MICROSOFT
TRAINING
AND CERTIFICATION

Microsoft Official Curriculum

Module 3: Securing a Windows 2000 Network

Contents

Microsoft

Project Lead: Red Johnston
Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)
Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.),
Jay Johnson (The Write Stuff)**,** Sonia Pande (NIIT (USA) Inc.)
Lead Program Manager: Jim Cochran (Volt)
Program Manager: Jamie Mikami (Volt)
Technical Contributors: Rodney Miller, Gregory Weber (Volt)
Testing Leads: Sid Benavente, Keith Cotton
Testing Developer: Greg Stemp (S&T OnSite)
Simulation Developer: Wai Chan (Meridian Partners Ltd.)
Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)
Graphic Artist: Julie Stone (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Patricia Rytkonen (The Write Stuff)
Copy Editor: Kaarin Dolliver (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: Eric Brandt (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Testing: Data Dimensions, Inc.
Production Support: Ed Casper (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
60 Minutes

Labs:
45 Minutes

This module provides students with a description of how Microsoft® Windows® 2000 protects network resources from unauthorized access. The module describes how the use of user accounts, passwords, and groups provides a secure network environment and how rights are granted to users and groups. The module also discusses permissions on files, folders, and printers.

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

- Describe the role and purpose of different types of user accounts.
- Describe the role and purpose of different types of groups.
- Identify common user and group rights.
- Describe file, folder, and shared folder permissions.

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 2151A_03.ppt
- Module 3, "Securing a Windows 2000 Network"

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Read the white paper, *Enterprise Class Storage in Windows 2000*, on the Trainer Materials compact disc.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- User Accounts

  Provide an overview of the different types of user accounts and their functions. Then introduce the tools used to create and modify the different types of user accounts.

- Groups

  Define a group and describe how groups are used in a Microsoft Windows 2000 network. Explain the difference between groups located on computers that are domain controllers and groups located on computers that are not domain controllers.

- User Rights

  Provide an overview of user rights. Then explain some of the common rights available in Windows 2000. Conclude by explaining how built-in groups are granted certain rights by default.

- Permissions

  Explain how assigning permissions can control the type of access users have to network resources. Describe the objects to which you can apply permissions (printers, files and folders) and the different permissions that you can apply to each.

Customization Information

This section identifies the lab setup requirements for a 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 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

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

Overview

Slide Objective
To provide an overview of the module topics and objectives

Lead-in
User accounts, groups, rights, and permissions are ways to establish security in a Windows 2000 network.

- **User Accounts**
- **Groups**
- **User Rights**
- **Permissions**

To protect network resources from unauthorized access, the identity of each user accessing the network must be verified when logging on. Each user must have a valid account name and correct password. The account name identifies each unique user in a domain. The password keeps the use of that account private, so that only users who know the password can use the account. After the user's identity is verified, the user's access to computers on the network is authenticated.

To facilitate network administration, you can organize users into groups and assign permissions to these groups to access network resources. You can control the kinds of actions users perform on the network by granting appropriate user rights.

To further ensure security, you can protect network resources with file, folder, and shared folder permissions.

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

- Describe the role and purpose of different types of user accounts.
- Describe the role and purpose of different types of groups.
- Identify common user rights and rights for each built-in group.
- Describe file, folder, and shared folder permissions.

User Accounts

Slide Objective
To introduce the concepts of local and domain user accounts.

Lead-in
In a Windows 2000 network, there are two kinds of user accounts: local user accounts and domain user accounts.

- Local User Accounts
- Domain User Accounts

User accounts enable individual users to access network resources. A user account is the user's unique set of credentials that is recognized by the network. An administrator creates user accounts for each person who regularly uses the network. The administrator also assigns and maintains user names and passwords for each user account. Microsoft® Windows® 2000 provides two types of user accounts: local user accounts and domain user accounts.

With a local user account, an account is created in the local security database, which gives the user the ability to log on to a specific computer and gain access to resources on that computer. This typically occurs in a workgroup. If the computer is a member of a workgroup, the account is stored on the local computer. With this account, a user has access to only the resources on that computer.

With a domain user account, a user can log on to the domain to access network resources. A user with a domain account can access all of the resources in the domain.

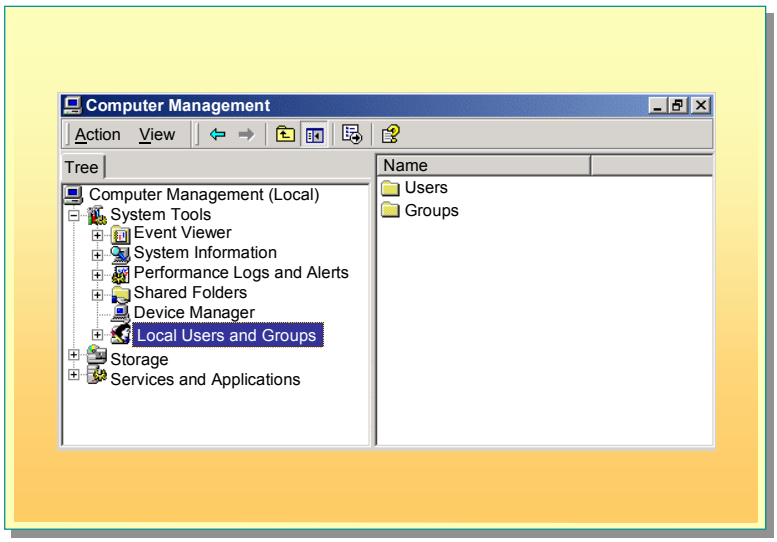
In a domain, it is possible to have both a domain user account and a user account on the local computer. An administrator can create these accounts, which are called user-defined accounts. A user's account can be stored in one of two places: the local security database if the computer is not a domain controller or in the Microsoft Active Directory™ directory service.

In addition to the user-defined user accounts, Windows 2000 provides two default built-in user accounts. These accounts can be used to perform administrative tasks or to gain temporary access to network resources. There are built-in user accounts for both local computers and domains.

Local User Accounts

Slide Objective
To describe the use of local user accounts.

Lead-in
A person with a local user account can gain access only to the resources of a specific computer.



To gain access to resources on a local computer, a user needs to have a local user account on the computer. There are two kinds of local user accounts: user-defined accounts and built-in accounts. When an account is created, it exists only in the local security database on that computer.

Delivery Tip
Remind the students that there are differences between a workgroup and a domain and that there are different tools for administering each.

User-defined Local User Accounts

User-defined local user accounts are those that an administrator creates to allow a user to gain access to only those computers where his or her user account exists. You can create local user accounts on member servers and computers running Microsoft Windows 2000 Professional, but not on computers that are domain controllers. A local user account is used only on stand-alone computers or on computers in a small network environment, such as a workgroup. It is possible to have an account on the local computer and another account in the domain; however, the user can use only one of the accounts at a time. The user determines which account to use when logging on the computer.

Built-in (Local) User Accounts

In addition to allowing user-defined accounts, Windows 2000 provides two built-in user accounts to aid administrators in performing administrative tasks and in providing users with temporary access to a local computer. Upon installation, Windows 2000 automatically creates two built-in user accounts—Administrator and Guest.

Administrator

Administrators use the built-in Administrator user account to create an account for themselves on computers on which Windows 2000 has been newly installed. The built-in Administrator account can never be deleted or disabled, thereby ensuring that the administrator is never locked out of the computer. This account requires a password, which an administrator provides at the time of installation.

Guest

Users who do not have a user account on a computer can log on using the Guest account. A user whose account is disabled can also use the Guest account. For a user to log on as a Guest, the administrator needs to enable the Guest account because it is disabled by default. This account does not require a password.

Local Users and Groups Utility

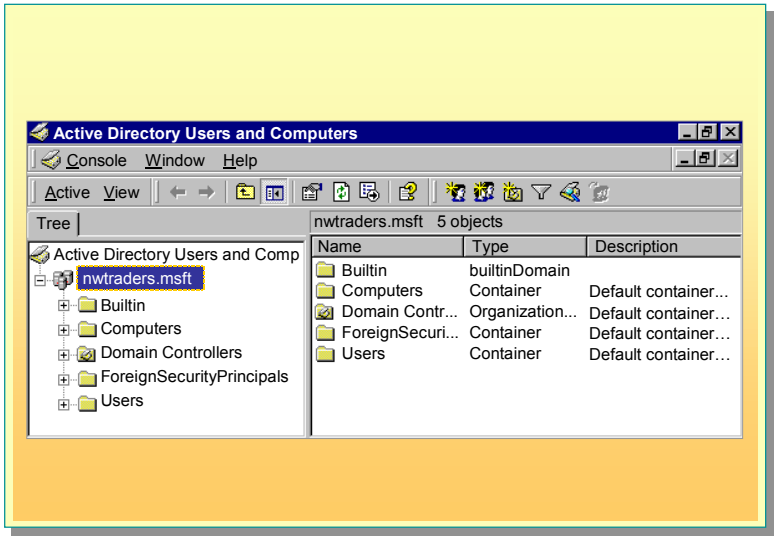
Windows 2000 provides a utility called Local Users and Groups that administrators can use to manage user accounts on a local computer. The Local Users and Groups utility is available on computers running Windows 2000 Professional and on member servers running Microsoft Windows 2000 Server. You can use the Local Users and Groups utility to perform the following tasks:

- Create a new user account or delete an existing user account
- Modify a user account by changing the user name or other account information, such as the password or description
- Reset the password for a user account
- Disable or enable a user account

Domain User Accounts

Slide Objective
To describe the use of domain user accounts.

Lead-in
A person with a domain user account can access the resources of the domain.



Delivery Tip
Refresh the students' memory by asking questions about what a domain is and what its features are.

A local user account allows a user to log on to a local computer to access local resources. However, in a network environment, users need to access resources located anywhere on the network. To access these resources, you need to use a domain user account. When a domain user account is created, it exists in Active Directory and is accessible from anywhere in the domain. By contrast, in a workgroup, the user account exists only on the local computer.

User-defined Domain Accounts

User-defined domain accounts are those that an administrator creates to allow users to log on to a domain and access resources anywhere on the network. User-defined domain accounts are created on a domain controller. The domain controller replicates the new user account information to all domain controllers in the domain. During the logon process, the user provides the user name and password and identifies the domain in which the account exists. The first available domain controller uses this information to validate the user account.

Built-in (Domain) User Accounts

In addition to allowing administrators to define new domain user accounts, Windows 2000 provides two built-in domain user accounts—Administrator and Guest. These built-in user accounts are similar to the built-in user accounts available on local computers in workgroups. The main difference is that these accounts enable access to the entire domain.

Administrator

The built-in Administrator account manages the overall computer and domain configuration. Using this account, an administrator can create and modify user accounts and groups, manage security, administer printers, and assign permissions to user accounts. You can rename this account, but you cannot delete it.

Guest

The built-in Guest account enables occasional users to access network resources. For example, in a low security environment, an employee who needs to access resources for a short time can use the Guest account. This account is disabled by default.

Active Directory Users and Computers Utility

Windows 2000 provides a utility called Active Directory Users and Computers that administrators can use to manage user accounts in Active Directory.

This utility is installed on computers configured as domain controllers. To use the Active Directory Users and Computers utility, you must be logged on to a Windows 2000 domain (not the local computer) and have sufficient permissions to perform the particular operation.

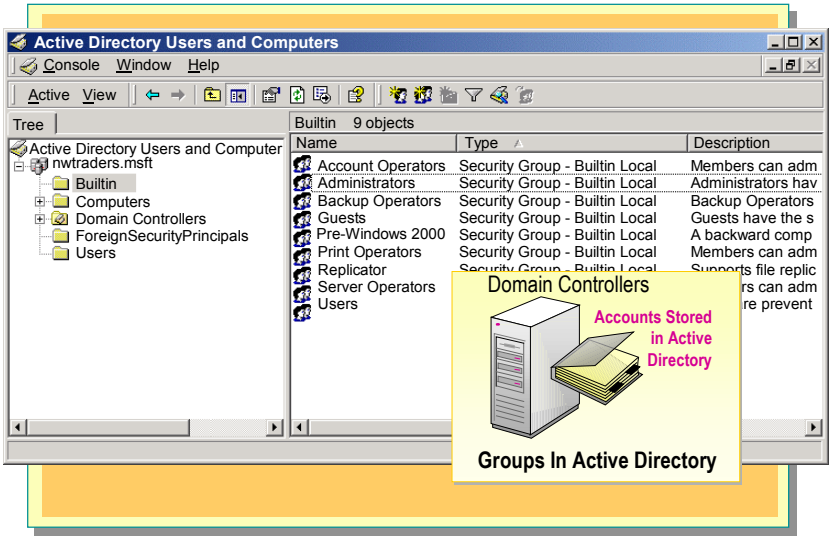
You can use the Active Directory Users and Computers utility to perform the following tasks in the domain:

- Add or delete user accounts
- Enable or disable user accounts
- Find or move user accounts
- Rename user accounts
- Reset user passwords

Groups

Slide Objective
To introduce the use of groups for Windows 2000 network administration.

Lead-in
You will find it easier to administer users by organizing them into groups.



A *group* is a collection of user accounts. You can assign access permission to all members of a group at one time, so that you do not need to assign the permissions individually. After you provide access to a group, you can simply add appropriate users to that group. You can use the default, or built-in, groups that Windows 2000 provides, or you can create new groups to meet your organization's needs.

A group can exist on a local computer only, on computers within a single domain, or on computers across multiple domains.

Groups on a Local Computer

On local computers (computers that are not domain controllers), you can create only local groups in the local security database. A group located on a computer that is not a domain controller provides security and access for the local computer only. For example, to grant administrative permissions on a local computer to a user, you add the user to the Administrators group on that computer by using the Local Users and Groups utility.

Groups on a Domain Controller

On a domain controller, you create groups in Active Directory. A group that exists on a domain controller can include users throughout the entire domain or across multiple domains. For example, to provide users with administrative privileges, you add them to the Administrators group on a domain controller by using the Active Directory Users and Computers utility.

Lab A: Examining Users and Groups

Slide Objective
To introduce the lab.

Lead-in
In this lab, you will identify the key properties of user and group accounts.

Objectives

After completing this lab, you will be able to:

- Identify key properties of user and group accounts.

Prerequisites

Before working on this lab, you must have:

- Experience logging on and off Microsoft Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1
Examining Domain User and Group Accounts

Scenario

You have been assigned the task of managing the Sales and Managers organizational units and need to find out which objects are contained in them. You will use Active Directory Users and Computers to view the organizational units.

Goal

In this exercise, you will examine the various organizational units that exist in the domain and record selected information about them.

Tasks	Detailed Steps
1. Open Active Directory Users and Computers, and determine which objects are contained in the Managers organizational unit.	**a.** Log on as Administrator with a password of **password**. **b.** Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. **c.** Maximize the Active Directory Users and Computers window. **d.** In the console tree, click **Managers**.
Examine the objects in the details pane of Active Directory Users and Computers. For which user accounts are you responsible? For which groups? **You are responsible for the user accounts Jae Pak and Kim Yoshida, and for the Managers group.**	
2. Determine which accounts are contained in the Sales organizational unit.	**a.** In the console tree, click **Sales**.
Examine the objects in the details pane of Active Directory Users and Computers. For which user accounts are you responsible? For which groups? **You are responsible for the user accounts Anne Paper and Don Hall, and for the Sales group.**	
3. Close all windows and log off from Windows 2000	**a.** Close all windows and log off from Windows 2000.

User Rights

Slide Objective
To introduce the concepts of user rights and of the rights assigned to built-in groups.

Lead-in
Rights apply to the entire system, rather than to a specific resource, and affect the overall operation of the computer or domain.

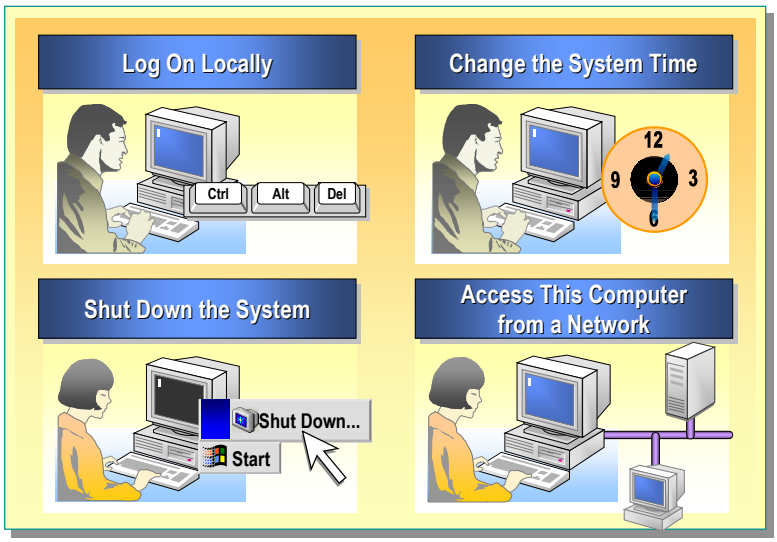
- Common User Rights
- Rights Assigned to Built-in Groups

Rights apply to the entire system, rather than to a specific resource, and affect the overall operation of the computer or domain. All users accessing network resources need to have certain common rights on the computers they use, such as the right to log on to the computer or change the system time of the computer. Administrators can grant specific common user rights to user groups or to individual users. Additionally, Windows 2000 grants certain rights to built-in groups by default. User rights determine which users can perform a specific task on a computer or in a domain.

Common User Rights

Slide Objective
To identify common user rights.

Lead-in
Rights authorize users to perform certain actions on the system.



A right authorizes a user who is logged on to a computer or a network to perform certain actions on the system. If a user does not have the appropriate rights to perform an action, attempts to carry out the action are blocked.

User rights can apply both to individual users and to groups. However, user rights are best administered on a group basis. This ensures that a user who logs on as a member of a group automatically receives the rights associated with that group. Windows 2000 allows an administrator to assign rights to users and user groups. Common user rights include the Log on locally user right, the Change the system time user right, the Shut down the system user right, and the Access this computer from a network user right.

- Log on locally

  This right allows a user to log on to the local computer or to the domain from a local computer.

- Change the system time

  This right allows a user to set the time for the internal clock of a computer.

- Shut down the system

  This right allows a user to shut down a local computer.

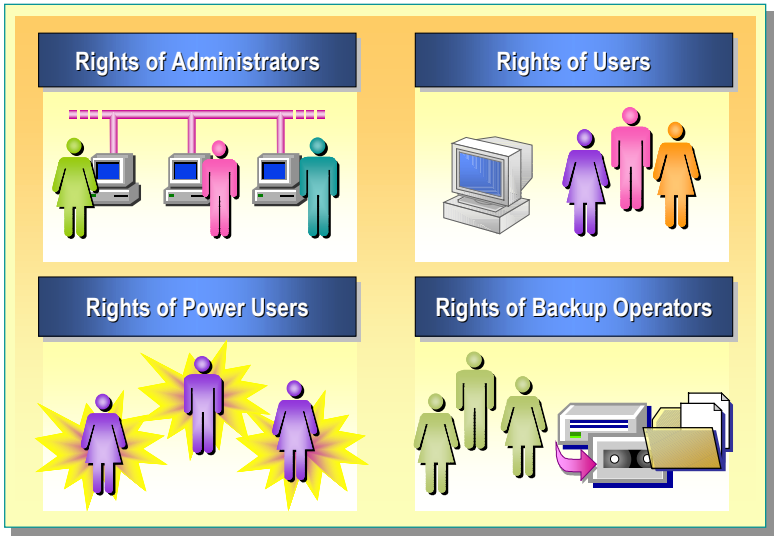
- Access this computer from a network

  This right allows a user to gain access to a computer running Windows 2000 from any other computer on the network.

Rights Assigned to Built-in Groups

Slide Objective
To identify the rights of built-in groups.

Lead-in
Built-in groups have certain rights by default.



By default, Windows 2000 grants certain rights to such built-in groups as Administrators, Users, Power Users, and Backup Operators.

Administrators

Administrators is a built-in group that exists both on computers that are domain controllers as well as on computers that are not domain controllers. Members of the Administrators group have full control over the computer or the domain. The Administrators group is the only built-in group that is automatically granted every built-in right in the system.

Users

Users is a built-in group that exists both on computers that are domain controllers as well as on computers that are not domain controllers. Members of the Users group can perform only those tasks for which they have been granted specific rights, such as running applications, using local and network printers, and shutting down and locking workstations. Members of the Users group can create local groups and can modify them, but they cannot share folders or create local printers.

Power Users

Power Users is a built-in group that exists on computers that are not domain controllers. Members of the Power Users group may perform specific administrative functions, but they do not have rights that grant them complete control over the system. Rights of the Power Users group include:

- Creating user accounts and groups on the local computer.
- Modifying and deleting the accounts that they create.
- Sharing resources.

However, members of the Power Users group cannot:

- Modify the Administrators or Backup Operators groups.
- Back up or restore folders.

Backup Operators

Backup Operators is a built-in group existing both on computers that are domain controllers and on computers that are not domain controllers. Members of the Backup Operators group can back up and restore files on the computer, regardless of the permissions that protect those files. Members of the Backup Operators group can also log on to the computer and shut down the computer, but they cannot alter security settings.

Lab B: Examining User Rights

Slide Objective
To introduce the lab.

Lead-in
In this lab, you will examine user rights.

Objectives

After completing this lab, you will be able to:

- Describe the effect user rights has on user accounts.

Prerequisites

Before working on this lab, you must have:

- Experience logging on and off Microsoft Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1
Verifying User Rights

Scenario

Another administrator has created several user accounts for your domain. You now need to test the effects of the user rights assigned to those user accounts.

Goal

In this exercise, you will log on as two different users and test to see whether the users have specific user rights granted to them.

Tasks	Detailed Steps
1. Log on as Kimyo with a password of **password**. Attempt to change the system time.	**a.** Log on to the computer using the following credentials: Username: **kimyo** Password: **password** Domain: *domainname* (where *domainname* is the name of your domain). **b.** Click **Start**, point to **Settings**, and then click **Control Panel**. **c.** In Control Panel, double-click **Date/Time**.
What message appears when you try to change the system time? Why? **You do not have the proper privilege level to change the system time.** **Because the user Kimyo does not have the user right to change the system time.**	
2. Attempt to run the Add/Remove Hardware wizard.	**a.** In Control Panel, double-click **Add/Remove Hardware**.
Does the user Kimyo have the right to add new hardware using the Add/Remove Hardware wizard? Why might you want to restrict this right? **No.** **To prevent unauthorized users from making critical changes to the system, which can affect system operation and performance.**	

(*continued*)

Tasks	Detailed Steps
3. Attempt to log on as user Donha.	**a.** Log off the computer. **b.** Log on to the computer using the following credentials: Username: **donha** Password: **password** Domain: *domainname.***nwtraders.msft** (where *domainname* is the name of your domain).
Can Donha log on to the computer? Why or why not? **No. Donha does not have the right to log on interactively.**	
4. Close the message box.	**a.** Click **OK** to close the message box.

Permissions

Slide Objective
To introduce the use of permissions in a network.

Lead-in
You use permissions to control user access to network resources.

- Introduction to Permissions
- NTFS File Permissions
- NTFS Folder Permissions
- Shared Folder Permissions
- Printer Permissions

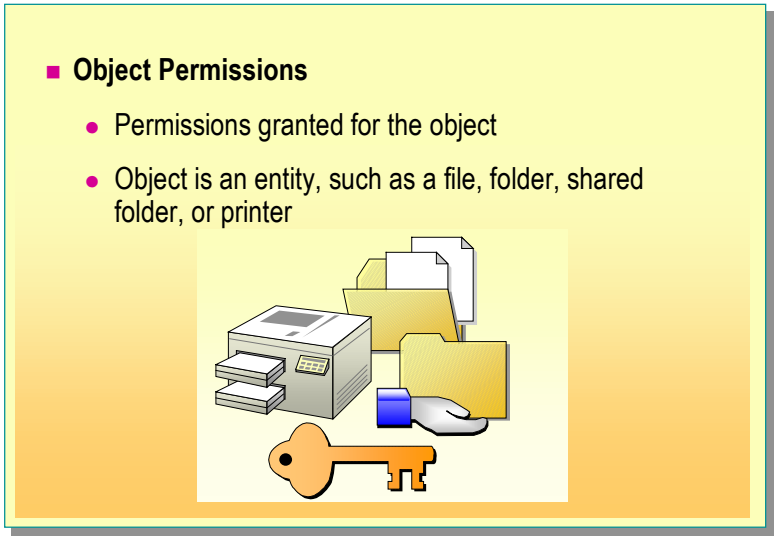
When you provide access to file resources on a computer running Windows 2000, you can control who has access to resources and the nature of their access by assigning the appropriate permissions. Permissions define the type of access assigned to a user or group for any resource. For example, users in the human resources (HR) department of an organization might need to modify the company's HR policies document. To facilitate this, the administrator needs to assign the appropriate permission to the members of the HR department.

In order to assign permissions to individual files and folders, Windows 2000 uses the NTFS file system. You can also control the permissions assigned to users for accessing shared folder resources and network printers.

Introduction to Permissions

Slide Objective
To describe object permissions.

Lead-in
Permissions are used to control who has access to objects in the network and define what type of access is allowed.
Permissions to access an object may be assigned to either a user or a group.



Permissions define the type of access a user or a group has to an object. The type of permissions that you can assign to a user depends on the type of object.

Object Permissions

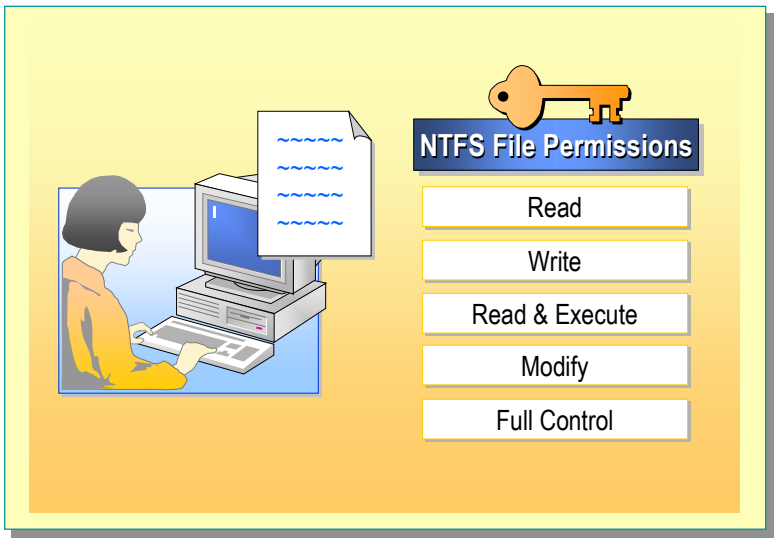
An object is defined as an entity, such as a file, folder, shared folder, or printer. The permissions that are assigned to a user for the objects are called object permissions.

You can assign permissions for objects in Active Directory or on a local computer. When assigning permissions, it is best to assign permissions to a group of users instead of to individual users. Using groups in this way eases the task of managing permissions on objects.

NTFS File Permissions

Slide Objective
To describe NTFS file permissions.

Lead-in
You can use NTFS file permissions to control user access to files on an NTFS partition.



Delivery Tip
Demonstrate how to view NTFS file permissions. At this point it is not necessary to explain the details of how to set the permissions.

NTFS file permissions control access to individual files by specifying which users can access them and what kind of access the users can have.

Note For more information about NTFS, see *File and Print Services Technical Overview* under **Additional Reading** on the Web page on the Student Materials compact disc.

The following table lists the standard NTFS file permissions and the type of access that each permits, from the most restrictive to the least restrictive permissions.

NTFS file permission	Allows a user to
Read	Read the file and view file attributes, ownership, and permissions.
Write	Overwrite the file, change file attributes, and view file ownership and permissions.
Read & Execute	Run applications and perform the actions permitted by the Read permission.
Modify	Modify and delete the file and perform the actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, and perform the actions permitted by all other NTFS file permissions.

Verifying File Permissions

An administrator assigns permissions to a file from the **Security** tab of the **Properties** dialog box for the file. You can also view the current permissions to the file on the same tab.

To access the Security tab

1. In Windows Explorer, right-click the file.
2. Click **Properties**.
3. In the **Properties** dialog box, click the **Security** tab.

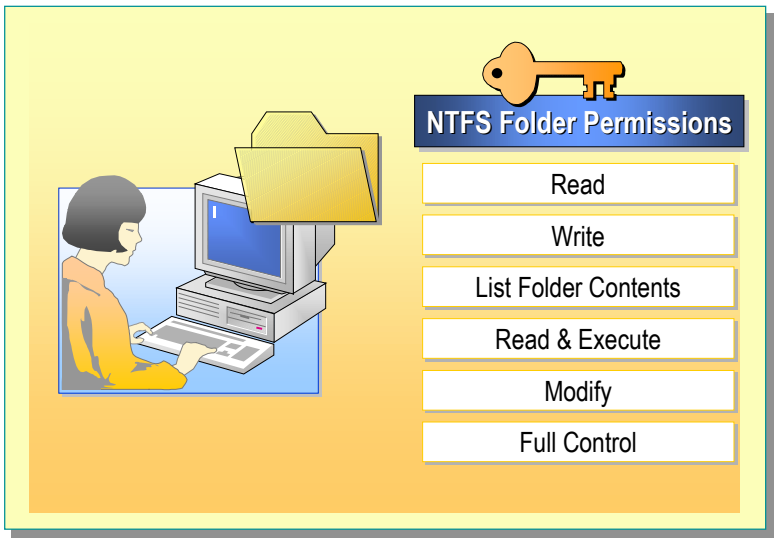
The **Security** tab consists of two sections—Name and Permissions. The Name section displays a list of existing users or groups who have permissions to the file. The Permissions section displays a list of permissions that you can grant or deny to the user or group.

You normally select the permissions that you want to grant. However, in some cases it may be easier to specify the permissions you want to deny. For example, although you allow everyone access to a file, you may need to restrict any users who connect to the resource using the Guest account. To do this, you deny permission to the Guest account.

NTFS Folder Permissions

Slide Objective
To describe NTFS folder permissions.

Lead-in
You can use NTFS folder permissions to control user access to folders on an NTFS partition.



Delivery Tip
Demonstrate the procedure for viewing NTFS folder permissions. Point out the permissions but do not explain how to set the permissions.

NTFS folder permissions control user access to folders and to the files and subfolders contained within them. If permission is denied to a file that is inside a folder that has an Allow permission, the Deny attribute takes precedence over the Allow permission applied to the folder.

The following table lists the standard NTFS folder permissions and the type of access that each provides, from the most restrictive to the least restrictive permissions.

NTFS folder permission	Allows a user to
Read	See files and subfolders in the folder and view folder ownership, permissions, and attributes, such as Read-Only, Hidden, Archive, and System.
Write	Create new files and subfolders within the folder, change folder attributes, and view folder ownership and permissions.
List Folder Contents	View the names of files and subfolders in the folder.
Read & Execute	Move through folders to reach other files and folders, plus perform actions permitted by the Read permission and the List Folder Contents permission.
Modify	Delete the folder and perform actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, delete subfolders and files, and perform actions permitted by all other NTFS folder permissions.

Verifying Folder Permissions

An administrator assigns permissions to a folder from the **Security** tab of the **Properties** dialog box for the folder. You can also view the current folder permissions in the same dialog box.

To access the Security tab

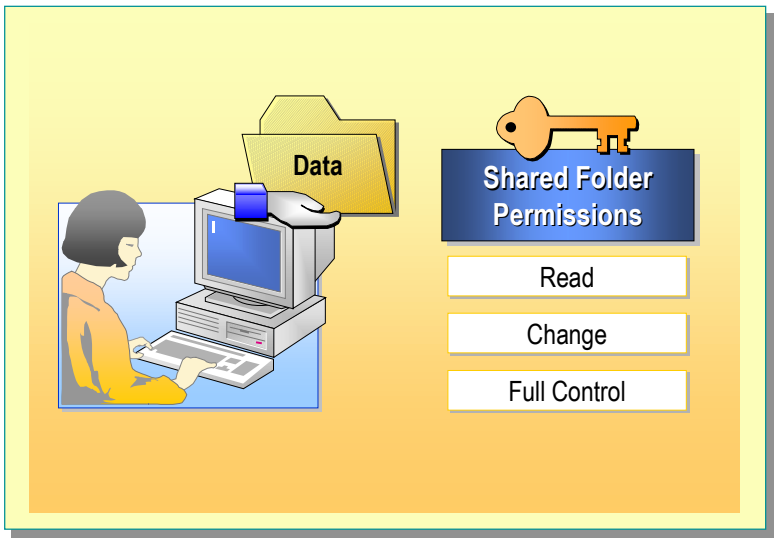
1. In Windows Explorer, right-click the folder.
2. Click **Properties**.
3. In the **Properties** dialog box, click the **Security** tab.

The **Security** tab consists of two sections—Name and Permissions. The Name section displays a list of existing users or groups who have permissions to the folder. The Permissions section displays a list of permissions granted or denied to the user or group.

Shared Folder Permissions

Slide Objective
To describe shared folder permissions.

Lead-in
Use permissions to shared folders to provide access to network resources.



Delivery Tip
Demonstrate the procedure for viewing shared folder permissions. Point out the shared resources but do not explain the details of how to set the permissions.

To provide multiple users with access to the same resource, such as a folder, you must share the folder. Sharing a folder refers to the process by which the folder is made accessible to multiple users simultaneously over the network. After a folder is shared, users can access all of the files and subfolders within the shared folder if they have been granted permission.

You can only share folders, not individual files. If multiple users need access to the same file, you must enclose the file in a folder and then share the folder.

Shared Folders

Shared folders are usually placed on a file server, but you can also place them on any computer on the network. You can store files in shared folders according to categories or functions. For example, you can place shared data files in one shared folder and shared application files in another.

Some of the characteristics of shared folders are listed below:

- A shared folder appears in Microsoft Windows Explorer with an icon of a hand holding the folder.
- Permissions are assigned to the entire folder only, not to individual files or subfolders within the shared folder.
- When a folder is shared, the Full Control permission is assigned to the Everyone group as the default permission.

- When a user is added to a shared folder, the user receives the Read permission by default.
- When a shared folder is copied, the original shared folder is still shared, but the copy is not shared. When a shared folder is moved to another location, the folder is no longer shared.

You can control the level of access to a shared folder by assigning permissions to it. The following table lists the shared folder permissions and the tasks they enable a user to perform.

Shared folder permission	Allows a user to
Read	Display folder names, file names, file data, and attributes; run application files; and change folders within the shared folder.
Change	Create folders, add files to folders, change data in files, append data to files, change file attributes, delete folders and files, and perform actions permitted by the Read permission.
Full Control	Change file permissions, take ownership of files, and perform all tasks permitted by the Change permission.

Note Shared folder permissions can be granted or denied to users. To deny all access to a shared folder, deny the Full Control permission.

Verifying Shared Folder Permissions

After creating a shared folder, an administrator can assign shared folder permissions to users and groups from the **Permissions** dialog box of the shared folder. You can view existing shared folder permissions in this dialog box as well.

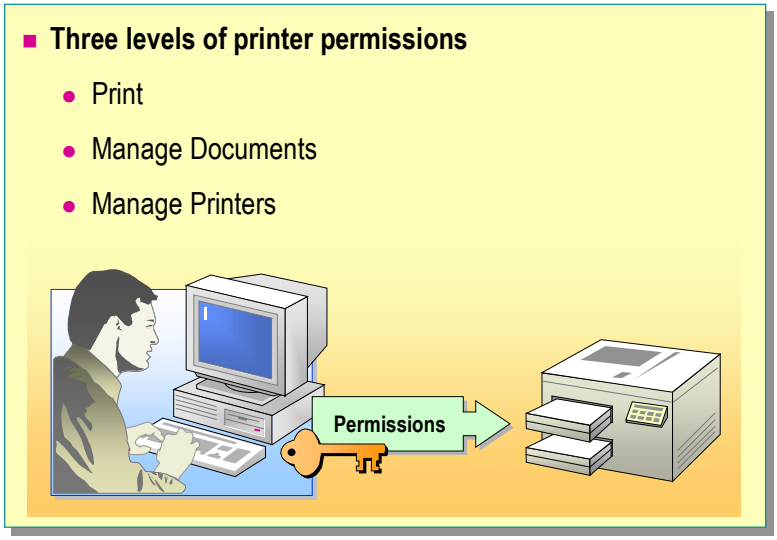
To verify permissions assigned to users and groups for a shared folder

1. In Windows Explorer, right-click the shared folder.
2. Click **Properties.**
3. On the **Sharing** tab of the **Properties** dialog box, click **Permissions**.
4. Select the user account or group for which you want to view permissions.

Printer Permissions

Slide Objective
To describe the levels of printer permissions.

Lead-in
You can assign three levels of printer permissions.



Delivery Tip
Demonstrate the user interface for printer permissions.

In addition to assigning permissions on shared folders, an administrator also needs to assign permissions on printers. These permissions are assigned to users who are not administrators. Printer permissions control the types of printing activities users may perform and also can be used to limit user access to certain printers for security reasons.

Levels of Printer Permissions

Windows 2000 provides three levels of printer permissions—Print, Manage Documents, and Manage Printers.

Print

The Print permission allows you to connect to a printer. It also allows you to print and cancel your own documents.

Manage Documents

The Manage Documents permission allows you to connect to a printer. It also allows you to pause, resume, restart, and cancel printing of all documents.

Manage Printers

The Manage Printers permission allows you to perform all of the tasks that the Print and Manage Documents permissions allow. In addition, this permission allows you to share a printer, change printer properties, delete a printer, and change printer permissions.

Verifying Printer Permissions

You can assign printer permissions to individual users or to groups. By default, Windows 2000 assigns the Print permission for each printer to the built-in Everyone group, thereby allowing all users to send documents to each printer. However, an administrator can change these permissions if there is a need to restrict printer access to specific users or groups. For example, an administrator might need to limit the use of a color printer to users from the marketing department. In this case, the default permission of the Everyone group can be removed and permission can be assigned exclusively to the Marketing group.

To view existing printer permissions

1. On the **Start** menu, point to **Search**, and then click **For Printers** to display the **Find Printers** dialog box.
2. In the **Name** box on the **Printers** tab, type the printer name, and then click **Find Now**.
3. Right-click the printer name, and then click **Properties**.
4. In the **Properties** dialog box, click the **Security** tab. Here you can view existing printer permissions for users and groups.

Lab C: Examining File and Folder Permissions

Slide Objective
To introduce the lab.

Lead-in
In this lab, you will explore file and folder permissions.

Objectives

After completing this lab, you will be able to:

- Describe the function of file and folder permissions.

Prerequisites

Before working on this lab, you must have:

- Experince logging on and off Microsoft Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1
Examining File and Folder Permissions

Scenario

You want to determine whether you are able to create files within various folders.

Goal

In this exercise, you will examine the permissions on files and folders and verify the effect of those permissions on day-to-day tasks. You will use the following chart to determine which users are in the different groups for the exercise.

Groups	Users in the Groups
Sales	Don Hall Anne Paper
Managers	Jae Pak Kim Yoshida

Tasks	Detailed Steps
1. Log on as user Kimyo with a password of **password**. Create a text file called Meeting.txt in the folder C:\MOC\WIN2151A\ labfiles\lab03\managers.	**a.** Log on to the computer using the following credentials: Username: **kimyo** Password: **password** Domain: *domainname*.**nwtraders.msft** (where *domainname* is the name of your domain). **b.** Using Windows Explorer, open the folder C:\moc\win2151a\ labfiles\lab03\managers. **c.** Right-click the **Managers** window, point to **New**, and then click **Text Document**. **d.** Type **meeting** and then press ENTER.
To create the file in this folder, you must have the appropriate permissions for the Managers folder. What permissions should be assigned to the user Kimyo for the Managers folder? **Read and Write permissions.**	
2. Examine the permissions for the folder C:\MOC\WIN2151A\ labfiles\lab03\managers.	**a.** Using Windows Explorer, open the folder C:\MOC\WIN2151A\ labfiles\lab03. **b.** Right-click the **Managers** folder, and then click **Properties**. **c.** Click the **Security** tab.

(*continued*)

Tasks	Detailed Steps
	Notice the entries in the **Security** tab. Are the entries for users or for groups? How can you tell? **Groups. The entries have the icon representing groups.** Which group has Full Control permissions? Is the user Kimyo a member of that group? **Managers. Yes, Kimyo is a member of the Managers group. This can be verified in the table at the beginning of the exercise.**
2. (*continued*)	**d.** Click **Cancel** to close the Managers Properties window.
3. Attempt to create a file called Meetings1.txt in the folder C:\MOC\WIN2151A\ labfiles\lab03\sales.	**a.** Using Windows Explorer, open the folder C:\MOC\WIN2151A\ labfiles\lab03\sales. **b.** Right-click the **Sales** window, point to **New**, and then click **Text Document**.
	Can user Kimyo create a file in this folder? What permission does Kimyo need to create a file in this folder? **No. Kimyo will need at least the Write permission to create a file in this folder.**
3. (*continued*)	**c.** Click **OK** to close the **Sales** message box.
4. Examine the permissions for the folder C:\MOC\WIN2151A\ labfiles\lab03\sales.	**a.** Using Windows Explorer, open the folder C:\MOC\WIN2151A\ labfiles\lab03. **b.** Right-click the **Sales** folder, and then click **Properties.** **c.** Click the **Security** tab. **d.** Click **Managers** in the Name window.

(*continued*)

Tasks	Detailed Steps
Which permissions does the Managers group have for the Sales folder? **Read and Execute, List Folder Contents, and Read permissions.**	
Which permissions does the Sales group have for the Sales folder? **Full Control permissions**.	
4. *(continued)*	**e.** Click **Cancel** to close the **Sales Properties** dialog box. **f.** Close all open windows and log off.

Review

Slide Objective
To reinforce module objectives by reviewing key points.

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

- User Accounts
- Groups
- User Rights
- Permissions

1. Two new employees have joined the marketing department. The network administrator needs to create user accounts for them, so that they can access such network resources as shared folders and printers. Which type of user accounts should the network administrator create for the new employees?

   a. Domain user accounts.

   b. Local user accounts.

   c. Built-in Administrator accounts.

   d. Built-in Guest accounts.

   A is the correct answer. With the domain account, the new employees will be able to access resources throughout the network. If they have an account on only the local computer, they will be able to access resources on only the local computer.

2. The network administrator has set up a computer to run Windows 2000 Server. Which of the following accounts does she use to access the computer, before creating an account for herself?

   a. Domain user account.

   b. Local user account.

   c. Built-in Administrator account.

   d. Built-in Guest account.

   C is the correct answer. When the computer is first installed, only two accounts exist—the built-in Administrator account and the built-in Guest account. Of the two, only the Administrator account has the appropriate rights to log on and manage the computer.

3. A new trainee has joined the network administration team. The network administrator wants this trainee to be able to perform all common administrative tasks in the domain, such as creating and modifying user accounts and user groups and sharing resources. However, he does not want the trainee to have full control over the system. The trainee should not be able to modify the Administrator or Backup Operators group or to manage the security auditing logs. What can the administrator do to achieve this? Select all that apply.

   a. Grant appropriate rights directly to the trainee.

   b. Add the trainee to the built-in Power Users group.

   c. Add the trainee to the Administrators group.

   d. Create a new group and add the trainee to the group. Then grant appropriate rights to the group.

   A & D are the correct answers. The administrator can grant the appropriate rights directly to the trainee, but trainee permissions will be easier to manage if the administrator creates a group, puts the appropriate users in the group, and then grants rights to the group a single time instead of multiple times. The Power Users group exists only on computers that are not domain controllers and does not provide any rights in the domain, only on the local computer. If the administrator adds the trainee to the Administrators group, the trainee will have full control over the domain.

4. The annual audit is going to take place in your organization. The head of the finance department wants only certain authorized users from the department to view the balance sheets of the organization. These documents are stored in the Balance Sheets folder. Which of the following approaches would be the best for assigning permissions to the users from the finance department?

   a. All of the users in the finance department should be assigned permission to the folder.

   b. The Finance group, containing all users in the finance department, should be assigned permission to the folder.

   c. Permissions should be assigned individually to each authorized user.

   d. A group of authorized users should be created. This group should then be assigned appropriate permission to the folder.

   D is the correct answer. Because only certain members of the finance department need access to this information, the administrator should create a group that contains only the users that need access, and then grant that group the permissions to the folder.

5. Users in the products department constantly need to refer to product-related information stored in a folder on the server. This folder also contains some applications that the users might need to run. However, users are not allowed to make any modifications to the files in the folder. What permissions should be assigned for this folder?

   a. Read.

   b. Read & Execute.

   c. List Folder Contents.

   d. Read & Write.

   B is the correct answer. While all of the answers enable the users to see the information, only B enables the users to open the files and run any applications contained in the folder, but not to make any changes to the files or folder.

6. The network administrator wants you to administer the color printer, which has been set up for the sales department. What printer permission should be assigned to you, so that you can manage the printing of documents as well as share the printer and change its properties?

   a. Print.

   b. Full Control.

   c. Manage Documents.

   d. Manage Printer.

   D is the correct answer. The Manage Printer permission enables a user to perform all of the actions necessary. The Print permission enables a user only to print a document. Manage Documents enables a user to affect all of the documents that the printer currently has in its queue. The Full Control permission does not exist for printers.

7. The network administrator of the engineering department needs to limit the use of the printer purchased exclusively for the department. What should be done to ensure that only employees from the Engineering group are able to access the printer?

   a. Add the Print permission to all of the users in the engineering department.

   b. Add the Print permission to the Engineering group. However, retain the default permission of the Everyone group.

   c. Remove the default Print permission of the Everyone group and assign permission only to the Engineering group.

   d. Remove the default Print permission of the Engineering group and assign the Print permission to the Everyone group.

   C is the correct answer. The default permissions on a printer give Print permission to the Everyone group. The administrator must first remove this group and then add only the group that needs access to the printer, in this case the Engineering group.