

Administering Windows Server 2012

Training Guide

Orin Thomas

Administering Windows Server 2012



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

This Microsoft Training Guide:

- Provides in-depth, hands-on training you take at your own pace
- Focuses on job-role-specific expertise for deploying and managing Windows Server 2012 core services
- Creates a foundation of skills which, along with on-the-job experience, can be measured by Microsoft Certification exams such as 70-411

Sharpen your skills. Increase your expertise.

- Deploy and update Windows Server 2012
- Manage account policies and service accounts
- Configure name resolution
- Administer Active Directory
- Manage Group Policy application and infrastructure
- Work with Group Policy settings and preferences
- Administer network policies
- Configure the network to enable remote access
- Manage file services
- Monitor and audit Windows Server 2012

microsoft.com/mspress



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

Operating Systems/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 70-411.

Exam Ref 70-411: Administering Windows Server 2012 ISBN 9780735673557





Training Guide: Administering Windows Server 2012

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: 978-0-735-67413-4

2345678910 LSI 876543

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. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

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

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

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

Acquisitions Editor: Michael Bolinger
Developmental Editor: Troy Mott
Production Editor: Holly Bauer

Editorial Production: Box Twelve Communications

Technical Reviewer: Randall Galloway

Copyeditor: Nancy Sixsmith **Indexer:** Angle Martin

Cover Design: Twist Creative • Seattle **Cover Composition:** Karen Montgomery

Illustrator: Rebecca Demarest

Contents at a glance

	Introduction	XV
CHAPTER 1	Deploying and updating Windows Server 2012	1
CHAPTER 2	Managing account policies and service accounts	61
CHAPTER 3	Configuring name resolution	119
CHAPTER 4	Administering Active Directory	177
CHAPTER 5	Managing Group Policy application and infrastructure	237
CHAPTER 6	Group Policy settings and preferences	275
CHAPTER 7	Administering network policies	339
CHAPTER 8	Administering remote access	413
CHAPTER 9	Managing file services	481
CHAPTER 10	Monitoring and auditing Windows Server 2012	565
APPENDIX A	Setup instructions for exercises and labs	627
	Index	631

Contents

	Introduction	XV
	System requirements	xvi
	Virtual Machine setup instructions	xvii
	Acknowledgments	xvii
	Errata & book support	xvii
	We want to hear from you	xvii
	Stay in touch	xvii
Chapter 1	Deploying and updating Windows Server 2012	1
	Before you begin.	1
	Lesson 1: Configuring and servicing Windows Server 2012 image	s 2
	Understanding Windows images	2
	Configuring Windows images	3
	Servicing Windows images	4
	Lesson summary	10
	Lesson review	11
	Lesson 2: Automated deployment of Windows Server 2012 image	es12
	Automating installation	12
	Configuring answer files	13
	Windows Deployment Services	14
	WDS requirements	15
	Managing images	18
	Configuring transmissions	24
	Lesson summary	26
	Lesson review	26

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/

	Lesson 3: Servicing and updating deployed servers	27
	Automated update deployment with WSUS	28
	New WSUS features	28
	Deploy and manage WSUS	29
	WSUS groups	34
	WSUS policies	34
	Deploying updates	36
	Automatic approval rules	38
	Lesson summary	39
	Lesson review	40
	Practice exercises	41
	Suggested practice exercises	57
	Answers	58
	Lesson 1	58
	Lesson 2	59
	Lesson 3	60
Chapter 2	Managing account policies and service accounts	61
	Before you begin	61
	Lesson 1: Implementing domain password and lockout policies	62
	Domain user password policies	62
	Account lockout settings	66
	Account management tasks	67
	Lesson summary	72
	Lesson review	72
	Lesson 2: Using fine–grained password policies	74
	Delegate password settings permissions	74
	Fine-grained password policies	76
	Lesson summary	81
	Lesson review	81
	Lesson 3: Mastering group Managed Service Accounts	83
	Group Managed Service Accounts	84
	Kerberos delegation	88
	Kerberos policies	89
	rendered peneled	

	Service principal name management	91
	Lesson summary	91
	Lesson review	92
	Practice exercises	93
	Suggested practice exercises	112
	Answers	113
	Lesson 1	113
	Lesson 2	114
	Lesson 3	116
Chapter 3	Configuring name resolution	119
	Before you begin	119
	Lesson 1: DNS zones and forwarders	120
	DNS zone types	120
	Zone delegation	126
	Split DNS	127
	Forwarders and conditional forwarders	128
	Stub zones	131
	Lesson summary	132
	Lesson review	133
	Lesson 2: WINS and GlobalNames zones	134
	WINS	135
	GlobalNames zones	139
	Peer Name Resolution Protocol	140
	Lesson summary	142
	Lesson review	142
	Lesson 3: Advanced DNS options	143
	Resource records	144
	Zone aging and scavenging	147
	DNSSEC	149
	Lesson summary	152
	Lesson review	153
	Practice exercises	154
	Suggested practice exercises	171

	Answers	172
	Lesson 1	172
	Lesson 2	173
	Lesson 3	175
Chapter 4	Administering Active Directory	177
	Before you begin	177
	Lesson 1: Domain controller management	177
	Managing operations masters	178
	Global Catalog servers	183
	Universal group membership caching	184
	Read-only domain controllers	185
	Domain controller cloning	193
	Lesson summary	194
	Lesson review	194
	Lesson 2: Domain controller maintenance	195
	Active Directory database optimization	196
	Active Directory metadata cleanup	198
	Active Directory snapshots	199
	Lesson summary	201
	Lesson review	202
	Lesson 3: Active Directory recovery	203
	Active Directory Recycle Bin	203
	Active Directory backup	206
	Active Directory recovery	208
	Lesson summary	211
	Lesson review	211
	Practice exercises	212
	Suggested practice exercises	231
	Answers	232
	Lesson 1	232
	Lesson 2	234
	Lesson 3	235

Chapter 5	Managing Group Policy application and infrastructure	237
	Before you begin	237
	Lesson 1: Group Policy Object maintenance	237
	Managing Group Policy Objects	238
	Migrate Group Policy Objects	242
	Delegate GPO management	243
	Lesson summary	246
	Lesson review	247
	Lesson 2: Managing Group Policy application	248
	Policy processing precedence	248
	Policy enforcement and blocking	249
	Group Policy security filtering	250
	Group Policy WMI filtering	252
	Loopback processing	253
	Lesson summary	255
	Lesson review	256
	Practice exercises	257
	Suggested practice exercises	270
	Answers	271
	Lesson 1	271
	Lesson 2	272
Chapter 6	Group Policy settings and preferences	275
	Before you begin	275
	Lesson 1: Folder Redirection, software installation, and scripts	275
	Folder Redirection	276
	Software installation	279
	Scripts	285
	Lesson summary	287
	Lesson review	287

	Lesson 2: Administrative templates	290
	Administrative templates	290
	Administrative template settings	291
	Central store	292
	ADMX Migrator	294
	Filter property settings	294
	Lesson summary	296
	Lesson review	296
	Lesson 3: Group Policy preferences	297
	Group Policy preference settings	298
	Item-level targeting	299
	Mapping network drives	300
	Configuring printers	302
	Configuring power options	303
	Configuring the registry	308
	Internet options	309
	Additional settings	311
	Lesson summary	315
	Lesson review	316
	Practice exercises	318
	Suggested practice exercises	332
	Answers	333
	Lesson 1	333
	Lesson 2	335
	Lesson 3	335
Chapter 7	Administering network policies	339
	Before you begin	339
	Lesson 1: Network Policy Server policies	339
	NPS deployment	340
	Connection request policies	344
	Client configuration	356
	IP filters	360
	Encryption	361

	IP settings	362
	Creating network policies	362
	NPS templates	367
	Lesson summary	368
	Lesson review	368
	Lesson 2: Network Access Protection enforcement methods	370
	DHCP enforcement	370
	IPsec enforcement	373
	802.1X enforcement	376
	VPN enforcement	379
	RD Gateway enforcement	381
	Lesson summary	384
	Lesson review	385
	Lesson 3: Network Access Protection infrastructure	386
	Windows Security Health Validator	387
	System Health Validators and System Health Agents	389
	Health policies	389
	Health Registration Authorities	391
	Remediation server groups	392
	Lesson summary	393
	Lesson review	393
	Practice exercises	394
	Suggested practice exercises	406
	Answers	407
	Lesson 1	407
	Lesson 2	408
	Lesson 3	410
Chapter 8	Administering remote access	413
	Before you begin	413
	Lesson 1: Configuring RADIUS	413
	RADIUS servers	414
	RADIUS proxies	417
	RADIUS clients	421

	RADIUS accounting	424
	Lesson summary	428
	Lesson review	428
	Lesson 2: Configuring VPN and routing	429
	Deploy Routing and Remote Access	430
	Configure VPN settings	432
	Configure routing	439
	Network Address Translation (NAT)	441
	Lesson summary	444
	Lesson review	444
	Lesson 3: Configuring DirectAccess	445
	Understanding DirectAccess	446
	DirectAccess infrastructure	446
	Configure DirectAccess	453
	Lesson summary	464
	Lesson review	465
	Practice exercises	466
	Suggested practice exercises	475
	Answers	476
	Lesson 1	476
	Lesson 2	477
	Lesson 3	479
Chapter 9	Managing file services	481
	Before you begin	481
	Lesson 1: Configure File Server Resource Manager	481
	Quotas	482
	File screens	483
	File classification	486
	File management tasks	487
	Storage reports	488
	Lesson summary	489
	Lesson review	490

	Lesson 2: Configure a Distributed File System	492
	Distributed File System	492
	DFS namespaces	492
	DFS replication	495
	Lesson summary	500
	Lesson review	500
	Lesson 3: Configure file and disk encryption	502
	Configure BitLocker	502
	Configuring Network Unlock	508
	Configuring Encrypting File System	510
	Using EFS with an Enterprise CA	511
	Key and data recovery	512
	Lesson summary	513
	Lesson review	513
	Practice exercises	515
	Suggested practice exercises	557
	Answers	558
	Lesson 1	558
	Lesson 2	560
	Lesson 3	562
Chapter 10	Monitoring and auditing Windows Server 2012	565
	Before you begin	565
	Lesson 1: Monitor servers	565
	Data collector sets	566
	Alerts	569
	Event Viewer	571
	Event subscriptions	575
	Event-driven tasks	578
	Network monitoring	581
	Lesson summary	584
	Lesson review	584

	Lesson 2: Advanced audit policies	585
	Advanced auditing	586
	Expression-based audit policies	588
	Configuring file and folder auditing	589
	Using auditpol with auditing	590
	Lesson summary	591
	Lesson review	592
	Practice exercises	593
	Suggested practice exercises	623
	Answers	624
	Lesson 1	624
	Lesson 2	625
Appendix A	Setup instructions for exercises and labs	627
	Index	631

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:

Introduction

When Microsoft Learning 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 70-411 exam are a list of tasks and areas of knowledge that describe what an 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. The objectives don't cover everything that a Windows Server 2012 systems administrator would know, and there will be tasks and areas that will be relevant to one person's real world role and not another, but the exam objectives provide a reasonable approximation of that role.

This book covers the majority of the topics and skills that are the subject of the Microsoft certification exam 70-411. The idea behind this book is that by reading it, you can learn how to perform tasks you may need to perform on a day-to-day basis in your role as a Windows Server 2012 administrator. Using the exam objectives as a working definition of that role has the additional benefit of giving you a better understanding of the topics and tasks listed on the 70-411 exam objectives. 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 *Exam Ref 70-411: Administering Windows Server 2012* (Microsoft Press, 2013) to help bolster your real-world experience. For your reference, a mapping of the topics in this book to the exam objectives is included in the back of the book in the Objectives Map.

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

- Deploy, manage, and maintain servers
- Configure file and print services
- Configure network services and access
- Configure a network policy server infrastructure
- Configure and manage Active Directory
- Configure and manage Group Policy

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 in the Appendix 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. That physical host computer must meet the following minimum hardware requirements:

- x64-based processor that includes both hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection. (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 Level Address Translation (SLAT).
- 8 GB of RAM (more is recommended).
- 80 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

The instructions for building the virtual machine environment that allow you to perform the exercises in this book are located in the Appendix.

Acknowledgments

I'd like to thank the following people for their dedication and help in getting this book written: Troy Mott, Randall Galloway, Nancy Sixsmith, Holly Bauer, and Jeff Riley.

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 on our Microsoft Press site:

http://aka.ms/TGAdminWinServer2012/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*.

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

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

Stay in touch

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

Managing Group Policy application and infrastructure

There is far more to managing Group Policy than knowing the location of specific policy items. After your environment has more than a couple of Group Policy Objects (GPOs), you have to start thinking about issues such as how they apply, who can edit them, what to do if substantive changes in policy need to be rolled back, and how you can track changes in Group Policy over time. In this chapter, you'll learn how to back up, restore, import, and export GPOs. You'll learn how to delegate the process of editing and applying GPOs and how to resolve configuration problems related to the application of Group Policy.

Lessons in this chapter:

- Lesson 1: Group Policy Object maintenance
- Lesson 2: Managing the application of Group Policy

Before you begin

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

Lesson 1: Group Policy Object maintenance

As an experienced systems administrator pursuing certification, you have a reasonable idea of how to use Group Policy. The administration of Group Policy doesn't just occur at the level of configuring individual policies. In large organizations with many policies, it's necessary to have a maintenance strategy. Ensuring that important Group Policy Objects (GPOs) are backed up and recoverable is as important as backing up and recovering other critical services such as DNS and Dynamic Host Configuration Protocol (DHCP). In this lesson, you'll learn how to back up, restore, import, and copy GPOs. You'll also learn how to delegate the management of GPOs.

237

After this lesson, you will be able to:

- Back up, import, copy, and restore GPOs.
- Migrate GPOs between domains and forests.
- Delegate GPO management.

Estimated lesson time: 45 minutes

Managing Group Policy Objects

As an experienced systems administrator, you are aware that GPOs enable you to configure settings for multiple users and computers. After you get beyond editing GPOs to configure settings, you need to start thinking about issues such as GPO maintenance. For example, if an important document is lost, you need to know how to recover it from backup. Do you know what to do if someone accidentally deletes a GPO that has hundreds of settings configured over a long period of time?



The main tool you'll use for managing GPOs is the Group Policy Management Console (GPMC), shown in Figure 5-1. You can use this console to back up, restore, import, copy, and migrate. You can also use this console to delegate GPO management tasks.

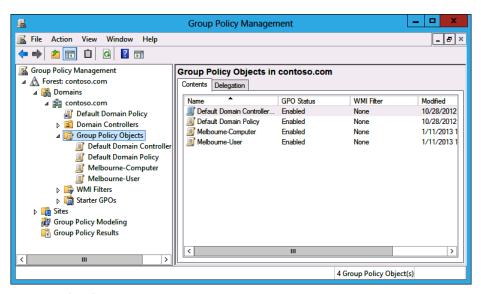


FIGURE 5-1 GPMC

There are also a substantial number of cmdlets available in the Windows PowerShell Group Policy module, including the following:

- **Get-GPO** Enables you to view GPOs. The output of this cmdlet is shown in Figure 5-2.
- **Backup-GPO** Enables you to back up GPOs.

- **Import-GPO** Enables you to import a backed-up GPO into a specified GPO.
- **New-GPO** Enables you to create a new GPO.
- **Copy-GPO** Enables you to copy a GPO.
- **Rename-GPO** Enables you to change a GPO's name.
- **Restore-GPO** Enables you to restore a backed-up GPO to its original location.
- **Remove-GPO** Enables you to remove a GPO.

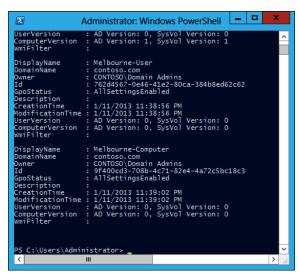


FIGURE 5-2 Output of the Get-GPO cmdlet

Backing up a GPO enables you to create a copy of a GPO as it exists at a specific point in time. A user must have read permission on a GPO to back it up. When you back up a GPO, the backup version of the GPO is incremented. It is good practice to back up GPOs prior to editing them so that if something goes wrong, you can revert to the unmodified GPO.

REAL WORLD BACKING UP GPOS

If your organization doesn't have access to the Microsoft Desktop Optimization Pack (MDOP), you should back up GPOs before you or other people modify them. If a problem occurs, it's quicker to restore a backup than it is to reconfigure the modified GPO with the existing settings.

To back up a GPO, perform the following steps:

- Open the GPMC.
- Right-click the GPO that you want to back up and click Back Up. In the Back Up Group Policy Object dialog box, shown in Figure 5-3, enter the location of the backup and a description for the backup.

239

Back Up Group Policy Object
Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.
Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.
To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.
Location:
C:\GPO-Backup ✓
Browse
Description:
Backup 28-12-2012
Back Up Cancel

FIGURE 5-3 Backing up a GPO

You can restore a GPO using the Restore-GPO cmdlet. Restoring a GPO overwrites the current version of the GPO if one exists or re-creates the GPO if the GPO has been deleted. To restore a GPO, right-click the Group Policy Objects node in the GPMC and click Manage Backups. In the Manage Backups dialog box, shown in Figure 5-4, select the GPO that you want to restore and click Restore. If multiple backups of the same GPO exist, you can select which version of a GPO to back up.

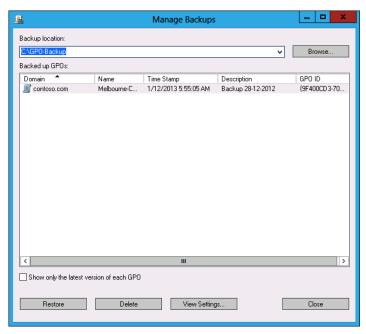


FIGURE 5-4 Restoring a GPO from backup

Import and copy GPOs

Importing a GPO enables you to take the settings in a backed-up GPO and import them into an existing GPO. To import a GPO, perform the following steps:

- Right-click an existing GPO in the GPMC and click Import Settings.
- 2. In the Import Settings Wizard, you are given the option of backing up the destination GPO's settings. This enables you to roll back the import.
- 3. Specify the folder that hosts the backed-up GPO.
- 4. On the Source GPO page of the Import Settings Wizard, shown in Figure 5-5, select the source GPO. You can view the settings that have been configured in the source GPO prior to importing it. Complete the wizard to finish importing the settings.

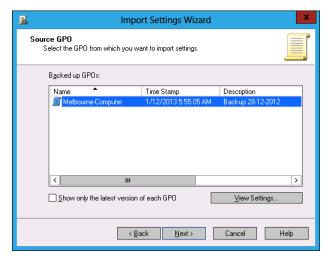


FIGURE 5-5 Importing GPO settings

Remember that when you import settings from a backed-up GPO, the settings in the backed-up GPO overwrite the settings in the destination GPO.



Copying a GPO creates a new GPO and copies all configuration settings from the original to the new. You can copy GPOs from one domain to another. You can also use a migration table when copying a GPO to map security principals referenced in the source domain to security principals referenced in the destination domain.

To copy a GPO, perform the following steps:

- Right-click the GPO that you want to copy and click Copy.
- Right-click the location that you want to copy the GPO to and click Paste.

241

In the Copy GPO dialog box, choose between using the default permissions and preserving the existing permissions assigned to the GPO (see Figure 5-6).



FIGURE 5-6 Copying a GPO

Migrate Group Policy Objects

When moving GPOs between domains or forests, you need to ensure that any domainspecific information is accounted for, so locations and security principals in the source domain aren't used in the destination domain. You can account for these locations and security principals using migration tables. You use migration tables when copying or importing GPOs.

Migration tables enable you to alter references when moving a GPO from one domain to another or from one forest to another. An example is when you are using GPOs for software deployment and need to replace the address of a shared folder that hosts a software installation file so that it is relevant to the target domain. You can open the Migration Table Editor (MTE), shown in Figure 5-7, by right-clicking Domains in the GPMC and clicking Open Migration Table Editor.

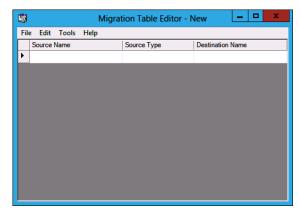


FIGURE 5-7 Opening the MTE

When you use the MTE, you can choose to populate from a GPO that is in the current domain or choose to populate the MTE from a backed-up GPO. When you perform this action, the MTE will be populated with settings that reference local objects. If, when you perform this action, there are no results, then no local locations are referenced in the GPO that you are going to migrate.

MORE INFO WORKING WITH MIGRATION TABLES

You can learn more about working with migration tables at http://technet.microsoft.com/ en-us/library/cc754682.aspx.

Delegate GPO management



In larger environments, there is more than one person in the IT department. In very large organizations, one person's entire job responsibility might be creating and editing GPOs. Delegation enables you to grant the permission to perform specific tasks to a specific user or group of users. You can delegate some or all of the following Group Policy management tasks:

- GPO creation
- GPO modification
- GPO linking to specific sites, organizational units (OUs), or domainsPermission to perform Group Policy Modeling analysis at the OU or domain levelPermission to view Group Policy Results information at the OU or domain levelWindows Management Instrumentation (WMI) filter creation

Users in the Domain Admins and Enterprise Admins groups can perform all Group Policy management tasks. Users that are members of the Group Policy Creator Owners domain group can create GPOs. They also have the right to edit and delete any GPOs that they have created.

You can delegate permissions to GPOs directly using the GPMC, as shown in Figure 5-8.

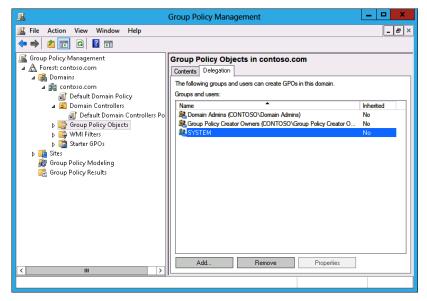


FIGURE 5-8 Group Policy permissions

243

Lesson 1: Group Policy Object maintenance

Creating GPOs

If you want to delegate the ability for users to create GPOs, you can add them to the Group Policy Creator Owners group. You can also explicitly grant them permission to create GPOs using the GPMC. To do this, perform the following steps:

- **1.** Open the GPMC from the Tools menu of Server Manager.
- 2. Expand the domain in which you want to delegate the ability to create GPOs, click Group Policy Objects, and click the Delegation tab.
- 3. Click Add and select the group or user that you want to give the ability to create GPOs in that domain.



Quick check

What group should you add users to if you want to enable them to create GPOs in the domain, but not add them to the Domain Admins or Enterprise Admins groups?

Quick check answer

■ Add them to the Group Policy Creator Owner group.

Editing GPOs

To edit a GPO, users must be either a member of the Domain Admins or Enterprise Admins group. They can edit a GPO if they created it. They can also edit a GPO if they have been given Read/Write permissions on the GPO through the GPMC.

To grant a user permission to edit a GPO, perform the following steps:

- 1. Click the GPO in the GPMC.
- **2.** Click the Delegation tab, as shown in Figure 5-9.
- 3. Click Add, specify the user or group that should have permission to edit the GPO, and then specify the permissions that you want to give this user or group. You can choose from one of the following permissions:
 - Read
 - Edit Settings
 - Edit Settings, Delete, Modify Security

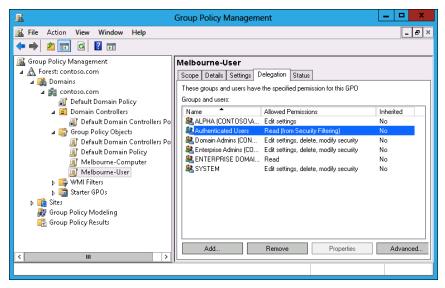


FIGURE 5-9 Delegating permissions

Linking GPOs

To enable a user to link a GPO to a specific object, you need to edit the permission on that object. You can perform this task in the GPMC, as shown in Figure 5-10. For example, to grant a user or group permission to link a GPO to an OU, select the OU in the GPMC, select the Delegation tab, click Add, and then select the user or group to which you want to grant this permission.

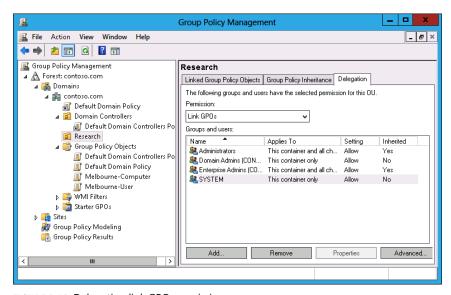


FIGURE 5-10 Delegating link GPO permission

Modeling, results, and WMI filters



Delegating permissions to perform tasks related to Group Policy Modeling and Group Policy Results is performed at the domain level, as shown in Figure 5-11. You can delegate the ability to create WMI filters by selecting the WMI Filters node in the GPMC and granting the permission on the Delegation tab.

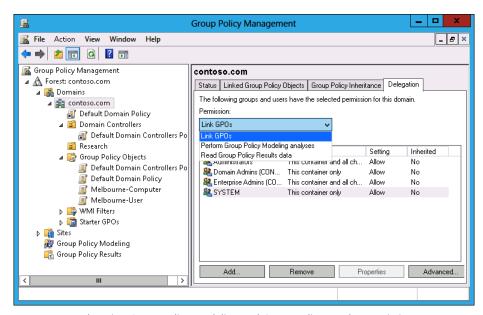


FIGURE 5-11 Delegating Group Policy Modeling and Group Policy Results permissions

Lesson summary

- Each time you back up a GPO, it creates a copy of that GPO at a particular point in time.
- Restoring a GPO overwrites the existing GPO if it still exists or recovers it if it has been deleted.
- Importing a GPO overwrites the settings in the destination GPO with the settings from the imported GPO.
- Copying a GPO creates a duplicate of the GPO.
- You use migration tables when moving GPOs between domains and forests to account for local references in the source domain.
- You can delegate the permission to create, edit, and link using the GPMC. Nonadministrative users can then perform some Group Policy tasks, such as editing policies, without giving them unnecessary privileges.

Lesson review

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

- 1. You have 200 individual GPO settings in a backed-up GPO named Melbourne-2012 that you want to include in an existing GPO named Sydney-2013. Which of the following Windows PowerShell cmdlets should you use to accomplish this goal?
 - A. Backup-GPO
 - B. Import-GPO
 - C. Restore-GPO
 - D. Copy-GPO
- 2. Prior to editing a Group Policy, your assistant makes a backup of the GPO that she is going to edit. Unfortunately, she makes a mistake in configuring the GPO. You need to revert the GPO to the state it was in prior to your assistant's edits. Which of the following Windows PowerShell cmdlets should you use to accomplish this goal?
 - A. Copy-GPO
 - B. Restore-GPO
 - **C.** Import-GPO
 - D. Backup-GPO
- 3. You want to copy a GPO from one domain to another in a forest. Which tool should you use to ensure that references to objects in the source domain updated are relevant to the destination domain? (Choose all that apply.)
 - A. Active Directory Sites And Services
 - **B.** Active Directory Users And Computers
 - Migration Table Editor
 - **D.** Group Policy Management Editor
- **4.** Which of the following security groups have the right to create GPOs by default? (Choose all that apply.)
 - A. Group Policy Creator Owners
 - **B.** Enterprise Admins
 - C. Domain Admins
 - D. Domain Controllers

- You are about to make substantial modifications to the default domain GPO. You want to ensure that you can return to the current state of the GPO if the modifications cause problems. Which of the following Windows PowerShell cmdlets should you use?
 - A. Copy-GPO
 - Restore-GPO
 - **C.** Import-GPO
 - D. Backup-GPO

Lesson 2: Managing Group Policy application

For environments in which you need to apply more than one Group Policy, understanding the rules of precedence is critical. Not only do you need to understand that where you apply a Group Policy determines its overall influence but also that GPOs may or may not apply due to inheritance blocks, security filtering, or loopback processing. In this lesson, you'll learn the rules on Group Policy application and how to determine which Group Policy settings have precedence in complex environments.

After this lesson, you will be able to:

- Determine policy processing order and precedence.
- Configure policy enforcement and blocking.
- Perform Group Policy security filtering.
- Configure WMI filtering.
- Enable loopback processing.
- Configure slow-link processing.

Estimated lesson time: 45 minutes

Policy processing precedence



In organizations with large Group Policy deployments, multiple GPOs might apply to a single user account or computer account; or when a user is signed on to a specific computer, to both. Group Policy processing precedence is the set of rules that determines which Group Policy items apply when multiple GPOs are configured.

Group Policies are processed in the following manner:

■ **Local** Settings configured at the local level apply first. If multiple local policies apply, settings in machine policies apply first, settings in admin and nonadmin local policies override them, and settings in per-user policies override any configured at the machine and admin/nonadmin level.

Site Policies based on location apply next. Any settings configured at the site level override settings configured at the local level. You can link multiple GPOs at the site level. When you do this, policies with a lower numerical link order override policies with a higher numerical link order. For example in Figure 5-12, settings in the Melbourne-Computer policy override settings configured in the Melbourne-User policy.

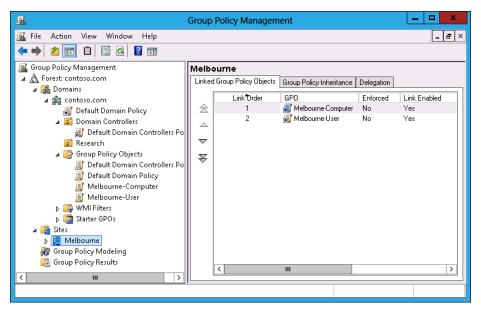


FIGURE 5-12 GPO link order

- **Domain** Settings applied at the domain level override settings applied at the site and local levels. You can link multiple GPOs at the domain level. The Default Domain Policy is linked at this level.
- Organizational unit (OU) Settings applied at the organizational unit level override settings applied at the domain, site, and local levels. When an account is a member of a child OU, policies applied at the child OU level override policies applied at the parent OU level. You can apply multiple GPOs at the OU level. Policies with a lower numerical link order override policies with a higher numerical link order.

Group Policy processing precedence is relevant only when there are conflicts in policies. If policy A applies at the domain level, and policy B applies at the OU level, both policy A and policy B apply.

Policy enforcement and blocking

When configuring a Group Policy, you can choose to enforce that policy. To enforce a Group Policy, right-click that policy at the location in which you link the policy and then click Enforced. When you choose to enforce a policy, that policy will apply and override settings configured

at other levels. For example, normally a policy linked at the OU level would override a policy linked at the domain level. If you configure the policy at the domain level as Enforced, it instead overrides the policy linked at the OU level.



The Block Inheritance function enables you to block policies applied at earlier levels. For example, you can use Block Inheritance at the OU level to block policies applied at the domain and site level. Block Inheritance does not stop the application of policies configured as Enforced. For example, Figure 5-13 shows the Research OU configured with the Block Inheritance setting. The Melbourne-Computer policy, applied at the domain level as Enforced, still applies because a setting of Enforced overrides a setting of Block Inheritance.

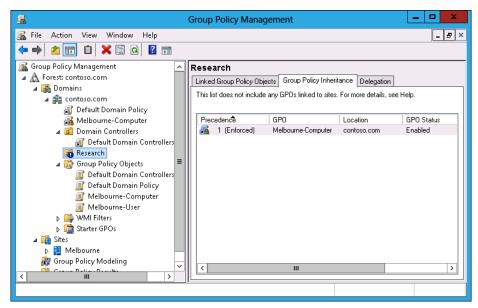


FIGURE 5-13 Override versus Enforced

Group Policy security filtering



Security filtering enables you to configure permissions on GPOs. By default, Group Policies apply to the Authenticated Users group. By changing the default permissions, you can make the Group Policy apply only to a specific group. For example, if you remove the Authenticated Users group and add another security group such as the Melbourne-Users group (shown in Figure 5-14), the Group Policy applies to only that configured security group.

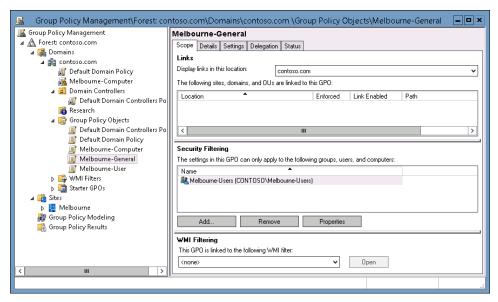


FIGURE 5-14 Security filtering

When considering whether to use security filtering, keep the following in mind:

- A security filter applies to the GPO, so it applies wherever the GPO is linked. You can't have one security filter apply to the GPO when linked at the domain level and another security filter apply to the GPO when linked at the OU level.
- Filtered policies still need to be checked during the Group Policy processing process, which can increase the amount of time spent on Group Policy processing. Startup and logon times may increase.

It is also possible to apply a Deny permission on the basis of security account or group. Deny permissions override Allow permissions. You block a particular security group from receiving a Group Policy by setting the Apply Group Policy (Deny) advanced permission, as shown for the Sydney-Users group for the Melbourne-General GPO in Figure 5-15. You can do this on the Delegation tab of a GPO's properties instead of the Scope tab.

CHAPTER 5

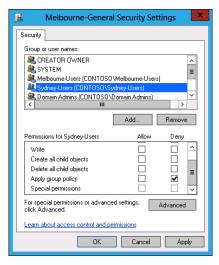


FIGURE 5-15 Security filtering



Quick check

■ How would you block a GPO from applying to members of a particular security group?

Quick check answer

■ Configure an Apply Group Policy (Deny) advanced permission on the Delegation tab of a GPO's properties.

Group Policy WMI filtering

WMI filtering enables you to filter the application of policy based on the results of a WMI query. For example, you might write a WMI query to determine whether a computer has an x86 or x64 processor, or whether there is more than a certain amount of disk space available. WMI queries are often used with policies related to software deployment to determine whether the target computer has the appropriate system resources to support the installation of the application.

The drawback of WMI queries is that they are complicated for systems administrators who are unfamiliar with programming beyond simple scripting. WMI queries also cause significant delays in Group Policy processing. In environments in which sophisticated logic needs to be applied to targeted application distribution, products such as Microsoft System Center 2012 Configuration Manager are more appropriate. System Center 2012 Configuration Manager enables administrators performing software deployment to configure ways of checking hardware configuration prior to software deployment that do not require writing queries in WMI Query Language (WQL).

You can create WMI filters by using the New WMI Filter dialog box (shown in Figure 5-16).

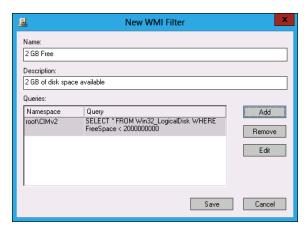


FIGURE 5-16 Creating a WMI filter

MORE INFO MORE INFO TITLE

You can learn more about WMI queries at http://msdn.microsoft.com/en-us/library/ms186146(VS.80).aspx.

Loopback processing

As you are aware, each GPO has two distinct sections: Computer Configuration and User Configuration (see Figure 5-17). The resultant policies for a user are based on the cumulative user configuration settings in GPOs that apply to the user's accounts at the site, domain, and OU setting. The resultant computer policies are applied based on the cumulative computer configuration settings in GPOs that apply to the computer's account at the site, domain, and OU level.



FIGURE 5-17 GPO structure



In some situations, you'll want only the GPOs that apply to the computer account to apply. You might want to do this with conference room computers, for which you want people to be able to sign on with domain accounts but to have a very controlled configuration. When you enable loopback processing, user settings are determined based on the settings in the User Configuration settings area of GPOs that apply to the computer account.

There are two types of loopback processing that you can configure by setting the Group Policy loopback processing mode policy, shown in Figure 5-18 and located under Computer Configuration\Administrative Templates\System\Group Policy: Replace And Merge.

- Replace When you configure Replace, only the GPOs that apply to the computer account will apply. Settings in the User Configuration area of the GPOs that apply to the computer account will apply.
- Merge The settings in the User Configuration area of GPOs that apply to the user account will still apply, but will be overridden by settings in the User Configuration area of GPOs that apply to the computer account.

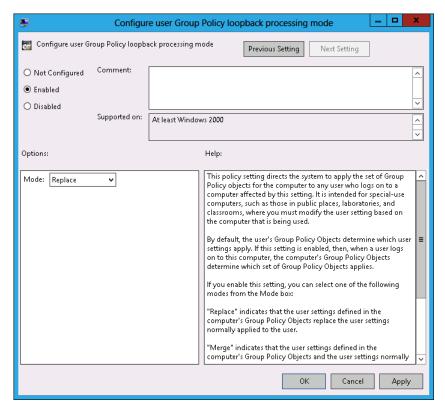


FIGURE 5-18 Loopback processing policy



Slow-link processing enables you to configure Group Policy application to be performed in a different manner, depending on the speed of the connection from the client to the domain controller. It enables you to block activities such as software deployment when the connection between Active Directory and the client is detected as falling below a particular threshold. You configure slow link detection by configuring the Group Policy slow link detection policy, as shown in Figure 5-19. This policy is located under Computer Configuration\ Administrative Templates\System\Group Policy.

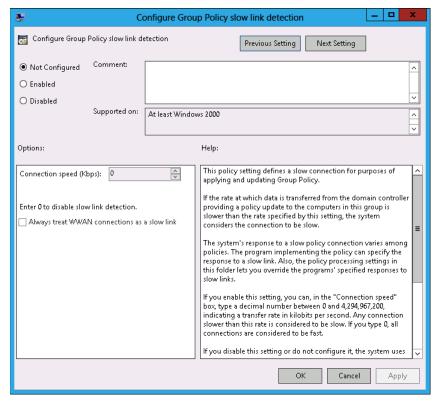


FIGURE 5-19 Slow link detection

Lesson summary

- Group policies are processed in the following order: local, site, domain, and OU. Policies processed later override policies processed earlier.
- When there are parent and child OUs, and the user or computer account is a member of the child OU, the policy applied at the child OU overrides policies applied at the parent OU.
- Policy processing order is important only when policies conflict.

- A policy with the Override setting will override other policies in the processing order, including when Block Inheritance has been configured.
- Security filtering applies on a GPO, no matter where it is linked.
- Loopback processing enables GPO settings applied to the computer account to override GPO settings applied to the user account.
- Slow-link processing enables you to configure policies not to be processed when low bandwidth connections to Active Directory are detected.

Lesson review

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

- 1. You want to ensure that a Group Policy applies only to computers that have more than 2 gigabytes (GB) of disk space. Which of the following should you configure to accomplish this goal?
 - A. Security filtering
 - WMI filtering
 - c. Loopback processing
 - **D.** Slow-link processing
- 2. A Group Policy named Alpha applies at the site level. A Group Policy named Beta is assigned link order 2 at the domain level. A Group Policy named Gamma is assigned link order 1 at the domain level. A Group Policy named Delta is assigned to the Research OU. A computer account is located in the Research OU. If the same setting is configured differently in the Alpha, Beta, Gamma, and Delta GPOs, which GPO's version of this setting will apply to the computer?
 - A. Alpha
 - B. Beta
 - C. Gamma
 - D. Delta
- 3. A Group Policy named Alpha applies at the site level. A Group Policy named Beta is assigned link order 2 at the domain level. A Group Policy named Gamma is assigned link order 1 at the domain level. A Group Policy named Delta is assigned to the Research OU. A computer account is located in the Research OU. GPO Gamma is configured with the No Override setting. If the same setting is configured differently in the Alpha, Beta, Gamma, and Delta GPOs, which GPO's version of this setting will apply to the computer?

- A. Alpha
- B. Beta
- C. Gamma
- D. Delta
- 4. A Group Policy named Alpha applies at the site level. A Group Policy named Beta is assigned link order 2 at the domain level. A Group Policy named Gamma is assigned link order 1 at the domain level. A Group Policy named Delta is assigned to the Research OU. A computer account is located in the Research OU. GPO Beta is configured with the No Override setting. OU Research is configured with the Block Inheritance setting. If the same setting is configured differently in GPOs Alpha, Beta, Gamma, and Delta, which GPO's version of this setting will apply to the computer?
 - A. Alpha
 - B. Beta
 - C. Gamma
 - D. Delta
- 5. You have a policy applied at the domain level that you don't want applied to five computers in your organization. Which of the following should you configure to accomplish this goal?
 - A. Security filtering
 - B. WMI filtering
 - C. Loopback processing
 - D. Slow-link processing

Practice exercises

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

- Creating, backing up, and restoring GPOs
- Delegating GPO permissions
- Enabling loopback processing
- Configuring blocking and enforcement
- Configuring GPO security filtering

To perform the exercises in this section, you need access to the virtual machines you created by following the instructions in the Appendix. You should ensure that you have a snapshot of the virtual machines in their unaltered configuration so that you can revert to this snapshot after you have completed these exercises.

EXERCISE 1 Prepare GPOs, security groups, and OUs

In this exercise, you will prepare GPOs. To complete this exercise, perform the following steps:

- Sign in to DC with the Contoso\Administrator account.
- In Server Manager, click the Tools menu and click Group Policy Management.
- 3. Expand the Forest: contoso.com\Domains\Contoso.com node and click Group Policy Objects, as shown in Figure 5-20.

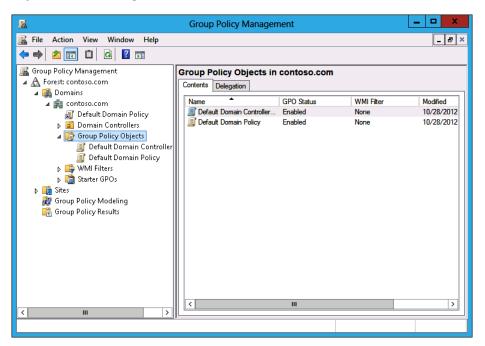


FIGURE 5-20 Clicking Group Policy Objects

- 4. In the Action menu, click New.
- In the New GPO dialog box, type **Melbourne**, as shown in Figure 5-21, and click OK.

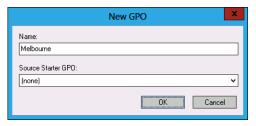


FIGURE 5-21 New GPO dialog box

Repeat steps 4 and 5 to create new GPOs named Sydney and Adelaide.

7. Verify that there are five GPOs listed, as shown in Figure 5-22.

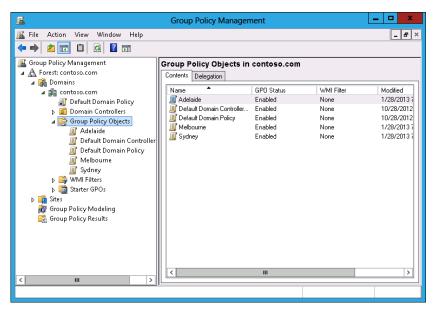


FIGURE 5-22 Three new GPOs

- 8. In Server Manager, click Active Directory Administrative Center.
- **9.** In Active Directory Administrative Center, click Contoso (Local) and then click Users, as shown in Figure 5-23.

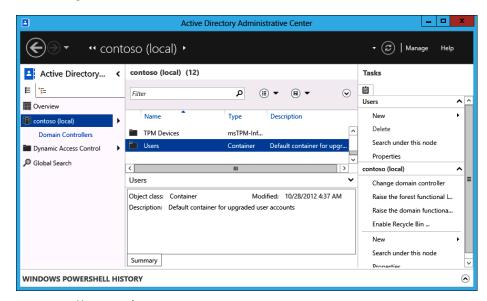


FIGURE 5-23 Users container

- 10. In the Tasks pane, click New and click Group.
- 11. In the Create Group dialog box, enter the group name Melbourne_GPO_Editors; click Security, Global, and Protect From Accidental Deletion, as shown in Figure 5-24; then click OK.

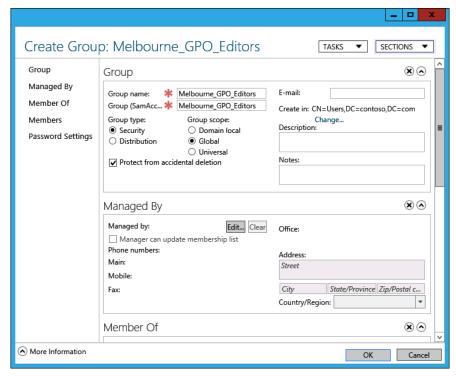


FIGURE 5-24 Creating a security group

- **12.** Repeat steps 10 and 11 to create the Adelaide_Computers security group.
- 13. In the Active Directory Administrative Center, in the Tasks pane, under Contoso (Local), click New and then click Organizational Unit.
- 14. In the Create Organizational Unit dialog box, enter the name Melbourne_Computers, as shown in Figure 5-25, and click OK.

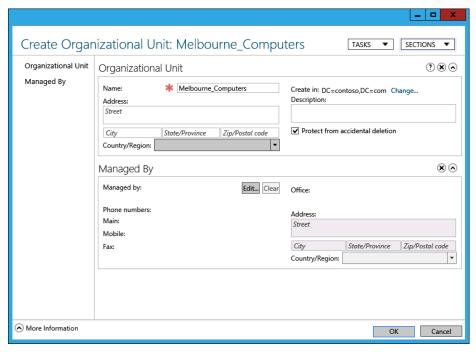


FIGURE 5-25 Create Organizational Unit dialog box

- 15. Close the Active Directory Administrative Center.
- **16.** On the taskbar, click File Manager.
- 17. In File Manager, click Computer and then double-click Local Disk (C:) .
- **18.** On the title bar of the Local Disk (C:) window, click the New Folder icon.
- **19.** Name the new folder **GPO_Backup**.
- 20. Close the Local Disk (C:) window.

EXERCISE 2 Manage GPOs

In this exercise, you will perform several Group Policy management-related tasks. To complete this exercise, perform the following steps:

- In the GPMC, click the Melbourne GPO.
- **2.** When the Melbourne GPO is selected, click the Delegation tab, as shown in Figure 5-26.

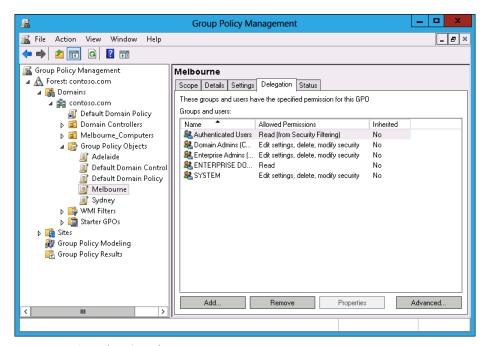


FIGURE 5-26 OU Delegation tab

- 3. On the Delegation tab, click Add.
- **4.** In the Select User, Computer, Or Group dialog box, type **Melbourne_GPO_Editors**, click Check Names, and click OK.
- **5.** In the Add Group Or User dialog box, use the drop-down menu to select Edit Settings, Delete, Modify Security, as shown in Figure 5-27, and click OK.



FIGURE 5-27 OU Delegation tab

- 6. In the GPMC, click the Sydney GPO.
- **7.** In the Action menu, click Back Up.
- **8.** In the Back Up Group Policy Object dialog box, type **C:\GPO_Backup** as the location, as shown in Figure 5-28, and click Back Up.

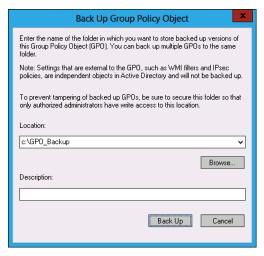


FIGURE 5-28 Back Up Group Policy Object dialog box

- **9.** In the Backup dialog box, click OK.
- **10.** In the GPMC, click the Sydney GPO.
- 11. In the Action menu, click Delete.
- 12. In the Group Policy Management dialog box, click Yes.
- **13.** Verify that the Sydney GPO is no longer listed under Group Policy Objects, as shown in Figure 5-29.

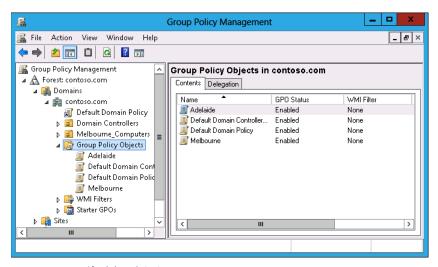


FIGURE 5-29 Verify deleted GPO

14. Click Group Policy Objects. In the Action menu, click Manage Backups.

15. In the Manage Backups dialog box, click the Sydney GPO, as shown in Figure 5-30, and click Restore.

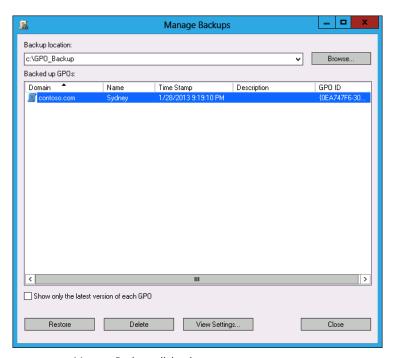


FIGURE 5-30 Manage Backups dialog box

- **16.** In the Group Policy Management dialog box, click OK.
- 17. In the Restore dialog box, click OK.
- 18. In the Manage Backups dialog box, click Close.
- **19.** Verify the presence of the Sydney GPO in the list of Group Policy Objects.

EXERCISE 3 Manage Group Policy processing

In this exercise, you will perform Group Policy management tasks related to Group Policy processing. To complete this exercise, perform the following steps:

- 1. In the GPMC, click the Adelaide GPO.
- 2. In the Action menu, click Edit.
- 3. In the Group Policy Management Editor, expand the Computer Configuration\Administrative Templates\System\Group Policy node and select the Configure User Group Policy loopback processing mode policy, as shown in Figure 5-31.

CHAPTER 5

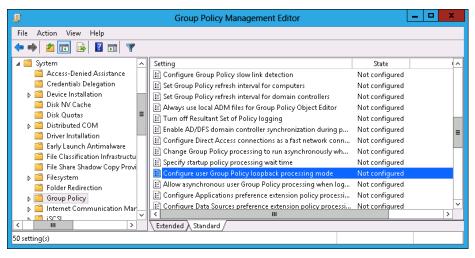


FIGURE 5-31 Select Group Policy loopback processing mode policy

- In the Action menu, click Edit.
- In the Configure User Group Policy Loopback Processing Mode dialog box, click Enabled. Set the mode to Replace, as shown in Figure 5-32, and click OK.

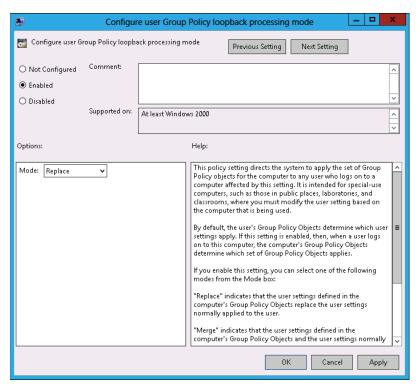


FIGURE 5-32 Configure replace mode

- 6. Close the Group Policy Management Editor.
- 7. In the GPMC, click the Adelaide GPO and click the Scope tab.
- **8.** On the Scope tab, click the Authenticated Users group and click Remove.
- **9.** In the Group Policy Management dialog box, click OK.
- 10. Under Security Filtering, click Add.
- **11.** In the Select User, Computer, Or Group dialog box, type **Adelaide_Computers**, click Check Names, and click OK.
- **12.** Verify that the security filtering properties of the Adelaide GPO match those in Figure 5-33.

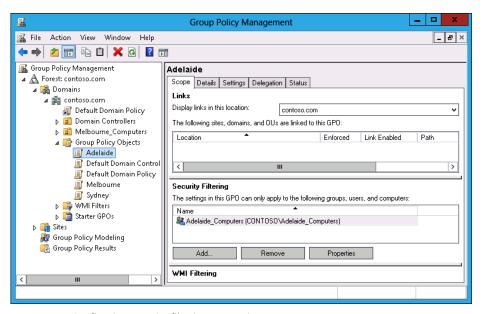


FIGURE 5-33 Configuring security filtering properties

- **13.** In the GPMC, click Contoso.com and click the Linked Group Policy Objects tab.
- **14.** Click contoso.com. In the Action menu, click Link An Existing GPO.
- 15. In the Select GPO dialog box, click Adelaide, as shown in Figure 5-34, and click OK.

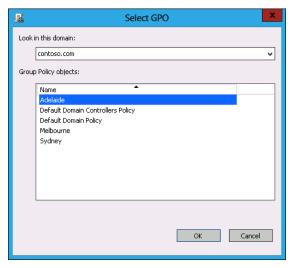


FIGURE 5-34 Selecting the GPO to link

16. In the GPMC, verify that the Adelaide GPO and the Default Domain Policy GPO are linked to the domain, as shown in Figure 5-35.

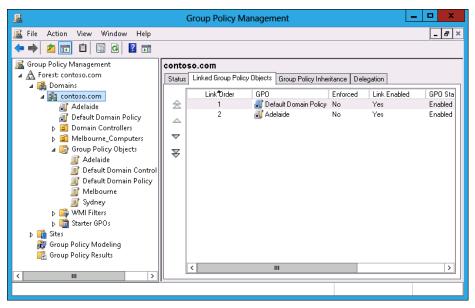


FIGURE 5-35 GPOs linked to the domain

EXERCISE 4 Group Policy Inheritance and Enforcement

In this exercise, you will perform Group Policy management tasks related to Group Policy processing. To complete this exercise, perform the following steps:

- 1. In the GPMC, click the Melbourne Computers OU.
- 2. In the Action menu, click Block Inheritance.
- 3. In the GPMC, click contoso.com.
- 4. In the Action menu, click Link An Existing GPO.
- **5.** In the Select GPO dialog box, click Melbourne and then click OK.
- Click the Melbourne GPO under contoso.com.
- 7. In the Action menu, click Enforced.
- **8.** Verify that the GPMC shows the Melbourne policy as Enforced and the Melbourne_Computers OU set to Block Inheritance, as shown in Figure 5-36.

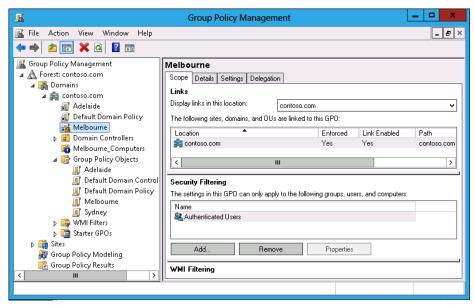


FIGURE 5-36 Block Inheritance and Enforced GPOs

- **9.** In the GPMC, click the Group Policy Modeling node.
- **10.** In the Action menu, click Group Policy Modeling Wizard.
- 11. In the Welcome page of the Group Policy Modeling Wizard, click Next.
- **12.** In the Domain Controller Selection page, click This Domain Controller and click DC.contoso.com. Click Next.
- **13.** In the User And Computer Selection page, click Browse next to Container in the Computer Information section.
- **14.** In the Choose Computer Container dialog box, click Melbourne_Computers and click OK.
- **15.** Verify that the User And Computer Selection page matches Figure 5-37 and click Next.

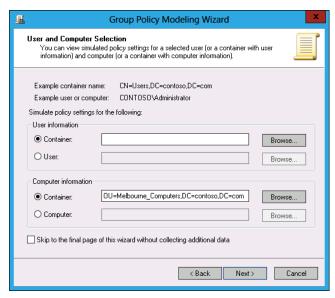


FIGURE 5-37 Group Policy Modeling Wizard

- **16.** In the Summary Of Selections page, click Next and then click Finish.
- 17. In the Warning dialog box, click OK.
- **18.** Verify that the report for the Melbourne_Computers OU matches Figure 5-38 and that only the Melbourne GPO is listed.

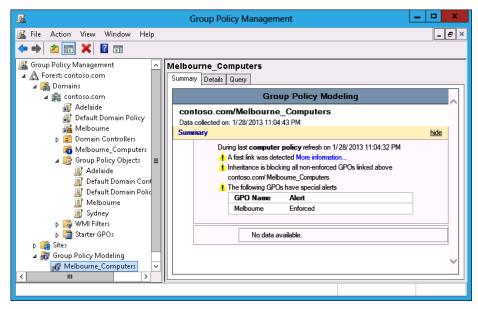


FIGURE 5-38 Group Policy Modeling results

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 GPO settings in the Melbourne GPO. Import these settings into the Sydney GPO.
- **Exercise 2** Configure the Melbourne GPO so that it will not apply to members of the Adelaide_Computers group.

Answers

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

Lesson 1

1. Correct answer: B

- **A.** Incorrect: You use the Backup-GPO cmdlet to back up an existing GPO.
- **B.** Correct: You use the Import-GPO cmdlet to import settings from a backed-up GPO to an existing target GPO.
- **C. Incorrect:** You use the Restore-GPO cmdlet to restore a backed-up GPO to a previous state.
- D. Incorrect: You use the Copy-GPO cmdlet to create a copy of an existing GPO.

2. Correct answer: B

- **A. Incorrect:** You use the Copy-GPO cmdlet to create a copy of an existing GPO.
- **B. Correct:** You use the Restore-GPO cmdlet to restore a backed-up GPO to a previous state.
- C. Incorrect: You use the Import-GPO cmdlet to import settings from a backed-up GPO to an existing target GPO. Although it would import the settings from the backed-up GPO, it is possible that other settings not included in the original backed-up GPO were configured by your assistant.
- **D. Incorrect:** You use the Backup-GPO cmdlet to back up an existing GPO.

3. Correct answer: C

- **A. Incorrect:** You use the Active Directory Sites And Services console to manage Active Directory sites. You can't use this console to configure GPO migration settings.
- **B. Incorrect:** You use this console to manage Active Directory security principals and containers. You can't use this console to configure GPO migration settings.
- **C. Correct:** You use this tool to configure the migration table, which is necessary when migrating objects from one domain or forest to another.
- **D. Incorrect:** You use this to edit GPOs. You can't use this console to configure GPO migration settings.

4. Correct answers: A, B, and C

- A. Correct: Members of the Group Policy Creator Owners group can create GPOs by default.
- **B.** Correct: Members of the Enterprise Admins group can create GPOs by default.
- **c. Correct:** Members of the Domain Admins group can create GPOs by default.
- **D. Incorrect:** The Domain Controllers group is a group for the accounts of domain controllers. It does not grant any permissions on GPOs.

5. Correct answer: D

- **A.** Incorrect: You use the Copy-GPO cmdlet to create a copy of an existing GPO. It does not allow you to revert the default domain GPO to its original state.
- B. Incorrect: You use the Restore-GPO cmdlet to restore a backed-up GPO to a previous state. You need to create the backup first.
- **C. Incorrect:** You use the Import-GPO cmdlet to import settings from a backed-up GPO to an existing target GPO.
- **D.** Correct: You use the Backup-GPO cmdlet to back up an existing GPO.

Lesson 2

1. Correct answer: B

- A. Incorrect: You use Security Filtering to filter GPO application based on security group membership.
- B. Correct: You can use a WMI query to filter GPO application based on the properties of a target computer, such as how much disk space it has available.
- **C. Incorrect:** You use loopback processing to enforce settings that apply to the computer account rather than the user account.
- **D. Incorrect:** You use slow-link processing to configure Group Policy not to apply across low-bandwidth connections.

2. Correct answer: D

- **A.** Incorrect: In this scenario, GPO Delta has precedence over the other GPOs.
- **B.** Incorrect: In this scenario, GPO Delta has precedence over the other GPOs.
- **C. Incorrect:** In this scenario, GPO Delta has precedence over the other GPOs.
- **D. Correct:** In this scenario, GPO Delta has precedence over the other GPOs.

3. Correct answer: C

- **A. Incorrect:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.
- **B. Incorrect:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.
- **C. Correct:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.
- **D. Incorrect:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.

4. Correct answer: B

- **A. Incorrect:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.
- **B.** Correct: No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.
- **C. Incorrect:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.
- **D. Incorrect:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.

5. Correct answer: A

- **A. Correct:** You use Security Filtering to filter GPO application based on security group membership. In this case, you configure the Apply Group Policy (Deny) advanced permission.
- **B. Incorrect:** You can use a WMI query to filter GPO application based on the properties of a target computer, such as how much disk space it has available.
- **c. Incorrect:** You use loopback processing to enforce settings that apply to the computer account rather than the user account.
- **D. Incorrect:** You use slow-link processing to configure Group Policy not to apply across low-bandwidth connections.

Monitoring and auditing Windows Server 2012

Properly monitoring servers is a critical component in administering them. If you monitor servers correctly, you'll know well in advance if the server is under resource pressure from lack of disk space, RAM, or processor resources. You'll be able to deal with those issues before they start to affect the people that use the servers on a day-to-day basis. Auditing servers enables you to track object access and configuration changes, from modifications to security settings to users who are accessing a particularly sensitive spreadsheet.

In this chapter, you will learn how to monitor and configure auditing for computers running the Windows Server 2012 operating system.

Lessons in this chapter:

- Lesson 1: Monitor servers
- Lesson 2: Configure advanced audit policies

Before you begin

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

Lesson 1: Monitor servers

Unwatched servers, like unwatched children, invariably end up in a chaotic state. Monitoring a server using data collector sets, alerts, and events enables you to keep an eye on the server's performance and configuration. Although effective monitoring is unlikely to stop a server from ever experiencing problems, it often provides warning signs about developing problems, giving you a chance to resolve them before they cause a service disruption. In this lesson, you will learn how to configure data collector sets, manage alerts, monitor events, and perform network monitoring.

565

After this lesson, you will be able to:

- Configure data collector sets.
- Manage alerts.
- Monitor events.
- Configure event subscriptions.
- Perform network monitoring.

Estimated lesson time: 45 minutes

Data collector sets



Data collector sets enable you to collect performance data, system configuration information, and statistics into a single file. You can use Performance Monitor or other third-party tools to analyze this information to make a determination about how well a server is functioning against an assigned workload.

You can configure data collector sets to include the following:

- **Performance counter data** The data collector set not only includes specific performance counters but also the data generated by those counters.
- **Event trace data** Enables you to track events and system activities. Event trace data can be useful when troubleshooting misbehaving applications or services.
- **System configuration information** Enables you to track the state of registry keys and record any modifications made to those keys.

Windows Server 2012 includes the following built-in data collector sets, as shown in Figure 10-1.

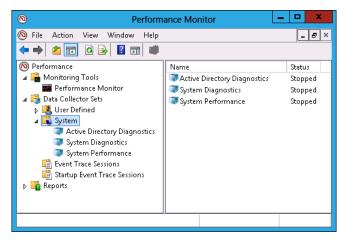


FIGURE 10-1 Built-in data collector sets

- Active Directory Diagnostics Available if you have installed the computer as a domain controller; it provides data on Active Directory health and reliability.
- System Diagnostics Enables you to troubleshoot problems with hardware, drivers, and STOP errors.
- System Performance Enables you to diagnose problems with sluggish system performance. You can determine which processes, services, or hardware may be causing performance bottlenecks.

To create a data collector set, perform the following steps:

- 1. Open Performance Monitor from the Tools menu of the Server Manager console.
- **Expand Data Collector Sets.** 2.
- 3. Click User Defined. On the Action menu, click New and click Data Collector Set.
- 4. You are given the option of creating the data collector set from a template, which enables you to select from an existing data collector set, or to create a data collector set manually. If you choose to create a data collector set manually, you have the option of creating a data log, which can include a performance counter, event trace data, and system configuration information; or a performance counter alert. This choice is shown in Figure 10-2.

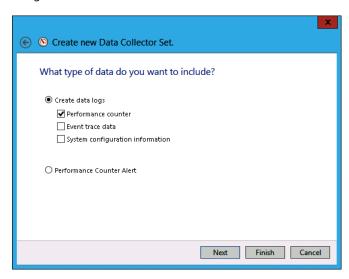


FIGURE 10-2 Creating a new data collector set

5. If you select Performance Counter, you then choose which performance counters to add to the data collector set. You also specify how often Windows should collect data from the performance counters. Figure 10-3 shows data being collected once every 15 seconds.

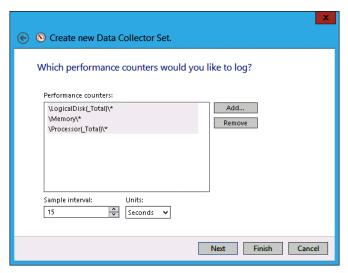


FIGURE 10-3 Setting an interval for the data collector set

6. If you choose to include event trace data, you need to enable event trace providers. As Figure 10-4, shows, a large number of event trace providers are available with Windows Server 2012. You use event trace providers when troubleshooting a specific problem. For example, the Microsoft Windows-AppLocker event trace provider helps you diagnose and troubleshoot issues related to AppLocker.

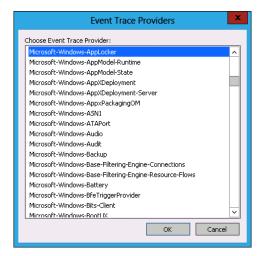


FIGURE 10-4 Event trace providers

7. If you choose to monitor system configuration information, you can select registry keys to monitor, as shown in Figure 10-5. Selecting a parent key enables you to monitor all registry changes that occur under that key while the data collector set is running.

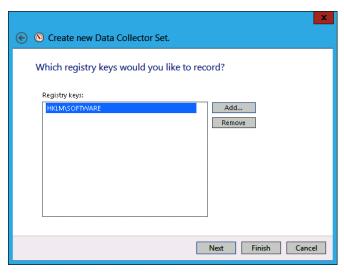


FIGURE 10-5 Setting registry keys to record

- 8. You then specify where you want data collected by the data collector set to be stored. The default location is the %systemdrive%\PerfLogs\Admin folder. If you intend to run the data collector set for an extended period of time, you should store the data on a volume separate from the one that hosts the operating system.
- 9. The final step in setting up a data collector set is to specify the account under which the data collector set runs. The default is Local System, but you can configure the data collector set to use any account for which you have the credentials.

MORE INFO DATA COLLECTOR SETS

For more information about data collector sets, consult the following TechNet link: http://technet.microsoft.com/en-us/library/cc749337.aspx.

Alerts

Performance counter alerts enable you to configure a task to run when a performance counter, such as available disk space or memory, falls under or exceeds a specific value. To configure a performance counter alert, you create a new data collector set, choose the Create Manually option, and select the Performance Counter Alert option, as shown in Figure 10-6.

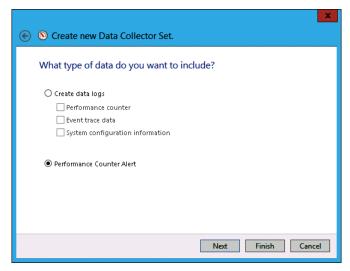


FIGURE 10-6 Configuring the performance counter alert

You add the performance counter, threshold value, and whether the alert should be triggered if the value exceeds or falls below this value. Figure 10-7 shows an alert that is triggered when the amount of available memory falls below 512 megabytes.

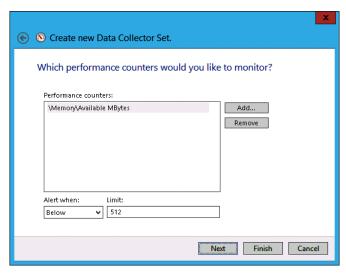


FIGURE 10-7 Setting an alert threshold

When you create an alert, all it does when triggered is to add an event to the event log. You can also configure an alert to run a scheduled task when triggered. You do this by editing the properties of the alert and specifying the name of the scheduled task on the Task tab, as shown in Figure 10-8.

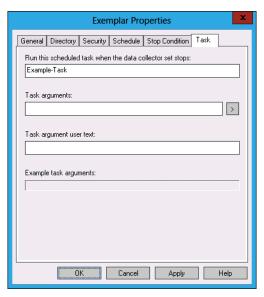


FIGURE 10-8 Running a scheduled task

Event Viewer



Event Viewer, shown in Figure 10-9, enables you to access recorded event information. The Windows Server 2012 Event Viewer differs from the Event Viewer in earlier versions of the Windows Server operating system, such as Windows Server 2003, in that it not only offers the application, security, setup and system logs but it also contains separate application and service Logs. These logs are designed to provide information on a per-role or per-application basis, rather than having all application and role service-related events funneled into the application log. When searching for events related to a specific role service, feature, or application, check to see whether that role service, feature, or application has its own application log.

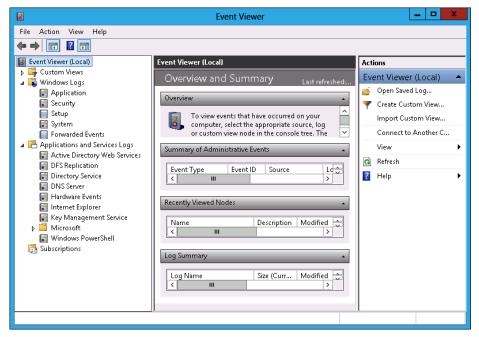


FIGURE 10-9 Event Viewer

MORE INFO EVENT VIEWER

For more information about Event Viewer, consult the following TechNet link: http://technet.microsoft.com/en-us/library/cc766042.aspx.

Event log filters

Filters and event logs enable you to view only those events that have specific characteristics. Filters apply only to the current Event Viewer session. If you constantly use a specific filter or set of filters to manage event logs, you should instead create a custom view. Filters apply only to a single event log. You can create filters on a log based on the following properties:

- **Logged** Enables you to specify the time range for the filter.
- **Event Level** Enables you to specify event levels. You can choose the following options: Critical, Warning, Verbose, Error, and Information.
- **Event Sources** Enables you to choose the source of the event.
- Event IDs Enables you to filter based on event ID. You can also exclude specific event IDs.
- **Keywords** Enables you to specify keywords based on the contents of events.

- User Enables you to limit events based on user.
- **Computer** Enables you to limit events based on the computer.

To create a filter, perform the following steps:

- Open Event Viewer and select the log that you want to filter.
- Determine the properties of the event that you want to filter.
- On the Actions pane, click Filter Current Log.
- In the Filter Current Log dialog box, shown in Figure 10-10, specify the filter properties.

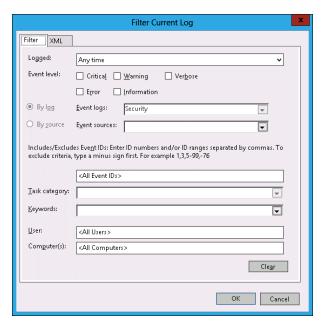


FIGURE 10-10 Specifying filter properties

Event log views

Event log views enable you to create customized views of events across any event log stored on a server, including events in the forwarded event log. Rather than looking through each event log for specific items of interest, you can create event log views that target only those specific items. Event Viewer includes a custom view named Administrative Events. This view displays critical, warning, and error events from a variety of important event logs such as the application, security and system logs.

Views differ from filters in the following ways:

■ Persistent You can use a view across multiple Event Viewer sessions. If you configure a filter on a log, it is not available the next time you open the Event Viewer.

- **Include multiple logs** A custom view can display events from separate logs. Filters are limited to displaying events from one log.
- **Exportable** You can import and export event log views between computers.

Creating an event log view is a similar process to creating a filter. The primary difference is that you can select events from multiple logs and you give the event log view a name and choose a place to save it. To create an event log view, perform the following steps:

- 1. Open Event Viewer.
- Click the Custom Views node and then click Create Custom View from the Actions menu.
- **3.** In the Create Custom View dialog box, shown in Figure 10-11, select the properties of the view, including:
 - When the events are logged
 - The event level
 - Which event log to draw events from
 - Event source
 - Task category
 - Keywords
 - User
 - Computer

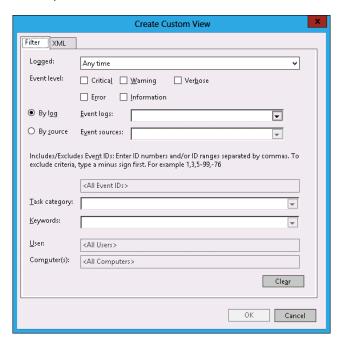


FIGURE 10-11 Creating a custom view

In the Save Filter To Custom View dialog box, enter a name for the custom view and a location in which to save the view (see Figure 10-12). Click OK.

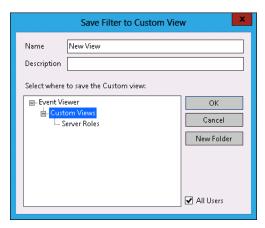


FIGURE 10-12 Entering the custom view name

5. Verify that the new view is listed as its own separate node in the Event Viewer.

You can export a custom event log view by selecting the event log view and clicking Export Custom View. Exported views can be imported on other computers running Windows Server 2012.

MORE INFO EVENT LOG VIEWS

For more information about event log views, consult the following TechNet link: http://technet.microsoft.com/en-us/library/cc766522.aspx.

Event subscriptions

Event log forwarding enables you to centralize the collection and management of events from multiple computers. Rather than having to examine the event log of each computer by making a remote connection to that computer, event log forwarding enables you to do one of the following:

- Configure a central computer to collect specific events from source computers. Use this option in environments in which you need to consolidate events from only a small number of computers.
- Configure source computers to forward specific events to a collector computer. Use this option when you have a large number of computers from which you want to consolidate events. You configure this method using Group Policy.

Event log forwarding enables you to configure the specific events that are forwarded to the central computer. This enables the computer to forward important events. It isn't necessary to forward all events from the source computer. If you discover something that warrants further investigation from the forwarded traffic, you can log on to the original source computer and view all the events from that computer in a normal manner.

REAL WORLD OPERATIONS MANAGER

In large environments, you use Microsoft System Center 2012 Operations Manager as a way of monitoring large numbers of computers for important events instead of searching through the event log manually looking for events that require further investigation.

Event log forwarding uses Windows Remote Management (WinRM) and the Windows Event Collector (wecsvc). You need to enable these services on computers that function as event forwarders and event collectors. You configure WinRM using the winrm quickconfig command. You configure wecsvc using the wecutil qc command. If you want to configure subscriptions from the security event log, you need to add the computer account of the collector computer to the local Administrators group on the source computer.

To configure a collector-initiated event subscription, configure WinRM and Windows Event Collector on the source and collector computers. In the Event Viewer, configure the Subscription Properties dialog box, shown in Figure 10-13, with the following information:

- **Subscription Name** The name of the subscription.
- **Destination Log** The log where collected events will be stored.
- Subscription Type And Source Computers: Collector Initiated Use the Select Computers dialog box to add the computers that the collector will retrieve events from. The collector must be a member of the local Administrators group or the Event Log Readers group on each source computer, depending on whether access to the security log is required.
- **Events To Collect** Create a custom view to specify which events are retrieved from each of the source computers.

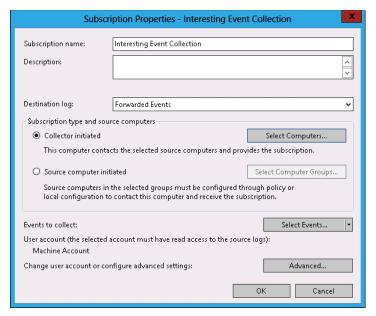


FIGURE 10-13 Configuring a collector-initiated event subscription

If you want to instead configure a source computer-initiated subscription, you need to configure the following group policies on the computers that will act as the event forwarders:

- Configure Forwarder Resource Usage This policy determines the maximum event forwarding rate in events per second. If this policy is not configured, events will be transmitted as soon as they are recorded.
- Configure Target Subscription Manager This policy enables you to set the location of the collector computer.

MORE INFO EVENT SUBSCRIPTIONS

For more information about event subscriptions, see http://technet.microsoft.com/en-us/ library/cc749183.aspx.

Both these policies are located in the Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding node. When configuring the subscription, you must also specify the computer groups that hold the computer accounts of the computers that will be forwarding events to the collector. You do this in the Computer Groups dialog box, as shown in Figure 10-14.

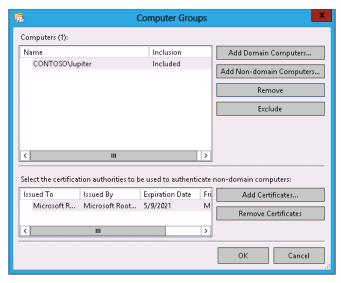


FIGURE 10-14 Configuring subscription computer groups for the subscription



Quick check

■ You want to view specific events across multiple event logs. What tool should you use to accomplish this goal?

Quick check answer

You should use custom views.

Event-driven tasks

Event Viewer enables you to attach tasks to specific events. A drawback to the process of creating event-driven tasks is that you need to have an example of the event that triggers the task already present in the event log. Events are triggered based on an event having the same log, source, and event ID.

To attach a task to a specific event, perform the following steps:

1. Open Event Viewer. Locate and select the event upon which you want to base the new task.

- 2. On the Event Viewer Actions pane, click Attach Task To This Event. The Create Basic Task Wizard displays.
- 3. On the Create A Basic Task page, review the name of the task that you want to create. By default, the task is named after the event. Click Next.
- 4. On the When An Event is Logged page, review the information about the event. This will list the log from which the event originates, the source of the event, and the event ID. Click Next.
- 5. On the Action page, shown in Figure 10-15, you can choose the task to perform. The Send An E-Mail and Display A Message tasks are deprecated, and you get an error if you try to create a task using these actions. Click Next.

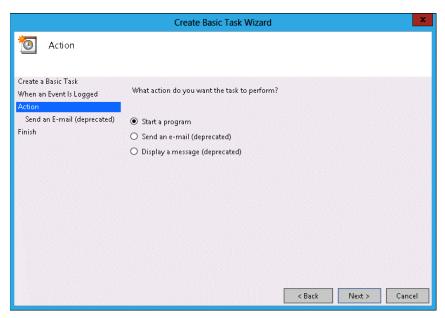


FIGURE 10-15 Attaching a task to a specific event

6. On the Start A Program page, shown in Figure 10-16, specify the program or script that should be automatically triggered as well as additional arguments.

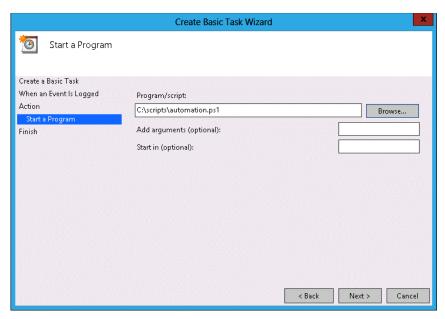


FIGURE 10-16 Specifying a triggered script

7. After you complete task creation, you can modify the task to specify the security context under which the task executes. By default, event tasks run only when the user is signed on. You can configure the task to run whether the user is signed on or not, as shown in Figure 10-17.

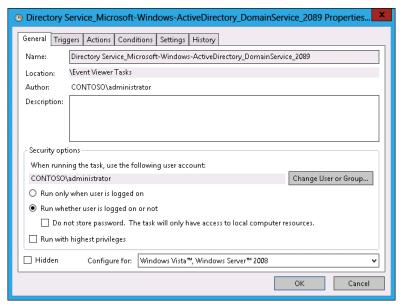


FIGURE 10-17 Run your task if the user is logged on or off

REAL WORLD IT'S NOT ABOUT SENDING EMAIL, IT'S ABOUT SENDING A MESSAGE

Even though the Send An Email task is deprecated, you can use the Start A Program option to execute a Windows PowerShell script that sends an email. In many cases, however, instead of sending a message to an administrator so the administrator can perform a task, it's better to have the task directly called wherever possible. Creating automated tasks that resolve problems without requiring direct intervention saves time and money. You should send email messages only when you need to notify yourself about an issue that cannot be resolved by running a script.

Network monitoring



Network monitoring enables you to track how a computer interacts with the network. Through network monitoring, you can determine which services and applications are using specific network interfaces, which services are listening on specific ports, and the volume of traffic that exists. There are two primary tools through which you can perform network monitoring on computers running Windows Server 2012:

- Resource Monitor
- Message Analyzer

Resource Monitor

Resource Monitor enables you to monitor how a computer running the Windows Server 2012 operating system uses CPU, memory, disk, and network resources. Resource Monitor provides real time information. You can't use Resource Monitor to perform a traffic capture and review activity that occurred in the past. You can use Resource Monitor to view activity that is currently occurring. The Network tab of Resource Monitor is shown in Figure 10-18.

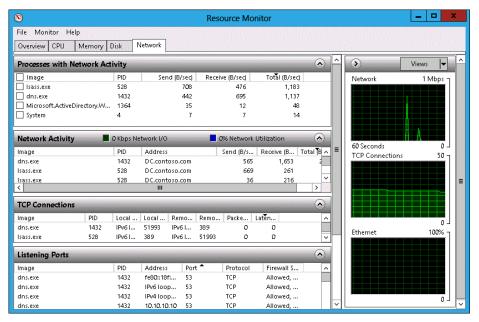


FIGURE 10-18 Resource Monitor Network tab

Resource Monitor provides the following information that is relevant to network monitoring:

- Processes With Network Activity This view lists processes by name and ID; and provides information on bits sent per second, bits received per second, and total bits per second.
- **Network Activity** Lists network activity on a per-process basis, but also lists the destination address, sent bits per second, received bits per second, and total bits per second.
- **TCP Connections** Provides information on connections on the basis of local address, port, and remote address and port.
- Listening Ports Lists the ports and addresses that services and applications are listening on. Also provides information about the firewall status for these roles and services.

Message Analyzer

Microsoft Message Analyzer is the successor to Network Monitor. You can use Message Analyzer to perform network traffic capture and analysis. Message Analyzer also functions as a replacement for LogParser, which enables you to manage system messages, events, and log files. When performing a capture, you select the scenario that best represents the type of event about which you are interested in capturing traffic. For example, the LAN scenario, shown in Figure 10-19, enables you to capture traffic on local area network (LAN) interfaces.

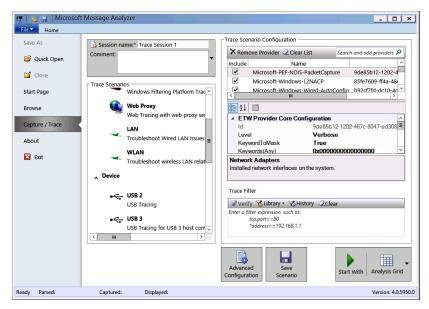


FIGURE 10-19 LAN scenario

When performing certain types of network traffic capture, you need to run Message Analyzer using an account that is a member of the local Administrators group. After the capture has been performed, you can analyze the content of each message, as shown in Figure 10-20. By applying appropriate filters, you can locate network traffic that has specific characteristics, such as using a particular TCP port, source, or destination address.

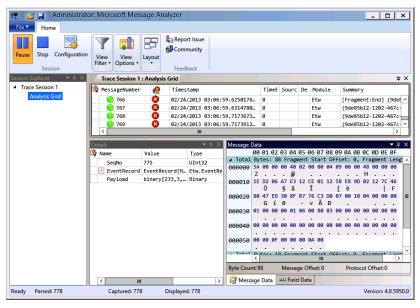


FIGURE 10-20 Message Analyzer

NOTE MESSAGE ANALYZER

At the time of writing, Message Analyzer is still beta software. There is a blog on Tech-Net that describes the features and functionality of the new product: http://blogs.technet .com/b/messageanalyzer/archive/2012/09/17/meet-the-successor-to-microsoft-networkmonitor.aspx.

Lesson summary

- Data collector sets enable you to collect performance counter data, event trace data, and system configuration information.
- Performance counter alerts enable an event to be written to the event log and a command to be run when a specified performance counter exceeds or falls below a configured value.
- Event log filters apply to a single event log and are not persistent.
- Event log views are persistent, can include items from multiple event logs, and can be imported and exported.
- Event subscriptions enable you to configure one computer to consolidate the event logs of multiple computers.
- Event-driven tasks enable you to configure a program or script to be run when a specific event is written to the event log.
- Message Analyzer, which is the successor to Network Monitor, enables you to capture and analyze network traffic.

Lesson review

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

- 1. You want to collect processor, memory, and network interface utilization data over the course of several hours. You need to be able to review the data at a later period in time. Which of the following tools should you use to accomplish this goal?
 - A. Resource Monitor
 - B. Task Manager
 - c. Data collector set
 - D. Message Analyzer

- 2. A particular network service on a computer running Windows Server 2012 that you are responsible for managing is not functioning correctly. You suspect that the service is listening on a TCP port that Windows Firewall is configured to block, but you don't know which TCP port the service uses. Which of the following tools should you use to determine this information?
 - A. Task Manager
 - Resource Monitor
 - C. Message Analyzer
 - **D.** Data collector set
- Which of the following tools can you use to capture and analyze network traffic?
 - A. Data collector set
 - Message Analyzer
 - C. Resource Monitor
 - D. Task Manager
- 4. You are configuring event log subscriptions. Computer SYD-A will function as the event log collector, and computers MEL-A, MEL-B, and MEL-C will function as the event log sources. You want SYD-A to collect events from the security logs on computers MEL-A, MEL-B, and MEL-C. To which of the following security groups on MEL-A, MEL-B, and MEL-C should you add the computer account of SYD-A?
 - A. Backup operators
 - **B.** Power users
 - **c.** Event log readers
 - D. Administrators

Lesson 2: Advanced audit policies

Auditing enables you to track both actual and attempted access and changes to objects and policies. Auditing enables you to verify that the policies that you've put in place to secure your organization's network infrastructure are actually being enforced, from tracking modifications to sensitive user accounts through to access to sensitive files and folders. In this lesson, you will learn about advanced audit policy, how to configure expression-based audit policies, and how you can use auditpol.exe to manage auditing.

After this lesson, you will be able to:

- Understand advanced audit policies.
- Configure auditing using Group Policy.
- Use auditpol.exe to manage auditing.

Estimated lesson time: 45 minutes

Advanced auditing



There are two sets of audit policies in a Group Policy Object (GPO): traditional audit policies and advanced audit policies. The traditional audit policies are located in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policies node and are shown in Figure 10-21. They are the audit policies that have been available with the Windows Server operating system since Windows 2000. The drawback of these policies is that they are general, and you can't be specific in the way you configure auditing. When you use these policies, you'll not only audit the events that you're interested in but you'll also end up auditing many events that you don't need to know about.

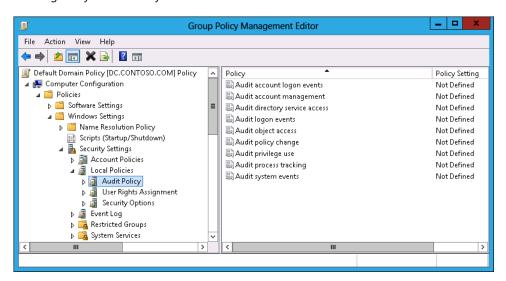


FIGURE 10-21 General auditing policies

REAL WORLD NEEDLES AND HAYSTACKS

The trick of implementing a successful audit policy is to reduce the size of the haystack so that finding the needles is easier. An audit policy that records only activity that you are interested in produces fewer events than a more general audit policy, in which interesting events can get lost in the clutter.

The advanced audit policies enable you to be more specific in the types of activity you audit. The advanced audit policies are located under the Computer Configuration\Policies\ Windows Settings\Security Settings\Advanced Audit Policy Configuration node, as shown in Figure 10-22.

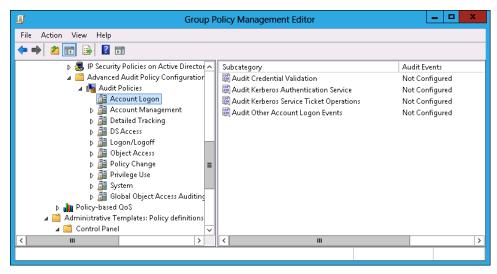


FIGURE 10-22 Advanced audit policies

There are 10 groups of audit policy settings and 58 individual audit policies available through Advanced Audit Policy Configuration. The audit policy groups contain the following settings:

- Account Logon You can audit credential validation and Kerberos-specific operations.
- Account Management You can audit account management operations, such as changes to computer accounts, user accounts, and group accounts.
- Detailed Tracking You can audit encryption events, process creation, process termination, and RPC events.
- **DS Access** You can audit Active Directory access and functionality.
- Logon/Logoff You can audit logon, logoff, and other account activity events, including IPsec and Network Policy Server (NPS) events.
- Object Access You can audit access to objects including files, folders, applications, and the registry.
- **Policy Change** You can audit changes to audit policy.
- Privilege Use You can audit the use of privileges.
- **System** You can audit changes to the security subsystem.
- Global Object Access Auditing You can configure expression-based audit policies for files and the registry.

REAL WORLD CONFIGURE AN AUDIT POLICY

Determine what you want to audit first and then enable the policies to audit that type of activity. A mistake that many administrators make is that they aren't entirely sure what they should be auditing, so they audit everything. They become frustrated with the process because the auditing events that they might be interested get lost in the vast sea of auditing events that they are not interested in.

Expression-based audit policies

Traditional object audit policies involve specifying a group and configuring the type of activities that will trigger an event to be written to the security log. Specifying that an audit event will be written each time a member of the Managers group accesses a file in a specific folder is a good example.



Expression-based audit policies enable you to go further. These policies enable you to put conditions as to when auditing might occur. For example, you might want to configure auditing so that members of the Managers group have access to sensitive files tracked only when they access files from computers that aren't part of the Managers_Computers group. Figure 10-23 shows auditing configured in this way. This way, you don't bother tracking access when members of this group access sensitive files from within the office, but you do track all access to those sensitive files when members of this group are accessing them from an unusual location.

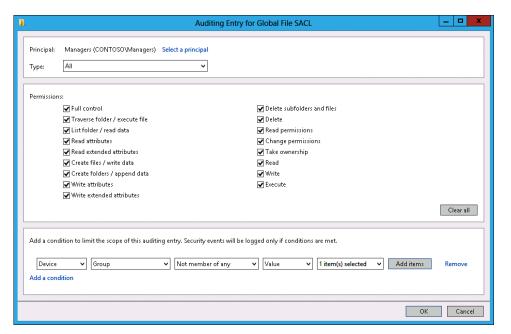


FIGURE 10-23 Expression-based audit policies

You can integrate expression-based audit policies with Dynamic Access Control (DAC) to create targeted audit policies that are based on user, computer, and resource claims. Instead of just adding claims based on user or device group membership, the claim can be based on document metadata such as confidentiality settings and site location. You can configure expression-based audit policies at the file or folder level, or apply them through Group Policy using policies in the Global Object Access Auditing node of Advanced Audit Policy Configuration.



Quick check

 What type of auditing should you configure if you want to audit file access by a specific group of people only when they aren't signed on to a specific group of computers?

Quick check answer

■ You configure an expression-based audit policy to audit file access by a specific group of people who are accessing files from computers other than those in a specific group.

Configuring file and folder auditing

After you configure auditing of object access, either through the traditional or advanced audit policies, you can configure auditing at the file and folder level. The simplest way to configure auditing is at the folder level because you can then configure all folders and subfolders to inherit those auditing settings. If you change the auditing settings at the folder level, you can use the Replace All Child Object Auditing Entries option to apply the new auditing settings to the folder's child files and folders.

You can configure auditing for a specific file and folder through the Advanced button on the Security tab of the object's properties. You can configure basic success and failure auditing, as shown in Figure 10-24. You can also configure expression-based auditing so that activity by members of a specific security group are audited only if other conditions, such as membership of other security groups, are also met.

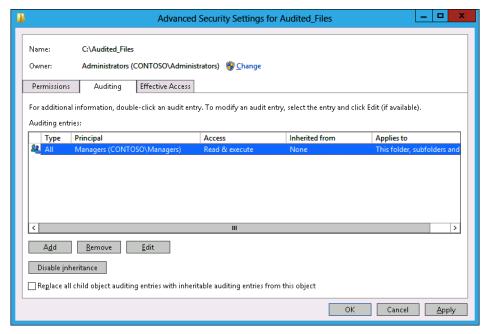


FIGURE 10-24 Configuring basic success and failure auditing

The advantage of using Global Object Access Auditing is that when you have it configured, you can use file classification to apply metadata to files and then automatically have auditing enabled for those files. For example, using file classification and DAC, you can configure a Windows Server 2012 file server so that all files that contain the phrase "code secret" are marked as Sensitive. You can then configure Global Object Access Auditing so that all access to files marked as Sensitive are automatically audited. Instead of having an administrator track down all the files that are sensitive and configuring auditing on those files, the process is automatic. All that needs to happen to trigger it is the inclusion of the phrase "code secret" in the file.

Using auditpol with auditing



Auditpol.exe is a command-line utility that you can use to configure and manage audit policy settings from an elevated command prompt. You can use auditpol.exe to perform the following tasks:

- View the current audit policy settings with the /get subcommand
- Set audit policy settings with the /set subcommand
- Display selectable policy elements with the /list subcommand

- Back up and restore audit policies using the /backup and /restore subcommands
- Delete all per-user audit policy settings and reset the system policy settings using the /clear subcommand
- Remove all per-user audit policy settings and disable all system policy settings using the /remove subcommand

For example, to enable success and failure auditing for the File System subcategory of Object Access, execute this command:

Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable

To view the current audit policy settings for all audit policies, issue this command:

Auditpol.exe /get /category:*

To view the current audit policy settings for a specific category, such as Object Access, issue this command:

Auditpol.exe /get /category: "Object Access"

MORE INFO AUDITPOL.EXE

To learn more about auditpol.exe, consult the following TechNet article at: http://technet .microsoft.com/en-us/library/cc731451(v=ws.10).aspx.

Lesson summary

- Advanced audit policies enable you to perform more granular auditing than is possible with the traditional auditing policies available in earlier versions of Windows server.
- Expression-based audit policies enable you to configure auditing based on object metadata. You can also use expression-based audit policies to perform conditional auditing.
- After you have enabled the auditing of object access, you can configure auditing at the file and folder level. File- and folder-level auditing supports expression-based audit policies.
- You can use the auditpol.exe command-line utility from an elevated command prompt to configure and manage audit policy settings.

Lesson review

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

- 1. Which of the following commands should you use to enable success and failure auditing for all audit policies under the Object Access category on a computer running Windows Server 2012?
 - **A.** Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.
 - Auditpol.exe /set /Category: "Object Access" /success: Enable /Failure: Enable
 - Auditpol.exe /get /Category: "Object Access" /success:Disable /Failure:Disable.
 - Auditpol.exe /get /Category: "Object Access" /success:Disable /Failure:Enable.
- You want to enable failure auditing, but not success auditing, for all audit policies under the Object Access category on a computer running Windows Server 2012. Which of the following commands should you use to accomplish this goal?
 - **A.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable.
 - Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable.
 - **C.** Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable.
 - **D.** Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.
- You want to enable success and failure auditing only for the File System subcategory. Which of the following commands should you use to accomplish this goal?
 - **A.** Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable.
 - Auditpol.exe /get /Category: "Object Access" /success:Disable /Failure:Enable.
 - Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.
 - Auditpol.exe /get /Category: "Object Access" /success: Disable /Failure: Disable.
- 4. You want to disable all success and failure auditing on all auditing subcategories under the Object Access category. Which of the following commands should you use to accomplish this goal?
 - A. Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable.
 - Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable.
 - Auditpol.exe /set /Category: "Object Access" /success: Enable /Failure: Enable.
 - Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.

Practice exercises

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

- Configure data collector sets
- Configure alerts
- Manage event subscriptions
- Perform network monitoring
- Configure removable device auditing
- Configure logon auditing
- Configure expression-based audit policies
- Enable folder auditing

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, SYD-A, and SYD-B, the setup instructions for which are as described in the Appendix. 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 Configure data collector sets

In this exercise, you will configure data collector sets. To complete this exercise, perform the following steps:

- 1. On DC, click Performance Monitor in the Tools menu of Server Manager.
- 2. In the Performance Monitor console, expand the Performance\Data Collector Sets\User Defined, as shown in Figure 10-25.

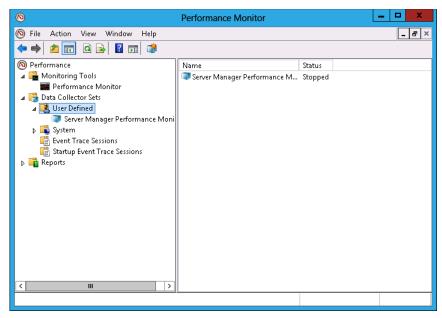


FIGURE 10-25 Accessing data collector sets

- 3. On the Action menu, click New and click Data Collector Set.
- 4. In the Create New Data Collector Set dialog box, enter the name DC-Performance-Measurement and click Create Manually (Advanced), as shown in Figure 10-26. Click Next.

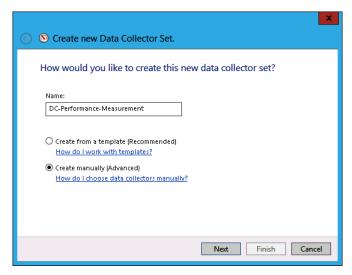


FIGURE 10-26 Entering the data collector set name

5. On the What Type Of Date Do You Want To Include? page, click Performance Counter, as shown in Figure 10-27, and click Finish.

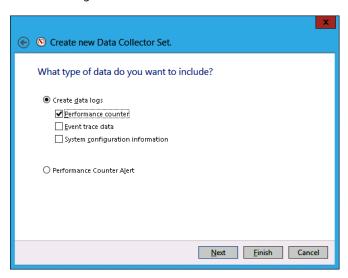


FIGURE 10-27 Selecting Performance Counter

- In the Performance Monitor console, click DC-Performance-Measurement.
- **7.** In the details pane, click DataCollector01.
- On the Action menu, click Properties.
- In the DataCollector01 Properties dialog box, shown in Figure 10-28, click Add.

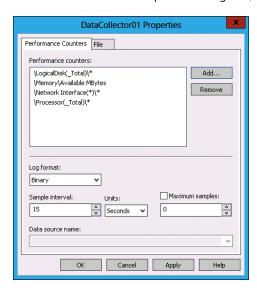


FIGURE 10-28 Performance counters

- 10. In the Available Counters dialog box, click Logical Disk and click Add.
- 11. Click Memory, click the arrow, click Available Mbytes, and click Add.
- 12. Click Network Interface and click Add.
- 13. Click Processor and click Add.
- **14.** Verify that the list of added counters matches Figure 10-29 and click OK.

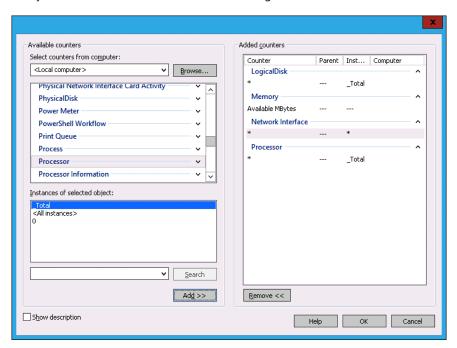


FIGURE 10-29 Matching added counters

15. In the DataCollector01 Properties dialog box, set the Sample Interval to 15 seconds (see Figure 10-30) and click OK.

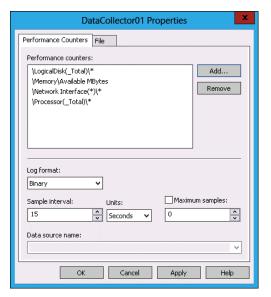


FIGURE 10-30 Setting the interval

EXERCISE 2 Collect data

In this exercise, you will collect data from the data collector set. To complete this exercise, perform the following steps:

- In Performance Monitor, click Data Collector Sets\User Defined\DC-Performance-Measurement.
- 2. On the Action menu, click Start.
- **3.** After 2 minutes, on the Action menu, click Stop.
- **4.** Expand Reports, expand User Defined, and click DC-Performance-Measurement.
- **5.** Click the report listed in the details pane, as shown in Figure 10-31.

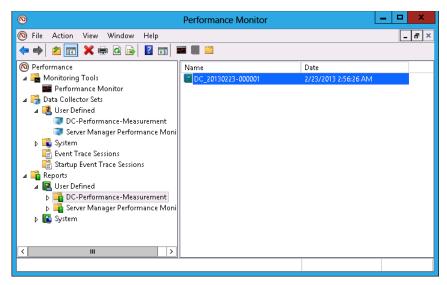


FIGURE 10-31 Selecting a report

- Click View Data In Performance Monitor.
- 7. Click Change Graph Type and click Report.
- 8. View the report, as shown in Figure 10-32.

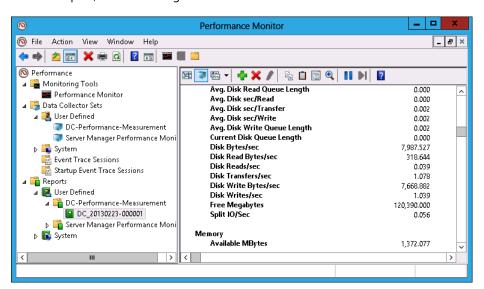


FIGURE 10-32 Viewing the report

EXERCISE 3 Configure alerts

In this exercise, you will configure a free disk space alert. To complete this exercise, perform the following steps:

- 1. In Performance Monitor, click User Defined under Data Collector Sets.
- 2. On the Action menu, click New and click Data Collector Set.
- 3. On the Create New Data Collector Set page, type **Disk Space Alert**, click Create Manually (Advanced), and click Next.
- 4. On the Create New Data Collector Set page, click Performance Counter Alert, as shown in Figure 10-33, and click Next.

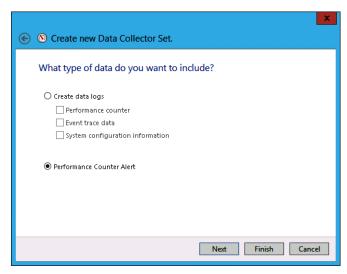


FIGURE 10-33 Choosing Performance Counter Alert

- 5. On the Which Performance Counters Would You Like To Monitor? page, click Add.
- 6. In the Available Counters dialog box, click LogicalDisk, click %Free Space, click C:, and click Add, as shown in Figure 10-34. Click OK.

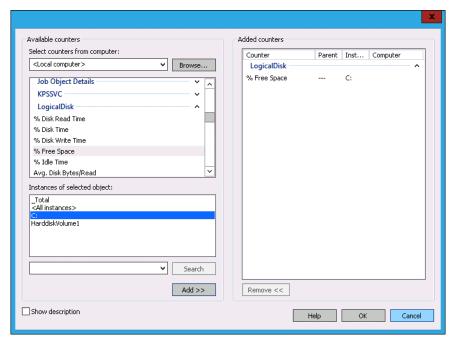


FIGURE 10-34 Selecting LogicalDisk

- 7. Set the Alert When drop-down menu to Below.
- **8.** Set the Limit value to 5, as shown in Figure 10-35, and click Next.

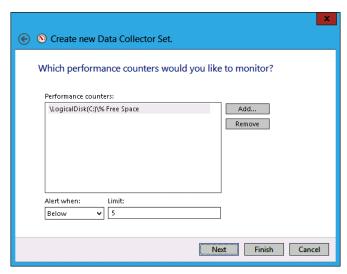


FIGURE 10-35 Setting the limit value

Click Finish.

EXERCISE 4 Prepare computers for event subscriptions

In this exercise, you will configure computers to support event log subscriptions. To complete this exercise, perform the following steps:

- 1. On DC, click Windows PowerShell on the task bar.
- Enter the following command and press Enter:

Wecutil qc

- When prompted, press Y and press Enter.
- Close the Windows PowerShell prompt.
- Sign on to SYD-A as Contoso\Administrator.
- In the Tools menu on Server Manager, click Computer Management.
- In the Computer Management console, expand Local Users And Groups, click Groups, and then click Administrators, as shown in Figure 10-36.

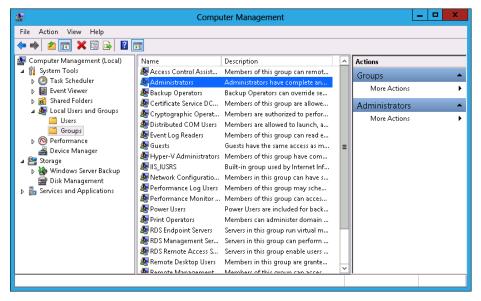


FIGURE 10-36 Accessing Administrators

- On the Actions pane, click More Actions and click Properties under Administrator.
- In the Administrators Properties dialog box, click Add.
- 10. In the Select Users, Computers, Service Accounts, Or Groups dialog box, click Object Types.

11. In the Object Types dialog box, enable the Computers check box, as shown in Figure 10-37, and click OK.

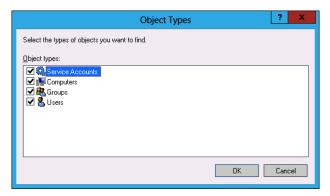


FIGURE 10-37 Selecting Computers

- **12.** In the Select Users, Computers, Service Accounts, Or Groups dialog box, type **DC**, click Check Names, and click OK.
- **13.** Verify that the Administrators Properties dialog box matches Figure 10-38 and click OK.

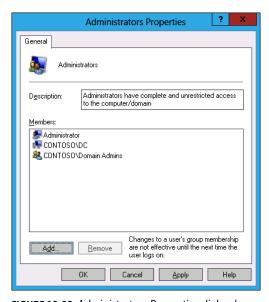


FIGURE 10-38 Administrators Properties dialog box

14. Restart SYD-A.

EXERCISE 5 Configure event subscriptions

In this exercise, you will configure event subscriptions. To complete this exercise, perform the following steps:

- 1. In the Server Manager console on DC, open the Tools menu and click Event Viewer.
- In Event Viewer, click the Subscriptions node, as shown in Figure 10-39.

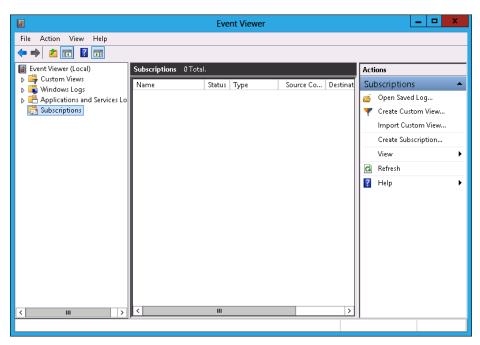


FIGURE 10-39 Clicking the Subscriptions node

- **3.** On the Actions pane, click Create Subscription.
- In the Subscription Properties dialog box, enter the name as **Subscription-Alpha**, click Collector Initiated, and click Select Computers.
- 5. In the Computers dialog box, click Add Domain Computers.
- In the Select Computer dialog box, type SYD-A, click Check Names, and click OK.
- **7.** Verify that the Computers dialog box matches Figure 10-40 and click Test.

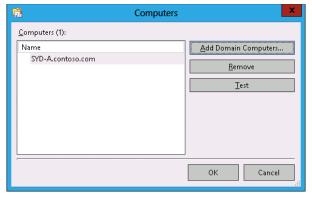


FIGURE 10-40 Computers dialog box

- 8. In the Event Viewer dialog box, click OK.
- **9.** In the Computers dialog box, click OK.
- 10. Click Select Events.
- **11.** In the Query Filter dialog box, select Critical, Error, Warning, and Information.
- 12. Click the Event Logs drop-down menu and click Windows Logs.
- **13.** Verify that the Query Filter appears the same as Figure 10-41 and click OK.

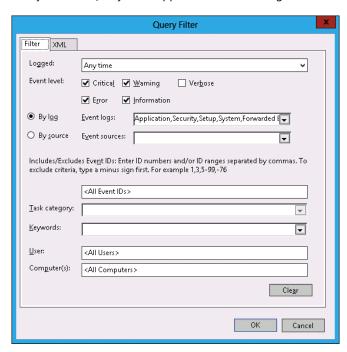


FIGURE 10-41 The Query Filter dialog box

- **14.** In the Subscription Properties dialog box, click Advanced.
- 15. In the Advanced Subscription Settings dialog box, click Minimize Latency, as shown in Figure 10-42, and click OK.

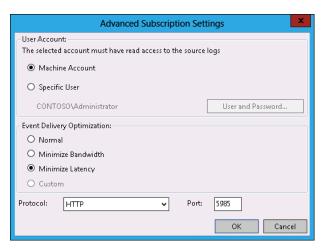


FIGURE 10-42 Advanced Subscription Settings dialog box

16. Verify that the Subscription Properties – Subscription-Alpha dialog box matches Figure 10-43 and then click OK.

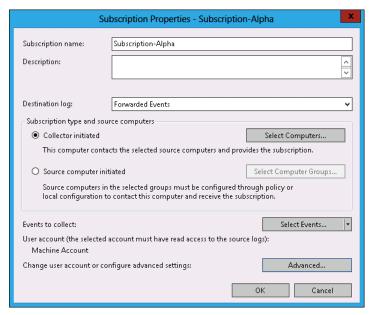


FIGURE 10-43 Subscription Properties dialog box

- 17. Restart server SYD-A.
- 18. Expand the Windows Logs node and click Forwarded Events.
- **19.** Verify the presence of items in the event log, as shown in Figure 10-44.

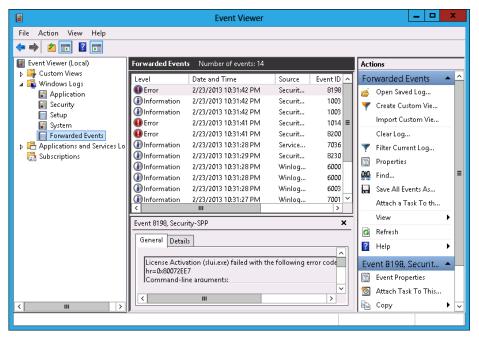


FIGURE 10-44 Event log

20. Close Event Viewer.

EXERCISE 6 Configure network monitoring

In this exercise, you will monitor the processes and services that use network interfaces. To complete this exercise, perform the following steps:

- 1. On the Tools menu of the Server Manager console on DC, click Resource Monitor.
- 2. On the Network tab, click the arrow next to TCP Connections, as shown in Figure 10-45.

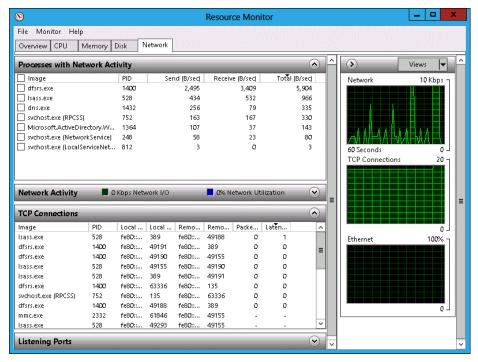


FIGURE 10-45 Network tab of the Resource Monitor

Click the arrow next to Listening Ports to list the ports on which different services are listening (see Figure 10-46).

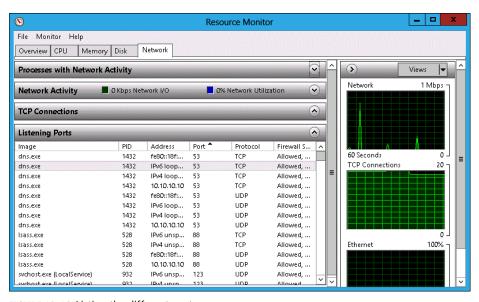


FIGURE 10-46 Listing the different ports.

EXERCISE 7 Using Message Analyzer

In this exercise, you use Message Analyzer to perform network monitoring. This exercise requires that you have downloaded Message Analyzer from the Microsoft website and installed it on SYD-A, but have not run the program yet. To complete this exercise, perform the following steps:

- 1. In Server Manager on SYD-A, click Local Server and then select IE Enhanced Security Configuration.
- 2. In the Internet Explorer Enhanced Security Configuration dialog box, set the Administrators setting to Off, as shown in Figure 10-47, and click OK.



FIGURE 10-47 Internet Explorer security

- 3. In the Search charm on SYD-A, type Microsoft Message Analyzer.
- Click Microsoft Message Analyzer in the results list.
- 5. On the File menu, click SMB Server Full PDU on the Capture/Trace option, as shown in Figure 10-48, and click Start With.

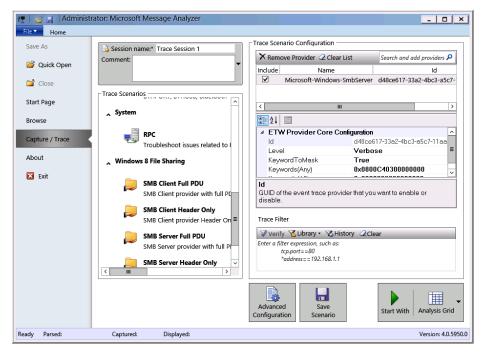


FIGURE 10-48 SMB Server Full PDU

- On the taskbar, click File Explorer.
- **7.** In File Explorer, click Computer and then double-click Local Disk (C:).
- On the title bar, click New Folder. Name the new folder **TEST**.
- Right-click the TEST folder, click Share With, and click Specific People.
- **10.** In the File Sharing dialog box, click Share and then click Done.
- 11. In Microsoft Message Analyzer, verify that messages have been recorded and click the final message, as shown in Figure 10-49.

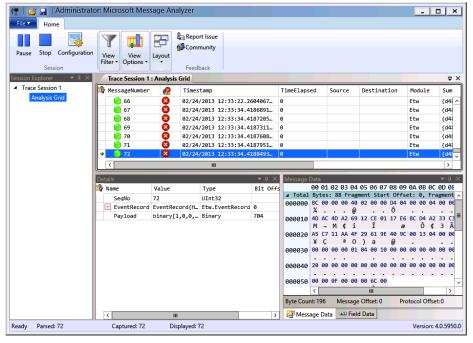


FIGURE 10-49 Verifying that messages have been recorded

- 12. Use File Explorer to navigate to C:\TEST.
- Create a text file in C:\TEST named secretfile.txt. The content of the file should be the words "secret secret".
- 14. Switch to DC.
- **15.** On DC, in the Search charm, type **\\SYD-A\TEST\secretfile.txt** and click secretfile. txt in the Results pane.
- **16.** Switch to SYD-A.
- 17. Verify that additional traffic has been recorded.
- **18.** Examine the message data for network addresses, such as server SYD-A.contoso.com (see Figure 10-50).

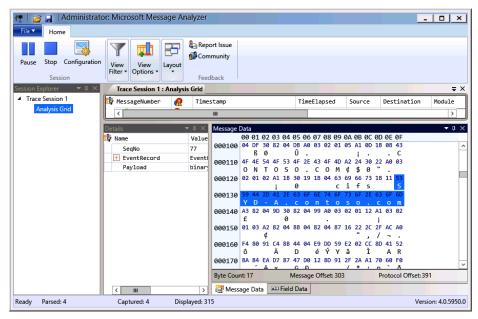


FIGURE 10-50 Examining message data

- 19. Close Microsoft Message Analyzer.
- **20.** When prompted to save the captured trace, click No.

EXERCISE 8 Configure removable device auditing

In this exercise, you will configure a GPO so that removable device usage is audited. To complete this exercise, perform the following steps:

- On DC, click Group Policy Management in the Tools menu of Server Manager.
- **Expand Forest:** contoso.com\Domains\contoso.com\Group Policy Objects and click Default Domain Policy, as shown in Figure 10-51.

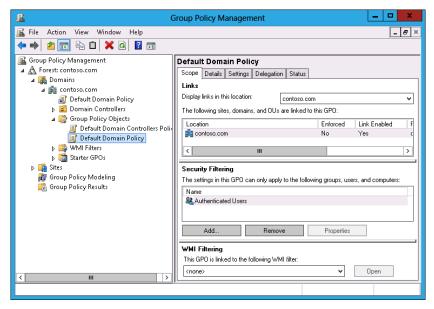


FIGURE 10-51 Clicking Default Domain Policy

- 3. On the Action menu, click Edit.
- **4.** In the GPME, navigate to the Computer Configuration\Policies\Windows Settings\ Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access node and click Audit Removable Storage, as shown in Figure 10-52.

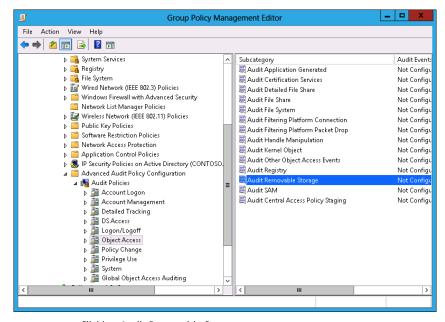


FIGURE 10-52 Clicking Audit Removable Storage

- 5. Double-click Audit Removable Storage.
- 6. In the Audit Removable Storage Properties dialog box, select Configure The Following Audit Events, Success, and Failure; then click OK (see Figure 10-53).

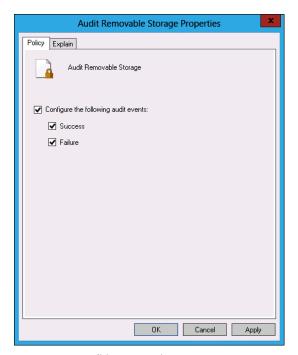


FIGURE 10-53 Auditing properties

- Close the GPME.
- 8. On the taskbar, click Windows PowerShell.
- **9.** In the Windows PowerShell window, type the following command and press Enter: Gpupdate /force
- **10.** In the Windows PowerShell window, type the following command and press Enter: Auditpol /get /category:"Object Access"
- 11. Verify that Removable Storage is configured for Success And Failure auditing, as shown in Figure 10-54.

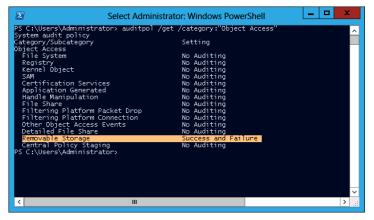


FIGURE 10-54 Configuring Removable Storage

EXERCISE 9 Configure logon auditing

In this exercise, you will configure logon auditing. To complete this exercise, perform the following steps:

- 1. In the Group Policy Management Console (GPMC) on DC, right-click the Default Domain Policy and click Edit.
- 2. In the GPME, navigate to the Computer Configuration\Policies\Windows Settings\
 Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff and click Audit Logon, as shown in Figure 10-55.

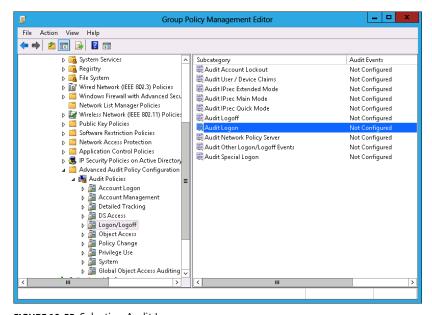


FIGURE 10-55 Selecting Audit Logon

- 3. On the Action menu, click Properties.
- 4. In the Audit Logon Properties dialog box, select Configure The Following Audit Events, Success, and Failure (see Figure 10-56). Click OK.



FIGURE 10-56 Setting audit properties

- 5. Close the GPME.
- 6. In the Tools menu of the Server Manager console, click Active Directory Users And Computers.
- 7. In Active Directory Users And Computers, select Users and then click Administrator.
- 8. On the Action menu, click Copy.
- 9. In the Copy Object User dialog box, configure the following information, as shown in Figure 10-57, and click Next.
 - First Name: Don
 - Last Name: Funk
 - User Logon Name: Don_Funk

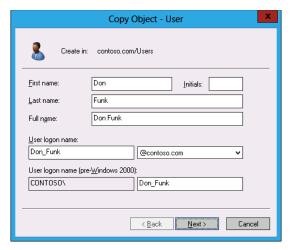


FIGURE 10-57 Setting copy object data

- Enter Pa\$\$w0rd in the Password and Confirm Password text boxes, click Next, and click Finish.
- 11. Close Active Directory Users And Computers.
- **12.** In Windows PowerShell, enter the following command and press Enter: Gpupdate /force
- **13.** In Windows PowerShell, enter the following command and press Enter:

 Auditpol /get /category:"Logon/Logoff"
- **14.** Verify that Logon is configured for Success And Failure auditing, as shown in Figure 10-58.

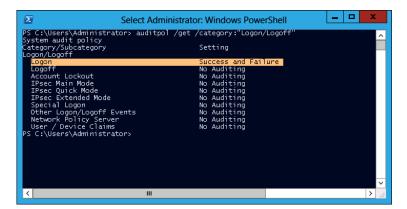


FIGURE 10-58 Logon for Success And Failure auditing

- **15.** Switch to SYD-A.
- **16.** Sign out and sign on as contoso\don_funk with the password **Pa\$\$w0rd**.
- 17. Switch to DC.
- **18.** On the Tools menu of the Server Manager console, click Event Viewer.
- 19. Expand Windows Logs\Security Logs and click the most recent event with Event ID 4624.
- 20. Click the Details pane and verify that the TargetUserName Don_Funk is listed, as shown in Figure 10-59. You may need to scroll through several events to find this TargetUserName.

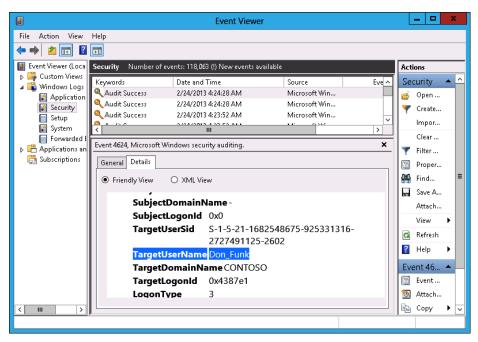


FIGURE 10-59 TargetUserName Don_Funk

EXERCISE 10 Configure expression-based audit policies

In this exercise, you will configure expression-based audit policies in Group Policy. To complete this exercise, perform the following steps:

- On DC, open Active Directory Users And Computers from the Tools menu of the Server Manager console.
- Right-click the Users container, click New, and click Group.
- In the New Object Group dialog box, enter the name **Jupiter**, as shown in Figure 10-60, and click OK.

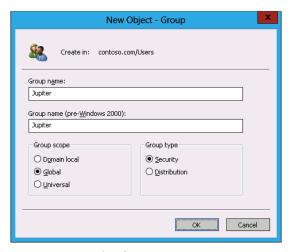


FIGURE 10-60 Entering the group name

- Right-click the Users container, click New, and click Group.
- In the New Object Group dialog box, enter the name **Saturn** and click OK.
- Right-click the Users container, click New, and click Group.
- In the New Object Group dialog box, enter the name **Neptune** and click OK. 7.
- Right-click the Users container, click New, and click Group.
- In the New Object Group dialog box, enter the name **Mars** and click OK.
- **10.** Close Active Directory Users And Computers.
- 11. In the GPMC, right-click Default Domain Policy and click Edit.
- 12. In the GPME, navigate to the Computer Configuration\Policies\Windows Settings\ Security Settings\Advanced Audit Policy Configuration\Audit Policies\Global Object Access Auditing and click File System, as shown in Figure 10-61.

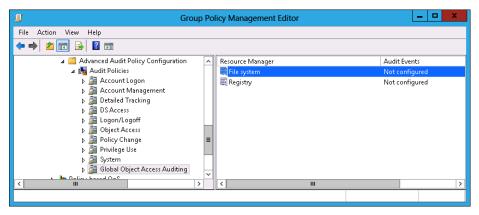


FIGURE 10-61 Selecting File System

- **13.** On the Action menu, click Properties.
- 14. In the File System Properties dialog box, click Define This Policy Setting and click Configure.
- **15.** In the Advanced Security Settings for Global File SACL dialog box, click Add.
- **16.** In the Auditing Entry For Global File SACL dialog box, click Select A Principal Link.
- 17. In the Select User, Computer, Service Account, Or Group dialog box, type Jupiter, click Check Names, and click OK.
- **18.** In the Type drop-down menu, click All.
- 19. Click the Add A Condition link.
- **20.** Click the Add Items button.
- 21. In the Select User, Computer, Service Account, Or Group dialog box, type Saturn, click Check Names, and click OK.
- 22. Verify that the Auditing Entry For Global File SACL dialog box matches Figure 10-62 and click OK.

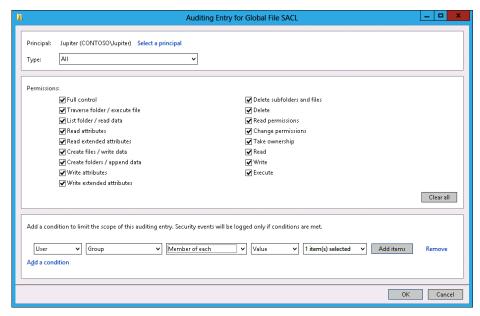


FIGURE 10-62 Auditing the Entry For Global File SACL dialog box

- 23. In the Advanced Security Settings For Global File SACL dialog box, click Add.
- 24. In the Auditing Entry For Global File SACL dialog box, click Select A Principal link.
- 25. In the Select User, Computer, Service Account, Or Group dialog box, type Mars, click Check Names, and click OK.
- **26.** Set the Type drop-down menu to Fail.
- 27. Click the Add A Condition link.
- 28. Click the Member Of Each drop down menu and select Not Member Of Any.
- 29. Click the Add Items button.
- 30. In the Select User, Computer, Service Account, Or Group dialog box, type Neptune, click Check Names, and click OK twice.
- **31.** Verify that the Advanced Security Settings For Global File SACL dialog box matches Figure 10-63 and click OK.

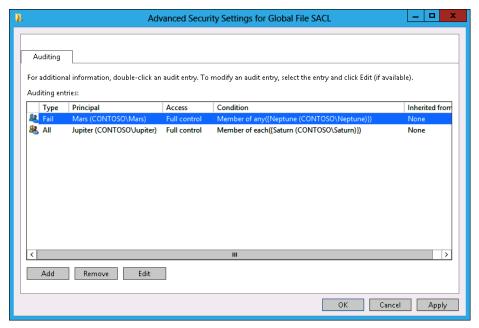


FIGURE 10-63 Advanced Security Settings For Global File SACL dialog box

32. Click OK to close the File System Properties dialog box and close the GPME.

EXERCISE 11 Configure folder auditing

In this exercise, you will configure expression-based audit policies at the folder level. To complete this exercise, perform the following steps:

- Click File Explorer on the taskbar.
- Click Computer and double-click Local Disk (C:).
- On the title bar, click the New Folder icon.
- Name the new folder **Audited_Files**.
- 5. Right-click the Audited_Files folder and click Properties.
- **6.** On the Security tab, click Advanced.
- 7. On the Auditing tab of the Advanced Security Settings For Audited_Files dialog box, shown in Figure 10-64, click Add.

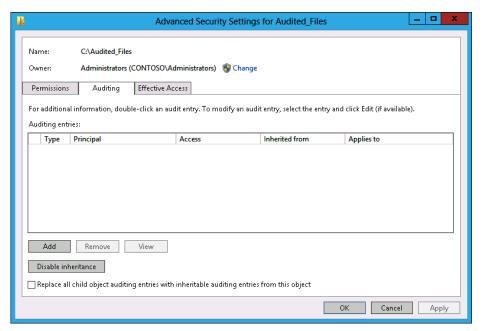


FIGURE 10-64 Auditing tab of the Advanced Security Settings For Audited_Files dialog box

- **8.** In the Auditing Entry For Audited_Files dialog box, click Select A Principal link.
- 9. In the Select User, Computer, Service Account, Or Group dialog box, type Neptune, click Check Names, and click OK.
- **10.** Change the type from Success to Fail.
- 11. Click the Add A Condition link.
- 12. Click the Add Items button.
- 13. In the Select User, Computer, Service Account, Or Group dialog box, type Saturn, click Check Names, and click OK.
- 14. Verify that the Auditing Entry For Audited Files dialog box matches Figure 10-65 and click OK.

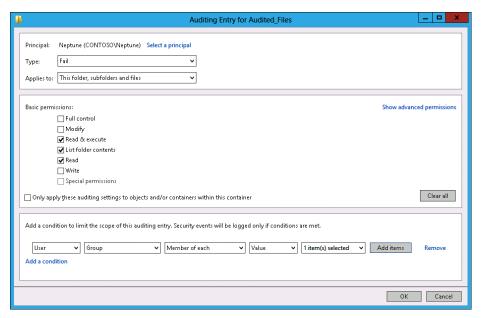


FIGURE 10-65 Auditing Entry For Audited Files dialog box

15. Click OK twice to close all dialog boxes.

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 Use auditpol.exe to enable File System, Registry, and File Share Success And Failure auditing on SYD-A.
- **Exercise 2** Create a test share on DC and populate it with text files. Add user accounts to the Mars, Jupiter, Saturn, and Neptune groups. Sign on to SYD-A and access the files across the network using different accounts. Verify that the expression-based audit policies record auditing information appropriately.

Answers

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

Lesson 1

1. Correct answer: C

- A. Incorrect: Resource Monitor enables you to view point in time resource utilization information. You can't use this tool to record resource utilization information for later review.
- B. Incorrect: Task Manager does enable you to view resource utilization information, but you can't record that data for later review.
- **C.** Correct: A data collector set can be used to capture performance counters and trace information related to resource utilization for later review.
- **D.** Incorrect: Message Analyzer, the successor to Network Monitor, enables you to capture and analyze network traffic. Although it can capture and record network traffic, you can't use this tool to record processor and memory utilization information

2. Correct answer: B

- **A.** Incorrect: Task Manager provides real-time information about network utilization, but doesn't provide information about port utilization and firewall configuration.
- B. Correct: Resource Monitor provides information about services, the ports that they listen on, and firewall configuration.
- **C. Incorrect:** Message Analyzer enables you to capture and analyze network traffic, but it can't be used to determine port utilization and associated firewall configuration.
- **D.** Incorrect: A data collector set can record performance information and system trace information, but it can't be used to determine port utilization and associated firewall configuration.

3. Correct answer: B

- A. Incorrect: A data collector set can be used to capture performance counters and trace information related to network traffic, but it can't be used to capture network traffic.
- B. Correct: Message Analyzer, the successor to Network Monitor, enables you to capture and analyze network traffic.
- **C. Incorrect:** Resource Monitor enables you to view point in time network utilization information. You can't use Resource Monitor to capture and analyze network traffic.
- D. Incorrect: Task Manager does enable you to view network traffic, but doesn't enable you to capture and analyze that traffic.

Correct answer: D

- A. Incorrect: Members of the Backup Operators group are enabled to perform backups; they do not have access to the Security event log.
- **B.** Incorrect: The Power Users group is included for backward compatibility; members of this group do not have access to the Security event log.
- C. Incorrect: Although members of the Event Log Readers group have access to the other event logs, they don't have access to the Security event log. Only members of the local Administrators group have access to the Security event log.
- **D.** Correct: When configuring event log subscriptions involving events in the Security event log, it is necessary to add the account of the collector computer to the local Administrators group on the source computer.

Lesson 2

1. Correct answer: B

- A. Incorrect: This command enables success and failure auditing for the File System subcategory.
- **B.** Correct: This command enables success and failure auditing for all subcategories under the Object Access category.
- C. Incorrect: This command disables success and failure auditing for all subcategories under the Object Access category.
- **D.** Incorrect: This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.

Correct answer: A

- A. Correct: This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.
- **B.** Incorrect: This command disables success and failure auditing for all subcategories under the Object Access category.
- **c. Incorrect:** This command enables success and failure auditing for all subcategories under the Object Access category.
- D. Incorrect: This command enables success and failure auditing for the File System subcategory.

3. Correct answer: C

- **A. Incorrect:** This command enables success and failure auditing for all subcategories under the Object Access category.
- B. Incorrect: This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.
- **C. Correct:** This command enables success and failure auditing for the File System subcategory.
- **D.** Incorrect: This command disables success and failure auditing for all subcategories under the Object Access category.

4. Correct answer: A

- **A. Correct:** This command disables success and failure auditing for all subcategories under the Object Access category.
- **B.** Incorrect: This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.
- **C. Incorrect:** This command enables success and failure auditing for all subcategories under the Object Access category.
- **D. Incorrect:** This command enables success and failure auditing for the File System subcategory.

Index

Symbols	Active Directory
802.1X enforcement, 376–379 .admx files, 290 .msi files, 280 .NET Framework 3.5 server, 8	backup, managing BitLocker recovery keys, 506 domain controller maintenance, 195–201 database optimization, 196–198 metadata cleanup, 198–199 snapshots, 199–201
.zap files, 280–281	domain controller management, 177–194 cloning, 193 Global Catalog servers, 183–184 operations masters, 178–184
A	RODC (read-only domain controller), 185–193 UGMC (Universal group membership cach-
AAAA records, 144	ing), 184–185 domain controllers, 450
Access Client IPv4 Address condition, 347, 364	
Access Client IPv6 Address condition, 347, 364	integrated zones, 120–123 recovery, 203–211
accidental deletion (objects), 207–208	authoritative/non-authoritative restore, 208–211
Accounting Configuration Wizard, 426	backup, 206–208
accounting (RADIUS), 424–427, 471–473	Recycle Bin, 203–205, 229–231
account lockout policies	Rights Management Services, 510
Account Lockout Duration, 66	security groups, 453
Account Lockout Threshold, 67	Active Directory Administrative Center Global Search
Account Logon setting (advanced audit policies), 587	option, 70–71
Account Management setting (advanced audit poli-	Active Directory Certificate Services (AD CS), 375, 446
cies), 587	Active Directory Domain Services (AD DS), 62
account requests, logging, 427	Active Directory Zone Replication Scope page, 131
accounts, 62	AD CS (Active Directory Certificate Services), 375, 446
configuring user accounts, 309–310	Add-ADDSReadOnlyDomainControllerAccount
domain, password policies, 62–66	cmdlet, 188
group Managed Service Accounts, 83–90	Add-ADServiceAccount cmdlet, 85
creating, 85–86	Add Certification Authority task, 391
Kerberos delegation, 88 Kerberos policies, 89–90	Add-DnsServerConditionalForwarderZone PowerShell
practice exercises, 110–111	cmdlet, 131
requirements, 85	Add-DNSServerDirectoryPartition cmdlet, 122
service principal name (SPN) management, 91	Add-DnsServerForwarder cmdlet, 129
virtual accounts, 87	Add-DnsServerPrimaryZone cmdlet, 123
Local System, 286	Add-DnsServerResourceRecordAAAA cmdlet, 144
Action option, configuring, 301	Add-DnsServerResourceRecordA cmdlet, 144
Action page (Create Basic Task Wizard), 579	Add-DnsServerResourceRecordCName cmdlet, 144

Add-DnsServerResourceRecordMX PowerShell cmdlet

Add-DnsServerResourceRecordMX PowerShell	logon auditing, 614–619
cmdlet, 145	removable device auditing, 611-615
Add-DnsServerResourceRecordPtr cmdlet, 146	Advanced Audit Policy Configuration, 587
Add-DnsServerStubZone cmdlet, 132	advanced DNS options, 143–151
Add-DnsServerZoneDelegation cmdlet, 127	aging and scavenging, 147–149
/Add-Driver switch (DISM), 6	DNSSEC, 149–152
/Apply-Image switch (DISM), 10	resource records, 144–147
Add Image Wizard, 19	Advanced Features view option, 84
Add-KDSRootKey cmdlet, 85	Advanced option, configuring Folder Redirection
/Add-Package switch (DISM), 7	policy, 278
Add RADIUS Server dialog box, 419	Advanced Password Replication Policy dialog box, 190
Add/Remove Templates dialog box, 293	Advanced tab
address allocation, NAT servers, 443	configuring WDS, 24
Add Roles And Features Wizard, 17, 135, 186, 206, 341	New RADIUS Client dialog box, 423–424
Add Roles And Features Wizard dialog box, 342	aging (DNS zones), 147–149
Add Rule dialog box, 38–39	alerts (monitor servers), 569–570
AD DS (Active Directory Domain Services), 62	alias records, 144
ADM files, 290	Allow Clients To Connect Without Negotiating An
ADM format, importing an administrative	Authentication Method, 351
template, 294	Allowed EAP Types condition, 364
administration	
	Allowed RODC Password Replication Group, 189 Allow permissions, 251
Active Directory domain controller maintenance, 195–201	answer files
domain controller management, 177–194	
recovery, 203–211	automating operating system deployment, 12–13
network policies	configuring, 13–14
NAP enforcement methods, 370–385	application management, Group Policy, 248–256
NAP infrastructure, 386–393	enforcement/blocking, 249–252
NPS policies, 339–367	loopback processing, 253–256
remote access	processing precedence, 248–249
configuring DirectAccess, 445–465	WMI filtering, 252–253
configuring network routing, 439–441 configuring RADIUS, 413–428	application servers, configuring DirectAccess, 464–465
configuring VPN settings, 432–440	applications, MSI (Microsoft Windows Installer) format
deploying Routing and Remote Access, 430–432	assigning an application, 281
NAT (Network Address Translation), 441–442	deployment recommendations, 283
administrative templates	.msi files, 280
Group Policy, 290–297	publishing applications, 282
ADMX Mitigator, 294	upgrading applications, 284
central store, 292–293	.zap files, 280–281
settings, 291	Applications option, configuring Windows settings, 311
importing, 293	Apply Group Policy (Deny) advanced permission, 251–
practice exercises, 324–325	252
.admx files, 290	app packages, adding to Windows images, 8–9
ADMX Mitigator, 294	Approved for Install setting (Approve Updates dialog
advanced auditing policies, 585–591	box), 37
auditpol utility, 590–591	Approved for Removal setting (Approve Updates dialog
configuring file and folder auditing, 589–590,	box), 37
621–623	Approve The Update For A Specific Computer Group
expression-based, 588-589, 617-621	option (Add Rule dialog box), 39

App-V, 282 A records, 144 Assign A Static IPv4 Address (IP setting), 362 assigning applications, 281 audit policies, 585–591 advanced auditing, 586–589 auditipol utility, 590–591 advanced auditing, 586–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Object dialog box, 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Balanced password policies, 65–66 Adapter) topology, 448 Behind An Edge Device (With Two Network Adapters) topology, 448 BitLocker, 502–507 configuring policies, 555–557 Group Policy, 505 Network Unlock, 508–510 requirements, 503–505 BitLocker Provisioning option, 503 BitLocker Provisioni	Approve Updates dialog box, 37	Behind An Edge Device (With A Single Network
Assign A Static IPv4 Address (IP setting), 362 assigning applications, 281 audit policies, 585–591 advanced auditing, 586–589 auditpol utility, 590–591 advanced auditing, 586–589 auditpol utility, 590–591 aconfiguring file and folder auditing, 589–590, 621–623 expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 auditpol utility, 590–591 auditentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring ganswer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B B B B B B B B Backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Object s), 239–240 Eack Up Group Policy Object dialog box, 239–240 Eack Up Group Policy Object dialog box, 239–240 Eack Up Group Policy Object dialog box, 239–240 (CAP), 437 Toonfiguring policies, 555–557 Group Policy, 505 Network Unlock, 508–510 recofiguring policies, 292–507 Server Group Policy, 505 Network Unlock, 508–510 requirements, 503–505 BitLocker, 702–507 Server Worl Unlock, 508–510 requirements, 503–505 BitLocker, 702–507 Server Worl Unlock, 508–510 requirements, 503–505 BitLocker, 702–507 Server Worl Unlock, 508–510 requirements, 503–505 BitLocker, 702–505 BitLocker, 502–507 Server Worl Unlock, 508–510 requirements, 503–505 BitLocker, 508–510 requirements, 503–505 BitLocker, 502–507 Server Worl Unlock, 508–510 requirements, 503–505 BitLocker, 508–510 requirements, 503–50 BitLocker, 502–507 Server Group Solicy, 505 BitLocker, 502–509 BitLocker, 506–507 BitLocker, 506–510 Rework Unlock, 508–510 requirements, 503–50 BitLocker, 502–505 BitLocker, 506–510 Revorsion Unlock, 508–510 Revorsion Unlock, 508–510	App-V, 282	Adapter) topology, 448
assigning applications, 281 audit policies, 585–591 advanced auditing, 586–589 auditpol utility, 590–591 configuring file and folder auditing, 589–590, 621–623 expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B B B B B B B B B B B	A records, 144	Behind An Edge Device (With Two Network Adapters)
audit policies, 585–591 advanced auditing, 586–589 auditpol utility, 590–591 configuring file and folder auditing, 589–590, 621–623 expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication Type condition, 364 authoritative restore, 208–210 Auto-Cats, configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 BB B backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Objects), 239–240 Backup-GPO cmulet, 238 Back Up Group Policy Objects), 239–240 ER Configuring policies, 555–557 Group Policy, 505 Network Unlock, 508–510 requirements, 503–505 BitLocker Provisioning option, 503 BitLocker To Go, 505 blocking, Group Polices, 249–252 Block Inheritance function, 250 block-level replication, 495 Boot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 build and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Canary users, 39 Capture images, 18 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate Revocation List (CRL) distribution point, 450 certificate Revocation Ist (CRL) distribution Protocol CHAP), 437	Assign A Static IPv4 Address (IP setting), 362	topology, 448
advanced auditing, 586–589 auditpol utility, 590–591 621–623 expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B B Caroip Policy, 505 Network Unlock, 508–510 requirements, 503–505 BitLocker Provisioning option, 503 BitLocker To Go, 505 BitLocker Provisioning veralletic, 249–252 Block Inheritance function, 250 block-level replication, 495 Boot images, 18 Boot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 bill and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 build and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 CC CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID property, 365 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 Carlor Own Device (BYOD) scenarios, 382 burnel own Device (BYOD) scenarios, 382 bot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 bot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 build and capture process, servicing Windows images, 12 Called Station ID condition, 349, 364 Called Station ID condition, 349, 364 Called Station ID	assigning applications, 281	BitLocker, 502–507
advanced auditing, 586–589 auditpol utility, 590–591 621–623 expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B B Caroip Policy, 505 Network Unlock, 508–510 requirements, 503–505 BitLocker Provisioning option, 503 BitLocker To Go, 505 BitLocker Provisioning veralletic, 249–252 Block Inheritance function, 250 block-level replication, 495 Boot images, 18 Boot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 bill and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 build and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 CC CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID property, 365 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 Carlor Own Device (BYOD) scenarios, 382 burnel own Device (BYOD) scenarios, 382 bot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 bot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 build and capture process, servicing Windows images, 12 Called Station ID condition, 349, 364 Called Station ID condition, 349, 364 Called Station ID		configuring policies, 555–557
auditpol utility, 590–591 configuring file and folder auditing, 589–590, 621–623 expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 BB BB BC BC Network Unlock, 508–510 requirements, 503–505 BitLocker Provisioning option, 503 BitLocker To Go, 505 blocking, Group Policy, 611–615 block-level replication, 495 Boot images, 18 Boot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 build and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 CC C C C C C C C C C C C		
configuring file and folder auditing, 589–590, 621–623	=	Network Unlock, 508–510
expression-based, 588–589, 617–621 logon auditing, 614–619 removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication Authoritizer process, 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic update Detection Frequency policy, 35 B B B B B B B B B B B B B		requirements, 503-505
logon auditing, 614–619 removable device auditing, 611–615 anditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B B backing up Active Directory, 206–208 client data, 277 GPOS (Group Policy Object dialog box, 239–240 blocking, Group Policies, 249–252 Block Inheritance function, 250 block-level replication, 495 Boot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 bloot options, configuring WDS, 22 Bring Your Own Device, Boot options, configuring WDS, 22 Bring Your Own Device, Broot Options, 382 build and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture images, 18 //Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate templates, 547–553 Certificate templates, 547–553 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437		•
logon auditing, 614–619 removable device auditing, 611–615 anditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B B backing up Active Directory, 206–208 client data, 277 GPOS (Group Policy Object dialog box, 239–240 blocking, Group Policies, 249–252 Block Inheritance function, 250 block-level replication, 495 Boot options, configuring WDS, 22 Bring Your Own Device (BYOD) scenarios, 382 bloot options, configuring WDS, 22 Bring Your Own Device, Boot options, configuring WDS, 22 Bring Your Own Device, Broot Options, 382 build and capture process, servicing Windows images, 9–10 built-in data collector sets, 566–567 BYOD (Bring Your Own Device) scenarios, 382 C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture images, 18 //Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate templates, 547–553 Certificate templates, 547–553 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437	expression-based, 588-589, 617-621	BitLocker To Go, 505
removable device auditing, 611–615 auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B B B B B B B B B B B		blocking, Group Policies, 249–252
auditpol utility, 590–591 authentication logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID property, 365 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 //Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy Objects), 239–240 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture-Image switch (DISM), 10 centralized deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate templates, 547–550 Certificate plantation protocol		Block Inheritance function, 250
logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B B B B B B B B B B B		
logging requests, 427 remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B B B B B B B B B B B B	authentication	Boot images, 18
remote access, 461 VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B B B B B B B B B B B B	logging requests, 427	
VPN, 437–438 Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B B B C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID property, 365 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 //Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437		
Authentication/Accounting tab (New Remote RADIUS Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437	VPN, 437–438	
Server Group dialog box), 420 authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B B B C C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID property, 365 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 Capture-image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority), 342–343 Called Station ID condition, 348, 364 canary users, 39 Capture-image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority, (2,4), 342–343 Challenge Handshake Authentication Protocol	•	
authentication methods (connection request policies), 351–352 Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B C CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID property, 365 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437	<u> </u>	9
Authentication Type condition, 364 authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 CA (Certification Authority), 342–343 Called Station ID condition, 348, 364 canary users, 39 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 Certificate enrollment, 549–553 Certificate enrollment, 549–553 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437	authentication methods (connection request poli-	BYOD (Bring Your Own Device) scenarios, 382
authoritative restore, 208–210 Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Backup-GPO cmdlet, 238 Backup-GPO cmdlet, 238 Backup-GPO policy Object dialog box, 239–240 CA (Certification Authority), 342–343 Called Station ID condition, 348, 364 canary users, 39 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 Certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certificate templates, 547–550 Certificate templates, 547–550 Certificate templates, 24–25 Called Station ID condition, 349, 364 canary users, 39 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring average, 18 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring average, 18 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring average averag	**	
Auto-Cast, configuring WDS transmissions, 25 automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic Update Detection Frequency policy, 35 B B CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437		
automated deployment, Windows images, 12–25 configuring answer files, 13–14 configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B B CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Called Station ID condition, 348, 364 canary users, 39 Capture images, 18 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Backup-GPO cmdlet, 238 CA (Certification Authority), 342–343 Called Station ID condition, 349, 364 Capture images, 18 C		C
configuring answer files, 13–14	5 5	CA (C. 1/1 1) A (I. 1/1) 242 242
configuring transmissions, 24–25 image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol		· · · · · · · · · · · · · · · · · · ·
image management, 18–19 installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Calling Station ID condition, 348, 364 canary users, 39 Capture images, 18 Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 Certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437		
installation, 12–13 WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B Capture images, 18 (Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Capture images, 18 Centralized deployment, automating server operating system deployment, 12–13 central store Configuring, 324–325 Group Policy administrative templates, 292–293 Certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437		
WDS (Windows Deployment Services), 14–24 automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B Capture images, 18 /Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Capture images, 18 Capture images, 18 Capture images, 18 Centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 Certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437		_
automatic approval rules (WSUS), 38–39 Automatic Update Detection Frequency policy, 35 B Capture-Image switch (DISM), 10 centralized deployment, automating server operating system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437	·	•
Automatic Update Detection Frequency policy, 35 Centralized deployment, automating server operating system deployment, 12–13 Central store Configuring, 324–325 Group Policy administrative templates, 292–293 backing up Active Directory, 206–208 Client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Certificate Revocation List (CRL) distribution point, 450 Certificate templates, 547–550 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437		· -
system deployment, 12–13 central store configuring, 324–325 Group Policy administrative templates, 292–293 backing up certificate enrollment, 549–553 Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Backup-GPO cmdlet, 238 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437	••	
Configuring, 324–325 Group Policy administrative templates, 292–293 backing up Certificate enrollment, 549–553 Active Directory, 206–208 Client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Backup-GPO cmdlet, 238 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437	Automatic Opuate Detection Frequency policy, 35	
Group Policy administrative templates, 292–293 backing up		central store
backing up certificate enrollment, 549–553 Active Directory, 206–208 client data, 277 GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Group Policy administrative templates, 292–293 Certificate enrollment, 549–553 Certificate Revocation List (CRL) distribution point, 450 certificate templates, 547–550 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol	В	configuring, 324–325
Active Directory, 206–208 Client data, 277 GPOs (Group Policy Objects), 239–240 Certificate templates, 547–550 Certificate templates, 547–550 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437		Group Policy administrative templates, 292–293
client data, 277 certificate templates, 547–550 GPOs (Group Policy Objects), 239–240 Certification Authority (CA), 342–343 Backup-GPO cmdlet, 238 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437	backing up	certificate enrollment, 549-553
GPOs (Group Policy Objects), 239–240 Backup-GPO cmdlet, 238 Back Up Group Policy Object dialog box, 239–240 Certification Authority (CA), 342–343 Challenge Handshake Authentication Protocol (CHAP), 437	Active Directory, 206–208	Certificate Revocation List (CRL) distribution point, 450
Backup-GPO cmdlet, 238 Challenge Handshake Authentication Protocol Back Up Group Policy Object dialog box, 239–240 (CHAP), 437	client data, 277	certificate templates, 547–550
Back Up Group Policy Object dialog box, 239–240 (CHAP), 437	GPOs (Group Policy Objects), 239–240	Certification Authority (CA), 342–343
	Backup-GPO cmdlet, 238	Challenge Handshake Authentication Protocol
balanced password policies, 65–66 Change Directory Server dialog box, 200	Back Up Group Policy Object dialog box, 239–240	(CHAP), 437
	balanced password policies, 65-66	Change Directory Server dialog box, 200
Basic option, configuring Folder Redirection policy, 277 Change Schema Master dialog box, 179	Basic option, configuring Folder Redirection policy, 277	
Before You Begin page (Add Roles and Features wizard), 341 CHAP (Challenge Handshake Authentication Protocol), 437	Before You Begin page (Add Roles and Features	_
CHAP (Encrypted Authentication), 351	W.Ed. 4), 5 11	

Cisco-NAC (Cisco Network Access Control)

Cisco-NAC (Cisco Network Access Control), 340	Configure Remote Access dialog box, 433-434
Cisco Network Access Control (Cisco-NAC), 340	Configure Settings page, 352
client configuration, NPS policies, 356–360	Configure Target Subscription Manager policy, 577
client data, backing up, 277	configuring
Client Friendly Name condition, 364	802.1X enforcement, 376-379
Client IPv4 Address condition, 349, 364	answer files, 13–14
Client IPv6 Address condition, 349, 364	automatic approval rules, 38-39
Client May Request An IP Address (IP setting), 362	BitLocker-related policies, 555–557
Client Naming Policy, configuring WDS, 21	central store, 324–325
client policies, configuring, 400–402	certificate enrollment, 549-553
clients	certificate templates, 547–550
DirectAccess, 452-453	client policies, 400–402
RADIUS (Remote Authentication Dial-In User	collector-initiated event subscriptions, 576–577
Service), 421–424	connection request forwarding setting, 350
Client Vendor condition, 349, 364	Control Panel settings, 313–315
cloning virtualized domain controllers, 193	data collection sets, 566–567, 593–598
clouds, 141	data encryption, 502–514
cmdlets	BitLocker, 503–508
Add-ADDSReadOnlyDomainControllerAccount, 188	EFS (Encrypting File System), 510–512
Add-ADServiceAccount, 85	key and data recovery, 512–513
Add-DnsServerConditionalForwarderZone	Network Unlock, 508–510
PowerShell, 131	DFS (Distributed File System), 492–500
Add-DNSServerDirectoryPartition, 122	DFS replication, 537–542
Add-DnsServerForwarder, 129	DHCP enforcement, 370-373, 402-405
Add-DnsServerPrimaryZone, 123	DirectAccess, 445–465
Add-DnsServerResourceRecordA, 144	application servers, 464–465
Add-DnsServerResourceRecordAAAA, 144	infrastructure, 446–452 Infrastructure Servers, 462–465
Add-DnsServerResourceRecordCName, 144	Remote Access Server, 461–462
Add-DnsServerResourceRecordMX PowerShell, 145	Remote Clients, 458–461
Add-DnsServerResourceRecordPtr, 146	domain user password policies, 62–66
Add-DnsServerStubZone, 132	event subscriptions, 603–607
Add-DnsServerZoneDelegation, 127	expression-based audit policies, 617–621
Add-KDSRootKey, 85	file and folder auditing, 589–590, 621–623
CNAME records, 144	file expiration, 526–529
collecting data, data collector sets, 597–600	file quotas, 519–523
collector-initiated event subscriptions, 576–577	file screens, 523–527
Command option (notification thresholds), 483	Folder Redirection, 276–279, 320–323
•	FSRM (File Server Resource Manager), 481–488
/Commit option (DISM), 9	file classification, 486–487
committing Windows images, 9	file management tasks, 487
Computer groups dialog box, 577	file screens, 483–484
Computer property (event logs), 573	quotas, 482–483
conditional forwarders, 130–131	storage reports, 488–489
Configure Authentication Methods page (NPS	Group Policy enforcement, 249–252
console), 365	Group Policy preferences, 298–299, 325–332
Configure Automatic Updates policy, 35	Group Policy scripts, 323–325
Configure Constraints page (NPS console), 365	health policies, 389–390
Configure Forwarder Resource Usage policy, 577	HRAs (Health Registration Authorities), 391–392
Configure NAP Wizard, 371, 374–375	Internet options, 309–312

IP filters, 360	wired/wireless network policies, 356–360
IPsec enforcement, 373–375	WMI filtering, 252–253
IP settings, 362–363	WSHV (Windows Security Health Validator),
logon auditing, 614–619	387–389, 397–398
name resolution, 119–152	WSUS (Windows Server Update Services), 52–56
advanced DNS options, 143-151	Confirm Installation Selections page (Add Roles and
conditional forwarders, 130–131	Features Wizard), 344
DNS zones, 120–125	Conflict and Deleted folder (DFS replication), 495
forwarders, 128–129	Connect As option, configuring, 301
Split DNS, 127–128	connection request forwarding setting, 350
stub zones, 131–132 WINS (Windows Internet Name Service), 119–123	connection request policies, 344–356
zone delegation, 126–127	authentication methods, 351–352
network access servers, 345–346	connection request forwarding setting, 350
network monitoring, 606–607	creating, 354–356
network routing, 439–441	default policy, 353–354
NPS templates, 367–368	
	network access server type, 345–346
NRPT (Name Resolution Policy Table), 151–152	realm names/RADIUS attributes, 352–353
partition-based replication, 156–157	Control Panel, configuring settings, 313–315
power options (Group Policy), 303–307	Copy-GPO cmdlet, 239
printers, 302–303	Copy GPO dialog box, 242–243
PSOs (Password Settings Objects), 78–80	copying GPOs (Group Policy Objects), 241–242
RADIUS (Remote Authentication Dial-In User	Create A Basic Task page (Create Basic Task
Service), 413–428, 470–471	Wizard), 579
accounting, 424–427 clients, 421–424	Create Basic Task Wizard, 579
proxies, 417–420	Create Custom View dialog box, 574–575
server groups, 468–470	Create Group dialog box, 107
servers, 414–417, 467–469	Create Multicast Transmission Wizard, 24
RD Gateway enforcement, 381–384	creating
registry (Group Policy), 308	conditional forwarders, 130–131
remediation server groups, 392–393, 399–400	connection request policies, 354–356
removable device auditing, 611–615	data collection sets, 567–570
replication partners, 137	DFS namespaces, 535–537
secondary zones, 163–166	event log filters, 573
SHAs (System Health Agents), 389	event log views, 574–575
SHVs (System Health Validators), 389	fine-grained password policies
source-computer-initiated subscriptions, 577	practice exercises, 106–110
storage reports, 529–532	GPOs (Group Policy Objects), 243–245
VPN enforcement, 379–381	group Managed Service Accounts, 85–86
VPN servers, 474–475	Group Policy central store, 292–293
VPN settings, 432–440	network policies, 362–366
tunneling protocols, 437–439	NRPT (Name Resolution Policy Table), 151
VPN authentication, 437–438	reverse lookup zones, 124–125
WDS transmissions, 24–25	shared folders, 515–519
WDS (Windows Deployment Services), 19–24, 44–53	stub zones, 131–132
Windows images, 3–4, 41–45	Creator Owners domain group, creating GPOs, 243-245
Windows settings, 311–313	credential roaming, 511
WINS (Windows Internet Name Service) role,	CRL (Certificate Revocation List) distribution point, 450
135–136	cryptographic policies, 391

D	deploying updates, 36–37
	WSUS groups, 34 WSUS management, 29–33
DAC (Dynamic Access Control), expression-based audit	WSUS policies, 34–35
policies, 589	deployment
data	automated, 12–25
accounting, 426	GlobalNames zones, 139
collection, 597–600	Group Policy software, 283
encryption, 502–514	NPS (Network Policy Server), 340–344
BitLocker configuration, 502–507	NPS role, 396–397
EFS (Encrypting File System), 510–512	RODCs (read-only domain controllers), 186,
key and data recovery, 512–513 Network Unlock, 508–510	220–225
performance	
alerts, 569–570	Routing and Remote Access, 430–432
data collection sets, 566–570	scripts, 286
database optimization (Active Directory), 196–198	Windows images, 2, 12–25
data collector sets, 566–570, 593–598, 597–600	WSUS (Windows Server Update Services), 29–37
data recovery agent (DRA), 506, 512	Deployment Image Servicing and Management (DISM)
Data Sources option, configuring Control Panel, 313	tool, 3–10
Date-Time property (file classification), 486	/Add-Driver switch, 6
Day And Time Restrictions condition, 348, 364	/Add-Package switch, 7
Day And Time Restrictions property, 365	/Apply-Image switch, 10
Deadline setting (Approve Updates dialog box), 37	/Capture-Image switch, 10
default connection request policy, 353–354	/Commit option, 9
Default Domain Policy GPO, 63	/Enable-Feature switch, 8
defragmenting Active Directory database, 196–197	/Get-Driver option, 6
delegation	/Get-Features switch, 8
DNS zones, 158–163	/Get-Package option, 7
	/Unmount-Wim switch, 9
GPO management, 243–247	Destination Log property (Event Viewer), 576
Kerberos, group Managed Service Accounts, 88 password setting permissions, 74–76	Detailed Tracking setting (advanced audit policies), 587
	Devices option, configuring Control Panel, 313
zones (DNS), 126–127	DFS (Distributed File System), 283, 492–500
Delegation of Control Wizard, 75	insatallation, 532–536
deleted objects, Active Directory recovery	namespaces, 492–495, 535–537
authoritative/non-authoritative restore, 208–211	replication, 495–500, 537–542
backup, 206–208	schedules, 498–500
Recycle Bin, 203–205	targets, 497 topologies, 497–498
deleting inactive user accounts, 71	DHCP (Dynamic Host Configuration Protocol), 129
Deny permissions, 251	enforcement, 370–373, 402–405
deployed servers	installation, 395–396
servicing, 27–38 automated deployment with WSUS, 28–39	servers. 16
automatic approval rules, 38–39	
deploying updates, 36–37	DHCP Quarantine Enforcement Client, 372
WSUS groups, 34	DHCP Server option, 346
WSUS management, 29–33	dialog boxes
WSUS policies, 34–35	Add (Rampys Tamplates 202
updating	Add Poles And Footures Wizard 343
automated deployment with WSUS, 28–29	Add Roles And Features Wizard, 342
automatic approval rules, 38–39	Add Rule, 38–39

Advanced Password Replication Policy, 190 Approve Updates, 37	DISM (Deployment Image Servicing and Management) tool, 3–10
	/Add-Driver switch, 6
Back Up Group Policy Object, 239–240	·
Change Schoma Master, 170	/Add-Package switch, 7
Change Schema Master, 179	/Apply-Image switch, 10
Computer Groups, 577	/Capture-Image switch, 10
Configure Remote Access, 433–434	/Commit option, 9
Copy GPO, 242–243	/Enable-Feature switch, 8
Create Custom View, 574–575	/Get-Driver option, 6
Create Group, 107	/Get-Features switch, 8
Enable Recycle Bin Confirmation, 204–205	/Get-Package option, 7
Filter Options, 295	/Unmount-Wim switch, 9
New Drive Properties, 300–301	Distributed File System (DFS), 283, 492–500
New Host, 144–145	installation, 532–536
New Object-User, 104	namespaces, 492–495, 535–537
New RADIUS Client, 422–423	replication, 495–500, 537–542
New Remediation Server Group, 392–393	schedules, 498–500
New Remote RADIUS Server Group, 418–419	targets, 497
New Resource Record, 144–145, 145	topologies, 497–498
New Shared Printer Properties, 302	DNS (Domain Name Server)
New Wired Network Policy Properties, 358	advanced options, 143–151
New WMI Filter, 253	aging and scavenging, 147–149
Operations Master, 180	DNSSEC, 149–152 resource records, 144–147
Operations Masters, 178–179	conditional forwarders, 130–131
Replication Partner Properties, 137–138	•
Save Filter To Custom View, 575	delegation, 158–163
Storage Reports Task Properties, 488	forwarders, 128–129
Subscription Properties, 576–577	Split DNS, 127–128
dial-up servers, as RADIUS clients, 421	stub zones, 131–132
dictionary attacks, 66	zone delegation, 126–127
digital signatures (DNSSEC), 149	zones, 120–125
DirectAccess	Active Directory integrated zones, 120–123
	practice exercises, 154–156 primary and secondary, 123–125
configuring, 445–465 application servers, 464–465	reverse lookup zones, 124–125
infrastructure, 446–452	DNSKEY recource records, 151
Infrastructure Servers, 462–465	DNS page (Infrastructure Server Setup Wizard), 462
Remote Access Server, 461–462	DNSSEC (Domain Name System Security
Remote Clients, 458–461	Extensions), 149–152, 168–170
servers, 448–451	DNSSEC Key Master, 151
Directory Services Restore Mode (DSRM) password, 187	
disabling inactive user accounts, 71	DNS Suffix Search List (Infrastructure Server Setup
Discover images, 18	Wizard), 463
disk encryption, 502–514	domain accounts, password policies, 62–66
BitLocker, 502–507	account lockout settings, 66–67
Group Policy, 505	account management tasks, 67–72
recovery, 506–508	balance, 65–66
requirements, 503–505	fine-grained policies, 74–81
EFS (Encrypting File System), 510–512	practice exercise, 93–99
key and data recovery, 512–513	
Network Unlock, 508–510	

Domain Admins group, Group Policy management tasks

Domain Admins group, Group Policy management tasks, 243	Dynamic Host Configuration Protocol (DHCP) servers, 16
domain-based namespaces, 493–494	dynamic updates, 122
domain controllers	dynamic apadies, 122
installation, 213–221	
maintenance, 195–201	_
database optimization, 196–198	E
metadata cleanup, 198–199	FAR MOE CHAR (F. 1. 'III A. 1. 1.' 1.' R. 1.
snapshots, 199–201	EAP-MD5 CHAP (Extensible Authentication Protocol-
management, 177–194	Message Digest 5 Challenge Handshake Authenti-
cloning, 193	cation), 437
Global Catalog servers, 183–184	EAP Quarantine Enforcement Client policy, 377
operations masters, 178–184	EAPs (Extensible Authentication Protocols), 351
RODC (read-only domain controller), 185–193	EAP-TLS (Extensible Authentication Protocol-Transport
UGMC (Universal group membership cach- ing), 184–185	Level Security), 437
domain controllers, Active Directory, 450	Edge topology, 448
domain-level operations masters, 178	editing GPOs (Group Policy Objects), 244
Domain Name Server (DNS)	EffectiveImmediately option (Add-KDSRootKey com-
advanced options, 143–151	mand), 85
aging and scavenging, 147–149	EFS (Encrypting File System), 510–512
DNSSEC, 149–152	E-mail option (notification thresholds), 483
resource records, 144–147	Enable Client-Side Targeting policy, 35
conditional forwarders, 130–131	/Enable-Feature switch (DISM), 8
delegation, 158–163	Enable Keyword Filters (Filter Options dialog box), 295
forwarders, 128–129	Enable Recycle Bin Confirmation dialog box, 204–205
Split DNS, 127–128	Enable Requirement Filters (Filter Options dialog
stub zones, 131–132	box), 295
zone delegation, 126-127	enabling Active Directory Recycle Bin, 204–205
zones, 120–125	Encrypted Authentication (CHAP), 351
Active Directory integrated zones, 120–123	Encrypting File System (EFS), 510–512
practice exercises, 154–156	encryption, 502–514
primary and secondary, 123–125	BitLocker configuration, 502–507
reverse lookup zones, 124–125	Group Policy, 505
Domain Name System Security Extensions (DNS-	recovery, 506–508 requirements, 503–505
SEC), 149–152, 168–170	•
domain naming master, 180	configuring network policies, 361–362
Domain Services Configuration Wizard, 183	EFS (Encrypting File System), 510–512
Do Not Display This Package In The Add/Remove	key and data recovery, 512–513
Programs Control Panel deployment option, 281	Network Unlock, 508–510
DRA (data recovery agent), 506, 512	Enforce Account Lockout Policy option (PSO), 80
Drive Letter option, configuring, 301	Enforce Maximum Password Age option (PSO), 80
Drive Maps (Group Policy preference), 300	enforcement, Group Policies, 249–252
drivers, adding to images, 6–8	enforcement methods (NAP), 370–385
DS Access setting (advanced audit policies), 587	802.1X, 376–379
DSRM (Directory Services Restore Mode) password, 187	DHCP, 370–373
Duplicate Files storage report, 488	IPsec, 373–375
Dynamic Access Control (DAC), expression-based audit policies, 589	RD Gateway, 381–384 VPN, 379–381
Dynamic Host Configuration Protocol (DHCP), 129	Enforce Minimum Password Age option (PSO), 80

Enforce Minimum Password Length option (PSO), 79	EFS (Encrypting File System), 510–512
Enforce Password History option (PSO), 79	key and data recovery, 512-513
Enforce password history password policy, 64	Network Unlock, 508–510
Enforce User Logon Restrictions (Kerberos policy), 90	Files By File Group storage report, 488
Enterprise Admins group, Group Policy management	Files By Owner storage report, 488
tasks, 243	Files By Property storage report, 488
Enterprise CA, installation, 542–547	File Screening Audit storage report, 488
Environment option, configuring Windows settings, 311	file screens, 483-484, 523-527
Essentials version, 446	File Server Resource Manager (FSRM), 481–488
event-driven tasks (monitor servers), 578–580	file classification, 486–487
Event IDs property (event logs), 572	file management tasks, 487
Event Level property (event logs), 572	file screens, 483–484
event logging, RADIUS accounting, 425	installation, 515-519
Event Log option (notification thresholds), 483	quotas, 482–483
event logs	storage reports, 488–489
filters, 572–573	file servers, management of
forwarding, 575–577	DFS (Distributed File System), 492–500
views, 573–575	namespaces, 492–495
Event Sources property (event logs), 572	replication, 495–500
Events To Collect property (Event Viewer), 576	encryption, 502–514
event subscriptions (monitor servers), 575–577,	BitLocker configuration, 502–507
601–607	EFS (Encrypting File System), 510–511
event trace data, 568–569	key and data recovery, 512 Network Unlock, 508–510
Event Viewer, 571–575	·
•	FSRM (File Server Resource Manager), 481–488 file classification, 486–487
EXE format, file deployment, 280–281	file management tasks, 487
exercises. See practice exercises	file screens, 483–484
expiration, files, 526	quotas, 482–483
expression-based audit policies, 588–589	storage reports, 488–489
Extensible Authentication Protocol-Message Digest 5	Files option, configuring Windows settings, 311
Challenge Handshake Authentication (EAP-MD5	Filter Options dialog box, 295
CHAP), 437	filters, event logs, 572–573
Extensible Authentication Protocols (EAPs), 351	fine-grained password policies, 74-81
Extensible Authentication Protocol-Transport Level	delegating password setting permissions, 74-76
Security (EAP-TLS), 437	determining password settings, 80–81
	management, 77–78
	practice exercises, 106–110
F	PSOs (Password Settings Objects), 78–80
•	firewall rules, 455
features, adding to Windows images, 8–9	Flexible Single Master Operations (FSMO) roles, 179
file classification, 486–487	domain naming master, 180
file formats, WIM (Windows Imaging), 2	infrastructure master, 181–182
file groups, 483	PDC emulator, 180-181
files	RID (relative identifier) master, 182
ADM, 290	schema master, 179
.admx, 290	seizing, 182
configuring auditing, 589–590	transferring roles, 225–228
encryption, 502–514	Folder Options, configuring Control Panel, 314
BitLocker configuration, 502–507	

Folder Redirection

Folder Redirection, 275–279	Getting Started Wizard, 456
configuring, 320–323	Global Catalog servers, 183–184
practice exercise, 318–319	Global cloud (PNRP), 141
folders	GlobalNames zones, 139–140
configuring auditing, 589-590, 621-623	Global Object Access Auditing, 590
Folder Redirection, 275–279	Global Object Access Auditing setting (advanced audit
Folders By Property storage report, 488	policies), 587
Folders option, configuring Windows settings, 312	GPMC (Group Policy Management Console), 238–239,
Follow The Documents Folder, configuring Folder	356
Redirection policy option, 278	creating GPOs, 244
force tunneling, 459	delegating permissions to GPOs, 243–244
Forefront Threat Management Gateway, 449	editing GPOs, 244
Forefront Unified Access Gateway, 449	linking GPOs, 245
forest-level operations masters, 178	WMI filters, 246–247
forwarders, 128–131	GPME (Group Policy Management Editor), 360
Forwarders tab, 128–129	GPOs (Group Policy Objects), 62. See also Group Policy
forwarding event logs, 575–577	audit policies, 586
FQDNs (fully qualified domain names), 119	DirectAccess clients, 452
Framed Protocol condition, 347, 364	maintenance, 237–247
FriendlyName field (.zap files), 280	backing up GPOs, 239–240
FSMO (Flexible Single Master Operations) roles, 179	delegating GPO management, 243–247
domain naming master, 180	importing/copying GPOs, 241–242 migrating GPOs, 242–243
infrastructure master, 181–182	practicing management tasks, 261–264
PDC emulator, 180–181	preparing exercise, 258–261
RID (relative identifier) master, 182	security filtering, 249–252
schema master, 179	group Managed Service Accounts, 83–90
seizing, 182	creating, 85–86
transferring roles, 225–228	Kerberos delegation, 88
FSRM (File Server Resource Manager), 481–488	Kerberos policies, 89–90
file classification, 486–487	practice exercises, 110–111
file management tasks, 487	requirements, 85
file screens, 483–484	service principal name (SPN) management, 91
installation, 515–519	virtual accounts, 87
quotas, 482–483	Group Policy
storage reports, 488–489	administrative templates, 290–297
Full Mesh topology (DFS replication), 497	ADMX Mitigator, 294
fully qualified domain names (FQDNs), 119	central store, 292–293
	settings, 291
	application management, 248–256
G	enforcement/blocking, 249–252
	loopback processing, 253–256
Get-ADDCCloningExcludedApplicationsList cmdlet, 193	processing precedence, 248–249 WMI filtering, 252–253
get-ADDomain cmdlet, 178	assigning WSUS groups, 34
get-AdForest cmdlet, 178	BitLocker, 505
/Get-Driver option (DISM), 6	configuring domain user password policies, 62–66
/Get-Features switch (DISM), 8	configuring scripts, 323–325
Get-GPO cmdlet, 238	configuring WSUS client options, 34
/Get-Package option (DISM), 7	object maintenance, 237–247

backing up GPOs, 239–240 delegating GPO management, 243–247 importing/copying GPOs, 241–242	H hard quotas, 483
migrating GPOs, 242–243	hardware requirements, xvi
preferences, 297–318	HCAP (Host Credential Authorization Protocol), 340
configuring power options, 303–307	HCAP Server, 346
configuring printers, 302–303 configuring the registry, 308	HCAP User Groups condition, 364
Control Panel settings, 313–315	health policies, 389–390
Internet options, 309–312	Health Policies condition, 364
item-level targeting, 299–300	Health Policies (NPS template), 367
mapping network drives, 300–302	
practice exercise, 325–332 settings, 298–299	Health Registration Authorities (HRAs), 340, 346, 391–392
Windows settings, 311–313	hibernation (power state), 304
settings, 275–287	Hide/Show All Drives option, configuring, 301
Folder Redirection, 276–280	Hide/Show This Drive option, configuring, 301
scripts, 285	Host Credential Authorization Protocol (HCAP), 340
software installation, 279–285	host records, 144–145
Group Policy loopback processing mode policy, 254–255	HRAs (Health Registration Authorities), 340, 346, 391–392
Group Policy Management Console (GPMC), 238–239,	Hub And Spoke topology (DFS replication), 497
356	7 7 37 7
creating GPOs, 244	
delegating permissions to GPOs, 243–244 editing GPOs, 244	1
linking GPOs, 245	
WMI filters, 246–247	IAS (Internet Authentication Service), 425
•	Identity Type condition, 348, 364
Group Policy Management Editor, 293	Idle Timeout property, 365
Group Policy Management Editor (GPME), 360	IKEv2 VPN protocol, 438–439
Group Policy Modeling, 100–103	images, Windows Server 2012, 2–3
Group Policy Modeling Wizard, 100	automated deployment, 12–25
Group Policy Objects (GPOs), 62. See also Group Policy	configuring, 3–4
audit policies, 586	servicing, 4–10
DirectAccess clients, 452	implementing password policies, 62–72
maintenance, 237–247	Import-GPO cmdlet, 239
backing up GPOs, 239–240	importing
delegating GPO management, 243–247 importing/copying GPOs, 241–242	administrative templates, 293
migrating GPOs, 242–243	GPOs (Group Policy Objects), 241–242
practicing management tasks, 261–264	Import Settings Wizard, 241
preparing exercise, 258–261	inactive user accounts, 71–72
security filtering, 249–252	infrastructure
Group Policy slow link detection policy, 255–256	DirectAccess, 446–452
groups, WSUS (Windows Server Update Services), 34	clients, 452–453
groups, vvsos (vviridows server opuate services), 34	DirectAccess server, 448–451
	NLS (Network Location Server), 451 topology, 447–448

infrastructure master

NAP (Network Access Protection), 386–393 health policies, 389–390	K
HRAS (Health Registration Authorities), 391–392 remediation server groups, 392–393 SHAs (System Health Agents), 389 SHVs (System Health Validators), 389 WSHV (Windows Security Health Validator), 387–389	Keep Existing Approvals setting (Approve Updates dialog box), 37 Kerberos group Managed Service Accounts delegation, 88
infrastructure master, 181–182 Infrastructure Server Setup Wizard, 462	policies, 89–90 SPN (service principal name) management, 91
Infrastructure Server Section (Remote Access	key distribution services root key, 85
Setup), 462–465	key recovery agent, 512–513
Ini Files option, configuring Windows settings, 312	Key Signing Key (KSK), 151 Keywords property (event logs), 572
Install-ADServiceAccount cmdlet, 86	KSK (Key Signing Key), 151
installation DFS (Distributed File System), 532–536	1.01. (1.0) 3.g.m.g 1.0// 202
DHCP role, 395–396	
domain controllers, 213–221	L
Enterprise CA, 542–547	_
FSRM (File Server Resource Manager), 515–519	L2TP/IPsec VPN protocol, 439
NPS role, 341–344, 414–415	Label As option, configuring, 301
software, Group Policy settings, 279–285	LAN Routing, 440–441
VPN servers, 473–474	Large Files storage report, 488
Windows Server 2012, 2–3	ldp.exe utility, 204
WINS (Windows Internet Name Service), 135–136	Least Recently Accessed Files storage report, 488
Install images, 18	linking GPOs (Group Policy Objects), 245
Install This Application At Logon deployment op-	Link-local cloud (PNRP), 141
tion, 281	Listening Ports view (Resource Monitor), 582
Integrated Administration console, 28	load-balanced configuration, DirectAccess, 450
integrated zones (Active Directory), 120–123	Load Balancing tab (New Remote RADIUS Server Group dialog box), 420
integration, WINS with DNS, 138 integrity check (databases), 197	local groups, configuring, 309–310
Internet Authentication Service (IAS), 425	local policies, 248
Internet, configuring Group Policy preferences,	Local System account, 286
309–312	Local Users And Groups option, configuring, 309–310
intervals, data collection, 568	locating
IP filters, 360	Folder Redirection policies, 276
IP Filters (NPS template), 367	inactive user accounts, 71–72
IPsec enforcement, 373–375	locked-out user accounts, 70–71
IPsec Relying Party Properties policy, 375	non-expiring passwords, 104–106
IP settings, configuring, 362–363	Location Groups condition, 347, 363
IPv6 routing, 440–441	Location option, configuring, 301
item-level targeting	locked-out accounts, 70–71
configuring power options, 303–304	lockout policies, 66–67, 93–102
Group Policy preferences, 299–300	Logged property (event logs), 572
	logging events, 426
	Logoff script, 285
	logon auditing, 614–619
	Logon/Logoff setting (advanced audit policies), 587

Logon script, 285	Windows images, 18–19
LogParser, 425, 582	WSUS (Windows Server Update Services), 29–34
loopback processing, Group Policies, 253–256	Management Servers page (Infrastructure Server Setup Wizard), 463
	mapping network drives, 300–302
RA	masters (operations), 178–184
M	domain naming master, 180
Machine Groups condition, 363	infrastructure master, 181–182
Mail exchanger (MX) records, 145	PDC emulator, 180–181
Mail Server Priority field (New Resource Record dialog	RID (relative identifier) master, 182
box), 145	schema master, 179
maintenance	seizing FSMO roles, 182
domain controllers, 195–201	Maximum Lifetime For Service Ticket (Kerberos
database optimization, 196–198	policy), 90
metadata cleanup, 198–199	Maximum Lifetime For User Ticket (Kerberos policy), 90
snapshots, 199–201	Maximum Lifetime For User Ticket Renewal (Kerberos
GPOs (Group Policy Objects), 237–247	policy), 90
backing up GPOs, 239–240	Maximum password age password policy, 64
delegating GPO management, 243–247 importing/copying GPOs, 241–242	Maximum Tolerance For Computer Clock Synchroniza-
migrating GPOs, 242–243	tion (Kerberos policy), 90
Managed Service Account Container, 84–85	MDOP (Microsoft Desktop Optimization Pack), 239
Managed Service Accounts, 83–90	Merge loopback processing, 254
creating, 85–86	Message Analyzer, 582–583, 608–611
Kerberos delegation, 88	metadata cleanup (Active Directory), 198-199
Kerberos policies, 89–90	Microsoft Challenge Handshake Authentication
practice exercises, 110–111	Protocol version 2 (MS-CHAPv2), 437
requirements, 85	Microsoft Desktop Optimization Pack (MDOP), 239
service principal name (SPN) management, 91	Microsoft Encrypted Authentication (MS-CHAP), 351
virtual accounts, 87	Microsoft Encrypted Authentication Version 2 (MS-
management	CHAP-v2), 351
domain account password policies, 67–72	Microsoft Forefront Threat Management Gateway, 449
domain controllers, 177–194	Microsoft Forefront Unified Access Gateway, 449
cloning, 193	Microsoft Management Console (MMC), Schema
Global Catalog servers, 183–184	snap-in, 179
operations masters, 178–184	Microsoft Windows Installer (MSI) format, packaged
RODC (read-only domain controller), 185–193 UGMC (Universal group membership cach-	applications
ing), 184–185	assigning an application, 281
file servers	deployment recommendations, 283
DFS (Distributed File System), 492–500	.msi files, 280
encryption, 502–514	publishing applications, 282
FSRM (File Server Resource Manager), 481–488	upgrading applications, 284
fine-grained password policies, 77–78	.zap files, 280–281
Group Policy application, 248–256	migrating GPOs, 242–243
enforcement/blocking, 249–252	Migration Table Editor (MTE), 242
loopback processing, 253–256 processing precedence, 248–249	migration tables, 242–243
WMI filtering, 252–253	Minimum password age password policy, 64
SPN (service principal name), 91	Minimum password length password policy, 64

MMC (Microsoft Management Console), Schema snap-in

MMC (Microsoft Management Console), Schema	stub zones, 131–132
snap-in, 179	zone delegation, 126–127
Modeling permissions (Group Policy), 246–247	PNRP (Peer Name Resolution Protocol), 140–141
monitor servers, 565–583	single-label, 134–141
alerts, 569–570	GlobalNames zones, 139–140
data collector sets, 566-570, 593-598	practice exercises, 166–168 WINS (Windows Internet Name Service), 135–139
event-driven tasks, 578–580	Name Resolution Policy Table (NRPT), 151–152
event subscriptions, 575–577	· · · · · · · · · · · · · · · · · · ·
Event Viewer, 571–575	namespaces (DFS), 492–495, 535–537
network monitoring, 581-583, 606-607	domain-based, 493–494
Most Recently Accessed Files storage report, 488	stand-alone, 494–495
mounting snapshots, 200, 211	NAP-Capable Computers condition, 364
mounting Windows images, 5–6	NAP (Network Access Protection), 339
Move-ADDirectoryServerOperationMasterRole	enforcement methods, 370–385
cmdlet, 182	802.1X, 376–379 DHCP, 370–373
MS-CHAP (Microsoft Encrypted Authentication), 351	IPsec, 373–375
MS-CHAPv2 (Microsoft Challenge Handshake Authenti-	RD Gateway, 381–384
cation Protocol version 2), 437	VPN, 379–381
MS-CHAP-v2 (Microsoft Encrypted Authentication	infrastructure, 386-393
Version 2), 351	health policies, 389–390
msDS-deletedObjectLifetime attribute, 204	HRAs (Health Registration Authorities), 391–392
.msi files, 280	remediation server groups, 392–393
MSI (Microsoft Windows Installer) format, packaged	SHAs (System Health Agents), 389
applications	SHVs (System Health Validators), 389 WSHV (Windows Security Health Validator),
assigning an application, 281	387–389
deployment recommendations, 283	NAS Identifier condition, 349, 364
.msi files, 280	NAS IPv4 Address condition, 349, 365
publishing applications, 282	NAS IPv6 Address condition, 349, 365
upgrading applications, 284	NAS Port Type condition, 349, 365
zap files, 280–281	NAS Port Type property, 365
MS-RAS Vendor condition, 364	NAT (Network Address Translation), 441–442
MS-Service Class condition, 364	NAT servers, 441–442
MTE (Migration Table Editor), 242	NCA (Network Connectivity Assistant), 460
Multicast options, WDS configuration, 23	Netlogon share, storing scripts, 286 Network Access Protection (NAP), 339
Multiple Choice List property (file classification), 486	, ,
Multi-string property (file classification), 486	enforcement methods, 370–385 802.1X, 376–379
MX (Mail exchanger) records, 145	DHCP, 370–373
	IPsec, 373–375
	RD Gateway, 381–384
N	VPN, 379–381
	infrastructure, 386-393
Name option (PSO), 79	health policies, 389–390
name resolution	HRAs (Health Registration Authorities), 391–392
configuring, 119–152	remediation server groups, 392–393
advanced DNS options, 143–151	SHAs (System Health Agents), 389 SHVs (System Health Validators), 389
conditional forwarders, 130–131	WSHV (Windows Security Health Validator),
DNS zones, 120–125 forwarders, 128–129	387–389
Split DNS. 127–128	network access servers, configuring, 345–346

Network Activity view (Resource Monitor), 582	New Shared Printer Properties dialog box, 302
Network Address Translation (NAT), 441–442	New Topology Wizard, 497
Network Connectivity Assistant (NCA), 460	New Wired Network Policy Properties dialog box, 358
network drives, mapping, 300-302	New WMI Filter dialog box, 253
Network Location Server (NLS), 451	New Zone Wizard, 120–121
network monitoring, 581-583, 606-607	Next Secure (NSEC/NSEC3) records, 151
Network Options, configuring Control Panel, 315	NLS (Network Location Server), 451
network policies	non-authoritative restore, 210
creating, 362–366	non-expiring passwords, 67–70, 104–106
NAP (Network Access Protection)	Not Approved setting (Approve Updates dialog
enforcement methods, 370–385	box), 37
infrastructure, 386–393	notification thresholds (quotas), 483
NPS (Network Policy Server), 339–367	NPS (Network Policy Server), 339, 414
client configuration, 356–360	deployment, 396–397
connection request policies, 344–356 deploying NPS role, 340–344	policies, 339–367
encryption, 361–362	client configuration, 356–360
IP filters, 360	connection request policies, 344–356
IP settings, 362–363	deploying NPS role, 340–344
templates, 367–368	encryption, 361–362
Network Policy Server (NPS), 339, 414	IP filters, 360 IP settings, 362–363
deployment, 396–397	templates, 367–368
policies, 339–367	NRPT (Name Resolution Policy Table), 151–152
client configuration, 356–360	NSEC/NSEC3 (Next Secure) records, 151
connection request policies, 344–356	NTDS Site Settings properties, enabling UGMC,
deploying NPS role, 340–344	184–185
encryption, 361–362	ntdsutil.exe command, 182, 196–197, 210
IP filters, 360 IP settings, 362–363	NTFS Permissions, 279
templates, 367–368	Number property (file classification), 486
network routing, 430, 439–441	Number property (me classification), 400
Network tab, configuring WDS, 24	
Network tab (Resource Monitor), 581	
network traffic capture and analysis, 582	0
Network Unlock, 508–510	
Network Unlock option, 503	Object Access setting (advanced audit policies), 587
New-ADDCCloneConfig Windows PowerShell	object deletion, Active Directory recovery
cmdlet, 193	authoritative/non-authoritative restore, 208–210
New Connection Request Policy Wizard, 356	backup, 206–208
New Drive Properties dialog box, 300–301	Recycle Bin, 203–205
New-GPO cmdlet, 239	objects (Group Policy). See GPOs (Group Policy Objects)
New Host dialog box, 144–145	offline files, Folder Redirection, 276
New Local Group Group Policy preference, 310	opening MTE (Migration Table Editor), 242
New Network Policy Wizard, 366	Operating System condition, 364
New Object-User dialog box, 104	operating systems, automating deployment, 12–13
New RADIUS Client dialog box, 422–423	Operations Master dialog box, 180
New Remediation Server Group dialog box, 392–393	operations masters, 178–184
New Remote RADIUS Server Group dialog box, 392–393	domain naming master, 180
418–419	infrastructure master, 181–182
	PDC emulator, 180–181
New Resource Record dialog box, 144–145	RID (relative identifiers) master, 182

Operations Masters dialog box

schema master, 179	performance data
seizing FSMO roles, 182	alerts, 569–570
Operations Masters dialog box, 178–179	data collector sets, 566–570
Ordered List property (file classification), 486	Performance Monitor, 566
organizational unit (OU) level settings, 249	periodic accounting status, logging, 427
	periodic authentication status, logging, 427
	permissions
P	delegating GPO management, 243–247
Г	password settings, 74–76
packaged applications (MSI format)	PIN/Password mode, 505
	PNRP (Peer Name Resolution Protocol), 140–141
assigning an application, 281	pointer (PTR) records, 144, 146–147
deployment recommendations, 283	policies
.msi files, 280	auditing, 585–591
publishing applications, 282	advanced auditing policies, 586–589
upgrading applications, 284	auditpol utility, 590–591
.zap files, 280–281	configuring file and folder auditing, 589–590,
PAP (Password Authentication Protocol), 437	621–623
partition-based replication, 156–157	expression-based, 588–589, 617–621 logon auditing, 614–619
partners, replication, 136	removable device auditing, 611–615
pass phrases, 64	configuring BitLocker-related policies, 555–557
Password Authentication Protocol (PAP), 437	domain user passwords, 62–66
Password Must Meet Complexity Requirements option	account lockout settings, 66–67
(PSO), 64, 79	account management tasks, 67–72
Password Never Expires setting, 67–68	balance, 65–66
password policies, domain accounts, 62–66	fine-grained policies, 74–81
account lockout settings, 66–67	practice exercise, 93–99
account management tasks, 67–72	fine-grained password policies, 106–110
balance, 65–66	Group Policy. See Group Policy
fine-grained policies, 74–81	Kerberos, Managed Service Accounts, 89–90
practice exercise, 93–99	NPS (Network Policy Server), 339–367
passwords	client configuration, 356–360
DSRM (Directory Services Restore Mode), 187	connection request policies, 344–356
group Managed Service Accounts, 83–90	deploying NPS role, 340–344 encryption, 361–362
creating, 85–86	IP filters, 360
Kerberos delegation, 88	IP settings, 362–363
Kerberos policies, 89–90 practice exercises, 110–111	templates, 367–368
requirements, 85	WSUS (Windows Server Update Services), 34–35
service principal name (SPN) management, 91	Policy Change setting (advanced audit policies), 587
virtual accounts, 87	Policy Expiration condition, 364
non-expiring, 104–106	power options
Password Settings Objects (PSOs), configuring, 78–80	configuring with Group Policy preferences, 303–307
PDC emulator, 180–181	Windows XP, 304–305
PEAP (Protected EAP), 351	power plans, 306–307
peer groups (PNRP), 141	Power Scheme (Windows XP), 305–306
Peer Name Resolution Protocol (PNRP), 140–141	PowerShell, WDS installation, 17
Performance Counter Alert option, 569	PPTP VPN protocol, 439
performance counter alerts, 569–570	,

preparing GPOs (Group Policy Objects), 258-261 Active Directory Recycle Bin, 229-231 RADIUS accounting, 471-473 administrative templates, 324-325 RADIUS servers, 467-469 collecting data from data collector sets, 597-600 removable device auditing, 611-615 configuring BitLocker-related policies, 555-557 RODC deployment, 220-225 configuring certificate enrollment, 549-553 secondary zones, 158–163 configuring certificate templates, 547-550 setup instructions, 627–630 configuring data collector sets, 593-598 single-label name resolution, 166-168 configuring DFS replication, 537-542 transferring FSMO roles, 225-228 configuring file expiration, 526-529 WDS configuration, 44-53 configuring file quotas, 519-523 WSUS configuration, 52-56 configuring file screens, 523-527 Pre-boot Execution Environment (PXE)-compliant configuring Folder Redirection, 320–323 network adapters, 14 configuring Group Policy scripts, 323-325 Precedence option (PSO), 79 configuring RADIUS clients, 470-471 preferences, Group Policy, 297-318 configuring remote RADIUS server groups, 468-470 configuring power options, 303-307 configuring secondary zones, 163-166 configuring printers, 302-303 configuring storage reports, 529-532 configuring the registry, 308 configuring VPN servers, 474-475 Control Panel settings, 313-315 configuring Windows images, 41-45 Internet options, 309-312 creating DFS namespaces, 535-537 item-level targeting, 299-300 DFS installation, 532-536 mapping network drives, 300-302 DNS delegation, 158-163 practice exercise, 325-332 **DNSSEC (Domain Name System Security** Windows settings, 311–313 Extensions), 168-170 primary zones, 123-125 DNS zones, 154-156 PrincipalsAllowedToDelegateAccount parameter, 88 domain controller installation, 213-221 printers, configuring, 302-303 Enterprise CA installation, 542-547 Privilege Use (advanced audit policies), 587 event subscriptions, 601-607 Processes With Network Activity view (Resource expression-based audit policies, 617-621 Monitor), 582 processing precedence, Group Policies, 248-249, fine-grained password policies, 106-110 264-267 folder auditing, 621-623 Folder Redirection, 318-319 Protected EAP (PEAP), 351 FSRM installation, 515–519 Protect From Accidental Deletion option (PSO), 79 GPO management, 261-264 protocols, TFTP (Trivial File Transfer Protocol), 24 group Managed Service Accounts, 110-111 protocols, VPN tunneling, 437-439 Group Policy Inheritance and Enforcement, 268–271 Protocol Type: ICMPv6 property (firewall rules), 455 Group Policy Modeling, 100-103 proxies (RADIUS), 417-420 Group Policy preferences, 325-332 PSOs (Password Settings Objects), configuring, 78-80 Group Policy processing, 264–267 PTR (pointer) records, 144, 146-147 installing VPN servers, 473-474 public keys, trust anchors, 151 lockout policies, 98-101 publishing applications, 282 logon auditing, 614-619 Pull partner (replication), 136 Message Analyzer, 608–611 Push partner (replication), 136 network monitoring, 606-607 PXE (Pre-boot Execution Environment)-compliant netnon-expiring passwords, 104-106 work adapters, 14 partition-based replication, 156-157 PXE Response Delay setting, 20 password policies, 93-99 PXE response settings, configuring WDS, 20

practice exercises

Q	remote access
4	configuring DirectAccess, 445–465
quotas, 482-483, 519-523	Infrastructure Servers, 462–465
quota templates, 482	Remote Access Server, 461–462
Quota Usage storage report, 488	Remote Clients, 458–461
	configuring network routing, 439–441
	configuring RADIUS, 413–428
n	accounting, 424–427
R	clients, 421–424 proxies, 417–420
PADILIS Clients (NIPS template) 267	servers, 414–417
RADIUS Clients (NPS template), 367 RADIUS (Remote Authentication Dial-In User Service)	configuring VPN settings, 432–440
•	tunneling protocols, 437–439
accounting, 471–473	VPN authentication, 437–438
attributes, connection request policies, 352–353	deploying Routing and Remote Access, 430–432
configuring, 413–428 accounting, 424–427	NAT (Network Address Translation), 441–442
clients, 421–424, 470–471	Remote Access console, selecting wizard, 456–457
proxies, 417–420	Remote Access Enforcement Client for Windows XP And
server groups, 468–470	Windows Vista policy, 380
servers	Remote Access Server section (Remote Access Setup
as RADIUS clients, 421	Wizard), 461–462
configuring, 414-417, 467-469	Remote Access Server (VPN-Dial Up), 346
RD Gateway enforcement, 381–384	Remote Access Server Wizard, 447
RD Gateway Quarantine Enforcement Client Properties	Remote Access Setup Wizard, 456
policy, 383	Remote Authentication Dial-In User Service (RADIUS)
RD Gateway (Remote Desktop Gateway), 339, 346	accounting, 471–473
RD RemoteApp applications, 381	configuring
RD Session Host servers, 381	accounting, 424–427
read-only domain controller (RODC), 123, 185-193,	clients, 421-424, 470-471
220–225	proxies, 417–420
Read/Write permissions (GPMC), 244	server groups, 468–470
realm names, connection request policies, 352-353	servers, 414–417, 413–428, 467–469
receiving folder (DFS replication), 496	Remote Clients section (Remote Access Setup),
recommendations, deploying software using Group	458–461
Policy, 283	Remote Desktop, 381
Reconnect option, configuring, 301	Remote Desktop Connection Broker, 381
recovery, Active Directory administration, 203–211	Remote Desktop Gateway (RD Gateway), 339, 346
authoritative/non-authoritative restore, 208-211	remote differential compression, 495
backup, 206–208	Remote RADIUS Servers (NPS template), 367
Recycle Bin, 203–205, 229–231	Remote Server Administration Tools, 342
recovery, BitLocker configuration, 506–508	Remote Server Administration Tools (RSAT), 17, 86
recovery keys, 506	removable device auditing, 611–615
Recycle Bin (Active Directory), 203–205, 229–231	Remove-GPO cmdlet, 239
Regional Options, configuring Control Panel, 315	Rename-GPO cmdlet, 239
registry, configuring, 308	Replace loopback processing, 254
registry keys, monitoring, 569–570	replication
relative identifier (RID) master, 182	DFS (Distributed File System), 537–542
remediation server groups, 392–393, 399–400	partition-based, 156–157
Remediation Server Groups (NPS template), 367	partners, 136

replication, DFS, 495–500	schema master, 179
schedules, 498–500	Schema snap-in (Active Directory), 179
targets, 497	scripts, Group Policy settings, 285, 323–325
topologies, 497–498	secondary zones, 123-125, 163-166
Replication Partner Properties dialog box, 137–138	Secured Password (EAP), 351
ReplicationScope parameter, 123	Security Account Manager (SAM) names, 85
Report option (notification thresholds), 483	security filtering, Group Policy, 249–252
requirements	security groups, Active Directory, 453
BitLocker encryption, 503–505	security identifiers (SIDs), 182
BitLocker Network Unlock, 508–509	Security Updates Settings (WSHV), 388
DirectAccess clients, 452–453	seizing FSMO roles, 182
DirectAccess servers, 449–451	Select Destination Server page (Add Roles and Features
group Managed Service Accounts, 85	wizard), 341
hardware and software, xvi	Select Installation Type page (Add Roles and Features
RODCs (read-only domain controllers), 186	wizard), 341
SSTP, 438	Select Server Roles page (Add Roles and Features
system, xvi	wizard), 341
WDS (Windows Deployment Services), 15–18	self-service password reset portals, 76
Reset Account Lockout Counter After policy, 67	semantic consistency check, 197
Resource Monitor, 581	Server Application Virtualization, 9
resource records, 144–147	Server Core, WDS (Windows Deployment Services), 17
Resource Record Signature (RRSIG) records, 150	server groups, configuring RADIUS, 468–470
Restore-GPO cmdlet, 239	Server Must Supply An IP Address (IP setting), 362
restoring GPOs (Group Policy Objects), 240	servers
Results permissions (Group Policy), 246–247	application, configuring DirectAccess, 464–465
reverse lookup zones, 124–125	automated operating system deployment, 12–13
RID (relative identifier) master, 182	DirectAccess, 448–451
Rights Management Services (Active Directory), 510	monitor servers, 565–583
RIP (Routing Information Protocol), 430	alerts, 569–570
RODC (read-only domain controller), 123, 185–193,	data collection sets, 593–598
220–225	data collector sets, 566–570
Routing and Remote Access, 430–432	event-driven tasks, 578–580 event subscriptions, 575–577
Routing And Remote Access Server Setup Wizard, 440	Event Viewer, 571–575
Routing Information Protocol (RIP), 430	network monitoring, 581–583, 606–607
RRSIG (Resource Record Signature) records, 150	NAT, 441–442
RSAT (Remote Server Administration Tools), 17, 86	NPS (Network Policy Server), 339
Rule Type: Custom property (firewall rules), 455	policies, 339–367
	RADIUS (Remote Authentication Dial-In User
	Service), 414-417, 467-469
S	servicing deployed servers, 27-38
3	VPN
SAM (Security Account Manager) names, 85	configuring, 474–475
Save Filter To Custom View dialog box, 575	deploying Windows Server 2012 as, 432–440
scavenging (DNS zones), 147–149	installation, 473–474
Scheduled-Cast, configuring WDS transmissions, 25	VPN (Virtual Private Network), 339
scheduled tasks, 571	Server Settings Determine IP Address Assignment (IP
Scheduled Tasks, configuring Control Panel, 315	setting), 362

schedules, DFS replication, 498-500

service accounts, Managed Service Accounts

service accounts, Managed Service Accounts, 83–90	SHVs (System Health Validators), 373, 389
creating, 85–86	SIDs (security identifiers), 182
Kerberos delegation, 88	signing zones (DNSSEC), 149
Kerberos policies, 89–90	Simple Mail Transfer Protocol (SMTP) gateways, 125
practice exercises, 110–111	single-label name resolution, 134–141
requirements, 85	GlobalNames zones, 139–140
service principal name (SPN) management, 91	practice exercises, 166–168
virtual accounts, 87	WINS (Windows Internet Name Service), 135–139
service principal name (SPN), 91	site level policy settings, 249
Service Type condition, 347, 364	slow-link processing, 255–256
servicing	Smart Card (EAP), 351
deployed servers, 27–38	SMTP (Simple Mail Transfer Protocol) gateways, 125
automated deployment with WSUS, 28–29	snapshots, 199–201, 211
automatic approval rules, 38–39	soft quotas, 483
deploying updates, 36-37	software
WSUS groups, 34	installation, Group Policy settings, 279–285
WSUS management, 29–33	requirements, xvi
WSUS policies, 34–35	Software Update Services (SUS), 28
Windows images, 4–10	source-computer-initiated subscriptions, 577
adding drivers and updates, 6–8 adding features and app packages, 8–9	SPAP (Challenge Handshake Authentication
build and capture process, 9–10	Protocol), 437
committing an image, 9	**
mounting images, 5–6	Specific ICMP Types: Echo Request property (firewall
Session Timeout property, 365	rules), 455
Set-ADComputer cmdlet, 88	Specify Access Permission page (NPS console), 365
Set-ADObject cmdlet, 204	Specify Authentication Methods page (NPS con-
Set-ADObject Windows PowerShell cmdlet, 208	sole), 351, 356
Set-ADServiceAccount cmdlet, 85, 88	Specify Conditions page (NPS console), 355, 363
Set-ADUser cmdlet, 88	Specify Connection Request Forwarding page (NPS
Set An Approval Deadline option (Add Rule dialog	console), 350, 355
box), 39	Specify Connection Request Policy Name And Connec-
Set-DnsServerScavenging cmdlet, 148	tion Type page (NPS console), 345, 355
settings	Specify Intranet Microsoft Update Service Location
administrative templates, 291	policy, 35
Group Policy, 275–287	Specify Network Policy Name And Connection Type
Folder Redirection, 276–280	page (NPS console), 363
preferences, 298–299	Split DNS, 127–128
scripts, 285	SPN (service principal name)
software installation, 279–285	management, 91
SetupCommand field (.zap file), 280	SSTP VPN protocol, 438
setup instructions (exercises), 627–630	staging folder (DFS replication), 496
shared folders, creating, 515–519	stand-alone namespaces (DFS), 494–495
Shared Secrets (NPS template), 367	standard primary zones, 123
shared secrets, RADIUS clients, 422	Standard User PIN And Password Change option, 503
Share Permissions For Root Folder, 278	standby (power state), 304
SHAs (System Health Agents), 373, 389	Start A Program page (Create Basic Task Wizard), 579
Shiva Password Authentication Protocol (SPAP), 437	Start Menu, configuring Control Panel, 315
Shortcuts option, configuring Windows settings, 312	Startup Key mode, 505
Shutdown script, 285	Startup script, 285

static routes, 430	tools
storage reports, 488-489, 529-532	ADMX Mitigator, 294
Storage Reports Task Properties dialog box, 488	DISM (Deployment Image Servicing and Manage-
Store BitLocker recovery, 506	ment), 3–10, 19
Store Passwords Using Reversible Encryption policy, 65	ldp.exe utility, 204
Store Password Using Reversible Encryption option	ntdsutil.exe utility, 182, 196
(PSO), 79	RSAT (Remote Server Administration Tools), 17, 86
storing scripts, 286	Sysprep.exe, 9
String property (file classification), 486	Windows Server Backup, 206–208
stub zones, 131–132	topologies, DFS replication, 497–498
Subscription Name property (Event Viewer), 576	topologies, DirectAccess, 447–448
Subscription Properties dialog box, 576–577	TPM Allow Startup Key, 504
Subscription Type And Source Computers: Collector	TPM-Only Mode, 504
Initiated property (Event Viewer), 576	TPM (Trusted Platform Module), 503
SUS (Software Update Services), 28	TPM With PIN/Password And Startup Key mode, 505
switches, as RADIUS clients, 421	TPM With PIN/Password mode, 504
Sysprep.exe utility, 9	traditional audit policies, 586
system administration, Active Directory	transport policies, 392
domain controller maintenance, 195–201	Trivial File Transfer Protocol (TFTP), 24
domain controller management, 177–194	trust anchors, 151
recovery, 203–211	Trusted Platform Module (TPM), 503
System Center 2012 Configuration Manager, 19, 28, 35	tunneling protocols (VPN), 437–439
System Center Configuration Manager 2012, 283, 307	Tunnel Type condition, 348, 364
System Health Agents (SHAs), 373, 389	Two-Factor Authentication, 449
System Health Validators (SHVs), 373, 389	
System Out-of-Box Experience (OOBE), 10	П
System Out-of-Box Experience (OOBE), 10 system requirements, xvi	U
System Out-of-Box Experience (OOBE), 10	
System Out-of-Box Experience (OOBE), 10 system requirements, xvi	UEFI (Unified Extensible Firmware Interface), 504
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185
System Out-of-Box Experience (OOBE), 10 system requirements, xvi	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC),
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24 TFTP (Trivial File Transfer Protocol), 24	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346 updates, adding to images, 6–8
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24 TFTP (Trivial File Transfer Protocol), 24 Threat Management Gateway, 449	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346 updates, adding to images, 6–8 Update Services console, 34, 36, 196
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24 TFTP (Trivial File Transfer Protocol), 24 Threat Management Gateway, 449 Threshold option (notification thresholds), 483	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346 updates, adding to images, 6–8 Update Services console, 34, 36, 196 updating
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24 TFTP (Trivial File Transfer Protocol), 24 Threat Management Gateway, 449 Threshold option (notification thresholds), 483 thresholds, alerts, 570–571	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346 updates, adding to images, 6–8 Update Services console, 34, 36, 196 updating deployed servers, 27–38
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24 TFTP (Trivial File Transfer Protocol), 24 Threat Management Gateway, 449 Threshold option (notification thresholds), 483	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346 updates, adding to images, 6–8 Update Services console, 34, 36, 196 updating
System Out-of-Box Experience (OOBE), 10 system requirements, xvi System setting (advanced audit policies), 587 T targets, DFS replication, 497 tasks, event-driven, 578–580 TCP Connections view (Resource Monitor), 582 templates file screens, 483 quotas, 482–483 templates (NPS), 367–368 test groups, automatic approval rules, 39 TFTP tab, configuring WDS, 24 TFTP (Trivial File Transfer Protocol), 24 Threat Management Gateway, 449 Threshold option (notification thresholds), 483 thresholds, alerts, 570–571	UEFI (Unified Extensible Firmware Interface), 504 UGMC (Universal group membership caching), 184–185 Unassigned Computers group, 34 Unencrypted Authentication, 351 Unified Access Gateway, 449 Unified Extensible Firmware Interface (UEFI), 504 Uninstall-ADDSDomainController cmdlet, 198 Uninstall The Application When It Falls Out Of The Scope Of Management deployment option, 281 Universal group membership caching (UGMC), 184–185 /Unmount-Wim switch (DISM), 9 Unspecified connection, 346 updates, adding to images, 6–8 Update Services console, 34, 36, 196 updating deployed servers, 27–38 automated deployment with WSUS, 28–29

upgrading applications, Group Policy

WSUS management, 29–33 WSUS policies, 34–35	When An Update Is In A Specific Classification option
Windows images, 2	(Add Rule dialog box), 38
upgrading applications, Group Policy, 284	WIM (Windows Imaging) file format, 2
usage scenarios, RODCs, 191	Windows 2000 mode (domain-based namespaces), 493
-	Windows 2008 mode (domain-based namespaces), 493
Used Disk Space Only Encryption option, 503 user accounts	Windows ADK (Windows Assessment and Deployment
	Kit), 13
backing up data, 277	Windows Assessment and Deployment Kit (Windows
configuring, 309–310	ADK), 13
User Groups condition, 363	Windows, configuring settings, 311–313
User Name condition, 347	Windows Deployment Services (WDS), 14–18, 508
User property (event logs), 573	configuring, 19–24, 44–53
Use Windows Authentication For All Users, 353	transmissions, 24–25
utilities. See tools	Windows Event Collector (wecsvc), 576
	Windows Groups condition, 363
	Windows Imaging (WIM) file format, 2
V	Windows Internet Name Service (WINS), 135–139
V	Windows Intune, 283
views, event logs, 573–575	Windows PE, 18–19
virtual accounts, Managed Service Accounts, 87	Windows PowerShell Group Policy module, GPO
Virtual Machine Manager (VMM), 19	management, 238
Virtual Machines (VMs), BitLocker and, 503	Windows Remote Management (WinRM), 576
Virtual Private Network (VPN) servers, 339	Windows Security Health Validator (WSHV), 373,
virtulaization hardware requirements, xvi	387–389, 397–398
VMM (Virtual Machine Manager), 19	Windows Server 2012
	group Managed Service Accounts, 83–90
VMs (Virtual Machines), BitLocker and, 503	creating, 85–86
VPN enforcement, 379–381	Kerberos delegation, 88
VPN servers	Kerberos policies, 89–90
as RADIUS clients, 421	practice exercises, 110–111
configuring, 474–475	requirements, 85
deploying Windows Server 2012 as, 432–440	service principal name (SPN) management, 91
installation, 473–474	virtual accounts, 87
VPN settings, configuring, 432–440	images, 2, 2–3
tunneling protocols, 437–439	automated deployment, 12–25
VPN authentication, 437–438	configuring, 3–4
VPN (Virtual Private Network) servers, 339	servicing, 4–10
	WSUS (Windows Server Update Services), 27–38 automated update deployment, 28–29
	automatic approval rules, 38–39
W	deploying updates, 36–37
VV	deployment and management, 29–34
WDS (Windows Deployment Services), 14–18, 508	groups, 34
configuring, 19–24, 44–53	new features, 28
transmissions, 24–25	policies, 34–35
wecsvc (Windows Event Collector), 576	Windows Server Backup, 206–208
When An Event is Logged page (Create Basic Task	Windows Server Update Services (WSUS), 27–38
Wizard), 579	automated update deployment, 28–29
When An Update Is For A Specific Product option (Add	automatic approval rules, 38-39
Rule dialog box), 39	configuring, 52–56

deploying updates, 36-37 deployment and management, 29-34 groups, 34 new features, 28 policies, 34-35 Windows SIM, answer files, 13-14 Windows Vista, power plans, 304 Windows XP Power Options item, 304-305 Power Scheme item, 305-306 WinRM (Windows Remote Management), 576 WINS Server feature, 135-136 WINS (Windows Internet Name Service), 135–139 Wired Network (IEEE 802.3) Policies, 357 wired networks, configuring 802.1X enforcement, 377-378 wireless access points, as RADIUS clients, 421 Wireless Network (IEEE 802.11) Policies, 357 wireless networks, configuring 802.1X enforcement, 378-379 wizards Accounting Configuration, 426 Add Image, 19 Add Roles And Features, 19, 135, 186, 206, 341 Configure NAP, 371, 374-375 Create Basic Task, 579 Create Multicast Transmission, 19 Delegation of Control, 75 Domain Services Configuration, 183 Getting Started, 456 Group Policy Modeling, 100 Import Settings, 241 Infrastructure Server Setup, 462 New Connection Request Policy, 356 New Network Policy, 366 New Topology, 497 New Zone. 120-121 Remote Access Server, 447 Remote Access Setup, 456 Routing And Remote Access Server Setup, 440 WMI filtering, Group Policies, 252-253 WMI filters, GPMC (Group Policy Management Console), 246-247 WMI gueries, 252-253 WMI Query Language (WQL), 252 WQL (WMI Query Language), 252

WSHV (Windows Security Health Validator), 373, 387–389
WSUS (Windows Server Update Services), 27–38 automated update deployment, 28–29 automatic approval rules, 38–39 configuring, 52–56 deploying updates, 36–37 deployment and management, 29–34 groups, 34 new features, 28 policies, 34–35



XML format, administrative templates, 290



Yes/No property (file classification), 486

Z

.zap files, 280–281
Zone In Active Directory option (New Zone Wizard), 120
zones (DNS), 120–125
Active Directory integrated zones, 120–123
delegation, 126–127
GlobalNames, 139–140
practice exercises, 154–156
primary zones, 123–125
reverse lookup zones, 124–125
secondary, 123–125, 163–166
stub, 131–132
Zone Signing Key (ZSK), 151
Zone Transfers tab, 123–124
ZSK (Zone Signing Key), 151

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 1990s. 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 Users Group. You can follow him on Twitter at http://twitter.com/orinthomas.

Training Guide: Administering Windows Server 2012 and Exam 70-411

The following is a list of 70-411 objectives and the mapping between those topics and the chapters in this book.

DEPLOY, MANAGE, AND MAINTAIN SERVERS			
Deploy and manage server images	Chapter 1, Lessons 1 and 2		
Implement patch management	Chapter 1, Lesson 3		
Monitor servers	Chapter 10, Lesson 1		
CONFIGURE FILE AND PRINT SERVICES			
Configure Distributed File System (DFS)	Chapter 9, Lesson 2		
Configure File Server Resource Manager (FSRM)	Chapter 9, Lesson 1		
Configure file and disk encryption Chapter 9, Lesson 3			
Configure advanced audit policies Chapter 10, Lesson 2			
CONFIGURE NETWORK SERVICES AND ACCESS			
Configure DNS zones	Chapter 3, Lesson 2		
Configure DNS records	Chapter 3, Lesson 3		
Configure VPN and routing	Chapter 8, Lesson 2		
Configure DirectAccess	Chapter 8, Lesson 3		
CONFIGURE A NETWORK POLICY SERVER INFRASTRUCTURE			
Configure Network Policy Server (NPS)	Chapter 8, Lesson 1		
Configure NPS policies	Chapter 7, Lesson 1		
Configure Network Access Protection (NAP) Chapter 7, Lessons 2 and 3			
CONFIGURE AND MANAGE ACTIVE DIRECTORY			
Configure service authentication	Chapter 2, Lesson 3		
Configure domain controllers	Chapter 4, Lesson 1		
Maintain Active Directory	Chapter 4, Lessons 2 and 3		
Configure account policies	Chapter 2, Lesson 2		

CONFIGURE AND MANAGE GROUP POLICY	
Configure Group Policy processing	Chapter 5, Lesson 2
Configure Group Policy settings	Chapter 6, Lesson 1
Manage Group Policy objects (GPOs)	Chapter 5, Lesson 1
Configure Group Policy preferences	Chapter 6, Lesson 3

Exam Objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning website for the most current listing of exam objectives: http://www.microsoft.com/learning/en/us/exam-70-411.aspx.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

