

Module 7: Implementing Group Policy

Contents

Overview	1
Introduction to Group Policy	2
Group Policy Structure	3
Working with Group Policy Objects	9
How Group Policy Settings Are Applied in Active Directory	17
Modifying Group Policy Inheritance	27
Lab A: Implementing Group Policy	33
Delegating Administrative Control of Group Policy	44
Lab B: Delegating Group Policy Administration	47
Monitoring and Troubleshooting Group Policy	52
Best Practices	59
Review	60



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BackOffice, FrontPage, IntelliMirror, PowerPoint, Visual Basic, Visual Studio, Win32, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
150 Minutes

Labs:
75 Minutes

This module provides students with an introduction to Group Policy in Microsoft® Windows® 2000 and the general knowledge and skills to implement Group Policy settings. Students will learn about the structure of Group Policy, and how to create and link Group Policy objects (GPOs). This module also explains how Group Policy settings are applied to Active Directory® directory service, and how to delegate control of GPOs. Students will also learn about Group Policy inheritance, and monitoring and troubleshooting Group Policy.

At the end of this module, students will be able to:

- Identify how Group Policy simplifies administering a Windows 2000 network.
- Identify the structure of Group Policy in a Windows 2000 network.
- Identify the options provided by Windows 2000 for creating Group Policy objects and managing them.
- Describe how Group Policy is applied in Active Directory.
- Modify Group Policy inheritance.
- Delegate administrative control of Group Policy objects.
- Monitor and troubleshoot Group Policy.
- Apply best practices for implementing Group Policy.

In the two hands-on labs in this module, students will have a chance to implement Group Policy. In the first lab, students will create and link GPOs and work with Group Policy inheritance. In the second lab, students will delegate administrative control of a GPO.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2154A_07.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read the white paper, *Introduction to Windows 2000 Group Policy*, on the Student Materials compact disc.
- Read the white paper, *Using Group Policy Scenarios*, on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- Introduction to Group Policy

In this topic, you will introduce Group Policy and provide a high-level overview of how Group Policy works. Mention the tasks that an administrator can perform with Group Policy. Emphasize that by using Group Policy, an administrator can configure settings once, and Windows 2000 continually applies those settings to multiple users and computers.

- Group Policy Structure

In this topic, you will explain the structure of Group Policy in a network. First, explain the different types of Group Policy settings. Next, present information on GPOs. Emphasize that a GPO consists of a Group Policy container (GPC) and a Group Policy template (GPT). Then mention that there are Group Policy settings for computers and users, and present information on the linking of GPOs to Active Directory containers. Emphasize that settings in the GPO affect computers and users in the containers to which the GPO is linked.

- Working with Group Policy Objects

In this topic, you will explain how to create, link, and manage GPOs. Demonstrate the process of creating linked and unlinked GPOs. Also, explain how to link an existing GPO, and demonstrate the process. Finally, explain the methods and options available for selecting a domain controller for managing GPOs.

- How Group Policy Settings Are Applied in Active Directory

In this topic, you will explain how Group Policy is applied in Active Directory. First, explain the order in which Windows 2000 processes Group Policy settings. Emphasize that Windows 2000 processes computer settings before user settings. Then, present information on Group Policy inheritance. Emphasize that the order in which Group Policy objects are applied is sites, domains, and then organizational units (OUs). Next, explain how Group Policy settings are processed and how the processing of Group Policy is controlled. Describe how Group Policy determines a slow link and explain how conflicts between multiple Group Policy settings are resolved. Finally, lead the class discussion on how Group Policy is applied. There are two slides. The first slide poses the question, and the second slide provides the answer. Display the second slide after students have provided their answers.

- Modifying Group Policy Inheritance

In this topic, you will explain how to modify Group Policy inheritance. First, present information on how to block the inheritance of Group Policy settings from parent containers. Demonstrate the process. Emphasize that a block cannot stop a No Override setting. Then, present information about the No Override option and demonstrate how to force Group Policy settings. Next, present information on filtering the Group Policy settings by using Group Policy permissions. Finally, lead the class discussion on how Group Policy is applied. The first slide poses the question, and the second slide provides the answer. Display the second slide after students have provided their answers.

- Lab A: Implementing Group Policy

Prepare students for the lab in which they will create and link GPOs and modify Group Policy inheritance. Students will work alone. Make sure that they run the command file for the lab. After students have completed the lab, ask them whether they have any questions.

- Delegating Administrative Control of Group Policy

In this topic, you will explain how to delegate administrative control of a GPO. Emphasize that an administrator delegates control of a GPO only if the user who needs control of the GPO settings does not have administrative privileges for the container to which the GPO is linked.

- Lab B: Delegating Group Policy Administration

Prepare students for the lab in which they will delegate control of GPOs. Students will work alone. After students have completed the lab, ask them whether they have any questions.

- Monitoring and Troubleshooting Group Policy

In this topic, you will explain how to monitor and troubleshoot Group Policy. First, explain the monitoring of Group Policy by diagnostic logging and verbose logging. Next, present information about the various tools provided by the Windows 2000 Support Tools package and the Windows 2000 Resource Kit for troubleshooting problems associated with Group Policy. Finally, identify the common problems encountered when implementing Group Policy and explain the suggested strategies for resolving the problems.

- Best Practices

Present best practices for implementing Windows 2000 Group Policy. Emphasize the reason for each best practice.

Customization Information

This section identifies the lab setup requirements for the module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Setup

The labs in this module require that the student computers be configured as domain controllers. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete Module 3, “Creating a Windows 2000 Domain,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Autodc.vbs from the C:\Moc\Win2154A\Labfiles\Custom\Autodc folder.
- Run Dcpromo.exe on the student computers using the following parameters:
 - A domain controller for a new domain.
 - A new domain tree.
 - A new forest of domain trees.
 - Full DNS domain name, which is *computerdom.nwtraders.msft* (where *computer* is the assigned computer name).
 - NetBIOS domain name, which is *COMPUTERDOM*.
 - Default location for the database, log files, and SYSVOL.
 - Permission compatible only with Windows 2000–based servers.
 - Directory Services Restore Mode Administrator Password, which is **password**.

Note Before you use Module 3, “Creating a Windows 2000 Domain,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*, you must successfully complete Module 2, “Implementing DNS to Support Active Directory,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about using Group Policy to manage desktop environments in a Windows 2000 network.

- Introduction to Group Policy
- Group Policy Structure
- Working with Group Policy Objects
- How Group Policy Settings Are Applied in Active Directory
- Modifying Group Policy Inheritance
- Delegating Administrative Control of Group Policy
- Monitoring and Troubleshooting Group Policy
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly present the course objectives. Do not go into details in this topic.

Group Policy in Microsoft® Windows® 2000 provides you with greater 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 Windows 2000 to continually enforce the Group Policy settings that you defined. You can apply Group Policy settings across a network or you can apply Group Policy that pertains only to specific groups of users and computers.

Lost productivity is frequently attributed to user error. By using Group Policy to reduce the complexity of user environments and remove the possibility of users incorrectly configuring these environments, productivity increases, and the network requires less technical support. Consequently, you lower your total cost of ownership (TCO).

At the end of this module, you will be able to:

- Identify how Group Policy simplifies administering a Windows 2000 network.
- Identify the structure of Group Policy in a Windows 2000 network.
- Identify the options provided by Windows 2000 for creating Group Policy objects and managing them.
- Describe how Group Policy is applied in Active Directory® directory service.
- Modify Group Policy inheritance.
- Delegate administrative control of Group Policy objects.
- Monitor and troubleshoot Group Policy.
- Apply best practices for implementing Group Policy.

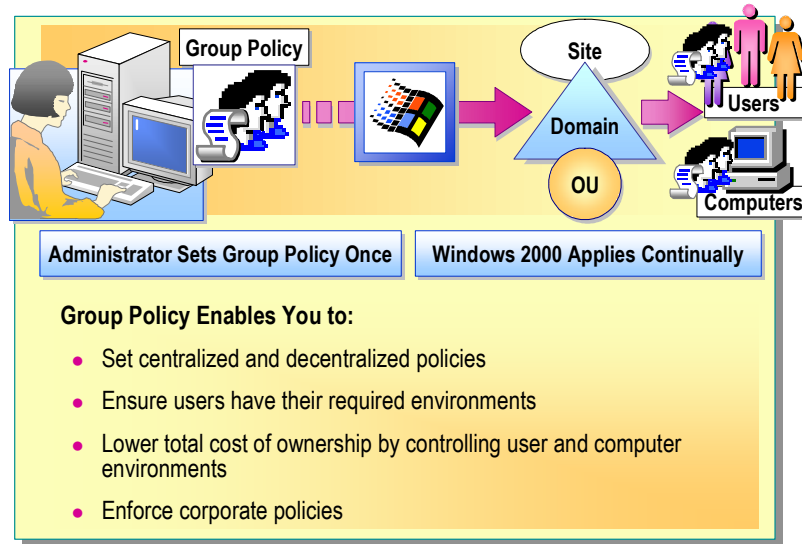
Introduction to Group Policy

Topic Objective

To introduce Group Policy and present the advantages of using Group Policy when administering a Windows 2000 network.

Lead-in

Group Policy provides you with tremendous capabilities to administer your network.



*****ILLEGAL FOR NON-TRAINER USE*****

After defining what Group Policy can do, briefly discuss the bullets on the slide.

Key Points

Administrators can use Group Policy to configure settings once and have Windows 2000 continually apply those settings.

You can associate Group Policy with specific Active Directory containers (sites, domains, and OUs).

Group Policy is the technology that allows you to define user desktop environments once, with user and computer settings, and then rely on Windows 2000 to continually enforce throughout the network the Group Policy that you defined. You can associate Group Policy settings with the following Active Directory containers, sites, domains, and organizational units (OUs). Group Policy then affects all users and computers in those containers.

By using Group Policy, you can:

- Centralize policies by setting Group Policy for an entire organization at the site or domain level, or decentralize Group Policy settings by setting Group Policy for each department at an OU level.
- Ensure that users have the user environments that they need to perform their jobs. You can make sure users have Group Policy settings that control the application and system configuration settings in the registry, scripts to modify the computer and user environments, automated software installations, and security settings for local computers, domains, and networks. You can also control where users' data folders are stored.
- 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. For example, by using Group Policy, you can prevent users from making changes to system configurations that can make a computer inoperable, or you can prevent them from installing applications that they do not require.
- Enforce a corporation's policies, including business rules, goals, and security needs. For example, you can ensure that security requirements for all users match the security required by the corporation, or that all users have a particular set of applications installed.

Note Group Policy applies only to Windows 2000 and not earlier versions of the Windows operating system family.

◆ Group Policy Structure

Topic Objective

To introduce how Group Policy is structured in Windows 2000.

Lead-in

You need to understand the structure of Group Policy to apply it efficiently and correctly.

- Types of Group Policy Settings
- Group Policy Objects
- Group Policy Settings for Computers and Users
- Group Policy Objects and Active Directory Containers

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly mention the Group Policy structure topics that are covered here. Do not go into details in this topic.

The structure of Group Policy provides flexibility in managing users and computers. The detailed settings contained in a Group Policy object (GPO) allow you to control specific user and computer configurations. You can associate GPOs with specific Active Directory containers—sites, domains, or OUs.

Types of Group Policy Settings

Topic Objective

To describe the types of Group Policy settings that an administrator can configure.

Lead-in

To set up Group Policy, you must configure the Group Policy settings that you want to apply. Windows 2000 organizes these settings into different types to make this easier.

Types of Group Policy Settings	
Administrative Templates	Registry-based Group Policy settings
Security	Settings for local, domain, and network security
Software Installation	Settings for central management of software installation
Scripts	Startup, shutdown, logon, and logoff scripts
Remote Installation Services	Settings that control the options available to users when running the Client Installation wizard used by RIS
Internet Explorer Maintenance	Settings to administer and customize Microsoft Internet Explorer on Windows 2000–based computers
Folder Redirection	Settings for storing of users' folders on a network server

*****ILLEGAL FOR NON-TRAINER USE*****

Show the different Group Policy settings to students by opening Group Policy and expanding **Computer Configuration** or **User Configuration**.

Tell students that they should review the settings in detail when planning their Group Policy strategies.

Mention to students that there are a large number of administrative template settings.

Key Point

Because of the different types of Group Policy settings, administrators have flexibility in how they use Group Policy.

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

- *Administrative templates.* Registry-based settings for configuring application settings and user desktop environments. These settings include the operating system components and applications to which users can gain access, the degree of access to Control Panel options, and control of users' offline files.
- *Security.* Settings for configuring local computer, domain, and network security settings. These settings include controlling user access to the network, setting up account and audit policies, and controlling user rights. For example, you can set the maximum number of failed logon attempts that a user account can have before it is locked out.
- *Software installation.* Settings for centralizing the management of software installations, updates, and removals. You can cause applications to automatically install on client computers, to be automatically upgraded, or to be automatically removed. You can also publish applications so that they appear in Add/Remove Programs in Control Panel, which provides users with a central location to obtain applications for installation.
- *Scripts.* Settings for specifying when Windows 2000 runs specific scripts. You can specify scripts to run when a computer starts and shuts down, and when a user logs on and logs off. You can specify scripts to perform batch operations, control multiple scripts, and determine the order in which they run.

-
- *Remote installation services.* Settings that control the options available to users when running the Client Installation wizard used by Remote Installation Services (RIS).
 - *Internet Explorer maintenance.* Settings to administer and customize Microsoft Internet Explorer on Windows 2000–based computers.
 - *Folder redirection.* Settings for storing specific user profile folders on a network server. The settings create a link in the profile to the network shared folder, but the folders appear locally. The user can gain access to the folder on any computer on the network. For example, you can redirect a user's My Documents folder to a network shared folder.

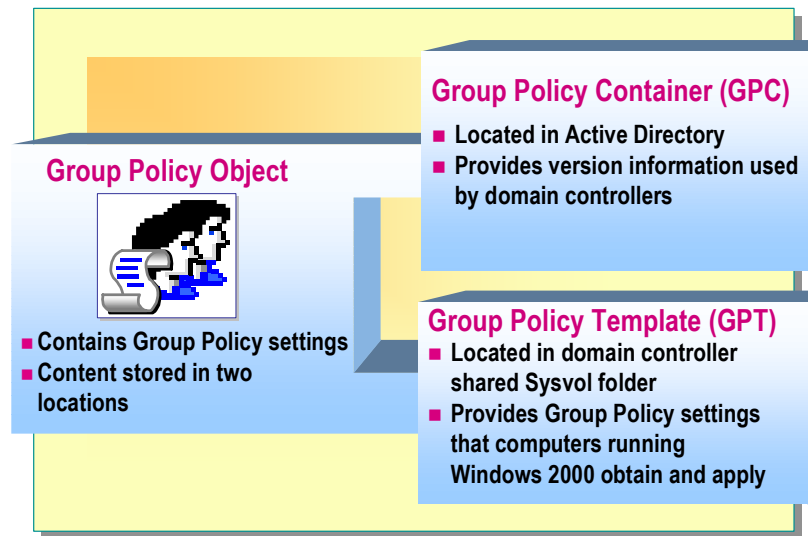
Group Policy Objects

Topic Objective

To explain the GPO and its components.

Lead-in

The mechanism for implementing Group Policy settings is the Group Policy object. It contains the settings that you configure.



*****ILLEGAL FOR NON-TRAINER USE*****

If students ask about the globally unique identifier (GUID), mention that it is a unique 128-bit number that a domain controller assigns to an object when it is created. The GUID is stored as an attribute of the object and is used to identify the object in the domain, domain tree, and forest. Users cannot change or remove the GUID.

Delivery Tip

Open Active Directory Users and Computers and show students where the GPC is stored. Then open the `systemroot\SYSVOL\sysvol` folder in Windows Explorer and show students where a GPT is stored.

Key Points

The GPO is the mechanism for implementing Group Policy. Its content is stored in the GPC and the GPT. The GPC is stored in Active Directory and provides the version information. The GPT contains the settings and is stored in the SYSVOL folder on domain controllers.

You can implement Group Policy by using the Group Policy object (GPO). Windows 2000 applies the Group Policy settings contained in the GPO to the user and computer objects in the site, domain, or OU with which the GPO is associated.

The content of a GPO is stored in two different locations. Those locations are:

- *The Group Policy container (GPC)*. The GPC is an Active Directory object that contains GPO attributes and version information. Because the GPC is in Active Directory, computers can access it to locate Group Policy templates, and domain controllers can access it to obtain version information.

A domain controller uses the version information to verify that it has the most recent version of the GPO. If the domain controller does not have the most recent version, replication occurs with the domain controller that has the latest version of the GPO.

Note To view the GPC in Active Directory, enable Advanced Features in Active Directory Users and Computers, expand the domain, expand the System container, and then expand the Policies container.

- *The Group Policy template (GPT)*. The GPT is a folder hierarchy in the shared sysvol folder on domain controllers. When you create a GPO, Windows 2000 creates the corresponding GPT folder hierarchy. The GPT 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 used to identify the GPO in the GPC. The path to the GPT on a domain controller is `systemroot\SYSVOL\sysvol`.

Group Policy Settings for Computers and Users

Topic Objective

To introduce the Group Policy settings for computers and users.

Lead-in

You can enforce Group Policy settings for computers and users on the network by using the Computer Configuration and User Configuration nodes in Group Policy, respectively.

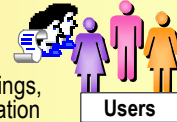
■ Group Policy Settings for Computers:

- Specify operating system behavior, desktop behavior, security settings, computer startup and shutdown scripts, computer-assigned application options, and application settings
- Apply when the operating system initializes and during the periodic refresh cycle



■ Group Policy Settings for Users:

- Specify operating system behavior, desktop settings, security settings, assigned and published application options, application settings, folder redirection options, and user logon and logoff scripts
- Apply when users log on to the computer and during the periodic refresh cycle



*****ILLEGAL FOR NON-TRAINER USE*****

You can enforce Group Policy settings for computers and users on the network by using the Computer Configuration and User Configuration nodes in Group Policy, respectively.

Group Policy Settings for Computers

Group Policy settings for computers specify operating system behavior, desktop behavior, security settings, computer startup and shutdown scripts, computer-assigned application options, and application settings. Computer-related Group Policy is applied when the operating system initializes and during the periodic refresh cycle. In general, computer Group Policy takes precedence over conflicting user Group Policy.

Group Policy Settings for Users

Group Policy settings for users specify operating system behavior, desktop settings, security settings, assigned and published application options, application settings, folder redirection options, and user logon and logoff scripts. User-related Group Policy is applied when users log on to the computer and during the periodic refresh cycle.

Note For more information about Group Policy settings for computers and users, see *Introduction to Windows 2000 Group Policy* under **Additional Reading** on the Web page on the Student Materials compact disc.

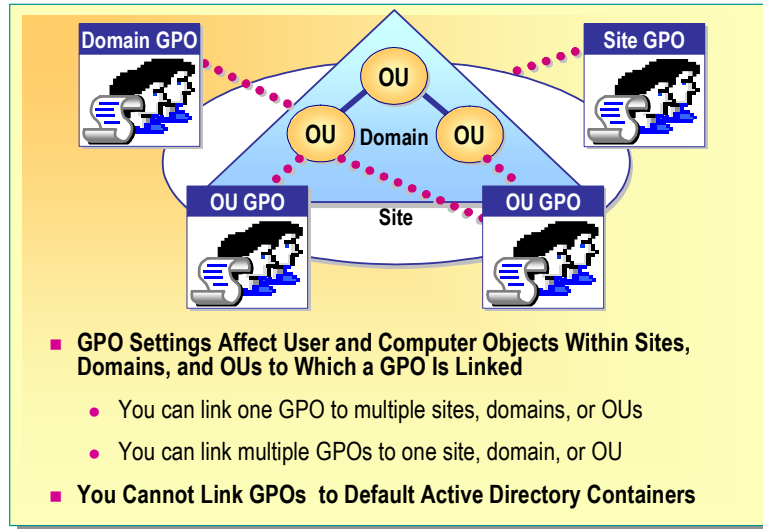
Group Policy Objects and Active Directory Containers

Topic Objective

To show how GPOs are linked in Windows 2000.

Lead-in

GPOs are linked to or associated with sites, domains, and OUs. After you link a GPO to a site, domain, or OU, the settings in that GPO apply to the users and computers in the site, domain, or OU.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

GPOs are linked to sites, domains, and OUs. This linking makes the GPO settings affect computers and users in the sites, domains, and OUs to which the GPO is linked.

An administrator can link one GPO to multiple sites, domains, or OUs, and multiple GPOs to one site, domain, or OU.

An administrator cannot link GPOs to the default Active Directory containers—Computers, Users, and Builtin—because they are not OUs.

GPOs are associated with, or linked to, sites, domains, and OUs to allow you to set centralized policies that affect the entire organization and decentralized policies that are localized by department. The linking of a GPO to a site, domain, or OU causes the Group Policy settings to affect user and computer objects in that site, domain, or OU. The information that describes which GPOs are linked to an Active Directory container is stored in two attributes of that container—gPLink and gPOptions. The gPLink attribute contains the prioritized list of GPOs linked to a container and the gPOptions attribute contains the container setting that prevents the inheritance of any GPO.

The ability to link existing GPOs provides flexibility when implementing Group Policy settings. You can link GPOs in the following ways:

- Link one GPO to multiple sites, domains, or OUs in your network. This provides you with the ability to configure Group Policy settings that apply to users and computers in different sites, domains, or OUs. For example, you can create a GPO that runs a logon script and then link it to OUs that have users for whom you want the script to run.
- Link multiple GPOs to one site, domain, or OU. Rather than have all of the types of Group Policy settings for a site, domain, or OU in one GPO, you can create several GPOs for different types of Group Policy settings and then link them to the appropriate sites, domains, or OUs. For example, you can link a GPO that contains network security settings, and another GPO that contains software installation, to the same OU. These multiple GPOs can also be linked to other OUs.

Important You cannot link GPOs to the default Active Directory containers—Users, Computers, and Builtin. Although these containers exist within Active Directory, they are not OUs.

◆ Working with Group Policy Objects

Topic Objective

To introduce the options available for creating and managing Group Policy objects.

Lead-in

Windows 2000 provides you with various options to create and manage Group Policy objects.

- **Creating Linked Group Policy Objects**
- **Creating Unlinked Group Policy Objects**
- **Linking an Existing Group Policy Object**
- **Specifying a Domain Controller for Managing Group Policy Objects**

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly present the topics for this section.

Windows 2000 provides you with various options to create a new Group Policy object (GPO) if any of the existing GPOs do not have the settings that you want. When creating a GPO, you can either create a linked GPO or an unlinked GPO. However, if the Group Policy settings that you want to apply to computers and users in an OU are in an existing GPO, you can link the GPO to the container.

When you create a new GPO, or open Group Policy to edit an existing GPO, the default behavior is to manage GPOs on the domain controller that holds the PDC emulator role.

Creating Linked Group Policy Objects

Topic Objective

To explain how to create a new GPO.

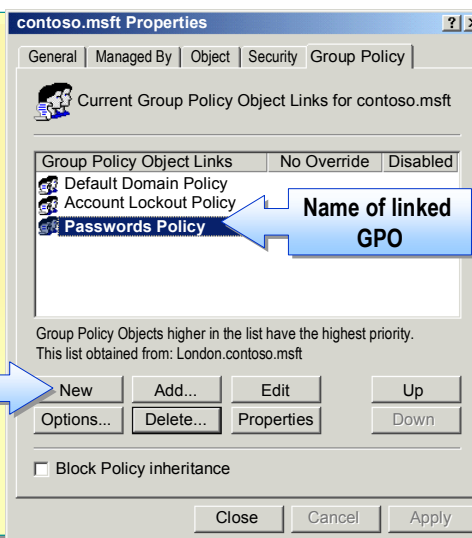
Lead-in

Create a new GPO when the existing ones do not have the settings that you want. Otherwise, link an existing GPO to the site, domain, or OU for which you want to set a Group Policy.

To Apply Group Policy to a Container, Create a GPO Linked to the Container:

- Create GPOs linked to domains and OUs by using Active Directory Users and Computers
- Create GPOs linked to sites by using Active Directory Sites and Services

To create a GPO



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to create a GPO for an OU by using Active Directory Users and Computers.

Key Point

When an administrator creates a GPO, there are no settings configured.

When you create a GPO, it is linked to the container for which you create it. However, there is no Group Policy setting defined in a new GPO.

Creating GPOs Linked to Domains and OUs

You create a GPO for domains and OUs by using Active Directory Users and Computers. To create a new GPO for a domain or OU, perform the following steps:

1. Open Active Directory Users and Computers.
2. Right-click the domain or OU for which you want to create a GPO, and then click **Properties**.
3. On the **Group Policy** tab, click **New**, type a name for the new GPO, and then press ENTER. The GPO that you create appears in the list of GPOs associated with the OU or domain on the **Group Policy** tab for the OU or domain.

Creating GPOs Linked to Sites

Creating a GPO for a site is different from creating a GPO for a domain or OU because you use Active Directory Sites and Services to administer sites. To create a new GPO for a site, perform the following steps:

1. Open Active Directory Sites and Services.
2. Right-click the site for which you want to create a GPO, and then click **Properties**.
3. On the **Group Policy** tab, click **New**, type a name for the new GPO, and then press ENTER. The GPO that you create appears in the list of GPOs associated with the site on the **Group Policy** tab for the site.

Note You must be a member of the Enterprise Admins group to create GPOs linked to sites.

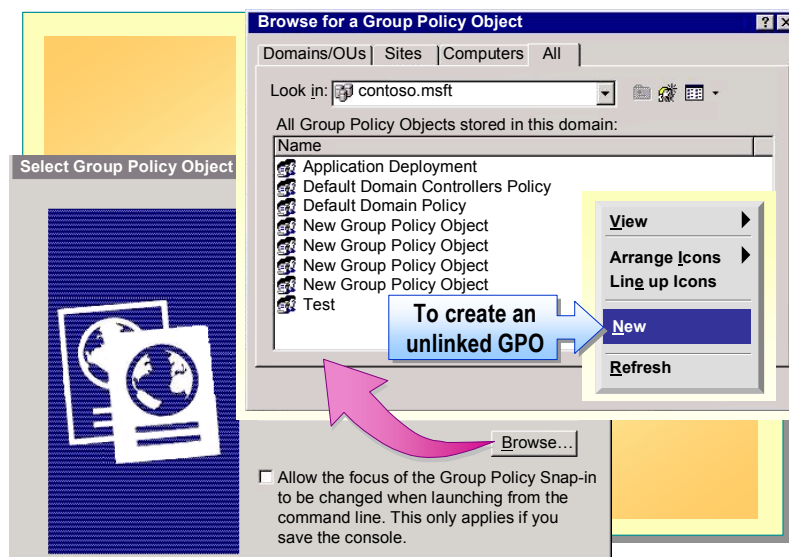
Creating Unlinked Group Policy Objects

Topic Objective

To explain how to create a new unlinked Group Policy object.

Lead-in

You can create new GPOs that are not linked to sites, domains, or OUs.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the functions of the buttons on the dialog box displayed on the slide.

Delivery Tip

Demonstrate adding the Group Policy snap-in to an MMC console to open the **Select Group Policy Object** dialog box. Create a new unlinked GPO.

When you create a GPO linked to a site, domain, or OU, you actually perform two separate operations: creating a new GPO, and then linking it to the site, domain, or OU. To link a GPO to a site, domain, or OU, you must have read and write permissions on the `gPLink` and `gPOptions` attributes of the container to which the GPO is being linked. By default, only members of the Domain Admins and Enterprise Admins groups have the necessary permissions to link GPOs to domains and OUs, whereas only members of the Enterprise Admins group have the permissions to link GPOs to sites. Members of the Group Policy Creator Owners group can create GPOs, but cannot link them. You can create an unlinked GPO by adding a Group Policy snap-in to the MMC console.

To create an unlinked GPO, perform the following steps:

1. Run `Mmc.exe` and add the Group Policy snap-in.
2. In the **Select Group Policy Object** dialog box, click **Browse**.
3. In the **Browse for a Group Policy Object** dialog box, on the **All** tab, right-click anywhere in the **All Group Policy Objects stored in this domain** list, and then click **New**.
4. Type a name for the new GPO, and then click **OK** to close the **Browse for a Group Policy Object** dialog box.
5. If you want to edit the new GPO, in the **Select Group Policy Object** dialog box, click **Finish**, otherwise click **Cancel**.

Unlinked GPOs may be created in big organizations where one group is responsible for creating GPOs while another group links the GPOs to the required site, domain, or OU.

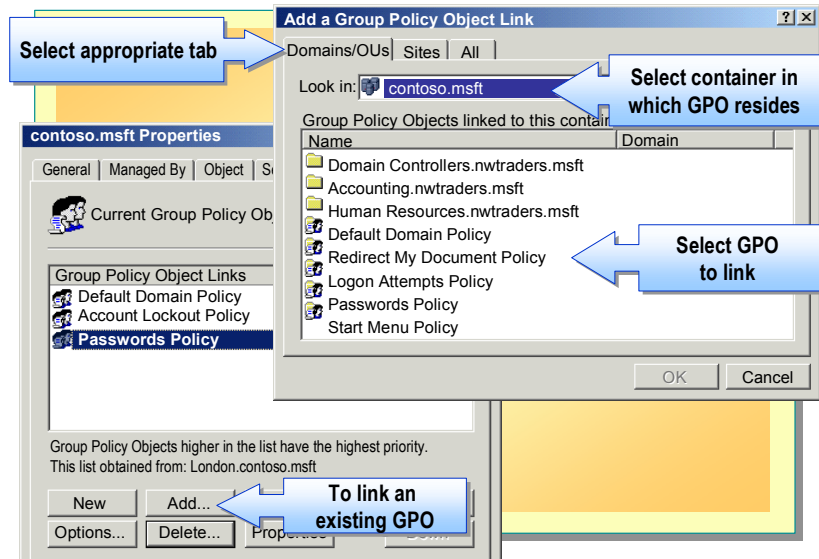
Linking an Existing Group Policy Object

Topic Objective

To explain how to link an existing GPO to a site, domain, or OU.

Lead-in

If the Group Policy settings that you want to apply to computers and users in an OU are in an existing GPO, link the GPO to the container.



*****ILLEGAL FOR NON-TRAINER USE*****

Remind students that when they link a GPO to a container, the settings in the GPO affect all of the computers and users in that container.

Remind students that they can link one GPO to multiple containers and multiple GPOs to one container.

Delivery Tip

Demonstrate linking the GPO that you created in the previous topic to another OU in the same domain by using Active Directory Users and Computers.

Mention that the **Group Policy Objects linked to this container** list contains all of the GPOs that exist for the container selected in the **Look in** list.

You can apply existing Group Policy settings to additional Active Directory containers by linking the GPO that contains the required settings to those containers. To link a GPO to a site, domain or OU, you must have read and write permissions on the gPLink and gPOptions attributes of that site, domain, or OU.

Linking an Existing GPO to Domains and OUs

You link an existing GPO to domains and OUs by using Active Directory Users and Computers.

To link a GPO to a domain or OU, perform the following steps:

1. Open Active Directory Users and Computers.
2. Right-click the domain or OU that you want to link to an existing GPO, and then click **Properties**.
3. On the **Group Policy** tab, click **Add**.
4. Click the **Domain/OU's**, **Sites**, or **All** tab, depending on the location to which the GPO that you want to link is presently linked.
5. In the **Look in** list, click the domain that contains the GPO that you want.
6. In the **Group Policy Objects linked to this container** list, click the GPO to which you want to link, and then click **OK**.

The **Group Policy Objects linked to this container** list contains all of the GPOs that exist in the domain.

Linking an Existing GPO to a Site

You link an existing GPO to a site by using Active Directory Sites and Services.

To link an existing GPO to a site, perform the following steps:

1. Open Active Directory Sites and Services.
2. Right-click the site that you want to link to an existing GPO, and then click **Properties**.
3. On the **Group Policy** tab, click **Add**.
4. Click the **Domain/OUs**, **Sites**, or **All** tab, depending on the location to which the GPOs that you want to link are presently linked.
5. In the **Look in** list, click the domain that contains the GPO that you want.
6. In the **Group Policy Objects linked to this container** list, click the GPO to which you want to link, and then click **OK**.

The **Group Policy Objects linked to this container** list contains all of the GPOs that exist in the site.

Caution Although you have the ability to link existing GPOs to sites, you need to think carefully about using this ability. If you link a GPO to a site, anyone who has read and write permissions to that GPO can make changes to it, and because the GPO is linked to the site, those changes are processed throughout the entire site. Consider always creating new GPOs for sites, rather than linking existing ones.

Note By default, the GPO for a site is created in the root domain of the forest. This could affect network traffic patterns with cross-domain traffic.

Specifying a Domain Controller for Managing Group Policy Objects

Topic Objective

To explain how a domain controller can be specified for managing GPOs.

Lead-in

You can manage GPOs to avoid data loss if two administrators were working on changes to the same GPO on different domain controllers within the same replication cycle.

■ When You Create a New GPO or Edit an Existing GPO, by Default, the Domain Controller That Holds the PDC Emulator Role Performs the Operation



■ The Options Available to Specify a Domain Controller for Managing GPOs Include:

- The one with the Operations Master token for the PDC emulator
- The one used by the Active Directory snap-ins
- Use any available domain controller

■ To Specify a Domain Controller for Managing Group Policy Objects:

- Use the DC Options command on the View menu in the Group Policy snap-in
- Enable a Group Policy setting that specifies which domain controller should be used

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to specify a domain controller for managing GPOs.

Key Point

Data loss could occur if two administrators were working on changes to the same GPO on different domain controllers within the same replication cycle.

When you create a new GPO or open Group Policy to edit an existing GPO, by default, the operation is performed on the domain controller that holds one of the operations master roles, specifically the primary domain controller (PDC) emulator role. Understanding which domain controller is used while creating or editing GPOs helps you resolve problems associated with creating or editing GPOs.

This default behavior forces the Group Policy snap-in to use the same domain controller regardless of the computer from which it is being run. Data loss could occur if two administrators work on changes to the same GPO on different domain controllers within the same replication cycle. In Windows 2000, Group Policy writes data to the GPO for each change. If two administrators edit a GPO on different domain controllers, it increases the possibility of changes being overwritten by replication. It is strongly recommended that the number of administrators be limited, that Group Policy use the PDC Emulator role, and that the administrator be aware of other administrators that may be editing the same GPO.

Options for Selecting a Domain Controller

You can specify a domain controller for managing GPOs by selecting any of the following three options:

- *The one with the Operations Master token for the PDC emulator.* This is the default and preferred option. Using this option helps ensure that no data loss occurs.
- *The one used by the Active Directory Snap-ins.* Uses the domain controller that the Active Directory management snap-in tools are currently using. Each of these snap-ins includes an option for changing which domain controller is the focus of its current operation. When this option is selected, the Group Policy snap-in uses the same domain controller.
- *Use any available domain controller.* The third, and least desirable option in most cases, allows the Group Policy snap-in to choose any available domain controller. When this option is used, it is likely that a domain controller in the local site will be selected.

Methods for Specifying a Domain Controller

To specify a domain controller for managing GPOs:

- Use the **DC Options** command on the Group Policy snap-in **View** menu. Clicking this command displays a dialog box with the three options for selecting a domain controller.
- Enable a Group Policy setting that specifies which domain controller option should be used. If that option is not available, an error message will be displayed. In such cases, the **DC Options** command will be disabled because a Group Policy is in place that overrides any setting that the user picks. The DC options Group Policy setting is located in the Administrative Templates node for User Configuration in the System\Group Policy sub-container. The available DC options are the same as the preference settings listed in the Options for Selecting a Domain Controller section. This functionality is useful in some corporate scenarios. For example, if you are an administrator in Japan and the PDC Emulator is in New York, you can implement a Group Policy to ensure that all changes are made locally.

◆ How Group Policy Settings Are Applied in Active Directory

Topic Objective

To introduce how Group Policy settings are applied in Active Directory.

Lead-in

The manner in which Windows 2000 processes GPOs affects the resultant Group Policy settings that apply to computers and users.

- Group Policy Inheritance
- How Group Policy Settings Are Processed
- Controlling the Processing of Group Policy
- Group Policy and Slow Network Connections (Links)
- Resolving Conflicts Between Group Policy Settings
- Class Discussion: How Group Policy Is Applied

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly mention the topics that this section covers.

Define resultant Group Policy settings for students.

How Group Policy is applied in Active Directory determines the resultant Group Policy settings that are applied. *Resultant Group Policy settings* are the settings that take effect when there are multiple GPOs and multiple settings that could affect computer and user objects. To obtain the results that you want, you need to be aware of how resultant Group Policy settings are determined; otherwise you may configure settings that are never applied.

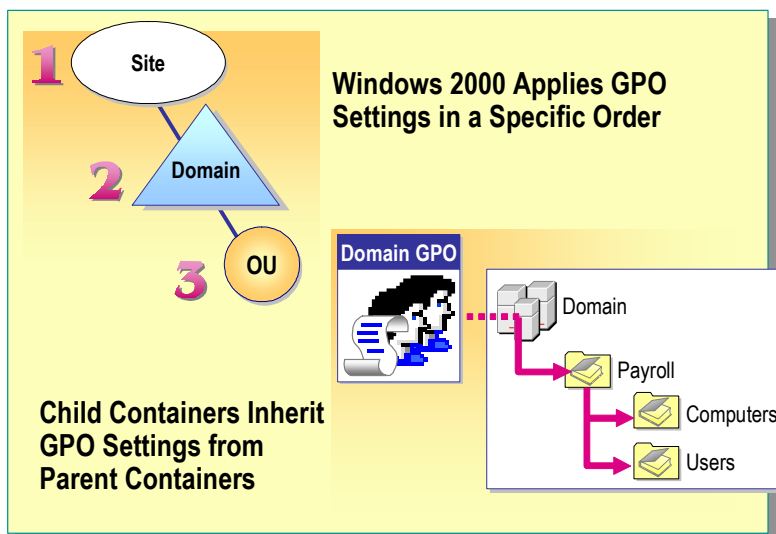
Group Policy Inheritance

Topic Objective

To show the order in which Windows 2000 applies Group Policy and how Group Policy settings are inherited in Active Directory.

Lead-in

Group Policy inheritance includes the order in which Windows 2000 processes GPOs in Active Directory, as well as the inheritance of Group Policy settings in a GPO linked to parent containers.



*****ILLEGAL FOR NON-TRAINER USE*****

When discussing the order of application, mention that an OU can be a parent to a child OU.

Key Points

The order in which Windows 2000 applies GPOs is based on the Active Directory containers to which they are linked.

The GPOs of the parent container are processed and applied to a child container before the child container's own GPOs are applied.

The Group Policy settings of the OU of which a user or computer is a member are the final Group Policy settings applied to that user or computer.

Group Policy inheritance is the order in which Windows 2000 applies GPOs. The order in which Group Policy is applied and how Group Policy settings are inherited ultimately determines which settings affect users and computers.

Order of Application

The order in which Windows 2000 applies GPOs is based on the Active Directory container to which the GPOs are linked. The GPOs are applied first to the site, which is the furthest away from the computer or user, and then applied to domains, and then to OUs. Thus, the Group Policy settings of the OU of which a user or computer is a member are the final Group Policy settings that are applied.

Flow of Inheritance

By default, GPOs are inherited. Inheritance flows down the Active Directory tree from site, to domain, and then to OU. The child container inherits the GPO from the parent container. This means that the child container could have a multitude of Group Policy settings applied to its users and computers without having a GPO linked to it.

If a child container does have GPOs linked to it, the Group Policy settings from parent containers higher in the Active Directory tree are applied to its users and computers first. Then the child container's own Group Policy settings are applied.

Note There is no hierarchy of domains as there is for OUs, such as parent OU, child OU, and so on.

GPOs Linked to Sites

Because sites represent the physical network, and domains and OUs represent the logical network, it is important to understand how GPOs linked to sites are applied. Any given site may contain computers from one or more domains. If a site contains computers from more than one domain, the Group Policy settings defined in the GPO linked to that site will apply to all computers in that site and all users who log on to computers in that site, regardless of the domain in which the computer or user accounts exist.

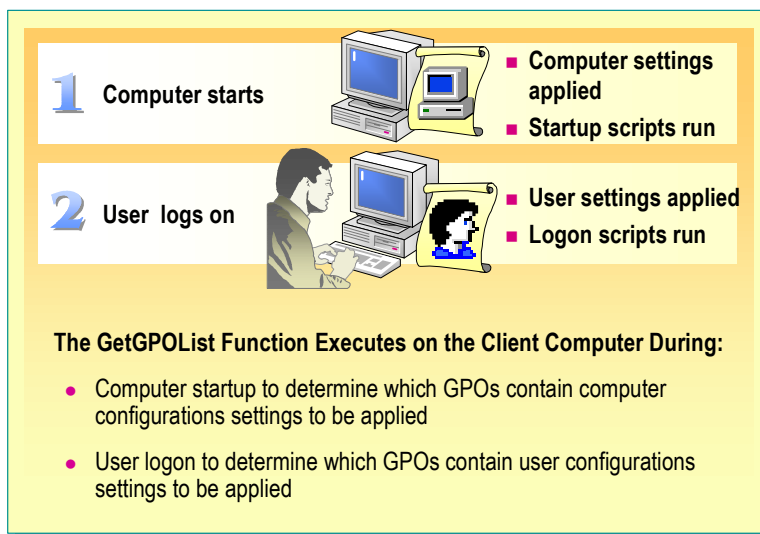
How Group Policy Settings Are Processed

Topic Objective

To explain how Windows 2000 processes Group Policy settings.

Lead-in

Windows 2000 processes Group Policy settings in a specific order, and that order affects the resultant Group Policy settings that are applied.



*****ILLEGAL FOR NON-TRAINER USE*****

Remind students how scripts are assigned in the user profile.

Key Points

When a computer is started and a user logs on, Windows 2000 processes computer settings first and then user settings.

Because domain controllers refresh Group Policy every five minutes, critical Group Policy settings take effect on critical servers quickly.

Windows 2000 processes the Group Policy settings in a specific order and at established intervals. By understanding the order in which Windows 2000 processes Group Policy settings, you can avoid overriding Group Policy settings. When a computer is started and a user logs on, Windows 2000 processes computer settings first and then user settings. When Windows 2000 processes computer settings, the startup scripts run. Similarly, the logon scripts run when Windows 2000 processes user settings.

Determining Which GPOs to Process

The list of GPOs that need to be processed is determined by a Win32® function, GetGPOList. This function is executed on the client computer during computer start up to determine which GPOs contain computer configuration settings that should be applied, and it is executed again during the user log on process to determine which GPOs contain user configuration settings that should be applied.

Processing Group Policy

The processing of Group Policy occurs at the client side. Group Policy is actually processed by a number of different dynamic-link libraries (DLLs) that are known as client-side extensions. Each client-side extension is responsible for processing a different type of Group Policy setting. The following table lists the client-side extensions and the type of Group Policy setting for which each is responsible:

Client-side Extension	Group Policy Settings
Userenv.dll	Registry-based settings (Administrative Templates)
Dskquota.dll	Disk Quota settings (Administrative Templates)
Fdeploy.dll	Folder Redirection settings
Gptext.dll	Script and IP Sec settings
Appmgmts.dll	Software Installation
Scecli.dll	Security and Encrypting File System Recovery Settings
Iedkcs32.dll	Internet Explorer Maintenance settings

After the list of GPOs that need to be processed is determined by the GetGPOList function, the client computer loops through the client-side extensions and determines whether each client-side extension has any data to process in the GPOs. If the client-side extension has data to be processed in the GPOs, it is executed and processes the data in the applicable GPOs. If there is no data for a particular client-side extension, it is not executed.

Controlling the Processing of Group Policy

Topic Objective

To describe how the processing of Group Policy is controlled.

Lead-in

Windows 2000 processes Group Policy settings in a specific order, and that order affects the resultant Group Policy settings that are applied.

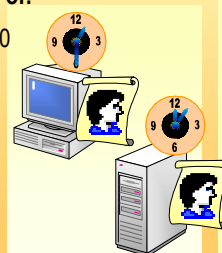
■ Synchronous and Asynchronous Processing

- By default, the processing of Group Policy is synchronous
- You can change the processing of Group Policy to asynchronous by using a Group Policy setting for both computers and users



■ Refreshing Group Policy at Established Intervals of:

- 90 minutes for computers running Windows 2000 Professional and for member servers running Windows 2000 Server
- 5 minutes for domain controllers



■ Processing Unchanged Group Policy Settings

- You can configure each client-side extension to process all applicable Group Policy settings

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

By default, the processing of Group Policy is synchronous.

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

You can control the processing of Group Policy, which can be synchronous or asynchronous. Asynchronous refers to processes that do not depend on each other's outcome, and can therefore occur on different threads simultaneously. The opposite is synchronous. Synchronous processes wait for the previous one to complete before beginning the next. For those Group Policy settings for which both types of processing are available as options, you can choose between the faster asynchronous or the safer, more predictable synchronous processing.

Synchronous and Asynchronous Processing

By default, the processing of Group Policy is synchronous. The Group Policy setting for computers is completed before the Welcome to Windows message is presented, and the Group Policy setting for users is completed before the command interpreter that is used to pass commands to the operating system is active and available for the user to interact with it.

You can change this default behavior by using a Group Policy setting for each so that processing is asynchronous. This is not recommended unless there are compelling performance reasons. To provide the most reliable operation, leave the processing as synchronous.

Refreshing Group Policy at Established Intervals

Computers running Windows 2000 refresh, or reapply, Group Policy settings at established intervals. The refresh ensures that Group Policy settings are applied to computers and users even if users never restart their computers or log off.

The following list provides the default refresh intervals:

- Computers running Windows 2000 Professional and not configured as domain controllers, and member servers running Windows 2000 Server, refresh every 90 minutes with a randomized time offset of 30 minutes. The time offset ensures that multiple computers do not contact a domain controller at the same time.
- Domain controllers refresh every five minutes. This means that critical new Group Policy settings, such as security settings, are applied after no more than five minutes.

You can change the default refresh values by modifying the administrative template settings for the user or computer configuration. Group Policy refreshing can not be scheduled to occur at a specific time.

Note The processing of software installation and folder redirection settings in a GPO occurs *only* when a computer starts or when the user logs on, rather than on a periodic basis.

Processing Unchanged Group Policy Settings

By default, each client-side extension, with the exception of the Remote Installation Service client-side extension, only processes Group Policy settings that have changed since the last time Group Policy was processed by the client-side extension. Although this default behavior provides the best performance, it may not produce the desired results. For example, if a user changes a setting that is controlled by a Group Policy setting during a session and the Group Policy setting has not been changed in the GPO, the user's change will not be reversed when Group Policy is applied again. Each client-side extension can be configured to process all applicable Group Policy settings regardless of whether they have been changed. This configuration can be accomplished with an administrative template setting.

Group Policy and Slow Network Connections (Links)

Topic Objective

To explain how Group Policy detects a slow link.

Lead-in

Group Policy has the ability to detect a slow link, and, if a slow link is detected, it sets a flag to indicate that fact to the client-side extensions.

- Group Policy Can Detect a Slow Link
- Group Policy Uses an Algorithm to Determine Whether a Link Should Be Considered Slow
- Group Policy Sets a Flag to Indicate a Slow Link to the Client-side Extensions



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Group Policy can detect a slow link.

Group Policy sets a flag to indicate a slow link to the client-side extensions.

Group Policy uses an algorithm to determine whether a link should be considered slow.

Group Policy has the ability to detect a slow link, and, if a slow link is detected, it sets a flag to indicate that fact to the client-side extensions. If this flag is set, the individual client-side extensions can determine whether to process applicable Group Policy settings. The connection speed of the link is compared with 500 kilobits per second (Kbps), or with an alternative threshold of your choice if you change from the default Group Policy setting of 500 Kbps. Group Policy uses an algorithm to determine whether a link should be considered slow. If the connection speed is less than 500 Kbps, the connection is considered slow.

The following table indicates the default settings for slow link processing:

Client-side Extension	Slow Link Processing
Registry-based settings (Administrative Templates)	On (cannot be turned off)
Internet Explorer Maintenance settings	Off
Software Installation settings	Off
Folder Redirection settings	Off
Scripts settings	Off
Security settings	On (cannot be turned off)
IP Security settings	Off
EFS Recovery settings	On
Disk Quota settings	Off

The behavior of the client-side extensions over a slow link can be modified with an administrative template setting, except for Registry-based settings and Security settings, which are always processed.

Note For more information about how Group Policy detects slow links, see Appendix B, “Determining Slow Network Connections,” on the Student Materials compact disc.

Resolving Conflicts Between Group Policy Settings

Topic Objective

To show how multiple GPOs set at different levels of Active Directory affect users and computers and how conflicts between multiple settings are resolved.

Lead-in

Resultant Group Policy settings are settings that apply unless there are conflicting settings. If there are conflicts, the last settings that are applied override by default.

■ All Group Policy Settings Apply Unless There Are Conflicts



■ The Last Setting Processed Applies

- When settings from different GPOs in the Active Directory hierarchy conflict, the child container GPO settings apply
- When settings from GPOs linked to the same container conflict, the settings for the GPO highest in the GPO list apply

■ A Computer Setting Applies When It Conflicts with a User Setting

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Show students the **Group Policy** tab for a container. Mention to students that if there are multiple GPOs, Windows 2000 processes them in order, from bottom to top.

Key Point

If there are conflicts between Group Policy settings, the last setting that was applied overrides all others, except when a user setting and a computer setting conflict. Then, in most instances, the computer setting overrides the user setting.

Group Policy is cumulative, that is, all Group Policy settings in all of the GPOs that affect a user or computer account (as determined by the GetGPOList function) are applied, unless two or more settings conflict.

The rules for determining which Group Policy settings apply when they conflict are as follows:

- Settings from a parent container GPO conflict with settings from a child container GPO. When this happens, the settings in the child container are applied last and take effect.
- Settings from different GPOs linked to the same container conflict. When this happens, the settings in the GPO at the top of the list of GPOs on the **Group Policy** tab of the **Properties** dialog box for the container are applied last and take effect. To change the order in which multiple GPOs assigned to the same container are processed, click a GPO in the list on the **Group Policy** tab, and then click **Up** or **Down** to change its position.

The one exception to the application of the most recent setting processed is when computer and user settings conflict. When this occurs, in almost all instances the computer setting overrides the user settings and applies, even though the user setting was processed last. You can verify whether the computer or user setting applies by using the **Explain** tab of the **Properties** dialog box for a setting. This is not enforced by the Group Policy infrastructure, but is rather a convention that is followed by the operating system and by applications that take advantage of Group Policy. This convention is followed unless there are specific reasons that the convention is not appropriate for a given Group Policy setting.

The exceptions to the cumulative processing of Group Policy are IP Security settings and User Rights settings. When processing IP Security or User Rights settings, the last GPO processed overwrites any previous GPOs.

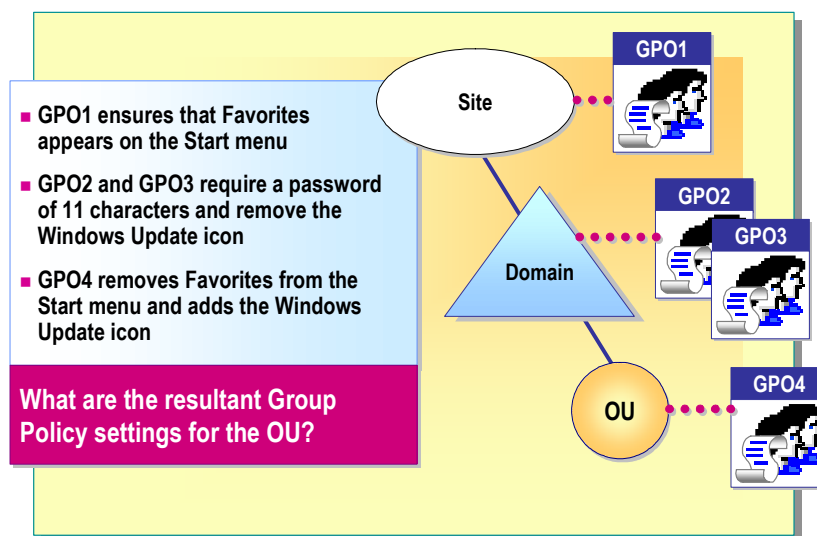
Class Discussion: How Group Policy Is Applied

Topic Objective

To check students' understanding of how Group Policy is applied.

Lead-in

This is an example of how resultant Group Policy settings are determined. Let's go through the example together and determine the resultant Group Policy settings as a class.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class.

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

On your network, you have the following GPOs linked to Active Directory containers:

GPO	Contains
GPO1	An account Group Policy setting that ensures Favorites appears on the Start menu
GPO2	An account Group Policy setting that requires a minimum of 11 characters in a password
GPO3	A Start menu setting that removes the Windows Update icon from the Start menu
GPO4	Start menu settings that ensure the Windows Update icon is on the Start menu and that remove Favorites from the Start menu

What are the resultant Group Policy settings for user objects in the OU, and why?

The resultant Group Policy settings are:

- User passwords must be at least 11 characters long.
- The Windows Update icon appears on the Start menu.
- Favorites does not appear on the Start menu.

The Group Policy setting that removes Favorites from the Start menu was processed after the Group Policy settings that ensure it is on the Start menu. The Group Policy setting ensuring that the Windows Update icon is on the Start menu was processed after the Group Policy setting that removed it from the desktop.

◆ Modifying Group Policy Inheritance

Topic Objective

To introduce the options available for modifying Group Policy inheritance.

Lead-in

Windows 2000 provides you with the ability to modify Group Policy inheritance. This allows you to fine-tune your network's Group Policy settings.

- **Enabling Block Inheritance**
- **Enabling No Override**
- **Filtering Group Policy Settings**
- **Class Discussion: Changing Group Policy Inheritance**

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly present the topics for this section.

Windows 2000 provides you with the ability to modify Group Policy inheritance and control how Group Policy settings are applied to specific computers and users. Modifying inheritance enables you to block, force, or filter the inheritance of Group Policy settings for your network, computers, and users.

Enabling Block Inheritance

Topic Objective

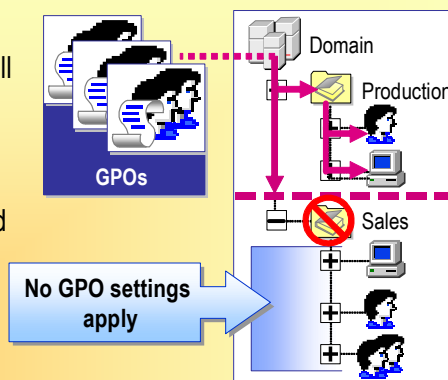
To explain blocking and how to block inheritance of Group Policy settings.

Lead-in

One way to modify Group Policy settings is to block settings that would normally be inherited from parent containers.

Block Inheritance:

- Stops inheritance of all GPOs from all parent containers
- Cannot selectively choose which GPOs are blocked
- Cannot stop No Override



*****ILLEGAL FOR NON-TRAINER USE*****

Mention that links configured with No Override cannot be blocked, and use this statement as a transition to the next topic on No Override.

Delivery Tip

Demonstrate Block Inheritance on the **Group Policy** tab for an OU.

Key Points

Block Inheritance prevents a child container from inheriting all Group Policy settings from all parent containers.

Links configured with No Override are applied despite and Block Inheritance settings.

Block Inheritance allows an Active Directory container to have unique Group Policy settings.

You can prevent a child container from inheriting any GPOs from parent containers by enabling Block Inheritance on the child container. Enabling Block Inheritance on a child container prevents the container from inheriting all Group Policy settings and not individual settings. This is useful when an Active Directory container requires unique Group Policy settings and you want to ensure that settings are not inherited. For example, you can use Block Inheritance when it is necessary that the administrator of an OU control all GPOs for that container.

To block inheritance of a GPO for a child container, perform the following steps:

1. Open the **Properties** dialog box for the domain or OU at which you want to block inheritance.
2. On the **Group Policy** tab, click **Block Policy Inheritance**.

The two limitations to blocking inheritance are as follows:

- You cannot selectively choose which GPOs are blocked. Block Inheritance affects all GPOs from all parent containers, except when the GPO is configured with the No Override option.
- Block Inheritance cannot stop the inheritance of a GPO linked to a parent container if the link is configured with the No Override option.

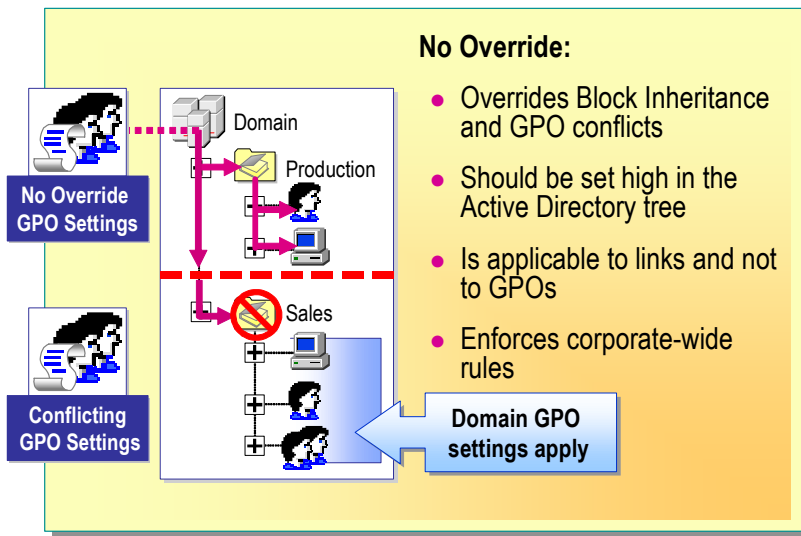
Enabling No Override

Topic Objective

To explain the No Override option and how to force the inheritance of Group Policy settings by using No Override.

Lead-in

Windows 2000 allows you to force GPOs down the Active Directory tree to ensure that their settings always apply, regardless of Block Inheritance settings and the normal conflict resolution methods.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate enabling No Override by clicking **No Override** in the **Default Domain Policy Options** dialog box.

Key Points

When you enable No Override, nothing can block it lower in the Active Directory tree.

Include only critical settings in GPOs when using No Override, because they take effect regardless of how other GPOs are set up. You want to be sure that you are not overriding important GPOs.

Enabling No Override means that all Group Policy settings contained in the GPO whose link is configured with No Override apply, even if they conflict with settings processed after them, or if blocking occurs lower in the Active Directory tree. You should set to No Override only the links to GPOs that represent critical corporate-wide rules. Link the GPO high in the Active Directory tree so that it affects multiple OUs. For example, link a GPO with network security settings to a domain or site.

Note that the No Override option is actually being set on the link and not on the actual GPO. This means that if you have a GPO that is linked to multiple containers, you can configure the No Override option on each container, independently of the others.

When more than one link is set to No Override, and the linked GPOs all apply to a common container, and they contain conflicting settings, the GPO that is highest in the Active Directory hierarchy takes precedence.

To set the No Override option, perform the following steps:

1. Open the **Properties** dialog box for the container to which the GPO is linked.
2. On the **Group Policy** tab, click **Options**.
3. In the **Options** dialog box for the GPO, click **No Override**, and then click **OK**.

Note Include only critical settings in linked GPOs that are marked as No Override, because they take effect regardless of how other GPOs are set up. You want to be sure that you are not overriding important GPOs.

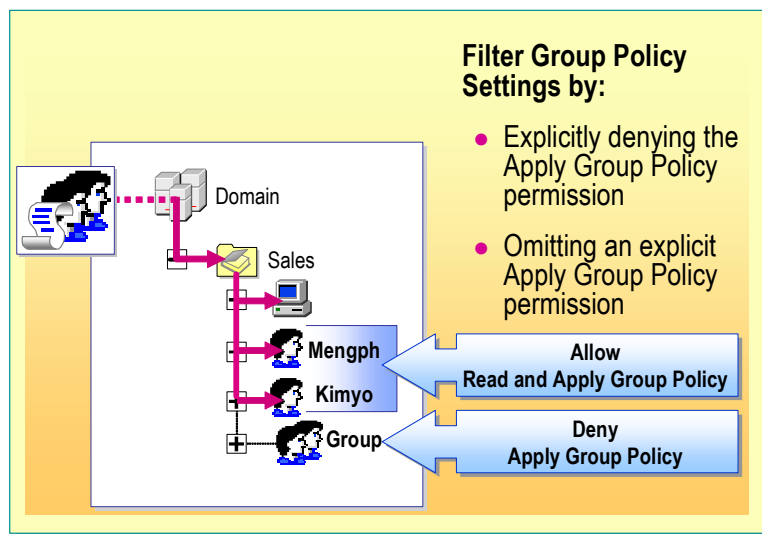
Filtering Group Policy Settings

Topic Objective

To explain what filtering is and how to filter Group Policy settings.

Lead-in

Another method used to modify Group Policy inheritance is filtering. Filtering allows you to prevent a GPO and its settings from applying to specific computers, users, and security groups within a container.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate filtering Group Policy settings on the **Security** tab in the **Properties** dialog box for a GPO.

Key Points

All authenticated users, which include computers, have the Read and Apply Group Policy permissions.

If a user or computer account does not have both the Read and Apply Group Policy permissions allowed, Group Policy will not be applied.

By default, for any given container, the Group Policy settings contained within all of the GPOs that affect the container are applied to all users and computers within that container. This may not produce the results that you desire. For example, if you have delegated administrative control of a child OU to one or more users whose accounts are in that OU, you may not want Group Policy to apply to those user accounts. You can control or filter the application of Group Policy by using security groups and the discretionary access control list (DACL) of one or more GPOs.

For Group Policy to apply to a user or computer account, the account needs to have an access control entry (ACE) in the DACL for a GPO that allows the Read permission and an ACE that allows the Apply Group Policy permission. The default DACL for a new GPO has the following ACEs:

- Authenticated Users – Allow Read and Allow Apply Group Policy.
- Domain Admins, Enterprise Admins and SYSTEM – Allow Read, Allow Write, Allow Create All Child Objects, Allow Delete All Child Objects.

Note Authenticated Users, CREATOR OWNER, Domain Admins, Enterprise Admins, and SYSTEM also have special permissions on GPOs. These special permissions are not listed in the previous paragraph because they do not affect the application of Group Policy.

To filter Group Policy so that Group Policy settings that would normally apply to all accounts in the OU do not affect the OU administrators in the example, you can use one of the following two methods:

Method 1

The first method is to explicitly deny the Apply Group Policy permission for the security group that contains the OU administrators. To filter Group Policy by explicitly denying the Apply Group Policy permission, perform the following steps:

1. Create a domain local security group and add the OU administrators to this group.
2. In the **Properties** dialog box, on the **Security** tab, add the security group for the GPO that you do not want to apply to the OU administrators.
3. Deny the Apply Group Policy permission for this security group.

Method 2

The second method is to remove Authenticated Users. By omitting the OU administrators from the security group, they have no explicit permissions on the GPO. To filter Group Policy by omitting an explicit Apply Group Policy permission, perform the following steps:

1. Remove the Authenticated Users groups from the DACL.
2. Create a domain local security group and add all computer and user accounts except the OU administrator accounts to this group.
3. In the **Properties** dialog box, on the **Security** tab, add the security group for the GPO that you do not want to apply to the OU administrators.
4. Allow the security group Read and Apply Group Policy permissions.

Class Discussion: Changing Group Policy Inheritance

Topic Objective

To check students' understanding of how Group Policy inheritance can be changed.

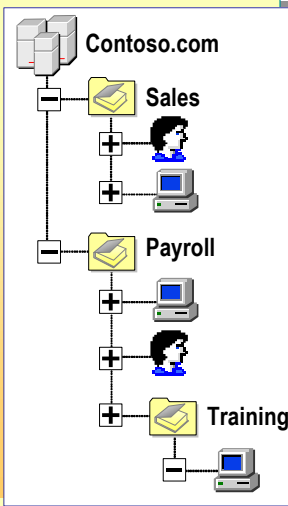
Lead-in

This is an example of how you can control the Group Policy settings applied by modifying Group Policy inheritance. Now we will go through the example together and determine the resultant Group Policy settings.

Settings That Are Needed

- An anti-virus application must be installed on all computers in the domain
- The Office suite must be installed on all computers in the domain, except for those in the Payroll department
- An accounting application must be installed on all client computers in the Payroll department, except for the computers used by the Payroll OU administrators

How do you set up your GPOs?



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

There are two slides in the presentation for this topic. Use the first slide to introduce the scenario and present the question.

After students have provided their answers, use the second slide to discuss the correct answer with the class.

After you have presented the second slide, mention to students that this slide is on the Lab Answers page on the Student Materials compact disc.

You have determined that the following conditions must exist in your network:

- An anti-virus application must be installed on all computers in the domain.
- The Microsoft Office suite must be installed on computers in the domain, except for users in the Payroll department.
- A line-of-business accounting application must be installed on all computers in the Payroll department, except those that are used by the Payroll OU administrators.

How should you set up GPOs so that the above conditions are met?

Create a GPO linked to the domain that installs the anti-virus application, and set the No Override option on the link. Create and link another GPO at the domain level that installs the Office suite.

At the Payroll OU, enable Block Inheritance. The No Override option on the link for the GPO that deploys the anti-virus application ensures that it is not blocked. Create and link a GPO to the Payroll OU that installs the accounting application on client computers. Modify the DACL of this GPO so that the computer accounts used by the Payroll administrators are denied Apply Group Policy permission.

Lab A: Implementing Group Policy

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create GPOs, link existing GPOs, and identify the effects of Group Policy inheritance. Then you will enable Block Inheritance, enable No Override, and filter Group Policy inheritance.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Link a Group Policy object (GPO) to an organizational unit (OU).
- Identify the effects of inheritance when multiple GPOs are assigned.
- Block Group Policy inheritance.
- Force a Group Policy to be applied to child OUs.
- Filter a Group Policy to be applied to selected users and groups within an OU.

Prerequisite

Before working on this lab, you must have experience using Active Directory Users and Computers.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a domain controller.
- An OU structure. To create the required OUs and users, run the 2154A.cmd batch file from C:\Moc\Win2154A\Labfiles.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Estimated time to complete this lab: 45 minutes

Exercise 1

Creating and Linking Group Policy Objects

Scenario

You need to assign a number of standard Group Policy settings to OUs in your domain. You also need to create GPOs for each OU so that you can delegate some of the Group Policy administration tasks to junior administrators in your organization. Users in the Accounting OU require only moderate restrictions. For these users, you will apply the Corporate Standard Desktop GPO. Users in the Accounts Payable and Accounts Receivable OUs are task workers and require a more restricted desktop environment. For these users, you will apply the Restricted Desktop GPO to add additional restrictions to the Corporate Standard Desktop Group Policy settings inherited from the parent OU.

Goal

You will link the Corporate Standard Desktop GPO in the nwtraders.msft domain to the Accounting OU. You will then link the Restricted Desktop GPO to the Accounts Payable OU and to the Accounts Receivable OU. For each OU, you will create a GPO that you will later use to delegate Group Policy administration for the Accounting OUs.

Tasks	Detailed Steps
1. Link the Corporate Standard Desktop GPO to the Accounting OU.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - In the Accounting Properties dialog box, click the Group Policy tab.  <i>Notice that no Group Policy objects are currently linked to this OU.</i> - On the Group Policy tab, click Add. - In the Add a Group Policy Object Link dialog box, on the All tab, under All Group Policy Objects stored in this domain, click Corporate Standard Desktop, and then click OK.  <i>Corporate Standard Desktop appears in the list of Group Policy Object Links. The Corporate Standard Desktop GPO is now linked to the Accounting OU.</i> - Leave the Accounting Properties dialog box open.
2. Create a new GPO for the Accounting OU. Name the new GPO Accounting Policy.	- In the Accounting Properties dialog box, click New. - Type Accounting Policy and then press ENTER. - Click Close to close the Accounting Properties dialog box. - Leave Active Directory Users and Computers open.

Tasks	Detailed Steps
3. Link the Restricted Desktop GPO to the Accounts Payable OU.	a. In the console tree, expand Accounting, right-click Accounts Payable, and then click Properties. b. In the Accounts Payable Properties dialog box, on the Group Policy tab, click Add. c. In the Add a Group Policy Object Link dialog box, on the All tab, under All Group Policy Objects stored in this domain, click Restricted Desktop, and then click OK. d. Leave the Accounts Payable Properties dialog box open.
4. Create a new GPO for the Accounts Payable OU. Name the new GPO Accounts Payable Policy.	a. In the Accounts Payable Properties dialog box, click New. b. Type Accounts Payable Policy and then press ENTER. c. Click Close to close the Accounts Payable Properties dialog box. d. Leave Active Directory Users and Computers open.
5. Link the Restricted Desktop GPO to the Accounts Receivable OU.	a. In the console tree, right-click Accounts Receivable, and then click Properties. b. In the Accounts Receivable Properties dialog box, on the Group Policy tab, click Add. c. In the Add a Group Policy Object Link dialog box, on the All tab, under All Group Policy Objects stored in this domain, click Restricted Desktop, and then click OK. d. Leave the Accounts Receivable Properties dialog box open.
6. Create a new GPO for the Accounts Receivable OU. Name the new GPO Accounts Receivable Policy.	a. In the Accounts Receivable Properties dialog box, click New. b. Type Accounts Receivable Policy and then press ENTER. c. Click Close to close the Accounts Receivable Properties dialog box. d. Close Active Directory Users and Computers, and then log off.

Exercise 2

Verifying Group Policy Settings

Scenario

The Corporate Standard Desktop GPO contains settings that make the following changes to users' desktop environments:

- The Administrative Tools folder does not appear on the Start menu.
- The Windows Update icon does not appear on the Start menu.
- The list of recent documents should not be kept.

The Restricted Desktop GPO contains settings that make the following changes to users' desktop environments:

- Taskbar and Start Menu settings cannot be changed.
- Users cannot browse the network.

You need to log on as a user from the Accounting and Accounts Receivable OUs to verify that the correct settings are being applied.

Goal

You will log on by using user accounts in the Accounting and Accounts Receivable OUs and record which Group Policy settings are enforced.

Tasks	Detailed Steps
1. Log on as Acctguser and verify the Group Policy settings for a user in the Accounting OU.	a. Log on as Acctguser with a password of password .
? Are the following settings, contained in the Corporate Standard Desktop GPO, enforced? ■ The Administrative Tools menu does not appear on the Start menu. ■ The Windows Update icon does not appear on the Start menu. ■ The Documents icon does not appear on the Start menu. Yes, all of the restrictions in the Corporate Standard Desktop GPO are enforced.	

Tasks	Detailed Steps
1. <i>(continued)</i>	b. Log off.
2. Log on as Aruser and verify the Group Policy settings for a user in the Accounts Receivable OU.	a. Log on as Aruser with a password of password .
? Are the following Group Policy settings, contained in the Corporate Standard Desktop GPO, enforced? ▪ The Administrative Tools menu does not appear on the Start menu. ▪ The Windows Update icon does not appear on the Start menu. ▪ The Documents icon does not appear on the Start menu. Yes, all of the restrictions in the Corporate Standard Desktop GPO are enforced.	
? Are the following settings, contained in the Restricted Desktop GPO, enforced? ▪ Taskbar and Start Menu settings cannot be changed. ▪ Users cannot browse the network. Yes, all of the restrictions in the Restricted Desktop GPO are enforced.	
? Why did the restrictions in the Corporate Standard Desktop GPO apply to the user in the Accounts Receivable OU? The Accounts Receivable OU is a child of the Accounting OU and inherits the Group Policy settings from the Accounting OU.	
2. <i>(continued)</i>	b. Log off.

Exercise 3

Blocking Group Policy Inheritance

Scenario

Group Policy settings assigned anywhere else in Active Directory should not affect the Accounts Receivable department.

Goal

You will configure the Accounts Receivable OU so that policies that exist higher in the hierarchy are not applied by blocking Group Policy inheritance. You will then verify the new settings for Accounts Receivable and Account Payable users.

Tasks	Detailed Steps
1. Block Group Policy inheritance for the Accounts Receivable OU.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, expand Accounting, right-click Accounts Receivable, and then click Properties. - On the Group Policy tab, click Block Policy inheritance, and then click OK. - Log off.
2. Log on as Aruser and verify that Group Policy inheritance is blocked for the Accounts Receivable OU.	Log on as Aruser with a password of password.
 Are the following settings, contained in the Corporate Standard Desktop GPO, enforced? Why or why not? - The Administrative Tools menu does not appear on the Start menu. - The Windows Update icon does not appear on the Start menu. - The Documents icon does not appear on the Start menu. No, none of the restrictions in the Corporate Standard Desktop GPO is enforced. Group Policy inheritance is blocked for the Accounts Receivable OU. Because the Corporate Standard Desktop GPO is linked to a parent OU, the settings are not applied.	

Tasks	Detailed Steps
? Are the following settings, contained in the Restricted Desktop GPO, enforced? Why or why not? ▪ Taskbar and Start Menu settings cannot be changed. ▪ Users cannot browse the network. Yes, all of the restrictions in the Restricted Desktop GPO are enforced. The Restricted Desktop GPO is linked directly to the Accounts Receivable OU so the Block Policy inheritance setting has no effect on this GPO.	
2. (continued)	b. Log off.
3. Log on as Appuser and verify that Group Policy inheritance is not blocked for the Accounts Payable OU.	a. Log on as Appuser with a password of password .
? Are the following settings, contained in the Corporate Standard Desktop GPO, enforced? Why or why not? ▪ The Administrative Tools menu does not appear on the Start menu. ▪ The Windows Update icon does not appear on the Start menu. ▪ The Documents icon does not appear on the Start menu. Yes, because Block Policy inheritance is not enabled for the Accounts Payable OU, Group Policy objects linked to parent containers are still applied.	
3. (continued)	b. Log off.

Exercise 4

Forcing Group Policy Inheritance

Scenario

A new GPO has been created that specifies that all users should be prevented from changing the location of My Documents. You have to ensure that even OUs configured to block Group Policy inheritance receive the new settings.

Goal

You will link the Restricted My Documents GPO to the Accounting OU, and verify the users to which the settings apply. You will then configure the Restricted My Documents GPO with the No Override option so that it will always be applied to all child containers.

Tasks	Detailed Steps
1. Link the Restricted My Documents GPO to the Accounting OU and enable the No Override option for the GPO.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - In the Accounting Properties dialog box, on the Group Policy tab, click Add. - In the Add a Group Policy Object Link dialog box, on the All tab, under All Group Policy Objects stored in this domain, click Restricted My Documents, and then click OK. - In the Group Policy Object Links list, right-click Restricted My Documents, and then click No Override.  Notice that a check mark now appears in the No Override column to the right of the Restricted My Documents GPO. - Click OK, close Active Directory Users and Computers, and then log off.
2. Log on as Aruser and verify that the Restricted My Documents GPO is applied.	- Log on as Aruser with a password of password. - On the desktop, right-click My Documents, and then click Properties.
 Can you change the target folder location? Why or why not? No, the target folder location cannot be changed. Although the Accounts Receivable OU has the Block Policy inheritance option enabled, the Restricted My Documents GPO has the No Override option enabled, which takes precedence over Block Policy inheritance.	
2. (continued)	Log off.

Exercise 5

Filtering Group Policy

Scenario

A line of business applications used by the Accounting department requires a domain user account in the Accounting OU. Because of compatibility problems, the Corporate Standard Desktop GPO cannot apply to the user. You need to configure the GPO to filter the application user account from having the Group Policy applied.

Goal

You will configure permissions for the Corporate Standard Desktop GPO so that it will not be applied to the Application User account in the Accounting OU. You will then verify that the GPO settings no longer apply to the Application User.

Tasks	Detailed Steps
1. Configure the Corporate Standard Desktop GPO so that it will not be applied to the Application User account.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - In the Accounting Properties dialog box, on the Group Policy tab, right-click Corporate Standard Desktop, and then click Properties. - On the Security tab, click Add. - Under Name, double-click Application User, and then click OK. - With Application User selected, select the Deny check box next to Apply Group Policy, and then click OK. - In the Security dialog box, click Yes to continue. - Click OK to close the Accounting Properties dialog box, close Active Directory Users and Computers, and then log off.
2. Verify that the settings in the Corporate Standard Desktop GPO do not apply to the Application User account.	Log on as Appuser with a password of password.

Tasks	Detailed Steps
?	Are the following settings, contained in the Corporate Standard Desktop GPO, enforced? Why or why not? ▪ The Administrative Tools menu does not appear on the Start menu. ▪ The Windows Update icon does not appear on the Start menu. ▪ The Documents icon does not appear on the Start menu. No, none of the restrictions in the Corporate Standard Desktop GPO is enforced. The discretionary access control list for the Corporate Standard Desktop GPO contains an access control entry denying the Apply Group Policy permission for the Application User account.
2. (continued)	b. Log off.

Delegating Administrative Control of Group Policy

Topic Objective

To explain when and why to delegate administrative control of a GPO.

Lead-in

Windows 2000 allows you to delegate control of a GPO to an administrator or user. That administrator or user has control over only the setting of the GPO, not the container to which the GPO is linked.

- **Enable a User to Manage Group Policy Links for a Site, Domain, or OU by:**
 - Assigning the user read and write permissions to the gPLink and gPOptions attributes of the site, domain, or OU
 - Using the Delegation of Control wizard
- **Enable a User or Group to Create GPOs by:**
 - Adding the user or group to the Group Policy Creator Owners group
- **Enable a User to Edit GPOs by:**
 - Assigning the user read and write permissions to the GPO
 - Making the user a member of either Domain Admins, Enterprise Admins, or GPO Creator Owners groups
 - Granting the user access to the GPO by using the Security tab in the GPO Properties dialog box

*****ILLEGAL FOR NON-TRAINER USE*****

Active Directory enables an administrator to delegate control of Group Policy objects (GPOs). This section explains how Group Policy fits in with the delegation of sites, domains, and organizational units.

The delegation of Group Policy consists of the following three aspects, which can be used together or separately, as a particular situation requires:

- Managing Group Policy links for a site, domain, or OU
- Creating GPOs
- Editing GPOs

Managing Group Policy Links for a Site, Domain, or OU

The **Group Policy** tab in the **Properties** dialog box of a site, domain, or OU allows the administrator to specify which GPOs are linked to that site, domain, or OU. This information is stored in the gPLink and gPOptions attributes of the container to which the GPO is linked.

Active Directory supports security settings on a per-property basis. This means that a non-administrator can be given read and write access to specific properties. In this case, if non-administrators have read and write access to the gPLink and gPOptions attributes, they can manage the list of GPOs linked to that site, domain, or OU.

To give a group read and write access to these attributes, use the Delegation of Control wizard and select the Manage Group Policy links predefined task.

Creating GPOs

In Windows 2000, by default, only the System account and members of the Domain Admins, Enterprise Admins, and Group Policy Creator Owners groups can create GPOs. If you want a non-administrator or group to be able to create GPOs, you can add that user or group to the Group Policy Creator Owners security group.

When a non-administrator who is a member of the Group Policy Creator Owners group creates a GPO, that user becomes the creator and owner of the GPO; therefore, the user can edit the GPO. Being a member of the Group Policy Creator Owners group gives the non-administrator full control of only those GPOs that the user creates or those explicitly delegated to that user; it does not give the non-administrator full control of all of the GPOs for the domain.

If you add a user or group to the Group Policy Creator Owners group, but do not also use the Delegation of Control wizard to allow the user or group read and write access to the gPLink and gPOptions attributes of a site, domain, or OU, the user or group will be able to create GPOs, but will not be able to link the new GPOs.

Note When an administrator creates a GPO, the Domain Administrators group becomes the Creator Owner of the GPO.

Editing GPOs

To edit a GPO, the user must have both read and write access to the GPO. To edit a GPO, the user must be one of the following:

- A member of Domain Admins or Enterprise Admins.
- A Creator Owner.
- A user with access to the GPO. That is, an administrator or a user to whom the Creator Owner has granted access to the GPO.

By default, GPOs give members of Domain Admins, Enterprise Admins, the Group Policy Creator Owners groups, and the System account full control without the Apply Group Policy attribute. This means that they can edit the GPO, but the policies contained in that GPO do not apply to them.

Authenticated Users have read access to the GPO with the Apply Group Policy attribute set to Allow.

Administrators are also authenticated users, which means that they have the Apply Group Policy attribute set. If this is not desired, administrators have two choices:

- Remove authenticated users from the list and add their own security group with the Apply Group Policy attribute set to Allow. This new group should contain all of the users whom this Group Policy is intended to affect.
- Set the Apply Group Policy attribute to Deny for the Domain and Enterprise Administrators, and possibly the Creator Owner groups. This setting prevents the GPO from being applied to members of those groups. Remember that an ACE set to Deny always takes precedence over an ACE set to Allow. Therefore, if a given user is a member of another group that is set to explicitly Allow the Apply Group Policy attribute for this GPO, it will still be denied.

Note For more information about delegating administrative control of Group Policy, see *Using Group Policy Scenarios* under **Additional Reading** on the Web page on the Student Materials compact disc.

Lab B: Delegating Group Policy Administration

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will plan a Group Policy implementation, create GPOs, and set permissions to delegate control of a GPO.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Delegate control of Group Policy to allow a user to manage Group Policy links.
- Delegate control of Group Policy to allow a user to create Group Policy objects.
- Delegate control of Group Policy to allow a user to edit Group Policy objects.

Prerequisite

Before working on this lab, you must have experience using Active Directory Users and Computers and configuring permissions for objects.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a domain controller.

Estimated time to complete this lab: 30 minutes

Exercise 1

Delegating Group Policy Administration

Scenario

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

Goal

In this exercise, you will modify the discretionary access control lists (DACLS) for the existing GPOs to allow the junior administrator to modify them, add the junior administrator's account to the Group Policy Creator Owners group to allow the junior administrator to create new GPOs, and then delegate the ability to manage Group Policy links to the junior administrator.

Tasks	Detailed Steps
1. Verify whether the acctadmin user can currently accomplish the following tasks: • Link and unlink GPOs in the Accounting OU. • Create new GPOs in the Accounting OU. • Modify the current GPOs linked to the Accounting OU.	a. Log on as Acctadmin with a password of password . b. Open Active Directory Users and Computers by typing dsa.msc in the Run box. c. In the console tree, expand your domain, right-click Accounting , and then click Properties . d. In the Accounting Properties dialog box, click the Group Policy tab.
 Can the acctadmin user accomplish any of the following tasks? ▪ Link and unlink GPOs? ▪ Create new GPOs? ▪ Edit existing GPOs? No, the acctadmin user cannot accomplish any of the tasks.	
1. <i>(continued)</i>	e. Click Cancel , close Active Directory Users and Computers, and then log off.

Tasks	Detailed Steps
2. Modify the DACL on the GPOs currently linked to the Accounting OU to allow the acctadmin account to modify them.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - On the Group Policy tab, in the Group Policy Object Links list, right-click Corporate Standard Desktop, and then click Properties. - On the Security tab, click Add, type acctadmin and then click OK. - On the Security tab, with the Accounting Admin account selected, select the Allow check box beside Write, and then click OK. - Repeat steps d, e, and f for the Accounting Policy and the Restricted My Documents GPOs. - Click OK to close the Accounting Properties dialog box, close Active Directory Users and Computers, and then log off.
3. Verify whether the acctadmin user can currently accomplish the following tasks: - Link and unlink GPOs in the Accounting OU. - Create new GPOs in the Accounting OU. - Modify the current GPOs linked to the Accounting OU.	- Log on as Acctadmin with a password of password. - Open Active Directory Users and Computers by clicking Start, clicking Run, typing dsa.msc and then clicking OK. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - In the Accounting Properties dialog box, click the Group Policy tab.
? Can the acctadmin user accomplish any of the following tasks? - Link and unlink GPOs? - Create new GPOs? - Edit existing GPOs? The acctadmin user can only edit existing GPOs.	
3. (continued)	Click Cancel, close Active Directory Users and Computers, and then log off.

Tasks	Detailed Steps
4. Use the Delegation of Control wizard to delegate the Manage Group Policy Links task to the acctadmin user account.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, right-click Accounting, and then click Delegate Control. - On the Welcome to the Delegation of Control Wizard page, click Next. - On the Users or Groups page, click Add, type acctadmin click OK, and then click Next. - On the Task to Delegate page, click Manage Group Policy links, and then click Next. - On the Completing the Delegation of Control Wizard page, review the settings, and then click Finish. - Close Active Directory Users and Computers, and then log off.
5. Verify whether the acctadmin user can currently accomplish the following tasks: - Link and unlink GPOs in the Accounting OU. - Create new GPOs in the Accounting OU. - Modify the current GPOs linked to the Accounting OU.	- Log on as Acctadmin with a password of password. - Open Active Directory Users and Computers by clicking Start, clicking Run, typing dsa.msc and then clicking OK. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - In the Accounting Properties dialog box, click the Group Policy tab.
? Can the acctadmin user accomplish any of the following tasks? - Link and unlink GPOs? - Create new GPOs? - Edit existing GPOs? The acctadmin user can edit existing GPOs and can link and unlink GPOs, but cannot create new GPOs.	
5. (continued)	Click Cancel to close the Accounting Properties dialog box, close Active Directory Users and Computers, and then log off.

Tasks	Detailed Steps
6. Allow the acctadmin user account to create new GPOs by making it a member of the Group Policy Creator Owners group.	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand your domain, and then click Users. - In the details pane, double-click Group Policy Creator Owners. - On the Members tab, click Add, type acctadmin and then click OK. - Click OK to close the Group Policy Creator Owners Properties dialog box, close Active Directory Users and Computers, and then log off.
7. Verify whether the acctadmin user can currently accomplish the following tasks: - Link and unlink GPOs in the Accounting OU. - Create new GPOs in the Accounting OU. - Modify the current GPOs linked to the Accounting OU.	- Log on as Acctadmin with a password of password. - Open Active Directory Users and Computers by typing dsa.msc in the Run box. - In the console tree, expand your domain, right-click Accounting, and then click Properties. - In the Accounting Properties dialog box, click the Group Policy tab.
 Can the acctadmin user accomplish any of the following tasks? - Link and unlink GPOs? - Create new GPOs? - Edit existing GPOs? The acctadmin user can accomplish all of the tasks.	
7. (continued)	Click Cancel to close the Accounting Properties dialog box, close Active Directory Users and Computers, and then log off.

◆ Monitoring and Troubleshooting Group Policy

Topic Objective

To introduce methods of monitoring Group Policy, explain various troubleshooting tools, and discuss common problems encountered when implementing Group Policy.

Lead-in

There are various methods of monitoring Group Policy and various troubleshooting tools for common problems with implementing Group Policy.

- **Monitoring Group Policy**
- **Group Policy Troubleshooting Tools**
- **Troubleshooting Group Policy**

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly present the topics for this section.

There are various methods of monitoring Group Policy for implementation problems. If you encounter any problem in the implementation of Group Policy, you can use one of the many tools provided by Windows 2000 to troubleshoot such problems. To successfully resolve any problem in the implementation of Group Policy, you must know the common implementation problems and understand their possible causes.

Monitoring Group Policy

Topic Objective

To describe how to enable diagnostic logging and verbose logging to monitor Group Policy.

Lead-in

You can monitor Group Policy by enabling diagnostic logging and verbose logging.

You Can Monitor Group Policy by:



■ Enabling Diagnostic Logging to the Event Log

- Causes Group Policy to generate detailed events in the Event Log

■ Enabling Verbose Logging

- Tracks all changes and settings applied to the local computer and the users who log on to the computer
- Involves the addition of the registry keys for verbose logging

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate to the class how to enable diagnostic logging to the Event Log.

There are various methods of monitoring Group Policy. You can monitor Group Policy by enabling diagnostic logging and verbose logging.

Enabling Diagnostic Logging to the Event Log

Enabling diagnostic logging for Group Policy causes Group Policy to generate detailed events in the Event Log. These detailed events can help assist in diagnosing problems associated with Group Policy processing by backtracking the events and providing additional information about them.

► To enable diagnostic logging:

1. Log on as the local administrator.
 2. Click **Start**, and then click **Run**.
 3. In the **Open** text box, type **regedit** and then click **OK**.
 4. Open the **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion** key.
 5. On the **Edit** menu, point to **New**, click **Key**, type **Diagnostics** and then press ENTER.
 6. With the **Diagnostics** key selected, on the **Edit** menu, point to **New**, click **DWORD Value**, type **RunDiagnosticLoggingGlobal** and then press ENTER.
 7. Double-click **RunDiagnosticLoggingGlobal**, type **1** and then click **OK**.
- Events generated by Group Policy are recorded in the Application log.

Note Enabling diagnostic logging for Group Policy generates a large number of events during computer startup and when a user logs on. You should increase the size of the Application log prior to enabling diagnostic logging so that the Application log does not fill up. Also, enable diagnostic logging only when troubleshooting Group Policy and disable it when you are finished.

Enabling Verbose Logging

Verbose logging tracks all changes and settings applied to the local computer and to users who log on to the computer by Group Policy. The log file is located in the *systemroot*\Debug\UserMode folder and is named Userenv.log. Enabling verbose logging involves adding the registry key for verbose logging.

To enable verbose logging, add a DWORD value named **UserEnvDebugLevel** with a value of 30002 to the **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon** key in the registry.

Note A value of 30002 enables verbose logging, 30001 enables logging of errors and warnings only, and 30000 logs nothing.

To disable verbose logging, delete the UserenvDebugLevel value from the registry.

Group Policy Troubleshooting Tools

Topic Objective

To describe the tools provided by Windows 2000 for troubleshooting problems associated with Group Policy.

Lead-in

Windows 2000 provides a number of different tools that you can use to help troubleshoot and resolve problems associated with Group Policy.

■ Windows 2000 Support Tools for Group Policy Troubleshooting:

- Netdiag.exe
- Replmon.exe



■ Windows 2000 Resource Kit Tools for Group Policy Troubleshooting:

- Gpoutil.exe
- Gpresult.exe

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 provides a number of different tools that you can use to help troubleshoot and resolve problems associated with Group Policy. Some of these tools are included on the Windows 2000 Server CD-ROM in the Windows 2000 Support Tools\Tools folder, whereas others are included in the Windows 2000 Resource Kit.

Windows 2000 Support Tools for Group Policy Troubleshooting

You can resolve Group Policy issues by using the following tools that are included in the Windows 2000 Support Tools package on the Windows 2000 Server CD-ROM:

- *Netdiag.exe*. This command-line diagnostic tool helps isolate networking and connectivity problems by performing a series of tests to determine the state of your network client and whether it is functional. These tests and the key network status information they expose give network administrators and support personnel a more direct means of identifying and isolating network problems. This tool can help you diagnose and resolve Group Policy problems that are related to network connectivity.
- *Replmon.exe*. This tool can help you diagnose and resolve Group Policy problems that are related to incomplete replication of the GPC and the GPT. This tool enables administrators to view the low-level status of Active Directory replication, force synchronization between domain controllers, view the topology in a graphical format, and monitor the status and performance of domain controller replication through a graphical interface.

Windows 2000 Resource Kit Tools for Group Policy Troubleshooting

You can resolve Group Policy issues by using the following tools that are included in the Windows 2000 Resource Kit:

- *Gpoutil.exe*. This command-line tool allows you to check the health of the Group Policy objects on domain controllers.
- *Gpresult.exe*. This command-line tool displays information about the result Group Policy has had on the current computer and logged-on user.

Note For details and usage of these tools, refer to the Windows 2000 Resource Kit.

Troubleshooting Group Policy

Topic Objective

To identify the common problems encountered when implementing Group Policy and explain the suggested strategies for resolving the problems.

Lead-in

You may encounter problems when implementing Group Policy.



Cannot Access or Open the Group Policy Object



Group Policy Settings Not Taking Effect as Expected

*****ILLEGAL FOR NON-TRAINER USE*****

You may encounter problems when implementing Group Policy. Here are some of the more common problems that you may encounter, along with suggested strategies for resolving them.

- You attempt to either open or edit a Group Policy object, and receive an error indicating that the Group Policy object cannot be accessed or opened. Possible causes and their solutions are:
 - You do not have permissions to access the GPO. Check the DACL for the GPO that you are trying to open or edit. You must have both Read and Write permissions to open or edit a GPO.
 - The domain controller that Group Policy is trying to reach is offline or cannot be resolved with Domain Name System (DNS). Confirm that the domain controller is online, if it is, confirm that you can resolve the name of the domain controller with DNS.

- Group Policy settings are not applied as expected. Possible causes and their solutions are:
 - Inheritance Conflicts. If it appears that Group Policy settings are not being applied, the problem may be due to inheritance conflicts. Starting at the top of the Active Directory hierarchy, check the order of the GPOs linked to each site, domain, and OU that may affect the user or computer that is not receiving Group Policy settings. Next, see if there are conflicts between computer and user settings. Remember that in most cases, computer settings take precedence over conflicting user settings. Check GPO links for No Override and check domains and OUs for Block Inheritance.
 - Permission Issues. Check the DACLs of the GPOs that you expect to be applied. Ensure that the user or computer account has both Read and Apply Group Policy permissions on all GPOs that should be applied. Also, check security group membership for the computer or user account and ensure that the security group or groups that the account is a member of is listed on the DACL. Also, check for Deny ACEs. Remember that Deny takes precedence over all Allow permissions.
 - Disabled GPO Nodes. Check all GPOs to see if either the Computer Configuration or User Configuration nodes have been disabled.
 - Replication Issues. Ensure that both Active Directory replication and Sysvol replication are complete. Remember that if the GPC and GPT portions of a GPO are not both replicated, Group Policy will not be applied.
 - Inter-Domain GPO Link Issues. If a site, domain, or OU is linked to a GPO in another domain, the GPO is accessed through a trust relationship. If the trust fails for any reason, access to the linked GPO fails and so does Group Policy processing. You can prevent this type of problem by ensuring that you have multiple domain controllers per domain, or by creating explicit trusts between domains.
 - Computer or User Object Moved. Client computers cache the Active Directory location for thirty minutes. If the computer or user account is moved from one OU to another, the client computer may not have the correct location for the object. If Group Policy refreshes before the cached location does, the new Group Policy settings will not be processed. However, the new Group Policy settings will be processed the next time Group Policy is refreshed.

Best Practices

Topic Objective

To present best practices for implementing Group Policy.

Lead-in

Review this checklist before you implement Group Policy.

-  **Limit the Use of Blocking, No Override, and Filtering of GPOs**
-  **Limit the Number of GPOs That Affect Any Computer or User**
-  **Group Related Settings in a Single GPO**
-  **Delegate Administrative Control of a GPO to One or Two Users**
-  **Avoid Linking GPOs to a Site with Multiple Domains**
-  **Plan and Test GPOs Before You Implement Them**

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Emphasize the reason for each best practice.

Emphasize that it is a good practice to use a domain local group, a global group, or a universal group when you assign GPO permissions.

The following list provides best practices for implementing Group Policy. Review this checklist before you implement Group Policy:

- Limit the use of Block Inheritance, No Override, and filtering of GPOs, especially across domains. Each one of these introduces a further level of complexity. When you must use one of these methods, try to use only one at a time.
- Limit the number of GPOs that affect any given computer or user. If there is a problem with the settings that apply to a computer or user, it will be easier to troubleshoot if there are fewer GPOs.
- Group related settings in a single GPO. For example, a GPO that you use to publish Microsoft Office 2000 should also contain any registry-based Group Policy settings for Office 2000, which makes it easier to manage related settings.
- Limit the number of administrators to whom you delegate control of a GPO to one or two. This limits the possibility of multiple administrators making changes to Group Policy settings at the same time.
- Avoid linking a GPO to a site that contains multiple domains. A GPO linked to a site affects all computers in that site, requiring all computers to contact a domain controller in the domain in which the GPO resides. This can increase network traffic. Instead, link the GPO to all domains in the site.
- Plan a model of how you want to implement Group Policy in your network before you start adding GPOs. Create two or more models and compare them to determine what best meets your needs. Planning ensures that your Group Policy settings match your corporate and network needs, are easy to manage, and that you have the flexibility to make future changes.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Group Policy
- Group Policy Structure
- Working with Group Policy Objects
- How Group Policy Settings Are Applied in Active Directory
- Modifying Group Policy Inheritance
- Delegating Administrative Control of Group Policy
- Monitoring and Troubleshooting Group Policy
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Give students time to read and answer the review questions on their own, and then go over the answers as a group.

1. You want to set corporate-wide Group Policy settings and at the same time set policies that affect only certain departments. How do Active Directory and Group Policy facilitate this?

By associating multiple Group Policy objects with sites, domains, or OUs, you can set Group Policy settings that affect the entire domain or policies that apply to only a single OU.

2. Users in three OUs (Sales, Production, and Training) need the same applications. Each OU has a different parent OU. What is the simplest way to use Group Policy to ensure that the users in the three OUs have the applications that they need?

Create a GPO at one of the OUs with the required user settings to install the applications. Link that GPO to the other two OUs.

3. Your network has one domain. All user accounts in your network reside in either the Sales OU or the Production OU. You need to ensure that all users have a specific application on their desktops. How do you set up the Group Policy?

At the domain level, you link a GPO that installs the application on user desktops.

4. All domain user accounts are in the Employees OU. You want to prevent users from accessing the Internet, except for a few users who do research. What can you do to make sure that these users can gain access to the Internet, but not other users?

You configure a GPO with settings that remove access to the Internet and link it to the Employees OU. Then you remove the Group Policy permissions Read and Apply Group Policy for the Research group. The GPO will no longer apply to the Research group.

5. You have linked a GPO to the domain that prevents users from installing a particular application on their client computers. Yet you notice that several users in the Developers OU have the application installed. Why might this have happened? How do you ensure that the application is not installed?

An administrator has linked a GPO that allows users to install the application to the Developers OU, or the administrator has blocked Group Policy inheritance, preventing the domain GPO from applying to users in the OU. To ensure that users cannot install the application, you should select the No Override option at the domain level.

6. Your company has a software administrator who is responsible for installing the correct applications on the computers for all users in the Human Resources OU by using Group Policy. The software administrator should not be able to make changes to users or computers. What do you do to ensure that the software administrator can install the necessary software by using Group Policy?

Create a GPO linked to the Human Resources OU that is used to assign software settings, and then delegate control of the GPO to the software administrator. To do this, assign the Read and Write permissions for the GPO to the Software Administrators group. Members of the Software Administrators group can then edit the settings for the GPO.

