



# Administering Windows Server 2012 R2

## Training Guide

Orin Thomas

# Training Guide: Administering Windows Server® 2012 R2

Orin Thomas

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

Copyright © 2014 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.

Library of Congress Control Number: 2014937581  
ISBN: 978-0-7356-8469-0

Printed and bound in the United States of America.

First Printing

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

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

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

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

**Acquisitions Editor:** Anne Hamilton

**Developmental Editor:** Karen Szall

**Editorial Production:** Troy Mott, Backstop Media LLC

**Technical Reviewer:** Telmo Sampaio

**Copyeditor:** Christina Rudloff

**Indexer:** Judy Hoer

**Cover:** Twist Creative • Seattle

# Contents at a glance

	<i>Introduction</i>	<i>xvii</i>
<b>CHAPTER 1</b>	<b>Deploying and updating Windows Server 2012 R2</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Managing account policies and service accounts</b>	<b>65</b>
<b>CHAPTER 3</b>	<b>Configuring name resolution</b>	<b>123</b>
<b>CHAPTER 4</b>	<b>Administering Active Directory</b>	<b>181</b>
<b>CHAPTER 5</b>	<b>Managing Group Policy application and infrastructure</b>	<b>241</b>
<b>CHAPTER 6</b>	<b>Group Policy settings and preferences</b>	<b>281</b>
<b>CHAPTER 7</b>	<b>Administering network policies</b>	<b>345</b>
<b>CHAPTER 8</b>	<b>Administering remote access</b>	<b>417</b>
<b>CHAPTER 9</b>	<b>Managing file services</b>	<b>501</b>
<b>CHAPTER 10</b>	<b>Monitoring and auditing</b>	<b>591</b>
	<i>Index</i>	<i>659</i>

*This page intentionally left blank*

# Contents

<b>Introduction</b>	<b>xvii</b>
<b>Chapter 1: Deploying and updating Windows Server 2012 R2</b>	<b>1</b>
Before you begin . . . . .	1
Lesson 1: Configuring and servicing Windows Server images . . . . .	1
Understanding Windows images	2
Configuring Windows images	3
Servicing Windows images	4
Lesson summary	10
Lesson review	10
Lesson 2: Automatically deploying Windows Server images . . . . .	11
Automating installation	12
Configuring answer files	12
Windows Deployment Services	14
WDS requirements	15
Managing images	17
Configuring WDS	19
Configuring transmissions	24
Driver groups and packages	25
Lesson summary	26
Lesson review	26
Lesson 3: Servicing and updating deployed servers . . . . .	27
Automated update deployment with WSUS	28
New WSUS features	28

---

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

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

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

Deploy and manage WSUS	28
WSUS groups	33
WSUS policies	33
Deploying updates	35
Automatic approval rules	36
Lesson summary	38
Lesson review	38
Practice exercises . . . . .	39
Exercise 1: Prepare update files	40
Exercise 2: Servicing a WIM image	42
Exercise 3: Deploy Windows Deployment Services	43
Exercise 4: Configure Windows Deployment Services	47
Exercise 5: Import driver package	52
Exercise 6: Deploy WSUS	54
Exercise 7: Configure WSUS	56
Exercise 8: WSUS groups and rules	58
Suggested practice exercises . . . . .	60
Answers. . . . .	61
Lesson 1	61
Lesson 2	61
Lesson 3	62

**Chapter 2: Managing account policies and service accounts      65**

Before you begin. . . . .	65
Lesson 1: Implementing domain password and lockout policies. . . . .	65
Domain user password policies	66
Account lockout settings	70
Account management tasks	71
Lesson summary	76
Lesson review	76
Lesson 2: Using fine-grained password policies . . . . .	77
Delegate password settings permissions	78
Fine-grained password policies	80
Lesson summary	85

Lesson review	85
Lesson 3: Mastering Group Managed Service Accounts . . . . .	87
GMSAs	87
Kerberos delegation	91
Kerberos policies	92
Service principal name management	94
Lesson summary	94
Lesson review	94
Practice exercises . . . . .	95
Exercise 1: Configure password and account lockout policies	96
Exercise 2: Configure account lockout policies	101
Exercise 3: Group Policy Modeling	104
Exercise 4: Locate non-expiring passwords	107
Exercise 5: Create fine-grained password policies	110
Exercise 6: Prepare MEL-DC and ADL-DC	113
Exercise 7: Create and configure GMSAs	114
Suggested practice exercises . . . . .	116
Answers . . . . .	117
Lesson 1	117
Lesson 2	118
Lesson 3	119

### **Chapter 3: Configuring name resolution 123**

Before you begin . . . . .	123
Lesson 1: Understanding DNS zones and forwarders . . . . .	123
DNS zone types	124
Zone delegation	129
Split DNS	131
Forwarders and conditional forwarders	131
Stub zones	134
Lesson summary	136
Lesson review	136
Lesson 2: Configuring WINS and managing GlobalNames zones . . . . .	138
WINS	138



GlobalNames zones	142
Peer Name Resolution Protocol (PNRP)	144
Lesson summary	145
Lesson review	146
Lesson 3: Understanding advanced DNS options . . . . .	147
Resource records	147
Zone aging and scavenging	151
DNSSEC	153
Lesson summary	157
Lesson review	157
Practice exercises . . . . .	158
Exercise 1: Manage DNS zones	159
Exercise 2: Configure partition-based replication	161
Exercise 3: DNS delegation and secondary zones	163
Exercise 4: Configure a secondary zone	168
Exercise 5: Single-label name resolution	171
Exercise 6: Configure and manage DNSSEC	173
Suggested practice exercises . . . . .	176
Answers . . . . .	177
Lesson 1	177
Lesson 2	178
Lesson 3	179

## **Chapter 4: Administering Active Directory** **181**

Before you begin . . . . .	181
Lesson 1: Managing domain controllers . . . . .	181
Managing operations masters	182
Global Catalog servers	187
Universal group membership caching	189
Read-only domain controllers	190
Domain controller cloning	197
Lesson summary	198
Lesson review	199

Lesson 2: Maintaining domain controllers . . . . .	200
Active Directory database optimization	200
Active Directory metadata cleanup	203
Active Directory snapshots	204
Lesson summary	206
Lesson review	207
Lesson 3: Recovering Active Directory . . . . .	208
Active Directory Recycle Bin	208
Active Directory backup	210
Active Directory recovery	212
Lesson summary	215
Lesson review	216
Practice exercises . . . . .	217
Exercise 1: Domain controller installation	217
Exercise 2: RODC deployment	225
Exercise 3: Transfer operations master roles	230
Exercise 4: Active Directory Recycle Bin	234
Suggested practice exercises . . . . .	236
Answers . . . . .	237
Lesson 1	237
Lesson 2	238
Lesson 3	239

## **Chapter 5: Managing Group Policy application and infrastructure 241**

Before you begin . . . . .	241
Lesson 1: Maintaining Group Policy Object . . . . .	241
Managing Group Policy Objects	242
Migrate Group Policy Objects	247
Delegate GPO management	248
Lesson summary	251
Lesson review	252
Lesson 2: Managing Group Policy application . . . . .	253
Policy processing precedence	253

Policy enforcement and blocking	254
Group Policy security filtering	255
Group Policy WMI filtering	257
Loopback processing	258
Group Policy caching	260
Force Group Policy update	261
Lesson summary	263
Lesson review	263
Practice exercises	265
Exercise 1: Prepare GPOs, security groups, and OUs	265
Exercise 2: Manage GPOs	268
Exercise 3: Manage Group Policy processing	271
Exercise 4: Group Policy inheritance and enforcement	274
Suggested practice exercises	277
Answers	278
Lesson 1	278
Lesson 2	279

## **Chapter 6: Group Policy settings and preferences** **281**

Before you begin	281
Lesson 1: Folder redirection, software installation, and scripts	281
Folder Redirection	282
Software installation	285
Scripts	291
Lesson summary	293
Lesson review	293
Lesson 2: Administrative templates	296
Administrative templates	296
Administrative template settings	297
Central store	297
ADMX Migrator	299
Filter property settings	300
Lesson summary	302
Lesson review	302

Lesson 3: Group Policy preferences . . . . .	303
Group Policy preference settings	303
Item-level targeting	305
Mapping network drives	306
Configuring printers	308
Configuring power options	309
Configuring the registry	314
Internet options	314
Additional settings	317
Lesson summary	321
Lesson review	322
Practice exercises . . . . .	323
Exercise 1: Prepare Folder Redirection and scripts	324
Exercise 2: Configure Folder Redirection	325
Exercise 3: Configure Group Policy scripts	329
Exercise 4: Configure the central store and administrative template filtering	330
Exercise 5: Configure Group Policy preferences	331
Suggested practice exercises . . . . .	338
Answers . . . . .	339
Lesson 1	339
Lesson 2	340
Lesson 3	341

## **Chapter 7: Administering network policies 345**

Before you begin . . . . .	345
Lesson 1: Understanding Network Policy Server policies . . . . .	345
NPS deployment	346
Connection request policies	350
Client configuration	363
IP filters	367
Encryption	368
IP settings	368
Creating network policies	369

NPS templates	374
Lesson summary	375
Lesson review	375
Lesson 2: Understanding Network Access Protection enforcement methods . . . . .	376
DHCP enforcement	377
IPsec enforcement	380
802.1X enforcement	382
VPN enforcement	385
RD Gateway enforcement	387
Lesson summary	390
Lesson review	391
Lesson 3: Understanding Network Access Protection infrastructure. . . . .	392
Windows Security Health Validator	392
System Health Validators and System Health Agents	395
Health policies	395
Health Registration Authorities	397
Remediation server groups	398
Lesson summary	399
Lesson review	399
Practice exercises . . . . .	400
Exercise 1: Installing the DHCP role	401
Exercise 2: Deploying the NPS role	402
Exercise 3: Configuring Windows Security Health Validator	403
Exercise 4: Configuring a remediation server group	405
Exercise 5: Configuring client policies for DHCP enforcement	406
Exercise 6: Configuring NAP DHCP enforcement	408
Suggested practice exercises . . . . .	412
Answers. . . . .	413
Lesson 1	413
Lesson 2	414
Lesson 3	415

## **Chapter 8: Administering remote access 417**

Before you begin . . . . .	417
Lesson 1: Configuring RADIUS . . . . .	417
RADIUS servers	418
RADIUS proxies	421
RADIUS clients	426
RADIUS accounting	429
Lesson summary	433
Lesson review	433
Lesson 2: Configuring VPN and routing . . . . .	434
Deploy Routing and Remote Access	435
Configure VPN settings	437
Configure routing	446
Network address translation (NAT)	448
Web Application Proxy in pass-through mode	451
Lesson summary	453
Lesson review	453
Lesson 3: Configuring DirectAccess . . . . .	454
Understanding DirectAccess	455
DirectAccess infrastructure	455
Configure DirectAccess	462
Lesson summary	473
Lesson review	474
Practice exercises . . . . .	475
Exercise 1: Configure a RADIUS server	475
Exercise 2: Configure a remote RADIUS server group	477
Exercise 3: Configure a RADIUS client	479
Exercise 4: Set up RADIUS accounting	480
Exercise 5: Install a VPN server	481
Exercise 6: Configure a VPN server	482
Exercise 7: Prepare for Web Application Proxy	483
Exercise 8: Configure AD FS to support Web Application Proxy	489

Exercise 9: Deploy Web Application Proxy with pass-through preauthentication	491
Suggested practice exercises	495
Answers	496
Lesson 1	496
Lesson 2	497
Lesson 3	498

## **Chapter 9: Managing file services** **501**

Before you begin	501
Lesson 1: Configuring File Server Resource Manager	501
Configuring quotas	502
Configuring file screens	504
Enabling file classification	505
Configuring file management tasks	506
Generating reports	507
Lesson summary	509
Lesson review	509
Lesson 2: Configuring a Distributed File System	511
Understanding Distributed File System namespaces	511
Understanding DFS replication	514
Cloning the DFS Replication database	519
Understanding DFSR and database recovery	520
Lesson summary	520
Lesson review	520
Lesson 3: Configuring file and disk encryption	522
Configuring BitLocker	522
Configuring Network Unlock	528
Configuring Encrypting File System	530
Using EFS with an enterprise CA	531
Key and data recovery	532
Lesson summary	533
Lesson review	534

Practice exercises .....	535
Exercise 1: Install the File Server Resource Manager role service and create a shared folder	536
Exercise 2: Configure file quotas	541
Exercise 3: Configure file screen	545
Exercise 4: Configure file expiration	549
Exercise 5: Configure storage reports	552
Exercise 6: Install DFS	555
Exercise 7: Create a DFS namespace and add a namespace server 558	
Exercise 8: Configure DFS replication	560
Exercise 9: Install Enterprise CA	566
Exercise 10: Configure certificate templates	571
Exercise 11: Configure certificate enrollment	574
Exercise 12: Configure EFS-related Group Policies	578
Exercise 13: Configure BitLocker-related policies	582
Suggested practice exercises .....	584
Answers .....	585
Lesson 1	585
Lesson 2	586
Lesson 3	588

## **Chapter 10: Monitoring and auditing** **591**

Before you begin .....	591
Lesson 1: Monitoring servers .....	591
Configuring data collector sets	592
Managing alerts	597
Monitoring events with viewer	599
Configuring event subscriptions	603
Attaching event-driven tasks	606
Performing network monitoring	609
Lesson summary	612
Lesson review	613



Lesson 2: Advanced audit policies .....	614
Configuring advanced auditing	614
Using auditpol with auditing	619
Lesson summary	619
Lesson review	620
Practice exercises .....	621
Exercise 1: Configure data collector sets	621
Exercise 2: Collect data	626
Exercise 3: Configure alerts	628
Exercise 4: Prepare computers for event subscriptions	630
Exercise 5: Configure event subscriptions	632
Exercise 6: Configure network monitoring	636
Exercise 7: Using Message Analyzer	638
Exercise 8: Configure removable device auditing	641
Exercise 9: Configure logon auditing	645
Exercise 10: Configure expression-based audit policies	649
Exercise 11: Configure folder auditing	652
Suggested practice exercises .....	654
Answers .....	655
Lesson 1	655
Lesson 2	656
 <i>Index</i>	 659

---

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

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

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

# Introduction

---

When Microsoft 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 and Windows Server 2012 R2 operating systems with several years of on-the-job experience (managing other server operating systems as well as Windows Server 2012 and Windows Server 2012 R2) does and understands. The objectives don't cover everything that a Windows Server 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 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 R2* (Microsoft Press, 2014) 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, Windows 8.1 or the version available in Windows Server 2012 or Windows Server 2012 R2. You can use other virtualization software instead, such as VirtualBox or VMWare Workstation, but the practice setup instructions 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 or Windows 8.1, 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 R2 evaluation. You can download an evaluation edition of Windows Server 2012 R2 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 here.

This set of exercises contains abbreviated instructions for setting up the SYD-DC, MEL-DC, ADL-DC, and CBR-DC computers used in the practice exercises in all chapters of this training guide. To perform these exercises, first install Windows Server 2012 R2 Standard edition using the default configuration, setting the administrator password to **Pa\$\$w0rd**.

### Exercise 1: SYD-DC to function as a Windows Server 2012 R2 domain controller

1. Log on to the first computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password **Pa\$\$w0rd**.
2. Open an elevated PowerShell prompt and issue the following commands:  

```
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.10.10.10 -PrefixLength 24
Rename-Computer SYD-DC
Restart-Computer
```
3. Restart the computer and log back on using the Administrator account.
4. Open an elevated PowerShell prompt and issue the following command:  

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```
5. Open the Server Manager console. Click the Refresh icon.
6. Click on the Notifications icon and then click Promote This Server to Domain Controller.
7. On the Deployment Configuration page, choose Add a New Forest. Enter **Contoso.com** as the root domain name and then click Next.
8. On the Domain Controller Options page, configure the following settings and then click Next:
  - Forest Functional Level: **Windows Server 2012 R2**
  - Domain Functional Level: **Windows Server 2012 R2**
  - Domain Name System (DNS) Server: **Enabled**
  - Global Catalog: **Enabled**
  - DSRM Password: **Pa\$\$w0rd**
9. On the DNS Options page, click Next.
10. On the Additional Options page, click Next.

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

## Exercise 2: Prepare Active Directory Domain Server (AD DS)

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

```
Set-DNSClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.10.10.10
```

## Exercise 3: Prepare ADL-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the second computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password **Pa\$\$w0rd**.
3. Open an elevated PowerShell prompt and issue the following commands:  

```
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.10.10.20 -PrefixLength 24  
Set-DNSClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.10.10.10  
Rename-Computer ADL-DC  
Restart-Computer
```
4. After the computer restarts, log on again using the Administrator account.
5. Shut down the computer.

## Exercise 4: Prepare CBR-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the third computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password **Pa\$\$wOrd**.
3. Open an elevated PowerShell prompt and issue the following commands:

```
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.10.10.30 -PrefixLength 24
Set-DNSClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.10.10.10
Rename-Computer CBR-DC
Restart-Computer
```

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

## Exercise 5: Prepare MEL-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the third computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password **Pa\$\$wOrd**.
3. Open an elevated PowerShell prompt and issue the following commands:

```
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.10.10.40 -PrefixLength 24
Set-DNSClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 10.10.10.10
Rename-Computer MEL-DC
Restart-Computer
```

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

## Exercise 6: Checkpoint all virtual machines

1. Checkpoint all virtual machines. This is the state that they need to be in prior to performing exercises. Checkpoints were termed snapshots in prior versions of Hyper-V.

## Acknowledgments

---

I'd like to thank the following people for their dedication and help in getting this book written: Karen Szall , Troy Mott, Telmo Sampaio and Christina Rudloff.

## Errata, updates, & book support

---

We've made every effort to ensure the accuracy of this book. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

*<http://aka.ms/TG411R2>*

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at [mspinput@microsoft.com](mailto:mspinput@microsoft.com).

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *<http://support.microsoft.com>*.

## We want to hear from you

---

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

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

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

## Stay in touch

---

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

# 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: Maintaining Group Policy Object **241**
- Lesson 2: Managing the application of Group Policy **253**

## Before you begin

---

To complete the practice exercises in this chapter:

- You need to have deployed computers SYD-DC, MEL-DC, and ADL-DC, as described in the Introduction, using the evaluation edition of Windows Server 2012 R2.

## Lesson 1: Maintaining Group Policy Object

---

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.



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.

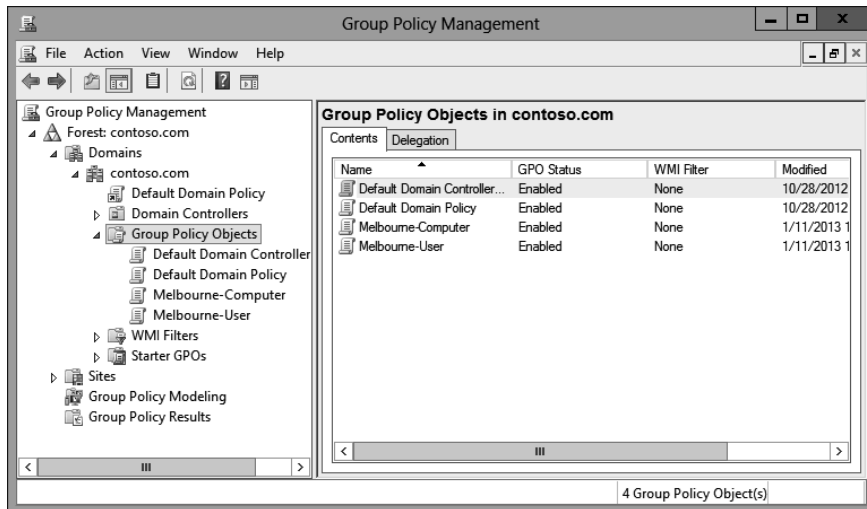


FIGURE 5-1 GPMC

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.

```

Administrator: Windows PowerShell
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter       :
DisplayName      : Default Domain Policy
DomainName       : contoso.com
Owner            : CONTOSO\Domain Admins
Id               : 31b2f340-016d-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 2/11/2014 7:10:18 PM
ModificationTime : 2/11/2014 7:21:40 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 3, SysVol Version: 3
WmiFilter       :
DisplayName      : Melbourne-Users
DomainName       : contoso.com
Owner            : CONTOSO\Domain Admins
Id               : 544d784e-8fe9-4e8e-bcec-fbf0a7e5a02c
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 2/18/2014 4:38:55 AM
ModificationTime : 2/18/2014 4:38:54 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter       :
DisplayName      : Default Domain Controllers Policy
DomainName       : contoso.com
Owner            : CONTOSO\Domain Admins
Id               : 6ac1786c-016f-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 2/11/2014 7:10:18 PM
ModificationTime : 2/18/2014 4:38:42 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 2, SysVol Version: 2
WmiFilter       :

PS C:\Users\Administrator> get-gpo -all_

```

**FIGURE 5-2** Output of the Get-GPO cmdlet

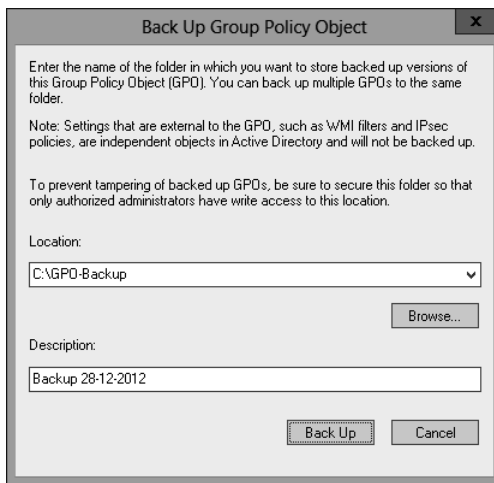
Backing up a GPO enables you to create a copy of a GPO as it exists at a specific point in time. A user must have read permission on a GPO to back it up. When you back up a GPO, the backup version of the GPO is incremented. It is good practice to back up GPOs prior to editing them so that if something 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. MDOP provides the ability to use GPO versioning as well as other advanced functionality.

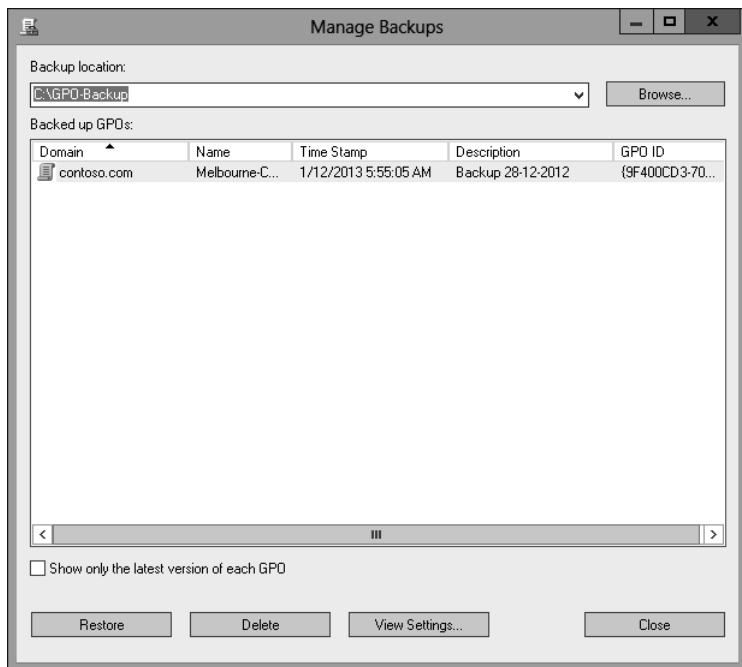
To back up a GPO, perform the following steps:

1. Open the GPMC.
2. 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.



**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 restore.

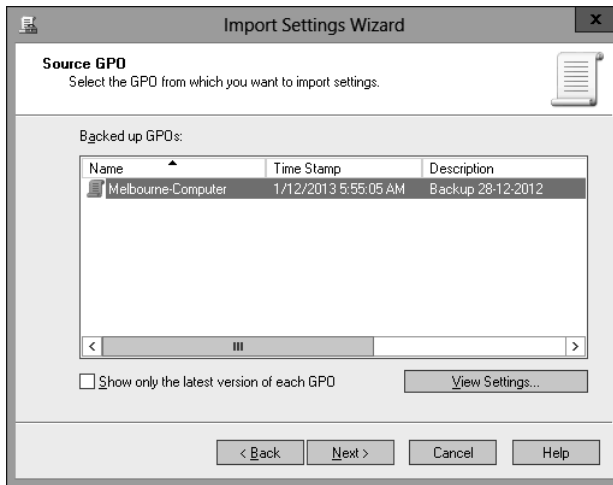


**FIGURE 5-4** Restoring a GPO from backup

## 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:

1. 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:

1. Right-click the GPO that you want to copy and click Copy.
2. Right-click the location that you want to copy the GPO to and click Paste.
3. 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

## Fixing GPO problems

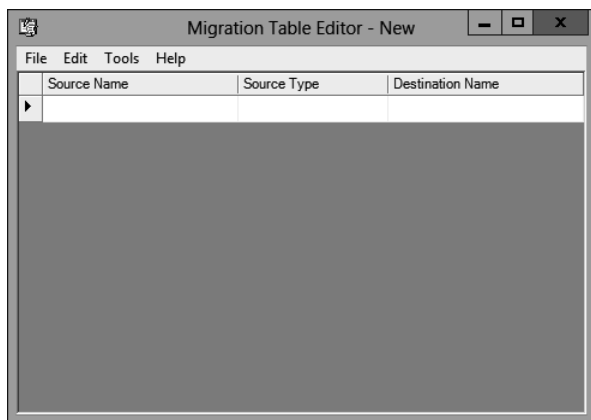
Windows Server 2012 and Windows Server 2012 R2 include command line utilities that allow you to repair GPO after you perform a domain rename or recreate default GPOs. If you need to recreate the default GPOs for a domain, use the DCGPOFix.exe command. If you perform

a domain rename, you can use the GPFixup.exe command to repair name dependencies in GPOs and Group Policy links.

## Migrate Group Policy Objects

When moving GPOs between domains or forests, you need to ensure that any domain-specific 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 domains
- Permission to perform Group Policy Modeling analysis at the OU or domain level
- Permission to view
- Group Policy Results information at the OU, or domain level
- Windows 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.

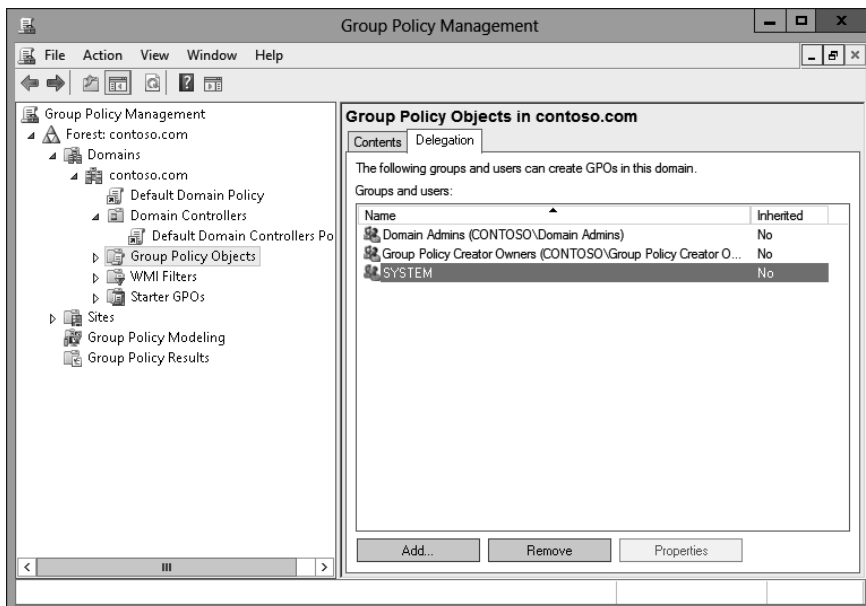


FIGURE 5-8 Group Policy permissions

## 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



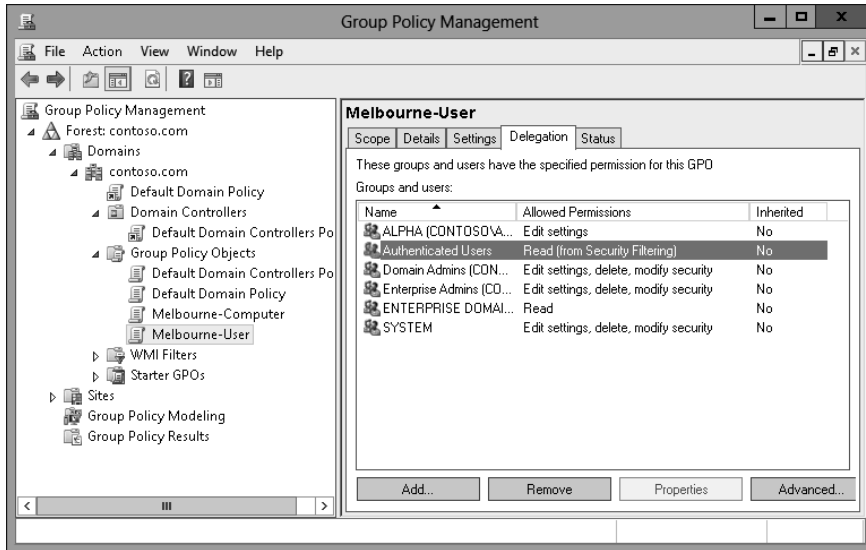


FIGURE 5-9 Delegating permissions

## 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.

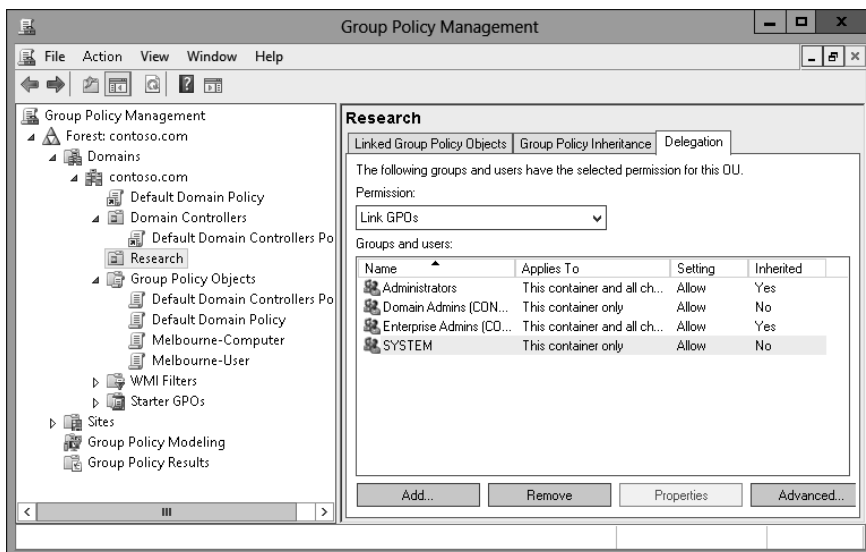


FIGURE 5-10 Delegating link GPO permission

## 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.

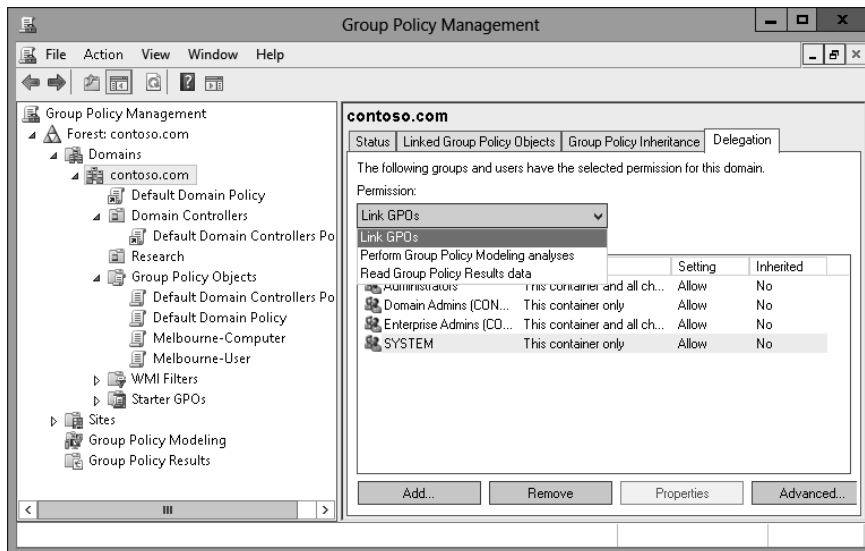


FIGURE 5-11 Delegating Group Policy Modeling and Group Policy Results permissions

## 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. Non-administrative 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
  - C. 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
5. 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

- B. 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.

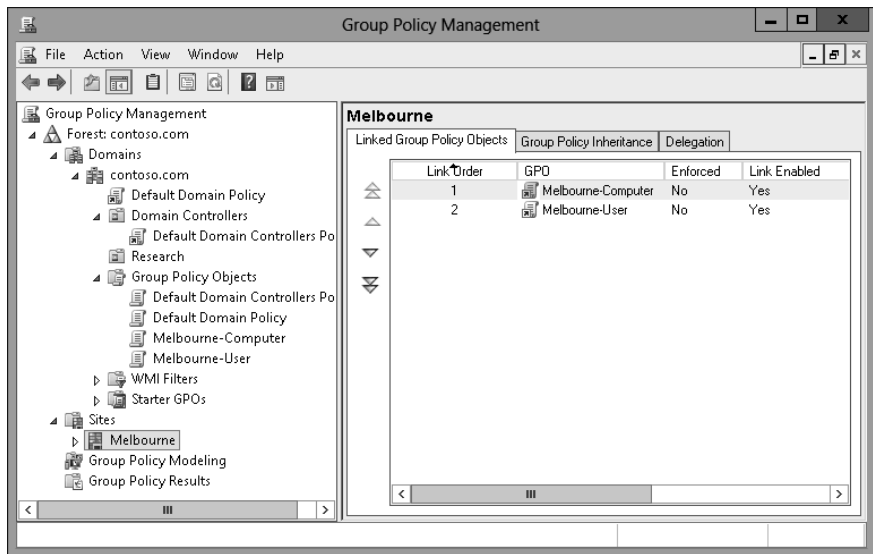


FIGURE 5-12 GPO link order

- **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.

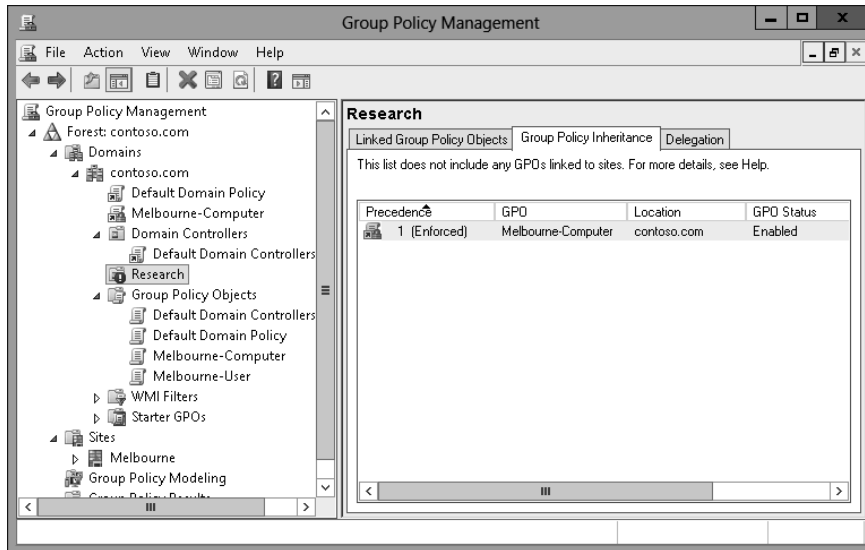
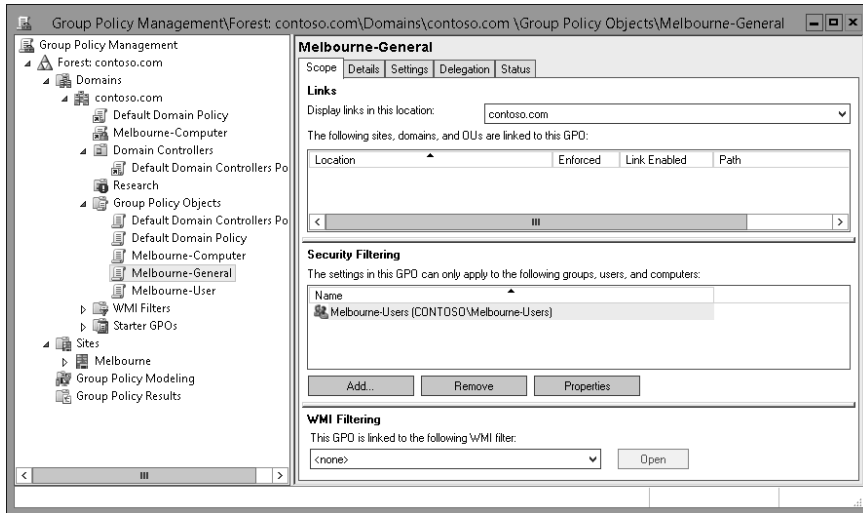


FIGURE 5-13 Override versus Enforced

## 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.

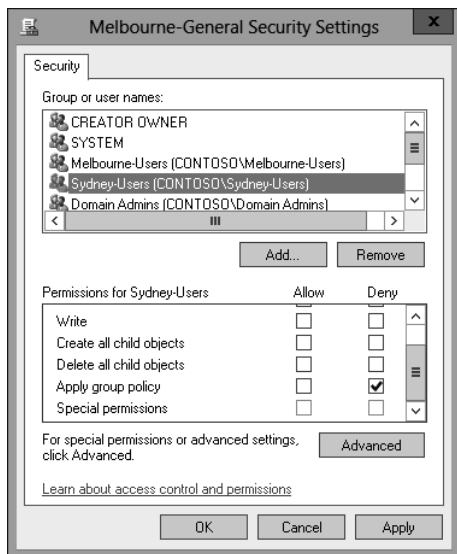


FIGURE 5-15 Security filtering

### ✓ 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).

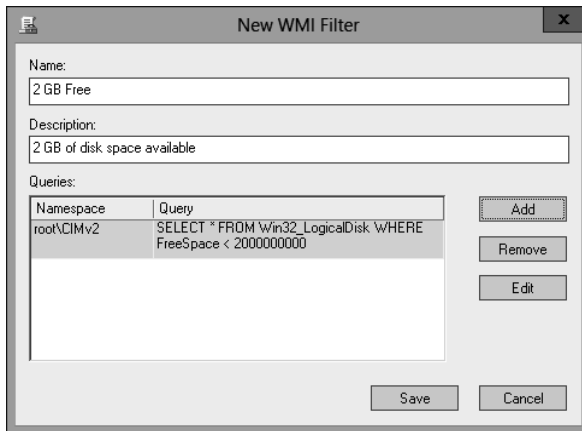


FIGURE 5-16 Creating a WMI filter

### **MORE INFO** WMI QUERIES

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

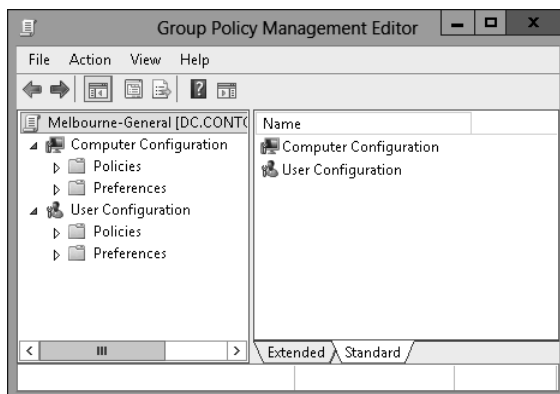


FIGURE 5-17 GPO structure



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.

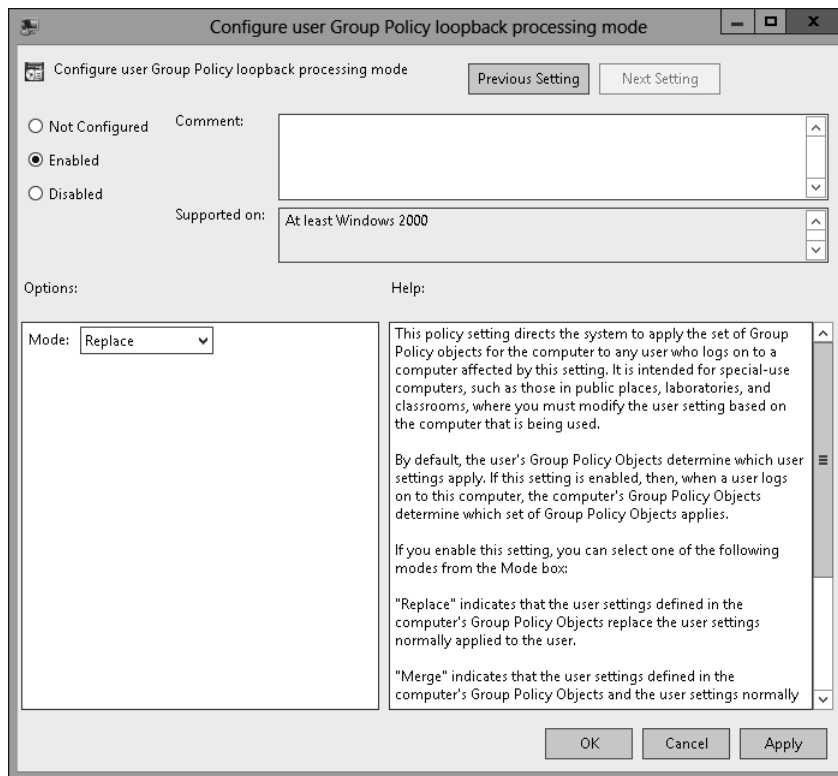
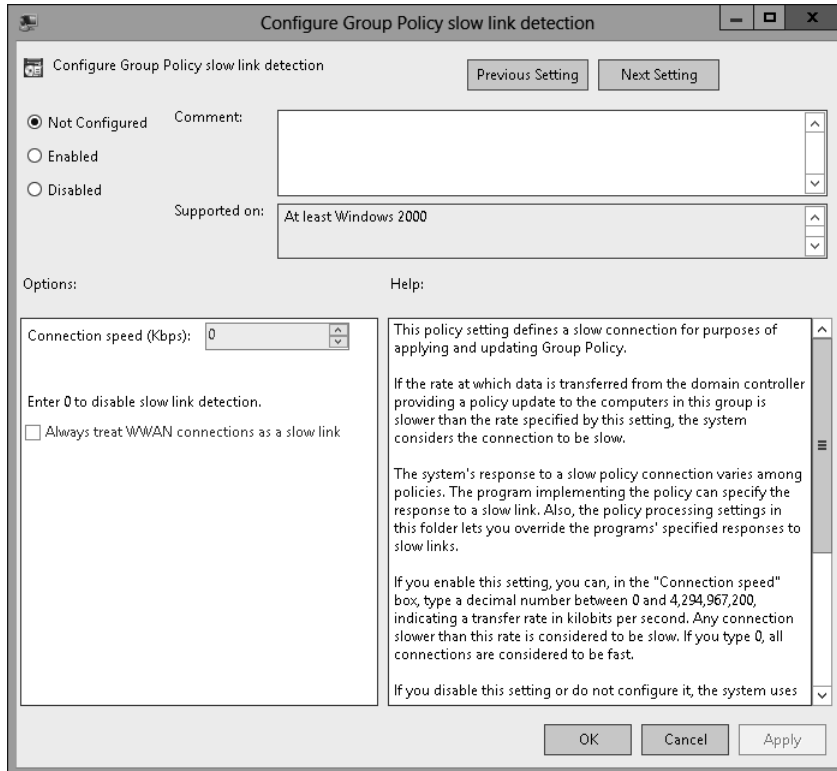


FIGURE 5-18 Loopback processing policy



*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. When a slow link is detected, registry settings from administrative templates, security policies, EFS recovery policy, and IPsec policies are applied. Policies related to application deployment, scripts, folder redirection, and disk quotas will not be applied.



**FIGURE 5-19** Slow link detection

## Group Policy caching

Group Policy caching reduces the amount of time taken to process Group Policy during computer startup and user sign on. Rather than retrieve the Group Policies that apply to the computer from a domain controller when a computer starts up or a user signs on, the client will use a cached copy of the last Group Policies downloaded from the domain controller. After this initial application of the cached policies during startup and user sign on, policies will

be retrieved and applied normally from a domain controller. You enable Group Policy caching by configuring the Configure Group Policy Caching policy as shown in Figure 5-20. This policy is located under Computer Configuration\Policies\Administrative Templates\System\Group Policy. Group Policy caching applies only to computers running Windows Server 2012 R2, Windows 8.1, or Windows RT 8.1.

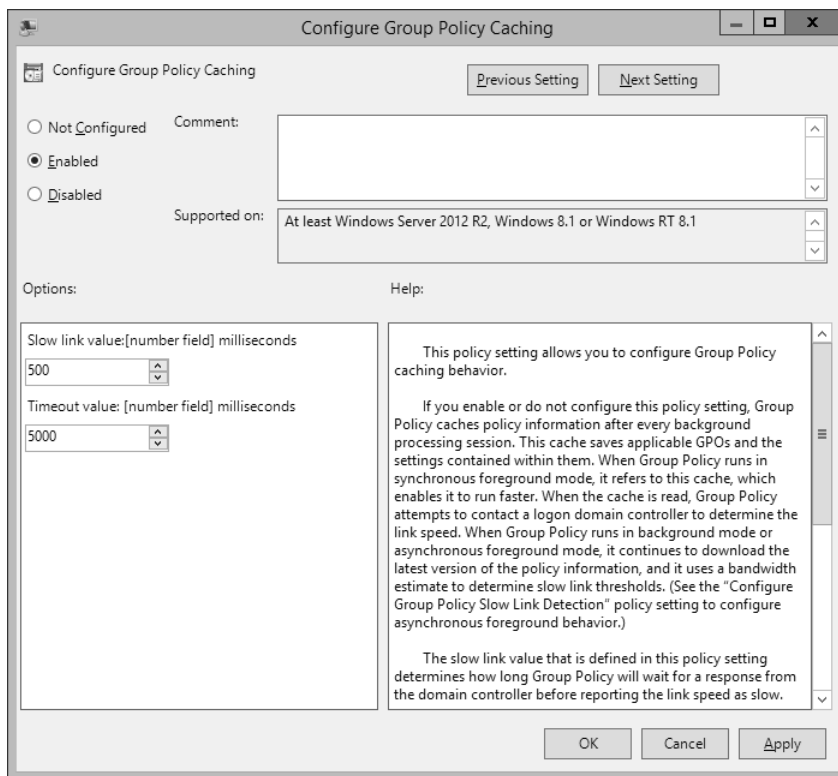


FIGURE 5-20 Configure Group Policy caching

### **MORE INFO GROUP POLICY CACHING**

You can learn more about Group Policy caching by reading this blog post by Group Policy MVP Darren Mar-Elia at <http://sdmsoftware.com/group-policy-blog/group-policy/understanding-group-policy-caching-in-windows-8-1/>.

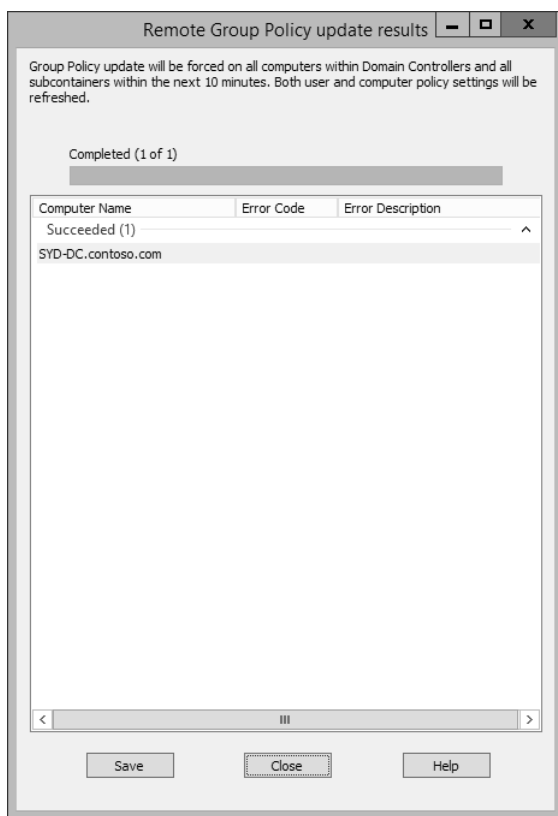
## Force Group Policy update

Windows Server 2012 and later support remote Group Policy update. Remote Group Policy update allows you to force a remote computer to perform a Group Policy update without having to sign on to the computer and run the GPOupdate.exe command. Remote Group

Policy update will work on clients running the Windows Vista and later operating system. Remote Group Policy requires the following firewall rules be enabled on clients:

- Remote Scheduled Tasks Management (RPC)
- Remote Scheduled Tasks Management (RPC-EPMAP)
- Windows Management Instrumentation (WMI-In)

You can run remote Group Policy update from the Group Policy Management Console by right-clicking on a container or OU. An update will run on all computers within the container or OU as well as on any computer accounts stored within child OUs. Figure 5-21 shows the result of running remote Group Policy update on the Domain Controllers container. You can also use the `Invoke-GPUdate Windows PowerShell cmdlet` to trigger a remote Group Policy update. The advantage of the Windows PowerShell cmdlet is that you can target a specific computer rather than all computer accounts in an OU.



**FIGURE 5-21** Remote Group Policy update

## **MORE INFO USING REMOTE GPUPDATE**

You can learn more about remote Group Policy update at <https://blogs.technet.com/b/grouppolicy/archive/2012/11/27/group-policy-in-windows-server-2012-using-remote-gpupdate.aspx>.

## 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.
- Group Policy caching allows cached copies of GPOs that apply to users and computers to be applied at startup and sign on.
- Remote Group Policy update allows you to force a Group Policy update on a remote client. Remote Group Policy update requires that 3 firewall rules be configured on clients.

## 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
  - B. 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 an evaluation version of Windows Server 2012 R2. You should also have access to virtual machines SYD-DC, MEL-DC, CBR-DC, and ADL-DC, the setup instructions for which are described in the Introduction. You should ensure that you have a checkpoint of these virtual machines that you can revert to at the end of the practice exercises. You should revert the virtual machines to this initial state prior to beginning these exercises.

## Exercise 1: Prepare GPOs, security groups, and OUs

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

1. Sign in to SYD-DC with the Contoso\Administrator account.
2. 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 5-22.

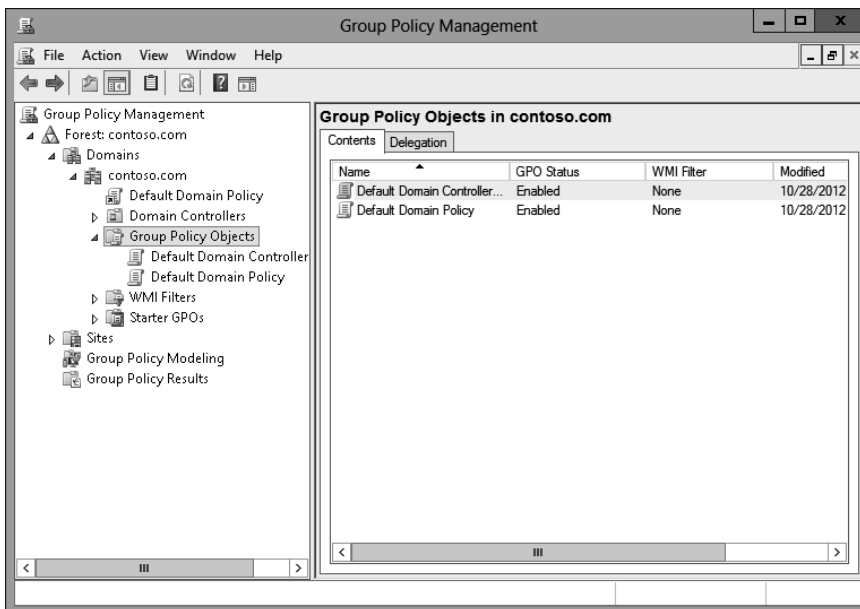
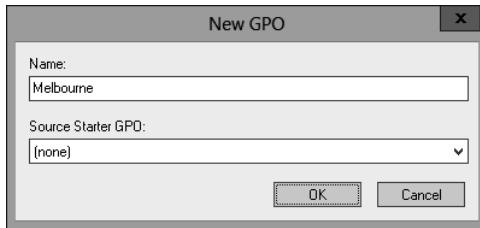


FIGURE 5-22 Clicking Group Policy Objects

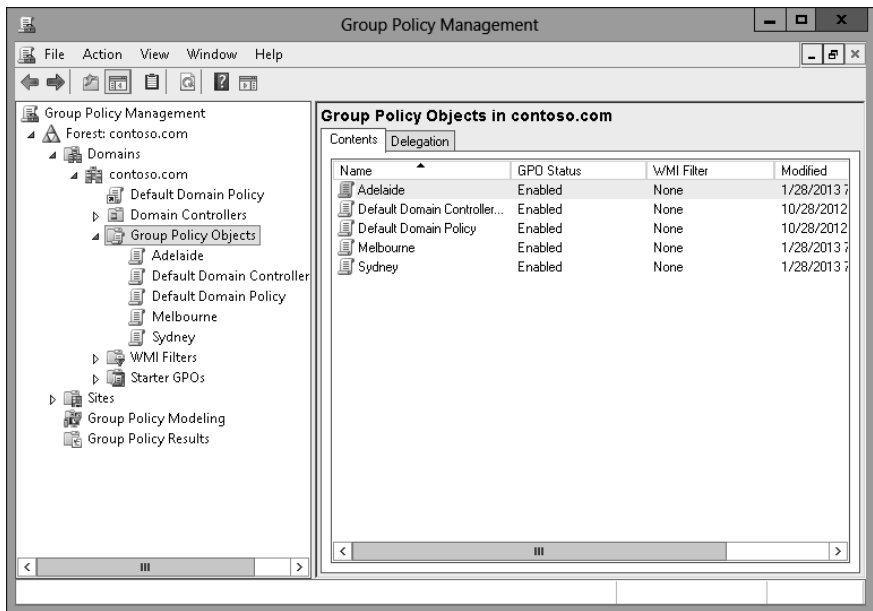


4. On the Action menu, click New.
5. In the New GPO dialog box, type **Melbourne**, as shown in Figure 5-23, and click OK.



**FIGURE 5-23** New GPO dialog box

6. 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 5-24.



**FIGURE 5-24** 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 5-25.

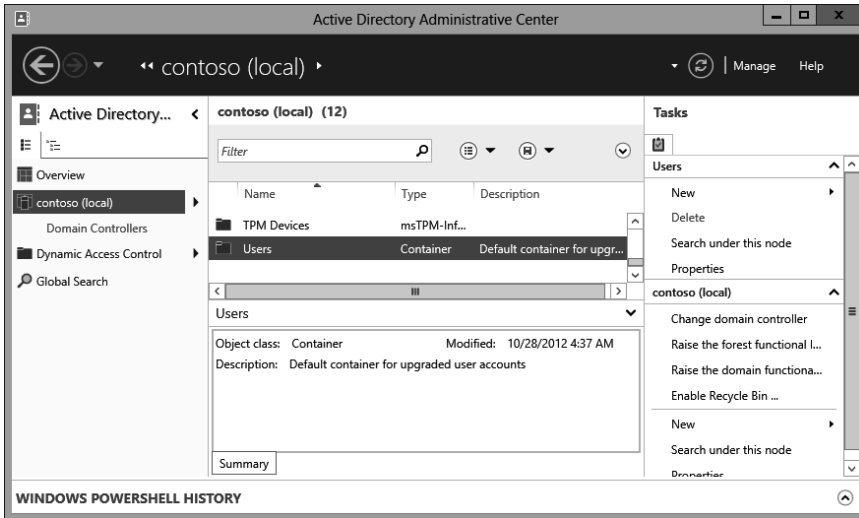


FIGURE 5-25 Users container

10. In the Tasks pane, click New, and click Group.
11. In the Create Group dialog box, type the group name **Melbourne\_GPO\_Editors**; click Security, Global, and Protect From Accidental Deletion, as shown in Figure 5-26; then click OK.

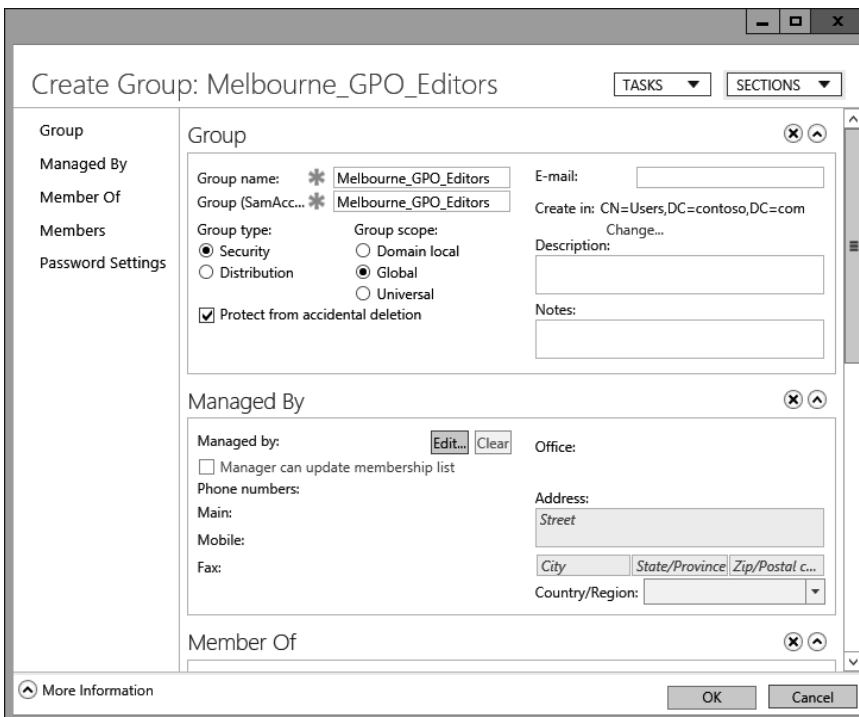


FIGURE 5-26 Creating a security group

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, type the name **Melbourne\_Computers**, as shown in Figure 5-27, and click OK.

**FIGURE 5-27** 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 perform several Group Policy management-related tasks. To complete this exercise, perform the following steps:

1. In the GPMC, click the Melbourne GPO.
2. When the Melbourne GPO is selected, click the Delegation tab, as shown in Figure 5-28.

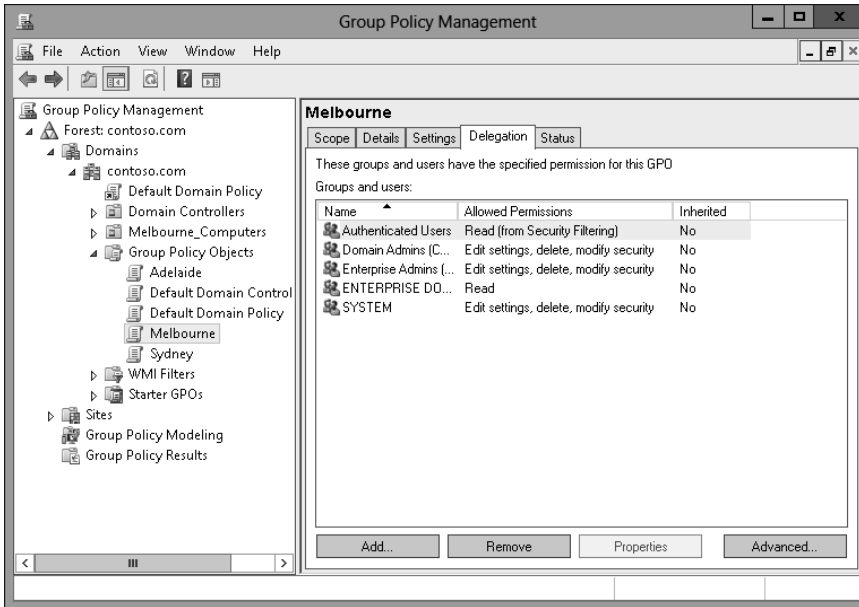


FIGURE 5-28 OU Delegation tab

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 5-29, and click OK.

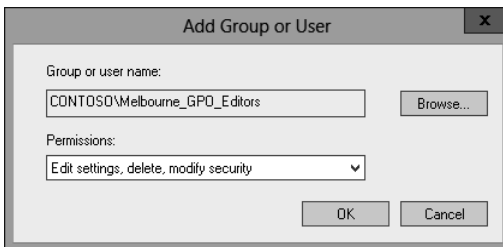
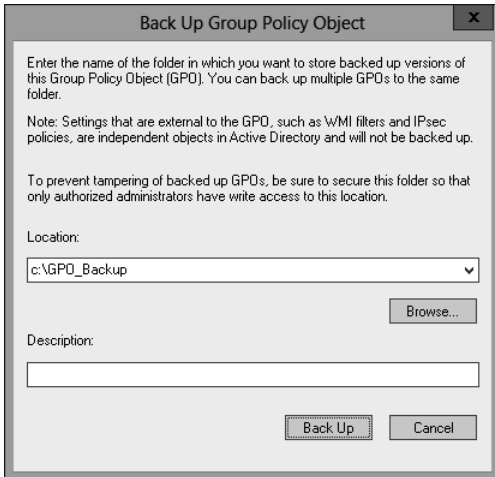


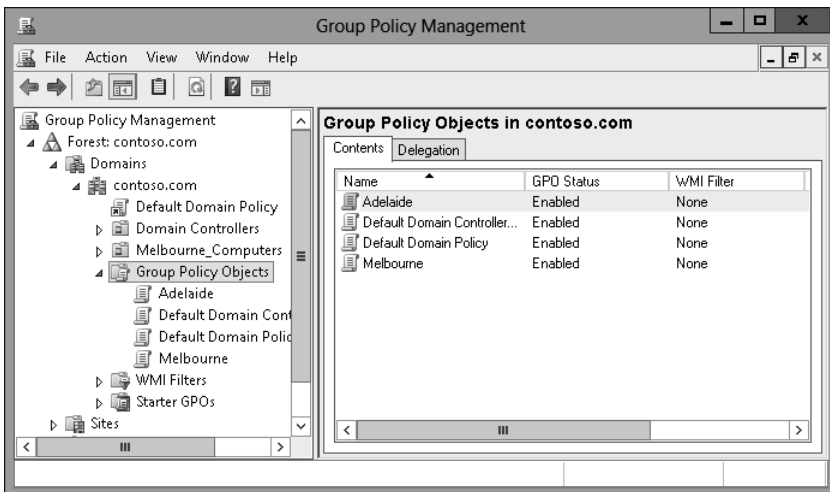
FIGURE 5-29 OU Delegation tab

6. In the GPMC, click the Sydney GPO.
7. On 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 5-30, and click Back Up.



**FIGURE 5-30** Back Up Group Policy Object dialog box

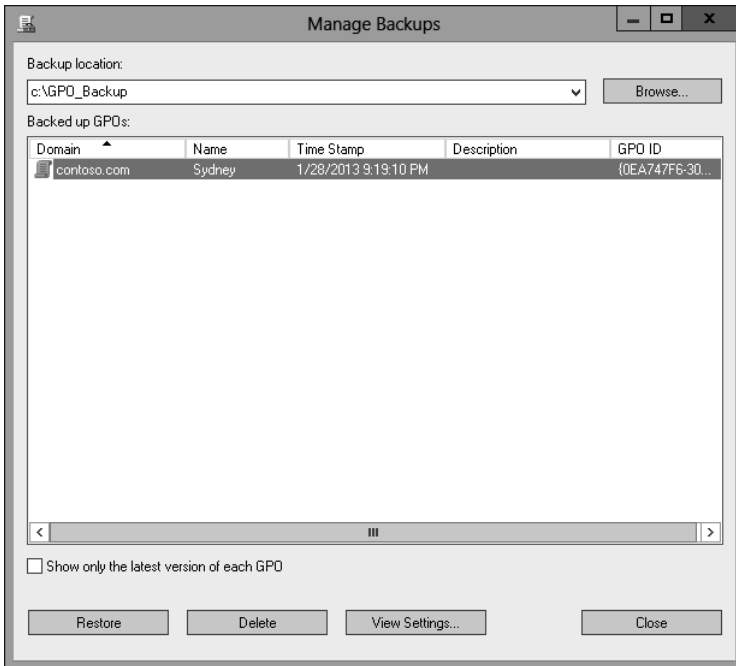
9. In the Backup dialog box, click OK.
10. In the GPMC, click the Sydney GPO.
11. On the Action menu, click Delete.
12. In the Group Policy Management dialog box, click Yes.
13. Verify that the Sydney GPO is no longer listed under Group Policy Objects, as shown in Figure 5-31.



**FIGURE 5-31** Verify deleted GPO

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

15. In the Manage Backups dialog box, click the Sydney GPO, as shown in Figure 5-32, and click Restore.



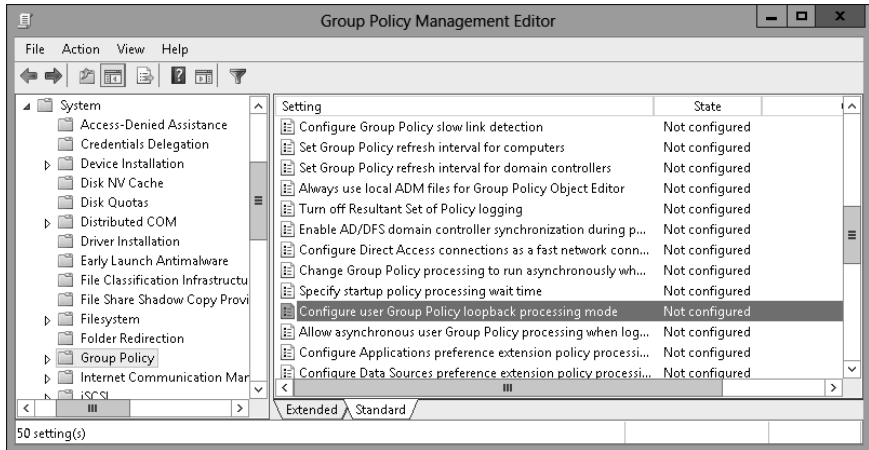
**FIGURE 5-32** Manage Backups dialog box

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

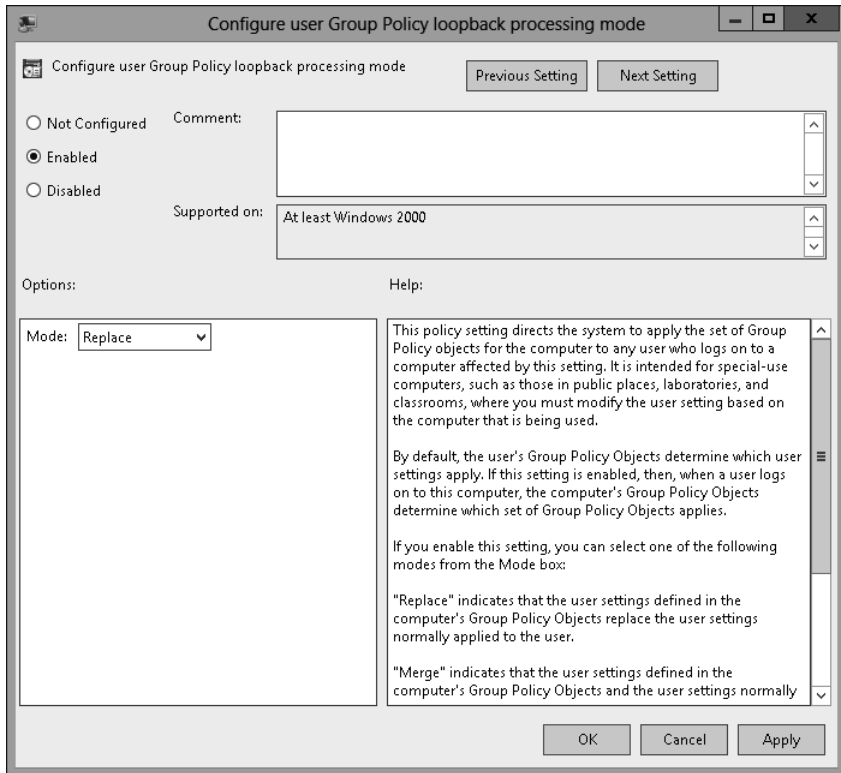
In this exercise, you perform Group Policy management tasks related to Group Policy processing. To complete this exercise, perform the following steps:

1. In the GPMC, click the Adelaide GPO.
2. On 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 5-33.



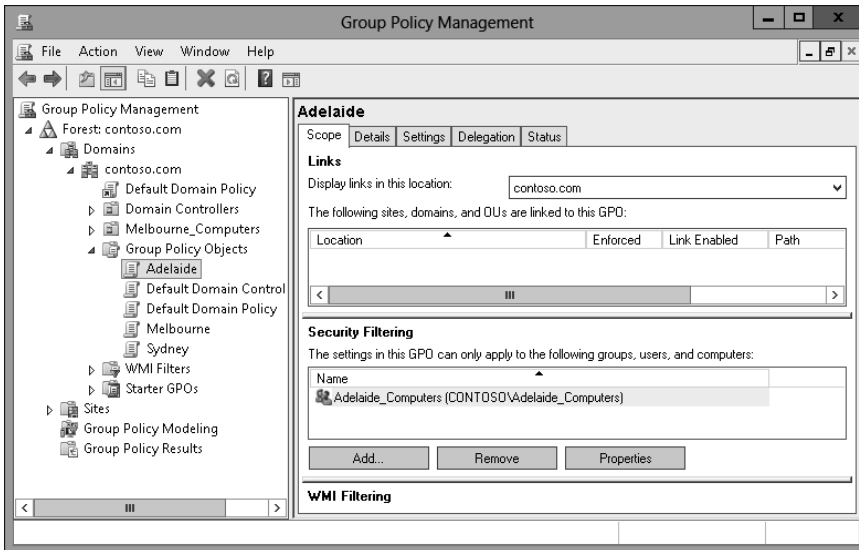
**FIGURE 5-33** Select Group Policy loopback processing mode policy

4. On the Action menu, click Edit.
5. In the Configure User Group Policy Loopback Processing Mode dialog box, click Enabled. Set the mode to Replace, as shown in Figure 5-34, and click OK.



**FIGURE 5-34** Configure replace mode

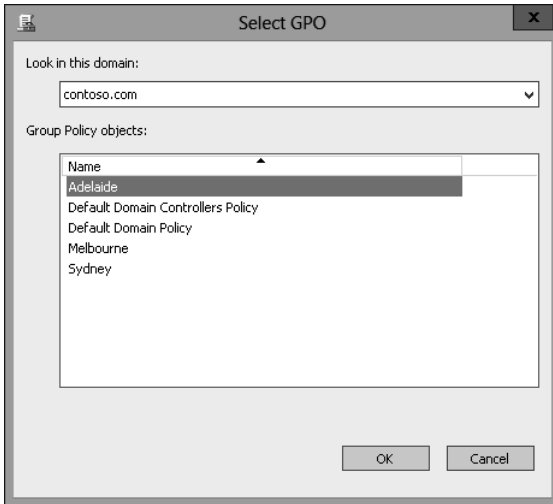
6. Close the Group Policy Management Editor.
7. In the GPMC, click the Adelaide GPO, and click the Scope tab.
8. On the Scope tab, click the Authenticated Users group, and click Remove.
9. In the Group Policy Management dialog box, click OK.
10. Under Security Filtering, click Add.
11. In the Select 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 5-35.



**FIGURE 5-35** Configuring security filtering properties

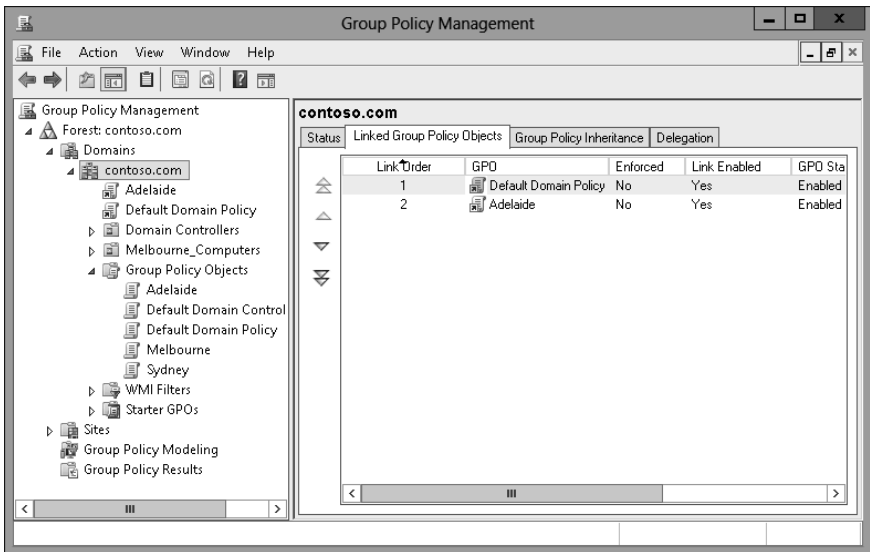
13. In the GPMC, click Contoso.com, and click the Linked Group Policy Objects tab.
14. Click Contoso.com. On the Action menu, click Link An Existing GPO.
15. In the Select GPO dialog box, click Adelaide, as shown in Figure 5-36, and click OK.





**FIGURE 5-36** 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 5-37.

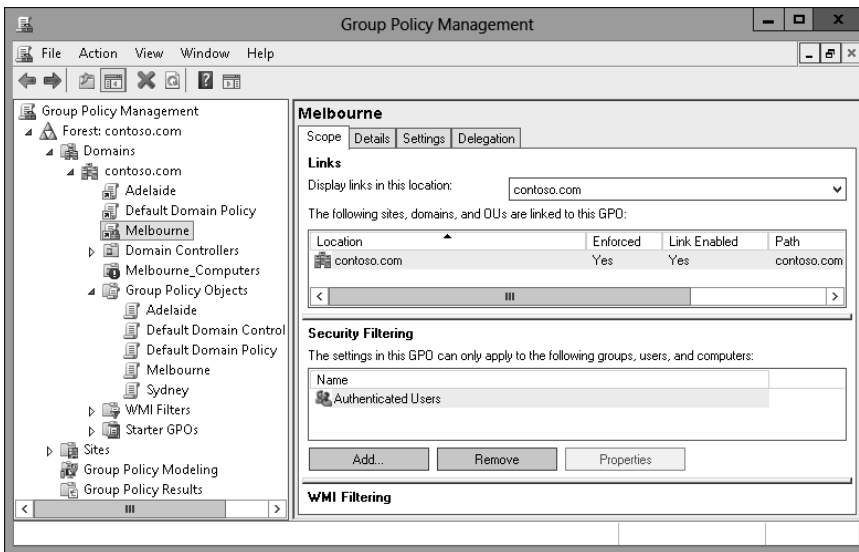


**FIGURE 5-37** GPOs linked to the domain

## 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. On the Action menu, click Block Inheritance.
3. In the GPMC, click Contoso.com.
4. On the Action menu, click Link An Existing GPO.
5. In the Select GPO dialog box, click Melbourne, and then click OK.
6. Click the Melbourne GPO under Contoso.com.
7. On 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 5-38.



**FIGURE 5-38** Block Inheritance and Enforced GPOs

9. In the GPMC, click the Group Policy Modeling node.
10. On the Action menu, click Group Policy Modeling Wizard.
11. On the Welcome page of the Group Policy Modeling Wizard, click Next.
12. On the Domain Controller Selection page, click This Domain Controller, and click SYD-DC.contoso.com. Click Next.
13. On 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 Filter Selection page matches Figure 5-39, and click Next.

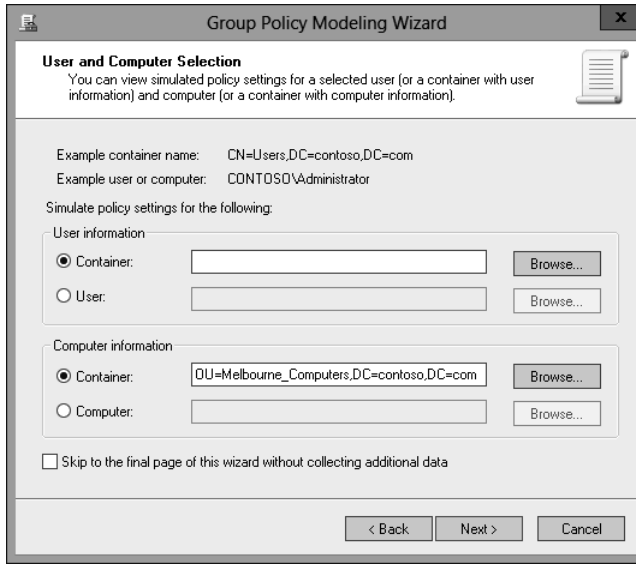


FIGURE 5-39 Group Policy Modeling Wizard

16. On 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 5-40, and that only the Melbourne GPO is listed.

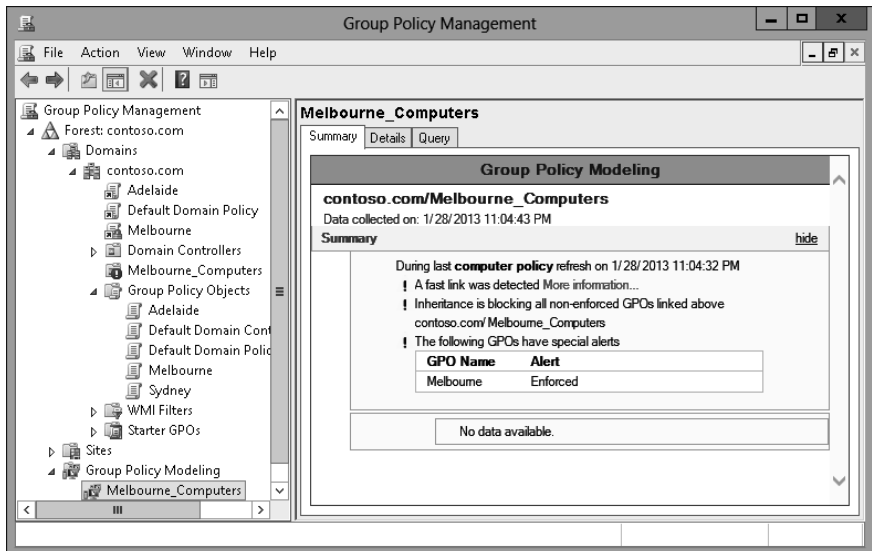


FIGURE 5-40 Group Policy Modeling results

## 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

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 and Windows Server 2012 R2 operating system.

## Lessons in this chapter:

- Lesson 1: Monitoring servers **591**
- Lesson 2: Configuring advanced audit policies **614**

## Before you begin

---

To complete the practice exercises in this chapter:

- You need to have deployed computers SYD-DC, MEL-DC, and ADL-DC, as described in the Introduction, using the evaluation edition of Windows Server 2012 R2.

## Lesson 1: Monitoring 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 learn how to configure data collector sets, manage alerts, monitor events, and perform network monitoring.



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

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

**Estimated lesson time: 45 minutes**

## Configuring data collector sets

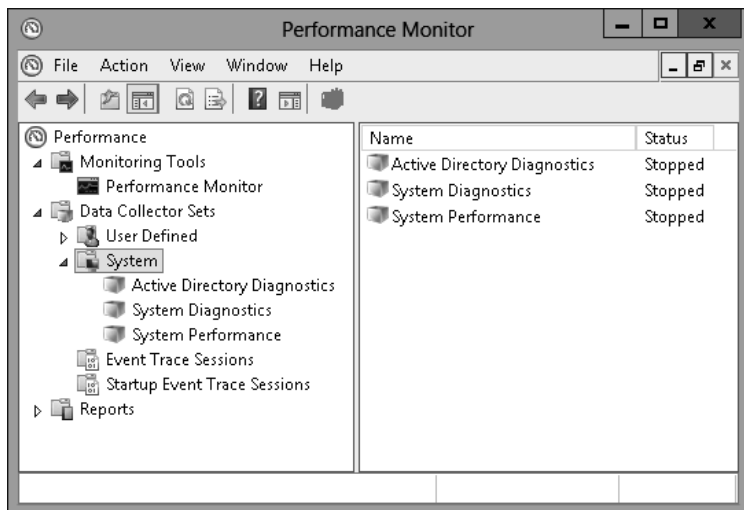


*Data collector sets* enable you to collect performance data, system configuration information, and statistics into a single file. You can use Performance Monitor or other third-party tools to analyze this information to make a determination about how well a server is functioning against an assigned 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 and Windows Server 2012 R2 include the following built-in data collector sets, as shown in Figure 10-1.

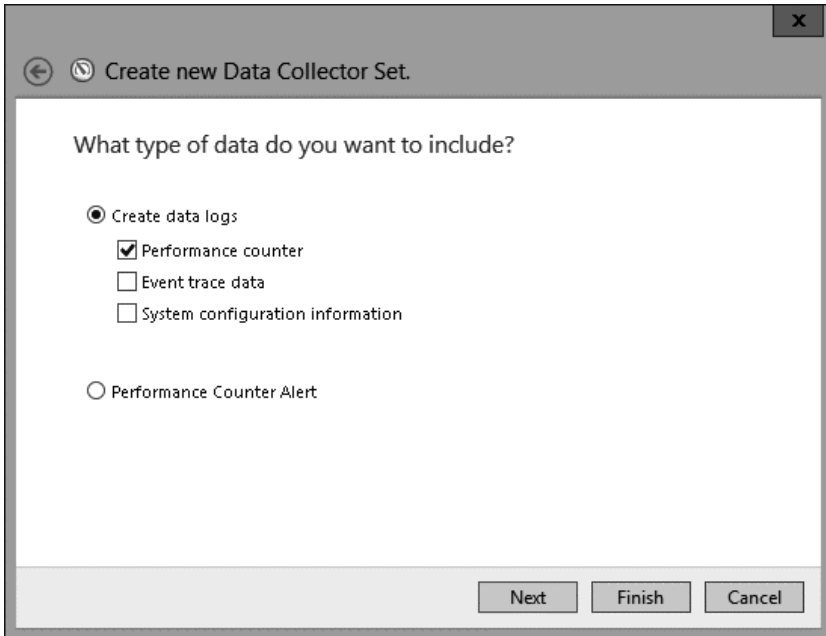


**FIGURE 10-1** Built-in data collector sets

- **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.

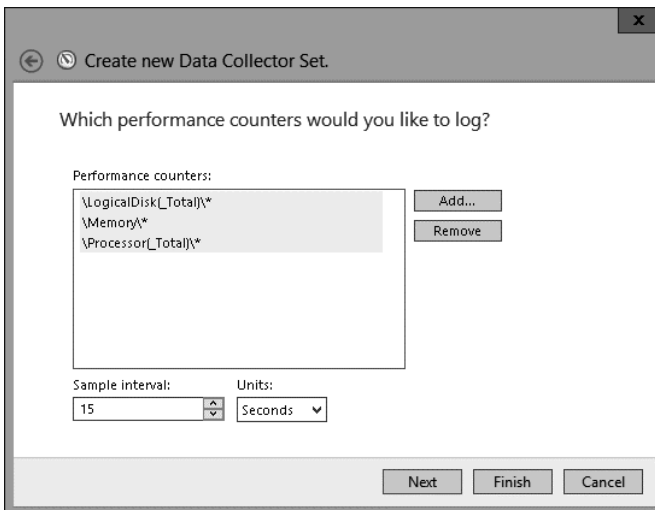
To create a data collector set, perform the following steps:

1. Open Performance Monitor from the Tools menu of the Server Manager console.
2. Expand Data Collector Sets.
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.



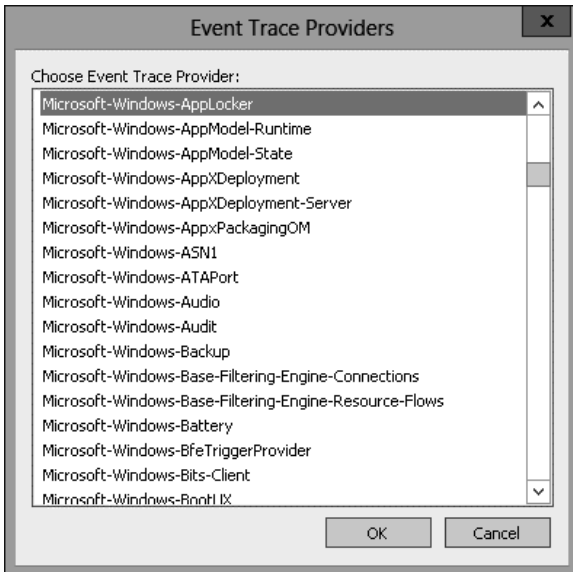
**FIGURE 10-2** Creating a new data collector set

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.



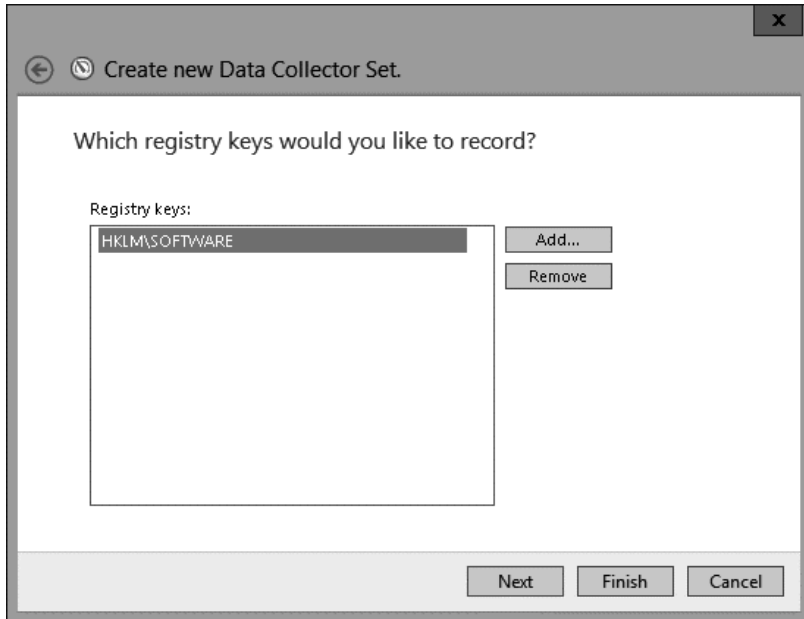
**FIGURE 10-3** Setting an interval for the data collector set

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 R2. 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.

You can schedule when a data collector set runs by configuring the Schedule tab of a data collector set's properties as shown in Figure 10-6.



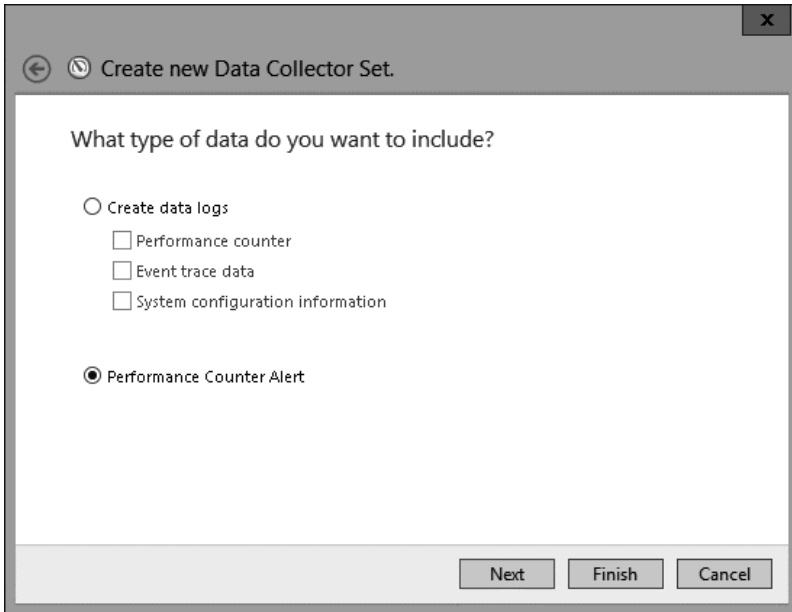
FIGURE 10-6 Configure data collector set schedule

### **MORE INFO** DATA COLLECTOR SETS

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

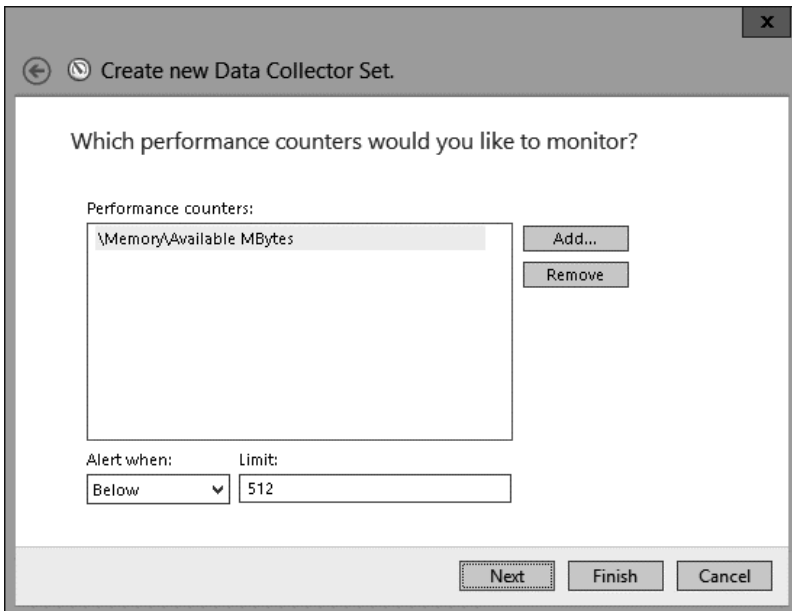
## Managing alerts

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 10-7.



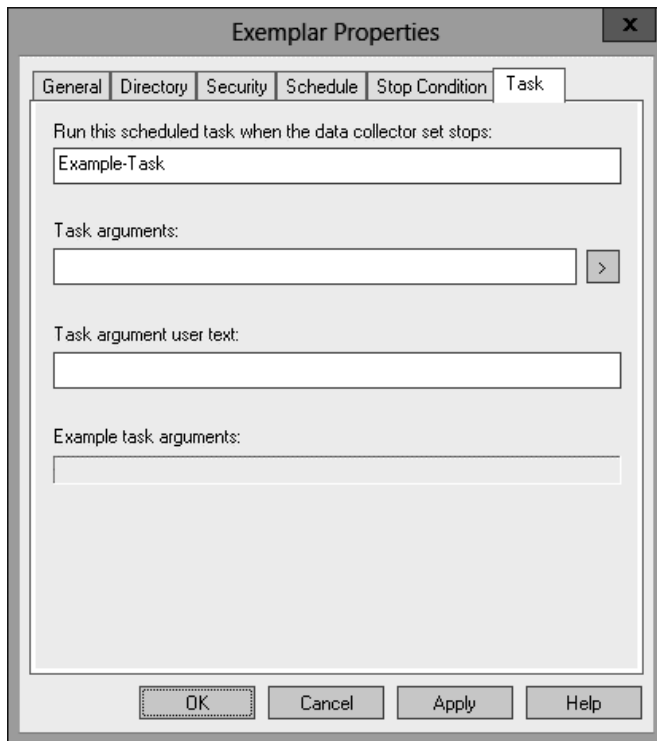
**FIGURE 10-7** Configuring the performance counter alert

You add the performance counter, threshold value, and whether the alert should be triggered if the value exceeds or falls below this value. Figure 10-8 shows an alert that is triggered when the amount of available memory falls below 512 megabytes.



**FIGURE 10-8** 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 10-9.



**FIGURE 10-9** Running a scheduled task

## Monitoring events with viewer

*Event Viewer*, shown in Figure 10-10, enables you to access recorded event information. The Windows Server 2012 and Windows Server 2012 R2 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.



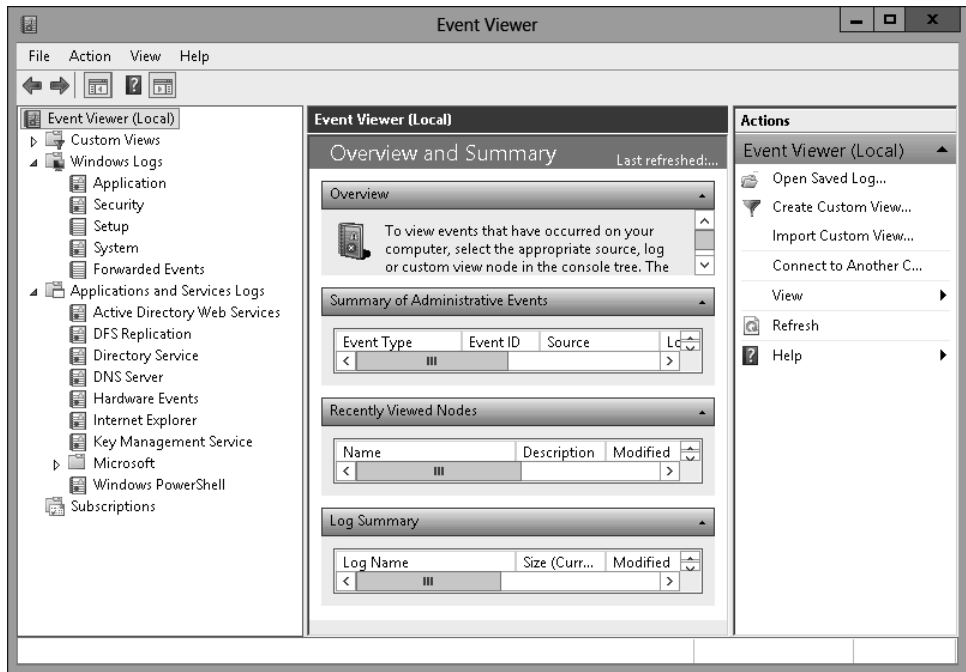


FIGURE 10-10 Event Viewer

### **MORE INFO** EVENT VIEWER

For more information about Event Viewer, consult the following TechNet article at <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:

1. Open Event Viewer and select the log that you want to filter.
2. Determine the properties of the event that you want to filter.
3. On the Actions pane, click Filter Current Log.
4. In the Filter Current Log dialog box, shown in Figure 10-11, specify the filter properties.

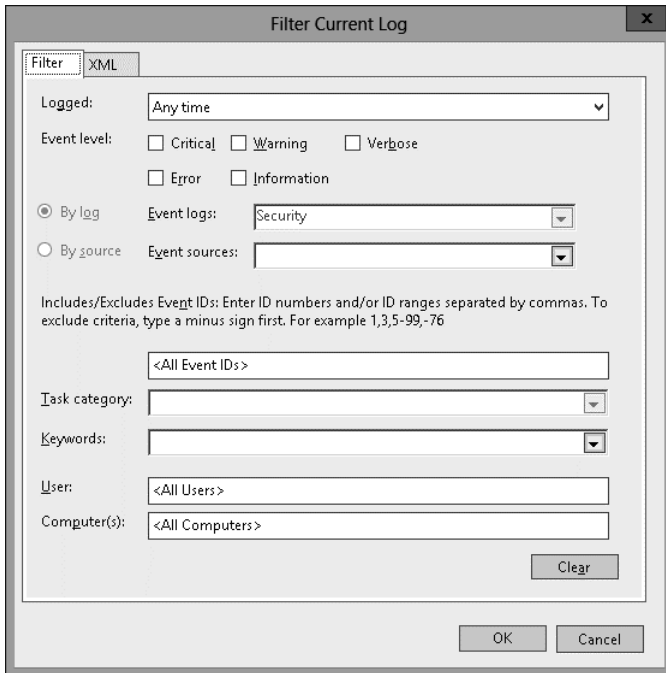


FIGURE 10-11 Specifying filter properties

## Event log views

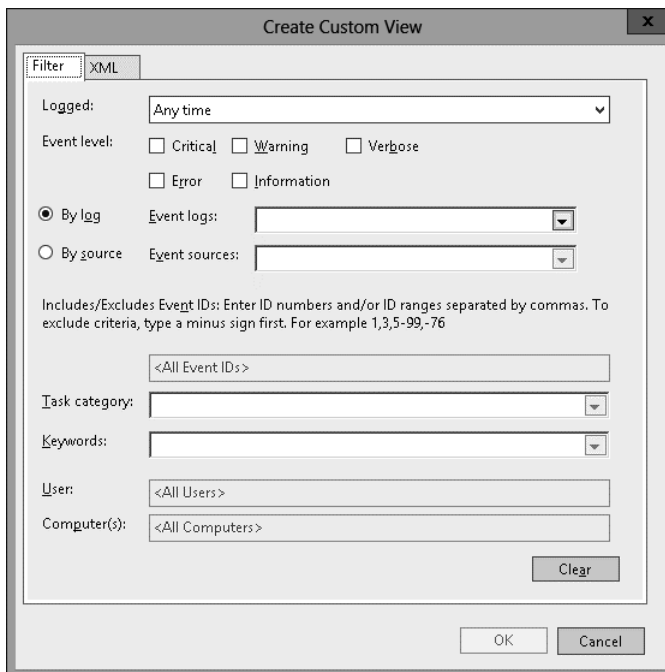
*Event log views* enable you to create customized views of events across any event log stored on a server, including events in the forwarded event log. Rather than looking through each event log for specific items of interest, you can create event log views that target only those specific items. Event 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.

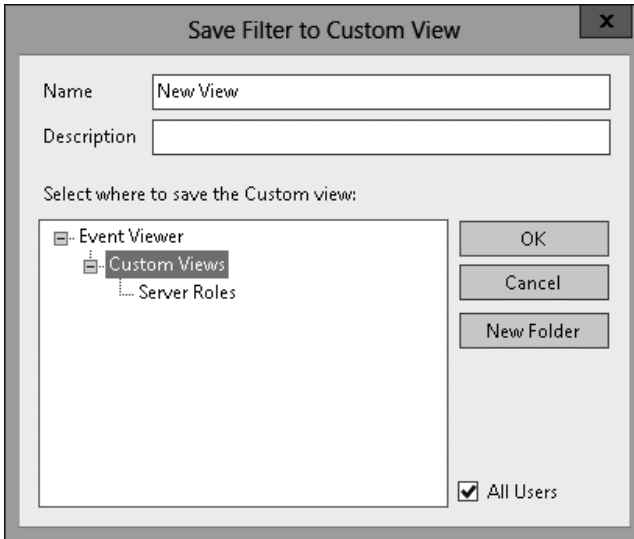
Creating an event log view is a similar process to creating a filter. The primary difference is that you can select events from multiple logs, and you give the event log view a name and choose a place to save it. To create an event log view, perform the following steps:

1. Open Event Viewer.
2. 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 10-12, 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 10-12** Creating a custom view

4. 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 10-13). Click OK.



**FIGURE 10-13** 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 and Windows Server 2012 R2.

#### **MORE INFO** EVENT LOG VIEWS

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

## Configuring 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.

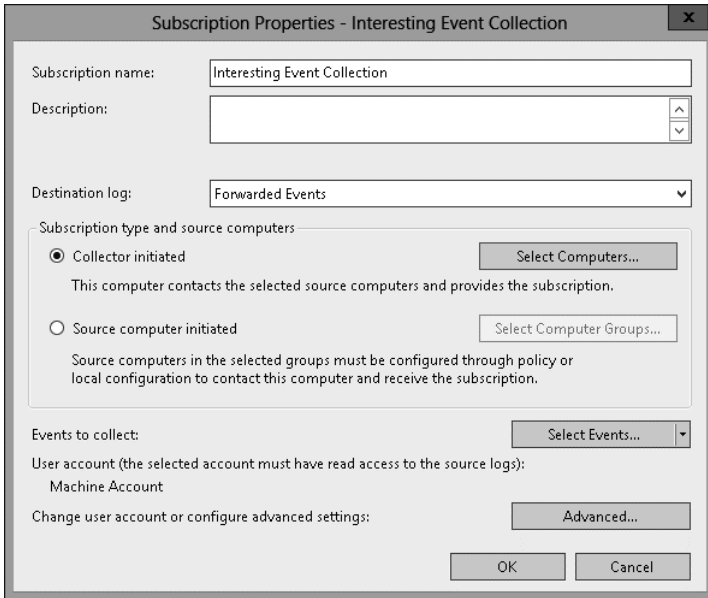
### **REAL WORLD OPERATIONS MANAGER**

**In large environments, you use Microsoft System Center 2012 R2 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 10-14, 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 10-14** Configuring a collector-initiated event subscription

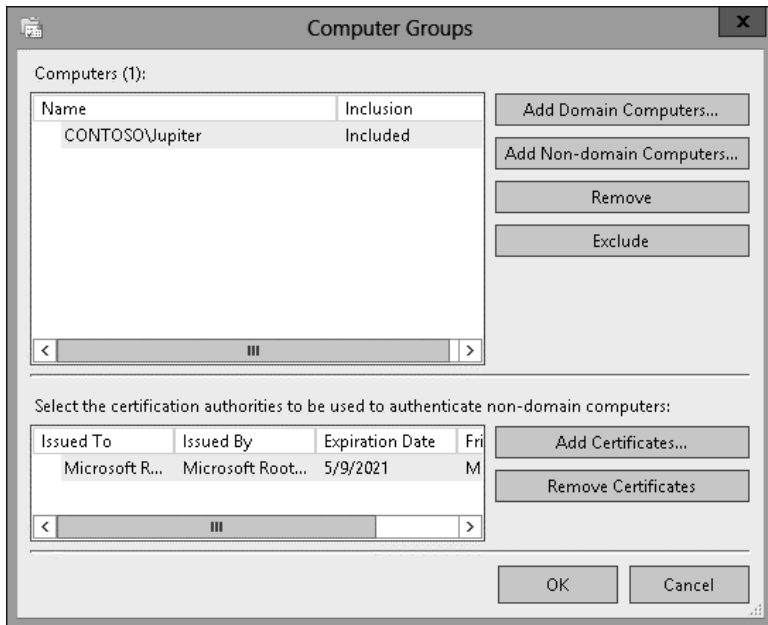
If you want to instead configure a source computer-initiated subscription, you need to configure the following group policies on the computers that will act as the event forwarders:

- **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 of 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 10-15.



**FIGURE 10-15** 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.

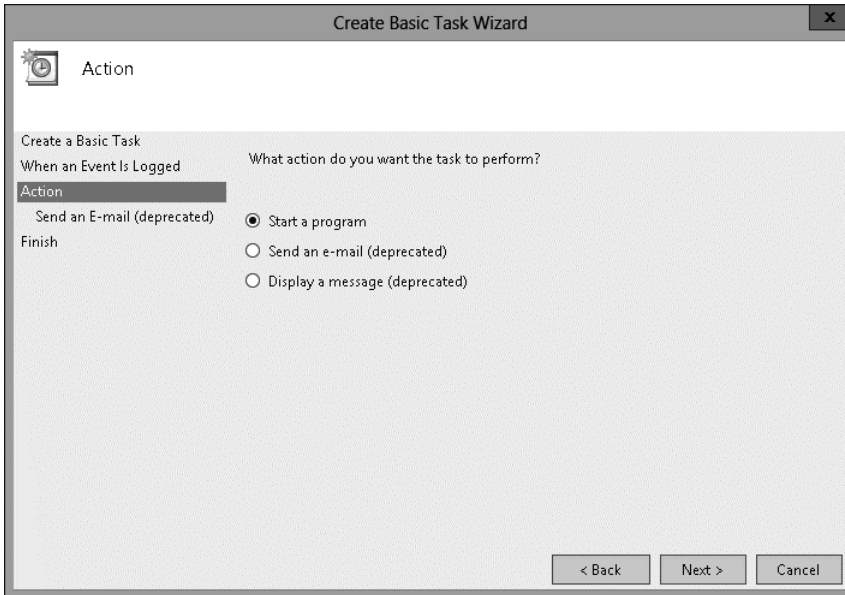
## Attaching event-driven tasks

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**.

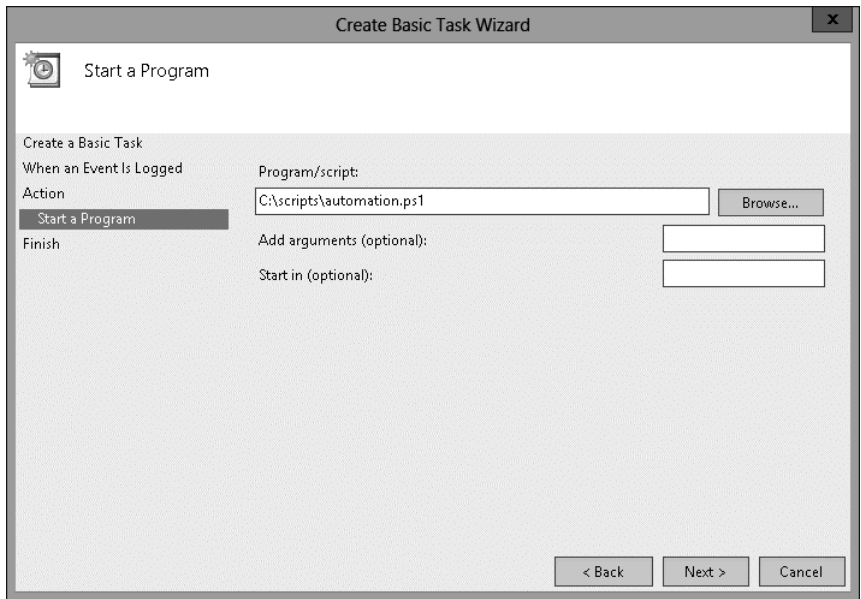
4. On the When An Event is Logged page, review the information about the event. This will list the log from which the event originates, the source of the event, and the event ID. Click Next.
5. On the Action page, shown in Figure 10-16, you can choose the task to perform. The Send An E-Mail and Display A Message tasks are deprecated, and you get an error if you try to create a task using these actions. Click Next.



**FIGURE 10-16** Attaching a task to a specific event

6. On the Start A Program page, shown in Figure 10-17, specify the program or script that should be automatically triggered as well as additional arguments.





**FIGURE 10-17** 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 10-18.

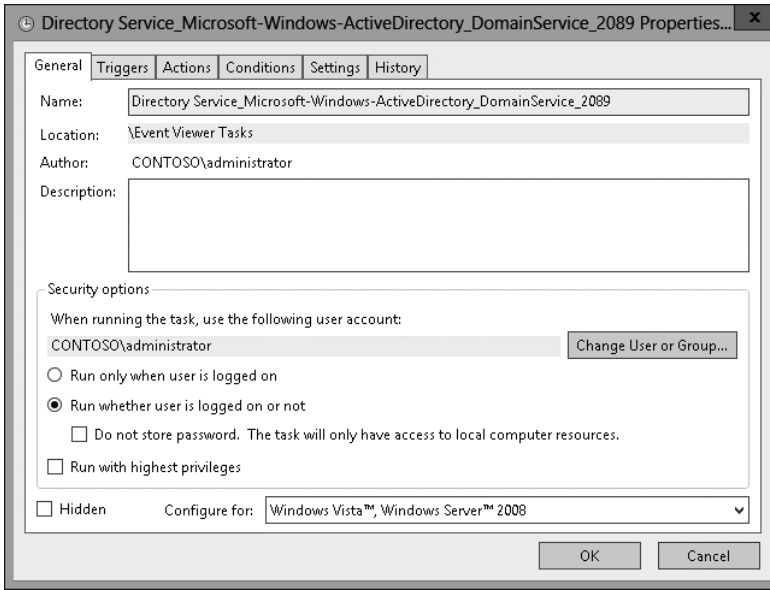


FIGURE 10-18 Run your task if the user is logged on or off

### **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.

## Performing 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 and Windows Server 2012 R2:

- Resource Monitor
- Message Analyzer



## Resource Monitor

*Resource Monitor* enables you to monitor how a computer running the Windows Server 2012 and Windows Server 2012 R2 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 10-19.

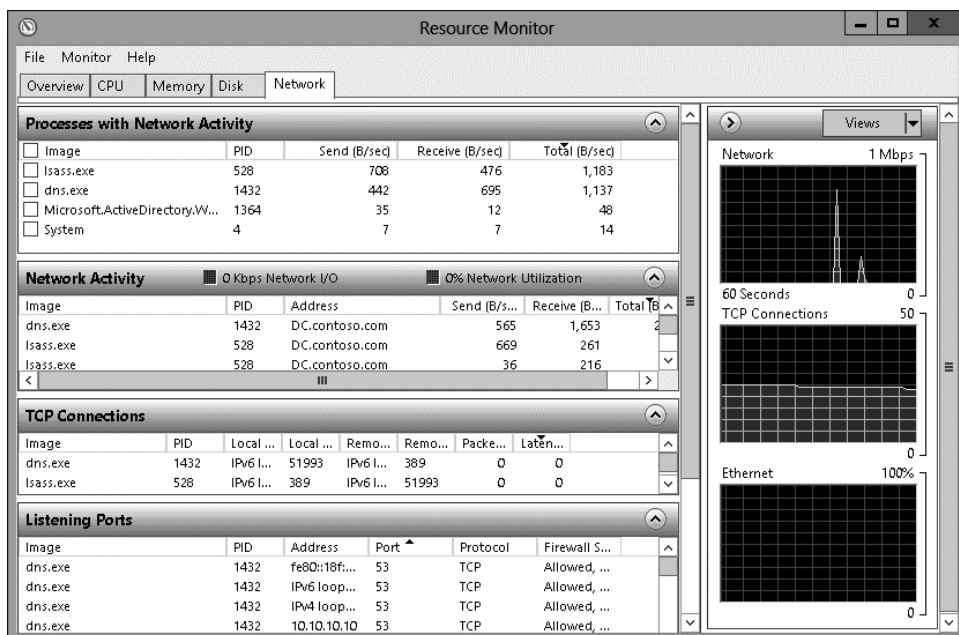


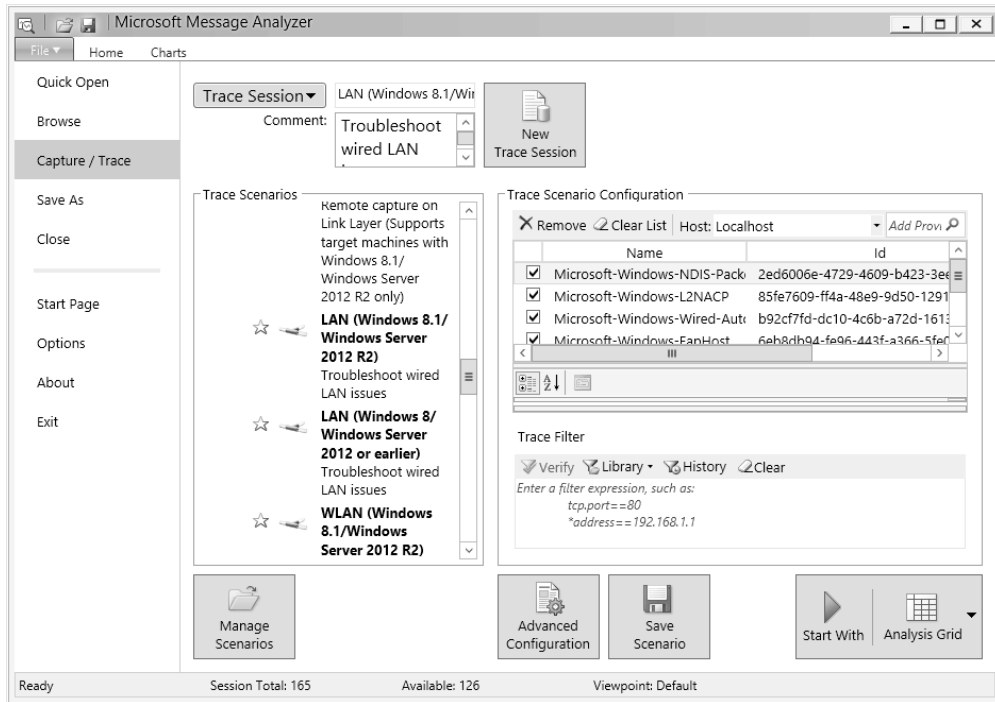
FIGURE 10-19 Resource Monitor Network tab

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 10-20, enables you to capture traffic on local area network (LAN) interfaces.



**FIGURE 10-20** 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 10-21. By applying appropriate filters, you can locate network traffic that has specific characteristics, such as using a particular TCP port, source, or destination address.

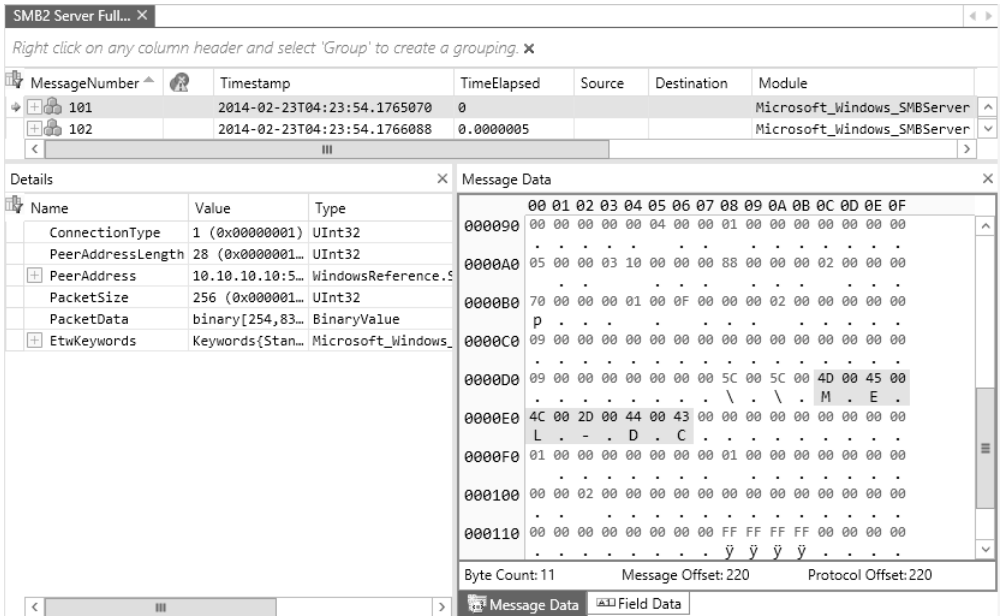


FIGURE 10-21 Message Analyzer

**MORE INFO MESSAGE ANALYZER**

You can find out more about Microsoft Message Analyzer by consulting the Microsoft Message Analyzer Operating Guide at <http://technet.microsoft.com/en-us/library/jj649776.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 R2 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
  - B. Resource Monitor
  - C. Message Analyzer
  - D. Data collector set
3. Which of the following tools can you use to capture and analyze network traffic?
  - A. Data collector set
  - B. Message Analyzer
  - C. Resource Monitor
  - D. Task Manager
4. You are configuring event log subscriptions. Computer MEL-DC 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 MEL-DC 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 MEL-DC?
  - 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.

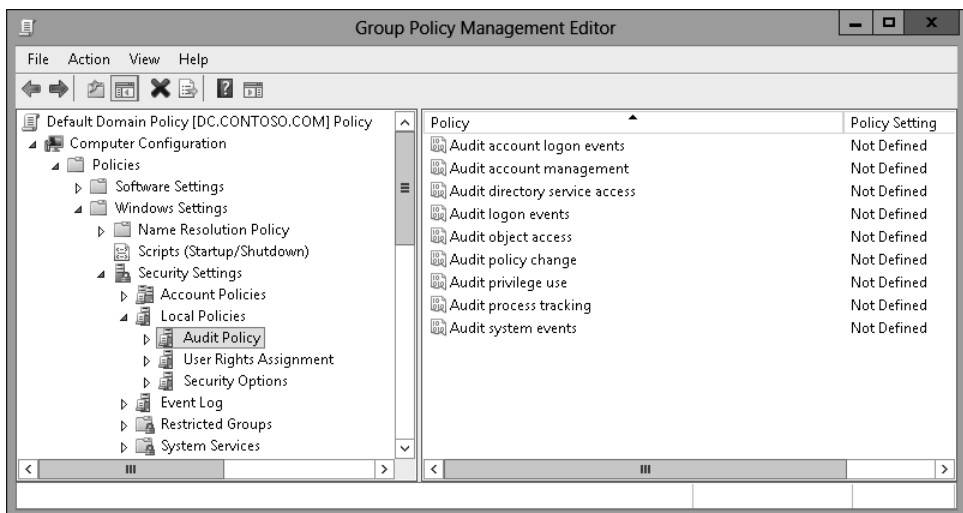
**After this lesson, you will be able to:**

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

**Estimated lesson time: 45 minutes**

### Configuring 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 10-22. 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 10-22** 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 10-23.

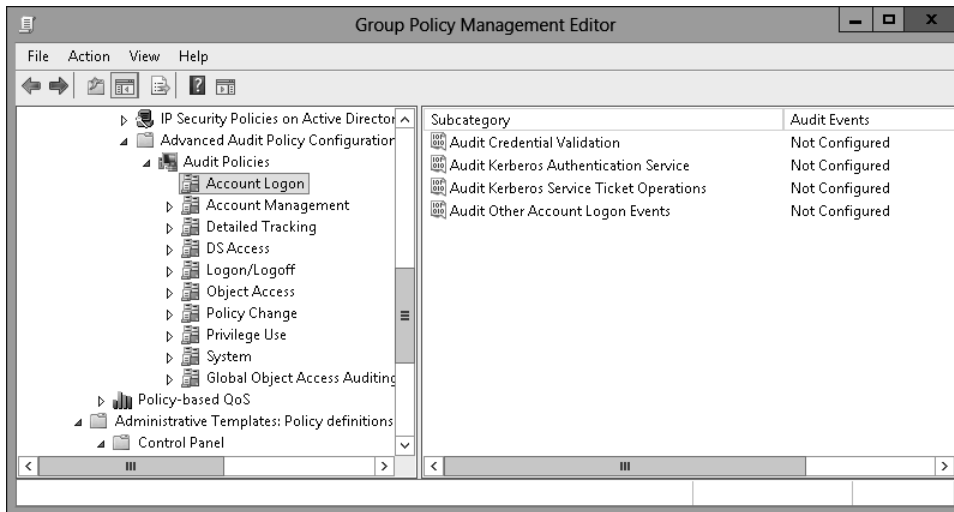


FIGURE 10-23 Advanced audit policies

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**

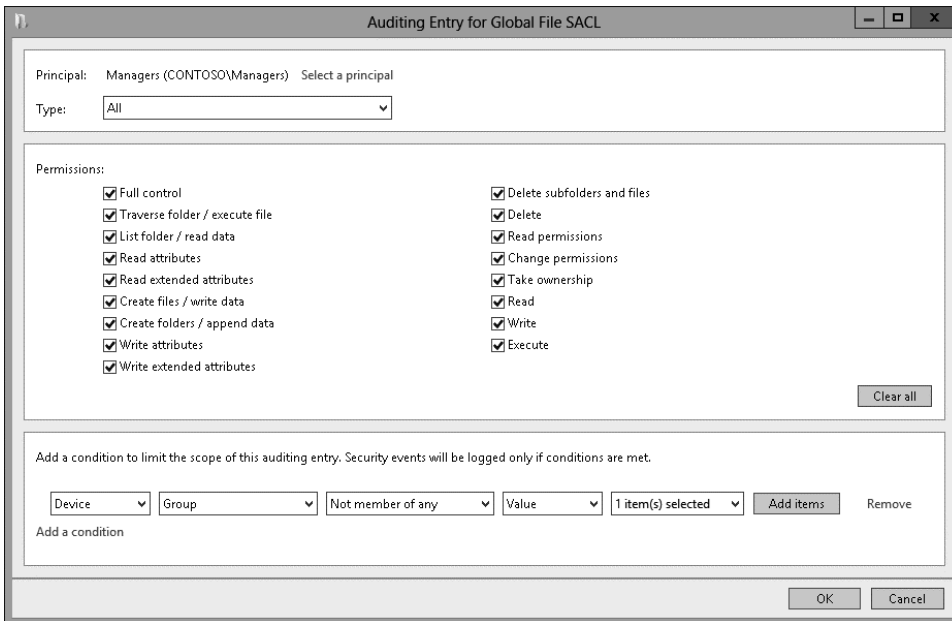
Determine what you want to audit first and then enable the policies to audit that type of activity. A mistake that many administrators make is that they aren't entirely sure what they should be auditing, so they audit everything. They become frustrated with the process because the auditing events that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

## Implementing 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 10-24 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 10-24** 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 10-25. 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 10-25** 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 R2 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](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-level 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 R2?
  - A. `Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable`
  - B. `Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable`
  - C. `Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable`
  - D. `Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable`
2. 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 R2. Which of the following commands should you use to accomplish this goal?
  - A. `Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable`
  - B. `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`
3. 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`
  - B. `Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable`
  - C. `Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable`
  - D. `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`
  - B. `Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable`
  - C. `Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable`
  - D. `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 R2. You should also have access to virtual machines SYD-DC, MEL-DC, CBR-DC, and ADL-DC, the setup instructions for which are described in the Introduction. You should ensure that you have a checkpoint of these virtual machines that you can revert to at the end of the practice exercises. You should revert the Virtual Machines (VMs) to this initial state prior to beginning these exercises.

### Exercise 1: Configure data collector sets

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

1. Start SYD-DC, and sign on as CONTOSO\Don\_Funk.
2. On SYD-DC, click Performance Monitor in the Tools menu of Server Manager.
3. In the Performance Monitor console, expand the Performance\Data Collector Sets\User Defined, as shown in Figure 10-26.

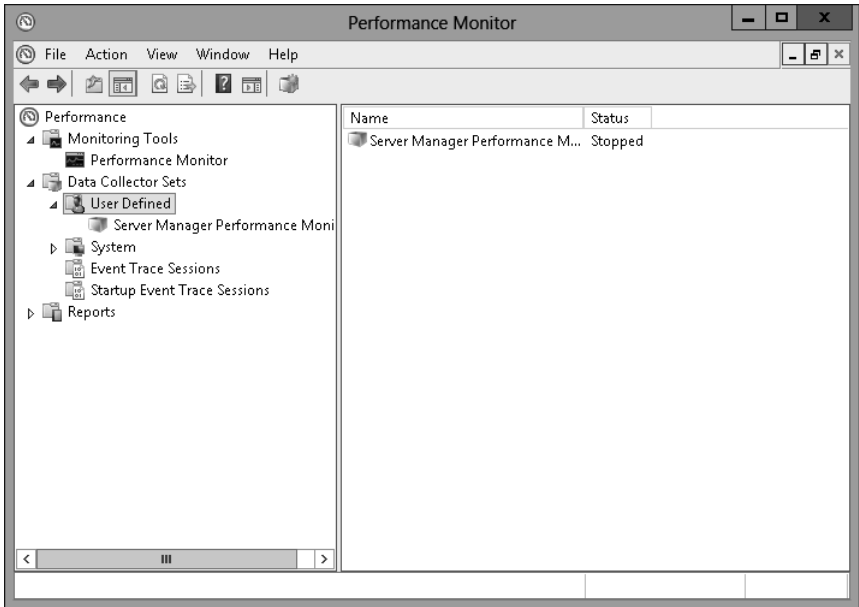


FIGURE 10-26 Accessing data collector sets

4. On the Action menu, click New, and click Data Collector Set.
5. In the Create New Data Collector Set dialog box, type the name **SYD-DC-Performance-Measurement** and click Create Manually (Advanced), as shown in Figure 10-27. Click Next.

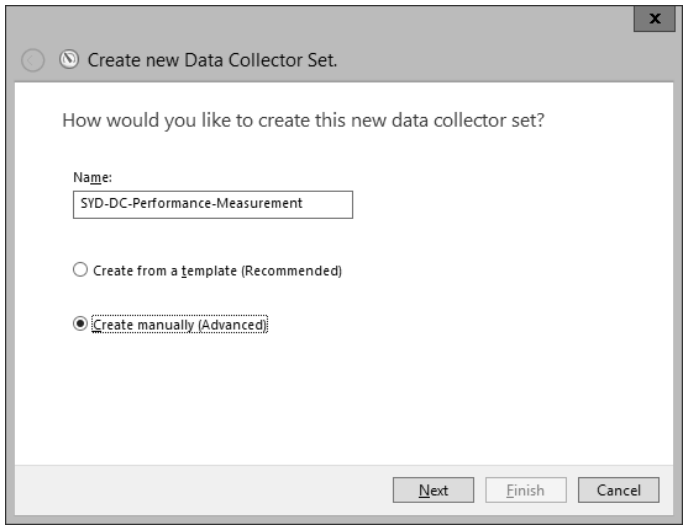
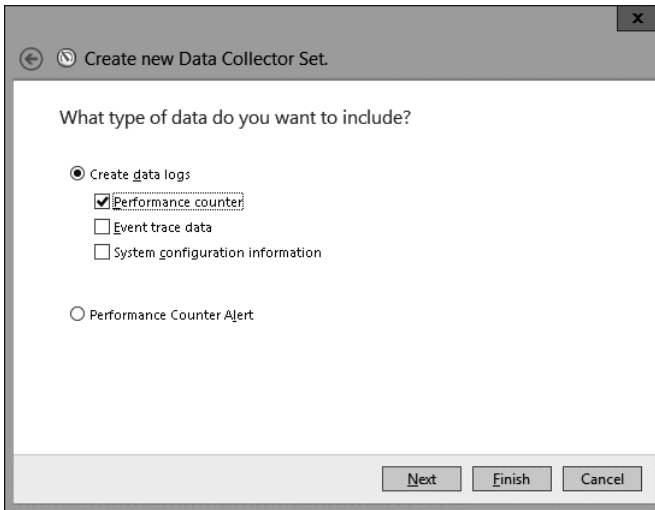


FIGURE 10-27 Entering the data collector set name

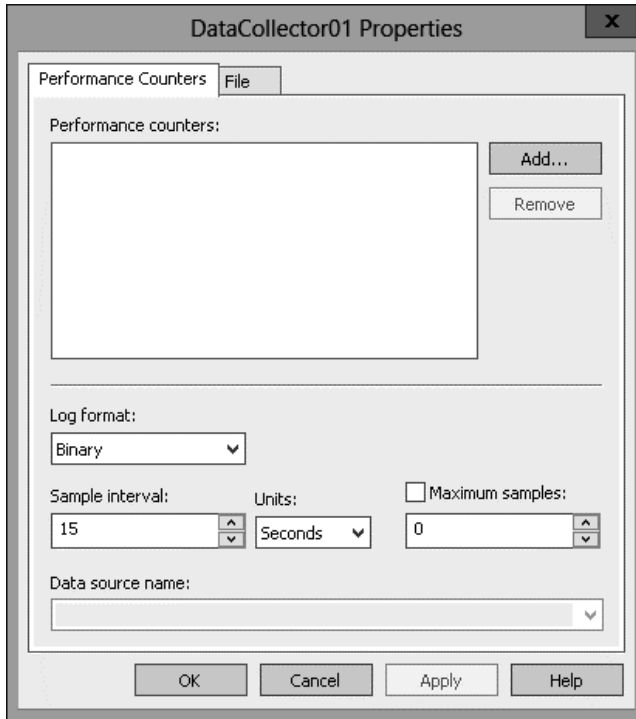
6. On the What Type Of Date Do You Want To Include? page, click Performance Counter, as shown in Figure 10-28, and click Finish.



**FIGURE 10-28** Selecting Performance Counter

7. In the Performance Monitor console, click SYD-DC-Performance-Measurement.
8. In the details pane, click DataCollector01.
9. On the Action menu, click Properties.
10. In the DataCollector01 Properties dialog box, shown in Figure 10-29, click Add.





**FIGURE 10-29** Performance counters

- 11.** In the Available Counters dialog box, click Logical Disk, and click Add.
- 12.** Click Memory, click the arrow, click Available Mbytes, and click Add.
- 13.** Click Network Interface, and click Add.
- 14.** Click Processor, and click Add.
- 15.** Verify that the list of added counters matches Figure 10-30, and click OK.

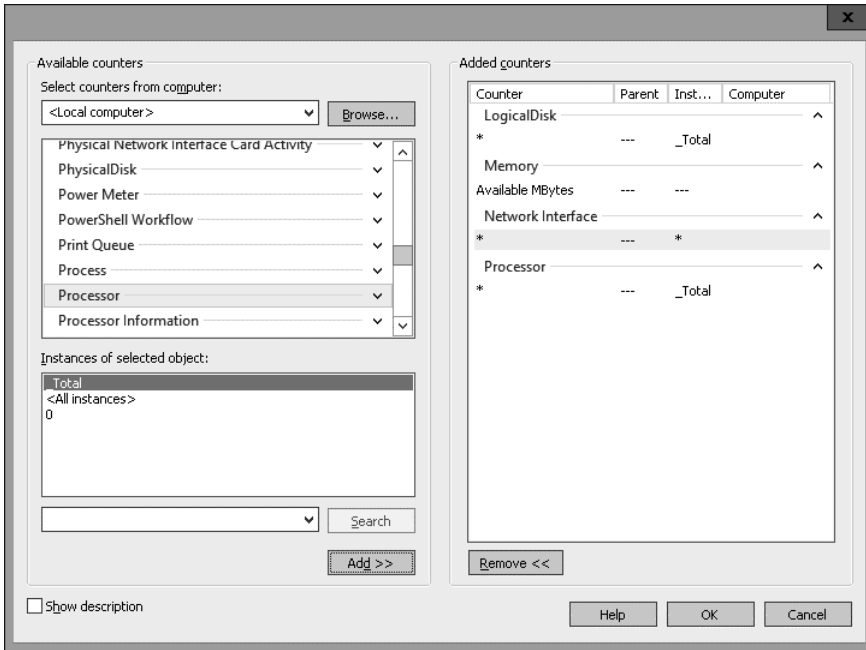


FIGURE 10-30 Matching added counters

- In the DataCollector01 Properties dialog box, set the Sample Interval to 15 seconds (see Figure 10-31), and click OK.

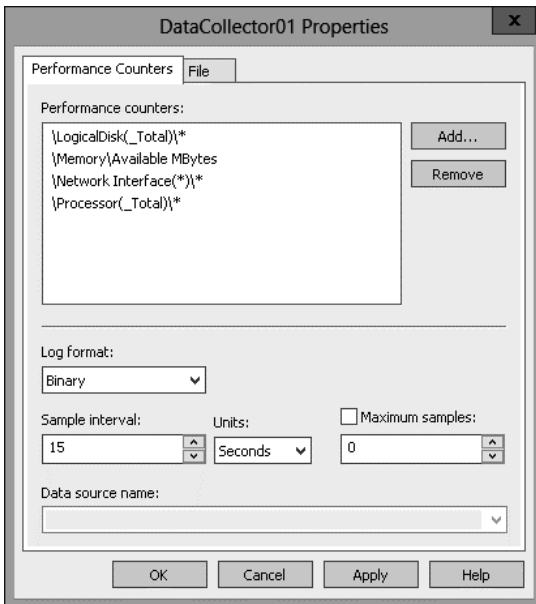
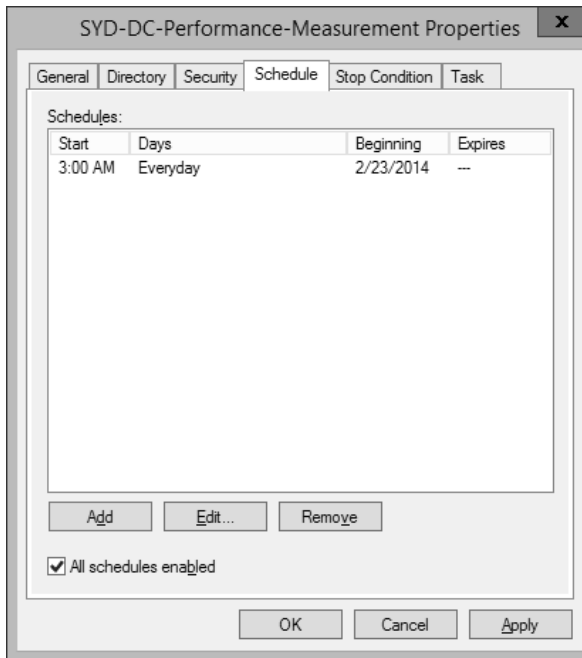


FIGURE 10-31 Setting the interval

17. In Performance Monitor, click Data Collector Sets\User Defined\SYD-DC-Performance-Measurement.
18. On the Action menu, click Properties.
19. On the Schedule tab of the SYD-DC-Performance-Measurement Properties dialog box, click Add.
20. On the Folder Action dialog box, set a time of 3:00:00 AM, and click OK.
21. Verify that the Schedule tab appear similar to Figure 10-32, and click OK



**FIGURE 10-32** Configure data collector set schedule

## Exercise 2: Collect data

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

1. In Performance Monitor, click Data Collector Sets\User Defined\SYD-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 SYD-DC-Performance-Measurement.
5. Double-click the report listed in the details pane, as shown in Figure 10-33.

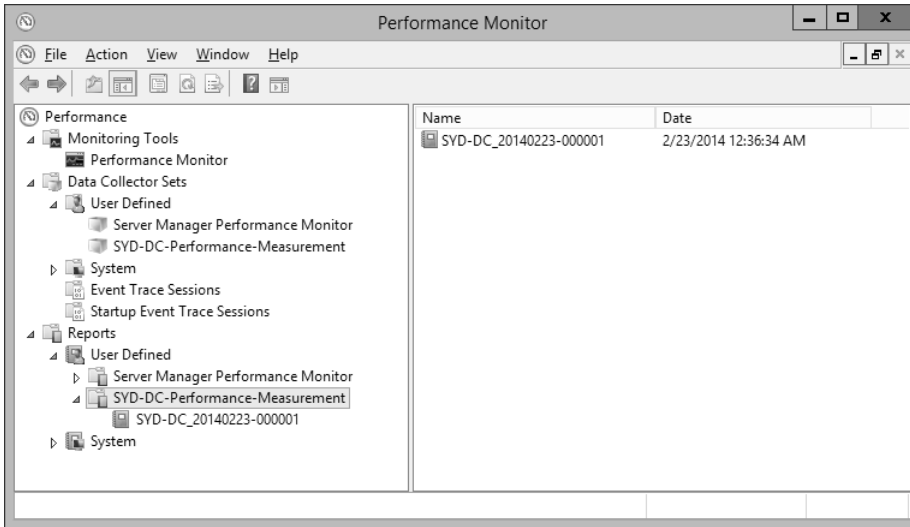


FIGURE 10-33 Selecting a report

6. Click Change Graph Type, and click Report.
7. View the report, as shown in Figure 10-34.

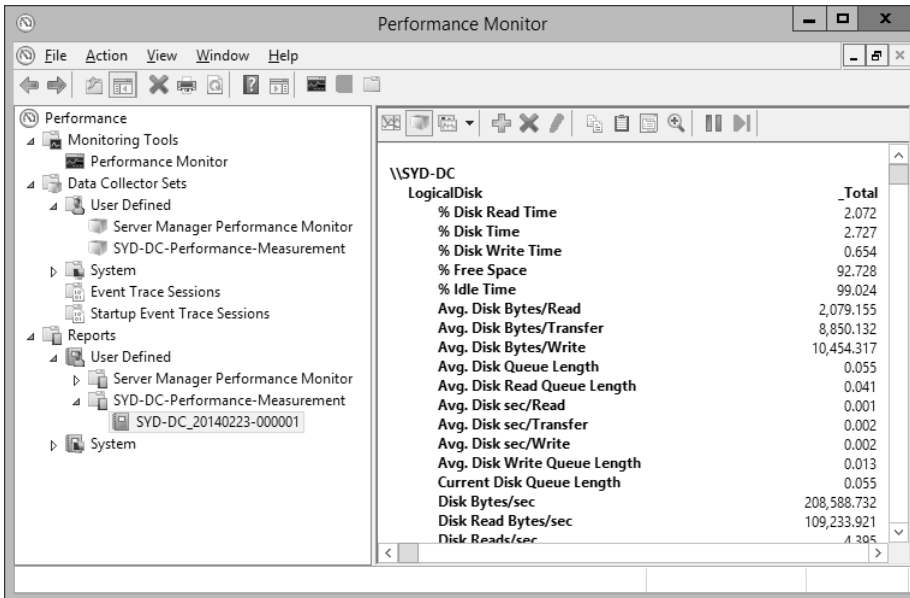
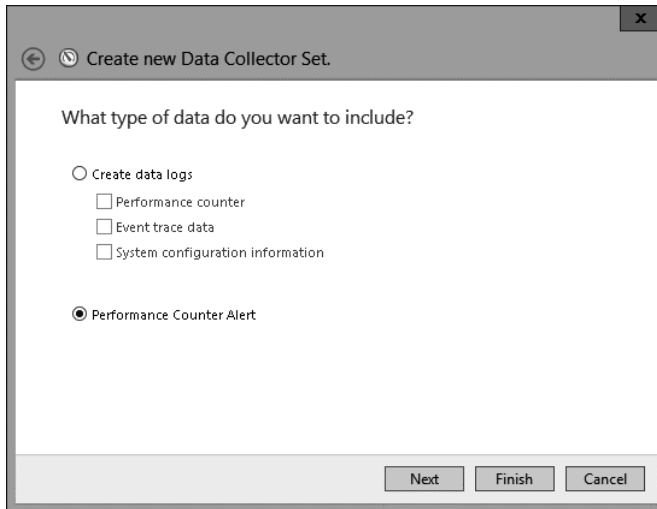


FIGURE 10-34 Viewing the report

## Exercise 3: Configure alerts

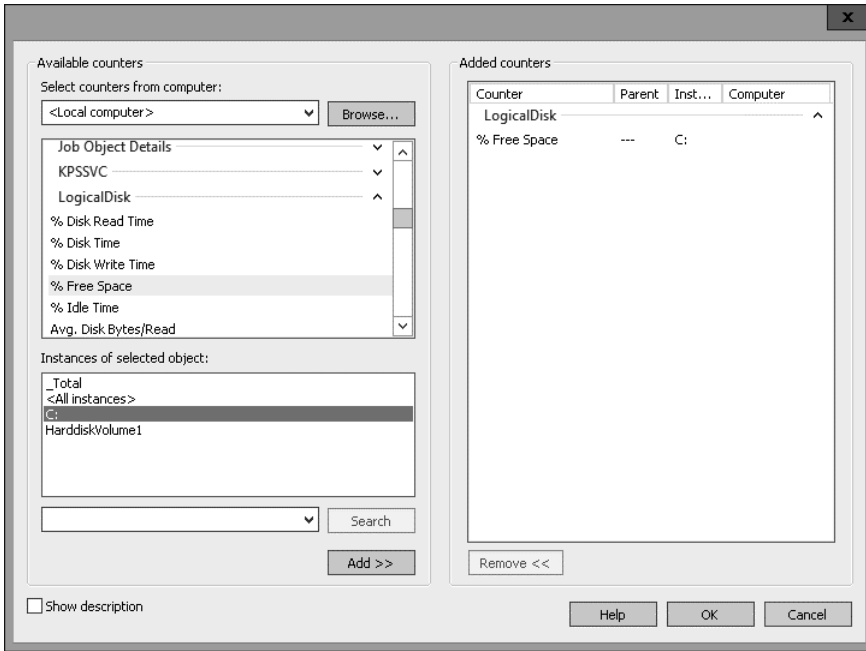
In this exercise, you configure a free disk space alert. To complete this exercise, perform the following steps:

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 10-35, and click Next.



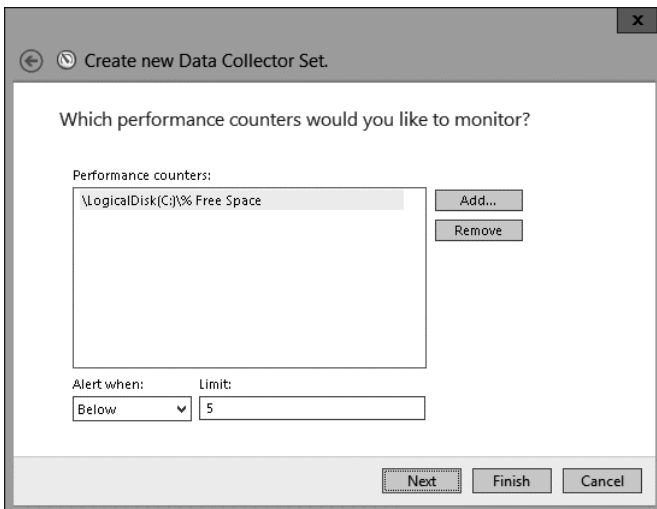
**FIGURE 10-35** Choosing Performance Counter Alert

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 10-36. Click OK.



**FIGURE 10-36** Selecting LogicalDisk

7. Set the Alert When menu to Below.
8. Set the Limit value to 5, as shown in Figure 10-37, and click Next.



**FIGURE 10-37** Setting the limit value

9. Click Finish.

## Exercise 4: Prepare computers for event subscriptions

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

1. On SYD-DC, right-click Windows PowerShell on the task bar, and click Run As Administrator.
2. Enter the following command and press Enter.  

```
Wecutil qc
```
3. When prompted, press Y, and press Enter.
4. Close the Windows PowerShell prompt.
5. Sign on to MEL-DC as Administrator.
6. Open the Windows PowerShell prompt and type the following commands.  

```
Add-Computer -DomainName contoso.com
```
7. In the Windows PowerShell Credentials dialog box, type **don\_funk@contoso.com** and **Pa\$\$w0rd**, and click OK.
8. Type the following command at the Windows PowerShell prompt to restart the computer.  

```
Restart-Computer
```
9. Sign on to MEL-DC as Contoso\don\_funk.
10. On the Tools menu on Server Manager, click Computer Management.
11. In the Computer Management console, expand Local Users And Groups, click Groups, and then click Administrators, as shown in Figure 10-38.

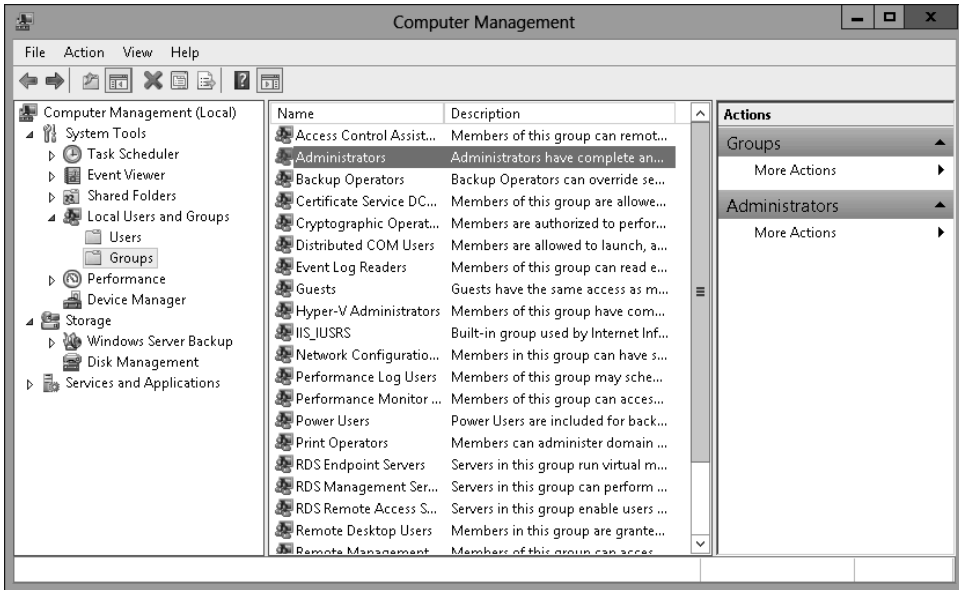


FIGURE 10-38 Accessing Administrators

12. On the Actions pane, click More Actions, and click Properties under Administrator.
13. In the Administrators Properties dialog box, click Add.
14. In the Select Users, Computers, Service Accounts, Or Groups dialog box, click Object Types.
15. In the Object Types dialog box, enable the Computers check box, as shown in Figure 10-39, and click OK.

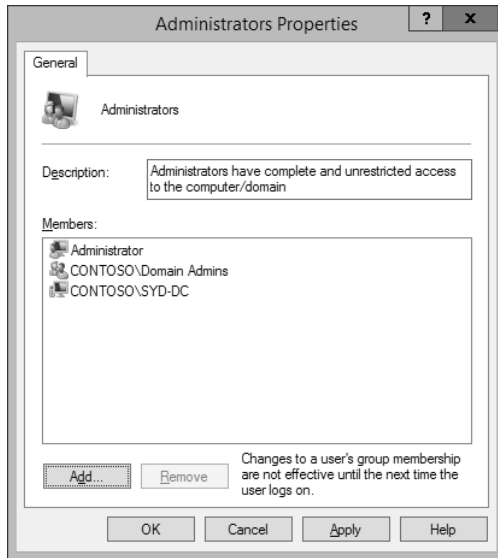


FIGURE 10-39 Selecting Computers

16. In the Select Users, Computers, Service Accounts, Or Groups dialog box, type **SYD-DC**, click Check Names, and click OK.



17. Verify that the Administrators Properties dialog box matches Figure 10-40 and click OK.



**FIGURE 10-40** Administrators Properties dialog box

18. Restart MEL-DC.

## Exercise 5: Configure event subscriptions

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

1. In the Server Manager console on SYD-DC, open the Tools menu, and click Event Viewer.
2. In Event Viewer, click the Subscriptions node, as shown in Figure 10-41.

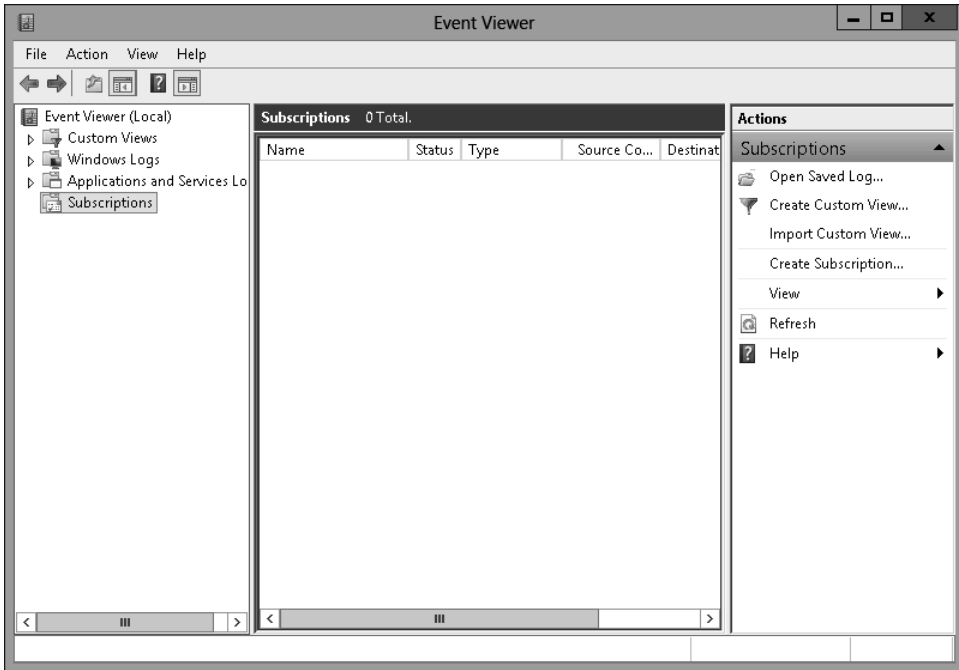


FIGURE 10-41 Clicking the Subscriptions node

3. On the Actions pane, click Create Subscription.
4. In the Subscription Properties dialog box, type the name as **Subscription-Alpha**, click Collector Initiated, and click Select Computers.
5. In the Computers dialog box, click Add Domain Computers.
6. In the Select Computer dialog box, type **MEL-DC**, click Check Names, and click OK.
7. Verify that the Computers dialog box matches Figure 10-42, and click Test.

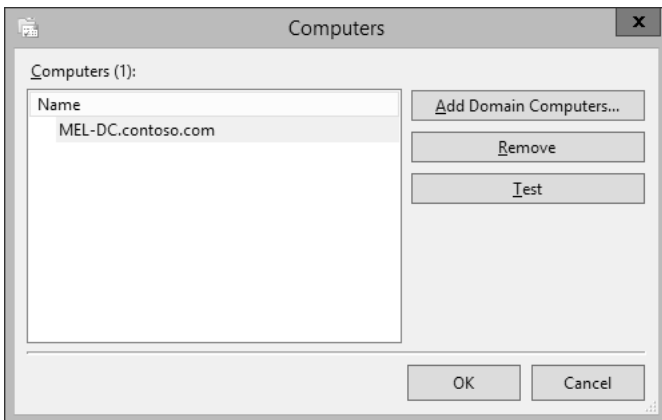
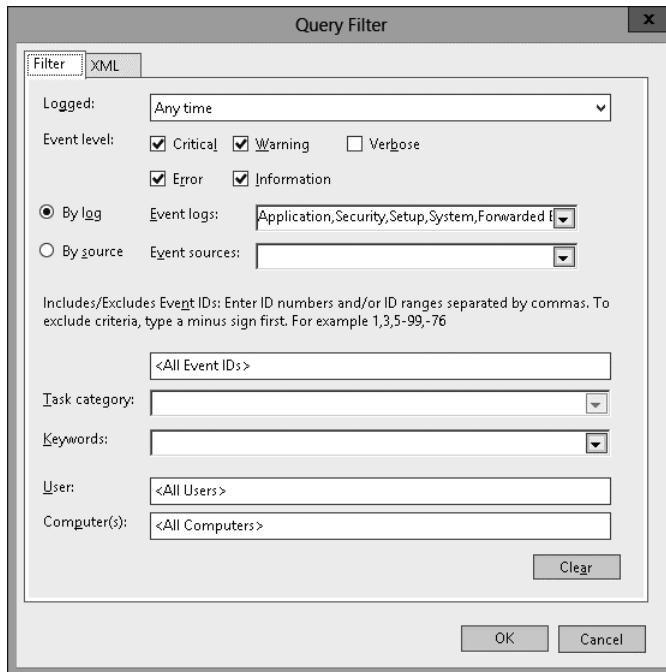


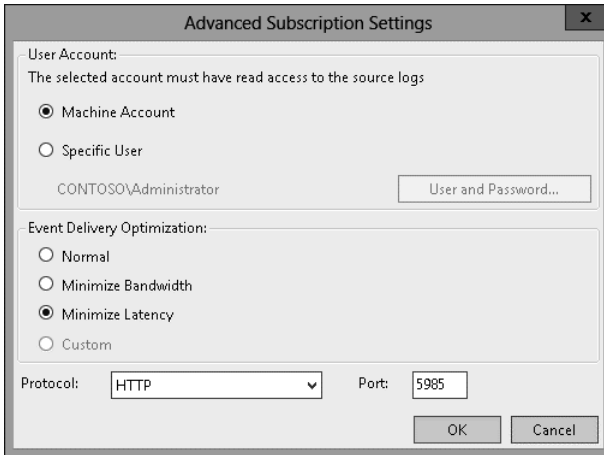
FIGURE 10-42 Computers dialog box

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 menu, and click Windows Logs.
13. Verify that the Query Filter appears the same as Figure 10-43, and click OK.



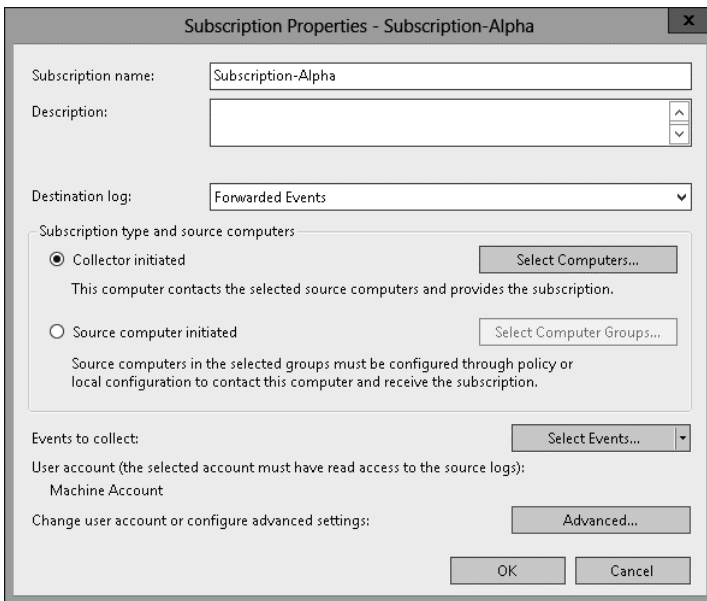
**FIGURE 10-43** The Query Filter dialog box

14. In the Subscription Properties dialog box, click Advanced.
15. In the Advanced Subscription Settings dialog box, click Minimize Latency, as shown in Figure 10-44, and click OK.



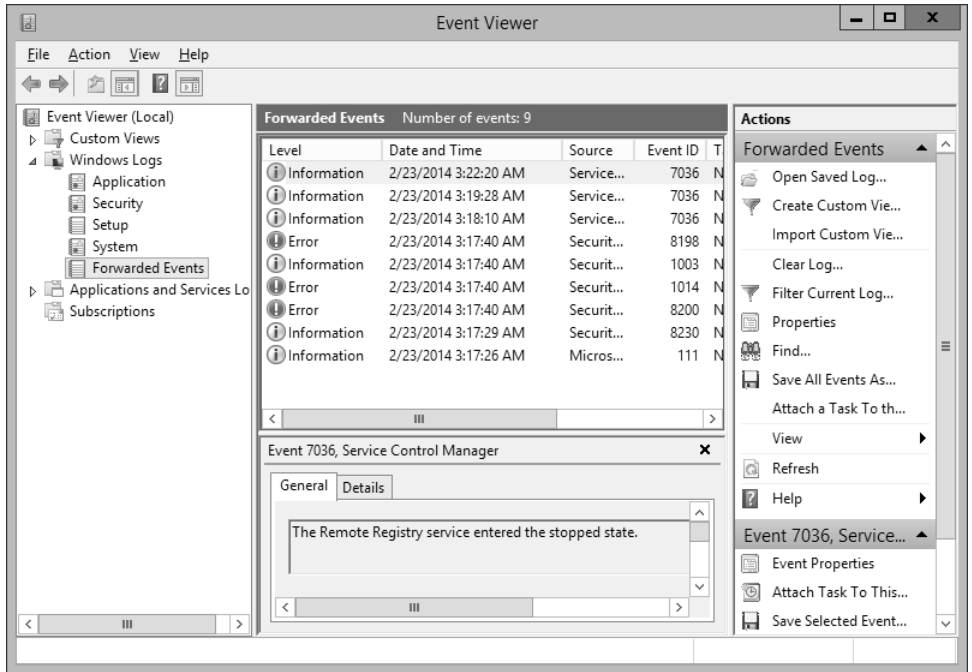
**FIGURE 10-44** Advanced Subscription Settings dialog box

16. Verify that the Subscription Properties – Subscription-Alpha dialog box matches Figure 10-45, and then click OK.



**FIGURE 10-45** Subscription Properties dialog box

17. Restart server MEL-DC.
18. Expand the Windows Logs node, and click Forwarded Events.
19. Verify the presence of items in the event log, as shown in Figure 10-46.



**FIGURE 10-46** Event log

20. Close Event Viewer.

## Exercise 6: Configure network monitoring

In this exercise, you 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 SYD-DC, click Resource Monitor.
2. On the Network tab, click the arrow next to TCP Connections, as shown in Figure 10-47.

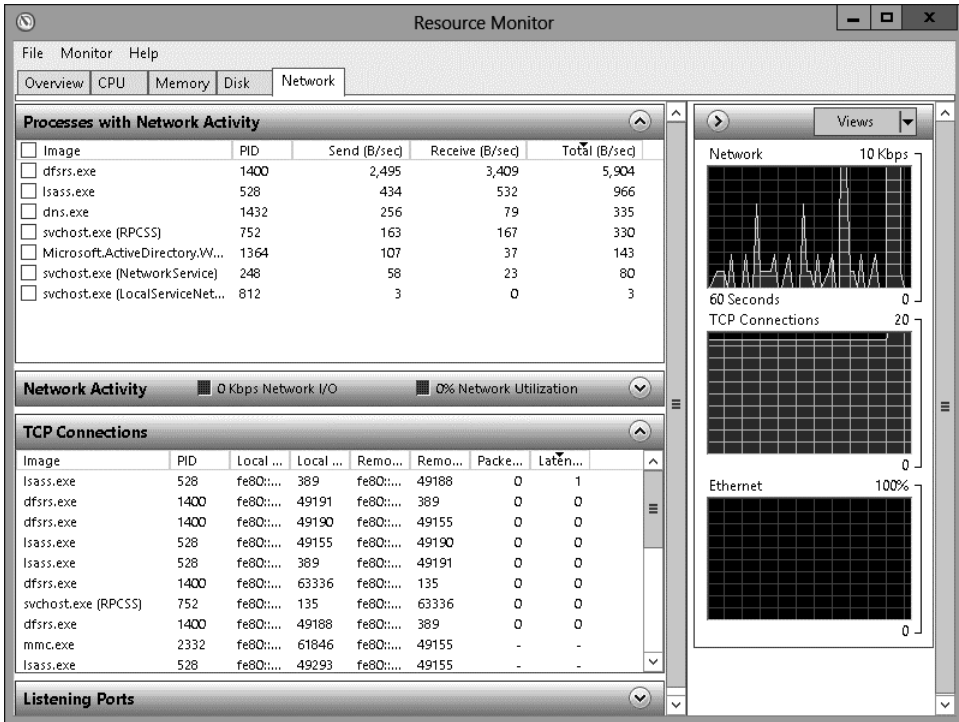


FIGURE 10-47 Network tab of the Resource Monitor

3. Click the arrow next to Listening Ports to list the ports on which different services are listening (see Figure 10-48).

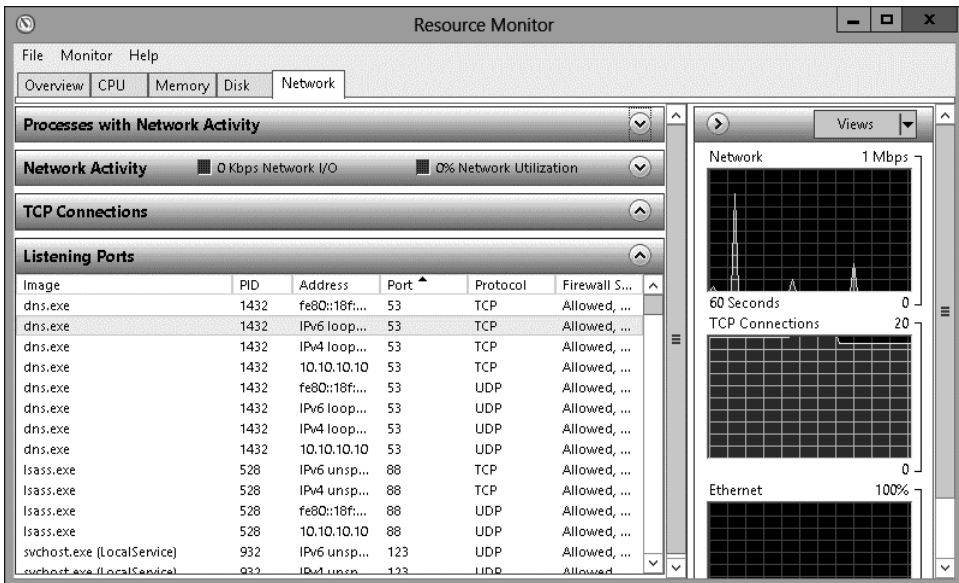


FIGURE 10-48 Listing the different ports.

## Exercise 7: Using Message Analyzer

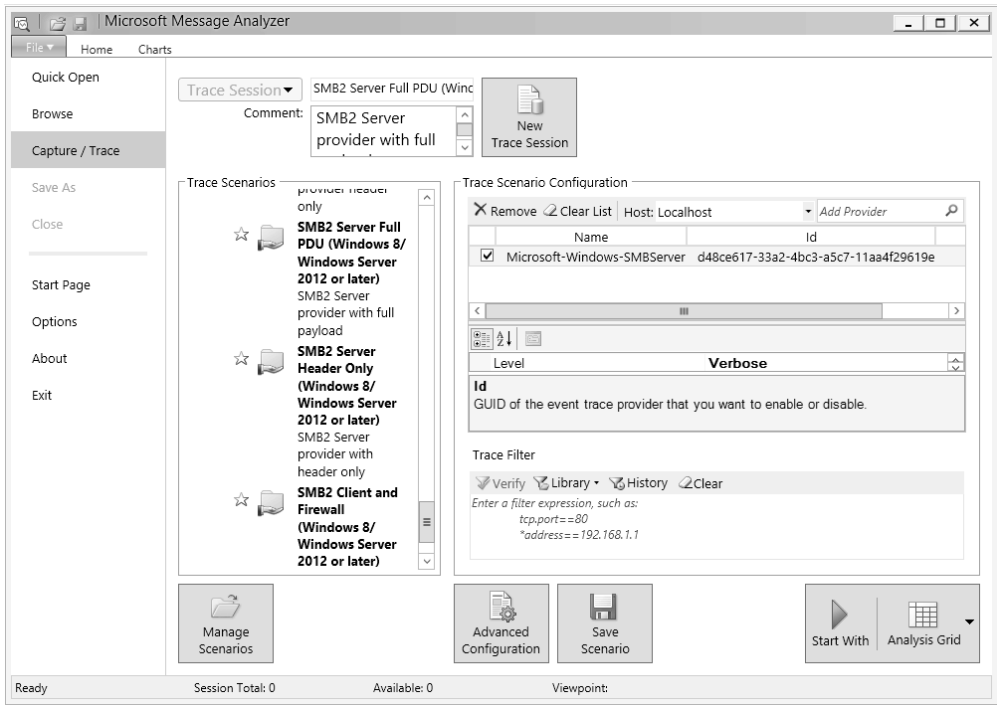
In this exercise, you use Message Analyzer to perform network monitoring. To perform this exercise, you need to download Message Analyzer from the following website: <http://www.microsoft.com/en-au/download/details.aspx?id=40308> (or just use a search engine to locate the installer) and then install it on MEL-DC. Ensure that you do not run the program and that you sign off after installation. To complete this exercise, perform the following steps:

1. Ensure that you are signed on to MEL-DC as contoso\don\_funk.
2. In the Server Manager on MEL-DC, click Local Server, and then select IE Enhanced Security Configuration.
3. In the Internet Explorer Enhanced Security Configuration dialog box, set the Administrators setting to Off, as shown in Figure 10-49, and click OK.



**FIGURE 10-49** Internet Explorer security

4. In the Search charm on MEL-DC, type **Microsoft Message Analyzer**.
5. Click Microsoft Message Analyzer in the results list.
6. On the Welcome To The Microsoft Message Analyzer dialog box, click Do Not Update Items, and click OK.
7. On the File menu, click Capture Trace, and click SMB2 Server Full PDU (Windows 8/ Windows Server 2012 or later) as shown in Figure 10-50, and click Start With.



**FIGURE 10-50** SMB Server Full PDU

8. On the taskbar, click File Explorer.
9. In File Explorer, click Computer, and then double-click Local Disk (C:).
10. On the title bar, click New Folder. Name the new folder **TEST**.
11. Right-click the TEST folder, click Share With, and click Specific People.
12. In the File Sharing dialog box, click Share, and then click Done.
13. In Microsoft Message Analyzer, click Analysis Grid, and verify that messages have been recorded, and click the final message, as shown in Figure 10-51.



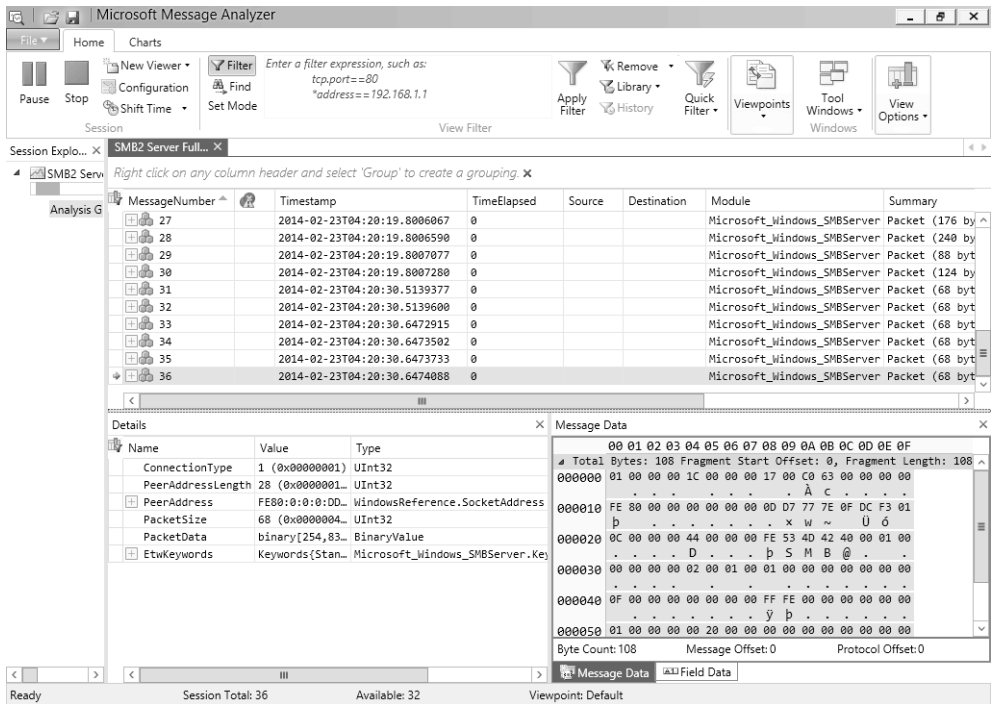


FIGURE 10-51 Verifying that messages have been recorded

14. Use File Explorer to navigate to C:\TEST.
15. Create a text file in C:\TEST named **secretfile.txt**. The content of the file should be the words "secret secret." Switch to SYD-DC.
16. On SYD-DC, in the Search charm, type **\\MEL-DC\TEST\secretfile.txt** and click Secretfile.txt in the Results pane.
17. Switch to MEL-DC.
18. Verify that additional traffic has been recorded.
19. Examine the message data for network addresses, such as server MEL-DC (see Figure 10-52).

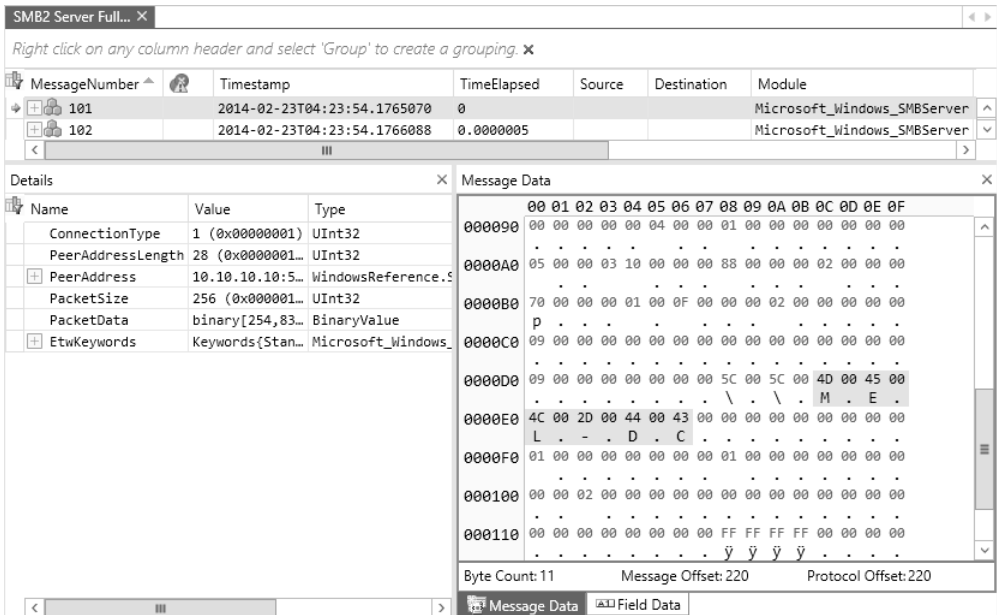


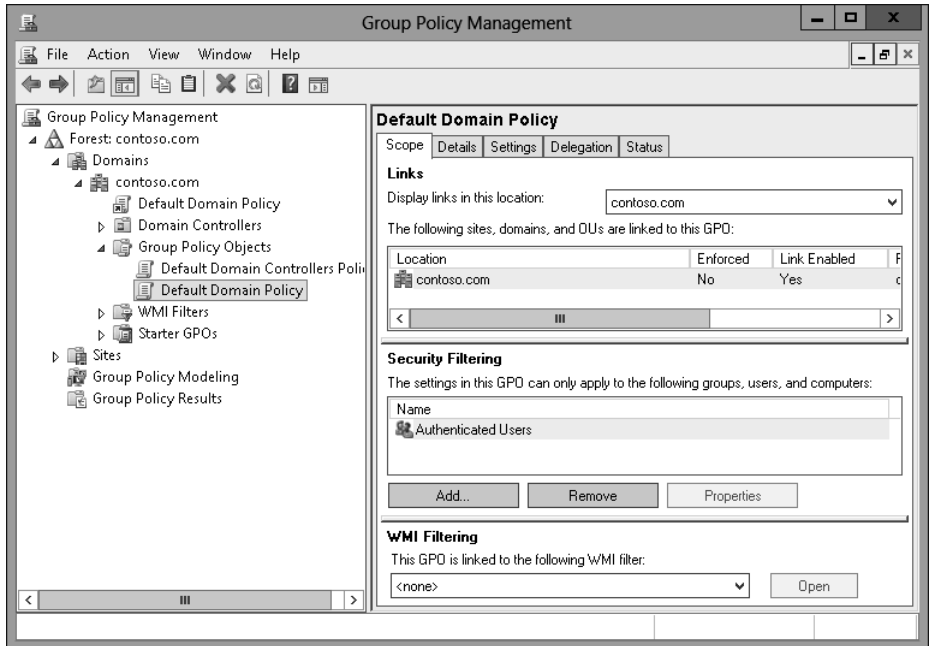
FIGURE 10-52 Examining message data

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

## Exercise 8: Configure removable device auditing

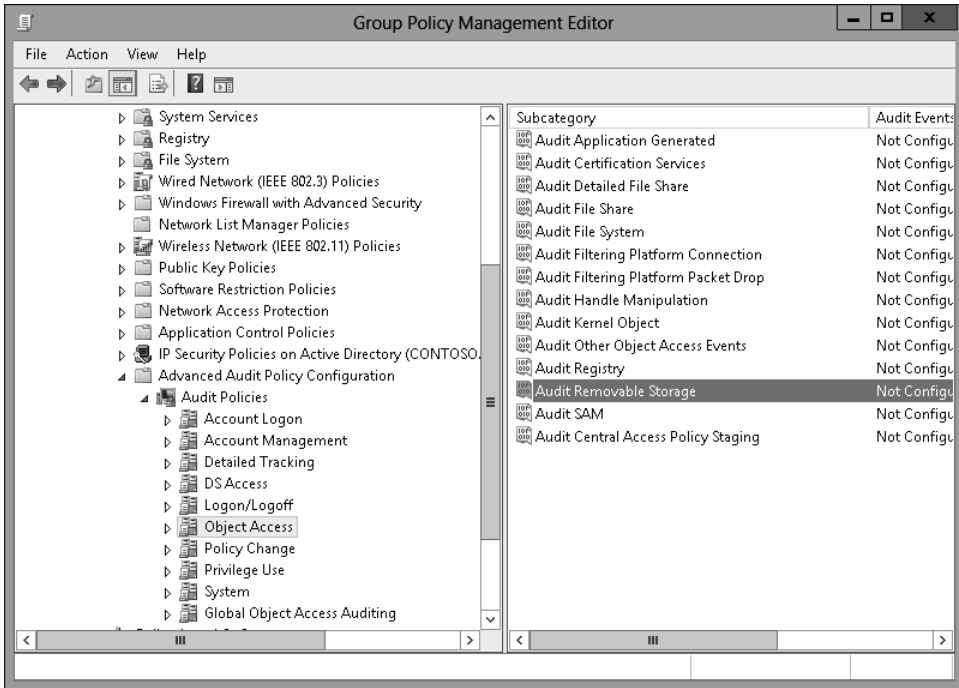
In this exercise, you configure a GPO so that removable device usage is audited. To complete this exercise, perform the following steps:

1. On SYD-DC, click Group Policy Management on the Tools menu of Server Manager.
2. Expand Forest: Contoso.com\Domains\contoso.com\Group Policy Objects, and click Default Domain Policy, as shown in Figure 10-53.



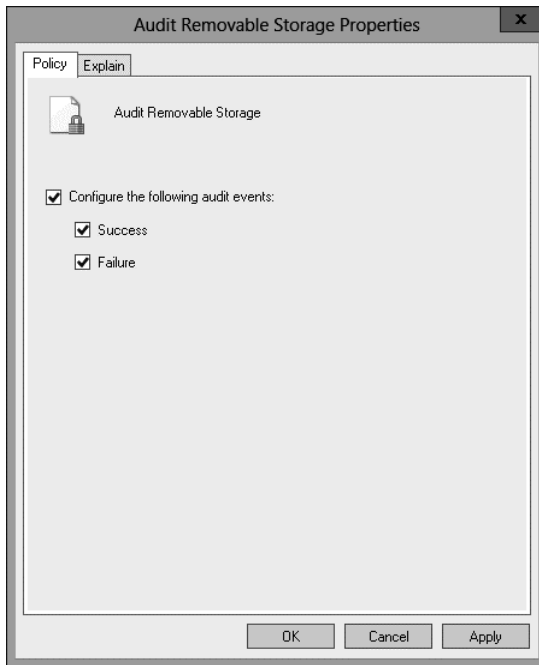
**FIGURE 10-53** Clicking Default Domain Policy

3. On the Action menu, click Edit.
4. In the Group Policy Management Editor, 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 10-54.



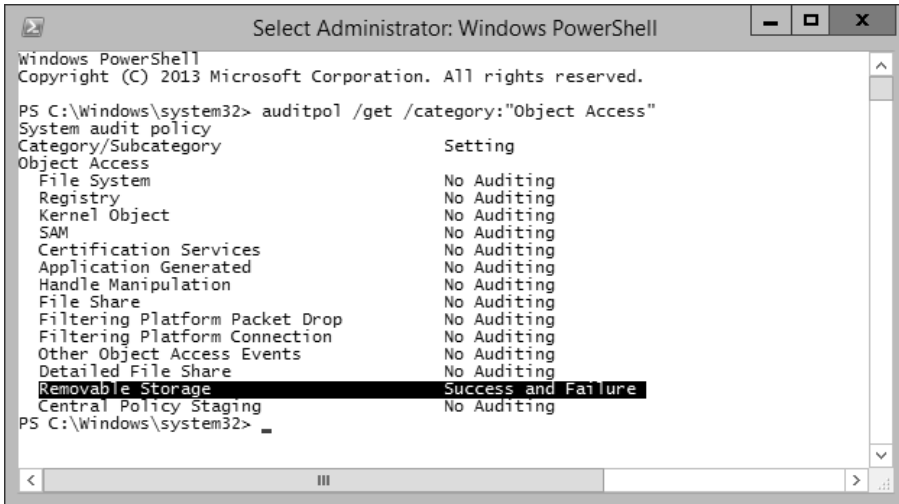
**FIGURE 10-54** Clicking Audit Removable Storage

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 10-55).



**FIGURE 10-55** Auditing properties

7. Close the Group Policy Management Editor.
8. On the taskbar, right-click Windows PowerShell, and click Run As Administrator.
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 10-56.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

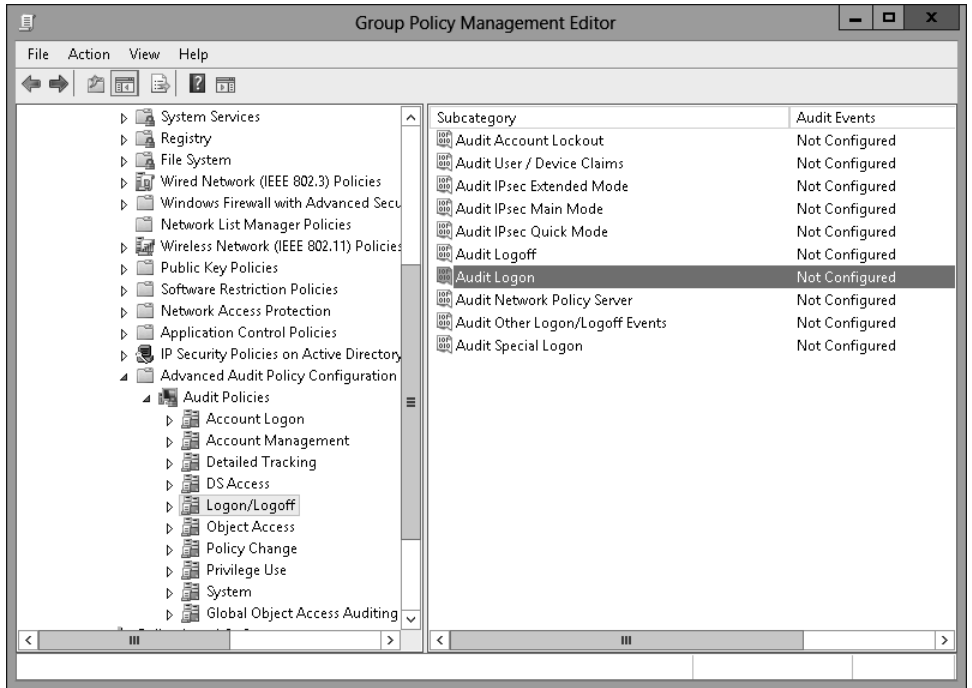
PS C:\Windows\system32> auditpol /get /category:"Object Access"
System audit policy
Category/Subcategory          Setting
-----
Object Access
File System                   No Auditing
Registry                     No Auditing
Kernel Object                 No Auditing
SAM                           No Auditing
Certification Services        No Auditing
Application Generated         No Auditing
Handle Manipulation           No Auditing
File Share                    No Auditing
Filtering Platform Packet Drop No Auditing
Filtering Platform Connection No Auditing
Other Object Access Events    No Auditing
Detailed File Share           No Auditing
Removable Storage             Success and Failure
Central Policy Staging        No Auditing
PS C:\Windows\system32> _
```

**FIGURE 10-56** Configuring Removable Storage

## Exercise 9: Configure logon auditing

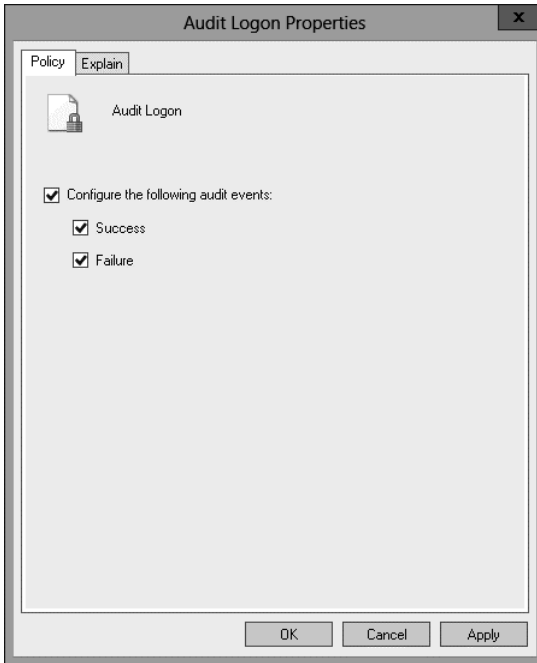
In this exercise, you configure logon auditing. To complete this exercise, perform the following steps:

1. In the Group Policy Management Console (GPMC) on SYD-DC, right-click the Default Domain Policy, and click Edit.
2. In the Group Policy Management Editor, 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 10-57.



**FIGURE 10-57** Selecting Audit Logon

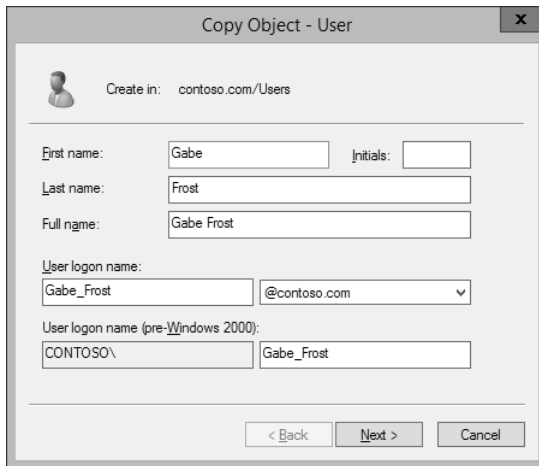
3. On the Action menu, click Properties.
4. In the Audit Logon Properties dialog box, select Configure The Following Audit Events, Success, and Failure (see Figure 10-58). Click OK.



**FIGURE 10-58** Setting audit properties

5. Close the Group Policy Management Editor.
6. On 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 10-59, and click Next.
  - First Name: **Gabe**
  - Last Name: **Frost**
  - User Logon Name: **Gabe\_Frost**



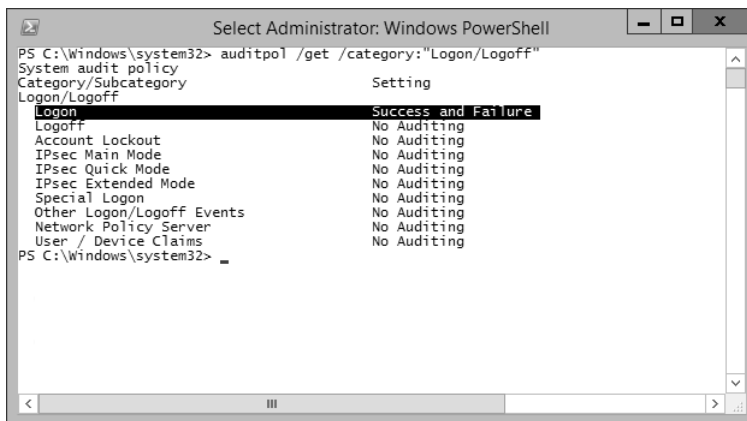


**FIGURE 10-59** Setting copy object data

10. Type **Pa\$\$w0rd** in the Password and Confirm Password text boxes, ensure User Must Change Password At Next Logon is not selected, click Next, and click Finish.
11. Close Active Directory Users And Computers.
12. In Windows PowerShell, type the following command and press Enter.
 

```
Gpupdate /force
```
13. In Windows PowerShell, type 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 10-60.



**FIGURE 10-60** Logon for Success And Failure auditing

15. Switch to MEL-DC.

16. Sign out and sign on as contoso\gabe\_frost with the password **Pa\$\$wOrd**.
17. Switch to SYD-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 Gabe\_Frost is listed, as shown in Figure 10-61. You may need to scroll through several events to find this TargetUserName.

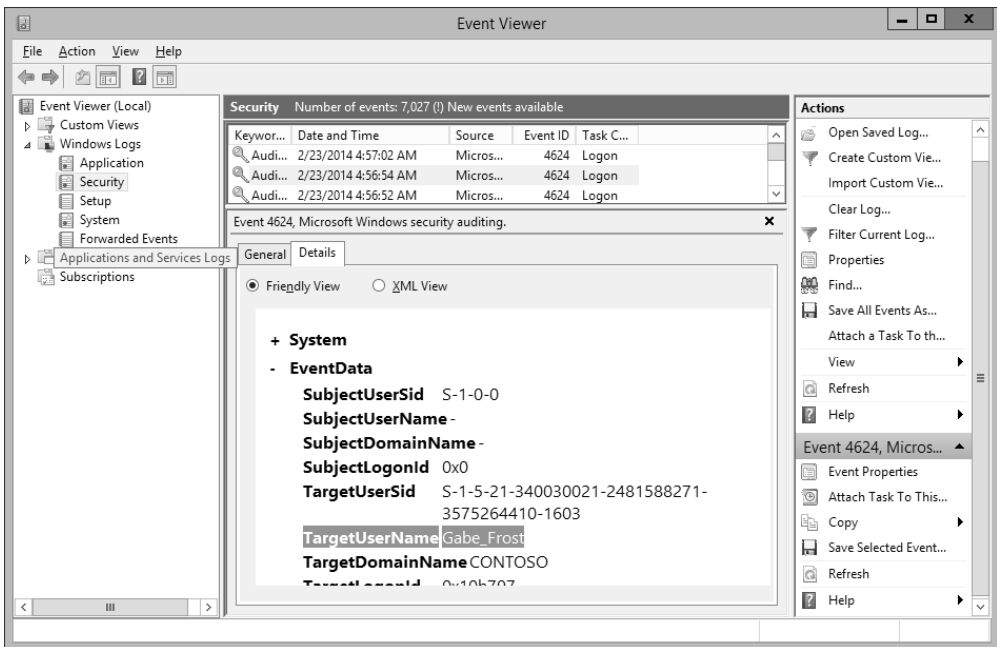
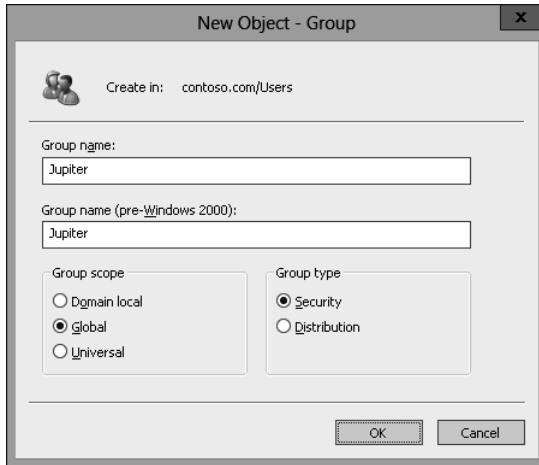


FIGURE 10-61 TargetUserName Gabe Frost

## Exercise 10: Configure expression-based audit policies

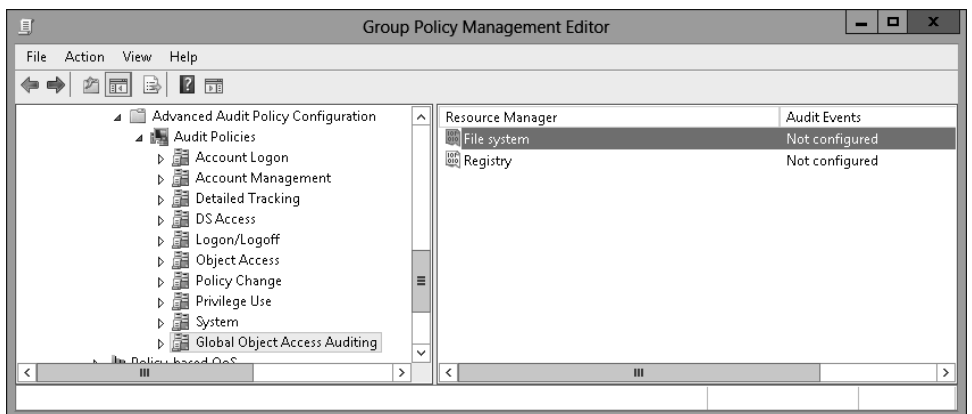
In this exercise, you configure expression-based audit policies in Group Policy. To complete this exercise, perform the following steps:

1. On SYD-DC, open Active Directory Users And Computers from the Tools menu of the Server Manager console.
2. Right-click the Users container, click New, and click Group.
3. In the New Object – Group dialog box, type the name **Jupiter**, as shown in Figure 10-62, and click OK.



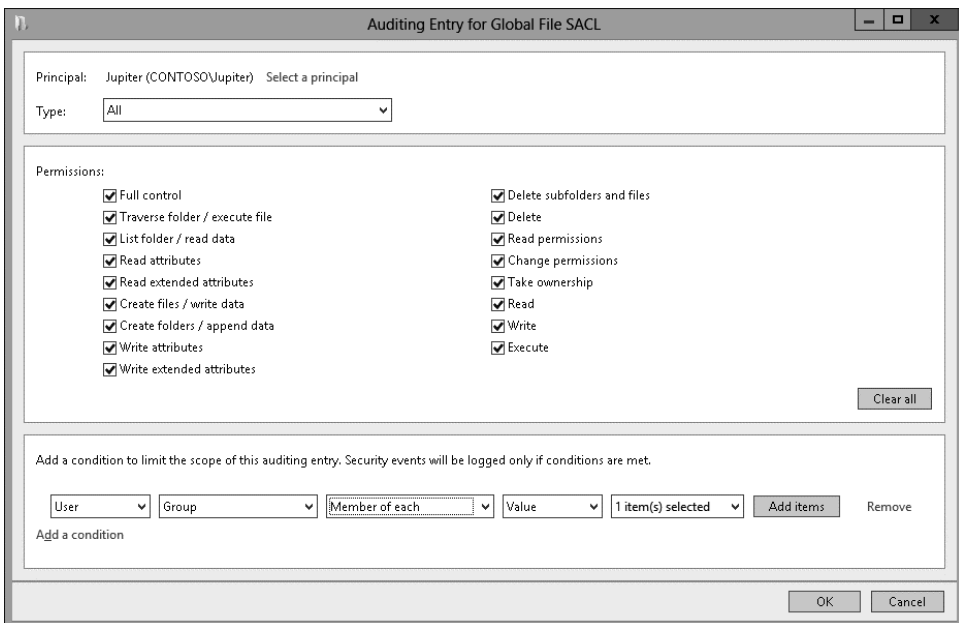
**FIGURE 10-62** Typing the group name

4. Right-click the Users container, click New, and click Group.
5. In the New Object – Group dialog box, type the name **Saturn** and click OK.
6. Right-click the Users container, click New, and click Group.
7. In the New Object – Group dialog box, type the name **Neptune** and click OK.
8. Right-click the Users container, click New, and click Group.
9. In the New Object – Group dialog box, type 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 Group Policy Management Editor, 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 10-63.



**FIGURE 10-63** Selecting File System

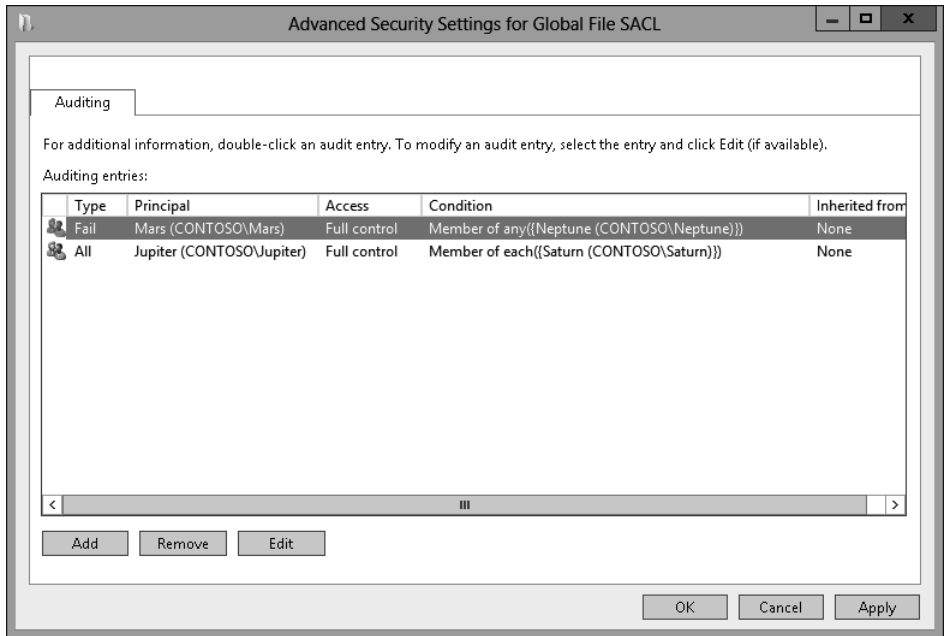
13. On the Action menu, click Properties.
14. In the File System Properties dialog box, click Define This Policy Setting, and click Configure.
15. In the Advanced Security Settings For Global File SACL dialog box, click Add.
16. In the Auditing Entry For Global File SACL dialog box, click Select A Principal Link.
17. In the Select User, Computer, Service Account, Or Group dialog box, type **Jupiter**, click Check Names, and click OK.
18. On 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 10-64 and click OK.



**FIGURE 10-64** 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 10-65, and click OK.



**FIGURE 10-65** Advanced Security Settings For Global File SACL dialog box

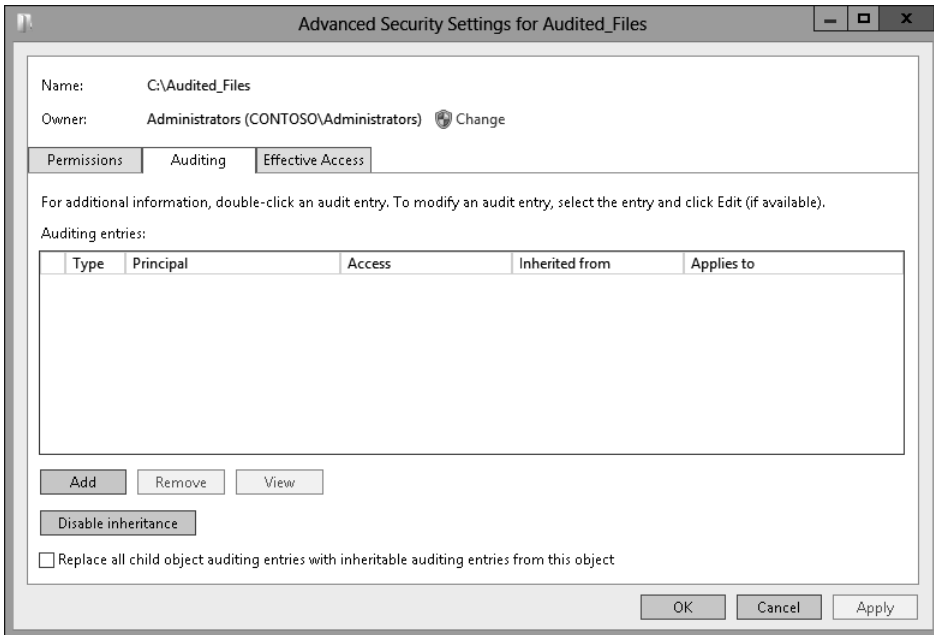
32. Click OK to close the File System Properties dialog box and close the Group Policy Management Editor.

## Exercise 11: Configure folder auditing

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

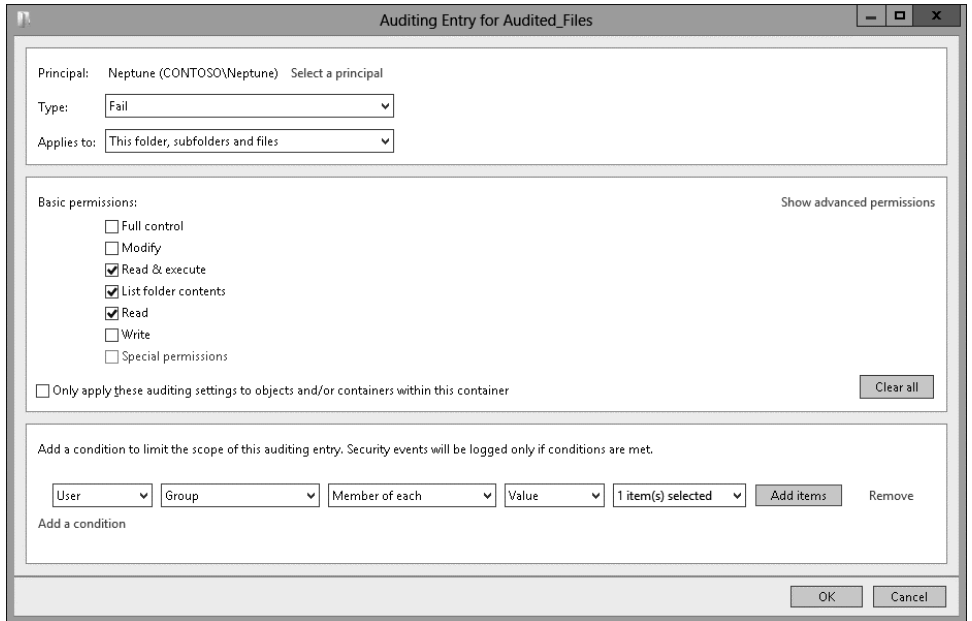
1. Click File Explorer on the taskbar.
2. Click Computer and double-click Local Disk (C:).
3. On the title bar, click the New Folder icon.
4. Name the new folder **Audited\_Files**.
5. Right-click the Audited\_Files folder, and click Properties.

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 10-66, click Add.



**FIGURE 10-66** 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 10-67, and click OK.



**FIGURE 10-67** 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 MEL-DC.
- **Exercise 2** Create a test share on SYD-DC and populate it with text files. Add user accounts to the Mars, Jupiter, Saturn, and Neptune groups. Sign on to MEL-DC 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.
- 4. 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.
- 2. 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.

*This page intentionally left blank*

# Index

## Symbols

802.1X enforcement, configuring for NAP 382–385  
802.1X group policies, cconfiguring authentication 363–367

## A

A records 148  
AAAA records 148  
access-based enumeration 513  
accidental deletion of objects, protecting from 212  
accounting, RADIUS 429–432  
Account Lockout Duration policy 71  
    practice exercise 101  
account lockout policies 70, 74  
    practice exercise for configuring 101–104  
Account Lockout Threshold policy 71  
    practice exercise 102  
account management tasks 71–75  
Active Directory  
    backing up 210–212  
    database optimization 200–203  
    defragmenting the database 200–203  
    domain naming master 184  
    metadata cleanup 203  
    operations masters  
        managing 182–187  
        practice exercise 230–234  
    recovering deleted objects 208–215  
    snapshots 204–206, 215  
Active Directory Administrative Center  
    deploying an RODC 193  
    domain functional level, configuring 80  
    enabling Recycle Bin 208  
    fine-grained password policies  
        managing 81  
        practice exercise 110–113  
    non-expiring passwords, locating 72  
        practice exercise 107–110  
    password settings, determining 84  
    practice exercise 234  
Active Directory BitLocker recovery 526  
Active Directory Domain Services (AD DS) 66  
Active Directory Domain Services Configuration Wizard  
    configuring a Global Catalog server 188  
    deploying an RODC 191–193  
    practice exercise 221–225  
    removing domain controllers 203  
Active Directory integrated zones 124–126  
    practice exercise 159  
Active Directory Recycle Bin 208–210  
    practice exercise 234  
Active Directory Schema 183  
Active Directory Schema snap-in 183  
    practice exercise 232  
Active Directory Users And Computers  
    accessing snapshots 205  
    cleaning up metadata 204  
    operations masters, managing 182–186  
    practice exercise 230–232  
Add-ADDSSReadOnlyDomainControllerAccount cmdlet 193  
Add-DnsServerConditionalForwarderZone PowerShell cmdlet 134  
Add-DNSServerDirectoryPartition cmdlet 125  
Add-DnsServerForwarder cmdlet 132  
Add-DnsServerPrimaryZone cmdlet 127  
Add-DnsServerResourceRecordA cmdlet 148  
Add-DnsServerResourceRecordCName cmdlet 148  
Add-DnsServerResourceRecordMX PowerShell cmdlet 149  
Add-DnsServerResourceRecordPtr cmdlet 150  
Add-DnsServerStubZone cmdlet 136

## Add-DnsServerStubZone cmdlet

- Add-DnsServerZoneDelegation cmdlet 130
- /Add-Driver switch 6
- Add-KDSRootKey cmdlet 88–90
- /Add-Package switch 7
- /Add-ProvisionedAppxPackage switch 8
- Add Roles And Features Wizard 139
  - deploying an RODC 191
  - installing Windows Server Backup 210
  - practice exercise 218–221, 226
- AD DS (Active Directory Domain Services) 66
- Add-WsusComputer command 31
- Administrative Events custom view 601
- administrative templates 296–302
  - central store 297
    - practice exercise 330
  - filtering 300
    - practice exercise 330
  - importing in ADM format 299
- ADMX format 296–300
- ADMX Migrator tool 299
- advanced audit policies 614–620
  - practice exercises 641–654
- Advanced Encryption Services (AES). *See* AES
- aging and scavenging DNS zones 151
- alerts, for monitoring servers 597–599
  - practice exercise 628
- alias (CNAME) records 148
  - in GlobalNames zones 143
- answer files 12–14
- application directory partitions, creating 125
- applications
  - assigning 287
  - publishing 288
  - upgrading existing 290
- /Apply-Image switch 10
- app packages, adding to Server images 8
- Approve-WsusUpdate command 31
- assigning applications using Group Policy 287
- auditpol.exe utility 619
- audit policies, advanced 614–620
  - practice exercises 641–654
- authentication methods 357–359
  - configuring with 802.1X group policies 363–367
  - for network policies 372
- authentication protocols for VPN 443–446
- Authentication Requirements, configuring for HRA 349
- authoritative restore for Active Directory objects 212–214
- autoenrollment, enabling using EFS 531

- automatic approval rules for WSUS 36–38
  - practice exercise for 58
- Automatic Update Detection Frequency policy 34
- automating server operating system deployment 12–14
- autonomous mode, configuring WSUS 30
- Autounattend.xml file 12

## B

- backing up Active Directory 210–212
- backing up GPOs 243
  - practice exercise 269–271
- Backup-GPO cmdlet 242
- BitLocker 522–529
  - DRA (data recovery agent) 527
  - modes, configuring 523–525
  - Network Unlock feature 528
  - practice exercise 566–571
  - recovering data 525–528
  - TPM (Trusted Platform Module) 523–525
- BitLocker, protecting RODC virtual machines 196
- BitLocker To Go 525
- blocking Group Policies 254
- Block Inheritance function 255
  - practice exercise 275
- block-level replication, used by DFS 514–516
- boot environment, protecting with BitLocker 522–529
- boot images, used by WDS 17
- boot options for WDS 21
- Boot.wim file 2
- build and capture process 9
- BYOD (Bring Your Own Device) scenarios 388

## C

- caching Group Policies 260
- capture images, used by WDS 18
- /Capture-Image switch 10
- capturing traffic using Message Analyzer 611–613
- centralized deployment 12
- central store
  - creating 297
  - practice exercise 330
- certificate enrollment practice exercise 574–578
- Certification Authority (CA)
  - choosing 348
  - practice exercise 484, 566–571
  - using with an HRA 397

- CHAP (Challenge Handshake Authentication Protocol) 444
- Cisco Network Access Control (Cisco NAC) 346
- client naming policy 20
- cloning DFS replication databases 519
- cloning domain controllers 197
- CNAME records 148
  - in GlobalNames zones 143
- collector-initiated event subscription, configuring 604
- Computer Configuration settings 258–260
- conditional forwarders, DNS 131–133
- conditions
  - for connection request policies 353–356
  - for network policies 370–372
- Configure Automatic Updates policy 34
- Configure Forwarder Resource Usage policy 605
- Configure Target Subscription Manager policy 605
- connection request policies 350–363
  - adding conditions 353–356
  - creating 361–363
  - default policy 360
  - forwarding 356
  - network access servers, specifying type 351
  - realm name, applying 359
- constraints, configuring for network policies 372
- Control Panel settings, configuring with Group Policy preferences 319–321
- Copy-GPO cmdlet 243
- copying GPOs 246
- corrupted DFS databases, recovering 520
- counter alerts, for monitoring servers 597–599
  - practice exercise 628
- Create Multicast Transmission Wizard 24
- creating GPOs 249
- credential roaming, enabling using EFS 531
- cryptographic policies of an HRA 397

## D

- data collector sets, for monitoring servers 592–596
  - practice exercise 621–626
- DCCloneConfig.xml file 198
- DCGPOFix.exe command 246
- Default Domain Policy GPO 67
- defragmenting Active Directory database 200–203
- delegating GPO management 248–251
- delegating password settings permissions 78–80
- Delegation Of Control Wizard 79
- deleted Active Directory objects, recovering 208–215
- Deny-WsusUpdate command 32
- deployed servers, servicing and updating 27–39
- deploying scripts to users and computers 291–293
  - practice exercise 329–332
- deploying software using Group Policy 285–291
- deploying Windows Server images 11–27
  - practice exercise for 43–47
- Deployment Image Servicing and Management (DISM) tool 3
- deployment topologies supported by DirectAccess 456
- device drivers
  - adding to Server images 6
  - importing packages into WDS 25
- DFS (Distributed File System)
  - cloning replication databases 519
  - configuring 511–521
  - domain-based namespaces 512
  - namespaces 511–513
    - practice exercise 558–560
  - practice exercise 555–558
  - recovering databases 520
  - remote differential compression 514–516
  - replication 514–520
    - practice exercise 560–566
    - targets, adding 516
  - staging folders 515
  - stand-alone namespaces 512
- DHCP enforcement, configuring for NAP 377–380
  - practice exercise 401, 406–412
- DirectAccess 454–473
  - application servers, configuring 473
  - benefits of 455
  - client requirements 461
  - configuring a DirectAccess server 457–460
  - DNS, configuring for 463
  - firewall rules, configuring 464
  - infrastructure 455–460
  - infrastructure servers, configuring 470–472
  - Network Location Server (NLS) 460, 463, 470
  - network topologies supported 456
  - remote access servers, configuring 469
  - Remote Access Setup diagram, configuring with 465–473
  - remote clients, configuring 467–469
- Directory Services Restore Mode. *See* DSRM
- discover images, used by WDS 15, 18
- Dism.exe command-line utility 3–10

## DISM tool

- DISM tool. *See* Deployment Image Servicing and Management tool
  - Distributed File System (DFS). *See* DFS
  - DNS (Domain Name System)
    - configuring, for DirectAccess 463
    - preparing servers for DirectAccess 459
  - DNSKEY record 155
  - DNSSEC. *See* Domain Name System Security Extensions
  - DNSSEC Key Master 155
  - DNS zones 123–136
    - Active Directory integrated zones 124–126
    - aging and scavenging 151
    - GlobalNames zones 142–144
    - host records in 148
    - mail exchanger (MX) records in 149
    - pointer (PTR) records in 150
    - practice exercise 159
    - primary zones 127
    - resource records in 147
    - reverse lookup zones 128–130
    - secondary zones 127
      - practice exercise 168–170
    - signing a zone 153
    - split DNS 131
    - stub zones 134
    - supporting dynamic updates 126
    - types of 124–130
    - using DNSSEC with 153–157
    - zone delegation 129
      - practice exercise 163–168
  - domain-based namespaces 512
  - domain controllers
    - cloning 197
    - Global Catalog servers 187–189
    - maintaining 200–207
    - managing 181–200
    - non-authoritative restore 214
    - operations masters 182–187
    - practice exercise 217–225
    - removing 203
    - RODC (read-only domain controller) 190–197
    - snapshots, managing 204–206
    - universal group membership caching (UGMC) 189
  - domain functional level
    - fine-grained password policies and 80
    - for GMSAs 88
  - Domain Name System (DNS). *See* DNS
  - Domain Name System Security Extensions (DNSSEC) 147, 153–157
    - practice exercise 173–175
  - domain naming master 184
  - domain user password policies 66–70
    - fine-grained 80–82
  - downloading software updates, practice exercise for 40–42
  - DRA (data recovery agent)
    - using with BitLocker 527
    - using with EFS 533
  - driver packages, importing into WDS 25
    - practice exercise for 52–54
  - dsmain command 205
  - DSRM (Directory Services Restore Mode)
    - and the Active Directory Recycle Bin 208
    - configuring domain controller as RODC 192
    - performing authoritative restore 212–214
  - Dynamic Host Configuration Protocol (DHCP). *See* DHCP
  - dynamic update options for DNS zones 126
    - practice exercise 159
- ## E
- EAP-MD5 CHAP (Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication) 443
  - EAP Quarantine Enforcement Client policy 383, 386
  - EAPs (Extensible Authentication Protocols) 357
  - EAP-TLS (Extensible Authentication Protocol-Transport Level Security) 443
  - EFS (Encrypting File System) 530–533
    - certificates, configuring 531–533
      - practice exercise 571–574
    - practice exercise 566–571, 578–582
    - recovering data 532
  - Enable Client-Side Targeting policy 34
  - /Enable-Feature switch 8
  - Encrypting File System (EFS). *See* EFS
  - encryption
    - using BitLocker 522–529
    - using EFS (Encrypting File System) 530–533
  - encryption, selecting types of 368
  - Enforce password history policy 68
    - practice exercise 96
  - Enforce User Logon Restrictions policy 93
  - enforcing Group Policies 254
  - event-driven tasks 606–609
  - event log filters 600
  - event log forwarding 603–606

- event log views 601–603
- event subscriptions 603–606
  - practice exercise 630–635
- event trace providers 595
- Event Viewer 599–609
- EXE format, deploying files in 286
- Export-DfsrClone Windows PowerShell cmdlet 519
- expression-based audit policies 616
  - practice exercise 649–652
- Extensible Authentication Protocols. *See* EAPs

## F

- file classification, FSRM 505
- file expiration, practice exercise 549–552
- file integrity check, performing 200
- file-level auditing 618
  - practice exercise 652–654
- file management tasks, FSRM 506
- file quotas, FSRM 502
  - practice exercise 541–545
- file screens, FSRM 504–506
  - practice exercise 545–549
- File Server Resource Manager. *See* FSRM
- filtering administrative templates 300
  - practice exercise 330
- filtering policies for GPOs 255–257
- filters for event logs 600
- fine-grained password policies 66, 77–85
  - practice exercise 110–113
- Flexible Single Master Operations. *See* FSMO
- folder-level auditing 618
  - practice exercise 652–654
- folder redirection 282–285
  - practice exercise 324–328
- folder replication, DFS 514–520
- forwarders, DNS 132
- forwarding connection requests 356
- forwarding event logs 603–606
- FSRM (File Server Resource Manager)
  - configuring 501–508
    - practice exercise 536–541
  - file classification 505
  - file expiration, practice exercise 549–552
  - file management tasks 506
  - file screens 504–506
    - practice exercise 545–549
  - quotas 502
    - practice exercise 541–545

- storage reports 507
  - practice exercise 552–556
- Full Mesh topology 516
- fully qualified domain names (FQDNs)
  - host records and 148
  - pointer (PTR) records and 150
  - resource record maps and 147
  - reverse lookup zones and 128

## G

- Get-ADDCloningExcludedApplicationsList cmdlet 198
- Get-ADDomain cmdlet 182
- Get-ADForest cmdlet 182
- Get-DfsrCloneState cmdlet 519
- /Get-Features switch 8
- Get-GPO cmdlet 242
- /Get-ProvisionedAppxPackage switch 8
- Get-Service cmdlet 91
- /Get-wiminfo switch 5
- Get-WsusClassification command 32
- Get-WsusComputer command 32
- Get-WsusProduct command 32
- Get-WsusServer command 32
- Global Catalog servers 187–189
- global clouds 145
- GLobalNames zones 142–144
- Global Object Access Auditing node 617
- Global Search function, Active Directory Administrative Center 84
- GMSAs. *See* Group Managed Service Accounts
- GPFixup.exe command 247
- GPOs (Group Policy Objects) 66
- Group Managed Service Accounts (GMSAs) 87–90
  - practice exercise 114
  - requirements 88
- Group Policy Management Console (GPMC) 242
  - configuring password policies 96–100
  - delegating permissions 248–251
  - linking GPOs 250
  - policy processing precedence 253
  - practice exercise 268–271
  - practice exercise, using Group Policy Modeling 104–107
  - remote Group Policy update 262
- Group Policy Modeling
  - delegating permissions 251
  - practice exercise 275
- Group Policy Objects (GPOs) 66
  - administrative templates 296–302



## Group Policy Modeling

- advanced audit policies 614–620
  - practice exercise 641–645
- assigning applications 287
- backing up 243
  - practice exercise 269–271
- BitLocker, configuring 525
  - practice exercise 582–584
- block inheritance 254
  - practice exercise 275
- caching 260
- copying 246
- creating 249
- delegating management of 248–251
- deploying applications 285–291
- editing 249
- enforcing 254
- fixing problems 246
- importing 245
- linking 250
- loopback processing 258–260
  - practice exercise 271
- maintaining 241–251
- migrating 247
- .msi files, installing applications from 286
- permissions, delegating 248–251
  - practice exercise 265–268
- processing precedence 253
- publishing applications 288
- redirecting folders 282–285
  - practice exercise 324–328
- restoring 244
- scripts, deploying to users 291–293
  - practice exercise 329–332
- security filtering 255–257
  - practice exercise 273
- slow-link processing 260
- upgrading deployed packages 290
- .zap files, deploying installations with 286

Group Policy preferences 303–321

- Control Panel settings 319–321
- Internet Explorer, configuring 314
- item-level targeting 305
  - power options, configuring 309
  - practice exercise 336–338
- Local Users and Groups option 315
- mapping network drives 306–308
- mapping network printers 308
- power options, configuring 309–313
- practice exercise 331–338

- registry, configuring 314
- settings commonly used 303
- Windows settings 317–319

Group Policy Results, delegating permissions 251

Group Policy, using with WSUS 33

## H

HCAP (Host Credential Authorization Protocol), installing 346–350

health policies, configuring for NAP 395

Health Registration Authority (HRA). *See* HRA

health validators, configuring for Network Access Protection 392–399

Host Credential Authorization Protocol (HCAP).  
*See* HCAP

host records in DNS zones 148

HRA (Health Registration Authority) 397

- installing 346–350

Hub And Spoke topology 516

## I

IKEv2 tunneling protocol 444

Import-DfsrClone cmdlet 519

Import-GPO cmdlet 242

importing GPOs 245

inactive user accounts 75

-IncludeManagementTools switch 17

infrastructure master 186

Install-ADServiceAccount cmdlet 89

install images, used by WDS 17

Install.wim file 2

Install-WindowsFeatureWINS command 139

Internet Explorer, configuring with Group Policy preferences 314

Invoke-GPUupdate Windows PowerShell cmdlet 262

Invoke-WsusServerCleanup command 32

IP filters, configuring for Network Policy Server 367

IPsec enforcement, configuring for NAP 380–382

IP settings, configuring 368

item-level targeting 305

- power options, configuring 309
- practice exercise 336–338

## K

- Kerberos constrained delegation 91–94
- key distribution services root key, creating 88–90
- Key Signing Key (KSK) 156
- KRA (key recovery agent), using with EFS 533

## L

- L2TP/IPsec tunneling protocol 445
- linking GPOs 250
- link-local clouds 145
- Local Users and Groups option 315
  - practice exercise 333
- lockout policies. *See* account lockout policies
- logoff scripts 291
- logon auditing practice exercise 645–649
- logon scripts 291
  - mapping network drives 306–308
- loopback processing 258–260
  - practice exercise 271

## M

- mail exchanger (MX) records in DNS zones 149
- mail gateways, locating 149
- Managed Service Accounts 87
- mapping network drives 306–308
- mapping network printers 308
- Maximum Lifetime For Service Ticket policy 93
- Maximum Lifetime For User Ticket policy 93
- Maximum Lifetime For User Ticket Renewal policy 93
- Maximum password age policy 68
  - practice exercise 97
- Maximum Tolerance For Computer Clock Synchronization policy 93
- Merge (loopback processing) 259
- Message Analyzer tool 611–613
  - practice exercise 638–641
- metadata cleanup, Active Directory 203
- migrating GPOs 247
- Migration Table Editor (MTE) 247
- Minimum password age policy 68
  - practice exercise 98
- Minimum password length policy 69
  - practice exercise 99
- monitoring servers 591–611
  - using data collector sets 592–596

- practice exercise 621–626
    - using Event Viewer 599–609
    - using network monitoring 609–612
      - practice exercise 636–641
    - using performance counter alerts 597–599
  - /Mount-image switch 6
  - mounting Windows Server images 5
  - Move-ADDirectoryServerOperationMasterRole cmdlet 187
  - MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) 443
  - .msi files, installing applications from 286
  - multicast transmissions 14
    - configuring settings for 22, 24

## N

- Name Resolution Policy Table (NRPT), creating 156
- namespaces, DFS 511–513
  - practice exercise 558–560
- NAP. *See* Network Access Protection
- NAT (network address translation) 448–451
- Network Access Protection (NAP)
  - 802.1X enforcement, configuring 382–385
  - DHCP enforcement, configuring 377–380
    - practice exercise 401, 406–412
  - enforcement methods 376–390
  - health policies, configuring 395
  - health validators, configuring 392–399
  - IPsec enforcement, configuring 380–382
  - network policies, creating 369–373
  - RD Gateway enforcement, configuring 387–390
  - remediation server groups 398
    - practice exercise 405, 410
  - SHAs and SHVs, configuring 395
  - VPN enforcement, configuring 385–387
  - WSHV, configuring 392–394
    - practice exercise 403
- network address translation (NAT) 448–451
- Network Connectivity Assistant (NCA) 469
- network drives, mapping 306–308
- Network Location Server (NLS) 460, 463, 470
- network monitoring, for monitoring servers 609–612
  - practice exercise 636–641
- Network Policy Server (NPS) 345–376
  - authentication methods 357–359
    - configuring with 802.1X group policies 363–367
  - client configuration 363–367
  - connection request policies 350–363

## Network Location Server (NLS)

- adding conditions 353–356
- creating 361–363
- default policy 360
- forwarding 356
- network access servers, specifying type 351
- realm name, applying 359
- deploying 346–350
- encryption, selecting types of 368
- IP filters, configuring 367
- IP settings, configuring 368
- network policies
  - adding conditions 370–372
  - creating 369–373
- practice exercise 402
- RADIUS proxy and server 346
- templates 374–376
- Network Policy Service (NPS)
  - RADIUS accounting 429–432
    - practice exercise 480
  - RADIUS clients 426–429
    - practice exercise 479
  - RADIUS proxies 421–425
  - RADIUS servers 418–421
    - practice exercise 475–478
- network printers, mapping 308
- network topologies supported by DirectAccess 456
- network traffic, capturing using Message Analyzer 611–613
- Network Unlock feature, BitLocker 528
- New-ADDCCloneConfig Windows PowerShell cmdlet 198
- New-ADServiceAccount cmdlet 89
- New Delegation Wizard 130
- New-GPO cmdlet 243
- New Zone Wizard 124, 135, 143
- Next Secure (NSEC/NSEC3) record 155
- non-authoritative restore for Active Directory objects 214
- non-expiring passwords 71–73
  - practice exercise 107–110
- NPS. *See* Network Policy Server
- ntdsutil.exe command
  - creating Active Directory snapshots 204–206
  - defragmenting Active Directory database 200–203
  - performing authoritative restore 213
  - seizing FSMO roles 187

## O

- operations master
  - domain naming master 184
  - practice exercise 230–234
  - RID master 186
  - schema master 183
  - seizing FSMO roles 187
- operations masters
  - managing 182–187
  - practice exercise 230–234

## P

- packages, upgrading using Group Policy 290
- PAP (Password Authentication Protocol) 444
- pass-through mode, Web Application Proxy in 451
- Password must meet complexity requirements policy 69
  - practice exercise 100
- Password Never Expires option 71
- password policies
  - domain-based 66–70
  - fine-grained 76–84, 77–85
    - practice exercise 110–113
  - non-expiring passwords 71–73
    - practice exercise 107–110
  - practice exercise for configuring 96–100
- Password Replication Policy for RODCs 194–196
- Password Settings Container (PSC) 81
- Password Settings Object (PSO)
  - configuring 82–84
  - creating 81
- PDC emulator 185
- Peer Name Resolution Protocol (PNRP) 144
- performance counter alerts, for monitoring servers 597–599
  - practice exercise 628
- Performance Monitor 592–595
  - practice exercise 621–626
- permissions
  - setting for folder redirection 284
- (PNRP) Peer Name Resolution Protocol 144
- pointer (PTR) records in DNS zones 150
- policy processing precedence 253
- power options, configuring 309–313
- Power Options (Windows XP) 309–311
- Power Plans 312
- Power Scheme (Windows XP) 311

PPTP tunneling protocol 445  
 Pre-boot Execution Environment. *See* PXE  
 precedence, Group Policy processing 253  
 prestaging an RODC account 193  
 primary zones 127  
 PSO. *See* Password Settings Object  
 publishing applications 288  
 push partners and pull partners, configuring WINS servers 140  
 PXE-compliant network adapters 14–16  
 PXE response settings, configuring WDS with 19

## Q

quotas, FSRM 502  
 practice exercise 541–545

## R

RADIUS accounting 429–432  
 practice exercise 480  
 RADIUS clients 426–429  
 practice exercise 479  
 RADIUS, configuring 417–434  
 RADIUS proxies 421–425  
 RADIUS proxy 346  
 connection request policies and 359  
 RADIUS server 346  
 connection request policies and 359  
 RADIUS servers 418–421  
 practice exercise 475–478  
 RD Gateway enforcement, configuring for NAP 387–390  
 read-only domain controller. *See* RODC  
 realm name, applying to connection request policies 359  
 recovering Active Directory objects 208–215  
 recovering data  
 from BitLocker-protected volumes 525–528  
 from corrupted DFS databases 520  
 from EFS-encrypted files 532  
 Recycle Bin, Active Directory 208–210  
 practice exercise 234  
 redirecting folders 282–285  
 practice exercise 324–328  
 registry keys, selecting to monitor 595  
 registry settings, configuring with Group Policy preferences 314  
 relative identifiers (RIDs) 186  
 remediation server groups 398  
 practice exercise 405, 410  
 Remote Access role service  
 configuring on VPN server 438–443  
 installing 435–437  
 Web Application Proxy 451  
 practice exercise 483–489  
 Remote Access Setup diagram 465–473  
 configuring application servers 473  
 configuring infrastructure servers 470–472  
 configuring remote access servers 469  
 configuring remote clients 467–469  
 Remote Authentication Dial-In User Service. *See* RADIUS  
 Remote Desktop Services. *See* RDS  
 remote differential compression, used by DFS 514–516  
 remote Group Policy update 261  
 Remote Server Administration Tools (RSAT) 89  
 managing WDS with 16  
 removable device auditing practice exercise 641–645  
 Remove-GPO cmdlet 243  
 /Remove-ProvisionedAppxPackage switch 8  
 Rename-GPO cmdlet 243  
 Replace (loopback processing) 259  
 replica mode, configuring WSUS 30  
 replication, DFS 514–520  
 cloning databases 519  
 practice exercise 560–566  
 targets, adding 516  
 replication partners, configuring WINS servers 140  
 replication scope  
 configuring 125–127  
 practice exercise 161–163  
 Reset Account Lockout Counter After policy 71  
 practice exercise 103  
 resetting password permissions 78–80  
 Resource Monitor tool 610  
 Resource Record Signature (RRSIG) records 154  
 resource records in DNS zones 147  
 Restore-GPO cmdlet 243  
 restoring Active Directory objects 208–215  
 restoring GPOs 244  
 reverse lookup zones 128–130  
 RID (relative identifier) master 186  
 RODC (read-only domain controller) 190–197  
 Password Replication Policy 194–196  
 practice exercise 225–230

## schedules, replication

- Routing and Remote Access
  - configuring server routing 446–448
  - configuring VPN server 439–443
  - deploying 435–437
  - NAT (network address translation) 448–451
- Routing Information Protocol v2 (RIP) 446
- RSAT. *See* Remote Server Administration Tools

## S

- schedules, replication 517
- schema master 183
- scripts, deploying to users and computers 291–293
  - practice exercise 328–331, 329–332
- secondary zones 127
  - practice exercise 168–170
- security filtering for GPOs 255–257
  - practice exercise 273
- security identifiers (SIDs) 186
- security roles in WSUS 32
- seizing FSMO roles 187
- self-service password reset 79
- semantic integrity check, performing 200
- Server Core version of Windows Server
  - installing WDS on computers with 16
  - installing WSUS on computers with 28
- Server images. *See* Windows Server images
- servers, monitoring. *See* monitoring servers
- service principal names (SPNs) 94
- service tickets, determined by Kerberos policies 92
- servicing Windows Server images 4–11
  - practice exercise for 42
- Set-ADComputer cmdlet 92
- Set-ADDomainMode Windows PowerShell cmdlet 80
- Set-ADObject cmdlet 209
- Set-ADObject Windows PowerShell cmdlet 213
- Set-ADServiceAccount cmdlet 89, 92
- Set-ADUser cmdlet 92
- Set-DnsServerScavenging cmdlet 152
- SetSPN command-line utility 94
- Set-WsusClassification command 32
- Set-WsusProduct command 32
- Set-WsusServerSynchronization command 32
- shared folders, locating with DFS 511, 516
- shared secret, configuring 424, 427
- SHA (System Health Agent), configuring for NAP 395
- shutdown scripts 291
- SHV (System Health Validator), configuring for NAP 395

- signing DNS zones 153
- single-label name resolution solutions
  - GlobalNames zones 142–144
  - practice exercise 171
  - WINS 138–142
- slow-link processing 260
- snapshots, Active Directory 204–206
- software deployment using Group Policy 285–291
- SPAP (Shiva Password Authentication Protocol) 444
- Specify Intranet Microsoft Update Service Location policy 34
- split DNS 131
- SQL Server logging, configuring 430–432
- SSL certificate, obtaining for DirectAccess server 459, 463
- SSTP tunneling protocol 445
- staging folder, DFS 515
- stale resource records in DNS zones 151
- stand-alone namespaces 512
- startup scripts 291
- storage reports, FSRM 507
  - practice exercise 552–556
- Store Passwords Using Reversible Encryption policy 69
- stub zones 134
- subscriptions, event 603–606
  - practice exercise 630–635
- success and failure auditing, configuring 618–620
- Sysprep.exe utility 9
- System Health Agent (SHA), configuring for NAP 395
- System Health Validator (SHV), configuring for NAP 395

## T

- targeting categories when applying Group Policy preferences 305, 309
  - practice exercise 336–338
- tasks, event-driven 606–609
- templates for Network Policy Server (NPS) 374–376
- Ticket Granting Ticket (TGT) 93
- time synchronization, performed by PDC emulator 185
- tombstone lifetime setting 212
- tombstone reanimation 214
- topologies supported by DirectAccess 456
- topology, replication 516
- TPM (Trusted Platform Module), using with BitLocker 523–525
- transport agent policies, configuring for an HRA 398
- Trust anchors 155

tunneling protocols, VPN 444–446  
two-factor authentication, configuring 458

## U

Uninstall-ADDSDomainController cmdlet 203  
universal group membership caching (UGMC) 189  
/Unmount-Wim switch 9  
update deployment using WSUS 28  
update files, downloading 40–42  
upgrading deployed packages 290  
User Configuration settings 258–260  
user password policies, domain-based 66–70  
user tickets, determined by Kerberos policies 92

## V

views of event logs 601–603  
virtual service accounts 90  
VPN authentication protocols 443–446  
VPN enforcement, configuring for NAP 385–387  
VPN servers  
    configuring Remote Access role service on 438–443  
    practice exercise 481–483  
VPN settings, configuring 437–446  
VPN tunneling protocols 444–446

## W

WDS. *See* Windows Deployment Services  
Web Application Proxy 451  
    practice exercise 483–495  
wecsvc (Windows Event Collector) 604  
Windows Assessment and Deployment Kit (Windows ADK) 12  
Windows Deployment Services (WDS) 14–27  
    client naming policy for 20  
    configuring 19–23  
        practice exercise for 47–51  
    driver packages, importing into 25  
        practice exercise for 52–54  
    images, importing into 17–19  
    installing on Server Core versions 16  
    multicast transmissions 14, 22  
    practice exercise for 43–47  
    requirements for 15  
    transmissions, configuring 24  
Windows Imaging (WIM) files 2  
    practice exercise for servicing 42  
Windows PE 17  
Windows PowerShell  
    importing 16  
    support in WSUS 28, 31  
Windows Security Health Validator (WSHV), configuring  
    for NAP 392–394  
Windows Server Backup, installing 210  
Windows Server images  
    adding device drivers to 6  
    answer files and 12  
    automating deployment of 12–14  
    build and capture process 9  
    committing 9  
    configuring 3  
    deploying automatically 11–27  
    mounting 5  
    payload-removed features of 8  
    servicing 4–11  
    software updates to 6  
    understanding 2  
Windows Server Update Services (WSUS) 27–39  
    automatic approval rules for 36–38  
    configuring, practice exercise for 56–58  
    deploying 28–32  
        practice exercise for 54–56  
    deploying updates 35  
    groups  
        creating 33  
        practice exercise for 58  
    installing on Server Core versions 28  
    new features of 28  
    policies 33  
    replica mode, configuring 30  
    security roles in 32  
    updating files 30  
    Windows PowerShell support in 28, 31  
Windows settings, configuring with Group Policy preferences 317–319  
Windows System Image Manager (Windows SIM) 12  
WinRM (Windows Remote Management) 604  
WINS, configuring 138–142  
wired network policies, configuring 363–367  
wired networks, configuring 802.1X enforcement for 383  
wireless network policies, configuring 363  
wireless networks, configuring 802.1X enforcement for 384

## **.zap files**

WMI filters

and Group Policies 257

delegating ability to create 251

WSHV (Windows Security Health Validator), configuring  
for NAP 392–394

practice exercise 403

WSUS. *See* Windows Server Update Services

## **Z**

.zap files, deploying applications with 286

zone delegation 129

practice exercise 163–168

Zone Signing Key (ZSK) 156

zone transfers

managing 127

practice exercise 168