CHAPTER 23

Expanding on the Use of Group Policies to Better Manage Windows Vista Systems

Available Group Policy Objects (GPOs)

Perhaps the most daunting task when working with GPOs is determining what GPOs should be used and which ones are best left alone. Generally speaking, GPOs should be created only when there is a specific need that can be addressed by a GPO. This is to say, the GPO should be driven by a company decision rather than being implemented because it looks useful.

Some companies fall into the trap of flipping through every possible GPO setting and deciding yes or no on each setting. This is a bad idea and will generally cause more issues than it will fix. The better approach is to ask yourself, "What have I always wished I could set for a common group of computers?" and then see if you can automate that setting with a GPO.

Existing GPOs That Work with Vista

Generally speaking, most GPOs that worked with Windows XP will continue to work with Microsoft Vista. This is because Microsoft wrote Vista to be backward compatible whenever possible. Even with this in mind, it is still a good idea to thoroughly test existing GPOs when first deploying Vista into the environment to make sure the systems are still being conformed to your existing standards. This is especially critical with GPOs that are in place to enforce security settings or to point to update servers for patches or definition files.

New Vista-Specific GPOs

For administrators wanting to familiarize themselves with all the new GPOs available for Vista, Microsoft has posted a spreadsheet detailing the new settings at the following location:

http://go.microsoft.com/fwlink/?linkid=54020

This spreadsheet includes

- Filename containing the GPO
- Scope (user versus machine)
- Policy path (where to find it)
- Policy setting name
- Version of OS supported by the GPO
- Explanation of the GPO
- Reboot requirements (if any)
- Logoff requirements (if any)
- Schema or Domain requirements

With this information, administrators can more easily plan for future GPOs to implement to conform new Vista systems to their corporate standards.

Further Understanding GPOs

Chapter 22, "Understanding Group Policy Basics to Manage Windows Vista Systems," touched on many of the rules and requirements around GPOs and their use in a domain environment. This chapter builds on the information presented there to give administrators a greater understanding of their uses and limitations.

Understanding the Order in Which Group Policies Are Applied

As mentioned previously, GPOs are applied in a specific order. Computers and users whose accounts are lower in the Directory tree can inherit Policies applied at different levels within the Active Directory tree. Group Policy is applied in the following order throughout the AD tree:

- Local Security Policy is applied first.
- Site GPOs are applied next.

- Domain GPOs are applied next.
- Organizational Unit (OU) GPOs are applied next.
- Nested OU GPOs and on down are applied next, until the OU at which the computer or user is a member is reached.

If a setting in a GPO is set to Not Configured in a policy higher up, the existing setting remains. However, if conflicts exist in configuration, the last GPO to be applied prevails. For example, if a conflict exists in a Site GPO and in an OU GPO, the settings configured in the OU GPO will "win."

If multiple GPOs are applied to a specific AD object, such as a site or OU, they are applied in reverse of the order they are listed. The last GPO is applied first, and therefore if conflicts exist, settings in higher GPOs override those in lower ones. For example, if a Contacts OU has the following three Group Policies applied to it and they appear in this order the policies will be applied from the bottom up:

- Contacts Default Group Policy
- Contacts Software Policy
- Contacts Temporary Policy

The Contacts Temporary Policy will be applied first. The Contacts Software Policy will apply next, and finally the Contacts Default Group Policy will be applied. Any settings in the Contacts Default Group Policy will override the settings configured in the two policies below, and the settings in the Contacts Software Policy will override any settings in the Contacts Temporary Policy.

Modifying Group Policy Inheritance

The Block Inheritance, Enforcement, and Link Enabled features allow control over the default inheritance rules.

GPOs can be configured to use the Enforcement feature. This setting does not allow the parent organizational unit to be overridden by the settings of the child OU if conflicts exist. Additionally, it nullifies the effects of Block Policy Inheritance if that functionality is applied on sub-GPOs.

OUs can be set to Block Policy Inheritance. This feature prevents the AD object that has the GPO applied to it from inheriting GPOs from its parent organizational unit, site, or domain (unless the parent GPO had Enforcement enabled as described previously).

To block Policy Inheritance on an OU, perform the following steps:

1. Launch the Group Policy Management console (GPMC) (Start, Run, **`gpmc.msc`**).
2. Expand the Forest container.
3. Expand the Domains container.
4. Browse to the OU to which you plan to Block Inheritance.
5. Right-click the OU and choose Block Inheritance.

The OU will now display a blue circle with a white exclamation mark to indicate that Policy Inheritance is blocked from this point down in the hierarchy (see Figure 23.1). This is to say, GPOs set above this point will not affect objects below the point of blocking. This behavior can be overwritten by setting a GPO to Enforced.

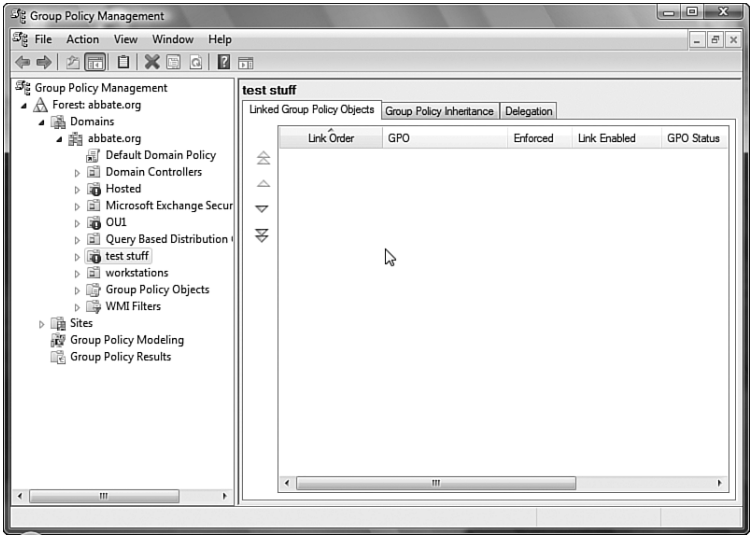

FIGURE 23.1
The OUs that are blocking inheritance display a blue circle with a white exclamation mark.

Finally, the option exists that allows for the disabling of a GPO, also known as the GPO's Link Enabled status. By right-clicking the Group Policy in the Group Policy Management console and unchecking Link Enabled, you can disable the policy and render it unused until the time it is reenabled.

Configuring Group Policy Loopback

Loopback allows Group Policy to be applied to the user logging in based on the location of the computer object, not the location of the user object in AD. Loopback applies a Group Policy based on the computer the user is using, not the user logging in to the computer. An example of a good use of the loopback option concerns Terminal Services. If you need to apply specific permissions to everyone who logs in to a particular Terminal Server, regardless of the user Group Policies, loopback in replace mode will accomplish this objective by ignoring all user GPOs. Loopback also provides a merge mode that merges the GPOs that apply to the user and computer but gives precedence to the computer GPOs, overriding any conflicting user GPOs.

The GPO setting for Group Policy Loopback processing is located under `Computer Configuration / Administrative Templates / System / Group Policy / User Group Policy loopback processing mode`.

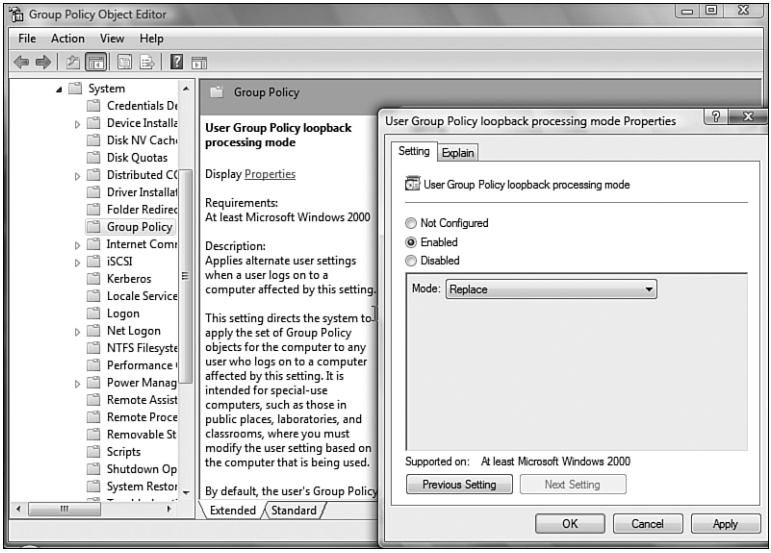

FIGURE 23.2
Selecting Group Policy Loopback mode.

Leveraging Local Policy

Local Policies can be used to enforce many of the same settings that GPOs can enforce. The advantage of the Local Policy is that it is enforced regardless

of whether the computer can contact a domain controller. This means that settings can be placed into the initially deployed image and will be in effect from the moment the computer is powered on.

One very useful way to use Local Policy is to essentially reverse the paradigm of GPOs when dealing with security-related settings. For example, suppose that you want to configure Vista workstations so that their users can't run the Registry Editor. In this example, we assume that we'd like the local help desk staff to be able to run the Registry editor. The two ways to do this are the following:

- **Option 1**—Block the capability to run Registry Editor via GPO. Link the GPO to the container holding typical users. Place help desk personnel in another container in Active Directory. Do not link the Registry Editor blocking GPO to those users.
- **Option 2**—Block the capability to run Registry Editor in Local Policy on the deployed Vista image. Create a GPO that enables running the Registry Editor. Link it to a container that holds help desk personnel.

Although at first glance the two options might seem equivalent, they are in fact somewhat different in their scopes. Imagine that Vista systems are being deployed to remote users. The system is built and shipped out to the end user. The user receives the computer and powers it on for the first time. If the user is on the network at this first boot, the GPO will be received and applied properly. If the system is not on the network, the domain GPOs cannot take effect. In Option 1, the remote user would be able to run the Registry Editor and make modifications to the system. In Option 2, the user would not be able to modify the system. In cases where the computer needs to be protected or modified prior to its first logon to the domain, Local Policy is a better option.

Local Policy can be accessed by performing the following steps:

1. Click Start.
2. Click All Programs.
3. Click Administrative Tools.
4. Click Local Security Policy (see Figure 23.3).

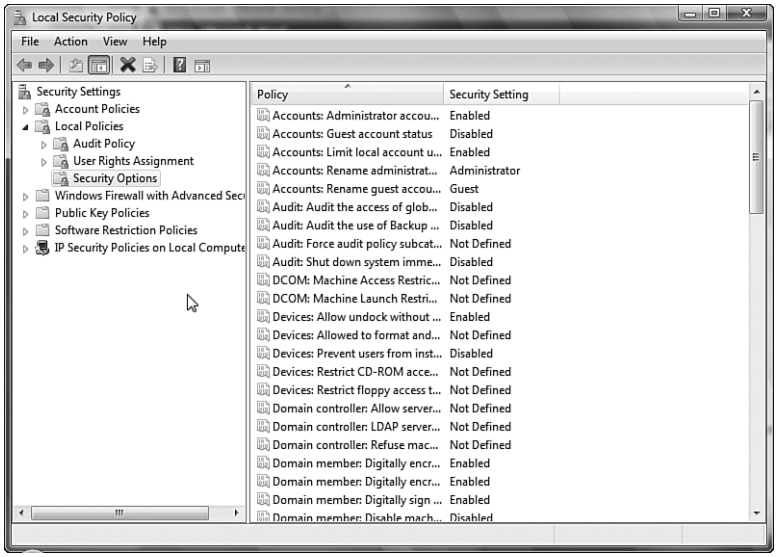

FIGURE 23.3
Viewing Local Security Policy.

Examples of Useful GPOs in Vista

Administrators who are relatively new to GPOs and Vista are likely wondering what GPOs other administrators are commonly configuring in their environments. This section will cover some of the more commonly used GPO settings and will walk you through the process of configuring them.

Example 1—Deployed Printers

One very common use of GPOs is to assign printers to users based on either group membership or the site they log in to. This allows an administrator to ensure that users have access to a local printer that is not only conveniently located, but is enabled for their use. This prevents calls to the help desk for printer assignments and allows users to easily roam from office to office without interruption to their productivity.

How to Configure Deployed Printers

To properly deploy printers via Group Policy, you should perform a few prerequisites. First, printers should be shared from a print server. This is done with the following steps:

1. From a print server, click Start, Settings, Printers and Faxes.
2. Click Add Printer.
3. When the wizard launches, click Next.
4. If you are going to host a networked printer (this is the most common scenario) choose Local Printer Attached to This Computer and click Next.
5. Choose Create a New Port and change the drop-down to read Standard TCP/IP Port. Click Next.
6. When the Printer Port Wizard launches, click Next.
7. Type the IP address of the networked printer (for example, 192.168.10.12). This will populate the Port name field for you. Click Next.
8. When the printer is contacted, click Next.
9. The Printer Port Wizard will display a summary of the port created. Click Finish.
10. In the left pane, choose the manufacturer of the printer. In the right pane, choose the model of printer. Click Next.
11. Type the name of the printer and click Next.
12. Choose Share Name and type the name you want to use for sharing this printer. This is the name that users will see. Click Next.
13. In the Location field, type a description of where the printer is located. This will help in cases where users want to "self-serve" a different printer. Type any necessary comments. Click Next.
14. Choose Yes to print a test page. This will enable you to ensure that the driver and print configuration are correct. Click Next.
15. Review the printer configuration and click Finish.

Now that network printers are available (assuming they didn't already exist) you can configure the Group Policy to deploy printers. From a Vista system, logged in with the rights necessary in the domain to create a GPO, perform the following steps:

1. Click Start, Run, and type **gpmc.msc**.
2. Expand Forest.
3. Expand Domains.
4. Expand the domain in which you will deploy the new GPO.
5. Expand Group Policy Objects.
6. Right-click and choose New.
7. Type a name for the new GPO and click OK.
8. Right-click the new GPO and choose Edit.
9. Expand Computer Configuration.
10. Expand Windows Settings.
11. Right-click Deployed Printers and choose Deploy Printer.
12. Click Browse, navigate to your print server, and click Select.
13. Click the printer you want to deploy and click Select.
14. Click Add to deploy the printer via GPO. You can add more than one printer. Click OK.
15. Close the GPO Editor.

In this example, we are deploying a printer for the accounting department in Building 4 (see Figure 23.4). As such, we will link the GPO to the site "Building 4" and filter the GPO by the accounting group. This will result in only the Accounting users in Building 4 getting this printer deployed.

We will perform this filtering with the following steps:

1. In the GPMC, expand Sites.
2. If your sites aren't present, right-click and choose Show Sites, select all, and click OK.
3. Right-click the site to which you want to link the Deploy Printers GPO and choose Link an Existing GPO.
4. Select the GPO from the list and click OK.

   At this point, systems located on the site to which the GPO is linked will attempt to process the GPO at startup.
5. Click the GPO linked to the site. You will receive a pop-up stating that you have selected a link rather than an actual GPO and that changes made here will affect the actual GPO. Click OK to accept this fact.

6. In the Security Filtering window, in the lower-right pane, you will see Authenticated Users listed. This is by default.
7. Click Authenticated Users and click Remove. Click Yes to confirm.
8. Click Add.
9. Type the name of the group you want to add. In this example, we'll add Accounting. Click Check Names and then click OK.

With this security filtering set, the GPO will apply only to accounting users located in the Building 4 site. Clever administrators can use this methodology to create multiple GPOs to account for all the sites and groups that they manage. In this way users can travel seamlessly between sites and get the printers that are most appropriate for their use.

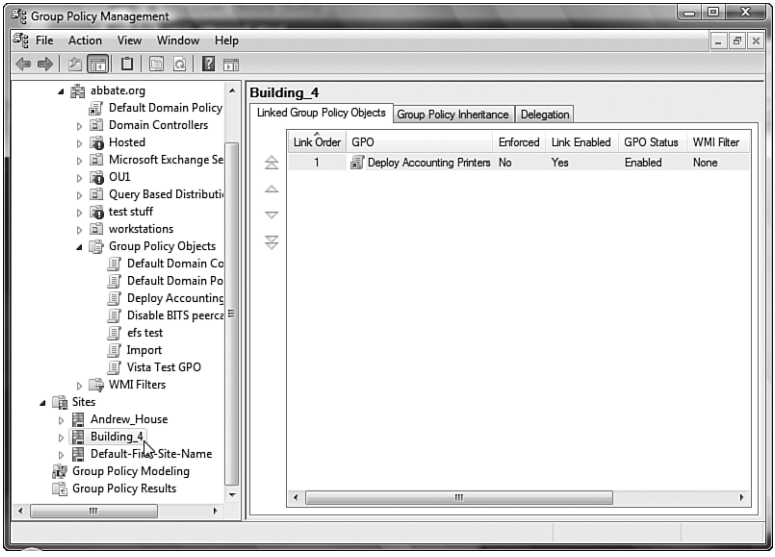

FIGURE 23.4
GPOs linked to Sites.

How to Test Whether a GPO Was Applied Correctly

Although most GPOs can be verified by simply checking the local settings to see if they've been applied, a more systematic method of testing is to query the workstation and see which GPOs it tried to apply.

Vista maintains an application that many administrators may already be familiar with, called `GPResult.exe`. By running `GPResult.exe`, the local system will report several things:

- Computer OU membership
- User OU membership
- Computer site membership
- Computer group memberships
- User group memberships
- Domain name and type
- Domain controller that provided the GPOs
- Applied Group Policies
- Filtered Group Policies

By reviewing this data, you can quickly determine which GPOs were applied and which were filtered. This allows you to quickly troubleshoot GPOs that were not applied. Often this tool will uncover issues with security filtering, inheritance blocking, or replication of GPOs between domain controllers.

Example 2—Standardizing Event Logging on Vista Clients

One of the great things that can be done with GPOs is the conforming of systems to a corporate standard. A good example of this is using a GPO to enforce logging settings on all systems of a particular type. Servers might get one set of settings, domain controllers another, and clients yet another. Setting this via GPO ensures that any system joining the domain will be conformed to the expected standard without anyone having to remember to set them.

How to Configure Event Logging

To deploy a GPO that enforces Event Logging settings, perform the following steps from a Vista system logged in with the necessary rights to create a GPO:

1. Click Start, Run, and type **`gpmc.msc`**.
2. Expand Forest.
3. Expand Domains.
4. Expand the domain in which you will deploy the new GPO.

5. Expand Group Policy Objects.
6. Right-click and choose New.
7. Type a name for the new GPO and click OK.
8. Right-click the new GPO and choose Edit.
9. Expand Computer Configuration.
10. Expand Administrative templates.
11. Expand Windows Components.
12. Expand Event Log Service.
13. Click Application.
14. In the right pane, double-click Maximum Log Size.
15. Select Enabled, enter a Maximum Log Size, and then click OK.
16. In the right pane, double-click Backup Log Automatically.
17. Select Enabled and click OK.
18. In the right pane, double-click Retain Old Events.
19. Select Enabled and click OK.
20. Repeat these steps for Security, Setup, and System.
21. Close the Group Policy Editor.

Now that the settings have been standardized in the GPO, it is necessary to attach the GPO to the objects that should receive these settings. In this example, we'll assume that these settings should be applied to all client workstations but not servers.

In our sample Active Directory is an OU for Managed_Computers, and all workstations have been placed under that container. An observant administrator might wonder why computers were not left in the default Computers container. The reason for this is that the Computers container is not an OU. This means that GPOs can't be linked directly to this container. One could apply the GPO to the domain level and therefore affect all computers but in this case, we only want to affect workstations and not servers or domain controllers. Although one could place the servers in a container where inheritance is blocked, it is simpler and cleaner to put the workstations into another OU, knowing that servers and domain controllers are likely going to receive a different GPO that conforms their Event Log settings.

With the GPO built, it is ready to link to put it into use. In this example, we'll assume that there are OUs below Managed_Computers where local

administrators have been delegated full control over their OUs. In our example, we'll also assume that the chief information security officer has stated that it is company policy to retain 50MB event log files and that when the logs fill, they should be backed up and retained. As such, it is necessary to ensure that local administrators cannot prevent these log settings from affecting their computers. This can be accomplished with the following steps:

1. Launch the GPMC (Start, Run, **gpmc.msc**).
2. Expand the Forest container.
3. Expand the Domains container.
4. Browse to the OU to which you plan to link the GPO.
5. Right-click the OU and choose Link an Existing GPO.
6. Choose the GPO you want and click OK.
7. Right-click the newly linked GPO in the right pane and select Enforced.
8. When prompted, click OK to change the Enforced setting.

By setting the GPO to Enforced, the GPO will ignore any Block Policy Inheritance settings on an OU in the hierarchy. Generally speaking, you should only use the Enforced flag in situations where a GPO is being used to directly enforce written IT policies.

Moving Policies Between Domains

In many situations it is useful to be able to take GPOs created in one domain and move them into another. Common scenarios for this would be in the case of a merger/acquisition or even something as simple as taking a GPO that was developed in an isolated task lab and moving it into production. You would initially expect that you'd have to print out the GPO settings and re-create the GPO from scratch with the same settings. Although this is a perfectly acceptable method of doing things, it becomes difficult and time consuming if a GPO contains a significant number of settings. In the case of needing to export or import a large GPO, the simpler solution is to use the import function that allows you to "rewrite" a backed-up GPO to reference objects in your domain. This rewrite is based on a migration table that is configurable by the administrator. Importing a GPO in this manner can be accomplished with the Group Policy Management console with the following steps:

1. Launch the GPMC (Start, Run, **gpmc.msc**).
2. Expand the Forest container.

3. Expand the Domains container and the domain containing the GPO.
4. Browse to the Group Policy Objects container.
5. Right-click the Group Policy Objects container and select Open Migration Table Editor.
6. In the table, input source objects, declare the object type, and enter the destination object (see Figure 23.5).

   For example, you might define groups from one domain and add the equivalent group from another domain as the destination. This would be helpful in GPOs where a group is being modified or granted specific rights on a system.

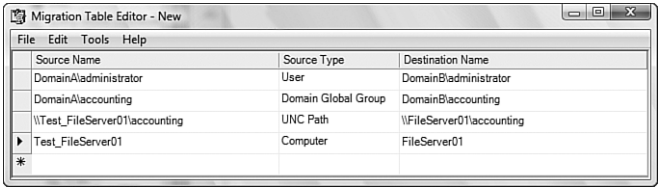

FIGURE 23.5
Populating the Migration Table Editor.

7. When the migration table is updated, click File, Save.
8. Enter a filename and click Save.
9. Close the editor.

Now that a translation table has been defined, a GPO can be imported. In the source domain, back up the GPO you want to migrate with the following steps:

1. Launch the GPMC (Start, Run, **`gpmc.msc`**).
2. Expand the Forest container.
3. Expand the Domains container.
4. Expand the Domain Object that holds the GPO you are interested in.
5. Expand Group Policy Objects.
6. Right-click the GPO in question and choose Back Up.

7. Browse to the location where you want to store the backed up GPO and enter a description. Click Back Up.
8. When the backup is completed, click OK.

Copy the backed up GPO to portable media and copy it to the system in the new domain that is running the GPMC.

To import the GPO, perform the following steps from the Group Policy Management console:

1. Launch the GPMC (Start, Run, **gpmc.msc**).
2. Expand the Forest container.
3. Expand the Domain container.
4. Expand the Domain Object that holds the GPO you are interested in.
5. Expand Group Policy Objects.
6. Right-click Group Policy Objects and select New.
7. Enter a name for the GPO that will receive the imported settings. Click OK.
8. Right-click the empty GPO that was created in step 6 and choose Import Settings.
9. The Import Wizard will launch. Click Next.
10. Because the GPO is empty, skip the backup step and click Next.
11. Browse to the location where the backup file from the other domain's GPO is stored. Click OK, then Next.
12. Select the GPO backup and click Next.
13. The Import Wizard will detect security principals and/or UNC (Universal Naming Convention) paths that are foreign. It will walk you through the translations. Click Next.
14. At the Migrating References Wizard, choose to use a migration table. Browse to the previously created migration table and click Next.
15. Review the summary and click Finish.
16. When the import succeeds, click OK.

By mastering the process of mapping security principals and UNC names and such between domains, you can quickly and easily move GPOs back and forth between multiple domains for testing and deployment purposes.

Recommended Practices with Group Policy

If you plan to use GPOs in your environment, you should develop several habits that are useful for reducing the possibilities of negatively impacting the user community when testing and deploying GPOs.

GPO Pilot OU

When linking a GPO in production, it is very helpful to initially limit the scope of who will be affected by it. Although GPOs should always be tested extensively in an isolated lab environment, in many cases a GPO can't be fully tested without access to all the production objects in Active Directory. For example, a GPO might include scripts that map network drives. It might create database connectors or even redirect the user's Documents directory to a file share. Unless all the systems involved were available in the lab, the GPO could not be fully tested. In this case, you will want to apply the GPO to a beta testing group in production first before linking it to a larger group.

The best way to handle this is to create an OU in the production Active Directory where new GPOs will be initially linked and tested. Create dedicated test accounts in addition to test workstations running the operating systems that you support in production. Utilizing Microsoft Virtual PC is an excellent way to deploy multiple operating systems into this testing OU without tying up a lot of resources. After you're comfortable with the results in production, you should then link the GPOs to the OUs they were intended to serve.

Isolating Critical Accounts

Another good habit for administrators is placing critical accounts into an OU that is filtered from receiving Group Policies. This would include accounts such as service accounts and administrative-level accounts. The goal here is to ensure that GPOs can't negatively affect the accounts that would be used to undo the negative effects.

Respecting OU Administrators

Linking a GPO can have far-reaching consequences for users. This is especially true when a GPO is linked near the top of an OU hierarchy or even at the domain level. In these situations, GPOs may affect users in OUs that are controlled by other groups or other administrators.

One of the most common OU structures in Active Directory is loosely based on geography. In these cases, different locations are separated out into OUs, and local administrative staff is delegated control. In these environments,

it's critical to properly communicate the implications of GPOs to those other administrators and make sure they are okay with the new GPO.

The simplest way to pass the information to others is in the form of an HTML file. HTML, or Hypertext Markup Language, can be easily viewed from a web browser and is natively supported by the GPMC.

You can export the settings from a GPO into an XML file with the following steps:

1. Launch the GPMC (Start, Run, **`gpmc.msc`**).
2. Expand the Forest container.
3. Expand the Domains container.
4. Expand the Domain Object that holds the GPO you are interested in.
5. Expand Group Policy Objects.
6. Right-click the GPO you want to export a summary for and choose Save Report.
7. Enter a name for the file and save it in HTML format. (XML is also an option.)
8. Browse to the location where you want to save the file and click Save.

This HTML file can be placed on a commonly accessible web server to act as a quick reference for administrators who want to see what GPOs are currently in place in the environment. Newly proposed GPOs can be placed there as well to give OU administrators a place to look at new settings and give them an opportunity to either authorize or deny the changes before they are placed into production.

Leveraging Other People's Work

As you use GPOs more and more, you will likely make the discovery that your needs are really not that different from other companies', and odds are that most everything you are planning to implement via GPO has been done before by someone else. Rather than always reinventing the wheel, look around to see if the GPO you are considering has already been created by someone else.

A good example is the set of common scenario GPOs that have already been created by Microsoft. Many companies find themselves in need of computers that act as common workstations that might be used by people who aren't necessarily employees. Or perhaps they need a computer on a manufacturing

floor that can be used for only one or two specific applications. Rather than researching all the settings necessary to create a kiosk-type machine, you can start with the work that someone else has already done.

Microsoft has published several such GPOs at the following location:

http://technet2.microsoft.com/windowsserver/en/library/9a758138-d9c0-49bd-ae57-14fb9b6decbe1033.mspx?mfr=true

This page contains descriptions of several common desktop configuration scenarios as well as the GPOs that enforce the settings. Although these scenarios might not be a 100% match for what a particular administrator needs, they nonetheless provide excellent starting points where settings can be tweaked rather than created from scratch.

Summary

This chapter has built on the information presented in Chapter 22 to help administrators further understand how to implement and manage Group Policy Objects in order to make the management of Vista systems easier. It has also offered advice on how to manage users and computers to ensure that GPO manipulation can't accidentally cause problems in the enterprise.

Administrators should take the opportunity to get more familiar and confident with GPOs in a lab environment and use the processes given in this chapter to implement the GPOs into production with minimal impact to the domain.