CHAPTER 22

Understanding Group Policy Basics to Manage Windows Vista Systems

What Are Group Policy Objects (GPOs)?

Group Policy describes the Microsoft implementation of a methodology of managing computers and users in a centralized fashion in an Active Directory environment. Group Policy Objects (GPOs) are the collections of various application and Registry settings that have been defined by an administrator to enforce a particular behavior on a user or computer object.

This concept was initially introduced back in the Windows NT 4.0 days when an administrator was able to use Policy Enforcement to force a workstation to conform to particular behaviors. This was usually limited to restricting a user's local rights to prevent the user from changing things like the UI or locally installed applications. It was initially a clunky way of doing things, but it set the stage for the introduction of Group Policy Objects in Windows 2000 with the advent of Active Directory (AD). In Windows 2000, administrators were given the capability to easily configure hundreds of common settings in the area of application publishing to security settings to Internet Explorer settings. This was done through a provided editor that utilized ADM files that contained definitions for the user and computer objects to interpret. The drawback to these ADM files was that the format was somewhat cryptic, and it made it difficult for administrators to create their own ADM files for modifying custom applications or to modify

applications for which Microsoft had not yet released ADM files. This situation didn't change much with the release of Windows 2003, but it did introduce a new tool called the Group Policy Management console. This tool allowed administrators to more easily view and manage Group Policy Objects as well as to back them up and even port them from one domain to another. It was not until the release of Vista that Microsoft fundamentally changed the way that GPO settings were stored. With Vista came the new ADMX format of files. ADMX is based on XML, or Extensible Markup Language. XML is an open standard for data formatting that is meant to put data into a more human-friendly format. The result is that ADMX files are much easier to create than their ADM predecessors.

Why Administrators Should Use Group Policy Objects

GPOs are designed as a way to globally modify user and computer settings through a controllable and manageable central interface. This is to say, GPOs are meant to replace manual intervention on systems and custom logon scripts.

Take, for example, the implementation of a new web proxy server in an environment. In the old days, you would either go from system to system, logging in as the user and setting the Proxy configuration in Internet Explorer, or if you were adept at scripting, you might write a custom script that would modify the Proxy settings and set it to run in the user's logon script. This situation is very easily handled by GPO. In fact, it can be done with much greater granularity with a GPO. Imagine that in our example there are multiple Proxy servers, and the goal is for users to use the Proxy server that is closest to them. Although this could be accomplished manually, it wouldn't account for users who travel. If a user in the United States was configured to use the Proxy in the U.S., it would result in poor performance if the user were to visit an office in Japan that had a local Proxy server. If the user was well versed in scripting, he or she might be able to write a subroutine that was "location aware" and modify the Proxy settings when the system was in another location, but that would really be reinventing the wheel. If the administrator used Group Policy, the administrator could create a GPO for each Proxy server and link the GPOs to the sites defined in AD. This would result in systems using the closest Proxy server no matter where they were. The term *linking* in this context refers to tying an Organizational Unit (OU) or a site to a particular OU so that only objects in that site or OU

will attempt to use the GPO. This will be explained in further depth later in this chapter.

As you can see from the preceding example, GPOs should be used in situations where an administrator wants to push a setting or configuration to multiple systems and needs the flexibility to limit which systems or users receive the settings.

GPOs are also extremely useful for enforcing the rules of an environment. For example, if a company changed its policy to require computers to be locked after a period of inactivity, this setting could easily be configured via GPO. Although many companies may configure a setting like this when deploying a system, the advantage to doing it by GPO is that no one can "forget" to make the setting. As soon as a computer is joined to the domain, it will inherit the domain-level GPOs and automatically conform the system to your rules.

How to Configure GPOs

GPOs are created in a central manner and are stored on all domain controllers in a forest. GPOs can be accessed via Active Directory Users and Computers:

1. Click Start.
2. Click All Programs.
3. Select Administrative Tools.
4. Pick Active Directory Users and Computers.
5. Expand to an OU.
6. Right-click and choose Properties.
7. Select the Group Policy tab. If you have the GPMC loaded, it will prompt you to open it.

GPOs can also be accessed through the Group Policy Management console:

1. Click Start, Run, type **`gpmc.msc`**, and then press Enter. If Run is not available from the Start menu, it can be accessed by pressing the Windows and R keys at the same time.

The Group Policy Management Console is preinstalled on Vista.

Introducing the Group Policy Management Console (GPMC)

The release of the GPMC provided huge improvements in the creation and management of GPOs. Prior to the GPMC, an administrator had to open each GPO in the editor and examine all possible settings to determine which settings had been changed from the defaults. In the GPMC, you can view all the unique settings of a given GPO via 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. Left-click the GPO in question.
7. Click the Settings tab in the right pane.

GPMC will show Generating Report and then the containers that are modified. Click Show All to see all settings contained in the GPO, as shown in Figure 22.1.

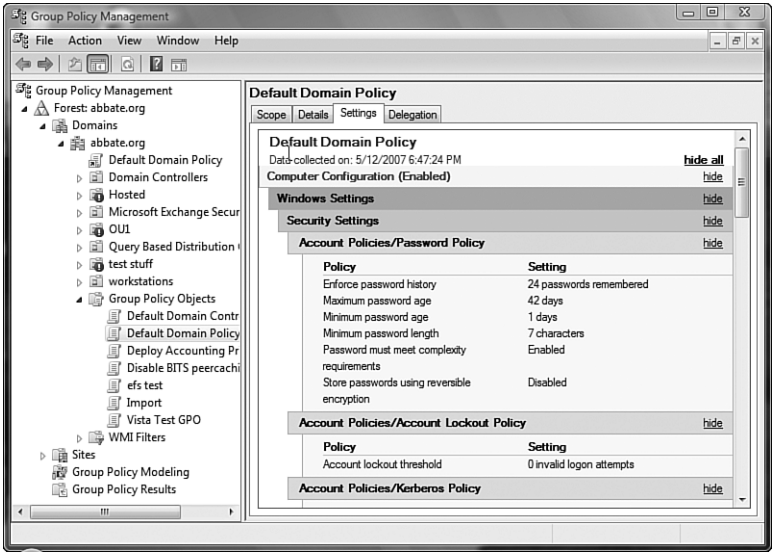

FIGURE 22.1
GPO settings in the Group Policy Management console.

The GPMC is also useful for backing up and restoring GPOs. This should be used whenever a GPO is to be modified. This way, if the GPO causes unwanted issues, an administrator can restore the previous version of the GPO to return systems to their previous configuration. To back up a GPO with the GPMC, follow these 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 Backup.
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.

To restore a GPO with the GPMC, follow these 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 Restore from Backup.
7. When the wizard launches, click Next.
8. Browse to the location of the backup and click Next.
9. Choose the backup you want to restore (Note: this is where entering a description was helpful) and click Next.
10. Click Finish and the restore will begin.
11. When the restore has completed successfully, click OK.

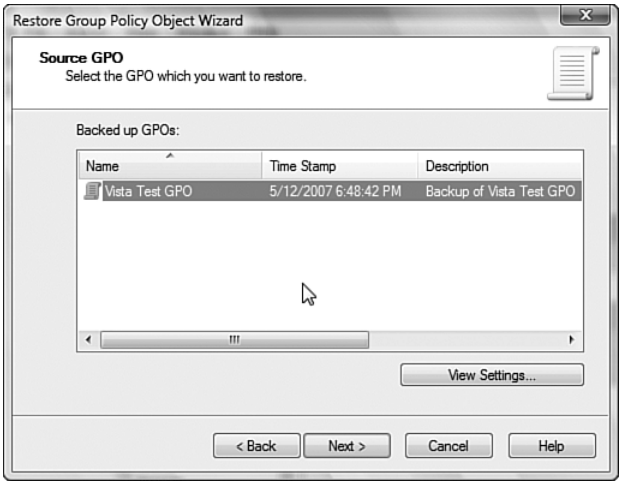

FIGURE 22.2
Selecting the backup to restore.

Creating a New GPO in the GPMC

The GPMC is the logical place to create new GPOs. Generally speaking, the creation of a GPO should coincide with the desire to automate some specific configuration across multiple machines. This means that the person creating the GPO should already know what settings to assign to a given GPO.

To create a new GPO, follow these steps:

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. Right-click Group Policy Objects and choose New.
6. Enter the name of the GPO you want to create (use a descriptive name) and click OK.

This will create a new, empty GPO in the management console.

To modify settings within the GPO, you need to use the GPO Editor. Right-clicking the new GPO and choosing Edit will launch the GPO Editor.

Using the GPO Editor

The GPO Editor that is triggered via the GPMC is the same editor originally used since Windows 2000. Not much has changed. The editor expresses the GPO in two sections, Computer and User settings, as shown in Figure 22.3. Although an administrator can set both user and computer settings in the same GPO, it is considered a best practice to limit a given GPO to either User or Computer settings. This is related to the way GPOs are linked and is discussed in more detail later in this chapter.

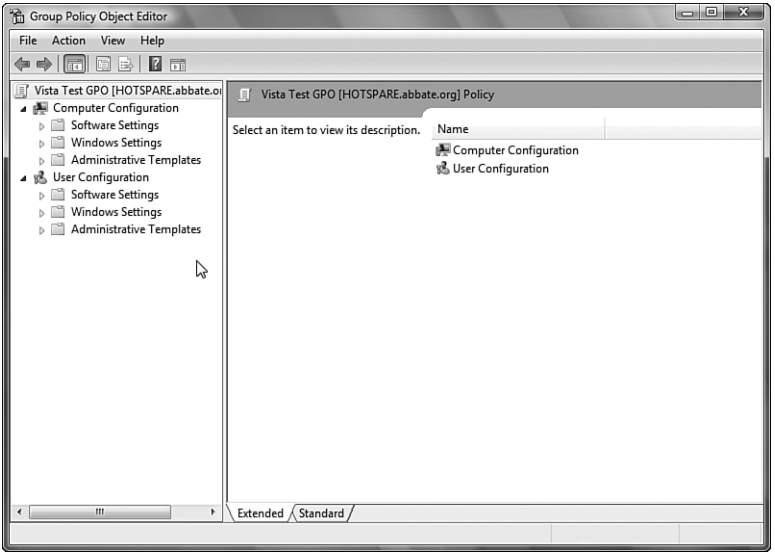

FIGURE 22.3
The Group Policy Object Editor.

The editor allows the administrator to browse through the available configuration settings in a graphic format. For example, you could expand User Configuration, Administrative Templates, System, and Windows HotStart to have the ability to turn off Windows HotStart. Because this is a new GPO setting, you might wonder what Windows HotStart is. By selecting Turn Off Windows HotStart, you will see that an explanation of the setting has appeared to the left of the setting. To save space in the window, you could click the Standard tab at the bottom of the screen. To get the explanation back, click the tab labeled Extended.

What's New in GPOs?

With the release of Vista, Microsoft has added several new areas that can be managed via GPOs and has expanded several existing areas. These areas include the following:

- Antivirus
- Background Intelligent Transfer Service (BITS)
- Client Help
- Deployed Printer Connections
- Device Installation
- Disk Failure Diagnostic
- DVD Video Burning
- Enterprise Quality of Service (QoS)
- Hybrid Hard Disk
- Internet Explorer 7
- Networking: Quarantine
- Networking: Wired Wireless
- Power Management
- Removable Storage
- Security Protection
- Shell Application Management
- Shell First Experience, Logon, and Privileges
- Shell Sharing, Sync, and Roaming
- Shell Visuals
- Tablet PC
- Terminal Services
- Troubleshooting and Diagnostics
- User Account Protection
- Windows Error Reporting

With these new areas available, administrators are able to continue to manage functions and settings on the client workstations to reduce overall administrative efforts.

ADMX Format

Vista brings with it a new format for storing GPO-related information. Whereas in the past, GPOs were built with `.adm` files that stored the individual configuration objects, Vista uses a new `.admx` format. The new format allows for language-neutral as well as language-specific resources. This allows the various Group Policy tools to adjust their operating system to the administrator's configured language. The net result of this is that an administrator in the United States can create a GPO and a colleague in France can review the same GPO, but the colleague will see it in French.

The new `.admx` files are based on XML. This makes it easier for developers to integrate GPO information into their applications.

An observant administrator will notice that the available settings are different when viewed from Vista in contrast to viewing via a Windows 2003 domain controller. This is because Vista is able to see the settings available from the new `.admx` entries.

Network Location Awareness (NLA)

Network Location Awareness (NLA) is a mechanism that improves the ability of Group Policy to deal with changes in network conditions. NLA allows Group Policy to utilize event notification and resource detection within Vista to become aware of events, such as leaving standby or hibernation or the establishment of a VPN connection. Even an event such as connecting to a wireless network can be detected to trigger processing of GPOs.

Some of the major benefits of NLA include the following:

- **More efficient startup times**—NLA will allow Group Policy to determine the state of the network connection, resulting in a reduction of timeouts while waiting for a connection to a domain controller. NLA will accurately determine whether a network card is enabled or disabled and will use this information to determine whether to try to contact a domain controller to download a GPO.
- **NLA allows a client to apply a policy when a connection to a domain controller is restored**—This is especially helpful in the case of wireless network connections that require user interaction or in the case of Virtual Private Network connections where connection to a domain controller doesn't occur until after the login event has been processed. This same behavior will occur when a client exits hibernation or standby. The benefit here is that if the refresh period of the GPO has expired, the client will immediately attempt to download and

process GPOs as soon as connectivity to a domain controller is restored. This will improve overall system protection because there is no delay in processing new settings.

- **NLA also removes the dependency on ICMP (Ping) for determining available bandwidth when determining whether to process GPOs**—This allows administrators to further protect clients by blocking ICMP in the local firewall without breaking GPO functionality.

How to Manage GPOs

As you can likely tell from this chapter, GPOs are an extremely useful and powerful way to manage workstations in a domain. Like most utilities that are powerful, it is easy to cause problems for yourself if you don't manage the process well. Knowing how GPOs work, where the components are stored, and what you need to do to utilize them are the key pieces to making GPOs work for you.

Where Are GPOs Stored?

For GPOs to be useful across the forest, the GPOs must be available to users and computers. The way in which Active Directory deals with this is to store the GPOs in the SYSVOL volume that is replicated across all domain controllers in the forest. Specifically, the files are stored in `\\Domain\sysvol\domain\policies`.

They will appear in directories with names like {162EBD2C-FAAC-4852-8B28-FB2D4ABA1CD5}, as shown in Figure 22.4. Contained in these directories is a configuration file (`gpt.ini`) as well as subfolders for the Machine and User settings.

New to Vista and Windows 2008 is an additional directory under Policies called PolicyDefinitions. This directory contains the new ADMX files that are used by Vista and Windows 2008. This directory is referenced by new GPOs that contain Vista or Windows 2008 settings.

If the directory for a newly created GPO does not appear on remote DCs within 15–30 minutes, you should suspect that there may be issues with the File Replication Service on one domain controller or more.

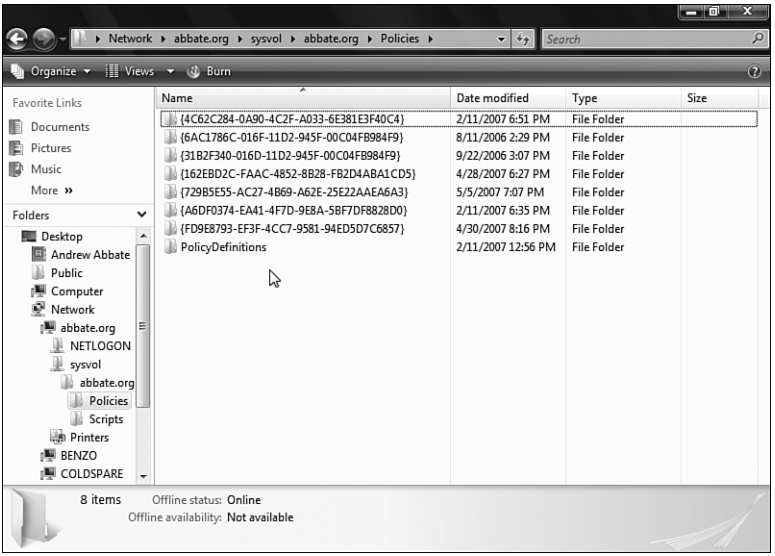

FIGURE 22.4
Group Policy Object directories.

How GPOs Replicate Throughout the Domain

Because GPOs are stored in the SYSVOL volume of domain controllers, they are automatically replicated to all domain controllers in the domain through the File Replication Service (FRS). It is very important that FRS be operating successfully to ensure that all users in the domain are getting consistent settings via GPOs. If a domain controller is having FRS issues, it may not become aware of changes to a given GPO. This will result in some systems not getting the correct version of the GPO. This can be a major issue if GPOs are being used to configure important security settings or to apply patches or hotfixes to workstations.

A very simple way to verify the health of FRS is to place a text file in the SYSVOL directory of a domain controller and check the SYSVOL directory of other domain controllers to ensure that the new file appears within the expected replication intervals.

Keeping an eye on the FRS section of the event viewer of domain controllers is another easy way to become aware of FRS problems. If you want to keep a more watchful eye for potential FRS problems, Microsoft has a tool called

SONAR, available at www.microsoft.com/downloads/details.aspx?FamilyID=158cb0fb-fe09-477c-8148-25ae02cf15d8&DisplayLang=en that will allow you to keep closer tabs on FRS performance.

How to Link a GPO to an OU

After a GPO has been created, it needs to be linked to an OU or site to actually do anything. Interesting to note is that the User and Computer containers in Active Directory are not actually OUs and thus can't be used as a link point for a GPO.

The concept of linking a GPO is that the GPO is effectively being assigned to objects contained in or under the OU to which it is linked. This is traditionally the largest point of confusion to administrators. As mentioned previously in this chapter, GPOs are separated out into two sections: Computer and User settings. When a GPO with both Computer and User settings is linked to an OU, there are two potential things that can occur. If a user object is in or below the OU where the GPO is linked, the User settings will be applied (assuming the user has permissions to apply the GPO). Similarly, if a computer object is in or under the OU where the GPO is linked, it will attempt to apply the Computer settings (if the computer has permission to apply the GPO).

The common mistake made by administrators is assuming that both User and Computer settings will get applied if *either* the user or computer object is in or under the linked OU. This is an incorrect assumption.

In some situations, it may be very desirable to apply both Computer and User settings when a user logs on to a specific computer. A classic example of this is when a user is logging on to a Terminal Server. It may be useful to apply User settings when the user is on the Terminal Server that wouldn't be desired when the user logs in to their normal workstation. This is where the concept of *loopback processing* comes into play. Loopback processing is a Computer GPO setting that will effectively apply User settings based on the computer object being in a linked OU when the user object isn't. The two options are to append the User settings to existing inherited user GPOs or to replace the existing GPOs.

To link an existing GPO to an OU, perform 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 and Existing GPO.
6. Choose the GPO you want and click OK.

The domain and OU view in GPMC is an excellent way to quickly tell what GPOs are being applied to what containers, as shown in Figure 22.5.

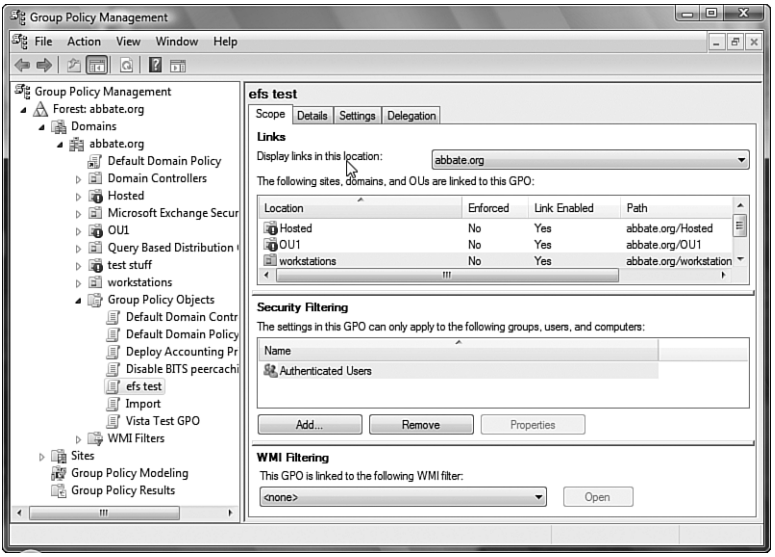

FIGURE 22.5
Viewing OUs to which GPOs are linked.

How to Control Who Can Modify a GPO

After a GPO has been created, an administrator can control who is allowed to edit an existing GPO. This can be helpful in environments where the creation of GPOs is a centralized and controlled event but where a local OU Admin might be empowered to make modifications to existing GPOs. To alter the rights on a GPO to allow for editing, perform 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 Group Policy container.
5. Highlight the GPO you want to alter permissions on.
6. In the right pane, click the Delegation tab.
7. Click Add and type the name of the user or group to which you want to delegate rights.
8. Click Check Names and then click OK.
9. In the Permissions drop-down list, choose Edit and click OK.

Now the person or group that was delegated is able to edit the existing GPO but is not able to alter the permissions on it.

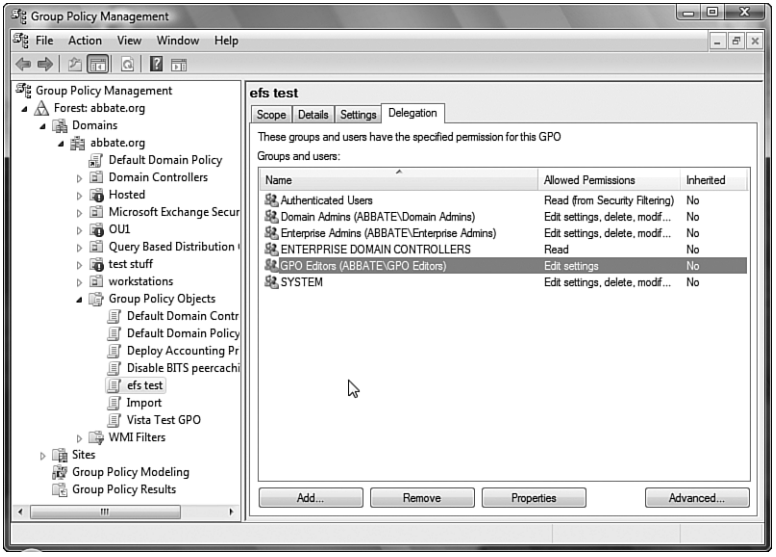

FIGURE 22.6
Viewing security delegations.

How to Limit Who Can Apply a GPO

Typically, the role of GPO administrator is limited to a particular subset of administrators in Active Directory. This minimizes the potential for an administrator to make an unauthorized change that could potentially impact all users in the domain.

A best practice is to separate out the two key roles of Group Policy: creation and application. One group should have the capability to create GPOs but should not have the rights to link them to any containers. Another group should have the capability to link but not create. This creates a situation where no one person has the capability to place new GPOs into production. To delegate these rights, perform the following steps on a domain controller:

1. Click Start.
2. Click All Programs.
3. Click Administrative Tools.
4. Click Active Directory Users and Computers.
5. Click View and then click Advanced Features.
6. Right-click the domain object and select Delegate Control; then click Next.
7. Click Add and type in the name of the group to which you are delegating the capability to link GPOs.
8. Click OK twice and you should see the group you added. Click Next.
9. Check the box for Manage Group Policy Links and click Next.
10. Click Finish.

To control who can create GPOs, follow these steps:

1. Click Start, Run, and type **`gpmc.msc`**.
2. Expand Forest.
3. Expand Domains.
4. Expand the domain you are managing.
5. Highlight Group Policy Objects.
6. Select the Delegation tab in the right pane.

This shows the groups and users that are currently able to create GPOs in the domain.

To delegate a new group to be able to link GPOs, perform the following additional steps:

1. Click Add.
2. Type the name of the group you want to add and click Check Names.
3. Click OK.

How to Filter a GPO

In many cases, an administrator might want to apply a GPO to most users or computers but exclude specific groups. Although this can be done by controlling where the GPO is applied in the OU structure, sometimes this would require too much granularity in the OU structure. In these cases, you can use GPO filtering to prevent specific groups of objects (users or computers) from applying the GPO. This is called *GPO filtering*.

Imagine, for example, that you create a GPO that will enable a screensaver with a password after 60 seconds of inactivity. Although this might be great for security, it can really bug an executive who is trying to do a PowerPoint presentation that requires a lot of talking. In this situation, it might be worthwhile to filter the presenter from the GPO. To accomplish this task, perform the following steps from a domain controller:

1. Click Start, Run, and type **`gpmc.msc`**.
2. Expand Forest.
3. Expand Domains.
4. Expand the domain you are managing.
5. Highlight Group Policy Objects.
6. Right-click the GPO in question and click Scope.
7. Add the group you want to filter and change the permissions to Apply GPO—Deny.

Blocking Inheritance

In most OU structures, there is a container for protected objects that in many cases should not have GPOs applied to them. This might include administrator accounts, validated computer systems, or even service accounts. The safest way to protect these accounts from accidental changes via GPO is to place them in an OU that is blocking inheritance. This is to say that even though a GPO might be applied to a container that is above the protected container in the OU hierarchy, the GPO will still be blocked.

To set blocking on an OU, from a domain controller follow these steps:

1. Click Start.
2. Click All Programs.
3. Click Administrative Tools.
4. Chose Active Directory Users and Computers.

5. Click View and then click Advanced Features.
6. Right-click the OU you want to set inheritance blocking on and select Properties.
7. Click the Group Policy tab.
8. Check the box for Block Policy Inheritance and click OK.

Important to note is that if a GPO exists at a higher level in the hierarchy, the blocked inheritance is set to Enforce. This setting will trump the inheritance block and will be applied anyway.

Troubleshooting GPOs

Although GPOs generally work very well in Active Directory environments, occasionally administrators will encounter issues when working with GPOs. If this should occur, there are several client and server side tools that can be used to determine the issue that is preventing a given GPO from applying properly.

Using the Resultant Set of Policies Tool

Resultant Set of Policies (RSoP) is part of the GPMC that provides a GUI interface that enables you to test a policy implementation prior to rolling it out in production and also enables you to view what policies a user or computer is actually receiving. The RSoP allows an administrator to pick a computer and user object and determine which GPOs would get applied. This allows an administrator to model the results without needing access to the user or the user's computer.

Group Policy Modeling Using RSoP

RSoP Planning mode enables you to simulate the deployment of a specified Group Policy, check the results, change, and then test the deployment again. This is very helpful in a lab environment where you can create and test a new set of policies. After RSoP shows that the GPO is correct, you can then use the backup functionality to back up the GPO configuration and import it into production.

To run RSoP in simulation mode, right-click Group Policy Modeling in the forest that will be simulated, and choose Group Policy Modeling Wizard. The wizard allows for inputting the possibility of slow links, loopback configuration, and WMI filters as well as other configuration choices. Each modeling is presented in its own report as a subnode under the Group Policy Modeling mode.

Using RSoP Logging Mode to Discover Applied Policies

RSoP in Logging mode enables you to view what exact policies a user or computer might be receiving. It shows in a readable format what polices are enforced, where conflicts exist, and what different policies are being applied to the user/computer. It can be run either on the local computer or on a remote computer by choosing the proper options in the wizard. To run RSoP in Logging mode, right-click Group Policy Results in the GPMC, and then click the Group Policy Modeling Wizard selection and follow the wizard that appears.

Using GPResult

One of the most common questions in GPO troubleshooting is, "How do I know it even tried to apply my GPO?" This is a very easy thing to test, and it tends to provide a lot of interesting information. Vista workstations have a utility available called GPResult. To run this, open a command prompt, type **`gpresult`**, and press Enter.

The utility will determine what groups the user and the computer belong to, and it will show you what GPOs it found linked to the OU hierarchy. It will point out GPOs that were skipped because of security filtering, and it will show you which ones were applied. It will even go so far as to tell you what OU your user and computer objects are in. This can be very helpful in determine why a GPO was or was not applied.

Using GPUpdate

Another helpful tool for testing out GPOs is the GPUpdate utility. This will trigger a download and application of GPOs outside of the normal GPO processing schedule.

You can limit the tool to only request updates to user or computer GPOs by using:

```
Gpupdate /target:computer
```

or

```
Gpupdate /target:user
```

You can force the system to immediately apply changes by using

```
Gpupdate /force
```

And you can even use `Gpupdate /sync` to include a reboot of the system to process GPO settings that occur only on system startup.

Best Practices in Working with GPOs

GPOs can be very powerful when used correctly, and they can also be very dangerous when used incorrectly. Many tricks can be employed to improve overall management and application of GPOs, ranging from ways to make GPOs faster to process to ways to more easily roll back mistakes with GPOs.

Speeding Up GPO Processing

To speed up login and boot times for users, it is recommended that if the entire User Configuration or Computer Configuration section is not being used in a GPO, the unused section should be disabled for the GPO. This expedites the user logon time or the computer boot time because the disabled sections aren't parsed on boot or login.

To disable configuration settings using Active Directory Users and Computers, follow these steps:

1. Right-click a Group Policy.
2. Click Properties.
3. Go to the General tab.
4. Click one of the boxes, either Disable Computer Configuration Settings or Disable User Configuration Settings, whichever section is not being utilized.

To disable configuration settings using the GPMC, follow these steps:

1. Click the Group Policy in GPMC.
2. Click the Details tab.
3. Click the drop-down box at the bottom of the Details tab.
4. Choose Computer Configuration Settings Disabled or User Configuration Settings Disabled, depending on which portion needs to be disabled.

Reusing Basic GPOs

If a Group Policy will be applied to many locations, you should create the policy once, assign the permissions, and then link the policy to the other locations rather than creating the policy multiple times. Linking the policies achieves the following objectives:

- **Creates fewer group policies in SYSVOL**—This allows for quicker domain controller promotion and less replication traffic.

- **A single point of change for the GPO**—If the GPO is changed, the change is applied to all the locations where the GPO is linked.
- **A single point of change for permissions**—When permissions are configured or changed in one location on a linked GPO, the permissions are applied universally to each place where the GPO is linked.

Understanding Inheritance

Group Policy objects 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.
- 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 there are conflicts 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 (as shown in Figure 22.7) 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.

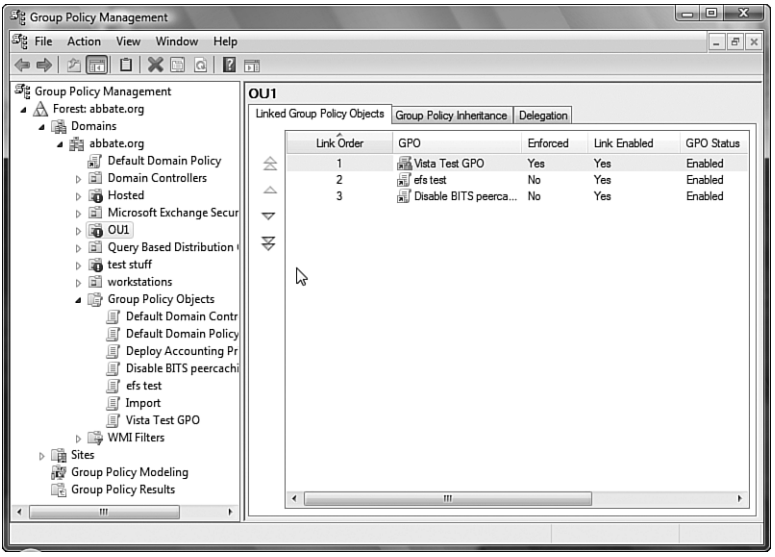

FIGURE 22.7
Group Policy objects are applied in order.

Where to Link GPOs

Administrators will quickly find that it can be very confusing to determine what GPOs are applied to a given user or computer and which aren't. One way to reduce this confusion is to try to eliminate questions of security filtering and policy inheritance overwrite whenever possible. This is to say that in many cases, it's best to push the application of a GPO as far down the hierarchy as is possible. This may result in the same GPO being linked to multiple locations.

Utilizing WMI Filtering

Linking WMI Filters enables you to apply group policies and establish their scopes based on attributes of target computers. You can do this by using the WMI filters to query the WMI settings of the target computers for true/false and apply group policies based on the true/false WMI queries. A "false" on the target computer results in the GPO not being applied. Conversely, a "true" results in the application of the GPO.

Because WMI filters are separate from GPOs, they must be linked to GPOs in the GPO Scope tab to function properly. Only one WMI filter can be

applied to each GPO. Additionally, WMI filters will work only on Windows XP and later workstations, not Windows 2000 or before, or non-Microsoft operating systems.

Rolling Back Bad Ideas

Most administrators will experience a bad idea GPO at least once in their career. Sometimes settings that seem innocuous will cause problems, or perhaps an administrator will try to save time and link a GPO that hasn't been fully tested. In these cases it's necessary to quickly revert to an older version of a GPO. Unfortunately, there isn't a native method for rolling back a GPO; however, a few simple administrative tasks can allow for a quick restore to a known good GPO.

The key to being able to quickly revert from a bad GPO is to ensure that GPOs are always backed up and that they are always given a descriptive name.

Let's take as an example a GPO that we'll call Disable BITS Peercaching. It has a simple setting that disables BITS Peercaching. We've followed our first rule and given the GPO a descriptive name. We'll back up this GPO with the following steps:

1. From within GPMC, right-click the GPO and select Back Up.
2. Click Browse and choose the location where you will store your GPOs.
3. Enter a description that explains the last set of changes and the date that it was saved; click Back Up.
4. When the backup is completed, click OK.

Now imagine that an administrator has modified this GPO to include some settings that are incorrect or that are causing problems. It is very possible that the contents of the original GPO have been forgotten. You can revert to the old version of the GPO by doing the following:

1. Select the GPO you want to revert, right-click, and choose Restore from Backup.
2. The Restore Group Policy Object Wizard will launch. Click Next.
3. Click Browse and navigate to the location where the GPOs are saved. Click Next.
4. In this screen, you will see all GPOs that have been backed up with a description and a time stamp. Select the version of the GPO you want to restore and click Next.

Note

You can use the View Settings button when highlighting a backed up GPO to review the settings of that GPO in an XML format. This can be helpful if you just want to see what the old version of the GPO was and not actually restore it.

5. Review the summary information and click Finish.
6. When the GPO has successfully restored, click OK.

Because the GPO is restored on the Domain Controller that currently has focus within the Group Policy Management console, it may take a short while for the restored GPO to replicate to all domain controllers in the domain.

Summary

As we've seen, Vista has brought with it many changes to the available GPO settings as well as to the way in which they are stored and managed. We've seen the necessity of carefully managing and maintaining GPOs and have discussed ways to troubleshoot GPOs should any problems occur.

Always remember to carefully delegate who can create GPOs and who can link them. This will make it much less likely that you ever deploy a GPO that can cause problems for your users. Always try to do a peer review of a GPO before it's linked, and always first link it to a test OU to make sure it has no unintended effects.

Keep these things in mind, and GPOs will help you more easily maintain your Vista community.