

Network Management and Administration

Code:3360703

UNIT – 4

Network Configuration

Prepared By:

Chirag Patel

Lecturer in Computer Engineering,

K D Polytechnic, Patan

4.1 Working with User Accounts

- Administrator has an account on the server to access a server.
- The user must have an account established on the server or in the domain.
- The account defines the user name and the user's password, along with a host of other information specific to each user.
- A creating, maintaining, and deleting user account is easy with Windows Server.
- To maintain user accounts, by using two ways.
 1. Use the Active Directory Users and Computers console. Open this console by going to the Start screen and then clicking Active Directory Users And Computers.
 2. From Server Manager, Open the Tools menu, and select Active Directory Users and Computers from the menu.

4.1 Working with User Accounts

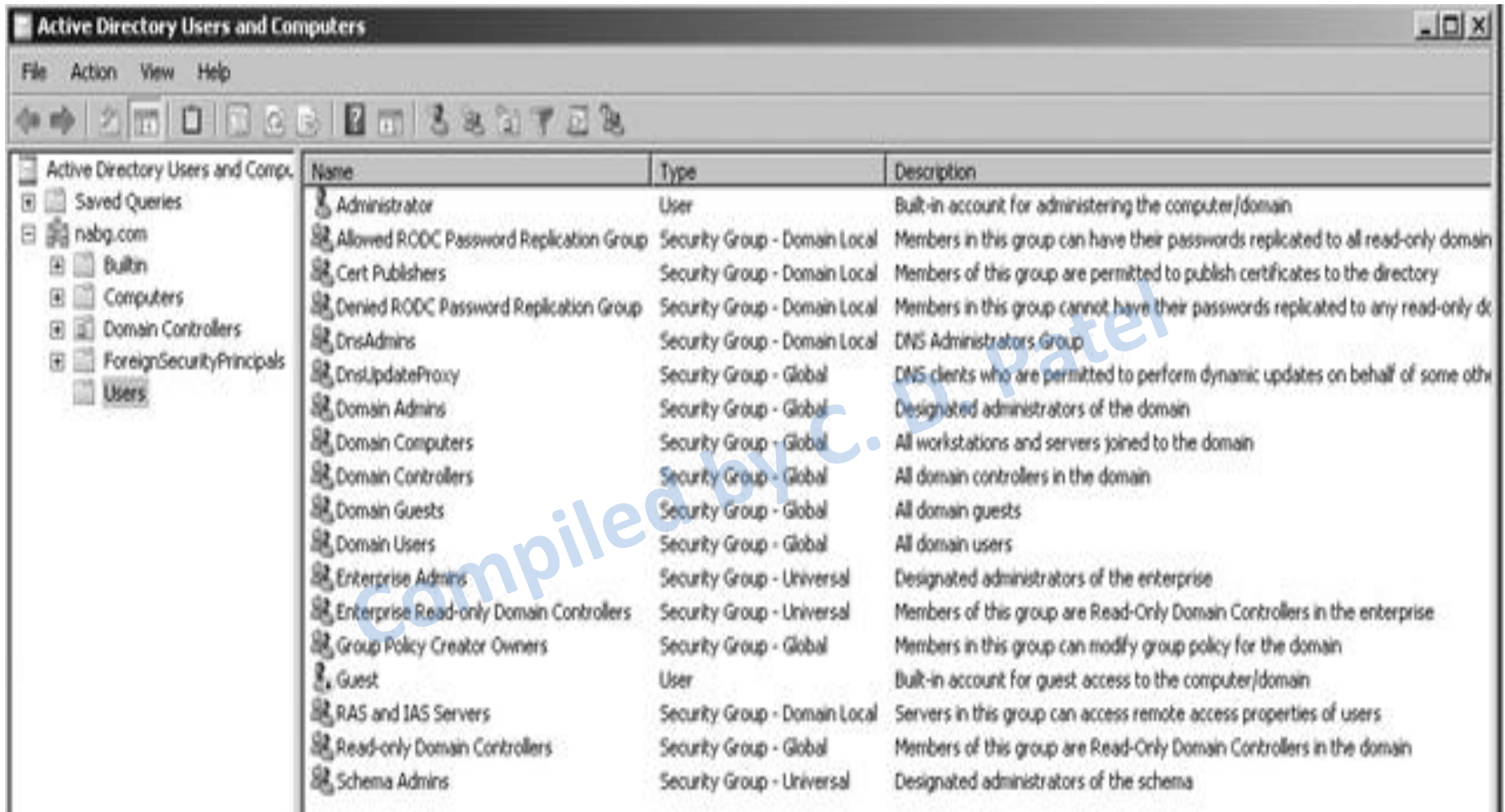


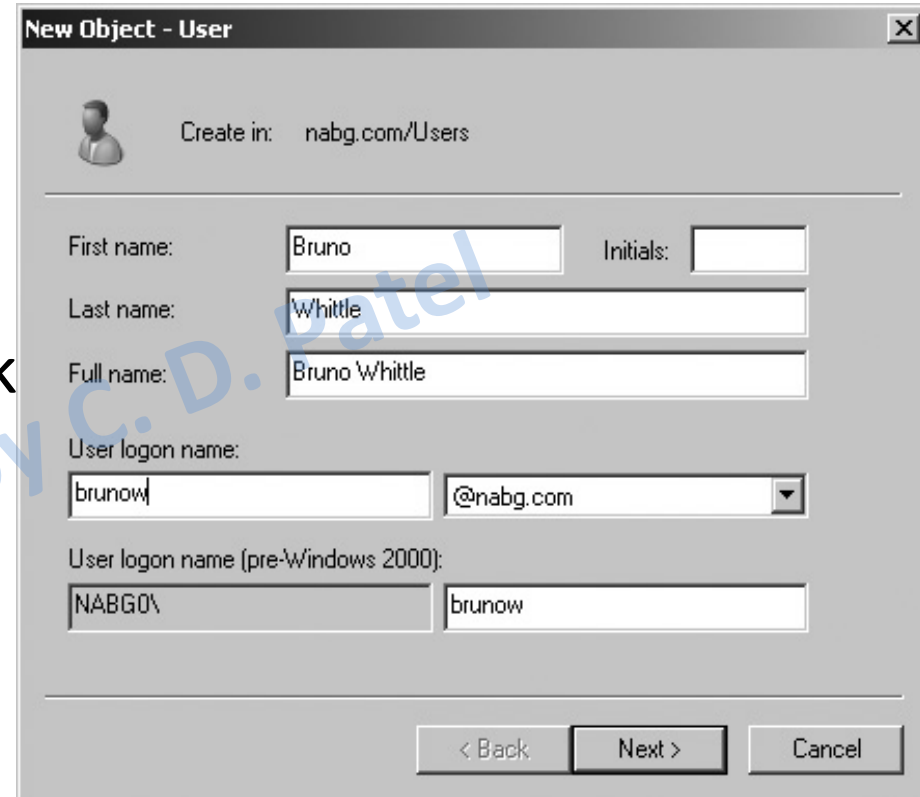
Figure 4.1. The Active Directory Users And Computers console allows to manage user accounts.

4.1.1 Adding a User

- To add User following steps are necessary.
- **Step1**
 - Open the Active Directory Users and Computers console by going to the Start screen and then clicking Active Directory Users And Computers.
- **Step2**
 - To add user select the Users container in the left pane as shown in Figure 4.1.
- **Step3**
 - Then right-click the Users container, choose New from the pop-up menu, and choose User from the submenu. Pop-up New Object – User dialog box, as shown in Figure 4.2.

4.1.1 Adding a User

- **Step4**
- Fill up first name, Initials, Last name, Full name, User logon name, User logon name(pre-Windows 2000) then left- click Next button.



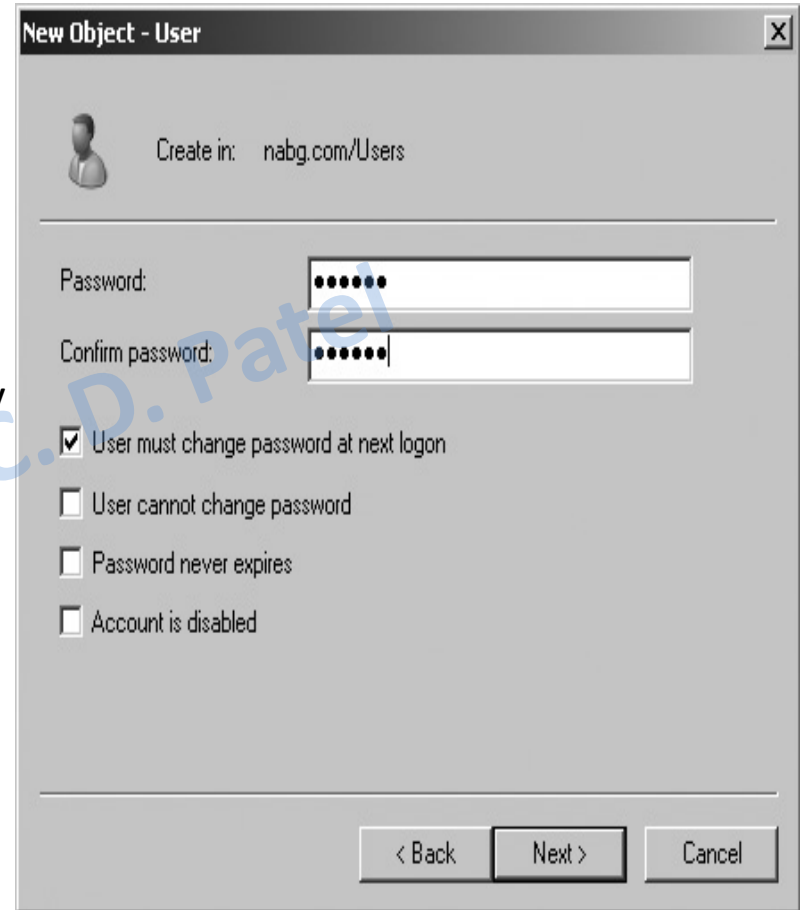
The image shows a 'New Object - User' dialog box. At the top, it says 'Create in: nabg.com/Users'. Below this, there are several input fields: 'First name:' with 'Bruno', 'Initials:' (empty), 'Last name:' with 'Whittle', 'Full name:' with 'Bruno Whittle', 'User logon name:' with 'brunow' and a dropdown menu showing '@nabg.com', and 'User logon name (pre-Windows 2000):' with 'NABGO\' and 'brunow'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Field	Value
Create in:	nabg.com/Users
First name:	Bruno
Initials:	
Last name:	Whittle
Full name:	Bruno Whittle
User logon name:	brunow @nabg.com
User logon name (pre-Windows 2000):	NABGO\' brunow

Figure 4.2 Use the New Object –User dialog box to add a new user.

4.1.1 Adding a User

- **Step 5 :**
- On clicking the Next button a New Form will be opened (shown in Figure 4.3) in which you need to provide the Password for the new user. Also select several options that apply to the account, as follows:
- **User Must Change Password at Next Logon:** Users to choose their own password when they first log in to the system.
- **User Cannot Change Password:** Users are not allowed to change their password.
- **Password Never Expires:** The password to remain feasible for as long as the user chooses to use it.
- **Account Is Disabled:** This option is disables the new account.



The screenshot shows a window titled "New Object - User". It contains a user icon and the text "Create in: nabg.com/Users". Below this are two password input fields labeled "Password:" and "Confirm password:", both filled with dots. Underneath the fields are four checkboxes with labels: "User must change password at next logon" (checked), "User cannot change password", "Password never expires", and "Account is disabled". At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

Figure 4.3 Setting the user's password

4.1.2 Modifying a User Account

- Open the Active Directory Users and Computers console by going to the Start screen and then clicking Active Directory Users and Computers shown in Figure 4.1.
- Right-click on the user objects to modify and choose Properties from the pop-up menu. Then see the tabbed dialog box shown in Figure 4.4
- In the first two tabs, General and Address, User add some additional information such as job title, mailing address, telephone number, e-mail account.

The screenshot shows the 'Bruno Whittle Properties' dialog box with the 'General' tab selected. The 'Account' tab is also visible in the background. The 'General' tab contains the following fields:

- First name: Bruno
- Last name: Whittle
- Display name: Bruno Whittle
- Description: (empty)
- Office: (empty)
- Telephone number: (empty)
- E-mail: (empty)
- Web page: (empty)

The 'Account' tab contains the following fields:

- Member Of: (empty)
- Dial-in: (empty)
- Environment: (empty)
- Sessions: (empty)
- Remote control: (empty)
- Terminal Services Profile: (empty)
- COM+: (empty)

Figure 4.4 Setting properties for a user's account

4.1.2 Modifying a User Account

- In the Account tab, shown in Figure 4.5, Users can set some important user account options.
- **User logon name:** the user's logon name, as well as the Windows domain in which the user has primary membership.

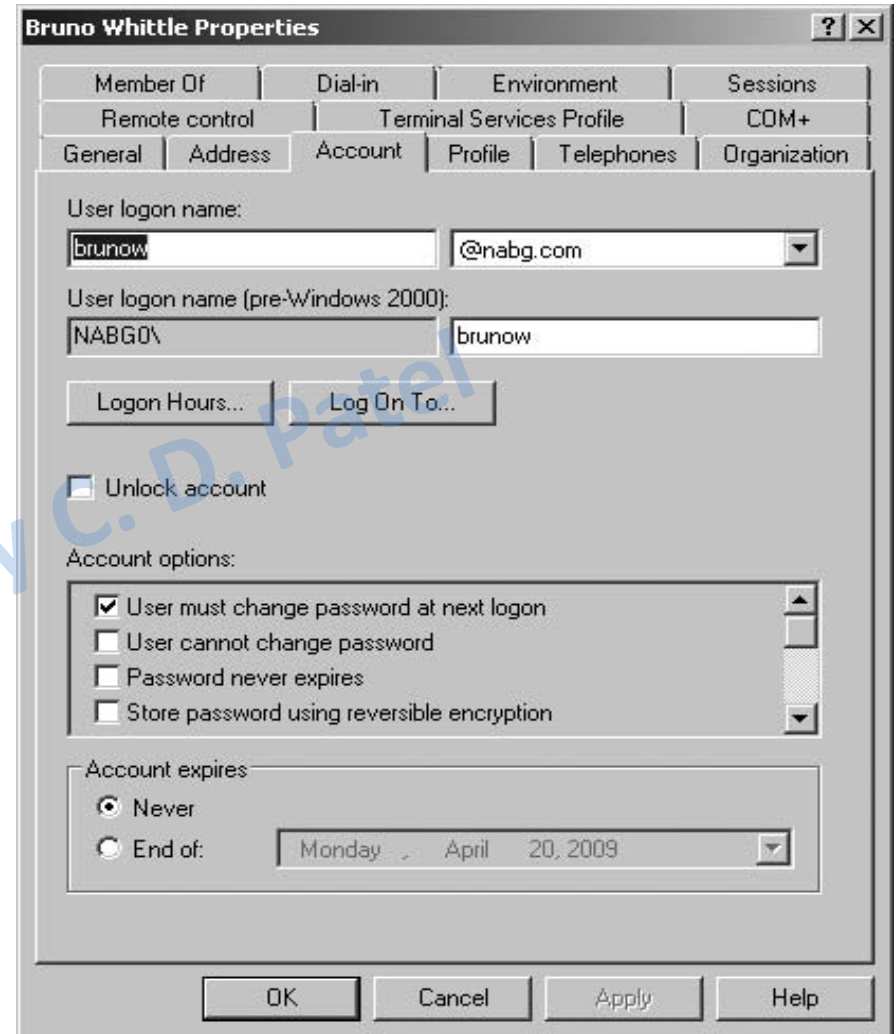


Figure 4.5 The Account tab of a user's Properties dialog box lets you

4.1.2 Modifying a User Account

- **Logon Hours:** This option use for to permit or deny access to the network for specific time period shown in Figure 4.6.

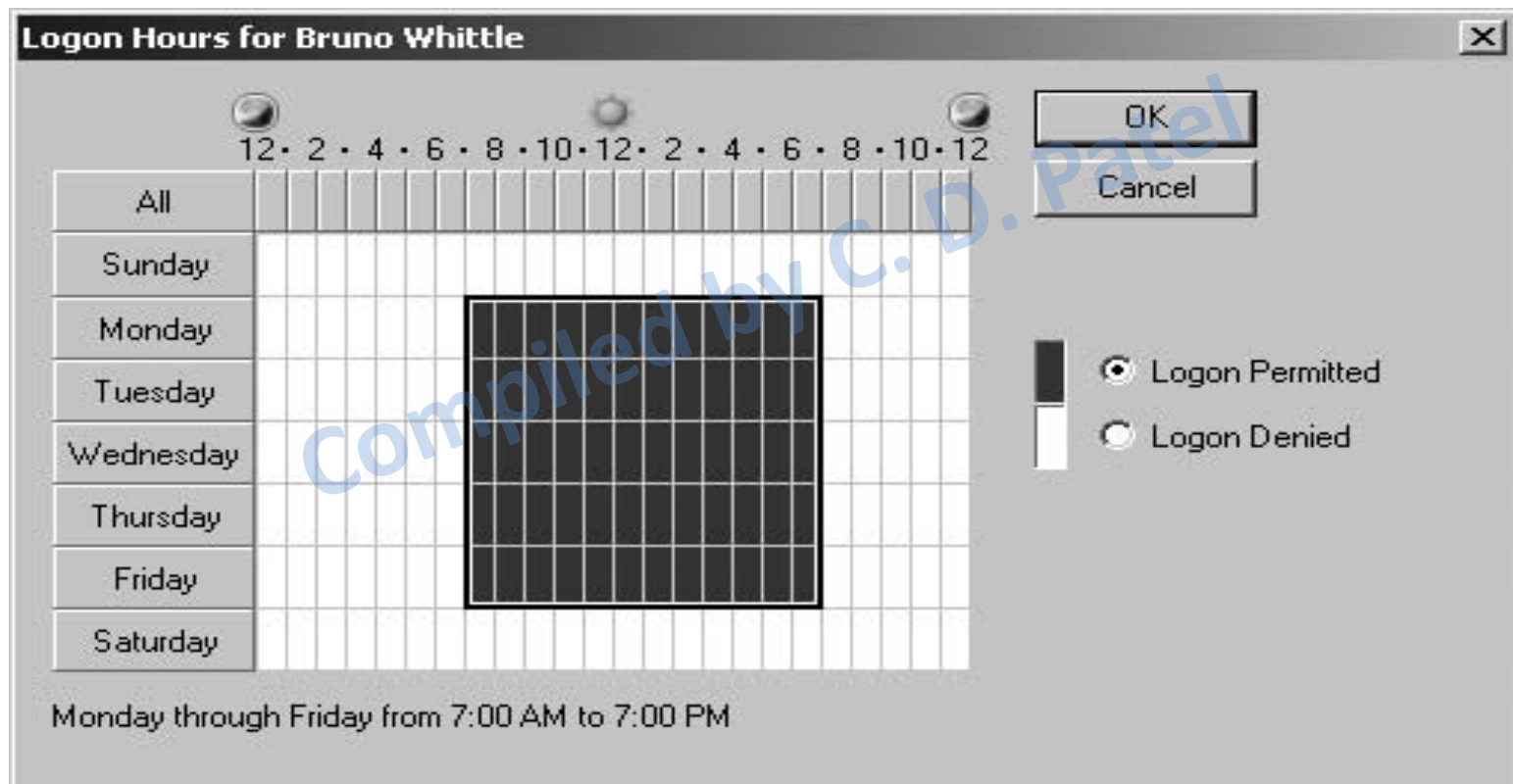


Figure 4.6 Setting logon time restrictions for a user

4.1.2 Modifying a User Account

- **Log On To:** users can log on to any workstation in the domain, and the domain authenticates them. In some cases, a system might require stricter security, some specific computers in which a user account can log on.

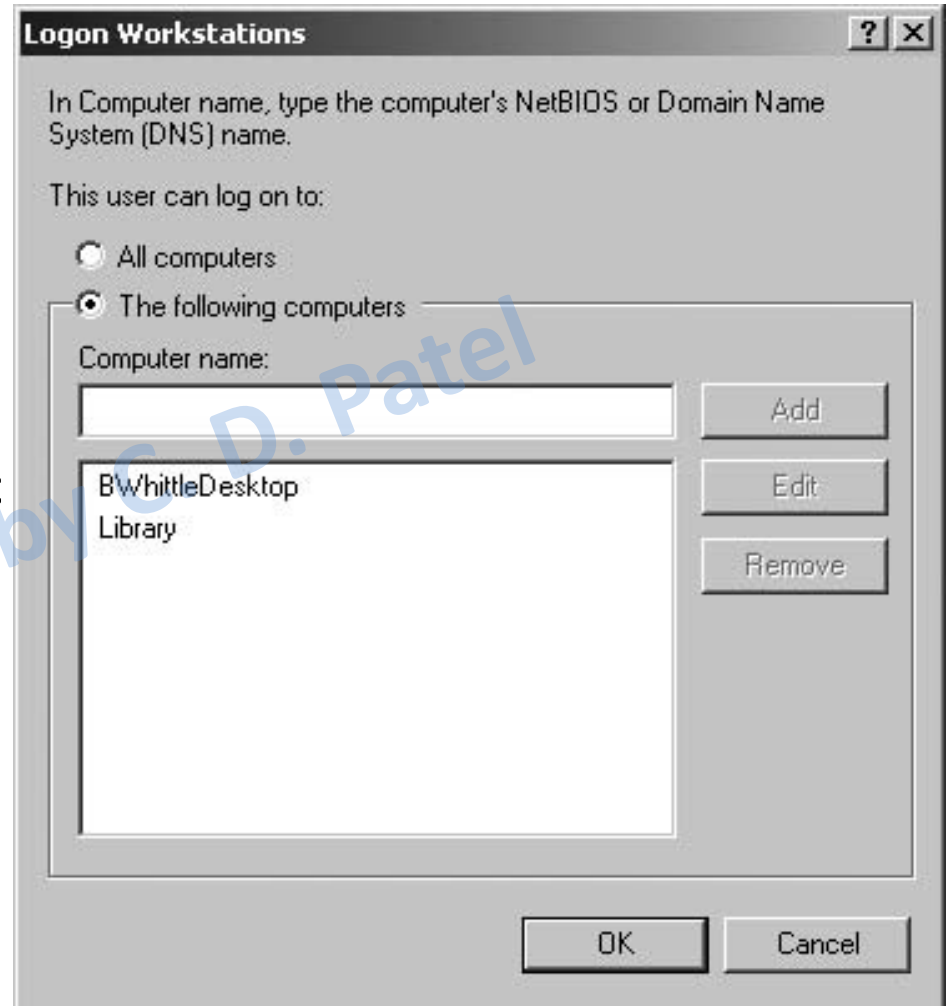


Figure 4.7 Restricting the computers to which a user can log on

4.1.3 Deleting a User Account

- **Step1**

Use the Active Directory Users and Computers console. Open this console by going to the Start screen and then clicking Active Directory Users And Computers.

- **Step2**

Select the Users folder that contains the user account.

- **Step3**

Right-click the user account, and then click **Delete**.

4.1.4 Disabling a User Account

- **Step1**
- Use the Active Directory Users and Computers console. Open this console by going to the Start screen and then clicking Active Directory Users And Computers.
- **Step2**
- Select the Users folder that contains the user account.
- **Step3**
- Right-click user account, and click Disable Account.

4.2 Working with Active Directory Security Groups

- Groups are used to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps simplify network maintenance and administration.
- Groups appear in two of the domain's containers: Builtin and Users.
- The built-in groups are fixed. They cannot be deleted or made members of other groups.

4.2.1 Creating Groups

1. Open Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers.
2. In the console tree, double-click the domain node.
3. Right-click the folder in which the group is to be added, point to New, and then click Group.
4. Type the name of the new group.
5. Select the desired **Group scope**.
6. Select the desired **Group type**.
7. Click **OK**. The new group will appear in the details pane of the Active **Directory Users and Computers**.

4.2.1 Creating Groups

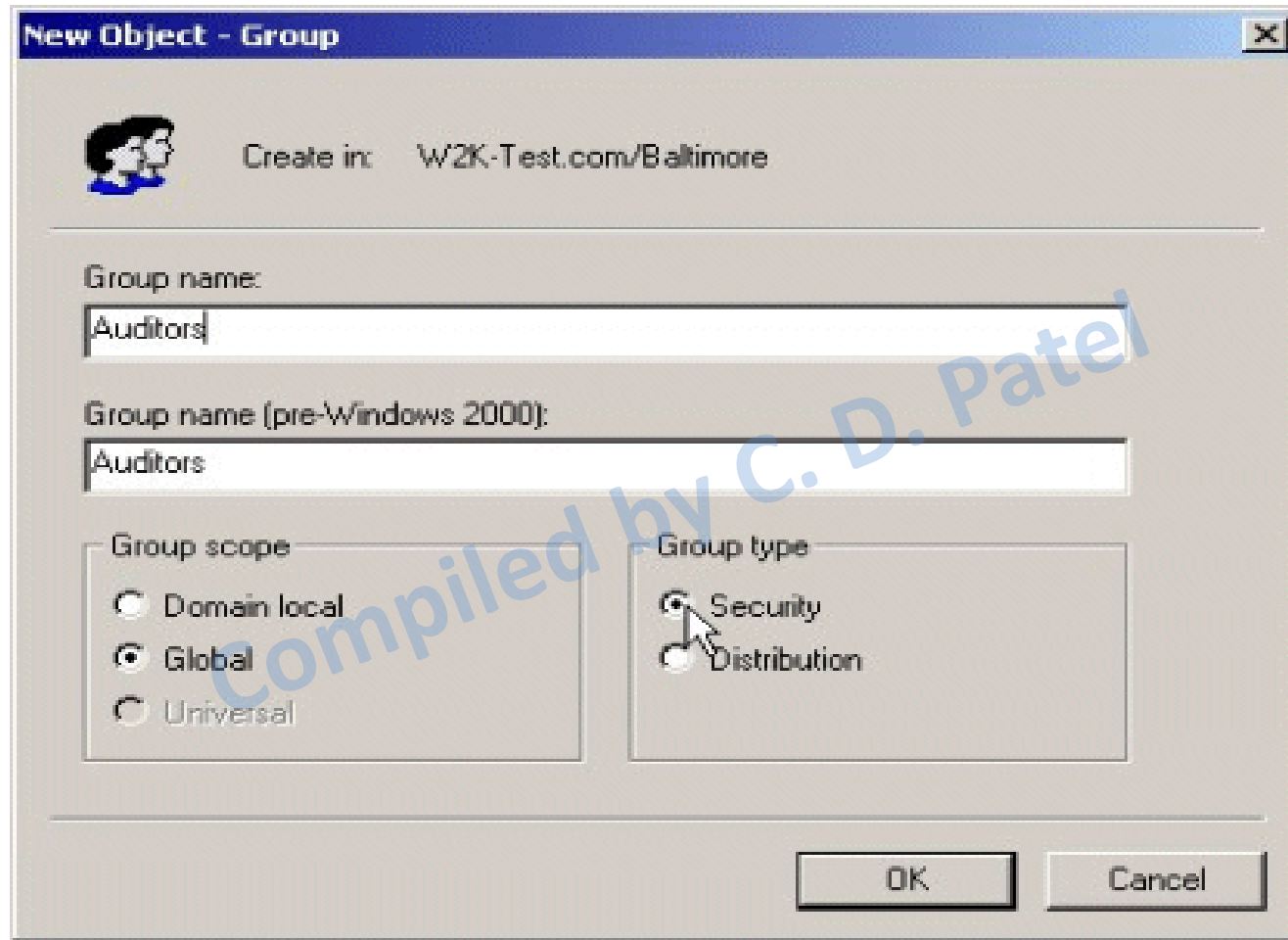


Figure 4.10 A brand-new group does not have any members.

4.2.2 Maintaining Group Membership

- A new group starts out without any members. To set the membership for a group, follow these steps:
 1. Select the group and open its Properties dialog box (by right-clicking it and choosing Properties from the pop-up menu).
 2. Then click the Members tab, as shown in Figure 4.11.
 3. Click the Add button.

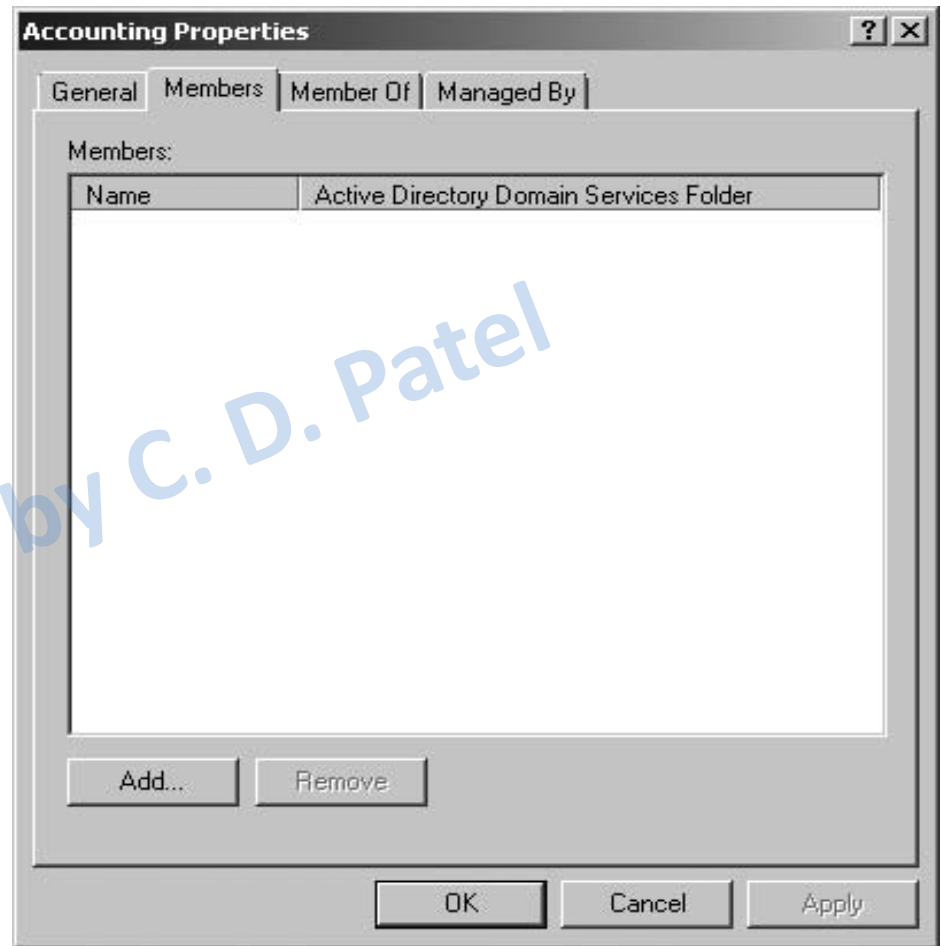


Figure 4.11. Adding a member to a group

4.2.2 Maintaining Group Membership

4. You see the Select Users, Contacts, Computers, or Groups dialog box, as shown in Figure 4.12.
5. Type a user or another group's name to identify it, and then click the Check Names button. If you type in too few characters to uniquely identify the user or group, Windows will show you a list of the possible matches from which you can select the correct one.
6. Choose the member you want to add, and then click OK.
7. Repeat steps 3 and 4 to complete the group membership.

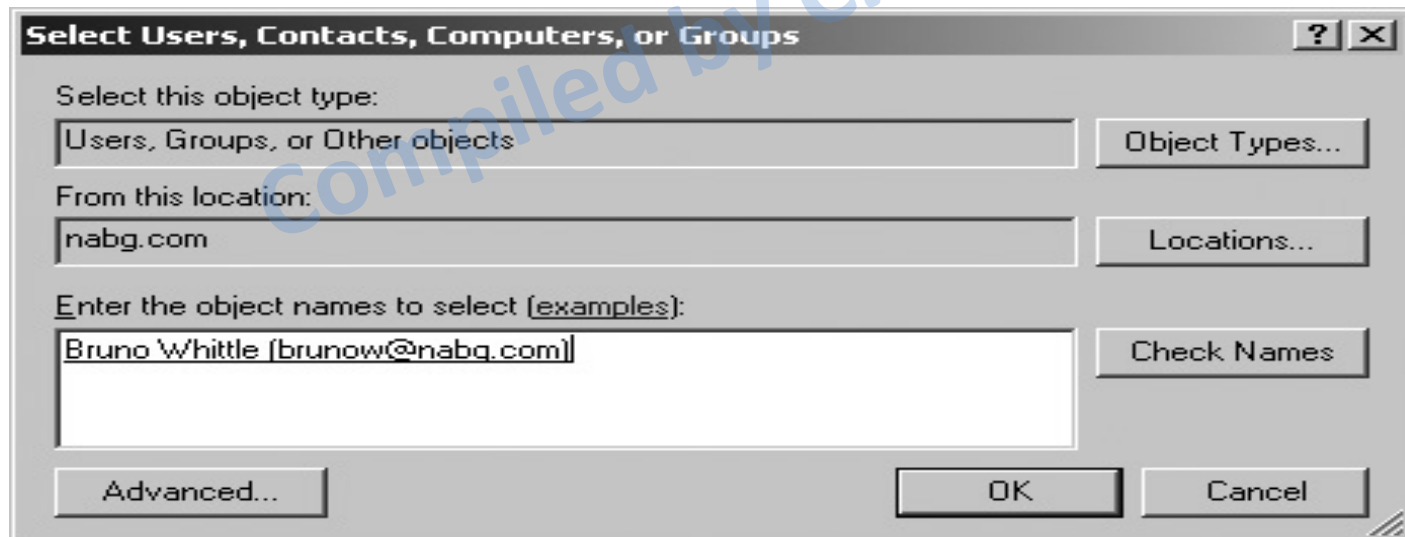


Figure 4.12 Adding a member to a group

4.3 Working with Shares

- Drives and folders under Server are made available to users over the network as shared resources, simply called shares.

4.3.1 Understanding Share Security

- Share permissions apply to users who connect to a shared folder over the network.
- **Read**
 - Read is the default permission that is assigned to the Everyone group. Read allows:
 - Viewing file names and subfolder names
 - Viewing data in files
 - Running program files
- **Change**
 - Change is not default permission for any group. The Change permission allows all Read permissions, plus:
 - Adding files and subfolders
 - Changing data in files
 - Deleting subfolders and files

4.3.1 Understanding Share Security

- **Full Control**
 - Full Control is the default permission that is assigned to the Administrators group on the local computer. Full Control allows all Read and Change permissions, plus:
 - Changing permissions (NTFS files and folders only)
- **No access**
 - If you apply this permission to folder or file user can not access those file and folder.
 - If you set No access permission for every group the member of that group will also receive No access because it overrides any other permission.

4.3.2 Creating Shares

1. Open either My Computer or Windows Explorer on the server.
2. Right-click the folder or drive you want to share, and then choose Share from the pop-up menu.
3. In the field provided, enter enough of a user's name to identify that person in the system, and then click Add.
4. Click the down arrow next to the user's name to set that user's permission level. The permission levels available are Owner, for full read and write access, plus the ability to grant permissions to other users; Contributor, for full read and write access; and Reader, for read-only access.
5. Click the Share button to create the share. You will see a confirmatory dialog box. Click OK, and the share will be created.

4.3.3 Mapping Drives

- The process of simulating a disk drive with a network share is called mapping.
- Many applications that store files on the network require that the network folders be accessible as normal drive letters.
- To create a drive mapping follow these steps:
 1. Open Network from the client computer
 2. Locate the share you want to map, right-click it, and choose Map Network Drive.
 3. In the dialog box that appears, the name of the domain and share will already be filled in for you. Simply select an appropriate drive letter(D:,E:..) for the mapping
 4. click OK.
 5. From then on, the share will appear to your computer as that drive letter, and users will see this share's letter in My Computer.

4.4 Administering Printer Shares

- As an administrator, two main things required so users throughout a network can access print devices connected to workstation or server.
 1. Set up a workstation or server as a print server.
 2. Use the print server to share print devices on the network.

4.4.1 Setting Up a Network Printer

- Steps to set up Network Printer:
 1. Open the server's Devices And Printers folder, which lists all the installed printers.
 2. Right-click the one you want to share and choose Printer Properties from the pop-up menu.
 3. The Properties dialog box for the printer will appear.
 4. Choose the Sharing tab, which displays the dialog box shown in Figure 4.14.
 5. On the Sharing tab, click the Share This Printer checkbox, and then assign the printer a share name by which the client computers will recognize the printer.
 6. At this point, you can click the OK button because the default permissions for a shared printer are for everyone group to be able to print to it alternatively.

4.5 Working with Windows Backup

- Backup Server: A server responsible for backing up and restoring files, folders, databases and hard drives on a network in order to prevent the loss of data in the event of a hard drive failure, user error, disaster or accident..
- Windows Server Backup use to back up a full server (all volumes), selected volumes, the system state, or specific files or folders.
- Windows Server Backup create and manage backups for the local computer or a remote computer. And schedule backups to run automatically.
- Data will be lost due to hard disk failures and application or user mistake. So having good copies of that data on multiple backup can save data lost.

Types of Back Up: Full Backup

1. **Full backup:** all the files and folders selected for the backup will be backed up. When subsequent backups are run, the entire list of files and will be backed up again.
- **Advantage:**
 - Restores are fast and easy
 - Easy to maintain.
- **Disadvantage:**
 - Time consuming because the entire list of files is copied again.
 - Required more storage space.

Types of Back Up: Incremental Backup

2. **Incremental backup:** One full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.
 - **Example:** a full backup was done on Day 1, Day 2's incremental will back up all of the files that have changed since Day 1. Likewise, Day 3's incremental backup will only copy those files that have changed since Day 2's incremental took place.
 - **Advantage:**
 - Much faster backups.
 - Efficient use of storage space as files is not duplicated.
 - Less storage space used compared to running full backups.
 - **Disadvantage:**
 - Restores are slower.
 - Restores are a little more complicated.

Types of Back Up: Differential Backup

- 3. Differential backup:** one full backup is done first and subsequent backup runs are the changes made since the **last full backup**.
- **Example:** a full backup was done on Day 1, Day 2's differential will copy all of the files that have changed since Day 1's backup copied everything. Day 3's differential backup will also copy all of the files that have changed since Day 1's full copy was made.
 - **Advantage:**
 - 1) Faster restores than incremental backups
 - 2) More efficient use of storage space than full backups.
 - **Disadvantage:**
 - 1) Backups are slower than incremental backups
 - 2) Not as efficient use of storage space as compared to incremental backups.
 - 3) Restores are a little more complicated than full backups but simpler than incremental backups.

Types of Back Up: Copy Backup

4. Copy backup:

Copy backup is a backup that copies all selected files but does not mark each file as having been backed up. It does not affect these other backup operations.

- Microsoft Windows Server operating systems also include a built-in Windows Server Backup feature that can be used to perform basic backup and recovery operations on backup servers.

Assignments

1. Explain user accounts with their types. How to create and manage the user in active directory?
2. What is mapping drive? Write a step to map network drive.
3. What is sharing? Write a step to perform file sharing in network.
4. Explain Group account & windows security groups.
5. Explain Printer Server **OR** what is network printer? Write the steps to install network printer.

Assignments

6. Write a step to perform windows server backup.
7. Define Backup Server & Discuss different types of back up.
8. List steps to Modify, Delete User Account.
9. Write down steps to activate a user.
10. What do you mean by group membership?
Discuss create and maintain a group membership.