Realtime
publishers
"Leading the Conversation"

The Definitive Guide™ To

Building a Windows Server 2008 Infrastructure

sponsored by

triCerat

Greg Shields

Chapter 6: Managing & Customizing Group Policy..130
The Benefits of Centralized Management with Group Policy...131
Navigating the GPMC...132
Creating a Simple GPO...133
Applying That Simple GPO..136
Applying Multiple GPOs..136
Administrative Templates and the Group Policy Central Store...137
Network Location Awareness..140
Starter GPOs...141
GPO and GPO Settings Comments..143
GPO Filters..145
Scripting the GPMC...147
Group Policy Preferences..148
Group Policy's Centralized Control Enhances Your Ability to Manage Your Infrastructure.....153

Copyright Statement

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at http://nexus.realtimepublishers.com.]

Chapter 6: Managing & Customizing Group Policy

The advent of client/server computing brought about many changes to the tasks commonly associated with IT. In the mainframe days, actual computers were few in number, with terminals being the mechanism for connecting users to their applications. This centralization was a boon to systems management, as relatively few touch points were in need of control and all were centralized onto just a few computers.

But times change and so do computer architectures. The mainframe computing model eventually gave way to the client/server approach, where processing was distributed between the server and the clients connecting to that server. This new way of computing reduced the reliance on massive computers in the data center, but at the same time, significantly increased the total count of computers under management. With more individual computers to manage, IT found itself with a new problem: How to control the configuration of the machines across the network.

Early on, Microsoft recognized this growing management problem. Upon the initial release of Active Directory (AD) for Windows 2000 Server, Microsoft attempted to solve the problem with a centralized control mechanism called Group Policy. This mechanism for centralized control of individual desktops was made possible through integration with AD. Since every computer was a member of AD, each could be forced to follow “the rules” as laid down through Group Policy configurations. Using Group Policy, it became possible to create a single policy that mandated the configuration of multiple systems.

This mechanism for centralized control has been hugely successful within Windows environments and has been continually augmented and improved with each successive OS upgrade. The release of Windows Server 2008 is no different. With Windows Server 2008, Group Policy gains new policy settings, deployment abilities, and troubleshooting toolsets that add to its already rich set of capabilities as a powerful tool in centrally managing desktop configurations in any AD environment.

The Benefits of Centralized Management with Group Policy

When an IT organization makes the decision to manage its Windows Server 2008 infrastructure using Group Policy, it immediately gains a set of operational benefits. Those benefits include:

- Centralized control—A single policy with one or more configuration settings can be deployed to multiple sets of users and/or computers to configure them identically.
- Capability for mass change—When changes are made to a deployed policy, all objects that are assigned that policy will make the change. This provides a method for cohesive configuration control to managed objects.
- Enhanced machine resiliency—A large portion of break/fix problems within an IT infrastructure relate to inappropriate configurations. If those configurations are controlled through an enforcement mechanism such as Group Policy, there is a reduced chance of machine failure. This translates to greater uptime for the IT environment.
- Improved security—Group Policy provides a mechanism for controlling the security posture of systems as well. By controlling the necessary security settings through a centralized and controllable mechanism, the overall security of the environment is enhanced.

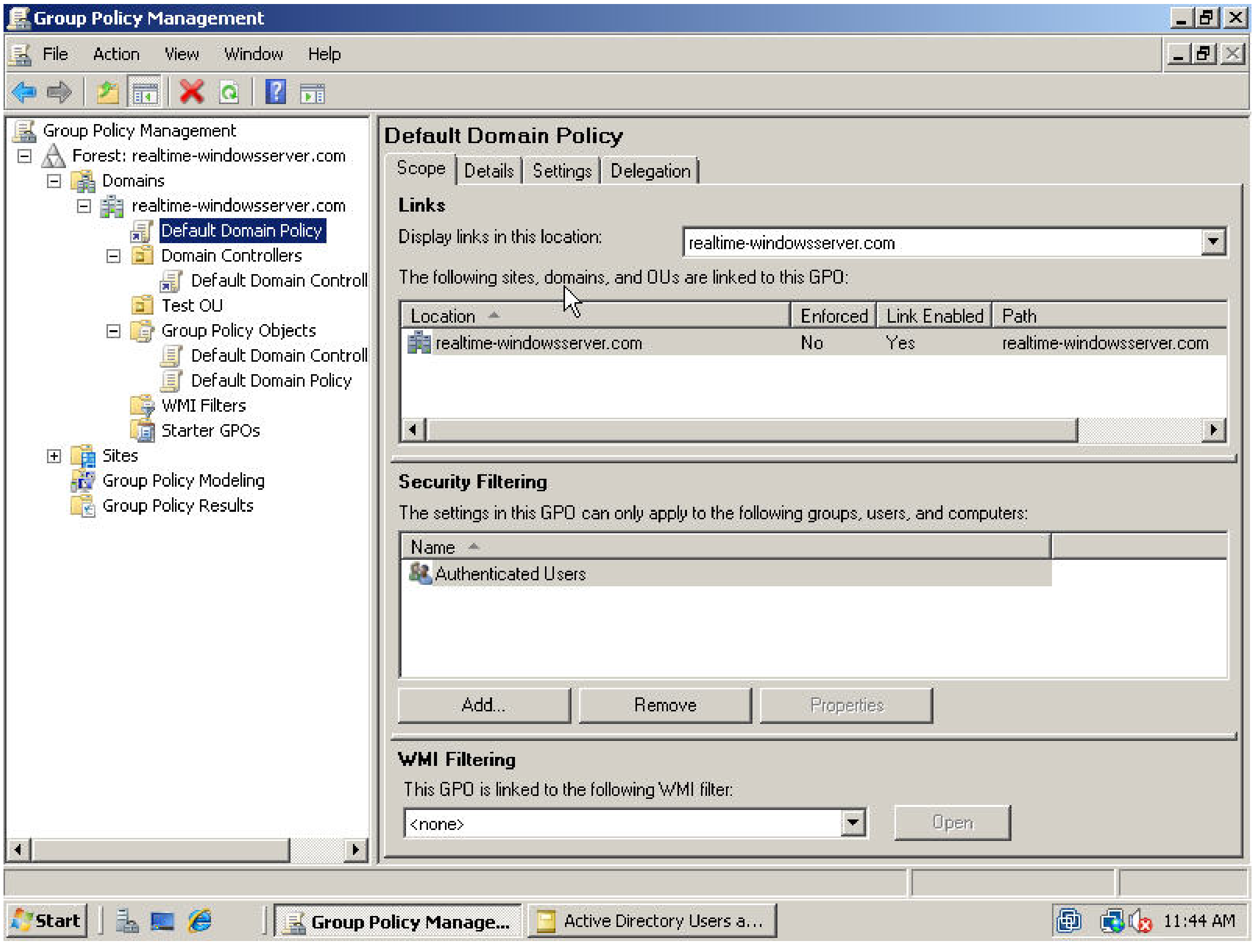
With the release of Windows Server 2008, there are now more than 2500 individual settings that can be set and controlled through Group Policy. These settings relate to virtually every part of a Windows computer, from desktop settings to security and firewall configurations; from pluggable devices to power management. In fact, there are so many possible settings that in many environments, the most difficult part about embracing Group Policy is merely deciding what to control.

This chapter will attempt to unravel some of the complexities of implementing Group Policy in your Windows Server 2008 infrastructure. That being said, the body of knowledge surrounding Group Policy is huge, and a comprehensive conversation on it can require hundreds of pages. So this chapter will focus specifically on simple examples of how you can immediately use Group Policy to benefit your Windows Server 2008 infrastructure. We'll focus on the Group Policy Management Console (GPMC) that is used to interact with policies within an AD domain, and then drill down into the creation and application of Group Policies.

Navigating the GPMC

Virtually all interaction with domain-based Group Policy is done using the GPMC. This tool, the initial screen of which is shown in Figure 6.1, can be installed onto a Server 2008 instance by adding the Group Policy Management feature through Server Manager. For Vista workstations, the GPMC is available as part of the Remote Server Administration Tools (RSAT), a separate download that can be obtained from the Microsoft Web site. The GPMC can also be used on Windows XP through a separate download also from Microsoft's Web site.

> 🕮 For Windows Vista, the RSAT can be downloaded from http://support.microsoft.com/kb/941314. For Windows XP, the GPMC can be downloaded from http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.



Group Policy Management
- Forest: realtime-windowsserver.com
  - Domains
    - realtime-windowsserver.com
      - Default Domain Policy
      - Domain Controllers
        - Default Domain Controll
      - Test OU
      - Group Policy Objects
        - Default Domain Controll
        - Default Domain Policy
      - WMI Filters
      - Starter GPOs
  - Sites
  - Group Policy Modeling
  - Group Policy Results

Default Domain Policy

Links

Display links in this location: realtime-windowsserver.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
realtime-windowsserver.com	No	Yes	realtime-windowsserver.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Figure 6.1: The GPMC is available natively in Server 2008 and as a separate download for Windows Vista.

Once installed and launched, the GPMC looks much like what is shown in Figure 6.1. On the left is a tree view that shows available domains and sites as well as Group Policy Modeling and Group Policy Results tools. By navigating down through the tree view to the domain of choice, the configured Organizational Units (OUs) for that domain are displayed. Any Group Policy Objects (GPOs) that are linked to a particular OU are shown in the tree view below that OU. For example, in Figure 6.1, you can see that the *Default Domain Controllers* GPO is currently attached to the *Domain Controllers* OU.

When considering the operational use of Group Policy, you can think of each policy as having a number of elements. The combination of these elements enables you to make a configuration change on targeted users or computers:

- GPOs—The GPO itself is the object that contains the settings to be changed. It can also contain filtering information used for specific targeting.
- Group Policy settings—Each GPO will have one or more settings. These settings represent the configuration changes the policy will enact on targeted objects.
- Group Policy links—Once a GPO is ready to be used to configure settings for targeted users or computers, it is then linked to an OU. This linkage instructs the targeted objects to begin processing the GPO’s configurations at the next processing interval.

Creating a Simple GPO

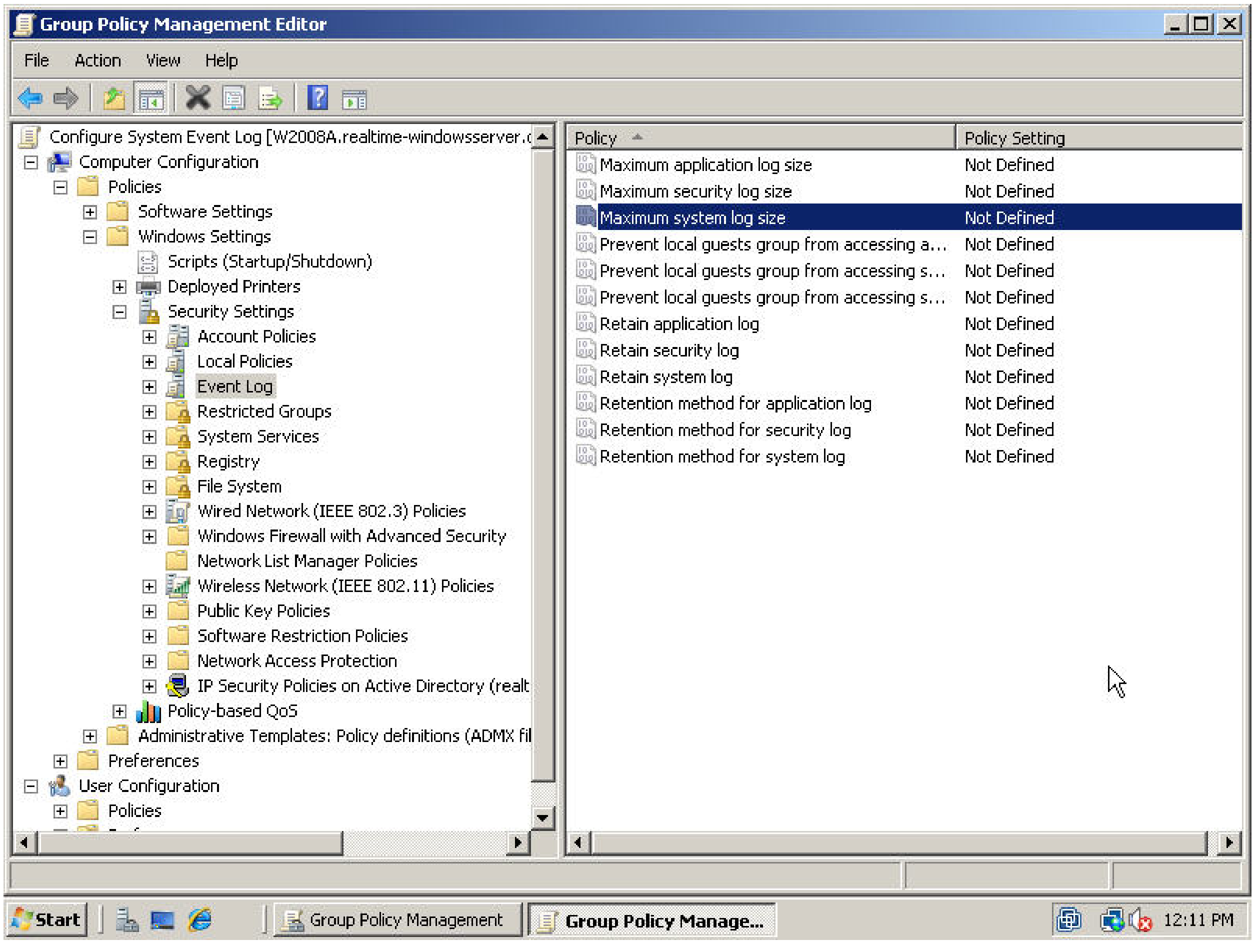
Considering all this, let’s talk now about the process by which a set of computers can be configured through Group Policy. To do so, we’ll use an example. Let’s assume that you are interested in configuring Event Log settings for a set of targeted computers so that the *Maximum system log size* is set to *40,000KB*. This is a useful setting within many environments to support storing a larger-than-default quantity of troubleshooting information about client computers.

For any GPO to configure a user or computer, that GPO must be linked to either the domain itself or an OU within the domain. In Figure 6.1, an OU for testing has already been created named *Test OU*. For the purposes of this example, this OU contains a set of computers to be used in testing the creation and application of this new GPO.

To create a new GPO, right-click *Group Policy Objects*, and choose *New*. In the resulting window, name the GPO *Configure System Event Log* and click *OK*.

> ☞ This process creates an empty GPO but does not yet link that GPO to an OU or the domain. Although it is possible to create a new GPO that is already linked to an OU or the domain, this is not often a best practice. Any users or computers in the linked OU will automatically begin making configuration changes based on the settings within the GPO. Although an initially created GPO will always be empty and lacking any settings, once a setting is enabled, it will begin applying to users and computers. For this reason, it is usually a good idea to first create unlinked GPOs and link them only once they are fully configured and ready for deployment.

Once you have created your GPO, you then need to configure within it your settings of interest. To do so, right-click the GPO, and choose Edit. The resulting screen will look similar to Figure 6.2. This screen is the Group Policy Management Editor (GPME), and is used to enable settings and set their configuration within each GPO.



```
Configure System Event Log [W2008A.realtime-windowsserver.c
⊟ Computer Configuration
  ⊟ Policies
    ⊞ Software Settings
    ⊟ Windows Settings
        Scripts (Startup/Shutdown)
      ⊞ Deployed Printers
      ⊟ Security Settings
        ⊞ Account Policies
        ⊞ Local Policies
        ⊞ Event Log
        ⊞ Restricted Groups
        ⊞ System Services
        ⊞ Registry
        ⊞ File System
        ⊞ Wired Network (IEEE 802.3) Policies
        ⊞ Windows Firewall with Advanced Security
          Network List Manager Policies
        ⊞ Wireless Network (IEEE 802.11) Policies
        ⊞ Public Key Policies
        ⊞ Software Restriction Policies
        ⊞ Network Access Protection
        ⊞ IP Security Policies on Active Directory (realt
      ⊞ Policy-based QoS
    ⊞ Administrative Templates: Policy definitions (ADMX fil
  ⊞ Preferences
⊟ User Configuration
  ⊞ Policies
```

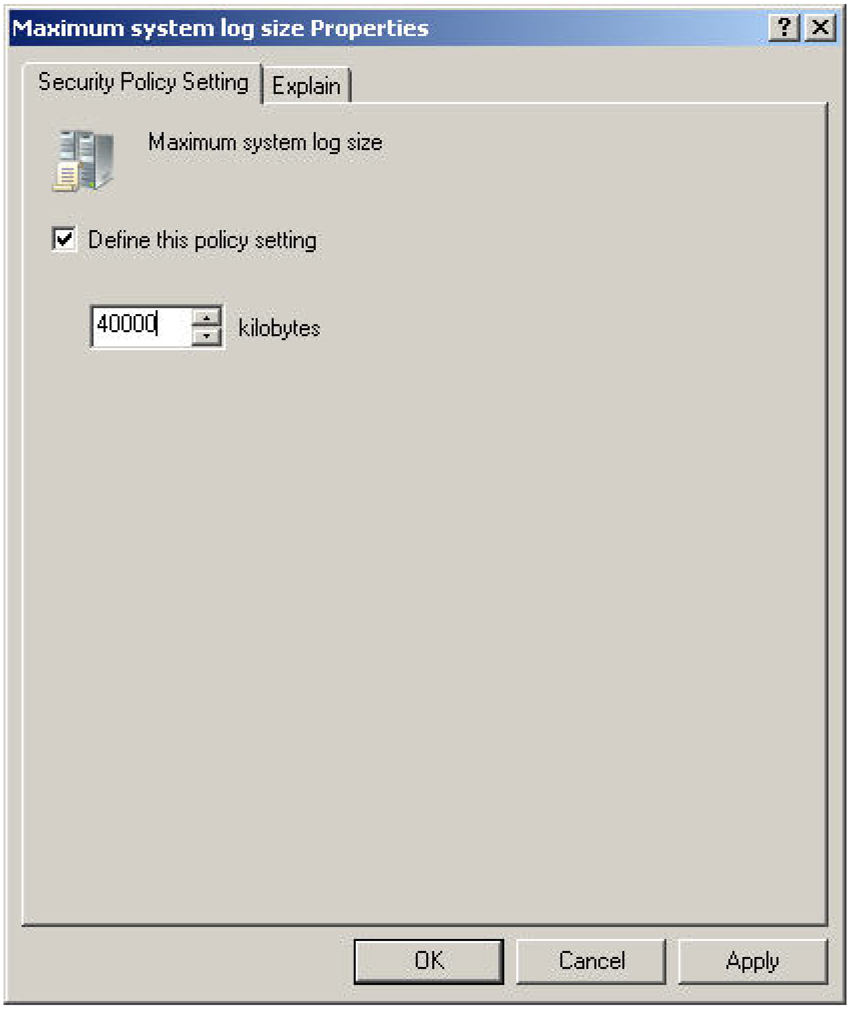
Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing a...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Figure 6.2: The GPME is used to manage individual settings within a GPO.

As the figure shows, each GPO is broken first into two halves. The first half, called Computer Configuration, is used to manage settings that generally relate to the entire targeted computer. The second half, called User Configuration, is used to manage settings that generally relate to an individual user. Settings that are configured in the Computer Configuration section of a GPO are only relevant when that GPO is applied to a computer object. Conversely, the settings that are configured in the User Configuration section are only relevant when the GPO is applied to a user object. OUs within your domain typically contain one or the other of these objects, and sometimes both. We'll talk about the process of linking a GPO in a minute, but for now, be aware that by default only half of any particular GPO will typically apply to a particular object type.

> ✎ Actually, that last statement isn't entirely true. It is possible for a computer object to process settings from the User Configuration half when a Group Policy setting called Loopback Mode is enabled. This is done when you want the settings within the User Configuration half of the GPO to apply based on the OU location of the computer object. For more information on Loopback Mode, see http://support.microsoft.com/kb/231287.

For our example, you want to manage the configuration of the Event Log on targeted computers. To do so, navigate to Computer Configuration | Policies | Windows Settings | Security Settings | Event Log. The resulting view is displayed in Figure 6.2, where you should see the configuration for *Maximum system log size* in the right pane. By double-clicking the setting, you will be presented with a window similar to Figure 6.3. There, select the *Define this policy setting* check box and set the value to 40000. Each policy setting must be specifically enabled for it to apply to targeted users or computers. Click OK to complete the configuration.


Maximum system log size Properties

Maximum system log size

☑ Define this policy setting

40000 kilobytes

Figure 6.3: An individual setting within a GPO that configures the Event Log.

You’ll note that there is no location to save the configuration. There is no Save button and no Save link under the File menu. This is the case because policy settings are saved immediately upon clicking OK. This can become an issue if you are not careful in how settings are configured. This is also a good reason why GPOs should not be linked to an OU until they are fully created, tested, and ready for production.

Applying That Simple GPO

Once the Group Policy is configured, you can close the GPME and return back to the GPMC. To begin applying this change to the computers in the Test OU, right-click the Test OU and select Link an Existing GPO. Select the Configure System Event Log GPO from the list and click OK.

It is important to note at this point that clients will not immediately begin processing the GPO. Group Policy on each individual client is by default configured to check for new GPOs and GPO changes each time the machine is powered on as well as every 90 minutes thereafter (plus a randomized zero to 30 minute offset). Thus, once the GPO is linked to the Test OU, client computers in that OU that have successfully authenticated to the domain will begin processing this new GPO and its settings at some random time between 90 and 120 minutes later. This period of time is called the Refresh Interval.

It is possible to speed this process if you don’t want to wait out the refresh interval period. To speed the process on any individual client, use the command

```
gpupdate /force
```

This command will instruct the client to ignore the refresh interval and check for new policies immediately. It is possible to verify that the GPO is applying correctly by using the gpresult command. For Windows XP, from a command line, enter

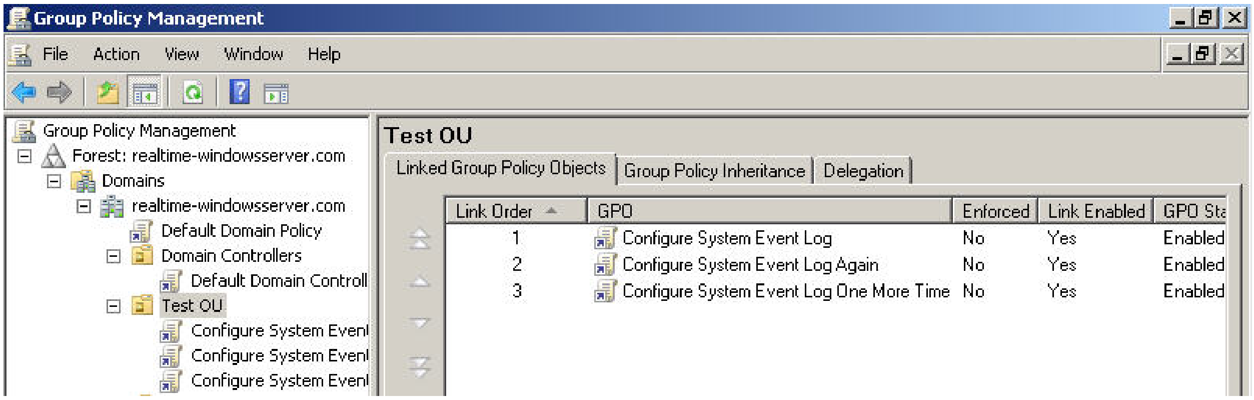
```
gpresult
```

to show a report detailing which policies have and have not been applied. For Windows Vista, use the command gpresult /r.

Applying Multiple GPOs

This example shows how a single simple policy can be applied to an OU. But what if you want to apply multiple GPOs to the same OU? How do the client computers know which policy to process first? Figure 6.4 shows an example of the Linked Group Policy Objects tab shown when focusing the view on an OU in the GPMC. There, you can see three GPOs that have been linked to the Test OU. From their names, each GPO appears to configure similar settings in the System Event Log.

Clients will process multiple Group Policies linked to the same OU based on their Link Order, starting with the highest number first and working backwards. The Link Order is shown in the left column of the right pane of Figure 6.4. In this case, the Configure System Event Log One More Time GPO will actually apply first. Layering over the top—and potentially overwriting any settings that are in conflict—will be the Configure System Event Log Again policy. Last to apply—again with any settings in conflict being overwritten by its settings—is the original policy Configure System Event Log. It is possible to reorder the Link Order by selecting a policy and clicking the arrows to the left of the right pane.



Group Policy Management
- Forest: realtime-windowsserver.com
  - Domains
    - realtime-windowsserver.com
      - Default Domain Policy
      - Domain Controllers
        - Default Domain Controll
      - Test OU
        - Configure System Event
        - Configure System Event
        - Configure System Event

Test OU

Link Order	GPO	Enforced	Link Enabled	GPO Sta
1	Configure System Event Log	No	Yes	Enabled
2	Configure System Event Log Again	No	Yes	Enabled
3	Configure System Event Log One More Time	No	Yes	Enabled

Figure 6.4: Link Order determines the order in which multiple GPOs are applied.

Administrative Templates and the Group Policy Central Store

One component of GPOs that we've glossed over to this point is found within the GPME. Under the Policies node in either Computer or User Configuration is the Administrative Templates node. These templates are used by Group Policy in the configuration of numerous settings within client systems. They make up the largest part of the 2500 settings that can be enabled and configured with Group Policy.

> ✎ If you think of using the GPME to enable and configure GPO settings as similar to filling out a form, then you can easily think of the Group Policy templates as the forms themselves. The templates are files that store the possible settings you may be interested in enabling for any particular GPO.

Prior to the release of Windows Vista, five templates were natively available for configuring Windows (system.adm), Internet Explorer (inetres.adm), NetMeeting (conf.adm), Windows Media Player (wmplayer.adm), and Automatic Updates (wuau.adm). These five templates—and primarily system.adm where the vast majority of settings were stored—were used for the storage of potential settings under the Administrative Templates node for every newly created GPO. However, over time, a number of problems emerged with the implementation of these templates. Most important of these was in how they were stored.

Part of every GPO is stored in a domain's SYSVOL. You can see this part in your own domain by navigating to *\\{domainName}\SYSVOL\{domainName}\Policies*. In that location, you'll see a number of GUIDs, each that relates to a configured GPO. Drilling further into any particular GUID, you will find a series of files the contents of which instruct clients to process configured GPO settings. In the adm subfolder, you should also find the five templates discussed earlier.

AD's SYSVOL is replicated between all domain controllers in the domain and has historically had problems with that replication when the size of the SYSVOL grows large. The combination of these five templates adds a little more than 4MB of space to every newly created GPO. Thus, when the number of GPOs grows large, the size of the SYSVOL grows large as well.

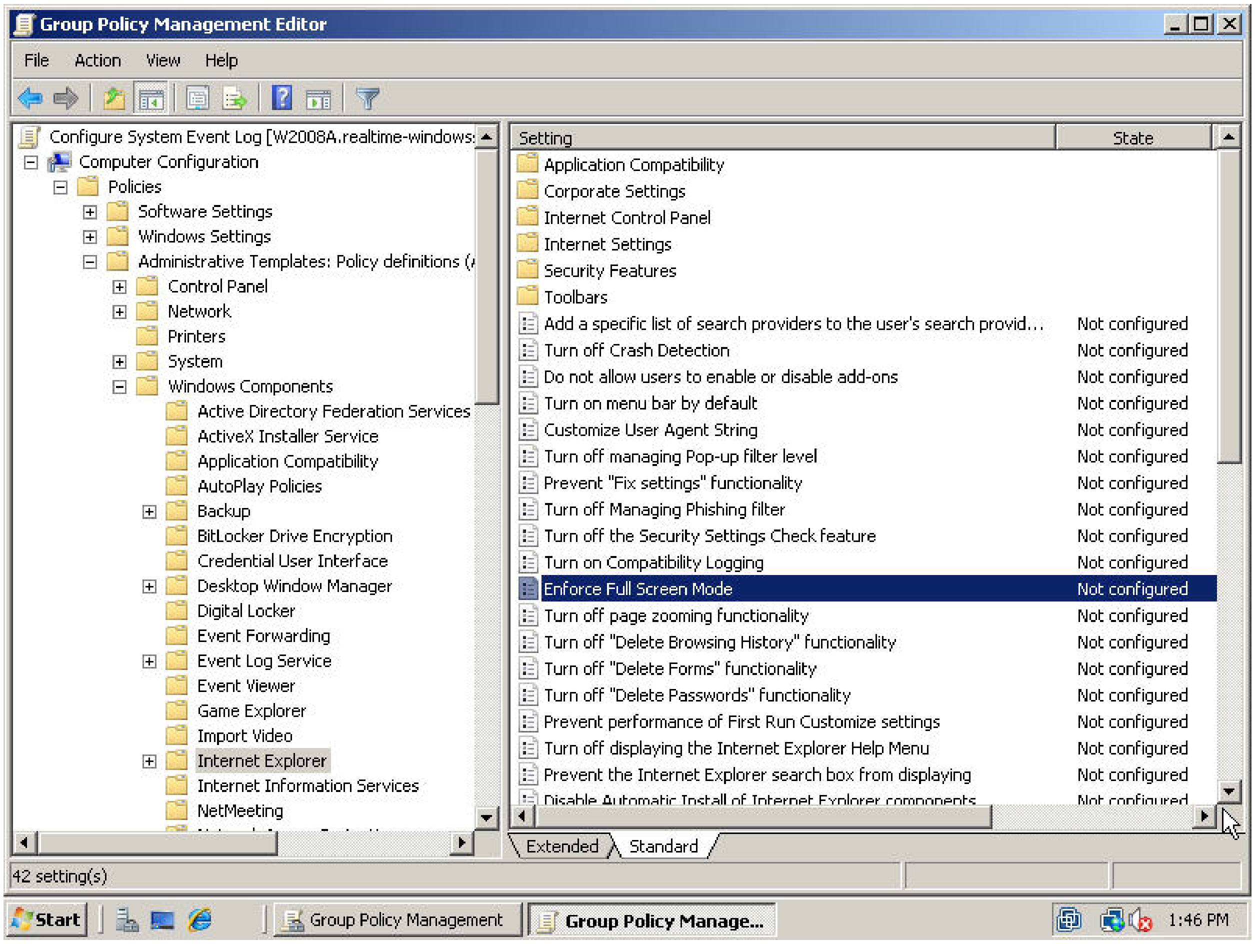
One new feature that actually arrived with the release of Windows Vista is the Group Policy Central Store. The Central Store is a new architecture for storing Group Policy template files that alleviates some the problems of the old storage mechanism. Specifically, rather than replicating template files into each GPO’s SYSVOL folder, a single folder is created to store them all. This store houses all the administrative template files for the entire domain within a single folder in the SYSVOL, reducing the overall size of the SYSVOL and the stress on replication.

> ✎ Another change that arrived with the release of Windows Vista has to do with the file format to the templates themselves. Formerly, Microsoft used a proprietary scripting language to create the template files but with the release of Windows Vista, that language has changed to XML. One of the benefits of this change is the new support for multiple languages. Template files are now broken into two halves, with one half (the ADMX file) containing the data about the setting to be configured. The other half (the ADML file) contains the text within the GPME that explains to the administrator what the template will do. By breaking the files apart in this way, one ADMX file can support multiple ADML files, and so one template can explain text in multiple languages.

The Group Policy Central Store is not created by default. Instead, you must manually create it within your domain’s SYSVOL through a manual process. To create the central store, as a Domain Administrator complete the following steps:

- From the *Run* prompt, navigate to *\\{domainName}\SYSVOL\{domainName}\Policies*.
- In the Policies folder, create a subfolder named *PolicyDefinitions*.
- From a Windows Server 2008 computer, navigate to C:\Windows\PolicyDefinitions. Copy the contents of this folder to the PolicyDefinitions folder you just created.
- Navigate into the PolicyDefinitions folder, and create a subfolder there named after your particular language code. For the English language, this subfolder will be named en-US.
- Finally, from the same Windows Server 2008 computer, navigate to C:\Windows\PolicyDefinitions\{language}. Copy the contents of this folder to the language folder you just created in the SYSVOL. For the English language, this will be C:\Windows\PolicyDefinitions\en-US.

Once this has been completed, the GPMC on Windows Vista and Windows Server 2008 machines will immediately begin using the templates within the central store instead of the original five within each individual GPO. If you’re used to using Group Policy with the old templates, you’ll immediately see another added benefit of the change. Separated into 146 different files, these new templates provide much more granular controls over Windows clients. As you can see in Figure 6.5 where the Administrative Templates node is expanded, there are a vast number of settings and categories of settings that can be configured.



Configure System Event Log [W2008A.realtime-windows:
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (/
Control Panel
Network
Printers
System
Windows Components
Active Directory Federation Services
ActiveX Installer Service
Application Compatibility
AutoPlay Policies
Backup
BitLocker Drive Encryption
Credential User Interface
Desktop Window Manager
Digital Locker
Event Forwarding
Event Log Service
Event Viewer
Game Explorer
Import Video
Internet Explorer
Internet Information Services
NetMeeting

Setting	State
Application Compatibility	
Corporate Settings	
Internet Control Panel	
Internet Settings	
Security Features	
Toolbars	
Add a specific list of search providers to the user's search provid...	Not configured
Turn off Crash Detection	Not configured
Do not allow users to enable or disable add-ons	Not configured
Turn on menu bar by default	Not configured
Customize User Agent String	Not configured
Turn off managing Pop-up filter level	Not configured
Prevent "Fix settings" functionality	Not configured
Turn off Managing Phishing filter	Not configured
Turn off the Security Settings Check feature	Not configured
Turn on Compatibility Logging	Not configured
Enforce Full Screen Mode	Not configured
Turn off page zooming functionality	Not configured
Turn off "Delete Browsing History" functionality	Not configured
Turn off "Delete Forms" functionality	Not configured
Turn off "Delete Passwords" functionality	Not configured
Prevent performance of First Run Customize settings	Not configured
Turn off displaying the Internet Explorer Help Menu	Not configured
Prevent the Internet Explorer search box from displaying	Not configured
Disable Automatic Install of Internet Explorer components	Not configured

42 setting(s)

Figure 6.5: The vast majority of possible settings are contained within the Administrative Templates.

For the most part, once the setup process is complete, configuring Administrative Template settings happens in much the same way as was explained previously for Windows Settings. Simply create a GPO, then open the GPME to edit that GPO. Under the Administrative Templates node, enable the settings of interest and set any necessary configurations.

When configuring settings, be aware of the product for which the setting is supported. When viewing the properties of any setting, look at the bottom of the window for the words *Supported on*. If you attempt to apply a setting to a client that is below the *Supported on* level, that setting will not work on that client.

Network Location Awareness

As you can see, Group Policy is a great tool for locking down the configuration of clients within your domain. But the processing of GPO settings can be a network-intensive task, especially when clients are connected to the domain over slow links. Due to these situations, Group Policy has always had the ability to determine the link speed of the connection between client and domain controller. If the connection speed was not at a level that Group Policy deemed fast enough, non-critical portions would simply not apply.

📖 More information about Group Policy processing, how link speed is determined, and what parts of Group Policy are and are not processed over slow links can be found at http://technet2.microsoft.com/windowsserver/en/library/89d7ec5f-a909-4f61-aded-c5b69f5f730b1033.mspx?mfr=true.

Prior to the release of Windows Vista and Windows Server 2008, that determination was done using ICMP ("ping"). This protocol and the timing response received from sending and receiving a ping packet was used to determine the speed of the connection. However, one problem with this method is that "ping" is often disabled in highly secured networks such as those used for remote access. Because of this and other issues, in Windows Vista and Windows Server 2008, Group Policy's reliance on "ping" was replaced with a new protocol called Network Location Awareness (NLA). Without diving too deep into its technical detail, NLA is used by Group Policy to uniquely identify each network the computer connects to as well as determine the effective bandwidth and status of each network. As the status of a connected network changes, the NLA service is responsible for notifying the client's Group Policy engine of the change.

The result is an elimination of the reliance on "ping" and an enhanced ability on the part of the client to process Group Policy during periods of changing network connectivity. These periods include establishing VPN sessions, recovering from hibernation or standby, successfully exiting quarantine, and docking a laptop, all of which were previously challenging situations for Group Policy application.

✎ NLA is not solely used by Group Policy. Any network-aware application can leverage its network status and notification features. The most obvious way to see how NLA is functioning is to view network properties. The Network and Sharing Center shows a graphical representation of the currently connected network and its status. This information comes from the NLA service (see http://msdn.microsoft.com/en-us/library/ms739931.aspx).

Starter GPOs

As discussed above, one of the hardest parts about embracing Group Policy can be in navigating through the sheer number of policies to find the ones of interest. With over 2,500 policies available for Windows Vista and Windows Server 2008, determining which are useful and which can be problematic for your environment can be a challenging activity. To assist with this problem, another new and interesting new feature that arrives with the release of Windows Vista and Windows Server 2008 are Starter GPOs.

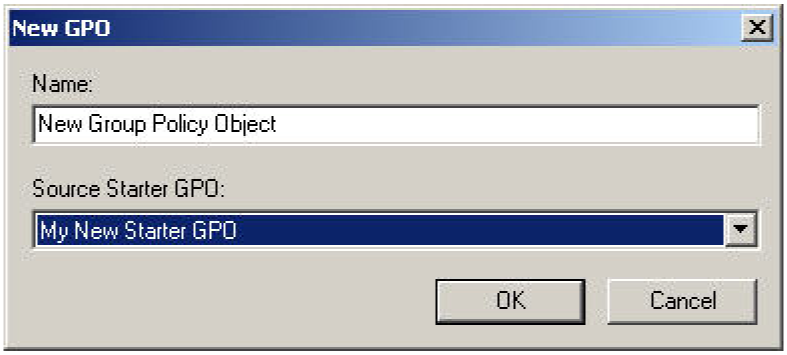
Starter GPOs in implementation are actually quite simple. They are little more than a mechanism to collect, export, and distribute GPO settings to others, specifically those within Administrative Templates. Consider the situation where you have completed a large project to lock down the configuration of workstations and servers within your domain. That activity likely looked through all the possible GPO settings to find just the ones of interest to you and your environment. Perhaps the activity also aligned the configured settings with those required by established security practices or compliance regulations.

> 🕮 Microsoft provides a set of four sample Starter GPOs that relate to recommended security configurations at http://www.microsoft.com/Downloads/details.aspx?familyid=AE3DDBA7-AF7A-4274-9D34-1AD96576E823&displaylang=en.

In this case, after implementing them in your organization you may want to share the fruits of your work with others in your organization or within the IT community. Starter GPOs are a way to export your configured GPO settings into a CAB file that can be distributed to others. Other organizations can import the file into their GPMC and use your GPO settings as a “starting point” for the creation of their own lockdown configuration. Hence the name: Starter GPOs.

To begin making use of Starter GPOs, you must first create their containing folder. Within the GPMC, click the Starter GPOs node. In the right-pane of the resulting screen, you will find the text *The Starter GPOs folder does not currently exist in this domain. Click on the button below to create this folder*. Click the button to create the folder.

Once created, Starter GPOs can be used as the starting point for the creation of new GPOs in the domain. For example, let’s assume that a Starter GPO named *My New Starter GPO* has already been imported into the GPMC. That Starter GPO includes Administrative Template settings to be used in the creation of a standard GPO. When creating a new standard GPO, change the value for *Source Starter GPO* to *My New Starter GPO* to start the new GPO with the already-configured settings from the Starter GPO. The *New GPO* window where this is selected is shown in Figure 6.6.



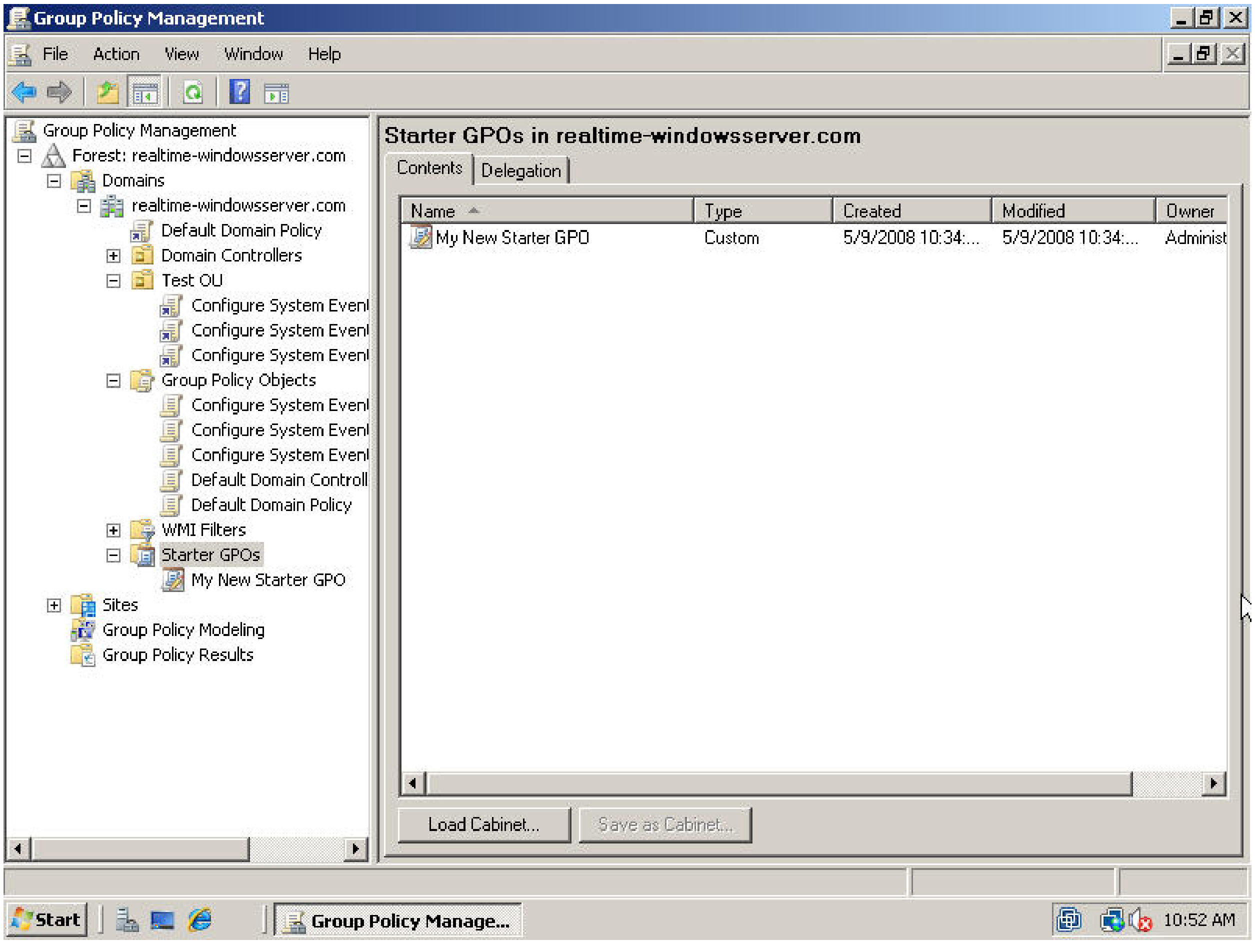
Name: New Group Policy Object

Source Starter GPO: My New Starter GPO

Figure 6.6: Starter GPOs provide a way to pre-populate new GPOs with settings.

Once imported into a domain or newly created within a domain, Starter GPOs are configured in the same way as standard GPOs. Figure 6.7 shows an example of the GPMC with the My New Starter GPO available. Right-clicking *My New Starter GPO* and selecting *Edit* brings forward the *Group Policy Starter GPO Editor*, where the contents and configuration of the Starter GPO can be edited. Clicking the *Load Cabinet* and *Save as Cabinet* button provides for the import and export of GPOs from external sources.

There are a couple of fairly significant limitations associated with Starter GPOs. First Starter GPOs can only configure the settings found in the Administrative Templates. The other elements of Group Policy outside the Administrative Templates simply aren't available for Starter GPOs. Also, there currently is no direct way to turn a standard GPO into a Starter GPO. The only way to create a Starter GPO is by manually re-creating the settings.



Name	Type	Created	Modified	Owner
My New Starter GPO	Custom	5/9/2008 10:34:...	5/9/2008 10:34:...	Administ

Figure 6.6: A view of the Starter GPOs node with one Starter GPO imported into the interface.

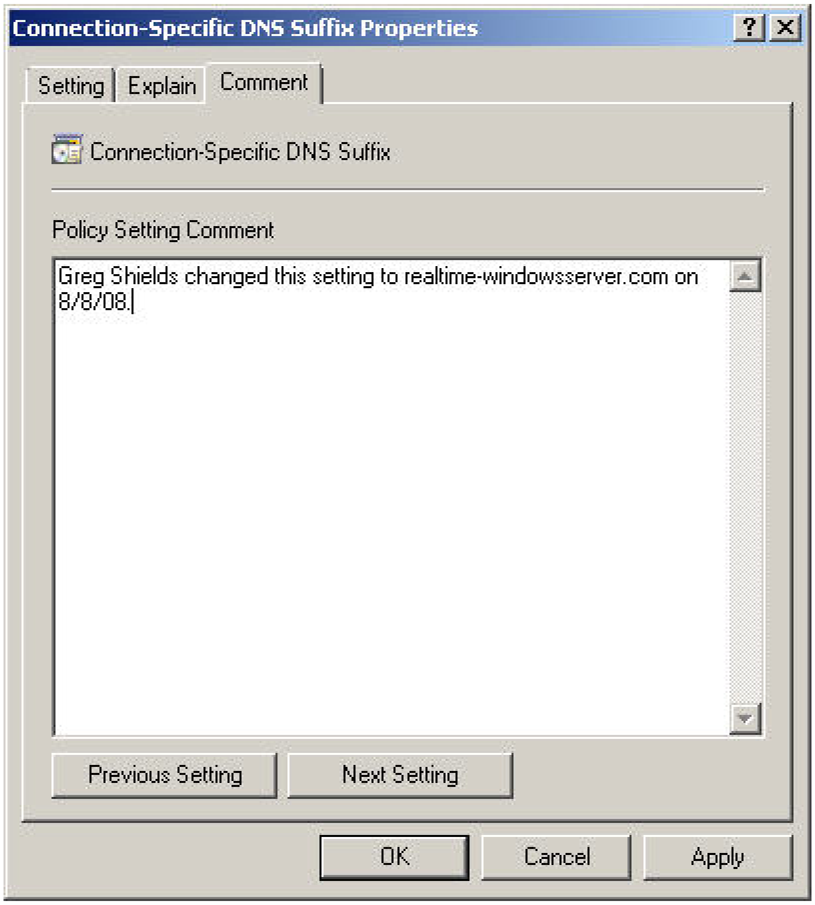
GPO and GPO Settings Comments

Although you may not have made use of the feature in your own environment, virtually every object within Active Directory contains the ability to attach a comment. This commenting feature allows you to make notes about the object that are contained directly within that object. This is handy for sharing information in environments where multiple administrators work within the same directory. However, prior to the release of Windows Vista and Windows Server 2008, there was no commenting capability for GPOs and their settings. This omission has now been remedied.

With the GPMC on Windows Vista or Windows Server 2008, comments can now be attached to either the GPOs itself or to individual settings within a GPO. This new feature is a boon to environments where information about configuration settings needs to be kept close at hand. Adding a comment to a GPO enables administrators to share information about the creation, use, and reason for the GPOs presence. It also allows administrators to easily show ownership of the GPO.

For settings within a GPO, adding comments to individual settings allows administrators to document the reason, creation or modification date/time, owner, and other necessary information about individual settings. If you've ever created a GPO and wondered years later how and why its settings got changed, you'll be excited to make use of this feature.

To add a comment to a GPO, first edit the GPO in the GPME. Then, right-click the top-level node for the GPO and select *Properties*. Comments can be added under the *Comment* tab. To add a comment to an individual setting within a GPO, double-click the setting and navigate to the *Comment* tab. Figure 6.7 shows the resulting window with a sample comment entered.



Greg Shields changed this setting to realtime-windowsserver.com on 8/8/08.

Figure 6.7: A sample comment added to a GPO setting.

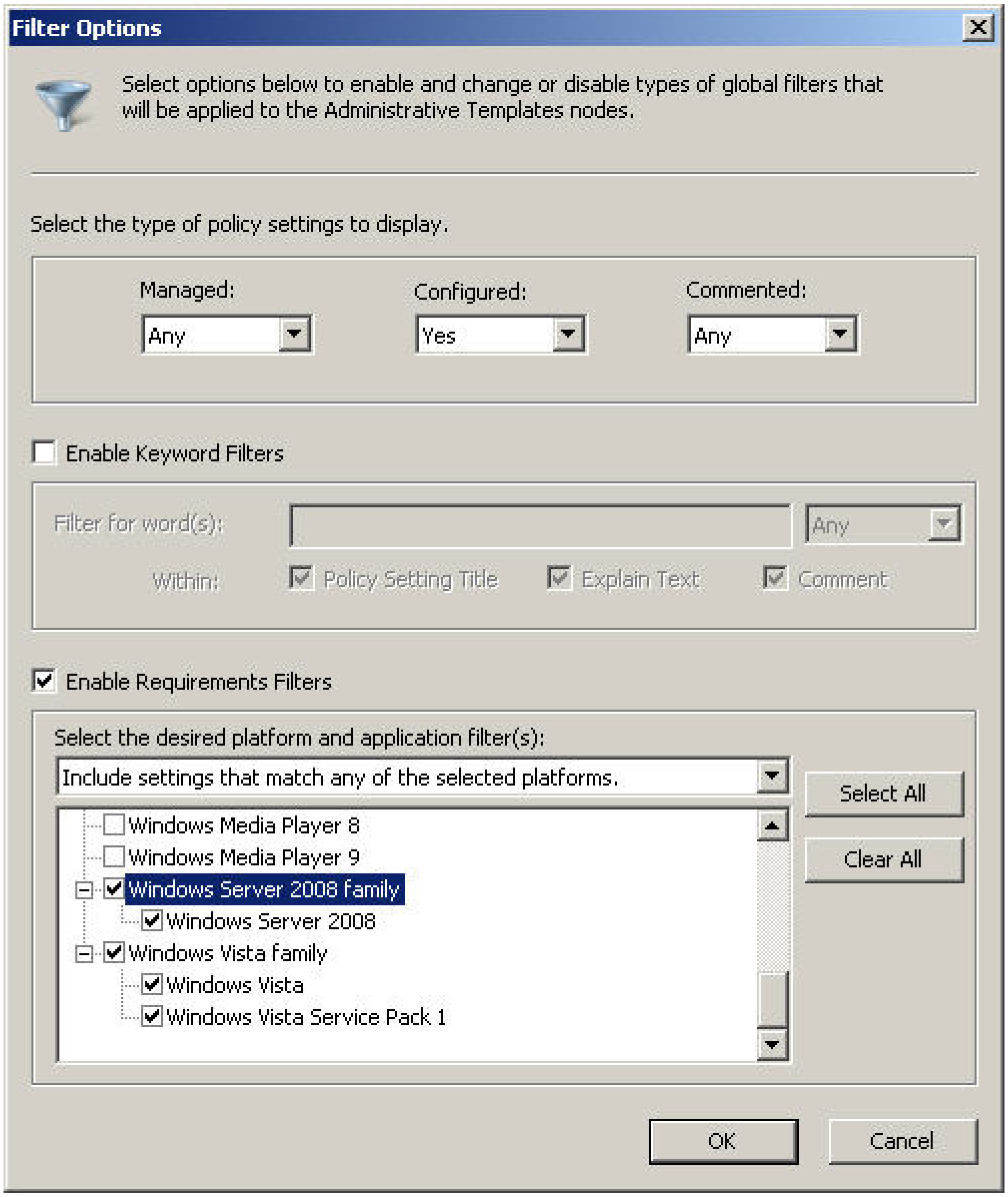
GPO Filters

Another major omission in previous versions of Group Policy was in an ability to search and filter through available policies to locate those of interest. Without a searching and filtering mechanism in place, the only way previously to identify which policies were enabled or configured was to navigate through the entire folder structure within the GPME. With Windows Vista and Windows Server 2008, this inability would be particularly pronounced due to the large number of folders that now make up the structure.

Thankfully, a filtering and searching feature is now available with the GPMC on Windows Vista and Windows Server 2008. This filtering and searching feature provides a way to narrow down the large field of possible GPO settings to just those of interest. It further allows an administrator to easily create a listing of just those GPO settings that have been configured for a particular GPO without needing to step through the entire folder structure as was the case in previous versions.

Figure 6.8 shows an example of the *Filter options* available for narrowing down the field of settings. As you can see there, settings can be filtered through any of five possible selections:

- *Managed.* Group Policy Administrative Templates can be those provided by Microsoft or others that you create yourself. Those provided by Microsoft have the benefit in that they don't permanently change the registry, allowing them to revert back to the original setting when removed. These policies are termed *Managed*. Other customized policies are termed *Unmanaged*.
- *Configured.* When a policy has been set to anything other than Not Configured, it is considered Configured by the filter.
- *Commented.* When a policy has a comment attached to it, it is considered Commented by the filter.
- *Keyword filters.* A keyword can be any word that exists in the setting title, explain text, or within an attached comment.
- *Requirements filters.* The Supported on label as seen within each Group Policy setting determines which OS or application level is required for the setting to apply. Requirements filters can limit the available settings to just those that support a particular OS or application level.



Filter Options

Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.

Select the type of policy settings to display.

Managed: Any

Configured: Yes

Commented: Any

□ Enable Keyword Filters

Filter for word(s): Any

Within: ☑ Policy Setting Title ☑ Explain Text ☑ Comment

☑ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms.

- □ Windows Media Player 8
- □ Windows Media Player 9
- ☑ Windows Server 2008 family
  - ☑ Windows Server 2008
- ☑ Windows Vista family
  - ☑ Windows Vista
  - ☑ Windows Vista Service Pack 1

Figure 6.7: An example of a GPO filter that restricts the view to only those settings that have been configured and relate to Windows Vista or Windows Server 2008.

You'll also notice that after clicking the *Administrative Templates* node in the GPME that a filter icon appears in the toolbar. Once a filter has been created, implementing that filter is done by either clicking the icon or by right-clicking *Administrative Templates* and selecting *Filter On*. Once the filter has been applied, the Administrative Templates node will restrict to show only the results of the filter.

> ✎ This includes the folder structure as well. Once a filter is applied, the tree structure only shows those parts of the tree that contain filtered settings.

Another useful tool within the Administrative Templates node that can be used either in with or without the use of filters is the *All Settings* node. With no filter in place, this node effectively eliminates the entire tree structure associated with the Administrative Templates. It instead lists all the potential settings in a flat format. This can be exceptionally useful if you desire a more user-friendly way to browse through available settings without having to navigate the tree structure. With a filter in place, this node will show—also without the tree structure—only those settings that relate to the filter. Thus, after applying a filter, you can use All Settings to find the complete list of settings that relate to the filter's characteristics.

> ☞ The combination of commenting and filtering should significantly reduce the headache associated with locating configured settings as well as finding new settings of interest.

Scripting the GPMC

As you've already seen in this chapter, the GPMC arrives full of features that can be accessed through the GUI. However, sometimes the workflow within your Windows Server 2008 infrastructure requires the use of command-line tools and scripts for scheduling or custom purposes. In those cases, Microsoft has made available a set of GPMC scripts that augment the capabilities of the GUI. These scripts provide scripting and command line support for a set of needed Group Policy functionality. The GPMC scripts with Windows Vista and Windows Server 2008 are not natively installed with the GPMC, but are instead a separate download. Be aware that this is a different behavior than with Windows XP, where the scripts were available with the GPMC installation.

> 🕮 You can download the GPMC scripts from the Microsoft Web site at http://www.microsoft.com/downloads/details.aspx?familyid=38c1a89b-a6d2-4f2a-a944-9236999aee65&displaylang=en.

Thirty-three in number, the GPMC Scripts enable a set of mostly VBScript-based tools that integrate with Group Policy to enable its manipulation via the command line. Once installed, you can access the scripts from the location *C:\Program Files\Microsoft Group Policy\GPMC Sample Scripts*. These tools provide the ability to list, locate, copy, delete, and get reports on GPOs as well as their status. They also enable a very easy way to backup and restore GPOs and their settings right from the command line.

As an example, one script in particular can be extremely handy for emergency situations. The *BackupAllGPOs.wsf* provides a way to create a file-based backup of all GPOs within a domain along with their settings. This file-based backup is significantly easier to restore in the case of an accidental deletion than would be the Active Directory-based restoration process otherwise required. By combining this script with the Windows Task Scheduler, it is possible to create a daily backup of all GPOs to be used should a GPO be accidentally deleted.

To create a scheduled backup, navigate to the Windows Task Scheduler and create a new task that runs a command similar to the following on a regular basis:

```
cscript.exe “C:\Program Files\Microsoft Group Policy\GPMC Sample
Scripts\BackupAllGPOs.wsf” {backupLocation}
```

The above command assumes that you’ve installed the GPMC Scripts to their default location and that the *{backupLocation}* folder has already been created. Upon running this script, any GPOs within the domain as well as their settings will be backed up to *{backupLocation}*. To restore any of these previously backed up GPOs use the *RestoreGPO.wsf* script with the following syntax:

```
cscript.exe “C:\Program Files\Microsoft Group Policy\GPMC Sample
Scripts\RestoreGPO.wsf” {backupLocation} {backupID}
```

In the command above, the value for *{backupLocation}* should be the location where the scripts were previously backed up. The value for *{backupID}* will be the name or GUID of the GPO to restore.

> 📖 In addition to this simple example, there are a number of additional functions that can be run via command line or scripted using the GPMC scripts. For more information on the scripts and the functionality they can provide, navigate to the article “GPMC Scripting: Automate GP Management Tasks” at http://technet2.microsoft.com/windowsserver/en/library/885ed84e-80da-4025-bd76-0ea4d05127f11033.mspx?mfr=true.

Group Policy Preferences

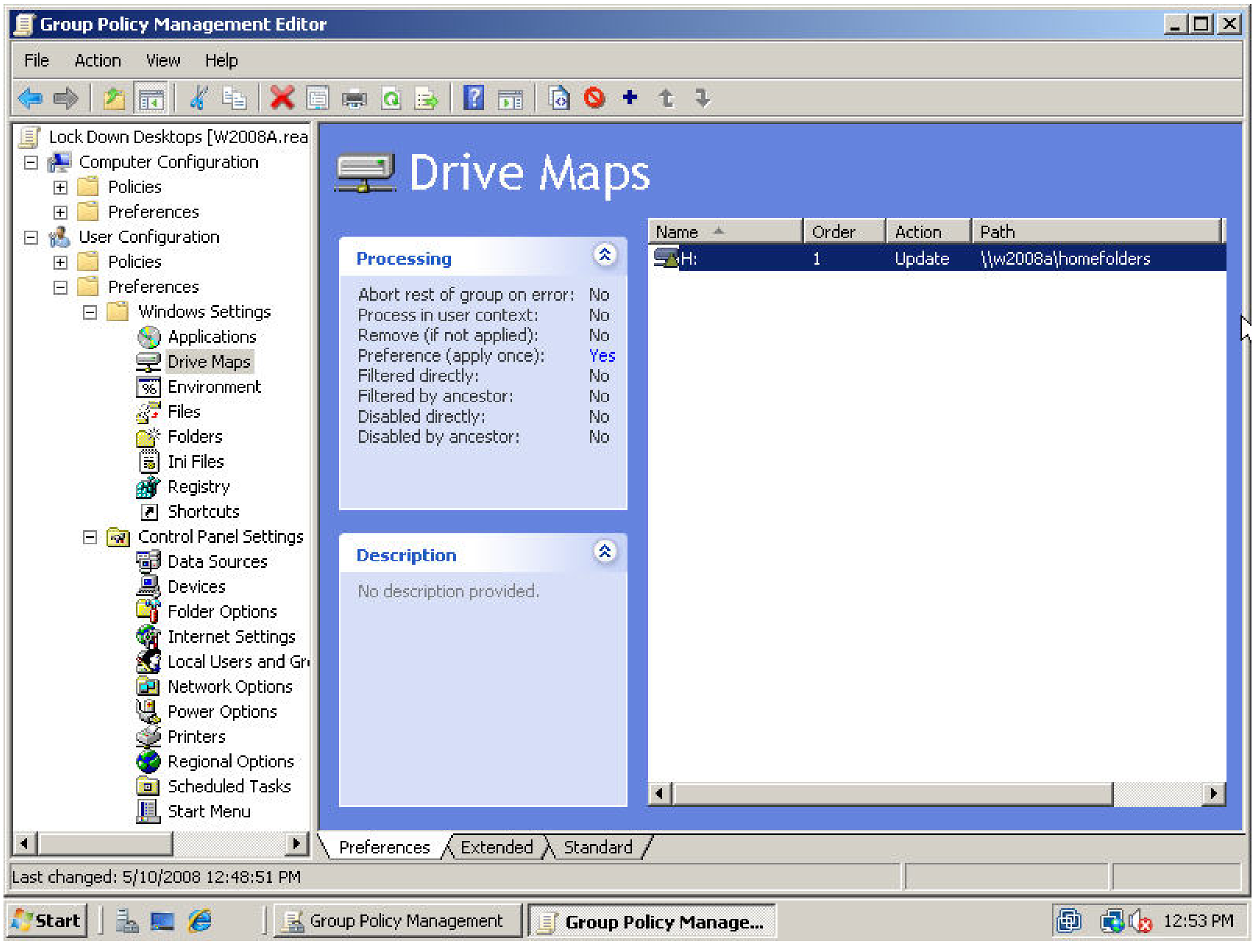
Even with the more than 2500 individual settings that can now be configured with Group Policy, the nature of Group Policy itself may not fulfill all the needs of your Windows Server 2008 infrastructure. Due to their highly-customizable nature, IT infrastructures have traditionally made use of login scripts to handle the customized needs of their individual environment.

But there has always been a few issues with login scripts for these sorts of customizations. First, they are only processed at the time of login. If you desire a custom change to occur, you must first change the login script and then wait for each client to re-login in order for the change to process. Additionally, the coding of complex customizations can often be challenging using shell scripting or VBScript languages. In order to properly use login scripts, you need to learn these scripting languages and the best practices associated with their use.

Upon the release of Group Policy with Windows Server 2008 comes a much-desired new enhancement to Group Policy called Group Policy Preferences (GPPs). GPPs bring together much of the customization power of login scripts with the rich targeting and regular update capabilities of Group Policy.

Take a look through the settings found in the traditional Group Policy Administrative Templates. There, you'll find a significant level of ability to control the configuration of workstations and servers attached to your domain. But that configuration control is limited to just the areas that Microsoft has made available through the Administrative Templates. If you want to make your own customized changes that aren't already a part of a Group Policy setting, you're forced to code your own template using XML. This rather difficult process can make cumbersome the process of customization. GPPs overcome this limitation by making available a set of tools that allow for GUI-based customization of areas commonly handled through login scripts.

Take another look at any particular Group Policy within the GPME. Within the left pane of the tree view, as shown in Figure 6.8, you will see that the both the Computer Configuration and the User Configuration nodes are further broken into two halves apiece. Each contains two top-level nodes titled *Policies* and *Preferences*. The Policies node is where traditional Group Policy settings are configured. The Preferences node is where preferences are enabled.



Processing

Abort rest of group on error:	No
Process in user context:	No
Remove (if not applied):	No
Preference (apply once):	Yes
Filtered directly:	No
Filtered by ancestor:	No
Disabled directly:	No
Disabled by ancestor:	No

Description

No description provided.

Name	Order	Action	Path
H:	1	Update	\\w2008a\homefolders

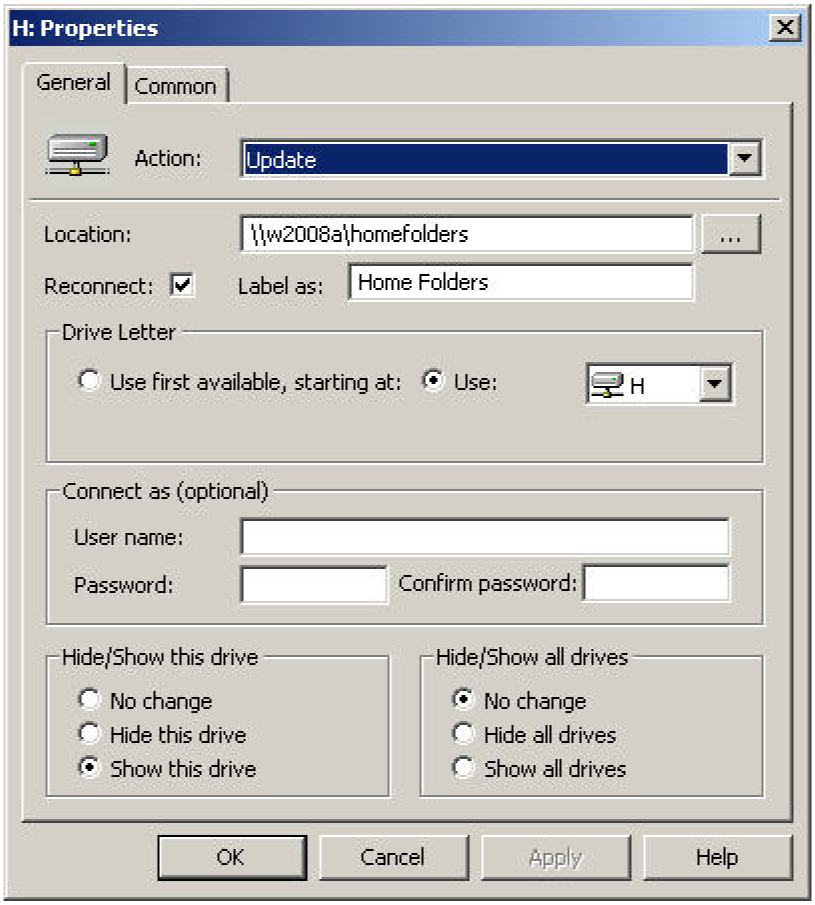
Last changed: 5/10/2008 12:48:51 PM

Figure 6.8: Group Policy Preferences enable rich customization of the windows environment, including elements like mapping drive letters to common shares.

As you'll also see in Figure 6.8, the potential for customizable control available through GPPs is remarkable. Within either half, one can easily control elements like drive mappings, environment variables, files and folders, data sources, local users and groups, power options, printers, and much more.

To give you an example of one use of GPPs that has traditionally been accomplished through login scripts, consider your need for setting drive mappings for users' home drives. With login scripts, the process to accomplish this task typically involves creating the script, storing that script in the domain's SYSVOL, and configuring each user to process the script through their user object within Active Directory Users and Computers. Using GPPs this process gets quite a bit simpler. In this example, let's assume that home drives are typically mapped to the *H:* drive and are stored within the *\\w2008a\homefolders* share. To use a GPP to set this for all computers in the domain, use the following process:

- Create a new GPO and launch the GPME. Navigate to *User Configuration* | *Preferences* | *Windows Settings* | *Drive Maps*.
- In the right pane of the resulting screen, select *New* | *Mapped Drive*. The window will look similar to Figure 6.9.
- Within that window, change the selections to match what is shown in Figure 6.9. Click *OK* when complete.
- Close the GPME and link the GPO to the domain.



H: Properties

General | Common

Action: Update

Location: \\w2008a\homefolders

Reconnect: ☑ Label as: Home Folders

Drive Letter

○ Use first available, starting at: ● Use: H

Connect as (optional)

User name:

Password: Confirm password:

Hide/Show this drive

○ No change
○ Hide this drive
● Show this drive

Hide/Show all drives

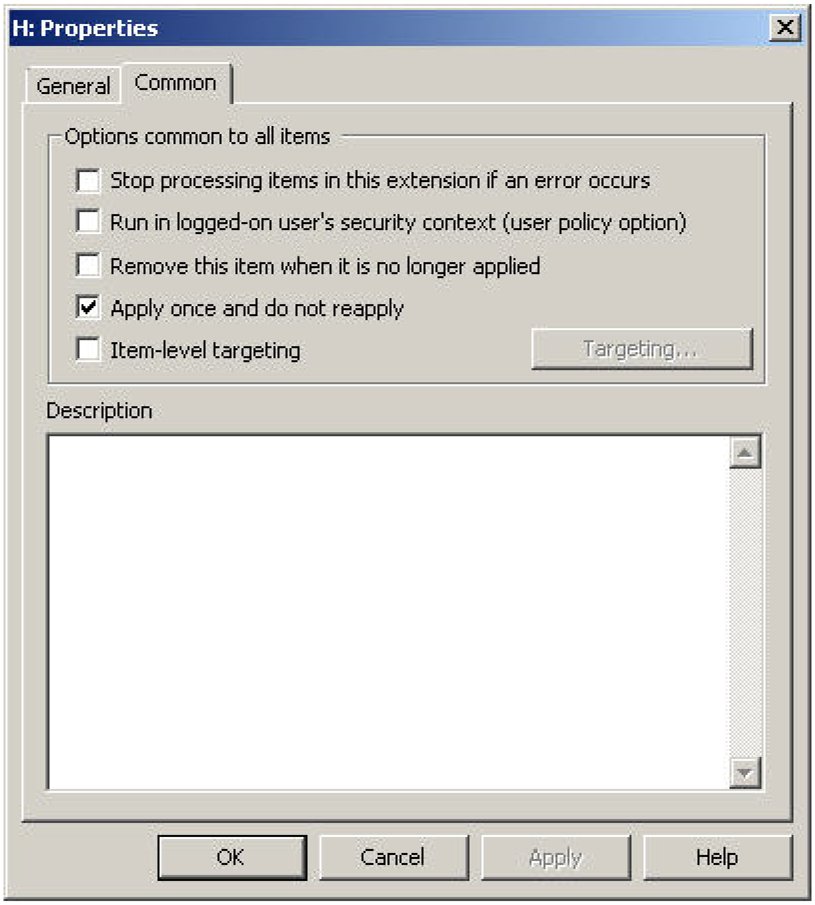
● No change
○ Hide all drives
○ Show all drives

Figure 6.9: Much of the ease of GPPs stems from their graphical interface for common administrative tasks. This window configures drive mappings.

By completing these four steps you have accomplished the same drive mapping that required scripting knowledge as well as the time-consuming management of user-specific settings within Active Directory Users and Computers. Yet this is completed in a much shorter amount of time and with much easier management and troubleshooting in the future. Through their reliance on Group Policy for distribution, GPPs enable common customizations to be managed through the same tools used to manage Group Policy.

> The client-side code required to process GPPs is natively available within Windows Server 2008. However, Client-Side Extensions (CSEs) must be downloaded and installed to all other operating systems for them to recognize and process GPPs. You can find links for CSEs at: http://support.microsoft.com/kb/943729.

What we haven't discussed yet with GPPs has to do with one of their greatest strengths. Unlike most of traditional Group Policy, GPPs have the unique capability in that they can be configured to be mere "suggestions" rather than enforced "policies" as we're used to seeing. Consider the situation where you want to "suggest" an initial environment variable setting for users, but allow them the ability to later change that setting if they desire. Using traditional Group Policy, this is not possible because traditional Group Policy is intended to be an enforcement mechanism. Each time the Group Policy Refresh Interval passes, the Group Policy client will change any modified settings back to their initial configuration.



Options common to all items

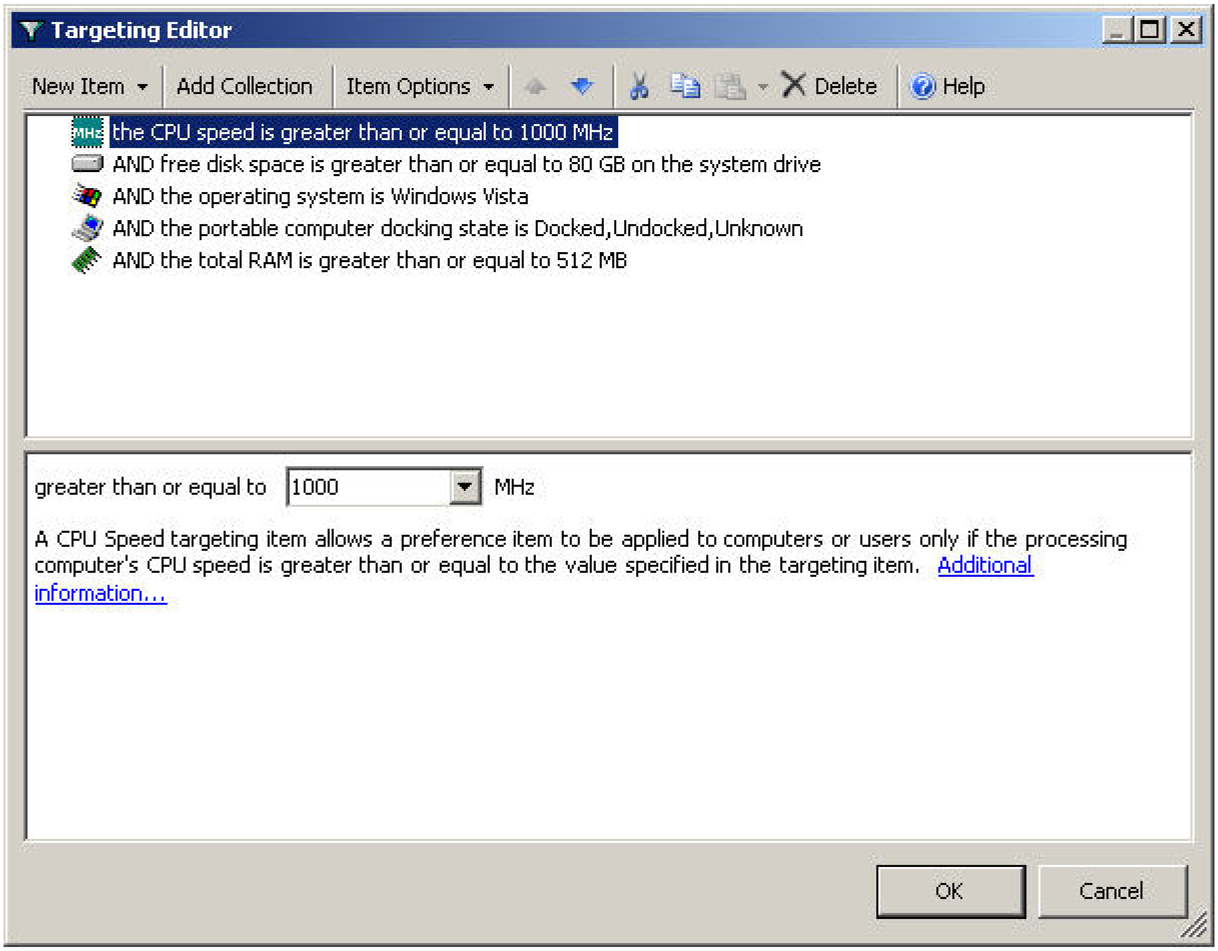
- □ Stop processing items in this extension if an error occurs
- □ Run in logged-on user's security context (user policy option)
- □ Remove this item when it is no longer applied
- ☑ Apply once and do not reapply
- □ Item-level targeting

Figure 6.10: A major portion of GPPs power arrives from what can be set within the Common tab.

Figure 6.10 shows the *Common* tab found within all GPP settings. There look for the configuration titled *Apply once and do not reapply*. By checking this box, the GPP will make the configuration change, but it will not reset that change if a user later decides that they want to change their setting away from what you "suggest".

> This ability to make GPP settings optional gives you the ability to set up a standard operating environment, while still allowing your users to customize that environment to their needs.

Yet another of GPP's powers arrives from the ability to further target GPP application based on a set of characteristics. Also seen under the *Common* tab is a link titled *Item-level targeting*. Checking this box and then clicking the *Targeting* button brings forward a screen similar to Figure 6.11. Item-level targeting provides you the ability to link a GPP to an Organizational Unit, but instruct the policy only to process when the client object meets a preconfigured set of criteria.



the CPU speed is greater than or equal to 1000 MHz
AND free disk space is greater than or equal to 80 GB on the system drive
AND the operating system is Windows Vista
AND the portable computer docking state is Docked,Undocked,Unknown
AND the total RAM is greater than or equal to 512 MB

greater than or equal to 1000 MHz

A CPU Speed targeting item allows a preference item to be applied to computers or users only if the processing computer's CPU speed is greater than or equal to the value specified in the targeting item. Additional information...

Figure 6.11: GPP item-level targeting enables an enhanced mechanism for granularly targeting GPPs to specific objects.

In Figure 6.11 item-level targeting has been set to only apply the GPP when the object's CPU speed is greater than 1000 MHz, free disk space is greater than or equal to 80 GB, the operating system is Windows Vista, the machine is a portable computer that is docked, undocked, or unknown, and the RAM is greater than or equal to 512 MB. Considering the options available, the level of targeting can be as granular as your needs.

To set item-level targeting, simply click the *New Item* button and select an item. Upon selecting an item, configure its options in the bottom pane. Click *OK* to complete the process. Once complete, objects will only apply the policy when they meet the targeting guidelines.

Group Policy's Centralized Control Enhances Your Ability to Manage Your Infrastructure

In this short chapter, we have only scratched the surface of what you can enable and control using Group Policy and Group Policy Preferences within your Windows Server 2008 infrastructure. There are additional topics associated with targeting, best practices, design and implementation elements, and supportability that go far beyond what we can cover in this short chapter.

> 📖 If you want to learn more about Group Policy in Windows Vista and Windows Server 2008, start your learning with this Web site: http://technet2.microsoft.com/WindowsVista/en/library/5ae8da2a-878e-48db-a3c1-4be6ac7cf7631033.mspx?mfr=true.

In Chapter 7, we'll start a two-chapter series on the topic of Terminal Services. Terminal Services gets a substantial facelift in Windows Server 2008, finally getting some of the benefits formerly only available through other application platforms like Citrix XenApp (Presentation Server). This two-part series on Terminal Services will start with an introductory exploration of the new features and later conclude with a discussion on the new and advanced topics that you're sure to enjoy.

Download Additional eBooks from Realtime Nexus!