Module 5: Implementing Group Policy

Contents
Overview 1
Lesson: Creating and Configuring GPOs 2
Lesson: Configuring Group Policy Refresh Rates and Group Policy Settings 16
Lesson: Managing GPOs 27
Lesson: Verifying and Troubleshooting Group Policy 39
Lesson: Delegating Administrative Control of Group Policy 45
Lesson: Planning a Group Policy Strategy for the Enterprise 54
Lab A: Implementing Group Policy 61
Instructor Notes

Presentation: 180 minutes
Lab: 75 minutes

This module provides students with the knowledge and skills necessary to plan and implement a Group Policy strategy to centrally manage users and computers in an enterprise.

After completing this module, students will be able to:

- Create and configure Group Policy objects (GPOs).
- Configure Group Policy refresh rates and Group Policy settings.
- Manage GPOs.
- Verify and troubleshoot Group Policy.
- Delegate administrative control of Group Policy.
- Plan a Group Policy strategy for the enterprise.

Required materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2279A_05.ppt
- Macromedia Flash file 2274_6_A_IntroGP.swf
- Macromedia Flash file and 2274_6_i_GP.swf

Important It is recommended that you use PowerPoint 2002 or later to display the slides for this course. If you use PowerPoint Viewer or an earlier version of PowerPoint, all the features of the slides may not appear correctly.

Preparation tasks

To prepare for this module:

- Read all of the materials for this module. Throughout the module, anticipate questions that students may ask and prepare answers for each question.
- Complete the lab.
- Study the practices and assessment questions and the answers that are provided. Where possible, anticipate alternate answers that students may suggest and prepare responses to those answers.
How to Teach This Module

This section contains information that will help you to teach this module.

Important  This module contains assessment items for each lesson, which are located on the Student Materials compact disc. You can use them as pre-assessments to help students identify areas of difficulty, or you can use them as post-assessments to validate learning.

Consider using them to reinforce learning at the end of the day. You can also use them at the beginning of the day as a review for the content that you taught on the previous day.

Give students 10 minutes to prepare the answers for the assessment questions. You may choose to discuss the questions and answers together or ask the students to prepare the answers on their own.

Note  Some topics refer to additional information in the Appendices. Students do not require this supplemental information to complete the tasks that are presented in the module. Before teaching the class, review this information on the Appendices page on the Student Materials compact disc. During the class, refer the students to the Appendices page for additional information.

How To pages, practices, and labs

Explain to the students how the How To pages, practices, and labs are designed for this course. A module includes two or more lessons. Most lessons include How To pages and a practice. After students complete the lessons, the module concludes with a lab.

How To pages

The How To pages are designed for you to demonstrate how to perform a task. The students do not perform the tasks on the How To page with you. They will use these steps to perform the practice at the end of each lesson.

Practices

After you present a topic and demonstrate the How To procedures for the lesson, explain that a practice gives students an opportunity to perform the tasks that were discussed in the lesson.

Labs

At the end of each module, students use the lab to practice the tasks that were discussed throughout the module.

Each lab presents a scenario that is relevant to the students’ job role and a set of instructions in a two-column format. The left column provides the task (for example: Create a group). The right column contains specific instructions to perform the task (for example: in Active Directory Users and Computers, double-click the domain node).

An answer key for each lab exercise is located on the Student Materials compact disc, in case the students need step-by-step instructions to complete the lab. They can also refer to the practices and How To pages in the module.
Lesson: Creating and Configuring GPOs

In this lesson, students review basic concepts of implementing Group Policy, including how to specify a domain controller for managing GPOs, filter Group Policy settings by using Windows Management Instrumentation (WMI) filters, and configure the User Group Policy loopback processing mode.

The lesson begins with a multimedia presentation that explains the basic concepts of Group Policy. Because these concepts are explained in detail in Course 2274, Managing a Microsoft Windows Server 2003 Environment, the animation summarizes the tasks. If some students are unfamiliar with basic concepts of Group Policy, refer them to Module 8, “Implementing Group Policy” in Course 2274.

Refer students to Appendices for additional information about Group Policy container (GPC).

Practice

During the practice at the end of the lesson, ask students to refer to the business scenario as they create and configure GPOs.

Lesson: Configuring Group Policy Refresh Rates and Group Policy Settings

In this lesson, students will learn how to control Group Policy processing and how Group Policy determines a slow link. Explain the order in which Microsoft Windows® Server 2003 processes Group Policy settings for computers and users and then demonstrate the procedures to configure Group Policy processing.

Refer students to the Appendices for additional information about Group Policy processing, a sample logon script, and the algorithm that Group Policy uses to detect slow links.

Practice

In the practice at the end of the lesson, ask students to refer to the business scenario as they configure Group Policy processing.

Lesson: Managing GPOs

In this lesson, students learn how to manage GPOs by using the new Group Policy Management feature of Windows Server 2003. Remind students that when they install the Group Policy Management console, it replaces the Group Policy tab in Active Directory Users and Computers.

Practice

In the practice at the end of the lesson, ask students to refer to the business scenario as they manage GPOs.
Lesson: Verifying and Troubleshooting Group Policy

This lesson explains the different utilities and command-line tools you use to identify common problems when you implement Group Policy and strategies for resolving these problems.

Refer students to the Appendices page for more information about using the Gpresult.exe command-line tool to verify Group Policy settings and enabling diagnostic logging and verbose logging to monitor Group Policy.

Practice

In the practice at the end of the lesson, ask students to refer to the business scenario as they verify and troubleshoot Group Policy.

Lesson: Delegating Administrative Control of Group Policy

In this lesson, students learn how to delegate administrative control of a GPO to users who require control but do not have administrative privileges for the container that the GPO is linked to.

Discuss how Group Policy Management has simplified the delegation of Group Policy. Refer students to the Appendices page for additional information about delegating administrative control.

Practice

In the practice at the end of the lesson, ask students to refer to the business scenario as they delegate administrative control of Group Policy.

Lesson: Planning a Group Policy Strategy for the Enterprise

This lesson presents guidelines for planning a Group Policy strategy. Discuss the guidelines for determining GPO inheritance, Group Policy strategy for sites, domains, and organizational units, administration of GPOs, and deploying GPOs.

Practice

In the practice at the end of the lesson, ask students to refer to the business scenario as they plan a Group Policy strategy for the enterprise.

Lab: Implementing Group Policy

In this lab, students create and configure GPOs, link GPOs, and verify the Group Policy settings. Students will work alone. Ensure that Group Policy Management console is installed before students begin this lab.

Lab Setup

The following list describes the setup requirements for the lab in this module.

Setup requirement 1

The lab in this module requires that the Group Policy Management console is installed. To prepare student computers to meet this requirement, ensure that students have completed the practice titled Creating and Configuring GPOs.
Lab Results

Performing the lab in this module introduces the following configuration change:

- Creates the Accounting, Accounts Receivable, and Accounts Payable organizational units.
- Creates the Accounting, Accounts Receivable, and Accounts Payable GPOs.
Module 5: Implementing Group Policy

Overview

Introduction
You use Group Policy in the Active Directory® directory service to centrally manage users and computers in an enterprise. You can centralize policies by setting Group Policy for an entire organization at the site domain or at an organizational unit level. Or, you can decentralize Group Policy settings by setting Group Policy for each department at an organizational unit level.

You can ensure that users have the user environments that they require to perform their jobs and enforce an organization’s policies, including business rules, goals, and security requirements. Additionally, you can lower the total cost of ownership by controlling user and computer environments, thereby reducing the level of technical support that users require and the lost user productivity due to user error.

Objectives
After completing this module, you will be able to:

- Create and configure Group Policy objects (GPOs).
- Configure Group Policy refresh rates and Group Policy settings.
- Manage GPOs.
- Verify and troubleshoot Group Policy.
- Delegate administrative control of Group Policy.
- Plan a Group Policy strategy for the enterprise.
Lesson: Creating and Configuring GPOs

Introduction

Group Policy gives you administrative control over users and computers in your network. By using Group Policy, you can define the state of a user’s work environment once, and then rely on Microsoft® Windows® Server 2003 to continually enforce the Group Policy settings that you defined. You can apply Group Policy settings across an entire organization or to specific groups of users and computers.

Lesson objectives

After completing this lesson, you will be able to:

- Explain the purpose of Group Policy and how it is processed in Active Directory.
- Describe GPO components.
- Explain the purpose of specifying a domain controller for GPO management.
- Specify a domain controller for managing GPOs.
- Explain the purpose of Windows Management Instrumentation (WMI) filters.
- Filter Group Policy settings by using WMI filters.
- Explain the purpose of loopback processing.
- Configure the User Group Policy loopback processing mode.
Multimedia: Review of Group Policy

To view the Review of Group Policy presentation, open the Web page on the Student Materials compact disc, click Multimedia, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

After completing this lesson, you will be able to:

- Describe the types of settings that you can define in Group Policy.
- Describe how Windows Server 2003 applies Group Policy objects.

You can configure Group Policy settings to define the policies that affect users and computers. The following table presents the types of settings that you can configure.

<table>
<thead>
<tr>
<th>Type of setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative templates</td>
<td>Registry-based settings for configuring application settings and user workstation environments</td>
</tr>
<tr>
<td>Scripts</td>
<td>Settings for specifying when Windows Server 2003 runs specific scripts</td>
</tr>
<tr>
<td>Remote installation services</td>
<td>Settings that control the options available to users when they run the Client Installation Wizard used by Remote Installation Services (RIS)</td>
</tr>
<tr>
<td>Internet Explorer maintenance</td>
<td>Settings for administering and customizing Microsoft Internet Explorer on computers running Windows Server 2003</td>
</tr>
<tr>
<td>Folder redirection</td>
<td>Settings for storing specific user profile folders on a network server</td>
</tr>
<tr>
<td>Security</td>
<td>Settings for configuring local computer, domain, and network security</td>
</tr>
<tr>
<td>Software installation</td>
<td>Settings for centralizing the management of software installations, updates, and removals</td>
</tr>
</tbody>
</table>
GPOs are linked to sites, domains, and organizational units. You can set centralized policies that affect the entire organization and decentralized policies that affect a particular department. There is no hierarchy of domains like there is for organizational units, such as parent and child organizational units.

The order in which Windows Server 2003 applies GPOs is based on the Active Directory container that the GPOs are linked to. Windows Server 2003 applies the GPOs first to the site, then to domains, and then to organizational units within the domains.

Some GPO settings are multivalued. These settings are treated like single valued settings. That is, if the setting is defined in multiple GPOs, only the settings in one of the GPOs that adheres to the inheritance rules apply.

You can prevent a child container from inheriting all GPOs from parent containers by enabling Block Inheritance on the child container. Block Inheritance is useful when an Active Directory container requires unique Group Policy settings.

The Enforced (named No Override if the Group Policy Management console is not installed) option is an attribute of the link, not of the GPO. If the same GPO is linked elsewhere, the Enforced option does not apply to that link unless you modify that link as well. If you have a GPO that is linked to multiple containers, you can configure the Enforced option individually for each container. When more than one link is set to Enforced, the linked GPOs apply to a common container. If they contain conflicting settings, the GPO that is highest in the Active Directory hierarchy takes precedence.

You may need to link GPOs that are associated with other directory objects. By setting the appropriate permissions for security groups, you can filter Group Policy to apply only to the computers and users you specify.

The Group Policy Management console is a set of programmable interfaces for managing Group Policy and a Microsoft Management Console (MMC) snap-in that is built on those programmable interfaces. Together, the components of Group Policy Management unify the management of Group Policy across the enterprise.

Note  For more information about creating and linking GPOs and Group Policy inheritance, see Module 8, “Implementing Group Policy,” in Course 2274, Managing a Microsoft Windows Server 2003 Environment.
Introduction

Windows Server 2003 applies the Group Policy settings that are contained in the GPO to the user and computer objects in the site, domain, or organizational unit that the GPO is associated with. The content of a GPO is stored in two locations: the Group Policy container (GPC) and the Group Policy template (GPT).

The Group Policy container

The GPC is an Active Directory object that contains GPO status, version information, WMI filter information, and a list of components that have settings in the GPO. Computers can access the GPC to locate Group Policy templates, and domain controllers can access the GPC to obtain version information. If the domain controller does not have the most recent version of the GPO, replication occurs to obtain the latest version of the GPO.

The Group Policy template

The GPT is a folder hierarchy in the shared SYSVOL folder on a domain controller. When you create a GPO, Windows Server 2003 creates the corresponding GPT, which contains all Group Policy settings and information, including administrative templates, security, software installation, scripts, and folder redirection settings. Computers connect to the SYSVOL folder to obtain the settings.

The name of the GPT folder is the globally unique identifier (GUID) of the GPO that you created. It is identical to the GUID that Active Directory uses to identify the GPO in the GPC. The path to the GPT on a domain controller is `systemroot\SYSVOL\sysvol`.

Note

For more information about GPC, see “GPO Components” in Module 5 on the Appendices page on the Student Materials compact disc.
Why Specify a Domain Controller for Managing GPOs?

Introduction
Group Policy Management uses the primary domain controller (PDC) emulator in each domain as the default domain controller.

Why select a specific domain controller?
To avoid replication conflicts, consider the selection of domain controller, especially because the GPO data resides in both Active Directory and the SYSPOL folder. Active Directory uses two independent replication mechanisms to replicate GPO data to the various domain controllers in the domain. If two administrators simultaneously edit the same GPO on different domain controllers, one administrator’s changes can overwrite those made by the other administrator, depending on replication latency.

The PDC emulator
By default, the Group Policy Management console uses the PDC emulator in each domain to ensure that all administrators use the same domain controller. However, you may not always want to use the PDC emulator. For example, if you reside in a remote location, or if the majority of the users or computers targeted by the GPO are in a remote location, you may want to target a domain controller there.

Important
If multiple administrators manage a common GPO, it is recommended that all administrators use the same domain controller when editing a particular GPO to avoid collisions in File Replication Services (FRS).
You can specify a domain controller to manage GPOs by selecting any of the following options:

- **The domain controller with the Operations Master token for the PDC emulator.** This is the default and the preferred option.
- **Any available domain controller.** When you use this option, you are likely selecting a domain controller in the local site.
- **Any available domain controller running Windows 2003 or later.** This option is unavailable in environments that contain both Windows Server 2003 and Windows 2000 servers.
- **This domain controller.** When you use this option, you are selecting the current domain controller.
How to Specify a Domain Controller for Managing GPOs

Introduction
You use the Group Policy Management console to specify a domain controller for domains or sites.

Procedure
To specify a domain controller, perform the following steps:

1. Open Group Policy Management, expand the forest, expand Domains, and then use one of the following methods:
   • To specify a domain controller to use for domain operations, right-click the required domain, and then click Change Domain Controller.
   • To specify a domain controller to use for operations on sites, right-click Sites, and then click Change Domain Controller.

2. In the Change Domain Controller dialog box, under Change to, click This domain controller, and then click OK.
What Are WMI Filters?

You use Windows Management Instrumentation (WMI) filters to dynamically determine the scope of GPOs based on attributes of the user or computer. In this way, you can extend the filtering capabilities for GPOs beyond the security group filtering mechanisms that were previously available.

A WMI filter is linked to a GPO. When you apply a GPO to the destination computer, Active Directory evaluates the filter on the destination computer. A WMI filter consists of one or more queries that Active Directory evaluates against the WMI repository of the destination computer. If the total set of queries is false, Active Directory does not apply the GPO. If all queries are true, Active Directory applies the GPO. You write the query by using the WMI Query Language (WQL), which is a language similar to SQL for querying the WMI repository.

Each GPO can have only one WMI filter. However, you can link the same WMI filter to multiple GPOs. Like GPOs, WMI filters apply to only one domain object at a time.

You can use WMI filters to target policies based on various objects in the network. The following list includes some sample uses of WMI filters.

- **Services.** Computers where DHCP is installed and running.
- **Hardware inventory.** Computers that have a Pentium III processor and at least 128 megabytes (MB) of RAM.
- **Software configuration.** Computers with multicasting turned on.

For client computers running Windows 2000, Active Directory ignores WMI filters and always applies the GPO.

**Note** For more information about WMI filters, see “What Are WMI Filters?” in Module 5 on the Appendices page on the Student Materials compact disc.
How to Filter Group Policy Settings Using WMI Filters

Introduction

You can create new WMI filters from the WMI Filters container in the Group Policy Management console. You can also import a filter that was previously exported.

Procedure

To create a WMI filter and link it to a GPO, perform the following steps:

1. Open Group Policy Management, expand the forest that contains the GPO that you want to add a WMI filter to, expand Domains, expand the domain that contains the GPO, expand WMI Filters, right-click WMI Filters, and then click New.

2. In the New WMI Filter dialog box, in the Name box, type a name of the query.

3. In the Description box, type a description of the query.

4. Click Add.

5. In the WMI Query dialog box, in the Namespace box, type the namespace path of the query, or click Browse to see a list of available namespaces.

   For each query, you must specify the WMI namespace where the query is to be executed. The default namespace is root\CIMv2, which should be appropriate for most scenarios.

6. In the Query box, type a valid WQL query statement, and then click OK.

7. In the New WMI Filter dialog box, click Save.

8. Expand Group Policy Objects, and then drag the WMI filter to a GPO.
Example WQL query

For example, to target computers that have more than 10 MB of available space on the C, D, or E drive, the partitions must be located on one or more hard disks and they must be running NTFS file system. Type the following WMI query:

```wql
Select * FROM Win32LogicalDisk WHERE (Name = "C:" OR Name = "D:" OR Name = "E:" ) AND DriveType = 3 AND FreeSpace > 10485760 AND FileSystem = "NTFS"
```

In the example, DriveType value = 3 is a hard disk. The FreeSpace units are in bytes (10 MB = 10,485,760 bytes).

**Note** For more examples of WMI filters, see “How to Filter Group Policy Settings by Using WMI Filters” in Module 5 on the Appendices page on the Student Materials compact disc.
What Is Loopback Processing?

Introduction

By default, a user’s GPOs determine which user settings apply when a user logs on to a computer. In contrast, loopback processing applies the set of GPOs for the computer to any user who logs on to the computer who is affected by this setting. Loopback processing is intended for special-use computers, such as computers in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used.

Example

For example, the user whose user object is located in the Sales organizational unit logs on to a computer. The computer object is located in the Servers organizational unit. The Group Policy settings that are applied to the user are based on any GPOs that are linked to the Sales organizational unit or to any parent containers. The settings that are applied to the computer are based on any GPOs that are linked to the Servers organizational unit or to any parent containers.

This default behavior, however, may not be appropriate for certain servers or computers that are dedicated to a certain task. For example, applications that are assigned to a user should not be automatically available on a server.

Loopback processing modes

Loopback processing has two modes:

- **Replace mode.** This mode replaces the user settings that are defined in the computer’s GPOs with the user settings that are normally applied to the user.

- **Merge mode.** This mode combines the user settings that are defined in the computer’s GPOs and the user settings that are normally applied to the user. If the settings conflict, the user settings in the computer’s GPOs take precedence over the user’s normal settings.
How to Configure the User Group Policy Loopback Processing Mode

Introduction
To enable loopback processing, you select the User Group Policy Loopback Processing mode option in Group Policy Management.

Procedure
To configure the User Group Policy Loopback Processing mode, perform the following steps:

1. Open Group Policy Management, expand the forest, expand Domains, expand your domain, and then click Group Policy Objects.
2. In the details pane, right-click the Group Policy object, and then click Edit.
3. In Group Policy Object Editor, expand Computer Configuration, expand Administrative Templates, expand System, and then click Group Policy.
4. Double-click User Group Policy loopback processing mode, if it is not already selected, click Enabled.
5. Under Mode, click Replace or Merge, and then click OK.
Practice: Creating and Configuring GPOs

In this practice, you will:

- Install the Group Policy Management console
- Create and configure GPOs
Practice: Creating and Configuring GPOs

- Create and configure GPOs

1. Click Start, point to Administrative Tools, right-click Group Policy Management, and then click Run as.
2. In the Run As dialog box, click The following user, type a user name of YourDomain\Administrator with a password of P@ssw0rd and then click OK.
3. Expand Forest, expand Domains, expand your domain, expand Group Policy Objects, right-click Group Policy Objects, and then click New.
4. Type PracticeGPO as the name for your GPO, and then click OK.
5. Right-click your domain name, click Link an Existing GPO, click PracticeGPO, and then click OK.
6. Right-click PracticeGPO, and then click Edit.
7. In Group Policy Object Editor, under User Configuration, expand Administrative Templates, and then click Start Menu and Taskbar.
8. In the details pane, double-click Remove Run menu from Start Menu, click Enabled, and then click OK.
9. In the details pane, double-click Remove and prevent access to the Shut Down command, click Enabled, and then click OK.
11. In Group Policy Management, expand and right-click WMI Filters, and then click New.
12. Type PracticeFilter as the name for the WMI filter, click Add, type an appropriate query to retrieve the required information, click OK, and then click Save.
13. In the console tree, in the list under Group Policy Objects, click PracticeGPO.
14. In the details pane, select PracticeFilter in the This GPO is linked to the following WMI filter box.
15. In the Group Policy Management dialog box, click Yes.
Lesson: Configuring Group Policy Refresh Rates and Group Policy Settings

When Is Group Policy Applied?
How to Assign Group Policy Script Settings
How to Configure Refresh Rates for Group Policy Components
How to Configure Refresh Rates for Domain Controllers and Computers
How to Refresh the Group Policy Settings on a User’s Computer Using Gpupdate.exe

Introduction
Windows Server 2003 executes computer and user settings and policies in a specific order. By understanding Group Policy processing and their order, you can create appropriate scripts and configure refresh rates.

Lesson objectives
After completing this lesson, you will be able to:

- Explain the process of applying Group Policy.
- Assign Group Policy Script settings.
- Configure refresh rates for Group Policy components.
- Configure refresh rates for domain controllers and computers.
- Refresh the Group Policy settings on a user’s computer by using Gpupdate.exe.
When Is Group Policy Applied?

When a user starts a computer and logs on, Windows Server 2003 processes computer settings first and then user settings.

When a user starts a computer and logs on, the following things occur:

1. The network starts. Remote Procedure Call System Service (RPCSS) and Multiple Universal Naming Convention Provider (MUP) start.
2. Windows Server 2003 obtains an ordered list of GPOs for the computer. The list depends on the following factors:
   - Whether the computer is part of a domain and therefore subject to Group Policy through Active Directory.
   - The location of the computer in Active Directory.
   - Whether the list of GPOs has changed.
3. Windows Server 2003 applies the computer policy. These are the settings under Computer Configuration from the gathered list of GPOs. This list is synchronous by default and in the following order: local, site, domain, organizational unit, and child organizational unit. No user interface appears while computer policies are processed.
4. The startup scripts run. The scripts are hidden and synchronous by default. Each script must be completed or time out before the next one starts. The default time-out is 600 seconds. You can use Group Policy settings to modify the default time-out.

**Note** You can adjust the time-out value by configuring the wait time in “Maximum wait time for Group Policy scripts” under Computer Configuration\Administrative Templates\System\Logon\. This setting affects all scripts that run.
5. The user presses CTRL-ALT-DEL to log on.

6. After Windows Server 2003 validates the user, it loads the user profile, which is controlled by the Group Policy settings that are in effect.

7. Windows Server 2003 obtains an ordered list of GPOs for the user. The list depends on the following factors:
   - Whether the user is part of a domain and therefore subject to Group Policy through Active Directory.
   - Whether loopback processing is enabled, and the state of the loopback policy setting.
   - The location of the user in Active Directory.
   - Whether the list of GPOs has changed.

8. Windows Server 2003 applies the user policy, which includes the settings under User Configuration from the gathered list. The settings are synchronous by default and in the following order: local, site, domain, organizational unit, and child organizational unit. No user interface appears while user policies are processed.

9. Logon scripts run. Logon scripts that are based on Group Policy are hidden and asynchronous by default.

10. The operating system user interface that Group Policy prescribes appears.

   Computers running Windows Server 2003 refresh or reapply Group Policy settings at established intervals. Refreshing settings ensures that Group Policy settings are applied to computers and users even if users never restart their computers or log off.

**Note** For more information about when Group Policy is applied and a sample logon script, see “When Is Group Policy Applied?” in Module 5 on the Appendices page on the Student Materials compact disc.
How to Assign Group Policy Script Settings

Introduction
When you implement a script, you use Group Policy to add the script to the appropriate setting in the GPT so that it runs during startup, shutdown, logon, or logoff.

Procedure for copying a script
To copy a script to the appropriate GPT, perform the following steps:

1. Locate the script on your hard disk by using Windows Explorer.
2. Edit the appropriate GPO in Group Policy Management, expand either Computer Configuration (for startup and shutdown scripts) or User Configuration (for logon and logoff scripts), expand Windows Settings, and then click Scripts.
3. Double-click the appropriate script type (Startup, Shutdown, Logon, or Logoff), and then click Show Files.
4. Copy the script file from Windows Explorer to the window that appears, and then close the window.

**Important** You cannot perform this task using Run as; you must be logged on as Administrator in order to perform this task.

Procedure for adding the script
To add a script to a GPO, perform the following steps:

1. In the Properties dialog box for the script type, click Add.
2. Click Browse, select a script, and then click Open.
3. Add any necessary script parameters, and then click OK.

**Note** For more information about creating a script in the Microsoft Visual Basic®, Scripting Edition (VBScript) language, see Course 2433, Microsoft Visual Basic Scripting Edition and Microsoft Windows Script Host Essentials, and Course 2439, WMI Scripting.
How to Configure Refresh Rates for Group Policy Components

Introduction

If Group Policy detects a slow link, it sets a flag to indicate the slow link to the client-side extensions. The client-side extensions can then determine whether to process applicable Group Policy settings.

Group Policy and slow links

Group Policy compares the connection speed of the link with 500 kilobytes per second (KBps)—the speed that it considers slow—or with a threshold of your choice. Group Policy uses an algorithm to determine whether a link is considered slow.

Default settings

The following table shows the default settings for slow link processing.

<table>
<thead>
<tr>
<th>Client-side extension</th>
<th>Slow-link processing</th>
<th>Refreshed</th>
<th>Can it be changed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry policy processing</td>
<td>On</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>Internet Explorer Maintenance policy processing</td>
<td>Off</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>Software Installation policy processing</td>
<td>Off</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Folder Redirection policy processing</td>
<td>Off</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Scripts policy processing</td>
<td>Off</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>Security policy processing</td>
<td>On</td>
<td>On</td>
<td>No</td>
</tr>
<tr>
<td>IP Security policy processing</td>
<td>Off</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>Wireless policy processing</td>
<td>Off</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>EFS recovery policy processing</td>
<td>On</td>
<td>On</td>
<td>Yes</td>
</tr>
<tr>
<td>Disk Quota policy processing</td>
<td>Off</td>
<td>On</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Procedure

To configure which Group Policy components are refreshed and can be modified, perform the following steps:

1. Open the appropriate GPO in Group Policy, expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, click **Group Policy**, and then double-click each item in the preceding table.

2. Click **Enabled**.

3. Click **Do not apply during periodic background processing**.

4. If available, click **Allow processing across a slow network connection**, and then click **OK**.

**Note**  For more information about the algorithm that Group Policy uses to detect slow links, see “How to Configure Which Group Policy Components Are Refreshed” in Module 5 on the Appendices page on the Student Materials compact disc.
How to Configure Refresh Rates for Domain Controllers and Computers

Introduction
You can change the default refresh rates by modifying the administrative template settings for a user or computer configuration.

Default refresh intervals
The following table lists the default intervals for refreshing Group Policy.

<table>
<thead>
<tr>
<th>Type of computer</th>
<th>Refresh interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers running Windows XP Professional and domain member servers running Windows Server 2003</td>
<td>Every 90 minutes. It also refreshes on a random time offset every 30 minutes, which helps load balance application processing of Group Policy and ensures that multiple computers do not contact a domain controller at the same time.</td>
</tr>
<tr>
<td>Domain controllers</td>
<td>Every five minutes. This way, critical new Group Policy settings, such as security settings, are applied at least every five minutes unless you change the default setting.</td>
</tr>
</tbody>
</table>
To configure refresh rates, perform the following steps:

1. Open the appropriate GPO in Group Policy, expand User Configuration or Computer Configuration (depending on which GPO you want to edit), expand Administrative Templates, expand System, click Group Policy, and then double-click one of the following settings:
   - Group Policy refresh interval for users
   - Group Policy refresh interval for computers
   - Group Policy refresh interval for domain controllers

2. Select Enabled.

3. Set the refresh interval in minutes.

4. Set the random time offset, and then click OK.

**Note**  If you disable these settings, Group Policy is updated by default every 90 minutes. To specify that Group Policy should never be updated when the computer is in use, select the Turn off background refresh of Group Policy option.
How to Refresh the Group Policy Settings on a User’s Computer Using Gpupdate.exe

You can refresh a Group Policy object by using the `gpupdate` command.

To refresh the Group Policy settings on a user’s computer by using the `gpupdate` command, perform the following steps:

1. In the Run dialog box, type `cmd` and then press ENTER.
2. Type

   ```
   ```

The following table describes each parameter of the `gpupdate` syntax.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/target:{computer</td>
<td>user}</td>
</tr>
<tr>
<td>/force</td>
<td>Reapplies all settings and ignores processing optimizations.</td>
</tr>
<tr>
<td>/wait:value</td>
<td>Specifies the number of seconds that policy processing waits to finish, which by default, is 600 seconds. A value of 0 means no wait; -1 means wait indefinitely.</td>
</tr>
<tr>
<td>/logoff</td>
<td>Logs off after the policy refresh is completed. This parameter is required for Group Policy client-side extensions that do not process Group Policy settings on a background refresh cycle but do process them when the user logs on. This option has no effect if there are no extensions called that require the user to log off.</td>
</tr>
<tr>
<td>/boot</td>
<td>Restarts the computer after the policy refresh is completed. Restarting the computer is required for those Group Policy client-side extensions that do not process Group Policy settings on a background refresh cycle but do process them when the computer starts up. This option has no effect if there are no extensions called that require the computer to be restarted.</td>
</tr>
</tbody>
</table>
Practice: Configuring Group Policy Refresh Rates and Group Policy Settings

In this practice, you will:
- Configure the Group Policy refresh interval for client computers
- Configure Group Policy settings for synchronizing offline files

Objective
In this practice, you will configure the Group Policy refresh interval for client computers and then configure Group Policy settings for synchronizing offline files.

Scenario
Northwind Traders relies heavily on Group Policy to manage client computers and to keep the organization agile. Because of the large number of GPOs you must modify daily, you want to reduce network traffic by decreasing the refresh interval for client computers to 180 minutes and by using a random time offset of 60 minutes.

People in your organization often travel and use slow dial-up connections. They also frequently visit remote sales offices that have high-speed connections to the corporate network. They need access to files that normally are accessible only by using a network connection to a file server. These files must be up to date as soon as the user logs on to the corporate network. You must configure the availability and synchronization of offline files in Group Policy for the users who require this capability.

Practice
1. Open Group Policy Management as YourDomain\Administrator by using Run as.
2. Expand Forest, expand Domains, expand your domain, expand Group Policy Objects, click Group Policy Objects, right-click PracticeGPO, and then click Edit.
3. In Group Policy Object Editor, under Computer Configuration, expand Administrative Templates, expand System, and then click Group Policy.
4. Double-click Group Policy Refresh Interval for computers, click Enabled, type the appropriate time intervals, and then click OK.
5. In Group Policy Object Editor, under User Configuration, expand Administrative Templates, expand Network, and then click Offline Files.

6. Double-click Synchronize all offline files when logging on, click Enabled, and then click OK.

7. Close Group Policy Object Editor, and then close Group Policy Management.
Lesson: Managing GPOs

You use the Group Policy Management console to manage GPOs, which includes copying a GPO to another location, backing up a GPO, restoring a GPO from the backup, and importing settings from one GPO to another.

After completing this lesson, you will be able to:

- Explain the purpose of copying a GPO.
- Copy a GPO by using Group Policy Management.
- Explain the purpose of backing up a GPO.
- Back up a GPO by using Group Policy Management.
- Explain the purpose of restoring a GPO.
- Restore a GPO by using Group Policy Management.
- Explain the purpose of importing settings into a GPO.
- Import settings into a GPO by using Group Policy Management.
What Is a Copy Operation?

A copy of a GPO transfers only the settings in the GPO. The newly created GPO has a new GUID and the default discretionary access control list (DACL) for the GPO. The new GPO is created unlinked because links are a property of the object that defined the GPO, rather than a property of the GPO.

When you copy a GPO from one domain to another, you must specify the mapping behavior of the security principals for the copy operation. Group Policy Management provides two basic mapping techniques for copying GPOs:

- Copy them identically from the source
- Use a migration table to map them to new values in the new GPO

To use either approach, references to security principals and Universal Naming Convention (UNC) paths must exist in the source GPO.

When you copy GPOs across domains or forests, Group Policy Management can perform security principal mapping. That is, it can modify settings that refer to security principals by translating the destination security principals to new values in the new GPO.

If you require additional customization, you can use scripting to implement a migration table, which is an Extensible Markup Language (XML) text file that specifies custom mapping of security principals from the source domain to the destination domain. The migration table contains a security principal mapping section and a path mapping section. You use these sections to set specific mapping rules.
How to Copy a GPO

To copy a GPO, you must have permission to create GPOs in the destination domain.

To copy a GPO, perform the following steps:

1. Open Group Policy Management, expand Group Policy Objects in the forest and domain that contains the GPO that you want to copy, right-click the GPO, and then click Copy.

2. Do one of the following:
   - To place the copy of the GPO in the same domain as the source GPO, right-click Group Policy Objects, and then click Paste.
     i. On the Copy GPO page, select either Use the default permissions for New GPOS or Preserve the existing permissions, and then click OK.
     ii. When copy progress has completed, click OK.
   - To place the copy of the GPO in a different domain, whether in the same forest or a different forest, expand the destination domain, right-click Group Policy Objects, and then click Paste.
     i. On the Welcome to the Cross-Domain Copying Wizard page, click Next.
     ii. On the Specifying permissions page, select either Use the default permissions for new GPOS or Preserve or migrate the permissions from the original GPOs, and then click Next.
     iii. On the Scanning Original GPO page, click Next.

If the source GPO contains references to security principals and UNC paths, you will see the window mentioned in the next step. Otherwise, continue to step v.
iv. On the Migrating References page, select either Copying them identically from the source or Using this migration table to map them to new values in the new GPOs, select the migration table from the list, and then click Next.

v. On the Completing the Cross-Domain Copying Wizard page, click Finish.

vi. After the copy operation is completed, click OK.

Note Some of these steps may not appear if you are copying a GPO to the same domain.
What Is a Backup Operation?

Introduction

When Group Policy Management backs up a GPO, it exports the data to a file that you choose and saves all Group Policy template (GPT) files. You can send the backed-up GPO to a folder by using a restore or import operation. You can only restore a backed-up GPO to another domain by using an import operation.

How to store a backup?

You can store multiple backed-up GPOs, including versions of the same GPO, in one file folder. Regardless of how many GPOs you store in a folder, you can identify each backed-up GPO by one of the following criteria:

- GPO display name
- GPO GUID
- Description of the backup
- Date and time stamp of the backup
- Domain name.

You can back up one or more GPOs to a previously specified backup location, or you can specify a new backup location.

Note  Be sure that the backup directory is in a secure location in the file system.
How to Back Up a GPO

To back up a GPO, you must have Read permission to the GPO and Write permission to the file system location where you want to store the backed-up GPO.

To back up a GPO, perform the following steps:

1. Open Group Policy Management, expand the forest that contains the GPO that you want to back up, expand Domains, expand the domain that contains the GPO, expand Group Policy Objects, and then do one of the following:
   - To back up a single GPO, right-click the GPO, and then click Back Up.
   - To back up all GPOs, right-click Group Policy Objects, and then click Back Up All.

2. In the Backup Group Policy Object dialog box, type the path to the location where you want to store the backed-up GPO.

3. Type a description for the GPO that you want to back up, and then click Backup.

4. After the backup operation is completed, click OK.
What Is a Restore Operation?

The restore operation returns the contents of the GPO to the same state it was in when the backup was performed. This operation is only valid in the domain where the GPO was created.

You can restore an existing GPO or a deleted GPO that was backed up. The permissions that are required to restore a GPO depend on whether the GPO exists in Active Directory when you restore it.
How to Restore a GPO

Introduction

To restore an existing GPO by using Group Policy Management, you must have Edit, Delete, and Modify Security permissions for the GPO. You must also have Read permission to the folder that contains the backed-up GPO.

To restore a deleted GPO that was backed up, you must have the permission to create GPOs in the domain and also Read permission to the file system location of the backed-up GPO.

Procedure for restoring a previous version of a GPO

To restore a previous version of an existing GPO, perform the following steps:

1. Open Group Policy Management, expand the forest that contains the GPO that you want to restore, expand Domains, expand the domain that contains the GPO, right-click Group Policy Objects, and then click Manage Backups.

2. In the Manage Backups dialog box, select the backed-up GPO that you want to restore, and then click Restore.

3. When you are prompted to restore the selected backup, click OK.

4. In the Restore Progress dialog box, click OK after the restore is completed.

5. In the Manage Backups dialog box, either select another GPO to restore or click Close to complete the restore operation.

Procedure for restoring a deleted GPO

To restore a deleted GPO that appears in the list of Group Policy Objects, perform the following steps:

1. Open Group Policy Management, expand the forest that contains the GPO that you want to restore, expand Domains, and then expand the domain that contains the GPO.

2. Right-click Group Policy Objects, and then click Manage Backups.

3. In the Manage Backups dialog box, click Browse, locate the file system that contains the deleted GPO, select the GPO, click Restore, and then click OK to confirm the restore operation.
What Is an Import Operation?

---

**Introduction**

An import operation copies all of the GPO settings from the source GPO to the destination GPO.

**Why specify a migration table?**

You specify a migration table to ensure that the UNC path in the source GPO maps correctly to the UNC path of the destination GPO. You provide the path to the appropriate migration table when you import GPO settings from one domain to another. If you specify a migration table, you must specify the UNC path mapping behavior.

If you do not select the **Use migration table exclusively** check box, you must specify the mapping behavior for security principals that are not contained in the migration table.

If you do not specify a migration table, all security principals are mapped according to the behavior that you specify.
How to Import Settings into a GPO

To import settings into a GPO, you must have Edit permissions on the GPO.

To import settings into a GPO, perform the following steps:

1. Open Group Policy Management, expand the forest that contains the GPO that you want to import settings into, expand **Domains**, expand the domain that contains the GPO, expand **Group Policy Objects**, right-click the GPO, and then click **Import Settings**.

2. On the **Welcome to the Import Settings Wizard** page, click **Next**.

3. On the **Backup GPO** page, click **Backup**.

4. In the **Backup Group Policy Object** dialog box, type a location and description for the GPO backup, and then click **Backup**.

5. When the backup operation is complete, click **OK**, and then click **Next**.

6. On the **Backup location** page, click **Browse** to locate the backup folder that you want to import settings from, and then click **Next**.

7. On the **Source GPO** page, select the GPO that you want to import settings from, and then click **Next**.

If the source GPO contains references to security principals and UNC paths, the **Migrating References** dialog box appears. Choose how to migrate security principals and UNC paths by selecting either **Copying them identically from the source** or **Using this migration table to map them in the destination GPO**, and then select a migration table.

8. Click **Next**.

9. On the **Completing the Import Settings Wizard** page, click **Finish**.

10. When the import operation is completed, click **OK**.
**Practice: Managing GPOs**

In this practice, you will:

- Copy a GPO
- Back up the GPO
- Delete the backed-up GPO
- Restore the deleted GPO

---

**Objectives**

In this practice, you will copy a GPO, create a backup of it, delete the backed-up copy, and then restore it.

**Scenario**

You are responsible for implementing the corporate desktop standards by using Group Policy for your domain. Although most groups in the domain can use the same standard corporate desktop configuration, some departments require a slightly different configuration. You will create a base GPO, copy it to the various applications, and then modify the settings.

Because you are concerned that backing up and restoring GPOs may not work correctly, you want to test recovery capabilities and simulate your implementation plan in your test environment.

---

**Practice: Copying a GPO**

► **Copy a GPO**

1. Open Group Policy Management as `YourDomain\Administrator` by using `Run as`.
2. In your domain, expand `Group Policy Objects`, right-click `PracticeGPO`, click `Copy`, right-click `Group Policy Objects`, and then click `Paste`.
3. In the `Copy GPO` dialog box, click `OK`.
4. After the copy progress is completed, click `OK`.

---

**Practice: Backing up a GPO**

► **Back up a GPO**

1. In Group Policy Management, right-click `Copy of PracticeGPO`, and then click `Back Up`.
2. In the `Back Up Group Policy Object` dialog box, type `C:` in the `Location` box, and then click `Backup`.
3. After the operation is completed, click `OK`.
Practice: Restoring a GPO

► Delete and restore a GPO

1. In Group Policy Management, right-click Copy of PracticeGPO, click Delete, and then click OK.

2. Right-click Group Policy Objects, and then click Manage Backups.

3. In the Manage Backups dialog box, select Copy of PracticeGPO, and then click Restore.

4. When prompted to restore the backup, click OK.

5. In the Restore Progress dialog box, click OK after the backed-up copy is restored.

6. In the Manage Backups dialog box, click Close.

7. Verify that the GPO has been restored.

Lesson: Verifying and Troubleshooting Group Policy

Introduction

You may encounter problems when you implement Group Policy. When you troubleshoot Group Policy problems, be sure to consider dependencies between components. For example, Group Policy relies on Active Directory, which relies on proper configuration of network services.

Windows Server 2003 has two new Group Policy management features that help you determine the effect of Group Policy settings for a particular user or computer. These features are Group Policy Modeling Wizard and Group Policy Results.

Lesson objectives

After completing this lesson, you will be able to:

- Identify the common problems with implementing Group Policy.
- Verify Group Policy settings by using Group Policy Modeling Wizard.
- Verify Group Policy settings by using Group Policy Results.
Common Problems with Implementing Group Policy

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot open a GPO</td>
<td>Read and Write permissions for the GPO are not assigned</td>
</tr>
<tr>
<td>Cannot edit a GPO</td>
<td>A networking problem</td>
</tr>
<tr>
<td>Cannot apply Group Policy on a security group</td>
<td>GPOs are not applied to security groups</td>
</tr>
<tr>
<td>No effect of Group Policy on a site, domain, or organizational unit</td>
<td>Group Policy settings are not configured correctly</td>
</tr>
<tr>
<td>No effect of Group Policy in an Active Directory container</td>
<td>GPOs cannot be linked to Active Directory containers</td>
</tr>
<tr>
<td>No effect of Group Policy on a client computer</td>
<td>A non-local GPO can overwrite local policies</td>
</tr>
</tbody>
</table>

Introduction

The first step in troubleshooting Group Policy is to identify the symptoms and possible causes.

How to verify if the correct Group Policy settings are applied

In most cases, a Group Policy setting is not being applied as expected because another GPO contains a conflicting value for the same setting. The GPO is taking precedence because of Block Inheritance, Enforced, filtering, or the order of application. Use the Group Policy Modeling Wizard or the Group Policy Results Wizard to determine which GPO is being used for the setting.

Symptoms, cause, and resolution

The following table lists some common symptoms and their possible resolution methods.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot open a GPO, even with Read permission</td>
<td>Be a member of a security group with Read and Write permission for the GPO.</td>
</tr>
<tr>
<td>When you try to edit a GPO, the message Failed To Open The Group Policy Object appears</td>
<td>Make sure DNS is working properly.</td>
</tr>
<tr>
<td>Group Policy is not applied to users and computers in a security group that contains them, even though a GPO is linked to an organizational unit that contains the security group</td>
<td>Link GPOs to sites, domains, and organizational units only.</td>
</tr>
<tr>
<td>Group Policy is not affecting users and computers in an Active Directory container</td>
<td>Link a GPO to an organizational unit that is a parent to the Active Directory container. Those settings are then applied by default to the users and computers in the container through inheritance.</td>
</tr>
<tr>
<td>Group Policy is not taking effect on the client computer</td>
<td>Determine which GPOs are being applied through Active Directory and if those GPOs have settings that are in conflict with the local settings.</td>
</tr>
</tbody>
</table>
How to Verify Group Policy Settings Using Group Policy Modeling Wizard

Introduction

You can simulate a policy deployment for users and computers before actually applying the policies. This feature in Group Policy Management is known as Resultant Set of Policies (RSoP) – Planning Mode. It requires a domain controller running Windows Server 2003 in the forest. To verify Group Policy settings by using Group Policy Modeling Wizard, you first create a Group Policy Modeling query and then view that query.

Procedure for creating a Group Policy Modeling query

To create a new Group Policy Modeling query, perform the following steps:

1. Open Group Policy Management, browse to the forest in which you want to create a Group Policy Modeling query, right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.

2. On the **Welcome to the Group Policy Modeling Wizard** page, click **Next**, type the appropriate information in the wizard pages, and then click **Finish**.

Procedure for viewing the Group Policy Modeling query

To view the Group Policy Modeling query, perform the following steps:

1. Open Group Policy Management.

2. Browse to the forest that contains the Group Policy Modeling query that you want to view, expand **Group Policy Modeling**, right-click the query, and then click **Advanced View**.

**Note**

For information about verifying Group Policy settings by using Gpresult.exe, see “How to Verify Group Policy Settings by Using Group Policy Results” in Module 5 on the Appendices page on the Student Materials compact disc.
How to Verify Group Policy Settings Using Group Policy Results

Introduction
You use Group Policy Results to determine the policy settings that are applied to a computer and the user who logged on to that computer. Although this data is similar to Group Policy Modeling data, it is obtained from the client computer, rather than simulated on the domain controller. To obtain data by using Group Policy Results, the client computer must be running Windows XP or Windows Server 2003.

Procedure for creating a Group Policy Results query
To create a Group Policy Results query, perform the following steps:

1. In Group Policy Management, browse to Group Policy Results, right-click Group Policy Results, and then click Group Policy Results Wizard.
2. On the Welcome to the Group Policy Results Wizard page, click Next.
3. On the Computer Selection page, select the current computer or click Browse to select another computer, and then click Next.
4. On the User Selection page, select the current user or specify a user, and then click Next.
5. On the Summary of Selections page, verify your selections, and then click Next.
Procedure for viewing the Group Policy Results query

To view the Group Policy Results query, perform the following steps.

1. Open Group Policy Management.

2. Browse to the forest that contains the Group Policy Modeling query that you want to view, expand **Group Policy Results**, right-click the query, and then click **Advanced View**.

**Note** You can monitor Group Policy by enabling diagnostic logging and verbose logging. For information about enabling Group Policy logging, see “How to Troubleshoot Conflicts in Group Policy Settings” in Module 5 on the Appendices page on the Student Materials compact disc.
Practice: Verifying and Troubleshooting Group Policy

In this practice, you will verify Group Policy settings by using Group Policy Modeling Wizard.

Scenario
You want to verify that the GPO settings that you plan to deploy—including user and computer settings for your domain—take effect and are accurate at Northwind Traders. You decide to use the Group Policy Management console to verify the settings.

Practice
► Verify user and computer settings for your domain
1. Open Group Policy Management as YourDomain\Administrator by using Run as.
2. Right-click Group Policy Modeling, and then click Group Policy Modeling Wizard.
5. On the User and Computer Selection page, in the User Information and Computer Information sections, click Browse, select your domain for each section, and then click Next.
6. On each of the following wizard pages, click Next to accept the default settings.
8. If an Internet Explorer dialog box appears, click Add, in the Trusted Sites dialog box, click Add, and then click Close.
9. View the report in the details pane, and then close Group Policy Management.
Lesson: Delegating Administrative Control of Group Policy

Introduction
You can use Group Policy to delegate certain Group Policy tasks to other administrators. For example, the creation, linking, and editing of GPOs are independent permissions that you can delegate separately. Group Policy Management simplifies the management of permissions by combining the low-level permissions on an object and managing them as a single unit. You use Group Policy Management to delegate administrative control of GPOs, Group Policy for a site, domain, and organizational unit, and WMI filters.

Lesson objectives
After completing this lesson, you will be able to:

- Explain the delegation of GPOs.
- Explain the delegation of Group Policy for a site, domain, or an organizational unit.
- Explain the delegation of WMI filters.
- Delegate administrative control for managing Group Policy links.
- Delegate administrative control for creating and editing Group Policy objects.
Delegation of GPOs

You can delegate the ability to create GPOs in a domain and assign permissions on an individual GPO by using Group Policy Management.

By default, the Group Policy Creator Owners group is assigned the ability to create GPOs. However, you can delegate that ability to any group or user by using one of the following two ways:

- Add the group or user to the Group Policy Creator Owners group. This was the only method available prior to Group Policy Management.
- Explicitly assign the group or user permission to create GPOs. This method is available only by using Group Policy Management.

For users and groups within the domain, use the Group Policy Creator Owners group to assign permissions for creating a GPO. Because the Group Policy Creator Owners group is a domain global group, it cannot contain members from outside the domain. If users outside the domain need the ability to create GPOs, do the following:

1. Create a new domain local group in the domain.
2. Assign that group permission for GPO creation in the domain.
3. Add external domain users to that group.

The permissions are identical, whether you add a user to the Group Policy Creator Owners group or assign the user permissions for GPO creation directly by using Group Policy Management. Users can create GPOs in the domain and enjoy full control of them, but they do not have permissions on GPOs that other users create.

Granting a user the ability to create GPOs in the domain does not enable him to link the GPO to a site, domain, or organizational unit.
Delegate permissions on an individual GPO

You can also manage permissions on the GPO at the task level. The following five categories are Allowed Permissions on a GPO.

- Read
- Edit settings
- Edit, Delete, Modify Security
- Read (from Security Filtering)
- Custom

**Note**  For more information about delegating administrative control of Group Policy, see “Group Policy Tasks that Can Be Delegated” in Module 5 on the Appendices page on the Student Materials compact disc.
Delegation of Group Policy for a Site, Domain, or Organizational Unit

Introduction
Delegation of Group Policy for site, domain, and organizational unit includes delegating the ability to link GPOs, and delegate permissions for Group Policy Modeling and Group Policy Results.

Delegate the ability to link GPOs
Group Policy Management uses a single permission named Link GPOs to manage the gPLink and gPOptions attributes. You apply the settings in a GPO to users and computers by linking the GPO—either as a direct child or indirectly through inheritance—to a site, domain, or organizational unit that contains the user or computer objects.

The Link GPOs permission is specific to that site, domain, or an organizational unit. The permission equates to having the Read and Write permissions to the gPLink and gPOptions attributes on the site, domain, or organizational.

Delegate permissions for Group Policy Modeling
You can use Group Policy Modeling to simulate the set of policies for objects in a domain or organizational unit—or you can delegate it to other users or groups. This delegation assigns the user or group the Generate Resultant Set of Policy (Planning) permission, which is available in any forest that has the Windows Server 2003 schema.

Group Policy Management simplifies the management of this permission by listing it on the Delegation tab for any domain or organizational unit. The administrator can select Perform Group Policy Modeling Analyses, and then select the Name, Applies To, Setting, and Inherited properties for the delegations.
You can use Group Policy Results to read RSoP logging data for objects in the domain or organizational unit. Like Group Policy Management, you can delegate this permission to other users or groups. You delegate permissions on either a domain or an organizational unit. Users who have this permission can read Group Policy Results data for any object in that container. This delegation also assigns the user or group the Generate Resultant Set of Policy (Logging) permission, which is available in any forest that has the Windows Server 2003 schema.

Group Policy Management simplifies the management of this permission by listing it on the Delegation tab for the domain or organizational unit. The administrator can select Read Group Policy Results Data, and then select the users and groups that have this permission.
Delegation of WMI Filters

Introduction
You can delegate the ability to create WMI filters in a domain and assign permissions on them.

Delegate the ability to create WMI filters
You create WMI filters in the WMI Filters container in Group Policy Management. When you create a new WMI filter, Active Directory stores it in the WMIPolicy container in the domain’s System container. The permissions on the WMIPolicy container determine the permissions that a user has to create, edit, and delete WMI filters.

There are two permissions for creating WMI filters:

- **Creator Owner.** Allows the user to create new WMI filters in the domain. It does not assign the user permissions on WMI filters that other users create.

- **Full Control.** Allows the user to create WMI filters and assign Full Control on all WMI filters in the domain, including new filters that the user creates after she is granted this permission.

Delegate permissions on a WMI filter
You can use Group Policy Management to delegate permissions on a particular WMI filter. There are two permissions that you can assign to a user or group:

- **Edit.** Allows the user or group to edit the WMI filter.

- **Full Control.** Allows the user or group to edit, delete, and modify security on the WMI filter.
How to Delegate Administrative Control for Managing Group Policy Links

Introduction

You can delegate the ability to manage Group Policy links by selecting Manage Group Policy links in the Delegation of Control Wizard to enable a user to link and unlink GPOs.

Procedure

To delegate administrative control for managing Group Policy links, perform the following steps:

1. Open Group Policy Management.
2. Browse to the forest and the domain in which you want to delegate administrative control for managing Group Policy links, and then click the link.
3. In the details pane, on the Delegation tab, click Add.
4. In the Select User, Computer, or Group dialog box, in the Enter the object name to select (examples) box, type the security principal, click Check Names, and then click OK.
5. In the Add Group or User dialog box, in the Permissions box, select the appropriate permission, and then click OK.

Note If you prefer the flexibility of the Properties dialog box, it is still available in Group Policy Management by clicking Advanced on the Delegation tab.
How to Delegate Administrative Control for Creating and Editing GPOs

<table>
<thead>
<tr>
<th>Introduction</th>
<th>You use the Delegation of Control Wizard to delegate administrative control to create and edit GPOs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure for delegating administrative control for creating GPOs</td>
<td>To delegate administrative control for creating GPOs, perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Open Group Policy Management.</td>
</tr>
<tr>
<td></td>
<td>2. Browse to the forest and the domain in which you want to delegate administrative control for creating GPOs, and then click <strong>Group Policy Objects</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the details pane, on the <strong>Delegation</strong> tab, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Select User, Computer, or Group</strong> dialog box, in the <strong>Enter the object name to select (examples)</strong> box, type the security principal, click <strong>Check Names</strong>, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Procedure for delegating administrative control for editing GPOs</td>
<td>To delegate administrative control for editing GPOs, perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Open Group Policy Management.</td>
</tr>
<tr>
<td></td>
<td>2. Browse to the forest and the domain in which you want to delegate administrative control for editing GPOs, and then click the link.</td>
</tr>
<tr>
<td></td>
<td>3. In the details pane, on the <strong>Delegation</strong> tab, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Select User, Computer, or Group</strong> dialog box, in the <strong>Enter the object name to select (examples)</strong> box, type the security principal, click <strong>Check Names</strong>, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Add Group or User</strong> dialog box, in the <strong>Permissions</strong> box, select the appropriate permission, and then click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
Objectives

In this practice, you will add the junior administrator’s account to the Group Policy Creator Owners group and then delegate the ability for her to manage Group Policy links.

Scenario

You have decided to delegate Group Policy administration for the Accounting, Accounts Payable, and Accounts Receivable organizational units to a junior administrator. She will be responsible for linking and unlinking GPOs, creating new GPOs, and modifying the existing GPOs. She will also manage any other objects in the organizational units.

Practice

► Delegate administrative control of Group Policy to a user

1. Open Group Policy Management as YourDomain\Administrator by using Run as.

2. Expand Forest, expand Domains, expand YourDomain, expand Group Policy Objects, and then click PracticeGPO.

3. On the Delegation tab, add Nwtraders\ComputerNameUser to the list with Edit settings, delete, and modify security permissions, and then click OK.

4. In Group Policy Management, click YourDomain, and then in the details pane, click the link to PracticeGPO.

5. In the details pane, on the Delegation tab, click Add.

6. In the Select User, Computer, or Group dialog box, in the Enter the object name to select box, type Nwtraders\ComputerNameUser, click Check Names, and then click OK.

7. In the Add Group or User dialog box, in the Permissions box, select the appropriate permission, and then click OK.

Lesson: Planning a Group Policy Strategy for the Enterprise

Introduction

When you plan an Active Directory structure, create a plan for GPO inheritance, administration, and deployment that provides the most efficient Group Policy management for your organization.

Also consider how you will implement Group Policy for the organization. Be sure to consider the delegation of authority, separation of administrative duties, central versus decentralized administration, and design flexibility so that your plan will provide for ease of use as well as administration.

Lesson objectives

After completing this lesson, you will be able to:

- Explain guidelines for planning GPOs.
- Explain guidelines for determining GPO inheritance.
- Explain guidelines for determining a Group Policy strategy for sites.
- Explain guidelines for planning the administration of GPOs.
- Explain guidelines for deploying GPOs.
Guidelines for Planning GPOs

Create GPOs in a way that provides for the simplest and most manageable design—one in which you can use inheritance and multiple links.

Apply the following guidelines for planning GPOs:

1. **Apply GPO settings at the highest level.** This way, you take advantage of Group Policy inheritance. Determine what are the common GPO settings for the largest container, starting with the domain, and then link the GPO to this container.

2. **Reduce the number of GPOs.** You reduce the number by using multiple links instead of creating multiple identical GPOs. Try to link a GPO to the broadest container possible to avoid creating multiple links of the same GPO at a deeper level.

3. **Create specialized GPOs.** Use these GPOs to apply unique settings when necessary. GPOs at a higher level will not apply the settings in these specialized GPOs.

4. **Disable computer or user configuration settings.** When you create a GPO to contain settings for only one of the two levels—user or computer—disable the other area. It improves the performance of a GPO application during user logon and prevents accidental GPO settings from being applied to the other area.
Guidelines for Determining GPO Inheritance

Introduction
GPO inheritance plays an important part in implementing Group Policy in an enterprise. Therefore, you must decide beforehand whether to apply Group Policy to all or to specific users and computers.

Guidelines
Apply the following guidelines for determining GPO inheritance:

- *Use the Enforced option only when required.* Use this option only for GPOs that you want to absolutely enforce, such as corporate-mandated security settings. Ensure that you design these GPOs to contain only these important settings.

- *Use Block Inheritance sparingly.* These settings make the troubleshooting and administration of GPOs more difficult.

- *Use security filtering only when necessary.* Use security filtering when settings apply only to a specific security group in a container. Limit the amount of security filtering by creating and linking GPOs at the appropriate level.
Guidelines for Determining a Group Policy Strategy for Sites

You can link GPOs to a site, which enforces settings on all computers and users that are physically located at that site. When Group Policy is set at the site level, it does not affect mobile users on that site if they access the network from another site.

Apply the following guidelines for determining a Group Policy strategy for sites:

- **Apply a GPO to a site only when the settings are specific to the site and not to the domain**. Troubleshooting GPO settings that are linked to the site can be difficult.

- **Create GPOs in the domain that has the most domain controllers in that site**. A domain controller from the domain that contains the site-linked GPO is contacted before the GPO is applied, regardless of what domain the user or computer is a member of.
Guidelines for Planning the Administration of GPOs

Introduction
Be sure to document the following information about your strategy for managing GPOs in your organization.

Guidelines
Apply the following guidelines for planning the administration of GPOs:

- **Identify your administrative strategy for managing GPOs.** Determine who will create and link GPOs in your organization, and who will link GPOs but not create them. Also, determine who manages GPOs.

- **Organize GPOs according to administrative maintenance.** This way, you can delegate control of GPOs to the appropriate group and also reduce the potential for one administrator to overwrite changes that were made by another administrator on a given GPO. For example, you can organize Group Policy into the following categories of administration:
  - User configuration management
  - Data management
  - Software distribution

- **Plan for the auditing of GPOs.** Your organization may require you to log changes to GPOs and their use so that you can verify that Active Directory applied the settings correctly.
Guidelines for Deploying GPOs

Introduction
When planning to implement Group Policy, be sure to test and document your Group Policy strategy.

Guidelines
Apply the following guidelines for deploying GPOs:

- **Test Group Policy settings.** Test the results of GPOs in many situations. Many medium- and large-sized organizations create a miniature version of the production environment to use as a test bed. In small organizations that lack the resources to create a test bed, implement Group Policy in the production environment at off-peak times, and have a regression strategy in place to rectify any problems. Testing strategies include:
  - Log on as representative users at representative workstations to verify that the expected Group Policy settings have been applied and that inheritance conflicts do not occur. You can use the Group Policy Modeling Wizard and the Group Policy Results Wizard to determine which Group Policy settings from which GPOs have been applied.
  - Log on in all possible conditions to ensure that Group Policy settings are applied consistently.
  - Test portable computers by connecting them to the network from various sites where users are likely to log on.

- **Document the Group Policy plan.** Always keep a detailed list of all GPOs so that you can easily troubleshoot and manage Group Policy. Consider including the following information in your list:
  - The name and purpose of each GPO.
  - Group Policy settings in each GPO.
  - GPO links to a site, domain, or organizational unit.
  - Any special settings that are applied to the GPO, such as Enforce, partial disable, and full disable.
Practice: Planning a Group Policy Strategy for the Enterprise

In this practice, you will:
- Determine the effects of Group Policy settings
- Manage deployment of Group Policy

File Location
To view the Planning a Group Policy Strategy for the Enterprise activity, open the Web page on the Student Materials compact disc, click Multimedia, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

Objective
In this practice, you will determine the effect of applying some Group Policy settings and GPO inheritance.

Instructions
The Planning a Group Policy Strategy for the Enterprise activity includes multiple choice and drag-and-drop exercises that test your knowledge. Read the instructions, and then begin the activity on the Effects of Group Policy Settings tab.
Lab A: Implementing Group Policy

After completing this lab, you will be able to:

- Create and configure GPOs.
- Link GPOs.
- Verify the Group Policy settings.

Before working on this lab, you must have:

- Experience using Group Policy Management.
- Experience using the Group Policy Object Editor and the Group Policy Modeling Wizard.

Estimated time to complete this lab:
75 minutes
Exercise 1
Creating and Configuring GPOs

In this exercise, you will create an organizational unit for the Accounting department and separate organizational units for the Accounts Receivable and Accounts Payable groups in the Accounting department. Next, you will create and configure GPOs for the Accounts Receivable and Accounts Payable groups. You will perform these tasks on your domain in the forest.

Scenario

Northwind Traders wants strict control over policies that the Accounting department uses. You must ensure that the department uses certain global settings from the corporate GPO. You will create an Accounting standard GPO to remove the Run command from the Start menu and to remove the Shut Down command from users and computers. The corporate standard requires that passwords be reset every 30 days and have a minimum password length of eight characters. Each password must meet complexity requirements. Northwind Traders also wants to implement password history so that employees cannot reuse the past ten passwords.

The Accounting department wants a standard workstation for all users in each part of the organization. The Accounts Receivable group has a requirement to disable the Add or Remove Programs feature from Control Panel. The Accounts Payable group has an open computing environment that requires that users sometimes log on to different computers. For this reason, Northwind Traders wants to disable the computer locking feature.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific instructions</th>
</tr>
</thead>
</table>
| 1. Create the three organizational units. | a. Log on as Nwtraders\ComputerName\User (where ComputerName is the name of the computer you are working on) with a password of P@ssw0rd if you are not already logged on.  
   b. Use Run as to open Active Directory Users and Computers. Use YourDomain\Administrator as the user name with a password of P@ssw0rd and then create the following organizational units:  
     - Accounting  
     - Accounts Receivable  
     - Accounts Payable |
| 2. Create the Accounting GPO and ensure that key settings are propagated to all users in Accounting. | a. Create a new GPO.  
   b. Link the GPO to the Accounting OU.  
   c. Configure the following Group Policy settings:  
     - Remove Run menu from Start Menu  
     - Remove and prevent access to the Shut Down command  
     - Enforced |
(continued)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Copy the Accounting GPO and rename it Accounts Receivable.</td>
<td>a. Copy the Accounting GPO.</td>
</tr>
<tr>
<td></td>
<td>b. Rename the copy Accounts Receivable.</td>
</tr>
<tr>
<td>4. Configure the Accounts Receivable GPO.</td>
<td>▪ Edit the Accounts Receivable GPO to set the policies to enable the following value:</td>
</tr>
<tr>
<td></td>
<td>• Remove Add or Remove Programs</td>
</tr>
<tr>
<td>5. Copy the Accounting GPO and rename it Accounts Payable.</td>
<td>a. Copy the Accounting GPO.</td>
</tr>
<tr>
<td></td>
<td>b. Rename the copy Accounts Payable.</td>
</tr>
<tr>
<td>6. Configure the Accounts Payable GPO.</td>
<td>▪ Edit the Accounts Payable GPO to set the policies to the following value:</td>
</tr>
<tr>
<td></td>
<td>• Disable Computer locking – the path to this option is User Configuration\Administrative Templates\System\Ctrl+Alt+Del Options.</td>
</tr>
</tbody>
</table>
## Exercise 2
### Linking GPOs

In this exercise, you will link GPOs to the appropriate organizational unit. After you link the GPOs, you can begin to enforce policies at the computer or user level.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific instructions</th>
</tr>
</thead>
</table>
| ▪ Link the Accounts Receivable and Accounts Payable GPOs to the appropriate organizational unit. | ▪ In Group Policy Management, link the following organizational units to the appropriate GPO:  
  - Accounts Receivable  
  - Accounts Payable |
Exercise 3
Verifying Group Policy Settings

In this exercise, you will use the Group Policy Modeling Wizard to verify the GPO settings that you configured in the previous exercises.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific instructions</th>
</tr>
</thead>
</table>
| 1. Use the Group Policy Modeling Wizard to verify the Accounting GPOs. | a. In Group Policy Management, open Group Policy Modeling Wizard.  
b. Accept default values for each Accounting organizational unit. |
| 2. Review the Group Policy Modeling Wizard results to verify the GPO settings. | a. View the three modeling results that you created in the previous step.  
b. Review the settings for accuracy. |