Microsoft

Windows® Group Policy

William R. Stanek
Author and Series Editor

Administrator's Pocket Consultant

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

Copyright © 2009 by William R. Stanek

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: 2009920787

Printed and bound in the United States of America.

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

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 mspinput@microsoft.com.

Microsoft, Microsoft Press, Active Desktop, Active Directory, Internet Explorer, SQL Server, Win32, Windows, Windows NT, Windows PowerShell, Windows Serve, and Windows Vista are either registered trademarks or trademarks of the Microsoft group of companies. 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: Maria Gargiulo
Project Editor: Rosemary Caperton
Editorial Production: John Pierce, ICC Macmillan Inc.
Technical Reviewer: Mitch Tulloch; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Body Part No. X15-44299

Contents at a Glance

Contents

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:

microsoft.com/learning/booksurvey

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:

microsoft.com/learning/booksurvey

Acknowledgments

You know you've been at this thing called writing a long time when people ask how many books you've written and you just have no idea. For many years, my bio stated I was the author of more than 25 books. Several times my publishers have asked me to update the bio with a more precise number, so around number 61 I started counting to keep everyone happy. That was about five, six, seven years ago, so I'm now getting close to 100 or thereabouts. ;-)

For me, it's always been about the craft of writing. I love writing, and I love challenging projects most of all. The challenge in writing a day-to-day administrator's guide to Group Policy is that there's so much I'd like to cover, but pocket consultants aren't meant to be all-in-one references. Pocket consultants are meant to be portable and readable—the kind of book you use to solve problems and get the job done wherever you might be. With that in mind, I have to continually make sure I focus on the core of Group Policy administration. The result is the book you hold in your hand, which I hope you'll agree is one of the best practical, portable guides to Group Policy.

As I've stated in the three dozen or so pocket consultants I've written, the team at Microsoft Press is topnotch. Maria Gargiulo was instrumental throughout the writing process. She helped ensure that I had what I needed to write the book and was my primary contact at Microsoft. Martin DelRe was the acquisitions editor for the project. He believed in the book from the beginning and was really great to work with. Completing and publishing the book wouldn't have been possible without their help!

Unfortunately for the writer (but fortunately for readers), writing is only one part of the publishing process. Next came editing and author review. I must say, Microsoft Press has the most thorough editorial and technical review process I've seen anywhere—and I've written a lot of books for many different publishers. John Pierce managed the editorial process. He helped me stay on track and on schedule. Thank you so much!

Mitch Tulloch was the technical editor for the book. I always enjoy working with Mitch, and he did a solid review of the book's technical content. I would also like to thank Chris Nelson for his help during this project. Chris is terrific to work with and is always willing to help any way he can. Thanks also to everyone else at Microsoft who has helped at many points of my writing career and been there when I needed them the most.

Thanks also to Studio B, the Salkind Agency, and my agent, Neil Salkind.

I hope I haven't forgotten anyone, but if I have, it was an oversight. *Honest*. ;-)

Introduction

Windows Group Policy Administrator's Pocket Consultant is the only book on the market written from start to finish with both Group Policy preferences and Group Policy settings in mind. It is also the only book on the market written from start to finish with the Group Policy Management Console and Advanced Group Policy Management in mind. As a result, *Windows Group Policy Administrator's Pocket Consultant* offers Windows administrators a unique approach. The result, I hope, is a concise and compulsively usable resource for Windows administrators.

Because I focus on providing you with the maximum value in a pocket-sized guide, you don't have to wade through hundreds of pages of extraneous information to find what you're looking for. Instead, you'll find exactly what you need to get the job done. In short, the book is designed to be the one resource you consult whenever you have questions regarding Group Policy administration. To this end, the book concentrates on daily administration procedures, frequently performed tasks, documented examples, and options that are representative but not necessarily inclusive.

One of the goals is to keep the content so concise that the book remains compact and easy to navigate while ensuring that the book is packed with as much information as possible—making it a valuable resource. Thus, instead of a hefty thousand-page tome or a lightweight hundred-page quick reference, you get a valuable resource guide that can help you quickly and easily perform common tasks, solve problems, and implement features such as filtering Group Policy processing, migrating the SYSVOL, implementing change control, restoring Group Policy objects (GPOs), and troubleshooting.

Who Is This Book For?

Windows Group Policy Administrator's Pocket Consultant covers Group Policy for small, medium, and large organizations. The book is designed for:

- Current Windows and network administrators
- Support staff who maintain Windows networks
- Accomplished users who have some administrator responsibilities
- Administrators transferring from other platforms

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of both Windows and Active Directory. With this in mind, I don't devote entire chapters to understanding Windows architecture, Windows networking, or Active Directory. I do, however, provide complete

details on the components of Group Policy and how you can use these components. I explore the ins and outs of Group Policy. I cover how to keep pace with Group Policy changes, installing Group Policy extensions, applying Group Policy, and much more.

I also assume that you are fairly familiar with Windows commands and procedures as well as Active Directory. If you need help learning Active Directory basics, a good resource is *Active Directory Administrator's Pocket Consultant* (Microsoft Press, 2009).

How Is This Book Organized?

Windows Group Policy Administrator's Pocket Consultant is designed to be used in the daily administration of Group Policy, and as such the book is organized by job-related tasks rather than by features. Speed and ease of reference is an essential part of this hands-on guide. The book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick reference features have been added as well. These features include step-by-step instructions, lists, tables with fast facts, and extensive cross-references. The book is organized into both parts and chapters.

Group Policy is a collection of preferences and settings that can be applied to user and computer configurations. Part I, "Implementing Group Policy," reviews the fundamental tasks you need for Group Policy administration. Chapter 1 provides an overview of tools, techniques, and concepts related to Group Policy. Chapter 2 examines important changes to Group Policy and how these changes affect the way you use Group Policy. The chapter also provides detailed advice on using both policy preferences and policy settings, including tips on which technology to use when.

Part II, "Managing Group Policy," discusses the core tools and techniques you'll use to manage Group Policy. Chapter 3 explores techniques for configuring both Local Group Policy objects (LGPOs) and Active Directory–based Group Policy objects (GPOs). Not only will you learn about essential implementation considerations, you'll also find tips and techniques for working across domains, sites, and forests. Chapter 4 examines the change control features available when you implement Advanced Group Policy Management (AGPM). You'll learn how to manage workflow within the change control system and how to configure AGPM itself. In Chapter 5, you'll learn how to search and filter Group Policy. You can use the techniques discussed not only to find policy settings and search GPOs but also to control the security groups and computers to which policy is applied.

The book continues with Part III, "Maintaining and Recovering Group Policy." GPOs have two parts: a Group Policy container (GPC) stored in Active Directory, and a Group Policy template (GPT) stored in the SYSVOL. Chapter 6 shows you how

to migrate the SYSVOL to Distributed File System (DFS) Replication and how to maintain SYSVOL storage. You'll also find tips and techniques for troubleshooting replication. Chapter 7 discusses essential Group Policy concepts and provides tips and techniques for managing the way Group Policy works. Chapter 8 examines how to maintain, restore, and troubleshoot Group Policy. Finally, Appendix A provides a reference for installing Group Policy extensions and tools.

Conventions Used in This Book

I use a variety of elements to help keep the text clear and easy to follow. You'll find code terms and listings in monospace type, except when I tell you to actually type a command. In that case, the command appears in bold type. When I introduce and define a new term, I put it in italics.

Other conventions include:

- **Best Practices** To examine the best technique to use when working with advanced configuration and administration concepts
- **Cautions** To warn you when there are potential problems you should look out for
- **Notes** To provide details on a point that needs emphasis
- **Real World** To provide real-world advice when discussing advanced topics
- **Security Alerts** To point out important security issues
- **Tips** To offer helpful hints or additional information

I truly hope you find that *Windows Group Policy Administrator's Pocket Consultant* provides everything that you need to perform essential administrative tasks as quickly and efficiently as possible. You're welcome to send your thoughts to me at williamstanek@aol.com. Thank you.

Find Additional Content Online

As new or updated material becomes available that complements this book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. 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 is available at *http://www.microsoft.com/learning/books/online/serverclient* and is updated periodically.

Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address:

http://www.microsoft.com/mspress/support

If you have comments, questions, or ideas about this book, please send them to Microsoft Press using either of the following methods:

Postal Mail:

Microsoft Press
Attn: Editor, Windows Group Policy Administrator's Pocket Consultant
One Microsoft Way
Redmond, WA 98052-6399

E-mail:

mspinput@microsoft.com

Please note that product support isn't offered through these mail addresses. For support information, visit Microsoft's Web site at *http://support.microsoft.com/*.

CHAPTER 2

Deploying Group Policy

Group Policy provides a convenient and effective way to manage both preferences and settings for computers and users. With Group Policy, you can manage preferences and settings for thousands of users or computers in the same way that you manage preferences and settings for one computer or user—and without ever leaving your desk. To do this, you use one of several management tools to change a preference or setting to the value you want, and this change is applied throughout the network to the subset of computers and users you target.

Previously, making many of the administrative changes that Group Policy enables was possible only by hacking the Windows registry, and each change had to be made individually on each target computer. With Group Policy, you can simply enable or disable a policy to tweak a registry value or other preference or setting, and the change will apply automatically the next time Group Policy is refreshed. Because changes can be modeled through the Group Policy Management Console before the modifications are applied, you can be certain of the effect of each desired change. Prior to deploying a change, you can save the state of Group Policy. If something goes wrong, you can restore Group Policy to its original state. When you restore the state of Group Policy, you can be certain that all changes are undone the next time Group Policy is refreshed.

Before you deploy Group Policy for the first time or make changes to existing policy, you should ensure you have a thorough understanding of:

- How Group Policy has changed with the introduction of each new version of the Windows operating system.
- How you can update Group Policy to include the preferences and settings available in a new Windows operating system.

- How Group Policy is applied to a local computer as well as throughout an Active Directory environment.
- How default policy sets are used and when default policy applies.
- When to use policy preferences and when to use policy settings.

I discuss each of these subjects in this chapter.

Keeping Group Policy Up to Date

Group policies were introduced with Windows 2000 and apply only to systems running workstation and server versions of Windows 2000 and later. This means Group Policy applies only to systems running Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008, and later versions of Windows. Each new version of the Windows operating system has brought with it changes to the way Group Policy works, and I'll explore important changes in this section.

Core Process Changes

Unlike Windows 2000, Windows XP Professional, and Windows Server 2003, Windows Vista and Windows Server 2008 use the Group Policy Client service to isolate Group Policy notification and processing from the Windows logon process. Separating Group Policy from the Windows logon process reduces the resources used for background processing of policy while increasing overall performance and allowing delivery and application of new Group Policy files as part of the update process without requiring a restart.

Windows Vista and Windows Server 2008 don't use the trace logging functionality in Userenv.dll and don't write to the Application log. Instead, they write Group Policy event messages to the System log. Additionally, the Group Policy operational log replaces Group Policy trace logging events that previously were logged to %SystemRoot%\Debug\Usermode\Userenv.log. Thus, when you are troubleshooting Group Policy issues, you'll use the detailed event messages in the operational log rather than the Userenv log. In Event Viewer, you can access the operational log under Applications And Services Logs\Microsoft\Windows\GroupPolicy.

Windows Server 2008 uses Network Location Awareness instead of ICMP protocol (ping). With Network Location Awareness, a computer is aware of the type of network to which it is currently connected and can also be responsive to changes in the system status or network configuration. By using Network Location Awareness, the Group Policy client can determine the computer state, the network state, and the available network bandwidth. This change also allows Group Policy to be refreshed over Virtual Private Network (VPN) connections.

Policy Changes

Each new version of the Windows operating system introduces policy changes. Sometimes these changes have made older policies obsolete on newer versions of Windows. In this case the policy works only on specific versions of the Windows operating system, such as only on Windows XP Professional and Windows Server 2003. Generally speaking, however, most policies are forward compatible. This means that policies introduced in Windows 2000 can, in most cases, be used on Windows 2000, Windows XP Professional, Windows Server 2003, Windows Vista, and Windows Server 2008. It also means that Windows XP Professional policies usually aren't applicable to Windows 2000 and that policies introduced in Windows Vista aren't applicable to Windows 2000 or Windows XP Professional.

If a policy isn't applicable to a particular version of the Windows operating system, you can't apply it to computers running those versions of the Windows operating system. You will know if a policy is supported on a particular version of Windows because this is stated explicitly whenever you are working with a preference or setting.

Like Group Policy, the Group Policy Management Console (GPMC) has changed with new versions of Windows. GPMC version 1.0 worked with Windows XP and Windows Server 2003. The original Windows Vista release included GPMC version 1.5. When you install Service Pack 1 (SP1) on Windows Vista, GPMC version 1.5 is uninstalled. When you install the Remote Server Administration Tools (as discussed in Chapter 1, "Overview of Group Policy") and select GPMC as a tool you want to use, you install GPMC version 2.0. GPMC version 2.0 is also the version included with the original release of Windows Server 2008.

When you start using GPMC 2.0 or later in your domain environment, you should stop using previous versions of GPMC because GPMC 2.0 and later have been updated to work with new features and file formats that can only be managed using GPMC 2.0 or later. Because of this, you can only manage Windows Vista and Windows Server 2008 policies from computers running Windows Vista, Windows Server 2008, or later versions.

On a computer running Windows Vista, Windows Server 2008, or later versions, you'll automatically see the new features and policies as well as standard features and policies when you use GPMC 2.0 or later to work with Group Policy. However, the new features and policies aren't automatically added to Group Policy objects (GPOs). Don't worry—there's an easy way to fix this, and afterward you'll be able to work with new features and policies as appropriate throughout your domain.

To push new features and policies into the domain, you need to update the appropriate GPOs. Once you make the update, compatible clients are able to take advantage of the enhanced policy set, and incompatible clients simply ignore the settings they don't support.

You update a GPO for new features and policies by following these steps:

1. Log on to a computer running Windows Vista or a later release of Windows using an account with domain administrator privileges.
2. Open the Group Policy Management Console (GPMC) by clicking Start, pointing to Administrator Tools, and then selecting Group Policy Management.
3. In the GPMC, you'll see a Forest node representing the current forest to which you are connected (see Figure 2-1). When you expand the Forest node, you'll then see the Domains and Sites nodes. Use these nodes to work your way to the Group Policy object (GPO) you want to work with.

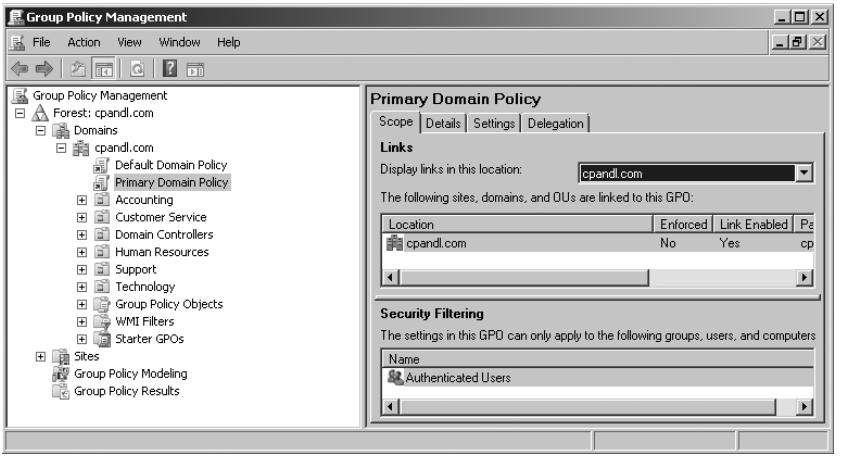

FIGURE 2-1 Group Policy Management Console connects to the local forest by default.

4. When you find the GPO you want to work with, right-click it and then select edit to open the Group Policy Management Editor, as shown in Figure 2-2.

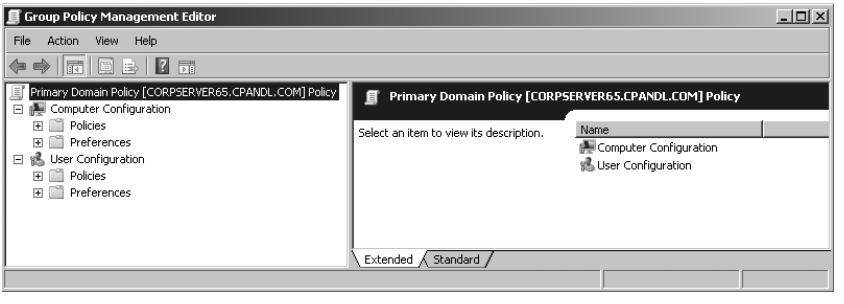

FIGURE 2-2 Editing a GPO in Group Policy Management Editor.

5. In the Group Policy Management Editor, click the Computer Configuration node and then click the User Configuration node. When you select these

nodes, the current administrative templates are read in and applied to the GPO you've selected. After Group Policy is refreshed, you can modify policy settings as necessary, and the changes will be updated as appropriate in the selected site, domain, or organizational unit.

6. Repeat this procedure to update the GPOs for other sites, domains, or organizational units.

Normally, nothing else about how Group Policy is used would change when you make this update. However, computers running Windows Vista and later support a new file format called ADMX. ADMX uses XML to format policies and changes the way data is stored in the SYSVOL.

SYSVOL Changes

With the original file format used with policies, called ADM, policy definition files are stored in the GPO to which they relate. As a result, each GPO stores copies of all applicable policy definition files and can grow to be multiple megabytes in size. In contrast, with the ADMX format, policy definition files are not stored with the GPOs with which they are associated by default. Instead, the policy definition files can be stored centrally on a domain controller and only the applicable settings are stored within each GPO. As a result, GPOs that use ADMX are substantially smaller than their counterparts that use ADM. For example, while a GPO that uses ADM may be 4 megabytes (MB) in size, a GPO that uses ADMX may be only 4 kilobytes (KB) in size.

The ADMX file format is entirely different from the ADM format previously used. ADMX files are divided into language-neutral files ending with the .admx file extension and language-specific files ending with the .adml extension. The language-neutral files ensure that a GPO has identical core policies. The language-specific files allow policies to be viewed and edited in multiple languages. Because the language-neutral files store the core settings, policies can be edited in any language for which a computer is configured, thus allowing one user to view and edit policies in English and another to view and edit policies in Spanish, for example. The mechanism that determines the language used is the language pack installed on the computer.

Language-neutral ADMX files are installed on computers running Windows Vista and Windows Server 2008 in the %SystemRoot%\PolicyDefinitions folder. Language-specific ADMX files are installed on computers running Windows Vista and Windows Server 2008 in the %SystemRoot%\PolicyDefinitions*LanguageCulture* folder. Each subfolder is named after the appropriate International Standards Organization (ISO) language/culture name, such as en-US for U.S. English.

Only policy editors that are compatible with the ADMX file format can read the policies that have been updated to use ADMX. When you start a compatible policy editor, it automatically reads in the ADMX files from the policy definitions folders. Because of this, you can copy ADMX files that you want to use to the appropriate policy definitions folder to make them available when you are editing GPOs. If the

policy editor is running when you copy the file or files, you must restart the policy editor to force it to read in the file or files.

In domains, ADMX files can be stored in a central store rather than in the PolicyDefinitions folder on each computer you use for GPO editing. Using a central store makes management of ADMX files easier and more efficient by allowing administrators to manage GPOs from any compliant computer on the network, simplifying version management of policy files and making it easier to add new policy files.

To create a central store for ADMX files, you must access a domain controller using an account that is a member of the Domain Admins group and then create a folder called PolicyDefinitions within the SYSVOL. This folder is where you'll place the language-neutral ADMX files. You'll also need to create subfolders within the PolicyDefinitions folder for each language that is supported in your ADMX files. These subfolders will store the language-specific resource files, which have the extension .adml. After you create the required folders, you need to copy the language-neutral ADMX definition files and the language-specific ADMX resource files to the appropriate folders in the central store.

Because the default location for the SYSVOL is %SystemRoot%\Sysvol, you would do the following to create and establish the central store in the default SYSVOL location:

1. Access a domain controller running Windows Server 2008 in the target domain using an account that is a member of Domain Admins, and then create a PolicyDefinitions folder under %SystemRoot%\Sysvol*DomainName*\Policies, where *DomainName* is the name of the domain in which the domain controller is located and for which you want to establish a central store. Within the PolicyDefinitions folder, create subfolders for each language that is supported in your ADMX files.

   REAL WORLD **As discussed in "Replication Changes" later in the chapter, domain controllers can replicate the SYSVOL using either File Replication Service (FRS) replication or Distributed File System (DFS) replication. The default SYSVOL location is %SystemRoot%\Sysvol when domain controllers replicate the SYSVOL using FRS replication. When domain controllers replicate the SYSVOL using DFS replication, the default SYSVOL location is %SystemRoot%\Sysvol_dfsr. If your domain controllers use DFS replication, you create the PolicyDefinitions folder under %SystemRoot%\Sysvol_dfsr*DomainName*\Policies and copy files to this location.**

2. Copy all the ADMX and ADML files from their original location on a target computer to the appropriate SYSVOL folders.

   Windows Vista SP1 and Windows Server 2008 have 146 default ADMX files. Each ADMX file has an associated ADML file located under one or more language-specific folders, such as en-US for U.S. English. These files are stored by default under %SystemRoot%\PolicyDefinitions and %SystemRoot%\PolicyDefinitions*LanguageCulture,* respectively. If you've created

custom ADMX files, these files are stored on the workstation on which they were created. If you are using an operating system later than Windows Vista SP1 or Windows Server 2008 RTM, there may be additional ADMX files that are available only on computers with this operating system and service pack combination installed.

If you want to create a central store for all languages supported by the computer on which you are currently logged on, you could copy all the required policy files from your computer to a target domain controller in a single step. Simply run the following commands at an elevated, administrator command prompt:

```
xcopy /s /y %SystemRoot%\PolicyDefinitions \\DC\Sysvol\DomainName\policies\
PolicyDefinitions\
```

where *DC* is the host name of the target domain controller, and *DomainName* is the fully qualified DNS name of the domain in which the domain controller is located. In the following example, you copy the ADMX and ADML files from your computer to CorpServer56 in the Cpandl.com domain:

```
xcopy /s /y %SystemRoot%\PolicyDefinitions \\CorpServer56\Sysvol\cpandl.com\
policies\PolicyDefinitions\
```

Two helpful environment variables when you are working with policy files are %UserDNSDomain% and %LogonServer%. %UserDNSDomain% represents the current log on domain, and %LogonServer% represents the domain controller that authenticated you during logon. Therefore, you could also copy all required policy files by entering the following command at an elevated, administrator command prompt:

```
xcopy /s /y %SystemRoot%\PolicyDefinitions \\%LogonServer%\Sysvol\
%UserDNSDomain%\policies\PolicyDefinitions\
```

As a recommended best practice, you should create the central store on the domain controller that holds the PDC (primary domain controller) Emulator role in the target domain. Why? By default, the PDC emulator is the domain controller that Group Policy relies on when you access GPOs for editing. Therefore, when you create the central store on the PDC emulator, you ensure that anyone who edits Group Policy objects sees the central store immediately rather than having to wait for SYSVOL replication. As part of normal SYSVOL replication, the PDC emulator will then replicate the central store to other domain controllers in the domain.

You can determine which domain controller in your logon domain has the PDC Emulator role by entering the following command at a command prompt:

```
dsquery server –o rdn –hasfsmo pdc
```

The resulting output is the host name of the PDC emulator in your logon domain. If you want the name for the PDC emulator in another domain, you must use the *–Domain* parameter. Consider the following example:

```
dsquery server –o rdn -hasfsmo pdc -domain tech.cpandl.com
```

Here you obtain the host name for the PDC emulator in the tech.cpandl.com domain. If there are multiple domains in the forest, you might also want a list of all the domain controllers that have the PDC emulator role on a per-domain basis. To do this, use the *-Forest* parameter, such as:

```
dsquery server -hasfsmo pdc –forest
```

For more information on why Group Policy relies on the PDC emulator by default, see "Connecting to and Working with GPOs" later in this chapter.

Replication Changes

A key change between earlier implementations of Active Directory and implementations for Windows Server 2008 and later has to do with how policies and related data are replicated. The Active Directory system volume (SYSVOL) contains domain policy; scripts used for log on, log off, shutdown, and startup; other related files; and files stored within Active Directory. While I'll provide an in-depth discussion of the SYSVOL in Chapter 7, "Managing and Maintaining the SYSVOL," let's take a quick look at the way SYSVOL replication works.

The way domain controllers replicate the SYSVOL depends on the domain functional level. When a domain is running at Windows 2000 native or Windows Server 2003 functional level, domain controllers replicate the SYSVOL using File Replication Service (FRS). When a domain is running at Windows Server 2008 functional level, domain controllers replicate the SYSVOL using Distributed File System (DFS).

FRS and DFS are replication services that use the Active Directory replication topology to replicate files and folders in the SYSVOL shared folders on domain controllers. The way this works is that the replication service checks with the Knowledge Consistency Checker (KCC) running on each domain controller to determine the replication topology that has been generated for Active Directory replication. Then the replication service uses this replication topology to replicate SYSVOL files to other domain controllers in the domain.

The storage techniques and replication architectures for DFS and FRS are decidedly different. File Replication Service (Ntfrs.exe) stores FRS topology and schedule information in Active Directory and periodically polls Active Directory to retrieve updated information using Lightweight Directory Access Protocol (LDAP). Internally, FRS makes direct calls to the file system using standard input and output. When communicating with remote servers, FRS uses the remote procedure call (RPC) protocol.

FRS stores configuration data in the registry and also stores various types of data in the NTFS file system. For example, FRS stores transactions in the FRS Jet database (Ntfrs.jdb), events and error messages in the FRS Event log (NtFrs.evt), and debug logs in the debug log folder (%SystemRoot%\Debug). The contents of the Replica tree determines what FRS replicates. The Replica tree for Active Directory is the SYSVOL. The SYSVOL contains domain, staging, and SYSVOL folders.

NTFS uses the update sequence number (USN) journal to track information about added, deleted, and modified files. FRS in turn uses the USN journal to determine when changes are made to the contents of the Replica tree and then replicates those changes according to the schedule in Active Directory.

Distributed File Service (Dfssvc.exe) stores information about stand-alone namespaces in the registry and information about domain-based namespaces in Active Directory. The stand-alone DFS metadata contains information about the configuration of each stand-alone namespace and is maintained in the registry of the root server at HKLM\SOFTWARE\Microsoft\Dfs\Roots\Standalone. Domain-based root servers have a registry entry for each root under HKLM\SOFTWARE\Microsoft\Dfs\Roots\Domain, but these entries do not contain the domain-based DFS metadata.

When the DFS service starts on a domain controller using Active Directory with DFS, DFS checks this path for registry entries that correspond to domain-based roots. If these entries exist, the root server polls the PDC emulator master to obtain the DFS metadata for each domain-based namespace and stores the metadata in memory.

In Active Directory, the DFS object stores the DFS metadata for a domain-based namespace. The DFS object is created in Active Directory when you establish a domain at or promote a domain to the Windows Server 2008 domain functional level. Active Directory replicates the entire DFS object to all domain controllers in a domain.

DFS uses a client-server architecture. A domain controller hosting a DFS namespace has both the client and the server components, allowing the domain controller to perform local lookups in its own data store and remote lookups in data stores on other domain controllers. DFS uses the Common Internet File System (CIFS) for communication between DFS clients, root servers, and domain controllers. CIFS is an extension of the Server Message Block (SMB) file sharing protocol.

It is an easy choice whether to use FRS or DFS. FRS enables interoperability with Windows 2000 Server and Windows Server 2003 but does not support the latest replication enhancements. DFS offers incremental improvements in Active Directory performance and features but is only available when all domain controllers are running Windows Server 2008 and the domain is running in the Windows Server 2008 functional level.

DFS supports the latest replication enhancements, including replication of changes only within files, bandwidth throttling, and improved replication topology. When you make a change to a GPO and FRS is being used, FRS replicates the entire GPO. When you make a change to a GPO and DFS is being used, only the changes in GPOs are replicated, thereby eliminating the need to replicate an entire GPO after a change.

FRS uses an older, less efficient technology for replication, called Rsync. DFS uses Remote Differential Compression (RDC) instead of Rsync to provide replication that

is up to 300 percent faster and compression that is 200 to 300 percent faster. With DFS, operational overhead for managing content and replication is also reduced by approximately 40 percent. Additionally, DFS supports automated recovery from database loss or corruption as well as replication scheduling. Together these features make DFS significantly more scalable than FRS.

Applying and Linking Group Policy Objects

You store Group Policy preferences and settings in Group Policy objects (GPOs). While I'll cover the nitty-gritty details in later chapters, I'll examine the basic concepts related to Group Policy application (initial processing) and refresh (subsequent processing) in this section.

Policy Sets Within GPOs

Within Group Policy, two distinct sets of policies are defined:

- **Computer policies** These apply to computers and are stored under Computer Configuration in a Group Policy object.
- **User policies** These apply to users and are stored under User Configuration in a Group Policy object.

Both Computer Configuration and User Configuration have Policies and Preferences nodes. You use:

- Computer Configuration\Policies to configure policy settings targeted to specific computers.
- Computer Configuration\Preferences to configure policy preferences targeted to specific computers.
- User Configuration\Policies to configure policy settings targeted to specific users.
- User Configuration\Preferences to configure policy preferences targeted to specific users.

Initial processing of the related policies is triggered by two unique events:

- **Processing of computer policies is triggered when a computer is started.** When a computer is started and the network connection is initialized, computer policies are applied.
- **Processing of user policies is triggered when a user logs on to a computer.** When a user logs on to a computer, user policies are applied.

Once applied, policies are automatically refreshed to keep settings current and to reflect any changes that might have been made. By default, Group Policy on domain controllers is refreshed every 5 minutes. For workstations and other types of servers, Group Policy is refreshed every 90 to 120 minutes by default. In addition, most security settings are refreshed every 16 hours regardless of whether any

policy settings have changed in the intervening time. Other factors can affect Group Policy refreshes, including how slow-link detection is defined (per the Group Policy Slow Link Detection Policy under Computer Configuration\Policies\Administrative Templates\System\Group Policy) and policy processing settings for policies under Computer Configuration\Policies\Administrative Templates\System\Group Policy. As discussed in "Determining Policy Settings and Last Refresh" in Chapter 7, you can check the last refresh of Group Policy using the Group Policy Management Console.

GPO Types

As discussed in Chapter 1, there are two types of policy objects: Active Directory–based Group Policy objects (GPOs) and Local Group Policy objects (LGPOs).

Active Directory supports three levels of Group Policy objects:

- **Site GPOs** Group Policy objects applied at the site level to a particular Active Directory site.
- **Domain GPOs** Group Policy objects applied at the domain level to a particular Active Directory domain.
- **Organizational Unit (OU) GPOs** Group Policy objects applied at the OU level to a particular Active Directory OU.

Through inheritance, a GPO applied to a parent container is inherited by a child container. This means that a policy preference or setting applied to a parent object is passed down to a child object. For example, if you apply a policy setting in a domain, the setting is inherited by organizational units within the domain. In this case, the GPO for the domain is the parent object and the GPOs for the organizational units are the child objects.

In an Active Directory environment, the basic order of inheritance goes from the site level to the domain level to the organizational unit level. This means that the Group Policy preferences and settings for a site are passed down to the domains within that site, and the preferences and settings for a domain are passed down to the organizational units within that domain.

> ***TIP*** **As you might expect, you can override inheritance. To do this, you specifically assign a policy preference or setting for a child container that contradicts the policy preference or setting for the parent. As long as overriding the policy is allowed (that is, overriding isn't blocked), the child's policy preference or setting will be applied appropriately. To learn more about overriding and blocking GPOs, see the section "Managing Group Policy Inheritance" in Chapter 7.**

While computers running versions of Windows prior to Windows 2000 have only one LGPO, Windows Vista, Windows Server 2008, and later versions allow the use

of multiple LGPOs on a single computer (as long as the computer is not a domain controller). On compliant computers, there are three layers of LGPOs:

- **Local Group Policy object** The Local Group Policy object is at the top of the policy hierarchy for the local computer. The LGPO is the only local computer policy object that allows both computer configuration and user configuration settings to be applied to all users of the computer.
- **Administrators Local Group Policy object / Non-Administrators Local Group Policy object** Whether the Administrators Local Group Policy object or the Non-Administrators Local Group Policy object applies depends on the account being used. If the account is a member of the local computer's Administrator's group, the Administrators Group Policy object is applied. Otherwise, the Non-Administrators Group Policy object is applied. This object contains only user configuration settings.
- **User-specific Local Group Policy object** A user-specific Local Group Policy object applies only to an individual user or to members of a particular group. This object contains only user configuration settings.

These layers of LGPOs are processed in the following order: Local Group Policy object, Administrators or Non-Administrators Local Group Policy object, and then user-specific Local Group Policy object.

REAL WORLD **When computers are being used in a stand-alone configuration rather than a domain configuration, you may find that multiple LGPOs are useful because you no longer have to explicitly disable or remove settings that interfere with your ability to manage a computer before performing administrator tasks. Instead, you can implement one local policy object for administrators and another local policy object for nonadministrators. In a domain configuration, however, you might not want to use multiple LGPOs. In domains, most computers and users already have multiple Group Policy objects applied to them—adding multiple LGPOs to this already varied mix can make managing Group Policy confusing. Therefore, you might want to disable processing of LGPOs, and you can do this through Group Policy. To disable processing of Local Group Policy objects on computers running Windows Vista or later, you must enable the Turn Off Local Group Policy Objects Processing setting in an Active Directory–based Group Policy object that the computer processes. When you are editing a GPO in the Group Policy Management Editor, this setting is located under Computer Configuration\Policies. Expand Administrative Templates\System\Group Policy, and then double-click the Turn Off Local Group Policy Objects Processing entry.**

Putting this all together when both Active Directory and local policies are in place, policies are applied in the following order:

1. Local GPOs
2. Site GPOs
3. Domain GPOs
4. Organizational unit GPOs
5. Child organizational unit GPOs

Because the available preferences and settings are the same for all policy objects, a preference or setting in one policy object can possibly conflict with a preference or setting in another policy object. Compliant operating systems resolve conflicts by overwriting any previous preference or setting with the last read and most current preference or setting. Therefore, the final preference or setting written is the one that Windows uses. For example, by default, organizational unit policies have precedence over domain policies. As you might expect, there are exceptions to the precedence rule. These exceptions are discussed in the section "Managing Group Policy Inheritance" in Chapter 7.

GPO Links

In Active Directory, each site, domain, or OU can have one or more GPOs associated with it. The association between a GPO and a site, domain, or OU is referred to as a *link*. For example, if a GPO is associated with a domain, the GPO is said to be linked to that domain.

GPOs are stored in a container called Group Policy Objects. This container is replicated to all domain controllers in a domain, so by default all GPOs are also replicated to all domain controllers in a domain. The link (association) between a domain, site, or OU is what makes a GPO active and applicable to that domain, site, or OU.

Linking can be applied in two ways:

- You can link a GPO to a specific site, domain, or OU. For example, if a GPO is linked to a domain, the GPO applies to users and computers in that domain. The main reason for linking a GPO to a specific site, domain, or OU is to keep with the normal rules of inheritance.
- You can link a GPO to multiple levels in Active Directory. For example, a single GPO could be linked to a site, a domain, and multiple OUs. In this case, the GPO applies to each of these levels within Active Directory. The main reason for linking a GPO to multiple levels within Active Directory is to create direct associations between a GPO and multiple sites, domains, and OUs irrespective of how inheritance would normally apply.

You can also unlink a GPO from a site, domain, or OU. This removes the direct association between the GPO and the level within Active Directory from which you've removed the link. For example, if a GPO is linked to a site called First Seattle Site and also to the cpandl.com domain, you can remove the link from the cpandl.com domain, removing the association between the GPO and the domain. The GPO is then linked only to the site. If you later remove the link between the site and the GPO, the GPO is completely unlinked. A GPO that has been unlinked from all levels within Active Directory still exists within the Group Policy Objects container, but it is inactive.

Connecting to and Working with GPOs

When you use the GPMC to work with GPOs, by default the corresponding changes are made on the domain controller that is acting as the PDC emulator. In this way, the PDC emulator is the central point of contact for GPO creation, modification, and deletion. Active Directory manages policy in this way to ensure that changes to the GPO structure can be implemented only on a single authoritative domain controller and that only one administrator at a time is granted access to a particular GPO. Because the PDC emulator role is specified at the domain level, there is only one PDC emulator in a domain, and therefore only one place where policy settings are changed by default. If the PDC emulator is unavailable when you are trying to work with policy settings, you get a prompt that enables you to work with policy settings on the domain controller to which you are connected or on any available domain controller.

Any user who is a member of the Domain Admins or Enterprise Admins group can view and work with Active Directory–based Group Policy. Unlike local Group Policy, GPO creation and linking are separate operations with Active Directory–based Group Policy. First you create a GPO and define a group of policy settings to achieve desired results. Then you apply your GPO and make it "live" by linking it to the container or containers within Active Directory where it will be applied.

Although creating and linking GPOs are two distinct operations, the GPMC does allow you to create GPOs and simultaneously link them to a domain or OU within the directory. This means you have two options for creating and linking GPOs. You can:

- Create a GPO and then later link it to a domain or OU within the directory.
- Create a GPO and simultaneously link it to a domain or OU within the directory.

To link a GPO to a site, the GPO must already exist.

The link is what tells Active Directory to apply the preferences and settings specified in the GPO. For example, you can create a GPO called Main Cpandl.com Domain Policy and then link it to the Domain container for cpandl.com. According to the default (standard) inheritance and policy processing rules, once you link a GPO to a container, the related policy preferences and settings are applied to that container, and lower-level containers within the directory can also inherit the preferences settings. This means a linked GPO can affect every user and computer throughout the enterprise—or some subset of users and computers throughout the enterprise.

Using Default Policies

With Windows 2000 or later, you create a domain by establishing the first domain controller for that domain. This typically means logging on to a stand-alone server as a local administrator, running the Domain Controller Installation Wizard (DCPROMO), and then specifying that you want to establish a new forest or domain.

When you establish the domain and the domain controller, two GPOs are created by default:

- **Default Domain Policy GPO** A GPO created for and linked to the domain within Active Directory. This GPO is used to establish baselines for a selection of policy settings that apply to all users and computers in a domain.
- **Default Domain Controllers Policy GPO** A GPO created for and linked to the Domain Controllers OU that is applicable to all domain controllers in a domain (as long as they aren't moved from this OU). This GPO is used to manage security settings for domain controllers in a domain.

These default GPOs are essential to the proper operation and processing of Group Policy. By default, the Default Domain Controllers Policy GPO has the highest precedence among GPOs linked to the Domain Controllers OU, and the Default Domain Policy GPO has the highest precedence among GPOs linked to the domain. As you'll learn in the sections that follow, the purpose and use of each default GPO is a bit different.

NOTE **The default GPOs are used to establish defaults for a limited subset of policy settings. Neither default GPO is used to establish default preferences.**

Working with the Default Domain Policy GPO

The Default Domain Policy GPO is a complete policy set that includes settings for managing any area of policy, but it isn't meant for general management of Group Policy. As a best practice, you should edit the Default Domain Policy GPO only to manage the default Account policies settings and three specific areas of Account policies:

- **Password policy** Determines default password policies for domain controllers, such as password history and minimum password length settings.
- **Account lockout policy** Determines default account lockout policies for domain controllers, such as account lockout duration and account lockout threshold.
- **Kerberos policy** Determines default Kerberos policies for domain controllers, such as maximum tolerance for computer clock synchronization.

To manage other areas of policy, you should create a new GPO and link it to the domain or an appropriate OU within the domain. That said, several policy settings are exceptions to the rule that the Default Domain Policy GPO (or the highest precedence GPO linked to the domain) is used only to manage Account policies. These policies (located in the Group Policy Management Editor under Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options) are as follows:

- **Accounts: Rename Administrator Account** Renames the built-in Administrator account on all computers throughout the domain, setting a new name for the account so that it is better protected from malicious users.

Note that this policy affects the logon name of the account, not the display name. The display name remains Administrator or whatever you set it to. If an administrator changes the logon name for this account through Active Directory Users And Computers, it automatically reverts to what is specified in this policy setting the next time Group Policy is refreshed.

- **Accounts: Administrator Account Status** Forcibly disables the built-in Administrator account on all computers throughout the domain. If you disable the Administrator account, keep in mind that this account is always available when you boot a computer in safe mode.
- **Accounts: Guest Account Status** Forcibly disables the built-in Guest account on all computers throughout the domain. If you disable the Guest account, keep in mind that network logons will fail if you set the security option Network Access: Sharing And Security Model For Local Accounts to Guest Only.
- **Accounts: Rename Guest Account** Renames the built-in Guest account on all computers throughout the domain, setting a new name for the built-in Guest account so that it is better protected from malicious users. Note that this policy affects the logon name of the account, not the display name. The display name remains Guest or whatever else you set it to. If an administrator changes the logon name for this account through Active Directory Users And Computers, it automatically reverts to what is specified in this policy setting the next time Group Policy is refreshed.
- **Network Security: Force Logoff When Logon Hours Expire** Forces users to log off from the domain when logon hours expire. For example, if you set the logon hours as 8 A.M. to 6 P.M. for the user, the user is forced to log off at 6 P.M.
- **Network Security: Do Not Store LAN Manager Hash Value On Next Password Change** Determines whether at the next password change the LAN Manager hash value for the new password is stored. Because this value is stored locally in the security database, a password could be compromised if the security database was attacked. On Windows Vista and later, this setting is enabled by default. On Windows XP, this setting is disabled by default.
- **Network Access: Allow Anonymous SID/Name Translation** Determines whether an anonymous user can request security identifier (SID) attributes for another user. If this setting is enabled, a malicious user could use the well-known Administrators SID to obtain the real name of the built-in Administrator account, even if the account has been renamed. If this setting is disabled, computers and applications running in pre–Windows 2000 domains may not be able to communicate with Windows Server 2003 domains. This communication issue specifically applies to the following:
  - Windows NT 4.0–based Remote Access Service servers
  - Microsoft SQL Server running on Windows NT 3.x–based or Windows NT 4.0–based computers

- Remote Access Service that is running on Windows 2000–based computers that are located in Windows NT 3.x domains or in Windows NT 4.0 domains
- SQL Server is running on Windows 2000–based computers that are located in Windows NT 3.x domains or in Windows NT 4.0 domains
- Users in Windows NT 4.0 resource domains who want to grant permissions to access files, shared folders, and registry objects to user accounts from account domains that contain Windows Server 2003 domain controllers.

Additionally, certificates stored as policy settings for data recovery agents in the domain are also exceptions. These policies are stored under Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System). You typically manage these policy settings through the GPO that is linked to the domain level and has the highest precedence. As with Account policies, this is the Default Domain Policy GPO by default.

Wondering why configuring policy in this way is a recommended best practice? Well, if Group Policy becomes corrupted and stops working, you can use the Dcgpofix tool to restore the Default Domain Policy GPO to its original state (which would mean that you would lose all the customized settings you've applied to this GPO). Further, some policy settings can only be configured at the domain level, and configuring them in the Default Domain Policy GPO (or the highest precedence GPO linked to the domain) makes the most sense.

NOTE **Bottom line, if you define Account policies in multiple GPOs linked to a domain, the settings will be merged according to the link order of these GPOs. The GPO with a link order of 1 will always have the highest precedence. I discuss link order in "Changing Link Order and Precedence" in Chapter 7. For more information on working with Dcgpofix, see "Recovering the Default GPOs" in Chapter 8 "Maintaining and Restoring Group Policy."**

You can access the Default Domain Policy GPO in several ways. If you are using the GPMC, you'll see the Default Domain Policy GPO when you click the domain name in the console tree, as shown in Figure 2-3. Right-click the Default Domain Policy node and select Edit to get full access to the Default Domain Policy GPO.

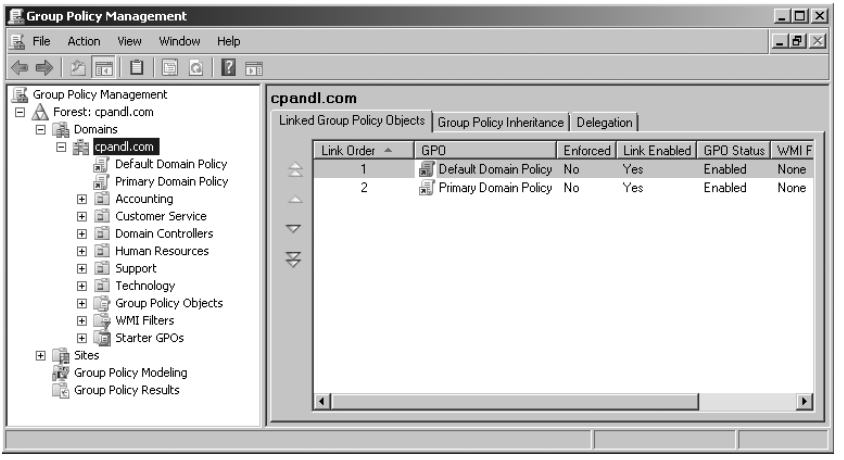

FIGURE 2-3 Accessing the Default Domain Policy GPO in GPMC.

In the Group Policy Management Editor, under Computer Configuration, expand Policies\Windows Settings\Security Settings\Local Policies as shown in Figure 2-4. You can then work with Audit Policy, User Rights Assignment, and Security Options as necessary.

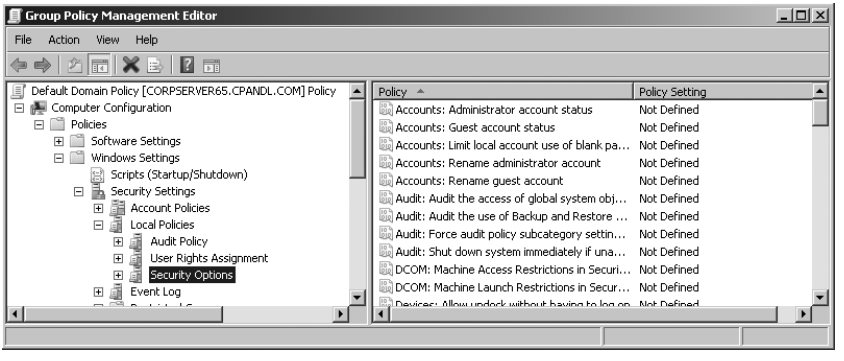

FIGURE 2-4 Editing the Default Domain Policy GPO.

Working with the Default Domain Controllers Policy GPO

The Default Domain Controllers Policy GPO is designed to ensure that all domain controllers in a domain have the same security settings. This is important because all domain controllers in an Active Directory domain are equal. If they were to have different security settings, they might behave differently, and this would be counter to the way Active Directory is designed to work. If one domain controller has a specific policy setting, this policy setting should be applied to all domain controllers to ensure consistent behavior across a domain.

The Default Domain Controllers Policy GPO is linked to the Domain Controllers OU. This ensures that it is applicable to all domain controllers in a domain as long as they aren't moved from this OU. Because all domain controllers are placed in the Domain Controllers OU by default, any security setting changes you make will apply to all domain controllers by default. The key security areas that you should manage consistently include:

- **Audit policy** Determines default auditing policies for domain controllers.
- **User rights assignment** Determines default user rights assignment for domain controllers.
- **Security options** Determines default security options for domain controllers.

Microsoft recommends that you not make any other changes to the Default Domain Controllers Policy GPO. Keep in mind that this GPO applies only to domain controllers because it is linked to the Domain Controllers OU and all domain controllers are members of this OU by default.

Moving a domain controller out of the Domain Controllers OU can adversely affect domain management and can also lead to inconsistent behavior during logon and authentication. Why? When you move a domain controller out of the Domain Controllers OU, the Default Domain Controllers Policy GPO no longer applies unless you've linked this GPO to the destination OU. Further, any GPO linked to the destination OU is applied to the domain controller.

Therefore, if you move a domain controller out of the Domain Controllers OU, you should carefully manage its security settings thereafter. For example, if you make security changes to the Default Domain Controllers Policy GPO, you should ensure that those security changes are applied to domain controllers stored in OUs other than the Domain Controllers OU.

You can access the Default Domain Controllers Policy GPO in several ways. If you are using the GPMC, you'll see the Default Domain Controllers Policy GPO when you click the Domain Controllers node in the console tree. Then right-click the Default Domain Controllers Policy and select Edit to get full access to the Default Domain Controllers Policy GPO.

REAL WORLD **Microsoft product support does not support moving a domain controller out of the Domain Controllers OU. If you've done so and are having problems with your domain controllers that could be related to this action, Microsoft product support will ask you to move the domain controller back to the Domain Controllers OU.**

Other components and products rely on the Default Domain Controllers Policy GPO being present and linked in the domain. For example, Exchange Server may generate error events stating it cannot find a global catalog. Often, this occurs because you do not have the Default Domain Controllers Policy linked to the Domain Controllers OU or because you have moved domain controllers out of the Domain Controllers OU.

Using Policy Preferences and Settings

So far we've discussed how Group Policy has changed, how you can update policy, and how policy is applied, but I haven't discussed the specific ways in which you can use preferences and settings to help you better manage your network. I'll remedy that now by detailing uses for both preferences and settings. Because some overlap occurs in management areas for preferences and settings, I'll also discuss whether using settings or preferences is better suited to a particular task.

Using Policy Settings for Administration

A policy setting is a managed setting that you apply to control configuration, such as to restrict access to the Run dialog box. Most policy settings have three basic states:

- **Enabled** The policy setting is turned on, and its settings are active. You typically enable a policy setting to ensure that it is enforced. Once enabled, some policy settings allow you to configure additional options that fine-tune how the policy setting is applied.
- **Disabled** The policy setting is turned off, and its settings are not applied. Typically, you disable a policy setting to ensure that it is not enforced.
- **Not Configured** The policy setting is not being used. No settings for the policy are either active or inactive and no changes are made to the configuration settings targeted by the policy.

By themselves, these states are fairly straightforward. However, these basic states can be affected by inheritance and blocking (which I touched on briefly and will discuss in detail in Chapter 5, "Searching and Filtering Group Policy"). That said, with the following two rules about inheritance and blocking in mind, you'll be well on your way to success with Group Policy:

- If inherited policy settings are strictly enforced, you cannot override them. This means the inherited policy setting is applied regardless of the policy state set in the current GPO.
- If inherited policy settings are blocked in the current GPO and not strictly enforced, the inherited policy setting is overridden. This means the inherited policy setting does not apply, and only the policy setting from the current GPO is applied.

Now that you know exactly how to apply individual policy settings, let's look at the administrative areas to which you can apply Group Policy. Through a special set of policies called Administrative Templates, you can manage just about every aspect of the Windows graphical user interface (GUI), from menus to the desktop, the taskbar, and more. The Administrative Template policy settings affect actual registry settings, so the available policies are nearly identical whether you are working

with local Group Policy or domain-based Group Policy. You can use administrative templates to manage:

- **Control Panel** Controls access to and the options of Control Panel. You can also configure settings for Add Or Remove Programs, Display, Printers, and Regional And Language Options.
- **Desktop** Configures the Windows desktop, the availability and configuration of Active Desktop, and Active Directory search options from the desktop.
- **Network** Configures networking and network client options, including offline files, DNS clients, and network connections.
- **Printers** Configures printer publishing, browsing, spooling, and directory options.
- **Shared folders** Allows publishing of shared folders and Distributed File System (DFS) roots.
- **Start menu and taskbar** Configures the Start menu and taskbar, primarily by removing or hiding items and options.
- **System** Configures policies related to general system settings, disk quotas, user profiles, logon, power management, system restore, error reporting, and more.
- **Windows components** Configures whether and how to use various Windows components, such as Event Viewer, Task Scheduler, and Windows Updates.

REAL WORLD **You can obtain additional administrative templates for Microsoft Office at the Microsoft Download Center (*http://download.microsoft.com*). At the Download Center, click Home & Office under Download Categories. Search the Home & Office category for "Office customization tool," and then click the link for the most recent release. Next, download and run the self-extracting executable. When prompted, accept the license terms and then click Continue. You will then be able to select a destination folder for the related files. Review the files you've just extracted.**

To use the administrative templates in GPMC on your computer, copy the ADMX files to the %SystemRoot%\PolicyDefinitions folder and the ADML files to the appropriate language-specific subfolder of the PolicyDefinitions folder. Otherwise, to make the administrative templates available throughout the domain, copy the ADMX and ADML files to the appropriate folders within the SYSVOL on a domain controller.

Table 2-1 provides a comprehensive list of administrative areas you can manage using Group Policy. Whether you are working with local Group Policy or Active Directory–based Group Policy, the areas of administration are similar. However, you can do much more with Active Directory–based Group Policy primarily because you cannot use local Group Policy to manage any features that require Active Directory.

TABLE 2-1 Key Administrative Areas That Can Be Managed with Policy Settings

GROUP POLICY CATEGORY	DESCRIPTION	LOCATION IN GROUP POLICY
Device/Drive installation	Controls the way device and driver installation works.	Computer Configuration\Policies\Administrative Templates\System\Device Installation Computer Configuration\Policies\Administrative Templates\System\Drive Installation User Configuration\Policies\Administrative Templates\System\Drive Installation
Device Installation restriction	Restricts the devices that can be deployed and used.	Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions
Disk quotas	Configures the way disk quotas are used and whether quotas are enforced, logged, or both.	Computer Configuration\Policies\Software Settings
Encrypted data recovery agents	Configures data recovery agents and their related certificates for use with the Encrypting File System (EFS).	Computer | User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System
File and folder security	Configures security permissions for files and folders.	Computer Configuration\Policies\Windows Settings\Security Settings\File System
Folder redirection	Moves critical data folders for users to network shares where they can be better managed and backed up regularly (domain-based Group Policy only).	User Configuration\Policies\Windows Settings\Folder Redirection

TABLE 2-1 Key Administrative Areas That Can Be Managed with Policy Settings

GROUP POLICY CATEGORY	DESCRIPTION	LOCATION IN GROUP POLICY
General computer security	Establishes security settings for accounts, event logs, restricted groups, system services, the registry, and file systems. (With local Group Policy, you can only manage general computer security for account policies.)	Computer Configuration\Policies\Windows Settings\Security Settings
Internet settings	Controls the ways Windows Internet Explorer can be used and establishes lockdown settings.	Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer
Internet Explorer maintenance	Configures the browser interface, security, important URLs, default programs, proxies, and more.	User Configuration\Policies\Windows Settings\Internet Explorer Maintenance
IP security	Configures IP security policy for clients, servers, and secure servers.	Computer Configuration\Policies\Windows Settings\Security Settings\IP Security Policies
Local security policies	Configures policy for auditing, user rights assignment, and user privileges.	Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies
Offline files	Determines whether and how offline files are used.	Computer | User Configuration\Policies\Administrative Templates\Network\Offline Files
Policy-based Quality of Service (QoS)	Manages network traffic to help improve quality of service for critical applications.	Computer | User Configuration\Policies\Windows Settings\Policy-based QoS
Power options	Configure power management plans and settings for devices. (Windows Vista or later)	Computer | User Configuration\Policies\Administrative Templates\System\Power Management
Printer deployment	Configures printers for use. (Windows Vista or later)	User Configuration\Policies\Windows Settings\Deployed Printers

TABLE 2-1 Key Administrative Areas That Can Be Managed with Policy Settings

GROUP POLICY CATEGORY	DESCRIPTION	LOCATION IN GROUP POLICY
Public key security	Configures public key policies for autoenrollment, EFS, enterprise trusts, and more.	Computer | User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies
Registry security	Configures security permissions for registry keys.	Computer Configuration\Policies\Windows Settings\Security Settings\Registry
Restricted groups	Controls the membership of both Active Directory–based groups and local computer groups.	Computer | User Configuration\Policies\Windows Settings\Security Settings\Restricted Groups
Scripts	Configures logon/logoff scripts for users and startup/shutdown scripts for computers.	Computer | User Configuration\Policies\Windows Settings\Security Settings\Scripts
Software installation	Configures automated deployment of new software and software upgrades (domain-based Group Policy only).	Computer | User Configuration\Policies\Software Settings\Software Installation
Software restriction	Restricts the software that can be deployed and used. Local Group Policy does not support user-based software restriction policies, only computer-based software restriction policies.	Computer | User Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies
Start menu	Defines the available options on and the behavior of the Start menu.	User Configuration\Policies\Administrative Templates\Start Menu And Taskbar
System services	Configures startup state and security permissions for system services.	Computer Configuration\Policies\Windows Settings\Security Settings\System Services

TABLE 2-1 Key Administrative Areas That Can Be Managed with Policy Settings

GROUP POLICY CATEGORY	DESCRIPTION	LOCATION IN GROUP POLICY
Wired networking (IEEE 802.3)	Configures wired network policies for authentication methods and modes that apply to wired clients (domain-based Group Policy only). Can also be used to validate server certificates, enable quarantine checks, enforce advanced 802.1X settings, and enable single sign on.	Computer Configuration\Policies\Windows Settings\Security Settings\Wired Network Policies
Wireless networking (IEEE 802.11)	Configures wireless network policies for access points, wireless clients, and preferred networks (domain-based Group Policy only). Can also be used to define permitted types of connections and block disallowed types of connections.	Computer Configuration\Policies\Windows Settings\Security Settings\Wireless Network Policies

Using Policy Preference for Administration

A policy preference is an unmanaged setting that you apply to preconfigure an option for a user, such as to map a network share to a drive. Most policy preferences can be established using one of four different actions:

- **Create** Creates the preference only if a preference does not already exist.
- **Replace** Deletes the preference if it exists and then creates it, or creates the preference if it doesn't yet exist.
- **Update** Modifies the preference if it exists. Otherwise, creates the preference.
- **Delete** Deletes the preference if it exists.

As with states for policy settings, these actions are fairly straightforward. However, these basic actions also can be affected by inheritance and blocking. To help you navigate inheritance and blocking, keep these basic rules in mind:

- If inherited policy preferences are strictly enforced, you cannot override them. This means the inherited policy preference is applied regardless of the action defined in the current GPO.
- If inherited policy preferences are blocked in the current GPO and not strictly enforced, the inherited policy preference is overridden. This means the

inherited policy preference does not apply, and only the policy preference from the current GPO is applied.

Unlike policy settings, policy preferences apply only to Active Directory–based Group Policy. When you are working with Active Directory–based Group Policy, you can use policy preferences to configure the items discussed in Table 2-2.

TABLE 2-2 Key Elements That Can Be Configured with Policy Preferences

CONFIGURATION AREA	CENTRALIZES CREATION, REPLACEMENT, UPDATING, AND DELETION OF	LOCATION IN GROUP POLICY
Applications	Application settings. Available when you install preference settings for an application.	User Configuration\Preferences\Windows Settings\Applications
Data Sources	Open Database Connectivity (ODBC) data sources	Computer | User Configuration\Preferences\Control Panel Settings\Data Sources
Devices	System devices, including USB ports, floppy drives, and removable media	Computer | User Configuration\Preferences\Control Panel Settings\Devices
Drive Maps	Network shares mapped to drive letters.	User Configuration\Preferences\Windows Settings\Drive Maps
Environment	System and user environment variables	Computer | User Configuration\Preferences\Windows Settings\Environment
Files	Files that can be copied from a source location to a destination location.	Computer | User Configuration\Preferences\Windows Settings\Files
Ini Files	Property values within .ini files.	Computer | User Configuration\Preferences\Windows Settings\Ini Files
Folders	Folders in a particular location on the file system.	Computer | User Configuration\Preferences\Windows Settings\Folders
Local Users And Groups	User and group accounts for the local computer.	Computer | User Configuration\Preferences\Control Panel Settings\Local Users And Groups

TABLE 2-2 Key Elements That Can Be Configured with Policy Preferences

CONFIGURATION AREA	CENTRALIZES CREATION, REPLACEMENT, UPDATING, AND DELETION OF	LOCATION IN GROUP POLICY
Network Options	Virtual Private Networking and Dial-up Networking connections	Computer | User Configuration\ Preferences\Control Panel Settings\ Network Options
Network shares	Shares, hidden shares, and administrative shares.	Computer or User Configuration\ Preferences\Windows Settings\
Printers	Printer configuration and mapping	Computer | User Configuration\ Preferences\Control Panel Settings\ Printers
Registry	Registry keys and values.	Computer | User Configuration\ Preferences\Windows Settings\ Registry
Scheduled Tasks	Scheduled tasks for automation	Computer | User Configuration\ Preferences\Control Panel Settings\ Scheduled Tasks
Services	System services	Computer Configuration\ Preferences\Control Panel Settings\ Services
Shortcuts	Shortcuts for file system objects, URLs, or shell objects.	Computer | User Configuration\ Preferences\Windows Settings\ Shortcuts

Through special preferences for Control Panel, you can also manage various aspects of the Windows graphical user interface (GUI). You can use these special preferences to manage:

- Folder settings as if you were using the options available in the Folder Options utility in Control Panel. Located in Computer | User Configuration\ Preferences\Control Panel Settings\Folder Options.
- Internet settings as if you are using the options available in the Internet Options utility in Control Panel. Located in User Configuration\Preferences\ Control Panel Settings\Internet Settings.
- Power schemes and power management options as if you were using the related utilities in Control Panel. Located in Computer | User Configuration\ Preferences\Control Panel Settings\Power Options. (Windows XP only.)
- Regional and language settings as if you were using the options available in the Regional And Languages utility in Control Panel. Located in User Configuration\Preferences\Control Panel Settings\Regional Options.

- Start menu as if you were using the Start Menu Properties dialog box. Located in User Configuration\Preferences\Control Panel Settings\Start Menu.

Choosing Between Preferences and Settings

Because some management areas overlap between policy preferences and policy settings, you can sometimes perform a particular task in more than one way. For example, using policy settings, you can identify logon scripts that should be used. Within these scripts, you can map network drives, configure printers, create shortcuts, copy files and folders, and perform other tasks. Using policy preferences however, you could perform these same tasks without the need of using logon scripts. So which one should you use? Well, the truth is that there really isn't one right answer. It depends on what you want to do. In the following sections, I describe some general guidelines for specific areas of overlap.

REAL WORLD **When a conflict occurs between a policy setting and a policy preference defined in a particular GPO, a registry-based policy setting will normally win. For conflicts between non-registry-based policy settings and preferences, the last value written wins (as determined by the order in which the client-side extensions for policy settings and preferences are processed). Determining whether a policy setting is registry-based or not is easy. All registry-based policy settings are defined in administrative templates.**

Controlling Device Installation

Through policy settings, you can control device installation and enforce specific restrictions. The goal is to prevent users from installing specific types of hardware devices. You can specify that certain approved devices can be installed (according to the hardware ID of the device). You can also prevent installation of specific disapproved devices (again according to the hardware ID of the device). These policy settings only apply to Windows Vista or later and are found under Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions.

While restrictions block the installation of a new device or prevent a device from being plugged back in after it has been unplugged, it doesn't prevent existing devices from being used. Why? The device drivers are already installed and the devices are already available, and because the device or drive isn't rechecked, it continues to work.

Using policy preferences, you can disable device classes, individual devices, port classes, and individual ports, but you cannot prevent a driver from loading. You disable devices by selecting a device class or device already installed on your management computer. You disable ports by selecting a port class or specific port already in use on your management computer. The related preferences are found under Computer | User Configuration\Preferences\Control Panel Settings\Devices.

While you can disable devices and ports using preferences, this doesn't prevent device drivers from installing. It also doesn't prevent a user with appropriate rights from enabling ports or devices in Device Manager. However, as Group Policy by default refreshes policy preferences using the same refresh interval as for policy settings, the preference would be reapplied during the next refresh interval. Therefore, unless you specifically elect to apply the preference once and not reapply it, the preference would be reapplied every 90 to 120 minutes.

Given how these technologies work, the best solution for your environment may depend on your goal. If you want to completely lock things down and prevent specific devices from being installed and used, you may want to use both policy settings and policy preferences to do the job. Policy settings could prevent specific devices from being installed, providing they weren't already installed. Policy preferences could disable devices already installed, providing that you've already installed the device on your management computer so it can be selected.

As a final thought, it is important to point out that the related policy settings apply only to Windows Vista or later, while the related policy preferences apply to any computer on which the client-side extensions for Group Policy Preferences are installed.

Controlling Files and Folders

Through policy settings, you can specify security permissions for files and folders. The goal is to establish specific access control lists (ACLs) for important files and folders. However, the files and folders must already exist on the target computers so that the ACLs can be applied. These policy settings apply to any computer that supports Group Policy and are found under Computer Configuration\Policies\Windows Settings\Security Settings\File System.

Using policy preferences, you can manage files and folders. Preferences for files work differently than preferences for folders. With files, you can create, update, or replace a file on a target computer by copying it from a source computer. You can also delete a file on a target computer. With folders, you can create, update, replace, or delete a folder in a specific location on a target computer. You can also specify whether to delete existing files and subfolders during the create, update, replace, or delete operation.

File and folder preferences apply to any computer on which the client-side extensions for Group Policy Preferences are installed. For files, the related preferences are found under Computer | User Configuration\Preferences\Windows Settings\Files. For folders, the related preferences are found under Computer | User Configuration\Preferences\Windows Settings\Folders.

TIP **Group Policy also provides preferences for working with .ini files and shortcuts. Preferences for .ini files are limited to modifying values for designated properties within a specific section of the .ini file. Shortcut preferences are used to create shortcuts to files, folders, URLs, and shell objects in a specific location, such as the desktop.**

Here, using policy settings and preferences together gives you the best of both worlds. Through preferences you have an easy way to copy files from a source computer to target computers and to manage folders. Through settings you have an easy way to apply desired security settings. Additionally, with files and folders, you might want to apply preferences only once and not reapply them. Otherwise, the create, update, replace, or delete operations will be reapplied during Group Policy refresh.

Controlling Internet Explorer

Group Policy offers a wide array of settings and preferences for Internet Explorer. There are so many options that even a few experts are confused as to what does what. The key things to focus on are the following:

- Policy settings under Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer are primarily meant to control Internet Explorer behavior. These settings configure browser security enhancements and help to lockdown Internet security zones.
- Policy settings under User Configuration\Policies\Windows Settings\Internet Explorer Maintenance are used to specify important URLs, such as those for home pages, search, support, favorites, and links. These settings are also used to customize the browser interface by adding custom logos, titles, and buttons to Internet Explorer and to establish default programs, proxies, and more.
- Preference settings under User Configuration\Preferences\Control Panel Settings\Internet Settings allow you to configure any of the options available in the Internet Options utility in Control Panel (which essentially includes every user-configurable option).

Because policy settings are managed and policy preferences are unmanaged, you can use policy settings when you want to enforce specific settings for Internet Explorer. Although you can configure Internet Explorer with preferences, the preferences are not enforced and users can change settings. That said, if you apply the preferences so that they are refreshed automatically as part of normal Group Policy refreshes, settings users change may be overwritten by your preferences.

When you want to customize the interface, the settings under Internet Explorer Maintenance are the ones you'll use. These settings allow you to configure home page URLs, search URLs, support URLs, favorites, and links. They also allow you to add custom logos, titles, and buttons.

Controlling Power Options

When you want to control power management settings, the choice between policy settings and policy preferences is easy. You use policy settings for Windows Vista or later and policy preferences for Windows XP.

Policy settings for Windows Vista or later are found under Computer | User Configuration\Policies\Administrative Templates\System\Power Management.

Policy preferences for Windows XP are located in Computer | User Configuration\Preferences\Control Panel Settings\Power Options.

Controlling Printers

With policy settings, you can deploy printers to computers running any version of Windows that supports Group Policy. This technology establishes a connection to an existing shared printer.

To deploy printers to computers running Windows Vista or later, you can use policy settings under User Configuration\Policies\Windows Settings\Deployed Printers. To deploy printers to computers running earlier versions of Windows, you can push a printer connection to the computer using PushPrinterConnection.exe as a logon or startup script.

With policy preferences, you can map and configure printers. These preferences include options for configuring local printers as well as for mapping both TCP/IP and shared network printers. These policy preferences apply to any computer on which the client-side extensions for Group Policy Preferences are installed.

As printer preferences are much more versatile than printer settings, you'll probably want to use preferences to deploy printers. That said, if you've already configured printers to be deployed using policy settings, you don't need to switch to policy preferences and redeploy the printers.

Controlling Registry Keys and Values

Through policy settings, you can specify security permissions for registry keys. The goal is to establish specific access control lists (ACLs) for important registry keys. However, the registry keys must already exist on the target computers so that the ACLs can be applied. These policy settings apply to any computer that supports Group Policy and are found under Computer Configuration\Policies\Windows Settings\Security Settings\Registry.

Using policy preferences, you can create, update, replace, or delete registry keys. The related preferences are found under Computer | User Configuration\Preferences\Windows Settings\Registry. Although you can modify just about any registry key, it is contradictory to widely manage registry values through preferences. Why? Policy settings defined within the administrative templates set registry values for you so that you don't have to modify the registry directly. You can install additional administrative templates to manage the registry settings of other applications. If administrative templates aren't available for a particular application, you can create your own custom administrative template to manage the registry settings for the application.

Because of the conflicting goals, I recommend using policy preferences to manage individual registry keys and only in a limited number of situations. When you need to work with multiple or many registry keys, you should use preexisting administrative templates or consider creating your own custom administrative templates. Additionally, with registry keys, you might want to apply preferences only once and not reapply them. Otherwise, the create, update, replace, or delete operation will be reapplied during Group Policy refresh.

Controlling the Start Menu

When it comes to the Start menu, there is a lot of overlap between what you can configure with policy settings and what you can configure with policy preferences. With this in mind, you use policy settings and policy preferences to work with the Start menu in very different ways.

Through policy settings, you can control the options available on the Start menu and define the behavior of various Start menu options. With over 70 settings to choose from under User Configuration\Policies\Administrative Templates\Start Menu And Taskbar, there are many possibilities. You can specify that you want to clear the history of recently opened documents when a user logs off or that drag and drop is disabled on the Start menu. You can lock the taskbar, remove system tray icons, and turn off notifications.

Policy preferences for working with the Start menu are located in User Configuration\Preferences\Control Panel Settings\Start Menu. With policy preferences, you manage the options and behavior of the Start menu as if you were using the Start Menu Properties dialog box. You can configure both the standard Start menu and the classic Start menu. There are, however, no options for configuring the taskbar.

Controlling System Services

When you want to control system services, the choice between policy settings and policy preferences is easy. You can use policy settings to:

- Configure the service startup mode
- Specify the access permissions for services (which control who can start, stop, and pause the service)

Policy settings for services are locatd under Computer Configuration\Policies\Windows Settings\Security Settings\System Services.

You can use policy preferences to:

- Configure the service startup mode
- Configure a service action that can be used to start a stopped service, stop a started service, or stop and restart a service
- Specify the account under which the service runs and set the password for this account
- Specify recovery actions that determine how the service responds to failure

Policy preferences for services are located under Computer Configuration\Preferences\Control Panel Settings\Services.

Because policy settings are managed and policy preferences are unmanaged, you can use policy settings when you want to enforce specific startup modes and access permissions. Although you can configure services with preferences, the preferences are not enforced and users can change settings. If you apply the preferences so that they are refreshed, settings users change may be overwritten by your preferences.

Controlling Users and Groups

When you want to control users and groups, the choice between policy settings and policy preferences is easy. You use policy settings when you want to restrict the membership of either a group defined in Active Directory or a group on the local computer. You do this by specifying the members of the group and the groups of which the group is a member. The related policy settings are found in Computer | User Configuration\Policies\Windows Settings\Security Settings\Restricted Groups.

You use policy preferences to create, replace, update, or delete users and groups on the local computer. With local user accounts, you can also:

- Rename existing user accounts
- Set user account passwords
- Set status flags for user accounts

Status flags can be used to require users to change passwords at next log on, disable the account, or set an expiration date.

With local groups, you can also:

- Rename existing groups
- Add or remove the current user as a member
- Delete member users, member groups, or both

Policy preferences for local users and groups are located under Computer | User Configuration\Preferences\Control Panel Settings\Local Users And Groups.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

About the Author

William R. Stanek (*http://www.williamstanek.com/*) was born in Burlington, Wisconsin, where he attended public schools, including Janes Elementary School in Racine, Wisconsin. He is the second youngest of five children. After a career in the military, he settled in Washington State, having been captivated by the rugged beauty of the Pacific Northwest.

In 1985 he enlisted in the U.S. Air Force and entered a two-year training program in intelligence and linguistics at the Defense Language Institute. After graduation he served in various field operations duties in Asia and Europe. In 1990 he won an appointment to Air Combat School and shortly after graduation served in the Persian Gulf War as a combat crewmember on an electronic warfare aircraft. During his two tours in the Persian Gulf War, William flew numerous combat and combat support missions, logging over 200 combat flight hours. His distinguished accomplishments during the war earned him nine medals, including the United States of America's highest flying honor, the Air Force Distinguished Flying Cross, as well as the Air Medal, the Air Force Commendation Medal, and the Humanitarian Service Medal. He earned 29 decorations in his military career.

In 1994 William earned his bachelor's degree magna cum laude from Hawaii Pacific University. In 1995 he earned his master's degree with distinction from Hawaii Pacific University. In 1996 he separated from the military, having spent 11 years in the U.S. Air Force. While in the military, he was stationed in Texas, Japan, Germany, and Hawaii. He served in support of Operation Desert Storm, Operation Desert Shield, and Operation Provide Comfort. His last station while in the Air Force was with the 324th Intelligence Squadron, Wheeler Army Airfield, Hawaii.

Born into a family of readers, William was always reading and creating stories. Even before he started school, he read classics like *Treasure Island, The Swiss Family Robinson, Kidnapped, Robinson Crusoe,* and *The Three Musketeers*. Later in his childhood, he started reading works by Jules Verne, Sir Arthur Conan Doyle, Edgar Rice Burroughs, Ray Bradbury, Herman Melville, Jack London, Charles Dickens, and Edgar Allan Poe. Of that he says, "Edgar Allan Poe can be pretty bleak and dark, especially when you're 10 years old. But I remember being fascinated with his stories. To this day I can still remember parts of 'The Raven,' *The Tell Tale Heart,* and *The Murders in the Rue Morgue*."

William completed his first novel in 1986 when he was stationed in Japan, but it wasn't until nearly a decade later that his first book was published. Since then, he has written and had published nearly 100 books, including *Active Directory Administrator's Pocket Consultant, Windows Server 2008 Administrator's Pocket Consultant, SQL Server 2008 Administrator's Pocket Consultant,* and *Windows Server 2008 Inside Out* (all from Microsoft Press).

In 1997 William was dubbed "A Face Behind the Future" in a feature article about his life in *The* (Wash.) *Olympian.* At that time he was breaking new ground in shaping the future of business on the Internet. Today William continues to help shape the future of Internet business and technology in general, writing authoritative books covering these subjects for a variety of publishers. William has won many awards from his colleagues and the publishing industry.

For fun he used to spend a lot of time mountain biking and hiking, but now his adventures in the great outdoors are mostly restricted to short treks around the Pacific Northwest. In 2009, William's one-hundredth book will be published by Microsoft. William's life-long commitment to the printed word has helped him become one of the leading technology authors in the world today.