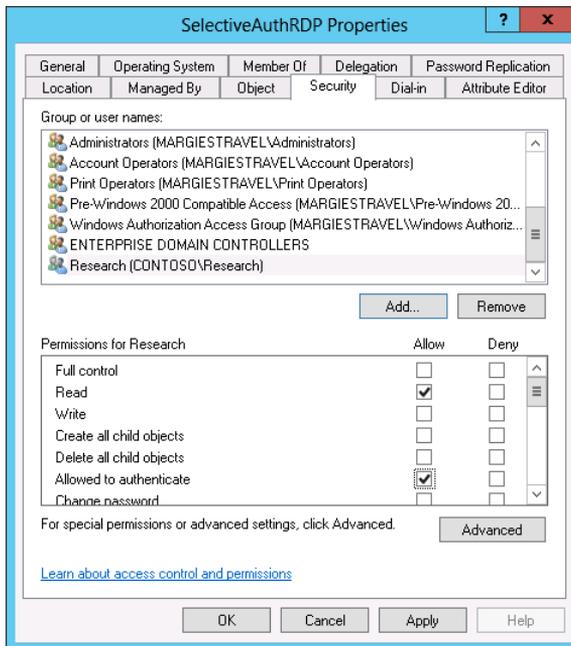
**FIGURE 1-46** Add a user

16. On the Select Users, Computers, Service Accounts, or Groups dialog box, click Locations.
17. On the Locations dialog box, click contoso.com as shown in Figure 1-47 and then click OK.



**FIGURE 1-47** The Locations dialog box

18. In the Select Users, Computers, Service Accounts, or Groups dialog box, type Research, click Check Names, and click OK.
19. On the SelectiveAuthRDP Properties dialog box, click Research (Contoso\Research) and click Allowed to Authenticate (Allow) as shown in Figure 1-48. Click OK.



**FIGURE 1-48** Configure Allowed to Authenticate permission

## Exercise 12: Configure additional UPN suffixes

In this exercise, you configure additional UPN suffixes. To complete this exercise, perform the following steps:

1. When signed on to SYD-DC as contoso\don\_funk, switch to the Active Directory Domains and Trusts console.
2. In the Active Directory Domains and Trusts console, right-click Active Directory Domains and Trusts and click Properties.
3. On the UPN Suffixes tab of the Active Directory Domains and Trusts dialog box, type contoso.internal in the Alternative UPN suffixes dialog box and then click Add as shown in Figure 1-49. Click OK.

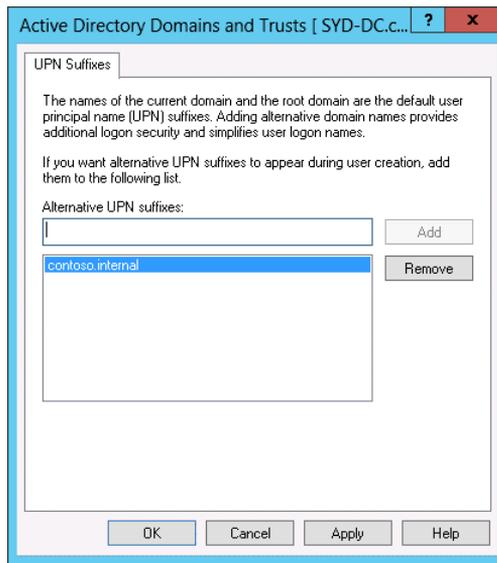


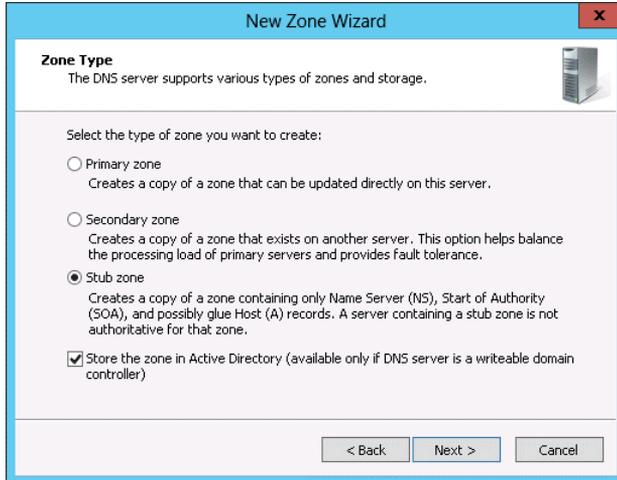
FIGURE 1-49 Configure a UPN suffix

## Exercise 13: Configure a shortcut trust

In this exercise, you configure a shortcut trust between the canberra.contoso.com domain and the wingtiptoy.com domain. To complete this exercise, perform the following steps:

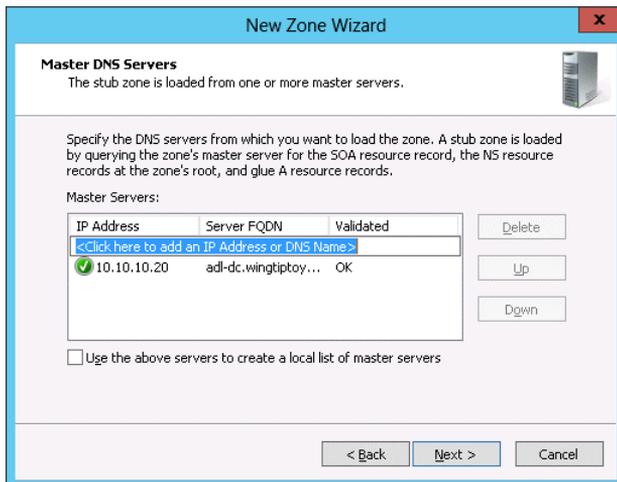
1. Sign on to CBR-DC as canberra\administrator.
2. In the Server Manager console, click the Tools menu and then click DNS.
3. In the DNS Manager console, expand CBR-DC, right-click Forward Lookup Zones, and click New Zone.
4. On the Welcome to the New Zone Wizard page, click Next.

- On the Zone Type page of the New Zone Wizard, click Stub Zone and ensure that Store the Zone in Active Directory (available only if the DNS server is a writable domain controller) is selected as shown in Figure 1-50 and click Next twice.



**FIGURE 1-50** Create a stub zone

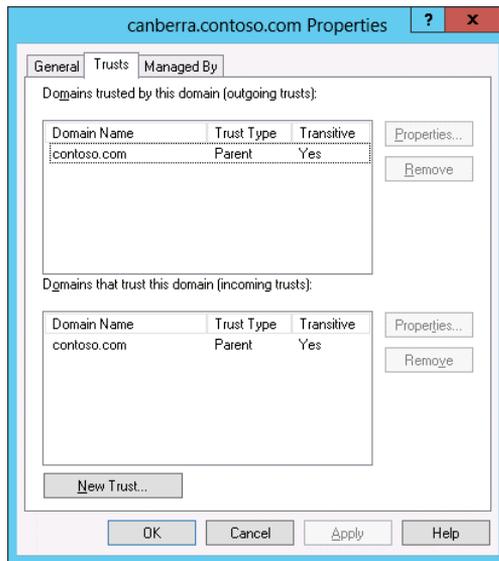
- On the Zone name page, type wingtiptoy.com and click Next.
- On the Master DNS Servers page, type 10.10.10.20 in the list of master DNS servers and press Enter as shown in Figure 1-51. Click Next and then click Finish.



**FIGURE 1-51** Configure a master DNS server

- In the Server Manager console, click the Tools menu and then click Active Directory Domains and Trusts.

9. In the Active Directory Domains and Trusts console, expand the contoso.com node, right-click canberra.contoso.com, and click Properties.
10. On the Trusts tab of the canberra.contoso.com Properties dialog box, show in Figure 1-52, click New Trust.



**FIGURE 1-52** Create a new trust

11. On the Welcome to the New Trust Wizard page, click Next.
12. On the Trust Name page of the New Trust Wizard, type wingtiptoys.com and click Next.
13. On the Direction of Trust page, click Two-Way and click Next.
14. On the Sides of Trust page, click Both This Domain and the Specified Domain as shown in Figure 1-53 and click Next.



**FIGURE 1-53** Configure trust sides

15. On the User Name and Password page, type wingtip toys\administrator in the user name text box, type Pa\$\$w0rd in the password text box, and click Next three times.
16. On the Confirm Outgoing Trust page, click Yes, Confirm the Outgoing Trust as shown in Figure 1-54, and click Next.



**FIGURE 1-54** Confirm the trust

17. On the Confirm Incoming Trust page, click Yes, Confirm the Incoming Trust and click Next.
18. Verify that the trust relationship was successfully created and click Finish.

19. Verify that the wingtiptoy.com trust is listed as a shortcut trust as shown in Figure 1-55 and then click OK.

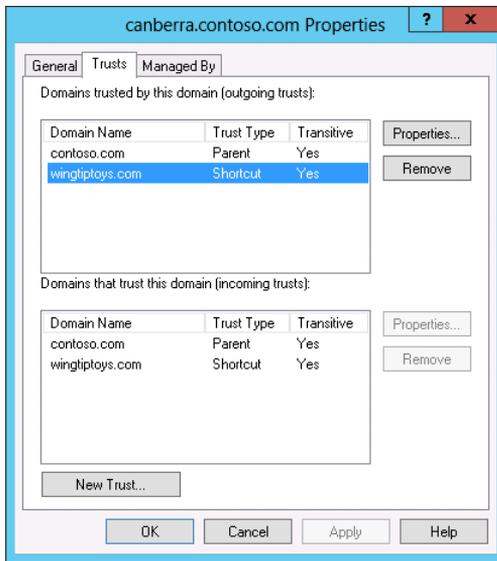


FIGURE 1-55 Verify the trust type

## 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.

- **Exercise 1:** Configure additional UPN suffixes for the margiestravel.com forest.
- **Exercise 2:** Use netdom.exe to disable and then re-enable SID filtering on the margiestravel.com forest.

# Answers

---

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

## Lesson 1

### 1. Correct Answer: C

- A. Incorrect:** This structure does not support the two different departments that have mutually exclusive Active Directory schema requirements. This structure supports only one Active Directory schema.
- B. Incorrect:** This structure does not support the two different departments that have mutually exclusive Active Directory schema requirements. This structure supports only one Active Directory schema.
- C. Correct:** This structure supports the two different departments that have mutually exclusive Active Directory schema requirements because each forest has a separate schema.
- D. Incorrect:** This structure does not support the two different departments that have mutually exclusive Active Directory schema requirements. This structure supports only one Active Directory schema.

### 2. Correct Answer: C

- A. Incorrect:** You need more than one domain to support the two separate domain names.
- B. Incorrect:** Implementing this solution requires the creation of additional trust relationships when compared to using a single forest with multiple domain trees.
- C. Correct:** You can accomplish this objective with a design that uses two domain trees, one for wingtiptoys.com and one for tailspintoys.com.
- D. Incorrect:** With a single domain tree, a child domain of the root domain needs to use a contiguous namespace. The requirements are that two domains with non-contiguous namespaces be available, which means at least two domain trees.

### 3. Correct Answer: A

- A. Correct:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.
- B. Incorrect:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.
- C. Incorrect:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.
- D. Incorrect:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.

**4. Correct Answers:** A and B

- A. Correct:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.
- B. Correct:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.
- C. Incorrect:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.
- D. Incorrect:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.

## Lesson 2

**1. Correct Answer:** D

- A. Incorrect:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest. In this instance you need to create a shortcut trust between two domains in the same forest.
- B. Incorrect:** You configure an external trust between two domains in different forests, often when you don't want to allow the trust to be transitive. In this instance you need to create a shortcut trust between two domains in the same forest.
- C. Incorrect:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm. In this instance you need to create a shortcut trust between two domains in the same forest.
- D. Correct:** In this instance you need to create a shortcut trust between two domains in the same forest.

**2. Correct Answer:** B

- A. Incorrect:** In this instance you need to create a shortcut trust between two domains in the same forest. You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
- B. Correct:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
- C. Incorrect:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest. You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
- D. Incorrect:** You configure an external trust between two domains in different forests, often when you don't want to allow the trust to be transitive. You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.

**3. Correct Answer: B**

- A. Incorrect:** You configure an external trust between two domains in different forests, often when you don't want to allow the trust to be transitive.
- B. Correct:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest.
- C. Incorrect:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
- D. Incorrect:** In this instance you need to create a shortcut trust between two domains in the same forest.

**4. Correct Answer: A**

- A. Correct:** You configure an external trust between two domains in different forests, often when you don't want to allow the trust to be transitive.
- B. Incorrect:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
- C. Incorrect:** In this instance you need to create a shortcut trust between two domains in the same forest.
- D. Incorrect:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest.

# Index

## A

- access auditing, files, 411–413
- access control, Windows Server Backup, 313–314
- Access Denied Assistance, configuring, 686–688
- accounts, resetting, 114–116
- Activate Scope page (Welcome to the New Scope Wizard), 177
- activation, DHCP roles, 169–175
- Active Directory
  - Administrative Center, 623
  - Certificate Services
    - installation and configuration, 209–223
    - managing certificates, 226–236
  - configuring group policy to support DAC, 623
  - configuring sites, 59–71
    - moving domain controllers, 70–71
    - sites and subnets, 60–68
    - SRV record registration, 68–70
  - Domains and Trusts console, 5
  - Domain Services role, 97–98
  - infrastructure
    - configuring domains and forests, 1–11
    - configuring trusts, 13–23
  - Migration Tool, 9
  - Recycle Bin, 7
  - replication, 73–86
    - directory partitions, 73–74
    - monitoring and management, 81–86
    - multi-master replication, 74–77
    - RODC password replication, 78–81
    - RODCs, 77–78
  - Rights Management Services. *See* RMS (Rights Management Services)
  - Sites and Services console, 89
  - Users and Computers console, 5
- Active Directory Application Mode (ADAM), 727
- Active Directory Certificate Services checkbox, 239
- Active Directory Federation Services. *See* AD FS
- Active Directory Lightweight Directory Services (AD LDS), 727
- Active Directory Rights Management Services (AD RMS) template, 410
- Active Directory Zone Replication Scope page (New Zone Wizard), 163
- ADAM (Active Directory Application Mode), 727
- AD CS Configuration Wizard, 241
- Add an Attribute Store dialog box, 728
- Add/Edit Port Rule dialog box, 500, 511
- Add Features That Are Required for Online Responder dialog box, 268
- Add Groups, Users and Computers dialog box, 107
- Add Host to Cluster: Connect dialog box, 509
- adding, cluster nodes, 527–529
- Add Initiator ID dialog box, 451
- Add IP Address dialog box, 507
- Add IPv4 Address dialog box, 201–202
- Add iSNS Server dialog box, 461
- Add Node Wizard, 529
- Add or Edit IPv4 Address Block dialog box, 201
- Add or Edit Server dialog box, 198
- Add or Remove Snap-ins dialog box, 282–283
- Add Roles and Features Wizard, 27, 170
- Add Servers dialog box, 169, 179, 580
- Add Superseded Template dialog box, 278
- Add Threshold dialog box, 429
- Add User Rights page (Create Distributed Rights Policy Template Wizard), 640
- Add Volumes dialog box, 349
- Add-WBBackupTarget cmdlet (Windows Server Backup), 316
- Add-WBSystemState cmdlet (Windows Server Backup), 316

## Add-WBVirtualMachine cmdlet (Windows Server Backup)

- Add-WBVirtualMachine cmdlet (Windows Server Backup), 316
- Add-WBVolume cmdlet (Windows Server Backup), 316
- AD FS, 721–730
  - attribute stores, 722–723, 727–728
  - claim rules, 722–723
  - claims, 722–723
  - claims providers, 723
  - claims provider trusts, 725
  - claims rules, 728–730
  - components, 722
  - configuring certificate relationships, 726–727
  - configuring proxy servers, 730
  - deployment, 737–740, 756–766
  - relying party, 724
  - relying party trust, 724
- AD LDS (Active Directory Lightweight Directory Services), 727
- administration, IPAM, 151
- Administrative Center (Active Directory), 623
- administrative role separation, certificate permissions, 219–221, 272–276
- Administrator groups (RMS), configuring, 642–644
- AD RMS (Active Directory Rights Management Services) template, 410
- Advanced Boot Options Menu, 365–366
- advanced DHCP solution implementation, 134–140
  - DHCP failover, 138–140
  - multicast scopes, 136–137
  - Name Protection feature, 137–138
  - split scopes, 137
  - superscopes, 135–136
- advanced DNS solution implementation, 121–132
  - delegated administration, 131–132
  - DNS Cache Locking, 128–129
  - DNS event logs, 124–126
  - DNS recursion, 129–130
  - DNSSEC, 122–124
  - DNS socket pool, 128
  - GlobalNames Zones, 126–128
  - netmask ordering, 130–131
- Advanced EFS Properties dialog box, 295
- Advanced Encryption Services (AES), 6
- advanced file services, 399–413
  - BranchCache, 406–410
  - file access auditing, 411–413
  - file classifications, 410–411
  - file screens, 400–403
  - quotas, 403–405
  - Server for NFS Data Store, 405–406
- Advanced Password Replication Policy dialog box, 80
- Advanced Password Replication Policy for ADL-DC dialog box, 110
- Advanced Security Settings for Research dialog box, 447
- Advanced Sharing dialog box, 472
- advanced storage options, 415–424
  - Features on Demand, 422–424
  - iSCSI target and initiation, 416–419
  - iSNS Server, 419–420
  - thin provisioning, 421
  - trim, 422
- Advanced tab
  - DNS Server properties dialog box, 129
  - SYD-DC Properties dialog box, 168
- AES (Advanced Encryption Services), 6
- affinity
  - configuring, 511–514
  - NLB (Network Load Balancing), 499–500
- AIA (Authority Information Access) distribution points, 215
- Allowed RODC Password Replication security group, 78
- Allow Macros rights (RMS), 640
- Allow Private Key to Be Exported (certificate template setting), 226
- All Servers node (Server Manager), 581
- All Servers Task Details dialog box, 172–173
- application exclusions (RMS), 646, 712
- application partitions, 74
- applications
  - high availability
    - failover clustering, 477–490
    - NLB (Network Load Balancing), 492–502
  - application-specific backups, 322–324
- Archive Subject's Encryption Private Key, 226, 234
- assigning iSCSI targets, 448–454
- Assign iSCSI Virtual Disk Wizard, 453, 515
- attribute-level replication, 6
- attributes, LastLogonTimestamp, 6
- attribute stores, AD FS, 722–723, 727–728
- Audit Central Access Policy Staging Properties policy, 632
- Audit File Share Properties dialog box, 445–446
- Audit File System policy, 411–412
- Audit File System Properties dialog box, 446
- auditing entries, configuring, 412–413

Auditing Entry for Research dialog box, 447  
 Audit Object Access policy, 411  
 Auditors group (RMS), 642  
 authentication  
     intra-forest, Multidomain Active Directory environments, 4–5  
     selective, configuring trusts, 17–18  
 Authentication Type for CES page (AD CS Configuration Wizard), 245  
 Authority Information Access (AIA) distribution points, 215  
 Authorization page (DHCP Post-Install Configuration Wizard), 173  
 autoenrollment, certificate management, 231–233  
     configuring certificate templates, 287–291  
     configuring group policy to support, 292–296  
 Autoenroll permission (certificates), 232  
 automatic certificate renewal, 230, 292–296

## B

backup, CAs (certificate authorities), 221–223  
 Backup Once Wizard, 351  
 Backup Operators group, Windows Server Backup, 313  
 backups, 311–328  
     configuring CBR-DC, 344–350  
     Data Protection Manager, 328  
     network, 352–356  
     performing to a local volume, 350–352  
     role- and application-specific backups, 322–324  
     system restore points, 327–328  
     Vssadmin, 324–327  
     Windows Azure Backup, 317–322  
     Windows Server Backup, 312–317  
 Backup Schedule Wizard, 346  
 BCD (Boot Configuration Data) store, 336–337, 370–374  
 bcdedit /v command, 370  
 Before You Begin page  
     Add Roles and Features Wizard, 170  
     Certificate Enrollment Wizard, 283  
     Provision IPAM Wizard, 190  
 blocks (IP address space), 147  
 Boot Configuration Data (BCD) store, 336–337, 370–374  
 booting into Safe Mode, 368–370  
 BranchCache, 406–410  
     configuring policies, 466–470  
     deployment, 470–473

BranchCache-Content Retrieval (Uses HTTP) firewall rule, 410  
 BranchCache for Network File Server role service, 407–408  
 BranchCache for Network Files role, 470–471  
 BranchCache-Hosted Cache Server (Uses HTTPS) firewall rule, 410  
 BranchCache-Peer Discovery (Uses WSD) firewall rule, 410  
 Bridge All Site Links checkbox, 67  
 Bring Disk Online dialog box, 456  
 Browse for Folder dialog box, 432  
 by-directional trust relationships, 14

## C

Cache Locking (DNS)  
     modifying, 161–163  
 CA Compromise issue, revoking a certificate, 228  
 CA for CES page (AD CS Configuration Wizard), 245  
 CA Name page (AD CS Configuration Wizard), 243  
 CAs (certificate authorities)  
     backup and recovery, 221–223  
     configuring templates  
         autoenrollment, 287–291  
         private key archival, 295–297  
     defined, 210  
     enterprise root CAs, 239–247  
     enterprise subordinate CAs, 247–253  
     installation, 210–216  
         enterprise root CAs, 213–214  
         hierarchies, 212–213  
         HSM (hardware security modules), 216  
         role services, 211–212  
         standalone root CAs, 215–216  
         standalone subordinate CAs, 216  
     managing certificates  
         recovery, 300–305  
         revocation, 297–300  
     standalone CAs, 257–260  
     standalone subordinate CAs, 253–257  
 CA trusts, configuring, 750–752  
 CA Type page (AD CS Configuration Wizard), 242  
 CAU (Cluster-Aware Updating), 484–486, 540–547  
 CDPs (CRL Distribution Points), 217–218, 260–265  
 Cease of Operation issue, revoking a certificate, 228  
 Central Access Policies Configuration dialog box, 631

## central access policies (DAC)

- central access policies (DAC), 630–631, 683–686
- central access rules (DAC), 628–630
  - configuring resource properties, 625–628
  - creating, 679–683
- certificate authorities. *See* CAs
- Certificate Enrollment Policy Web Service, 212
- Certificate Enrollment Web Service, 212
- Certificate Enrollment Wizard, 283
- Certificate Hold issue, revoking a certificate, 228
- Certificate Import Wizard, 304
- certificate revocation checks, 740–751
- Certificate Revocation dialog box, 298
- Certificate Revocation List (CRL)
  - Distribution Points, 217–218
- certificates
  - acquiring for servers, 752–755
  - AD FS, 726–727
  - management, 226–236
    - autoenrollment, 231–233
    - key archiving and recovery, 233–236
    - recovery, 300–305
    - renewal, 230–231
    - revocation, 227–229
    - templates, 226–227
  - RMS, configuring, 638–639
- Certificate Services
  - installation and configuration, 209–223
    - administrative role separation, 219–221
    - CA backup and recovery, 221–223
    - CAs (certificate authorities), 210–216
    - CDPs (CRL Distribution Points), 217–218
    - online responders, 218–219
  - managing certificates, 226–236
    - autoenrollment, 231–233
    - key archiving and recovery, 233–236
    - renewal, 230–231
    - revocation, 227–229
    - templates, 226–227
- Certificate Services Client-Auto-Enrollment group policy, 232
- Certificate Services Client-Auto-Enrollment policy, 292
- Certificate Services Client-Certificate Enrollment Policy dialog box, 293
- Certificate Services Client-Credential Roaming Properties dialog box, 294
- Certificates Snap-in dialog box, 283, 301–302
- Certification Authority Backup Wizard, 222
- Certification Authority Restore Wizard, 222–223
- Certification Authority role service, 211
- Certification Authority Web Enrollment role service, 211
- Certified for Windows Server 2012 logo requirement, 478
- Certutil-backup c:\backup command, 222
- Certutil-getkey <serial number> outputblob command, 304
- Certutil-urllcache crl delete command, 299
- Certutil-urllcache ocsps delete command, 299
- Change of Affiliation issue, revoking a certificate, 228
- Changing Key Archival Property dialog box, 296
- Changing RUP Exclusion List dialog box, 295
  - checkboxes
    - Active Directory Certificate Services, 239
    - Bridge All Site Links, 67
- Checkpoint-Computer cmdlet, 327
- child domains, 3
  - creating, 28–30
  - preparing domain controller to host contiguous namespace, 26–28
- claim rules, AD FS, 722–723, 728–730, 771–779
- claims AD FS, 722–723
- claims-based authentication, 722
- claims (DAC), 623–625
- claims providers AD FS, 723
- claims provider trust claim rules, 729–730
- claims provider trusts, AD FS, 725, 768–769
- classification (files)
  - applying RMS templates, 712–716
  - creating rules, 668–677
  - preparing server, 666–668
  - running/verifying, 677–679
- Classification Parameters dialog box, 441
- Classification Properties node, 440
- classifications, files, 410–411
  - configuring, 440–442
  - verification, 442–444
- client licensor certificates, 639
- cluster address input, installing RMS, 638
- Cluster-Aware Updating (CAU), 484–486, 540–547
- Cluster-Aware Updating dialog box, 540–541
- clustering, failover clustering, 477–490
  - CAU (Cluster-Aware Updating), 484–486
  - cluster quorum modes, 479–481
  - cluster storage and shared volumes, 481–484
  - continuously available shares, 489–490
  - migrating/updating clusters, 486–487

- preference settings, 487–489
  - cluster key passwords, installing RMS, 638
  - cluster key storage, installing RMS, 637
  - Cluster page RMS), 637
  - cluster quorum
    - configuration, 480–481, 529–530
    - modes, 479–481
  - clusters
    - hosts, 496–498
    - migrating/upgrading, 486–487
    - networks, 483–484
    - nodes, adding, 527–529
    - operation modes, 495–496
    - RMS (Rights Management Services), 636–638
    - validating configuration, 524–525
  - Cluster Shared Volumes (CSVs), 482, 552
  - ClusterStorage folder, 552
  - cmdlets
    - Checkpoint-Computer, 327
    - Get-ADTrust, 22
    - Install-WindowsFeature, 423
    - Invoke-IpamGpoProvisioning Windows PowerShell, 144
    - Move-ADDirectoryServer, 71
    - New-ADReplicationSiteLink, 67
    - New-ADReplicationSiteLinkBridge, 68
    - New-ADReplicationSite Windows PowerShell, 62
    - New-ADReplicationSubnet, 63
    - New-IscsiServerTarget, 418
    - New-IscsiVirtualDisk, 418
    - NLB (Network Load Balancing), 501–502
    - Set-ADDomainMode Windows PowerShell, 5
    - Set-ADForestMode Windows PowerShell, 7
    - Set-DhcpServerv4DnsSetting, 138
    - Set-DhcpServerv6DnsSetting, 138
    - Windows Server Backup, 316
  - CNAME records, 126–127, 166
  - commands
    - bcdedit /v, 370
    - Certutil-backup c:\backup, 222
    - Certutil-getkey <serial number> outputblob, 304
    - Certutil-urlcache cri delete, 299
    - Certutil-urlcache ocp delete, 299
    - Dnscmd /config /socketpoolsize, 161
    - Exit, 366
    - Get-DhcpServerv4DnsSetting-Computer MEL-DC, 183, 184
    - (Get-DNSServer).ServerSetting.SocketPoolSize, 161
    - get-DNSServerCache, 161, 162
    - Get-DNSServerGlobalNameZone, 164
    - Gpresult /r /scope computer, 197
    - Gpresult /r /scope:computer, 446
    - gpupdate /force, 193
    - Gpupdate /force, 160, 295, 299, 446
    - Ipconfig /renew, 366
    - Mkdir c:\new-vm-destination, 609
    - Mkdir c:\vm-store, 593
    - Netdom join ADL-DC /domain:contoso.com, 189
    - repadmin /kcc, 112
    - repadmin /prp view adl-dc reveal, 112
    - repadmin /replsummary, 111–112
    - repadmin /showrepl, 113
    - repadmin /syncall, 113
    - Resolve-dnsname per-dc.contosoc.com, 202
    - Restart-Computer, 427
    - Restart-Service DNS, 161, 162
    - Set-DhcpServerv4DnsSetting-Computer MEL-DC-NameProtection \$true, 184
    - Set-DNSServerCache-LockingPercent, 162
    - Set-DNSServerGlobalNameZone-ComputerName SYD-DC-Enable \$True, 164
    - Shutdown /r /t 0, 248
    - Vssadmin create shadow /For=C:, 357
    - Vssadmin list providers, 357
    - Vssadmin list shadows, 357
    - Vssadmin list volumes, 357
    - Wpeinit, 366
  - Compatibility tab (Properties of New Template dialog box), 276
  - Compatibility (certificate template setting), 226
  - Completing the New Zone Wizard page (New Zone Wizard), 164
  - components AD FS, 722
  - Compound Authentication policy, 623
  - Computer Management console, 344–345
  - Computer Name/Domain Changes dialog box, 154
  - Computer Name tab (System Properties dialog box), 154
  - conditional forwarders, 734–736
  - Confidential classification (files), 410–411
  - configuration partitions, 73
  - Configure BranchCache for Network Files dialog box, 469
  - Configure BranchCache for Network Files policy, 408
  - Configure DHCP Options page (Welcome to the New Scope Wizard), 176

## Configure Failover Wizard

- Configure Failover Wizard, 186–188
- Configure Hosted Cache Servers policy, 409
- Configure Recovery History page
  - Enable Replication Wizard, 570–571
  - Reverse Replication Wizard, 615–616
- Configure Server Discovery dialog box, 144, 191
- configuring
  - Access Denied Assistance, 633–634, 686–688
  - Active Directory Certificate Services, 209–223
  - additional domain controllers, 97–102
  - AD FS
    - CA trusts, 750–752
    - certificate relationships, 726–727
    - claim rules, 771–779
    - claims provider trusts, 768–769
    - proxy servers, 730
    - relying party trusts, 766–768
  - administrative role separation, 272–276
  - advanced storage options, 415–424
    - Features on Demand, 422–424
    - iSCSI target and intiation, 416–419
    - iSNS Server, 419–420
    - thin provisioning, 421
    - trim, 422
  - affinity, 511–514
  - application exclusions, 712
  - backups, 311–328
    - CBR-DC, 344–350
    - Data Protection Manager, 328
    - role- and application-specific backups, 322–324
    - system restore points, 327–328
    - Vssadmin, 324–327
    - Windows Azure Backup, 317–322
    - Windows Server Backup, 312–317
  - BranchCache policies, 466–470
  - Certificate Services
    - administrative role separation, 219–221
    - CA backup and recovery, 221–223
    - CDPs (CRL Distribution Points), 217–218
    - online responders, 218–219
  - certificate templates for autoenrollment, 287–291
  - certificate templates for private key archival, 295–297
  - CRL Distribution Points, 260–265
  - DAC (Dynamic Access Control)
    - resource properties, 625–628, 664–666
    - staging, 688–690
    - user and device claims, 623–625, 658–663
  - delegated administration, 131–132
  - DHCP failover, 186–189
  - DNS event logs, 124–126, 166–168
  - DNS forwarding, 734–736
  - DNS recursion, 129–130
  - DNSSEC, 122–124, 155–158
  - DNS socket pools, 128
  - domains and forests, 1–11
    - Multidomain Active Directory environments, 2–8
    - Multiforest Active Directory environments, 8
    - upgrading existing domains and forests, 9–10
    - UPN suffixes, 10–12
  - enterprise root CAs (certificate authorities), 239–247
  - failback settings, 536–539
  - failover settings, 536–539
  - file access auditing, 444–448
  - file classifications, 440–442
  - file screens, 400–403
  - File Server Resource Manager File Classification Rules, 625–626
  - GlobalNames Zones, 163–166
  - group policy, 292–296
  - group policy support for DAC, 623, 651–653
  - high availability file servers, 531–534
  - high availability file shares, 533–536
  - Hyper-V Live Migration, 605
  - Hyper-V Replica, 567–573
  - Hyper-V Replica Broker, 574
  - IPAM GPOs and server discovery, 190–192
  - iSCSI targets, 516
  - key recovery, 285–287
  - key recovery agent certificate templates, 276–281
  - MEL-DC, 154–155
  - move node, 536–539
  - Name Protection feature (DHCP), 182–184
  - name resolution policy, 158–160
  - name suffix routing, 44–47
  - netmask ordering, 130–131
  - online responders, 265–273
  - Password Replication Policy, 78–79
  - permissions, 132
  - port rules, 511–514
  - quotas, 403–405, 428–434
  - replication polling schedule, 75
  - RMS (Rights Management Services), 636–647, 695–704
    - Administrator and Super User groups, 642–644
    - applying templates automatically, 646–647

- certificates and licenses, 638–639
- exclusion policies, 645–646
- template distribution, 710–711
- templates, 639–642
- trusted user and publish domains, 644–645
- RODC replication, 106–108
- RODCs, 102–106
- selective authentication, 46–50
- server discovery (IPAM), 144–147
- server manageability, 146
- servers to be managed by IPAM, 192–198
- shortcut trusts, 51–55
- sites, 59–71
  - moving domain controllers, 70–71
  - sites and subnets, 60–68
  - SRV record registration, 68–70
- standalone CAs (certificate authorities), 257–260
- trusts (trust relationships), 13–23, 35–38
  - external trusts, 17–18
  - forest trusts, 16–17
  - name suffix routing, 23
  - netdom.exe, 21–22
  - realm trusts, 20–21
  - selective authentication, 17–18
  - shortcut trusts, 18–20, 51–55
  - SID filtering, 22–23
  - transitive trusts, 14
  - trust direction, 14–15
- UPN (User Principal Name) suffixes, 51
- virtual machines for replication, 599–603
- virtual switches, 586–588
- Windows Azure Backup, 379–383
- Confirmation page (AD CS Configuration Wizard), 244
- Confirm Password dialog box, 29
- conflict resolution multi-master replication, 76–77
- connecting to iSCSI targets, 454–456
- Constrained Delegation, 6
- contiguous namespace
  - preparing domain controller to host child domain, 26–28
- continuously available shares, failover clustering, 489–490
- Contoso Policy central access policy, 630
- Copy the Virtual Machine option, importing a virtual machine, 562
- Create a New Failover Relationship page (Configure Failover Wizard), 188
- Create Central Access Policy: Contoso Policy dialog box, 631
- Create Classification Rule dialog box, 440, 628
- Create DHCP Scope dialog box, 200
- Create Distributed Rights Policy Template Wizard, 640
- Create File Management Task dialog box, 647
- Create File Screen Exception dialog box, 438–439
- Create File Screen Template dialog box, 435
- Create Group dialog box, 106, 272
- Create Quota Template dialog box, 429
- creating
  - AD RMS Super User groups, 703–704
  - AD RMS templates, 705–710
  - central access policies, 683–686
  - central access rules, 679–683
  - child domains, 28–30
  - DAC users and groups, 653–657
  - DHCP scope, 200
  - DHCP superscopes, 175–179
  - file classification rules, 668–677
  - forests, 34–35
  - forest trust relationships, 38–41
  - iSCSI targets, 448–454
  - multicast scopes, 185–187
  - NLB clusters, 507–511
  - rights policy templates, 639
  - shared storage, failover clustering, 515–518
  - site link bridges, 67–68
  - site links, 64–67, 94–95
  - sites, 62–63, 89–91
  - split scopes, 179–182
  - storage pool, 456–460
  - subnets, 63–65, 91–94
  - thin provisioned virtual disks, 456–460
  - two-node failover cluster, 525–527
  - virtual machines, 595–598
- Credential page (AD CS Configuration Wizard), 241
- credential roaming, configuring group policy to support, 292–296
- Credential Security Support Provider (CredSSP), 557
- Credentials for Deployment Operation dialog box, 104
- CredSSP (Credential Security Support Provider), 557
- CRL (Certificate Revocation List)
  - Distribution Points, 217–218
- CRL Distribution Points (CDPs), 217–218, 260–265
  - dialog boxes, 217–218
- cross certification trusts, 213–214

cryptographic mode installing AD RMS, 637  
Cryptography for CA page (AD CS Configuration Wizard), 243  
CSVs (Cluster Shared Volumes), 482, 552  
Customize Message for Access Denied Errors policy, 633

## D

DAC (Dynamic Access Control), 621–634  
  central access policies, 630–631  
  central access rules, 628–630  
  configuring  
    group policy support, 623, 651–653  
    resource properties, 625–628, 664–666  
    user and device claims, 623–625, 658–663  
  staging, 632–633, 688–690  
  users and groups, creating, 653–657  
data  
  backups, 311–328  
    Data Protection Manager, 328  
    role- and application-specific backups, 322–324  
    system restore points, 327–328  
    Vssadmin, 324–327  
    Windows Azure Backup, 317–322  
    Windows Server Backup, 312–317  
  recovery, 330–337  
    BCD (Boot Configuration Data) store, 336–337  
    Last KNown Good Configuration, 336  
    restoring from backups, 330–333  
    Safe Mode, 335–336  
    Windows Recovery Environment, 333–335  
  Data Protection Manager (DPM), 328  
  Debug Logging tab (DNS server properties dialog box), 125–126  
  Default-First-Site-Name site, 60  
  DEFAULTIPSITELINK site link, 62, 64  
  default partitions, 73–74  
  default resource properties, 625  
  delegated administration advanced DNS solutions, 131–132  
  delegation authorization rules, 728  
  Delegation tab (MEL-HV-1 Properties dialog box), 589  
  Delete Domain Controller dialog box, 81, 115  
  Delete Failover Relationship dialog box, 189  
  Delta CRL list, 217

Deny setting (Allowed RODC Password Replication security group), 78  
deployment  
  AD FS, 737–740, 756–766  
  AD RMS, 691–695  
  BranchCache, 470–473  
  enterprise root CAs (certificate authorities), 239–247  
  enterprise subordinate CAs, 247–253  
  FSRM (File Server Resource Manager), 427–428  
  GlobalNames Zones, 127  
  IPAM (IP address management), 142–151  
    configuring server discovery, 144–147  
    installation, 143–144  
    introduction to, 143  
    IP address space, 147–149  
    IPAM administration, 151  
  IPAM (IP address mangement)  
    IP address tracking, 149–150  
    online responders, 219  
  deployment options, RODCs, 105  
  Description page (DHCP Post-Install Configuration Wizard), 173  
  device claims (DAC), configuring, 623–625, 658–663  
  DFS (Distributed File System), 85  
  DFS (Distributed File System) replication, 6  
  DHCP (Dynamic Host Control Protocol)  
    creating scope using IPAM, 200  
    failover, 138–140, 186–189  
    Name Protection feature  
      configuring, 182–184  
    roles, 169–175  
    solution implementation, 134–140  
      DHCP failover, 138–140  
      multicast scopes, 136–137  
      Name Protection feature, 137–138  
      split scopes, 137  
      superscopes, 135–136  
    superscopes, 175–179  
  DHCP Post-Install Configuration Wizard, 173  
  dialog boxes  
    Add an Attribute Store, 728  
    Add/Edit Port Rule, 500, 511  
    Add Features That Are Required for Online Responder, 268  
    Add Groups, Users and Computers, 107  
    Add Host to Cluster: Connect, 509  
    Add Initiator ID, 451  
    Add IP Address, 507

- Add IPv4 Address, 201–202
- Add iSNS Server, 461
- Add or Edit IPv4 Address Block, 201
- Add or Edit Server, 198
- Add or Remove Snap-ins, 282–283
- Add Server, 179
- Add Servers, 169, 580
- Add Superseded Template, 278
- Add Threshold, 429
- Add Volumes, 349
- Advanced EFS Properties, 295
- Advanced Password Replication Policy, 80
- Advanced Password Replication Policy for ADL-DC, 110
- Advanced Security Settings for Research, 447
- Advanced Sharing, 472
- All Servers Task Details, 172–173
- Audit Central Access Policy Staging Properties, 632
- Audit File Share Properties, 445–446
- Audit File System Properties, 446
- Auditing Entry for Research, 447
- Bring Disk Online, 456
- Browse for Folder, 432
- Central Access Policies Configuration, 631
- Certificate Revocation, 298
- Certificate Services Client-Certificate Enrollment Policy, 293
- Certificate Services Client-Credential Roaming Properties, 294
- Certificates Snap-in, 283, 301–302
- Changing Key Archival Property, 296
- Changing RUP Exclusion List, 295
- Classification Parameters, 441
- Cluster-Aware Updating, 540–541
- Computer Name/Domain Changes, 154
- Configure BranchCache for Network Files, 469
- Configure Server Discovery, 144, 191
- Confirm Password, 29
- Create Central Access Policy: Contoso Policy, 631
- Create Classification Rule, 440, 628
- Create DHCP Scope, 200
- Create File Management Task, 647
- Create File Screen Exception, 438–439
- Create File Screen Template, 435
- Create Group, 106, 272
- Create Quota Template, 429
- Credentials for Deployment Operation, 104
- CRL distribution points, 217–218
- Customize Message for Access Denied Errors, 634
- Delete Domain Controller, 115
- Delete Failover Relationship, 189
- Deleting Domain Controller, 81
- Domain Services, 45, 90
- Edit Claim Rules, 778
- Enable Automatic Hosted Cache Discovery by Service Connection Point, 468–469
- Enable Certificate Templates, 266–267, 280–281, 290–291
- Ethernet Properties, 27
- Exclude Application, 646
- Explorer Enhanced Security Configuration, 257–258
- Export Trusted Publishing Domain, 645
- Export Virtual Machine, 611
- Failover, 573, 613–614
- Failover-Cluster-Aware Updating, 541
- Failover-Preview Updates, 541
- File Group Properties for Audio and Video Files, 435
- File Server Resource Manager, 430
- File Sharing, 261, 353–354
- FS-Cluster Properties, 536
- Group Policy Management Console, 158, 292
- Hyper-V Settings, 556, 567–568
- Hyper-V Settings for MEL-HV-1, 594
- Import Trusted User Domain, 644
- Initialize Disk, 521
- Internet Explorer Enhanced Security Configuration, 376
- IPAM\_Managed\_Servers Properties, 194
- IPv4 Properties, 182
- iSCSI Initiator Properties, 416, 454–455, 518–519
- iSNS Firewall Configuration, 461
- iSNS Server Properties, 419, 462–463
- Key Recovery Agent Selection, 285–286
- Local Disk (C:) Properties, 358
- Locations, 50
- MEL-HV-1 Properties, 589
- Microsoft iSCSI, 454
- Name Protection, 183
- Network Load Balancing Manager, 513
- New Cluster: Cluster IP Addresses, 507
- New Cluster: Cluster Parameters, 508
- New Cluster: Connect, 507
- New Cluster: Host Parameter, 507
- New Cluster: Port Rules, 508
- New Conditional Forwarder, 736
- New GPO, 444

## direction, trusts

- New Group, 359
- New Object-Computer, 48
- New Object-Group, 194
- New Object-Site, 62
- New Object-Subnet, 63
- New Object-User, 108–109
- New Resource Record, 165
- New Virtual Machine, 553
- Object Types, 194
- OCSF Response Signing Properties, 265–266
- Offline Settings, 407, 472
- Optimize Backup Performance, 315
- Password, 29
- Permission Entry for Current Permissions, 630
- Planned Failover, 603–604
- Prepopulate Passwords, 110
- Properties, 38
- Properties of New Template, 276
- Publish CRL, 264, 299
- Quick Connect, 455–456
- Re-image Your Computer, 367
- Replicate Now, 102
- Research Properties, 447
- Resulting Changes, 276
- Revoked Certificates Properties, 229
- Save As, 114
- Secret\_Projects, 633
- Secret Properties, 443
- Select a Domain from the Forest, 28, 98
- Select a System Image Backup, 366–367
- Select Certification Authority, 269
- Select Computer, 587
- Select Computer or Group, 447
- Select Destination Volume, 349
- SelectiveAuthRDP Properties, 49
- Select User, Computer, Service Account, or Group, 447
- Select Users, Contacts, Computers, Service Accounts, or Other Objects, 194
- Server for NFS Properties, 405
- Set BranchCache Distributed Cache Mode, 467–468
- Shrink C:, 345
- Site Link properties, 66
- SYD-DC Properties, 166
- System Configuration, 335–336
- System Properties, 154
- User Account Control, 111, 515
- Virtual Switch Manager for MEL-HV-1, 587
- Virtual Switch Manager for MEL-HV-2, 588
- Windows Azure Backup Properties, 388
- Windows Internet Explorer 10, 258
- Windows PowerShell Credential, 339, 426
- Windows PowerShell Credential pop-up, 247
- Windows Security, 28
- Windows Setup, 598
- direction, trusts, 14–15
- directory partitions, replication, 73–74
- DirectoryServices performance counters, 82
- Disable The Port Range filtering mode (NLB), 500
- Discovery tab ( iSCSI Initiators Properties dialog box), 419–420
- disks, failover clustering, 481–483
- Disks node (Failover Cluster Manager console), 481–482
- Distributed Cache Mode (BranchCache), 409
- Distributed File System (DFS), 85
- Distributed File System (DFS) replication, 6
- DnsAdmins domain local group, 131
- Dnscmd /config /socketpoolsize command, 161
- DNS (Domain Name System)
  - Cache Locking, 128–129, 161–163
  - event logs, 124–126
    - configuring and viewing, 166–168
    - recursion, 129–130, 168–169
  - socket pool, 128
    - increasing size, 161
  - solution implementation, 121–132
    - delegated administration, 131–132
    - DNS Cache Locking, 128–129
    - DNS event logs, 124–126
    - DNS recursion, 129–130
    - DNSSEC, 122–124
    - DNS socket pool, 128
    - GlobalNames Zones, 126–128
    - netmask ordering, 130–131
- DNS forwarding configuring, 734–736
- DNSKEY records, 123
- DNSSEC, 122–124, 155–158
- DNS Security Extensions (DNSSEC) page (Zone Signing Wizard), 156
- DNS tab (IPv4 Properties dialog box), 182–183
- Domain Controller Options page, 35–36
- domain controllers
  - configuring additional controllers, 97–102
  - configuring RODC password replication, 78–81
  - domain functional levels, 5–7

- domain trees, 31–33
- hosting a child domain contiguous namespace, 26–28
- monitoring and managing replication, 81–82
- moving, 70–71
- multi-master replication, 74–77
- preparing to host a new forest, 33–34
- RODC replication, 77–78

Domain Name System. *See* DNS

domain partitions, 74

domain quarantine, 22–23

domains

- child, 3
- configuring, 1–11
- Multidomain Active Directory environments, 2–8
- Multiforest Active Directory environments, 8
- upgrading existing domains and forests, 9–10
- UPN suffixes, 10–12
- functional levels, 5–7
- root, 3

Domain Services dialog box, 45, 90

Domain Services role (Active Directory), 97–98

domain trees, 3–4, 31–33

DPM (Data Protection Manager), 328

Drainstop option (cluster nodes), 497

Dynamic Access Control. *See* DAC (Dynamic Access Control)

Dynamic Host Control Protocol. *See* DHCP

dynamic quorum, 575

Dynamic Update page (New Zone Wizard), 164

## E

Edit Claim Rules dialog box, 778

Edit rights (AD RMS), 639, 640

Enable Automatic Hosted Cache Discovery by Service Connection Point dialog box, 468–469

Enable Automatic Hosted Cache Discovery by Service Connection Point policy, 410

Enable Automatic Hosted Cache Discovery by Service Connection Policy policy, 468

Enable Certificate Templates dialog box, 266–267, 280–281, 290–291

Enable Permission Staging Configuration option, 632–633

Enable Replication Wizard, 570–571

enabling

- Archive Subject’s Encryption Private Key, 234
- Cache Locking, 128–129
- DHCP Name Protection, 183
- Live Migration, 556–557
- reverse replication, 614–616

enabling BranchCache, 472–473

end-user licenses, 639

Enroll permission (certificates), 232

Enterprise Administrators group (AD RMS), 642

enterprise root CAs (certificate authorities), 213–214

- deploying and configuring, 239–247

enterprise subordinate CAs deployment, 247–253

Ethernet Properties dialog box, 27

Event Logging tab (SYD-DC Properties dialog box), 166

event logs (DNS), 124–126, 166–168

Exclude Application dialog box, 646

exclusion policies (AD RMS), configuring, 645–646

exercises. *See* practice exercises

Exit command, 366

Explorer Enhanced Security Configuration dialog box, 257–258

exporting virtual machines, 562–564, 611

Export rights (AD RMS), 640

Export Trusted Publishing Domain dialog box, 645

Export Virtual Machine dialog box, 611

Extended Policy settings (AD RMS), 641–642

external trusts, 17–18

- SID filtering, 22–23

Extract rights (AD RMS), 640

## F

failback settings, configuring, 536–539

Failover-Cluster-Aware Updating dialog box, 541

failover clustering, 477–490

- CAU (Cluster-Aware Updating), 484–486
- cluster quorum modes, 479–481
- cluster storage and shared volumes, 481–484
- configuring settings, 536–539
- connecting cluster nodes to shared storage, 517–523
- continuously available shares, 489–490
- creating shared storage, 515–518
- creating two-node clusters, 525–527
- installation, 523
- migrating/updating clusters, 486–487

## Failover Cluster Manager console

- preference settings, 487–489
- virtual machine movement, 552–556
- Failover Cluster Manager console, 554–555, 574
- Failover - Configure Self-Updating Options Wizard, 542
- failover, DHCP, 138–140, 186–189
- Failover dialog box, 573, 613–614
- Failover-Preview Updates dialog box, 541
- Faster Backup Performance option, Windows Server Backup, 315
- FcoE (Fibre Channel over Ethernet), 478
- feature files, removing, 463–466
- Features on Demand, 422–424
- Federation Server Proxy role, 722
- Federation Server role, 722
- Federation Services. *See* AD FS (Active Directory Federation Services)
- Fibre Channel, 478
- Fibre Channel over Ethernet (FcoE), 478
- file access auditing, 411–413, 444–448
- file classification
  - applying RMS templates, 712–716
  - creating rules, 668–677
  - preparing server, 666–668
  - running/verifying, 677–679
- File Classification Rules, 625–627
- file classifications, 410–411
  - configuring, 440–442
  - verification, 442–444
- File Group Properties for Audio and Video Files dialog box, 435
- file groups, 400–401
- File Replication Service (FRS), 85
- files
  - payload, 422–423
  - .vhdx, 331
- file screens, 400–403, 435–439
- File Server Resource Manager dialog box, 430
- File Server Resource Manager (FSRM), 400, 403
  - deployment, 427–428
  - installation, 428
- File Server Resource Manager (FSRM) role service, 622
- file servers
  - advanced file services, 399–413
    - BranchCache, 406–410
    - file access auditing, 411–413
    - file classifications, 410–411
    - file screens, 400–403
    - quotas, 403–405

- Server for NFS Data Store, 405–406
- configuring high availability, 531–534
- file share witnesses, 575
- File Sharing dialog box, 261, 353–354
- filtering NLB (Network Load Balancing), 499–500
- filtering, group policy, 196
- fine-grained password policies, 6
- firewalls
  - BranchCache firewall rules, 410
- forests
  - configuring, 1–11
    - Multidomain Active Directory environments, 2–8
    - Multiforest Active Directory environments, 8
    - upgrading existing domains and forests, 9–10
    - UPN suffixes, 10–12
  - configuring trust relationships, 35–38
  - creating, 34–35
  - functional levels, 7–8
  - multidomain
    - reasons for implementation, 2–3
  - forest trusts, 16–17, 38–41
  - forest-wide authentication, 16
  - Forward rights (AD RMS), 640
  - FQDN (fully qualified domain name), 4
  - FRS (File Replication Service), 85
  - FS-Cluster Properties dialog box, 536
  - FSRM (File Server Resource Manager), 400, 403
    - deployment, 427–428
    - installation, 428
    - role service, 622
  - Full Control rights (AD RMS), 639
  - full network server recovery, 364–369
  - full system backups Windows Server Backup, 315
  - full volume backups Windows Server Backup, 315
  - fully qualified domain name (FQDN), 4
  - functional levels
    - domains, 5–7
    - forests, 7–8

## G

- Get-ADTrust cmdlet, 22
- Get-DhcpServerv4DnsSetting-Computer MEL-DC command, 183–184
- (Get-DNSServer).ServerSetting.SocketPoolSize command, 161
- get-DNSServerCache command, 161–162

- Get-DNSServerGlobalNameZone command, 164
- /getglobalstate switch, 86
- GlobalNames Zones, 126–128
  - configuring, 163–166
- Global Resource Property List, 626–627
- GPOs, IPAM
  - configuring, 190–192
- Gpresult /r /scope computer command, 197
- Gpresult /r /scope:computer command, 446
- GPT (GUID Partition Table), 482
- gpupdate /force command, 193
- Gpupdate /force command, 160, 295, 299, 446
- graphical user interface creating sites, 62–63
- group managed service accounts, 7
- group policy
  - filtering, 196
  - configuring, 292–296
    - configuring to support DAC, 623, 651–653
    - distribution of central access policies, 631
- Group Policy Management Console dialog box, 158, 292
- Group Policy Management Editor, 159
- groups (DAC), creating, 653–657
- GUID Partition Table (GPT), 482

## H

- hard quotas, 404
- hardware security modules (HSM), 216
- hierarchies, CAs (certificate authorities), 212–213
- high availability (apps and services)
  - configuring file shares, 533–536
  - failover clustering, 477–490
    - CAU (Cluster-Aware Updating), 484–486
    - cluster quorum modes, 479–481
    - cluster storage and shared volumes, 481–484
    - continuously available shares, 489–490
    - migrating/updating clusters, 486–487
    - preference settings, 487–489
  - installing/configuring file servers, 531–534
  - NLB (Network Load Balancing), 492–502
    - cluster hosts, 496–498
    - cluster operation modes, 495–496
    - cmdlets, 501–502
    - filtering and affinity, 499–500
    - overview, 492–494
    - port rules, 498–499
    - prerequisites, 494
- High Availability Wizard, 532
- Hosted Cache Mode (BranchCache), 406, 409
- Hot Standby mode (DHCP failover), 138
- HSM (hardware security modules), 216
- Hyper-V Live Migration, 556–559
  - configuring, 605
  - installing Hyper-V role, 580–586
- Hyper-V Manager, 596
- Hyper-V Replica, 566–575
  - configuring, 567–573
  - planned failover, 572–573
  - unplanned failover, 573–574
- Hyper-V Replica Broker, 574–575
- Hyper-V Settings dialog box, 556, 567–568
- Hyper-V Settings for MEL-HV-1 dialog box, 594

## I

- IGMP (Internet Group Management Protocol) multicast mode, 495
- implementation
  - AD FS, 721–730
    - advanced DHCP solutions, 134–140
      - DHCP failover, 138–140
      - multicast scopes, 136–137
      - Name Protection feature, 137–138
      - split scopes, 137
      - superscopes, 135–136
    - advanced DNS solutions, 121–132
      - delegated administration, 131–132
      - DNS Cache Locking, 128–129
      - DNS event logs, 124–126
      - DNS recursion, 129–130
      - DNSSEC, 122–124
      - DNS socket pool, 128
      - GlobalNames Zones, 126–128
      - netmask ordering, 130–131
  - DAC, 621–634
    - central access policies, 630–631
    - central access rules, 628–630
    - configuring group policy support, 623
    - configuring resource properties, 625–628
    - configuring user and device claims, 623–625
    - staging, 632–633
- importing virtual machines, 562–564, 612
- Import Trusted User Domain dialog box, 644
- inbound replication traffic, viewing, 83–84

## increasing socket pool size (DNS)

- increasing socket pool size (DNS), 161
- incremental backups Windows Server Backup, 315
- individual addresses (IP address space), 147
- infrastructure
  - Active Directory
    - configuring domains and forests, 1–11
    - configuring trusts, 13–23
- Initialize Disk dialog box, 521
- installation
  - AD RMS, 636–638, 695–704
  - Certificate Services, 209–223
    - administrative role separation, 219–221
    - CA backup and recovery, 221–223
    - CAs (certificate authorities), 210–216
    - CDPs (CRL Distribution Points), 217–218
    - online responders, 218–219
  - DHCP roles, 169–175
  - failover clustering, 523
  - FSRM (File Server Resource Manager), 428
  - high availability file servers, 531–534
  - IPAM (IP address management), 143–144
  - IPAM (IP address management) feature, 189–190
  - iSCSI target servers, 449
  - iSNS Server, 460–463
  - NLB (Network Load Balancing) feature, 506
  - standalone subordinate CAs, 253–257
  - Windows Server Backup, 340–344
- Installation Progress page (Add Roles and Features Wizard), 171
- installing Hyper-V role, 580–586
- Install-WindowsFeature cmdlet, 423
- Internet Explorer Enhanced Security Configuration dialog box, 376
- Internet Group Management Protocol (IGMP) multicast mode, 495
- Internet Small Computer Systems Interface (iSCSI), 478
- intra-forest authentication, Multidomain Active Directory environments, 4–5
- Introduction to DHCP Failover page (Configure Failover Wizard), 186
- Invoke-IpamGpoProvisioning Windows PowerShell cmdlet, 144
- IP addresses
  - managing space, 147–149
  - managing with IPAM, 201–202
  - tracking, 149–150
- IP address management. *See* IPAM

- IP Address Range page (Welcome to the New Scope Wizard), 176
- IPAM Administrators permissions, 151
- IPAM ASM Administrators permissions, 151
- IPAM (IP address management), 142–151
  - configuring GPOs and server discovery, 190–192
  - configuring server discovery, 144–147
  - configuring servers to be managed, 192–198
  - creating DHCP scope, 200
  - installation, 143–144, 189–190
  - introduction to, 143
  - IP address space, 147–149
  - IP address tracking, 149–150
  - IPAM administration, 151
  - managing IP addresses, 201–202
  - server management, 198–199
- IPAM IP Audit Administrators permissions, 151
- IPAM\_Managed\_Servers Properties dialog box, 194
- IPAM MSM Administrators permissions, 151
- IPAM Users permission, 151
- Ipconfig /renew command, 366
- IPv4 Properties dialog box, 182
- iSCSI Initiator, 416–419
  - properties, 455
- iSCSI Initiator Properties dialog, 518–519
  - dialog box, 416, 454–455
- iSCSI (Internet Small Computer Systems Interface), 478
- iSCSI targets, 416–419
  - configuring, 516
  - connecting to, 454–456
  - creating/assigning, 448–454
  - installing servers, 449
- iSCSI Target Server role service, 416
- iSNS Firewall Configuration dialog box, 461
- iSNS Server, 419–420
  - installation, 460–463
- iSNS Server Properties dialog box, 419, 462–463
- iSNS Server Service feature, 460–461
- issuance authorization rules, 728
- issuance transform rules, 728
- issuing CAs (certificate authorities), 212

## K

- KCC (Knowledge Consistency Checker), 75
- /kcc switch, 84
- KDC (Key Distribution Center), 7

- KDC Support for Claims policy, 623
- Kerberos Armoring policy, 623
- Kerberos authentication, 557
- Kerberos V5 authentication protocol, 13
- key archiving, certificate management, 233–236
- Key Distribution Center (KDC), 7
- Keymaster Key Recovery Agent Certificate, 286–287
- key recovery
  - configuring, 285–287
  - configuring agent certificate templates, 276–281
  - requesting agent certificates, 282–286
- Key Recovery Agent (KRA) certificate, 235
- Key Recovery Agent Selection dialog box, 285–286
- keys
  - KSK (Key Signing Key), 123
  - ZSK (Zone Signing Key), 123
- Key Signing Key (KSK), 123
- Knowledge Consistency Checker (KCC), 75
- KRA (Key Recovery Agent) certificate, 235
- KSK (Key Signing Key), 123

## L

- Last Known Good Configuration, data recovery, 336
- LastLogonTimestamp attribute, 6
- licenses (AD RMS), configuring, 638–639
- licensing-only clusters (AD RMS), 636
- licensor certificates, installing AD RMS, 638
- live migration, performing, 606–610
- Load Sharing mode (DHCP failover), 139
- Local Disk (C:) Properties dialog box, 358
- local groups, AD RMS servers, 642
- locations Windows Server Backup, 314–315
- Locations dialog box, 50
- lockbox exclusion, AD RMS, 645
- Logical Unit Number (LUN) masking, 482
- LostAndFound container, 76–77
- LUN (Logical Unit Number) masking, 482

## M

- machine certificates (AD RMS), 638
- MADCAP (Multicast Address Dynamic Client Allocation Protocol) scopes, 136
- Manage Central Access Policies policy, 631

- management
  - backups, 311–328
    - Data Protection Manager, 328
    - role- and application-specific backups, 322–324
    - system restore points, 327–328
    - Vssadmin, 324–327
    - Windows Azure Backup, 317–322
    - Windows Server Backup, 312–317
  - certificates, 226–236
    - autoenrollment, 231–233
    - key archiving and recovery, 233–236
    - recovery, 300–305
    - renewal, 230–231
    - revocation, 227–229
    - templates, 226–227
  - data recovery, 330–337
    - BCD (Boot Configuration Data) store, 336–337
    - Last KNown Good Configuration, 336
    - restoring from backups, 330–333
    - Safe Mode, 335–336
    - Windows Recovery Environment, 333–335
  - file servers, 399–413
    - BranchCache, 406–410
    - file access auditing, 411–413
    - file classifications, 410–411
    - file screens, 400–403
    - quotas, 403–405
    - Server for NFS Data Store, 405–406
  - IPAM (IP address management), 142–151
    - configuring server discovery, 144–147
    - installation, 143–144
    - introduction to, 143
    - IP addresses, 201–202
    - IP address space, 147–149
    - IP address tracking, 149–150
    - IPAM administration, 151
    - servers, 198–199
  - replication, 81–86
    - Repadmin tool, 83–85
    - upgrading SYSVOL replication, 85–86
  - SRV records registration, 68–70
- Management Console (AD RMS), creating rights policy templates, 639
- Master Boot Record (MBR), 482
- Maximum Client Lead Time, DHCP failover, 139
- MBR (Master Boot Record), 482
- MEL-DC, configuring, 154–155
- MEL-HV-1 Properties dialog box, 589

## Members tab ( IPAM\_Managed\_Servers Properties dialog box)

- Members tab ( IPAM\_Managed\_Servers Properties dialog box), 194
- Microsoft iSCSI dialog box, 454
- Microsoft Multipath I/O (MPIO), 482
- Microsoft Virtual System Migration Service, 589
- migrating clusters, 486–487
- Migration Tool, Active Directory, 9
- Mkdir c:\new-vm-destination command, 609
- Mkdir c:\vm-store command, 593
- modes cluster quorum, 479–481
- modifying
  - replication schedules, 95–96
  - site link costs, 95–96
- monitoring
  - replication, 81–86
    - practice exercise, 111–113
    - Repadm tool, 83–85
    - upgrading SYSVOL replication, 85–86
- Move-ADDirectoryServer cmdlet, 71
- move node, configuring, 536–539
- Move the Virtual Machine's Storage, storage migration, 560
- moving domain controllers, 70–71
- MPIO (Microsoft Multipath I/O), 482
- Multicast Address Dynamic Client Allocation Protocol (MADCAP) scopes, 136
- multicast mode (NLB cluster operation mode), 495
- multicast scopes, 136–137, 185–187
- Multidomain Active Directory environments, 2–8
  - domain functional levels, 5–7
  - domain trees, 3–4
  - forest functional levels, 7–8
  - intra-forest authentication, 4–5
- multidomain forests reasons for implementation, 2–3
- Multiforest Active Directory environments, 8
- multi-master replication, 74–77
- Multiple-Host filtering mode (NLB), 500
- multisite clustering site-level fault tolerance, 575–576

## N

- Name Protection dialog box, 183
- Name Protection feature (DHCP), 137–138, 182–184
- name resolution policy, configuring, 158–160
- Name Resolution Policy Table (NRPT), 123, 160
- name suffix routing, 23
  - configuring, 44–47

- Name Suffix Routing tab, 23
- NetBIOS name, verifying, 32–33
- netdom.exe, configuring trusts, 21–22
- Netdom join ADL-DC /domain:contoso.com command, 189
- netmask ordering, 130–131, 168–169
- network backups, 352–356
- Network Connections window, 27
- Network Device Enrollment Service, 211
- Network File System (NFS) protocol, 405
- Network Load Balancing Manager console, 496
- Network Load Balancing Manager dialog box, 513
- Network Load Balancing (NLB), 492–502
  - cluster hosts, 496–498
  - cluster operation modes, 495–496
  - cmdlets, 501–502
  - filtering and affinity, 499–500
  - installation, 506
  - overview, 492–494
  - port rules, 498–499
  - prerequisites, 494
  - upgrading NLB clusters, 500
- Networks node (Failover Cluster Manager console), 483–484
- New-ADReplicationSiteLinkBridge cmdlet, 68
- New-ADReplicationSiteLink cmdlet, 67
- New-ADReplicationSite Windows PowerShell cmdlet, 62
- New-ADReplicationSubnet cmdlet, 63
- New Cluster: Cluster IP Addresses dialog box, 507
- New Cluster: Cluster Parameters dialog box, 508
- New Cluster: Connect dialog box, 507
- New Cluster: Host Parameter dialog box, 507
- New Cluster: Port Rules dialog box, 508
- New Conditional Forwarder dialog box, 736
- New GPO dialog box, 444
- New Group dialog box, 359
- New Inbound Rule Wizard, 591
- New-IscsiServerTarget cmdlet, 418
- New-IscsiVirtualDisk cmdlet, 418
- New iSCSI Virtual Disk Wizard, 450
- New Object-Computer dialog box, 48
- New Object-Group dialog box, 194
- New Object-Site dialog box, 62
- New Object-Subnet dialog box, 63
- New Object-User dialog box, 108–109
- New Remote PowerShell Tab window, 342
- New Resource Record dialog box, 165

- New Simple Volume Wizard, 345
- New Technology File System (NTFS), 482
- New Trust Wizard, 19
- New Virtual Disk Wizard, 421, 457
- New Virtual Machine dialog box, 553
- New Virtual Machine Wizard, 554
- New Volume Wizard, 459
- New-WBPolicy cmdlet (Windows Server Backup), 316
- New Zone Wizard, 163
- Next Secure (NSEC/NSEC3) records, 123
- NFS (Network File System) protocol, 405
- NLB clusters
  - creating, 507–511
  - removing, 513–514
- NLB (Network Load Balancing), 492–502
  - cluster hosts, 496–498
  - cluster operation modes, 495–496
  - cmdlets, 501–502
  - filtering and affinity, 499–500
  - installation, 506
  - overview, 492–494
  - port rules, 498–499
  - prerequisites, 494
  - upgrading NLB clusters, 500
- node and disk majority (cluster quorum mode), 479
- node and file share majority (cluster quorum mode), 479
- node majority (cluster quorum mode), 479
- No Majority (cluster quorum mode), 479
- noncontiguous namespace creating a child domain, 28–30
- NRPT (Name Resolution Policy Table), 123, 160
- NSEC/NSEC3 (Next Secure) records, 123
- NTFS (New Technology File System), 482

## O

- Object Types dialog box, 194
- OCSP (Online Certificate Status Protocol) Response
  - Signing Certificate template, 219
- OCSP Response Signing Properties dialog box, 265–266
- offline root CAs (certificate authorities), 215
- Offline Settings dialog box, 407, 472
- one-off backups Windows Server Backup, 316
- Online Certificate Status Protocol (OCSP) Response
  - Signing Certificate template, 219
- Online Responder role service, 211

- online responders
  - certificate revocation, 218–219
  - configuring, 265–273
- Optimize Backup Performance dialog box, 315
- outgoing trusts, confirming, 42

## P

- partitions, replication, 73–74
- Password dialog box, 29
- password policies, 6
- password replication
  - RODCs (Read Only Domain Controllers), 78–81
- Password Replication Policy tab, 78
- payload files, 422–423
- PCI (Peripheral Component Interconnect) devices
  - HSM (hardware security modules), 216
- peer cache mode (BranchCache), 406
- performance counters DirectoryServices, 82
- Performance Monitor replication performance, 82
- perimeter networks, standalone subordinate CAs, 216
- Peripheral Component Interconnect (PCI) devices
  - HSM (hardware security modules), 216
- Permission Entry for Current Permissions dialog box, 630
- permissions
  - configuring, 132
  - IPAM Administrators, 151
  - IPAM ASM Administrators, 151
  - IPAM IP Audit Administrators, 151
  - IPAM MSM Administrators, 151
  - IPAM Users, 151
  - staged, 632–633
- Personal Virtual Desktops, 6
- planned failover Hyper-V Replica, 572–573
- Planned Failover dialog box, 603–604
- policies
  - BranchCache, configuring, 466–470
  - fine-grained password policies, 6
- policy CAs (certificate authorities), 212
- polling replication partners, 74
- port rules
  - configuring, 511–514
  - Network Load Balancing (NLB), 498–499
- practice exercises
  - acquiring certificates for servers, 752–755

## practice exercises

- adding cluster nodes, 527–529
- AD FS deployment, 756–766
- AD RMS deployment, 691–695
- AD RMS server role, 695–704
- applying RMS templates, file classification, 712–716
- booting into Safe Mode, 368–370
- CAU (Cluster-Aware Updating), 540–547
- certificate recovery, 300–305
- certificate revocation checks, 740–751
- changing cluster quorum configuration, 529–530
- configuring
  - Access Denied Assistance, 686–688
  - AD FS claims provider trusts, 768–769
  - administrative role separation, 272–276
  - AD RMS template distribution, 710–711
  - application excursions, 712
  - BranchCache policies, 466–470
  - CA trusts, 750–752
  - CBR-DC for local backup, 344–350
  - certificate templates autoenrollment, 287–291
  - certificate templates for private key archival, 295–297
  - claim rules, 771–779
  - CRL Distribution Points, 260–265
  - DAC resource properties, 664–666
  - DAC user and device claims, 658–663
  - DHCP failover, 186–189
  - DHCP Name Protection feature, 182–184
  - DNS event logs, 166–168
  - DNS forwarding, 734–736
  - DNSSEC, 155–158
  - failback settings, 536–539
  - failover settings, 536–539
  - file access auditing, 444–448
  - file classifications, 440–442
  - GlobalNames Zones, 163–166
  - group policy, 292–296
  - high availability file servers, 531–534
  - high availability file shares, 533–536
  - Hyper-V Live Migration, 605
  - IPAM GPOs and server discovery, 190–192
  - key recovery, 285–287
  - key recovery agent certificate templates, 276–281
  - MEL-DC, 154–155
  - move node, 536–539
  - name resolution policy, 158–160
  - online responders, 265–273
  - port rules, 511–514
  - quotas/quota templates, 428–434
  - relying party trusts, 766–768
  - selective authentication, 46–50
  - servers to be managed by IPAM, 192–198
  - shortcut trusts, 51–55
  - staging (DAC), 688–690
  - standalone CAs, 257–260
  - UPN suffixes, 51
  - virtual machines for replication, 599–603
  - virtual switches, 586–588
  - Windows Azure Backup, 379–383
- configuring additional domain controllers, 97–102
- configuring RODC replication, 106–108
- configuring RODCs, 102–106
- connecting cluster nodes to shared storage, 517–523
- connecting to iSCSI targets, 454–456
- creating
  - AD RMS Super User groups, 703–704
  - AD RMS templates, 705–710
  - central access policies, 683–686
  - central access rules, 679–683
  - child domains, 28–30
  - DAC users and groups, 653–657
  - DHCP scope using IPAM, 200
  - DHCP superscopes, 175–179
  - file classification rules, 668–677
  - forests, 34–35
  - forest trust relationships, 38–44
  - multicast scopes, 185–187
  - NLB clusters, 507–511
  - shared storage, failover clustering, 515–518
  - split scopes, 179–182
  - two-node failover clusters, 525–527
- creating/assigning iSCSI targets, 448–454
- creating site links, 94–95
- creating sites, 89–91
- creating storage pool, 456–460
- creating subnets, 91–94
- creating virtual machines, 595–598
- deploying
  - BranchCache, 470–473
  - enterprise root CAs, 239–247
  - enterprise subordinate CAs, 247–253
  - FSRM, 427–428
- deploying AD FS, 737–740
- DHCP roles, 169–175

- DNS recursion, 168–169
  - domain controllers
    - preparing to host a child domain, 26
    - preparing to host a new forest, 33–34
    - preparing to host domain tree, 31
    - promoting for new domain tree, 31–33
  - enabling group policy support for DAC, 651–653
  - enabling reverse replication, 614–616
  - exporting virtual machines, 611
  - file screens, 435–439
  - full server network recovery, 364–369
  - full volume recovery, Windows Server Backup, 359–363
  - importing virtual machines, 612
  - increasing DNS socket pool size, 161
  - installation
    - failover cluster feature, 523
    - high availability file servers, 531–534
  - installing Hyper-V role, 580–586
  - installing IPAM feature, 189–190
  - installing iSNS Server, 460–463
  - installing standalone subordinate CAs, 253–257
  - managing
    - IP addresses with IPAM, 201–202
    - servers using IPAM, 198–199
  - modifying BCD (Boot Configuration Data) store, 370–374
  - modifying Cache Locking (DNS), 161–163
  - modifying replication schedules, 95–96
  - monitoring replication, 111–113
  - name suffix routing, 44–47
  - netmask ordering, 168–169
  - network backups, 352–356
  - performing a backup to a local volume, 350–352
  - performing certificate revocation, 297–300
  - performing live migration, 606–610
  - preparing claim data, 769–771
  - preparing server for file classification, 666–668
  - preparing servers for live migration, 589–591
  - preparing servers for replication, 591–595
  - removing feature files, 463–466
  - removing NLB clusters, 513–514
  - removing RODCs and resetting accounts, 114–116
  - requesting key recovery agent certificates, 282–286
  - running/verifying file classification, 677–679
  - simulating unplanned failure, 539
  - storage migration, 609–611
  - thin provisioned virtual disks, 456–460
  - triggering replication, 101–102
  - unplanned failover, 613–615
  - validating cluster configuration, 524–525
  - verifying file classifications, 442–444
  - viewing account passwords replicated, 108–111
  - viewing replication health, 603–605
  - Vssadmin, 356–359
  - Windows Azure Backup
    - backing up data to, 383–391
    - configuring, 379–383
    - configuring a standalone computer for, 374–379
    - restoring data from, 391–394
  - Windows Recovery Environment, 363
  - Windows Server Backup installation, 340–344
  - predefined firewall rules, 568
  - preference settings failover clustering, 487–489
  - preferred owners (clusters), 487–488
  - preliminary steps, Windows Azure Backup, 318–320
  - Prepopulate Passwords dialog box, 110
  - prerequisites, Network Load Balancing (NLB), 494
  - Previous Versions tab (Vssadmin), 325
  - Print rights (AD RMS), 640
  - private key archival, configuring certificate templates, 295–297
  - Private Key page (AD CS Configuration Wizard), 243
  - Processor Compatibility settings, virtual machines, 556
  - properties
    - file groups, 400–401
    - iSCSI Initiator, 416, 455
    - quota templates, 432
    - transport protocol, 67
  - Properties dialog box, 38
  - Properties of New Template dialog box, 276
  - Provision IPAM Wizard, 190
  - proxy servers, configuring AD FS, 730
  - Publish Certificate in Active Directory. (certificate template setting), 226
  - Publish CRL dialog box, 264, 299
  - Publishing domains (AD RMS), configuring, 644–645
  - publishing licenses, 638, 639
  - pull replication, 74
- ## Q
- /queue switch (repadmin tool), 85
  - Quick Connect dialog box, 455–456
  - quick migration, 555

## quotas

- quotas, 403–405
  - configuring, 428–434
  - verification, 434
- quota templates, configuring, 428–434

## R

- RACs (rights account certificates), 638
- ranges (IP address space), 147
- Read Only Domain Controllers (RODCs)
  - configuring, 102–106
  - configuring replication, 106–108
  - password replication, 78–81
  - removing, 114–116
  - replication, 77–78
- realm trusts, 20–21
- records
  - CNAME, 126–127, 166
  - DNSKEY, 123
  - NSEC/NSEC3 (Next Secure), 123
  - RRSIG (Resource Record Signature), 123
- recovery, 330–337
  - BCD (Boot Configuration Data) store, 336–337
  - full server network recovery, 364–369
  - Last KNown Good Configuration, 336
  - restoring from backups, 330–333
  - Safe Mode, 335–336
  - Windows Recovery Environment, 333–335
- recovery, certificate management, 221–223, 300–305
- recovery points, configuring recovery history, 570–571
- recursion (DNS), 129–130, 168–169
- Recycle Bin, Active Directory, 7
- ReFS (Resilient File System), 482
- Register Server Wizard, 319, 384
- Register the Virtual Machine in Place option, importing a virtual machine, 562
- registration SRV records, 68–70
- Re-image Your Computer dialog box, 367
- relative identifiers (RIDs), 2
- Relay Agent (DHCP), 137
- relying party server AD FS, 724
- relying party trusts, AD FS, 724
  - claims rules, 728–729
  - configuring, 766–768
- Remote Server Administration Tools (RSAT), 478
- removing
  - feature files, 463–466
  - NLB clusters, 513–514
  - RODCs, 114–116
- renewal, certificate management, 230–231
- Renewal Period (certificate template setting), 226
- repadmin /kcc command, 112
- repadmin /prp view adl-dc reveal command, 112
- repadmin /replsummary command, 111–112
- repadmin /showrepl command, 113
- repadmin /syncall command, 113
- Repadmin tool, monitoring and managing replication, 83–85
  - practice exercise, 111
- Replicate Now dialog box, 102
- replicate-single-object (RSO) operation, 77
- /replicate switch (repadmin tool), 85
- replication, 73–86
  - attribute-level, 6
  - configuring RODCs, 106–108
  - configuring virtual machines, 567–573, 599–603
  - DFS (Distributed File System), 6
  - directory partitions, 73–74
  - modifying schedule, 95–96
  - monitoring and managing, 81–86
    - practice exercise, 111–113
    - Repadmin tool, 83–85
    - upgrading SYSVOL replication, 85–86
  - multi-master replication, 74–77
  - preparing servers for, 591–595
  - pull, 74
  - reverse, 614–616
  - RODC password replication, 78–81
  - RODCs, 77–78
  - synchronization, 113
  - triggering, 101
  - viewing replication health, 603–605
- Replication Configuration page (Hyper-V Settings dialog box), 567–568
- /repsingleobj switch (repadmin tool), 85
- Reply All rights (AD RMS), 640
- Reply rights (AD RMS), 640
- Request Certificates page (Certificate Enrollment Wizard), 283
- Request Certificates permission (CA administrative role separation), 220
- Request Handling tab (Advanced EFS Properties dialog box), 295–296
- requesting key recovery agent certificates, 282–286

- requirements DAC (Dynamic Access Control), 622
- Research\_Projects central access rule, 630–631
- Research Properties dialog box, 447
- resetting accounts, 114–116
- Resilient File System (ReFS), 482
- Resolve-dnsname per-dc.contosoc.com command, 202
- resource properties (DAC), configuring, 625–628, 664–666
- Resource Record Signature (RRSIG) records, 123–124
- Restart-Computer command, 427
- Restart-Service DNS command, 161–162
- Restore the Virtual Machine option, importing a virtual machine, 562
- restoring data from backups, 330–333
- Resultant Policy tab (Advanced Password Replication Policy dialog box), 80
- Resulting Changes dialog box, 276
- Resume option (cluster node), 497
- reverse replication, 614–616
- Reverse Replication Wizard, 614
- revocation, certificate management, 227–229, 297–300
- Revoked Certificates Properties dialog box, 229
- RIDs (relative identifiers), 2
- rights account certificates (RACs), 638
- rights policy templates, 638–642
- RMS (Rights Management Services), 636–647
  - configuring, 695–704
    - Administrator and Super User groups, 642–644
    - application exclusions, 712
    - applying templates automatically, 646–647
    - certificates and licenses, 638–639
    - exclusion policies, 645–646
    - template distribution, 710–711
    - templates, 639–642
    - trusted user and publish domains, 644–645
  - deployment, 691–695
  - installation, 636–638, 695–704
  - Super User groups, 703–704
  - templates, 705–710
    - applying using file classification, 712–716
- /rodcpwdrepl option (repadmin tool), 85
- RODCs (Read Only Domain Controllers)
  - configuring, 102–106
  - configuring replication, 106–108
  - password replication, 78–81
  - removing, 114–116
  - replication, 77–78

- role-based administration, CAs (certificate authorities), 219–220
- roles, DHCP, 169–175
- role services
  - FSRM (File Server Resource Manager), 622
  - Active Directory Certificate Services, 211–212
- role-specific backups, 322–324
- rolling upgrades (NLB clusters), 500
- root CAs (certificate authorities), 212
  - enterprise root CAs, 213–214, 239–247
  - offline root CAs, 215
- root clusters (AD RMS), 636–638
- root domains, 3
  - UPN (User Principal Name) suffixes, 10–11
- Router (Default Gateway) page (Welcome to the New Scope Wizard), 176
- RRSIG (Resource Record Signature) records, 123–124
- RSAT (Remote Server Administration Tools), 478
- RSO (replicate-single-object) operation, 77
- running file classification, 677–679

## S

- Safe Mode, data recovery, 335–336, 368–370
- SAS (Serial Attached SCSI), 478
- Save As dialog box, 114
- Save rights (AD RMS), 639
- scheduled backups Windows Server Backup, 316
- schema partition, 74
- Scope Name page (Welcome to the New Scope Wizard), 176
- SCP (service connection point), 638
- Secret\_Projects central access rule, 630–631
- Secret\_Projects dialog box, 633
- Secret Properties dialog box, 443
- security backups, 313
- Security (certificate template setting), 226
- security principles (CA administrative role separation), 220
- Security tab (DNS Server properties dialog box), 131
- Select a Domain from the Forest dialog box, 28, 98
- Select a System Image Backup dialog box, 366–367
- Select Certification Authority dialog box, 269
- Select Computer dialog box, 587
- Select Computer or Group dialog box, 447
- Select Destination Server page (Add Roles and Features wizard), 340

## Select Destination Server page (Add Roles and Features Wizard)

- Select Destination Server page (Add Roles and Features Wizard), 170
- Select Destination Volume dialog box, 349
- Select Features page (Add Roles and Features wizard), 341
- Select Installation Type Page (Add Roles and Features Wizard), 170
- selective authentication, 6
  - configuring, 46–50
  - trusts, 17–18
- SelectiveAuthRDP Properties dialog box, 49
- Select Provisioning Method page (Provision IPAM Wizard), 190
- Select Role Services to Configure page (AD CS Configuration Wizard), 241
- Select Server Roles page (Add Roles and Features wizard), 171, 341
- Select User, Computer, Service Account, or Group dialog box, 447
- Select Users, Contacts, Computers, Service Accounts, or Other Objects dialog box, 194
- Serial Attached SCSI (SAS), 478
- server discovery (IPAM), 144–147
  - configuring, 190–192
- Server for NFS Data Store, 405–406
- Server for NFS Properties dialog box, 405
- server licensor certificates (SLCs), 638
- Server Manager
  - All Servers node, 581
- Server Message Block (SMB) Transparent Failover, 489
- servers
  - advanced file services, 399–413
    - BranchCache, 406–410
    - file access auditing, 411–413
    - file classifications, 410–411
    - file screens, 400–403
    - quotas, 403–405
    - Server for NFS Data Store, 405–406
  - IPAM, 192–198
    - managing, 198–199
  - preparing for live migration, 589–591
  - preparing for replication, 591–595
  - recovery, 330–337
    - BCD (Boot Configuration Data) store, 336–337
    - full server network recovery, 364–369
    - Last KNown Good Configuration, 336
    - restoring from backups, 330–333
    - Safe Mode, 335–336
    - Windows Recovery Environment, 333–335
  - service accounts installing AD RMS, 637
  - service connection point (SCP), 638
  - services high availability
    - failover clustering, 477–490
      - NLB (Network Load Balancing), 492–502
  - Services for Network File System tool, 405
  - Set-ADDomainMode Windows PowerShell cmdlet, 5
  - Set-ADForestMode Windows PowerShell cmdlet, 7
  - Set BranchCache Distributed Cache Mode dialog box, 467–468
  - Set BranchCache Distributed Cache Mode policy, 467
  - Set BranchCache Hosted Cache Mode policy, 409
  - Set-DhcpServerv4DnsSetting cmdlet, 138
  - Set-DhcpServerv4DnsSetting-Computer MEL-DC-NameProtection \$true command, 184
  - Set-DhcpServerv6DnsSetting cmdlet, 138
  - Set Distributed Cache Mode policy, 409
  - Set-DNSServerCache-LockingPercent command, 162
  - Set-DNSServerGlobalNameZone-ComputerName SYD-DC-Enable \$True command, 164
  - Setup Type page (AD CS Configuration Wizard), 242
  - shadow copy snapshots, Vssadmin, 325
  - Shared Nothing Hyper-V Live Migration, 556–559
  - shared storage, failover clustering
    - connecting cluster nodes to, 517–523
    - creating, 515–518
  - shared volumes, failover clustering, 481–484
  - shortcut trusts, 18–20
    - configuring, 51–55
  - /showutdvec switch (repadmin tool), 85
  - Shrink C: dialog box, 345
  - Shutdown /r /t 0 command, 248
  - SID filtering, configuring trusts, 22–23
  - Signing Options page (Zone Signing Wizard), 156
  - simulating unplanned failure, 539
  - Single Host filtering mode (NLB), 500
  - single-label name resolution
    - GlobalNames Zones, 126
  - site-level fault tolerance, 565–576
    - Hyper-V Replica, 566–575
    - multisite clustering, 575–576
  - site link bridges creating, 67–68
  - Site Link properties dialog box, 66
  - site links
    - creating, 64–67, 94–95
    - modifying cost, 95–96
  - site resilience

- site-level fault tolerance, 565–576
    - Hyper-V Replica, 566–575
    - multisite clustering, 575–576
  - virtual machine movement, 551–563
    - failover clustering, 552–556
    - Hyper-V Live Migration, 556–559
    - import/export, 562–564
    - storage migration, 559–562
  - sites configuring, 59–71
    - moving domain controllers, 70–71
    - sites and subnets, 60–68
    - SRV record registration, 68–70
    - creating, 62–63, 89–91
    - verifying placement, 101
  - Sites and Services console, 60
  - SLCs (server licensor certificates), 638
  - SMB 3.0 storage, 560
  - SMB (Server Message Block) Transparent Failover, 489
  - socket pool (DNS)
    - increasing size, 161
  - soft quotas, 404, 434
  - space management, IP addresses, 147–149
  - Specify Expiration Policy page (Create Distributed Rights Policy Template Wizard), 641
  - Specify the Partner Server to Use for Failover page (Configure Failover Wizard), 187
  - split scopes, 137, 179–182
  - SRV records registration, 68–70
  - staged permissions, 632–633
  - staging (DAC), 632–633
    - configuring, 688–690
  - standalone CAs (certificate authorities)
    - configuring, 257–260
  - stand-alone federation server, 760
  - standalone root CAs, 215–216
  - standalone subordinate CAs, 216, 253–257
  - Start option (cluster node), 497
  - Start-WBBackup cmdlet (Windows Server Backup), 316
  - Start-WBFileRecovery cmdlet (Windows Server Backup), 316
  - Start-WBHyperVRecovery cmdlet (Windows Server Backup), 316
  - Start-WBSystemStateRecovery cmdlet (Windows Server Backup), 316
  - Start-WBVolumeRecovery cmdlet (Windows Server Backup), 316
  - Stop option (cluster node), 497
  - storage
    - advanced options, 415–424
      - Features on Demand, 422–424
      - iSCSI target and initiation, 416–419
      - iSNS Server, 419–420
      - thin provisioning, 421
      - trim, 422
      - trim storage, 421
    - failover clustering, 481–484
    - storage migration
      - practice exercise, 609–611
      - virtual machine movement, 559–562
    - storage pool, creating, 456–460
    - store and forward replication, 75–76
    - subnets creating, 63–65, 91–94
    - Subordinate Certification Authority template, 297
    - Summary page (Provision IPAM Wizard), 191
    - superscopes, 135–136, 175–179
    - Superseded reason, revoking a certificate, 228
    - Superseded Templates (certificate template setting), 226
    - Superseded Templates tab (Properties of New Template dialog box), 278
    - Super User groups (RMS), 642–644, 703–704
    - SYD-DC\Forward Lookup Zones node, 156
    - SYD-DC Properties dialog box, 166
    - synchronization replication, 113
    - System Configuration dialog box, 335–336
    - System Properties dialog box, 154
    - system restore points, 327–328
    - System State backups, 322–323
    - SYSVOL replication
      - upgrading, 85–86
- ## T
- Template Administrators group (AD RMS), 642
  - templates
    - AD RMS, 639–642, 705–710
      - applying automatically, 646–647
      - applying using file classification, 712–716
      - configuring distribution, 710–711
    - certificates, 226–227
    - file screens, 401–402, 436
    - quotas, 404
      - configuring, 428–434
    - thin provisioned virtual disks, creating, 456–460
    - thin provisioning, 421

## token-decrypting certificates, AD FS

- token-decrypting certificates, AD FS, 727
- token-signing certificates, AD FS, 727
- tools
  - Repadmin, monitoring and managing replication, 83–85
  - Services for Network File System, 405
- Track by Client ID parameter, tracking IP addresses, 149
- Track by Host Name parameter, tracking IP addresses, 149
- Track by IP Address parameter, tracking IP addresses, 149
- Track by User Name parameter, tracking IP addresses, 150
- tracking IP addresses, 149–150
- transitive trusts, 14
- transport protocol properties, 67
- triggering replication, 101
- trim storage, 422
- trust anchor keys, 123
- trusted domains/forests, 14
- trustsd user domains (TUDs), configuring, 644–645
- trusting domains/forests, 14
- trusts cross certification, 213–214
- trusts (trust relationships)
  - configuring, 13–23, 35–38
  - external trusts, 17–18
  - forest trusts, 16–17
  - name suffix routing, 23
  - netdom.exe, 21–22
  - realm trusts, 20–21
  - selective authentication, 17–18
  - shortcut trusts, 18–20, 51–55
  - SID filtering, 22–23
  - transitive trusts, 14
  - trust direction, 14–15
  - forests, 38–41
  - intra-forest authentication, 4–5
- /trust switch, 21
- TUDs (trustsd user domains), configuring, 644–645
- two-node failover clusters, creating, 525–527

## U

- Unicast mode (NLB cluster operation mode), 495
- Universal Serial Bus (USB) ports
  - HSM (hardware security modules), 216

- unplanned failover
  - Hyper-V Replica, 573–574
  - practice exercise, 613–615
- unplanned failure, simulating, 539
- Unspecified reason, revoking a certificate, 227
- updating clusters, 486–487
- upgrading
  - domains and forests, 9–10
  - SYSVOL replication, 85–86
- upgrading NLB clusters, 500
- UPN (User Principal Name) suffixes, 10–12, 51
- USB (Universal Serial Bus) ports
  - HSM (hardware security modules), 216
- use licenses, 638
- User Account Control dialog box, 111, 515
- user claims (DAC), configuring, 623–625, 658–663
- user exclusions, AD RMS, 645
- User Principal Name (UPN) suffixes, 10–12, 51
- users (DAC), creating, 653–657

## V

- Validate a Configuration Wizard, 484
- validating cluster configuration, 524–525
- Validity Period (certificate template setting), 226
- Validity Period page (AD CS Configuration Wizard), 244
- vaults, backup (Windows Azure Backup), 318–319
- verification
  - feature removal, 465
  - file classifications, 442–444
  - file screens and exceptions, 439
  - ISNS Server configuration, 462
  - quotas, 434
- verifying
  - file classification, 677–679
  - site placement, 101
- .vhdx files, 331
- viewing
  - DNS event logs, 166–168
  - inbound replication traffic, 83–84
  - replication health, 603–605
- View rights (AD RMS), 639
- virtual machines
  - configuring for replication, 599–603
  - creating, 595–598
  - exporting, 611
  - importing, 612

- movement, 551–563
  - failover clustering, 552–556
  - Hyper-V Live Migration, 556–559
  - import/export, 562–564
  - storage migration, 559–562
- site-level fault tolerance, 565–576
  - Hyper-V Replica, 566–575
  - multisite clustering, 575–576
- virtual switches, configuring, 586–588
- Virtual Switch Manager for MEL-HV-1 dialog box, 587
- Virtual Switch Manager for MEL-HV-2 dialog box, 588
- volume recovery Windows Server Backup, 359–363
- Volume Shadow Copy Services (VSS), 324
- volume shadow copy snapshots, Vssadmin, 325
- Vssadmin, 324–327
  - applications, 356–359
- Vssadmin create shadow /For=C: command, 357
- Vssadmin list providers command, 357
- Vssadmin list shadows command, 357
- Vssadmin list volumes command, 357
- VSS (Volume Shadow Copy Services), 324

## W

- WDS (Windows Deployment Services) multicast scopes, 136
- Welcome page (New Zone Wizard), 163
- Welcome to the Certification Authority Backup Wizard, 222
- Welcome to the New Scope Wizard, 176
- Welcome to the New Zone Wizard, 35
- windows
  - Network Connections, 27
  - New Remote PowerShell Tab, 342
- Windows Azure Backup, 317–322
  - backing up data to, 383–391
  - configuring, 379–383
  - configuring a standalone computer for, 374–379
  - restoring data from, 332–333, 391–394
- Windows Azure Backup Properties dialog box, 388
- Windows Deployment Services (WDS)
  - multicast scopes, 136
- Windows Internet Explorer 10 dialog box, 258
- Windows PowerShell Credential dialog box, 339, 426
  - pop-up dialog box, 247
- Windows Recovery Environment, 333–335, 363
- Windows Security dialog box, 28

- Windows Server 2003 domain functional level, 5–6
- Windows Server 2008 domain functional level, 6
- Windows Server 2008 R2 domain functional level, 6
- Windows Server 2012 domain functional level, 6–7
- Windows Server Backup, 312–317
  - installation, 340–344
  - volume recovery, 359–363
- Windows Setup dialog box, 598
- Windows Setup Wizard, 598
- wizards
  - AD CS Configuration, 241
  - Add Node, 529
  - Add Roles and Features, 27, 170
  - Assign iSCSI Virtual Disk, 453, 515
  - Backup Once, 351
  - Backup Schedule, 346
  - Certificate Enrollment, 283
  - Certificate Import, 304
  - Certification Authority Backup, 222
  - Certification Authority Restore, 222–223
  - Configure Failover, 186–188
  - Create Distributed Rights Policy Template, 640
  - DHCP Post-Install Configuration, 173
  - Enable Replication, 570–571
  - Failover - Configure Self-Updating Options, 542
  - High Availability, 532
  - New Inbound Rule, 591
  - New iSCSI Virtual Disk, 450
  - New Simple Volume, 345
  - New Trust, 19
  - New Virtual Disk, 421, 457
  - New Virtual Machine, 554
  - New Volume, 459
  - New Zone, 163
  - Provision IPAM, 190
  - Register Server, 319, 384
  - Reverse Replication, 614
  - Validate a Configuration, 484
  - Welcome to the Certification Authority Backup, 222
  - Welcome to the New Scope, 176
  - Welcome to the New Zone, 35
  - Windows Setup, 598
  - Zone Signing, 156
- Wpeinit command, 366

## Zone Name page (New Zone Wizard)

### Z

Zone Name page (New Zone Wizard), 163

Zone Replication Scope page, 36

Zone Signing Key (ZSK), 123

Zone Signing Wizard, 156

Zone Type page (New Zone Wizard), 163

ZSK (Zone Signing Key), 123

# About the author



**ORIN THOMAS** is an MVP, an MCT and has a string of Microsoft MCSE and MCITP certifications. He has written more than 25 books for Microsoft Press and is a contributing editor at *Windows IT Pro* magazine. He has been working in IT since the early 1990's. He regularly speaks at events like TechED in Australia and around the world on Windows Server, Windows Client, System Center and security topics. Orin founded and runs the Melbourne System

Center, Security, and Infrastructure Group. You can follow him on twitter at <http://twitter.com/orinthomas>.



Now that  
you've  
read the  
book...

Tell us what you think!

Was it useful?

Did it teach you what you wanted to learn?

Was there room for improvement?

**Let us know at <http://aka.ms/tellpress>**

Your feedback goes directly to the staff at Microsoft Press,  
and we read every one of your responses. Thanks in advance!

