

**GOVERNMENT POLYTECHNIC
AHMEDABAD
PROGRAM: DIPLOMA IN COMPUTER
ENGG**

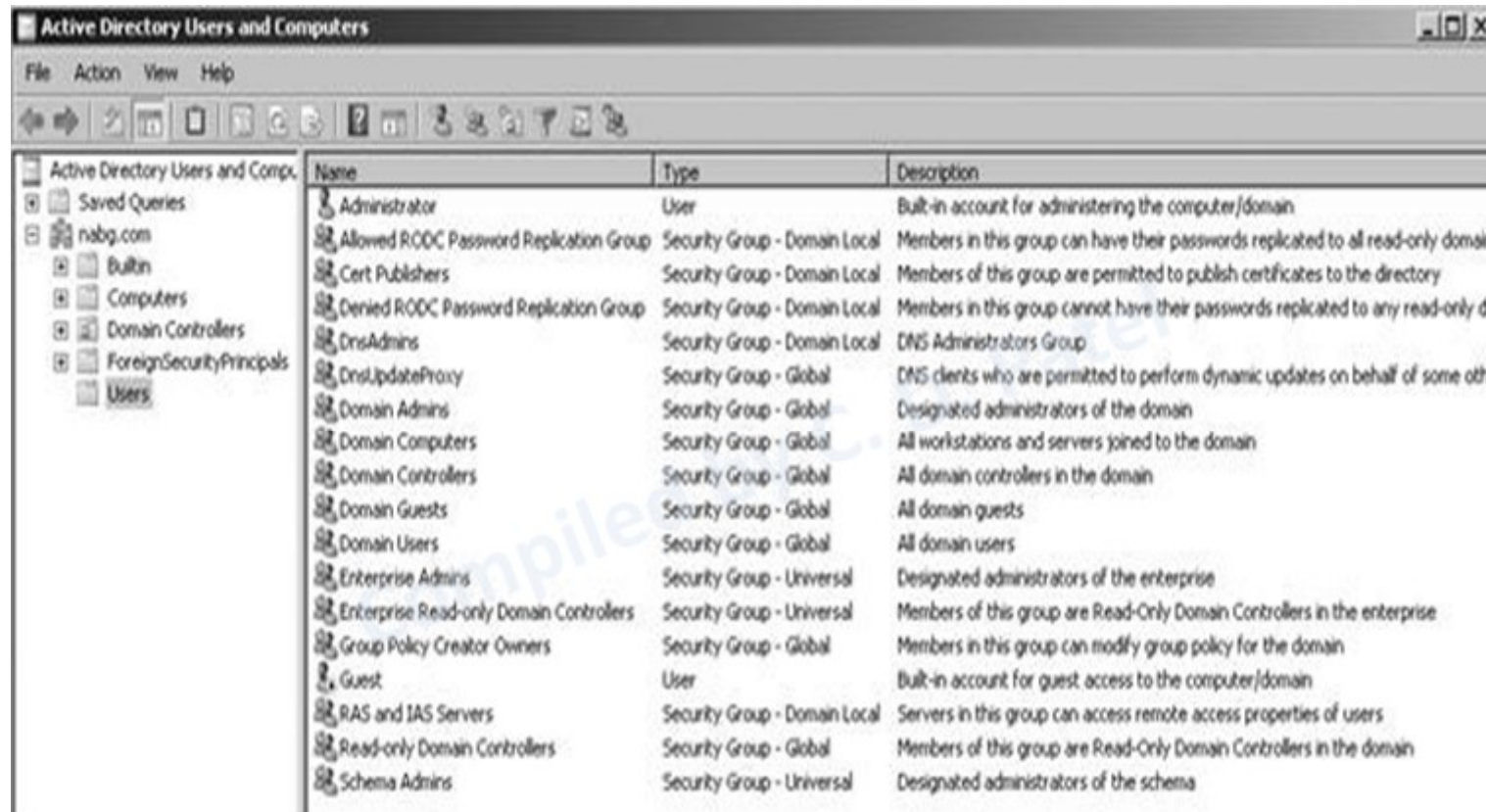
**NETWORK MANAGEMENT AND
ADMINISTRATION (3360703)**

**UNIT-4
NETWORK CONFIGURATION**

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.
 - 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.
 - From Server Manager, Open the Tools menu, and select
 - Active Directory Users and Computers from the menu.

4.1 Working with User Accounts



The screenshot shows the 'Active Directory Users and Computers' console window. The left pane shows a tree view with 'Users' selected under 'nabq.com'. The main pane displays a table of users and groups with columns for Name, Type, and Description.

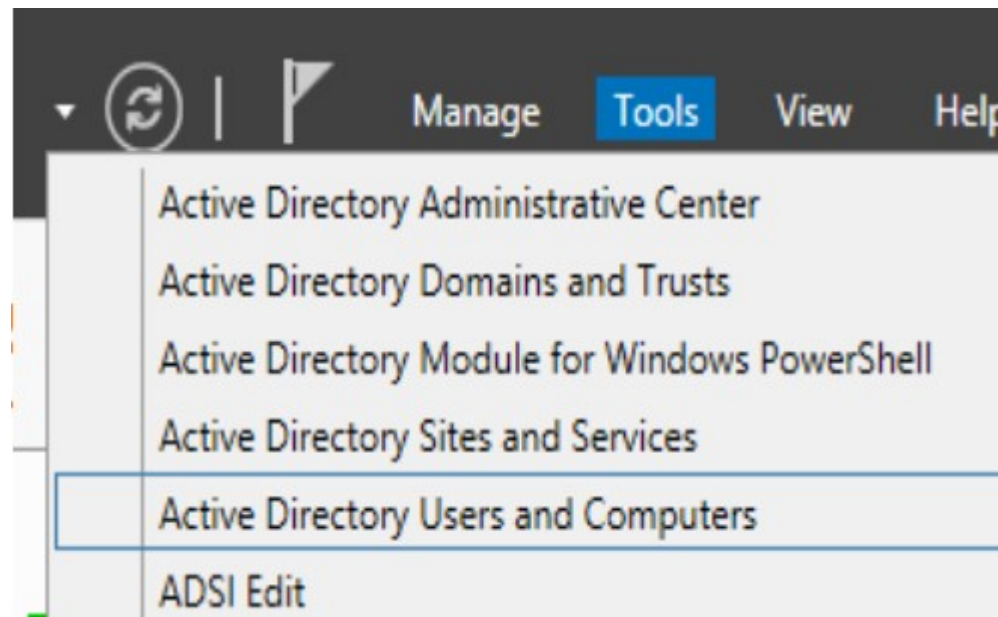
Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to all read-only domain controllers
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates to the directory
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicated to any read-only domain controllers
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates on behalf of some other client
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers in the enterprise
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access properties of users
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers in the domain
Schema Admins	Security Group - Universal	Designated administrators of the schema

4.1.1 ADDING A USER

- First start by selecting the users container in the left pane with the tree open to the domain you are administering.
- Right click in the user container, choose from the pop-up menu, and then choose user from the submenu.
- You see the create new object(user) dialog box
- Fill up the detail in field shown in figure like first name last name, name(full user name), user logon name and click in next.

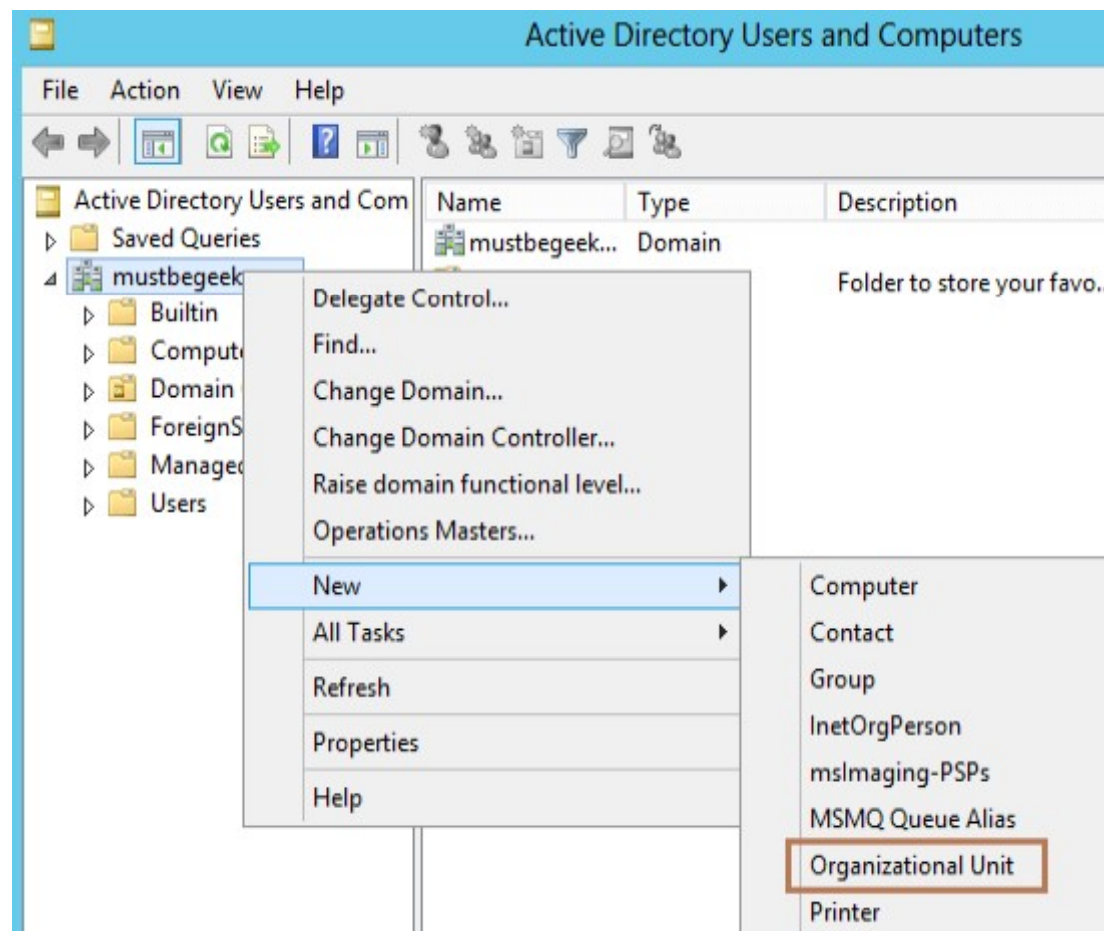
4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 1. Open server manager from taskbar
- 2. Go to Tools ->Active Directory Users and Computers



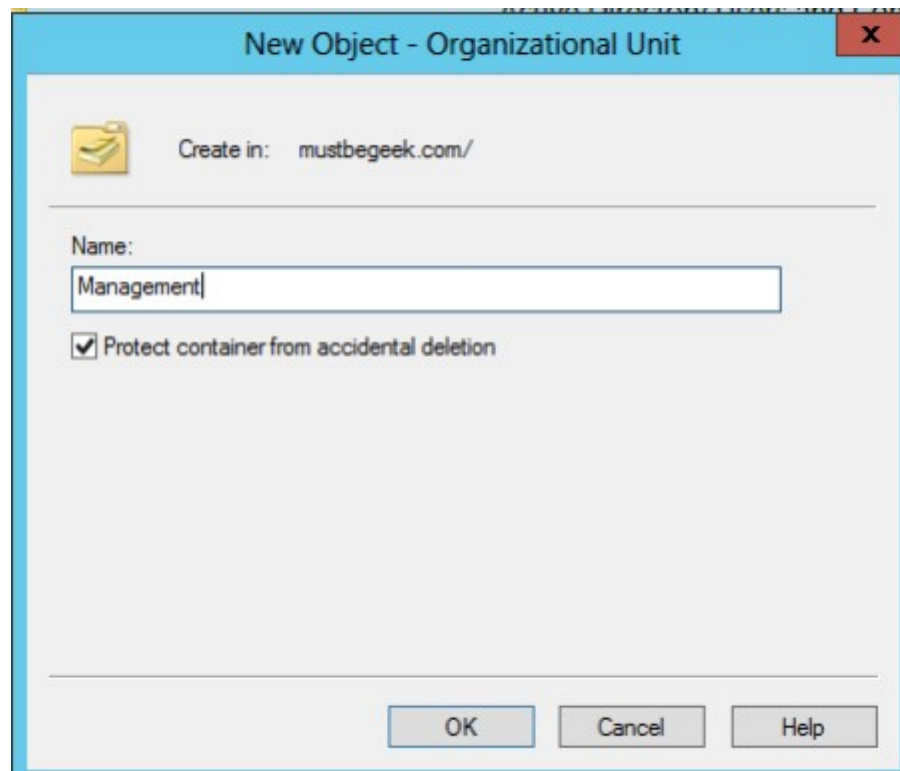
4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 2. Create An Organizational Unit



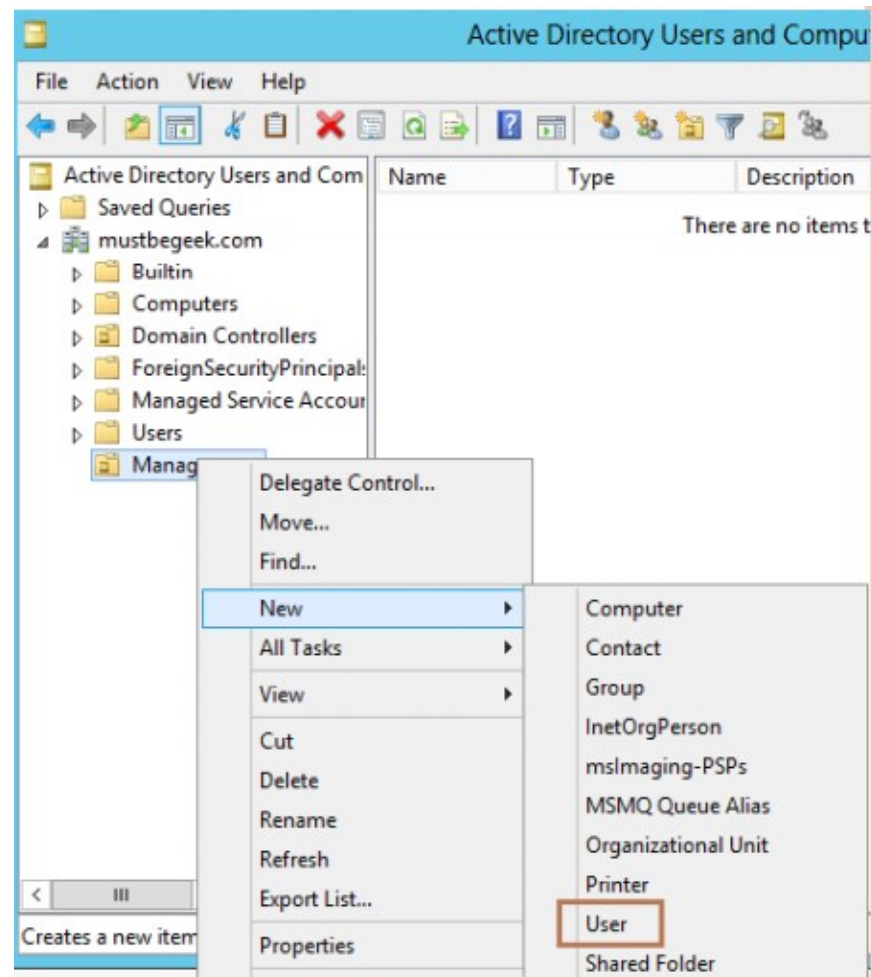
4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 3. Type Management To Name The Ou. Check The Protect Container From Accidental Deletion Option. This Option Will Protect This Object From Accidental Deletion.



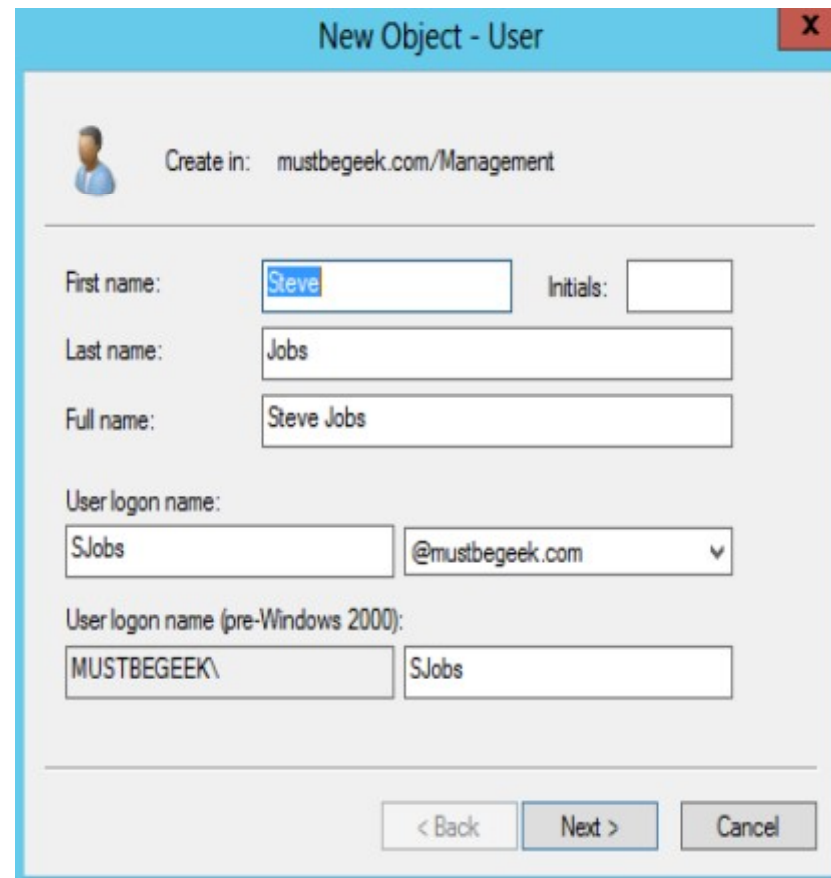
4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 3. Create New User Right-click The Management Ou, Click New And Click User.



4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 4. Now Type The User Information. Type The First Name And Last Name. Here User Logon Name Is The Name That The User Will Use To Actually Log In The Computer In The Network. So When User Tries To Log In, He Will Type Sjobs@mustbegeek.Com Or Mustbegeek\sjobs On Username Field. Now Click Next.



New Object - User

Create in: mustbegeek.com/Management

First name: Steve Initials:

Last name: Jobs

Full name: Steve Jobs

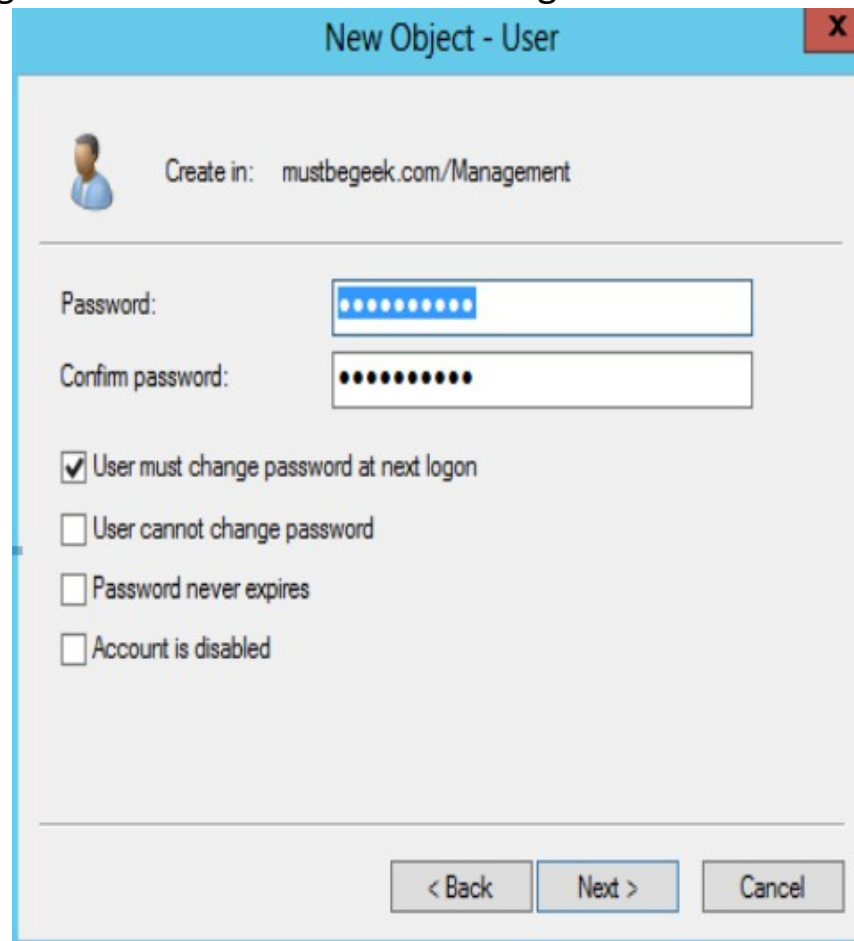
User logon name: SJobs @mustbegeek.com

User logon name (pre-Windows 2000): MUSTBEGEEK\SJobs

< Back Next > Cancel

4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 5. Now Type The Password. Check User Must Change Password At Next Logon. The User Will Be Forced To Change The Password When User Logs In. Click Next.



New Object - User

Create in: mustbegeek.com/Management

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

Cont..

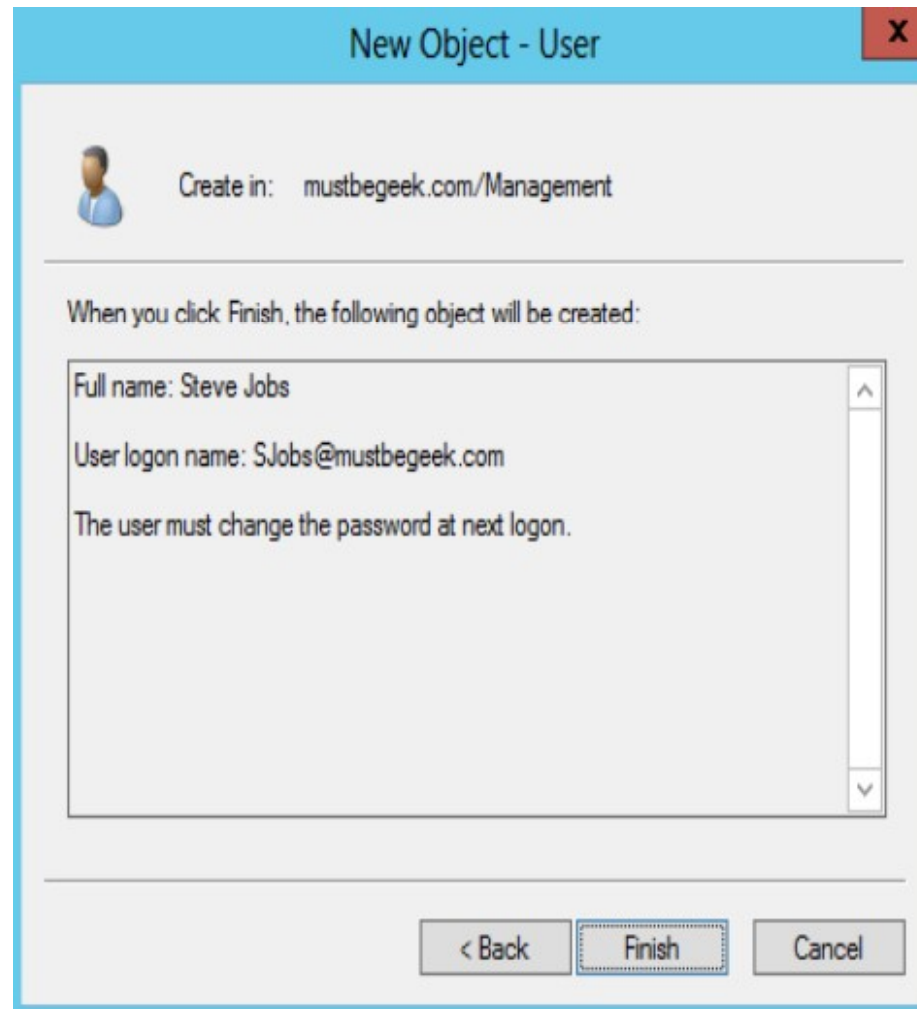
- On clicking the Next button a New Form will be opened in which you need to provide the Password for the new user. Also select several options that apply to the account, as follows:
- **User Must Change Password at Next Logon:** Users to choose their own password when they first log in to the system.
- **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.

4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 6. In this window, type the Password used to login to Computer in Password and Confirm password fields. In addition to that there are certain options that you can select as per your requirement.
 - Must change password at next logon: This option will force to change the password when they first logon.
 - Cannot change password: User will not be able to change the password and will be forced to use the password set by Administrator.
 - Password never expires: Password would not expire and will not force to change the password.
 - Account is disabled: Account will be created by it will be disabled i.e. user will not be able to login until the account is enabled.

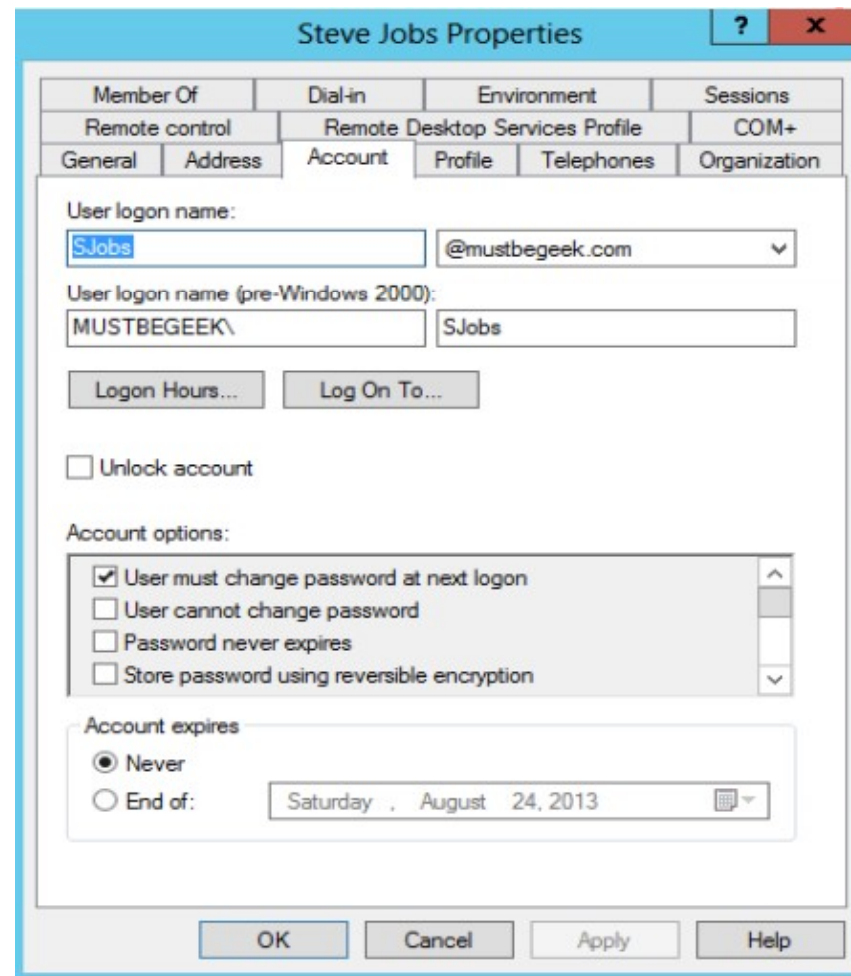
4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 7. Review The User Configuration And Click Finish.



4.1.1 ADDING USER: CREATE USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 8. You Have Successfully Created A User Account. You Can Open The Properties Of The User Account To Tweak Settings.

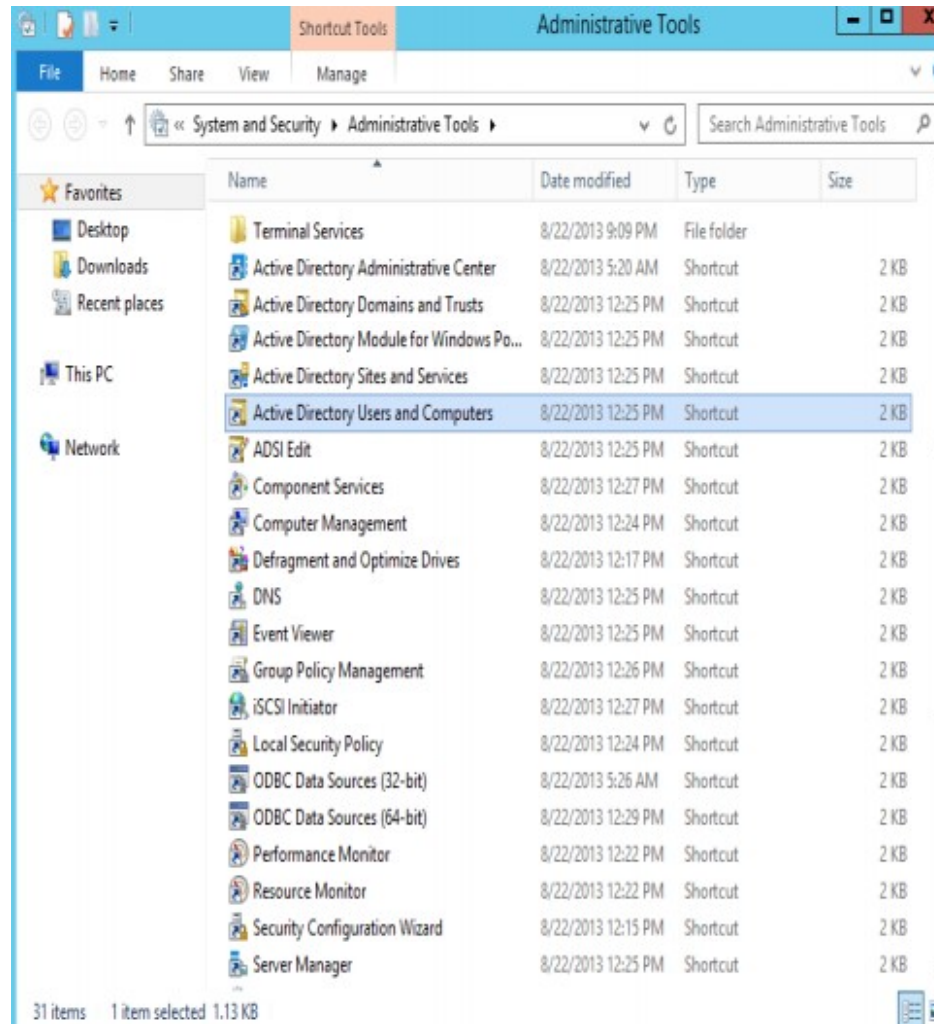


4.1.2 MODIFYING USER ACCOUNT

- You can see a dialog box of creating user account, creating a user account are much simpler than the one you see when modifying a user account. The dialog box in which you modify the information about a user contains many other fields that you can use to document the account and to set some other security option.
- To modify an existing user account, right click the user object you wish to modify and choose properties from the pop-up menu.

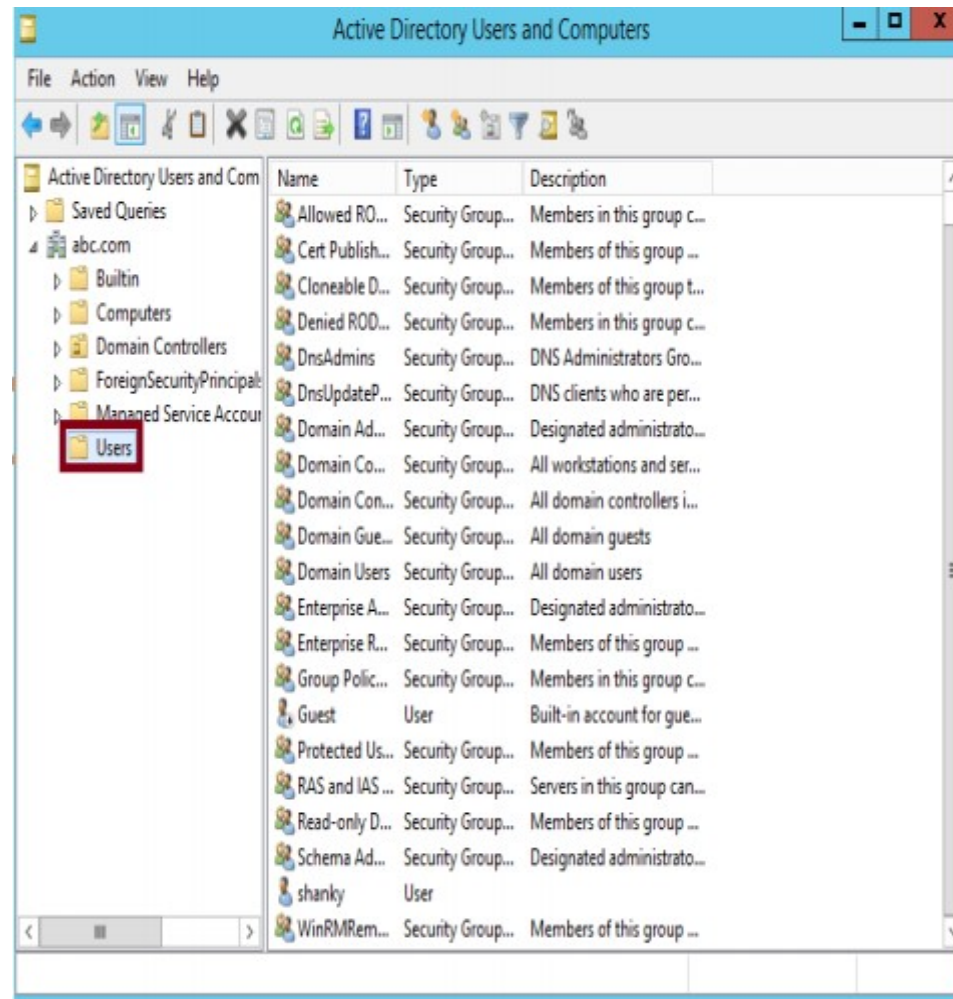
4.1.2 MODIFYING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 1. Open server manager from taskbar
- 2. Go to Tools ->Active directory users and computers



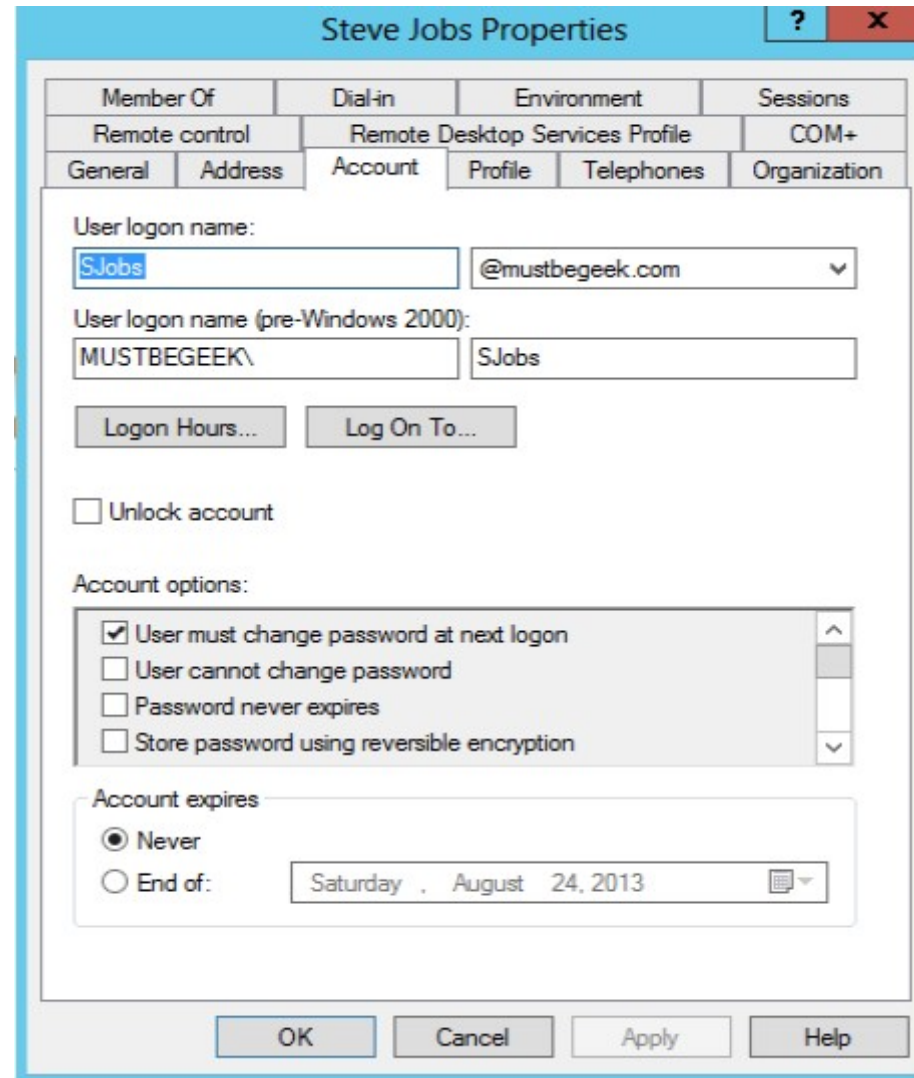
4.1.2 MODIFYING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 3. In the console we'll see all the Containers and Organizational Units. Select Users, it will show all the default users and groups that are created by default.



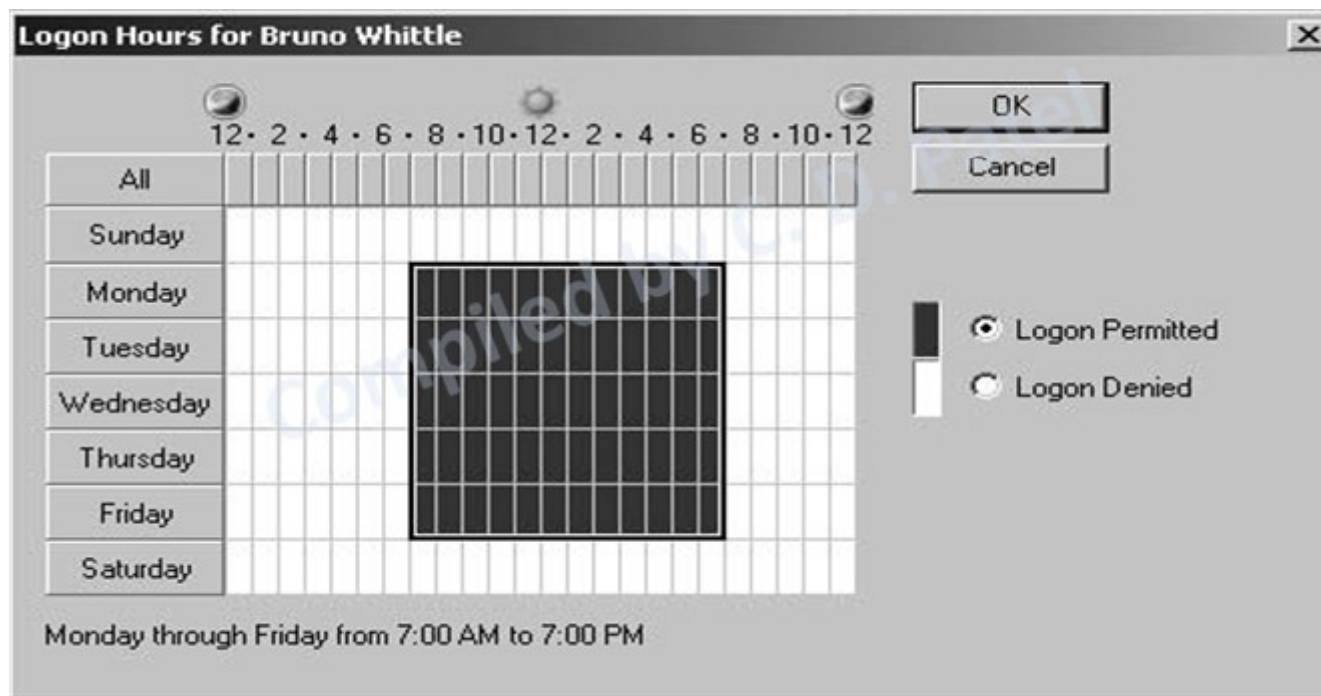
4.1.2 MODIFYING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 4. Right click on user name whose detail you want to modify and select properties.
- 5. Properties of the selected user will open.
- 6. Now you can modify user's general detail like its first name, last name, initials, description, e-mail, web page, telephone number, etc... from general tab.
- 7. Click apply and ok.



4.1.2 MODIFYING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

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



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.

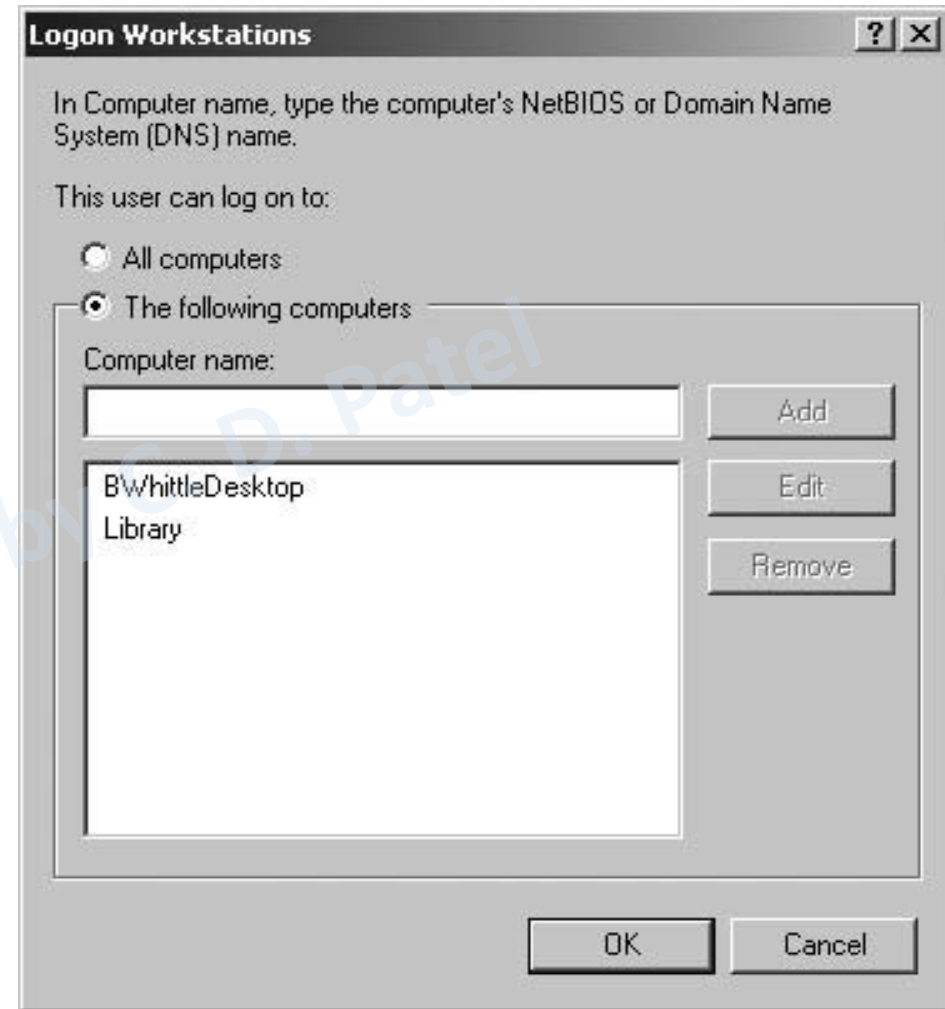


Figure Restricting the computers to which a user can log on

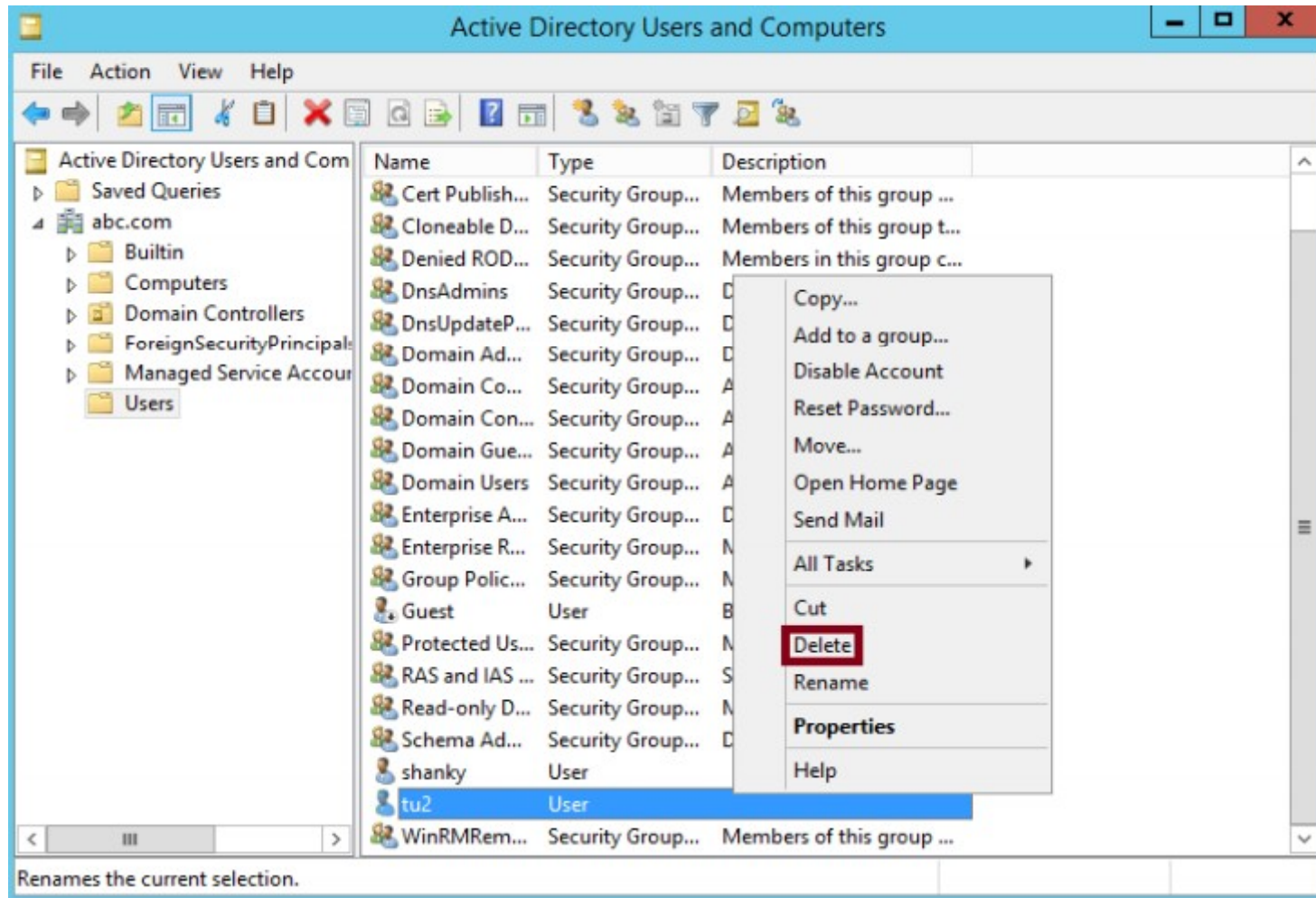
4.1.3 DELETING OR DISABLING A USER ACCOUNT.

- First click in start menu-control panel Administrative tools.
- Click on active directory users and group management console.
- Use the left pane to select the users folder.
- Select the user in the right pane.
- Right click on user and choose delete or open the action pull-down menu and choose delete.

4.1.3 DELETING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

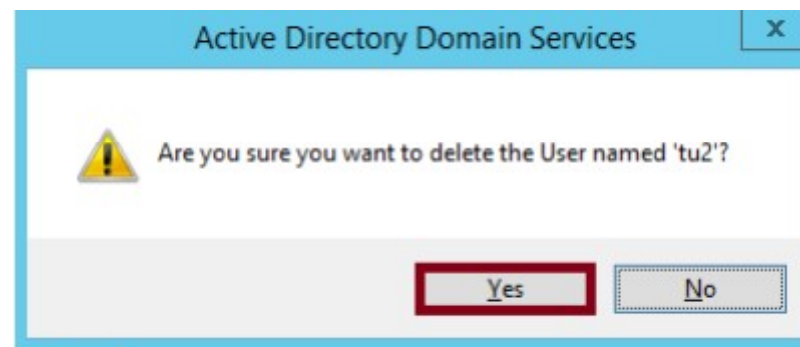
- 1. Follow steps 1 to 3 from the create user in Windows Server section.
- 2. Select the user that you want to delete. Right click the object and select “Delete”.

4.1.3 DELETING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER



4.1.3 DELETING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

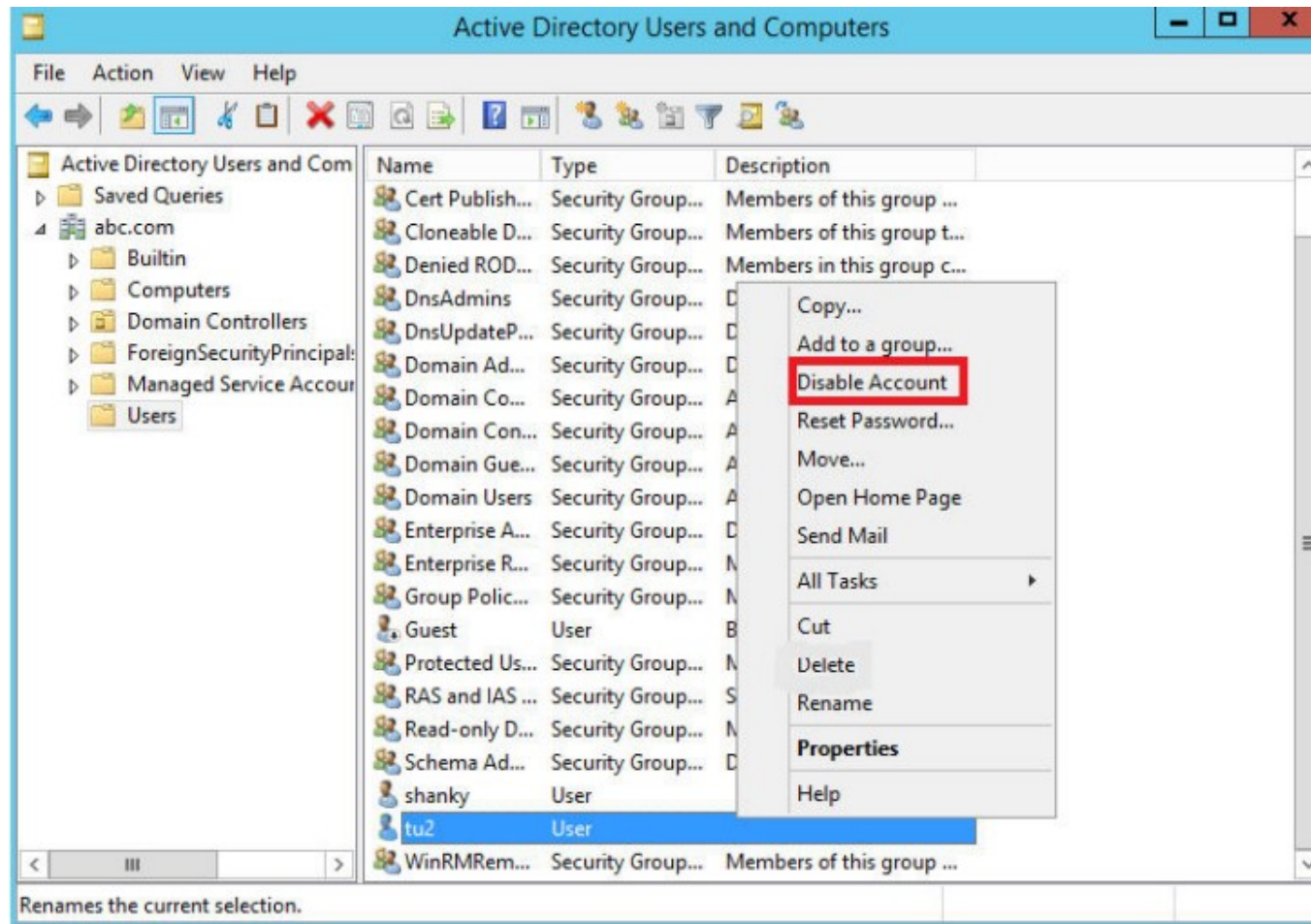
- 3. A pop-up window will open ask the confirmation to delete the account. Click on Yes if you want to process with user account deletion.



4.1.3 DISABLING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER

- 1. Follow steps 1 to 3 from the create user in Windows Server section.
- 2. Select the user that you want to delete. Right click the object and select “Disable Account”.
- 3. Right click on username which you want to disable.
- 4. Click Disable Account.
- 5. A pop-up window will open ask the confirmation to disable the account. Click on Yes.
- 6. Disabled user can be confirmed by looking into Active Directory Users and Computers window, denoted by down arrow.

4.1.3 DISABLING USER ACCOUNT IN SERVER 2012 DOMAIN CONTROLLER



4.2 WORKING WITH WINDOWS SECURITY GROUPS

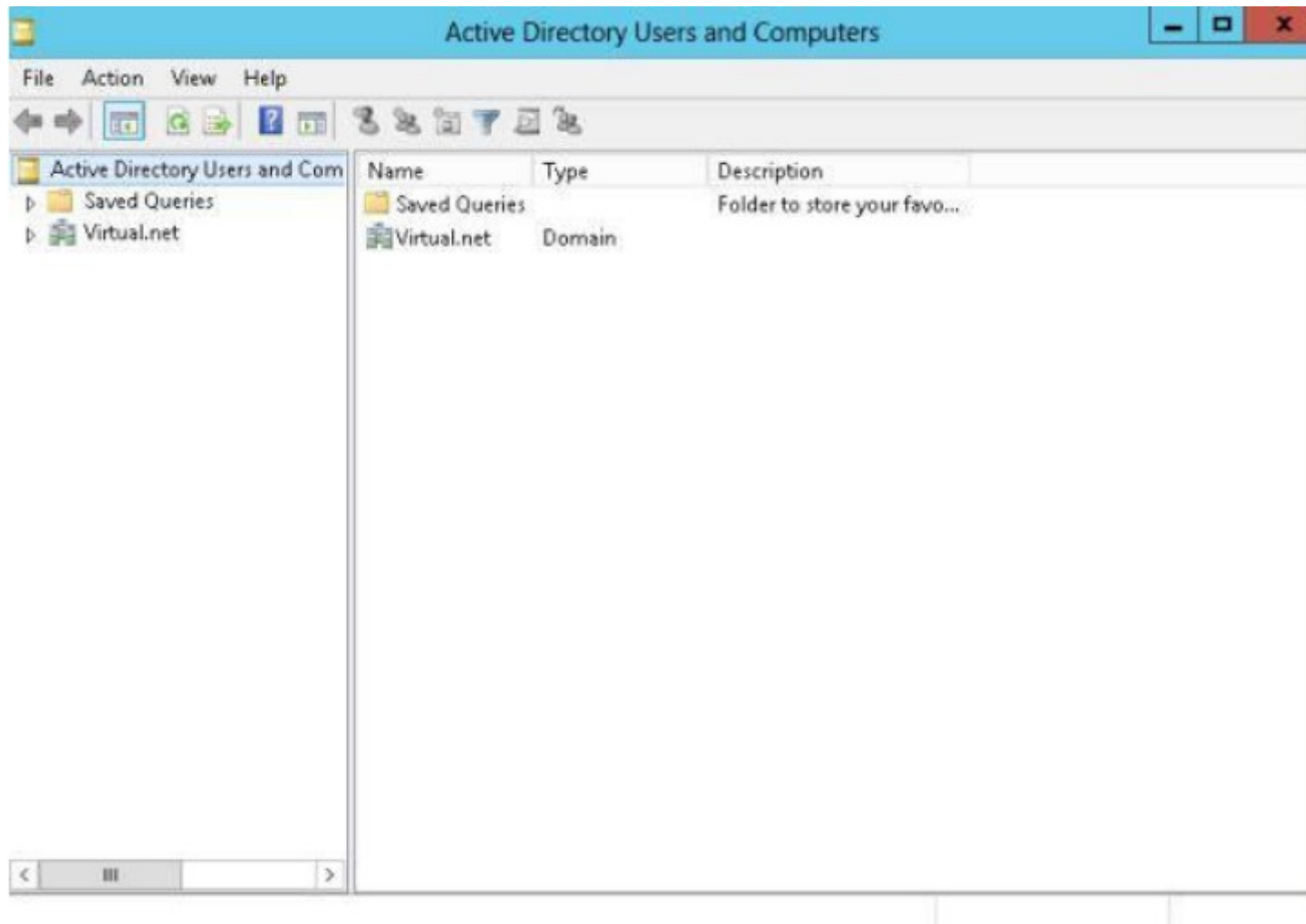
- In every network, you usually have to administrator permission to many different folders and files. If you were able to grant access only by user account.
- For example,30 folder and 20 files are in server, you can assign a permission to one group(like account group) can access 10 folder and 10 files only. You can assign a permission to another group(like sales) can access remaining folder and file but can not access folder and file to assign a account group
- All network operating systems support the concept of security groups.
- Not only can users be a member of groups, also groups can be members of other groups. This way you can build a hierarchy of groups that makes administration even easier

4.2.1 CREATING GROUP

- 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: Built in and Users.
- The built-in groups are fixed. They cannot be deleted or made members of other groups.

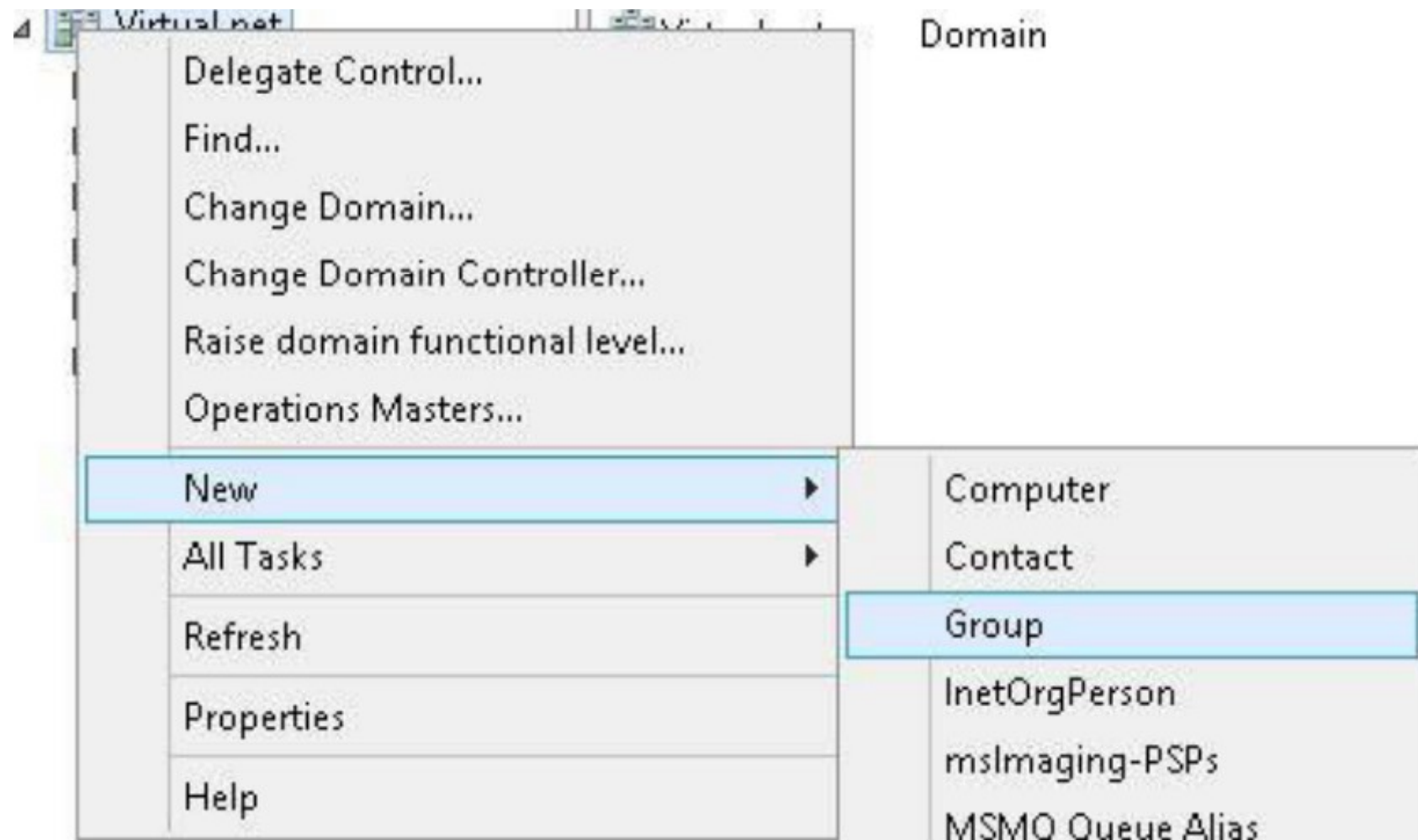
4.2.1 CREATING GROUP

- 1. Open server manager from taskbar
- 2. Go to Tools -Active directory users and computers



4.2.1 CREATING GROUP

- 3. Now right-click on your domain (Virtual.net) to add a new group.



4.2.1 CREATING GROUP

- 4. provide a few more items of information to create a new group like Group Name, Group Scope, Group Type etc. and then click the "Ok" Button.



New Object - Group

Create in: Virtual.net/

Group name:
Group1

Group name (pre-Windows 2000):
Group1

Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

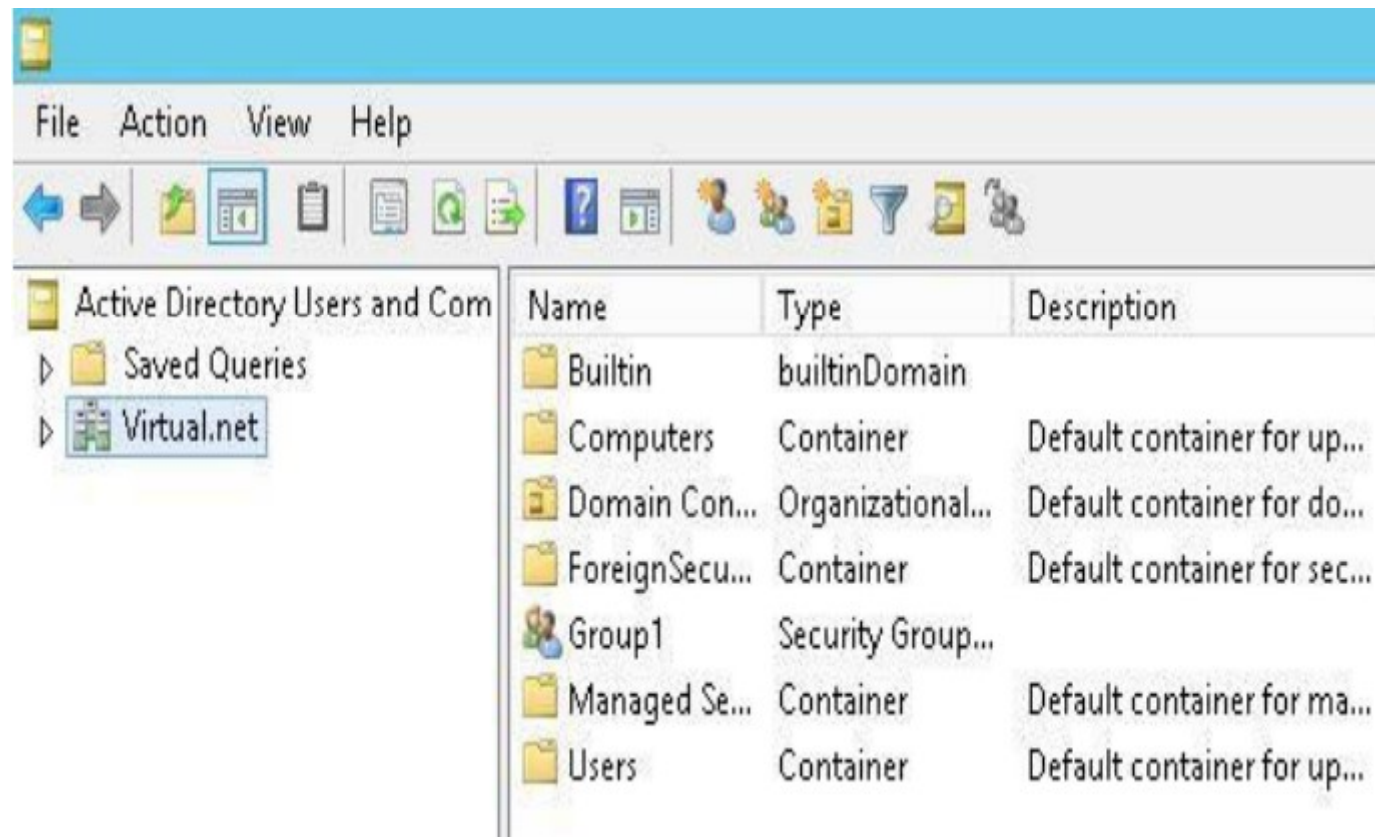
OK Cancel

4.2.1 CREATING GROUP

- After naming the group, you need to select the option buttons in the lower half of the dialog box.
- Group scope refers to how widely the group is populated throughout a domain.
 1. Domain local groups exist only within a single domain and it can contain members only from that domain.
 2. Global groups can contain members from domain in which they exist.
 3. Universal groups exist throughout an organization. Group types:
 - 1. Security group
 - 2. Distribution group

4.2.1 CREATING GROUP

- Now your domain will show your newly created group.

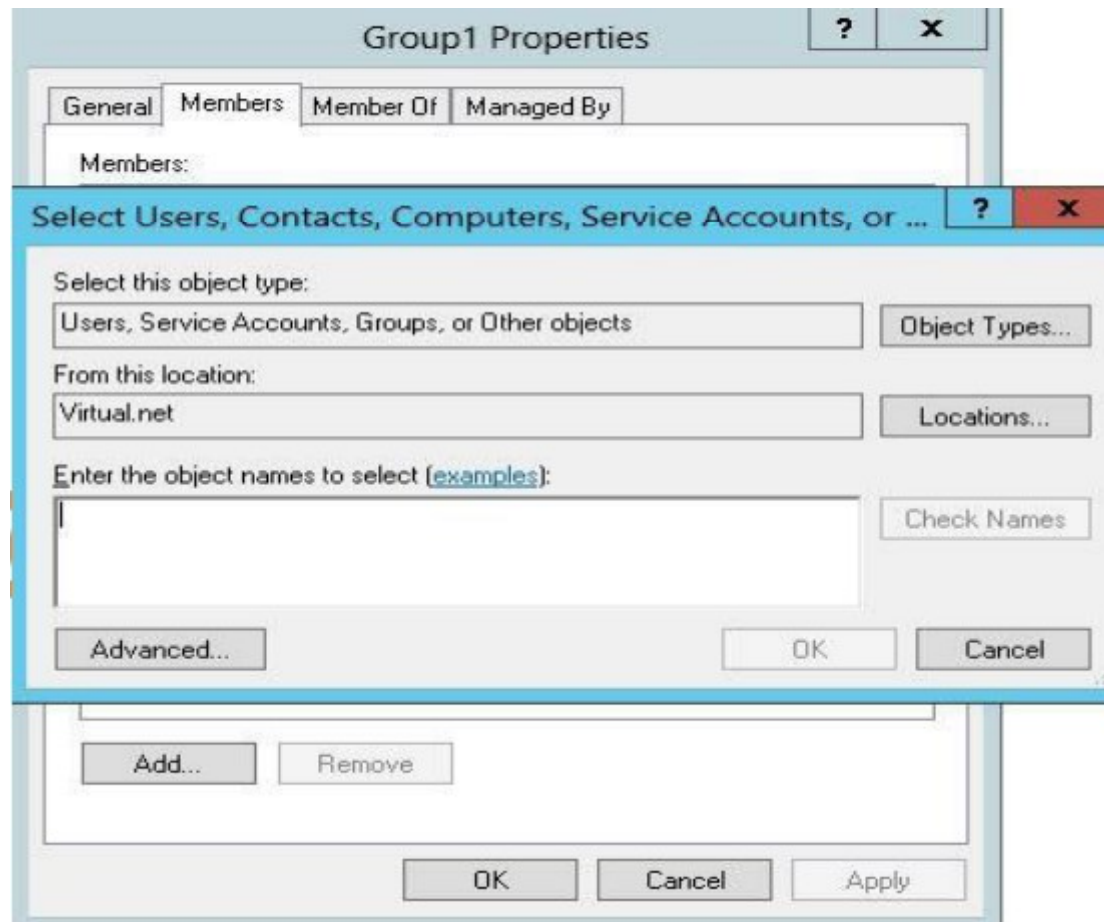


4.2.2 MAINTAINING GROUP MEMBERSHIP

- Select the group and open its properties dialog box (by right clicking and then choosing properties from the pop-up menu).
- Click the member tab. You see the group properties dialog box shown in figure A, you can see no member are added by default.
- Click the add button. You see the select users, contacts, computers, service account or group dialog box.
- Scroll through the list to select each member you want to add to the group and then click the add button to add your selected members to the list of members.
- The list displays only object that can be made of the group.

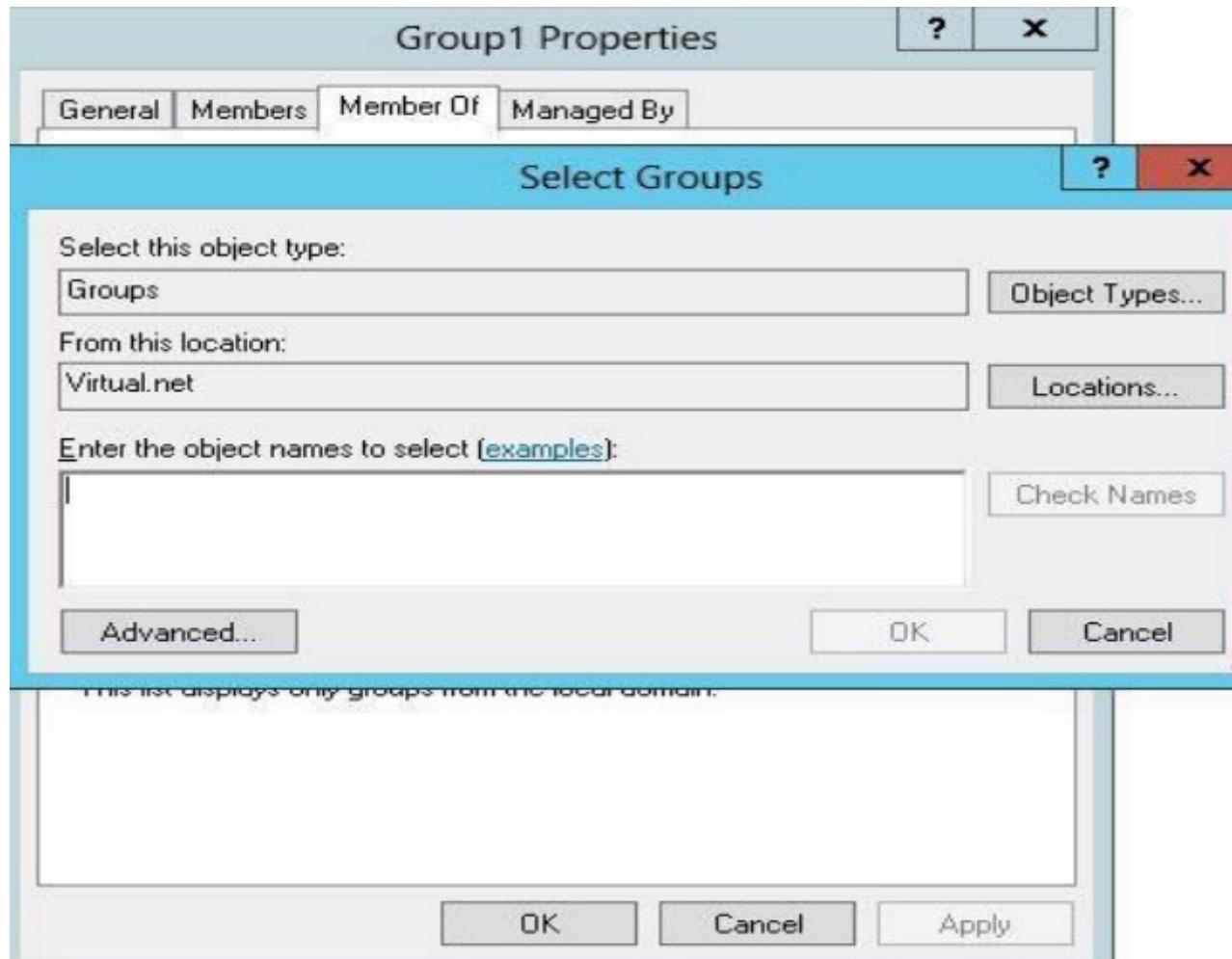
4.2.2 MAINTAINING GROUP MEMBERSHIP

- 1.You can add the user either by entering the user's name if you remember the name or you can do an Advanced Search to find the user and then add it.



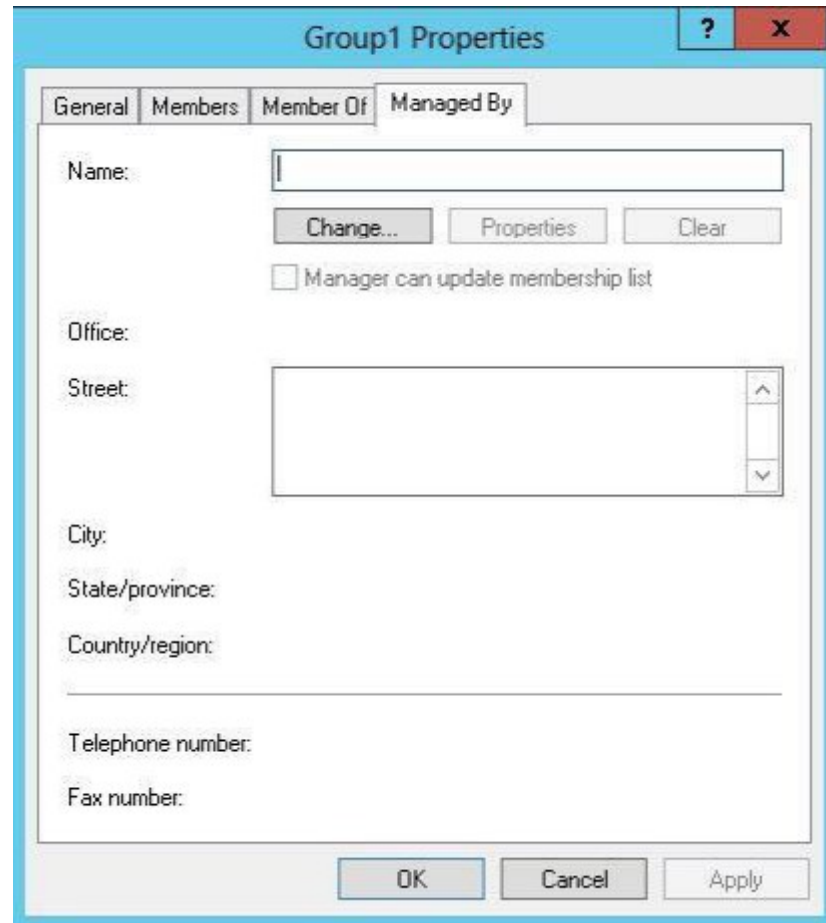
4.2.2 MAINTAINING GROUP MEMBERSHIP

- 2. The next page is named "Member of" from which you can make this group a member of any other group.



4.2.2 MAINTAINING GROUP MEMBERSHIP

- 3. The last page is for the user that will manage this group. You can provide the name and information of the person who will be responsible for managing this group.



The image shows a screenshot of a Windows-style dialog box titled "Group1 Properties". The dialog has a blue title bar with a question mark icon and a close button (X). Below the title bar are four tabs: "General", "Members", "Member Of", and "Managed By". The "Managed By" tab is currently selected. The main area of the dialog contains several input fields and buttons:

- Name:** A text input field with a "Change..." button to its left, a "Properties" button to its right, and a "Clear" button to its right.
- Manager can update membership list**
- Office:** A text input field.
- Street:** A text input field with a vertical scroll bar on its right side.
- City:** A text input field.
- State/province:** A text input field.
- Country/region:** A text input field.
- Telephone number:** A text input field.
- Fax number:** A text input field.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

4.3 WORKING WITH SHARES

- Drives and folders under windows server are made available to user over the network as shared resources, simply called shares in windows networking parlance.
- You select a drive or folder, enable it to be shared and then set the permission for the share.

4.3 WORKING WITH SHARES

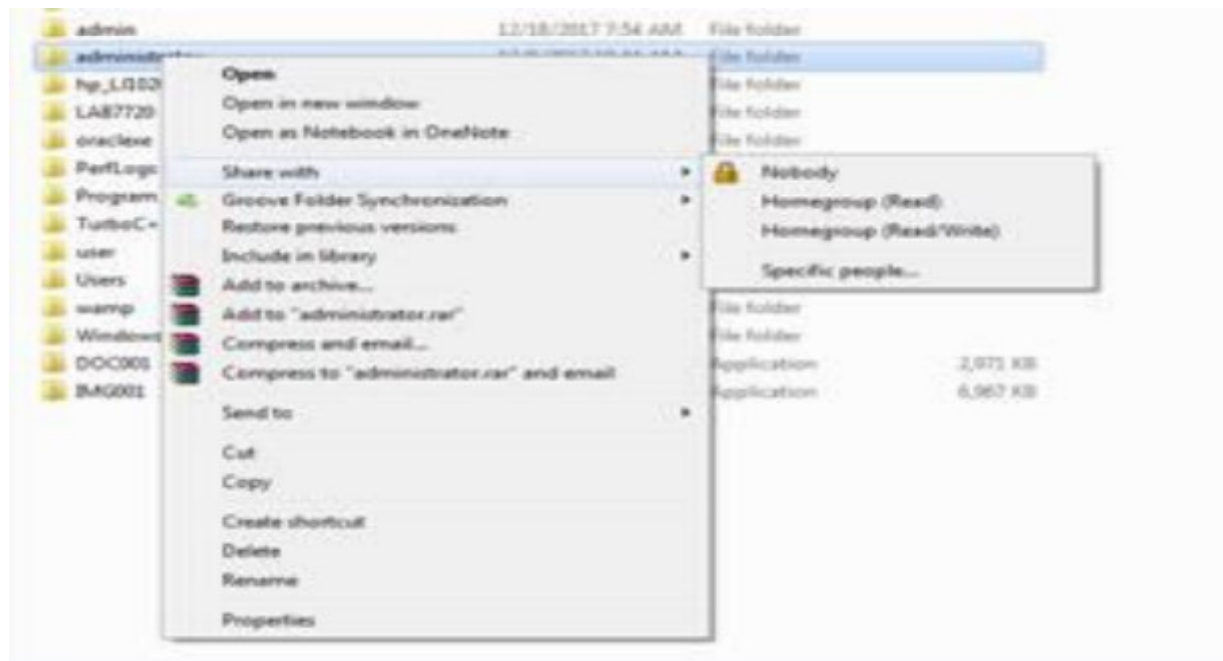
- Drives and folders under Server are made available to users over the network as shared resources, simply called shares.
- Understanding Share Security
 - Share permissions apply to users who connect to a shared folder over the network.
 - Change
 - Change is not default permission for any group. The Change permission allows all Read permissions, plus:
 - Adding files and subfolders
 - Changing data in files
 - Deleting subfolders and files
 - 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

4.3.1 Understanding Share Security

- 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.
- 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)

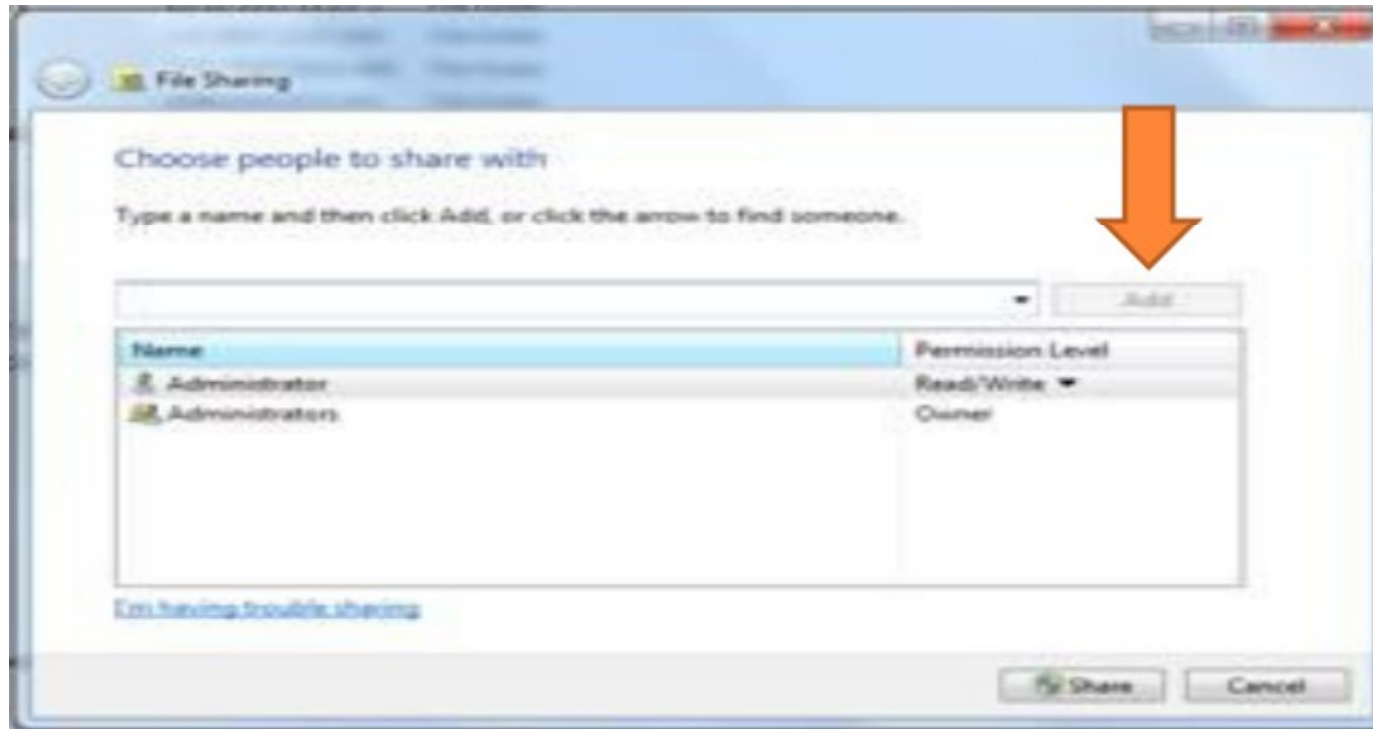
4.3.2 CREATING SHARES

- Steps to create a new share:
 - 1. Open either My computer or Windows Explorer on the server.
 - 2. Right click on folder or drive you want to share and then choose share from the pop-up menu. File sharing dialog box will appear.



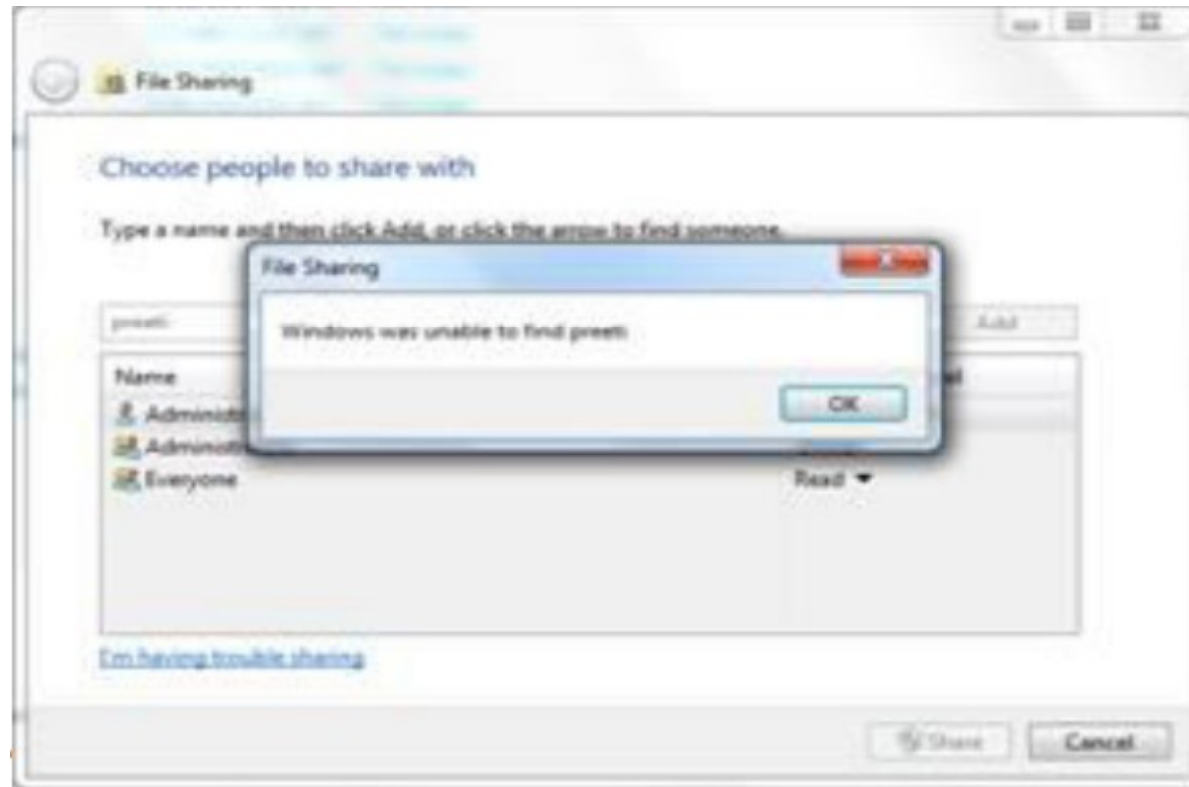
Cont..

- 3. In the field provided enter enough of a user's name (preeti) to identify that person in the system and click Add.



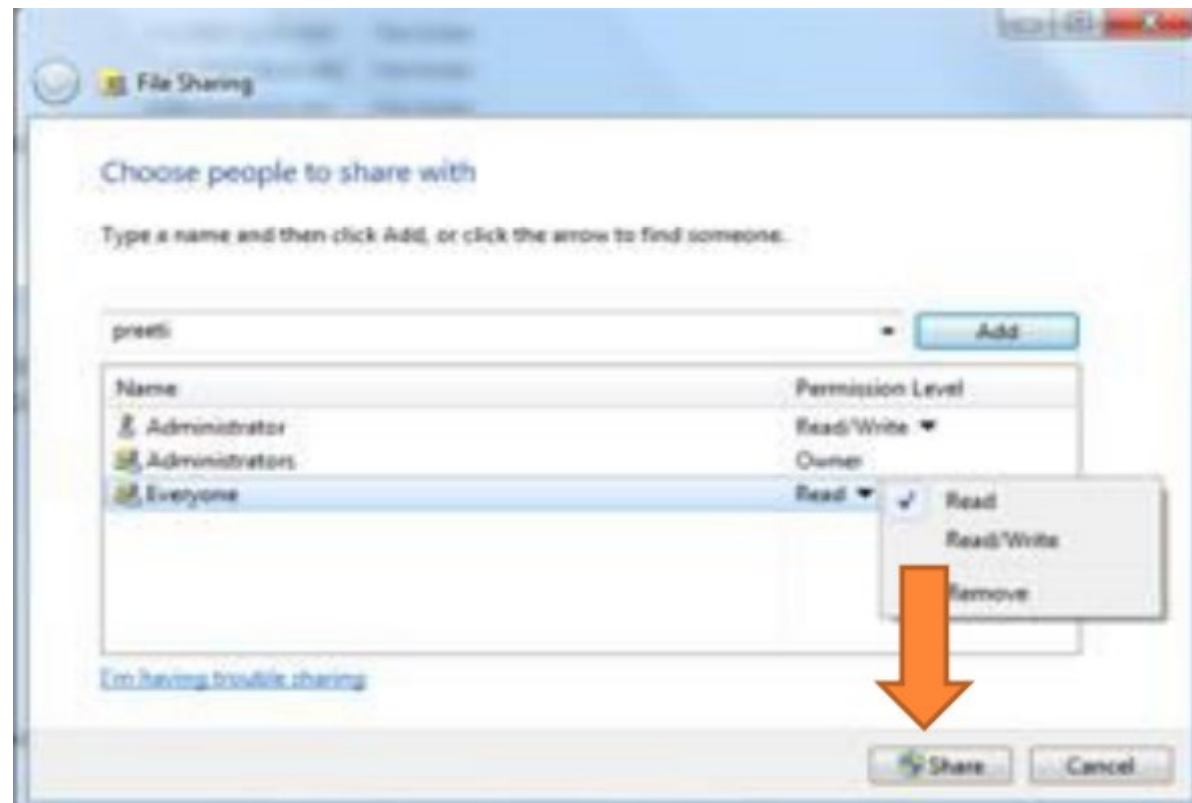
Cont...

- 4. You will get message windows was unable to find preeti, click Find



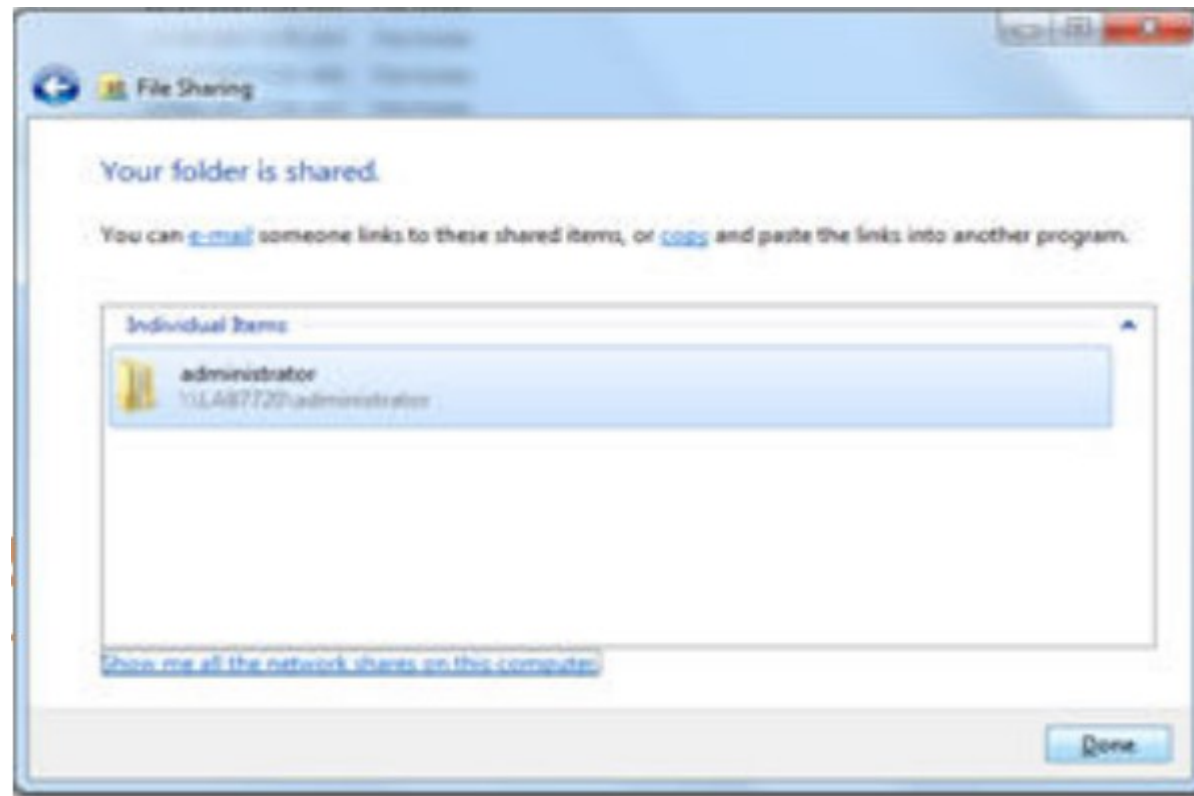
Cont...

- 5. In the textbox provided under “Enter object names to select” Write preeti (username) and click check names and then click ok.
- 6. Click the down arrow next to user’s name to set permission level. Click the share button to create the share.



Cont...

- 7. You will see a confirmatory dialog box. Click ok and share will be created. By default, share uses the folder's name as the share name. Note down the location of shared folder.

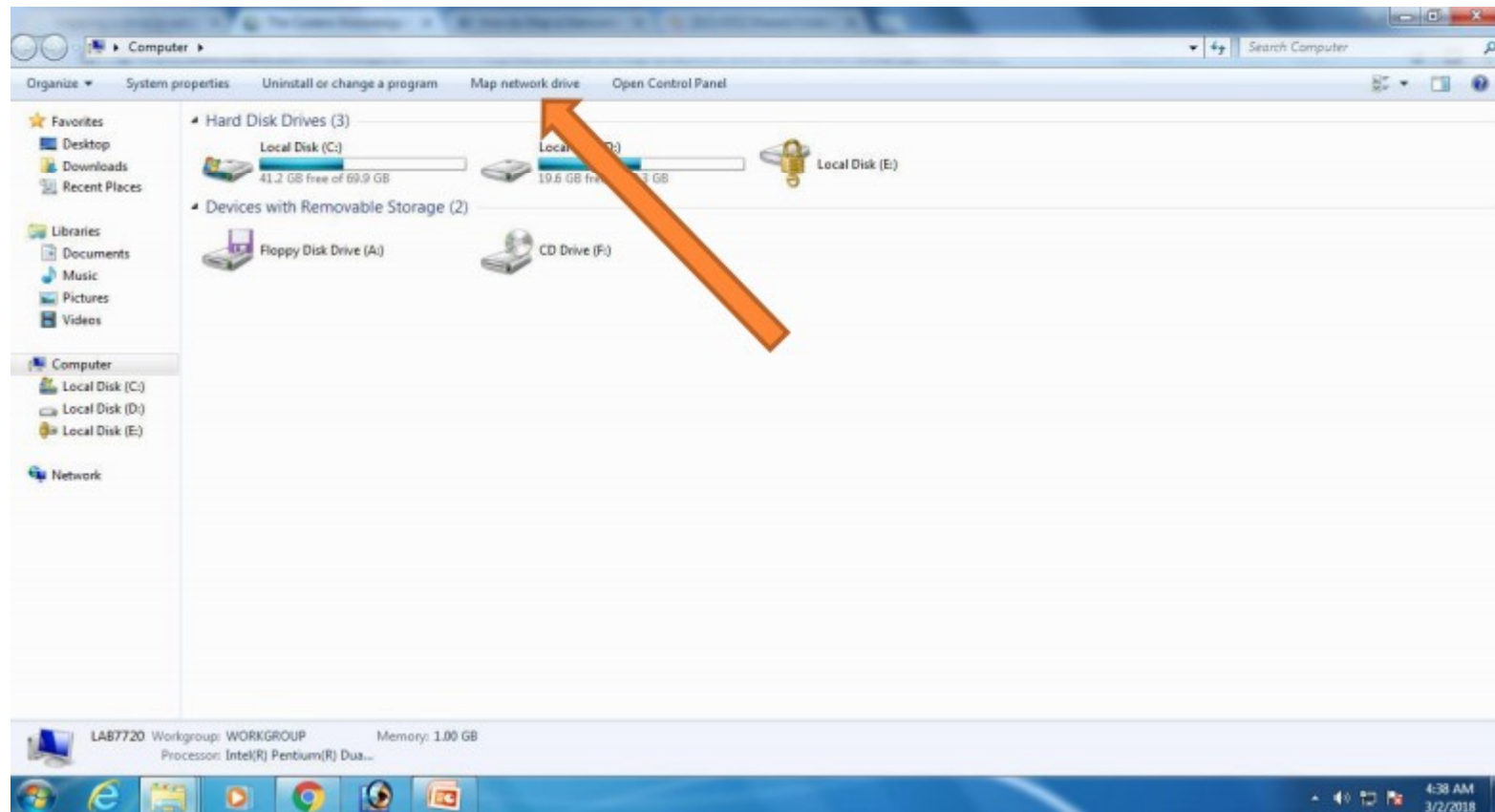


4.3.3 MAPPING DRIVES

- You can use shares by opening them in my network places and they function like the folders in my computer.
- However, you might frequently want to simulate a connected hard disk on your computer with a share from the network.
- Ex. Suppose you use network computer drive as normal drive on your computer.
- “The process of simulating a disk drive with a network share is called mapping.”
- Where you create a map between the drive letter you want to use and the actual network share to remain attached to that drive letter.

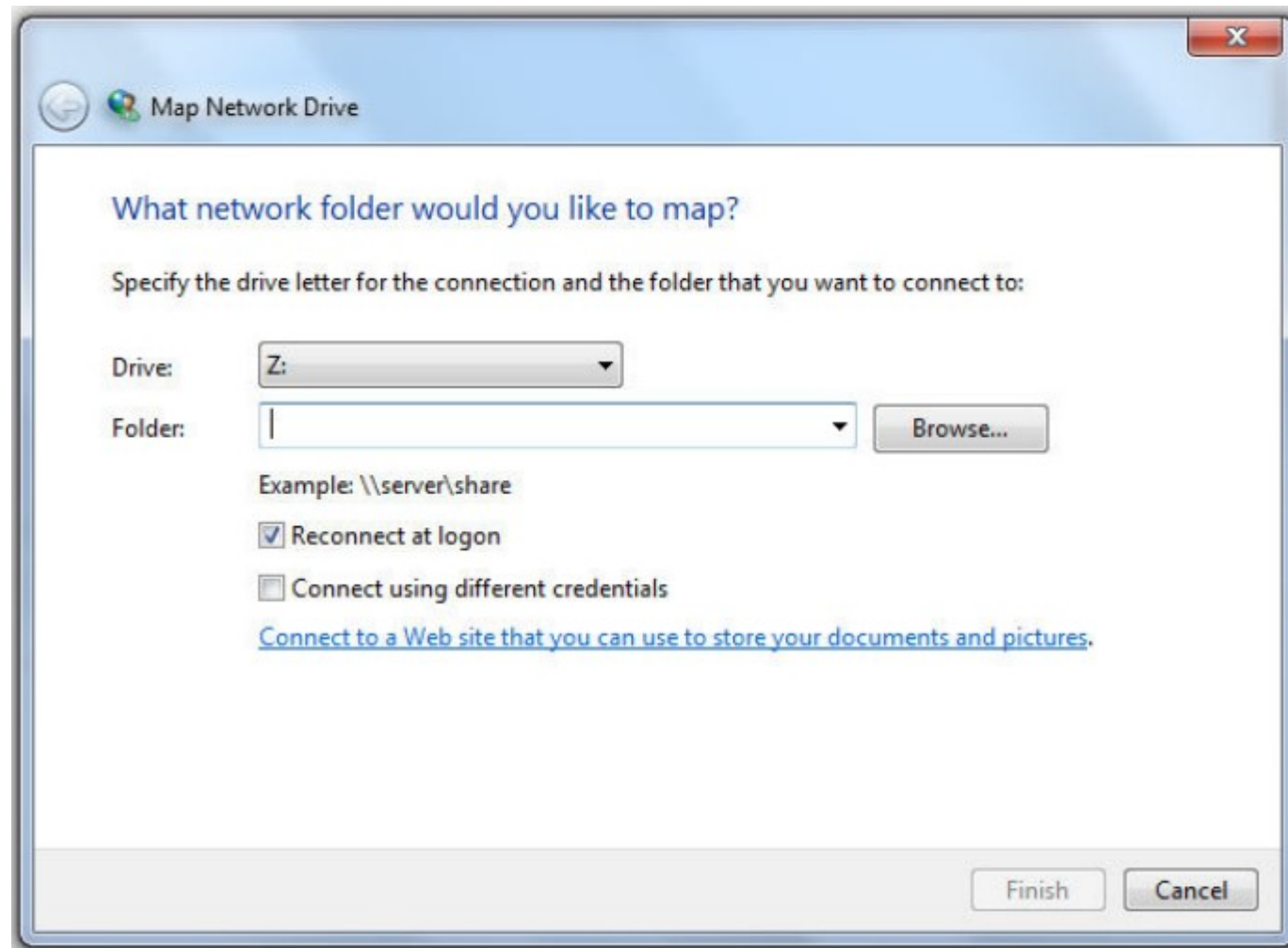
Cont...

- Steps to map a drive:
 - 1. Open network from client computer
 - 2. Locate share you want to map, right click it and choose Map Network Drive.



Cont...

- 3. Select appropriate drive for mapping and click Finish



4.4 WORKING WITH PRINTERS

- 4.4.1 UNDERSTANDING NETWORK PRINTING
 - A print job is a set of binary data sent from a network workstation to a network printer
 - A print job is the same data that a computer would send to a locally connected printer, its just redirect to the network for printing.
 - Network workstation sends the print job to the print queue is responsible for formatting the print data property for the printer. This is done by print driver installed in network workstation.
 - Printer driver are also specific to each operating system that uses them. For example, hp 1020 print driver for windows xp is different from hp 1020 print driver for windows7.



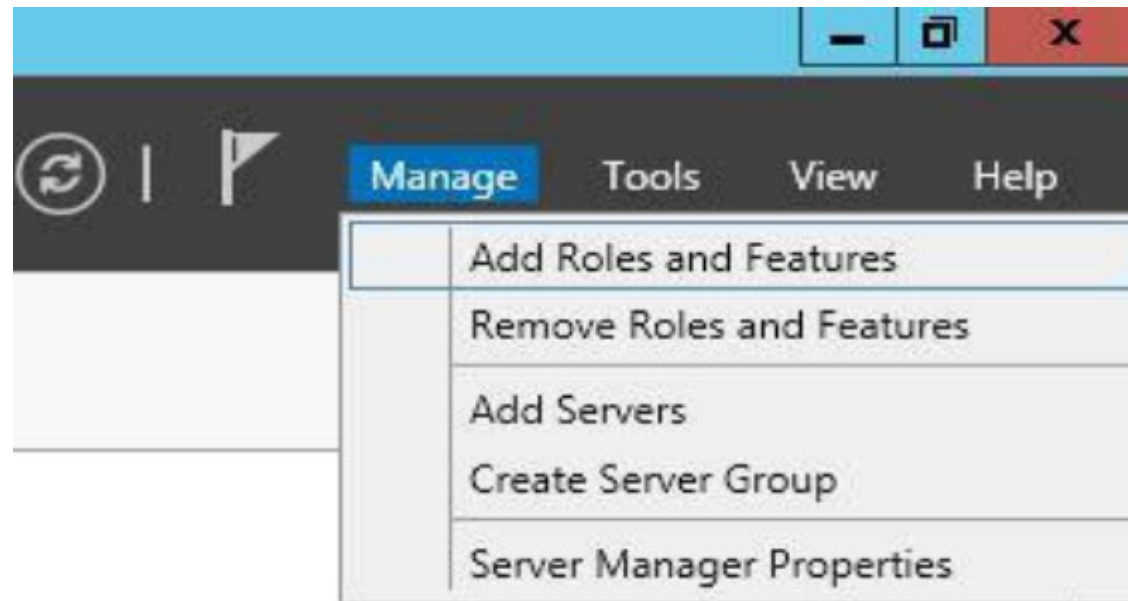
- Data to be printed goes first to the print server

4.4.2 SETTING UP NETWORK PRINTER

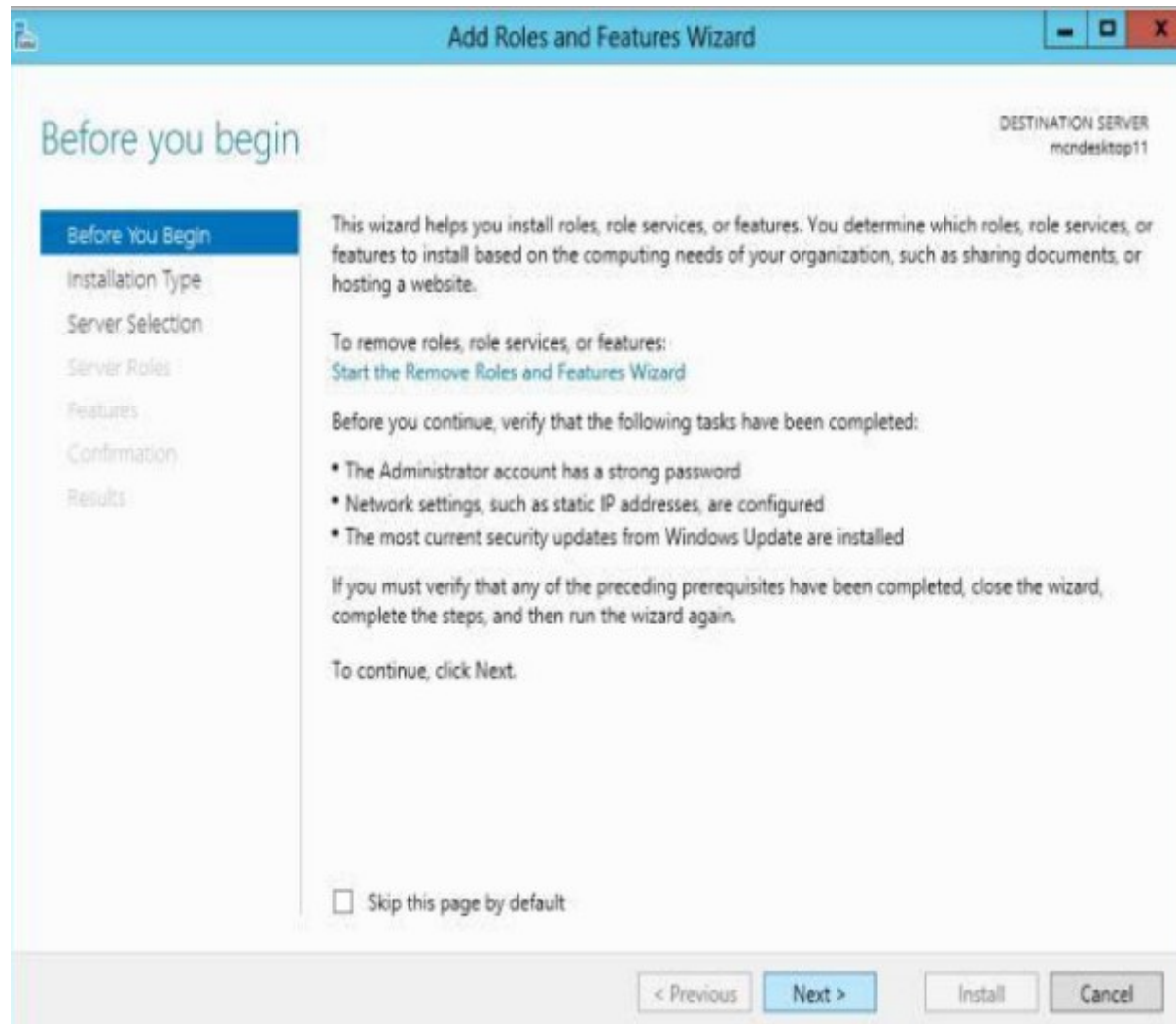
- To setup a network printer you need to install print and document services role.
- Steps to install print and document services role in windows server 2012 are as below:
- 1. Login to server 2012 as an administrator , also roles of
 - Active directory
 - DHCP server
 - DNS server must be present

CONTINUE...

- 2. Click on “Add roles and features”

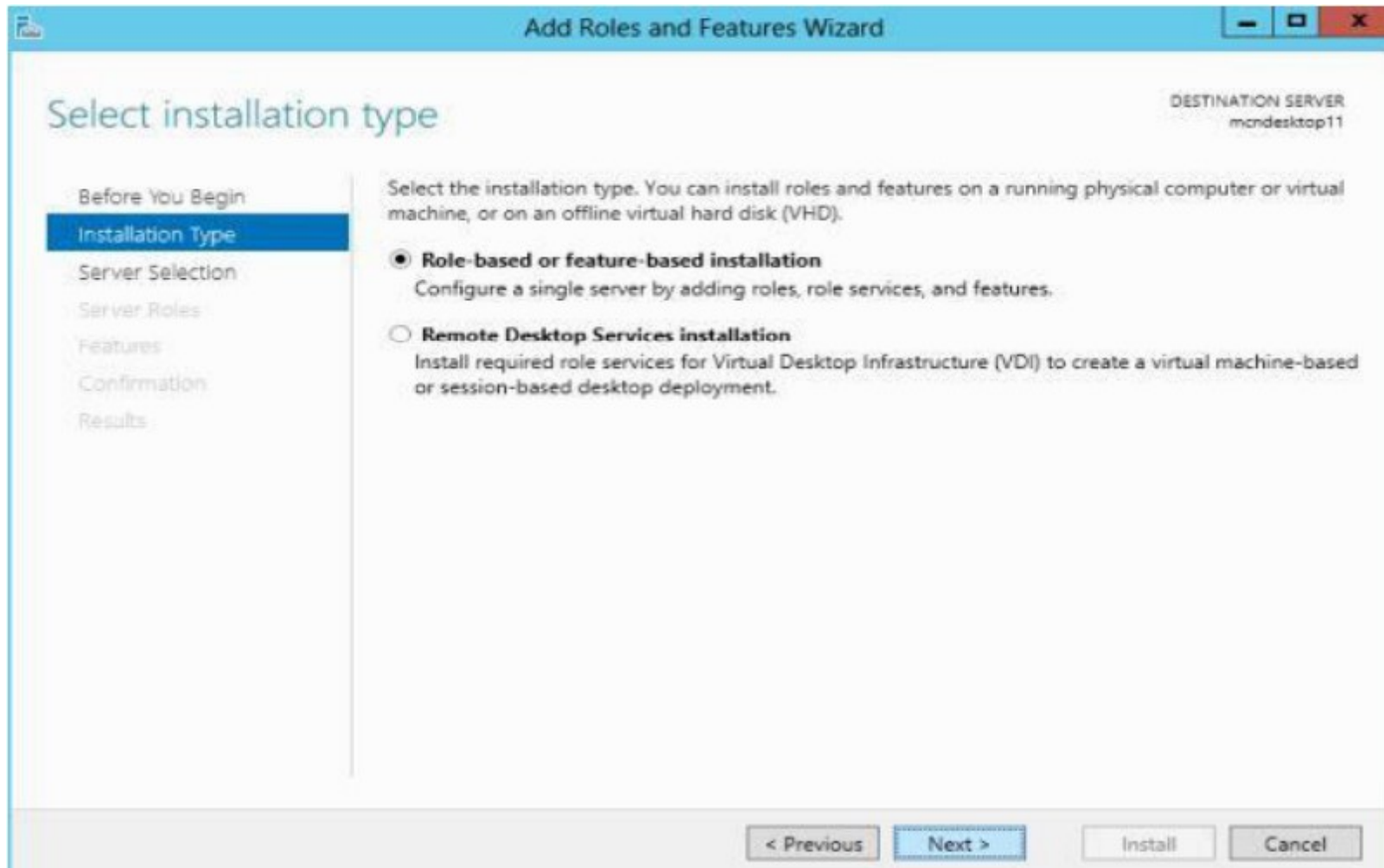


- Click Next on the “Add roles and features wizard”



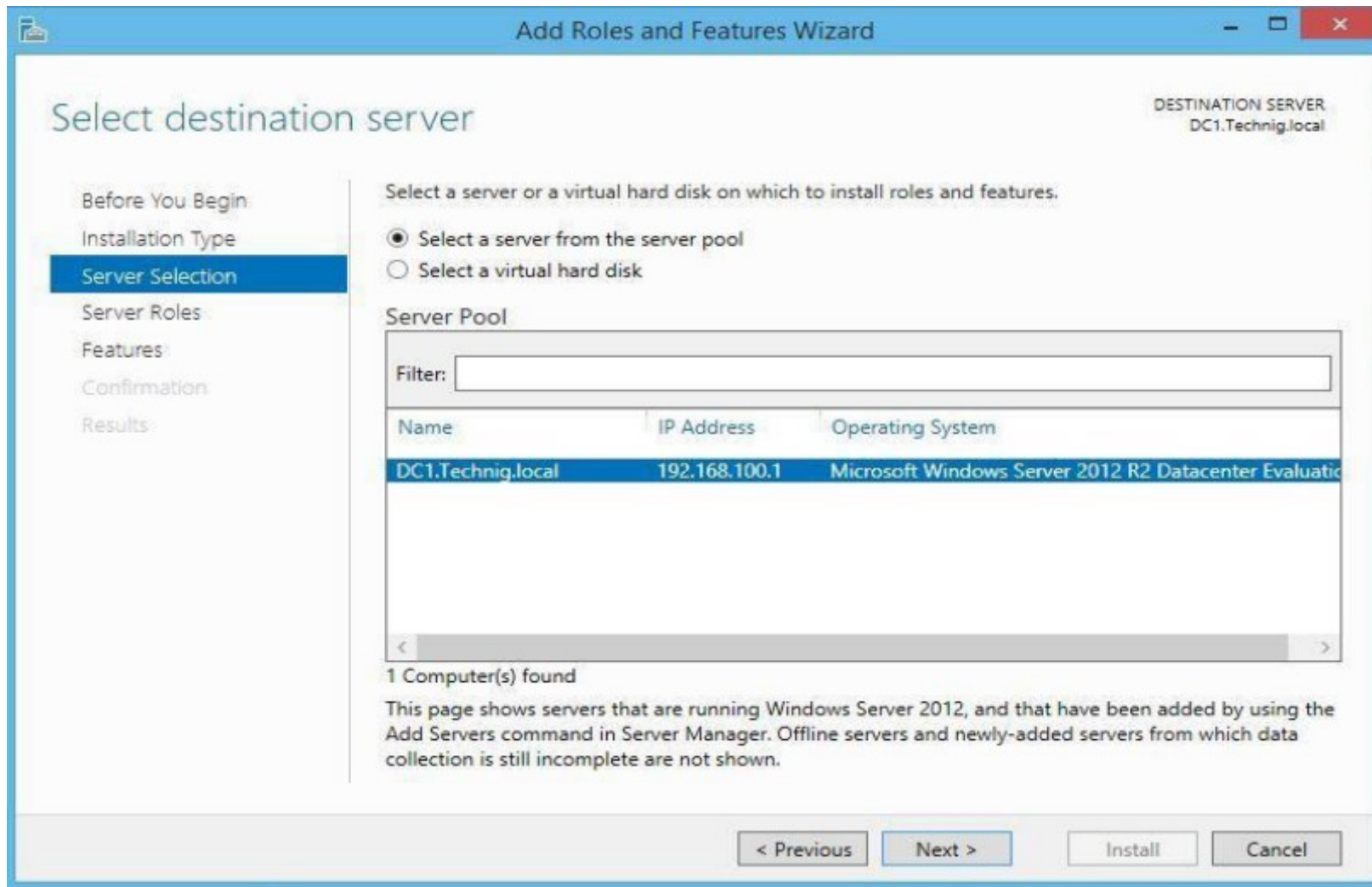
Cont..

- Make sure “Role-based or feature-based installation” option is selected.



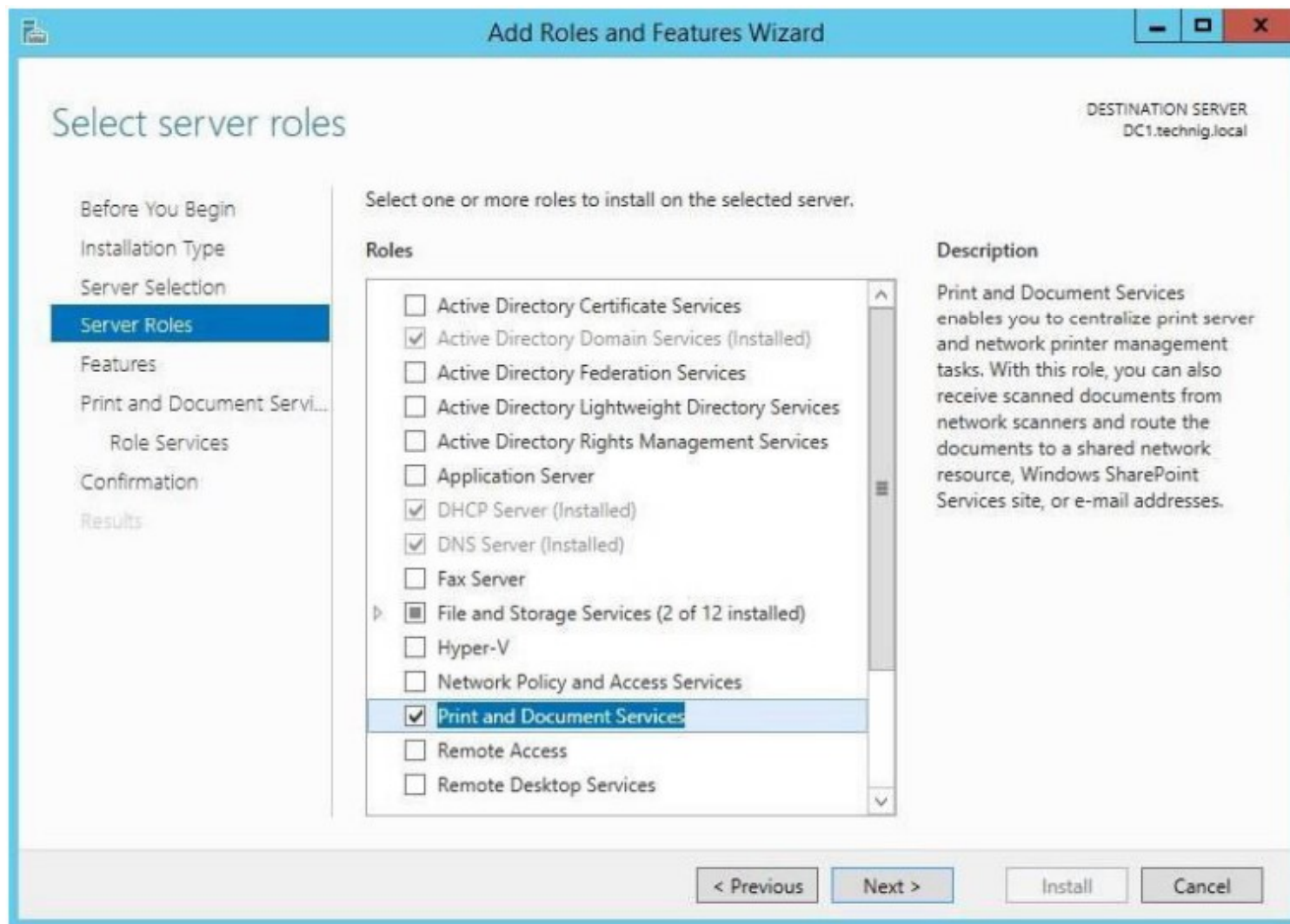
Cont...

- Select the destination server where this new role would be installed.



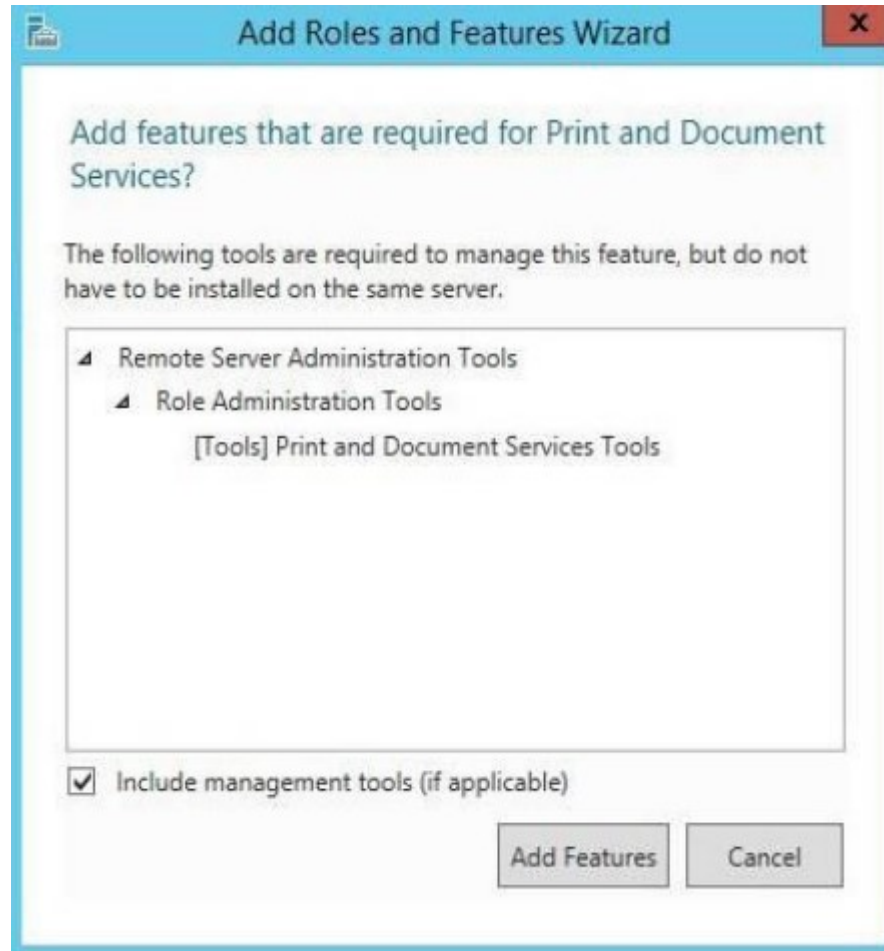
Cont..

- Select and tick the checkbox of Print and document services on the server roles page.



Cont.....

- Click Add Features On Add Roles And Features Wizard.



Cont...

- Click Next, no additional features are needed to be installed

DESTINATION SERVER
DC.yourdomain.com

Select features

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Print and Document Servi...
Role Services
Confirmation
Results

Select one or more features to install on the selected server.

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.5 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management (Installed)	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Ink and Handwriting Services	
<input type="checkbox"/> ...	

< Previous **Next >** activate Windows Install Cancel

Activate Windows
Go to System in Control Pa

Cont...

- Click Next on Print and document services role description page.

Print and Document Services

DESTINATION SERVER
DC.yourdomain.com

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Print and Document Servi...
Role Services
Confirmation
Results

Print and Document Services enables you to centralize print server and network printer management tasks. With this role, you can also receive scanned documents from network scanners and route the documents to a shared network resource, Windows SharePoint Services site, or e-mail addresses.

Things to Note

- Windows Server 2012 supports print queues using either Type 3 or Type 4 printer drivers.
- Microsoft recommends using Type 4 printer drivers where possible. With Type 4 printer drivers users who are not members of the local administrators group can connect to the printer by default and users on 32-bit clients can connect without a 32-bit driver on the print server.
- To enable clients to connect to shared print queues supported using Type 3 printer drivers on the print server, you should use signed, package aware drivers. If signed or package aware drivers are unavailable, client users must either be local administrators or you must have already set the "Computer\Administrative Templates\Printers\Point and Print Restrictions" group policy to configure security prompts.
- If you are using Type 3 printer drivers and have any 32-bit clients, you must install the matching 32-bit version of the printer driver on the print server. If you do not install the 32-bit drivers, clients may not be able to successfully connect to the printer.

[Learn more about the Printer Server Role](#)

Activate Windows
Go to System in Control Pa
activate Windows
Install Cancel

< Previous Next >

Cont....

- Select the Print server on Role services page

DESTINATION SERVER
DC.yourdomain.com

Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Print and Document Servi...
Role Services
Confirmation
Results

Select the role services to install for Print and Document Services

Role services	Description
<input checked="" type="checkbox"/> Print Server	Print Server includes the Print Management snap-in, which is used for managing multiple printers or print servers and migrating printers to and from other Windows print servers.
<input type="checkbox"/> Distributed Scan Server	
<input type="checkbox"/> Internet Printing	
<input type="checkbox"/> LPD Service	

< Previous **Next >** Install Cancel

Activate Windows
Go to System in Control Panel to activate Windows.

Cont..

- Confirm installation and click install

DESTINATION SERVER
DC.yourdomain.com

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Print and Document Servi...
Role Services
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Print and Document Services
Print Server

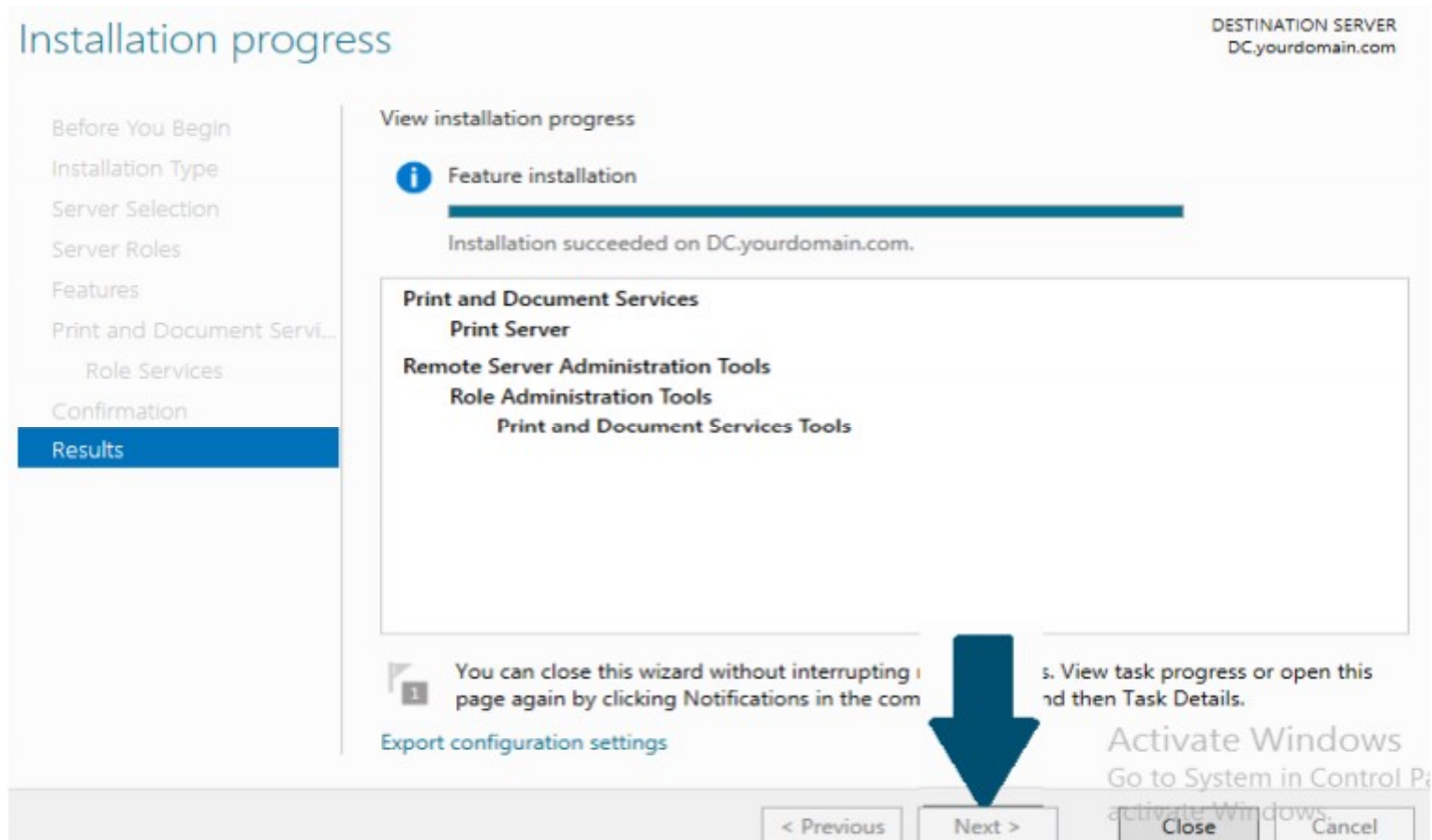
Remote Server Administration Tools
Role Administration Tools
Print and Document Services Tools

Export configuration settings
Specify an alternate source path

< Previous Next > **Install** Cancel

Cont..

- Installation Progress page appears as below



Click Close after installation succeeds

4.5 WORKING WITH WINDOWS BACKUP

- One task is more for a network administrator is making regular and reliable back for data on the system.
- You can use windows server backup to back up a full server, selected volumes, the system state, or specific files or folder.
- You can use windows server backup to create and manage backups for the local computer or a remote computer. And, you can schedule backups to run automatically.

Different types of backup.

- Full backup : Backs up and marks selected files, whether or not they have changed since the last backup.
- Copy backups : Back up all selected files without marking them as being backed up.
- Incremental backups: Back up and mark selected files only if they have changed since the last time they were backed up.
- Daily copy: Back up only those files that have been modified that day, without marking them as being backed up.
- Differential backup: Back up selected files only if they have changed since last time they were backed up, without marking them as being backed up.

ADVANTAGES OF WINDOWS BACKUP SERVER

- Faster backup technology
- Improved scheduling
- Simplified recovery of your OS
- Remote administration
- Ability to recover application
- Support for optical or removable media drives

4.6 USING WINDOWS SERVERS BACKUP SOFTWARE

- Click Start, click Server Manager.
- Click Features-> Add features.
- On the Select Features page, expand Window Server Backup Features, and then select checkboxes for Window Server Backup and Command-line Tools.
- Click Add Required Features and then click Next.
- On the Confirm Installation Selections page, review the choices that you made, and then click Install.
- If any error occurs the it will be noted on the Installation Results page.