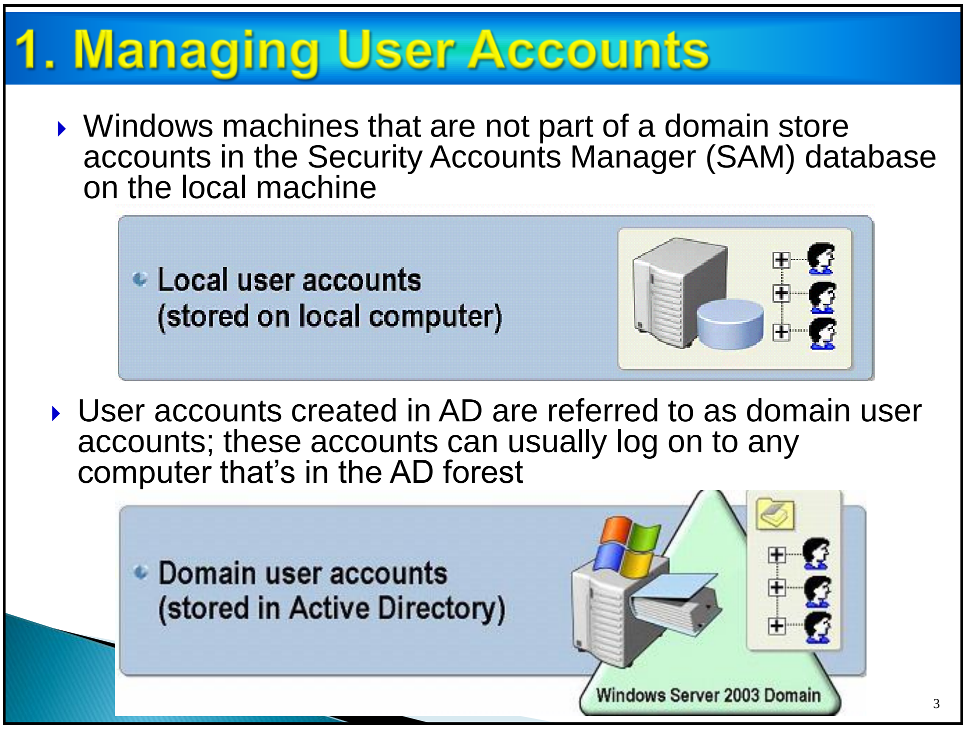
Chapter 6: Network Administration

Account and Group Management

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Objectives

1. Explain how to manage user accounts
2. Creating and Modifying User Accounts
3. Using user templates
4. Modifying Multiple Users
5. Modify account properties
6. Work with user profiles
7. Describe factors in managing group accounts
8. Work with computer accounts
9. Describe tools for automating account management



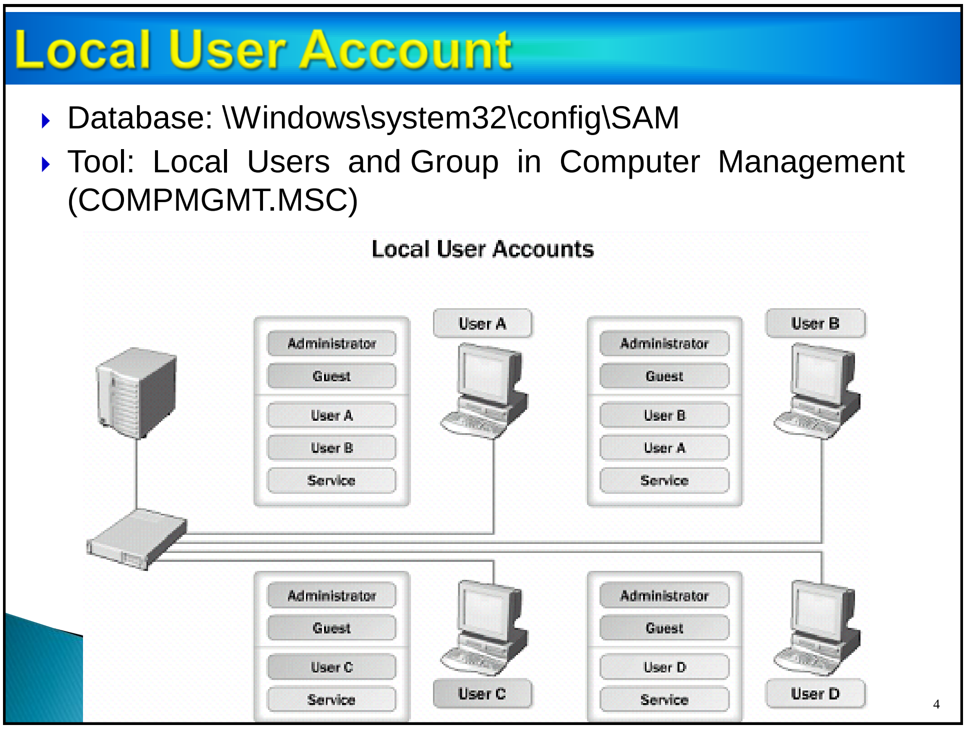
1. Managing User Accounts

- Windows machines that are not part of a domain store accounts in the Security Accounts Manager (SAM) database on the local machine

Local user accounts (stored on local computer)

- User accounts created in AD are referred to as domain user accounts; these accounts can usually log on to any computer that's in the AD forest

Domain user accounts (stored in Active Directory)



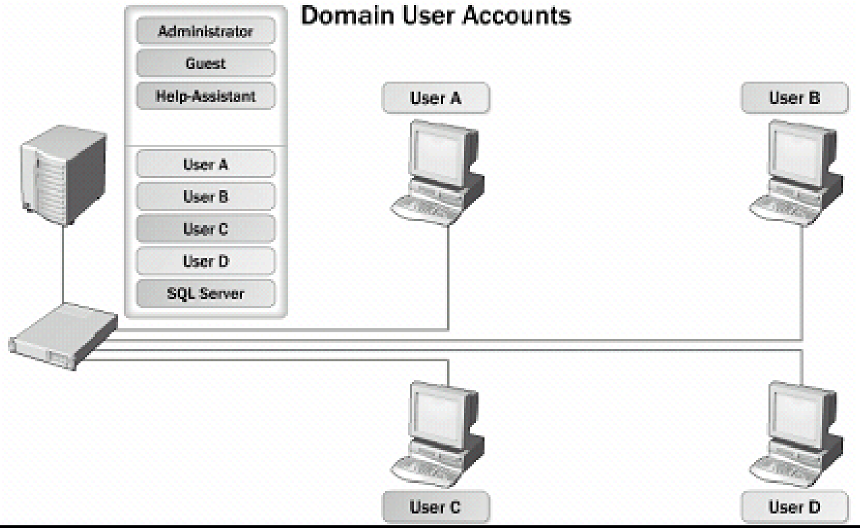
Local User Account

- Database: \Windows\system32\config\SAM
- Tool: Local Users and Group in Computer Management (COMPMGMT.MSC)

Local User Accounts

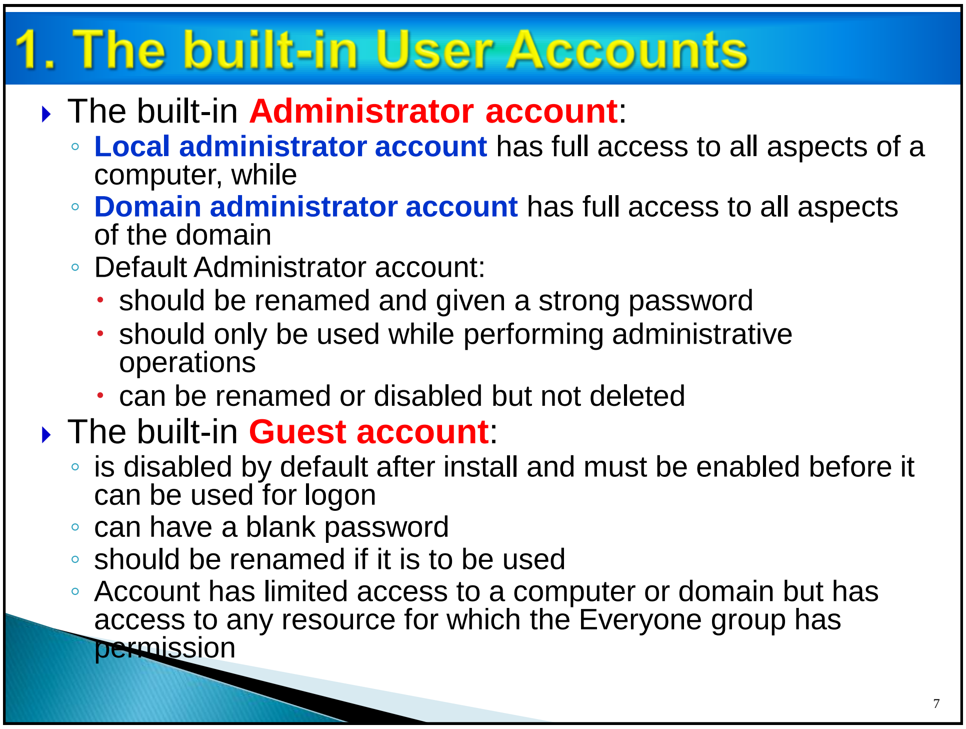
Domain User Account

- Database: \Windows\NTDS\NTDS.DIT
- Tool: Active Directory Users and Computer (DSA.MSC)



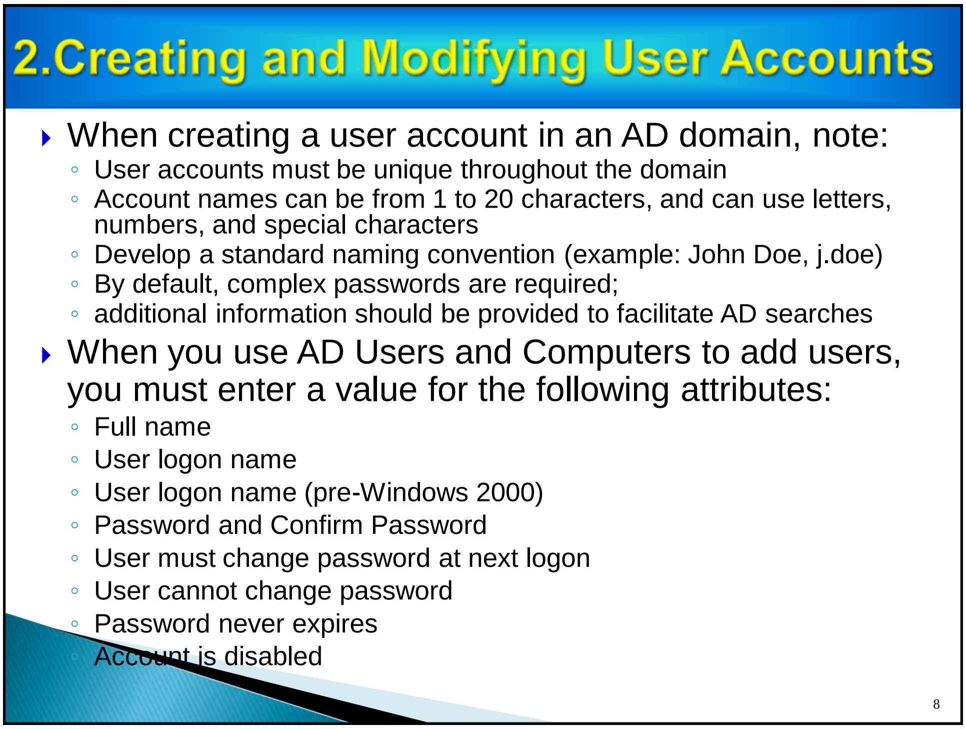
Managing User Accounts

- The built-in accounts
- Creating account
- Modify account
- Using user templates
- User properties
- User profile



1. The built-in User Accounts

- The built-in **Administrator account**:
  - **Local administrator account** has full access to all aspects of a computer, while
  - **Domain administrator account** has full access to all aspects of the domain
  - Default Administrator account:
    - should be renamed and given a strong password
    - should only be used while performing administrative operations
    - can be renamed or disabled but not deleted
- The built-in **Guest account**:
  - is disabled by default after install and must be enabled before it can be used for logon
  - can have a blank password
  - should be renamed if it is to be used
  - Account has limited access to a computer or domain but has access to any resource for which the Everyone group has permission



2.Creating and Modifying User Accounts

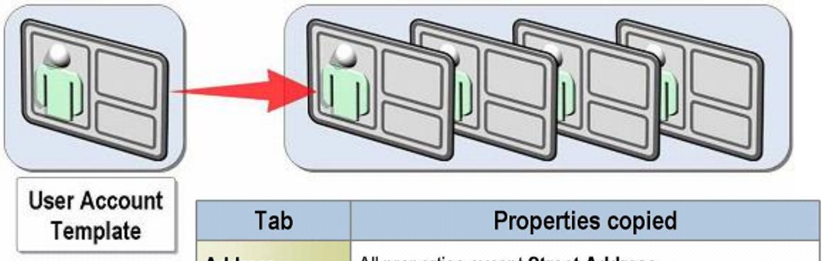
- When creating a user account in an AD domain, note:
  - User accounts must be unique throughout the domain
  - Account names can be from 1 to 20 characters, and can use letters, numbers, and special characters
  - Develop a standard naming convention (example: John Doe, j.doe)
  - By default, complex passwords are required;
  - additional information should be provided to facilitate AD searches
- When you use AD Users and Computers to add users, you must enter a value for the following attributes:
  - Full name
  - User logon name
  - User logon name (pre-Windows 2000)
  - Password and Confirm Password
  - User must change password at next logon
  - User cannot change password
  - Password never expires
  - Account is disabled

3. Modifying Multiple Users

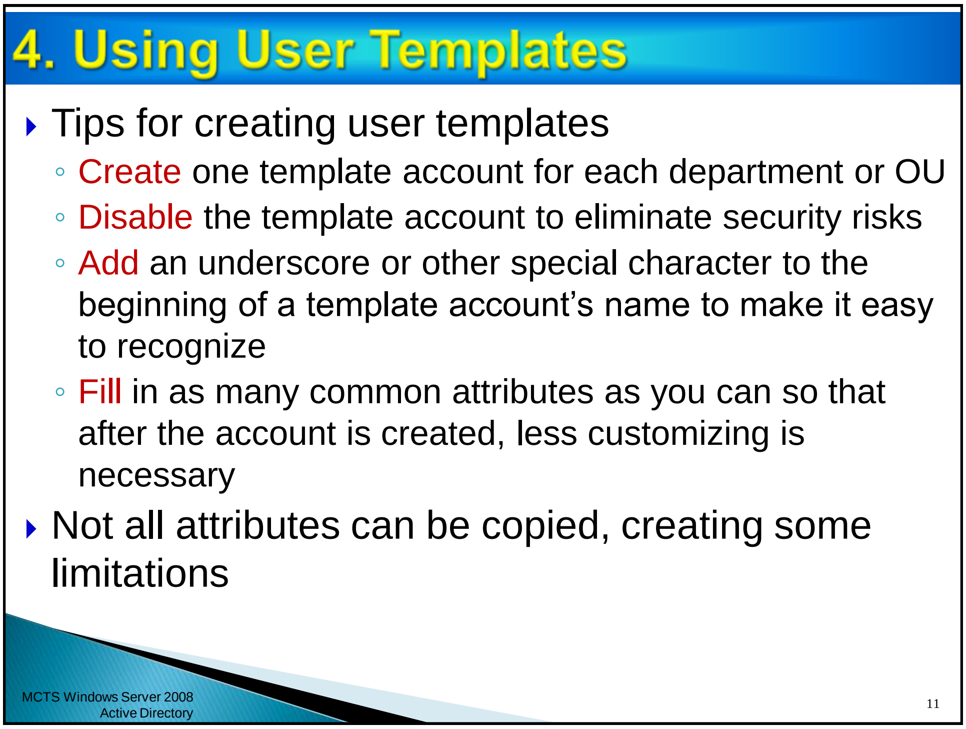
- Selecting multiple users using ctrl + click or shift + click allows them all to be edited simultaneously
- The following actions can be performed:
  - Add to a group
  - Disable account
  - Enable account
  - Move
  - Send Mail
  - Cut
  - Delete
  - Properties

4. Using User Templates

- A user template is a user account that contains the properties that apply to users with common requirements.
- User template make creating user accounts with standardized configuration more efficient

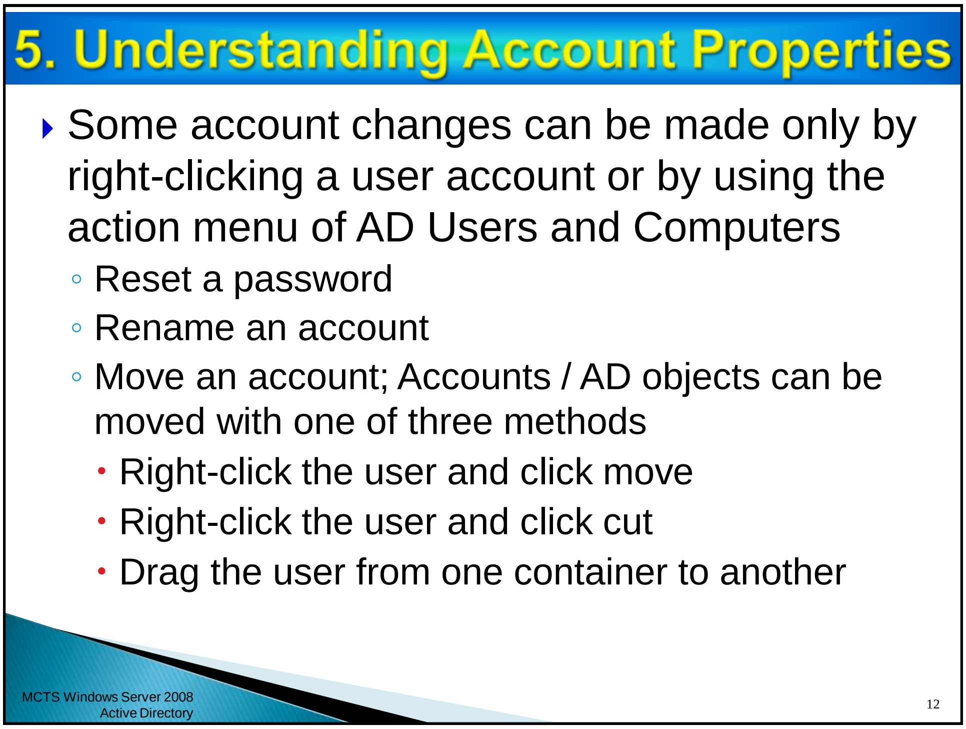


Tab	Properties copied
Address	All properties except **Street Address**
Account	All properties except **Logon Name**
Profile	All properties, except **Profile path** and **Home folder**, reflect new user's logon name
Organization	All properties except **Title**
Member Of	All properties



4. Using User Templates

- Tips for creating user templates
  - Create one template account for each department or OU
  - Disable the template account to eliminate security risks
  - Add an underscore or other special character to the beginning of a template account's name to make it easy to recognize
  - Fill in as many common attributes as you can so that after the account is created, less customizing is necessary
- Not all attributes can be copied, creating some limitations



5. Understanding Account Properties

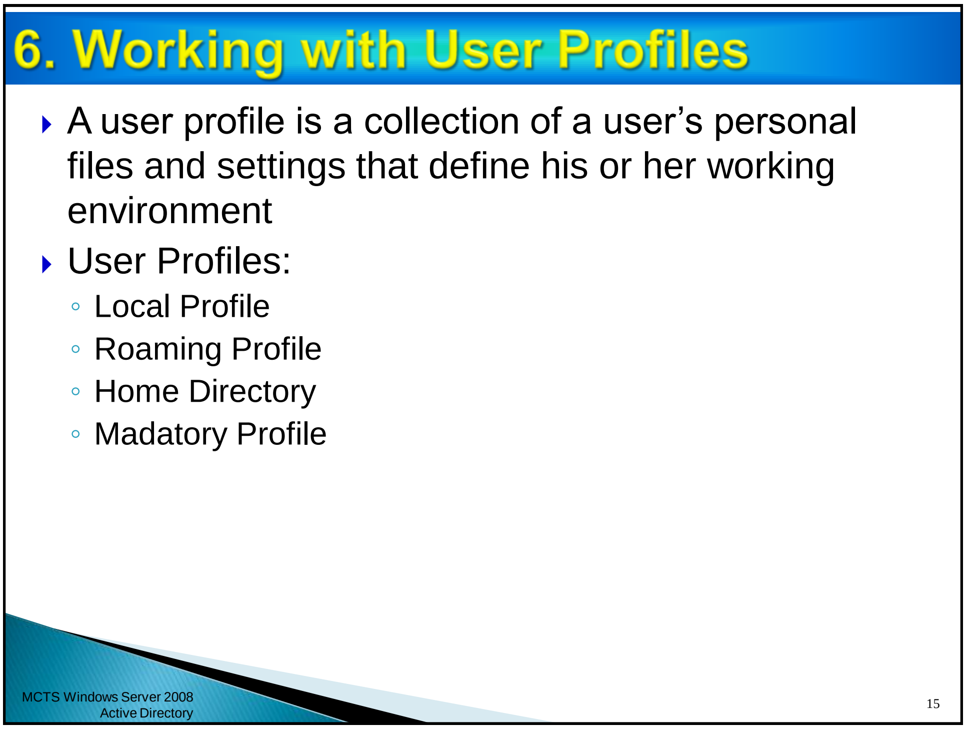
- Some account changes can be made only by right-clicking a user account or by using the action menu of AD Users and Computers
  - Reset a password
  - Rename an account
  - Move an account; Accounts / AD objects can be moved with one of three methods
    - Right-click the user and click move
    - Right-click the user and click cut
    - Drag the user from one container to another

The General Tab

- General Tab
  - Contains descriptive information about the account but does not affect the user’s account logon, group memberships, rights, or permissions
- Account Tab
  - Contains the information that most affects a user’s logon to the domain
- Profile Tab
  - Used to specify the location of files that make up a user’s profile, a logon script, and the location of a home folder
- Member Of Tab
- Terminal Services
  - Settings in these tabs affect a user’s session and connection properties when connecting to a Windows Server 2008 Terminal Services server

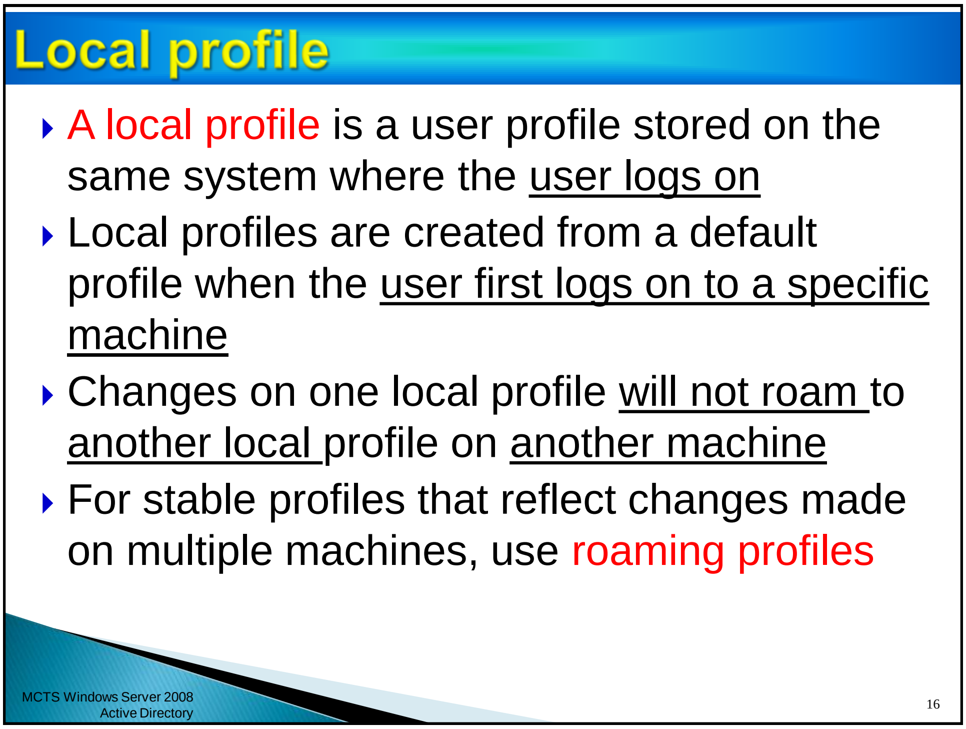
Using Contacts and Distribution Lists

- A contact is an Active Directory object that usually represents a person for informational purposes only
- Most common use of a contact is for integration into Microsoft Exchange’s address book
- Distribution lists are created in the same way as groups
- Distribution lists are also used with Microsoft Exchange to send e-mails, but to several people at once



6. Working with User Profiles

- A user profile is a collection of a user's personal files and settings that define his or her working environment
- User Profiles:
  - Local Profile
  - Roaming Profile
  - Home Directory
  - Madatory Profile



Local profile

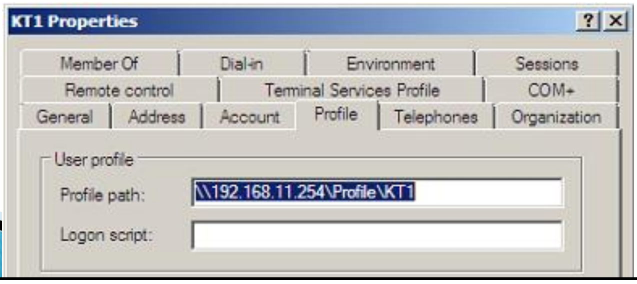
- A local profile is a user profile stored on the same system where the user logs on
- Local profiles are created from a default profile when the user first logs on to a specific machine
- Changes on one local profile will not roam to another local profile on another machine
- For stable profiles that reflect changes made on multiple machines, use roaming profiles

Roaming Profiles

- A roaming profile
  - follows the user no matter which computer he or she logs on to
  - Profile is copied from a network share when the user logs on to a computer in the network
  - Creates a local copy of the roaming profile, called a profile's cached copy
  - Changes made to the profile are then replicated from locally cached copy back to the profile on the network share when the user logs off.
- Configuring roaming profiles
  - Configuring a shared folder to hold roaming profiles
  - Configuring each user account's properties to specify the roaming profile's location
- The default or existing local profile will be copied to the roaming profile

How configure

- Create user
- Create folder: ex: Profile
- Share folder:
  - Sharing: full control-> everybody
  - Security: full control-> users
- User\properties\ Profile:
  - Profile path: \\IP\Profile\username (%username%)
- Test:
  - logon PC1 by KT1: creat 1 folder on Desktop
  - logon PC2 by KT1: have 1 folder on Desktop



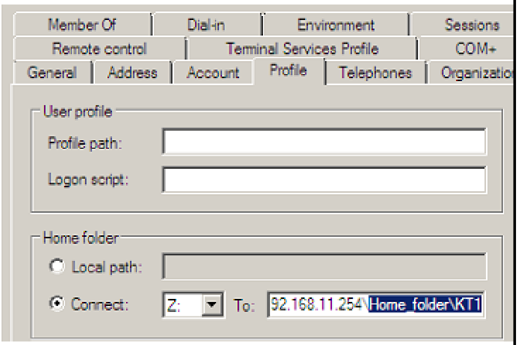
KT1 Properties

Profile path: \\192.168.11.254\Profile\KT1

Logon script:

Home folder

- Create user
- Create folder: ex: Home_folder
- Share folder:
  - Sharing: full control-> everybody
  - Security: full control-> users



User profile

Profile path:

Logon script:

Home folder

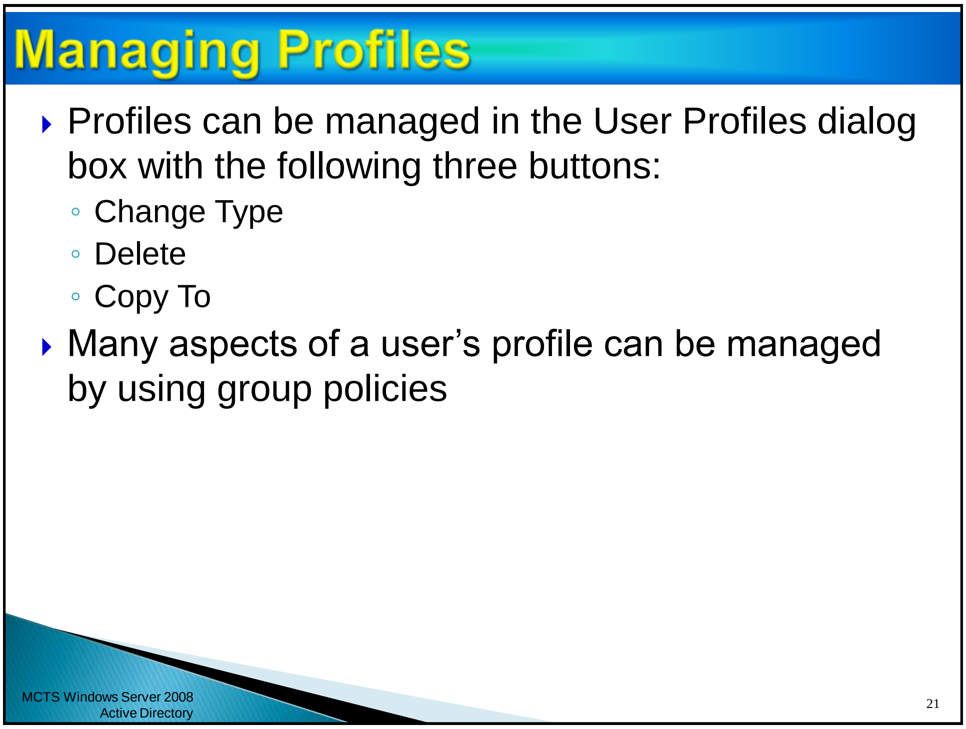
○ Local path:

● Connect: Z: To: 92.168.11.254\Home_folder\KT1

- User\properties\Profile:
  - Home folder:
    - Connect: X:.
    - To: \\IP\Home_folder\username
- Log on client PC and see:
  - (username)\Home_folder\ (Z:) -> network drive

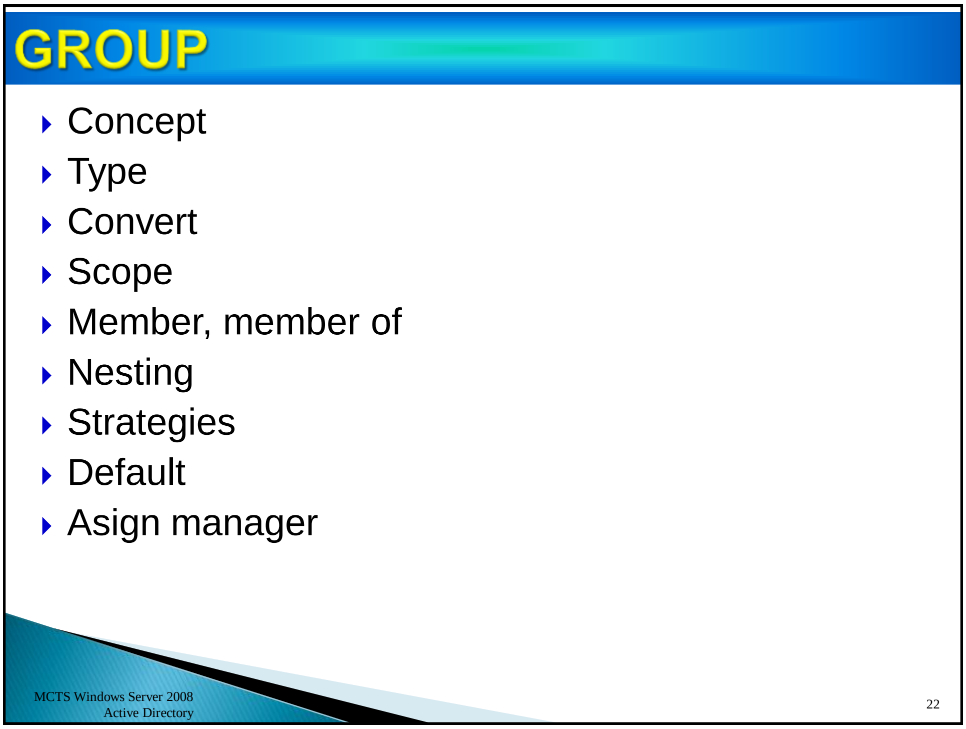
Mandatory Profiles

- Used when you don’t want users to be able to change their profile or only have the ability to make temporary changes
- Commonly used in situations where a common logon is assigned for multiple users
- Works like a roaming profile, but changes made to the profile will not be copied to the server



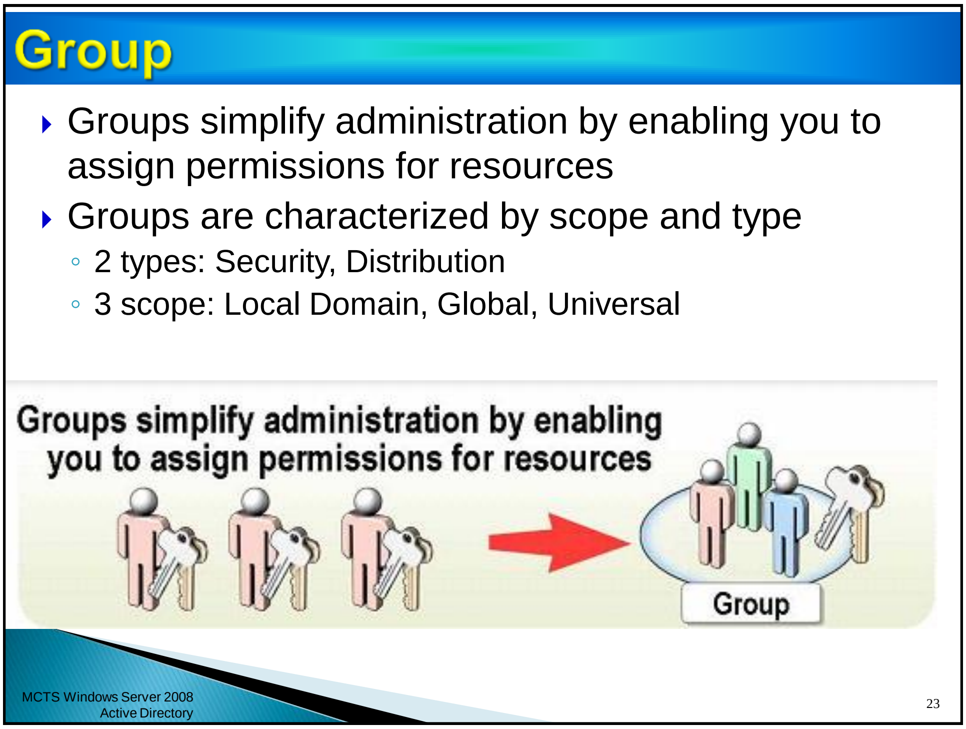
Managing Profiles

- Profiles can be managed in the User Profiles dialog box with the following three buttons:
  - Change Type
  - Delete
  - Copy To
- Many aspects of a user’s profile can be managed by using group policies



GROUP

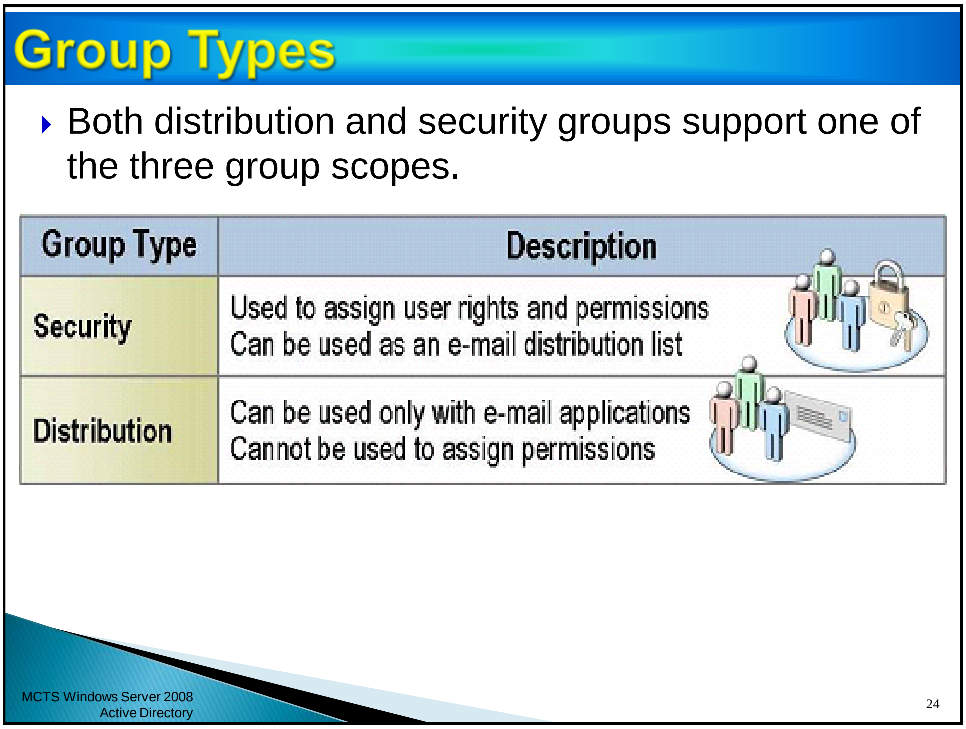
- Concept
- Type
- Convert
- Scope
- Member, member of
- Nesting
- Strategies
- Default
- Asign manager



Group

- Groups simplify administration by enabling you to assign permissions for resources
- Groups are characterized by scope and type
  - 2 types: Security, Distribution
  - 3 scope: Local Domain, Global, Universal

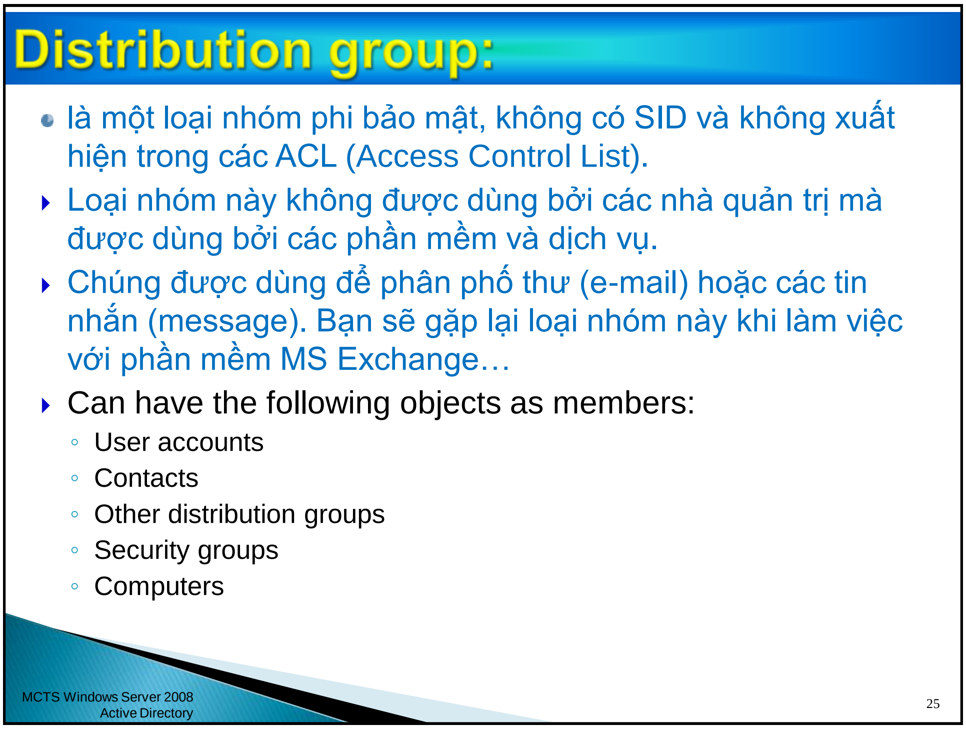
Groups simplify administration by enabling you to assign permissions for resources



Group Types

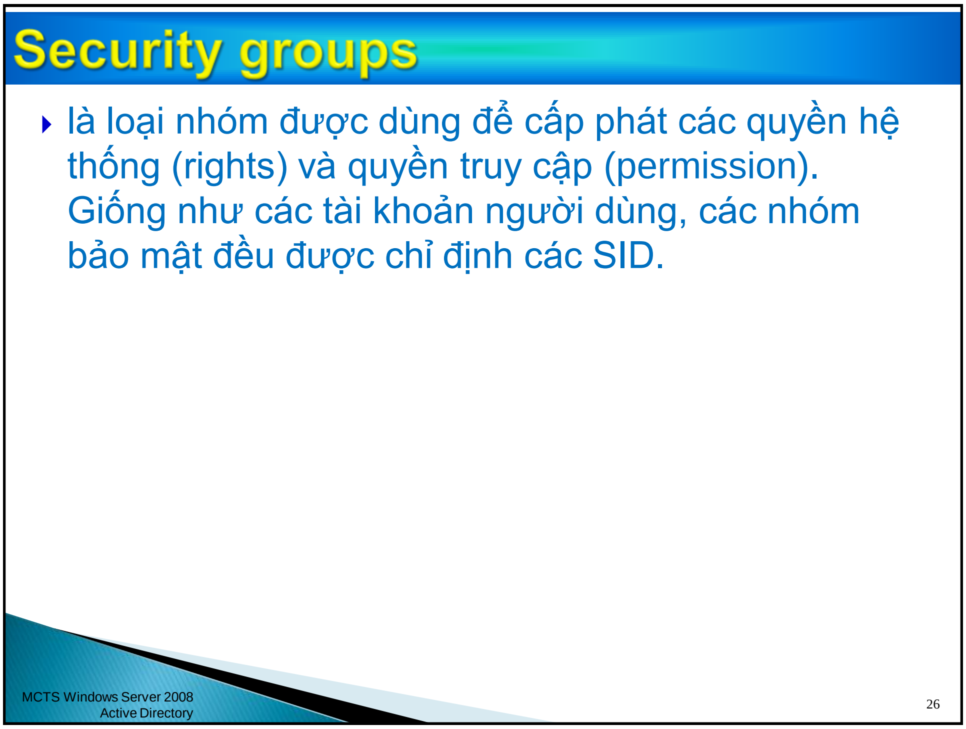
- Both distribution and security groups support one of the three group scopes.

Group Type	Description
Security	Used to assign user rights and permissions Can be used as an e-mail distribution list
Distribution	Can be used only with e-mail applications Cannot be used to assign permissions



Distribution group:

- là một loại nhóm phi bảo mật, không có SID và không xuất hiện trong các ACL (Access Control List).
- Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ.
- Chúng được dùng để phân phố thư (e-mail) hoặc các tin nhắn (message). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm MS Exchange…
- Can have the following objects as members:
  - User accounts
  - Contacts
  - Other distribution groups
  - Security groups
  - Computers



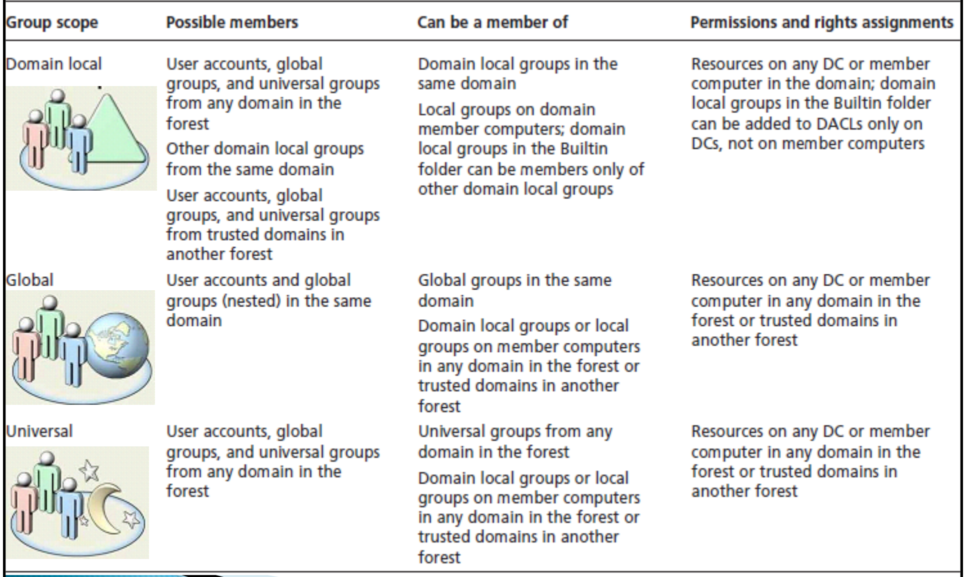
Security groups

- là loại nhóm được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập (permission). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các SID.

Group Scope

- Group scope determines the reach of a group’s application in a domain or a forest
- Three group scope options are possible in a Windows Server 2008 forest
  - Domain local
  - Global
  - Universal
  - Local group: (ext)

Group Scope (cont.)

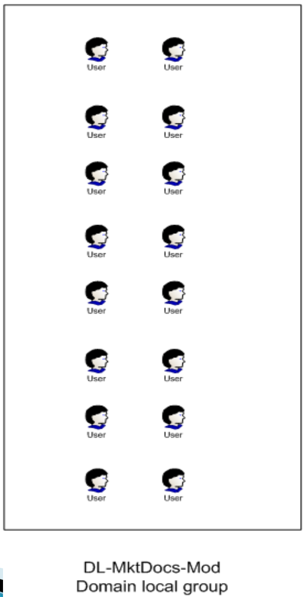


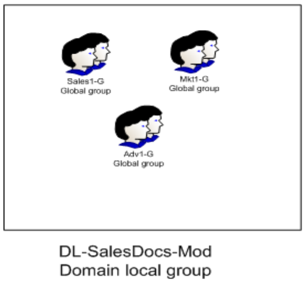
Group scope	Possible members	Can be a member of	Permissions and rights assignments
Domain local	User accounts, global groups, and universal groups from any domain in the forest Other domain local groups from the same domain User accounts, global groups, and universal groups from trusted domains in another forest	Domain local groups in the same domain Local groups on domain member computers; domain local groups in the Builtin folder can be members only of other domain local groups	Resources on any DC or member computer in the domain; domain local groups in the Builtin folder can be added to DACLs only on DCs, not on member computers
Global	User accounts and global groups (nested) in the same domain	Global groups in the same domain Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest
Universal	User accounts, global groups, and universal groups from any domain in the forest	Universal groups from any domain in the forest Domain local groups or local groups on member computers in any domain in the forest or trusted domains in another forest	Resources on any DC or member computer in any domain in the forest or trusted domains in another forest

Global Groups

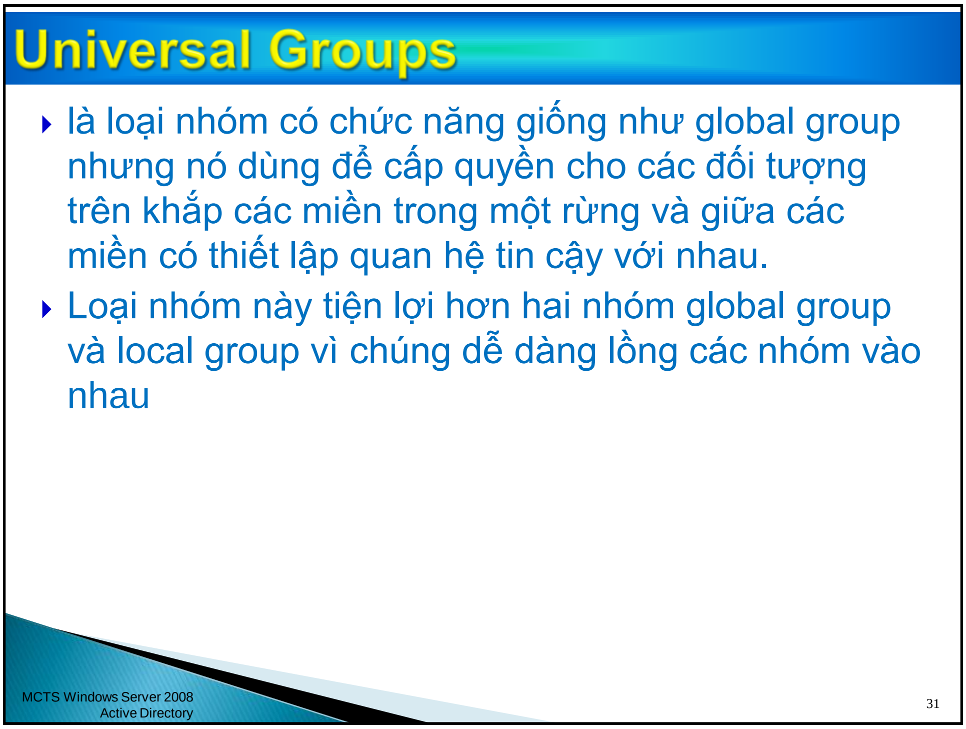
- là loại nhóm nằm trong Active Directory và được tạo trên các Domain Controller.
- Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền

Global Groups (cont.)



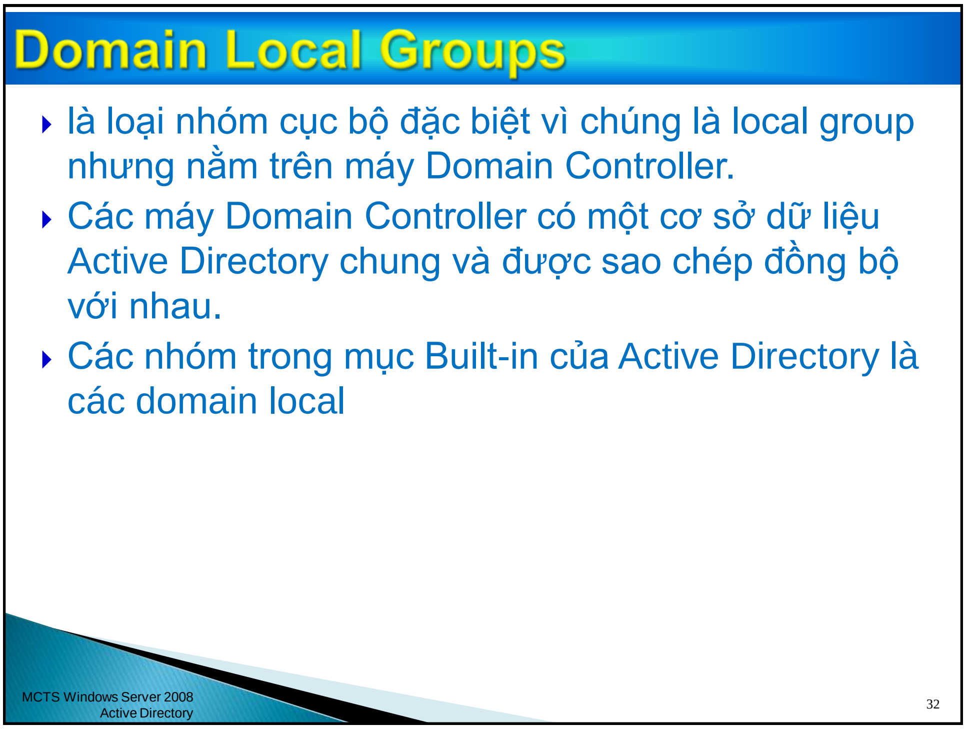


Use global groups to aggregate users and add those groups to domain local groups – easier to manage



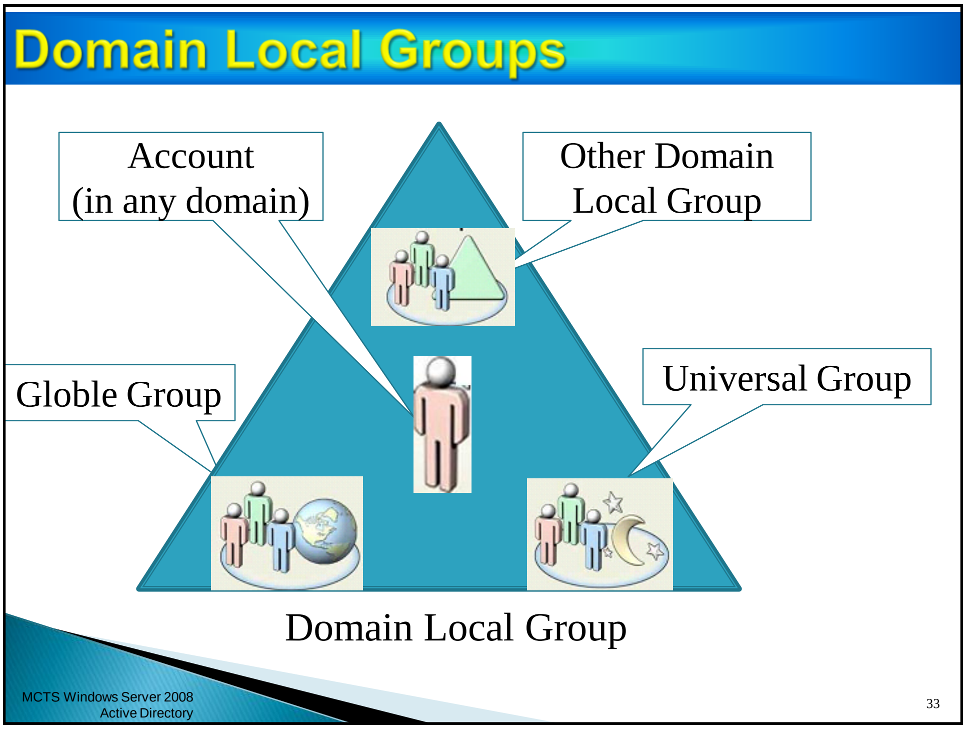
Universal Groups

- là loại nhóm có chức năng giống như global group nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau.
- Loại nhóm này tiện lợi hơn hai nhóm global group và local group vì chúng dễ dàng lồng các nhóm vào nhau



Domain Local Groups

- là loại nhóm cục bộ đặc biệt vì chúng là local group nhưng nằm trên máy Domain Controller.
- Các máy Domain Controller có một cơ sở dữ liệu Active Directory chung và được sao chép đồng bộ với nhau.
- Các nhóm trong mục Built-in của Active Directory là các domain local



Domain Local Groups

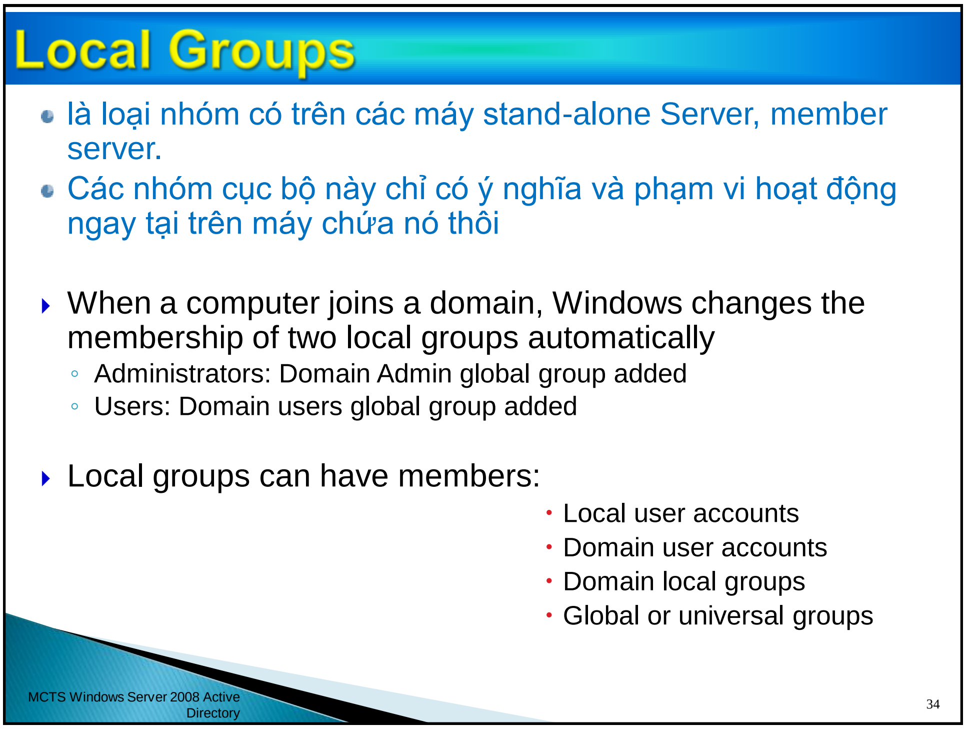
Account
(in any domain)

Other Domain
Local Group

Globle Group

Universal Group

Domain Local Group



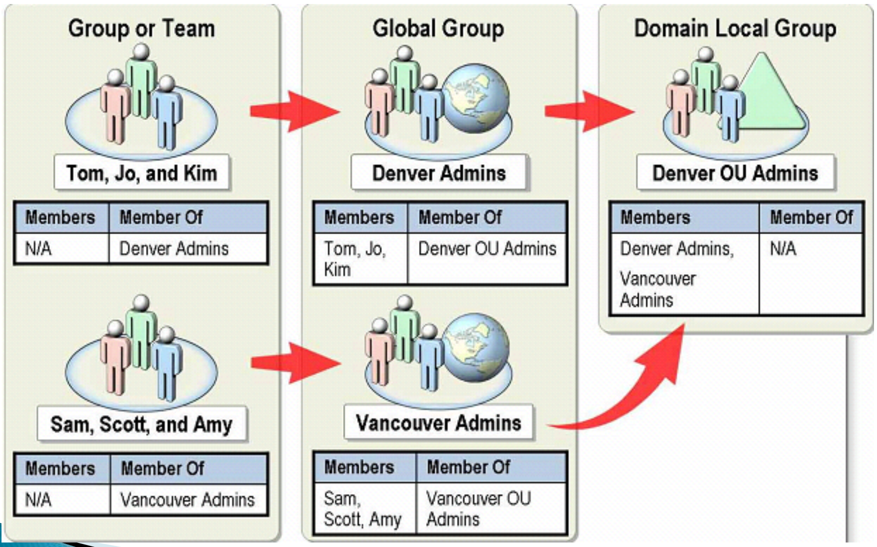
Local Groups

- là loại nhóm có trên các máy stand-alone Server, member server.
- Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi

- When a computer joins a domain, Windows changes the membership of two local groups automatically
  - Administrators: Domain Admin global group added
  - Users: Domain users global group added

- Local groups can have members:
  - Local user accounts
  - Domain user accounts
  - Domain local groups
  - Global or universal groups

Members and Member Of Properties



Group or Team

Tom, Jo, and Kim

Members	Member Of
N/A	Denver Admins

Sam, Scott, and Amy

Members	Member Of
N/A	Vancouver Admins

Global Group

Denver Admins

Members	Member Of
Tom, Jo, Kim	Denver OU Admins

Vancouver Admins

Members	Member Of
Sam, Scott, Amy	Vancouver OU Admins

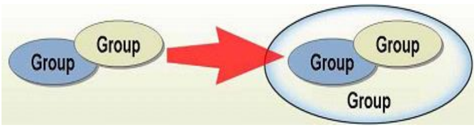
Domain Local Group

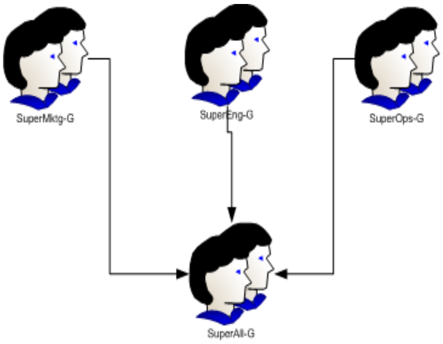
Denver OU Admins

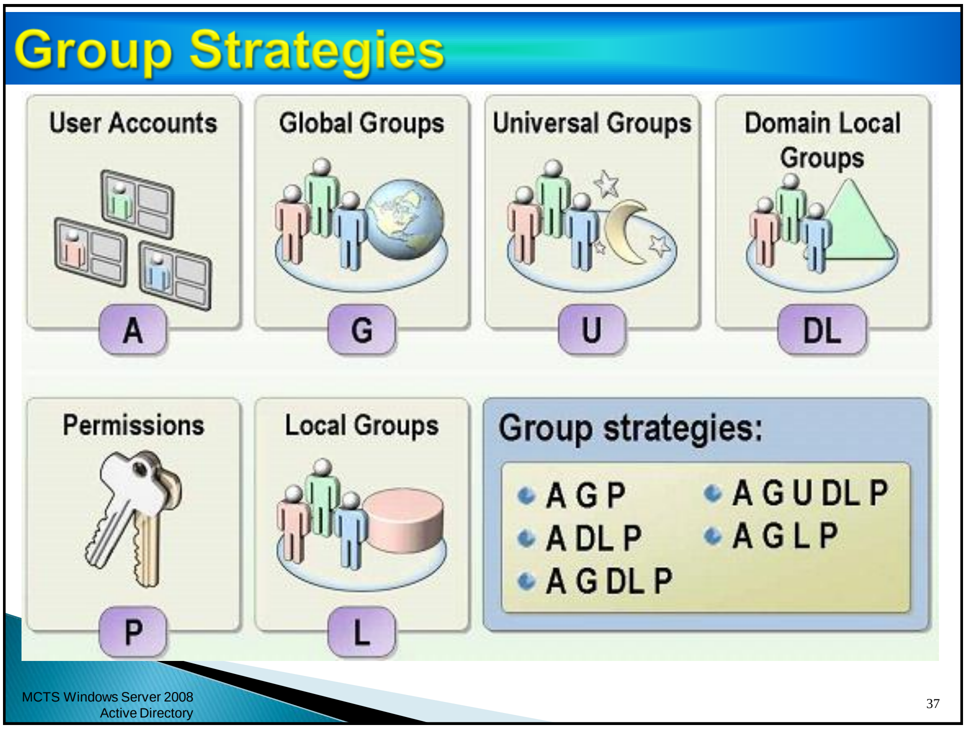
Members	Member Of
Denver Admins, Vancouver Admins	N/A

Nesting Groups

- Involves making a group a member of another group
- Group scope’s membership rules must be followed
- Usually used to group users who have similar roles but work in different departments







Group Strategies

User Accounts
A

Global Groups
G

Universal Groups
U

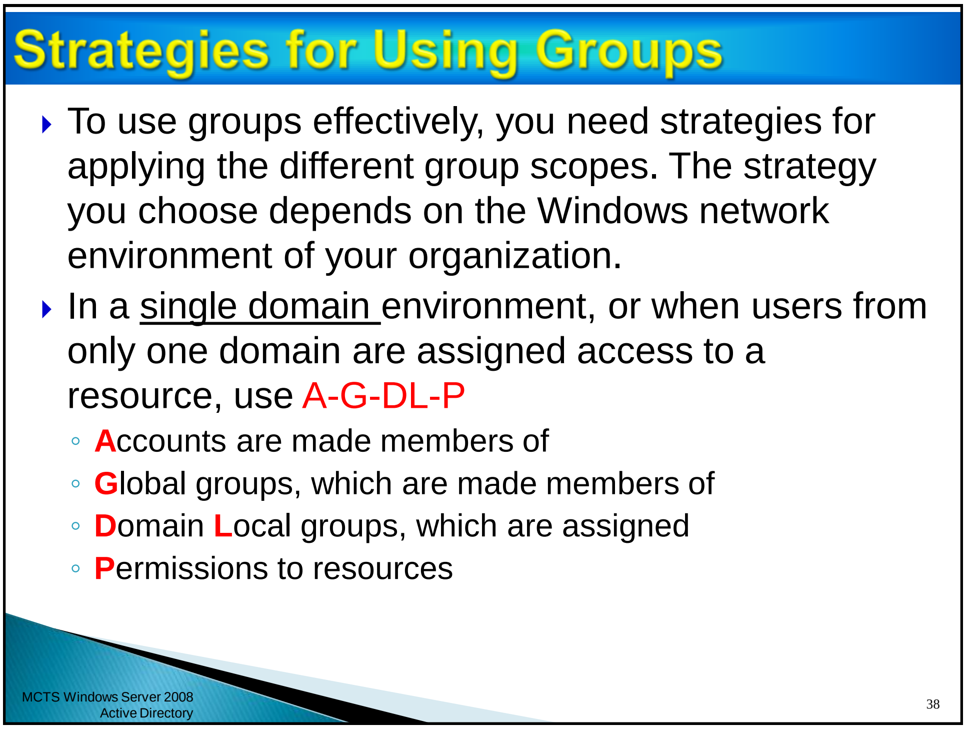
Domain Local Groups
DL

Permissions
P

Local Groups
L

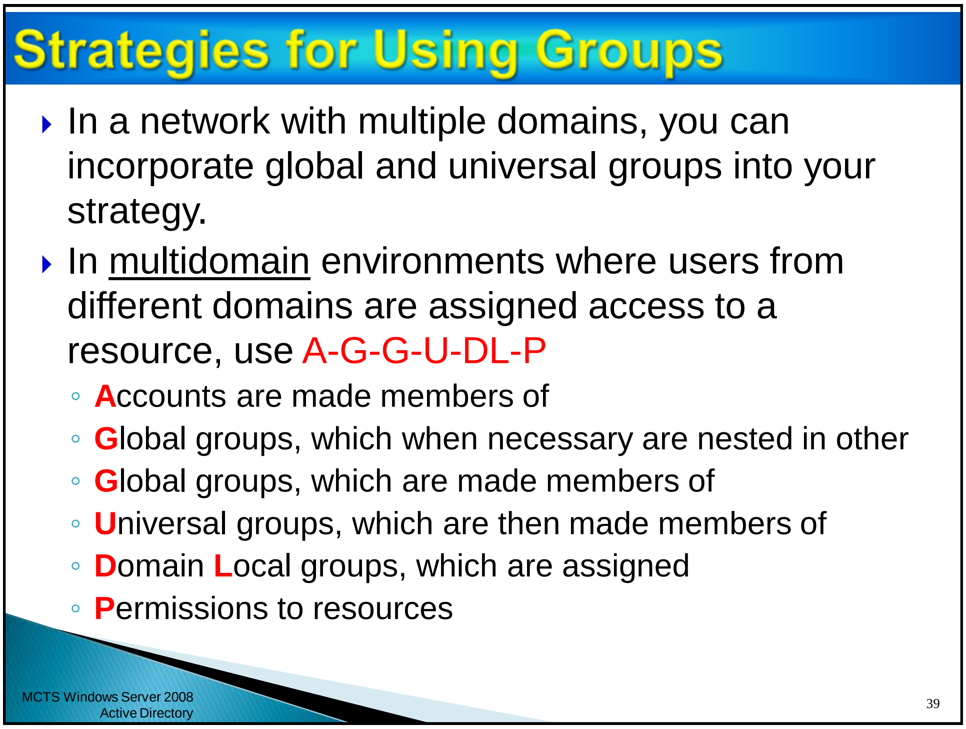
Group strategies:

- AGP
- ADLP
- AGDLP
- AGUDLP
- AGLP



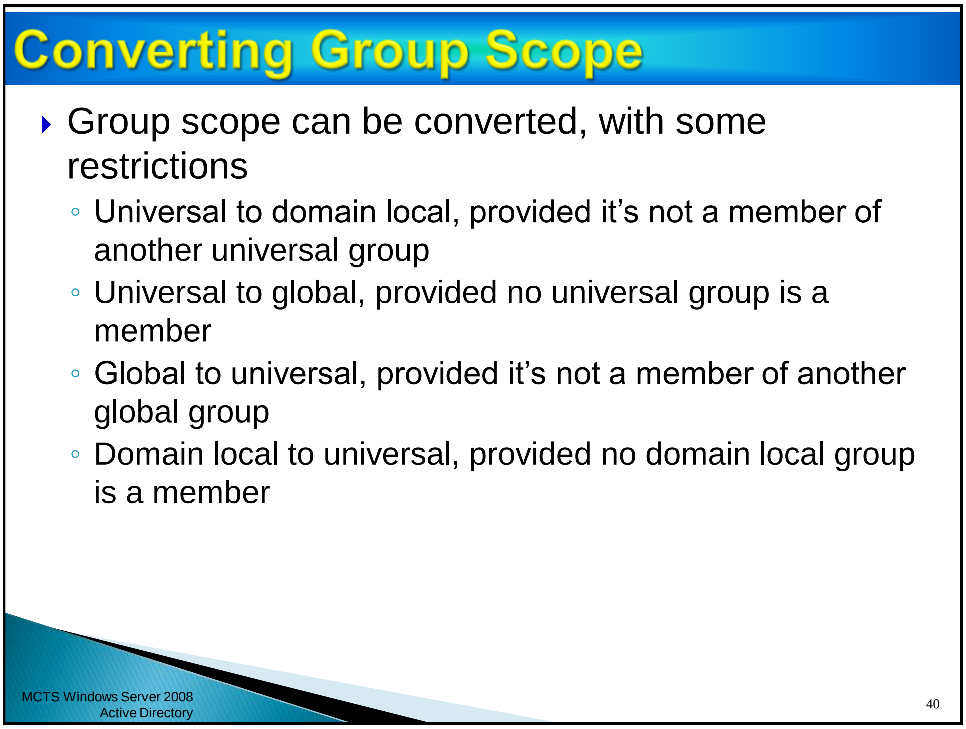
Strategies for Using Groups

- To use groups effectively, you need strategies for applying the different group scopes. The strategy you choose depends on the Windows network environment of your organization.
- In a single domain environment, or when users from only one domain are assigned access to a resource, use A-G-DL-P
  - Accounts are made members of
  - Global groups, which are made members of
  - Domain Local groups, which are assigned
  - Permissions to resources



Strategies for Using Groups

- In a network with multiple domains, you can incorporate global and universal groups into your strategy.
- In multidomain environments where users from different domains are assigned access to a resource, use A-G-G-U-DL-P
  - **A**ccounts are made members of
  - **G**lobal groups, which when necessary are nested in other
  - **G**lobal groups, which are made members of
  - **U**niversal groups, which are then made members of
  - **D**omain **L**ocal groups, which are assigned
  - **P**ermissions to resources



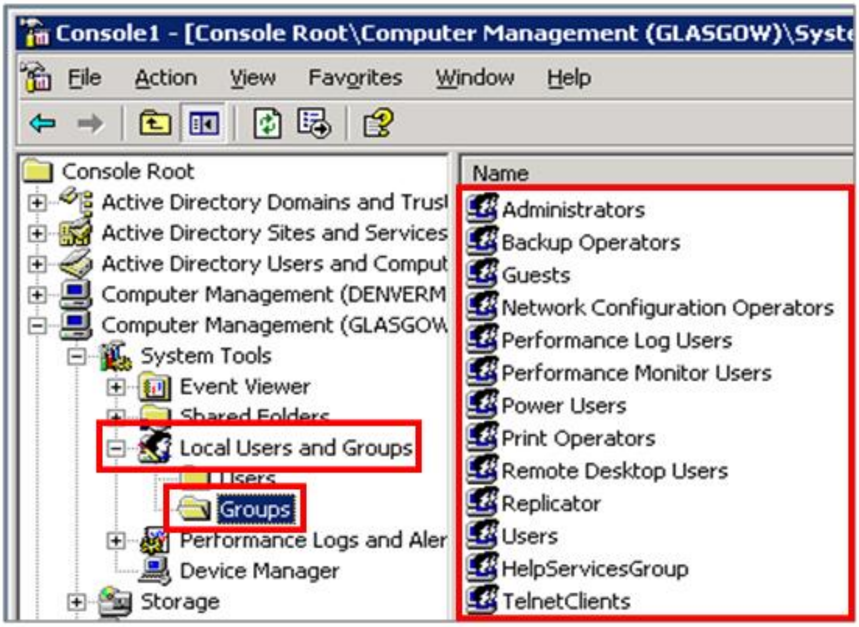
Converting Group Scope

- Group scope can be converted, with some restrictions
  - Universal to domain local, provided it's not a member of another universal group
  - Universal to global, provided no universal group is a member
  - Global to universal, provided it's not a member of another global group
  - Domain local to universal, provided no domain local group is a member

Default Groups in a Windows Domain

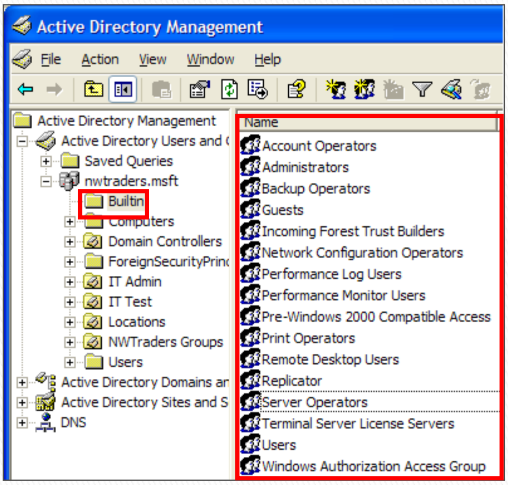
- Builtin folder
  - Domain local groups used for assigning rights and permissions in the local domain
- Users folder
  - Combination of domain local, global, and, in the forest root domain, universal scope
  - User accounts are generally added to global and universal groups in this folder for assigning permissions and rights in the domain and forest
- Special identity groups
  - Can be assigned permissions by adding them to resources' DACLs (Discretionary Access Control List)
  - Can not be changed manually

Default Groups in a Windows Domain


Console1 - [Console Root\Computer Management (GLASGOW)\Syste
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Domains and Trust
Active Directory Sites and Services
Active Directory Users and Comput
Computer Management (DENVERM
Computer Management (GLASGOW
System Tools
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance Logs and Aler
Device Manager
Storage
Name

Administrators
Backup Operators
Guests
Network Configuration Operators
Performance Log Users
Performance Monitor Users
Power Users
Print Operators
Remote Desktop Users
Replicator
Users
HelpServicesGroup
TelnetClients

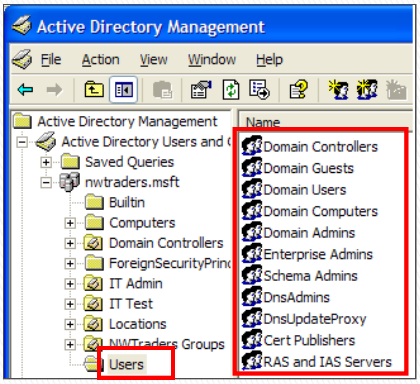
Default Groups in a Windows Domain



- Active Directory Management
  - Active Directory Users and C
    - Saved Queries
    - nwtraders.msft
      - Builtin
      - Computers
      - Domain Controllers
      - ForeignSecurityPrinc
      - IT Admin
      - IT Test
      - Locations
      - NWTraders Groups
      - Users
  - Active Directory Domains ar
  - Active Directory Sites and S
  - DNS

Name

- Account Operators
- Administrators
- Backup Operators
- Guests
- Incoming Forest Trust Builders
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Pre-Windows 2000 Compatible Access
- Print Operators
- Remote Desktop Users
- Replicator
- Server Operators
- Terminal Server License Servers
- Users
- Windows Authorization Access Group

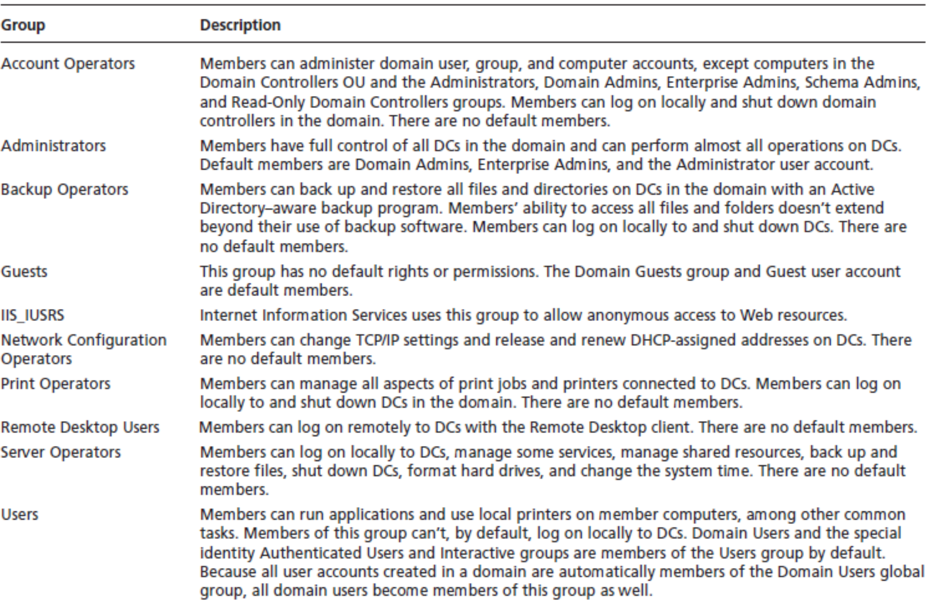


- Active Directory Management
  - Active Directory Users and C
    - Saved Queries
    - nwtraders.msft
      - Builtin
      - Computers
      - Domain Controllers
      - ForeignSecurityPrinc
      - IT Admin
      - IT Test
      - Locations
      - NWTraders Groups
      - Users

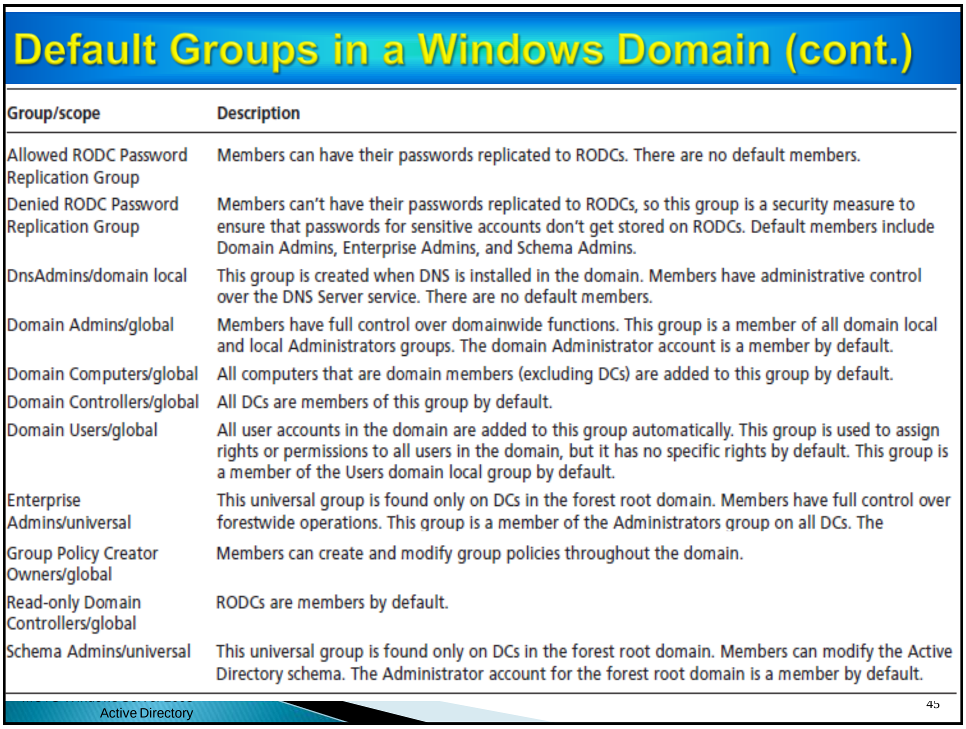
Name

- Domain Controllers
- Domain Guests
- Domain Users
- Domain Computers
- Domain Admins
- Enterprise Admins
- Schema Admins
- DnsAdmins
- DnsUpdateProxy
- Cert Publishers
- RAS and IAS Servers

Default Groups in a Windows Domain (cont.)

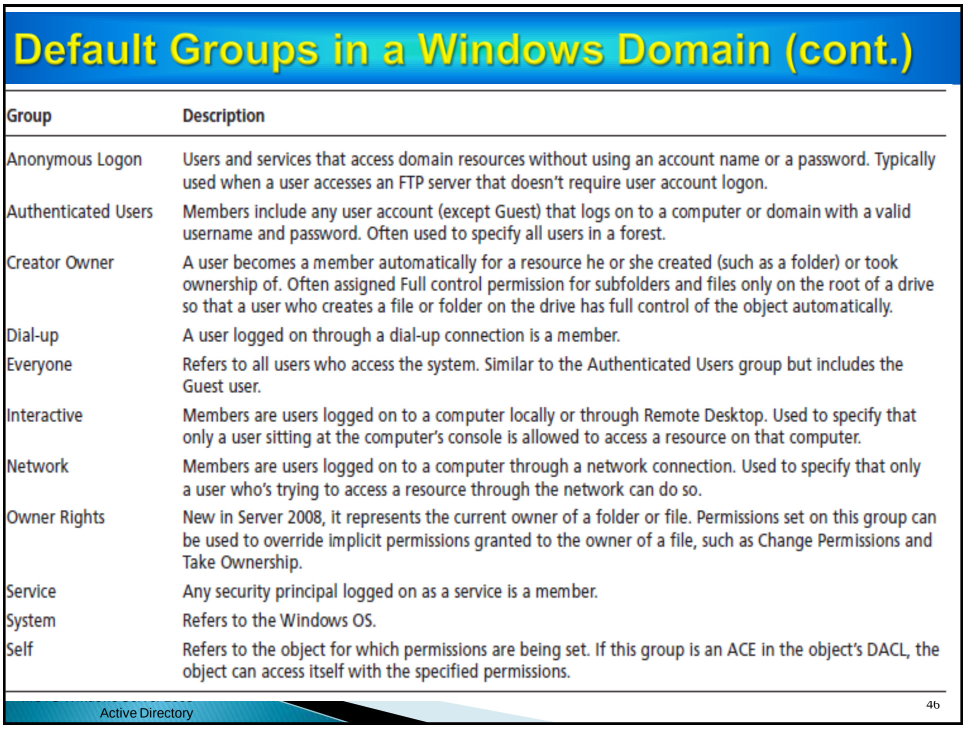


Group	Description
Account Operators	Members can administer domain user, group, and computer accounts, except computers in the Domain Controllers OU and the Administrators, Domain Admins, Enterprise Admins, Schema Admins, and Read-Only Domain Controllers groups. Members can log on locally and shut down domain controllers in the domain. There are no default members.
Administrators	Members have full control of all DCs in the domain and can perform almost all operations on DCs. Default members are Domain Admins, Enterprise Admins, and the Administrator user account.
Backup Operators	Members can back up and restore all files and directories on DCs in the domain with an Active Directory–aware backup program. Members' ability to access all files and folders doesn't extend beyond their use of backup software. Members can log on locally to and shut down DCs. There are no default members.
Guests	This group has no default rights or permissions. The Domain Guests group and Guest user account are default members.
IIS_IUSRS	Internet Information Services uses this group to allow anonymous access to Web resources.
Network Configuration Operators	Members can change TCP/IP settings and release and renew DHCP-assigned addresses on DCs. There are no default members.
Print Operators	Members can manage all aspects of print jobs and printers connected to DCs. Members can log on locally to and shut down DCs in the domain. There are no default members.
Remote Desktop Users	Members can log on remotely to DCs with the Remote Desktop client. There are no default members.
Server Operators	Members can log on locally to DCs, manage some services, manage shared resources, back up and restore files, shut down DCs, format hard drives, and change the system time. There are no default members.
Users	Members can run applications and use local printers on member computers, among other common tasks. Members of this group can't, by default, log on locally to DCs. Domain Users and the special identity Authenticated Users and Interactive groups are members of the Users group by default. Because all user accounts created in a domain are automatically members of the Domain Users global group, all domain users become members of this group as well.



Default Groups in a Windows Domain (cont.)

Group/scope	Description
Allowed RODC Password Replication Group	Members can have their passwords replicated to RODCs. There are no default members.
Denied RODC Password Replication Group	Members can't have their passwords replicated to RODCs, so this group is a security measure to ensure that passwords for sensitive accounts don't get stored on RODCs. Default members include Domain Admins, Enterprise Admins, and Schema Admins.
DnsAdmins/domain local	This group is created when DNS is installed in the domain. Members have administrative control over the DNS Server service. There are no default members.
Domain Admins/global	Members have full control over domainwide functions. This group is a member of all domain local and local Administrators groups. The domain Administrator account is a member by default.
Domain Computers/global	All computers that are domain members (excluding DCs) are added to this group by default.
Domain Controllers/global	All DCs are members of this group by default.
Domain Users/global	All user accounts in the domain are added to this group automatically. This group is used to assign rights or permissions to all users in the domain, but it has no specific rights by default. This group is a member of the Users domain local group by default.
Enterprise Admins/universal	This universal group is found only on DCs in the forest root domain. Members have full control over forestwide operations. This group is a member of the Administrators group on all DCs. The
Group Policy Creator Owners/global	Members can create and modify group policies throughout the domain.
Read-only Domain Controllers/global	RODCs are members by default.
Schema Admins/universal	This universal group is found only on DCs in the forest root domain. Members can modify the Active Directory schema. The Administrator account for the forest root domain is a member by default.



Default Groups in a Windows Domain (cont.)

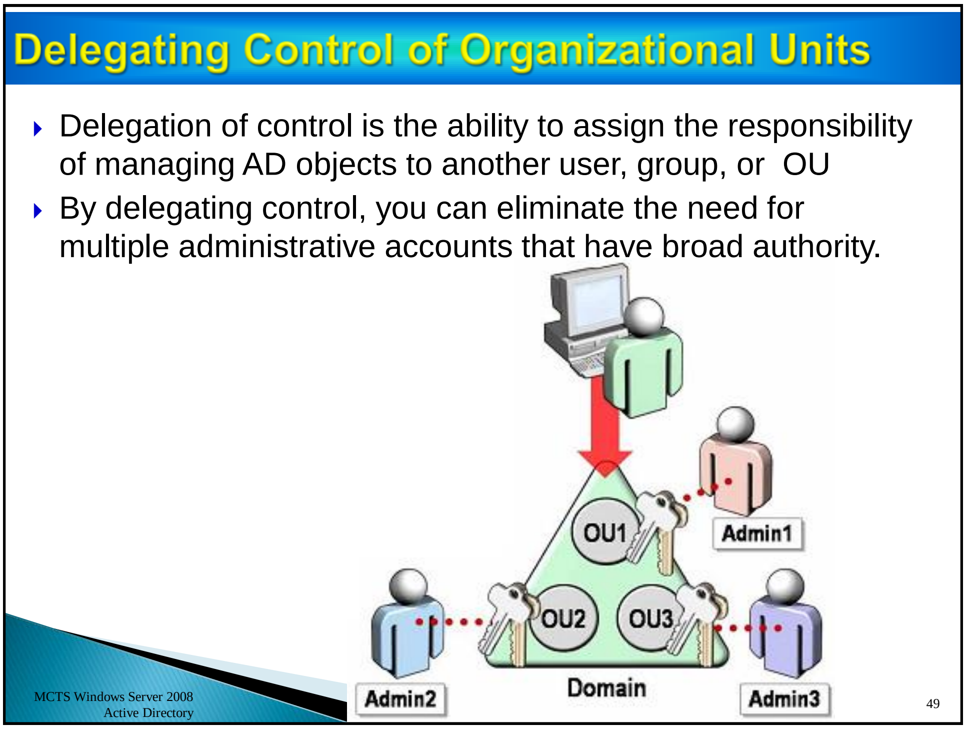
Group	Description
Anonymous Logon	Users and services that access domain resources without using an account name or a password. Typically used when a user accesses an FTP server that doesn't require user account logon.
Authenticated Users	Members include any user account (except Guest) that logs on to a computer or domain with a valid username and password. Often used to specify all users in a forest.
Creator Owner	A user becomes a member automatically for a resource he or she created (such as a folder) or took ownership of. Often assigned Full control permission for subfolders and files only on the root of a drive so that a user who creates a file or folder on the drive has full control of the object automatically.
Dial-up	A user logged on through a dial-up connection is a member.
Everyone	Refers to all users who access the system. Similar to the Authenticated Users group but includes the Guest user.
Interactive	Members are users logged on to a computer locally or through Remote Desktop. Used to specify that only a user sitting at the computer's console is allowed to access a resource on that computer.
Network	Members are users logged on to a computer through a network connection. Used to specify that only a user who's trying to access a resource through the network can do so.
Owner Rights	New in Server 2008, it represents the current owner of a folder or file. Permissions set on this group can be used to override implicit permissions granted to the owner of a file, such as Change Permissions and Take Ownership.
Service	Any security principal logged on as a service is a member.
System	Refers to the Windows OS.
Self	Refers to the object for which permissions are being set. If this group is an ACE in the object's DACL, the object can access itself with the specified permissions.

Use Default groups to:

- Control access to shared resources
- Delegate specific domain-wide administrative roles.
- Many default groups are automatically assigned a set of user rights that authorize members of the group to perform specific actions in a domain, such as log on to a local system or back up files and folders.
- When you add a user to a group, the user receives all the user rights assigned to the group and all the permissions assigned to the group for any shared resources.

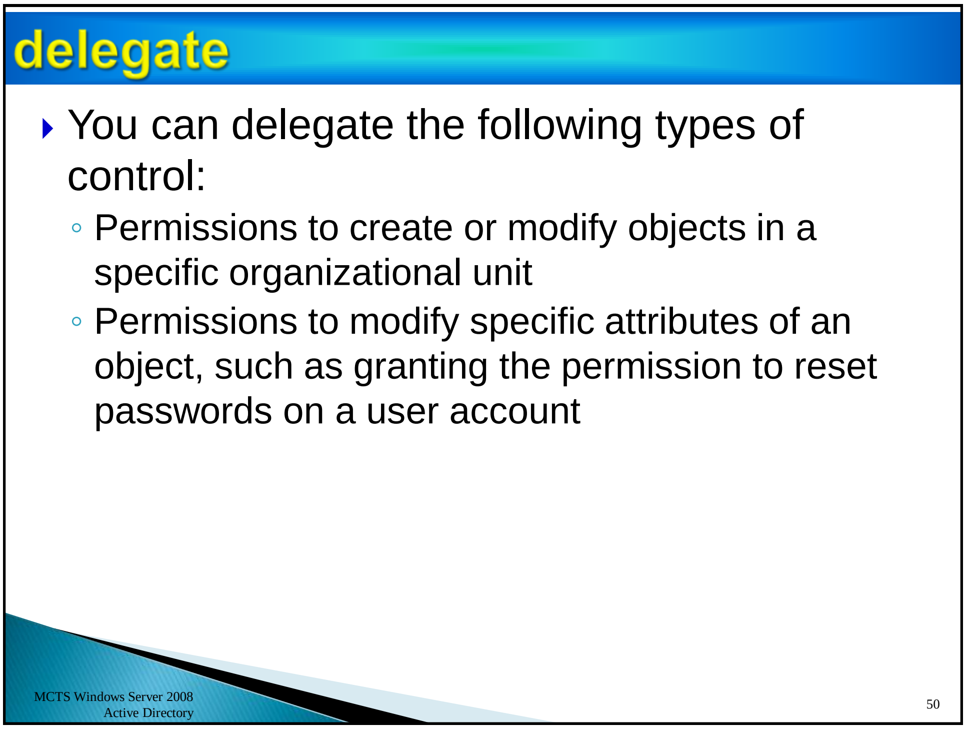
Assigning a Manager to a Group

- To enables you to:
  - Track who is responsible for groups.
  - Delegate to the manager of the group the authority to add users to and remove users from the group.
- Using in large organizations are added to and removed from groups so often, some organizations distribute the administrative responsibility of adding users to groups to the people who request the group.
- ….Properties\Manage by



Delegating Control of Organizational Units

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



delegate

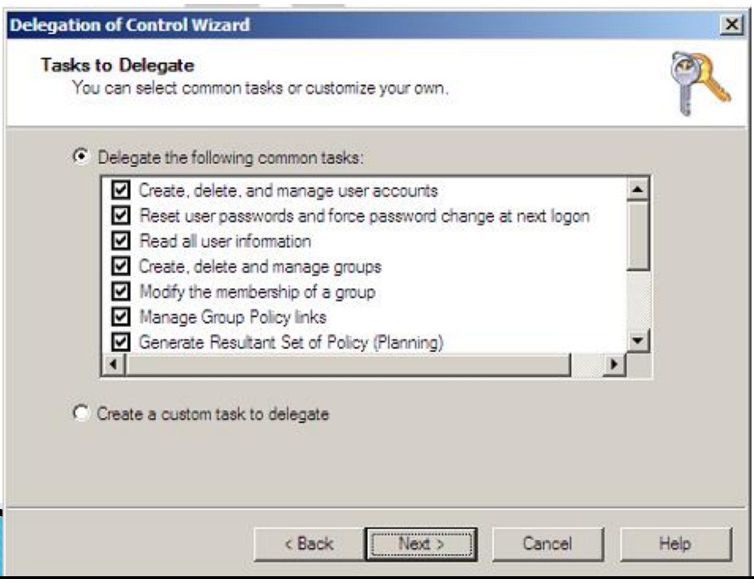
- You can delegate the following types of control:
  - Permissions to create or modify objects in a specific organizational unit
  - Permissions to modify specific attributes of an object, such as granting the permission to reset passwords on a user account

Why delegate administrative control?

- ease the administrative burden of managing your network by distributing routine administrative tasks to multiple users.
- assign basic administrative tasks to regular users or groups and assign domain-wide and forest-wide administrative tasks to trusted users in your Domain Admins and Enterprise Admins groups.
- help secure your network from accidental or malicious damage by limiting the membership of administrator groups.

How config Delegate

- Right click vào OU\ Delegate Control



Delegation of Control Wizard

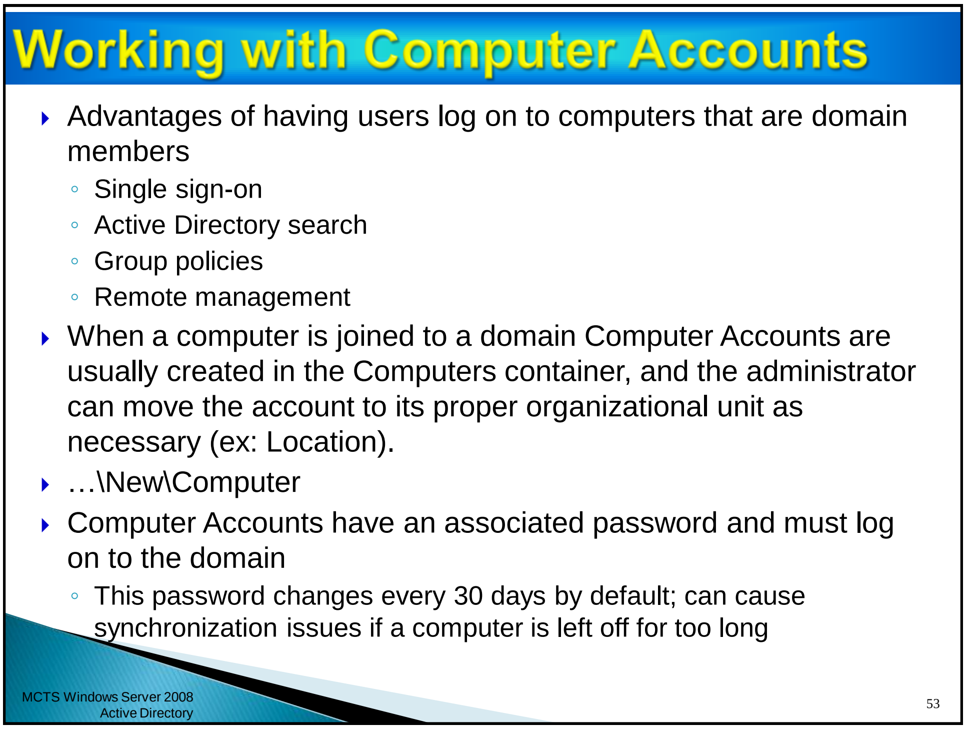
Tasks to Delegate

You can select common tasks or customize your own.

● Delegate the following common tasks:

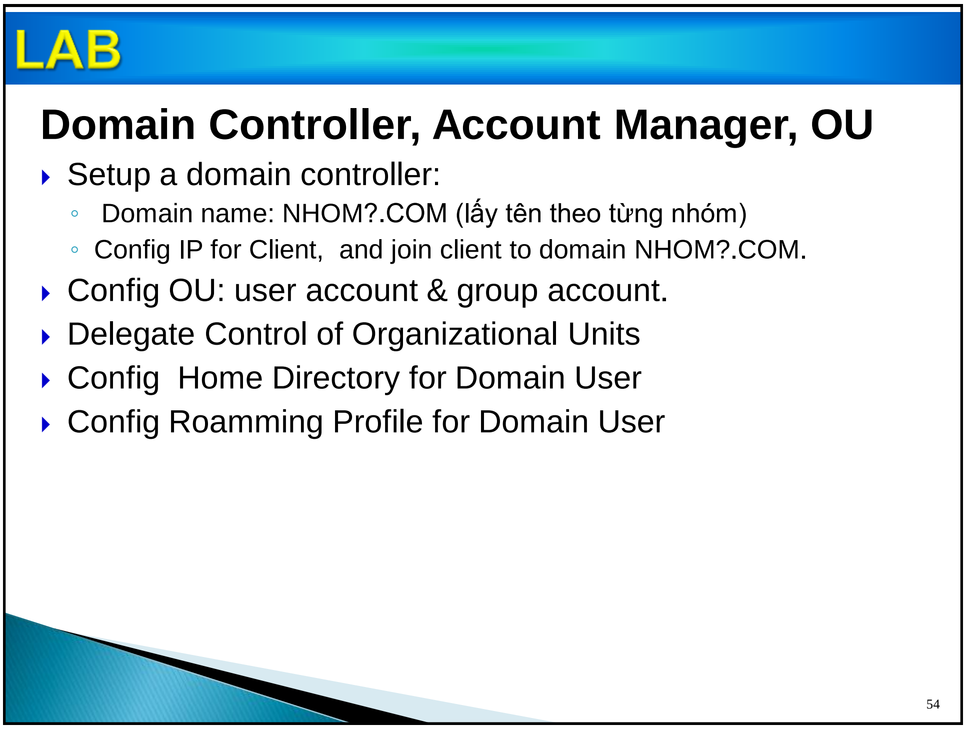
- ☑ Create, delete, and manage user accounts
- ☑ Reset user passwords and force password change at next logon
- ☑ Read all user information
- ☑ Create, delete and manage groups
- ☑ Modify the membership of a group
- ☑ Manage Group Policy links
- ☑ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate



Working with Computer Accounts

- Advantages of having users log on to computers that are domain members
  - Single sign-on
  - Active Directory search
  - Group policies
  - Remote management
- When a computer is joined to a domain Computer Accounts are usually created in the Computers container, and the administrator can move the account to its proper organizational unit as necessary (ex: Location).
- …\New\Computer
- Computer Accounts have an associated password and must log on to the domain
  - This password changes every 30 days by default; can cause synchronization issues if a computer is left off for too long



LAB

Domain Controller, Account Manager, OU

- Setup a domain controller:
  - Domain name: NHOM?.COM (lấy tên theo từng nhóm)
  - Config IP for Client, and join client to domain NHOM?.COM.
- Config OU: user account & group account.
- Delegate Control of Organizational Units
- Config Home Directory for Domain User
- Config Roamming Profile for Domain User