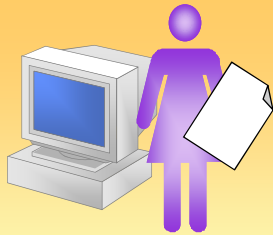


MICROSOFT OFFICIAL COURSE

Module 4

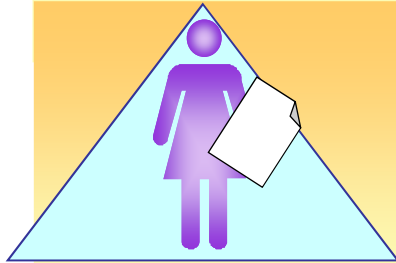
Implementing User Accounts and Groups

Introduction to User Accounts



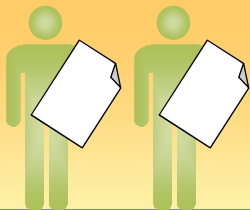
Local User Accounts

- Enable users to log on and access resources on a specific computer
- Reside in SAM



Domain User Accounts

- Enable users to log on to the domain to gain access to network resources
- Reside in Active Directory



**Administrator
and Guest**

Built-in User Accounts

- Enable users to perform administrative tasks or gain temporary access to network resources
- Reside in SAM (local built-in user accounts)
- Reside in Active Directory (domain built-in user accounts)

Guidelines for New User Accounts

- Naming Conventions
- Password Guidelines
- Account Options

What Are User Accounts?

A user account is an object that contains all of the information that defines a user in Windows Server 2008 R2

With a user account, you can:

- ☒ **Allow or deny users to log on based on their identity**
- ☒ **Grant users access to processes and services**
- ☒ **Manage users' access to resources**

Naming Conventions

- User Logon Names and Full Names Must Be Unique
- User Logon Names:
 - Can contain up to 20 characters
 - Can include a combination of special alphanumeric characters
- A Naming Convention Should:
 - Accommodate duplicate employee names
 - Identify temporary employees

Password Guidelines

- Assign a Password for the Administrator Account
- Determine Who Has Control over Passwords
- Educate Users on How to Use Passwords
 - Avoid obvious associations, such as a family name
 - Use long passwords
 - Use a combination of uppercase and lowercase characters

Account Options

- Set Logon Hours to Match Users' Work Hours
- Specify the Computers from Which a User Can Log On
 - Domain users can log on at any computer in the domain except for domain controllers, by default
 - Domain users can be restricted to specific computers to increase security
- Specify When a User Account Expires

Creating Local User Accounts

Local User Accounts Are:

- Created on Computers Running Windows 2000 Professional
- Created on Stand-alone or Member Servers Running Windows 2000 Server or Windows 2000 Advanced Server
- Reside in SAM

New User

User name: JYoung

Full name: Jonathan Young

Description:

Password: *****

Confirm: *****

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Create Close

What Is a Domain Controller?

Domain controllers :

- Provide authentication
- Host operations master roles
- Host the global catalog
- Support group policies and SYSVOL
- Provide for replication

Configuring DNS for AD DS

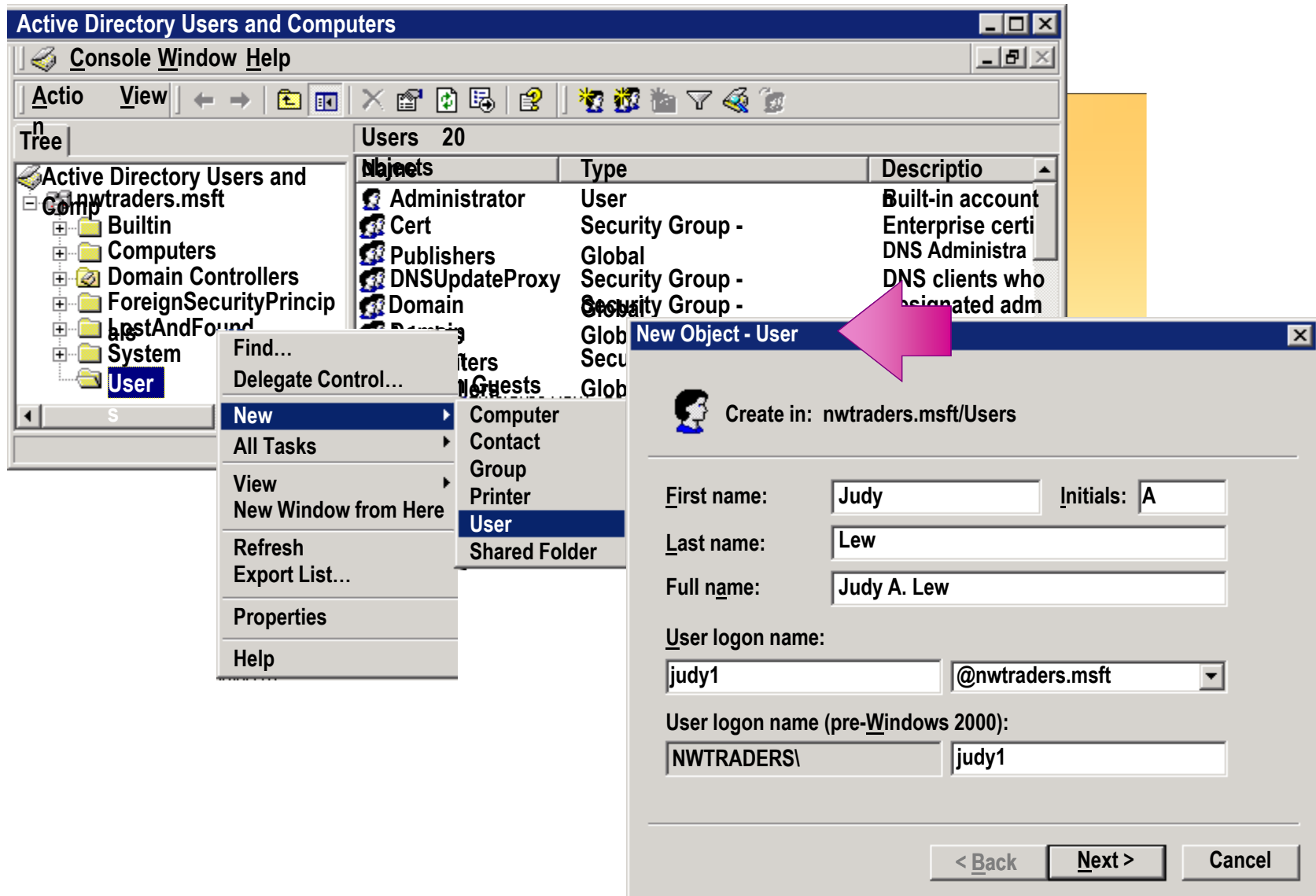
Considerations:

- You can install DNS as part of the domain controller deployment process
- You can integrate the DNS zone into AD DS
- Use secure dynamic updates for your DNS zone
- Use multiple DNS servers to provide for high availability and load balancing
- SRV records enable the location of AD DS and other services

Lesson 3: Managing Users, Groups, and Computers

- What Are User Accounts?
- What Are Groups?
- Nesting Groups
- Default Built-In Groups
- Computer Accounts
- Account Management Best Practices
- Demonstration: How to Manage Accounts

Creating a Domain User Account



Setting Password Requirements



The image shows a Windows-style dialog box titled "New Object - User". It features a user icon and a "Create in:" field with the path "nwtraders.msft/Users". Below this are two password input fields, both containing "*****". A list of four unchecked checkboxes follows: "User must change password at next logon", "User cannot change password", "Password never expires", and "Account is disabled". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

New Object - User

Create in: nwtraders.msft/Users

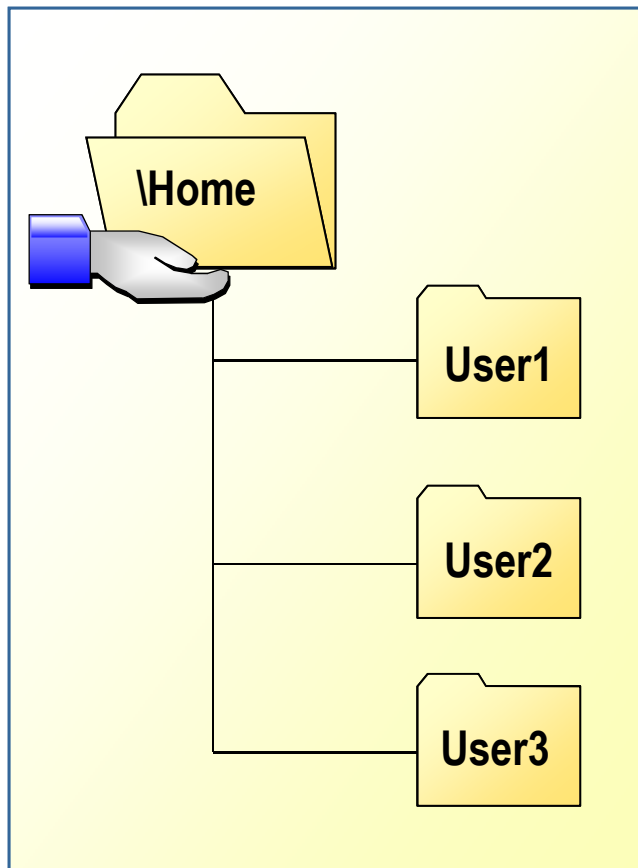
Password: *****

Confirm Password: *****

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled

< Back Next > Cancel

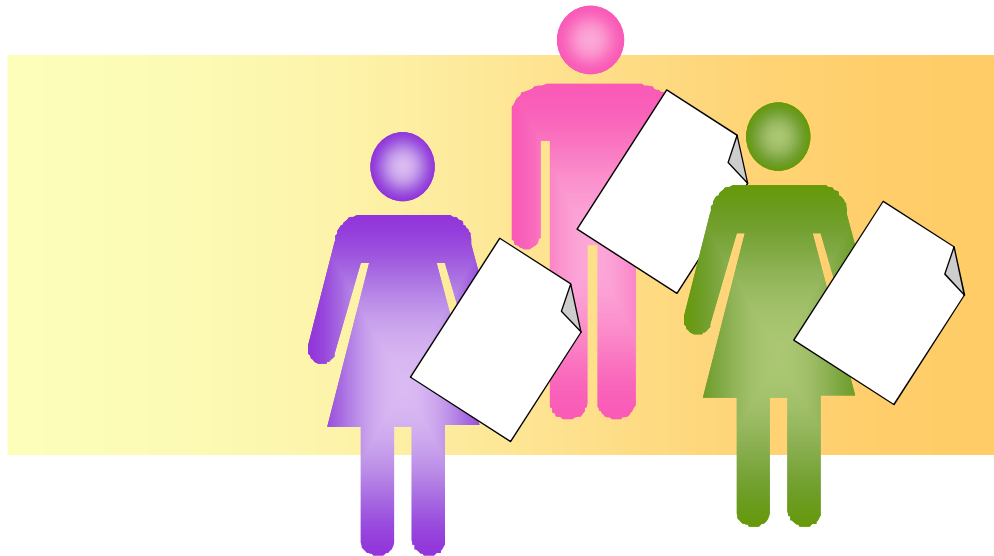
Managing User Data by Creating Home Folders



- Consider the Following When You Create a Home Folder:
 - Backup and restore capability
 - Sufficient space on the server
 - Sufficient space on users' computers
 - Network performance
- To Create a Home Folder:
 1. Create a shared folder on a server
 2. Assign the appropriate permission
 3. Provide a path for the user account

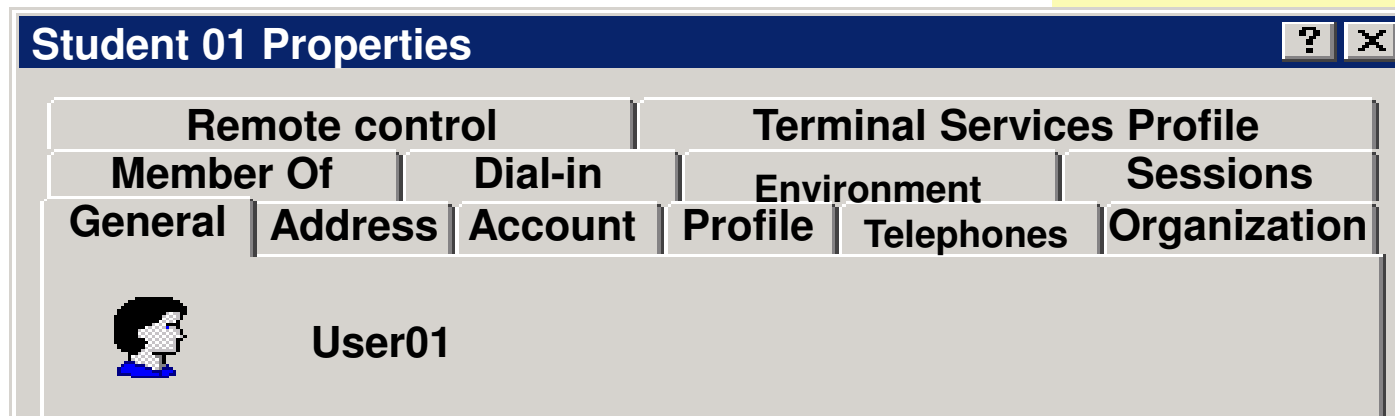
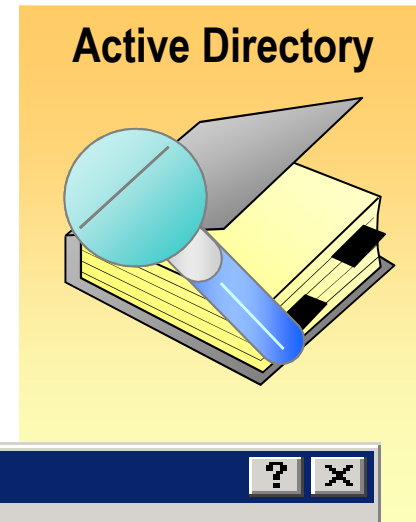
Setting Properties for Domain User Accounts

- **Setting Personal Properties**
- **Setting Account Properties**
- **Specifying Logon Options**
- **Copying Domain User Accounts**
- **Creating User Account Templates**

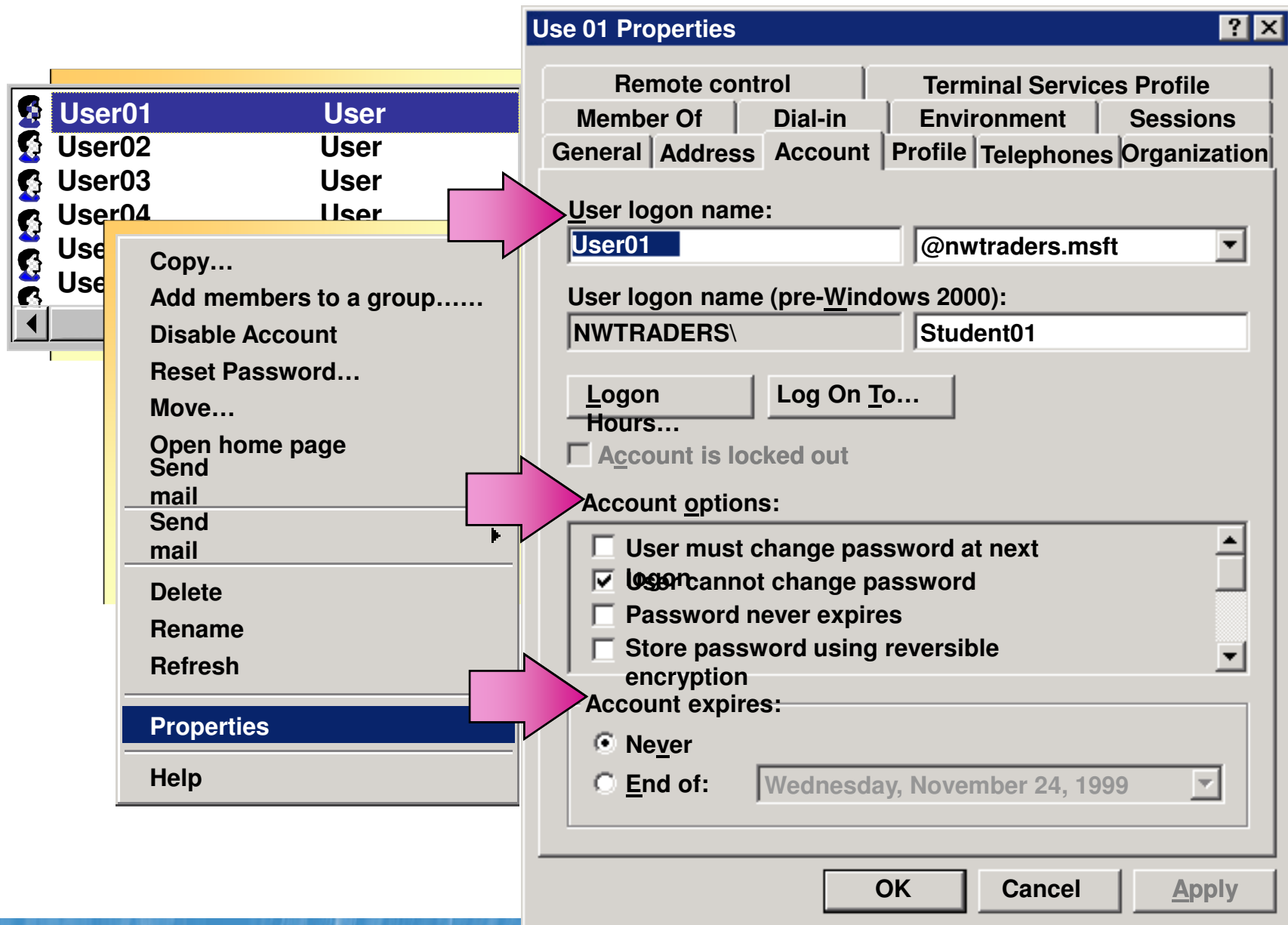


Setting Personal Properties

- Add Personal Information About Users As Stored in Active Directory
- Use Personal Properties to Search Active Directory



Setting Account Properties



Specifying Logon Options

Logon Hours for User01

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

Al	1	2	3	4	5	6	7	8	9	10	11	12
Sunday												
Monday												
Tuesday												
Wednesday												
Thursday												
Friday												
Saturday												

OK
Cancel

☐ Logon Permitted
☐ Logon Denied

Logon Workstations

This feature requires the NetBIOS protocol. In Computer name, type the pre-Windows 2000 computer name.

This user can log on to:

☐ All computers
☒ The following computers

Computer name:

Brisbane

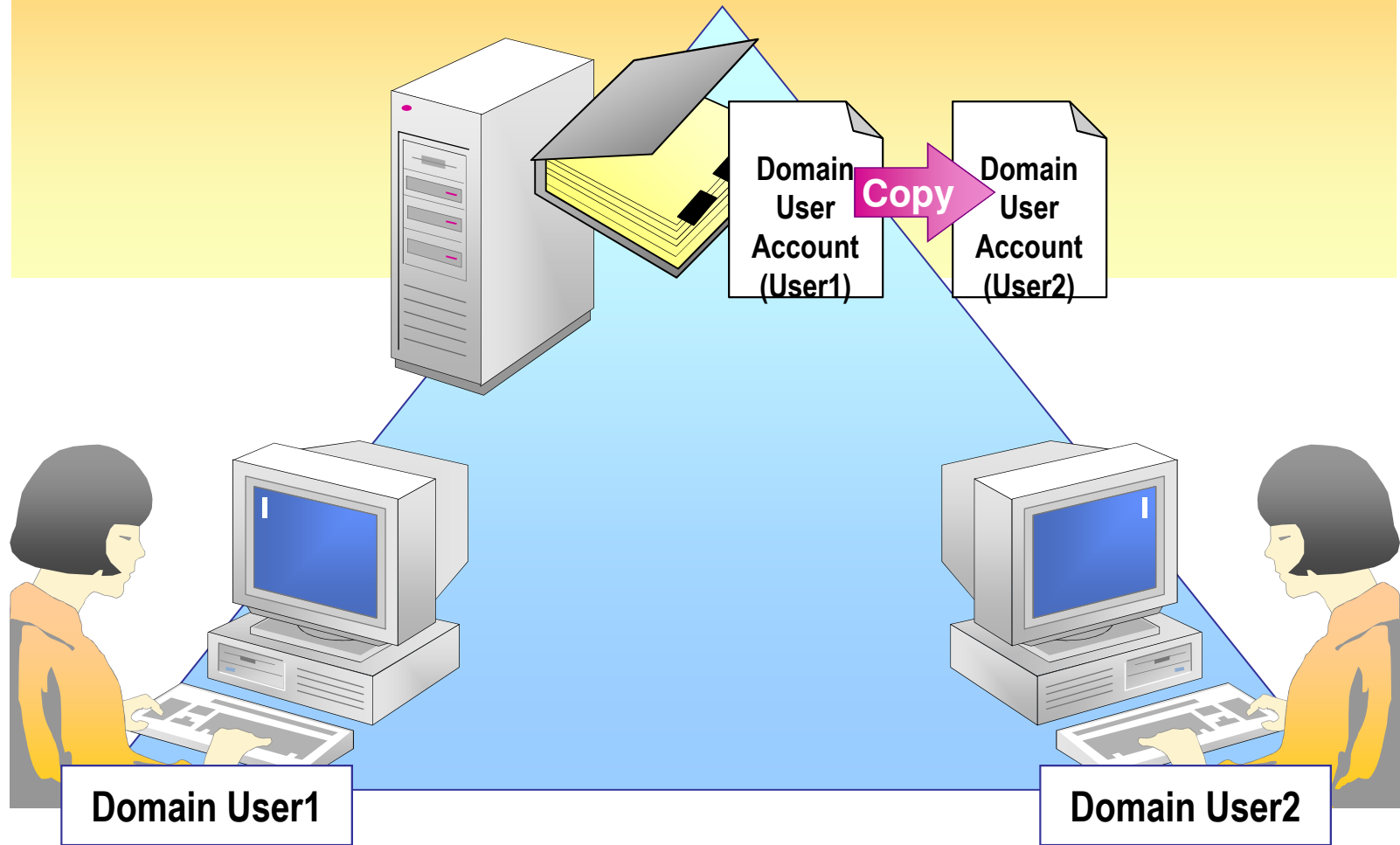
Perth

Add
Edit
Remove

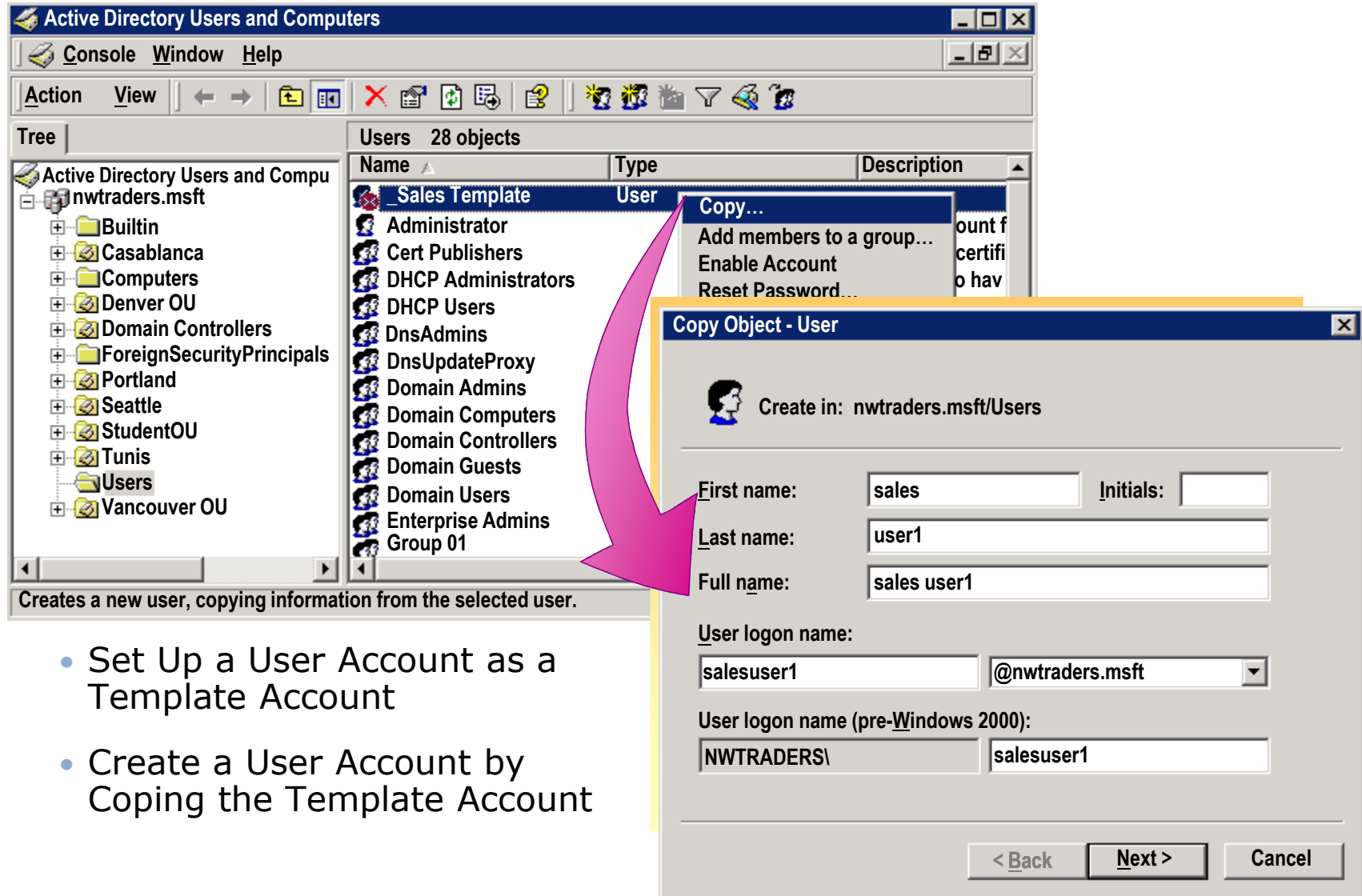
OK
Cancel

Copying Domain User Accounts

Copy an Existing Domain User Account to Simplify the Process of Creating a New Domain User Account.



Creating User Account Templates



The screenshot shows the 'Active Directory Users and Computers' console window. The left pane shows the tree structure with 'nwtraders.msft' expanded and 'Users' selected. The right pane shows a list of 28 objects, with 'Sales Template' (User) selected. A context menu is open over 'Sales Template', showing options: 'Copy...', 'Add members to a group...', 'Enable Account', and 'Reset Password...'. A pink arrow points from the 'Copy...' option to the 'Copy Object - User' dialog box. The dialog box is titled 'Copy Object - User' and shows 'Create in: nwtraders.msft/Users'. It contains fields for 'First name' (sales), 'Initials' (empty), 'Last name' (user1), 'Full name' (sales user1), 'User logon name' (salesuser1 @nwtraders.msft), and 'User logon name (pre-Windows 2000)' (NWTRADERS\ salesuser1). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Creates a new user, copying information from the selected user.

- Set Up a User Account as a Template Account
- Create a User Account by Coping the Template Account

What Are Groups?

A group is a collection of user accounts, computer accounts, contacts, and other groups that you can manage as a single unit

Two main types of groups:

- **Security**
- **Distribution**

Three scopes of groups:

- **Domain local**
- **Global**
- **Universal**

Nesting Groups

Use group nesting to add a group as a member to another group

Use the following best practices for nesting groups:



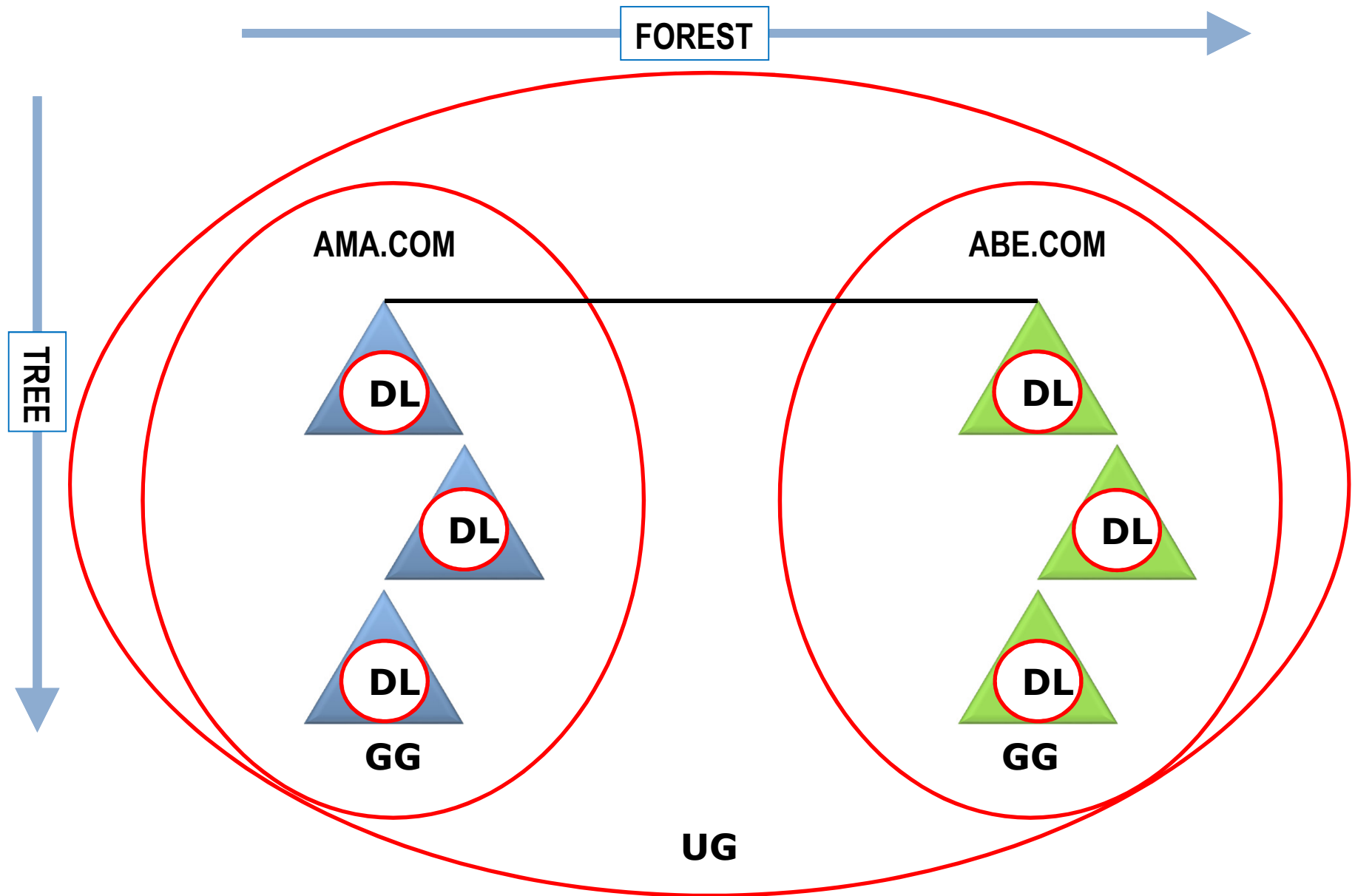
Accounts > Global > Domain Local < Permissions

For larger organizations, consider the following strategy:

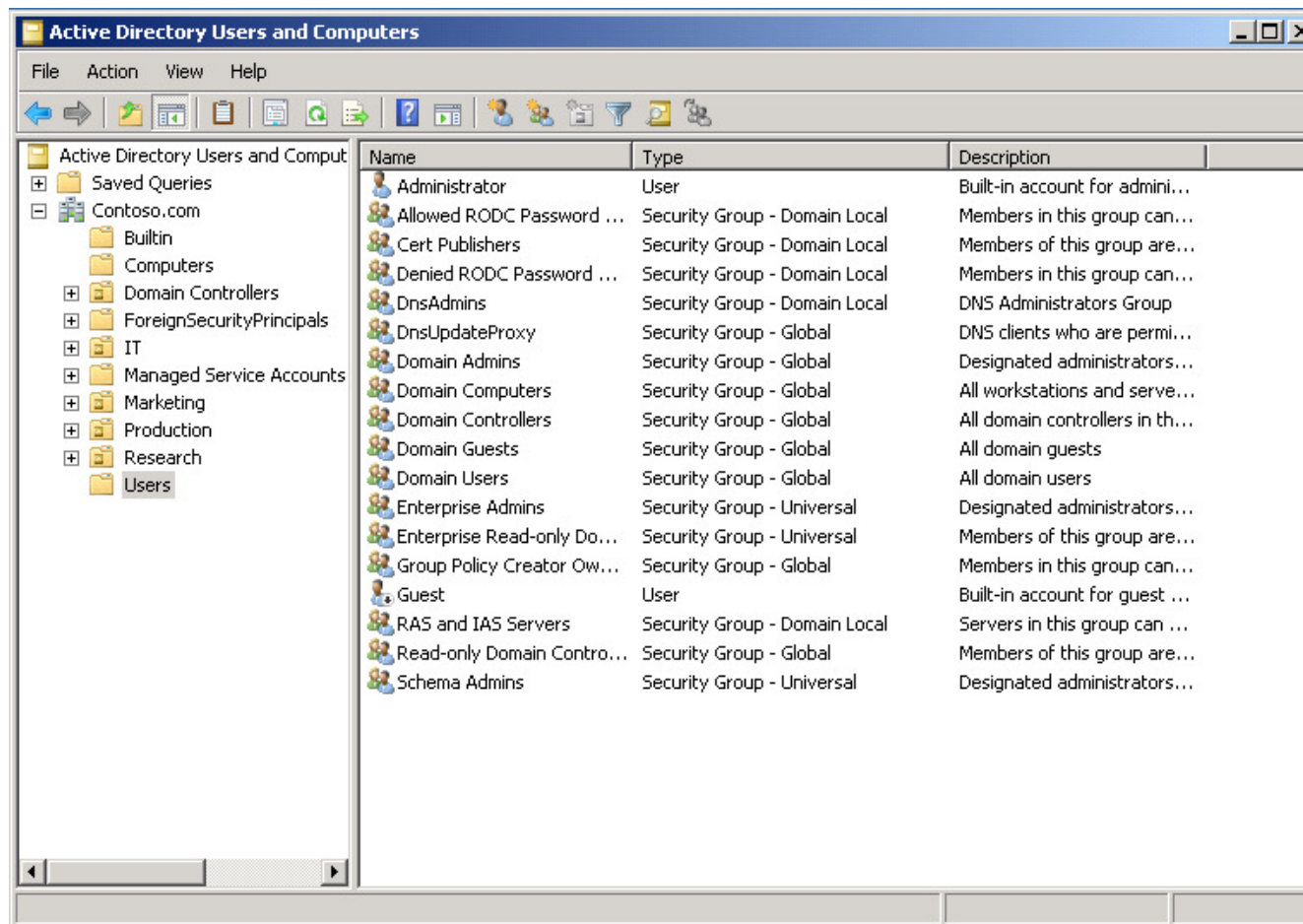


Accounts > Global > Universal > Domain Local < Permissions

Understanding Group Scope in a Domain

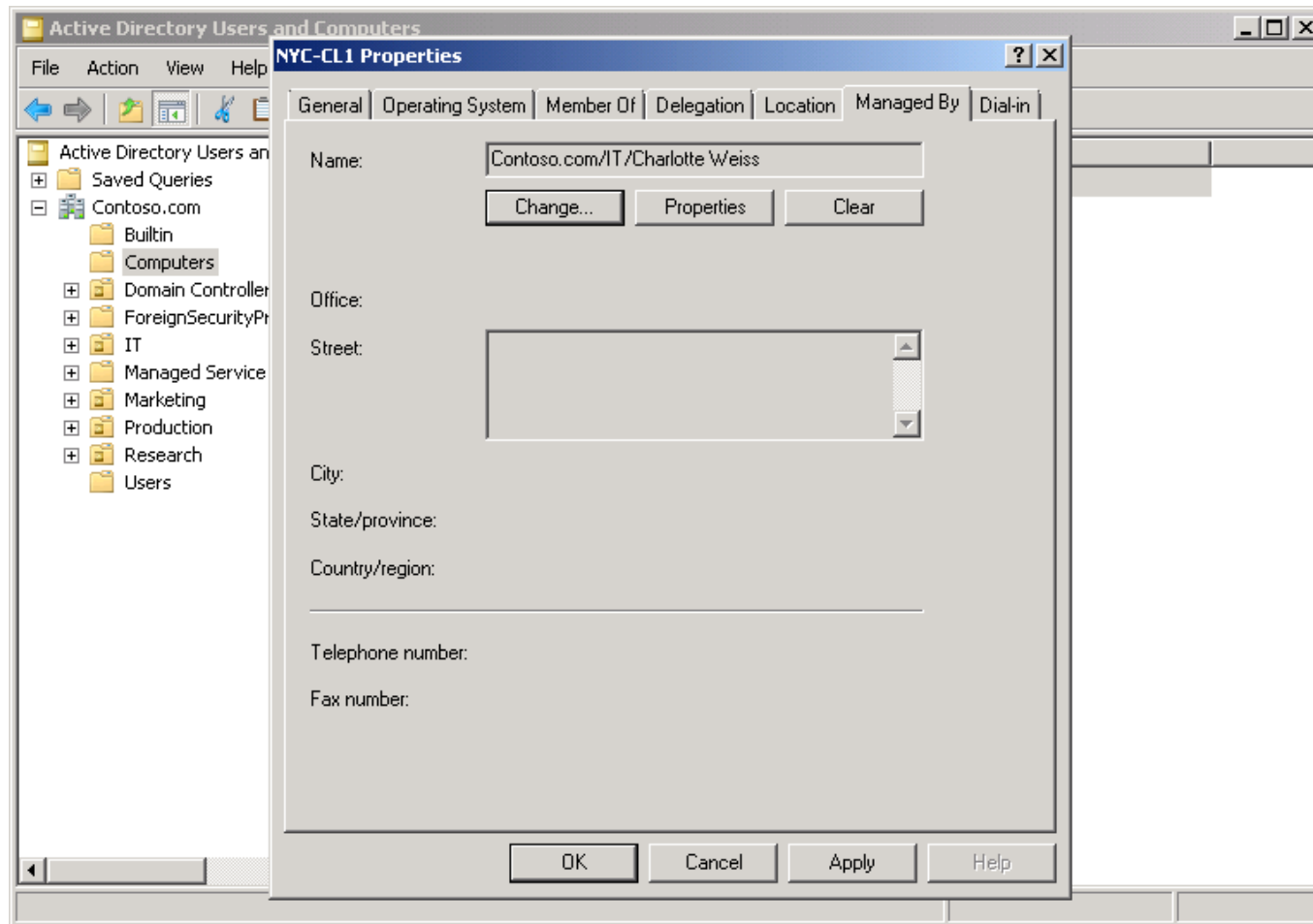


Default Built-In Groups



You can use the built-in groups to simplify administration

Computer Accounts



The most commonly used properties for computer accounts in AD DS are the Location and Managed By properties

Account Management Best Practices

- **Do not allow users to share accounts**
 - **Plan a naming convention for accounts**
 - **Do not use generic named accounts for temporary staff**
 - **Plan account policy settings to meet organizational needs**
- **Use built-in groups where appropriate**
 - **Nest groups for efficiency**
 - **Avoid assigning permissions directly to users**
 - **Use a naming convention that identifies group members**
- **Limit ability to create computer accounts**
 - **Implement a naming convention to identify computer role**
 - **Implement Manage By and Location Properties**

Demonstration: How to Manage Accounts

- In this demonstration, you will see how to manage a user account and add that account to a group

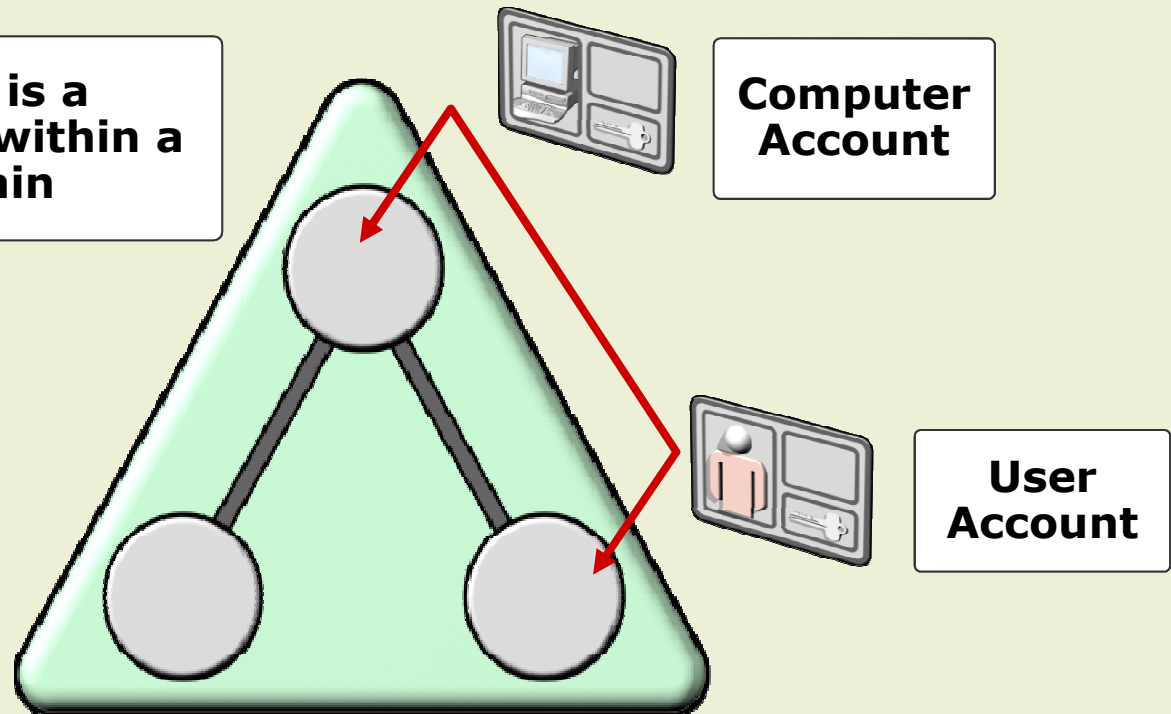
Lesson 4: Implementing Organizational Units

- Why Use Organizational Units?
- Demonstration: How to Manage Organizational Units
- Demonstration: How to Delegate Administration

Why Use Organizational Units?

Organizational units in a domain

An OU is a container within a domain



You can deploy your OUs into a hierarchical structure based on geography, department, resources, management requirements, or a combination of all of these

Demonstration: How to Manage Organizational Units

- In this demonstration, you will see how to create an organizational unit in ADAC and then add an object to it

Demonstration: How to Delegate Administration

- In this demonstration, you will see how to use Active Directory Users and Computers to allow a user to create and manage user objects in a specific organizational unit

Lesson 5: Implementing Group Policy

- What Is a GPO?
- Applying GPOs
- Creating and Managing GPOs
- Policies and Preferences
- Demonstration: How to Create a GPO and Link It to an Organizational Unit

What Is a GPO?

Group Policy enables IT administrators to automate one-to-many management of users and computers

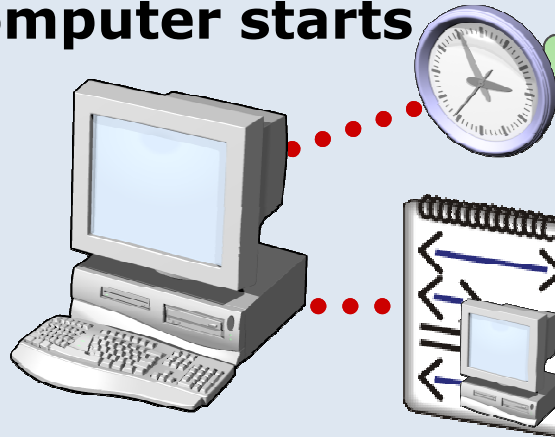
Use Group Policy to:

- **Apply standard configurations**
- **Deploy software**
- **Enforce security settings**
- **Enforce a consistent desktop environment**

Local Group Policy is always in effect for local and domain users and local computer settings

Applying GPOs

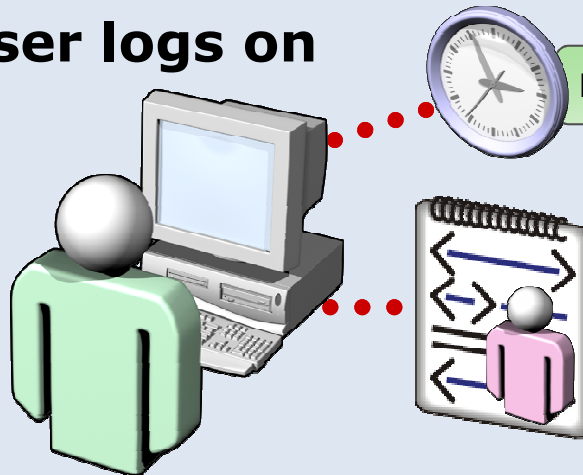
Computer starts



Refresh Interval: Every 90 minutes

- **Computer settings applied**
- **Startup scripts run**

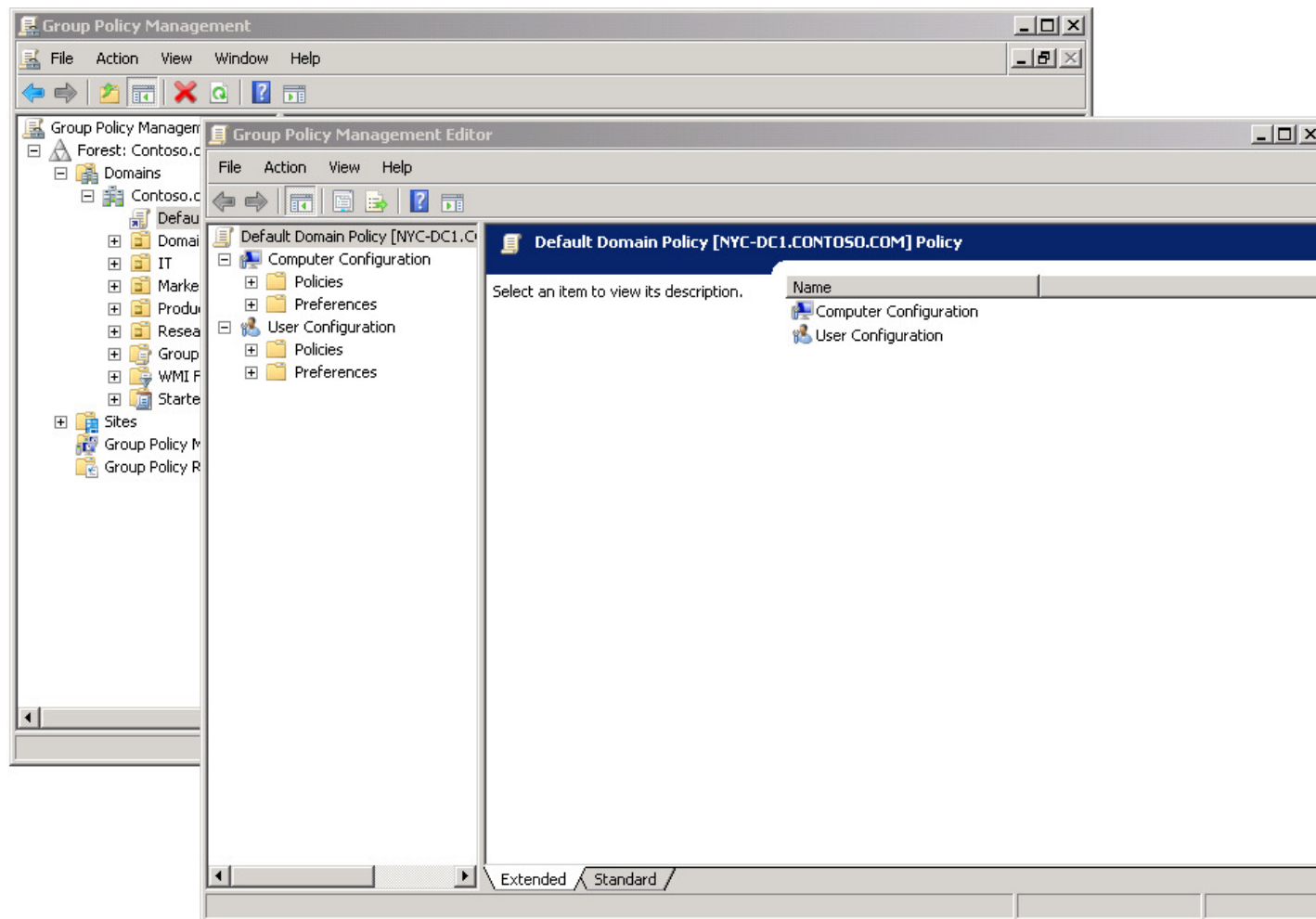
User logs on



Refresh Interval: Every 90 minutes

- **User settings applied**
- **Logon scripts run**

Creating and Managing GPOs



You can use a number of tools to create and manage GPOs, including the Group Policy Management Console

Policies and Preferences

Group Policy Preferences	Group Policy Settings
Are written to the normal locations in the registry that the application or operating system feature uses to store the setting.	Strictly enforce policy settings by writing the settings to areas of the registry that standard users cannot modify.
Do not cause the application or operating system feature to disable the user interface for the settings they configure.	Typically disable the user interface for settings that Group Policy is managing.
Refresh preferences by using the same interval as Group Policy settings by default.	Refresh policy settings at a regular interval.
Are not available on local computers.	Are available through local Group Policy.

Demonstration: How to Create a GPO and Link It to an Organizational Unit

- In this demonstration you will see how to create a GPO to restrict the use of task manager and how to link that GPO to a specific organizational unit

Module Review

- Review Questions
- Tools