

Module 4: Setting Up and Administering Users and Groups

Contents

Overview	1
Introduction to User Accounts and Groups	2
User Logon Names	3
Creating Multiple User Accounts	7
Administering User Accounts	14
Lab A: Setting Up and Administering User Accounts	21
Using Groups in Active Directory	27
Strategies for Using Groups in a Domain	32
Lab B: Setting Up and Administering Groups in a Single Domain	37
Troubleshooting Domain User Accounts and Groups	44
Best Practices	45
Review	46



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:
75 Minutes

Labs:
60 Minutes

This module provides students with the knowledge and skills to set up and administer domain user accounts and groups. Setting up user accounts enables users to gain access to resources in a Microsoft® Windows® 2000 network. Setting up groups enables administrators to manage resources access in a Windows 2000 network.

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

- Identify the purpose of using users and groups in Windows 2000.
- Identify the different types of user logon names, and create the user principal name suffix.
- Create multiple domain user accounts by importing user information into Active Directory® directory service.
- Administer domain user accounts.
- Use security groups in Active Directory.
- Implement strategies for using security groups in Active Directory.
- Troubleshoot common problems with administering domain user accounts and groups.
- Apply best practices for administering domain user accounts and groups.

In the hands-on labs in this module, students will create and use an alternate user principal name suffix, create multiple domain user accounts by using bulk import, and administer domain user accounts. They will also create and nest global groups, create domain local groups and assign permissions to resources, and implement and test the recommended group strategy.

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_04.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 appendix C, “LDAP Names,” on the Student Materials compact disc.
- Read appendix D, “Common User Account Attributes,” on the Student Materials compact disc.
- Read appendix E, “Using ADSI Programming to Automate Administrative Tasks,” on the Student Materials compact disc.
- Read Module 4, “Creating and Managing User Accounts,” in Course 2152, *Implementing Microsoft Windows 2000 Professional and Server*.
- Read Module 5, “Managing Access to Resources by Using Groups,” in Course 2152, *Implementing Microsoft Windows 2000 Professional and Server*.
- Read chapter 4, “Active Directory Schema” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.
- Read the white paper, *Active Directory Users, Computers, and Groups* on the Student Materials compact disc.
- Read the white paper, *Single Sign-On in Windows 2000 Networks* on the Student Materials compact disc.
- Read the white paper, *Microsoft Active Directory Service Interfaces* on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- Introduction to Users and Groups

In this topic, you will introduce users and groups. Rather than telling the students what these are, ask them to explain as they have already learned about users and groups in Course 2152, *Implementing Microsoft Windows 2000 Professional and Server*. After a brief discussion about users and groups, discuss the purpose of using domain user accounts to enable users to gain access to network resources. Use this topic only to refresh students on what user accounts and groups are. Do not spend too much time discussing this topic.

- User Logon Names

In this topic, you will introduce user logon names. Discuss the different logon names that a user can use to log on to a Windows 2000 domain. Demonstrate how to create alternative user principal name suffixes. Emphasize the uniqueness rules that the students should remember when creating user logon names.

- Creating Multiple User Accounts

In this topic, you will introduce how to create multiple domain user accounts by importing user information into Active Directory. Discuss how to create multiple domain user accounts simultaneously by importing information from another source. Explain how to use the **csvde** and **ldifde** commands to create multiple domain user accounts.

- Administering User Accounts

In this topic, you will introduce how to administer domain user accounts. Present the techniques used to administer domain user accounts. Discuss the common administrative tasks, which include resetting passwords and unlocking user accounts; renaming, disabling, enabling, and deleting user accounts; and moving user accounts within a domain. Explain how administrators can locate domain user accounts to perform administrative tasks by using the advanced features of Active Directory.

- Lab A: Setting Up and Administering Domain User Accounts

Prepare students for the lab in which they will create and use an alternative user principal name suffix, create multiple domain user accounts using bulk import, and perform common administrative tasks. After students have completed the lab, ask them if they have any questions concerning the lab.

- Using Groups in Active Directory

In this topic, you will introduce the different groups in Active Directory. Discuss the global groups, domain local groups, and universal groups. Because the universal groups are typically used in multiple domains, do not go into detail; these groups are covered in Module 10.

- Strategies for Using Groups in a Domain

In this topic, you will introduce the strategies for using groups in Active Directory. Discuss the recommended strategies for using global and domain local groups, including how to nest groups. Tell students groups can have up to 5,000 members. The user's primary group membership, such as Domain Users, is not stored in the group membership list. Conduct a class discussion on using groups in a single domain.

- Lab B: Setting Up and Administering Groups in a Single Domain

Prepare students for the lab in which they will create and nest global groups and implement the recommended group strategy. After students have completed the lab, ask them if they have any questions concerning the lab.

- Troubleshooting Domain User Accounts and Groups

In this topic, you will introduce troubleshooting options for resolving problems that may occur when setting up and administering user accounts and groups in Active Directory. Present some of the more common problems that students may encounter while setting up and administering user accounts and groups in Active Directory, and some suggested strategies for resolving these problems.

- Best Practices

Present best practices for setting up and administering user accounts and groups. Emphasize the reason for each best practice.

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 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Setup

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

Setup Requirement 1

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

- Complete the labs in Module 2, “Implementing DNS to Support Active Directory,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Dnssuf.vbs from the C:\Moc\Win2154A\Labfiles\Custom\Autodns folder.
- Install DNS on the student computers. Configure a forward and reverse lookup zone. Configure both zones to allow updates.

Setup Requirement 2

The labs in this module require each student computer to be configured as a domain controller in its own forest. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete the labs in 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 by 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**.

Setup Requirement 3

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

- Complete the labs in Module 3, “Creating a Windows 2000 Domain,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Nativesd.vbs from the C:\Moc\Win2154a\Labfiles\Custom\Autodc folder.
- Change the domain mode to native in the *domain* (where *domain* is your assigned domain name) **Properties** dialog box in Active Directory Domains and Trusts.

Setup Requirement 4

The labs in this module use the following files that were installed on the student computer during the classroom setup. These files are located under the folder C:\Moc\Win2154a\Labfiles:

- Lrights.bat
- Ntrights.exe
- PackA.txt
- PackAttr.txt
- Groups.bat

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

Performing the labs in this module introduces the following configuration changes:

- The Log on Locally user right has been granted to the Users local group.
- An alternative user principal name suffix called contoso.msft is created.
- The following OUs are created:
 - Contoso
 - Package Handling
 - Human Resources
 - Human Resources\Benefits
 - Human Resources\Payroll
 - Human Resources\Training
- The Package Handling OU contains 27 new user accounts specified in PackA.txt.
- The Contoso OU contains two user accounts, TestUPN and Derek Graham.
- The Human Resources OU contains the HR Managers global security group, and the HR Data domain local security group.
- The Benefits OU contains the Benefits Managers global security group, the Benefits Data domain local security group, and the user account TestBenefits.
- The Payroll OU contains the Payroll Managers global security group, and the Payroll Data domain local security group.
- The Training OU contains the Training Managers global security group, and the Training Data domain local security group.
- The following files are created:
 - C:\Hr\Benefits\Benefits.txt
 - C:\Hr\Payroll\Payroll.txt
 - C:\Hr\Training\Training.txt
 - C:\Moc\Win2154a\Labfiles\Pack.txt

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about setting up and administering domain user accounts to enable users to gain access to resources in a Windows 2000 network. You will also learn how to use groups in a single domain network.

- Introduction to Users and Groups
- User Logon Names
- Creating Multiple User Accounts
- Administering User Accounts
- Using Groups in Active Directory
- Strategies for Using Groups in a Domain
- Troubleshooting Domain User Accounts and Groups
- Best Practices

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

Active Directory® directory service is a directory service that stores and maintains data needed by network resources. A user account is an object stored in Active Directory that enables a *single sign-on* for a user account. A single sign-on means that users need to enter their names and passwords only once during a workstation logon to gain authenticated access to network resources. A domain user account provides the ability to log on to the domain to gain access to network resources, or to log on to an individual computer to gain access to resources on that computer.

A group is usually a collection of user accounts. You can use groups to efficiently manage access to domain resources, which helps simplify network maintenance and administration. You can use groups separately or you can place one group within another to further simplify administration.

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

- Identify the purpose of using user accounts and groups in Microsoft® Windows® 2000.
- Identify the different types of user logon names, and create a user principal name suffix.
- Create multiple user accounts by importing user information into Active Directory.
- Administer user accounts.
- Use groups to manage access to domain resources.
- Implement strategies for using security groups to manage access to domain resources.
- Troubleshoot common problems with administering user accounts and groups.
- Apply best practices for administering user accounts and groups.

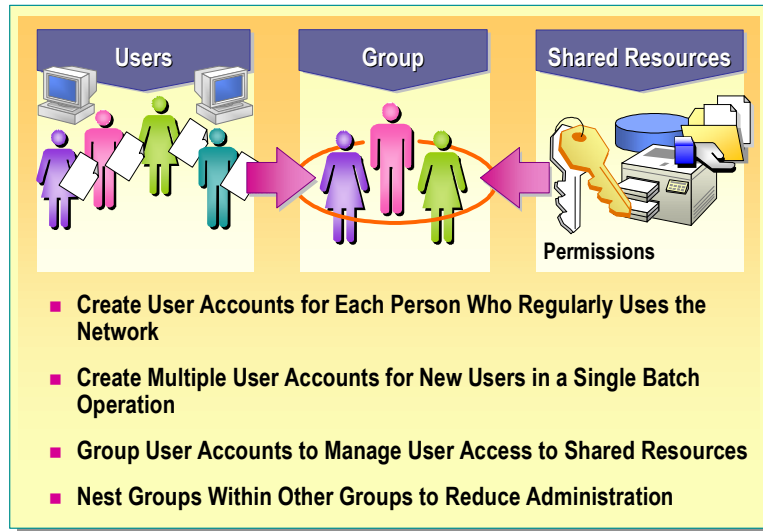
Introduction to User Accounts and Groups

Topic Objective

To identify the purpose of user accounts and groups.

Lead-in

To ensure that users can log on to the network and gain access to resources in a domain, an administrator must perform certain ongoing administrative tasks.



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

Do not spend too much time on this content. The students have already covered this in Course 2152.

Keep the focus on a domain when talking about user and groups in this module.

An administrator must perform certain ongoing administrative tasks to ensure that the users can log on to the network and gain access to resources in a domain. Some of these administrative tasks are:

- Creating a single sign-on for a user account. In Active Directory, a single sign-on enables users to enter their names and passwords once during a workstation logon and receive authentication to gain access to network resources in a domain. An administrator can create three types of user accounts, each having a specific function:
 - A local user account enables a user to log on to a specific computer to gain access to resources on that computer.
 - A domain user account enables a user to log on to the domain to gain access to network resources.
 - A built-in user account enables a user to perform administrative tasks or gain temporary access to network resources.
- Creating multiple user accounts in Active Directory for new users in a single batch operation. For example, an administrator can create user accounts by bulk importing data into Active Directory from a file containing user data.
- Grouping user accounts to efficiently manage access to domain resources, such as network shared folders, files, directories, and printers. By using groups, an administrator needs to assign permissions for shared resources only once rather than multiple times. You can also make computers and other groups members of a group.
- Nesting groups within other groups to reduce administration when creating a model for a hierarchical structure.

◆ User Logon Names

Topic Objective

To introduce topics related to user logon names.

Lead-in

Each user account has a user logon name, and a pre-Windows 2000 user logon name.

- Introduction to User Logon Names
- Creating a User Principal Name Suffix

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

In Active Directory, each user account has a user logon name, and a pre-Windows 2000 user logon name, which is the security account manager (SAM) account name. The user account information is used to authenticate and authorize users anywhere in the forest, which in turn enables single sign-on. When creating user accounts, you enter the user logon name prefix and select the user principal name suffix.

When creating the user account, you also need to ensure that the user accounts follow the uniqueness rules.

Introduction to User Logon Names

Topic Objective

To introduce the different types of user logon names.

Lead-in

In a Windows 2000 network, domain controllers can use either the user principal name or a user logon name (pre-Windows 2000) to log on.

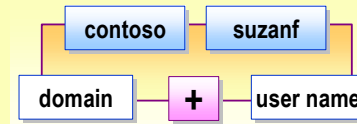
■ User Principal Name

- The suffix defaults to the name of the root domain, but it can be changed and others added



■ User Logon Name (Pre-Windows 2000)

- A user selects the domain when logging on



■ User Logon Name Uniqueness Rules

- Full name must be unique within the container
- User principal name is unique within the forest
- User logon name (pre-Windows 2000) is unique within the domain

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

Tell students that the user logon name (pre-Windows 2000) was previously known as the downlevel name.

Delivery Tip

Have students log off by pressing CTRL+ALT+DEL to display the **Log On to Windows** dialog box. Make sure that the **Log on to** box is displayed, and then have students type their user principal name to log on.

Key Points

There are two parts to a user logon name, the user principal name prefix and the suffix. You can select a user principal name suffix in Active Directory Users and Computers only if it exists in Active Directory.

To add a new suffix in Active Directory Domains and Trusts, an administrator must be a member of the predefined Enterprise Admins group.

In a Windows 2000 network, a user can log on with either a *user principal name* or a *user logon name* (pre-Windows 2000). Domain controllers can use either of these logon names to authenticate the logon request.

User Principal Name

The user principal name is the logon name used only for logging on to a Windows 2000 network. This name is also known as a user logon name.

There are two parts to a user principal name, and they are separated by the @ sign; for example, suzanf@contoso.msft. A user logon name has the following two components:

- The *user principal name prefix*, which in the suzanf@contoso.msft example is suzanf.
- The *user principal name suffix*, which in the suzanf@contoso.msft example is contoso.msft. By default, the suffix is the name of the root domain in the network. You can use the other domains in the network to configure additional suffixes for users. One example of when you would want to configure a suffix is when you want to create user logon names that match users' e-mail addresses.

Advantages of using the user principal names are that:

- The user principal name does not change when you move a user account to a different domain, because the name is unique within Active Directory.
- A user principal name can be the same as a user's e-mail address name, because it has the same format as a standard e-mail address.

User Logon Name (Pre-Windows 2000)

If a user logs on to the network from a client computer running a version of Windows earlier than Windows 2000, the user must log on by using the user logon name (pre-Windows 2000).

A user logon name (pre-Windows 2000) is a user account name, such as suzanf in the suzanf@contoso.msft example. When a user logs on by using a user logon name (pre-Windows 2000), the user must also provide the domain in which the user account exists, so that the authenticating domain controller can locate the user account.

If users connect to a network resource with a different user account than the one with which they logged on, the users must provide the domain and user logon name (pre-Windows 2000) for authentication, for example, contoso\suzanf.

User Logon Name Uniqueness Rules

User logon names for domain user accounts must follow *uniqueness rules* in Active Directory. When creating user logon names, consider the following uniqueness rules:

- The full name must be unique within the container in which you create the user account. The full name is used as the relative distinguished name.
- The user principal name must be unique within the forest.
- The user logon name (pre-Windows 2000) must be unique within the domain.

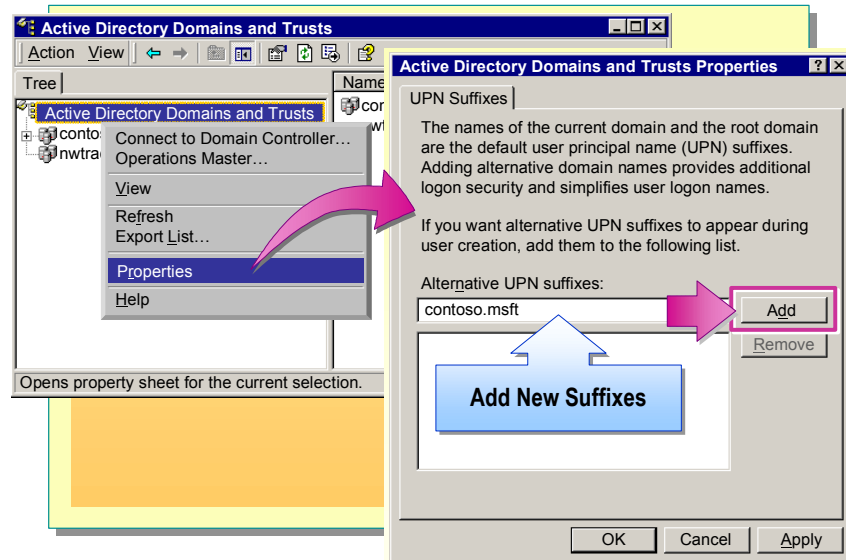
Creating a User Principal Name Suffix

Topic Objective

To illustrate how to create a user principal name suffix.

Lead-in

You can add new user principal name suffixes that you need if they do not already exist in Active Directory User and Computers.



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

Delivery Tip

Open Active Directory Domains and Trusts, and demonstrate adding a new user principal name suffix in the **Properties** dialog box.

Key Point

A user principal name suffix enables you to simplify administration and user logon processes by providing a single user principal name suffix for all users.

You select a user principal name suffix when creating a user account in Active Directory Users and Computers. If the suffix that you need does not exist in Active Directory User and Computers, you can add it. A user principal name suffix enables you to simplify administration and user logon processes by providing a single user principal name suffix for all users.

You must be a member of the Enterprise Admins predefined group to add suffixes in Active Directory Domains and Trusts.

To add a new suffix, perform the following steps:

1. In Active Directory Domains and Trusts, in the console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**.
2. On the **UPN Suffixes** tab, type an alternative UPN suffix for the domain, and then click **Add**.

Note If you have created a user account by using a program other than Active Directory Users and Computers, you are not limited by the user principal name suffixes stored in Active Directory. You can define a suffix when you create the account.

◆ Creating Multiple User Accounts

Topic Objective

To introduce topics related to creating multiple user accounts.

Lead-in

Instead of using Active Directory Users and Computers to create user accounts one by one, you can also use the bulk import process to create multiple user accounts in Active Directory.

- The Bulk Import Process
- Using CSVDE to Create Multiple User Accounts
- Using LDIFDE to Create Multiple User Accounts

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

Define bulk import if students do not know what it means.

You can use Windows 2000 to create multiple user accounts in Active Directory by importing data from a text file to populate the attributes of user accounts. This process is known as *bulk import*. Bulk import is the importing of multiple database records into the Active Directory database. The advantage of bulk importing is that you do not need to create each user account individually. Instead, you can import an existing file that contains the user information required to create all of the user accounts.

To create user accounts in a batch operation, Windows 2000 provides administrative utilities, such as Comma Separated Value Directory Exchange (CSVDE) and Lightweight Directory Access Protocol Data Interchange Format Directory Exchange (LDIFDE). These utilities enable you to administer large numbers of user accounts, and other Active Directory objects, such as groups, computers, and printers, in one operation. These utilities are installed automatically on all computers that run Windows 2000 Server.

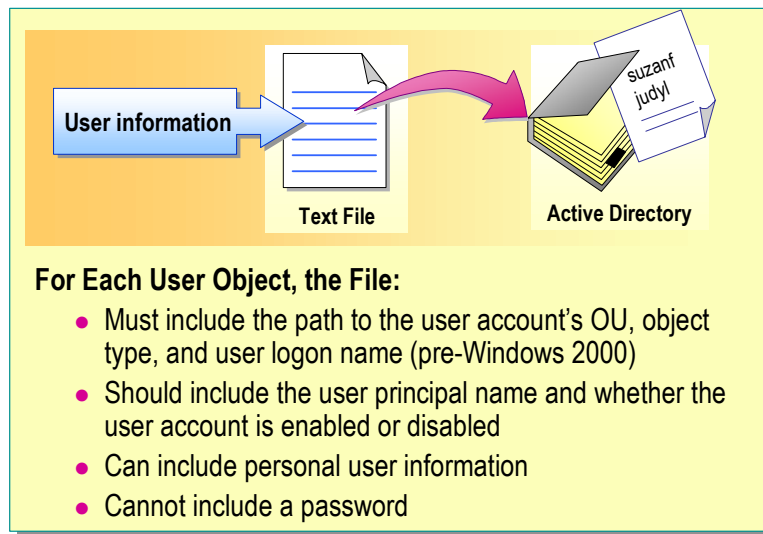
The Bulk Import Process

Topic Objective

To explain the bulk import process and the type of data that should be imported into Active Directory when using the **csvde** and the **ldifde** commands.

Lead-in

The bulk import process requires using a text file that contains information about user accounts that you want to create. The text file can be in different formats.



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

Mention to students that if users are not going to immediately use the accounts that they create, students should disable them. This is because these user accounts have blank passwords.

Key Points

The file being imported must include the path to the OU where the user account will reside, the type of object being imported, and the user logon name (pre-Windows 2000).

Also, the file being imported should specify the user logon name and whether the user accounts are enabled or disabled.

The bulk import process enables you to automatically create multiple user accounts in Active Directory. This process requires using a text file that contains information about the user accounts that you want to create. The text file can be a database application that already contains information about user accounts, or can also be from other applications, such as Microsoft Excel or Microsoft Word.

Depending on the format of the text file, you use the **csvde** or the **ldifde** command to import user account data from the file to simultaneously create multiple user accounts in Active Directory. You use the **csvde** command to import the text file that uses a *comma-delimited* format, also known as a *comma-separated value* format (CSVDE format). You use the **ldifde** command to import the text file that uses a *line-separated value* format (LDIF format). Most database applications can create text files that can be imported in one of these formats.

When creating multiple user accounts, the information in the CSVDE or LDIFDE file:

- Must include the path to the user account in Active Directory, the object type, which is the user account itself, and the user logon name (Pre-Windows 2000).
- Should include the user principal name, because this is the logon name recommended for users logging on from a computer that runs Windows 2000. You should also include whether the user account is disabled or enabled. If you do not specify a value, the account is disabled.
- Can include personal information, for example, telephone numbers or home addresses. The file needs to contain the information necessary to create *attributes* for the user account. Attributes, which are also referred to as *properties*, are categories of information for Active Directory objects. The values of these attributes define the characteristics of the object. You should include as much user account information as possible to provide more items on which users can search when conducting Active Directory searches.
- Cannot include passwords. Bulk import leaves the password blank for user accounts. By default, the first time that users log on, they must change their passwords. This is not a problem if users log on immediately, but it could be a problem if users do not log on for some time. Because a blank password allows an unauthorized person to gain access to the network by knowing only the user logon name, disable the user accounts until users start logging on.

Using CSVDE to Create Multiple User Accounts

Topic Objective

To illustrate how to edit, format, and run a CSVDE import file to create multiple domain user accounts in Active Directory.

Lead-in

You can use the CSVDE format file to add new user accounts.

Format Example

Attribute line containing the names of the attributes:
 DN,objectClass,samAccountName,userPrincipalName,displayName,userAccountControl

User account line containing values for attributes:
 "cn=Suzan Fine,ou=Human Resources,dc=asia,dc=contoso,dc=msft",user,suzanf,suzanf@contoso.msft,Suzan Fine,512

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

Mention to students that after they successfully import the file, they should verify that the user accounts were created correctly. In the example in the slide, the text should not wrap to the next line. It is displayed on multiple lines only to fit on the slide.

Key Points

The **csvde** command is used only to add objects in Active Directory.

The CSVDE format can be used only to add user objects, and other types of objects, to Active Directory. You cannot use the CSVDE format for deleting or modifying objects in Active Directory. Before importing a CSVDE file, you must ensure that the file that you are importing is properly formatted, so that the import will be successful. Typically, to edit and format a text file, you use an application that has good editing capabilities, such as Excel or Word. Then, save the file as a comma-delimited text file. You can export data from Active Directory to an Excel spreadsheet or import data from a spreadsheet into Active Directory.

Preparing a CSVDE File for Importing

Format the file so that it contains the following information:

- The attribute line, which is the first line of the file. It specifies the name of each attribute that you want to define for the new user accounts. Note that you can put the attributes in any order, but you must separate the attributes with commas. The following is an example of the attribute line:
 DN,objectClass,sAMAccountName,userPrincipalName,displayName,userAccountControl
- The user account line. For each user account that you create, the import file contains a line that specifies the value for each attribute in the attribute line. The following rules apply to the values in a user account line:
 - The attribute values must follow the sequence of the attribute line.
 - If a value is missing for an attribute, leave it blank, but include all commas.
 - If a value contains commas, include the value in quotation marks.

The following is an example of a user account line:

```
"cn=Suzan Fine,ou=Human Resources,dc=asia,dc=contoso,  
dc=msft",user,suzanf,suzanf@contoso.msft,Suzan Fine,512
```

The following table provides the attributes and values presented in the previous example.

Attribute	Value
DN (distinguished name)	cn=Suzan Fine,ou=Human Resources, dc=asia,dc=contoso,dc=msft (This specifies the path to the OU that contains the user account.)
objectClass	user
sAMAccountName	suzanf
userPrincipalName	suzanf@contoso.msft
displayName	Suzan Fine
userAccountControl	512 (The value 512 enables the user account, and the value 514 disables the user account.)

For more information about distinguished names, see appendix C, “LDAP Names,” on the Student Materials compact disc.

Note For a list of common attributes and their display names, see appendix D, “Common User Account Attributes,” on the Student Materials compact disc.

Using the csvde Command

After the file is properly formatted, you can use the **csvde** command to import the file and to create multiple user accounts in Active Directory.

To import the file, open a command prompt window, and type the following:

```
csvde -i -f filename
```

In the previous syntax, **-i** indicates that you are importing a file into Active Directory, and **-f** indicates that the next parameter is the name of the file that you are importing.

The **csvde** command provides status information on the success or failure of the process, and it also provides the name of the file to view for detailed error information. Even if the status information indicates that the process was successful, use Active Directory Users and Computers to verify some of the user accounts that you created to ensure that they have all of the information that you provided.

Using LDIFDE to Create Multiple User Accounts

Topic Objective

To illustrate how to edit, format, and run an LDIFDE import file to create multiple domain user accounts in Active Directory.

Lead-in

If you want to modify user accounts or delete user accounts, you cannot use the CSVDE format file. To do this, you use the LDIFDE format file. The LDIFDE format file can also be used for adding user accounts.

Format Example

```
DN:CN=Suzan Fine,OU=Human Resources,DC=asia,DC=contoso,DC=msft
objectClass: user
samAccountName: suzanf
userPrincipalName: suzanf@contoso.msft
displayName: Suzan Fine
userAccountControl: 512
```

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

After discussing the LDIFDE format, compare the CSVDE and LDIFDE formats. Tell the students that CSVDE can be used only for adding objects in Active Directory, but LDIFDE can be used to add, delete, and modify objects in Active Directory.

Key Point

The **ldifde** command allows you to create, modify, and delete objects in Active Directory.

Lightweight Directory Access Protocol Interchange Format (LDIF) is another file format that is used to perform bulk import for directories that conform to LDAP standards. The LDIF file format has a command-line utility called **ldifde** that allows you to create, modify, and delete objects in Active Directory. An LDIF file consists of a series of *records* that are separated by a blank line. A *record* describes either a single directory object or a set of modifications to the attributes of an existing object and consists of one or more lines in the file.

Preparing a LDIF File for Importing

Format the LDIF file so that it contains a record that consists of a sequence of lines describing an entry for a user account in Active Directory, or a sequence of lines describing a set of changes to a user account in Active Directory. The user account entry specifies the name of each attribute that you want to define for the new user account. The Active Directory schema defines the attribute names. For each user account that you create, the file contains a line that specifies the value for each attribute in the attribute line. The following rules apply to the values for each attribute:

- Any line that begins with a pound-sign (#) is a comment line, and is ignored when you run LDIF file.
- If a value is missing for an attribute, it must be represented as *AttributeDescription* ":" FILL SEP.

The following is an example of an entry in LDIF import file:

```
# Create Suzan Fine
DN: CN=Suzan Fine,OU=Human
Resources,DC=asia,DC=contoso,DC=msft
objectClass: user
sAMAccountName: suzanf
userPrincipalName: suzanf@contoso.msft
displayName: Suzan Fine
userAccountControl: 512
```

The following table provides the attributes and values presented in the example.

Attribute	Attribute's value
DN (distinguished name)	CN=Suzan Fine,OU=Human Resources, DC=asia,DC=contoso,DC=msft (This specifies the path to the object's container.)
objectClass	user
sAMAccountName	suzanf
userPrincipalName	suzanf@contoso.msft
displayName	Suzan Fine
userAccountControl	512 (The value 512 enables the user account, and the value 514 disables the user account.)

Using the Ldifde Command

After the file is properly formatted, use the **ldifde** command to import the file and create multiple user accounts in Active Directory.

To import the file, at the command line, type:

ldifde -i -f filename

In the previous syntax, **-i** indicates that you are importing a file into Active Directory. If this parameter is not specified, the default mode for LDIFDE is export. The **-f** parameter indicates the name of the file that you are importing.

Note Programs use Active Directory Service Interfaces (ADSI) to gain access to Active Directory. ADSI in conjunction with the Windows Script Host enables scripting batch operations in Active Directory by using Microsoft Visual Basic®, Scripting Edition (VBScript) or Java. For more information about creating ADSI scripts, see appendix E, “Using Active Directory Service Interfaces (ADSI) Programming to Automate Administrative Tasks,” on the Student Materials compact disc.

◆ Administering User Accounts

Topic Objective

To introduce topics related to administering user accounts.

Lead-in

After creating user accounts, you need to perform certain daily tasks for maintaining user accounts.

- Performing Common Administrative Tasks
- Locating User Accounts

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

After you have set up user accounts in Active Directory, you must perform ongoing administrative tasks to ensure that all users have the resources that they need, and that network security remains intact. Because there could be a large number of user accounts, you can use the **find** utility to help locate a particular user account.

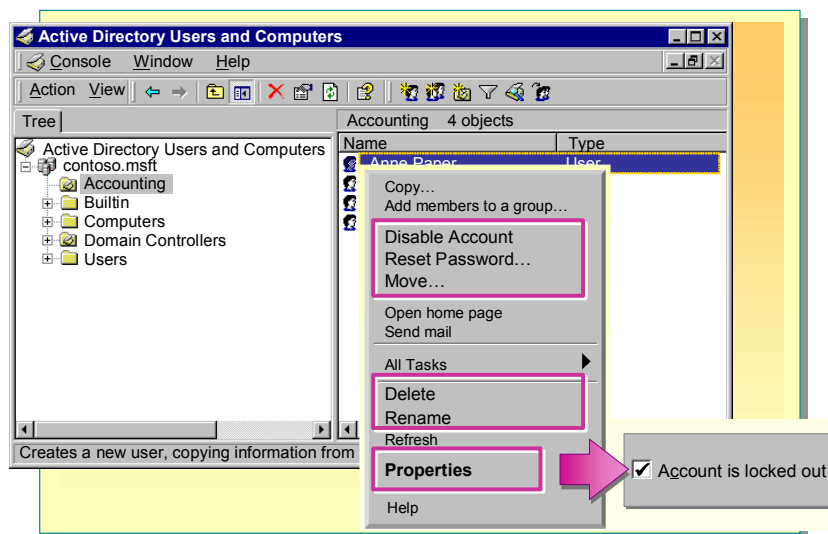
Performing Common Administrative Tasks

Topic Objective

To illustrate how to perform common administrative tasks.

Lead-in

Common administrative tasks include resetting passwords; unlocking user accounts; renaming, disabling, enabling, and deleting user accounts; and moving user accounts within a domain.



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

Delivery Tip

Demonstrate how to perform common administrative tasks.

Key Points

Disable a user account if the account will not be used for a certain period of time.

Reset a password when the password expires before the user changes it, or if the user forgets the password.

Move user accounts between OUs within the same domain when necessary.

Delete an unused user account.

Rename a user account if you want to retain all specified attributes, and then reassign it to a different user.

Unlock a user account if a security Group Policy setting locks that account.

After creating user accounts, you must perform frequent administrative tasks to ensure that the network reflects the evolving needs of the organizations that it supports. These administrative tasks include disabling and enabling user accounts, resetting passwords, moving user accounts within a domain, deleting user accounts, renaming user accounts; and unlocking user accounts.

Disabling and Enabling User Accounts

Disable user accounts when users will not need their accounts for an extended period, but will need to use them at a later time. You disable a user account as a security precaution against a potential misuse of the user account. For example, if the user takes a two-month leave of absence, disable the account when the user leaves and then enable the account when the user returns.

To disable or enable user accounts, perform the following step:

- In Active Directory Users and Computers, right-click the appropriate user account, and then click **Disable Account** or **Enable Account** depending on the current status of the account.

Resetting Passwords

You reset a password when the password expires before the user changes or if the user forgets it. You do not need to know a user's password before you can reset it. You should require the users to change their passwords the next time that they log on.

To reset user account passwords, perform the following step:

- In Active Directory Users and Computers, right-click the appropriate user account, and then click **Reset Password**.

Moving User Accounts Within a Domain

You can move user accounts between OUs in the same domain when necessary. For example, when an employee moves from one department to another and another administrator will administer the employee's user account. The following conditions apply when you move user accounts between OUs:

- Object permissions assigned directly to the user account move with the user account.
- Permissions that were previously inherited from the parent object no longer apply. Instead, permissions are inherited from the new parent object.
- You can move multiple user accounts at the same time.

To move a domain user account within a domain, perform the following steps:

1. In Active Directory Users and Computers, right-click the user account(s) to be moved, and then click **Move**.
2. In the **Move** dialog box, double-click the domain tree, click the OU to which you want to move the objects, and then click **OK**.

Deleting User Accounts

Delete a user account when an employee leaves the organization and you are not going to reuse the account. By deleting these accounts, you will not have unused accounts in Active Directory, that may cause a security risk if an authorized user was able log on using an obsolete account.

To delete user accounts, perform the following step:

- In Active Directory Users and Computers, right-click the appropriate user account, and then click **Delete**.

Renaming User Accounts

Rename a user account if you want to retain all rights, permissions, and group memberships that are associated with that account, and then reassign it to a different user. For example, if there is a new company accountant, rename the account by changing the first name, last name, and the user logon names to those of the new accountant. Also, you may need to change other properties for a new user, such as resetting the password, and changing the telephone number and address.

To rename user accounts, perform the following step:

- In Active Directory Users and Computers, right-click the appropriate user account, and then click **Rename**.

Unlocking User Accounts

You may be required to unlock a user account if a Group Policy setting locks that account when the user violates the Group Policy defined by the setting. For example, users are locked out if they exceed the limit that a Group Policy setting allows for failed logon attempts. When a user account is locked out, Windows 2000 displays an error message when the user attempts to log on.

To unlock a user account, perform the following step:

- In Active Directory Users and Computers, in the **Properties** dialog box for the user account, on the **Account** tab, clear the **Account is locked out** check box.

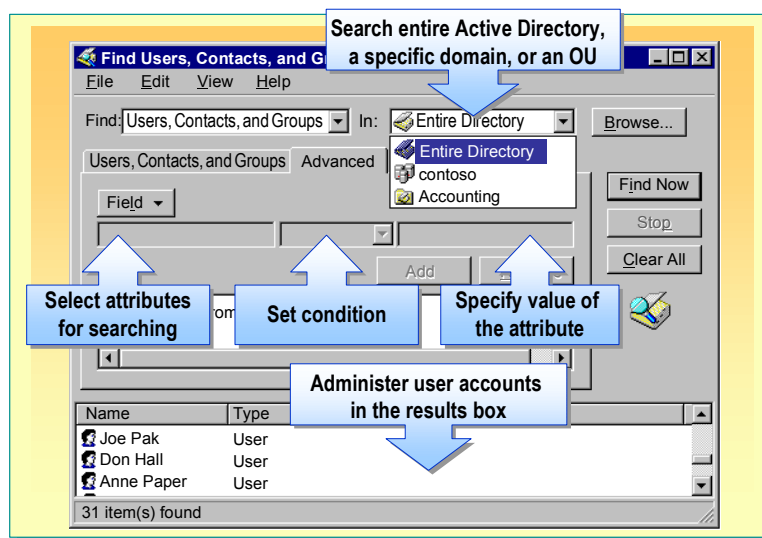
Locating User Accounts

Topic Objective

To illustrate how to locate user accounts in Active Directory.

Lead-in

Instead of browsing through hundreds and thousands of user accounts in Active Directory, you can use the search utilities in Active Directory Users and Computers to search for these accounts, and then administer them from the search results.



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

Delivery Tip

Demonstrate how to perform the basic and advanced search operations in Active Directory Users and Computers.

Demonstrate how to view and use different options in the **Find Users, Contacts, and Groups** dialog box. Be sure to demonstrate the Custom Search option.

In the results box, right-click one of the objects and demonstrate to students how to administer it.

Key Points

When you select the Entire Directory option, Windows 2000 searches the global catalog.

You can perform administrative functions on the objects that are listed in the search results box after a successful search operation has been completed.

Because all user accounts reside in Active Directory, administrators can search for the user account that they need to administer. Searching Active Directory for user accounts means that you do not need to browse through hundreds or thousands of user accounts in Active Directory Users and Computers. You can also search for other Active Directory objects, such as computers, printers, and shared folders. After locating these objects, you can administer these objects from the search results box.

Performing a Basic Search Operation

To start a basic search operation, perform the following steps:

1. In Active Directory Users and Computers, on the **Action** menu, click **Find**.
2. In the **Find Users, Contacts, and Groups** dialog box, select the type of object for which you want to search.
3. Enter the search text in the search criteria boxes in the **Find Users, Contacts, and Groups** dialog box. The types of search criteria that are available vary depending on the type of object that you selected.

The following table describes the basic options in the **Find Users, Contacts, and Groups** dialog box.

Option	Description
Find	The option that you use to select the type of objects for which you can search. • Use the Users, Contacts, and Groups option to locate users, contacts, or groups by name or description. • Use the Computers option to locate computers by name, owner, or role, such as workstation, server, or domain controller. • Use the Printers option to locate printers by name, location, or model. • Use the Shared Folders option to locate shared folders by name or keywords. • Use the Organizational Units option to locate OUs by name. • Use the Custom Search option to search for a wide range of object types, such as Computer, Contact, Group, OU, and User instead of selecting one object type at a time. You can specify additional attributes to use to locate these object types. • Use the Remote Installation Clients option to locate remote installation client computers by GUID or RIS server.
In	The option that you use to select the location that you want to search. • Use the Entire Directory option to locate objects by searching the global catalog. • Use the domain name option to locate objects in a specific domain.

Performing an Advanced Search Operation

Active Directory Users and Computers provides the Advanced option in the **Find Users, Contacts, and Groups** dialog box to allow administrators to customize searches and filter data retrieved from Active Directory. The Advanced option allows you to specify search criteria that define the resources for which you are searching. By using the Advanced option, you can search for resources by using any attribute that is valid for the object type. For example, you can search Active Directory for all printers in a specific location. You can then use the search results to edit the properties of each printer object.

The following table describes the advanced options in the **Find Users, Contacts, and Groups** dialog box.

Option	Description
Field	A list of the attributes for which you can search on the resource type that you select. Different resource types have different attributes that can be used for a search operation. For example, a user would have an attribute called Home Phone, but this attribute would not apply to a computer.
Condition	The methods that are available to further define the search for an attribute. • Use the Starts with option to specify that the value of the selected attribute begins with a given character or set of characters. • Use the Ends with option to specify that the value of the selected attribute ends with a given character or set of characters. • Use the Is (exactly) option to specify that the value of the selected attribute should be the same as the given character or set of characters. • Use the Is not option to specify that the value of the selected attribute should not be the same as the given character or set of characters. • Use the Present option to specify that the selected attribute has been defined for the object, regardless of what the attribute value is. • Use the Not present option to specify that the selected attribute has not been defined for the object.
Value	The character or set of characters that you use with the condition.

Also, if users want to find objects in Active Directory, they can click **Start**, and then click **Search**. The Search options in Windows Explorer and My Network Places can also be used to locate objects in Active Directory.

Administering User Accounts in the Results Box

After a search completes successfully, the search results are displayed. You can then perform administrative functions on the objects that are listed. The functions that are available depend on the type of object you located. For example, if you searched for user accounts, you can rename and delete the user account, disable the user account, reset the password, move the user account to another OU, or modify the user account's attributes.

To administer a user account from the search results, right-click the user account, and then click **Properties**.

When you right-click the object in the results box, the same property sheet that is invoked through Active Directory Users and Computers appears. Therefore, you can manage the objects by selecting an appropriate option related to the function that you want to perform on the object. The functions that are available depend on the type of object that you located.

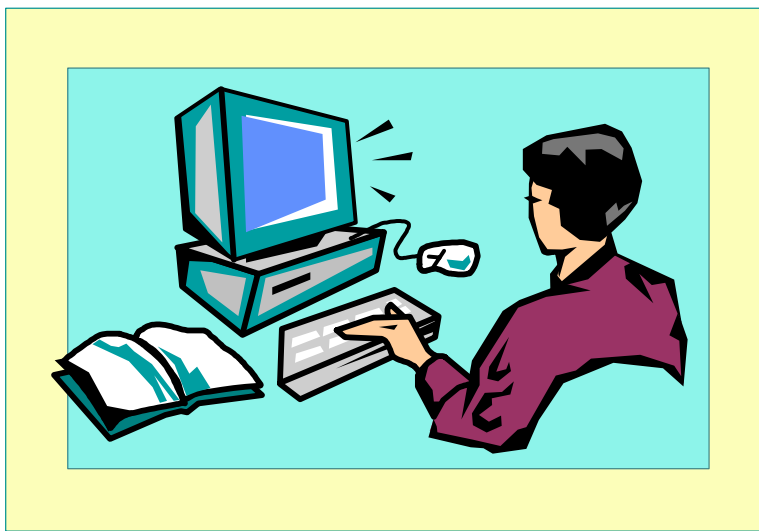
Lab A: Setting Up and Administering Domain User Accounts

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create and use an alternate user principal name suffix, and create multiple domain user accounts by using bulk import.



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

Explain the lab objectives.

Instruct the students to run the batch file noted in Lab Setup.

Objectives

After completing this lab, you will be able to:

- Create and use an alternate user principal name suffix.
- Create multiple domain user accounts by using bulk import.
- Administer domain user accounts.

Lab Setup

- To complete this lab, you need to run the batch file `C:\Moc\Win2154a\Labfiles\Lrights.bat` to set the Log on Locally user right for the Users group, so that any user will have the right to log on locally to your computer.

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: 30 minutes

Exercise 1

Creating User Accounts by Using an Alternative User Principal Name Suffix

Scenario

After acquiring a new organization, Contoso, Ltd., the parent organization Northwind Traders decides to add all Contoso, Ltd. user accounts to the Northwind Traders domain. To keep the identity of Contoso, Ltd. separate from Northwind Traders, a user principal name suffix will be created and used for the user accounts of former Contoso, Ltd. employees.

Goal

In this exercise, you will create a user principal name suffix and use this suffix to create a test user account. Then, you will verify that a user can log on by using this user principal name.

Tasks	Detailed Steps
1. Create the following user principal name suffix: contoso.msft	- Log on as Administrator with a password of password. - Open Active Directory Domains and Trusts from the Administrative Tools menu. - In the console tree, right-click Active Directory Domains and Trusts, and then click Properties. - In the Active Directory Domains and Trusts Properties dialog box, in the Alternative UPN suffixes box, type contoso.msft click Add, and then click OK. - Close Active Directory Domains and Trusts.
2. Within <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), create the following OU: Contoso	- Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, right-click <i>domain.nwtraders.msft</i>, point to New, and then click Organizational Unit. - In the New Object – Organizational Unit dialog box, in the Name box, type Contoso and then click OK.
3. Within the Contoso OU, create a user account with the following properties: - Full name: TestUPN - User logon name: TestUPN@contoso.msft	- In the console tree, expand <i>domain.nwtraders.msft</i>, and then click Contoso. - Right-click Contoso, point to New, and then click User. - On the New Object – User page, in both the Full name and the User logon name boxes, type TestUPN - Click the drop-down list next to User logon name to review the list of user principal name suffixes, click @contoso.msft, and then click Next. - Click Next, and then click Finish. - Close Active Directory Users and Computers.

Tasks	Detailed Steps
4. Log on using the user logon name of TestUPN@contoso.msft to verify that the account works, and then log off.	a. Log off, press CTRL+ALT+DELETE to initiate the logon process, click Options to display the Log on to box, and then in the User name box, delete the existing text.  Notice that the Log on to box is enabled. b. In the User name box, type TestUPN@contoso.msft  Notice that the Log on to box is disabled when a user principal name is entered because the domain information is not needed. c. Click OK to complete the logon process. d. After you have successfully logged on as TestUPN, log off.

Exercise 2

Creating User Accounts by Using Bulk Import

Scenario

Because Northwind Traders has acquired a new organization, it has needed to add a new Package Handling department. Therefore, you need to create new user accounts for the Package Handling department. The information about the employees in this department was provided to your organization in a file exported from a database, so you decide that the most efficient solution is to use a bulk import method to create the user accounts.

Goal

In this exercise, you will use the **csvde** utility to create the user accounts for the employees in the Package Handling department.

To speed the process of formatting the information, the PackA.txt file contains the user information already in comma-separated value format to reduce the work needed to use the **csvde** bulk import utility.

Tasks	Detailed Steps
1. Within <i>domain.nwtraders.msft</i> , create the following OU: Package Handling	a. Log on as Administrator with a password of password . b. Open Active Directory Users and Computers from the Administrative Tools menu. c. In the console tree, right-click <i>domain.nwtraders.msft</i> , point to New , and then click Organizational Unit . d. In the New Object – Organizational Unit dialog box, in the Name box, type Package Handling and then click OK .
2. In the C:\Moc\Win2154a\Labfiles folder, open the file PackA.txt, view the contents, and then determine which bulk import attributes are being used.	■ In the Run box, type C:\Moc\Win2154a\Labfiles\PackA.txt and then click OK to open the PackA.txt file in Notepad.
 Extrapolating from the data in PackA.txt, what are the seven bulk import attributes used? For a list of attributes, see Appendix D, “Common User Account Attributes,” on the Student Materials compact disc. The bulk import attributes used are: department, dn, objectClass, sAMAccountName, telephoneNumber, userAccountControl, and userPrincipalName.	

Tasks	Detailed Steps
3. Edit the distinguished name and user principal name in the PackA.txt file so you can import the user accounts into your domain by using the csvde utility.	■ In Notepad, use the Replace feature to replace all occurrences of <i>domain</i> with your assigned domain name.
4. Add the attribute line to the PackA.txt file to match the user account bulk import data.	■ Add the seven bulk import attributes in the correct order, separated by commas, to the first line of the file. Hint: The file C:\Moc\Win2154a\Labfiles\PackAttr.txt contains the necessary list of attributes.
5. Edit the PackA.txt file to disable all of the user accounts with no department. Save this file as Pack.txt.	a. Edit the userAccountControl column to disable all user accounts with no department. Hint: The currently used userAccountControl value, 512, indicates that the account will be enabled. b. Save the edited file as C:\Moc\Win2154a\Labfiles\Pack.txt. c. Close the Pack.txt - Notepad window.
6. Use the csvde utility to perform a bulk import of Pack.txt.	a. Open a command prompt window. b. At the command prompt, type cd C:\Moc\Win2154a\Labfiles and then press ENTER. c. At the command prompt, type csvde /? and then press ENTER. d. Review the -i and -f options in the usage statement. e. At the command prompt, type csvde -i -f Pack.txt and then press ENTER.  <i>The csvde utility displays that 26 entries were modified successfully.</i> f. Close the command prompt window.

Exercise 3

Administering User Accounts

Scenario

The Help desk at Northwind Traders has received a number of administrative requests for the user accounts in the new Package Handling OU. The requests include enabling a user account, disabling a user account, resetting a password for a user account, and moving a user account.

Goal

In this exercise, you will use Active Directory Users and Computers to fulfill the administrative requests.

Tasks	Detailed Steps
1. Within the Package Handling OU, enable the following user account: Amie Baldwin	a. In Active Directory Users and Computers, in the console tree, expand <i>domain.nwtraders.msft</i>, and then click Package Handling. b. Right-click Package Handling, and then click Refresh to display the new user accounts. c. In the details pane, right-click Amie Baldwin, click Enable Account, and then click OK to close the message confirming that the Amie Baldwin user account has been enabled.  Notice that the icon next to the user account Amie Baldwin reflects the enabled account status.
2. Within the Package Handling OU, disable the following user account: Matthew Dunn	▪ Click Package Handling, right-click Matthew Dunn, click Disable Account, and then click OK to close the message confirming that the Matthew Dunn user account has been disabled.  Notice that the icon next to the user account Matthew Dunn reflects the disabled account status.
3. Reset the password of the following user account to Sc1234: Scott Culp Then, ensure that Scott changes his password the next time he logs on.	a. Right-click Scott Culp, and then click Reset Password. b. In the Reset Password dialog box, in both the New password and Confirm password boxes, type Sc1234 c. Select the User must change password at next logon check box, click OK, and then click OK again to close the message confirming that the password was changed.
4. Move the following user account to the Contoso OU: Derek Graham Verify that the account has been moved, and then log off.	a. Right-click Derek Graham, and then click Move. b. In the Move dialog box, click Contoso, and then click OK. c. Click Contoso, and then verify that the account for Derek Graham is listed in the details pane. d. Close Active Directory Users and Computers, close all open windows, and then log off.

◆ Using Groups in Active Directory

Topic Objective

To introduce topics related to using groups in Active Directory.

Lead-in

Active Directory provides support for different types of groups. Groups enable you to assign permissions for all of these domain resources once, rather than assign permissions individually to each user.

- Introduction to Groups in Active Directory
- Using Global Groups
- Using Domain Local Groups
- Using Universal Groups

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

Groups simplify administration. Before you can effectively use groups, you need to understand the function of groups and the group types that you can create. Active Directory provides support for different types of groups, and also provides options to determine the group's scope, which is how the group can be used in multiple domains.

Introduction to Groups in Active Directory

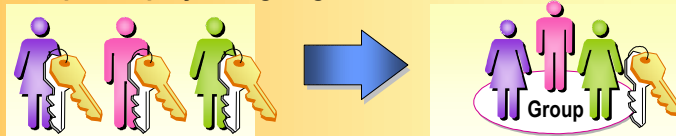
Topic Objective

To describe groups in Active Directory.

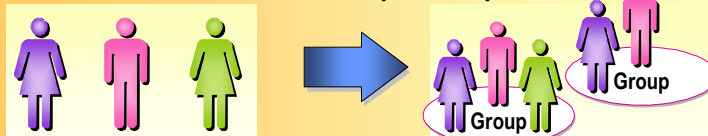
Lead-in

Use a security group to assign permissions to domain resources that are going to be used by several users.

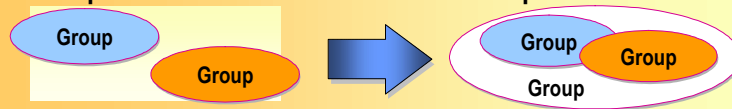
■ Groups Simplify Assigning Permission to Resources



■ Users Can Be Members of Multiple Groups



■ Groups Can Be Nested Inside Other Groups



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

Discuss groups in context of a domain and how users can be assigned permissions to gain access to resources across domains.

Emphasize that in a mixed domain mode there can be no nesting within the same group.

Key Points

When assigning permissions for resources, you should assign those permissions to a security group rather than to individual users.

Every user added to a security group receives the permissions defined for that group.

A user can be a member of many groups.

Groups can be nested into other groups. If a group is nested inside of another group, it inherits all of the permissions of that group.

Groups in Active Directory allow you to manage domain user access to domain resources by assigning permissions once to a group rather than multiple times to individual users. There are two group types in Active Directory, security groups and distribution groups. Both of these groups support one of the three group scopes, which are domain local, global, or universal. The group type and group scope that you can choose depend on the domain mode.

Users can be members of multiple groups. You use security groups to assign permissions to groups of users and computers. Distribution groups cannot be used for security purposes. Security and distribution groups have a scope attribute. The scope of a group determines who can be a member of the group, and where you can use that group in the network.

One way to use groups effectively is through *nesting*. Nesting means that you can add a group to another group. The nested group inherits the permissions of the group of which it is a member, thus simplifying the assigning of permissions to several groups at one time and reducing the traffic caused by replication of group membership changes. In a mixed-domain mode, there can be no nesting within the same group.

Note Groups can have up to 5,000 members. The user's primary group membership, such as Domain Users, is not stored in the group membership list.

For more information about groups, see Module 5, "Managing Access to Resources by Using Groups," in Course 2152, *Implementing Microsoft Windows 2000 Professional and Server*.

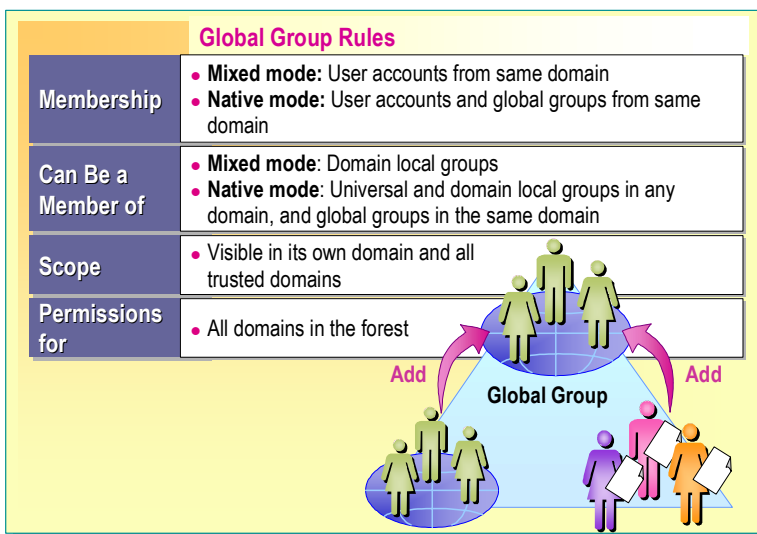
Using Global Groups

Topic Objective

To describe global groups and when to use them in Active Directory.

Lead-in

You use a global group to organize users who share the same job tasks and need similar network access requirements.



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

Some of the information discussed is not applicable for a universal distribution group.

Use a global group to organize users who share the same job tasks and need similar network access requirements.

The following summarizes the global group membership rules:

- *Membership.* Mixed mode can contain user accounts from the same domain. Native mode can contain user accounts and global groups from the same domain.
- *Can be a member of:* In mixed mode, the global group can be a member of only domain local groups. In native mode, the global group can be a member of universal and domain local groups in any domain, and global groups in the same domain.
- *Scope.* A global group is visible within its domain and all trusted domains, which include all of the domains in the forest.
- *Can be assigned permission for:* All domains in the forest.

Because global groups have a forest-wide visibility, they should not be created specifically for domain-specific resource access. Global groups are a good choice to organize users or groups of users. A different group type is more appropriate to control the access to resources within a domain.

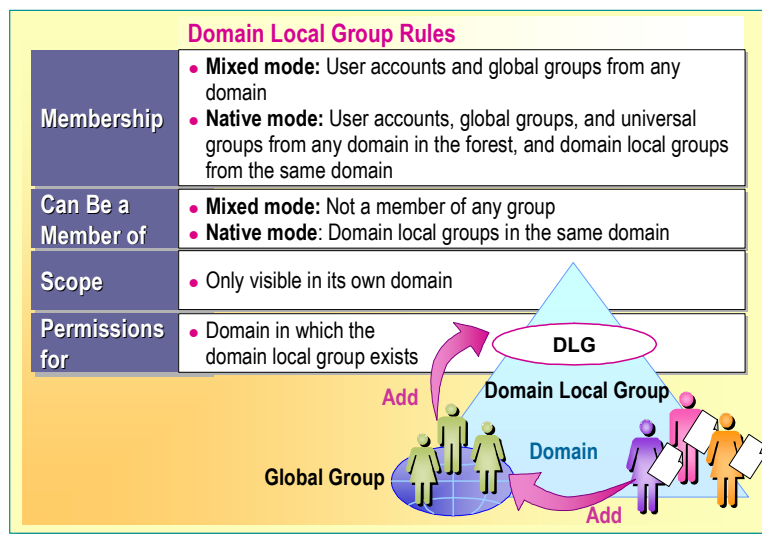
Using Domain Local Groups

Topic Objective

To describe domain local groups and when to use them in Active Directory.

Lead-in

You use a domain local group to assign access permissions to resources that are located in the same domain where you create the domain local group.



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

Use a domain local group to assign access permissions to resources that are located in the same domain in which you create the domain local group.

The following summarizes the domain local group membership rules:

- **Membership.** Mixed mode can contain user accounts and global groups from any domain. Native mode can contain user accounts, global groups, and universal groups from any domain in the forest, and domain local groups from the same domain.
- **Can be a member of:** In mixed mode, the domain local group cannot be a member of any group. In native mode, the domain local group can be a member of domain local groups in the same domain.
- **Scope.** The domain local group is visible only in its own domain.
- **Can be assigned permission for:** The domain in which the domain local group exists.

You can add all global groups that need to share the same resources into the appropriate domain local group.

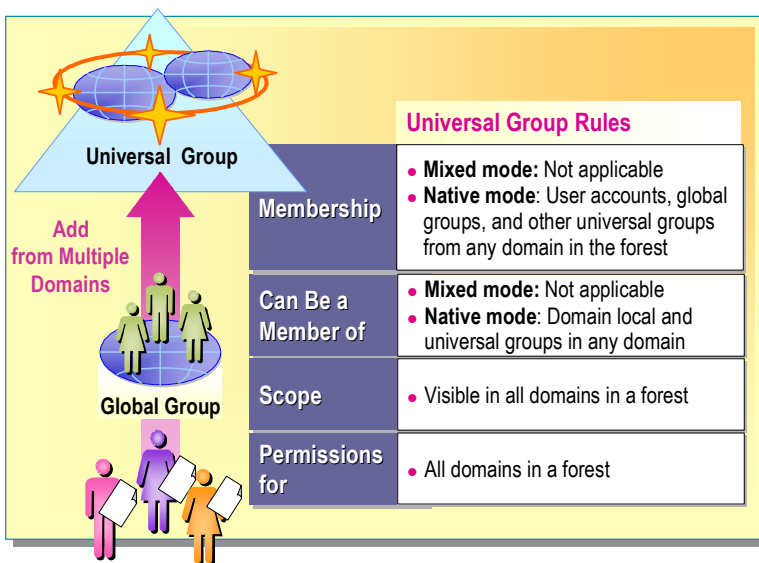
Using Universal Groups

Topic Objective

To illustrate the purpose of universal groups.

Lead-in

You use universal groups to nest global groups so that you can assign permissions to related resources in multiple domains.



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

When this module refers to universal groups, it is referring to the universal security group, not the distribution group.

The universal distribution group is available in a mixed-mode domain.

Use universal groups to nest global groups so that you can assign permissions to related resources in multiple domains. A Windows 2000 domain must be in native mode to use universal groups.

The following summarizes the universal group membership rules:

- *Membership.* You cannot create universal groups in mixed mode. Native mode can contain user accounts, global groups, and other universal groups from any domain in the forest.
- *Can be a member of:* The universal group is not applicable in mixed mode. In native mode, the universal group can be a member of domain local and universal groups in any domain.
- *Scope.* Universal groups are visible in all domains in the forest.
- *Can be assigned permission for:* All domains in the forest.

◆ Strategies for Using Groups in a Domain

Topic Objective

To introduce the topics related to using group strategies.

Lead-in

There are some recommended strategies that you can employ when using groups in Active Directory.

- Using Global and Domain Local Groups
- Class Discussion: Using Groups in a Single Domain

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

Make it clear to the students that the information about groups is presented in two separate modules. In this module, we will discuss using groups in a single domain, including global and domain local groups. In Module 10, we will discuss using groups in a multiple domain network, which includes universal groups.

To use groups effectively, you need a strategy for employing different group scopes. The scope of a group identifies the extent to which the group is applied in the tree or forest. In Active Directory, there are three different types of group scopes: universal, global, and domain local.

This topic addresses the scope of groups in a single domain network. In a single domain, global groups and domain local groups are the two group scopes that are available. By using the best group strategies for global and domain local groups, users will more effectively gain access to resources in a single domain network.

Note For more information about using groups in multiple domain networks, see Module 10, “Creating and Managing Trees and Forests,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

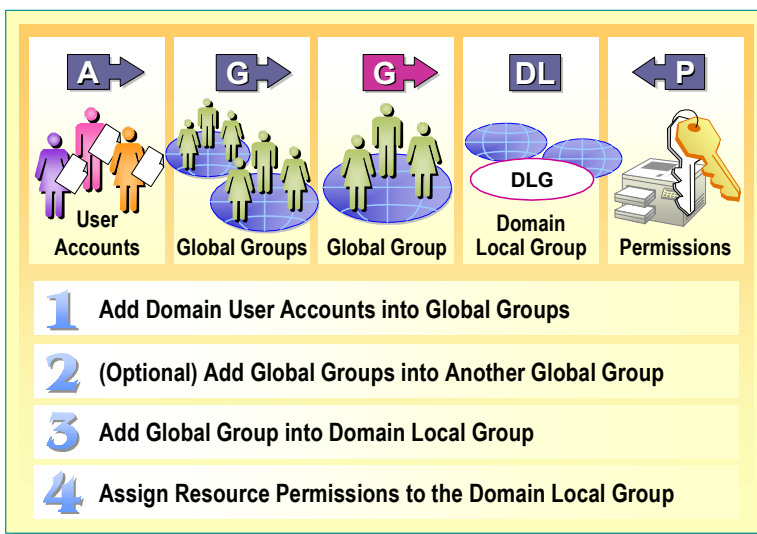
Using Global and Domain Local Groups

Topic Objective

To describe the best strategy to use global and domain local groups in Active Directory.

Lead-in

One of the recommended strategies for using both global and domain local groups is A G DL P.



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

The slide for this topic focuses on using the A G DL P strategy and the A G G DL P strategy.

There are other strategies that you can use; this one is recommended for its distributed administration and its scalability to multiple domains.

The recommended strategy for using both global and domain local groups is to add domain user accounts (A) into global groups (G), add global groups into domain local groups (DL), and then assign resource permissions (P) to the domain local groups. This strategy, *A G DL P*, provides the most flexibility while reducing the complexity of assigning access permissions to the network.

Using the A G DL P Strategy

As an example of using the A G DL P strategy, consider an organization that has users in the Accounts Payable OU and Accounts Receivable OU who need to gain access to accounting data in the Accounting database. Within the Accounts Payable OU and the Accounts Receivable OU, you create a global group for users who share the responsibility of reviewing accounting data. This global group needs to gain access to the accounting data in the accounting database. After the group is created, you add this group into a domain local group, and then the appropriate permissions on the accounting data are assigned to the domain local group.

The following example illustrates how to implement the A G DL P strategy:

1. Organize users based on administrative needs, such as their locations and job tasks, and then create a global group and add the user accounts into it. Create a global group called Accounts Payable and add all user accounts into it.
2. Create a domain local group into which you can add all global groups that need the same access to a resource. Add the Accounts Payable global group into the Accounting domain local group.
3. Assign the required permissions to the domain local group. Assign the necessary permissions to use the accounting data in the Accounting domain local group. In this way, if you add additional global groups to the Accounting domain local group, all users can gain access to the accounting data.

Using the A G G DL P Strategy

Consider another situation in which users in multiple departments need the same type of access to multiple resources. In such a situation, nesting of global groups is a good choice. For example, if all users in the Accounts Payable and Accounts Receivable departments in the Accounting division need access to the accounting data, use the existing global groups in each department.

The following example illustrates the A G G DL P strategy:

1. Create Accounts Payable and Accounts Receivable global groups, and add appropriate user accounts into each global group.
2. Create an Accounting Division global group representing all of the users in that Accounting division. Add the Accounts Payable and Accounts Receivable global groups into the Accounting Division global group.
3. Add the Accounting Division global group into the appropriate domain local groups that control access to resources.
4. Assign the necessary permissions to use the accounting data in the Accounting domain local group.

Class Discussion: Using Groups in a Single Domain

Topic Objective

To check students' understanding of how to use groups in a single-domain environment.

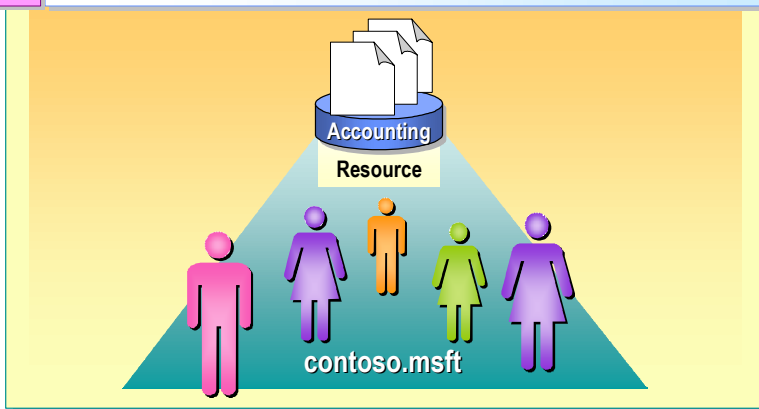
Lead-in

This example shows how to use groups in a single-domain environment. Take a few minutes to come up with a solution, and then we will discuss it as a class.



Managers Need to Gain Access to the Accounting Database

How Do You Set Up Groups?



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

Delivery Tip

There are three slides in the presentation for this topic. Use the first slide to introduce the scenario.

Use the second slide to discuss the solution for the first question.

Use the third slide to discuss the solution for the second question.

Contoso, Ltd. headquarters has a single domain that is located in Paris. Contoso, Ltd. has managers who need to gain access to the inventory database to perform their jobs.

- What would you do to ensure that the managers have the required access to the inventory database?
 - a. **Place all of the managers into a global group.**
 - b. **Create a domain local group for inventory database access.**
 - c. **Add the global group into the domain local group and assign permissions to gain access to the inventory database in the domain local group.**

Contoso, Ltd. wants to react more quickly to market demands. It has been determined that the accounting data needs to be available to the entire accounting staff. Contoso, Ltd. wants to create the group structure for the entire Accounting division that includes the Accounts Payable and Accounts Receivable departments.

- What would you do to ensure that the managers have the required access and that there is a minimum of administration?
 - a. **Make sure that your network is running in native mode. If not, you will first need to convert it to a native mode network.**
 - b. **Create three global groups. One group called Accounting Division will represent all department accountants. Name the other two groups Accounts Payable and Accounts Receivable to represent the organizational structure of the accounting department. Add the Accounts Receivable and Accounts Payable groups into the Accounting Division global group in each domain.**
 - c. **Place the Accounting Division global group into the domain local group so that users can gain access the accounting data.**
 - d. **Create a domain local group called Accounting Data. Add this group to the accounting data resources file with the appropriate permissions.**

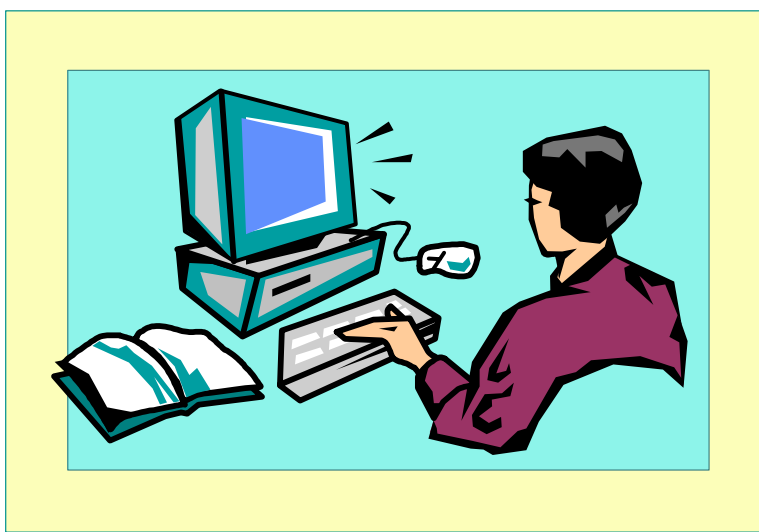
Lab B: Setting Up and Administering Groups in a Single Domain

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create and add global groups, and implement the recommended group strategy.



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

Explain the lab objectives.

Instruct the students to run the batch file noted in Lab Setup.

Objectives

After completing this lab, you will be able to:

- Create and nest global groups.
- Create domain local groups and assign permissions to resources.
- Implement and test the recommended group strategy.

Prerequisites

Before working on this lab, you must:

- Know the difference between mixed mode and native domain mode.
- Understand the recommended strategy for using groups to manage access to domain resources.

Lab Setup

- To complete this lab, you need to run the batch file
C:\Moc\Win2154a\Labfiles\Groups.bat to create folders and text files for the Human Resources departments so that you can assign permissions to these resources.

Estimated time to complete this lab: 30 minutes

Exercise 1

Creating the Global Group Structure

Scenario

The Human Resources division at Northwind Traders has recently grown to include the following three departments, Benefits, Payroll, and Training. The Human Resources vice president has announced a division-level initiative to make the administrative structure of all of the departments uniform. Therefore, you need to create a new global and domain local group structure for the managers in the Human Resources division. This structure must include the maintenance of groups at the department level while still maintaining a single current group for all managers at the division level. Resource access will be granted to the appropriate domain local groups for both department level data and division level data.

Goal

In this exercise, you will create the OU structure for the Human Resources division, which includes creating an OU for each of the three departments. You will then create global groups for managers in each of the departments, and then create a global group for all of the managers in the Human Resources division. You will then nest the three department global groups into the Human Resources division global group.

Tasks	Detailed Steps
 What domain mode should your domain be using to meet the stated goal and why? Native mode, because the goal states that the department global groups will be added to another global group. Mixed mode does not provide this type of group nesting.	
1. Within <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), create the following OU structure: - Human Resources - Human Resources\Benefits - Human Resources\Payroll - Human Resources\Training	- Log on as Administrator with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, right-click <i>domain.nwtraders.msft</i>, point to New, and then click Organizational Unit. - In the New Object – Organizational Unit dialog box, in the Name box, type Human Resources and then click OK. - Expand <i>domain.nwtraders.msft</i>, and then click Human Resources. - Right-click Human Resources, point to New, and then click Organizational Unit. - In the New Object – Organizational Unit dialog box, in the Name box, type Benefits and then click OK. - Repeat steps f and g, changing step g as required, to create the organizational units Payroll and Training under the Human Resources OU.

Tasks	Detailed Steps
2. Within the OUs corresponding to the group names, create the following global security groups for each department: • Benefits Managers • Payroll Managers • Training Managers	a. Expand Human Resources, right-click Benefits, point to New, and then click Group. b. In the New Object – Group dialog box, in the Group name box, type Benefits Managers. c. Ensure that Group scope is set to Global and that Group type is set to Security, and then click OK. d. Repeat steps a through c, changing steps a and b as required, to create Payroll Managers under the Payroll OU, and to create Training Managers under the Training OU.
3. Create the HR Managers global security group for the division in the Human Resources OU.	a. Right-click Human Resources, point to New, and then click Group. b. In the New Object – Group dialog box, in the Group name box, type HR Managers. c. Ensure that Group scope is set to Global and Group type is set to Security, and then click OK.
4. Make each department managers' group a member of the HR Managers group.	a. Click Human Resources, in the details pane, right-click the HR Managers global group, and then click Properties. b. In the HR Managers Properties dialog box, on the Members tab, click Add. c. In the Select Users, Contacts, Computers, or Groups dialog box, in the Name box, scroll to the bottom of the list and click Benefits Managers, and then click Add. d. Repeat step c to add Payroll Managers and Training Managers, and then click OK. e. In the HR Managers Properties dialog box, on the Members tab, ensure that the three department global groups are listed as members of the HR Managers global group, and then click OK.
 If a user account is added to the Benefits Managers group, will you also need to update the membership of the HR Managers group? No, because the HR Managers group has the Benefits Managers group as a member.	

Exercise 2

Creating the Domain Local Groups and Assigning Permissions to Resources

Scenario

The global group structure for the Human Resources division has been created. The domain local groups need to be created and used to assign the Human Resources managers access to resources. Permissions will be granted only to domain local groups.

Goal

In this exercise, you will create the domain local groups Benefits Data, Payroll Data, and Training Data for each department. You will assign to the domain local groups permissions to access the departmental resources. Having separate domain local groups for each department provides greater flexibility in assigning access to resources.

Tasks	Detailed Steps
1. Within the OUs corresponding to the group names, create the following domain local security groups for each department: - Benefits Data - Payroll Data - Training Data	a. In Active Directory Users and Computers, expand Human Resources, right-click Benefits, point to New, and then click Group. b. In the New Object – Group dialog box, in the Group name box, type Benefits Data. c. Set Group scope to Domain local and ensure that Group type is set to Security, and then click OK. d. Repeat steps a through c, changing steps a and b as required, to create Payroll Data under the Payroll OU, and Training Data under the Training OU.
2. Within the Human Resources OU, create the following domain local security group: HR Data.	a. Right-click Human Resources, point to New, and then click Group. b. In the New Object – Group dialog box, in the Group name box, type HR Data. c. Set Group scope to Domain local and ensure that Group type is set to Security, and then click OK.
3. Assign the domain local group in each department full control permission to the corresponding folder under C:\Hr.	a. In the Run box, type C:\Hr and then click OK. b. In the C:\HR window, right-click the Benefits folder, and then click Properties. c. In the Benefits Properties dialog box, on the Security tab, click Add. d. In the Select Users, Contacts, Computers, or Groups dialog box, in the Name box, scroll toward the bottom of the list and click Benefits Data, click Add, and then click OK. e. In the Benefits Properties dialog box, in the Permissions box, select the check box to allow Full Control, and then click OK. f. Repeat steps b through e, changing steps b through e as required, to assign Full Control permissions on the Payroll folder to Payroll Data, and on the Training folder to Training Data.

Tasks	Detailed Steps
4. Remove inherited permissions and assign read permissions on the C:\Hr folder to HR Data.	a. In the C:\HR window, change to the C:\ folder. b. Right-click the HR folder and then click Properties. c. In the HR Properties dialog box, on the Security tab, click Add. d. In the Select Users, Contacts, Computers, or Groups dialog box, in the Name box, scroll toward the bottom of the list and click HR Data, click Add, and then click OK. e. Click to clear the Allow inheritable permissions from parent to propagate to this object check box, click Remove to close the dialog box asking whether to copy or remove the inherited permissions, and then click OK to close the HR Properties dialog box. f. Close the C:\ window.

Exercise 3

Using Global and Domain Local Groups

Scenario

Managers will have full control of file resources within their departments. Managers will also have read access to resources in the other departments. User accounts will only directly belong to the global group for their department. Connect the global and domain local groups to achieve this result. Testing will be performed to verify proper access to resources.

Goal

In this exercise, you will add the division level global group to the domain local groups to allow access to resources. You will allow managers to have full control of file resources within their departments and read access to file resources in the other departments. You will create a test user account, and verify that a manager in the Benefits department has read access to all of the human resources data and full control access to the data the manager's own department.

Tasks	Detailed Steps
1. Add each department global group as a member of the corresponding domain local group.	- In Active Directory Users and Computers, expand the Human Resources OU. - Click the Benefits OU, in the details pane, right-click Benefits Data, and then click Properties. - In the Benefits Data Properties dialog box, on the Members tab, click Add. - In the Select Users, Contacts, Computers, or Groups dialog box, in the Name box, scroll toward the bottom of the list and click Benefits Managers, click Add, click OK, and then click OK again to close the Benefits Data Properties dialog box. - Repeat steps b through d, changing steps b through d as required, to add Payroll Managers to Payroll Data, and add Training Managers to Training Data.
2. Add the HR Managers global group as a member of the HR Data domain local group.	- In the console tree, click the Human Resources OU, in the details pane, right-click HR Data, and then click Properties. - In the HR Data Properties dialog box, on the Members tab, click Add. - In the Select Users, Contacts, Computers, or Groups dialog box, in the Name box, scroll toward the bottom of the list and click HR Managers, click Add, click OK, and then click OK again to close the HR Data Properties dialog box.

Tasks	Detailed Steps
3. To test the group structure, in the Benefits OU, create a user account with the following properties: Full name: TestBenefits User logon name: TestBenefits@domain.nwtraders.msft Add this user account to the Benefits Managers global group.	- Click the Benefits OU, right-click Benefits, point to New, and then click User. - On the New Object – User page, in both the Full name and the User logon name boxes, type TestBenefits and then click Next. - Click Next, and then click Finish. - Right-click the user TestBenefits, and then click Properties. - In the TestBenefits Properties dialog box, on the Member Of tab, click Add. - In the Select Groups dialog box, under the Name column, click Benefits Managers, click Add, click OK, and then click OK again to close the TestBenefits Properties dialog box. - Close Active Directory Users and Computers.
4. Log off, and then log on as TestBenefits. Verify that you can gain full control access to the resource C:\Hr\Benefits\Benefits.txt, and only read access to C:\Hr\Payroll\Payroll.txt.	- Log off, and then log on as TestBenefits without typing a password. - In the Run box, type C:\Hr\Benefits\Benefits.txt and then click OK. - In the Benefits.txt – Notepad window, in the text box, type Some Modifications and then save and close the document. - In the Run box, type C:\Hr\Payroll\Payroll.txt and then click OK. - In the Payroll.txt – Notepad window, in the text box, type Some Modifications and then save the document.  <i>The Save As dialog box appears, which indicates that you do not have the permissions to save changes to this document.</i> - Click Cancel to close the Save As dialog box. - Close the Payroll.txt – Notepad window, and then click No to close the dialog box indicating that your changes will be not be saved.
 Did you have full control access to C:\Hr\Benefits\Benefits.txt but only read access to C:\Hr\Payroll\Payroll.txt? Yes. Because the user account TestBenefits is a member of Benefits Data, you have full control to resources in C:\Hr\Benefits. Also, because Test Benefits is a member of HR Data (but not a member of Payroll Data) you only had read access to the resources in C:\Hr\Payroll.	
5. Log off.	▪ Close all open windows, and then log off.

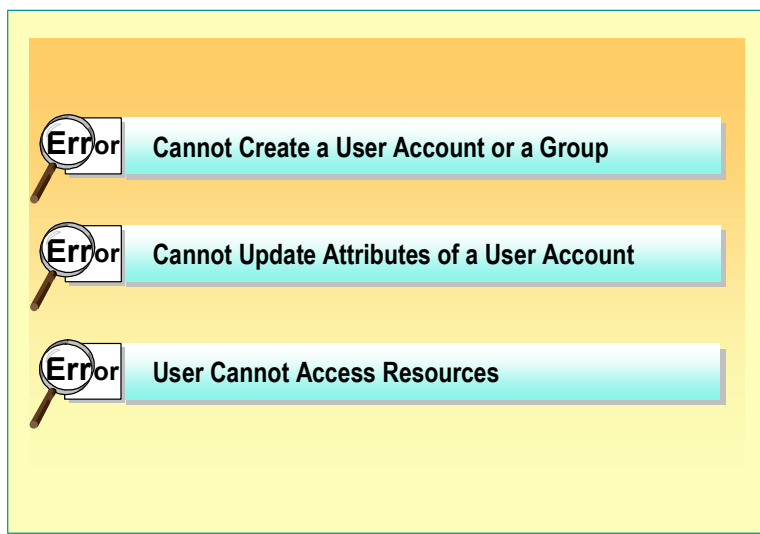
Troubleshooting Domain User Accounts and Groups

Topic Objective

To troubleshoot common problems with administering domain user accounts and groups.

Lead-in

You may encounter problems when setting up and administering users and groups in Active Directory.



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

You may encounter problems when setting up and administering domain user accounts and groups. The following list describes some of these potential problems and strategies for resolving them:

- Cannot create a user account or a group. The possible cause could be a violation of uniqueness rules. Recreate the user account or the group adhering to the uniqueness rules.
- Cannot update attributes of a user account. You may not have permission to update user accounts. Check the permissions assigned to you. If you do not have the permissions, log on as an administrator and then assign the appropriate permissions. You can also ask the administrator of that OU to assign you appropriate permissions.
- Users cannot access resources. The possible cause is that the user account is a member of a nested group that has been explicitly denied access to a resource.

Best Practices

Topic Objective

To apply best practices for administering domain user accounts.

Lead-in

Review this checklist before you set up and administer users and groups.



Have Users Use Their User Principal Names to Log On



Use the Forest Root Domain Name in a Multi-Domain Environment



Disable Imported User Accounts Until Needed



Create Global Groups Based on Job Functions

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

Emphasize the reason for each best practice.

The following list provides best practices for administering user accounts and groups:

- Have users use their user principal names, for example, `suzanf@contoso.msft`, instead of downlevel logon names, such as user names and domain names, when logging on from a computer running Windows 2000. By using their user principal name to log on, the user account can be moved from one domain to another without impacting the user.
- Use the forest root domain name for the user principal name suffix for user accounts in a multi-domain environment so that the name can be shorter and simpler. Also consider using a user principal name suffix that matches the user's e-mail address, which may include creating an alternative user principal name suffix.
- When creating multiple user accounts by using a bulk import method, disable the accounts if users are not going to use these accounts immediately. Because the password for an imported user account is initially blank, any unauthorized person with knowledge of the user account name could log on, set a new password, and then gain access to the network.
- Create global groups that are based on job functions. When you create a global group that is based on job functions and place the global groups in domain local groups, you need only change the group membership to accommodate changes in user job functions. For example, Cornelia Kunze is a user account in the global group Accountants, which is a member of the domain local group Accountant Files. The domain local group Accountant Files has read permissions to the accountants' audit share and modify permission to the accountant's documents share. If a new user is taking over Cornelia Kunze's job function, you need only remove Cornelia Kunze from the Accountant global group and add the new user to the Accountant global group. You do not need to change any permissions, because permissions are assigned to domain local groups that contain the global groups that contain the user accounts.

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 Users and Groups
- User Logon Names
- Creating Multiple User Accounts
- Administering User Accounts
- Using Groups in Active Directory
- Strategies for Using Groups in a Domain
- Troubleshooting Domain User Accounts and Groups
- Best Practices

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

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

1. Your organization has acquired a small subsidiary, and you want to use Active Directory Users and Computers to create domain user accounts for the new employees. For business reasons, the subsidiary wants to retain its former identity with its customers. How do you create user principal names for the new employees that match users' e-mail addresses without changing users' e-mail addresses?

Add a user principal name suffix to Active Directory that allows you to create logon names that match e-mail addresses. After you create this new suffix, you can then create user principal names that include the new suffix.

2. Your organization has recently hired many new employees to work in its new branch office, which is opening next month. You need to set up user accounts for these employees so that they can use and share network resources. You know that the Human Resources department has data on all new employees. What is the most efficient way to bulk import the user accounts?

Ask the Human Resources department to export their student data to a comma-delimited text file, or a line-separated text file. Edit the file so that it can be used for bulk import. Then use the csvde command or the ldifde command to create user accounts from the file that you edited. Because the new office has not yet opened, disable the user accounts during import.

3. What is the purpose of adding one group into another group?

Adding groups into other groups can reduce the number of times that you need to assign permissions.

4. What strategy should you apply when you use domain local and global groups?

Place user accounts (A) into global groups (G), optionally place global groups into global groups (G), place global groups into domain local groups (DL), and then assign permissions (P) on resources to the domain local groups.

