

Module 7: Managing Access to Objects in Organizational Units

Contents

Overview	1
Multimedia: The Organizational Unit Structure	2
Lesson: Modifying Permissions for Active Directory Objects	3
Lesson: Delegating Control of Organizational Units	18
Lab A: Managing Access to Objects in Organizational Units	27



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, place or event 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.

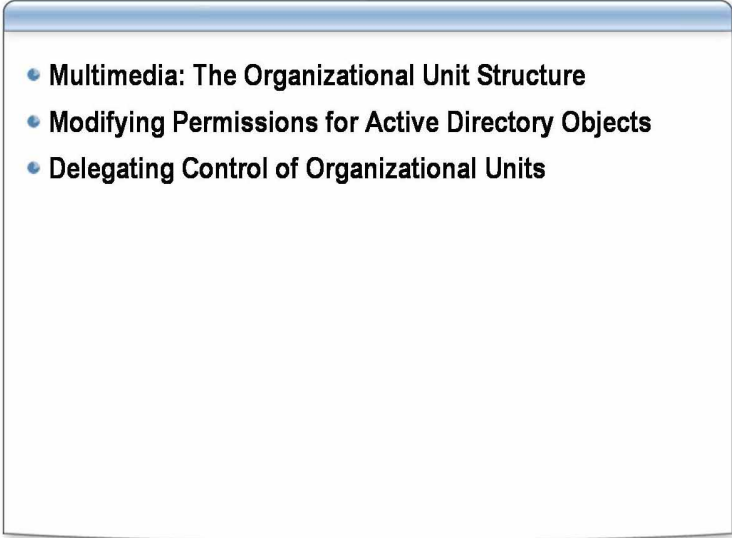
Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these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

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, IntelliMirror, MSDN, PowerPoint, Visual Basic, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Overview

- 
- **Multimedia: The Organizational Unit Structure**
 - **Modifying Permissions for Active Directory Objects**
 - **Delegating Control of Organizational Units**

Introduction

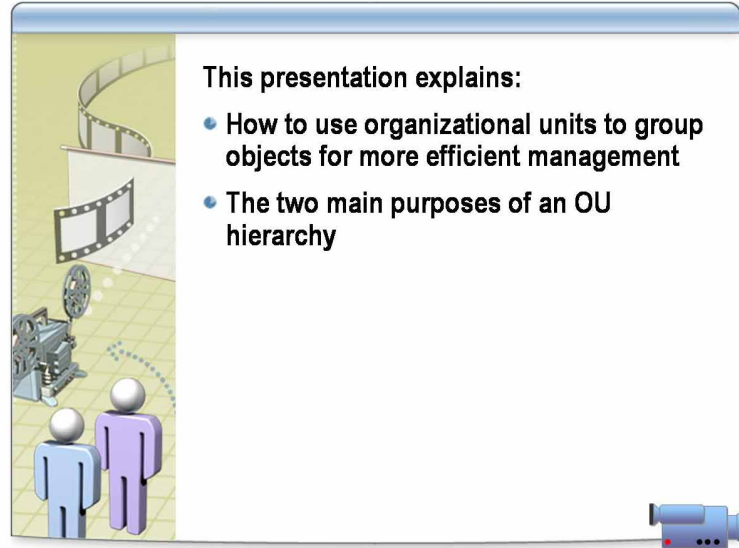
The information in this module introduces the job function of managing access to objects in organizational units. Specifically, the module provides the skills and knowledge that you need to explain the permissions available for managing access to objects in the Active Directory® directory service, move objects between organizational units in the same domain, and delegate control of an organizational unit.

Objectives

After completing this module, you will be able to:

- Identify the role of the organizational unit.
- Modify permissions for Active Directory objects.
- Delegate control of organizational units.

Multimedia: The Organizational Unit Structure



File location

To view the *The Organizational Unit Structure* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation. Do not open this presentation unless the instructor tells you to.

Objectives

After completing this lesson, you will be able to explain how to use organizational units to manage objects.

Lesson: Modifying Permissions for Active Directory Objects

- What Are Active Directory Object Permissions?
- Characteristics of Active Directory Object Permissions
- Permissions Inheritance for Active Directory Object Permissions
- Effects of Modifying Objects on Permissions Inheritance
- How to Modify Permissions on Active Directory Objects
- What Are Effective Permissions for Active Directory Objects?
- How to Determine Effective Permissions for Active Directory Objects

Introduction

Every object in Active Directory has a security descriptor that defines which accounts have permission to access the object and what type of access is allowed. The Microsoft® Windows® Server 2003 family uses these security descriptors to control access to objects.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what Active Directory object permissions are.
- Describe the characteristics of Active Directory object permissions.
- Describe permissions inheritance for Active Directory object permissions.
- Describe the effects of modifying objects on permission inheritance.
- Modify permissions for Active Directory objects.
- Explain what effective permissions are for Active Directory objects.
- Determine effective permissions for Active Directory objects.

What Are Active Directory Object Permissions?

Permission	Allows the user to:
Full Control	Change permissions, take ownership, and perform the tasks that are allowed by all other standard permissions
Write	Change object attributes
Read	View objects, object attributes, the object owner, and Active Directory permissions
Create All Child Objects	Add any type of object to an organizational unit
Delete All Child Objects	Remove any type of child object from an organizational unit

Introduction

Active Directory object permissions provide security for resources by enabling you to control which administrators or users can access individual objects or object attributes and the type of access allowed. You use permissions to assign administrative privileges for an organizational unit or a hierarchy of organizational units to manage network access. You can also use permissions to assign administrative privileges for a single object to a specific user or group.

Standard and special permissions

Standard permissions are the most frequently granted permissions and consist of a collection of special permissions. Special permissions give you a higher degree of control over the type of access you can grant for objects. The standard permissions include the following:

- Full Control
- Write
- Read
- Create All Child Objects
- Delete All Child Objects

Access authorized by permissions

An administrator or the owner of the object must grant permissions for the object before users can access it. The Windows Server 2003 family stores a list of user access permissions, called the discretionary access control list (DACL), for every object in Active Directory. The DACL for an object lists who can access the object and the specific actions that each user can perform on the object.

Additional reading

For more information about Active Directory permissions, see “Best practices for assigning permissions on Active Directory objects” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/ACLUI_acl_BP.asp.

Characteristics of Active Directory Object Permissions

Active Directory object permissions can be:

- Allowed or denied
- Implicitly or explicitly denied
- Set as standard or special permissions
 - Standard permissions* are the most frequently assigned permissions
 - Special permissions* provide a finer degree of control for assigning access to objects
- Set at the object level or inherited from its parent object

Introduction

Although NTFS permissions and Active Directory object permissions are similar, certain characteristics are specific to Active Directory object permissions. Active Directory object permissions can be allowed or denied, implicitly or explicitly denied, set as standard or special permissions, and set at the object level or inherited from its parent object.

Allowing and denying permissions

You can allow or deny permissions. Denied permissions take precedence over any permission that you otherwise allow to user accounts and groups. Deny permissions only when it is necessary to remove a permission that a user is granted by being a member of a group.

Implicit or explicit permissions

You can implicitly or explicitly deny permissions as follows:

- When permission to perform an operation is not explicitly allowed, it is *implicitly denied*.

For example, if the Marketing group is granted Read permission for a user object, and no other security principal is listed in the DACL for that object, users who are not members of the Marketing group are implicitly denied access. The operating system does not allow users who are not members of the Marketing group to read the properties of the user object.

- You *explicitly deny* a permission when you want to exclude a subset within a larger group from performing a task that the larger group has permissions to perform.

For example, it may be necessary to prevent a user named Don from viewing the properties of a user object. However, Don is a member of the Marketing group, which has permissions to view the properties of the user object. You can prevent Don from viewing the properties of the user object by explicitly denying Read permission to him.

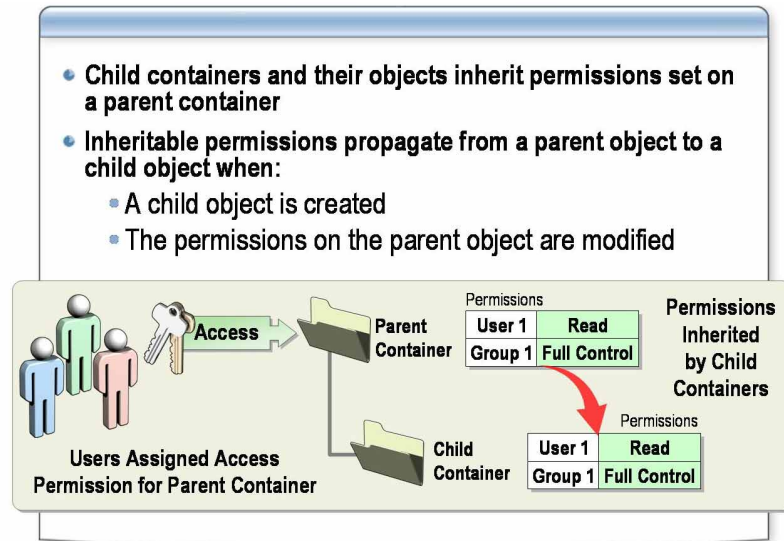
Standard and special permissions

Most Active Directory object permissions tasks can be configured through standard permissions. These permissions are the most commonly used, however if you need to grant a finer level of permissions, you will use special permissions.

Inherited permissions

When permissions are set on a parent object, new objects inherit the permissions of the parent. You can remove inherited permissions, but you can also re-enable them if you want to.

Permissions Inheritance for Active Directory Object Permissions



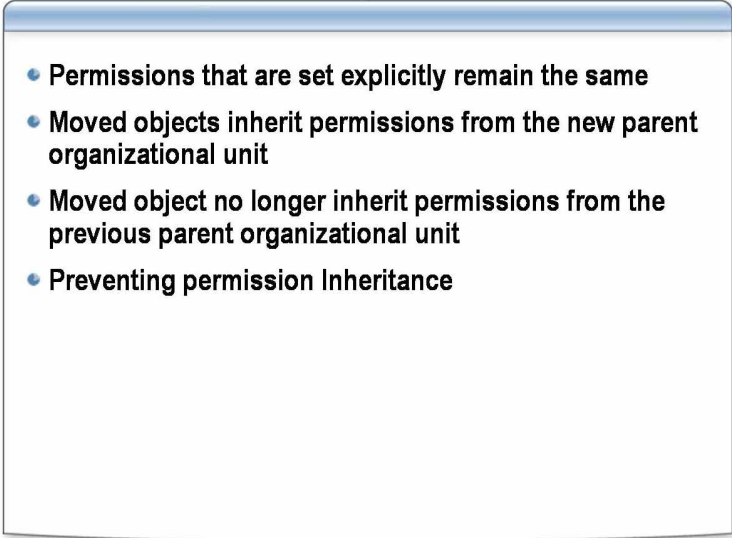
Benefits of permissions inheritance

A parent object is any object that has a relationship with another object called a child. A child object inherits permissions from the parent object. Permissions inheritance in Active Directory minimizes the number of times that you need to grant permissions for objects.

Permissions inheritance in Windows Server 2003 simplifies the task of managing permissions in the following ways:

- You do not need to apply permissions manually to child objects while they are created.
- The permissions applied to a parent object are applied consistently to all child objects.
- When you need to modify permissions for all objects in a container, you only need to modify the permissions for the parent object. The child objects automatically inherit those changes.

Effects of Modifying Objects on Permissions Inheritance

- 
- Permissions that are set explicitly remain the same
 - Moved objects inherit permissions from the new parent organizational unit
 - Moved object no longer inherit permissions from the previous parent organizational unit
 - Preventing permission Inheritance

Introduction

Modifying Active Directory objects affects permissions inheritance. As a systems administrator, you will be asked to move objects between organizational units in Active Directory when organizational or administrative functions change. When you do this, the inherited permissions will change. It is imperative that you are aware of these consequences prior to modifying Active Directory objects.

Effects of moving objects

When you move objects between organizational units, the following conditions apply:

- Permissions that are set explicitly remain the same.
- An object inherits permissions from the organizational unit that it is moved to.
- An object no longer inherits permissions from the organizational unit that it is moved from.

Note When modifying Active Directory objects, you can move multiple objects at the same time.

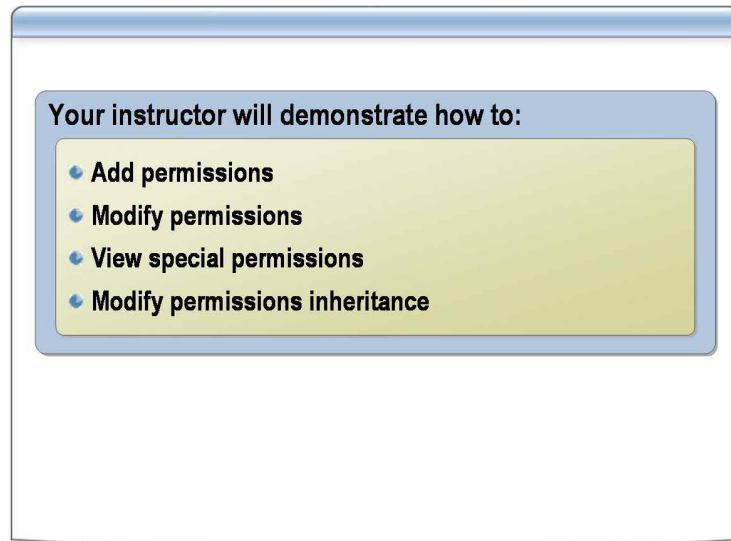
Preventing permissions inheritance

You can prevent permissions inheritance so that a child object does not inherit permissions from its parent object. When you prevent inheritance, only the permissions that you set explicitly apply.

When you prevent permissions inheritance, the Windows Server 2003 family enables you to:

- Copy inherited permissions to the object. The new permissions are explicit permissions for the object. They are a copy of the permissions that the object previously inherited from its parent object. After the inherited permissions are copied, you can make any necessary changes to the permissions.
- Remove inherited permissions from the object. By removing these permissions, you eliminate all permissions for the object. Then, you can grant any new permission that you want for the object.

How to Modify Permissions for Active Directory Objects



Introduction

Windows Server 2003 determines if a user is authorized to use an object by checking the permissions granted to the user for that object, which are listed in the DACL. When you allow or deny permissions for an object, those settings override permissions inherited from a parent object.

Procedure for adding permissions

To add permissions for an object:

1. If **Advanced Features** is not already checked, in **Active Directory Users and Computers**, on the **View** menu, click **Advanced Features**.
2. In the console tree, right-click the object, and then click **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, click **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, in the **Name** box, type the name of the user or group to which you want to grant permissions, and then click **OK**.

Procedure for modifying permissions

To modify an existing permission:

1. If **Advanced Features** is not already checked, in **Active Directory Users and Computers**, on the **View** menu, click **Advanced Features**.
2. In the console tree, right-click the object, and then click **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, in the **Permissions** box, select the **Allow** or **Deny** check box for each permission that you want to allow or deny.

Procedure for viewing special permissions

Standard permissions are sufficient for most administrative tasks. However, you may need to view the special permissions that constitute a standard permission.

To view special permissions:

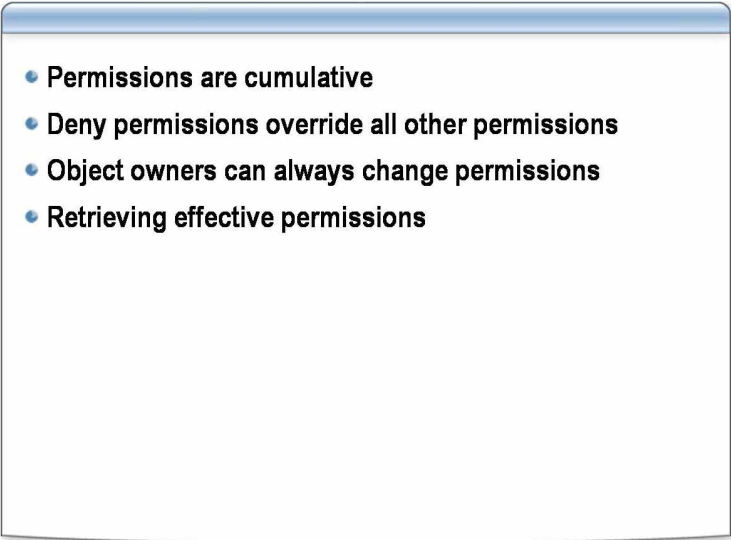
1. In the **Properties** dialog box for the object, on the **Security** tab, click **Advanced**.
2. In the **Advanced Security Settings** dialog box, on the **Permissions** tab, click the entry that you want to view, and then click **Edit**.
3. To view the permissions for specific attributes, in the **Permission Entry** dialog box, click the **Properties** tab.

Procedure for modifying permission inheritance

To modify permissions inheritance:

1. In the **Properties** dialog box for the object, on the **Security** tab, click **Advanced**.
2. In the **Advanced Security Settings** dialog box, on the **Permissions** tab, click the entry that you want to view, and then click **Edit**.
3. In the **Permission Entry** dialog box, on the **Object** tab, in the **Apply onto** box, select the option that you want.

What Are Effective Permissions for Active Directory Objects?

- 
- Permissions are cumulative
 - Deny permissions override all other permissions
 - Object owners can always change permissions
 - Retrieving effective permissions

Introduction

You can use the Effective Permissions tool to determine what the permissions for an Active Directory object are. The tool calculates the permissions that are granted to the specified user or group and takes into account the permissions that are in effect from group memberships and any permissions inherited from parent objects.

Characteristics

Effective permissions for Active Directory objects have the following characteristics:

- Cumulative permissions are the combination of Active Directory permissions granted to the user and group accounts.
- Deny permissions override all inherited permissions. Permissions explicitly assigned take priority.
- Every object has an owner, whether in an NTFS volume or Active Directory. The owner controls how permissions are set on the object and to whom permissions are granted.

By default, in Windows Server 2003, the owner is the Administrators group. The owner can always change permissions for an object, even when the owner is denied all access to the object.

The current owner can grant the Take ownership permission to another user, which enables that user to take ownership of that object at any time. The user must actually take ownership to complete the transfer of ownership.

Retrieving effective permissions

To retrieve information about effective permissions in Active Directory, you need the permission to read membership information. If the specified user or group is a domain object, you must have permission to read the object's membership information on the domain. The following users have relevant default domain permissions:

- Domain administrators have permission to read membership information on all objects.
- Local administrators on a workstation or stand-alone server cannot read membership information for a domain user.
- Authenticated domain users can read membership information only when the domain is in pre-Windows 2000 compatibility mode.

How to Determine Effective Permissions for Active Directory Objects



Your instructor will demonstrate how to determine effective permission for Active Directory objects

Introduction

Use the following procedure to view the effective permissions log for Active Directory objects.

Procedure

To view the effective permissions log:

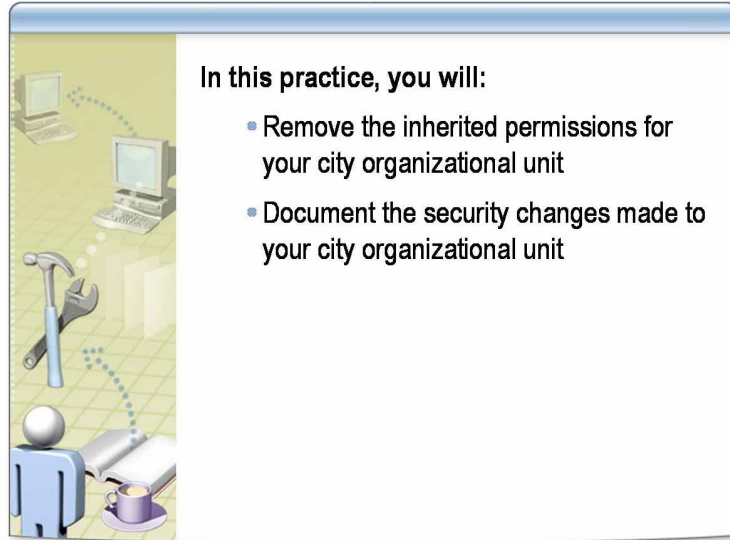
1. In Active Directory Users and Computers, in the console tree, browse to the organizational unit or object for which you want to view effective permissions.
2. Right-click the organizational unit or object, and then click **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
4. In the **Advanced Security Settings** dialog box, on the **Effective Permissions** tab, click **Select**.
5. In the **Select User, Computer, or Group** dialog box, in the **Enter the object name to select** box, enter the name of a user or group, and then click **OK**.

The selected check boxes indicate the effective permissions of the user or group for that object.

Additional reading

For more information about effective permissions, see “Effective Permissions tool” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/acl_effective_perm.asp.

Practice: Modifying Permissions for Active Directory Objects



Objective

In this practice, you will:

- Remove the inherited permissions for your city organizational unit.
- Document the security changes made to your city organizational unit.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains Active Directory Users and Computers.
- Ensure that you are viewing the advanced features of Active Directory Users and Computers.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

The system engineer for Northwind Traders has delegated administrative control to administrators at each *ComputerName* location. You need to determine what permissions are being inherited to your *ComputerName* organizational unit, and then remove all inherited permissions. Document the results of each step of the removal of inherited permissions.

Practice**► Document the security for your city organizational unit**

1. Open Active Directory Users and Computers.
2. View the security settings for your *ComputerName* organizational unit by doing the following:
 - a. Right-click your *ComputerName* organizational unit, and then click **Properties**.
 - b. In the **Properties** dialog box, click the **Security** tab.
3. Document the group or users names that have inherited or explicit permissions in the following table. Write a Y for yes under Inherited or Explicit for each item in the Group or user names column.

An explicit permission has a selected check box under **Allow** or **Deny**. Unchangeable and inherited permissions have a shaded selected check box under **Allow** or **Deny**.

Group or user names	Inherited	Explicit
Example: Account Operators	Y	
Account Operators	Y	
Administrators	Y	
Authenticated Users		Y
DL <i>ComputerName</i> OU Administrators		Y
Domain Admins		Y
Enterprise Admins	Y	
ENTERPRISE DOMAIN CONTROLLERS		Y
Pre-Windows 2000 Compatible Access	Y	
Printer Operators	Y	
System		Y

► Remove inherited permissions

1. In **Properties** dialog box for your city organizational unit, click **Advanced**.
2. In the **Advanced Security Settings** dialog box, on the **Permissions** tab, clear the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.** check box.
3. In the security dialog box, click **Remove**.
4. In the **Advanced Security Settings** dialog box, click **OK**.

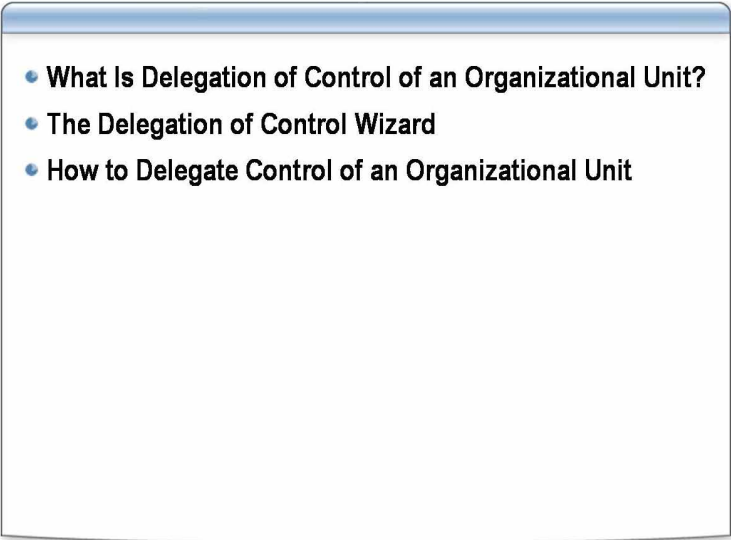
► **Document the security changes for your city organizational unit**

1. Open Active Directory Users and Computers.
2. View the security settings for your *ComputerName* organizational unit by doing the following:
 - a. Right-click your *ComputerName* organizational unit, and then click **Properties**.
 - b. In the **Properties** dialog box, click the **Security** tab.
3. Document the group or users names that have inherited or explicit permissions in the following table. Write a Y for yes under Inherited or Explicit for each item in the Group or user names column.

An explicit permission has a selected check box under **Allow** or **Deny**. Unchangeable and inherited permissions have a shaded selected check box under **Allow** or **Deny**.

Group or user names	Inherited	Explicit
Example: Account Operators	Y	
Account Operators	Y	
Administrators		
Authenticated Users		Y
DL <i>ComputerName</i> OU Administrators		Y
Domain Admins		Y
Enterprise Admins		
ENTERPRISE DOMAIN CONTROLLERS		Y
Pre-Windows 2000 Compatible Access		
Printer Operators	Y	
System		Y

Lesson: Delegating Control of Organizational Units

- 
- What Is Delegation of Control of an Organizational Unit?
 - The Delegation of Control Wizard
 - How to Delegate Control of an Organizational Unit

Introduction

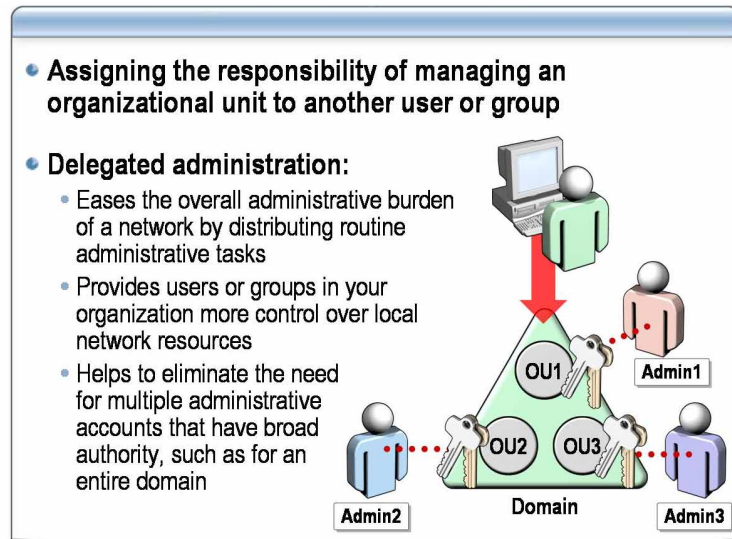
Active Directory enables you to efficiently manage objects by delegating administrative control of the objects. You can use the Delegation of Control Wizard and customized consoles in Microsoft Management Console (MMC) to grant specific users the permissions to perform various administrative and management tasks.

Lesson objectives

After completing this lesson, you will be able to:

- Describe what it means to delegate control of an organizational unit.
- Describe the purpose and function of the Delegation of Control Wizard.
- Delegate control of an organizational unit by using the Delegation of Control Wizard.

What Is Delegation of Control of an Organizational Unit?



Definition

Delegation of control is the ability to assign the responsibility of managing Active Directory objects to another user, group, or organization. By delegating control, you can eliminate the need for multiple administrative accounts that have broad authority.

You can delegate the following types of control:

- Permissions to create or modify objects in a specific organizational unit
- Permissions to modify specific attributes of an object, such as granting the permission to reset passwords on a user account

Why delegate administrative control?

Delegated administration in Active Directory helps ease the administrative burden of managing your network by distributing routine administrative tasks to multiple users. With delegated administration, you can assign basic administrative tasks to regular users or groups and assign domain-wide and forest-wide administrative tasks to trusted users in your Domain Admins and Enterprise Admins groups.

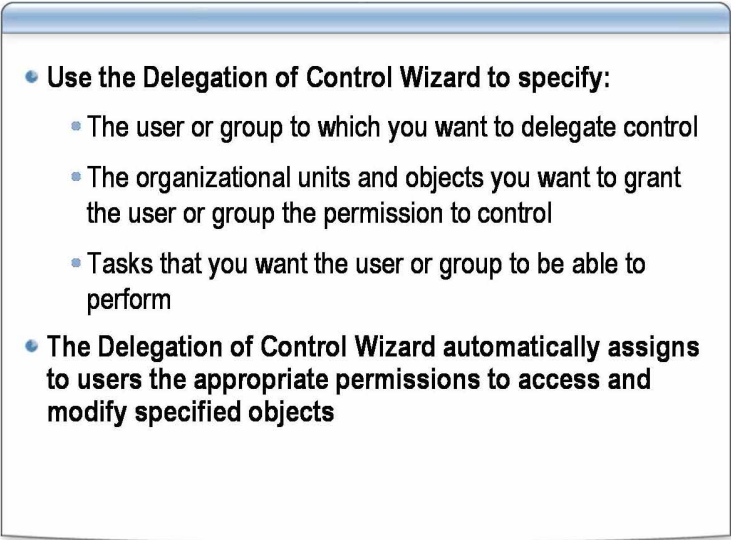
By delegating administration, you give groups in your organization more control of their local network resources. You also help secure your network from accidental or malicious damage by limiting the membership of administrator groups.

Ways to define the delegation of administrative control

You define the delegation of administrative control in the following three ways:

- Change properties for a particular container.
- Create and delete objects of a specific type under an organizational unit, such as users, groups, or printers.
- Update specific properties on objects of a specific type under an organizational unit. For example, you can delegate the permission to set a password on a user object or all objects in an organizational unit.

The Delegation of Control Wizard

- 
- Use the Delegation of Control Wizard to specify:
 - The user or group to which you want to delegate control
 - The organizational units and objects you want to grant the user or group the permission to control
 - Tasks that you want the user or group to be able to perform
 - The Delegation of Control Wizard automatically assigns to users the appropriate permissions to access and modify specified objects

Introduction

You use the Delegation of Control Wizard to select the user or group to which you want to delegate control. You also use the wizard to grant users permissions to control organizational units and objects and to access and modify objects.

Delegate permissions

You can use the Delegation of Control Wizard to grant permissions at the organizational unit level. You must manually grant additional specialized permissions at the object level.

In Active Directory Users and Computers, right-click the organizational units that you want to delegate control for, and then click **Delegate control** to start the wizard. You can also select the organizational unit and then click Delegate control on the Action menu.

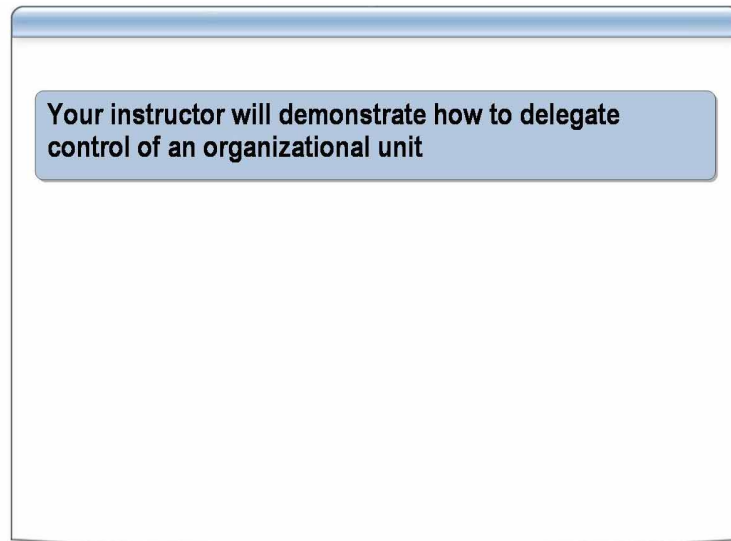
Options

The following table describes the options in the Delegation of Control Wizard.

Option	Description
Users or Groups	The user accounts or groups to which you want to delegate control.
Tasks to Delegate	A list of common tasks, or the option to customize a task. When you select a common task, the wizard summarizes your selections to complete the delegation process. When you choose to customize a task, the wizard presents Active Directory object types and permissions for you to choose from.
Active Directory Object Type	Either all objects or only specific types of objects in the specified organizational unit.
Permissions	The permissions to grant for the object or objects.

Note The Delegation of Control Wizard can append permissions to an organizational unit if it is run more than once. However, you must manually remove delegated permissions.

How to Delegate Control of an Organizational Unit



Introduction

To grant permissions at the organizational unit level, use the Delegation of Control Wizard. You can grant permissions for managing objects, or you can grant permissions for managing specific attributes of those objects. Using the Delegation of Control Wizard is the preferred method for delegating control, because it reduces the possibility of unwanted effects from permission assignments.

Procedure for delegating control for common tasks

To delegate administrative control for common tasks:

1. Start the Delegation of Control Wizard, by performing the following steps:
 - a. In Active Directory Users and Computers, click the organizational unit for which you want to delegate control.
 - b. On the **Action** menu, click **Delegate control**.
2. In the Delegation of Control Wizard, on the **Welcome** page, click **Next**.
3. On the **Users or Groups** page, select a user or group to which you want to grant permissions, and then click **Next**. If there are not Users or Groups displayed to select from, do the following:
 - a. Click **Add**.
 - b. In the Select Users, Computers or Groups dialog box, in the Enter the object names to select box, type the name of a user or group, and then click **OK**.

4. On the **Tasks to Delegate** page, specify one or more of the following tasks to delegate:
 - Create, delete, and manage user accounts
 - Reset user passwords and force password change at next logon
 - Read all user information
 - Create, delete, and manage groups
 - Modify the membership of a group
 - Manage Group Policy links

Note You can delegate a custom task to users or groups by clicking **Create a custom task to delegate**.

5. Click **Next**.
6. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

Procedure for delegating control for a custom task

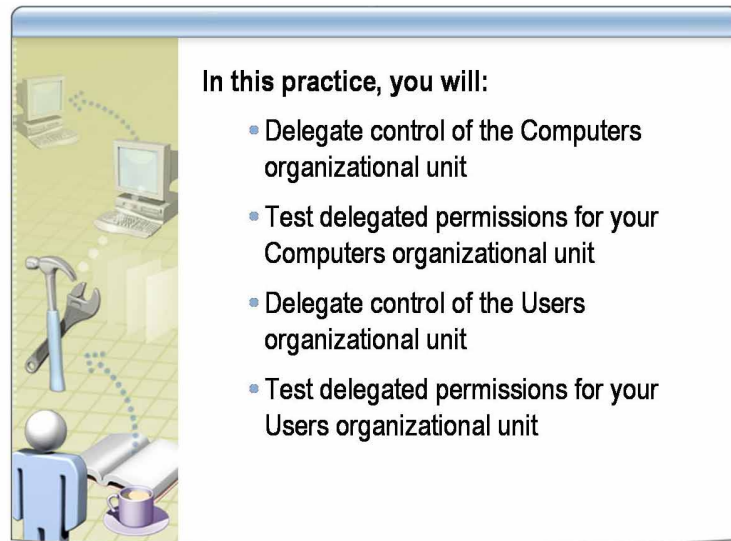
To delegate administrative control for a custom task:

1. Start the Delegation of Control Wizard, by performing the following steps:
 - a. In Active Directory Users and Computers, click the organizational unit for which you want to delegate control.
 - b. On the **Action** menu, click **Delegate control**.
2. In the Delegation of Control Wizard, on the **Welcome** page, click **Next**.
3. On the **Users or Groups** page, select a user or group to which you want to grant permissions, and then click **Next**.
4. On the **Tasks to Delegate** page, click **Create a custom task to delegate**, and then click **Next**.
5. On the **Active Directory Object Type** page, click **Next**.
6. On the **Permissions** page, specify the permissions that you want to grant to the organizational unit or its objects.

You can select the following types of permissions:

- *General*. Displays the most commonly used permissions that are available for the selected organizational unit or the objects in the organizational unit.
 - *Property specific*. Displays all attribute permissions applicable to the type of object.
 - *Creation/deletion of specific child object*. Displays permissions that you need to create new objects in the organizational unit.
7. Click **Next**.
 8. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

Practice: Delegating Control of an Organizational Unit



In this practice, you will:

- Delegate control of the Computers organizational unit
- Test delegated permissions for your Computers organizational unit
- Delegate control of the Users organizational unit
- Test delegated permissions for your Users organizational unit

Objective

In this practice, you will:

- Delegate control of the Computers organizational unit.
- Test delegated permissions for your Computers organizational unit.
- Delegate control of the Users organizational unit.
- Test delegated permissions for your Users organizational unit.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains Active Directory Users and Computers.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

To distribute the workload among administrators, Northwind Traders wants administrators to be able to do specific tasks in their designated organizational units. The following tasks must be delegated in the following organizational units:

- Organizational unit: *Locations/ComputerName/Computers*
Task: Create and delete computer accounts in the organizational unit
- Organizational unit: *Locations/ComputerName/Users*
Task: Reset user passwords and force password change at next logon
Task: Read all user information

Practice**► Delegate control of the Computers organizational unit**

1. In Active Directory Users and Computers, in the console tree, navigate to your *ComputerName* organizational unit, right-click **Computers**, and then click **Delegate Control**.
2. In the Delegation of Control Wizard, on the **Welcome** page, click **Next**.
3. On the **Users or Groups** page, add *ComputerNameUser*, and then click **Next**.
4. On the **Tasks to Delegate** page, click **Create a custom task to delegate**, and click **Next**.
5. On the **Active Directory Object Type** page, click **Only the Following Objects in the Folder**, and then select the **Computer objects** check box.
6. Select the **Create selected objects in this folder** and **Delete selected objects in this folder** check boxes, and then click **Next**.
7. On the **Permissions** page, select the **General** check box.
8. Under **Permissions**, select the **Read** and **Write** check boxes, and then click **Next**.
9. On the **Completing the Delegation of Control Wizard**, click **Finish**.

► Test permissions for the Computers organizational unit

1. Close CustomMMC, and then open it again without using the **Run as** command.
2. In Active Directory Users and Computers, create a computer account by using the following parameters:
 - Location: *Locations/ComputerName/Computers*
 - Computer account name: First three letters of the city and **Test** (Example: LonTest)

You should be able to create a computer account in the *Locations/ComputerName/Computers* organizational unit.

3. Close Active Directory Users and Computers.

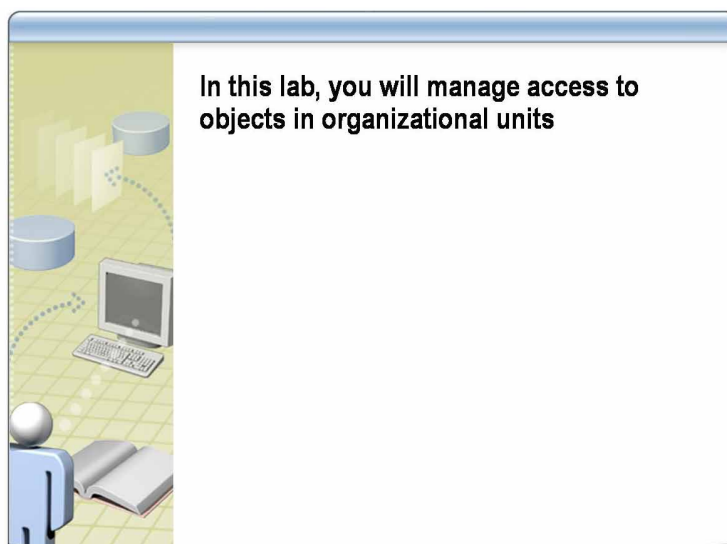
► Delegate control of the Users organizational unit

1. Open Active Directory Users and Computers with the **Run As** command by using the *ComputerNameAdmin* account.
2. Navigate to your *ComputerName* organizational unit, right-click **Users**, and then click **Delegate Control**.
3. In the **Delegation of Control Wizard**, on the Welcome page, click **Next**.
4. On the **Users of Groups** page, add *ComputerNameUser* and then click **Next**.
5. Delegate the following common tasks:
 - Reset user passwords and force password change at next logon
 - Read all user information
6. Click **Next**, and then click **Finish**.

► **Test your permissions for the Users organizational unit**

1. Close CustomMMC, and then open it again without using the **Run as** command.
2. In Active Directory Users and Computers, navigate to the Locations/ComputerName/Users organizational unit.
3. Try to delete a user account.
You should be unsuccessful.
4. Try to enable or disable any user account.
You should be unsuccessful.
5. Reset any user's password.
You should be able to reset any user accounts password in the Locations/ComputerName/Users organizational unit.

Lab A: Managing Access to Objects in Organizational Units



Objectives

After completing this lab, you will be able to manage access to objects in organizational units.

Instructions

Before you begin this lab:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains Active Directory Users and Computers.

**Estimated time to
complete this lab:**
15 minutes

Exercise 1

Delegating Administrative Control

In this exercise, you will delegate administrative control of objects in an organizational unit.

Scenario

Northwind Traders wants all IT personnel to be able to create, delete, and modify groups in every city organizational unit. You must delegate authority in your *ComputerName* organizational unit to enable a global group named G NWTraders IT Personnel to have permissions to Create, delete and manage groups and to Modify membership of a group.

Tasks	Specific instructions
1. Delegate control of the <i>ComputerName</i> /Groups organizational unit.	<ul style="list-style-type: none">▪ Organizational unit: nwtraders.msft/Locations/<i>ComputerName</i>/Groups▪ Users or Groups: G NWTraders IT Personnel▪ Tasks to Delegate:<ul style="list-style-type: none">• Create, delete, and manage groups• Modify the membership of a group

Exercise 2

Documenting Security of an Active Directory Object

In this exercise, you will document the security settings of the object created in the delegated organizational unit.

Scenario

You have just created many groups in a delegated organizational unit, and you have been asked to document what permissions one of those groups has inherited. Enter information in the following table to document the permissions of the group.

Tasks	Detailed steps
1. Document the special permissions for a group created in a delegated organizational unit.	<ul style="list-style-type: none">▪ Document the special permissions for the group G NWTraders IT Personnel. _____

