EXAM OBJECTIVES

Professional ▶

Exam 70-210

- Deploy service packs.
- Install applications by using Windows Installer packages.
- Implement, configure, manage, and troubleshoot local Group Policy.

Server ▶

Exam 70-215

- Deploy service packs.
- Implement, configure, manage, and troubleshoot policies in a Windows 2000 environment.
  - Implement, configure, manage, and troubleshoot Local Policy in a Windows 2000 environment.
  - Implement, configure, manage, and troubleshoot System Policy in a Windows 2000 environment.

Directory Services ▶

Exam 70-217

- Implement and troubleshoot Group Policy.
  - Create a Group Policy object (GPO).
  - Link an existing GPO.
  - Delegate administrative control of Group Policy.
  - Modify Group Policy inheritance.
  - Filter Group Policy settings by associating security groups to GPOs.
  - Modify Group Policy.
- Manage and troubleshoot user environments by using Group Policy.
  - Control user environments by using Administrative Templates.
  - Assign script policies to users and computers.

Continued ▶

EXAM OBJECTIVES ***Continued***

- Manage and troubleshoot software by using Group Policy.
  - Deploy software by using Group Policy.
  - Maintain software by using Group Policy.
  - Configure deployment options.
  - Troubleshoot common problems that occur during software deployment.
- Manage network configuration by using Group Policy.
- Apply security policies by using Group Policy.

CHAPTER

10 Using System Policy and Group Policy

Chapter 10 is all about using policies to manage users and computers in a Windows 2000 environment. After a quick overview of policies, I'll explain how to use System Policy to manage non-Windows 2000 client computers and their users on a Windows 2000 network.

I'll spend the rest of the chapter discussing how to use Group Policy to manage Windows 2000 computers and their users. *Group Policy* is a policy that contains rules and settings that are applied to Windows 2000 computers, their users, or both. Group policy settings can be stored on the local computer (local Group Policy), or in Group Policy objects (GPOs) that are stored in Active Directory. I'll explain how Group Policy is implemented and the order in which it is applied. Then I'll show you how to create and configure GPOs. After that, I'll address the numerous types of settings you can configure in Group Policy, including settings that manage user environments, scripts, security, folder redirection, and software deployment. Finally, I'll provide you with some tips for troubleshooting Group Policy.

Chapter Pre-Test

1. What is System Policy?
2. In what sequence is System Policy applied?
3. What is Group Policy?
4. What is Group Policy called when it is implemented directly on the local computer?
5. Fill in the blanks: Group Policy consists of two components: an Active Directory object, called a _____ _____ _____, and a series of files and folders that are automatically created when the Active Directory object is created.

Overview of Policies in Windows 2000

In a Windows 2000 network environment, various types of policies are used by administrators to manage users and computers. Some policies are set on the local computer and apply only to that computer, to users who log on to that computer, or both. Other policies are set at the domain, site, or organizational unit level, and apply to multiple users, computers, or both.

The two primary types of policies used in a Windows 2000 network environment are System Policy and Group Policy. *System Policy* is used to manage non-Windows 2000 client computers (and their users) on a Windows 2000 network. *Group Policy* is used to manage Windows 2000 computers, their users, or both. I'll explain how to manage both System Policy and Group Policy in this chapter.

Managing System Policy

System Policy is a collection of Administrator-created user, group, and computer system policies that enable an administrator to manage *non-Windows 2000* client computers (and their users) on a Windows 2000 network. For example, you can use System Policy to restrict the user's ability to perform certain tasks or to enforce mandatory display settings, such as wallpaper and color scheme. You can also use System Policy to configure computer settings, such as a custom logon banner that is displayed each time a user logs on to a particular computer.

The types of client computers that you can create System Policy for include: Windows NT 4.0 computers, Windows 95 computers, and Windows 98 computers. Microsoft originally intended to allow System Policy to apply to Windows 2000 computers, but that capability was removed between Beta 3 and the final release of Windows 2000.

System Policy, like mandatory user profiles, enables an administrator to control the work environment of users on the network. System Policy, however, gives the administrator far more configurable options than a mandatory user profile. Administrators can use System Policy to provide a consistent environment for a large number of users, or to enforce a specified work environment for problem users who demand a significant amount of administrator time.

In addition to enabling the administrator to limit the changes users can make to their work environments, System Policy can be used as a security measure to limit access to parts of the network, to restrict the use of specific tools such as the Registry Editor, and to remove the Run command option from the Start menu.

The following sections explain the components that can be included in System Policy, including user system policy, group system policy, and computer system policy.

User System Policy

A *user system policy* is a collection of settings that restrict a user's program and network options and can enforce a specified configuration on the user's work environment. There are two types of user system policies: an individual user policy and the Default User policy.

An *individual user policy* applies to a single, specific user. Normally, an individual user policy is created only when a user requires a unique policy that differs from any existing Default User or group system policy.

The *Default User policy*, contrary to what its name implies, does not exist by default. Rather, it is created when an Administrator initially creates a System Policy file. When the Default User policy is initially created, it doesn't contain any settings that restrict users. The Administrator must configure any desired user restrictions in the Default User policy. The Default User policy applies to a user only if the user does *not* have an individual user policy.

There are a variety of settings that you can configure in a user system policy. Figure 10-1 shows all of the configurable options for a Windows NT individual user policy. The same list of configurable options is available for the Default User policy.

The actual process of configuring the check boxes in this list is covered in the "Creating a System Policy File" section later in this chapter.

When a user logs on to a non-Windows 2000 client computer on a Windows 2000 network, Windows NT (or Windows 95 or 98) permanently overwrites the existing settings in the HKEY_CURRENT_USER section of the registry on the computer to which the user logs on with the settings contained in the user system policy.

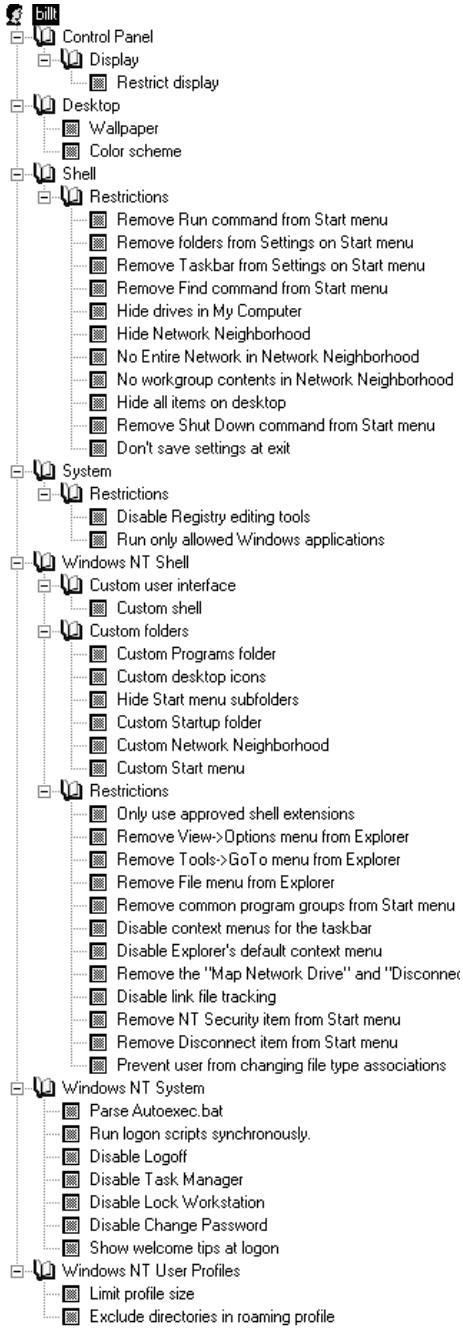

FIGURE 10-1 Configurable settings in a Windows NT 4.0 user system policy

Group System Policy

A *group system policy* is a policy that applies to a group of users. A group system policy applies to all users that are members of a group (that has a group policy) and that do *not* have individual user policies. Group system policies have the same configurable options as user system policies.

A group system policy should be created when more than one user requires the same settings, because it takes far less time to create one group policy than to create multiple individual user policies.

A user may belong to multiple groups that each have a group system policy. When this is the case, the policies are applied in a specific order.

For example, suppose that a user of a Windows NT 4.0 client computer, JohnS, belongs to three groups: Domain Admins, Managers, and Sales, and that each of these three groups has a group system policy. The groups are listed in this order, from the top down, in the Group Priority dialog box in System Policy Editor. Also suppose that JohnS does *not* have an individual user policy. When JohnS logs on to the domain, the group system policy for the Sales group (which has the lowest group priority because it is at the bottom of the list) is applied *first*. Then the group system policy for the Managers group is applied. Finally, the group system policy for the Domain Admins group (which has the highest group priority because it is at the top of the list) is applied to JohnS. As each group system policy is applied, it overwrites any conflicting settings from previously applied group policies. The last group system policy applied (in this case, the Domain Admins group system policy) takes precedence over the lower priority group system policies.

An Administrator can configure group system policy priority by moving a group up or down in the Group Priority dialog box. The group at the top of the box has the highest priority.

Computer System Policy

A *computer system policy* is a collection of settings that specifies a local computer's configuration. A computer system policy enforces the specified configuration on all users of a particular Windows NT 4.0, Windows 95, or Windows 98 client computer.

There are two types of computer system policies: an individual computer policy and the Default Computer policy.

An *individual computer policy* applies to a single, specific client computer. Normally, an individual computer policy is created only when a client computer requires a unique policy that differs from the Default Computer policy.

The *Default Computer policy*, like the Default User policy, is created when a System Policy file is initially created. The Default Computer policy applies to a client computer only if the computer does *not* have an individual computer policy.

There are a variety of settings that you can configure in a computer system policy, as shown in Figure 10-2.

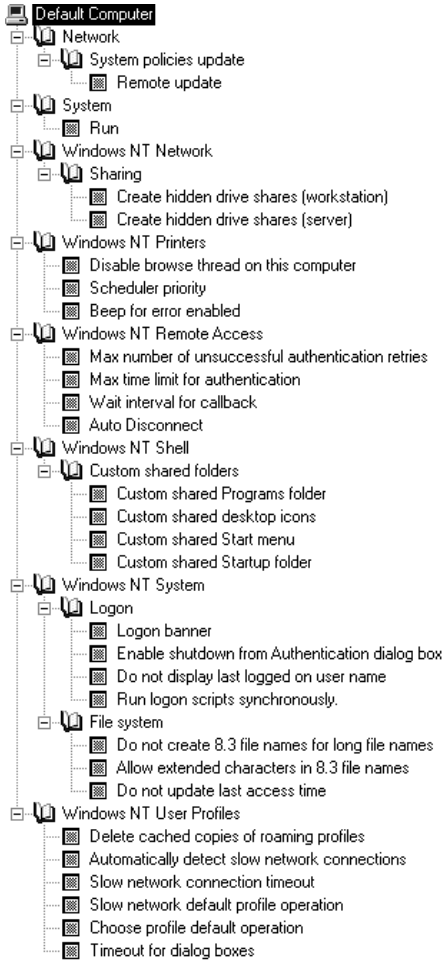

FIGURE 10-2 Configurable settings in a Windows NT 4.0 computer system policy

An individual computer policy and the Default Computer policy both have the same configurable options. The actual process of configuring a computer system policy is covered in the "Creating a System Policy File" section later in this chapter.

When a user logs on to a non-Windows 2000 client computer on a Windows 2000 network, Windows NT (or Windows 95 or 98) permanently overwrites the existing settings in the HKEY_LOCAL_MACHINE section of the registry on the computer to which the user logs on with the settings contained in the computer system policy.

How System Policy Is Applied

System Policy is applied to a user or a computer in a predefined, systematic manner. When a user logs on, the user's roaming or local user profile is applied first, and then System Policy is applied. If settings in the System Policy conflict with settings in the user profile, the System Policy settings take precedence.

System Policy is applied in the following sequence:

1. If a user has an individual user policy, it is applied.
2. If a user does *not* have an individual user policy, and the user is a member of a group that has a group system policy, then the group system policy (or policies, if the user is a member of multiple groups that each have a group system policy) is applied.
3. If a user does *not* have an individual user policy, then the Default User policy is applied.

TIP

If a user that does *not* have an individual user policy has a group system policy that conflicts with the Default User policy, then the settings in the Default User policy take precedence, because the Default User policy is applied *after* the group system policy is applied.

4. If the non-Windows 2000 client computer the user logs on to has an individual computer policy, it is applied.

5. If the non-Windows 2000 client computer the user logs on to does *not* have an individual computer policy, then the Default Computer policy is applied.

The end result is that a user has one of the following user and group system policy combinations applied:

- An individual user policy only
- The Default User policy only
- A combination of the Default User policy and a group system policy (or policies, if the user is a member of multiple groups that each have a group system policy)

In addition, the client computer to which the user logs on has either an individual computer policy or the Default Computer policy applied.

Creating a System Policy File

A System Policy file doesn't exist by default — it must be created, configured, and saved by an Administrator. System Policy is managed and configured by using the System Policy Editor (`Poledit.exe`). You can use the Windows 2000 System Policy Editor to create System Policy that will apply to Windows NT 4.0 client computers (and the users of these computers). System Policy Editor is installed, by default, on Windows 2000 Server/Advanced Server computers. You can make the System Policy Editor available on a Windows 2000 Professional computer by installing the ADMINPAK. After a System Policy file is created, it should be saved in the `NETLOGON` share of one of the domain controllers in the domain. A Windows NT 4.0 System Policy file should be named `Ntconfig.pol`.

You can use the System Policy Editor (`Poledit.exe`) on either a Windows 95 or Windows 98 computer to create a System Policy file that will apply to both Windows 95 and Windows 98 client computers (and the users of these computers). The System Policy Editor is not installed by default on Windows 95/98 computers — you must install this tool from the Windows 95/98 compact disc. A Windows 95/98 System Policy file should also be saved in the `NETLOGON` share of one of the domain controllers in the domain, and the file should be named `Config.pol`.

STEP BY STEP

CREATING A WINDOWS NT 4.0 SYSTEM POLICY FILE

1. Select Start ➪ Run.
2. In the Run dialog box, type **poledit** and click OK.
3. In the System Policy Editor dialog box, select File ➪ New Policy.
4. Two icons are displayed: Default Computer and Default User.

   Customize the Default Computer and Default User policies as appropriate. To customize a policy, double-click the policy's icon. Then, in the policy's Properties dialog box, click the + next to the options you want to expand and configure. Then configure the check box next to each option you want to configure. Each check box has three possible configurations:

   - **Grayed out:** Causes the current setting for this option to be retained. This is the default setting for all configurable options in System Policy.
   - **Checked:** Causes this option to be applied.
   - **Cleared (white):** Causes the *opposite* of this option to be applied. For example, if the option is called "Remove Run command from Start Menu," clearing this option will ensure that the Run command is displayed in the Start Menu.
5. Create and customize individual user, individual computer, and group system policies as appropriate.

   To create a new policy, select the appropriate option from the Edit menu (either Add User, Add Computer, or Add Group). Then, in the Add User, Add Computer, or Add Group dialog box, type the name of the user, computer, or group for which you want to create a policy. Click OK.

   Then customize your new policy (or policies) by using the instructions in Step 4.
6. After you create and customize policies, save the System Policy file. Select File ➪ Save As in the System Policy Editor dialog box. Save the file to the `NETLOGON` share on a domain controller as `Ntconfig.pol`.
7. Exit System Policy Editor.

To create a Windows 95 or Windows 98 System Policy file, follow the preceding steps, except:

1. Run the System Policy Editor on a Windows 95 or Windows 98 computer.
2. Save the System Policy file as `Config.pol` instead of `Ntconfig.pol`.

Using System Policy Editor to Manage the Local Windows 2000 Computer

As I mentioned earlier, you can't use System Policy to manage a Windows 2000 client computer (and its users). However, you can use System Policy Editor to directly edit the registry on a Windows 2000 computer. You must be a member of the Administrators group on the local computer to edit the registry.

CAUTION

This is *not* a recommended practice, because using System Policy Editor permanently changes the registry on a computer—if you decide you want to revert to default settings at a later date, you'll have to manually change each and every setting that you previously changed.

I recommend that you use Group Policy (or Local Group Policy) to configure settings on a Windows 2000 computer instead of using the System Policy Editor, because registry changes made by Group Policy are easily reversible.

That said, to edit the registry on a Windows 2000 computer by using System Policy Editor, start System Policy Editor, then select File ➪ Open Registry. Then configure local computer and local user settings as needed. When you're finished making changes, select File ➪ Save, then close System Policy Editor.

Troubleshooting System Policy

System Policy can present an administrator with some challenging problems. Here are a couple of the most common System Policy problems and their recommended solutions:

- **A group system policy setting is not being applied to all members of the group.** The most common cause of this problem is that some of the users of this group are also members of another group that has a conflicting group system policy with a higher group policy priority than the first group. To solve the problem, you may need to change the group policy priority, or perhaps change the users' group memberships.

- **After you remove the System Policy file from the domain controllers, its settings are still applied to users and computers.** Unfortunately, System Policy permanently modifies the registry, and does not revert to default settings even after the System Policy file is removed. To solve this problem, you must create a new System Policy file that reverses each setting that was previously changed in the original System Policy file.

TIP

In order to create the new System Policy file, you'll need to have a record of each and every change that was applied by the old System Policy file.

Once you've implemented the new System Policy, and each user has logged on, you can then remove the new System Policy file.

Managing Group Policy

Group Policy is a brand new Windows 2000 feature. *Group Policy* is a policy that contains rules and settings that are applied to Windows 2000 computers, their users, or both, that are located in a specific part of Active Directory. I like to think of Group Policy as System Policy on steroids — it's much bigger, meaner, and more powerful than System Policy.

Group Policy can only be used to manage Windows 2000 computers on a network (and the users of those computers). If you have other Windows-based client computers, such as Windows NT 4.0, Windows 95, or Windows 98 computers, you can only manage those computers (and their users) by using System Policy.

EXAM TIP

The Directory Services exam has multiple objectives on Group Policy. Add that to the fact that Group Policy is a nifty new feature in Windows 2000, and you can rest assured of finding several tough Group Policy questions on this exam.

By using Group Policy, an Administrator can specify and manage a number of user and computer settings, including:

- **Settings that manage user environments:** You can specify a user's desktop settings, such as wallpaper and Active Desktop settings. You can also configure the items that appear in a user's Start menu, and several other user and computer settings that affect a user's environment.
- **Settings that manage scripts:** You can configure user logon and logoff scripts, and computer startup and shutdown scripts.
- **Settings that manage security:** You can specify security settings, such as account policies, local policies, event log settings, and so on.
- **Settings that redirect folders:** You can cause folders in a user's profile to be redirected to a shared folder on a network server.
- **Settings that manage software deployment:** You can specify an application that will be automatically installed on a computer when the computer starts, or automatically installed when a user opens a file with an extension associated with that application. You can manage the deployment of multiple applications by using Group Policy.

Group Policy is typically implemented in Active Directory. However, Group Policy can be implemented directly on the local computer. When implemented on the local computer, Group Policy is called Local Group Policy.

Local Group Policy consists of a series of files and folders that are automatically created during the installation of Windows 2000 on the local computer. Local Group Policy files and folders are stored in the `SystemRoot\System32\GroupPolicy` folder. Local Group Policy applies to the local computer, and to users that log on to the local computer.

Group Policy consists of two components: an Active Directory object, called a Group Policy object (GPO), and a series of files and folders that are automatically created when the GPO is created. Group Policy files and folders are stored in the `SystemRoot\SYSVOL\sysvol\domain_name\Policies` folder on domain controllers in a Windows 2000 domain. Each GPO is associated with a specific Active Directory container, such as a site,

a domain, or an organizational unit (OU). Group Policy applies to computers, users, or both, that are contained within the site, domain, or OU with which the GPO is associated. An Active Directory container may have more than one GPO associated with it.

How Group Policy Is Applied

Before you actually configure Group Policy settings, it's a good idea to understand the order in which Group Policy settings are applied to Windows 2000 computers and their users. Group Policy is applied in a predefined, systematic manner.

In general, when a user logs on, the user's roaming or local user profile is applied first. Then Local Group Policy is applied, and finally Group Policy is applied. If any settings in Group Policy (either Local Group Policy or Group Policy) conflict with settings in the user's profile, the Group Policy settings take precedence. If any Local Group Policy settings conflict with Group Policy settings, the Group Policy settings take precedence and override the conflicting Local Group Policy settings, because the policy applied *last* takes precedence, and Group Policy is applied *after* Local Group Policy is applied.

By default, Group Policy is applied in the following order, and all processes that occur in one step are completed before the processes in the next step begin.

1. When a user powers on a Windows 2000 computer, all Group Policy settings that apply to the computer are applied.
2. If the Group Policy settings that apply to the computer specify that a startup script (or scripts) be run, this script is run.
3. When a user logs on, the user's profile is loaded, then all Group Policy settings that apply to the user are applied.
4. If the Group Policy settings that apply to the user specify that a logon script (or scripts) be run, this script is run. Then, if a user has an individual logon script assigned to his or her user account, this logon script is run.
5. When a user logs off, if the Group Policy settings that apply to the user specify that a logoff script (or scripts) be run, this script is run.
6. When a user shuts down a Windows 2000 computer, if the Group Policy settings that apply to the computer specify that a shutdown script (or scripts) be run, this script is run.

Inheritance and Group Policy

Another factor that affects how Group Policy is applied is inheritance. An Active Directory object, such as a user or a computer, normally inherits Group Policy from the container in which the object resides and from the parent containers above it in the Active Directory tree. Group Policy is applied from the top of the tree down. This means that the normal sequence of Group Policy application is first site, then domain, then OU.

The key point is that when Group Policy settings conflict, the Group Policy that is applied *last* is the policy that takes precedence. Because the last Group Policy that is normally applied is the Group Policy associated with the OU that a computer or user is contained in, the Group Policy of the OU normally takes precedence when settings conflict. Here are a couple of examples that explain how inheritance affects the application of Group Policy.

Example 1 Suppose that a user is contained in an OU named Denver that has a Group Policy. The Denver OU is contained in a domain named `domain1.com` that also has a Group Policy. When Group Policy is applied, it is applied first at the domain level, and then at the OU level. There are no conflicting Group Policy settings between `domain1.com` and the Denver OU. Therefore, in this case, the Group Policy settings are additive, and the Group Policy settings associated with `domain1.com` and the Group Policy settings associated with the Denver OU are both applied.

Example 2 Suppose that a user is contained in an OU named Seattle that has a Group Policy. The Seattle OU is contained in a domain named `domain3.org` that also has a Group Policy. There are some conflicting Group Policy settings between `domain3.org` and the Seattle OU. The Group Policy for `domain3.org` is applied first. Then the Group Policy for the Seattle OU is applied. All nonconflicting settings in the Group Policy for `domain3.org` remain applied after the Group Policy for the Seattle OU is applied. However, any settings in the Group Policy for `domain3.org` that conflict with the Group Policy for the Seattle OU are replaced by the Group Policy settings for the Seattle OU, because this Group Policy is applied last and takes precedence.

An Administrator can modify certain inheritance settings of GPOs and their associated containers. I'll explain how to configure these settings a little later in this chapter.

Periodic Updates of Group Policy

By default, all Windows 2000 computers (that are not domain controllers) request and receive Group Policy updates from domain controllers approximately every 90 minutes. Domain controllers request updates from Active Directory every 5 minutes.You can modify these intervals to suit your needs.

TIP

Just because Group Policy settings are updated throughout the day doesn't mean that all tasks specified by the Group Policy setting changes will occur. For example, software installation and folder redirection only occur at startup or user logon.

Managing Local Group Policy

Local Group Policy is configured on an individual Windows 2000 computer by using the Group Policy snap-in to the Microsoft Management Console (MMC). You must be a member of the Administrators group on the local computer to manage Local Group Policy.

As you may recall, Local Group Policy is applied first, so if its settings conflict with Group Policy settings, the conflicting Group Policy settings take precedence, because they are applied last.

STEP BY STEP

CONFIGURING LOCAL GROUP POLICY ON THE LOCAL COMPUTER

1. Select Start ➪ Run.
2. In the Run dialog box, type **gpedit.msc** and click OK.
3. The Group Policy snap-in to the MMC is displayed, as shown in Figure 10-3. Notice the separate Computer Configuration and User Configuration sections.

   Settings in the Computer Configuration section apply to the local computer. Settings in the User Configuration section apply to all users who log on to the local computer.

   To configure settings in this dialog box, expand folders in the left pane until the policy setting you want to configure is displayed in the right pane. Then, in the right pane, double-click the policy you want to configure, configure its settings as appropriate, and click OK.

STEP BY STEP *Continued*

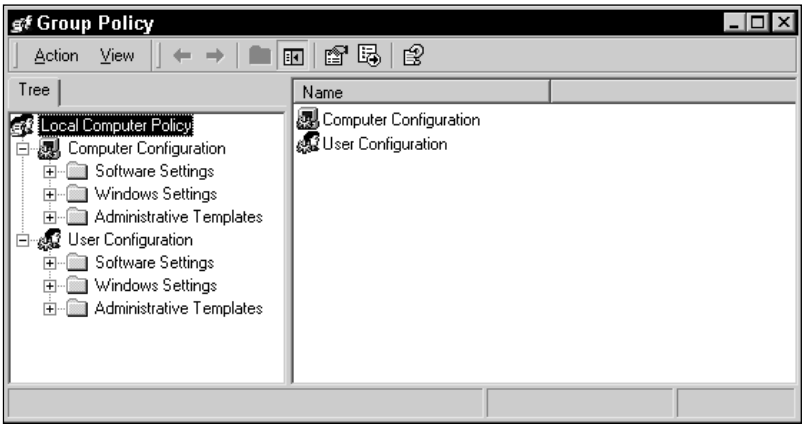

FIGURE 10-3 Configuring Local Group Policy

TIP

For more information on the many settings you can configure, see the sections later in this chapter titled "Configuring Group Policy Settings to Manage User Environments," "Configuring Group Policy Settings to Manage Scripts," "Configuring Group Policy Settings to Manage Security," "Configuring Group Policy Settings to Redirect Folders," and "Configuring Group Policy Settings to Manage Software Deployment."

4. When you're finished configuring Local Group Policy, close the Group Policy dialog box.

You may remember using the Local Security Policy tool (Start ➪ Programs ➪ Administrative Tools ➪ Local Security Policy) to set account policies (such as password policy and account lockout policy) and local policies (such as user rights assignment and audit policy) on the local Windows 2000 computer .The Local Security Policy tool was discussed in chapter 9. The Group Policy snap-in to the MMC enables you to configure these same policies, plus many more, on the local computer.

You can also configure Local Group Policy on a remote Windows 2000 computer by using the Group Policy snap-in to the MMC.

STEP BY STEP

CONFIGURING LOCAL GROUP POLICY ON A REMOTE WINDOWS 2000 COMPUTER

1. Select Start ➪ Run.
2. In the Run dialog box, type **mmc** and click OK.
3. A MMC dialog box named Console1 is displayed. Select Console ➪ Add/Remove Snap-in.
4. In the Add/Remove Snap-in dialog box, click Add.
5. In the Add Standalone Snap-in dialog box, highlight Group Policy and click Add.
6. In the Select Group Policy Object dialog box, click Browse.
7. In the Browse for a Group Policy Object dialog box, click the Computers tab.
8. On the Computers tab, select the "Another computer" option, and type in the name of the remote Windows 2000 computer for which you want to configure Local Group Policy. Click OK.
9. In the Select Group Policy Object dialog box, click Finish.
10. In the Add Standalone Snap-in dialog box, click Close.
11. In the Add/Remove Snap-in dialog box, click OK.
12. On the MMC console, maximize the window named Console Root. (This console is virtually identical to the console used to manage Local Group Policy on the local computer.)Then, in the left pane, click the + next to the name of the remote Windows 2000 computer. Expand folders in the left pane until the policy setting you want to configure is displayed in the right pane. Then, in the right pane, double-click the policy you want to configure, configure its settings as appropriate, and click OK.
13. When you're finished configuring the Local Group Policy for the remote Windows 2000 computer, close the MMC.

Creating Group Policy Objects in Active Directory

You can use several tools to create Group Policy objects (GPOs) in Active Directory. The specific tool used generally depends on what type of container (site, domain, or OU) will be associated with the GPO.

- **To create a GPO associated with a site,** use Active Directory Sites and Services (Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services).

- **To create a GPO associated with a domain or OU,** use Active Directory Users and Computers (Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers).

You can also use the Group Policy snap-in to the MMC to create and manage GPOs.

You must have the Read, Write, and Create All Child Objects Active Directory permissions to the container (site, domain, or OU) in order to create a GPO that will be associated with that container. If you're a member of the Enterprise Admins group, or a member of the domain's Administrators or Domain Admins groups, you have the necessary permissions to create GPOs.

Now I'll show you how to create a new GPO. You can use the steps that follow to create a GPO associated with a domain or OU by using Active Directory Users and Computers. The steps to create a GPO associated with a site are virtually identical, except that you must use the Active Directory Sites and Services tool.

STEP BY STEP

CREATING A NEW GROUP POLICY OBJECT

1. From the desktop, select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. The Active Directory Users and Computers dialog box appears. In the left pane, expand domains and OUs as necessary until the domain or OU for which you want to create a GPO is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties. (You can also right-click the domain or OU and select Properties from the menu that appears.)
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. The Group Policy tab is displayed, as shown in Figure 10-4. Notice that by default, this OU does not have a GPO associated with it. Also notice the "Block Policy inheritance" check box.

   To create a new GPO, click New.
5. The "New Group Policy Object" appears in the Group Policy Object Links column. To rename this new GPO, type in a new name and press Enter.

STEP BY STEP *Continued*

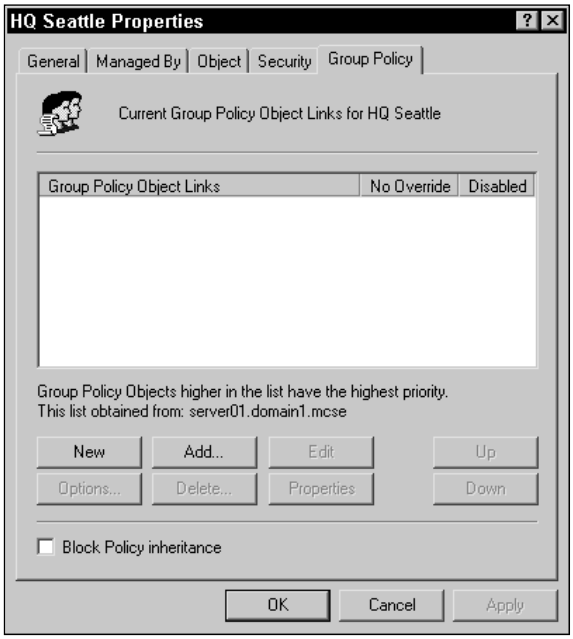

FIGURE 10-4 Creating a new Group Policy object (GPO)

6. To create additional GPOs, repeat Step 5.
7. When you're finished creating a GPO, you can configure its properties (which I'll discuss throughout the rest of this chapter), or you can click Close.
8. Close Active Directory Users and Computers.

Configuring and Modifying Group Policy Objects

When GPOs are first created, they have no initial settings. You must configure GPOs before you can use them to help you manage the Windows 2000 computers (and their users) on your network.

You use the same tool to configure a GPO that you used to create the GPO — either Active Directory Users and Computers (if the GPO is associated with a domain or an OU) or Active Directory Sites and Services (if the GPO is associated with a site).

In this section I'll explain how to modify a GPO's Group Policy inheritance settings, how to disable computer or user configuration settings, and how to configure security for a GPO.

TIP

I'll show you how to modify GPOs primarily by using Active Directory Users and Computers, but if you want to use Active Directory Sites and Services, the steps to perform the various tasks are virtually identical.

Modifying Group Policy Inheritance

An Administrator can modify how inheritance occurs when Group Policy settings are applied. There are two primary settings you can configure that affect Group Policy inheritance. One of these settings is configured on the Active Directory container with which the GPO is associated, and the second is configured on the GPO itself.

The setting you can configure on the Active Directory container (site, domain, or OU) with which a GPO is associated is a check box titled "Block Policy inheritance." If this check box is selected, Group Policy settings from parent objects in the Active Directory tree are blocked from this container and will not affect this container.

STEP BY STEP

BLOCKING GROUP POLICY INHERITANCE ON A SITE, DOMAIN, OR OU

1. If you want to block Group Policy inheritance on a domain or an OU, select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.

   Or, if you want to block Group Policy inheritance on a site, start Active Directory Sites and Services.

2. In the left pane of the dialog box, expand sites, domains, and OUs as necessary until the site, domain, or OU you want to configure is displayed in the left pane. Highlight the site, domain, or OU, then select Action ➪ Properties.
3. In the site, domain, or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab (which is shown earlier in Figure 10-4), select the check box next to "Block Policy inheritance." Click OK.
5. Close Active Directory Users and Computers (or Active Directory Sites and Services).

The setting you can configure on the GPO itself is an option called "No Override." When this option is selected, settings in this GPO will take precedence and will *not* be overridden by any conflicting settings in a child object's GPO.

STEP BY STEP

CONFIGURING THE NO OVERRIDE OPTION ON A GPO

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO you want to configure and click Options.
5. The GPO Options dialog box appears, as shown in Figure 10-5. Notice the two configurable options: No Override and Disabled.

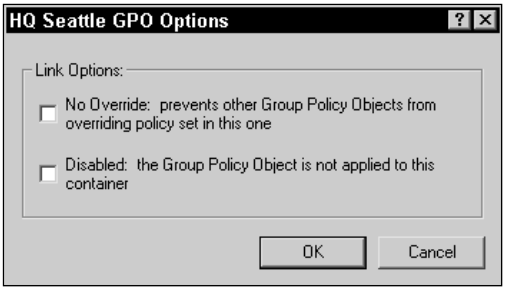

FIGURE 10-5 Configuring the No Override option

Select the check box next to "No Override: prevents other Group Policy Objects from overriding policy set in this one." Click OK.

6. The Group Policy tab reappears. A check mark is displayed in the No Override column next to the GPO you just configured. Click OK.
7. Close Active Directory Users and Computers.

Finally, there's a potential conflict between these two inheritance settings that I need to warn you about. For example, suppose that the No Override option is configured on a GPO associated with a domain (a parent object), *and* that the "Block Policy inheritance" option is configured on an OU in this domain (a child object). In this situation, the No Override option wins, and the "Block Policy inheritance" option on the OU is ignored. If the No Override option is configured on a GPO associated with a parent container, a child object *can't* block policy inheritance from that GPO. The No Override option always takes precedence.

EXAM TIP

If I were writing questions for the Directory Services exam, I'd write several long, convoluted questions testing the examinees' understanding of the No Override and "Block Policy inheritance" options. Make sure you thoroughly understand these two settings.

Disabling Computer Configuration or User Configuration Settings

If a particular GPO contains settings that will only affect computers, or contains settings that will only affect users, you should consider disabling the unused configuration settings in the GPO. Disabling computer configuration settings when only user settings are used (and disabling user configuration settings when only computer settings are used) will significantly speed up the application of the GPO.

STEP BY STEP

DISABLING UNUSED SETTINGS IN A GPO

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO you want to configure and click Properties.
5. The GPO Properties dialog box appears, as shown in Figure 10-6. Notice the two check boxes at the bottom of this dialog box.

STEP BY STEP *Continued*

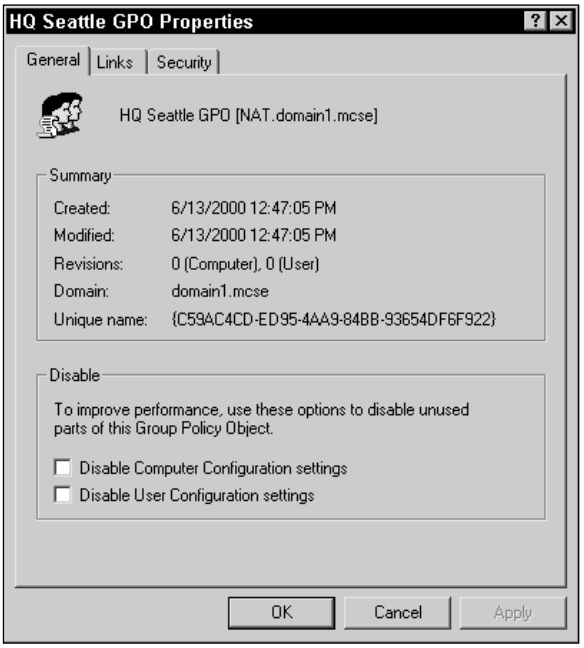

FIGURE 10-6 Disabling unused configuration settings in a GPO

Select either the "Disable Computer Configuration settings" check box or the "Disable User Configuration settings" check box, as appropriate, to disable the unused portion of this GPO.

6. When a check box is selected, Windows 2000 displays a Confirm Disable warning dialog box. Click Yes.
7. On the General tab in the GPO Properties dialog box, click OK.
8. On the Group Policy tab, click OK.
9. Close Active Directory Users and Computers.

Configuring Security for Group Policy Objects

Security is configured on GPOs to accomplish two different objectives:

- To specify the users, computers, or both to which the GPO applies
- To specify the users or groups who can administer the GPO

A GPO is applied only to users and computers that have the Read and Apply Group Policy Active Directory permissions to the GPO. By default, the Authenticated Users group is assigned the Read and Apply Group Policy Active Directory permissions to all newly created GPOs. The Authenticated Users group includes all users and computers in Active Directory.

If you don't want a GPO to be applied to all users and computers contained in the site, domain, or OU with which the GPO is associated, you must first remove the Authenticated Users group from the access control list for the GPO, then you must add the appropriate users, computers, and groups to the access control list for the GPO and assign these users, computers, and groups the Read and Apply Group Policy permissions.

The easiest way to specify the users and computers to which a GPO applies is to assign groups of users (or groups of computers) to the access control list for the GPO, and then to assign the Read and Apply Group Policy permissions to these groups for the GPO. This process is called *filtering Group Policy scope by using security groups*. If you filter the scope of a GPO by using security groups, it's conceivable that you could have multiple GPOs associated with a single container (such as an OU), with each GPO applying to a different group of users or computers within the container.

Security is also configured on GPOs so that the administration of the GPO can be delegated to other users on the network. A user (or group) must be assigned the Read and Write Active Directory permissions to the GPO in order to administer the GPO. By default, members of the Domain Admins and Enterprise Admins groups have both of these permissions.

STEP BY STEP

MODIFYING GPO SECURITY, FILTERING SCOPE BY USING SECURITY GROUPS, AND DELEGATING ADMINISTRATIVE CONTROL

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box. expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO you want to configure and click Properties.
5. In the GPO Properties dialog box, click the Security tab.

STEP BY STEP *Continued*

6. The Security tab appears, as shown in Figure 10-7. Notice that the Authenticated Users group is allowed, by default, the Read and Apply Group Policy permissions.

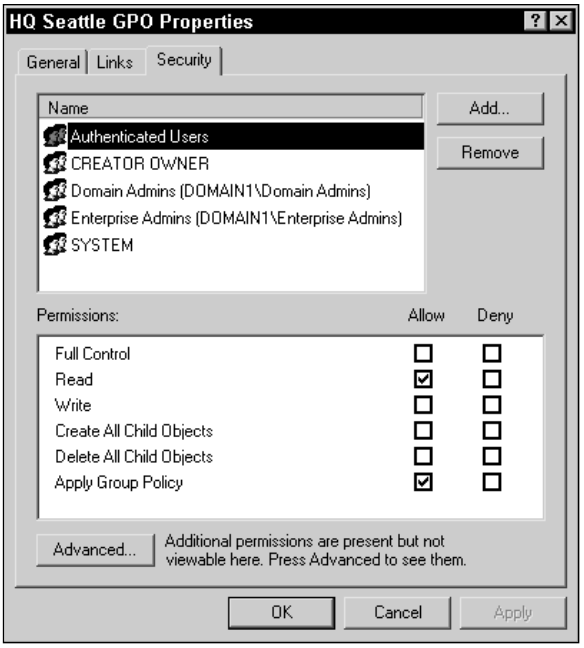

FIGURE 10-7 Assigning permissions to users, groups, and computers for a GPO

This tab is virtually the same as every other permissions dialog box you've seen so far in Windows 2000. It has the usual list of users and groups (and computers) at the top of the dialog box; and a list of permissions, along with a pair of Allow and Deny check boxes for each permission, at the bottom of the dialog box.

To *remove* a user, group (such as Authenticated Users), or computer from the permissions list for the GPO, highlight the user, group, or computer in the Name box, and click Remove.

To *add* a user, group, or computer to the Name box, click Add.

7. In the Select Users, Computers, or Groups dialog box, double-click each user, group, and computer you want to add. As you double-click each user, group, and computer, it appears in the bottom portion of the dialog box. Click OK.
8. On the Security tab, each user, group, and computer you added is automatically assigned the Read permission to the GPO.

STEP BY STEP *Continued*

If you want this GPO to apply to the user, group, or computer you just added, you'll have to manually assign the user, group, or computer the Apply Group Policy permission (in addition to the Read permission automatically assigned).

If you want to delegate administrative control of this GPO to a user or group you just added, you'll have to manually assign the user or group the Write permission (in addition to the Read permission automatically assigned).

To change the permissions of a user, group, or computer you added, highlight the user, group, or computer in the Name box, then select or clear the appropriate check boxes in the Permissions box.

When you're finished configuring permissions, click OK.

9. On the Group Policy tab, click OK.
10. Close Active Directory Users and Computers.

Linking an Existing Group Policy Object

If you need to apply the same user and computer Group Policy settings to more than one container in Active Directory, consider linking an existing GPO to the additional containers. Linking an existing GPO to another container is a quicker and easier task for an administrator to perform than creating and configuring a new GPO from scratch.

When you link an existing GPO to another container, the settings contained in the existing GPO apply to *both* of the containers. In addition, when you link an existing GPO to another container, a new Active Directory object is created. The new Active Directory object is a new GPO that is a pointer to the original GPO.

You can assign different users, groups, and computers to the new GPO, and you can change the permissions assigned to users, groups, and computers for the new GPO. These changes will apply only to the new GPO and not to the original GPO. However, you can't change the actual user and computer configuration settings in the new GPO without affecting the original GPO as well. In other words, the two GPOs share a common set of user and computer configuration settings.

STEP BY STEP

LINKING AN EXISTING GPO TO ANOTHER CONTAINER

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. The Active Directory Users and Computers dialog box appears. In the left pane, expand domains and OUs as necessary until the domain or OU (the additional container) to which you want to link an existing GPO is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, click Add.
5. The Add a Group Policy Object Link dialog box appears. Use the navigation features in this dialog box (such as the "Look in" drop-down list box and the Up button) to cause the original GPO to be displayed in the "Domains, OUs and linked Group Policy Objects" list box.

   Figure 10-8 shows this dialog box after I've located the GPO I want to link, in this case, the HQ Seattle GPO.

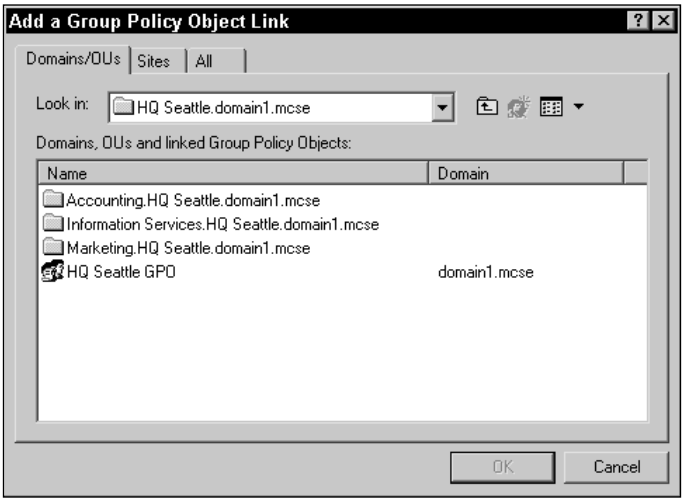

FIGURE 10-8 Linking an existing GPO

   To link the existing GPO once you've located it, highlight it and click OK.
6. The Group Policy tab reappears, and the linked GPO is listed. Click OK.
7. Close Active Directory Users and Computers.

Modifying the Order in Which Group Policy Is Applied

If you have more than one GPO associated with a container, and particularly if you filter Group Policy scope by using security groups, you may need to modify the order in which the GPOs for this container are applied.

For example, suppose that TinaT, a user in the HQ Seattle OU, belongs to four groups: Administrators, Managers, Accounting, and Everyone. The HQ Seattle OU has four GPOs associated with it, one for each of these groups, as shown in Figure 10-9. Notice the Up and Down command buttons in this dialog box.

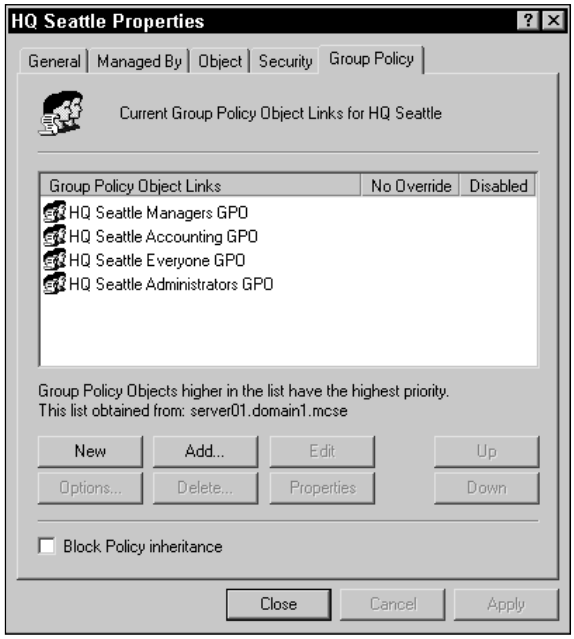

FIGURE 10-9 Modifying GPO order

GPOs are applied, in order, from the bottom of the list to the top of the list. The GPO at the bottom of the list (in this case, the HQ Seattle Administrators GPO) has the lowest priority, and is applied *first*. The GPO at the top of the list (in this case, the HQ Seattle Managers GPO) has the highest priority, and is applied *last*.

In our example, this means that settings in the HQ Seattle Administrators GPO will be overridden by any conflicting settings in any of the other GPOs in the list. Because of this, TinaT (and other members of the Administrators

group) may be unable to perform her administrative tasks. To prevent this from happening, the Administrator should move the HQ Seattle Administrators GPO to the top of the list.

To modify the order of GPOs, the Administrator can highlight any GPO in the list, and then use the Up and Down command buttons on the Group Policy tab in the container's Properties dialog box to move the GPO up or down in the list.

Configuring Group Policy Settings to Manage User Environments

As you've already learned, GPOs must be configured before you can use them to help you manage Windows 2000 computers on their users on a network. One of the primary uses of Group Policy is to manage user environments.

You can use Active Directory Users and Computers (or Active Directory Sites and Services, as appropriate) to configure numerous Group Policy options that affect a user's environment. You can also use the Group Policy snap-in to the MMC to configure Group Policy options. These configuration settings are contained within two primary sections in the Group Policy dialog box: Computer Configuration and User Configuration.

All configurations made in the Computer Configuration section are applied to all specified Windows 2000 computers that reside in the container (site, domain, or OU) with which the GPO is associated. It follows, then, that all configurations made in the Computer Configuration section also indirectly affect all users who log on to these computers.

All configurations made in the User Configuration section are applied to all specified users and groups that reside in the container with which the GPO is associated.

Both the Computer Configuration section and the User Configuration section have a subfolder that contains most of the Group Policy settings that directly affect a user's environment. This subfolder is called `Administrative Templates`. Figure 10-10 shows the two `Administrative Templates` subfolders and their various subfolders.

The `Administrative Templates` folder in the Computer Configuration section holds several subfolders that each contain various Group Policy options that you can configure to manage a user's environment:

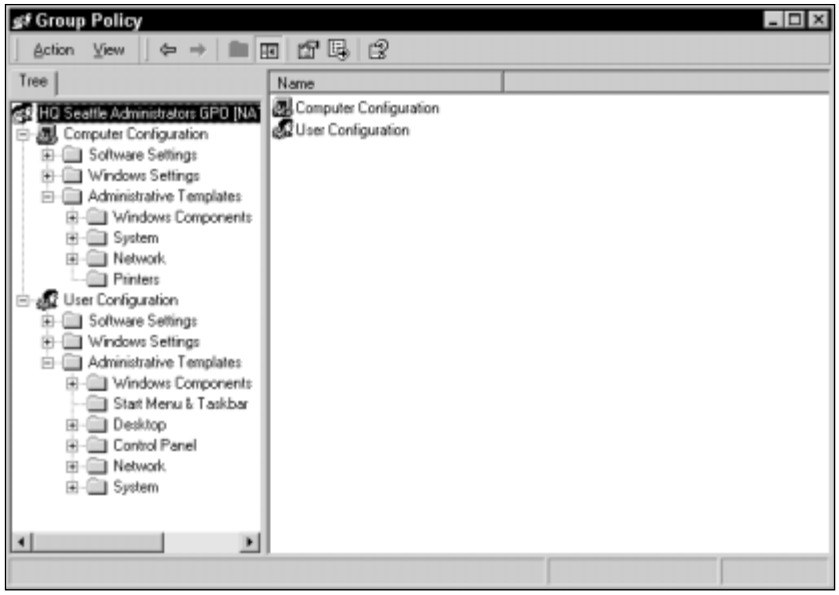

FIGURE 10-10 The Administrative Templates folders in Group Policy

- **`Windows Components`:** In this folder you can configure numerous settings that affect a user's ability to utilize specific features of four Windows 2000 components: NetMeeting, Internet Explorer, Task Scheduler, and Windows Installer. For example, you can prevent users from configuring remote desktop sharing in NetMeeting, and you can prevent users from creating new tasks in Task Scheduler.
- **`System`:** In this folder you can configure how Windows 2000 performs certain processes during logon. You can also configure and enable disk quotas, and configure a primary DNS suffix that will be assigned to the Windows 2000 computer. Finally, you can configure numerous settings that determine how Windows 2000 applies Group Policy, and set various Windows File Protection options.
- **`Network`:** In this folder you can configure numerous options to manage network configuration. The primary feature you can configure in this folder is offline files. There are several configurable settings that specify how Windows 2000 will process offline files. In the `Network and Dial-up Connections` subfolder, you can specify whether users can configure connection sharing.

- **Printers:** In this folder you can configure numerous printer settings. For example, you can specify whether printers will be automatically published in Active Directory, and you can configure whether Web-based printing will be supported on the Windows 2000 computer.

The `Administrative Templates` folder in the User Configuration section also holds several subfolders that each contain various Group Policy options that you can configure to manage a user's environment:

- **Windows Components:** In this folder you can configure numerous settings that affect a user's ability to utilize specific features of six Windows 2000 components: NetMeeting, Internet Explorer, Windows Explorer, Microsoft Management Console, Task Scheduler, and Windows Installer. For example, you can remove the File menu from Windows Explorer, and you can prevent users from changing home page settings in Internet Explorer.
- **Start Menu & Taskbar:** In this folder you can configure the appearance and functionality of the Start menu and taskbar on the user's computer. For example, you can remove Favorites, Help, Run, or Search from the Start menu. You can also prevent users from changing Start menu and taskbar settings.
- **Desktop:** In this folder you can configure various Active Desktop and Active Directory settings. For example, you can enable or disable Active Desktop, and you can hide the Internet Explorer icon on the desktop.
- **Control Panel:** In this folder you can configure settings that affect a user's ability to use Control Panel in general, and configure settings that restrict a user's ability to use specific features of four Control Panel applications: Add/Remove Programs, Display, Printers, and Regional Options. For example, you can prevent a user from using Control Panel entirely, and you can hide specified Control Panel applications from a user. You can also prevent a user from using Add/Remove Programs, or from seeing specific pages in the Add/Remove Programs Wizard. Likewise, you can hide several tabs from a user in the Display application. Finally, you can prevent a user from adding or deleting printers, or from browsing the network to find printers.

- **`Network`:** In this folder you can configure numerous options to manage network configuration. There are several configurable settings that specify how Windows 2000 will process offline files. For example, you can configure Windows 2000 to synchronize all offline files before a user logs off. There are also several network and dial-up connection settings you can configure. For example, you can prevent a user from viewing the properties of or deleting a RAS connection, and you can prevent a user from configuring connection sharing.
- **`System`:** In this folder you can configure how Windows 2000 performs certain processes when a user logs on or logs off. For example, you can prevent the user from changing his or her password, and you can prevent the user from logging off. You can also configure numerous settings that determine how Windows 2000 applies Group Policy to the user. For example, you can specify the Group Policy refresh interval for users.

Configuring the settings in the `Administrative Templates` folders is done on a GPO-by-GPO basis, and is fairly straightforward, as the following steps explain. As with other GPO configurations, you can use Active Directory Users and Computers to configure the `Administrative Templates` folder within a GPO associated with a domain or OU, and you can use Active Directory Sites and Services to configure the `Administrative Templates` folder within a GPO associated with a site.

TIP

Remember that when you configure the `Administrative Templates` folder in the Computer Configuration section your settings will apply to specified *computers*, and that when you configure the `Administrative Templates` folder in the User Configuration section your settings will apply to specified *users*.

STEP BY STEP

CONFIGURING THE ADMINISTRATIVE TEMPLATES FOLDER IN A GPO

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.

STEP BY STEP *Continued*

2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to configure `Administrative Templates` settings, and click Edit. (You can also double-click the GPO.)
5. The Group Policy dialog box appears. Click the + next to the `Administrative Templates` folder either in the Computer Configuration section or the User Configuration section. Then expand subfolders as necessary until the folder that contains the settings you want to configure is displayed in the left pane. Highlight the folder that contains the Group Policy settings you want to configure. The configurable settings in that folder are then displayed in the right pane.
6. In the right pane, double-click the setting you want to configure.
7. The setting's Properties dialog box appears, as shown in Figure 10-11. Notice the Not Configured, Enabled, and Disabled options. These three options are available when configuring many settings in the `Administrative Templates` folder.

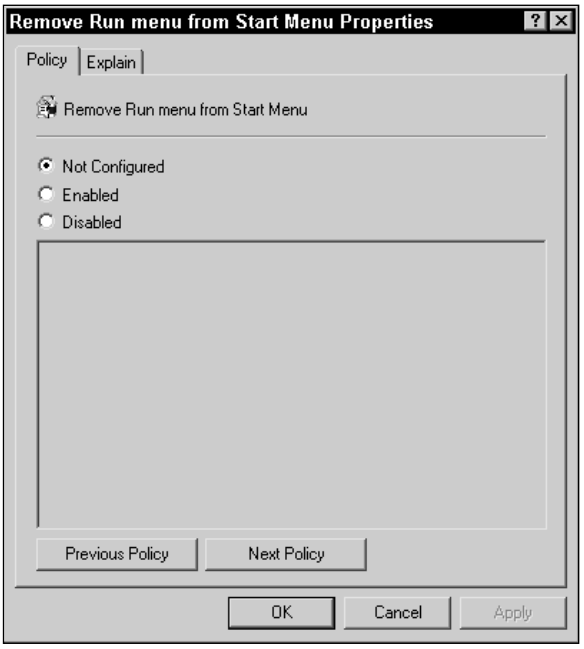

FIGURE 10-11 Configuring settings in the Administrative Templates folder

STEP BY STEP *Continued*

If you want more information about the setting you selected, click the Explain tab. Otherwise, configure options as appropriate on the Policy tab. (The possible settings vary substantially from setting to setting.) Click OK.

8. The Group Policy dialog box reappears. Repeat Steps 5, 6, and 7, as necessary, to configure additional Group Policy settings for this GPO. Close the Group Policy dialog box.
9. In the domain or OU's Properties dialog box, click OK.
10. Close Active Directory Users and Computers.

Configuring Group Policy Settings to Manage Scripts

You can configure Group Policy settings to manage several types of scripts. A *script* is a text file with a `.bat`, `.js`, or `.vbs` extension that can be used to configure a user's environment, to start programs, to install software, or to perform various other tasks. Script files that end with a `.bat` extension can include any MS-DOS 5.0 batch command. Script files that end with a `.js` extension can include any Microsoft JScript commands. Finally, script files that end with a `.vbs` extension can include any Visual Basic Scripting Edition (VBScript) commands.

Before you can assign a script to computers or users by using Group Policy, you must create the script. You can use any text editor, such as Notepad, to create a script file. Once you create the script file, you should save it with the appropriate extension (`.bat`, `.js`, or `.vbs`) depending on the type of commands contained in the file.

The types of scripts you can configure Group Policy settings for include startup, shutdown, logon, and logoff scripts. Startup and shutdown scripts apply to specified Windows 2000 *computers*, while logon and logoff scripts apply to specified *users*.

Both the Computer Configuration section and the User Configuration section have a subfolder, called `Windows Settings`, that contains Group Policy settings used to manage scripts. The `Windows Settings` folder in the Computer Configuration section has a container called Scripts (Startup/Shutdown), and the `Windows Settings` folder in the User Configuration section has a container called Scripts (Logon/Logoff). In these containers you can specify the name of a script (or scripts) that will run when the specified event (startup, shutdown, logon, or logoff) occurs,

and, if multiple scripts are specified for one event, you can specify the order in which scripts will run.

Configuring Group Policy settings to manage scripts is done on a GPO-by-GPO basis, and is fairly straightforward, as the following steps explain.

STEP BY STEP

ASSIGNING SCRIPTS TO USERS AND COMPUTERS

1. Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.
2. In the left pane, expand drives and folders as necessary until the folder that contains the script you previously created is displayed. Highlight the folder that contains the script. In the right pane, highlight the script file. Select Edit ➪ Copy.
3. Close Windows Explorer.
4. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
5. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
6. In the domain or OU's Properties dialog box, click the Group Policy tab.
7. On the Group Policy tab, highlight the GPO for which you want to configure script settings and click Edit. (You can also double-click the GPO.)
8. The Group Policy dialog box appears.

   To configure settings to manage startup or shutdown scripts, click the + next to the `Windows Settings` folder in the Computer Configuration section. Then highlight the Scripts (Startup/Shutdown) container in the left pane.

   To configure settings to manage logon or logoff scripts, click the + next to the `Windows Settings` folder in the User Configuration section. Then highlight the Scripts (Logon/Logoff) container in the left pane.
9. In the right pane, double-click the type of script (Startup, Shutdown, Logon, or Logoff) for which you want to configure Group Policy settings.
10. The Properties dialog box for the type of script you selected appears, as shown in Figure 10-12. Notice that I selected Logon Scripts. The Scripts tab is virtually identical no matter which type of script you select.

STEP BY STEP *Continued*

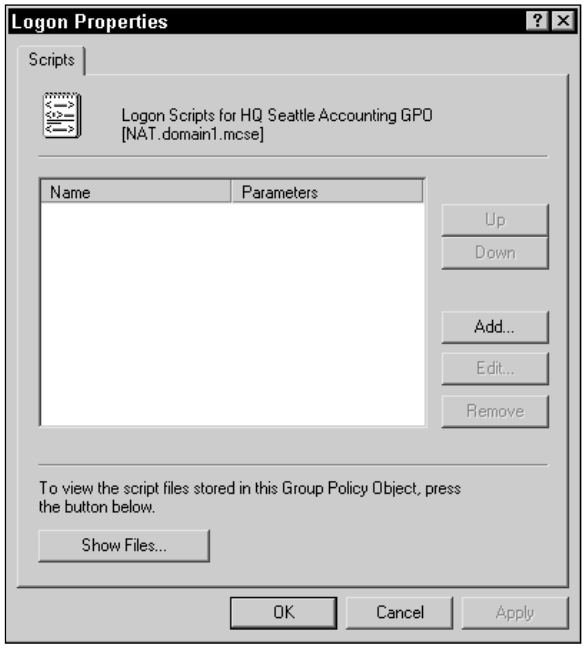

FIGURE 10-12 Configuring Group Policy script settings

To change the position of a script in the list (if multiple scripts are listed) in order to change the order in which the scripts are run, highlight the script you want to move, and use the Up and Down command buttons to change the script's position in the list. Scripts are run in the order they are listed on the Scripts tab, from the top of the list down.

To edit the name of a script in the list or to change optional script parameters, highlight the script and click Edit.

To remove a script from the list, highlight the script and click Remove.

To add a script to the list, click Show Files.

11. In the dialog box that appears (either Logon, Logoff, Startup, or Shutdown), select Edit➪Paste. Close the dialog box.
12. Click Add.
13. The Add a Script dialog box appears. In the Script Name text box, type the name of the script file you want to add. You can browse for the name of the script file if you need to. In the Script Parameters text box, type in any optional parameters for the script file. Click OK.

STEP BY STEP *Continued*

14. On the Scripts tab, click OK.
15. Close the Group Policy dialog box.
16. In the domain or OU's Properties dialog box, click OK.
17. Close Active Directory Users and Computers.

Just one final tip on working with scripts. Although you can assign a logon script to an individual user account by configuring a user account's properties, Microsoft recommends, for ease of administration, that you use Group Policy to assign logon scripts to users.

Configuring Group Policy Settings to Manage Security

You can configure numerous Group Policy settings to manage security settings for Windows 2000 computers, and their users, on your Windows 2000 network.

The `Windows Settings` folders in both the Computer Configuration section and the User Configuration section both have a container, called Security Settings, that contains Group Policy settings used to manage security. Although there is a Security Settings container in each section, virtually all of the configurable options are located in the Security Settings container in the Computer Configuration section — almost no security settings are available in the User Configuration section.

Figure 10-13 shows the many overall types of security settings available in the Computer Configuration section in the Group Policy dialog box.

The Security Settings container in the Computer Configuration section contains several subfolders and containers. Each of these subfolders and containers has various Group Policy options that you can configure to manage security:

- **Account Policies:** In this container, you can configure several password policy and account lockout policy options. (These options were discussed in detail in Chapter 9.) For example, you can specify the minimum number of characters a user's password must contain.

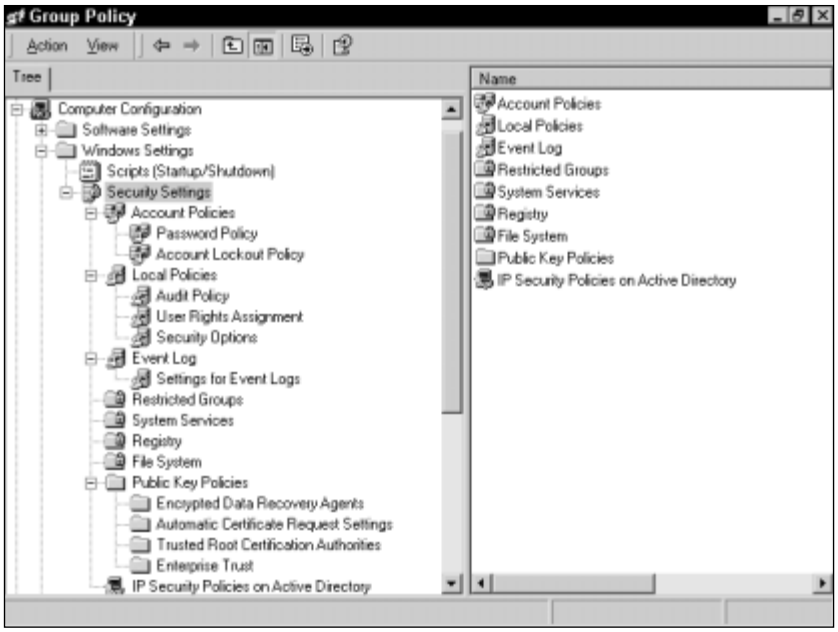

FIGURE 10-13 Security settings in Group Policy

- **Local Policies:** In this container you can configure audit policy, user rights assignment, and security options. For example, you can set a security option to automatically log off users when their logon time expires.

CROSS-REFERENCE

Specific user rights assignment settings are covered in Chapter 9, and specific audit policy settings are covered in Chapter 13.

- **Event Log:** In this container you can configure various settings for the Application, Security, and System logs that administrators view by using Event Viewer.
- **`Restricted Groups`:** In this folder you can configure Windows 2000 to monitor and maintain the membership lists of specified local groups (such as Power Users) on nondomain controllers to ensure that the membership in these groups is not modified by an Administrator on the local computer. To implement this feature, you add a specific group to this folder and then specify all of the group's members.

- **`System Services`:** In this folder you can specify the startup behavior of individual services on all Windows 2000 computers affected by this Group Policy. The possible configurations for service startup mode are Automatic, Manual, and Disabled. For example, you can set the service startup mode of the Task Scheduler service to be disabled. In this folder you can also specify which users and groups have permissions to start, stop, or manage the properties of a particular Windows 2000 service.
- **`Registry`:** In this folder you can specify individual registry settings that will be applied to all computers affected by this Group Policy.
- **`File System`:** In this folder you can configure security settings for common files and folders that exist on multiple computers in the container affected by this Group Policy. This enables you to standardize security settings for common files and folders across multiple computers. For example, you can assign a specific NTFS permission, such as Read, to the `Program Files` folder located on each computer affected by this Group Policy.
- **`Public Key Policies`:** In this folder you can set various certificate policies. For example, you can configure a user to be an encrypted data recovery agent, and you can specify a list of trusted root certification authorities.

CROSS-REFERENCE

I cover certificates and public key policies in detail in Chapter 18.

- **IP Security Policies on Active Directory:** In this container you can specify IP Security rules for clients, severs, and secure servers.

CROSS-REFERENCE

I discuss IP Security in Chapter 16.

The Security Settings container in the User Configuration section contains only one subfolder, named `Public Key Policies`. In this subfolder, you can configure an enterprise certificate trust list. This list specifies all certificate authorities that are trusted by all users affected by this Group Policy.

Group Policy security settings are configured on a GPO-by-GPO basis. As usual, use Active Directory Users and Computers to configure a GPO associated with a domain or OU, and use Active Directory Sites and Services to configure a GPO associated with a site.

STEP BY STEP

APPLYING SECURITY POLICIES BY USING GROUP POLICY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to configure security settings, and click Edit. (You can also double-click the GPO.)
5. The Group Policy dialog box appears. Click the + next to the `Windows Settings` folder in the Computer Configuration section (or the User Configuration section). Then click the + next to the Security Settings container. Expand subfolders or containers as necessary until the folder or container that has the security settings you want to configure is displayed in the left pane. Highlight the folder or container.
6. If the security setting you want to configure is displayed in the right pane, double-click the setting, and make the necessary configurations in the dialog box that appears. Click OK.

   If no security settings are displayed in the right pane, right-click the highlighted folder or container and select the Add option from the menu that appears. Make the necessary configurations and click OK.
7. When you're finished configuring security settings, close the Group Policy dialog box.
8. In the domain or OU's Properties dialog box, click OK.
9. Close Active Directory Users and Computers.

Configuring Group Policy Settings to Redirect Folders

You can configure Group Policy settings that will cause a specific folder (or folders) in a user's profile to be redirected to a different location, such as a shared folder on a network server. When a folder is redirected, it is no

longer stored on the local computer—it is only stored on the network server. The most common use of this feature is to redirect a user's `My Documents` folder to a shared folder on a network server that is backed up on a regular basis.

There are many different reasons for redirecting folders. Some of the more common ones are:

- To protect data from loss if a disk on a local computer fails.
- To speed up the process of loading roaming user profiles. (Folders that are redirected do not have to be copied to the local computer during the logon process.)
- To enable users to access all of their personal documents, regardless of which Windows 2000 computer on the network the users log on to.
- To maintain consistent security on user-created data.

The folders in a user's profile that can be redirected are the `Application Data`, `Desktop`, `My Documents`, `My Pictures`, and `Start Menu` folders.

Group Policy folder redirection settings are configured on a GPO-by-GPO basis. As usual, use Active Directory Users and Computers to configure a GPO associated with a domain or OU, and use Active Directory Sites and Services to configure a GPO associated with a site.

STEP BY STEP

REDIRECTING FOLDERS BY USING GROUP POLICY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to configure folder redirection settings, and click Edit. (You can also double-click the GPO.)
5. In the Group Policy dialog box, under User Configuration, click the + next to the `Windows Settings` folder. Click the + next to the `Folder Redirection` folder. Right-click the name of the folder you want to redirect and select Properties from the menu that appears.

STEP BY STEP *Continued*

6. The folder's Properties dialog box appears. Select one of the available redirection options from the Setting drop-down list box. The available options are:
   - **No administrative policy specified:** If you select this option, this GPO will not redirect the folder.
   - **Basic - Redirect everyone's folder to the same location:** If you select this option, Windows 2000 will redirect the specified folder (for *all* users affected by this GPO) to the same shared folder on the network. You will then need to specify a network location to redirect users' folders to. This is normally a UNC path such as `\\Server_name\Share_name\%username%`. The %username% variable creates a new folder in the shared network folder for each user whose folder is redirected.
   - **Advanced - Specify locations for various user groups:** If you select this option, users who belong to a specific group will have their folders redirected to a specific shared folder on the network. You can specify a different network location for each group you specify. You can use the %username% variable to give each user in the group an individual folder in the specified network share.

   Select the appropriate option and specify the network location(s) to which folders will be redirected. Click the Settings tab.
7. The Settings tab is displayed, as shown in Figure 10-14. Notice the options available in the Policy Removal section.

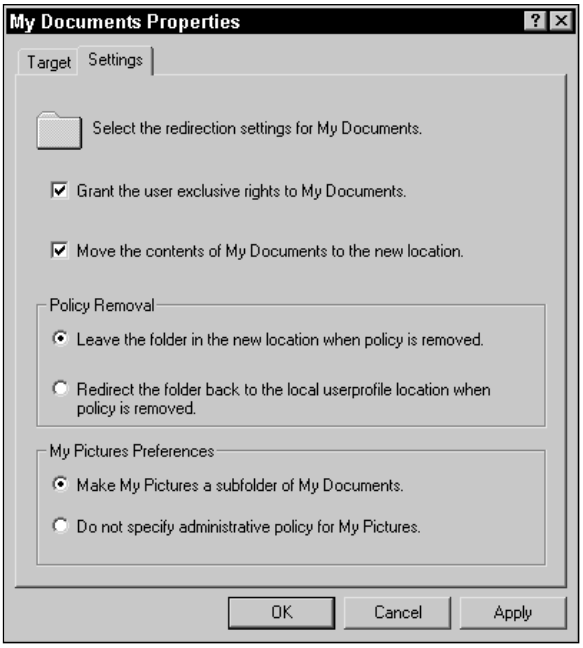

FIGURE 10-14 Configuring folder redirection options

STEP BY STEP *Continued*

Most of the options on this tab are self-explanatory. However, I want to point out the two options in the Policy Removal section. If you think that you will ever want to change the redirected folder back into a local folder, and you don't want to have to manually reconfigure each client computer, I recommend you select the option next to "Redirect the folder back to the local user profile location when policy is removed." If you want the folder to remain redirected when the policy is removed, accept the default option of "Leave the folder in the new location when policy is removed."

Configure options on this tab as appropriate. Click OK.

8. Close the Group Policy dialog box.
9. In the Properties dialog box for the domain or OU, click OK.
10. Close Active Directory Users and Computers.

Configuring Group Policy Settings to Manage Software Deployment

You can configure Group Policy to manage software deployment on your Windows 2000 network. You can deploy applications, deploy service packs, upgrade applications, and remove deployed applications. All of these tasks come under the software deployment umbrella.

EXAM TIP

The Directory Services exam has five objectives on using Group Policy to deploy and maintain software. This subject is sure to be well covered on this exam. So, if you don't get much opportunity to deploy software on the job, be sure to revisit this section before you take the exam.

There are three primary Group Policy software deployment methods:

- **Assign an application to a user:** When an application is assigned to a user by using Group Policy, that application's shortcuts appear in the user's Start menu. The application is not installed until the user starts the application from the Start menu, or until the user opens a document that has an extension that is associated with the application. An application that is assigned to a user is available regardless of which Windows 2000 computer on the network the user logs on to. If the application is removed from a computer, or if

any of the application's files are removed, the application will be reinstalled or repaired the next time the application is started.

- **Assign an application to a computer:** When an application is assigned to a computer by using Group Policy, that application is installed on the computer the next time the computer is restarted. The application is then available to all users who log on to that computer. If the application is uninstalled or if files are removed, the application is reinstalled or repaired the next time the computer boots.
- **Publish an application to a user:** When an application is published to a user, it is installed automatically when a user attempts to open a document that has an extension that is associated with that application. The application is not listed in the user's Start menu until it is installed. A published application can also be installed by starting the Add/Remove Programs tool in Control Panel. A published application is shown in the "Add programs from your network" list in the Add/Remove Programs tool. Published applications are not automatically reinstalled or repaired if they are removed or if files are accidentally deleted.

Preparing Software for Deployment

Before an application can be deployed, its installation files must be placed in a shared folder on a network server.

Any application that ships with a Windows Installer file (a file that ends with an `.msi` extension) can be deployed by using Group Policy. Applications that do not have a Windows Installer file can be deployed, but they must be prepared for deployment. You can prepare an application for deployment either by repackaging the application and creating a Windows Installer file for the application, or by creating a set of installation instructions for the application in a text file that ends with a `.zap` extension. Applications that use a `.zap` file for deployment can only be published—they can't be assigned to users or computers.

To repackage an application and create an `.msi` file, you need to use a special type of software application. Microsoft includes a third-party application named WinINSTALL LE with Windows 2000. You can use WinINSTALL LE to repackage an application and create an `.msi` file. WinINSTALL LE is located on the Windows 2000 Server/Advanced Server compact disc in the `\VALUEADD\3RDPARTY\WINSTLE` folder.

If you don't want to completely repackage an application, you can create a `.zap` file for the application that contains the instructions necessary to install and configure the application. You can use any text editor, such as Notepad, to create the `.zap` file. Listing 10-1 shows the contents of a sample `.zap` file that would be used to publish Adobe Acrobat Reader.

LISTING 10-1 Sample .zap File

```
[Application]
FriendlyName = "Adobe Acrobat Reader"
SetupCommand = ar405eng.exe
[Ext]
pdf=
```

■ ■ ■

Notice that a `.zap` file is separated into two primary sections: the `Application` section and the `Ext` (extensions) section.

In the `Application` section there are two required commands—FriendlyName and SetupCommand. FriendlyName is used to specify the name of the application as it will appear to the user. SetupCommand is used to specify the filename of the setup program used to install the application.

The `Ext` section consists of a list of all three-letter file extensions that will be associated with the application. If more than one extension will be associated with the application, each extension is placed on a separate line. Each application extension must be followed by the = sign.

When a `.zap` file is created, it must be saved in the same folder as the application's source files.

Deploying and Maintaining Software by Using Group Policy

Group Policy can be used not only to deploy software, but to maintain software as well. For example, you can use Group Policy to deploy a new application, and later, when a service pack becomes available, you can redeploy the application to install the service pack. Finally, when the application is no longer of value, you can use Group Policy to remove the application. I'll explain how to perform each of these tasks in the steps that follow.

Software applications are deployed on a GPO-by-GPO basis. As always, you can use Active Directory Users and Computers (or Active Directory Sites and Services, as appropriate) or the Group Policy snap-in to the MMC to manage Group Policy.

STEP BY STEP

DEPLOYING AN APPLICATION BY USING GROUP POLICY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to configure software deployment settings, and click Edit. (You can also double-click the GPO.)
5. In the Group Policy dialog box, under Computer Configuration or User Configuration (depending on whether you want to deploy software to computers or users), click the + next to the `Software Settings` folder. Right-click the Software installation container, and select New ➪ Package from the menu that appears.
6. If the package you want to install is not displayed in the Open dialog box, you can use this dialog box's browsing feature to browse the network for the folder that contains the package. Select the Windows Installer file for the package you want to install and click Open.

TIP

The application must be stored in a shared folder on a network server, or Group Policy will not be able to install the application on client computers.

7. The Deploy Software dialog box is displayed, as shown in Figure 10-15. Notice the three available options in this dialog box.

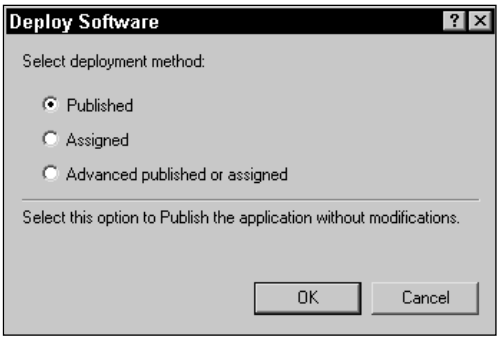

FIGURE 10-15 Configuring software deployment options

STEP BY STEP *Continued*

- **Published:** Select the Published option if you want Windows 2000 to publish the application using the default settings in the Windows Installer file you selected in Step 6. Skip to Step 14. If you are deploying software to computers, the Published option will be grayed out, and the Assigned option will be selected by default.
- **Assigned:** Select the Assigned option if you want Windows 2000 to assign the application using the default settings in the Windows Installer file you selected in Step 6. Skip to Step 14.
- **Advanced published or assigned:** Select the "Advanced published or assigned" option if you want to modify how the application is installed or assigned.

8. The package's Properties dialog box appears. There are six tabs in this dialog box: General, Deployment, Upgrades, Categories, Modifications, and Security. On the General tab, type in the name you want the package to use, or accept the default. Click the Deployment tab.
9. The Deployment tab appears, as shown in Figure 10-16. Notice the default deployment options for a package that is being deployed to users.

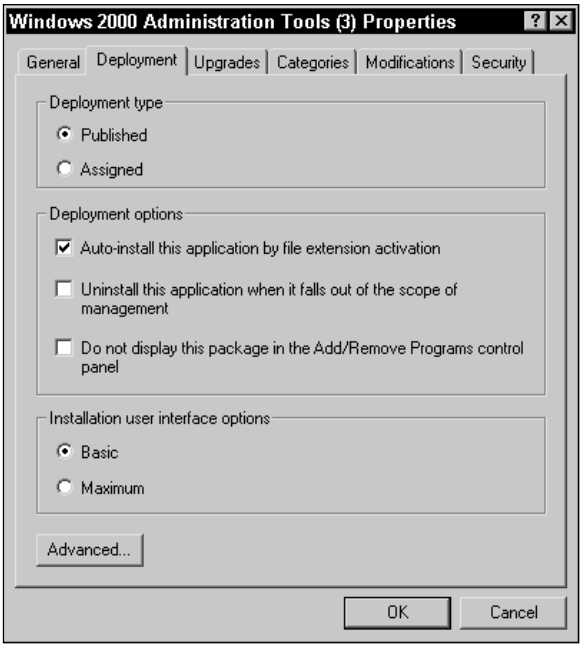

FIGURE 10-16 Configuring the Deployment tab

STEP BY STEP *Continued*

If the package is being deployed to computers, the Published option is grayed out and the Assigned option is selected. In addition, in the "Deployment options" section, the check box next to "Auto-install this application by file extension activation" is selected and grayed out, and the check box next to "Do not display this package in the Add/Remove Programs control panel" is not selected and is also grayed out.

Select the deployment type you want to use, then select the appropriate check boxes in the "Deployment options" section.

Select the appropriate option in the "Installation user interface options" section (in this particular case, Basic or Maximum). The settings available in this section will vary from application to application. Click the Upgrades tab.

10. On this tab, you can specify which applications (that have been previously deployed in this GPO by using Group Policy) will be upgraded by this application package. You can also specify application packages in the current GPO that will upgrade this package. Configure the selections on this tab as appropriate, and click the Categories tab.
11. On the Categories tab, you can select one or more categories to list the application in. (For more information on categories, see the step-by-step section titled "Creating Application Categories" later in this chapter.) When you finish selecting categories for the package, click the Modifications tab.
12. On the Modifications tab, add any modifications you have created to the package. Modifications have special Windows Installer files that end with an `.mst` extension. Files that end with an `.mst` extension are called *transforms*. Transforms are used to add features, such as templates, to applications. You can use a third-party tool to create `.mst` files. When you finish adding modifications to the application, click the Security tab.
13. On the Security tab you can assign users or computers permissions to the package as appropriate. Only users (or computers) that are allowed the Read permission to the package will be able to install the package. Configure permissions as appropriate and click OK.
14. Close the Group Policy dialog box.
15. In the domain or OU's Properties dialog box, click OK.
16. Close Active Directory Users and Computers.

Using Group Policy to Deploy Service Packs for Applications Once you have deployed an application, you might want to deploy a service pack for the application. To deploy a service pack, copy the service pack files into the

shared network folder that contains the application's original installation files. Ensure that the `.msi` file for the service pack replaces the original `.msi` file. Then use the following steps to redeploy the application.

STEP BY STEP

DEPLOYING A SERVICE PACK BY REDEPLOYING AN APPLICATION

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO that was originally used to deploy the application, and click Edit. (You can also double-click the GPO.)
5. In the Group Policy dialog box, in the Computer Configuration or User Configuration section (depending on whether you originally deployed the software package to computers or users), click the + next to the `Software Settings` folder. In the left pane, highlight Software installation. Then, in the right pane, right-click the application you want to redeploy and select All Tasks ➪ Redeploy application from the menu that appears.
6. In the Application's dialog box, click Yes to redeploy the application.
7. Close the Group Policy dialog box.
8. In the domain or OU's Properties dialog box, click OK.
9. Close Active Directory Users and Computers.

Using Group Policy to Create Application Categories If you plan to deploy many applications, you might want to create application categories that will be displayed in the Add/Remove Programs application in Control Panel. Application categories make it easier for users to find and install published or assigned applications that they need to perform their jobs. Once you create categories, you can assign them to software applications. You can assign categories to applications either during the deployment process or after they have been assigned or published. Figure 10-17 shows how software categories appear in the Add/Remove Programs application in Control Panel. Notice that only graphics applications are listed when Graphics is selected from the Category drop-down list box.

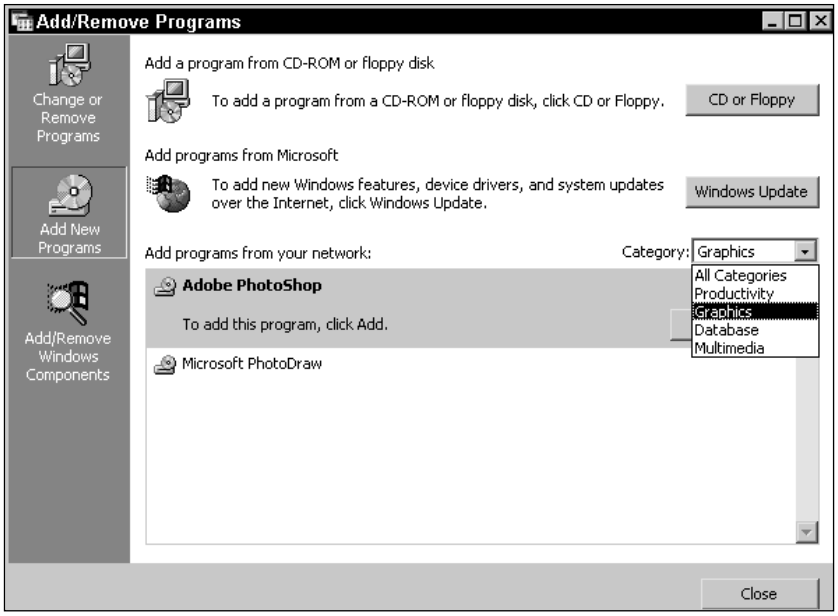

FIGURE 10-17 Using application categories

STEP BY STEP

CREATING APPLICATION CATEGORIES

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to create application categories and click Edit. (You can also double-click the GPO.)
5. In the Group Policy dialog box, under Computer Configuration or User Configuration (depending on whether you want to create categories for software applications that are deployed to computers or users), click the + next to the `Software Settings` folder. In the left pane, right-click Software installation and select Properties from the menu that appears.
6. In the Software installation Properties dialog box, click the Categories tab.
7. On the Categories tab, click Add to add a software category.

STEP BY STEP *Continued*

8. In the Enter new category dialog box, type in a name for the new software category and click OK.
9. Repeat Steps 7 and 8 until you have created all of the software categories you need. Click OK.
10. Close the Group Policy dialog box.
11. In the domain or OU's Properties dialog box, click OK.
12. Close Active Directory Users and Computers.

Using Group Policy to Remove Deployed Applications If the users on your network no longer need an application, or if you have replaced an application with one from a different vendor, you might want to remove an application that you have previously deployed. You can easily remove deployed applications by using Group Policy.

STEP BY STEP

REMOVING A DEPLOYED APPLICATION BY USING GROUP POLICY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO you want to configure is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO that was used to deploy the application and click Edit. (You can also double-click the GPO.)
5. In the Group Policy dialog box, under Computer Configuration or User Configuration (depending on whether you want to remove software that was originally deployed to computers or users), click the + next to the `Software Settings` folder. In the left pane, highlight Software installation. Then, in the right pane, right-click the application you want to remove and select All Tasks ➪ Remove from the menu that appears.

STEP BY STEP *Continued*

6. In the Remove Software dialog box, you can choose to either immediately uninstall the software, or allow users to continue using existing installations but prevent new installations. Select the appropriate removal method and click OK.
7. Close the Group Policy dialog box.
8. In the domain or OU's Properties dialog box, click OK.
9. Close Active Directory Users and Computers.

Troubleshooting Software Deployment

Sometimes software deployment doesn't work exactly the way you want it to. Because of this, I have included a few common software deployment problems and recommended solutions to those problems.

- **An application is assigned to computers in the GPO, but it is not installed on a particular computer:** The most likely cause of this problem is that the GPO does not apply to the computer. This might occur because the computer does not have the Read and Apply Group Policy permissions to the GPO, or because the computer is not in the container the GPO is associated with.
- **An application is published to a user, but the user is unable to install the application:** The most likely cause of this problem is that the user does not have enough permissions to access the shared network folder that contains the application. Ensure that the user is allowed at least the Read share permission and the Read & Execute NTFS permissions to the shared network folder that contains the application files.
- **An application is assigned to a user, but it doesn't install when it is invoked from the Start menu:** One of the most likely causes of this problem is that the application has been marked for removal from the computer in another GPO. If an application is marked for mandatory removal from a computer, the application will *not* install on that computer even if the application is assigned to a user on that computer.

Troubleshooting Group Policy

Group Policy is a very complex feature of Windows 2000. It can be configured for each domain, site, and OU in Active Directory. In addition, each domain, site, or OU can have more than one GPO assigned. To make matters even more complex, each computer can have Local Group Policy configured, as well. To top all that off, an administrator can modify how Group Policy is inherited and applied.

Because of Group Policy's complexity, it is fairly easy for two or more GPOs to have conflicting settings that apply to the same user, group of users, computer, or group of computers. Most Group Policy problems involve conflicting settings. Here are a few troubleshooting tips to help you resolve Group Policy problems.

- Verify that the No Override setting isn't configured on any GPO that applies to a parent container. If it is configured, verify that there are no conflicting settings between the GPO on the parent container and the GPO that is not working correctly.
- Verify that the "Block Policy inheritance" check box is not selected on any child containers that are affected by the GPO that is not being applied correctly.
- Verify that the Disabled option is not configured for a GPO that is not being applied.
- Verify that the users and computers that the GPO is intended to affect are actually in the container (or one of its subcontainers) with which the GPO is associated.
- Ensure that the users and computers the GPO is intended to affect are allowed the Read and Apply Group Policy permissions to the GPO.
- If multiple GPOs apply to a user or a computer (often due to the user's or computer's membership in multiple security groups), verify that there are no conflicting settings in the GPOs. If conflicts are present, reconfigure the GPOs as necessary, or consider modifying the order in which the GPOs are applied.
- Verify that the unused portions of GPOs that apply only to users (or only to computers) are disabled. This will speed up the application of GPOs during the boot-up and logon processes.

KEY POINT SUMMARY

This chapter introduced several important System Policy and Group Policy topics:

- System Policy is a collection of administrator-created user, group, and computer system policies that enable an administrator to manage *non-Windows 2000* client computers (and their users) on a Windows 2000 network. You can create System Policy for Windows NT 4.0, Windows 95, and Windows 98 computers (and their users).
- System Policy is managed and configured by using the System Policy Editor (`Poledit.exe`). The three types of policies that can be included in System Policy are a user system policy, a group system policy, and a computer system policy.
- Group Policy is a policy that contains rules and settings that are applied to Windows 2000 computers, their users, or both, that are located in a specific part of Active Directory. You can configure Group Policy settings to manage user environments, scripts, security, redirection of folders, and software deployment.
- Group Policy is typically implemented in Active Directory. However, Group Policy can be implemented directly on the local computer. When implemented on the local computer, Group Policy is called Local Group Policy.
- Group Policy consists of two components: an Active Directory object, called a Group Policy object (GPO), and a series of files and folders that are automatically created when the GPO is created.
- Group Policy is applied to Windows 2000 computers and their users in a predefined, systematic manner.
- Inheritance also affects how Group Policy is applied. A user or a computer normally inherits Group Policy from the container in which it resides and from the parent containers above it in the Active Directory tree. When Group Policy settings conflict, the Group Policy that is applied *last* is the policy that takes precedence.
- Local Group Policy is configured on an individual Windows 2000 computer by using the Group Policy snap-in to the Microsoft Management Console (MMC). You must be a member of the Administrators group on the local computer to manage Local Group Policy.

- You can use Active Directory Users and Computers to create a GPO associated with a domain or an OU. You can use Active Directory Sites and Services to create a GPO associated with a site. You can use these same tools to configure and modify the GPOs you create.
- You can use Group Policy to deploy software, upgrade software, apply service packs, and remove software. You can select from three software deployment methods: assigning software to computers, assigning software to users, and publishing software to users.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about System Policy and Group Policy, and to help you prepare for the Professional, Server, and Directory Services exams:

- **Assessment questions:** These questions test your knowledge of the System Policy and Group Policy topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenario, you are asked to analyze Group Policy and System Policy situations and recommend solutions for given problems. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab exercises:** These exercises are hands-on practice activities that you perform on a computer. The lab exercise in this chapter gives you an opportunity to practice various System Policy and Group Policy tasks.

Assessment Questions

1. You want to use System Policy to manage several Windows 98 client computers on your company's Windows 2000 network. Where must you create this System Policy file?
   A. On any Windows 2000 computer on the network on which the ADMINPAK is installed
   B. On any Windows 2000 Server computer on your network
   C. On a Windows 2000 Server computer on your network that is a domain controller
   D. On a Windows 98 computer

2. You create a System Policy file on a Windows 2000 Server computer to manage Windows NT 4.0 client computers (and their users) on your Windows 2000 network. What filename should you assign to this System Policy file?
   A. `Config.pol`
   B. `Ntconfig.pol`
   C. `Nt4config.pol`
   D. `Winntconfig.pol`
3. You want to create a Group Policy object (GPO) that will be associated with a specific domain. Which tool should you use?
   A. Domain Security Policy
   B. Domain Controller Security Policy
   C. Active Directory Users and Computers
   D. Active Directory Sites and Services
4. You recently created a Group Policy object (GPO) and associated this GPO with a particular OU. Now you want to link this existing GPO with two additional OUs. Which tool should you use to link the GPO?
   A. Windows Explorer
   B. Internet Explorer
   C. Active Directory Users and Computers
   D. Active Directory Sites and Services
5. You want to delegate administrative control of a Group Policy object (GPO) to an assistant network administrator. What are the *minimum* Active Directory permissions that the assistant must have for the GPO?
   A. Read and Write
   B. Write and Create All Child Objects
   C. Write and Apply Group Policy
   D. Full Control, Read, Write, Create All Child Objects, Delete All Child Objects, and Apply Group Policy
6. Which software deployment tasks can be performed by using Group Policy? (Choose all that apply.)
   A. Upgrading software
   B. Removing software

C. Deploying service packs

D. Repackaging an application and creating a Windows Installer (`.msi`) file for it

7. Which Windows 2000 feature should you use to manage user environments for 1000 Windows 2000 Professional client computers on your Windows 2000 network?

   A. System Policy

   B. Group Policy

   C. Local Group Policy

   D. Logon Scripts

8. You want to deploy a service pack for an application that was originally deployed by using Group Policy. You copy the service pack files to the shared network folder that contains the application's original installation files. What should you do next?

   A. Remove the application.

   B. Upgrade the application.

   C. Redeploy the application.

   D. Publish the service pack as a new application.

Scenarios

Using Group Policy and System Policy to manage your network can be an enormously complex task. For each of the following problems, consider the given facts and answer the question or questions that follow.

1. You manage a Windows 2000 network that has over 1,000 Windows 2000 Professional client computers. You just downloaded a service pack for an application that was deployed to all client computers by using Group Policy. What steps would you take to deploy the service pack?
2. You recently configured a GPO for an OU that contains 100 users and their computers. Many of the settings in the GPO are not taking effect. What should you do to resolve this problem?
3. You have configured several user settings in a GPO that is associated with an OU. These settings are not being applied to any users in the OU. What should you do to resolve this problem?

4. You want to use Group Policy to replace an old word processing application from one software vendor with a new word processing application from another software vendor. You want to make this change on 300 Windows 2000 Professional client computers on your Windows 2000 network. The new application can't be used to upgrade the old application. What should you do to accomplish this?
5. You have assigned an application to computers in a GPO that is associated with an OU. You have restarted all of the computers in the OU, but the application is only installed on some of the computers in the OU. What should you do to resolve this problem?
6. You recently used `Poledit.exe` on a Windows 2000 computer to create a System Policy file named `Ntconfig.pol`. The settings in this policy file are taking effect on all Windows NT Workstation 4.0 client computers on your network, but they are *not* taking effect on the Windows 98 client computers on your network. What is the cause of this problem, and what should you do to resolve it?
7. You configure Local Group Policy to remove the Run command from the Start menu on a Windows 2000 Professional client computer. After shutting down and restarting the computer, the Run command is still displayed in the Start menu. What should you do to resolve this problem?

Lab Exercises

Lab 10-1 Managing policies in Windows 2000

- ▶ Professional
- ▶ Server
- ▶ Directory Services

The purpose of this lab is to provide you with an opportunity to practice many of the tasks associated with managing policies in a Windows 2000 environment.

There are four parts to this lab:

- Part 1: Configuring Local Group Policy
- Part 2: Configuring System Policy

- Part 3: Sharing a Folder for Application Distribution
- Part 4: Configuring Group Policy

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Configuring Local Group Policy

In this part, you use the Group Policy snap-in to the Microsoft Management Console (`Gpedit.msc`) to manage Local Group Policy on a Windows 2000 Server computer.

1. Select Start ➪ Run.
2. In the Run dialog box, type **gpedit.msc** and click OK.
3. In the Group Policy snap-in to the MMC, click the + next to the `Administrative Templates` folder in the User Configuration section. Click the + next to the `System` folder. Highlight the `Logon/Logoff` folder.
4. In the right pane, double-click "Run logon scripts visible."
5. In the Run logon scripts visible Properties dialog box, select the Enabled option and click OK.
6. In the left pane, highlight the `Start Menu & Taskbar` folder.
7. In the right pane, double-click "Remove Help menu from Start Menu."
8. In the Remove Help menu from Start Menu Properties dialog box, select the Enabled option and click OK.
9. Close the Group Policy dialog box.
10. Select Start, and notice that the Help option is no longer displayed in the Start menu.
11. Select Start ➪ Run.
12. In the Run dialog box, ensure that **gpedit.msc** appears in the Open text box and click OK.
13. In the Group Policy dialog box, click the + next to the `Administrative Templates` folder in the User Configuration section. Highlight the `Start Menu & Taskbar` folder.
14. In the right pane, double-click "Remove Help menu from Start Menu."
15. In the Remove Help menu from Start Menu Properties dialog box, select the Not Configured option and click OK.
16. Close the Group Policy dialog box.

Part 2: Configuring System Policy

In this part, you use System Policy Editor (`Poledit.exe`) to create a Windows NT 4.0 System Policy and to manage the local Windows 2000 Server computer.

1. Select Start ➪ Run.
2. In the Run dialog box, type **Poledit.exe** and click OK.
3. In the System Policy Editor dialog box, select File ➪ New Policy.
4. In the System Policy Editor dialog box, double-click Default Computer.
5. In the Default Computer Properties dialog box, click the + next to Windows NT System, then click the + next to Logon. Select the check box next to "Do not display last logged on user name." The check box should be white with a check in it. Click OK.
6. In the System Policy Editor dialog box, double-click Default User.
7. In the Default User Properties dialog box, click the + next to Desktop. Select the check box next to Color scheme. The check box should be white with a check in it.

   In the "Scheme name" drop-down list box (located at the bottom of the Default User Properties dialog box), select Wheat.

   Click the + next to Shell, then click the + next to Restrictions. Select the check box next to "Remove Run command from Start menu," and select the check box next to "Don't save settings at exit." Click OK.
8. Select File ➪ Save As.
9. In the Save As dialog box type **\\Server01\NETLOGON\NTconfig.pol** in the File name text box. Click Save.
10. In the System Policy Editor dialog box, select File ➪ Close. Select File ➪ Open Registry.
11. In the System Policy Editor - Local Registry dialog box, double-click Local User.
12. In the Local User Properties dialog box, click the + next to Shell, then click the + next to Restrictions. Select the check box next to "Remove Run command from Start menu." Click OK.
13. Select File ➪ Save. Then select File ➪ Exit.

14. Click Start. Notice that the Run command has not been removed from the Start menu. The changes made in System Policy Editor will not take place until you log off and log on again.
15. Click Start ➪ Shut Down.
16. In the Shut Down Windows dialog box, select Log off Administrator from the drop-down list box. Click OK.
17. Press Ctrl+Alt+Delete. In the Log On to Windows dialog box, type in a user name of **Administrator** and a password of **password**. Click OK.
18. Click Start. Notice that the Run command is no longer displayed in the Start menu.
19. Select Start ➪ Programs ➪ Accessories ➪ Command Prompt.
20. At the command prompt, type **poledit** and press Enter.
21. In the System Policy Editor dialog box, select File ➪ Open Registry.
22. In the System Policy Editor - Local Registry dialog box, double-click Local User.
23. In the Local User Properties dialog box, click the + next to Shell, then click the + next to Restrictions. Clear the check box next to "Remove Run command from Start menu." Click OK.
24. Select File ➪ Save. Then select File ➪ Exit.
25. Close the Command Prompt dialog box. The next time you log off and log on, the Run command will reappear in the Start menu.

Part 3: Sharing a Folder for Application Distribution

In this part, you use Windows Explorer to create and share a folder that will be used for application distribution.

1. Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.
2. In the left pane, click the + next to My Computer. Highlight Local Disk (C:).
3. Select File ➪ New ➪ Folder.
4. In the right pane, type a folder name of **Apps** and press Enter.
5. Right-click the Apps folder and select Sharing from the menu that appears.

6. On the Sharing tab, select the option next to "Share this folder" and click OK.
7. Place your Windows 2000 Server compact disc in your computer's CD-ROM drive.
8. Close the Microsoft Windows 2000 CD dialog box.
9. In the left pane, click the + next to your CD-ROM drive. Highlight the `I386` folder.
10. In the right pane, scroll down until a file named `ADMINPAK` is displayed. (It may appear either as `ADMINPAK` or `ADMINPAK.MSI`.) Right-click the `ADMINPAK` file and select Copy from the menu that appears.
11. Click the + next to Local Disk (C:). Highlight the `Apps` folder. Select Edit ➪ Paste. Windows 2000 copies the `ADMINPAK` file from your compact disc to the `Apps` shared folder.
12. Close Windows Explorer.

Part 4: Configuring Group Policy

In this part, you use Notepad to create a logon script, and then use Active Directory Users and Computers to create a Group Policy object (GPO), modify Group Policy and Group Policy inheritance, filter Group Policy settings by associating security groups to the GPO, delegate administrative control of the GPO, and link an existing GPO. You also use Group Policy to assign a script policy to users, manage network configuration, and apply security policies. Finally, you manage software by using Group Policy, including deploying software (by using a Windows Installer package) and configuring deployment options.

1. Select Start ➪ Programs ➪ Accessories ➪ Notepad.
2. In the Untitled - Notepad dialog box, type the following lines as shown:

```
@echo off
echo This is my logon script
pause
```

3. Make sure you press Enter after the last line. Select File ➪ Save As. In the Save As dialog box, type **Logonscript.bat** in the "File name" text box, and select All Files from the "Save as type" drop-down list box. Click Save.

4. Exit Notepad.
5. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
6. In the left pane, right-click the HQ Seattle OU and select Properties from the menu that appears.
7. In the HQ Seattle Properties dialog box, click the Group Policy tab.
8. On the Group Policy tab, click New. Type a name of HQ Seattle GPO and press Enter. Click Options.
9. In the HQ Seattle GPO Options dialog box, select the check box next to No Override. Click OK.
10. On the Group Policy tab, ensure that HQ Seattle GPO is highlighted and click Properties.
11. In the HQ Seattle GPO Properties dialog box, click the Security tab.
12. On the Security tab, click Add.
13. In the Select Users, Computers, or Groups dialog box, double-click Mike Calhoun. Then double-click the Sales, Managers, and Accountants groups. Finally, double-click SERVER01. Click OK.
14. On the Security tab, highlight Mike Calhoun. In the Permissions box select the Allow check boxes next to Write, Create All Child Objects, Delete All Child Objects, and Apply Group Policy. (The Read check box is selected by default — don't deselect it.)
15. Repeat Step 14 for SERVER01 and for the Sales, Accountants and Managers groups.
16. Highlight Authenticated Users, and clear the Allow check box next to Apply Group Policy. Click OK.
17. On the Group Policy tab, click Edit.
18. In the Group Policy dialog box, in the User Configuration section, click the + next to the `Software Settings` folder. Right-click Software installation and select New ➪ Package from the menu that appears.
19. In the Open dialog box, type in a file name of **\\Server01\Apps\Adminpak.msi** and click Open.
20. In the Deploy Software dialog box, select the option next to Assigned. Click OK.
21. Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.

22. In the right pane, highlight `Logonscript.bat`. (If the `Logonscript.bat` file is not displayed in the right pane, click the + next to My Computer, and then highlight Local Disk (C:).) Select Edit ➪ Copy. Close Windows Explorer.
23. In the Group Policy dialog box, in the User Configuration section, click the + next to the `Windows Settings` folder. Highlight Scripts (Logon/Logoff). In the right pane, double-click Logon.
24. In the Logon Properties dialog box, click Show Files.
25. In the Logon dialog box, click Edit ➪ Paste. Close the Logon dialog box.
26. In the Logon Properties dialog box, click Add.
27. In the Add a Script dialog box, click Browse.
28. In the Browse dialog box, double-click `Logonscript.bat`.
29. In the Add a Script dialog box, click OK.
30. In the Logon Properties dialog box, click OK.
31. In the Group Policy dialog box, in the User Configuration section, click the + next to the `Administrative Templates` folder. Highlight the `Start Menu & Taskbar` folder. In the right pane, double-click "Add Logoff to the Start Menu."
32. In the Add Logoff to the Start Menu Properties dialog box, select the option next to Enabled. Click OK.
33. In the Group Policy dialog box, in the User Configuration section, click the + next to the `Network` folder. Highlight the `Network and Dial-up Connections` folder. In the right pane, double-click "Allow configuration of connection sharing."
34. In the Allow configuration of connection sharing Properties dialog box, select the option next to Disabled. Click OK.
35. In the Group Policy dialog box, in the Computer Configuration section, click the + next to the `Windows Settings` folder. Click the + next to the Security Settings container. Click the + next to the Local Polices container. Highlight Security Options. In the right pane, double-click "Automatically log off users when logon time expires (local)."
36. In the Security Policy Setting dialog box, select the check box next to "Define this policy setting." Select the option next to Enabled. Click OK.
37. Close the Group Policy dialog box.

38. In the HQ Seattle Properties dialog box, click Close.
39. In the Active Directory Users and Computers dialog box, right-click the Denver OU, and select Properties from the menu that appears.
40. In the Denver Properties dialog box, click the Group Policy tab.
41. On the Group Policy tab, click Add.
42. In the Add a Group Policy Object Link dialog box, click the up button next to the right of the "Look in" drop-down list box. In the Domains, OUs and linked Group Policy Objects list box, double-click HQ Seattle.domain1.mcse. Then double-click HQ Seattle GPO.
43. In the Denver Properties dialog box, the HQ Seattle GPO appears in the Group Policy Object Links list box. Click OK.
44. Close Active Directory Users and Computers.
45. Select Start ➪ Shut Down.
46. In the Shut Down Windows dialog box, select Restart from the drop-down list box. Click OK.
47. When Windows 2000 restarts, boot your computer to Windows 2000 Server. Press Ctrl+Alt+Delete. In the Log On to Windows dialog box, type in a user name of **MikeCa** and a password of **changeme**. Click OK.
48. Click OK in the Logon Message dialog box.
49. In the Change Password dialog box, type in a New Password of **password**, and confirm it by retyping it. Click OK. Click OK in the Change Password dialog box that appears.
50. Click the program on the taskbar with a title of C:\WINNT\System32\cmd . . . . The C:\WINNT\System32\cmd.exe dialog box appears. It should display:

```
This is my logon script
Press any key to continue . . .
```

51. Click anywhere in the dialog box. Then press the spacebar to close the logon script's dialog box.
52. Select Start. Notice that there is a Log Off MikeCa option in the Start Menu.
53. Select Start ➪ Programs ➪ Administrative Tools ➪ DHCP.
54. A Windows Installer dialog box appears. Windows 2000 installs the Windows 2000 Administrative Tools. Finally, the DHCP dialog box appears. Close the DHCP dialog box.

Answers to Chapter Questions

Chapter Pre-Test

1. System Policy is a collection of Administrator-created user, group, and computer system policies that enable an administrator to manage *non-Windows 2000* client computers (and their users) on a Windows 2000 network. The types of client computers that you can create System Policy for include: Windows NT 4.0 computers, Windows 95 computers, and Windows 98 computers.
2. System Policy is applied in the following sequence:
   a. If a user has an individual user policy, it is applied.
   b. If a user does *not* have an individual user policy, and the user is a member of a group that has a group system policy, then the group system policy (or policies, if the user is a member of multiple groups that each have a group system policy) is applied.
   c. If a user does *not* have an individual user policy, then the Default User policy is applied.
   d. If the non-Windows 2000 client computer the user logs on to has an individual computer policy, it is applied.
   e. If the non-Windows 2000 client computer the user logs on to does *not* have an individual computer policy, then the Default Computer policy is applied.
3. Group Policy is a policy that contains rules and settings that are applied to Windows 2000 computers, their users, or both, that are located in a specific part of Active Directory. Group Policy can only be used to manage Windows 2000 computers on a network (and the users of those computers).
4. When Group Policy is implemented directly on the local computer, it is called Local Group Policy.
5. Group Policy consists of two components: an Active Directory object, called a Group Policy object, and a series of files and folders that are automatically created when the Active Directory object is created.

Assessment Questions

1. **D.** The System Policy file for the Windows 98 client computers must be created on either a Windows 95 or Windows 98 computer. Since a Windows 98 computer was the only correct answer choice provided in the possible answers to this question, D is the correct answer.
2. **B.** A Windows NT 4.0 System Policy file should be named `NTconfig.pol`.
3. **C.** You can use Active Directory Users and Computers to create a GPO that will be associated with a specific domain or OU. If you are creating a GPO that will be associated with a site, you should use Active Directory Sites and Services.
4. **C.** Use Active Directory Users and Computers to link the existing GPO to the additional OUs.
5. **A.** In order to administer a GPO, the assistant network administrator must be allowed the Read and Write Active Directory permissions to the GPO.
6. **A, B, and C.** You can use Group Policy to upgrade software, remove software, and deploy service packs. However, you need a third-party application to repackage an application and create an `.msi` file for it.
7. **B.** You should use Group Policy to manage multiple Windows 2000 Professional computers on a Windows 2000 network. Using Local Group Policy would work, but you would have to manage each computer individually. You could also use System Policy Editor to individually edit the registry on each client computer, but it would be very inefficient, and System Policy does not have nearly as many features as Group Policy.
8. **C.** You should redeploy the application so that the new files in the service pack will be installed on all computers on which the original application was deployed.

Scenarios

1. First, copy the contents of the service pack to the shared network folder that contains the application's installation files. Make sure that the original Windows Installer file is replaced with the one in the service pack. Then use Group Policy to redeploy the application.
2. Ensure that all users and computers that should be affected by the GPO are allowed the Read and Apply Group Policy permissions to the GPO. In addition, ensure that no other GPOs that affect those users and computers are configured with conflicting settings.
3. Ensure that the user configuration settings portion of the GPO is not disabled. If that does not resolve the problem, ensure that all users in the OU are allowed the Read and Apply Group Policy permissions to the GPO. Finally, ensure that no other GPOs that affect those users are configured with settings that conflict with the new GPO.
4. Use Group Policy to mark the old word processing application for mandatory removal, and then use Group Policy to deploy the new word processing application to the appropriate users and computers.
5. Ensure that all computers in the OU are allowed the Read and Apply Group Policy permissions to the GPO. In addition, ensure that no other GPO that affects those computers is configured to specify mandatory removal of the application.
6. A System Policy file that is created on a Windows 2000 computer can't be used to manage Windows 98 client computers. You must create the System Policy file for the Windows 98 client computers by using `Poledit.exe` on a Windows 98 (or Windows 95) client computer and save that file as `Config.pol` (not as `Ntconfig.pol`).
7. Ensure that no GPOs in Active Directory are overriding the Local Group Policy settings. A GPO in Active Directory must be overriding the local settings, or they would have taken effect.

MCSE
EXAM
MATERIAL