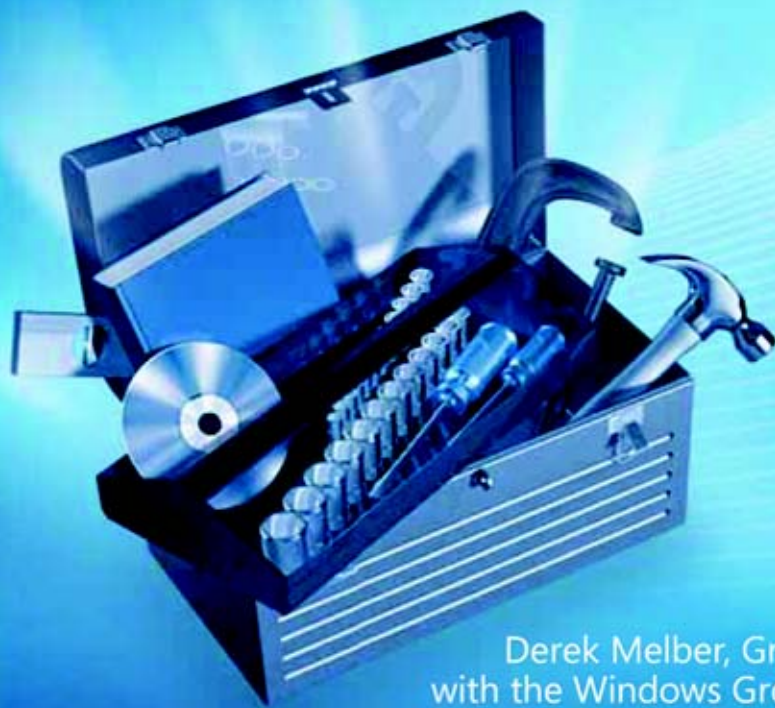


Microsoft

Windows® Group Policy

Windows Server® 2008 and Windows Vista®

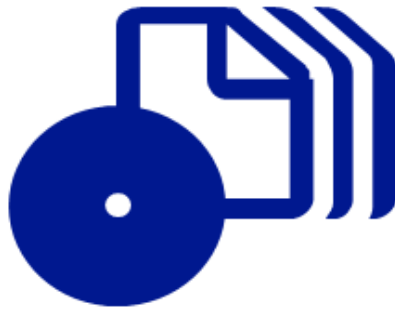


Derek Melber, Group Policy MVP
with the Windows Group Policy Team

Resource Kit



How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to <http://aka.ms/625143/files>, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

PUBLISHED BY

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

Copyright © 2008 by Derek Melber

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: 2008920568

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWT 3 2 1 0 9 8

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to rkinput@microsoft.com.

Microsoft, Microsoft Press, Active Desktop, Active Directory, ActiveX, BitLocker, Excel, FrontPage, HotStart, InfoPath, Internet Explorer, NetMeeting, OneNote, Outlook, PowerPoint, SideShow, Visio, Visual Basic, Visual Studio, Windows, Windows Live, Windows Media, Windows NT, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail 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: Martin DelRe

Developmental Editor: Karen Szall

Project Editor: Valerie Woolley

Editorial Production: S4Carlisle Publishing Services

Technical Reviewer: Linda Zacker; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Cover: Tom Draper Design

Body Part No. X14-55483

To Alexa and Ashelley, where I find inspiration, free spirit, and love without boundaries.

Contents at a Glance

Part I Introducing Group Policy

- 1 Why Group Policy? 3
- 2 What's New in Windows Vista and Windows Server 2008 23
- 3 Group Policy Basics 39

Part II Group Policy Structure

- 4 Architecture of Group Policy 67
- 5 Group Policy Processing 93

Part III Administering Group Policy

- 6 Using the GPMC 119
- 7 Advanced GPMC Management 141
- 8 Controlling GPOs with Scripts and Automation 173

Part IV Implementing Security

- 9 Security Delegation for Administration of GPOs 203

Part V Using Registry-Based Policy Settings

- 10 ADM Templates, ADMX Files, and the ADMX Central Store 233
- 11 Customizing ADM Templates and ADMX Files 257

Part VI Group Policy Settings

- 12 Group Policy Preferences 301
- 13 Settings Breakdown for Windows Server 2008
and Windows Vista 349

Part VII Advanced Topics

- 14 Advanced Group Policy Management 399
- 15 Troubleshooting GPOs 427

Part VIII Appendices

A	Third-Party Group Policy Tools	469
B	Additional Resources.....	489
	Index	497

Table of Contents

Dedication	iii
Acknowledgments.....	xvii
Introduction.....	xix

Part I Introducing Group Policy

1	Why Group Policy?.....	3
	The Past, Present, and Future of Group Policy.....	3
	Group Policy's Past.....	3
	Group Policy's Present.....	5
	Group Policy's Future.....	12
	Benefits of Group Policy.....	14
	More Efficient Management.....	15
	More Powerful Management.....	16
	Reliability.....	16
	Extensibility.....	17
	Security.....	17
	Diversity.....	18
	Consistency.....	18
	Stability.....	19
	Group Policy Negatives.....	19
	Summary.....	20
	Additional Resources.....	21
2	What's New in Windows Vista and Windows Server 2008.....	23
	Remember When.....	23
	New and Now.....	24
	New Group Policy Features in Windows Vista.....	24
	New Group Policy Features in Windows Server 2008.....	31

 **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/

- So, What About Those DesktopStandard Products? 36
- Summary 37
- Additional Resources 37
- 3 Group Policy Basics 39**
 - Group Policy Defined 40
 - Structural Overview of a GPO 40
 - Computer Configuration 42
 - User Configuration 44
 - Local GPOs 46
 - Local Policy Object 47
 - Administrators and Non-Administrators Local GPOs 47
 - Managing the Local GPOs 51
 - GPOs in Active Directory 52
 - Default GPOs 54
 - Default Domain Policy 55
 - Default Domain Controllers Policy 58
 - Creating Additional GPOs 61
 - Privileges for Creating New GPOs 62
 - Creating GPOs Correctly 62
 - Summary 64
 - Additional Resources 64

Part II Group Policy Structure

- 4 Architecture of Group Policy 67**
 - Group Policy Dependencies 68
 - Active Directory and Group Policy 68
 - Domain Name System 69
 - Replication 70
 - DFS 71
 - New Group Policy Service 72
 - Domain Controller Selection During GPO Management 73
 - Using the PDC Emulator 74
 - Selecting the Domain Controller for GPO Editing 75
 - Architectural Parts of a GPO 76
 - Group Policy Template 77

Group Policy Container	80
GPO Replication	84
Group Policy Template and SYSVOL Replication	84
Active Directory Replication	86
Client-Side Extensions	88
Summary	91
Additional Resources	91
5 Group Policy Processing	93
Scope of Management	93
Group Policy Processing	96
GPO Precedence for GPOs Linked to Different Nodes	97
GPO Precedence for GPOs Linked to the Same Node	99
Group Policy Processing Events	100
Background GPO Policy Processing	100
Foreground Group Policy Processing	101
Asynchronous vs. Synchronous Policy Processing	103
Using GPOUpdate	105
Version Checking During Updates	107
GPO Version Numbers on the Client	107
GPO Version Numbers on the Domain Controller	108
NLA Refresh in Windows Vista and Windows Server 2008	108
Altering Default GPO Processing and Inheritance	109
Block Policy Inheritance	109
Enforce	111
Security Filtering	112
WMI Filters	113
Group Policy Preferences	115
Summary	116
Additional Resources	116
Part III Administering Group Policy	
6 Using the GPMC	119
Getting Around in the GPMC	119
Launching the GPMC from Windows Server 2008	119
Launching the GPMC from Windows Vista	120
Domain Views in the GPMC	120

	Forest Views in the GPMC	121
	Site Views in the GPMC	122
	GPMC Management Limitations.....	122
	Selecting Domain Controllers for Administration of GPOs.....	123
	Administering GPOs	124
	Creating GPOs	124
	Linking GPOs	126
	Managing GPO Configurations.....	128
	Managing GPO Backups.....	130
	Starter GPOs.....	135
	Summary.....	138
	Additional Resources.....	139
7	Advanced GPMC Management	141
	Working with GPOs.....	141
	Searching GPOs	142
	Filtering Administrative Templates in the GPME	146
	Reporting on GPOs	148
	Group Policy Results	151
	Group Policy Modeling.....	154
	Comments.....	159
	Migrating GPOs	162
	Reasons for Migrating GPOs	162
	Requirements for Migrating GPOs Between Domains.....	163
	Settings in a GPO That Require Translation.....	163
	Migrating GPOs Across Domains	164
	Migration Tables.....	168
	Summary.....	171
	Additional Resources.....	171
8	Controlling GPOs with Scripts and Automation	173
	GPMC Scripts	173
	Backing Up and Restoring GPOs.....	174
	Copying and Importing GPOs.....	177
	Creating GPOs and Other GPMC Objects	179
	Deleting GPOs	183
	GPO Reporting.....	183
	Finding GPOs Based on Parameters.....	188

GPO Security	192
VBScript Scripting	197
Windows PowerShell	197
Summary	199
Additional Resources	199

Part IV Implementing Security

9	Security Delegation for Administration of GPOs	203
	Default Security Environment	203
	Default Security of the GPMC	204
	Default Security of AGPM	204
	Group Policy Management Console Delegation	207
	Creating GPOs	208
	Linking GPOs	211
	Managing GPOs	213
	Editing GPOs	215
	Modeling GPOs	216
	RSOP of GPOs	218
	Advanced Group Policy Management Delegation	218
	Full Control	218
	Editing	220
	Approving	221
	Reviewing	222
	Best Practices	224
	Creating GPOs	224
	Editing GPOs	225
	Linking GPOs	226
	Testing GPOs	226
	Summary	228
	Additional Resources	229

Part V Using Registry-Based Policy Settings

10	ADM Templates, ADMX Files, and the ADMX Central Store	233
	Administrative (.adm) Templates	234
	Default .adm Templates	234
	Working with .adm Templates	236

Default Installed .adm Templates	236
Importing .adm Templates	237
Adding .adm Templates	237
Removing .adm Templates	238
Managing .adm Templates	239
Policies vs. Preferences	242
ADMX Files	243
Default ADMX Files	243
Using Both .adm Templates and ADMX Files	244
Scenario 1: Administration of GPO with Windows Vista	244
Scenario 2: Administration of GPO with a Windows Server 2008 Domain Controller	244
Scenario 3: Administration of GPO from a Windows XP Workstation	245
Migrating .adm Templates to ADMX Files	245
File Syntax Conversion for .adm Template to ADMX Files	246
ADMX Migrator	249
Creating and Using the ADMX Central Store	251
Creating the Central Store	251
Copying ADMX and ADML Files to the Central Store	253
Summary	254
Additional Resources	255
11 Customizing ADM Templates and ADMX Files	257
Creating Custom .adm Templates	257
A Simple .adm Template	258
Using .adm Template Language	259
Structure of an .adm Template	260
#if version	261
Syntax for Updating the Registry	262
Syntax for Updating the GPME Interface	266
Additional Statements in the .adm Template	278
String and Tab Limits for .adm Templates	280
Best Practices for .adm Templates	281
Creating Custom ADMX and ADML Files	283
ADMX Schema	283
ADMX File Structure	284
ADML File Structure	285
Core ADMX File Concepts	286
Tying the ADMX and ADML Files Together	289

Using ADMX File Language	291
Summary	297
Additional Resources	297

Part VI Group Policy Settings

12	Group Policy Preferences	301
	Benefits of Group Policy Preferences	302
	User-Friendly Interface	302
	Thousands More Settings	303
	Practical and Valuable Settings	304
	Reduced Desktop Images	304
	Reduced Need for Log-on Scripts	304
	Working with Any Organizational Unit Design	305
	Preferences vs. Policies	306
	Management and Support of Group Policy Preferences	307
	Managing Group Policy Preferences Using the GPME	308
	Deploying the Group Policy Preferences CSEs	309
	Group Policy Preferences Settings	309
	Group Policy Preferences: Windows Settings	310
	Group Policy Preferences: Control Panel Settings	316
	Advanced Group Policy Preferences Settings	323
	Action Modes	323
	Common Tab	324
	Item-Level Targeting	326
	Process Variables	344
	Group Policy Preferences in Settings Reports	346
	Software Development Kit for Group Policy Preferences	347
	Summary	348
	Additional Resources	348
13	Settings Breakdown for Windows Server 2008 and Windows Vista	349
	Overall GPO Structure	349
	Policies	350
	Software Settings	350
	Windows Settings	352
	Administrative Templates	368
	Preferences	372
	Terminal Services	373

- User Account Control 376
- Log-on Scripts 377
- Servers 382
- Hardware Components 385
- Network Security 390
- Summary 395
- Additional Resources 395

Part VII Advanced Topics

- 14 Advanced Group Policy Management 399**
 - Architecture of AGPM 400
 - Operating System Support 400
 - GPMC Requirements 401
 - Server Installation 401
 - Client Installation 406
 - Offline Editing of GPOs 407
 - Change Management 408
 - When the Changes Were Made 409
 - Who Made the Changes 409
 - What Changes Were Made 409
 - Workflow 410
 - E-Mail Configuration 411
 - Pending Tab 412
 - Creating GPOs 413
 - Deploying GPOs 415
 - Rolling Back and Rolling Forward 417
 - Reporting 418
 - Settings Reports 418
 - Difference Reports 419
 - Using Templates 421
 - Recycle Bin 422
 - Restoring GPOs and GPO Links 423
 - Summary 424
 - Additional Resources 425
- 15 Troubleshooting GPOs 427**
 - Group Policy Troubleshooting Essentials 427

Common Problems with GPOs	428
DNS-Related Problems	428
Asynchronous Group Policy Processing	429
Foreground-Only GPO Settings	430
Network Connection	430
GPO Function after WMI Filter Deletion	430
Time Synchronization	431
Unavailable PDC Emulator	431
Using Event Logging for Troubleshooting	432
Group Policy Operational Log	433
Event Viewer Troubleshooting Procedure	437
Summary of Group Policy Event IDs	447
Common GPO Troubleshooting Tools	458
GPLogView	458
GPMC	460
Dcgpofix.exe	460
GPMonitor.exe	462
GPResult	462
GPOUpdate	464
GPOTool	464
Summary	465
Additional Resources	465

Part VIII **Appendices**

A	Third-Party Group Policy Tools	469
B	Additional Resources	489
	Index	497

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/

Acknowledgments

To my two beautiful girls, Alexa and Ashelley. They are patient and loving through the most troubling times in life. Thank you for teaching me what is important in life. Know I will always be here for you and will always love you above all others.

To my mom, Mary, and grandma, Opal. Where my strength, perseverance, logic, stubbornness, intelligence, caring, giving, and love for others come from. I love and admire these women for what they have accomplished in their lives and how they give to others so freely.

To my friends, who are more like family than just friends: Videssa, Frank, Michael, Danny, Bobby, Jeff, Morgan, Jim, Gordon, my racquetball buddies, friends at TechMentor, friends at the gym, and friends at the cabin.

To the entire Group Policy team for their insight, inside information, dedication to the book, dedication to Group Policy technology, and friendship. To the other Group Policy MVPs, thanks for helping me and keeping the entire Group Policy technology moving forward. To Darren, Todd, Rick, Don, Greg, Kevin, Mark, Kurt, Dan, Mark, and Jeremy, who provide guidance when things are not clear, direction when things stray, correction when things are wrong, and friendship all the time. To my friends in the industry who are supportive, honest, true, and always there for one another.

To the Microsoft Press team of acquisition editors, copy editors, technical editors, and reviewers. Without your in-depth diligence and attention to detail, the book would not be the top-notch quality document that it is today. Thank you!

To all who read my books, read my articles, come to see me speak, and trust me with your most important questions. It is an honor to be a part of this community with you, and I hope that I can continue to provide the technology insight, clarity, and excitement that I have been able to so far.

A special thanks to Videssa Djucich, Darren Mar-Elia, Chris Terpening, Kevin Sullivan, and Mark Gray, who helped with so much of the research, formatting, and support with the book. Thank you very much!

List of Reviewers from the Group Policy Team

Nafisa Bhojawala, program manager

Bryan Garretson, software design engineer in test

Joe Gettys, software design engineer in test

Mark Gray, program manager

Lilia Gutnik, program manager

Judith Herman, programming writer

Rajive Kumar, senior development lead

Jason Leznek, senior product manager

Kevin Sullivan, senior program manager lead

Sreeram Vaidyanath, software design engineer in test

Introduction

Welcome to this in-depth and comprehensive book on Group Policy. The Microsoft Group Policy team, the Group Policy Most Valuable Professionals (MVPs), and members of many other departments at Microsoft have spent countless hours molding Group Policy and making it what it is today. *Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista* explores the technology that is Group Policy, as well as some of the most innovative, exciting, and powerful additions to Group Policy that you could ever imagine or hope for.

Group Policy has been upgraded, expanded, and enhanced with features, functionality, and capabilities. Group Policy has more than 5,000 individual settings, nearly 40 client-side extensions (CSEs), and management capabilities that make Group Policy administration simple, so you will have no choice but to start to use Group Policy more in your Windows Server 2008 and Windows Vista environments. This book is meant to be your desktop reference, guide, and inside look into the foundational concepts of Group Policy, as well as its new and innovative features. If you are an IT professional who works in any way with Windows Active Directory, this book will make you more adept, efficient, and competent at designing, implementing, and troubleshooting Group Policy.

This book contains all of the technical detail you have come to expect from a Microsoft Resource Kit. The author, Derek Melber, has been crafting the outline and contents of this book for years. Derek has spoken and written about Group Policy for the past nine years and delivers an authoritative, world-class view and description of Group Policy for your reading pleasure, as well as for your career stability and growth. Derek has more than 15 books on his resume, and this book is at the apex of his career and publication library. With the assistance of the Microsoft Group Policy team and his friends and colleagues, Derek presents to you his “masterpiece.”

Overview of the Book

The book has 15 chapters and two appendices, with additional information included on the CD. The book is divided into eight sections.

Part I: Introducing Group Policy

- **Chapter 1, “Introduction to Group Policy”** This chapter provides an overview of what Group Policy technology is, as well as terminology that you will need to know when reading the book.
- **Chapter 2, “What’s New in Windows Vista and Windows Server 2008 with Group Policy”** This chapter focuses on the new features, technologies, and tools that you will see when you work with Group Policy in Windows Server 2008 and Windows Vista.

- **Chapter 3, “Group Policy Basics”** This chapter provides the fundamentals that everyone needs to work with Group Policy.

Part II: Group Policy Structure

- **Chapter 4, “Architecture of Group Policy”** This chapter provides an in-depth discussion of the core architecture of Group Policy, including Group Policy object (GPO) storage and details, as well as CSEs, which do the majority of the work of Group Policy.
- **Chapter 5, “Group Policy Processing”** Group Policy has a default and stable processing flow. You will see how this default behavior works, and you will learn about all of the toggles and switches available for altering this behavior when you need to.

Part III: Administering Group Policy

- **Chapter 6, “GPMC Basics”** The Group Policy Management Console (GPMC) is your command center for Group Policy management. This chapter focuses on the basics of the tool that you will need to be proficient.
- **Chapter 7, “Advanced GPMC Management”** This chapter discusses many of the new features and technologies that have been included in the new version of the GPMC.
- **Chapter 8, “Controlling Group Policy via Scripts and Automation”** Automation is a highly relevant topic today, and this chapter guides you through the tools and options that you can use to make your Group Policy management an automated process.

Part IV: Implementing Security

- **Chapter 9, “Security Delegation for Administration of GPOs”** Both the GPMC and Microsoft Advanced Group Policy Management (AGPM) provide mechanisms for securing the management of Group Policy. This chapter provides a description of how the technology works and describes how to implement a security structure that meets your needs.

Part V: Using Registry-Based Policy Settings

- **Chapter 10, “ADM Templates, ADMX Files, and the ADMX Central Store”** Much of Group Policy relies on the settings that are defined and described in .adm templates and ADMX files. As explained in this chapter, .adm templates are still used today, but the new ADMX file structure is innovative and more powerful than its predecessor.
- **Chapter 11, “Customizing ADM Templates and ADMX Files”** If the standard capabilities provided by .adm templates and ADMX files are not enough, you can create your own custom environment with both technologies. This chapter explains how to do this.

Part VI: Group Policy Settings

- **Chapter 12, “Group Policy Preferences”** With over 3,000 individual settings, Group Policy Preferences is a feature that should get your attention. This chapter focuses on this new and innovative addition to Group Policy.
- **Chapter 13, “Settings Breakdown for Windows Server 2008 and Windows Vista”** This chapter is meant to be a guide to the overall structure and settings capabilities that Group Policy provides. The chapter provides guidelines for grouping related settings, as well as a description of what each major section in a GPO is designed to do.

Part VII: Advanced Topics

- **Chapter 14, “Advanced GPO Management with AGPM”** Advanced Group Policy Management (AGPM) is a Microsoft tool that allows you to perform offline editing, change management, reporting, and so much more with your Group Policy infrastructure. This chapter explores every facet of AGPM to help you install and use it immediately.
- **Chapter 15, “Troubleshooting GPOs”** This chapter introduces the new Microsoft tools and capabilities that can help you track, pinpoint, and fix issues related to Group Policy.

Part VIII: Appendices

- **Appendix A, “Third-Party Group Policy Tools”** Microsoft has been working on updating and improving Group Policy, but so have many companies that provide Group Policy software and solutions. This chapter gives you a quick, yet solid, overview of the tools available, and it explains where to go to get help with Group Policy beyond this book.
- **Appendix B, “Additional Resources”** Some great resources are available when it comes to Group Policy knowledge and technology. This chapter helps you find the information you need.

Find Additional Content Online As new or updated material becomes available that complements your book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. Based on the final build of Windows Server 2008, the type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site will be available soon at <http://www.microsoft.com/learning/books/online/serverclient>, and it will be updated periodically.

Document Conventions

The following conventions are used in this book to highlight special features or usage.

Reader Aids

The following reader aids are used throughout this book to point out useful details.

Reader Aid	Meaning
Best Practices	
Caution	Warns you that failure to take or avoid a specified action can cause serious problems for users, systems, data integrity, and so on.
Important	Calls attention to essential information that should not be disregarded.
Note	Underscores the importance of a specific concept or highlights a special case that might not apply to every situation.
On the CD	Calls attention to a related script, tool, template, or job aid on the Companion CD that helps you perform a task described in the text.
Tip	
Warning	

Sidebars

The following sidebars are used throughout this book to provide added insight, tips, and advice concerning different Windows Vista features.

Sidebar	Meaning
Direct from the Source	Contributed by experts at Microsoft or MVPs to provide “from-the-source” insight into how Windows Vista works, best practices for managing security, and troubleshooting tips.
How It Works	Provides unique glimpses of Windows Vista features and how they work.

Command-Line Examples

The following style conventions are used in documenting command-line examples throughout this book.

Style	Meaning
Bold font	Used to indicate user input (characters that you type exactly as shown).
<i>Italic font</i>	Used to indicate variables for which you need to supply a specific value (for example, file_name can refer to any valid file name).
Monospace font	Used for code samples and command-line output.
%SystemRoot%	Used for environment variables.

Companion CD

In addition to the book itself, you also get a CD that contains some great tools and other resources. System requirements for running the CD are at the back of this book. The CD includes the following resources.

Elevation Tools

Many of the third-party Group Policy vendors have kindly provided evaluation versions of their tools that you can install and use to see how Group Policy can be taken to another level.

Management scripts

On the CD-ROM accompanying this book you will find a collection of scripts that illustrate working with Group Policy from within Windows Powershell. These scripts, while illustrative in nature, actually perform some very useful tasks and can simplify many common scenarios faced by network admins. These tasks include reporting on orphaned Group Policy Objects, creating Group Policy Objects, and auditing application of Group Policy Objects. For complete information on these exciting and powerful scripts please refer to the read me file in the same folder as the Group Policy Scripts.

eBook

If you would rather have a searchable electronic copy of the book, there is one on the CD.

Chapter-Related Materials

Some chapters have additional documentation or electronic tools; these are mentioned in the book text and located on the CD.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD. Visit <http://www.microsoftpressstore.com/title/9780735625143> to get your downloadable content. This content is always up-to-date and available to all readers.

Resource Kit Support Policy

Every effort has been made to ensure the accuracy of this book and the Companion CD content. Microsoft Press provides corrections to this book through the Web at the following location:

<http://www.microsoft.com/learning/support/search.asp>

The CD that accompanies the print edition of this book is not available with this eBook edition, although select CD content is available for download at <http://www.microsoftpressstore.com/title/9780735625143>.

If you have comments, questions, or ideas regarding the book or Companion CD content, or if you have questions that are not answered by querying the Knowledge Base, please send them to Microsoft Press by using either of the following methods:

E-mail:

rkinput@microsoft.com

Postal Mail:

Microsoft Press
Attn: Microsoft Group Policy Resource Kit, *Editor*
One Microsoft Way
Redmond, WA 98052-6399

Please note that product support is not offered through the preceding mail addresses. For product support information, please visit the Microsoft Product Support Web site at the following address:

<http://support.microsoft.com>

What's New in Windows Vista and Windows Server 2008

In this chapter:

Remember When	23
New and Now	24
Summary	37
Additional Resources	38

There has been a distinct push in recent years to make Group Policy a more integrated, reliable, stable, and useful product within Active Directory directory service. That is not to say that it has not been all of these things, but efforts within the Group Policy team and supporting teams have put great emphasis on making Group Policy even better in these areas.

Each iteration of Group Policy has brought something impressive. The continual improvement of technology is a testament to all of the teams working to make the technology work better and more efficiently for customers.

Remember When

If you look back at some of the major milestones in the life cycle of Group Policy, you will note that there have been distinct times of radical and amazing changes. Table 2-1 summarizes these milestones.

Table 2-1 Group Policy Technology Milestones

Place in Time	Feature
Windows 2000	Approximately 900 total Group Policy settings
Windows XP	Approximately 1,400 total Group Policy settings
Windows Server 2003	Group Policy Management Console 1.0 introduced as an add-in
Windows XP SP2	Approximately 1,600 total Group Policy settings
Windows Vista	Approximately 2,400 total Group Policy settings and Advanced Group Policy Management made available
Windows Server 2008	Group Policy Management Console 2.0 updated and added to Server Manager; Preferences added

Windows 2000 introduced Group Policy and accumulated about 900 settings before Windows XP shipped. When Windows XP shipped, there was a bit of “flux” in the industry as administrators tried to juggle the Windows 2000 settings, Windows XP settings, and ADM templates that shipped with each operating system. The Group Policy Management Console (GPMC) was a major improvement, because it moved the administration of Group Policy objects (GPOs) from the Active Directory Users and Computers snap-in to the GPMC snap-in. Of course, the GPMC also provided a lot of new functionality, which we will discuss in Chapter 7, “Using the GPMC.”

Windows XP Service Pack 2 (SP2) was a milestone, not only for Group Policy, but for Microsoft as a company. The security efforts that came along with SP2 were revolutionary, and Microsoft continues to use these efforts as a baseline for any desktop operating system. Microsoft views Windows Server 2003 SP1, the partner to Windows XP SP2, as the baseline for server operating systems.

New and Now

Now that Windows Vista and Windows Server 2008 have arrived, so have some new and cool technologies for Group Policy. Don't fret. The same great features are still there; they have just been enhanced and made more spectacular. Settings are expanded, new features abound, and many features that members of the community have wanted for a long time have finally arrived.

Some of these features came with Windows Vista. Features such as ADMX files and the ADMX central store have already been used by those who use Windows Vista. Because Windows Vista was released quite a few months before Windows Server 2008, some of these technologies might be more familiar to you. Windows Server 2008 introduced some great new features tied into the GPMC that will make administrative life much simpler when working with Group Policy. Some of the new features include searching GPO settings, filtering GPO settings, and adding the Preferences to all GPOs. Other technologies, like PolicyMaker from DesktopStandard, will show up in a GPO as Group Policy Preferences. A final addition, Advanced Group Policy Management (AGPM), works with Windows Server 2008 and Windows Vista to ensure management of GPOs is secure, stable, and consistent. AGPM is available through the Microsoft Desktop Optimization Pack (MDOP).

New Group Policy Features in Windows Vista

Windows Vista arrived on the market in early 2007. The new features that it introduced have had a significant effect in the Group Policy community. Windows Vista not only provides some impressive new graphical enhancements, it also comes with some overall changes to Group Policy that can affect the entire network of desktops—not just single machines. (The exception is the Multiple Local GPO enhancements, which do affect just one desktop at a time.) The new features that can affect either one desktop or many desktops include the following:

- Network Location Awareness
- ADMX templates
- ADMX repository
- Improved logging

Multiple Local GPOs

Some historical background will help you understand what has changed with local GPOs on a Windows Vista desktop. In previous versions of Windows, there was a single local GPO on every server and desktop. Beyond the local GPO on the individual computers, there could be many GPOs in Active Directory linked to the domain, organizational units, and sites. The local GPO had no power over the Active Directory GPOs unless nonconflicting settings were established. In such a case, the local GPO settings would make their way through the maze of Active Directory GPOs to the Resultant Set of Policy (RSOP) that molded the final policy settings on the computer.

Multiple Local GPOs were put into place in Windows Vista to solve many issues. One of the biggest problems this feature solves involves handling the ability for both users and administrators to log on to the same desktop, but be treated differently. Before Windows Vista, if local GPOs were configured to constrain the user account, both the administrator accounts and regular user accounts would receive the constraining settings. This caused some very odd results, either allowing the user to have too many privileges or restricting the administrator too severely. If the administrator needed to run elevated tasks in a restricted environment like this, he or she was forced to use “Run As” or other privilege-elevating technologies. Although this is an almost ideal situation, it can cause some issues in companies that do not want such restrictions on administrators logging on to desktops.

Windows Vista tackles all of these issues with new technology related to the local GPO. In reality, there is no longer just a single GPO on the local desktop, but three local GPOs, which Microsoft refers to as Multiple Local Group Policy objects (MLGPO). These three GPOs provide granular control over the users who log on to the desktop. Local GPOs can be used in a single-computer environment, home environment, small business environment, or even large corporate scenario.

The three local GPOs are designed to control desktop users in a hierarchical manner. This hierarchy allows control over the settings that will be configured in GPO. The three MLGPO options consist of the following, in their proper hierarchical order:

- Local Policy Object
- Administrators and Non-Administrators Local Group Policy
- User-specific Local Group Policy

Local Computer Policy Object The Local Computer Policy Object is identical to the local GPO in Windows 2000 and Windows XP. It can be accessed by using the Group Policy Management Editor (by running Gpedit.msc from the Run dialog box) or using the Microsoft Management Console (MMC). In either case, you can control both Computer Configuration and User Configuration settings, as shown in Figure 2-1.

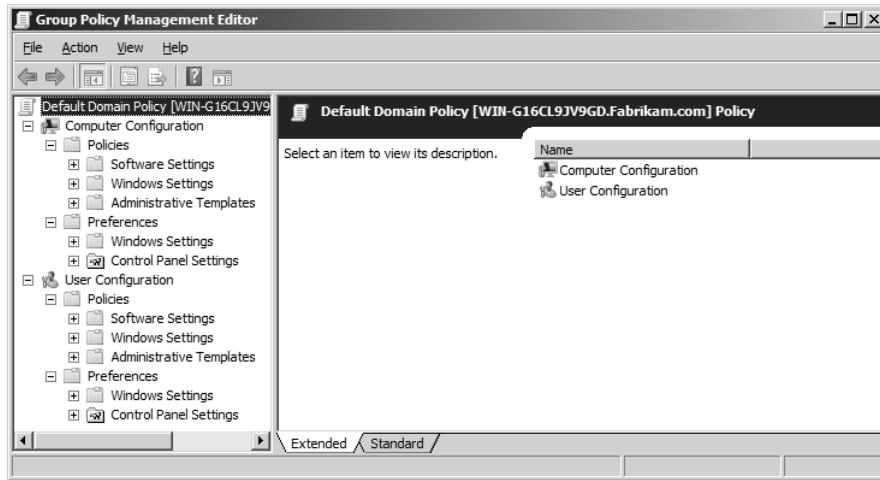


Figure 2-1 The local Group Policy can be opened in the Group Policy Management Editor by clicking Start, clicking Run, and then typing gpedit.msc in the Run dialog box.

Administrators and Non-Administrators Local GPOs The Administrators local GPO and the Non-Administrators local GPO are new in Windows Vista. As their names indicate, the GPOs in this layer are designed to control two types of user accounts. The delineation is based on which users have membership in the local Administrators group.



Note User accounts that belong to the Power Users group are not considered Administrators and will not be affected by GPO settings under the Administrators local GPO. Rather, they will be affected by the GPO settings in the Non-Administrators local GPO.

The reason for this delineation is obvious. The settings for administrator-type accounts and nonadministrator-type accounts should be different on a desktop. Without these two options for local GPOs, it is nearly impossible to make a distinction between these two types of user accounts.

These two GPOs are not easy to access, however. To access these GPOs, you must use the MMC. This console exposes both of these GPOs so that administrators can manage them, as shown in Figure 2-2.

User-Specific Local GPO The final local GPO layer is the user-specific local GPO. This GPO offers definitive granular control because it allows you to specify an individual user account to

receive special GPO settings. Do not use this GPO option very often, because individual user account settings are typically discouraged from an administrative efficiency standpoint.

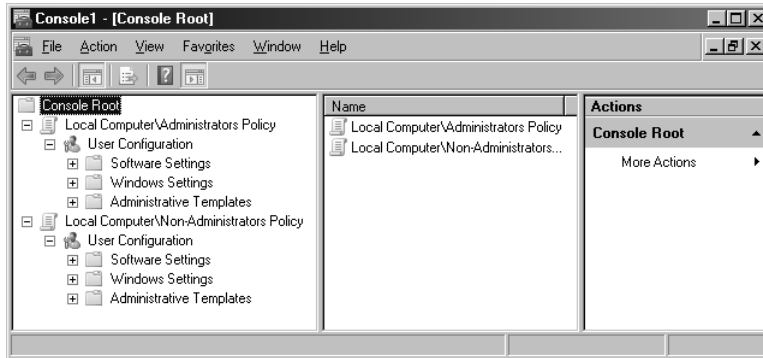


Figure 2-2 Both the Administrators local GPO and the Non-Administrators local GPO can be edited in the MMC.

This type of GPO is very useful on specialized desktops throughout the environment. Such desktops might include those functioning as a kiosk, those in a training or educational facility, or even those that have a shared user account. In such cases, the user account used to log on to these special desktops has a unique set of GPO settings, where all other user accounts are controlled by the Local Policy Object or even the Administrators or Non-Administrators local GPOs.

You do not access the administration of this type of GPO through the Group Policy Management Editor directly; rather, it is accessed through the MMC. When using the MMC to open this GPO, you select the GPO that is associated with any one of the local user accounts that are configured in the local Security Accounts Manager (SAM). After you add your GPO into the MMC, the interface will include only User Configuration settings. Because this local GPO affects user accounts only, the MMC removes Computer Configuration settings so that they do not confuse the administrator of the local GPO. This can be seen in Figure 2-3.

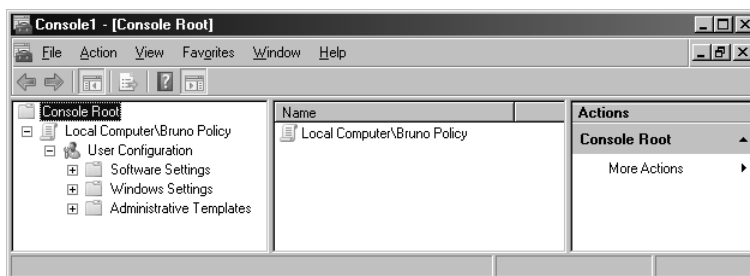


Figure 2-3 The local user-specific GPOs can be edited in the MMC and allow control over User Configuration settings only.

Precedence and Application Now that there are Multiple Local GPOs to configure and choose from, it is important to understand how they are tiered in the hierarchy, in case there

are ever any conflicting settings among them. The hierarchy of local GPOs is predetermined and creates the precedence for conflicting settings in different local GPOs. The most generic GPO has the least precedence, and the most specific GPO has the most precedence. Thus, the local GPO has the least precedence, the user-specific local GPO has the highest precedence, and the Administrators/Non-Administrators local GPOs fall between these two. The order of precedence from lowest to highest is summarized as follows:

- Local GPO
- Administrators/Non-Administrators
- User-specific local GPO

The hierarchy of the local GPOs must also coordinate with the GPOs that administrators link with Active Directory. The same rules apply here as before, where the local GPOs have the weakest precedence when compared to the GPOs from Active Directory.

Network Location Awareness

The Network Location Awareness technology that Windows XP delivered has been a successful solution for many aspects of the operating system and network connectivity. This technology allows the computer to be fully aware of its state and communication capabilities, thus allowing it to make intelligent decisions based on that state.

Group Policy has historically relied on dependable, yet not the most impressive, network identification technology. In the past, Group Policy has used the Internet Control Message Protocol (ICMP) to determine the state of the network, as well as network link speed. ICMP, which encompasses the PING command, is great for getting some network information, but it has not been ideal for helping Group Policy application.

Now that Group Policy relies on Network Location Awareness, the overall picture and state of Group Policy have been enhanced. Group Policy uses network location awareness in two primary fashions: it determines link speed, and it uses network location awareness to determine whether the computer needing to refresh Group Policy is connected to the domain.

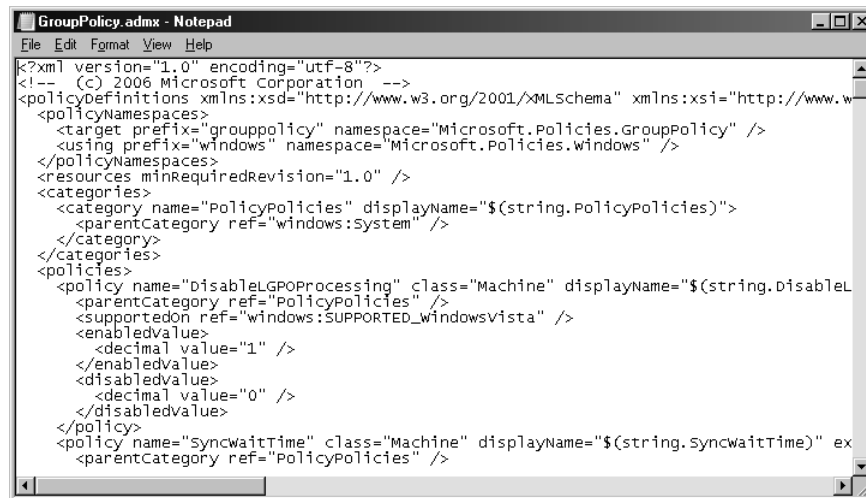
For the first use of Network Location Awareness, Group Policy determines whether the link from the computer receiving GPO settings has a fast or slow connection to the domain and domain controllers. Because some GPO settings can take a long time to apply because of the amount of data being sent, determining link speed can be an indicator as to whether the data should be sent at all. Network Location Awareness provides this assistance by determining the bandwidth of a TCP connection. Group Policy can then use this information to make decisions regarding the settings that it should deliver based solely on the bandwidth available.

Group Policy also uses Network Location Awareness for background refreshes. Network Location Awareness indicates whether the computer has authenticated to a domain controller and whether the domain controller is available to the computer. This feature is important for com-

puters that have failed to refresh Group Policy because the domain controller was not available. In the past, when Group Policy failed to apply, the computer would wait until the next refresh interval—90 to 120 minutes—to attempt to apply Group Policy. The domain controller might have been available only minutes after the failed refresh, but the system would wait the full refresh interval to apply the Group Policy updates. With Network Location Awareness, the Group Policy refresh occurs as soon as it detects the connection to the domain controller.

ADMX Templates

A change that surprised some, but was needed, was a new form of administrative template. The old ADM formatting was limiting in many ways, so a new format was developed. The new format, based on XML, has more flexibility and power than the old format. The new XML-based files have an .admx extension and have changed substantially from their predecessors. A sample of the new XML formatting is shown in Figure 2-4.



```
<?xml version="1.0" encoding="utf-8"?>
<!-- (c) 2006 Microsoft Corporation -->
<policydefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w
  <policyNamespaces>
    <target prefix="grouppolicy" namespace="Microsoft.Policies.GroupPolicy" />
    <using prefix="windows" namespace="Microsoft.Policies.Windows" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <categories>
    <category name="PolicyPolicies" displayName="$(string.PolicyPolicies)">
      <parentCategory ref="windows:system" />
    </category>
  </categories>
  <policies>
    <policy name="DisableLgpoProcessing" class="Machine" displayName="$(string.DisableL
      <parentCategory ref="PolicyPolicies" />
      <supportedOn ref="windows:SUPPORTED_windowsvista" />
      <enabledvalue>
        <decimal value="1" />
      </enabledvalue>
      <disabledvalue>
        <decimal value="0" />
      </disabledvalue>
    </policy>
    <policy name="SyncwaitTime" class="Machine" displayName="$(string.SyncwaitTime)" ex
      <parentCategory ref="PolicyPolicies" />
```

Figure 2-4 The ADMX files are now based on XML for flexibility of language and ease of administration.

The XML formatting was adopted primarily for its language flexibility. ADM formatting did not translate into other languages, forcing other countries and languages to use English, which is not always feasible. During migration to the new format, the structure of the ADM files was radically enhanced also. With the ADM structure, all settings lived in five ADM files. Now there are 132 ADMX files that contain all of the administrative template policy settings. Figure 2-5 shows some of these policy settings.



Note ADMX files, their structure, and additional details are described in Chapter 11, "Customizing ADM Templates and ADMX Files."

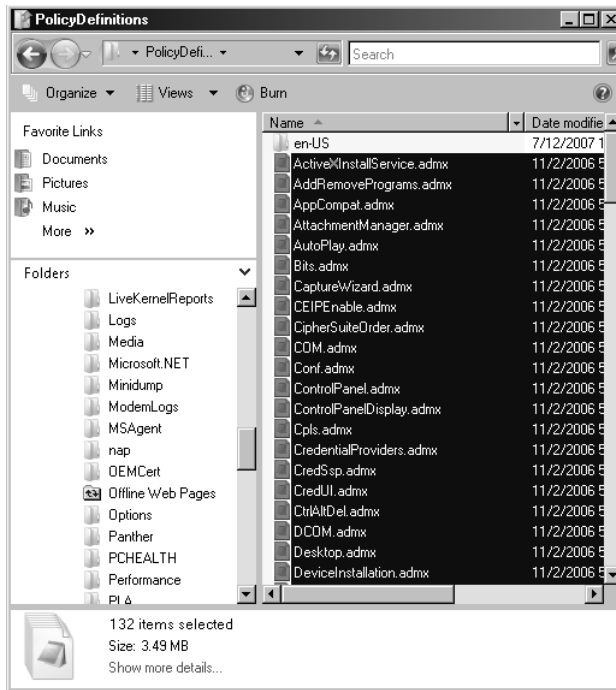


Figure 2-5 Now that the ADMX files are XML-based, 132 individual templates make up the Administrative Templates section of a GPO.

These new ADMX files reside by default on the local system drive of computers running Windows Vista and Windows Server 2008. The path to these ADMX files is %SystemRoot%\PolicyDefinitions, which is usually the default C:\Windows folder that the operating system uses to store the system files.

ADMX Repository

In conjunction with the changes to the administrative template file structure and formatting, GPO administrators create and utilize the central store so that all ADMX files now reside in one location, instead of administrators spreading these files throughout the network on their local computers.

ADM templates were difficult to control and manage, which is one of the major reasons for the change. Another key reason involved how each GPO handled ADM templates. Every GPO that administrators created copied the entire set of default ADM templates into the location where GPO settings were maintained (referred to as the Group Policy template). The Group Policy template is located on domain controllers. Because there can be hundreds or thousands of GPOs, the space required to store these ADM templates was substantial. With each set of default ADM templates (coming in at a massive 4 MB of data) being stored on domain controllers, this could also add to replication traffic between domain controllers.

These negative aspects triggered the development of new technology for handling administrative template files. If an administrator does not create the repository, the local ADMX files will still be used to edit a GPO. This keeps the administration of GPOs consistent, even if the technology is not used. It should be noted, however, that the ADMX files are *not* stored in the Group Policy template. This change helps with storage of files on domain controllers, as well as the replication of those files between domain controllers.



Note ADM template management and the ADMX repository are described in detail in Chapter 10, "ADM Templates, ADMX Files, and the ADMX Central Store."

Improved Logging

It is no secret that managing logging and documentation has been a struggle for Group Policy over the years. Obtaining information from the old Event Log entries was a bit problematic. You needed to be an expert in Group Policy and Microsoft server technologies to get much from the logging that occurred in the Event Viewer. The other logs, such as Userenv.log, were better, but still not ideal.

All of this has changed with the latest installment of GPO logging. The changes are like many of the other changes: stunning and extraordinary. The new logging is built within the updated Event Log service that is available with Windows Vista. It disposes of Userenv.log and instead stores information in a Group Policy Operational log found in Event Viewer. You can find this log in Event Viewer by opening Applications and Services Logs and then browsing to Microsoft\Windows\GroupPolicy\Operational. The resulting log view is shown in Figure 2-6.

These new logs also provide specific new features that help with extraction of information. The logging technology provides for forwarding events to a central location; this is called *subscribing to an event*. Another benefit of the new log structure is the ability to filter views of specific events, making mining information from large log files more efficient.

There is much more to logging, as you will learn in Chapter 15, "Troubleshooting GPOs."

New Group Policy Features in Windows Server 2008

Windows Vista introduced many new features, but Windows Server 2008 offers a few more. These features allow for easier management and configuration of Group Policy settings and will change the way you work with Group Policy in Windows Server 2008.

Filters

If you have ever tried to decrypt the myriad settings in a GPO while trying to troubleshoot a problem, you know that it is a difficult task. There have been very few options for filtering the thousands of potential settings in a GPO, until now. Windows Server 2008 introduces an entire platform for searching and filtering the settings in a GPO. Of course, it includes the obvious search options, such as title text, explanation text, and comments, as shown in Figure 2-7.

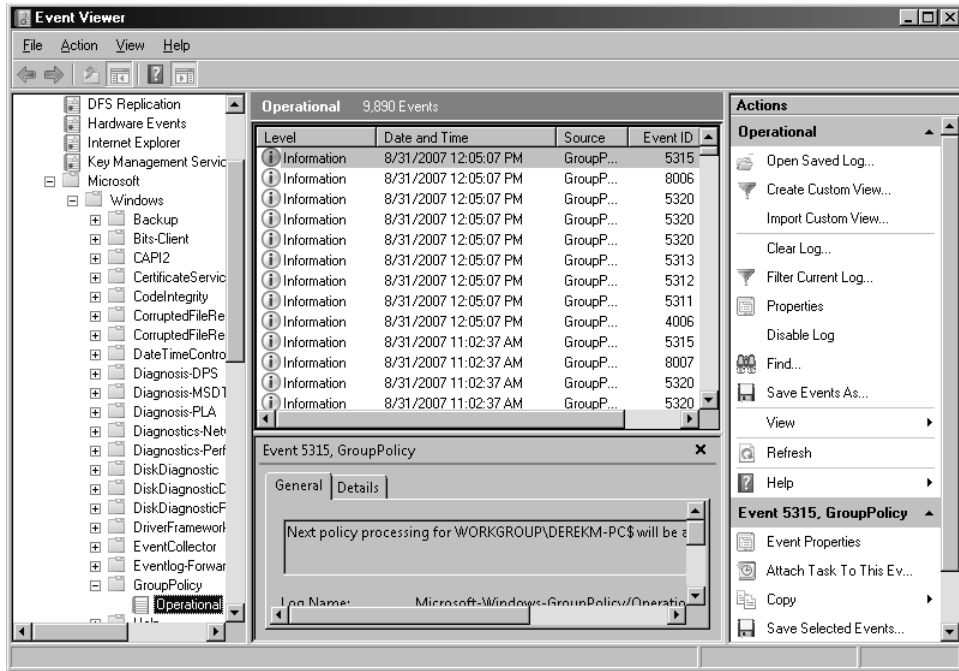


Figure 2-6 With the new logging that is available for Group Policy, new Group Policy events can be seen in the operational logs.

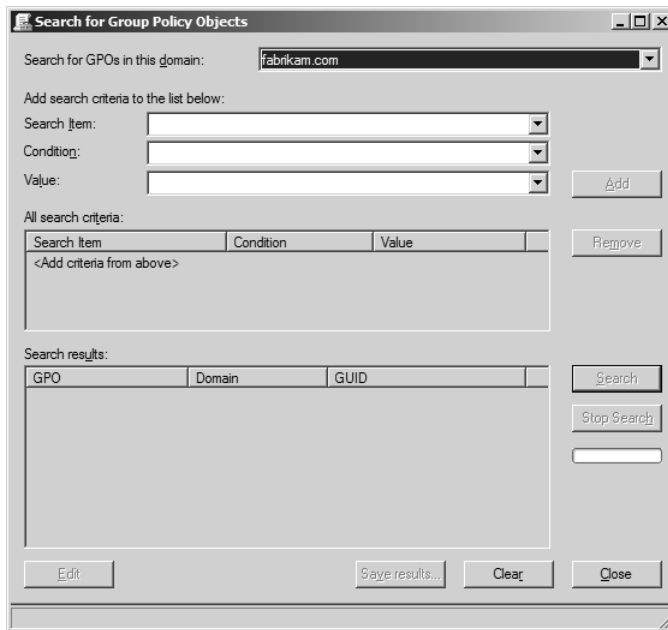


Figure 2-7 The new settings allow for basic searching and filtering of titles, explanation text, and comments within a GPO.

Additional options also allow you to search based on operating system platform support. With so many iterations of Group Policy, as discussed in Chapter 1, “Introduction to Group Policy,” it is important to be able to identify which settings work on which operating system versions.

Another option for searching is based on the application and version supported. With the variety of versions of Microsoft Internet Explorer and Microsoft Office in use, it is important to know which versions the Group Policy settings will affect.

The filtering capability applies only to the Administrative Templates area in a GPO, the area that handles registry modifications. The filter can denote *managed* (policies) settings versus *unmanaged* (preferences) settings. These two types of registry settings make a difference when applied and controlled; it is nice to be able to search for settings by category. For more information about the differences between how registry settings are applied, see Chapter 10, “ADM Templates, ADMX Files, and the ADMX Central Store.” and Chapter 13, “Settings Breakdown for Windows Server 2008 and Vista.”

Finally, you can filter settings based on whether they are disabled or enabled. This is important when working with the new Group Policy Preferences settings. All of these configurations allow for the individual setting to either be enabled or disabled. The filter quickly allows you to see which settings in the GPO administrators have configured, which helps with both troubleshooting and management. Figure 2-8 illustrates how filtering settings based on their enabled or disabled status can make your administrative efforts more efficient.

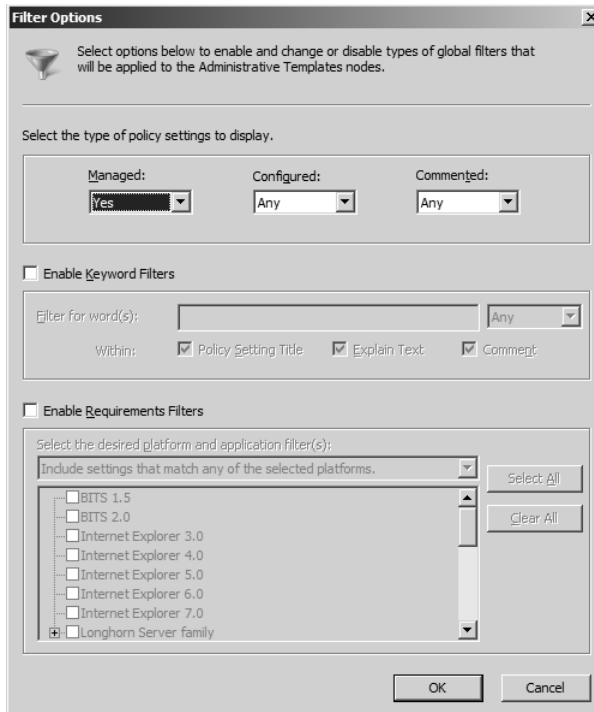


Figure 2-8 The new filtering options include the ability to search on enabled or disabled GPO settings.

Starter GPOs

You now have another tool in your toolkit if you are the lead GPO administrator or responsible for those who create GPOs in your environment. The new Starter GPOs provide an excellent way for you to create a baseline of settings within an off-line “Starter” GPO, which then can be copied to create a new GPO. The new GPO will contain all of the configurations and comments that were created in the Starter GPO.

The one small drawback to the use of Starter GPOs is that they can contain only Administrative Template settings. This is a bit limiting, but the ability to create a baseline of settings that can then be copied to create new GPOs is beneficial nonetheless. A sample Starter GPO is shown in Figure 2-9.

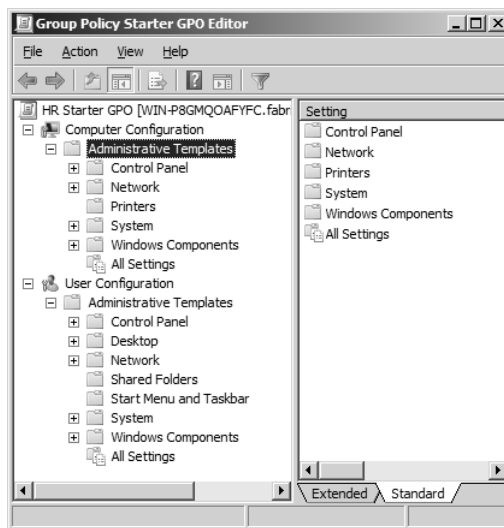


Figure 2-9 Starter GPOs allow you to configure any setting under the Administrative Templates section of a GPO.



Note If you want to create baseline GPOs that contain settings from any portion of a GPO, you can use AGPM. AGPM allows you to create GPO templates, which are in essence Starter GPOs that contain all areas of a GPO.

Another benefit of Starter GPOs is the ability to include them in your RSoP analysis. This gives you an inside look at the settings in the Starter GPO with regard to how they will interact with other GPOs that might have conflicting settings.

For more information on Starter GPOs, refer to Chapter 6, “GPMC Basics.”

Commenting

Changes to Group Policy objects can have a significant impact on the computers in the environment. A single change to a Group Policy setting can affect all computers in your company. With such a powerful tool as Group Policy, some mechanism had to be developed to help maintain a documentation system for changes that occur to GPO settings.

One of those mechanisms is the ability to add comments to every GPO as a whole, as well as every GPO setting individually. This provides a more global and comprehensive way to track changes that occur to GPOs and their settings.

It is common for quick changes to occur to GPOs that are fixes to exploits on a computer that need to be deployed quickly. For example, an exploit might occur that an Internet Explorer setting or a custom registry entry fixes. Changes like these usually occur quickly and without any documented reasoning, and administrators who perform future audits or analysis are left wondering why the change occurred.

With commenting, all changes are tracked immediately when the modification to the GPO occurs. This provides a very detailed trail of the changes that occur to a GPO throughout its life cycle. Figure 2-10 shows some sample comments.

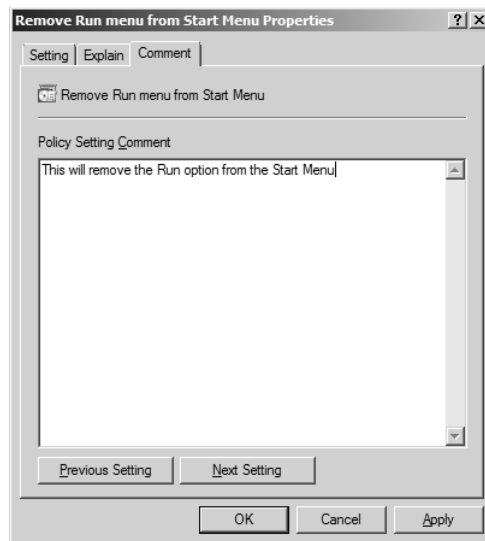


Figure 2-10 A GPO can include comments, allowing for administrators to document the changes that occur each time the GPO is altered.

Not all comments are created equal, though. The comments that are added to a new Starter GPO (at the GPO level) are not saved when a new GPO is created from that Starter GPO. The comments that are associated with the settings within the Starter GPO are copied and carried along to the new GPO.

The commenting mechanism is built this way to help senior administrators document information and details within the GPO for junior administrators who might use the Starter GPO to make a new GPO. Because the new GPO will carry along the settings configured in the Starter GPO, the comments associated with the settings go along with the GPO.

So, What About Those DesktopStandard Products?

In late 2006, Microsoft acquired many of the tools and employees from DesktopStandard. The acquisition was extremely valuable for the entire Group Policy landscape. The tools and products that DesktopStandard had to offer were leaders in the industry. These tools are now available in a variety of offerings by Microsoft.

Group Policy Preferences

Group Policy Preferences is scheduled for delivery to the market in early to mid-2008. This coincides with the release of Windows Server 2008, which Microsoft plans to release in early 2008.

For details about the technology and offerings that Group Policy Preferences will provide, read Chapter 12, “Group Policy Preferences,” which is dedicated to Group Policy Preferences. However, there must be some introduction to Group Policy Preferences here, simply because it is a spectacular product that is coming with Windows Server 2008.

Group Policy Preferences will relate directly to the way in which standard Group Policy is managed and controlled. You will use the Group Policy Management Console, Group Policy Management Editor, and Advanced Group Policy Management, just like you do today. Group Policy Preferences contributes 22 client-side extensions to a GPO. These extensions include settings related to files, folders, user accounts, local groups, drive mappings, printer mappings, and much more.

Group Policy Preferences provide control over areas of a desktop and server that past Group Policy settings did not. The technology has been on the market for many years, and customers have loved what it can do for them. If Group Policy Preferences is something that could benefit you, Chapter 12 is where you should be looking now.

Advanced Group Policy Management (GPOVault)

The other product line that Microsoft acquired from DesktopStandard is Advanced Group Policy Management (AGPM). DesktopStandard called it GPOVault when they owned it.

Unlike the other Group Policy products and technologies, AGPM is offered through the Microsoft Desktop Optimization Pack (MDOP). MDOP is available only to those companies that have bought software assurance for desktops running Windows Vista. Software assurance provides 24-hour phone support, partner services, training, and IT tools for the life of the license. MDOP is an enormous package that offers a great value.



Note For more information on MDOP, refer to <http://www.microsoft.com/windows/products/windowsvista/enterprise/mdopoverview.aspx>.

AGPM itself brings tremendous value to the Group Policy management arena. Although Chapter 14, “Advanced GPO Management with AGPM,” goes into the AGPM features and settings in full detail, the following is a list of benefits that AGPM can provide to your GPO management environment:

- Role-based delegation
- Roll back and roll forward to any GPO in the archive
- Off-line editing of GPOs
- Settings difference reports between two GPOs
- Workflow for GPO management tasks
- GPO templates for baseline configurations
- Built on GPMC
- Integrated change control for your Group Policy management environment

You can complete some of these tasks by using the GPMC and scripting, but AGPM performs these tasks seamlessly and automatically. AGPM is also a very lightweight installation, relying on a simple flat file structure and metadata to keep track of all of the changes within each GPO.

Summary

With every new operating system come new changes in every technology area. Group Policy is no different. Some exciting and amazing new technologies come with Windows Vista and Windows Server 2008. Windows Vista introduced some of these technologies, including local GPOs, Network Location Awareness, logging improvements, ADMX file format, and ADMX repository. New for Windows Server 2008 are many updates to GPMC, including searching, commenting, and filtering, as well as Group Policy Preferences technology. Last but not least is the new AGPM functionality, which makes management of Group Policy easier and more efficient.

Additional Resources

- The Microsoft Group Policy Web site, at <http://www.microsoft.com/grouppolicy>, includes more information on the new features and settings that are available in Windows Server 2008 and Windows Vista.

- The Microsoft TechNet article titled “Step-by-Step Guide to Managing Multiple Local Group Policy Objects,” at <http://go.microsoft.com/fwlink/?LinkId=73759>, includes more information on multiple local Group Policy objects in Windows Vista.
- Chapter 14, “Advanced Group Policy Management with AGPM,” includes information about installing AGPM, how to use AGPM, how to obtain AGPM, and the benefits of AGPM.
- Chapter 13, “Settings Breakdown for Windows Server 2008 and Windows Vista,” includes information about specific settings within a GPO.
- Appendix A, “Third-Party Group Policy Tools,” includes information about other companies that have extended Group Policy.

Chapter 4

Architecture of Group Policy

In this chapter:

Group Policy Dependencies	68
New Group Policy Service	72
Domain Controller Selection During GPO Management	73
Architectural Parts of a GPO	76
GPO Replication	84
Client-Side Extensions	88
Summary	91
Additional Resources	91

Like most technology, Group Policy is very logical and predictable. The structure of Group Policy has not changed much over the years, although some of the internal mechanisms have. Because Group Policy is such a stable and reliable technology, there has been no need for major changes.

With that said, there have been some radical changes to the underlying implementation of Group Policy with Windows Vista and Windows Server 2008. Although the core dependencies have not changed, the core engine of Group Policy has changed for the better. There is now a dedicated service for Group Policy, which gives Group Policy even more stability and efficiency.

Administration of your domain-based GPOs has not changed, either. The Group Policy Object Editor is now called the Group Policy Management Editor (GPME), but its functions and those of the Group Policy Management Console (GPMC) remain the same. The core architecture for updating domain-based GPOs is important to understand and manage, as it has always been.

Understanding the storage of Group Policy in terms of the Group Policy template (GPT) and the Group Policy container (GPC) is critical to efficient management of the GPOs, ADM files, replication, and troubleshooting. Of course, the biggest change that Windows Vista and Windows Server 2008 offer with regard to architecture is the addition of ADMX templates and the central repository.

An architecture overview cannot be complete without a rigorous discussion on replication. Replication for Group Policy is not simple, but a good summary of the subject will help you tackle most problems that arise. Replication and Group Policy are important concepts to understand when you need to troubleshoot an issue.

Finally, this chapter will review the architecture of client-side extensions (CSEs). CSEs are the soul of Group Policy settings. You will get an inside glimpse into the different CSEs, what they do, and how they function with the information provided by the GPT and the GPC.

Group Policy Dependencies

Although Group Policy is a large and complicated service and technology, it also relies heavily on other complicated services and technologies. You must understand these other services and technologies to fully understand Group Policy, especially when you encounter trouble. Understanding Group Policy's dependencies will help you pinpoint the source of the problem, whether it be Group Policy or one of these services.

The services and technologies that Group Policy has direct dependencies on include the following:

- Active Directory
- Domain Name System (DNS)
- Active Directory replication
- Distributed File System Replication (DFSR)—formerly File Replication Service (FRS)
- DFS publishing
- Network Location Awareness (NLA)

As you can see from the preceding list, the services and technologies that Group Policy depends on are extremely important, not only to Group Policy, but to your network as a whole. Without these services and technologies, you would not have a fully functional enterprise.

Each of these services and technologies is responsible for a specific aspect of Group Policy. Understanding how each component fits into the bigger picture will help you with design, implementation, management, and troubleshooting of Group Policy.

Active Directory and Group Policy

Active Directory has the biggest role as a dependent technology with Group Policy. Most certainly, without Active Directory you would not have much of a Group Policy infrastructure to work with. Active Directory provides the foundation upon which Group Policy is embedded.

First, consider that Active Directory houses all of the user and computer objects for the domain or domains. It is these user and computer objects that Group Policy controls. Next, Active Directory creates the structure that the objects are placed within. The structure is made up of organizational units. The design of the organizational units is essential in the deployment of Group Policy—the user and computer objects located within the organizational unit

where the GPO is linked, as well as those in child organizational units, are affected by the settings in the linked GPO by default.



Important A poorly designed Active Directory structure can make it very difficult to deploy Group Policy. It is always best to design Group Policy deployment into the initial Active Directory design. If the Active Directory design is too chaotic or disorganized, it might need to be completely redesigned before Group Policy can be correctly deployed.

A well designed Active Directory structure considers the user and computer object location within the organizational units. Because GPOs are linked primarily to organizational units, ensuring that the links are easy and efficient will help with the overall success and good design of Active Directory.



Note Active Directory should be designed to incorporate two important components: Group Policy and delegation of administration should be the two driving factors for your Active Directory design. As a best practice, delegation of administration should have the highest priority, because Group Policy can be filtered to apply to only certain objects in an organization unit.

GPOs can be linked to three Active Directory components. These include the domain, organization units, and sites. If Active Directory did not contain these components, GPOs would not be able to link to them.

As a side benefit, Active Directory allows for single sign-on for user accounts, which Group Policy can leverage because each user is unique within the Active Directory domain. Because each user is unique, administrators can mold and deploy the precise security settings, desktop settings, registry values, and profile environment for each user.



Note Local Group Policy objects can still be used without Active Directory, in a small business or home office environment, for example. In such cases, the Local Group Policy objects must be administered on each computer separately.

Domain Name System

You probably already know what the Domain Name System (DNS) is, but as a reminder, DNS is a distributed database that resolves DNS host names to Internet Protocol (IP) addresses. In Active Directory, DNS is the locator service that enables computers to find other computers, as well as important networking services.

For Active Directory networks, DNS has entries called Service Resource Records (SRVs) that are associated with different networking services. These include entries for Lightweight Directory Access Protocol (LDAP), Transmission Control Protocol (TCP), and Kerberos. These SRVs help computers in the Active Directory domain find the servers that are functioning as

domain controllers. At a domain controller, they might get a listing of Group Policy Objects, update their Kerberos ticket, find a resource, and so on. When DNS is not working properly or is misconfigured, computers will not be able to use DNS to find this information. At this point, Group Policy will fail to work properly; all updates and refreshes will cease until DNS is functioning properly again.

DNS is also used for Distributed File System (DFS). DFS can be used within Group Policy to share applications or other resources. When a GPO is configured to direct a desktop or user to a DFS distribution point for accessing software, the computer must use DNS to find these installation points. If DNS is not configured properly, the computer will never find the DFS distribution point and the software will not be installed or updated.

Finally, DNS is important for managing Group Policy. As you will see later in this chapter, domain controllers are the computers that store GPOs. Therefore, when you are managing a GPO, a domain controller must be contacted. If DNS is not functioning properly, a domain controller cannot be found and an error will occur when trying to update or view a GPO.

From the Source: Group Policy Dependency on DNS

Here's the simplest explanation I found for why Group Policy depends on DNS. As stated earlier, Group Policy queries Active Directory for information about GPOs, user and computer locations, security groups, and other information needed for processing Group Policy. A TechNet article on DNS integration (<http://technet2.microsoft.com/WindowsServer/en/library/2c6fde55-8d99-4c2d-9f38-95d6446ebdb51033.mspx>) states, "Active Directory provides an information repository and services to make information available to users and applications. Active Directory clients send queries to domain controllers using the Lightweight Directory Access Protocol (LDAP). In order to locate a domain controller, an Active Directory client queries DNS. Active Directory requires DNS to function." There are instances in which Group Policy uses a fully qualified domain name (FQDN) for its naming, but when you are attempting to bind to a domain, the domain controller must be located, which requires a functioning DNS.

Judith Herman, Programming Writer

Microsoft

Replication

One of the more significant tasks of Group Policy is to ensure that each GPO is synchronized with each domain controller. Domain controllers are the command center of GPO distribution. As you will see a little later in this chapter, a GPO is not just a single entity. It is really made up of two separate parts: the Group Policy template (GPT), which is stored in the SYSVOL of each domain controller, and the Group Policy container (GPC), which is stored in Active Directory, again on each domain controller.

Both portions of the GPO must be replicated to every domain controller within the domain. If the GPOs do not synchronize to all domain controllers after a change is made, strange behavior will occur. This behavior might include differing settings on two desktops that should have the same settings, errant settings on a server caused by a missing GPO setting, failure to apply policy altogether, or a desktop that is not secure because of a failure of the GPO to replicate.

As you can see, replication is a significant factor for Group Policy. There is a small concern with Group Policy replication, however. The GPO is made up of two different parts, but the SYSVOL replication and the Active Directory replication are not driven or supported by the same replication technology.

SYSVOL replication is controlled by either the Distributed File System Replication (DFSR) or the File Replication Service (FRS), depending on the domain functional level. Domain controllers running Windows 2000 or Microsoft Windows Server 2003 cannot take advantage of DFSR for replication of the SYSVOL, so they must still use FRS. Windows Server 2008 does support DFSR for SYSVOL replication, but all domain controllers must be running Windows Server 2008 to take advantage of this new technology. If any domain controllers in the domain are running Windows 2000 or Windows Server 2003, the Windows Server 2008 domain controllers must also use FRS to support the limitations of the older operating systems.

Active Directory replication is not controlled by DFSR or FRS. Instead, Active Directory replication is controlled by its own replication service. Active Directory replication is responsible for replicating the entire Active Directory database, not just the GPC. Because changes occur with the other objects in the database more than the GPC, the technology and details of replication were designed for those other objects more so than for Group Policy. With this said, the replication of Active Directory is quite complex, with many moving parts and considerations. Later in this chapter, an in-depth overview of Active Directory replication will explain how it affects and controls the GPC.

DFS

Another service that Group Policy depends on is DFS. You might miss this service unless you consider how DFS assists Group Policy in many different areas. If you think that DFS publishing can assist Group Policy when software is delivered through a GPO, you are correct. However, Group Policy does not *depend* on this service in this regard—DFS is simply an enabling service in this scenario.

So, how exactly does DFS function with Group Policy as a dependant service? DFS is the service that makes the SYSVOL on the domain controllers available. Every domain controller has the SYSVOL shared. There are two folders named SYSVOL, and only one of them is shared. The path to the shared SYSVOL is C:\Windows\SYSVOL\Sysvol.

This share is not a routine share. Rather, it is a domain-based DFS share. This type of share is very useful in situations in which all computers in the domain need to access the same resource. If you are not familiar with domain-based DFS, it has some significant advantages.

With domain-based DFS shares, all computers access the share by using the domain name, instead of the domain controller's NetBIOS computer name or DNS fully qualified domain name (FQDN). Therefore, all computers that communicate with SYSVOL on the domain controllers (every computer in the domain) do so by using `\\domainname\sysvol`.

Although this might seem simplistic and limited in rewards, the power is in the technology behind the scenes. With this form of communication to the domain controller and SYSVOL, the names of the domain controllers are irrelevant. Domain controllers can be added, removed, changed, taken offline, brought back online, and so on without the existing connections and mapped drives. As long as there is at least one domain controller online for the computers to access, the computers on the network will be able to communicate with the domain-based DFS share.

This is possible because domain-based DFS shares are accessed through DNS. SRV records that help the computer find the nearest domain controller are automatically registered in DNS. The nearest domain controller is relative, because DNS uses Active Directory sites, which represent physical networks. When a computer receives a list of domain controllers from DNS, the domain controllers in the computers' sites are listed first, followed by the other domain controllers.

This process and technology allows computers to receive the GPT information for the GPOs from the domain controllers. The process is very efficient for both keeping track of the domain controllers and allowing the computers on the network to find the closest domain controller to retrieve the Group Policy information from SYSVOL.

New Group Policy Service

One of the major changes that came with Windows Vista and is now being leveraged in Windows Server 2008 is a new Group Policy service. Earlier operating systems used the WinLogon service to run Group Policy. There were no inherent problems with using WinLogon, but there are significant benefits to using a separate service to control Group Policy. Considering the emphasis that Microsoft is putting into Group Policy, with advanced technologies being included in Group Policy and new management tools, the move to a separate service was not surprising.

The new Group Policy service improves the overall stability of the Group Policy infrastructure and computer by completely isolating it from WinLogon. The Group Policy service uses a completely new architecture for performing notifications and processing Group Policy. Not only does the Group Policy service change the architecture, it also adds these benefits:

- New Group Policy–related files can be delivered to computers administrating GPOs and computers consuming GPO settings without requiring a restart of the operating system.
- Group Policy application is more efficient because fewer resources are required for background processing.
- Less memory is used for Group Policy on computers consuming GPO settings, increasing performance and eliminating the need to load Group Policy in multiple services.
- The Group Policy service is started automatically and cannot be disabled, which creates a more stable environment.

To find the service in running services, look for gpsvc, as shown in Figure 4-1.



```
Administrator: Command Prompt
C:\Users\Administrator>sc query gpsvc
SERVICE_NAME: gpsvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4   RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT           : 0x0

C:\Users\Administrator>
```

Figure 4-1 The new Group Policy service runs as gpsvc and can be seen in a list of running services on a computer running Windows Vista or Windows Server 2008.

Domain Controller Selection During GPO Management

Consider a typical Active Directory environment that has multiple domain controllers. As you have seen, all domain controllers house a copy of each GPO. The replication of the GPOs is handled by the two replication technologies: DFSR and Active Directory replication. But which domain controller makes the initial changes to the GPOs?

The answer is quite simple. The domain controller that has the PDC emulator role is relied upon to make the changes to a GPO. Then this domain controller replicates the changes to the other domain controllers.



Note As a reminder, the first domain controller in each domain controls all three of the domain operation masters: PDC emulator, RID master, and infrastructure master.

In some instances, you either cannot or do not want to use the domain controller that has the PDC emulator role to make the initial changes, and you may want to use another domain controller to update the GPOs. For these reasons, there is a built-in ability to alter the default behavior.

Using the PDC Emulator

Every time a GPO is viewed or changed, the GPMC and the GPME locate the domain controller that is responsible for the PDC emulator role. It is the GPO from this domain controller that is viewed and updated. There is no inherent reason for choosing this domain controller by default; one domain controller must be selected, because changes must occur on one domain controller and then replicate to all domain controllers. Because the PDC emulator is already responsible for many other critical domain tasks, it makes sense to use this domain controller for GPO updates as well.

There are times when the domain controller running the PDC emulator role is not available or is not the ideal candidate for updating the GPOs. If the PDC emulator is not available when a change must be made to a GPO, the system displays an error message, as shown in Figure 4-2.



Figure 4-2 When the domain controller running the PDC emulator role is not available for editing the GPO, an error message appears.

Note that not only does the system display a dialog box indicating that the domain controller is not available, it also gives you the option to choose a different domain controller. In most cases, selection of the domain controller for updating a GPO has no effect on the result of updating a GPO. Sometimes, however, selecting a different domain controller will result in faster or slower GPO deployment situations. This is because of the way in which a computer receives information regarding domain controllers during initial bootup. Computers receive a list of domain controllers from DNS that prioritizes them based on network location. The domain controllers in the computer's own site are first; then the other domain controllers follow. If you make a change to a GPO that is initially updated on a domain controller that is not in the target computer's site, it can take a while to replicate to the domain controller in the computer's site. This could cause a delay in the processing of the GPO until all replication converges.

Selecting the Domain Controller for GPO Editing

To eliminate the processing delay described in the previous section, you can select a domain controller that is in the computer's site. Of course, you must know which site the target computers are in, as well as which domain controllers correspond to that site.

You can also control which domain controller is used when you edit a GPO within the GPMC. Again, this is beneficial when you want to update a specific domain controller to ensure the fastest and most reliable application of the policy settings. To change the domain controller used for editing GPOs from within the GPMC, follow these steps:

1. Right-click the domain name in the GPMC window.
2. Click Change Domain Controller.
3. Make your selection from the list of possible domain controller options, as shown in Figure 4-3.

The next time you edit a GPO from within the GPMC, you will be using the domain controller that you selected. Do not forget that you changed the domain controller in the interface.

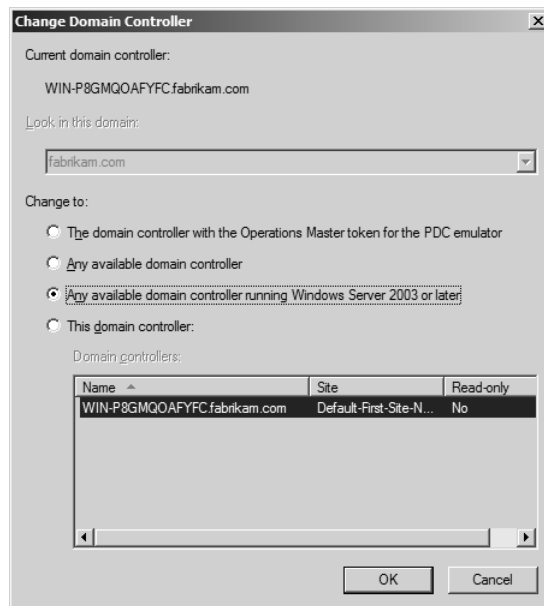


Figure 4-3 The domain controller used to edit GPOs can be selected from within the GPMC to optimize the application of the settings configured in the GPO.



Note One Group Policy setting allows you to configure the domain controller that will be used when editing GPOs. The setting, “Group Policy domain controller selection,” is under User Configuration\Administrative Templates\System\Group Policy, as shown in Figure 4-4. This policy setting is a bit out of date; it does not offer the same options as the GPMC, and it includes an option for using the domain controller that is being used by the snap-in, which refers to Active Directory Users and Computers.

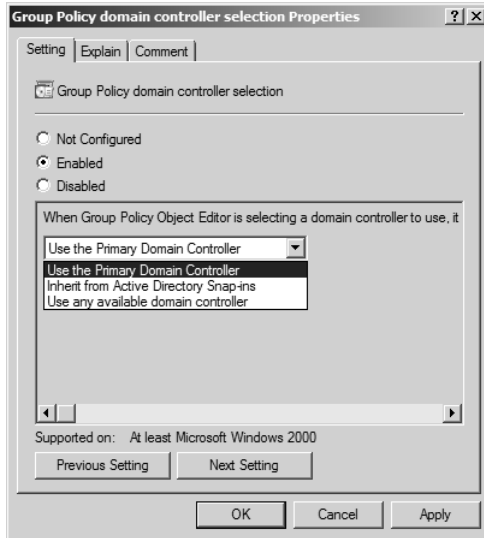


Figure 4-4 The domain controller that is used for editing GPOs can be configured in a GPO, located under User Configuration\Administrative Templates\System\Group Policy.

Architectural Parts of a GPO

A GPO is not as straightforward as you might think. The GPO is made up of two independent parts. These parts are not stored in the same location, they do not have the same structure, and they do not store the same information. If you were to look at the two parts separately, it would be hard to tell that they are related through Group Policy. However, they both perform very important duties for Group Policy and the storage of policy settings.

The first component is the GPT, which is responsible for storing the settings that are made in the GPO. The structure of the GPT can be very complex, because it is a dynamic set of folders and files. The information stored in the files is delivered to the target computers during Group Policy processing.

The second component is the Group Policy container (GPC). The GPC is the “glue” that ensures that all references, paths, network locations, Active Directory objects and paths, and so on are accounted for and correct. The contents of the GPC are usually limited or blank. The details for the GPC are in the Active Directory properties that are associated with each GPC.

Group Policy Template

The Group Policy template (GPT) is the portion of the GPO that is stored in the SYSVOL folder on the domain controllers. The GPT is not a single file or folder, but rather a suite of folders and files that are used to store and maintain the settings that are established in a GPO. The GPT is very dynamic, yet very simple.

Each GPO has a unique GPT where the files are stored. The GPT is kept unique between GPOs by its GUID (globally unique identifier). When a GPO is initially created, a new folder is created under the %windir%\SYSVOL\sysvol*<domainname>*\Policies folder. This new folder is named the same as the GPO's GUID, as you can see in Figure 4-5.

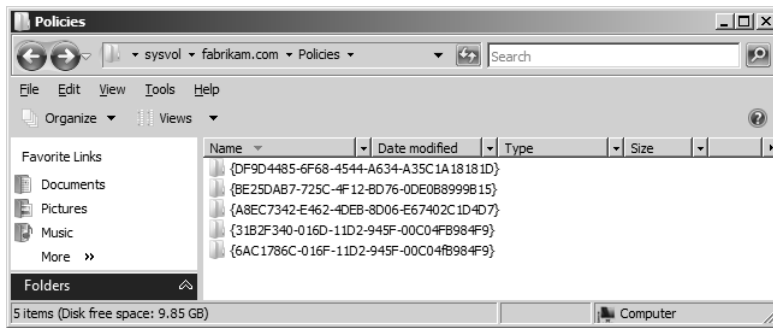


Figure 4-5 All Group Policy templates are stored in a unique folder named after the GPO's GUID; they are all stored in the SYSVOL\Policies folder on each domain controller.

During the creation of the GPT main folder, additional folders and files are created under this root folder. These folders and files include:

- **Group Policy folder** Holds the GPE.ini file. The GPE.ini file tracks the GUIDs for the CSEs that are referenced in the GPO. As settings within the GPO are added or removed, the associated GUID for the CSE controlling the setting is added or removed from this file.
- **Machine folder** Stores all GPO settings that are configured under the Computer Configuration node in the GPO.
- **User folder** Stores all GPO settings that are configured under the User Configuration node in the GPO.
- **Gpt.ini file** Tracks the GPO version number. The version number changes each time the GPO is modified.

Figure 4-6 illustrates the default folders and files that exist in the GPT.

As settings are created in the GPO, additional folders and files are created in the appropriate folder, depending on whether a Computer Configuration setting or a User Configuration setting is made.

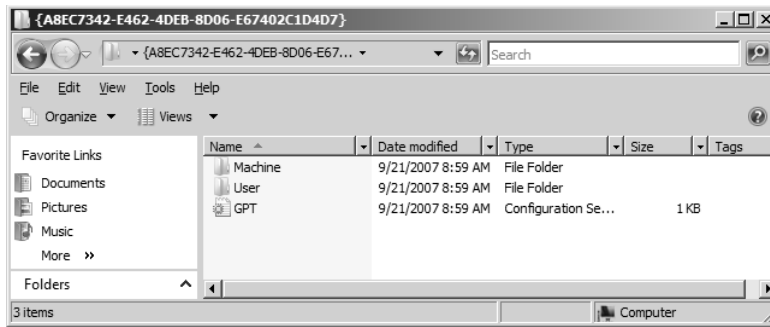


Figure 4-6 Newly created GPOs have only two default folders and one default file that make up the GPT in SYSVOL.

Not all settings create the same type of files. The different portions of the GPO make up the different client-side extensions supported in the GPO. When a setting is made for each client-side extension, the file in which it is stored within the GPT is also different. Table 4-1 shows the client-side extension in addition to the files used within the GPT for that extension. For more information about client-side extensions, refer to the section later in this chapter on the topic.

Table 4-1 Group Policy Template Files

Client-Side Extension	Folder Structure in GPT	File Name and Extension in GPT
Software Installation	Machine\Applications User\Applications	<GUID>.aas
Scripts	Machine\Scripts\Startup Machine\Scripts\Shutdown User\Scripts\Logon User\Scripts\Logoff	Varies (typically with .vbs, .bat, .cmd, .exe extension)
Security	Machine\Microsoft\Windows NT \SecEdit	GptTmpl.inf
Windows Firewall and Advanced Security	Machine	Registry.pol
Public Key Policies	Machine User	Registry.pol
Software Restriction Policy	Machine User	Registry.pol
Network Access Protection	Machine	Registry.pol
Policy Based QoS	Machine User	Registry.pol
Registry	Machine	Registry.pol
Remote Installation Services	Microsoft\RemoteInstall	Oscfilter.ini

Table 4-1 Group Policy Template Files

Client-Side Extension	Folder Structure in GPT	File Name and Extension in GPT
Folder Redirection	User\Documents & Settings	Fdeploy1.ini
Internet Explorer Maintenance	User\Microsoft\IEAK	Various folders and files
Group Policy Environment	Machine\Preferences \EnvironmentVariables User\Preferences\EnvironmentVariables	EnvironmentVariables.xml
Group Policy Data Sources	Machine\Preferences\DataSources User\Preferences\DataSources	DataSources.xml
Group Policy Devices	Machine\Preferences\Devices User\Preferences\Devices	Devices.xml
Group Policy Files	Machine\Preferences\Files User\Preferences\Files	Files.xml
Group Policy Folder Options	Machine\Preferences\Options User\Preferences\Options	Options.xml
Group Policy Folders	Machine\Preferences\Folders User\Preferences\Folders	Folders.xml
Group Policy Local Users and Groups	Machine\Preferences\Groups User\Preferences\Groups	Groups.xml
Group Policy Ini Files	Machine\Preferences\IniFiles User\Preferences\IniFiles	IniFiles.xml
Group Policy Network Options	Machine\Preferences\NetworkOptions User\Preferences\NetworkOptions	NetworkOptions.xml
Group Policy Network Shares	Machine\Preferences\NetworkShares User\Preferences\NetworkShares	NetworkShares.xml
Group Policy Power Options	Machine\Preferences\PowerOptions User\Preferences\PowerOptions	PowerOptions.xml
Group Policy Printers	Machine\Preferences\Printers User\Preferences\Printers	Printers.xml
Group Policy Registry	Machine\Preferences\Registry User\Preferences\Registry	Registry.xml
Group Policy Scheduled Tasks	Machine\Preferences\ScheduledTasks User\Preferences\ScheduledTasks	ScheduledTasks.xml
Group Policy Services	Machine\Preferences\Services User\Preferences\Services	Services.xml
Group Policy Shortcuts	Machine\Preferences\Shortcuts User\Preferences\Shortcuts	Shortcuts.xml

Table 4-1 Group Policy Template Files

Client-Side Extension	Folder Structure in GPT	File Name and Extension in GPT
Group Policy Applications	User\ Preferences\Applications	Applications.xml
Group Policy Drive Maps	User\ Preferences\Drives	Drives.xml
Group Policy Internet Settings	User\ Preferences\InternetSettings	InternetSettings.xml
Group Policy Regional Options	User\ Preferences\RegionalOptions	RegionalOptions.xml
Group Policy Start Menu	User\ Preferences\StartMenuTaskbar	StartMenuTaskbar.xml

Figure 4-7 illustrates what a complex set of GPO settings might look like through the files and folders that are created in the GPT.

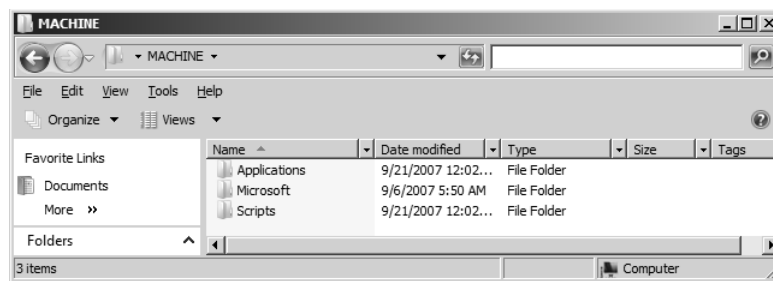


Figure 4-7 When a GPO has many settings configured in different areas of the GPO, folders and files may be created in the GPT.

As you can see, the GPT is responsible for housing all of the raw settings that are made in a GPO. Each setting is stored in a unique file structure, which correlates with the client-side extension under which it is categorized. The files that are stored in the GPT are delivered to the target computer during Group Policy processing.

Group Policy Container

The Group Policy container (GPC) is the portion of the GPO that is stored in Active Directory. The subfolder format of the GPC is similar to that of the GPT, but the GPC is radically different in content and overall use. The GPC has a suite of Active Directory properties associated with it, giving it the same feel as a typical Active Directory object, such as a user or computer object.

The GPC is also similar to the GPT, in the way in which it is tracked in the system; the GPC is also named after the GPO's GUID. You can find the GPC by using one of many tools that display the Active Directory objects. By using Active Directory Users and Computers, you can access the full list of GPCs by following these steps:

1. In Active Directory Users and Computers, expand the domain node.
2. Expand the System node.

- Expand the Policies node to expose the list of GUIDs that represent the GPCs, as shown in Figure 4-8.

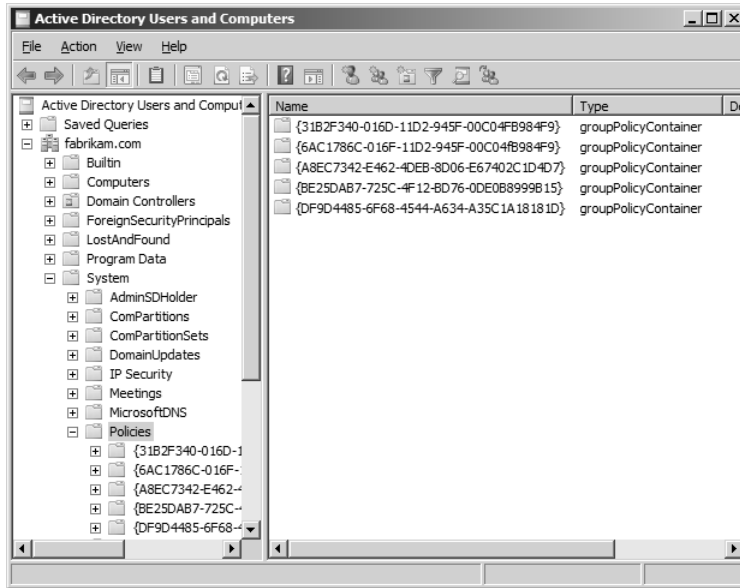


Figure 4-8 All GPCs are stored in Active Directory under the GPO's GUID, allowing the system to keep each GPO unique and distinguishable.



Note To see the System folder in Active Directory Users and Computers, you must first enable the Advanced Features option. To enable this option, click the domain node in Active Directory Users and Computers. Then click the Tools menu and select the Advanced Features menu option.

During the creation of the GPC, two main folders are created: Machine and User. These folders are empty by default; you can see nothing from the Active Directory Users and Computers interface with regard to the GPC. However, if you create some policy settings, you can see some folders and content within the Active Directory Users and Computers. Table 4-2 lists the folders and files associated with the policies that update the GPC.

Table 4-2 GPC Files

Client-Side Extension	Folder Structure in GPC	File Name and Extension in GPC
Software Installation	Machine\Class Store\Packages User\Class Store\Packages	<GUID>, which is a packageRegistration object
IP Security	Machine\Microsoft\Windows	IPSEC, which is an ipsecPolicy object
Wireless Network (IEEE 802.3) Policies	Machine\Microsoft\Windows \IEEE8023	<policyname>, which is a ms-net-ieee-8023-GroupPolicy object
Wireless Network (IEEE 802.11) Policies	Machine\Microsoft\Windows \Wireless	<policyname>, which is a msieee80211-Policy object

If you want to see details of the GPC, you can use Active Directory Users and Computers or an LDAP tool, such as ADSIEdit, which allows you to see the properties associated with the GPC. These properties help Active Directory and Group Policy apply the appropriate settings and point to the correct GPT and any other network location that might be configured within the GPO. Table 4-3 shows the default properties associated with the GPC.

Table 4-3 GPC Active Directory Properties

Property	Default Value
adminDescription	<not set>
adminDisplayName	<not set>
cn	(GUID of GPO)
defaultClassStore	<not set>
description	<not set>
displayName	(Name of GPO)
displayNamePrintable	<not set>
distinguishedName	CN={GUID of GPO}
dSASignature	<not set>
dSCorePropagationData	0x0 = ()
extensionName	<not set>
flags	0
fSMORoleOwner	<not set>
gPCFileSysPath	\\<domainname>\SysVol\<domainname>\Policies
gPCFunctionalityVersion	2
gPCMachineExtensionNames	<not set>
gPCUserExtensionNames	<not set>
gPCWQLFilter	<not set>
instanceType	0x4 = (WRITE)
isCriticalSystemObject	<not set>
isDeleted	<not set>
lastKnownParent	<not set>
mS-DS-ConsistencyChildCount	<not set>
mS-DS-ConsistencyGuid	<not set>
msDS-NcType	<not set>
msDS-ObjectReference	<not set>
Name	(GUID of GPO)
objectCategory	CN=Group-Policy-Container,CN=Schema, CN=Configuration, DC=<domainname>, DC=<domain name extention>

Table 4-3 GPC Active Directory Properties

Property	Default Value
objectClass	Top;container;groupPolicyContainer
objectGUID	GUID of GPO
objectVersion	<not set>
otherWellKnownObjects	<not set>
partialAttributeDeletionList	<not set>
partialAttributeSet	<not set>
proxiedObjectName	<not set>
proxyAddresses	<not set>
replPropertyMetaData	<Octet string table>
replUpToDateVector	<not set>
repsFrom	<not set>
repsTo	<not set>
revision	<not set>
schemaVersion	<not set>
showinAdvancedViewOnly	TRUE
subRefs	<not set>
systemFlags	<not set>
url	<not set>
uSNChanged	Dynamic numeric variable
uSNCreated	Dynamic numeric variable
uSNSDALastObjRemoved	<not set>
USNIntersite	<not set>
uSNLastObjRem	<not set>
uSNSSource	<not set>
versionNumber	0
wbemPath	<not set>
wellKnownObjects	<not set>
whenChanged	Date of change
whenCreated	Date of creation
wWWHomePage	<not set>

Figure 4-9 shows what the GPC looks like when viewed with ADSIEdit.

The GPC is not responsible for storing the settings that are in the GPO—that is the job of the GPT. The GPC ensures that all network links, resources, and paths are correct and tracked. When Group Policy processing occurs, the GPC properties are used to find all of the pertinent information for the GPT, software installation nodes, and so on.

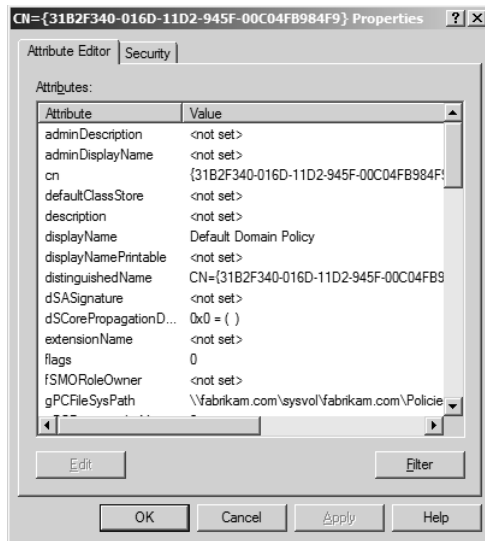


Figure 4-9 Each GPO is represented with a GPC, which in turn has a suite of Active Directory object properties that store information about the GPO resources.

GPO Replication

You just saw that a single GPO is not a single entity. A GPO has two major parts: the GPT and the GPC. Earlier in this chapter, we briefly discussed how Group Policy relied on replication services to move GPO settings from one domain controller to another. These replication services are essential for the success and efficiency of Group Policy application. Because Group Policy models the concept of a multi-master environment, changes to a GPO are made on only one domain controller. The replication services are responsible for making sure that the changes to the GPO get to all domain controllers.

The two parts of the GPO could not be more different, nor could the replication services that synchronize the parts on domain controllers. Understanding how the replication services are dissimilar can make you a troubleshooting expert. In many cases, failed Group Policy processing is the result of failed or errant replication of either the GPC or the GPT.

Group Policy Template and SYSVOL Replication

SYSVOL replication in Windows 2000 and Windows Server 2003 was driven by the File Replication Service (FRS). FRS was a stable and reliable service, but it had some issues for large organizations. FRS was difficult to troubleshoot, and when broken, it was hard to get running again.

With Windows Server 2008, a new replication service ensures that SYSVOL is synchronized among all domain controllers. The new service is the Distributed File System Replication (DFSR). DFSR was introduced with Windows Server 2003 R2, but this version did not support

replication of SYSVOL. The current version of DFSR in Windows Server 2008 supports replication of SYSVOL for Windows Server 2008 domain controllers, but it does not support Windows Server 2003 and earlier. The only way to use DFSR to replicate the SYSVOL is to raise your Windows Server 2008 domain to the Windows Server 2008 domain functional level. The service is installed and started by default, but the upgrade to the domain functional level will trigger it to control replication.

How It Works: Enabling DFSR for Your Active Directory Domain

Enabling DFSR will benefit your entire Active Directory infrastructure because it is much more efficient than the old FRS replication. The first step is to ensure that all of your domain controllers are running Windows Server 2008. This is a requirement for replicating the SYSVOL using DFSR, because only domain controllers running Windows Server 2008 support this form of replication of the SYSVOL. The second step is to raise the domain level to Windows Server 2008 functional level. The process is very similar to the process for raising the level of the domain in Windows 2000 and Windows Server 2003. Open the Active Directory User and Computers interface and do the following:

1. In the console tree pane, locate the domain name.
2. Right-click the domain name, and then click Raise Domain Functional Level, as shown in Figure 4-10.

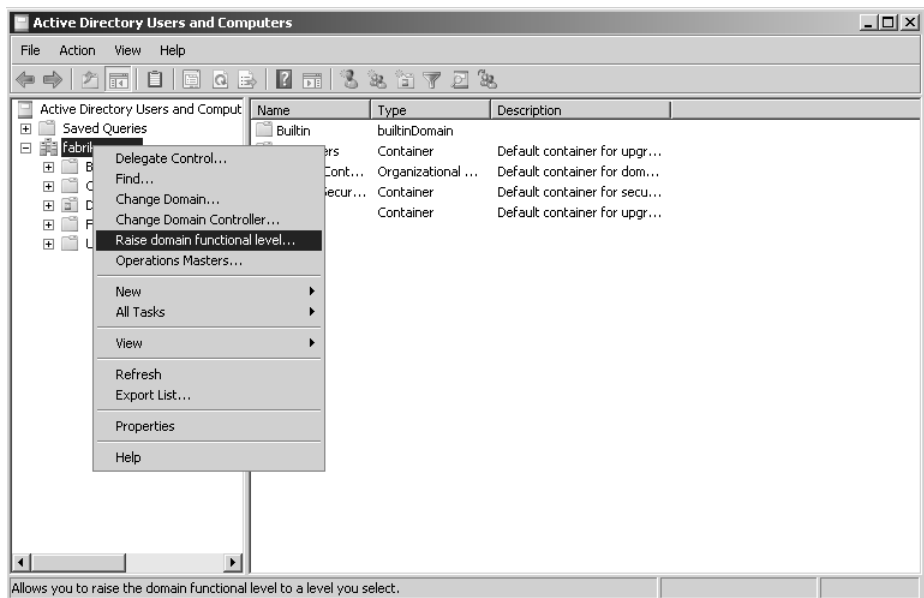


Figure 4-10 The Active Directory Users and Computers interface allows you to configure the domain functional level, including Windows Server 2008.

3. In the Domain Functional Level dialog box, select Windows Server 2008.
4. To Convert your SYSVOL from FRS to DFSR, you must run the `dfsrmig` command on all domain controllers to properly convert the SYSVOL to DFSR. After you do this, you will not have the option to convert back to FRS.



Warning After you upgrade to a new functional level, you cannot revert back to the original level. For more information about functional levels in Windows Server 2008 Active Directory, refer to the article titled "Appendix of Functional Level Features" at <http://technet2.microsoft.com/windowsserver2008/en/library/34678199-98f1-465f-9156-c600f723b31f1033.msp?mfr=true>.

DFSR provides additional benefits over its predecessor, FRS, such as the following:

- Bandwidth throttling and replication scheduling
- Support for replication groups
- Replication of GPO differences only
- File and subfolder filtering

Note that DFSR and FRS follow state-based replication schedules. This means that as soon as a change occurs in the SYSVOL, SYSVOL will replicate the changes to the replication partners. This state-based replication does not adhere to any Active Directory site topology, so the convergence of the changes is rather fast compared to schedule-based replication technologies.



Note DFSR does provide for scheduling and manipulating of the service, but it is a best practice to leave the replication of SYSVOL at the default values.

Active Directory Replication

Active Directory replication is controlled by...Active Directory replication. The underlying services that control Active Directory replication include the Knowledge Consistency Checker (KCC) and the Inter-Site Topology Generator (ISTG) services. The KCC is in charge of all Active Directory replication, whereas the ISTG is responsible only for replication of Active Directory between domain controllers in different sites.

Because the GPC is stored in Active Directory, it is important to understand how this replication differs from DFSR replication. First, Active Directory replication is not state based. There is a schedule associated with the replication of Active Directory, which is set in the Active Directory Sites and Services tool, as shown in Figure 4-11.

Note that the replication value available for configuration shown in Figure 4-11 is only for replication between sites. The replication of Active Directory between domain controllers in

the same site is not available for configuration. This replication, intra-site replication, is set to 15 seconds by default. The maximum time that a change to Active Directory should take to converge to all domain controllers in the same site is 45 seconds, which is a three-hop maximum between replication partners.

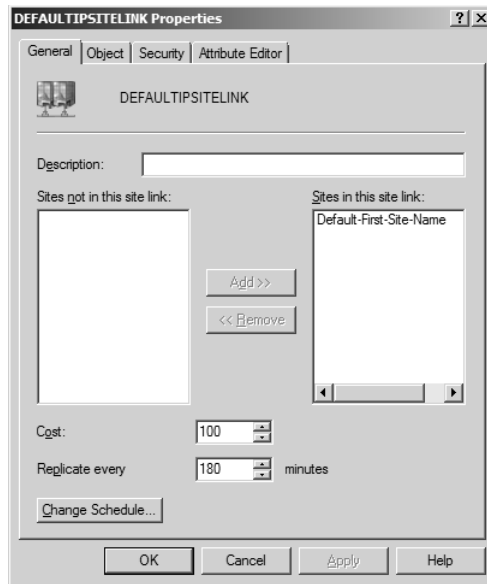


Figure 4-11 Site links have a schedule for Active Directory replication between sites, which is configured in Active Directory Sites and Services.

In Figure 4-11, you can see that a much longer convergence time could occur with domain controllers between sites. The default value is 180 minutes, with simple conversion to three hours. This is only the replication of the domain controllers chosen to replicated between sites (*bridgehead servers*), not the replication within the site between domain controllers. If multiple site hops must be completed, the convergence time could be substantially higher.



Note It has become a best practice for most companies to set the intra-site replication schedule to 15 minutes. This is because most site links are a high-bandwidth scenario. If your bandwidth is significantly less than 10 Mbps, you should consider keeping the replication schedule interval between 60 and 180 minutes.

As you can clearly see, Active Directory replication can lag behind DFSR replication substantially. This has caused dramatic effects in the past, but since the release of Windows XP, this lag in convergence of the two replication technologies has been almost eliminated because Group Policy processing now checks for version numbers in a different way. For more information about Group Policy processing with regard to the version numbers of the GPT and GPC, refer to Chapter 5, “Group Policy Processing.” For more information on troubleshooting replication issues with Group Policy, refer to Chapter 15, “Troubleshooting GPOs.”

Client-Side Extensions

Client-side extensions (CSEs) provide much of the intelligence behind Group Policy. CSEs are files that must reside on the computer that is consuming Group Policy settings. The CSEs are divided into logical categories that match the nodes within the GPO, which can be seen in the structure of the GPO in the GPME. For example, the Security Settings node and all of the settings under it are controlled by the security CSE. The Drive Maps policy under the Preferences nodes is controlled by its own CSE, the Group Policy Drive Maps CSE.

The CSEs are .dll files that contain code that applies the settings to the target computer. The settings are delivered from the domain controllers to the computer receiving the policy settings during Group Policy processing. The data delivered to the target computer is the information stored in the files that makes up the GPT of the GPO. When these raw settings are delivered to the target computer, the appropriate CSEs perform the correct action on the target computer. Each CSE is tracked and managed by a GUID. The GUID ensures that the CSE is unique—we saw earlier that the GPC tracks the correct CSE in the *gPCMachineExtensionNames* and *gPCUserExtentionNames* attributes.

Table 4-4 provides information about all of the CSEs that are supported in Windows Server 2008 and Windows Vista. The CSEs are referenced in the registry, where this information is kept and tracked. You can see the full list of CSEs in the registry at `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions`.

Table 4-4 Group Policy Client-Side Extensions

Client-Side Extension	CSE DLL	GUID
Wireless Group Policy	Wlgpclnt.dll	{0ACDD40C-75AC-47ab-BAA0-BF6DE7E7FE63}
Group Policy Environment	Gpprefcl.dll	{0E28E245-9368-4853-AD84-6DA3BA35BB75}
Group Policy Local Users and Groups	Gpprefcl.dll	{17D89FEC-5C44-4972-B12D-241CAEF74509}
Group Policy Device Settings	Gpprefcl.dll	{1A6364EB-776B-4120-ADE1-B63A406A76B5}
Folder Restriction	Fdeploy.dll	{25537BA6-77A8-11D2-9B6C-0000F8080861}
Microsoft Disk Quota	Diskquota.dll	{3610eda5-77ef-11d2-8dc5-00c04fa31a66}
Group Policy Network Options	Gpprefcl.dll	{3A0DBA37-F8B2-4356-83DE-3E90BD5C261F}
QoS Packet Scheduler	Gptext.dll	{426031c0-0b47-4852-b0ca-ac3d37bfc39}
Scripts	Gpscript.dll	{42B5FAAE-6536-11d2-AE5A-0000F87571E3}
Internet Explorer Zonemapping	ledkcs32.dll	{4CFB60C1-FAA6-47f1-89AA-0B18730C9FD3}
Group Policy Drive Maps	Gpprefcl.dll	{5794DAFD-BE60-433f-88A2-1A31939AC01F}
Group Policy Folders	Gpprefcl.dll	{6232C319-91AC-4931-9385-E70C2B099F0E}
Group Policy Network Shares	Gpprefcl.dll	{6A4C88C6-C502-4f74-8F60-2CB23EDC24E2}
Group Policy Files	Gpprefcl.dll	{7150F9BF-48AD-4da4-A49C-29EF4A8369BA}
Group Policy Data Sources	Gpprefcl.dll	{728EE579-943C-4519-9EF7-AB56765798ED}

Table 4-4 Group Policy Client-Side Extensions

Client-Side Extension	CSE DLL	GUID
Group Policy Ini Files	Gpprefcl.dll	{74EE6C03-5363-4554-B161-627540339CAB}
Windows Search Group Policy Extension	Srchadmin.dll	{7933F41E-56F8-41d6-A31C-4148A711EE93}
Security	Scecli.dll	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
Deployed Printer Connections	Gpprnext.dll	{8A28E2C5-8D06-49A4-A08C-632DAA493E17}
Group Policy Services	Gpprefcl.dll	{91FBB303-0CD5-4055-BF42-E512A681B325}
Internet Explorer Branding	ledkcs32.dll	{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}
Group Policy Folder Options	Gpprefcl.dll	{A3F3E39B-5D83-4940-B954-28315B82F0A8}
Group Policy Scheduled Tasks	Gpprefcl.dll	{AADCED64-746C-4633-A97C-D61349046527}
Group Policy Registry	Gpprefcl.dll	{B087BE9D-ED37-454f-AF9C-04291E351182}
EFS Recovery	Scecli.dll	{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
802.3 Group Policy	Dot3gpclnt.dll	{B587E2B1-4D59-4e7e-AED9-22B9DF11D053}
Group Policy Printers	Gpprefcl.dll	{BC75B1ED-5833-4858-9BB8-CBF0B166DF9D}
Group Policy Shortcuts	Gpprefcl.dll	{C418DD9D-0D14-4efb-8FBF-CFE535C8FAC7}
Microsoft Offline Files	Cscobj.dll	{C631DF4C-088F-4156-B058-4375F0853CD8}
Software Installation	Appmgmts.dll	{c6dc5466-785a-11d2-84d0-00c04fb169f7}
IP Security	Polstore.dll	{e437bc1c-aa7d-11d2-a382-00c04f991e27}
Group Policy Internet Settings	Gpprefcl.dll	{E47248BA-94CC-49c4-BBB5-9EB7F05183D0}
Group Policy Start Menu Settings	Gpprefcl.dll	{E4F48E54-F38D-4884-BFB9-D4D2E5729C18}
Group Policy Regional Options	Gpprefcl.dll	{E5094040-C46C-4115-B030-04FB2E545B00}
Group Policy Power Options	Gpprefcl.dll	{E62688F0-25FD-4c90-BFF5-F508B9D2E31F}
Group Policy Applications	Gpprefcl.dll	{F9C77450-3A41-477E-9310-9ACD617BD9E3}
Enterprise QoS	Gptext.dll	{FB2CA36D-0B40-4307-821B-A13B252DE56C}

You can see from Table 4-4 that some CSEs use the same file to store the code needed to apply settings delivered from the domain controller.



Note If a target computer is missing a CSE during Group Policy processing, the settings that are delivered from the domain controller will not apply to the computer.



Important The CSEs for the Group Policy Preferences must be installed on all computers running Windows XP SP2, Windows Server 2003 SP1, and Windows Vista that will consume these settings. You can download the CSEs from here: <http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>. The CSEs are all contained in one .dll file. The file is best distributed using Group Policy, because it is wrapped up in an .msi file. The .dll CSE files are stored in the C:\Windows\System32 folder. For more information about Group Policy Preferences, refer to Chapter 12, “Group Policy Preferences,” which provides details on these settings.

Each CSE is defined and tracked in the registry and includes a set of registry values that define and control its behavior. Clicking a CSE GUID in the registry will expose the registry settings that are configured by default and can be modified, as shown in Figure 4-12. The full list of possible registry value settings is shown in Table 4-5.

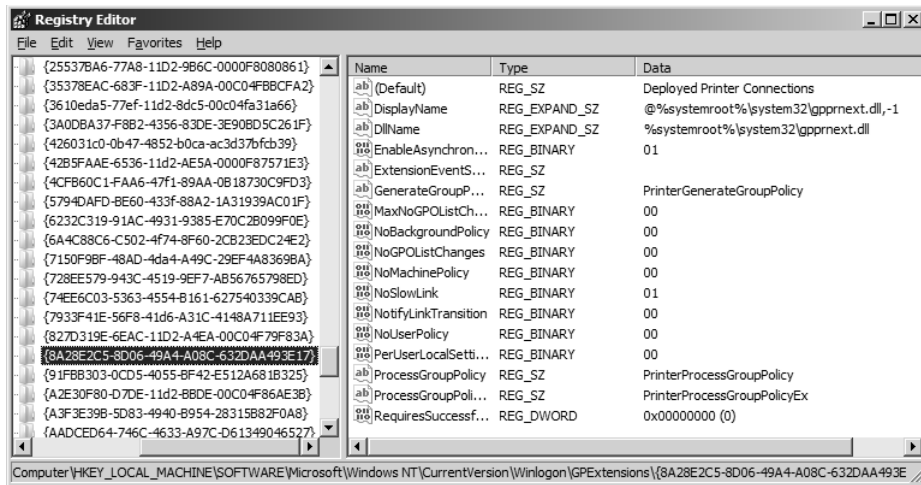


Figure 4-12 Each CSE in the registry has a set of values that control the behavior of the CSE.



Warning Modifying a registry value for a CSE could cause instability or operating system failure. Be sure to test all changes to any setting in the registry before deploying to any production computer. For more information about the registry values for the CSEs, refer to Table 4-4 and the TechNet article “NoSlowLink Entry,” at <http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>, which covers all registry entries and supported values for each.

Table 4-5 Table 4-5 Possible Group Policy Extension Registry Values

Registry Value	Value Type	Possible Values
(Default)	REG_SZ	<Name of Group Policy>
DisplayName	REG_EXPAND_SZ	@<CSE DLL>, -1 to -????
DLLName	REG_EXPAND_SZ	Name or path to DLL
EnableSynchronousProcessing	REG_DWORD	<0 or 1>
EnableAsynchronousProcessing	REG_BINARY or REG_DWORD	<0 or 01>
ExtensionDebugLevel	REG_DWORD	<0 or 1>
ExtensionEventSource	REG_SZ	Varies
ExtensionRsopPlanningDebugLevel	REG_DWORD	<0 or 1>
EventSources	REG_MULTI_SZ	Varies
GenerateGroupPolicy	REG_SZ	Varies
MaxNGPLstChangesInterval	REG_DWORD	<0 or 1>

Table 4-5 Table 4-5 Possible Group Policy Extension Registry Values

Registry Value	Value Type	Possible Values
NoBackgroundPol i cy	REG_DWORD	<0 or 1>
NoGPOLi stChanges	REG_DWORD	<0 or 1>
NoMachi nePol i cy	REG_DWORD	<0 or 1>
NoSI owLi nk	REG_DWORD	<0 or 1>
Noti fyLi nkTransi ti on	REG_DWORD	<0 or 1>
NoUserPol i cy	REG_DWORD	<0 or 1>
PerUserLocal Set ti ngs	REG_DWORD	<0 or 1>
ProcessGroupPol i cy	REG_SZ	Vari es
ProcessGroupPol i cyEx	REG_SZ	Vari es
Requi reSuccessful Regi stry	REG_DWORD	<0 or 1>

Summary

Group Policy can stand alone as a technology, but it also has many dependencies on other services and technologies; its close relationship with Active Directory explains these dependencies. Group Policy also runs under a new service, which provides a more reliable, flexible, and feature-rich environment.

Administration of Group Policy is mandatory, and understanding how GPOs are updated is essential. Understanding that the PDC emulator role domain controller is used for editing GPOs is important, as is the fact that you may choose a different domain controller. Selecting the domain controller in the correct site, as a best practice, will make Group Policy application more efficient.

Each GPO consists of two parts: the GPC and the GPT. Both parts are stored on a domain controller, but they have completely different structures and content, as well as different replication services, making the architecture of a GPO somewhat complex. Knowing that the DFSR service and the Active Directory replication have different schedules and mechanisms for replicating content can help with troubleshooting issues.

Client-side extensions are the working mechanism for configuring GPO settings on the target computer. The CSE DLL takes the information from the GPO and makes the setting on the computer. Windows Server 2008 provides over XZY CSEs, which is a large increase from the 13 that were available in Windows Server 2003.

Additional Resources

- The Microsoft TechNet article titled “How the Active Directory Replication Model Works,” at <http://technet2.microsoft.com/WindowsServer/en/Library/1465d773-b763-45ec-b971-c23cdc27400e1033.msp?mfr=true>, includes information about Active Directory replication.

- The Microsoft TechNet article titled “Appendix of Functional Level Features,” at <http://technet2.microsoft.com/windowsserver2008/en/library/34678199-98f1-465f-9156-c600f723b31f1033.msp?mfr=true>, includes information about Windows Server 2008 functional levels for Active Directory.
- Chapter 3, “Group Policy Basics,” includes information about configuring local Group Policy Objects.
- Chapter 5, “Group Policy Processing,” includes information about how Group Policy processes settings.
- Chapter 12, “Group Policy Preferences,” includes information about the Preferences settings in a GPO.
- Chapter 15 “Troubleshooting Group Policy,” includes information about how DNS can affect Group Policy application and how to troubleshoot Group Policy replication issues.

Index

Symbols and Numbers

#if version, 261–62, 280
%AppDataDir%, 345
%BinaryComputerSID%, 345
%BinaryUserSid%, 345
%CommonAppdataDir%, 345
%CommonDesktopDir%, 345
%CommonFavoritesDir%, 345
%CommonProgramsDir%, 345
%CommonStartMenuDir%, 345
%CommonStartUpDir%, 345
%ComputerName%, 345
%CurrentProcessID%, 345
%CurrentThreadId%, 345
%DateTime%, 345
%DateTimeEx%, 345
%DesktopDir%, 345
%DomainName%, 345
%FavoritesDir%, 345
%LastError%, 345
%LastErrorText%, 345
%LdapComputerSid%, 345
%LdapUserSid%, 345
%LocalTime%, 345
%LocalTimeEx%, 345
%LogonDomain%, 345
%LogonServer%, 345
%LogonUser%, 345
%LogonUserSid%, 345
%MacAddress%, 345
%NetPlacesDir%, 345
%OsVersion%, 345
%ProgramDir%, 345
%ProgramFilesDir%, 345
%RecentDocumentDir%, 346
%ResultCode%, 346
%ResultText%, 346
%ReversedComputerSid%, 346
%ReversedUserSid%, 346
%SendToDir%, 346
%StartMenuDir%, 346
%StartupDir%, 346
%SystemDir%, 346
%SystemDrive%, 346
%TempDir%, 346
%TimeStamp%, 346
%TraceFile%, 346
%windir%\Inf\folder,
235, 237–39
%windir%\Policy
Definitions, 243
%WindowsDir%, 346

(Default), 90
.adm. *See* Administrative Templates
(.adm)
.bat, 78
.cmd, 78
.exe, 78
.migtable, 168
.msi files, 42, 44, 351
.msp, 352
.vbs, 78
.zap files, 42, 44
/Boot, 106
/C.namespace, 251
/D:description, 251
/Force, 106
/L, 250
/Logoff, 106
/N:name, 251
/P:prefix, 251
/R:revision, 251
/S.namespace, 251
/Synch, 106
/Target, 106
/U:prefix, 251
/Wait, 106
/X, 250
<domainname> node, 142
<GUID>, 81
<GUID>.aas, 78
<policyname>, 81
<Strings>, 246

A

Aaxa.adm, 236
access control lists (ACLs), 13
migrating GPOs, 164
policies/preferences, 242
Access11.adm, 235
Access-based Enumeration, 313
Account Lockout Policy,
54, 56, 354
account passwords, 301
control of, 55–57
editing settings, 54
Local Users and Groups, 318
Password Policy, 56–57, 354
Security Settings, 353–54
user account, 43
Account Policies, 43
Default Domain Policy
settings, 57
password control, 55–57
Security Settings, 353
accounts, 41–42. *See also* user
accounts
administration of, 69, 205–7
AGPM administrator, 206–7
Local Users and Groups, 318
System, 324
ACLs. *See* access control lists (ACLs)
Action Modes, 323
ACTIONLIST, 277
ACTIONLISTOFF, 248
ACTIONLISTON, 248
Active Desk, 236
Active Directory, 6, 40, 52–54,
68–69
containers, 211
creating GPOs, 62–64, 124–26
default GPOs, 54
delegations, default, 204
Group Policy Container
(GPC), 80–82
linking GPOs, 126–28, 130,
211–13
management tools, 122
modeling GPOs,
154–59, 217
precedence, 51, 97–100
reliability, 16–17
replication, 71, 85–87
RSOP, delegation, 218
Security Settings, 353, 357
software distribution, 8
Active Directory schema,
320, 460–62
Active Directory Users and
Computers, 81, 211–13
ActivityID, 435, 438–39
Add/Remove Programs, 351
Additional Rules, 364
ADDITIVE, 275–76
additive attribute, 291
ADM Template Editor, 484
AdmFileLanguageVersion, 246
adminDescription, 82
adminDisplayName, 82
administration, 13.
See also
delegation;
permissions;
scope of management (SOM);
security

- Advanced Group Policy Management (AGPM), 218–24
 - AGPM Client, 406–7
 - best practices, 224–28
 - change management, 408–10
 - creating GPOs, 208–10
 - default security, 203–7
 - delegation, 203
 - domain controllers, 123–24
 - editing GPOs, 215–16
 - file ownership, 61
 - GPO backups, 130–32
 - Group Policy Management Console (GMPC), 204
 - linking GPOs, 210–13
 - managing GPOs, 213–15
 - modeling GPOs, 216–17
 - object ownership, 61
 - privileges, 62, 376
 - RSoP of GPOs, 218
 - Administrative Templates (.adm), 4, 9, 29–31, 43–46, 233–34
 - #if version, 261–62
 - adding, 237–39
 - additional statements, 278–80
 - best practices, 281–82
 - Comments, 159, 161–62
 - customizing, 257–59
 - default files, 234–36
 - filtering, 33, 146–48, 258
 - Help desk, 281
 - importing, 237
 - managing, 239–42
 - migrating to ADMX files, 245–51
 - policies/preferences, 242–43
 - removing, 238–39
 - starter GPOs, 34
 - string and tab limits, 280
 - structure of, 259
 - used with ADMX files, 244–45
 - Windows Settings
 - Control Panel, 368
 - Desktop, 368
 - Network, 368–69
 - Printers, 369–70
 - Shared Folders, 369–70
 - Start Menu, 369–70
 - Taskbar, 369–70
 - Windows Components, 370–72
 - Administrators Local GPOs, 26–27, 47–51
 - Administrators Local Group policy, 25
 - ADML (.adml) files, 281, 283–86, 289–96
 - ADMX central store, 233
 - creating, 245, 251–52
 - moving files to, 253–54
 - ADMX Editor, 249–50
 - ADMX files (.admx), 24, 29–30, 67, 243
 - .adm file migration, 245–51
 - .adm templates, use with, 244–45
 - ADML files, tying to, 289–90
 - CLASS options, 284
 - core concepts, 286–89
 - creating custom files, 283
 - default, 243
 - file element syntax, 291–96
 - file structure, 284
 - registry-based policy settings, 296
 - usage of, 254
 - ADMX Migrator, 249–51
 - ADMX Repository, 30–31, 67
 - ADMX schema, 283, 295
 - ADSIEdit, 82
 - Advanced Group Policy Management (AGPM), 13, 34, 36–37, 399–400
 - administrator, 206–7
 - architecture, 400
 - change management, 408–10
 - Client installation, 406–7
 - creating GPOs, 413–15
 - delegation, 203, 218–24
 - deploying GPOs, 415–17
 - difference reports, 419–21
 - editing GPOs, offline, 407
 - e-mail configurations, 411–12
 - GMPC, Change Control, 401
 - operating system support, 400–1
 - Pending tab, 412–13
 - Recycle Bin, 422–23
 - reporting, 418–21
 - restoring GPOs and links, 423–24
 - rolling back/rolling forward, 417–18
 - security, default, 204–7
 - server installation, 401–6
 - templates, using, 421–22
 - workflow, 410–11
 - Aer.1033.adm, 235
 - AGPM. *See* Advanced Group Policy Management (AGPM)
 - AGPM Client, 406–7
 - AGPM Server, 401–6
 - AGPMServer.msi, 402
 - appmservice, 206
 - Annotation, 246
 - annotation element, 291
 - anonymous connections, 6–8
 - Application Log, 357
 - Applications, preferences, 310
 - Applications.xml, 80
 - Appmgmts.dll, 89
 - approved registry keys, 242
 - Approver permission, 221
 - architecture, 67–68
 - Advanced Group Policy Management (AGPM), 400
 - client-side extensions (CSEs), 88–91
 - dependencies, 68–72
 - domain controller selection, 73–76
 - GPO replication, 84–87
 - Group Policy Container (GPC), 80–83
 - Group Policy Service, 72–73
 - Group Policy Template (GPT), 76–80
 - archives, 134
 - AGPM Server installation, 401–6
 - deploying GPOs, 416–17
 - settings reports, 419
 - tracking changes, 408–10
 - troubleshooting tools, 458–59
 - ASCII, EDITTEXT syntax, 274–75
 - asynchronous processing, 103–4, 429
 - Audit Policy, 354
 - auditing, 43, 59–60, 358
- B**
- background refresh, 11, 14, 28–29
 - editing GPOs, 216
 - policy processing, 100, 436
 - reliability, 17
 - Backup, migrating GPOs, 164, 166–67
 - BackupAllGPOs.wsf, 175
 - BackupGPO.wsf, 174
 - backups
 - Advanced Group Policy Management (AGPM), 417–18
 - Default Domain Controllers Policy, 60
 - Group Policy Objects (GPOs), 130–32, 134, 417–18
 - scripts for, 174–77
 - Starter GPOs, 136–37

- BaseTypes.xsd, 283
- batch jobs, 60
- Battery Present, 328
- best practices
 - Administrative Templates (.adm), 281–82
 - delegation, 224–28
- BeyondTrust Corporation, 469
- binary registry values, 281
- BITS, 147
- Block Inheritance, 109–12
- boolean element, 291
- BrainCore.Net, 494
- Browser User Interface, 367

- C**
- cabinet (CAB) files, 137–38
- categories elements, 284, 291
- CATEGORY, 247, 260, 266–68
- category elements, 287–88, 291, 295
- CATEGORYEXPLAIN, 248
- certificate authorities, 363–64
- certificate requests, 363–64
- certificate rules, 43
- certificate trust lists, 363–64
- Change Guardian (CG), 475
- change management, 408–10
- CharToOem<JavaScript
 - hhobj_1.Click(>, 274–75
- Chat.adm, 236
- checkBox, 290–91
- CHECKBOX, 247, 270–71
- class, 291
- CLASS, 246, 262–63, 284
- CLASS MACHINE, 259–60
- CLASS USER, 259
- Client policy, 366
- CLIENTEXT, 248, 270–71
- clientExtension, 248, 291
- client-side extensions (CSEs), 17
 - Administrative Templates (.adm), 234
 - ADMX files, 291
 - architecture, 88–91
 - CLIENTEXT, 271
 - Event IDs, 452, 458
 - Group Policy Preferences, 301, 308–9
 - PART syntax, 270
 - processing parameters, 104–5
 - Resultant Set of Policy Provider (RSSP), 158–59
 - security, 107
 - troubleshooting, 430, 445
- cn, 82
- comboBox, 291
- COMBOBOX, 248, 270–73
- command-line tools, 320–21
- comments, 35–36
 - Administrative Templates (.adm), 161, 278
 - filtering, 32, 147–48
 - types of, 159–62
- comments(;), 246
- Common tab, 324–25
- Common.adm, 234
- Component Status, 152
- computer access, Default Domain
 - Controllers Policy, 59
- Computer Configuration, 41–43.
 - See also* Policies node
 - Administrative Templates (.adm), 236
 - ADMX files, 243
 - CLASS options, 284
 - GPO reports, 150
 - GPO searching, 145
 - GPT Machine folder, 77
 - Group Policy Preferences, 303, 309, 325
 - hardware component settings, 385–86
 - network security settings, 390–91
 - Preferences settings, 372–73
 - searching GPOs, 143
 - server settings, 382
 - settings, viewing, 151
 - Terminal Services, 373
 - User Account Control, 376
- Computer Name, 328
- computer performance, 343
- computer roles, 442
- Computer, GPO migration
 - source, 169
- Conf.adm, 234, 236
- Configured policy setting, 147
- Connection policy, 367–68
- Connection Security Rule, 362
- connections, anonymous, 6–8
- connectivity, network, 28–29
- consistency, 18–19
- containers, 211. *See also* Group Policy Container (GPC)
- Control Panel, 43
 - Administrative Templates settings, 368
 - Data Sources, 315
 - Devices, 315
 - Folder Options, 316
 - Internet Settings, 317
 - Local Users and Groups, 318
 - Network Options, 318
 - Power Options, 318
 - Printers, 320
 - Regional Options, 320
 - Scheduled Tasks, 320
 - Services, 322
 - Start Menu, 322
- Copy, migrating GPOs, 164–65
- CopyGPO.wsf, 178
- corporate environment, 25
- CPU Speed, 328, 343
- CreateEnvironmentFromXML.wsf, 181
- CreateGPO.wsf, 179–80
- CreateMigrationTable.wsf, 182–83
- CreateXMLFromEnvironment, 180
- Cscobj.dll, 89
- CSEs. *See* client-side extensions (CSEs)
- currency settings, 320

- D**
- Data Sources preference, 315
- DataSources.xml, 79
- date format, 320
- Date Match, 329
- Dcgpfix.exe, 460–62
- DCName, 436
- debug programs, 60
- decimal, 247
- decimal elements, 292–95
- decimalTextBox, 247, 292
- default, 292
- DEFAULT, 274, 276
- Default Domain Controllers Policy, 58–59
 - audit procedures, 59
 - default configurations and values, 59–61
 - Security Settings, 353
 - troubleshooting, 460–62
- Default Domain Policy, 54–58
 - configurations and values, 58
 - default Account Policy settings, 57
 - Security Settings, 353–54
 - troubleshooting, 460–62
- default security environment, 203–4
 - Advanced Group Policy Management (AGPM), 204–7
 - Group Policy Management Console (GPMC), 204
- defaultChecked, 248, 292
- defaultClassStore, 82
- defaultItem, 292

- defaultKey, 292
 - defaultValue, 292
 - DEFCHECKED, 248
 - definitions, 292
 - delegation. *See also* permissions
 - Advanced Group Policy Management (AGPM), 203, 218–24
 - best practices, 224–28
 - creating GPOs, 208–10
 - default security, 203–7
 - deploying GPOs, 212
 - Domain, 221–23
 - editing GPOs, 215–16
 - Group Policy Management Console (GMPC), 203
 - linking GPOs, 210–13
 - managing GPOs, 213–15
 - modeling GPOs, 216–17
 - privileges, 62, 376
 - RSoP of GPOs, 218
 - delete element, 292
 - Delete, delegation, 213–15
 - DeleteGPO.wsf, 183
 - dependencies, Group Policy, 68–72
 - deploy permission, 415–17
 - Deployed Printer Connections, 89, 104
 - deployment strategy, 97–100
 - description
 - .adml file, 292
 - GPC Active Directory Properties, 82
 - desktop
 - images, 304
 - item-level targeting, 343
 - Local Users and Groups, 318
 - management, 15–16, 18, 45, 216, 301
 - security, 281, 356
 - specialized, 48
 - Desktop, Administrative Templates settings, 368
 - DesktopStandard, 36–37
 - destination name, 169–70
 - device drivers, 60
 - Devices preference, 315
 - Devices.xml, 79
 - DFS. *See* Distributed File System (DFS)
 - DFSR. *See* Distributed File System Replication (DFSR)
 - DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
 - Dial-Up Connection, 329
 - Dial-Up Networking (DUN), 318
 - difference reports, 419–21
 - digital signatures, 61
 - directories, 60–61
 - disabled GPO settings, 33
 - disabledList, 248, 292
 - disabledValue, 248, 292
 - DisableTaskMgr, 259
 - disaster recovery, 13, 149
 - Disk Space, 330, 343
 - Diskquota.dll, 88
 - displayName, 82, 292
 - DisplayName, 90
 - displayNamePrintable, 82
 - distinguishName, 82
 - Distributed File System (DFS), 54, 70–72
 - Distributed File System Replication (DFSR), 71, 84–86
 - diversity, management, 18
 - DLLName, 90
 - DLLs, 17
 - DNS. *See* Domain Name System (DNS)
 - docking stations, 61
 - document element, 294
 - documentation
 - Common tab, 324–25
 - GPO editing, 225
 - GPO reports, 148–51, 154
 - GPO settings changes, 35
 - Domain Admins group, 207
 - domain controllers
 - architecture, 73–76
 - discovery, troubleshooting, 441–42, 454
 - GPO administration, 123–24
 - GPO editing, 75–76
 - GPO version number, 108
 - Group Policy template, 30
 - Network Location Awareness, 28–29
 - security, 356
 - selection, 73–76
 - Domain Controllers Organizational Unit (OU), 122
 - Domain Delegation, 221–23
 - Domain Global Group, 168–69
 - Domain Local Group, 169
 - Domain Name System (DNS), 69–70
 - domain name, fully qualified (FQDN), 72
 - domain trusts, 121
 - domains
 - adding, 122
 - affiliation, 150
 - migrating GPOs, 163–68
 - test, 227
 - Domains node
 - GPO reports, 150
 - Group Policy Management Console (GPMC), 120
 - linking GPOs, 126
 - precedence, 97–100
 - targeting, 330
 - Dot3gpcInt.dll, 89
 - drive mappings, 11, 301, 343–44, 377–78
 - Drive Maps preference, 310–11
 - Drives.xml, 80
 - dropdownList, 292
 - DROPDOWNLIST, 248, 270, 273
 - dSASignature, 82
 - dSCorePropagationData, 82
 - DumpGPOInfo.wsf, 184
 - DumpSOMInfo.wsf, 184–85
 - Dw20.adm, 235
 - Dynamic Host Configuration Protocol (DHCP), 428–29
- ## E
- Edit Settings, 213–15
 - Editor permission, 220–21
 - EDITTEXT, 247–48, 261, 270, 273–75
 - EDIT-TEXT, 271
 - EFS. *See* Encrypting File System (EFS)
 - EFS Recovery, 89, 104, 363–64
 - elements, 247
 - elements, element, 292, 295
 - e-mail configuration, 411–12
 - Enable Keyword Filters, 147–48
 - Enable Requirements Filters, 147–48
 - EnableAsynchronousProcessing, 90
 - enabledList, 248, 292
 - enabledValue, 248, 293
 - EnableSynchronousProcessing, 90
 - Encrypting File System (EFS), 55
 - encryption, 61
 - END, 248
 - END CATEGORY, 261
 - END PART, 261
 - END POLICY, 261
 - Enforce option, 111–12
 - Enforcement Clients, 365

- enterprise administration, 13
 - Enterprise Admins, 225
 - Enterprise QoS, 89, 105
 - enum, 248, 293
 - Environment preference, 301, 311
 - Environment Variable, 343
 - EnvironmentVariables.xml, 79
 - Error event, 437, 446
 - ErrorCode, 437
 - ErrorDescription, 437
 - ES_OEMCONVERT, 274
 - Event IDs, 434, 447–48
 - applied GPO list, 455
 - client-side extension (CSE)
 - processing, 452
 - client-side failure, 458
 - computer information, 454
 - computer start/end, 450
 - computer startup wait, 456
 - domain controller discovery, 454
 - filtered GPO list, 455
 - loopback processing, 455
 - manual refresh, 451
 - network bandwidth, 457
 - network change, 450–51
 - network information, 455
 - network location awareness
 - service warning, 458
 - next policy processing, 456
 - periodic refresh, 452
 - scripts processing, 453
 - security principal, 454
 - service configuration, 457
 - Service Control Manager
 - notification, 457
 - successful or informational
 - interaction, 456
 - trace events, 453
 - user logon start/end, 450
 - Winlogon notification, 457
 - Event Log, 31, 357, 432–33
 - Event Viewer, 31, 354, 437
 - EventSources, 90
 - exandable, attribute, 293
 - Excel 2003, 235
 - Excel11.adm, 235
 - executables, 320
 - EXPANDABLETEXT, 274
 - EXPLAIN, 248, 267, 278–79
 - Explain Text, 147–48, 295
 - explainText, 248, 293
 - explanation text, 32
 - explicitValue, 293
 - EXPLICITVALUE, 276
 - extensibility. *See* extensions, Group Policy
 - extension files, 124, 445
 - Extension Registry Values, 90–91
 - ExtensionDebugLevel, 90
 - ExtensionEventSource, 90
 - extensionName, 82
 - ExtensionRsopPlanningDebugLevel, 90
 - extensions, 11, 17
- F**
- Failure events, 446
 - fallbackCulture, 293
 - falseList, 293
 - falseValue, 293
 - Fdeploy.dll, 88
 - Fdeploy1.ini, 79
 - file access, 354
 - file extensions, 316
 - File Match, 332, 343–44
 - File Replication System (FRS), 71, 84
 - File System, 163, 358–59
 - fileName, 293
 - files
 - back up, 60
 - ownership, 61
 - restore, 61
 - transfers, 377–78
 - Files preference, 312
 - Files.xml, 79
 - filters, 13, 31–33
 - Administrative Templates, 146–48, 258
 - Group Policy Preferences, 306
 - item-level targeting, 326
 - options, 147–48, 280
 - security, 112–13
 - FindDisabledGPOs.wsf, 188–89
 - FindDuplicateNamedGPOs.wsf, 189
 - FindGPOsbyPolicyExtension.wsf, 189
 - FindGPOsbySecurityGroup.wsf, 190
 - FindGPOsWithNoSecurityFiltering.wsf, 190–91
 - FindOrphanedGPOsInSysvol.wsf, 191
 - FindSOMsWithExternalGPOLinks.wsf, 191
 - FindUnlinkedGPOs.wsf, 191
 - firewall, settings, 54
 - firmware environment, 60
 - floppy drives, 315
 - Folder Options preference, 316
 - Folder Redirection, 11, 79, 104, 164, 366–67
 - Folder Restriction, 88
 - Folders preference, 312
 - Folders.xml, 79
 - foreground refresh, 101–3
 - foreign languages, 252
 - forests, 121–22, 142
 - Fp11.adm, 235
 - FQDN. *See* domain name, fully qualified (FQDN); fully qualified domain name (FQDN)
 - Free Text, 169
 - FrontPage2003, 235
 - FRS. *See* File Replication System (FRS)
 - fSMORoleOwner, 82
 - full control delegation, 218–19
 - FullArmor Corporation, 471
 - fully qualified domain name (FQDN), 72
- G**
- Gall1.adm, 235
 - GenerateGroupPolicy, 90
 - GetReportsForAllGPOs.wsf, 185–86
 - GetReportsForGPO.wsf, 186
 - GPAAnswers.com, 495
 - GPC. *See* Group Policy Container (GPC)
 - gPCFileSysPath, 82
 - gPCFunctionalityVersion, 82
 - gPCMachineExtensionNames, 82, 88
 - gPCUserExtensionNames, 82, 88
 - gPCWQLFilter, 82
 - GPE.ini, 77
 - gpedit.msc, 47
 - GPExpert Troubleshooting Pak, 476
 - GPExpertTM Backup Manager for Group Policy, 478
 - GPExpertTM Group Policy Spy 1.1, 477
 - GPExpertTM Health Reporter 1.6, 476
 - GPExpertTM Log Analyzer 1.1, 476
 - GPExpertTM Scripting Toolkit for PowerShell, 196–97, 477
 - GPExpertTM Status Monitor 1.1, 477
 - GphPath, 345
 - GPLogView, 458–59
 - GPMC. *See* Group Policy Management Console

- GPMC PowerShell Cmdlets, 478
 - GPME. *See* Group Policy Management Editor (GPME)
 - GPMonitor.exe, 462
 - GPOGuy.com, 494
 - GPOs. *See* Group Policy Objects (GPOs)
 - GPOTool, 464
 - GPOVault, 402
 - Gpprefcl.dll, 88–89
 - Gpprnext.dll, 89
 - GPResult, 462–63
 - Gpscript.dll, 88
 - GPT. *See* Group Policy Template (GPT)
 - Gpt.ini, 77
 - Gptext.dll, 88–89
 - GptPath, 345
 - GptTmpl.inf, 78
 - GPUdate, 105–7, 446, 464
 - GrantPermissionOnAllGPOs.wsf, 192–93
 - granular link control, 13
 - group permission, 150
 - Group Policy
 - benefits, 14–19
 - defined, 40
 - feature overview, 5–12
 - history, 3–4
 - negatives, 19–20
 - technology milestones, 23–24
 - Group Policy Administrator, 474
 - Group Policy Applications, 80, 89, 105
 - Group Policy Container (GPC)
 - architecture, 67, 70–71, 76, 80–83
 - deleting GPOs, 215
 - GPO version number, 107
 - Group Policy Creator Owners, 206, 225
 - Group Policy Data Sources, 79, 88, 104
 - Group Policy Device Settings, 88, 104
 - Group Policy Devices, 79
 - Group Policy Drive Maps, 80, 88, 104
 - Group Policy Environment, 79, 88, 104
 - Group Policy Files, 79, 88, 104
 - Group Policy Folder Options, 79, 89, 104
 - Group Policy Folders, 77, 79, 88, 104
 - Group Policy Ini Files, 79, 89, 104
 - Group Policy Internet Settings, 80, 89, 105
 - Group Policy Local Users and Groups, 79, 88, 104
 - Group Policy Management Console (GPMC), 13, 24, 36, 40, 67
 - Active Directory, 52–54
 - advanced features, 141
 - AGPM/Change Control, 401
 - creating GPOs, 208–10
 - default security environment, 204
 - delegation, 203, 207–8
 - domain views, 120
 - editing GPOs, 215–16
 - forest views, 121–22
 - Group Policy Preferences, 307–8
 - limitations, 122
 - linking GPOs, 127, 210–13
 - managing GPOs, 213–15
 - modeling GPOs, 154–59, 216–17
 - overview, 119–24
 - RSoP of GPOs, 218
 - scripts, 173–74
 - backup/restore GPOs, 174–77
 - copying and importing GPOs, 177–79
 - creating objects, 179–83
 - custom, 196
 - deleting GPOs, 183
 - finding GPOs by parameter, 188–91
 - GPO reporting, 183–88
 - security, 192–96
 - VBScript, 197
 - Windows PowerShell, 197–99
 - searching GPOs, 142–46
 - site views, 122
 - troubleshooting features, 460
- Group Policy Management Console 1.0, 23
- Group Policy Management Console 2.0, 23
- Group Policy Management Editor (GPME), 36, 40, 67
 - .adm/ADMX conversion syntax, 272–77
 - Administrative Templates (.adm), 146–48, 234
 - delegations, 215
 - Group Policy Preferences, 306–9
- Group Policy Manager, 475
- Group Policy Modeling, 154–59, 205, 216–17
- Group Policy Network Options, 79, 88, 104
- Group Policy Network Shares, 79, 88, 104
- Group Policy Object Editor. *See* Group Policy Management Editor (GPME)
- Group Policy Objects (GPOs), 40. *See also* Default Domain Controllers Policy; Default Domain Policy; reports; scripts
 - Active Directory, 52–54
 - Administrative Templates, filtering, 146–48
 - approver permission, 221
 - backups, 130–32, 134, 417–18
 - Block Inheritance, 109–12
 - client-side extensions (CSEs), 271
 - Comments, 159–62
 - configuration management, 128–29
 - creating, 61–64, 124–26, 224, 413–15
 - default, 54, 460–62
 - default processing, 109
 - delegations
 - creating GPOs, 208–10
 - default, 205
 - editing GPOs, 215–16, 220–21
 - full control, 218–19
 - linking GPOs, 210–13
 - managing GPOs, 213–15
 - modeling, 216–17
 - RSoP of GPOs, 218
 - deleting, 215
 - deploying, 415–17
 - disabling objects, 63, 276
 - discovery, troubleshooting, 443–44
 - documenting changes, 35
 - domain controllers, 123–24
 - Domain Name System (DNS), 70
 - editing, 75–76, 205, 225–26, 407
 - enabling/disabling, 129
 - Enforce, 111–12
 - foreground-only, 430
 - Group Policy Results, 152
 - linking, 126–28, 130, 205, 226, 423–24
 - management of, 73–76, 213–15
 - migrating, 162–67, 169–70
 - multiple local (MLGPO), 25–28
 - precedence, 96–100
 - Production GPOs, 160–61
 - Recycle Bin, 422–23

- registry-based, 282–83, 296
 - renaming, 130
 - replication, 84–87
 - reporting, 148–51, 154
 - restoring, 132–33, 417–18, 423–24
 - searching, 142–46
 - security filtering, 112–13
 - settings conflicts, 96–100
 - Starter, 34, 135–38
 - structural overview, 40–42, 349–50
 - testing, 226–28
 - updating, 107–9, 123
 - user-specific local, 26–27
 - version checking, 107–9
 - Group Policy Operational log, 31–32, 438–39
 - pre-processing, 439
 - computer role discovery, 442
 - domain controller discovery, 441–42
 - GPO discovery, 443–44
 - informational/success interaction, 440
 - loopback mode discovery, 442–43
 - nonsystem GP extension discovery, 445
 - retrieve account info, 440
 - security principal discovery, 442
 - slow link detection, 444–45
 - Start events, 440
 - trace component event, 440
 - Group Policy Policies, 306–7
 - Group Policy Power Options, 79, 89, 105
 - Group Policy Preferences, 17, 36, 301–2
 - Action Modes, 323
 - benefits, 302–5
 - client-side extensions (CSEs), 301, 308
 - Common tab, 324–25
 - Control Panel settings
 - Data Sources, 315
 - Devices, 315
 - Folder Options, 316
 - Internet Settings, 317
 - Local Users and Groups, 318
 - Network Options, 318
 - Power Options, 318
 - Printers, 320
 - Regional Options, 320
 - Scheduled Tasks, 320
 - Services, 322
 - Start Menu, 322
 - default processing, 115
 - environmental variables, 345–46
 - management and support, 307–9
 - policies vs preferences, 306–7
 - registry management, 9
 - settings, 306–7, 309
 - Settings reports, 346–47
 - software development kit, 347
 - Windows settings
 - Applications, 310
 - Drive Maps, 310–11
 - Environment, 311
 - Files, 312
 - Folders, 312
 - Ini Files, 313
 - Network Shares, 313
 - Registry, 313–14
 - Shortcuts, 315
 - Group Policy Printers, 79, 89, 104
 - Group Policy Regional Options, 80, 89, 105
 - Group Policy Registry, 79, 89, 104
 - Group Policy Results, 151–54, 205
 - Group Policy Scheduled Tasks, 79, 89, 104
 - Group Policy Script Repository, 492
 - Group Policy Service, 72–73, 79, 89, 104
 - Group Policy setting title, 295
 - Group Policy Shortcuts, 79, 89, 104
 - Group Policy Start Menu, 80
 - Group Policy Start Menu Settings, 89, 105
 - Group Policy Template (GPT), 30
 - Administrative Templates (.adm), 234
 - architecture, 67, 70, 76–80
 - deleting GPOs, 215
 - GPO version number, 107
 - registry-based GPO policies, 282–83, 296
 - SYSVOL replication, 84–86
 - Group Policy Webcast web site, 492
 - Group Policy Wiki, 489
 - GroupPolicyVersion, 345
 - Groups.xml, 79
 - GUID, 143, 145, 150, 271
- H**
- hard return, 279
 - hardware component settings, 385–86
 - hash rules, 43
 - Health Registration Settings, 365–66
 - Help desk, 216, 281
 - Help text, 278–79
 - hibernation, 109, 318
 - HKEY_CURRENT_USER, 262–63
 - HKEY_LOCAL_MACHINE, 262–63
 - HKEY_USERS, 262–63
 - home environment, 25, 69
 - HTML format, 149
- I**
- ICMP. *See* Internet Control Message Protocol (ICMP)
 - id, attribute, 293
 - Iedkcs32.dll, 88–89
 - IGroupPolicyObject C++, 196
 - Import, 164, 166–67
 - ImportAllGPO.wsf, 179
 - ImportGPO.wsf, 178
 - Inbound Rule, 360
 - Inetcorp.adm, 234
 - Inetesc.adm, 236
 - Inetres.adm, 234, 236
 - Inetset.adm, 234
 - Inf11.adm, 235
 - InfoPath 2003, 235
 - Informational event, 437
 - infrastructure master, 73
 - infrastructure, view of, 120
 - inheritance, default, 109–15
 - Ini Files preference, 313
 - IniFiles.xml, 79
 - Inslr11.adm, 235
 - instanceType, 82
 - inter-domain interactions, 20
 - inter-forest interactions, 20
 - Internet Control Message Protocol (ICMP), 28, 108–9
 - Internet Explorer
 - Administrative Templates, 234, 236
 - Connection policy, 367–68
 - Group Policy Preferences, 302
 - maintenance, 44
 - Requirements Filter, 147
 - settings, 54, 317
 - supportedOn values, 288–89
 - Internet Explorer Advanced Security Configuration, 236
 - Internet Explorer Branding, 89, 104
 - Internet Explorer Maintenance, 79, 317, 367

Internet Explorer Zonemapping, 88, 104

Internet Protocol (IP) addresses, 69

Internet Settings preference, 317

InternetSettings.xml, 80

Inter-Site Topology Generator (ISTG), 86

IP address configuration, 428

IP Address Range, 332

IP Security, 43, 81, 89, 105

IPSEC, 81

IPsec policies, 131, 366

ipsecPolicy objects, 81

IsAsyncProcessing, 435

IsBackgroundProcessing, 435

isCriticalSystemObject, 82

isDeleted, 82

IsDomainJoined, 435

ISO-style Language/Culture Names, 252

ISTG. *See* Inter-Site Topology Generator (ISTG)

item, 248

item, element, 293

K

Kerberos Policy, 56, 69–70, 353–54, 431

key, 248

key, attribute, 293

KEYNAME, 248, 261, 263–64, 268

keywords, element, 293

kiosks, 27, 48–49

Knowledge Consistency Checker (KCC), 86

L

label, element, 293

LAN Manager, 61

Language, targeting item, 333

Language/Culture Names, ISO-style, 252

language-specific ADMX files (.adml), 252, 283–86, 289–96

laptops, 109, 343

LastDriveMapped, 345

lastKnownParent, 82

LDAP. *See* Lightweight Directory Access Protocol (LDAP)

LDAP query, 334

LDAP server, 61

least user access (LUA), 469

license reporting, 8–9

Lightweight Directory Access Protocol (LDAP), 69–70, 129

line breaks, 248, 279

Link GPOs, 205

link speed, 28

Linked WMI Filter, 143–44

links, 130–32, 150, 423–24

list, 248

list, element, 293

ListAllGPOs.wsf, 186

listBox, 248, 293

LISTBOX, 248, 270, 275–76

ListSOMPolicyTree.wsf, 188

Local Computer Policy Object, 25–26. *See also* Administrators Local GPOs; Non-Administrators Local GPOs

Local Group Policy Editor, 47

Local Group Policy Objects, 46–51. *See also* Administrators Local GPOs; Local Policy Object; Non-Administrators Local GPOs; User Specific Local GPOs

Local Group Policy settings, 306

Local Policies, 43, 354

Local Policy Object, 47–48, 51

local user passwords, 301. *See also* passwords

Local Users and Groups preference, 318

local, site, domain, organizational unit (LSDOU), 96–100

logoff, forced, 58

logon, 58, 60, 450

logon scripts, 301, 304–5, 309–10, 377–78

logs, 31. *See also* auditing; Event Log; Group Policy Operational Log; Security Log; System Log

Loopback Merge, 436

loopback processing, 442–43, 455

Loopback Replace, 436

M

MAC Address Range, 334

MACHINE, 262–63

Machine folder, 77, 81

malware, 376

Managed policy setting, 147

Match by SID, 340

MAX, 276–77

MAXLEN, 274, 278

maxLength, 293

MaxNGPLISTChangesInterval, 90

maxValue, 293

MDOP. *See* Microsoft Desktop Optimization Pack

media, removable, 315

memory quotas, 60

Microsoft Advanced Group Policy Management (AGPM). *See* Advanced Group Policy Management (AGPM)

Microsoft Chat, 236

Microsoft Clip Organizer, 235

Microsoft Desktop Optimization Pack (MDOP), 36–37, 207

Microsoft Diagnostics and Recovery Toolset, 258

Microsoft Disk Quota, 88, 104

Microsoft Group Policy team blog, 491

Microsoft Group Policy web site, 490

Microsoft Installer (MSI), 8

Microsoft Internet Explorer. *See* Internet Explorer

Microsoft Management Console (MMC), 48–50

Microsoft NetMeeting, 234

Microsoft Office, 310

Microsoft Office Access 2003, 235

Microsoft Office Excel 2003, 235

Microsoft Office FrontPage 2003, 235

Microsoft Office InfoPath 2003, 235

Microsoft Office OneNote 2003, 235

Microsoft Office Outlook, 235, 310

Microsoft Office PowerPoint, 235, 310

Microsoft Office Publisher 2003, 235

Microsoft Office Resource Kit, 235

Microsoft Office Word, 235, 310

Microsoft Offline Files, 89, 104

Microsoft Outlook Express Identity Manager, 236

Microsoft TechNet web site, 492

Microsoft Visual Studio, 283

Microsoft Windows 2000. *See* Windows 2000

Microsoft Windows 95. *See* Windows 95

Microsoft Windows 98. *See* Windows 98

Microsoft Windows NT. *See* Windows NT

Microsoft Windows Server 2000.
 See Windows Server 2000

Microsoft Windows Server 2003.
 See Windows Server 2003

Microsoft Windows Server 2008.
 See Windows Server 2008

Microsoft Windows Vista.
 See Windows Vista

Microsoft Windows XP.
 See Windows XP

Microsoft.Policies.Windows, 286

Migration Table Editor, 168, 170

Migration Tables, 168–71, 227

MIN, 276–77

minRequiredRevision, 293

minValue, 294

MLGPO. *See* Multiple Local GPOs

MMC. *See* Microsoft Management Console (MMC)

Modify Security, 213–15

Moskowitz Inc., 472

mS-DS-ConsistencyChildcount, 82

mS-DS-ConsistencyGuid, 82

msDS-NcType, 82

msDS-ObjectReference, 82

MSI. *See* Microsoft Installer (MSI)

MSI Query, 334–36

msieee80211-Policy objects, 81

ms-net-ieee-8023-GroupPolicy objects, 81

Multiple Local GPOs (MLGPO), 25–28

N

Name, 82

name, attribute, 294

nameSpace, 294

NetIQ, 474

Network Access Protection, 78, 365

Network Location Awareness (NLA), 28–29, 108–9

Network node, 43, 368–69

Network Options preference, 318

Network Settings, 236

Network Shares preference, 313

NetworkOptions.xml, 79

networks

- access, 58, 69
- communication, 59
- connectivity, 28–29
- EventIDs, 450–51, 455, 457–58
- security, 58, 390–91
- troubleshooting, 430, 444–45
- zone rules, 43

NetworkShares.xml, 79

NLA. *See* Network Location Awareness (NLA)

NoBackgroundPolicy, 91

NoGPOListChanges, 91

NoMachinePolicy, 91

Non-Administrators Local GPOs, 26–27, 47–51

Non-Administrators Local Group Policy, 25

NoSlowLink, 91

noSort, 294

NotifyLinkTransition, 91

NoUserPolicy, 91

Ntdsutil, 13

NTFS permission, 358

number settings, 320

NUMERIC, 247, 270, 276–77

O

objectCategory, 82

objectClass, 83

objectGUID, 83

objects, 61

objectVersion, 83

Oe.adm, 236

OEM, 274

OEMCONVERT, 274

Office Access 2003, 235

Office Customization Tool (OCT), 310

Office Excel 2003, 235

Office FrontPage 2003, 235

Office InfoPath 2003, 235

Office OneNote 2003, 235

Office Outlook, 310

Office Outlook 2003, 235

Office PowerPoint, 310

Office PowerPoint 2003, 235

Office Publisher 2003, 235

Office Word, 235, 310

Office Word 2003, 235

Office11.adm, 235

Offline Pages, 236

on/off functionality, 281

OneNote2003, 235

Oment11.adm, 235

Open Database Connectivity (ODBC), 315

Open With, Folder options, 316

Operating System, 336, 343

operating systems. *See also* individual operating system names

Administrative Templates (.adm), 241

ADMX files, 284

Group Policy Preferences

- platform support, 301–2, 307–8
- SUPPORTED syntax, 280

Operation Master token, 123

operational log, 31–32, 433–39

Options.xml, 79

Organizational Unit

- Domain Controllers, 122
- linking GPOs, 63–64, 126
- targeting, 336

organizational units

- Active Directory, 68–69
- GPO links, 211
- GPO reports, 150
- precedence, 97–100
- testing, 226

Oscfilter.ini, 78

otherWellKnownObjects, 83

Outlk11.adm, 235

Outlook, 310

Outlook 2003, 235

P

packageRegistration objects, 81

pagefile, 60

parameter labels, 295

parentCategory, 247, 294

PART, 247, 261, 266, 269–70

partialAttributeDeletionList, 83

partialAttributeSet, 83

Password Policy, 56–57, 354

passwords

- control of, 55–57, 301
- editing settings, 54
- Local Users and Groups, 318
- Security Settings, 353–54
- user account, 43

Paste, migrating GPOs, 164–65

path rules, 43

PCMCIA, 336

PDC. *See* primary domain controller (PDC) emulator

PDC emulator, 73–74, 251, 431–32

pending GPOs, 415

Pending tab, 412–13

permissions

- Approver, 221–23
- creating GPOs, 206
- delegation, 192, 215
- deploy, 415–17
- Editor, 221
- linking GPOs, 212–13
- migrating GPOs, 165

- NTFS, 358
 - Read, 131
 - Read and Apply Group Policy, 215
 - Registry policy, 358
 - Reviewer, 220, 222–24
 - scripts for, 192–96
 - security filtering, 112–13
 - Write, 131
 - personnel management, 216
 - PerUserLocalSettings, 91
 - Ping command, 430
 - PKI. *See* Public Key Infrastructure (PKI)
 - policies
 - ADMX, 284, 294
 - creating, 44
 - filtering, 33
 - registry-based, 296
 - settings, 40
 - vs preferences, 242–43, 306–7
 - Policies node, 349–50
 - software settings, 350–52
 - Windows Settings
 - Remote Installation Services (RIS), 352
 - Scripts, 353
 - Security Settings, 353–68
 - POLICY, 247, 261, 266, 268
 - Policy Based QoS, 78
 - Policy Reporter, 486
 - Policy Setting Title, 147–48
 - policy, element, 294
 - PolicyActivityID, 435
 - PolicyApplicationMode, 435
 - Policy-Based QoS, 367
 - PolicyDefinitionFiles.xsd, 283
 - policyDefinitionResources, 294
 - policyDefinitions, 284, 294
 - PolicyDefinitions, 251
 - PolicyDefinitions.xsd, 283
 - policyDefinitionsResources, 286
 - PolicyMaker, 302. *See also* Group Policy Preferences
 - policyNamespaces, 284, 286, 294, 296
 - PolicyPak for Applications, 472
 - PolicyPak Group Policy Design Studio, 473
 - PolicyProcessingMode, 436
 - PolMan, 484
 - Polstore.dll, 89
 - Portable Computer targeting, 336
 - Power Options preference, 318
 - Power Users group, 26
 - PowerOptions.xml, 79
 - PowerPoint, 310
 - PowerPoint 2003, 235
 - Ppt11.adm, 235
 - precedence, 50–51, 96–100
 - Preference Settings, 40, 242–43, 372–73
 - preferences, 40. *See also* Group Policy Preferences
 - Applications, 310
 - default, 115
 - filtering, 33
 - vs policies, 242–43, 306–7
 - prefix, attribute, 294
 - presentation, 247
 - presentation attribute, 294
 - presentation elements, 294–95
 - presentationTable, 286, 294
 - primary domain controller (PDC) emulator, 123
 - PrincipalSamName, 435
 - printer mappings, 301, 377–78
 - Printers, 43, 320, 369–70
 - Printers.xml, 79
 - Privilege Manager, 469
 - privileges. *See also* delegation
 - creating new GPOs, 62
 - User Account Control, 376
 - process level token, 61
 - ProcessGroupPolicy, 91
 - ProcessGroupPolicyEx, 91
 - processing, 93
 - asynchronous, 103–4, 429, 436
 - background, 100
 - Block Inheritance, 109–12
 - default, 109
 - default inheritance, 109–15
 - Enforce option, 111–12
 - foreground, 101–3
 - loopback, 442–43
 - post-processing event IDs, 446
 - scope of management (SOM), 93–96
 - synchronous, 103–4, 429, 436
 - Processing Mode, 338
 - ProcessingTimeInMilliseconds, 436
 - Production GPOs, 160–61, 216
 - Production Organizational Unit, 227–28
 - Programs policy, 368
 - proxiedObjectName, 83
 - proxy settings, 54
 - proxyAddresses, 83
 - Pub11.adm, 235
 - Public Key Infrastructure (PKI), 43, 55, 57
 - Public Key Policies, 44, 78, 363–64
 - Publisher 2003, 235
- ## Q
- QoS Packet Scheduler, 88, 104
 - quarantine, 109
 - QueryBackupLocation.wsf, 176–77
 - Quest Software, 475
- ## R
- Radio Toolbar, 236
 - RAM, 339
 - Read and Apply Group Policy
 - permission, 215
 - Read gPLink, 212
 - Read GPOptions, 212
 - Read permission, 131
 - recovery options, 322
 - Recycle Bin, 422–23
 - ref, 294
 - refld, 294
 - refresh
 - background, 11, 17, 28, 100, 216, 436
 - Domain Name System, 69–70
 - Event IDs, 451–52
 - foreground, 101–3
 - GPUupdate, 105–7
 - Group Policy Preferences, 307, 325
 - network connectivity, 28
 - REG_BINARY, 90
 - REG_DWORD, 90–91, 270, 295
 - REG_EXPAND_SZ, 90, 270, 274, 293
 - REG_MULTI_SZ, 90
 - REG_SZ
 - extension registry values, 90–91
 - syntax, 270, 274, 277, 293, 295
 - Regional Options preference, 320
 - RegionalOptions.xml, 80
 - registry, 4
 - Administrative Templates, 234, 257, 260
 - client-side extensions (CSEs), 271
 - customization, 301, 377–78
 - filtering, 33
 - Group Policy Preferences, 306
 - management, 9
 - policy settings,
 - registry-based, 296
 - settings, 9, 40, 242–43
 - updating syntax, 262–66
 - values, binary, 281

- Registry
 - GPT files, 78
 - migrating GPOs, 163
 - Security Settings, 358
 - Registry Match, 339, 343–44
 - Registry preference, 313–14
 - Registry.pol, 78, 234, 239, 271, 282–83
 - Registry.xml, 79
 - REGMON, 258
 - reliability, 16–17
 - Remote Installation Services (RIS), 44, 57, 78, 352
 - Remote Server Administration Tools (RSAT), 308
 - replication
 - domain controllers, 70–71
 - edited GPOs, 216
 - Group Policy Objects (GPOs), 84–87
 - intra-site schedule, 87
 - replPropertyMetaData, 83
 - replUpToDateVector, 83
 - reports, 13–14
 - difference, 419–21
 - disaster recovery, 13, 149
 - Group Policy Objects (GPOs), 148–51, 154
 - scripts for, 183–88
 - settings, 346–47, 418–19
 - repsFrom, 83
 - repsTo, 83
 - REQUIRED, 274, 277–78
 - required, attribute, 294
 - REQUIREMENT field, 279–80
 - requirements filters, 147
 - RequireSuccessfulRegistry, 91
 - resources element, 284, 286, 293–94
 - restore
 - AGPM, 417–18, 423–24
 - deleted GPOs, 215
 - directories, 61
 - files, 61
 - scripts for, 174–77
 - RestoreAllGPOs.wsf, 176
 - RestoreGPO.wsf, 175
 - Restricted Groups, 163, 318, 353, 357
 - Resultant Set of Policy (RSoP), 34, 51, 93, 153, 158, 218
 - Resultant Set of Policy Provider (RSPP), 158–59
 - Reviewer permission, 220, 222–24
 - revision, 83, 246
 - revision, attribute, 295
 - RID master, 73
 - RIS. *See* Remote Installation Services (RIS)
 - RSAT. *See* Remote Server Administration Tools (RSAT)
 - RSoP. *See* Resultant Set of Policy (RSoP)
 - RSoPtools, 151
 - RSPP. *See* Resultant Set of Policy Provider (RSPP)
- S**
- SAM. *See* Security Accounts Manager (SAM)
 - Scecli.dll, 89
 - Scheduled Tasks preference, 320
 - ScheduledTasks.xml, 79
 - scheduling priority, 60
 - schema extensions, 124
 - schemaVersion, 83, 295
 - scope of management (SOM), 93–96, 352
 - delegation of permission, 192
 - precedence, 96–100
 - report scripts, 184–85, 188
 - settings conflicts, 96–100
 - screen saver, 54–55
 - scripts, 320
 - backup/restore GPOs, 174–77
 - copying/importing GPOs, 177–79
 - creating custom scripts, 196
 - creating objects, 179–83
 - deleting GPOs, 183
 - Event IDs, 453
 - finding GPOs by parameter, 188–91
 - GPO reports, 183–88
 - GPO security, 192–96
 - GPT files, 78
 - Group Policy Script repository, 492
 - logon, 377–78
 - Scripts node, 88, 104, 164, 353
 - searching, 31–33
 - Secedit, 105
 - Secure Server, 366
 - security, 17–18, 43.
 - See also* delegation
 - Account Policies, 55–57
 - Advanced Group Policy Management (AGPM), 204–7
 - anonymous connections, 7–8
 - audits, 60
 - client-side extensions (CSEs), 89, 104, 107
 - default environment, 203–7
 - desktop computers, 281
 - forest trusts, 121
 - GPO backups, 130–32
 - GPT files, 78
 - Group Policy Management Console (GPMC), 204
 - Group Policy Preferences, 301
 - Inbound Rule, 360
 - IP, 43
 - network, 58, 390–91
 - Outbound Rule, 361
 - passwords, resetting, 318
 - permissions, 170, 215
 - policy setting, 105, 368
 - principals, 165, 167–68, 442
 - reports, 150
 - scripts for, 190–91
 - tattooing, 9
 - User Account Control, 376
 - Security Accounts Manager (SAM), 50, 357
 - Security Filtering, 112–13, 150, 164, 205
 - Security Group, 143, 339
 - Security Group Membership, 152
 - Security Levels, 364
 - Security Log, 60, 357
 - Security Settings, 6–7, 353–54
 - Account Lockout Policy, 354
 - Account Policies, 353
 - Additional Rules, 364
 - Audit Policy, 354
 - Browser User Interface, 367
 - Client, 366
 - Connection, 367–68
 - Connection Security Rule, 362
 - default settings, 57
 - Enforcement Clients, 365
 - Event Log, 357
 - File System, 358–59
 - Folder Redirection, 366–67
 - Health Registration Settings, 365–66
 - Inbound Rule, 360
 - Internet Explorer Maintenance, 367
 - IPsec Policy, 366
 - Kerberos Policy, 354
 - Local Policies, 354
 - Network Access Protection, 365
 - Outbound Rule, 361

- Policy-Based QoS, 367
 - Programs, 368
 - Public Key Policies, 363–64
 - Registry, 358
 - Restricted Groups, 357
 - Secure Server, 366
 - Security, 368
 - Security Levels, 364
 - Security Options, 356
 - Server policy, 366
 - Software Restriction Policies, 364
 - System Services, 358
 - URLs, 368
 - User Interface Settings, 365
 - User Rights Assignment, 355–56
 - Windows Firewall with Advanced Security, 359
 - Wired Network (IEEE 802.3), 81, 89, 104, 359
 - Wireless Network (IEEE 802.11) Policies, 81, 362
 - see Also, 295
 - server management, 15–16, 18
 - installation, 401–6
 - Local Users and Groups, 318
 - security, 356
 - settings, 382
 - Server policy, 366
 - service account, 322
 - Service Control Manager, 457
 - Service Resource Records (SRVs), 69
 - Services preference, 322
 - Services.xml, 79
 - SetGPOCreationPermission.wsf, 193–94
 - SetGPOPermissions.wsf, 194
 - SetGPOPermissionsBySOM.wsf, 194–95
 - SetSOMPermissions.wsf, 195–96
 - Settings report, 148
 - shared computers, 48
 - Shared Folders, 45, 369–70
 - shared user accounts, 27
 - Shortcuts preference, 315
 - Shortcuts.xml, 79
 - showinAdvancedViewOnly, 83
 - shutdown
 - remote, forced, 60
 - system, 61
 - SID, 169
 - sign secure, 61
 - signatures, digital, 61
 - single process, 61
 - single-computer environment, 25
 - Site node, 97–100, 126
 - site views, 122
 - Site, targeting, 340
 - sites, 122
 - sleep, 318
 - small business environment, 25, 69
 - SMS Software, Inc., 14, 476
 - soft, attribute, 295
 - software deployment, 352
 - software distribution, 8–9, 11
 - software installation, 54, 352
 - client-side extensions (CSEs), 89
 - Domain Name System (DNS), 70
 - GPC files, 81
 - GPT files, 78
 - Software Installation, 105, 164
 - Software Restriction Policies, 43, 78, 353, 364
 - Software settings, 42
 - Software Update Service (SUS), 236
 - SOM. *See* scope of management (SOM)
 - source name, 168–69
 - Source type, 169
 - Sp1shell.adm, 236
 - Special Operations Software, 478
 - specialized desktops, 27, 48–49
 - Specops Command, 481
 - Specops Deploy, 479
 - Specops Gpupdate, 483
 - Specops Inventory, 480
 - Specops Password Policy, 482
 - SPIN 0, 277
 - SPIN value, 277
 - spin, attribute, 295
 - spinStep, 295
 - Srchatadmin.dll, 89
 - SRV. *See* Service Resource Records (SRVs)
 - SRV records, 72
 - stability, 19
 - standby, 109
 - Start events, troubleshooting, 440, 446
 - Start Menu, 45, 322, 369–70
 - Starter GPOs, 34, 135–38, 159–62, 209–10, 215–16
 - StartMenuTaskbar.xml, 80
 - startup type, 322
 - static nodes, 281
 - storeAsText, 295
 - Stored User Names and Passwords, 163
 - string, 246
 - string, element, 295
 - STRINGS, 266–67, 273
 - Stringsreference(!), 246
 - stringTable, 246, 286, 294–95
 - subRefs, 83
 - Subs.adm, 236
 - subscribing to an event, 31
 - suggestion elements, 294–95
 - SUGGESTIONS, 271
 - supersededAdm, 295
 - SUPPORTED, 247, 279–80
 - supportedOn, 247, 284, 288–89, 295
 - synchronous processing, 103–4, 429
 - Sysprosoft, 484
 - System account, 324
 - System Center Configuration Manager, 8, 14
 - System event log, 437
 - System Log, 357, 437
 - System node, 43
 - system performance, 61
 - System Policies, 4
 - System Policy Editor (Poledit.exe), 234–35
 - System Services, 163, 358
 - system settings, 9–10
 - system shut down, 61
 - System State, 215
 - system time, 60
 - system.adm, 235–36, 279
 - SystemFlags, 83
 - Systems Management Server (SMS), 8
 - SYSVOL
 - ADMX central store, 251
 - DFS/DFSR, 71–72, 84–86
 - GPO creation, 206
 - registry-based policy settings, 296
 - replication, 70–71, 84–86
- T**
- target, element, 295
 - Targeting Editor, 327, 342
 - targeting, item-level, 310, 318, 325–27
 - Battery Present, 328
 - common scenarios, 342–44
 - Computer Name, 328
 - CPU Speed, 328
 - Date Match, 329
 - default processing, 115
 - Dial-Up Connection, 329
 - Disk Space, 330

Domain, 330
 Environmental Variable, 331
 File Match, 332
 Group Policy Preferences, 306
 IP Address Range, 332
 Item-Level Targeting
 Controls, 342
 items, 327
 Language, 333
 LDAP query, 334
 MAC Address Range, 334
 MSI Query, 334–36
 Operating System, 336
 Organizational Unit, 336
 PCMCIA Present, 336
 Portable Computer, 336
 Processing Mode, 338
 RAM, 339
 Registry Match, 339
 Security Group, 339
 Site, 340
 Terminal Session, 340
 Time Range, 340
 User, 340
 WMI Query, 341
 Task Scheduler, 320
 Taskbar, 45, 369–70
 tattooing, 9
 TCP/IP printers, 320
 TeamGPExpert, 487
 TeamGPExpert.com, 494
 templates. *See also* ADM templates
 (.adm); ADMX files (.admx)
 AGPM and, 421–22
 Temporary Internet Files, 234
 Terminal Services, 373
 Terminal Session, 340
 testing
 best practices, 226–28
 environment, 20
 tools, 20
 text, 247–48
 TEXT, 247, 270, 277
 text, element, 295
 textBox, 247
 TextBox, decimal, 292
 textbox, element, 295
 Time Range, 340
 time, system, 60, 320, 431
 titles, 32
 TPC connection, 28
 trace events, 453
 tracking account management, 354
 tracking changes, 295, 408–10
 training facility desktops, 27, 48
 Transmission Control Protocol,
 69–70

troubleshooting, 427–28
 asynchronous processing, 429
 Common tab, 324–25
 DNS-related problems, 428–29
 event logs, using, 432–33
 Event Viewer, 437
 associate Starting events, 446
 errors, warnings, failures, 446
 evaluate operational log,
 438–39
 evaluate system log, 437
 GPUUpdate, 446
 isolate events, 446
 post-processing view, 446
 pre-processing view, 439–45
 processing view, 445
 foreground-only GPOs, 430
 GPO reports, 149
 network connections, 430
 operational log, 433–37
 PDC Emulator, 431–32
 tools, 12, 19
 Dcgpofix.exe, 460–62
 GPLogView, 458–59
 GPMonitor.exe, 462
 GPOTool, 464
 GPResult, 462–63
 GPUUpdate, 464
 Group Policy Management
 Console (GPMC), 460
 WMI filter deletion, 430–31
 true policies, 242
 trueList, 295
 trueValue, 296
 trust detection, 121
 trust relationships, 163
 TXTCONVERT, 277

U

UNC Path, 169
 Universal Group, 169
 Universal Naming Convention
 (UNC), 164–65, 167–68
 updates
 Administrative Templates
 (.adm), 240
 Domain Name System, 69–70
 version checking, 107–9
 upgrades, Group Policy Preferences,
 301–2
 URI, 294
 url, 83
 URLs, 368
 USB ports, 315
 User, 168–69, 340
 USER, 262–63

User Account Control (UAC),
 47, 376
 user accounts, 41–42. *See also*
 accounts
 administration of, 69
 AGPM administrator, 206–7
 passwords, 43, 55–57
 policy setting, 49
 Security Settings, 354
 shared, 27
 User Configuration, 41–42, 44–46,
 77. *See also* Policies node
 Administrative Templates
 (.adm), 236
 ADMX files, 243
 CLASS options, 284
 default settings, 57
 GPO reports, 150
 GPO searching, 143–44
 Group Policy Preferences, 303,
 309, 325
 hardware component settings,
 385–86
 logon scripts, 377–78
 network security settings, 390–91
 Preferences Settings, 372–73
 server settings, 382
 Terminal Services, 373
 User Account Control, 376
 User folder, 77, 81
 user interface, 306
 User Interface Settings, 365
 user logon, 354
 user permission, 150
 user profile, 45
 user rights, 43, 59
 User Rights Assignment, 163, 353,
 355–56
 user settings, viewing, 151
 Userenv, 432–33
 User-Specific Local GPOs, 26–27,
 49–51
 User-specific Local Group Policy, 25
 using, element, 296
 uSNChanged, 83
 uSNCreated, 83
 uSNDSALastObjRemoved, 83
 USNIntersite, 83
 uSNLastObjRem, 83
 uSNSource, 83

V

validation, 0–9
 value, attribute, 296
 value, element, 296
 valueList, 296

valueName, 248, 296
 VALUENAME, 248, 261, 264
 VALUEOFF, 248
 VALUEON, 248
 VALUEON/VALUEOFF, 264–66,
 270–71
 valuePrefix, 296
 VALUEPREFIX, 276
 VBScript, 196–97
 version checking, 107–9
 versionNumber, 83
 virtual private network (VPN),
 109, 318
 viruses, 376

W

Warning event, 437, 446
 wbemPath, 83
 wellKnownObjects, 83
 whenChanged, 83
 whenCreated, 83
 Window Advanced Security, 78
 Windows 2000, 23–24
 Administrative Templates,
 233–36
 AGPM operating system support,
 400–1
 AGPM Server installation, 402
 GPRResult, 462–63
 Group Policy Preferences,
 301–2, 308
 Help text, 278–79
 refresh, 105
 supportedOn values, 288–89
 SYSVOL, 71, 84
 Windows 2000 Service Pack 3
 (SP3), 235
 Windows 95, 262
 Windows 98, 235
 Windows 9x, 234–35
 Windows Components, 43, 370–72
 Windows Firewall, 43, 78
 Windows Firewall with Advanced
 Security, 359
 Windows Installer, 147, 235
 Windows Management
 Instrumentation (WMI),
 113–15, 130–32, 216
 Windows Media Player, 147, 235–36
 Windows NT, 4, 234–35, 262
 Windows PowerShell, 196–99
 Windows Search Group Policy, 104
 Windows Search Group Policy
 Extension, 89

Windows Server 2000, 262
 Windows Server 2003, 23, 236
 #if version, 262
 Administrative Templates,
 233–35
 AGPM Client, 406–7
 AGPM operating system support,
 400–1
 AGPM Server installation, 402
 forest trusts, 121
 GPRResult, 462–63
 Group Policy Modeling, 155, 158
 Group Policy Preferences, 308
 Resource Kit, 235
 scripts, 196
 security, default, 204
 Service Pack 1 (SP1), 24, 89, 276,
 301–2, 309
 supportedOn values, 288–89
 SYSVOL, 71, 84
 web site, 491
 Windows Server 2008, 23, 36
 Administrative Templates (.adm),
 244–46
 ADMX central store, 251–52
 ADMX files, 30, 243–45
 AGPM Client, 406–7
 AGPM operating system support,
 400–1
 AGPM/Desktop Optimization
 Pack, 207
 client-side extensions, 88
 Comments, 159–62
 event logs, 432–33
 functional levels, 86
 GPRResult, 462–63
 Group Policy Management
 Console (GPMC), 119–20
 Group Policy Preferences, 301–2,
 308–9
 local GPOs, 46
 Network Location Awareness
 (NLA), 108–9
 new features, 24, 31–36
 registry management, 9
 Requirements Filter, 147
 scripts, 196
 security, default, 204
 settings, 16, 349–52
 Starter GPOs, 135–38
 SYSVOL, 71, 84
 User Account Control, 376
 Windows Firewall, 359
 Windows settings, Group Policy
 Preferences

Applications, 310
 Drive Maps, 310–11
 Environment, 311
 Files, 312
 Folders, 312
 Ini Files, 313
 Network Shares, 313
 Registry, 313–14
 Shortcuts, 315
 Windows Settings, Policies node,
 42, 44
 Administrative Templates, 368
 Remote Installation Services
 (RIS), 352
 Scripts, 353
 Security Settings, 353–68
 Windows Update, 235–36
 Windows Vista, 23, 36
 Administrative Templates (.adm),
 244–46
 ADMX central store, 251–52
 ADMX files, 30, 233, 243–44
 AGPM Client, 406–7
 AGPM operating system support,
 400–1
 AGPM/Desktop Optimization
 Pack, 207
 client-side extensions, 88–89
 event logs, 432–33
 Folder Options, 316
 GPRResult, 462–63
 Group Policy Management
 Console (GPMC), 119–20
 Group Policy Preferences,
 308–9
 local GPOs, 46–47
 multiple local GPOs (MLGPO),
 25–28
 Network Location Awareness
 (NLA), 108–9
 new features, 24–26
 Power Options, 318
 precedence, 97–100
 Printers, 320
 Requirements Filter, 147
 scripts, 196
 settings, 349–52
 Start Menu, 322
 supportedOn values, 288–89
 Task Scheduler, 320
 User Account Control, 376
 Windows Firewall, 359
 Wired Network, 359
 Windows XP, 23–24, 236
 #if version, 262

Administrative Templates (.adm),
 233–35, 245
 ADMX files, 245
 Folder Options, 316
 GPRresult, 462–63
 Group Policy Preferences, 308
 Network Location Awareness,
 28–29
 Power Options, 318
 Requirements Filter, 147
 scripts, 196
 Service Pack 1 (SP1), 235
 Service Pack 2 (SP2), 23–24, 89,
 301–2, 309, 320
 Start Menu, 322
 supportedOn values, 288–89
 Wireless Network Policies, 362
 Windows XP Professional, 288–89
 Windows XP Professional SP2, 276
 Windows.adm, 235
 Windows.admx, 286–88
 Winlogon, 457
 WinLogon. *See* Group Policy Service
 Winnt.adm, 235
 Wired Network (IEEE 802.3)
 Policies, 81, 89, 104, 359
 Wireless Group Policy, 88, 104
 Wireless Network (IEEE 802.11)
 Policies, 81, 362
 Wlgpclnt.dll, 88
 WMI, 158–59
 WMI Filters, 150, 152, 430–31
 WMI Query, 114, 341
 Wmp.adm, 236
 Wmplayer.adm, 235–36
 Word, 235, 310
 Word11.adm, 235
 workflow, 410–11
 Workflow Studio, 471
 workstations, adding, 59

Write gPLink, 212
 Write gPOptions, 212
 Write permission, 131
 Wuau.adm, 235–36
 wWWHomePage, 83

X

XML format
 ADML files, 283
 ADMX files, 283
 declaration, 284, 286, 296
 GPO reports, 149
 XML-based files, 29–30, 180–81,
 233
 xmlns, 296

Y

yes/no functionality, 281