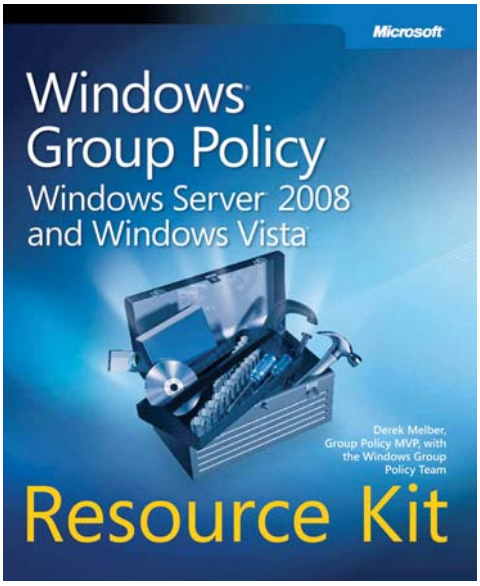

Windows® Group Policy Resource Kit: Windows Server® 2008 and Windows Vista®

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

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/9556.aspx

Microsoft® Press

978-0-7356-2514-3

Table of Contents

Part I Introducing Group Policy

1 Introduction to Group Policy

2 What's New in Windows Vista and Windows Server 2008 Group Policy

3 Group Policy Basics

Part II Group Policy Structure

4 Architecture of Group Policy

5 Group Policy Processing

Part III Administering Group Policy

6 Using the GPMC

7 More on Using the GPMC

8 Controlling GPOs via Scripts and Automation

Part IV Implementing Security

9 Security Delegation for Administration of GPOs

Part V Using Registry-Based Policy Settings

10 ADM, ADMX, and Repository

11 Customizing ADMs and ADMX

12 PolicyMaker Technology

13 Settings Breakdown for Windows Server 2008 and Vista

Part VI Advance Topics

14 Advanced GPO Management with AGPM

15 Troubleshooting GPOs

Part VII Appendices

A Third-Party Tools

B Additional Resources

Part I

Introducing Group Policy

Chapter 1
Why Group Policy?

With regard to many technologies from Microsoft and other software development companies, the question of "Why?" is many times hard to answer. When it comes to Active Directory and Group Policy, the answers are simple, easy to come by, and plentiful. If you are new to Group Policy or just want to learn more about how Group Policy can make managing an Active Directory enterprise more efficient and cost effective, you have certainly started in the right place. This chapter will take a quick, yet comprehensive view of where Group Policy has come from, where it is today, and where it is headed in the future. You will quickly gain an appreciation for what Group Policy can do for you, as well as how easy Group Policy can be to implement and maintain. From this lineage of Group Policy are many benefits of using the technology. Here, you will be shown the many different benefits that Group Policy can provide for you and your company, as it has for so many companies already.

The Past, Present, and Future of Group Policy

If you have been using Microsoft Windows for a long time, you most likely remember the good ol' days when the concepts of "Policy" first started. There have always been forms of management technology built into the enterprise level of the Microsoft network operating systems. Going all the way back to Windows NT 3x, you have had some form of management technology that you could use to control certain aspects of the network. These management technologies allowed you to control user password parameters, desktop settings, Registry settings, and more. Over time, the technologies placed in the different network operating systems have grown up. If you have not seen the latest version of the management technologies that Group Policy provides in Windows Server 2003 and Windows Server 2008, you are in for a real treat.

Group Policy's Past

Instead of going through the entire past of Group Policy and its' ancestors, it will be beneficial to look at the technology and features that Group Policy ancestors had. The benefits of looking at the past technologies that grew into Group Policy is to realize where policy management used to be, as well as realize some of the limitations of earlier policy management technologies.

To start the history lesson, you will begin at Windows NT with System Policies. System Policies were powerful during their time, but certainly there were limitations and issues. Like any new technology and feature set, System Policies looked like the "Good, Bad, and the Ugly." All-in-all, the good floated to the top and these features were the predecessors to what you know today as Group Policy.

So, what technologies and features grew from these System Policies? If you were asked to define a System Policy in a short phrase, what would you answer? You should have answered "a Registry modification." This is exactly what a System Policy was: a "fancy" and "centralized" mechanism to make Registry value changes and settings.

System Policies were based on files called ADM templates. These ADM templates had a file extension of ADM, which is where they got their name. The ADM template contents had a very easy and unique format and coding language. The structure was important because the contents of the ADM template performed the following two distinct functions:

- Create policy settings in the System Policy Editor.
- Establish the Registry path, value, and data.

The ADM template was not "active" in that it performed some action when the System Policy Editor was opened. Rather, the System Policy Editor would decrypt the coding that was in the ADM template to create the folders and policy settings that showed up in the interface. A simple change to the ADM template would result in an immediate change to the System Policy Editor next time it was opened and it read the changes in the ADM template.

The ADM templates were simple, mobile, and stable. There were, however, issues that came along with such a simple technology. These issues were not so horrific that it forced administrators to use other technologies. The issues just caused some glitches to the way that administrators could use and implement Registry changes using ADM templates. The major issues regarding ADM templates included:

- Persistence of Registry values. This was an issue referred to as "tattooing."
- Inability to control multi-value entries in the Registry.
- Inability to control binary value entries in the Registry.
- No easy way to develop custom ADM templates, although this was possible and done often.
- Version control of the ADM templates had to be managed manually. This included issues around having several administrators making modifications to System Policies, as well as any custom or updated ADM templates that needed to be managed and implemented on the network.

How It Works: Tattooing

To get a feel for how tattooing works, you need to look at a real world case of a System Policy setting from inception to completion. For this example, look at a System Policy that modifies the screen saver for a user account. Initially, the settings would be in a policy that targets a user account because this is a setting configured in the HKEY_Current_User portion of the Registry. (You will see more about policy settings and the Registry later in this book.)

When the user logs off and then logs on again, the new Registry data for the screen saver is set automatically. If the user were to configure the screen saver settings, the new screen saver file would be configured already.

Assume now that the administrator no longer wants the screen saver to be established using System Policy. The administrator goes into the System Policy and removes the setting for the screen saver. When the user logs off and then logs on, the screen saver settings established from the recent System Policy remain, even though the new System Policy did not establish a setting for the screen saver.

This behavior is referred to as *tattooing* because the setting tattoos itself in the Registry. The only way to alter a tattooed setting from System Policy would be one of the following:

- Create an alternate setting using System Policy that changes the Registry entry at next reboot or logoff and logon.
- Manually modify the Registry using a tool like RegEdit.exe or RegEdt32.exe.

Although there were so many issues associated with ADM templates in System Policies, they were used very often and relied upon to ensure that Registry settings were configured properly. Group Policy's Present

When talking about Group Policy in the present tense, you should be thinking about Windows 2000 Server and beyond. The the majority of the technology and features are built on the same foundation; it is just tidbits of features that have been added. Regardless, it is important to understand how Group Policy changed from System Policy to become the powerhouse that it is today.

At first glance, it is easy to see that Group Policy is much more than the ancestor of System Policy. Sure, Group Policy still contains some remnants of ADM templates and Registry alterations, but the overall makeup and structure has changed radically. You should be fully aware of what Group Policy does provide, as well as what it does not provide. Here are some guidelines and bullet points that give you that quick view.

Group Policy Requires Active Directory

It is not any secret that Group Policy requires Active Directory to be a full-fledged powerhouse of a management solution. Yes, it is true that you can have local GPOs that control the single computer, but this is really not a book for home use or small business use. For the enterprise, Group Policy relies on Active Directory's structure to help distribute the settings stored in Group Policy objects (GPOs) to the correct users and groups. This task is accomplished by intertwining Group Policy technology with the Active Directory design structure. In essence, GPOs are linked to the domain, organizational units (OUs), and Active Directory sites. Because user and computer objects are stored in these containers, it is logical that the objects in a container where a GPO is linked will receive those settings, by default of course!

Group Policy Includes Security Settings

A distinct area of interest to the entire computing world, especially that of Microsoft, is security. When Group Policy first hit the scene, it was key that an entire section within the GPO settings was dedicated to security. Throughout the lifecycle of the current Group

Policy ancestory, these security settings have grown, as well as grown up. Figure 1-1 illustrates the plethora of security settings that exist in a standard GPO.

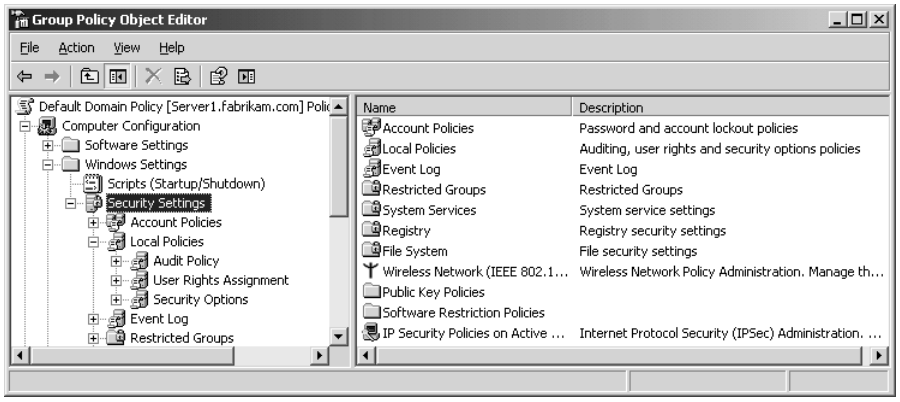

Figure 1-1 The security section of a Group Policy object has numerous settings that are all targetting security of the computer it is configuring.

These security settings have grown in numbers, as well as detail. For example, if you look at the Anonymous controls from first generation Group Policy through today, you will see a dramatic difference in the level of detail that can be configured. Figure 1-2 shows what the original version of a Group Policy object included with regard to Anonymous controls.

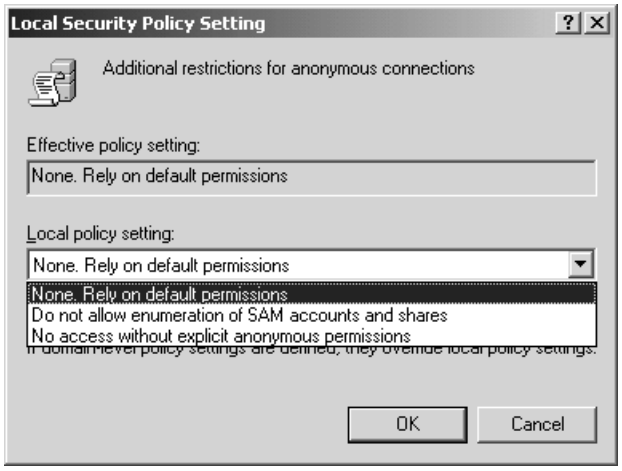

Figure 1-2 Windows 2000 Group Policy object controls for anonymous connections were limited.

Windows XP introduced the first "updated" security settings related to the Anonymous controls. These controls were a radical new approach to the security implications that an anonymous connection could expose to a Windows computer. Now, in the newer Group Policy objects for the latest operating systems, you can get very granular with your anonymous controls, as shown in Figure 1-3.

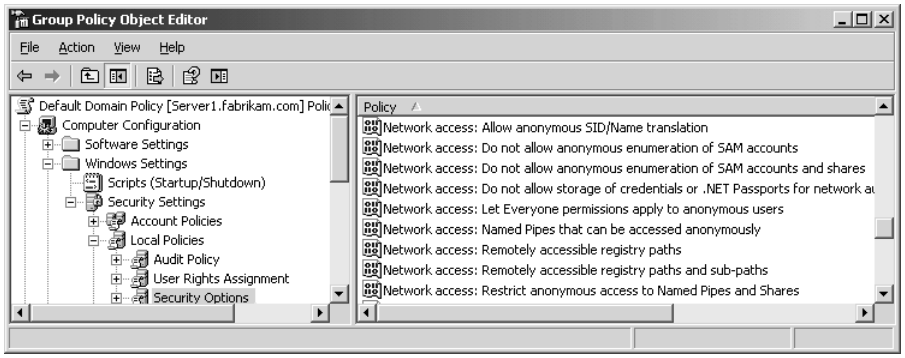

Figure 1-3 Updated list of anonymous controls in a Group Policy object.

This illustrates just some of the security settings that are available using Group Policy. Other settings allow control over passwords, group membership, Internet Explorer, firewall, and more. For more information about these other settings, see Chapter 12, "Settings breakdown for Windows Server 2008 and Vista."

How It Works: Anonymous Connections

Anonymous connections can be made to any Windows computer if the correct security settings are not in place. These connections can be made from any computer that is on the network; it does not need to be a computer that has been joined to the domain. With the parameters in place, all that is left is the command that needs to be run to establish the anonymous connection. From any command prompt, type:

```
Net use \\<computer name or IP address>\ipc$ /u:"" ""
```

This establishes an anonymous connection to the computer that is exposed,as shown in Figure 1-4.

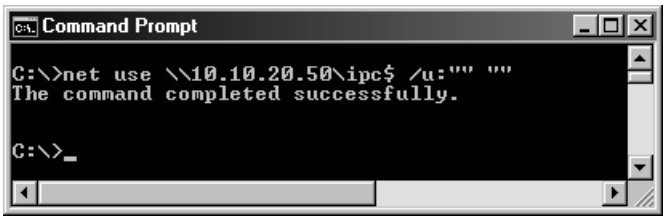

Figure 1-4 Anonymous connection made to a computer that does not have security established properly.

Once the computer is protected to not allow anonymous connections, the attempt to make the anonymous connection shown in Figure 1-4 is no longer valid. Figure 1-5 shows the result when you attempt anonymous access to a protected computer.

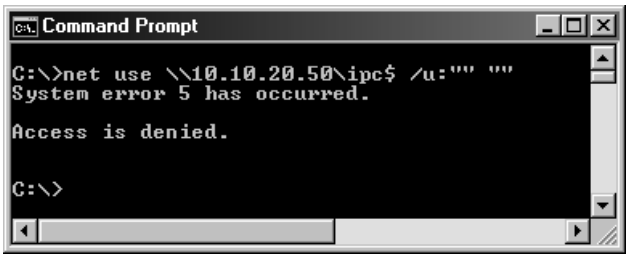

Figure 1-5 Anonymous connection made to a computer that does not allow anonymous connections.

It should be noted that Windows XP, Windows Server 2003, Vista, and Windows Server 2008 will not function in this manner. Because there are so many granular settings for anonymous connections, a connection will succeed, but the ability to access resources is limited by the settings that are made in the Group Policy.

Group Policy Includes Software Distribution

Another area that Group Policy grew up into is software distribution. With the ability to distribute software using Group Policy and Active Directory, you could take a lot of the complexity out of other tools such as System Management Server (SMS) and System Center Configuration Manager. When the software distribution feature of Group Policy was developed, it was important that MSI packages could be distributed using the technology. This made Group Policy a valid alternative to other technologies that managed the installation of software.

There were, however, some limitations of software distribution using Group Policy that made the more robust solutions, such as SMS and System Center, more attractive and viable. Group Policy software distribution was limiting to those companies and administrators that needed validation that the software installed successfully. Not only did the validation check point create a limitation, but the ability to do reporting to show where software was installed was also not in Group Policy. These limitations were not ommisions from Group Policy; they were left out because these other Microsoft solutions provided those services. In essence, Group Policy is designed to work for software distribution for smaller companies and for software that does not require validation or license reporting. If you need these features, you can get the enterprise solutions of SMS and System Center.

Group Policy Helps Eliminate Tattooing

One of the most heralded features of Group Policy is an approach that fixes some issues around tattooing. Thes concept that Registry settings would persist, even after the GPO was deleted, became an ongoing issue. As software, operating systems, system settings, and other aspects of the computer and user environment needed to be dynamic, tattooing needed to be "fixed."

Group Policy takes a whole new approach toward tattooing by creating special areas in the Registry that are volatile. These volatile areas of the Registry are wiped clean and rebuilt during policy refresh, so that tattooing is not an issue. Administrators can now use Group Policy to establish Registry values that are more suited to how desktop and server administration was initially intended.

However, earlier versions of Group Policy did leave some aspects of Registry management in a state of tattooing. These areas that still tattooed included the security settings and any custom Registry settings exposed through custom ADM templates. In the most recent addition of policy settings that are in Windows Server 2008, there are now Registry policy options that eliminate the entire landscape of tattooing.

The new settings that are available with Windows Server 2008 PolicyMaker technology allow you to configure virtually any Registry value (even those that were previously tabo, like multi-value and binary) setting. Not only can you make the policy set these Registry values, but you can make the entry non-persistent. This means that when the policy is no longer in place, the Registry value that you put in with the GPO will be removed, as can be seen here in Figure 1-6.

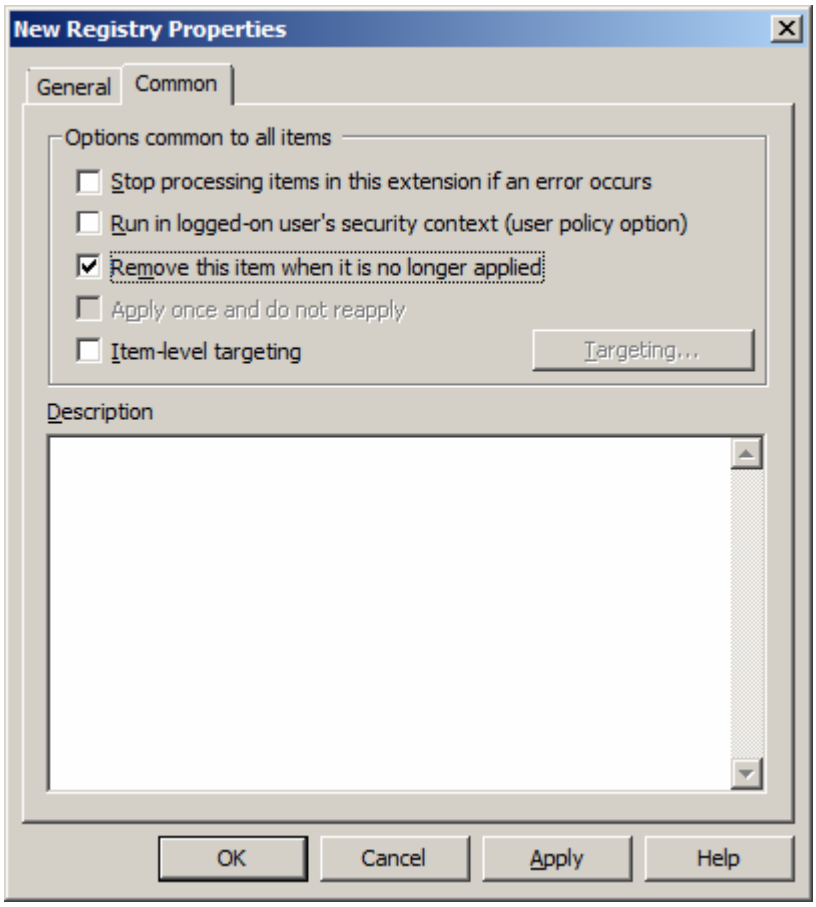

Figure 1-6 PolicyMaker technology now provides a Registry policy, where entries can be non-tattooing and volatile.

> **Important** If some Registry values are removed, leaving the value blank, the computer might see the blank values as a critical error and generate a stop error. Before implementing any Registry value modification, test the different scenarios and outcomes before putting it into production. For more information, see Chapter 12, "PolicyMaker Technology."

Group Policy Can Modify System Settings

Group Policy really progressed when the inclusion of system settings were exposed via a Group Policy object. These system settings are not in the Registry or are not exposed through routine Registry editing tools and techniques in most cases. These new settings in Group Policy work directly with the dynamic system settings on the computer, such as disabling the Administrator account.

Before Windows XP SP2 the Administrator account could not be disabled, deleted, or otherwise modified so that it would not function on a computer. Of course, this is the "default" Administrator account that is being referred to. However, now with new settings in a Group Policy, this account can be disabled on any computer with the use of a GPO, as shown in Figure 1-7.

Figure 1-7 System settings can be altered using a Group Policy, as seen with this control over the Administrator account status.

> ImportantDisabling the Administrator account is not something that should be done without tremendous forethought. Thorough consideration should be made as to the potential ramifications that this might cause on each computer being considered for this setting. This setting can be made to affect desktops, servers, and even domain controllers, which would disable the Administrator account that controls the Forest or Domain.

Group Policy is Extensible

Almost everything discussed here regarding additional features of Group Policy since it came out with Windows 2000 are "extensions" to Group Policy. In these cases, they are extensions that Microsoft made to Group Policy. In addition, anyone can extend Group Policy to add more settings and robust features to what Group Policy does out of the box.

There are numerous companies that have built their entire suite of products around extending Group Policy. In the case of PolicyMaker technology that now exists in Windows Server 2008, these extensions were not originally created by Microsoft. Rather, they were originally created by DesktopStandard, a company that no longer exists today.

Extensions exist today that can contribute amazing functionality to Group Policy. There are some companies that provide extensions to do reporting on Group Policy, others that

configure third-party applications, and others that allow for seamless integration of highly strict password policies for domain user accounts. The options for Group Policy extensibility are nearly endless and the push to make Group Policy the central location for desktop configuration and management will just grow as Group Policy continues to grow in popularity and effectiveness.

Group Policy is Very Dynamic

As any child learns new tricks their parents didn't learn, Group Policy is no slouch when it comes to being dynamic compared to System Policy. Group Policy provides a very dynamic environment due to the constant background refreshes that occur. These background refreshes are occurring on your network right now! They are built into Group Policy and are occurring approximately every 30 minutes on desktops and servers.

These background refreshes allow changes to GPOs to take affect without a reboot or logoff/logon by the user. This dynamic environment gives the administrators an advantage on efficiently managing the overall status and settings on any computer on the network. If a setting needs to be distributed to all computers in a short time frame, the standard Group Policy background refresh mechanism that exists by default will suffice to get the job done.

Some settings don't adhere to the background refresh rules. These settings include options such as folder redirection, software distribution, and drive mappings. They are ommited from the background refresh because they could cause data corruption—without any wanrning to the user--if they were to change in the background.

For example, you would not want your manager working on a letter in Microsoft Word which addresses the reasons why you should get a raise, only to have a GPO remove Microsoft Word before your manager can save and send the letter.

Much, Much More

If every feature were listed here, it would be the entire book! So, just keep in mind that there are many features, new and seasoned, that are not listed here. When you think of Group Policy, you should be considering it for all aspects of your daily needs. New technologies associated with PolicyMaker and Advanced Group Policy Management shed new and imaginative light on areas that were needing attention for a long time. You will be exposed to all aspects of Group Policy in this book… from the ground up and the outside in.

Group Policy's Future

The road to the current Group Policy has been one filled with excitement and amazing new technology. It is very clear that Microsoft has made a bold statement that Group Policy is not only here to stay, but will become more and more an integral part of managing a Windows environment over time. The Group Policy team has been a key driver in making sure that the Group Policy technology is alive, breathing, and growing with each new revision.

The big question is: "Where will Group Policy be in 1, 3, and 5 years?" The answer to that is not 100% solidified, but it can be assured that some new technologies will be sure to hit

the street. If you just look at where you would want Group Policy to be in the future, what would that list look like? Here are some ideas that have been thrown around by Group Policy MVPs, Group Policy software companies, and even inside the walls of Microsoft.

Troubleshooting Tools

It is no secret and there is a small gap in the ability to troubleshoot Group Policy. It has improved over the years, but no one tied directly to the Group Policy community would stand up in a crowded room and boast about the impressive troubleshooting tools and power that currently exists for Group Policy.

The entire community receives questions and suggestions regarding troubleshooting Group Policy all of the time. Here are some different requests that have come through loud and clear, which are most certainly on the "wish list" for the Group Policy team for the future.

- Verification that Group Policy has refreshed for specific computers
- Verification that specific Group Policy settings were applied during the past refresh
- Database of current state and version of all computers and users regarding GPOs
- Ability to do a comparison of Resultant Set of Policies against actual configured policies

It can be assured that you too have a troubleshooting need that you want to add to the "wish list." There is a resources page in this book that lists email addresses for many different people associated with Group Policy. This is your big chance to contribute to the list by emailing them and explaining the new troubleshooting features that you would like to see.

Enterprise Administration

Without question, the Group Policy Management Console (GPMC) provides an excellent view into the administration of Group Policy. With each domain specifically being listed within the console, you can clearly see which GPOs are associated with the appropriate domain.

Where the GPMC falls short and future technology will be developed, is in the arena of having GPOs move, copy, and otherwise update settings across domain boundaries. Today, Group Policy is very domain specific. There are migration tables that help you "translate" security principals from one domain to another, but these tables are not the most joyous things to work with.

The future of Group Policy will allow you to move GPOs across domains and even forests for easy duplication of your GPOs and settings. This will be especially useful for large organizations, multi-national organizations, and organizations that have test domains/forests which dupulicate the production environment.

Disaster Recovery

As you will see, the advent of Advanced Group Policy Management (AGPM) has brought Group Policy management and recovery to a respectable level in a short amount of time.

AGPM provides offline editing, roll-back, roll-forward, automatic backup/archiving, and change management to Group Policy in one easy tool.

There are still things missing from an all-in-one disaster recovery solution with regard to Group Policy. There is still a need to have Access Control Lists (ACLs), filters, granular link control, and specific settings controlled when recovering from a disaster tied to Group Policy. The goal is to get as granular as possible when recovering from a disaster, similar to what you have with Active Directory recovery in using ntdsutil.

The reason for such an elaborate disaster recovery suite of options is that the disaster could have been caused by one of many things. It might have been due to a server failure, hard drive failure, or even the Group Policy settings caused the destruction. In any case, the more options that you have the better your chances of getting all computers back and running in the shortest amount of time.

Reporting

Reporting borders along the same lines as troubleshooting in many cases, but here reporting is just gathering information for review, not to fix a problem. Therefore, some of the same reports used for troubleshooting would be nice for just gathering information. In addition to the reports for troubleshooting, more reports would be nice to query detailed settings and computer- or user-related information. This would require that some database of information be created to store all of the information that you would want to reported.

For example, say you want to run a report to know which computers have had the local Administrator account renamed using Group Policy. You might also want a report indicating how many computers, per new name, have been modified. With this type of reporting, you can get a very quick and useful report on a myriad of different configurations that are made in a GPO.

Reporting will also dive deep into every aspect of Group Policy fFrom settings, to links, administration, management, processing, failures, and more. With the developing technologies like SMS and System Center, this type of environment is not all that far off. Reporting is certainly a feature that is both wanted and deserved by all who use Group Policy.

Instant Configuration

As you have seen and most likely already know, policy settings were not always as "real time" as they are today. There was a time when System Policy required a reboot or logoff/logon, and today Group Policy has an automatic background refresh. This refresh occurs approximately every 30 minutes, but it handles only some–not all–GPO settings.

The future of Group Policy will hopefully provide more control over "pushing" settings to one or more computers or users. This form of control creates an instant configuration that is useful in many different scenarios.

There might be a security configuration that needs to be pushed out immediately. There might be a user requiring a new configuration so they can finalize a contract, trade, or other business deal. Regardless of the scenario that you can come up with, the ability to

have instant configurations of Group Policy settings would make desktop and server administration even more efficient.

Is the Future Already Here?

Do not get the impression that some of these "wish list" requests and bullet points are not already on the scene. That would be a false statement and one that could get everyone involved in a lot of trouble. Rather, be fully aware that many of these features and functions already exist. Yes, they already exist.

They just don't exist in the Microsoft suite of offerings. There are a handful of software vendors, small and large, that have been working and producing amazing tools for Group Policy for years. This is not the right time to go over those vendors, you can find that information in Appendix A, "Third-Party Tools.".

It should be stated that many of these vendors have been producing Group Policy solutions for many years and have driven many of the changes that have occurred within Microsoft for the Group Policy efforts. Still today, there are numerous companies and individuals that provide valuable input into the present and future of Group Policy.

Benefits of Group Policy

If you are a Windows administrator who is new to Group Policy, not convinced that it is all that it could be, or even a longtime administrator who has been exposed to all of the great benefits of Group Policy, you are in the right place. Here, you will be shown some of the most popular and heralded reasons that companies, administrators, and IT staffs use Group Policy.

If the list were short, there would be no reason to waste your time on the ins and outs of the benefits that Group Policy provides to a Windows network. However, the list is not short. In reality, this is an abridged list, which only highlights the most important and useful benefits of Group Policy. There have been bizarre and amazing reasons brought up in conferences, seminars, and training rooms throughout the years on why and how companies use Group Policy. All have validity, but these reasons seem to float to the top.

More Efficient Management

There is no doubt that centralized management of desktops and servers has proven to save millions of man hours over the past few years. It is even hard to believe that we used to manage computers in a "workgroup," requiring a "touch" of each computer in the enterprise everytime that something needed to get done. Heck, you might even live in that world today, where you have to touch every computer to get software loaded, a configuration set, make changes to the Registry, and more.

Group Policy is the king of centralized management. The key to Group Policy's centralized management and efficiency is in the way that it ties in with Active Directory. If Active Directory were not in the picture, Group Policy would not be as beneficial as it is. The reason that it is such an efficient technology along with Active Directory is due to the Active Directory structure. Active Directory provides you with the ability to create a hierarchy within the domain. This hierarchy is created using organizational units. You can

create single level organizational units or nest them fairly deep. The goal of this hierarchy is to, in the end, move computer, user, and group accounts into these organizational units. You will move these objects into the organizational units so that you can then manage them in a like manner.

For example, you will want to manage the IT Staff computers differently than the HR Staff computers. There would most likely be a different organizational unit for each of these computer categories. Once you have different organizational units for these different computers, you can manage them separately. It is as simple as creating two different GPOs, each containing the appropriate settings for each "type" of computer. Once this is completed, you just link the GPO to the respective organizational unit, and the operating systems and directory service takes over from there.

Not only can you make initial settings efficient, but you can also make changes on the fly to the GPO, which will in turn modify the entire group of comptuers that are located in the organizational unit.

This type of efficiency can make thousands of computers seem like just a few. In essence, you just need to manage the "types" of computers, allowing Group Policy and Active Directory handle the rest.

More Powerful Management

Group Policy comes with numerous settings. At latest count, the settings in a default GPO for Windows Server 2008 are hovering around 2500 With this many settings, the power is at your fingertips. There is almost nothing left out of the latest suite of GPO settings. For those settings that are left out, another option is available with Windows Server 2008, which is PolicyMaker technology.

PolicyMaker technology alone adds in thousands of settings to a GPO. How many you might ask… that number has not been determined. There are so many settings and options, no one has taken the time to count them all.

You have the ability, with all of these settings, to control key areas of a computer and user environment. The following are just a small listing of areas that you can control with a GPO:

- Drive and printer mappings
- User password maintenance
- Local and domain group memberships
- Software installation
- Internet Explorer
- Windows Firewall
- My Documents

This list can go on and on, and does later on in the book. With all of the new settings and areas of control, there is nothing left to manual or scripting maintenance. If you need to get something completed or configured on a desktop or server, in almost every case a Group Policy can manage that for you.

Reliability

Group Policy is one of the most reliable technologies that Microsoft has produced. With such a reliance on Active Directory, which itself has proven to be stable, strong, extensible, and reliable, Group Policy has had a fairly smooth ride to such a good reputation.

Active Directory has grown up right along with Group Policy, which makes the two equally responsible for the accolades that they have been given. Active Directory has numerous fault tolerant technologies built-in, including:

- Multi-master domain controllers
- Multi-master DNS servers
- Active Directory replication
- Domain controller authentication algorithms

The reason that these Active Directory technologies are so important when discussing the reliability of Group Policy is that Group Policy relies on all of these technologies too. The partnership that Group Policy has with Active Directory is seamless.

Group Policy is also very reliable due to the way that the settings are delivered and processed by the target computers and users. With an automatic background refresh that occurs every 30 minutes or so, the settings that reside in a GPO reliably get delivered to the desktop in plenty of time for most networks.

Extensibility

Group Policy has always been customizable. As you just witnessed with the history of policy within Microsoft, System Policy was also customizable. Even back in the prehistoric days (System Policy days), Microsoft provided an open platform to make policy not only customizable, but extensible.

This extensibility allows third-party vendors, as well as Microsoft, to add to the technology and GPO settings with great ease. Without getting into great detail at this point, this extensibility is primarily due to a simple structure that Group Policy relies upon, which includes technology called "client-side extensions."

Client-side extensions are the brains in the extensibility matrix. These client-side extensions, really just DLLs, live on the target computer, where policy settings will be delivered from Active Directory. Within these DLLs reside code that can handle the information that is delivered to the target computer from the originating GPO.

The extensibility of Group Policy has been mastered by many third-party vendors, as well as by Microsoft. It seems like every service pack or major operating system release comes with a new set of policy settings, which are handled in most cases by an extension to Group Policy.

One of the best examples of Group Policy extensions is the latest acquisition of PolicyMaker. PolicyMaker adds over 20 client-side extensions, which is nearly seamless to anyone that is not keeping up on Group Policy technology. With these extensions Group Policy now covers many new areas of configuration, not to mention the thousands of settings that the 20+ extensions add.

Security

Security is really a two-fold benefit when it comes to Group Policy. Initially, Group Policy is a reliable and secure technology. There has not been a report or documented incident of an issue arrising from an attacker using Group Policy to elevate privileges or cause damage to a computer. This is a testimony to the rigorous efforts put in by the Group Policy and Active Directory teams over the years. However, the security benefits only start here. There are many other security benefits when it comes to Group Policy.

Some of these security benefits are just coming to surface. I am referring to the awesome and powerful security settings that are available through the new PolicyMaker technology. There are three specific security settings that make Group Policy shine above many other technologies.

- The ability to reset the local Administrator (and any other user for that matter) password through a policy.
- The ability to control membership in local groups, such as the Administrators group, using Group Policy. This is a fantastic setting; this option allows you full granularity of the membership.
- The ability to reset service account passwords within the service itself. This promotes compliancy and security in an area where passwords and security were once thought too complex and mundane a task.

Other areas in a GPO have also benefited from immense efforts by the Group Policy community. There is an entire section in a GPO that is geared toward security settings. Here, setting help you to control anonymous connections, digital signatures, authentication protocols, SMB signing, and much more. Still other areas help you to control security related to Internet Explorer, Windows Firewall, file and folder ACLs, and so on.

With such an emphasis on security these days, Microsoft has not spared any effort in making sure all potential security settings are exposed in a GPO. By far this is one of the most important benefits of using Group Policy.

Diversity

When developing a strategy for managing desktops and servers, it is always a good idea to categorize each different type of computer. During this categorization, you need to consider a variety of different criteria for each computer type, including:

- Security settings
- Software installed
- User privileges
- User environment
- Internet Explorer settings
- Application settings
- And more…

The resulting matrix of combinations of these criteria and the associated settings can become quite complex and daunting. However, when you start to organize these areas into the Group Policy framework for distributing the settings, the solution becomes very manageable.

Although each computer requires a different set of needs, configurations and settings to facilitate the user to be productive, Group Policy, combined with Active Directory structuring, makes managing these diverse settings easy. It is as simple as creating different GPOs for each type of computer, then applying those settings through Active Directory organizational units so that only the correct computers and users receive the settings.

Consistency

Consistency is defined as "adherence to the same form." In terms of computers, this means that all desktops and servers should maintain a baseline of settings that ensure security, stability, ease of management, and maintain reliability. Whether you are creating baseline settings to meet internal guidelines or external compliancy regulations, computers need to be consistent.

Group Policy excels in ensuring that computers are maintained consistently. As we have seen in many of these other benefits regarding Group Policy, the design of Active Directory and the placement of computer and user objects within tha structure is the foundation for reliability and consistency. Once the GPOs are integrated into this structure, the inherent nature of Group Policy technology ensures that computers are consistent.

Without the Active Directory structure and constant refreshing of Group Policy in the background, the concept of consistency would not be as clean cut. Without these constructs of the technology, the process for creating, maintaining, and delivering the settings would become very manual, and thus would break down the level of consistency that an automated process delivers.

Stability

The result of a secure, reliable, consistent, and managed desktop or server is stability. Without a secure, reliable, consistent, and managed desktop or server, you are left with potential chaos and instability. The bottom line is that if you are not managing your computers tightly, your computers are managing you.

Time has proven that "end users" cause more damage and down time for their desktop than anything or anyone else can imagine. The more control administrators have over ensuring the desktops are configured properly, the more stable the desktop. The more secure a desktop can be made, the more stable the desktop will be. Finally, if the administrator can reduce the privileges that an "end user" has over the desktop, this is where most of the stability comes in.

Group Policy can do all of these things and even more. With such a powerful and robust system aiding administrators in their overall quest to manage everything and anything on a desktop, the results all equal a more stable environment.

Group Policy Negatives

As you can see, the benefits of Group Policy are certainly clear and compelling. There are, however, some negatives (not disadvantages though) of Group Policy. These negatives are not items that should push you away from Group Policy, but they do make managing and maintaining some settings more of a challenge. You have seen many of these in the list already, when you saw a list of where Group Policy was going in the future. Of course, if these items are futuristic, it is difficult to make them benefits today.

Limited Troubleshooting Tools

There are not as many tools and solutions for troubleshooting Group Policy as there needs to be. Microsoft and other third-party vendors are spending thousands of person hour cycles trying to produce and perfect some tools, but they are just not there yet. Within the next few years, there will be amazing tools on the market that will take this topic from the disadvantage list and make it a benefit.

Limited Testing Environment and Tools

With Group Policy being so powerful and manageable, it also leads to the fact that these features need to be tested. A single errant Group Policy setting can bring down a computer, department, application, and potentially halt production. Therfore, more attention and better tools need to be provided for testing of Group Policy. There are some mechanisms built in, such as Modeling, but more needs to be done. The Modeling only gets the testing to a certain point, but does not complete the task. It is suggested that a test environment be created to test all Group Policy settings and their interaction with computers before the GPOs are placed into production.

Limited Inter-Domain and Inter-Forest Support

If your company is one that has a complex Active Directory environment, then you have most likely already seen some of the pain points related to Group Policy across your enterprise. A limitation of today's Group Policy is that it does not handle cross domain and cross forest interactions very well. There are tools and features designed to aide in this, such as the GPMC and Migration Tables, but still more needs to be developed. The Group Policy team is working on these solutions already, as are many of the Group Policy software vendors. In no time, there will be integrated and robust solutions to solve this disadvantage.

Summary

Group Policy is not an infantile technology. This technology has been through growing pains and is now a full fledged enterprise technology. The history of Group Policy proves that it has seen substantial growth and maturity over the many, many years that Microsoft has been producing policy-based management.

Radical and innovative additions to Group Policy for Windows Server 2008 and Vista make this time in the Group Policy space very exciting. New technologies, new settings, new controls, and new possibilities allow administrators and companies to gain more control, resulting in more stable computers.

The future of Group Policy is just as exciting as the present Group Policy offering, maybe more so. Microsoft and other leading Group Policy software companies are daily making new products, new developments, and new features that allow Group Policy to become even more powerful than imagined.

Group Policy can benefit any sized company. Whether there are just a few desktops or servers, or thousands of computers, Group Policy can scale to help manage them. The benfits of Group Policy are like any other management platform, it is just that Group Policy is integrated with a technology that you rely on today, Active Directory. With Active Directory and Group Policy working hand-in-hand, the overall benefits of manageability, security, consistency, reliability, and stability are clearly evident.

Additional Resources

- Microsoft Group Policy Website, at *http://www.microsoft.com/grouppolicy*, includes more information the benefits of Group Policy for Active Directory enterprises
- Chapter 2, "What's New in Windows Vista and Windows Server 2008," includes information about new Group Policy features and settings with the newest operating systems.
- Chapter 13, "Settings Breakdown for Windows Server 2008 and Windows Vista," includes information about specific settings within a GPO.
- Appendix A, "Third Party Tools," includes information about other companies that have extended Group Policy.

Chapter 2

What's New in Windows Vista and Windows Server 2008 with Group Policy

There has been a distinct push to make Group Policy a more integrated, reliable, stable, and useful product within Active Directory. That is not to say that it has not been all of these things. It is to say that efforts within the Group Policy team and the supporting teams that tie into Group Policy have put great effort into making Group Policy everything and more.

Each iteration of Group Policy has brought something grandeous. The continual improvement of technology is a testament to the different teams working on making technology work better and more efficiently for customers.

Remember When

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

Table 2-1 Group Policy Technology Milestones

Place in Time	Feature
Windows 2000	Approximately 900 Total Group Policy settings
Windows XP	Approximately 1400 Total Group Policy settings
Windows Server 2003	Group Policy Management Console introduced
Windows XP SP2	Approximately 1600 Total Group Policy settings

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

When Windows XP Service Pack 2 arrived, it was a milestone not only for Group Policy, but for Microsoft as a company. The security efforts that came along with SP2 are revolutionary and what Microsoft often uses as a baseline for any desktop operating system. In many ways, Microsoft views the WindowsSever 2003 partner to Windows XP SP2, which is Service Pack 1, as the baseline for server operating systems.

New and Now

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

There are some features that came with Windows Vista. Since Windows Vista was released quite a few months before Windows Server 2008, some of these technologies might be more familiar to you. With Windows Server 2008, there were some great new features tied into the GPMC which will make administrative life much simpler when working with Group Policy. Still other technologies are outside of both Windows Vista and Windows Server 2008 at this time. They are the products that were acquired from DesktopStandard, including Advanced Group Policy Management and PolicyMaker technology.

New Group Policy Features in Windows Vista

It has been about a year since Windows Vista arrived on the market. The new features that it brought are making big waves in the Group Policy community. It is nice to write about technology that is proven, instead of technology that is still yet unknown in the overall marketplace.

Windows Vista not only provides some very cool new graphical enhancements, but it comes with some overall changes to Group Policy that can affect the entire network of desktops— not just single machines. However, there is one change that does affect just one desktop at a time, which is the Multiple Local GPO enhancements. The other new features can affect one desktop or many desktops. Those include:

- Network Location Awareness
- ADMX Templates
- ADMX Repository
- Improved Logging

Multiple Local GPOs

First, you need to get your bearings to understand what has changed with local GPOs on a Vista desktop. In previous versions of Windows there was a single local GPO, then there could be many GPOs in Active Directory linked to the domain, organizational units, and sites. The local GPO had no power over the Active Directory GPOs, unless there were non-conflicting settings established. In this case, the local GPO settings would make its way through the maze of Active Directory GPOs to the Resultant Set of Policies that molded the final policy settings on the computer.

Multiple local GPOs were put into place to solve many issues. One of the biggest problems this feature solves involves both users and administrators logging on to the same desktop. Until now, if there are local GPOs constraining the user account, both the administrator accounts and regular user accounts will receive the settings. This causes some very odd results, either allowing the user to have too many privileges or restricting

the administrator too severely. If the administrator needs to run elevated tasks in a restricted environment like this, he or she is forced to use "Run As" or other privilege-elevating technologies. Although this is an almost ideal situation, it can cause some issues with a company that does not want these restrictions on administrators logging into desktops.

WindowsVista tackles all of these issues with new technology surrounding the local GPO. In reality, there is no longer just a single GPO on the local desktop, but three local GPOs. These three GPOs provide granular control over the different users that log on to the desktop. Local GPOs can be used in a single computer environment, home environment, small business environment, or even large corporate scenario.

The three local GPOs are designed to control different users that log on to the desktop and to be hierarchical. This hierarchy allows control over the settings that will be configured in GPO. The GPO options consist of the following:

- Local Policy Object
- Administrators and Non-Administrators Local GPOs
- Specific User Local GPO

Local Policy Object

The Local Policy Object is identical to the local GPO that you know and love in Windows 2000 and Windows XP. It can be accessed using the Group Policy Object Editor (running Gpedit.msc from the Start, Run menu) or using the Microsoft Management Console (MMC). In either case, you are able to configure both Computer Configuration and User Configuration settings. This can be seen in Figure 2-1.

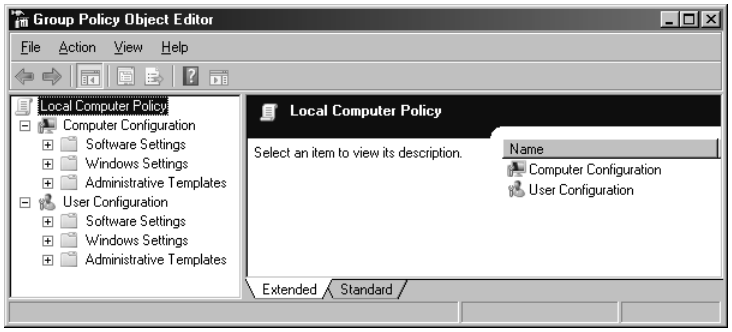

Figure 2-1 The Local Group Policy can be opened in the Group Policy Object Editor by clicking Start, Run and the typing gpedit.msc in the Run dialog box.

Administrators and Non-Administrators Local GPOs

The Administrators local GPO and non-Administrators local GPO are new in Windows Vista. As the name indicates, these GPOs are designed to control two types of user accounts. The delineation is based on which users have membership in the local Administrators group.

> NoteUser accounts having membership in the Power Users group are not considered Administrators and won't be affected by GPO settings under the Administrators local GPO. Rather, they will be affected by the GPO settings in the non-Administrators local GPO.

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

These two GPOs are not as easy to access however. To access these GPOs, you must use the MMC. This exposes both of these GPOs for you to administer them, as shown in Figure 2-2.

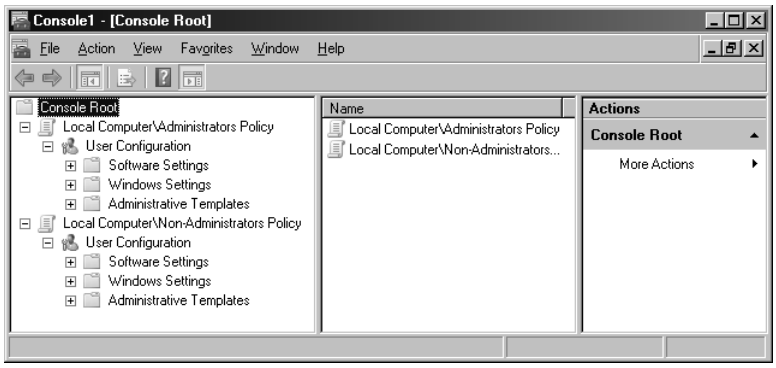

Figure 2-2 Both the Administrators local GPO and non-Administrators local GPO can be edited in the MMC.

Specific-User Local GPO

The final local GPO that you have at your disposal is the user-specific local GPO. This GPO offers the ultimate in granular control because it allows you to specify an individual user account to receive special GPO settings. This GPO option should not be used very often because individual user account settings are typically discouraged from an administrative efficiency standpoint.

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

The administration of this GPO is also not accessed through the Group Policy Object Editor directly, rather, it is accessed through the MMC. When using the MMC to open up this GPO, you will be able to select the GPO that is associated with any one of the local user accounts that are configured in the local Security Accounts Manager (SAM). Once you add your GPO into the MMC, the interface that you will see only includes User Configuration settings. Since this local GPO only affects user accounts, the Computer Configuration settings have been removed so that they do not confuse the administrator of the local GPO. This can be seen in Figure 2-3.

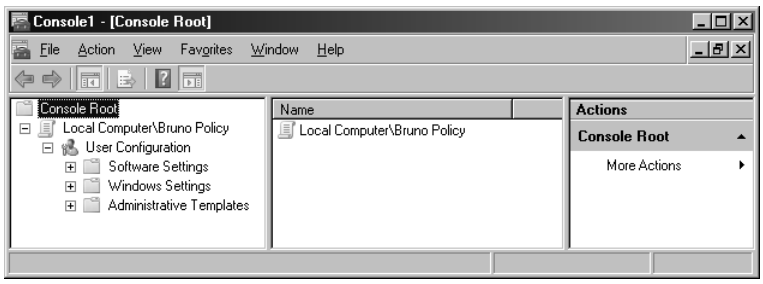

Figure 2-3 The local user-sSpecific GPOs can be edited in the MMC and only give the ability to control User Configuration settings.

Precedence and Application

Now that there are multiple local GPOs to configure and choose from, it is important to understand how they are tiered in the hierarchy, in case there are ever any conflicting settings between them. The hierarchy of local GPOs creates the precedence in which they will be structured for conflicting settings. The local GPOs have a precedence; the more generic GPO has little precedence and the most specific GPO has the most precedence. Thus, the local Group Policy object has the least precedence, the user-specific local GPO has the highest precedence, and the Administrators local GPOs fall in between these two.

The precedence of the local GPOs also must play along with the GPOs that are linked within Active Directory. The same rules here apply as they did before, where the local GPOs have the weakest precedence when being compared to the GPOs from Active Directory.

Network Location Awareness

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

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

Now that Group Policy relies on network location awareness, the overall picture and state of Group Policy has been enhanced. Group Policy uses network location awareness in two primary fashions. First, it uses it to determine link speed. Second, it uses network location awareness to determine wheter the computer needing to refresh Group Policy is connected to the domain.

For this first use of Network Location Awareness, Group Policy determines if the link from the computer receiving GPO settings has a fast or slow connection to the domain and domain controllers. Since some GPO settings can take a long time to apply due to the amount of data that is being sent, determining link speed can be an indicator as to whether the data should be sent at all. Network Location Awareness provides this by

determining the bandwidth of a TPC connection. This information can then be used by Group Policy to make decisions as to what settings will be delivered based solely on the bandwidth (slow link speed) that is available.

Group Policy also uses Network Location Awareness for background refreshes. This is accomplished by Network Location Awareness indicating whether the computer authenticated to a domain controller and whether the domain controller is available to the computer. This is important for computers that have failed to refresh Group Policy because the domain controller was not available. In the past when Group Policy failed to apply, the computer would wait until the next refresh interval—90 to 120 minutes—to attempt to apply Group Policy. The domain controller might have been available only minutes after the failed refresh, but the system would still wait the full refresh interval to apply the Group Policy updates. With Network Location Awareness, the computer does not wait the full refresh interval. Instead, as soon as the connection to the domain controller is detected, the Group Policy refresh occurs.

ADMX Templates

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

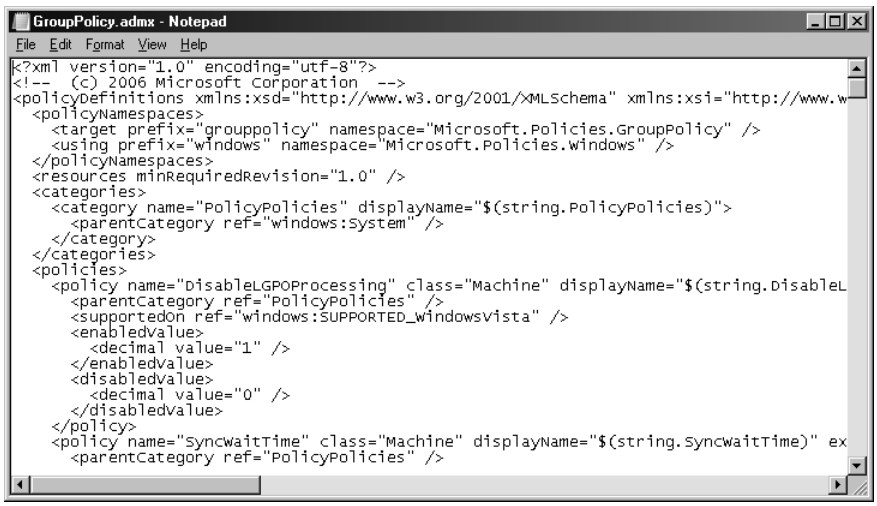

Figure 2-4 The ADMX files now are based on XML for flexibility of languages and ease of administration.

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

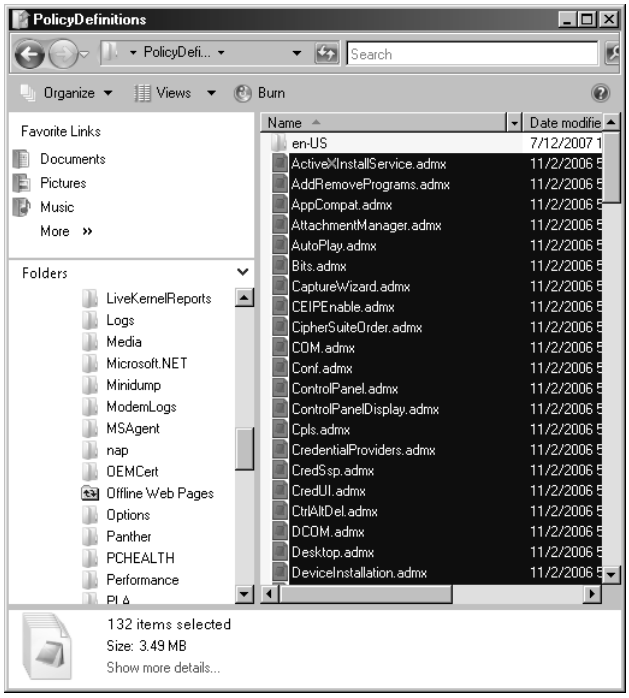

Figure 2-5 Now that the ADMX files are XML-based, there are 132 individual templates that make up the Administratative Templates section of a GPO.

> NoteADMX files, their structure, and details are described in detail in Chapter 10, "Customizing Administrative Templates."

These new ADMX files reside by default on the local system drive of Windows Vista and Windows Server 2008 computers. The path to these ADMX files is C:\Windows\PolicyDefinitions.

ADMX Repository

In conjunction with the changes to the administrative template file structure and formatting, another major change has occurred with the management of the administrative template files. A repository has been created and coded so that all ADMX files can now reside in one location, instead of being spread throughout the network on local computers.

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

These negatives of ADM templates triggered the change and new technology to handle administrative template files. If no repository is created, the local ADMX files will still be used to edit a GPO. This keeps the administration of GPOs is consistent, even if the technology is not used. It should be noted, however, that the ADMX files are *not* stored in the Group Policy template. This change helps with storage of files on domain controllers, as well as the replication of those files between domain controllers.

> NoteADM template management and ADMX repository are described in detail in Chapter 9, "ADM, ADMX, and the ADMX Repository."

Improved Logging

It is no secret that managing logging and documentation has been a struggle for Group Policy over the years. Trying to ferret out information from the old Event Log entries was a bit problematic. You needed to have a PhD in Group Policy and Microsoft to get much from the logging that occurred in the Event Viewer. The other logs, such as the userenv.log, were better, but still not ideal.

All of this has changed with the latest installment of GPO logging. The changes are like many of the other changes: stunning and fantastic. The new logging is built on the Event Log service that is available with Windows Vista. The new logging does away with the userenv.log and now stores information in a Group Policy Operational Log found in Event Viewer. You will find this log in Event Viewer by opening up the Applications and Services Logs, and then opening Microsoft\Windows\GroupPolicy\Operational. The resulting log view can be seen in Figure 2-6.

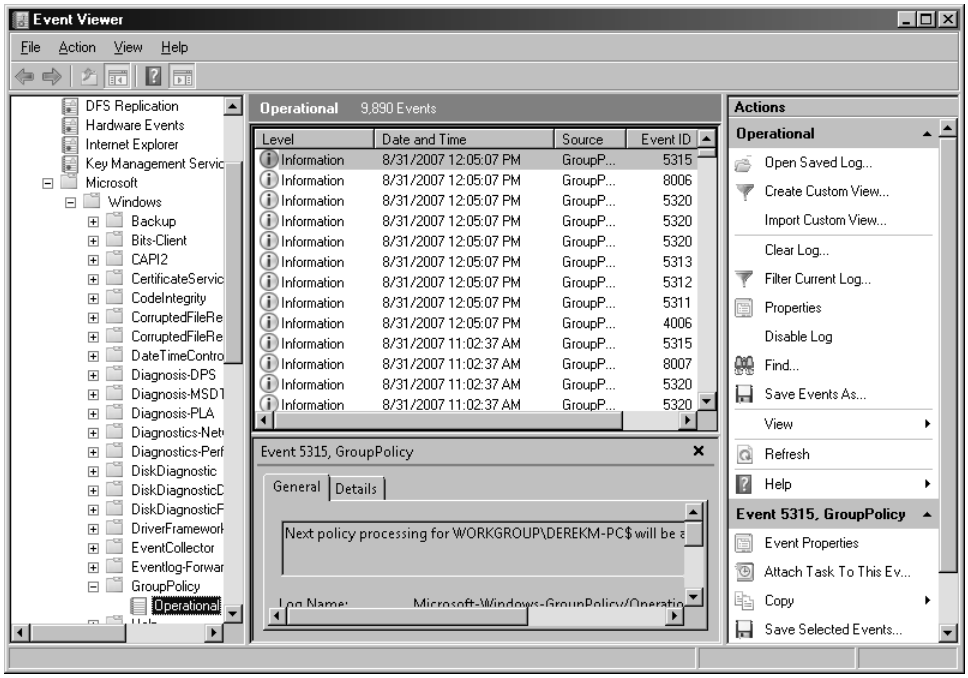

Figure 2-6 With the new logging that is available for Group Policy, new Group Policy events can be seen in the operational logs.

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

The is much more to logging. In Chapter 13, "Troubleshooting GPOs," you will get more information about logging.

New Group Policy Features in Windows Server 2008

Filters

If you have ever tried to decrypt the myriad settings that are in a GPO while trying to troubleshoot a problem, you know that it is a difficult task. With thousands of potential settings in a GPO, there has been very little with regard to filtering the settings, until now.

With Windows Server 2008, there is an entire platform for searching the settings in a GPO. The obvious search options are there, such as text searching for title, explanation text, and comments. These can be seen in Figure 2-7.

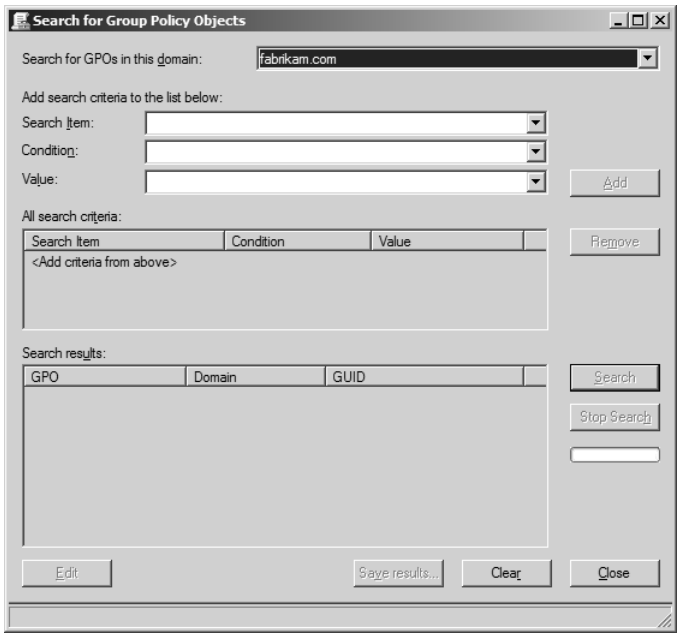

Figure 2-7 The new filtering of GPO settings allows for basic searching and filtering of title, explanation text, and comments within a GPO.

Additional searching also exists that allows you to search based on operating system platform support. With so many iterations of Group Poilcy, as was discussed in Chapter 1, it is important to be able to pinpoint which settings work on which version operating system.

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

For more information about the differences between how some Registry setting apply differently than other, see Chapter 10, "ADM, ADMX, and the ADMX Repository," and Chapter 12, "Settings breakdown for Windows Server 2008 and Vista." The difference is denoted as *managed* (policies) settings or *unmanaged*" (preferences) settings. With these Registy values making such a difference when applied and controlled, it is nice to be able to search for settings by category.

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

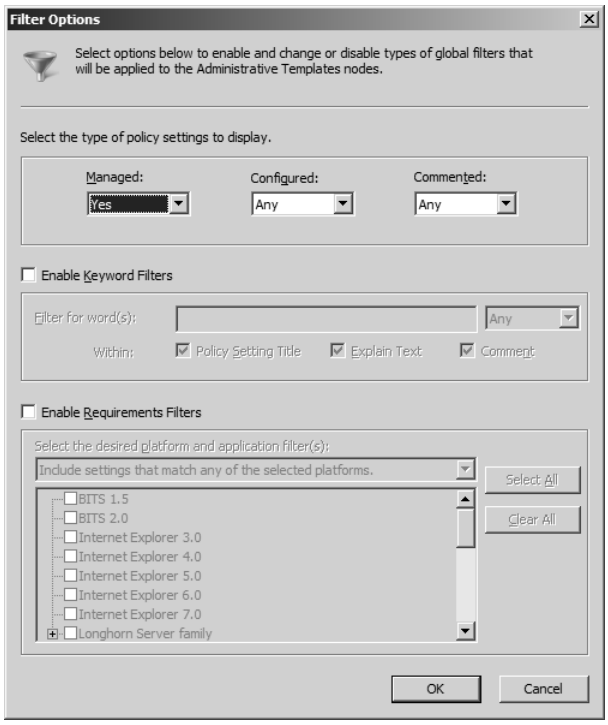

Figure 2-8 The new filtering options include the ability to search on enabled or disabled GPO settings.

Starter GPOs

If you are the lead GPO administrator or responsible for those that create GPOs in your environment, you now have another tool in your toolbelt. The new Starter GPOs provide an excellent way for you to create a baseline of settings within an offline "Starter" GPO, which then can be copied to create a new GPO. The new GPO will contain all of the configurations and comments that were created in the Starter GPO.

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

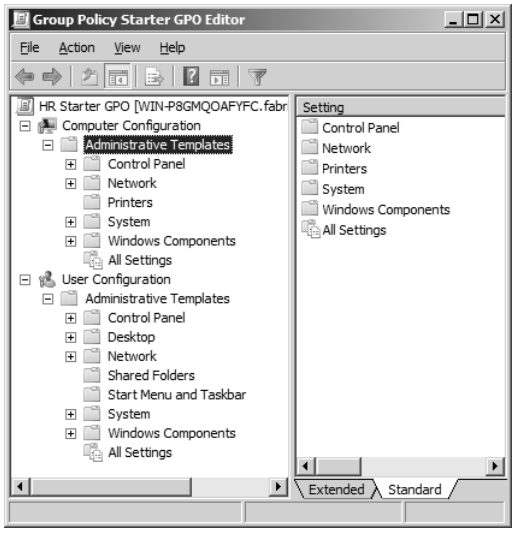

Figure 2-9 Starter GPOs allow you to configure any setting falling under the Administrative Templates section of a GPO.

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

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

For more information on Starter GPOs refer to Chapter 6, "Using the GPMC."

Commenting

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

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

It is very common for changes to occur to GPOs that are caused by incidences on a computer. For example, an exploit might come about that is fixed by an Internet Explorer setting or a custom Registry entry. Changes like these usually occur quickly and without any documented reasoning. The outcome of this is future audits or analysis are left wondering why the change occurred.

With commenting, all changes are tracked immediately when the modification to the GPO occurs. This provides a very detailed trail of the changes that occur to GPOs throughout its life. Sample comments can be seen in Figure 2-10.

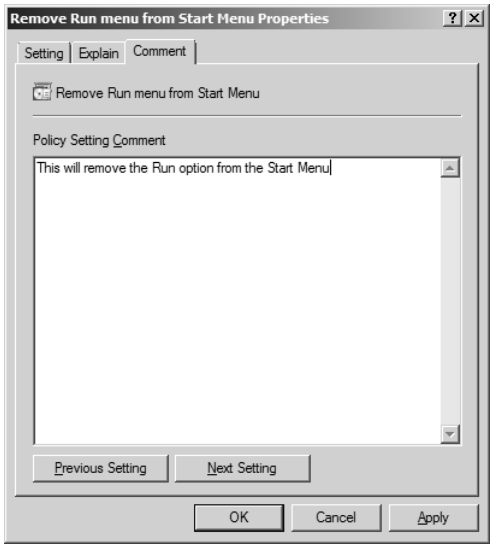

Figure 2-10 A GPO can include comments, allowing for administrators to document the changes that occur each time the GPO is altered.

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

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

So, What about Those DesktopStandard Products?

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

PolicyMaker

At the time of this writing, the PolicyMaker technology is scheduled to be delivered to the market in early to mid 2008. This falls in line with the release of Windows Server 2008, which is scheduled for early 2008.

As for the technology and offerings that PolicyMaker technology will provide, the majority of that information will be in Chapter 12, which is dedicated to PolicyMaker technology. However, there needs to be some introduction to PolicyMakerbecause it is a spectacular product and is coming with Windows Server 2008.

PolicyMaker technology will tie directly into the way that standard Group Policy is managed and controlled. You will use the Group Policy Management Console, Group Policy Object Editor, and Advanced Group Policy Management, just like you do today.

PolicyMaker technology contributes 22 client-side extensions to a GPO. These client side extensions include settings related to files, folders, user accounts, local groups, drive mappings, printer mappings, and much more.

PolicyMaker provides control over areas of a desktop and server that default Group Policy doesn't. The technology has been on the market for many years and customers have loved what it can do for them. Instead of going on and on here, if PoilcyMaker technology is something that could benefit you, Chapter 12 is where you should be looking now.

Advanced Group Policy Management (GPOVault)

The other product line that Microsoft acquired along with PolicyMaker technology from DesktopStandard is Advanced Group Policy Management (AGPM). You might know this product from when it was owned by DesktopStandard. It was named GPOVault back then.

This product is offered a bit different than the other Group Policy products and technologies. AGPM is offered through the Microsoft Desktop Optimization Pack (MDOP). MDOP is only available to those companies that have bought software assurance. MDOP is a enormous package that offers a great "bang for your buck."

> NoteFor more information on MDOP, refer to *http://www.microsoft.com/windows/products/windowsvista/enterprise/mdopoverview.mspx*.

AGPM itself brings tremendous value to the Group Policy management arena. Although Chapter 8 goes into the AGPM features and settings in full detail, the following is a list of benefits that AGPM can provide to your GPO management environment.

- Role Based Delegation
- Rollback and rollforward to any GPO in the archive
- Offline Editing of GPOs
- Settings Difference Reports between two GPOs
- Workflow for GPO management tasks
- GPO Templates for baseline configurations
- Built on Group Policy Management Console (GPMC)
- Integrated Change Control for your Group Policy management environment

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

Summary

With every new operating system comes new changes in every technology area. Group Policy is no different. There are some exciting and amazing new technologies with Windows Vista and Windows Server 2008. Some of these technologies were introduced with Windows Vista, including local GPOs, Network Location Awareness, logging improvements, ADMX file format, and ADMX repository. New for Windows Server 2008

are many updates to GPMC, including searching, commenting, and filtering, as well as PolicyMaker technology. Last and not least, is the new AGPM functionality which makes management of Group Policy easier and more efficient.

Additional Resources

- Microsoft Group Policy Website, at *http://www.microsoft.com/grouppolicy*, includes more information on the new features and settings that are available in Windows Server 2008 and Windows Vista
- Microsoft TechNet Website, at *http://technet2.microsoft.com/WindowsVista/en/library/9c7ecc7d-8784-4b8d-ba1f-ba1882ba83741033.mspx?mfr=true* titled "Step-by-Step Guide to Managing Multiple Local Group Policy Objects", includes more information on multiple local Group Policy objects in Windows Vista.
- Chapter 14, "Advanced Group Policy Management with AGPM", includes information about installing AGPM, how to use AGPM, how to obtain AGPM, and the benefits of AGPM.
- Chapter 13, "Settings Breakdown for Windows Server 2008 and Windows Vista", includes information about specific settings within a GPO.
- Appendix A, "Third Party Tools", includes information about other companies that have extended Group Policy.
- MLGPO overview and step-by-step guide at *http://technet2.microsoft.com/WindowsVista/en/library/9c7ecc7d-8784-4b8d-ba1f-ba1882ba83741033.mspx?mfr=true*