Ex.No 1 **Installing and updating Windows Server 2012**

Aim

To install and update Windows Server 2012.

Components Required

1.PC

2.Window Server 2012 R2 Software

Windows Server is a server operating system that enables a computer to handle network roles such as print server, domain controller, web server, and file server. As a server operating system, it is also the platform for separately acquired server applications such as Exchange Server or SQL Server. Windows Server 2012 is the fifth version of the Windows Server operating system by Microsoft, as part of the Windows NT family of operating systems.

PROCEDURE FOR INSTALLATION:-

STEP-1: Turn on the PC, insert appropriate windows server 2012 installation media into DVD drive

STEP-2: Reboot the system, press F2(or) Delete key to enter into BIOS setup. The BIOS screen appears, enter into the Boot sequence----> Change the boot priority ------> first bootable device----> DVD Drive. Save changes and press enter to reboot.

STEP-3: The window appears as shown in the figure 1.1 which is loading windows files.

FIG 1.1 - LOADING WINDOWS FILES

STEP-4: The Install windows setup opens, Select the Language to install – English Time and currency Format – English (United states)Keyboard (or) input method – US and click next to continue as shown in the figure 1.2

FIG 1.2 – SELECTING LANGUAGE TO INSTALL

STEP-5: In the next window, press Install to begin the installation process as shown in the figure 1.3

FIG 1.3 – SELECTING INSTALL OPTION

STEP-6: The type the product key for activation appears select skip product key option

STEP-7: The next window is to select the edition of windows to be installed. Select Windows server 2008 Enterprise (Full installation) as shown in the figure 1.4

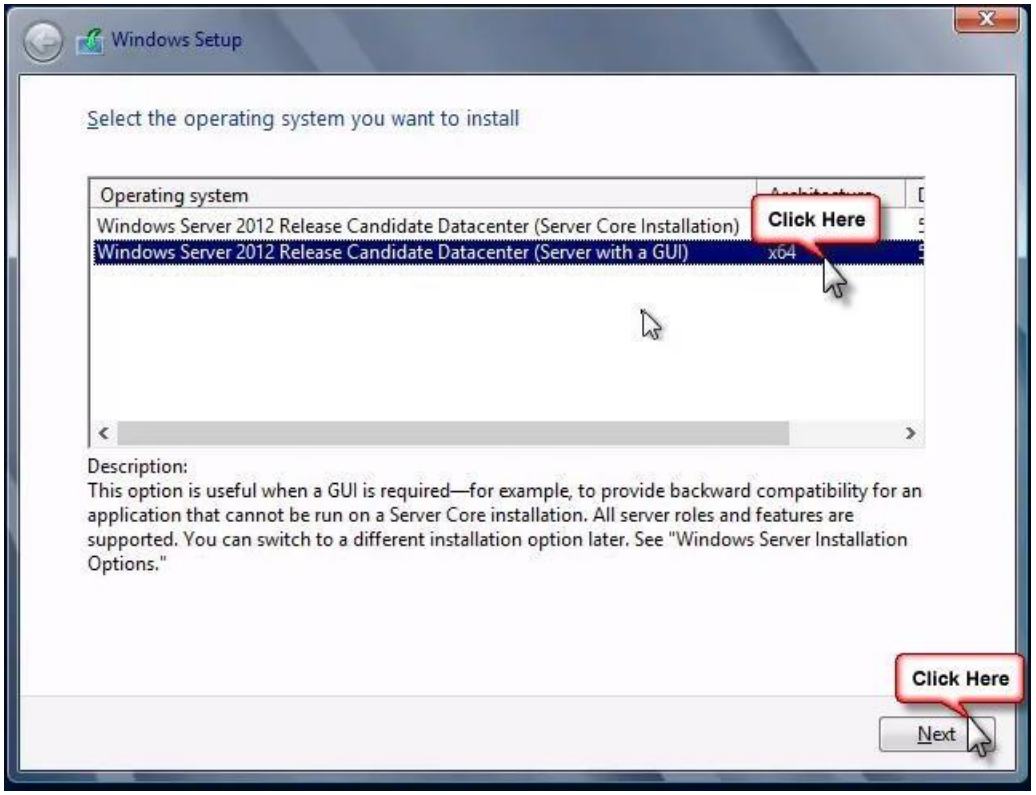


FIG 1.4 – SELECTING OPERATING SYSTEM TO INSTALL

STEP-8: In the License terms windows, select I accept the license terms as shown in the figure 1.5

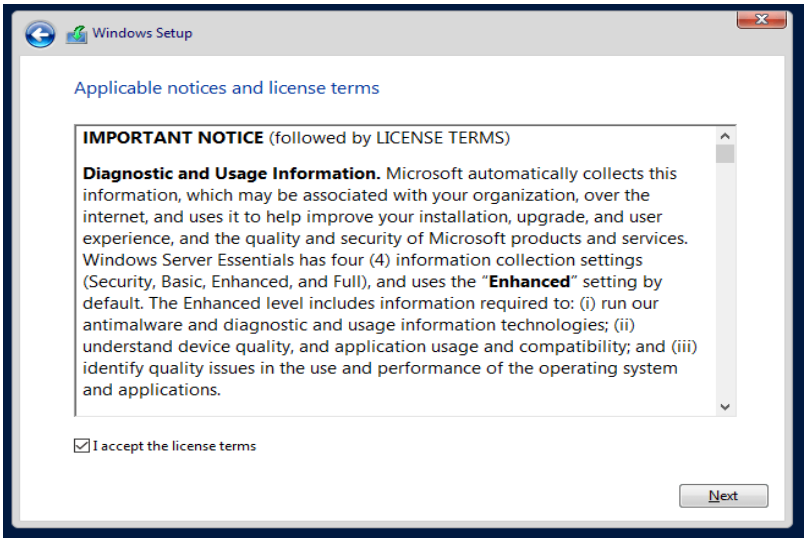


FIG 1.5 – ACCEPTING LICENSE AGREEMENT

STEP-9:

The next window is to select the installation type. Click on custom (advanced) option as shown in the figure 1.6

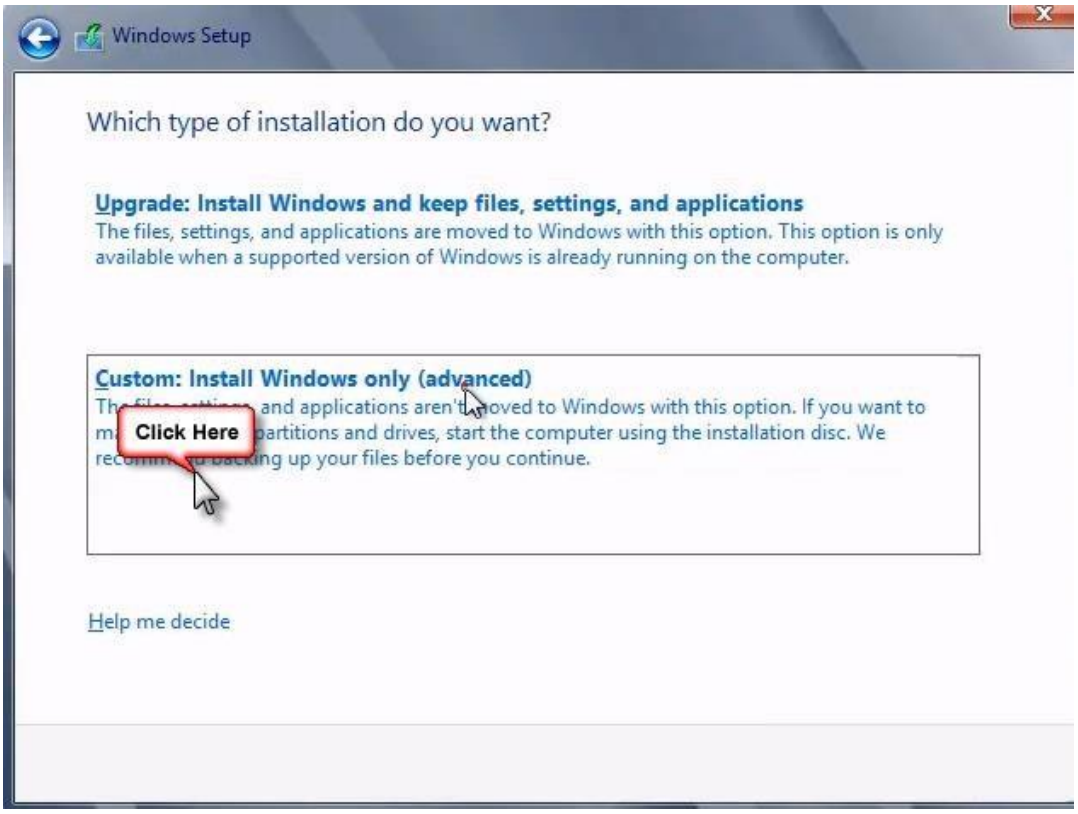


FIG 1.6 – SELECTING TYPE OF

INSTALLATION PROCEDURE FOR PARTITIONING:-

STEP-10: The window where the user want to install windows appears click on the unallocated space---

> select new from a list of unallocated disk spaces select anyone as shown in the figure 1.7

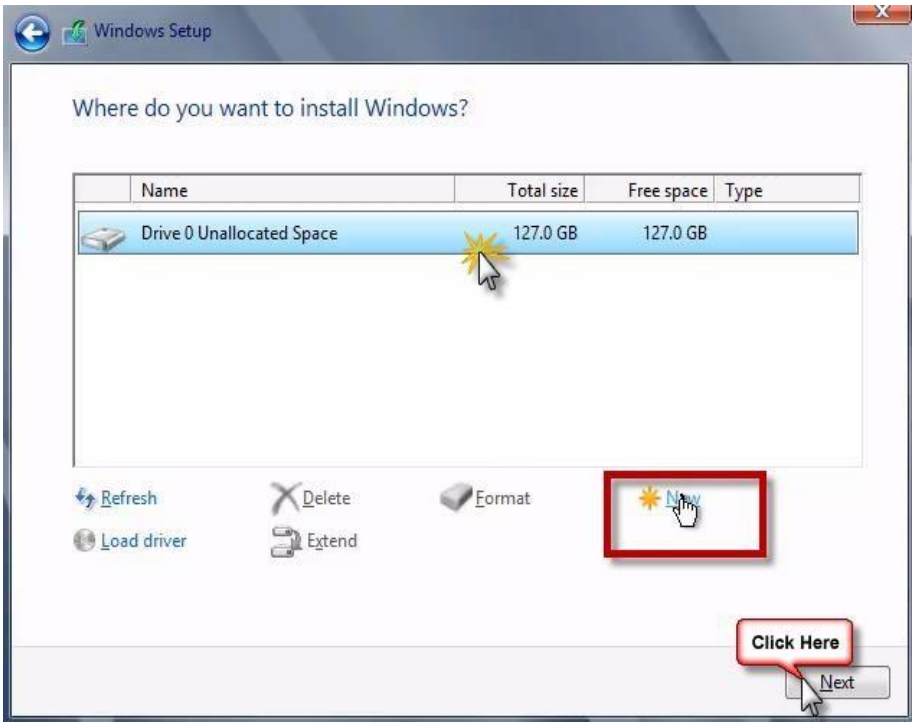


FIG 1.7 – SELECTING DISK SPACE TO INSTALL

STEP-11: The installing windows appears as shown in the figure 1.8

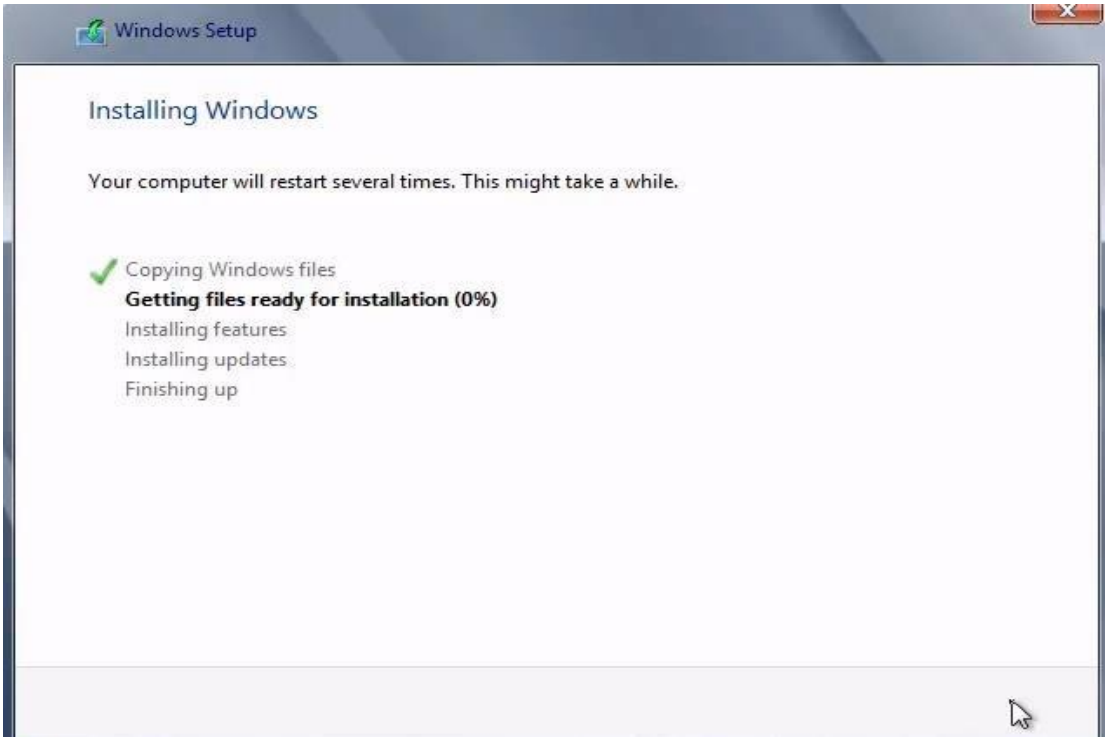


FIG 1.8 – INSTALLING WINDOWS

STEP-12: After installing and partitioning the system reboots. Press Ctrl+alt+delete to login as shown in the figure 1.10

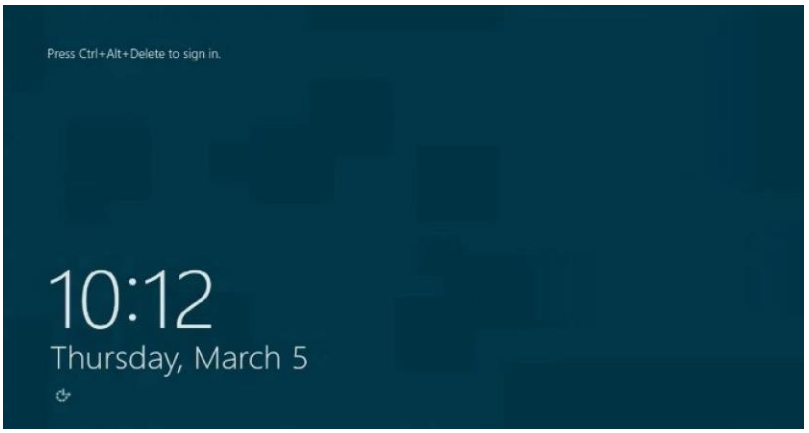


FIG 1.10 – PRESSING CTRL+ALT+DEL

STEP-13: In the next window type the

User name –

administrator

Password -

Confirm password –

Which should be a combination of capital, small, numeric and special characters is typed as shown in the figure 1.11

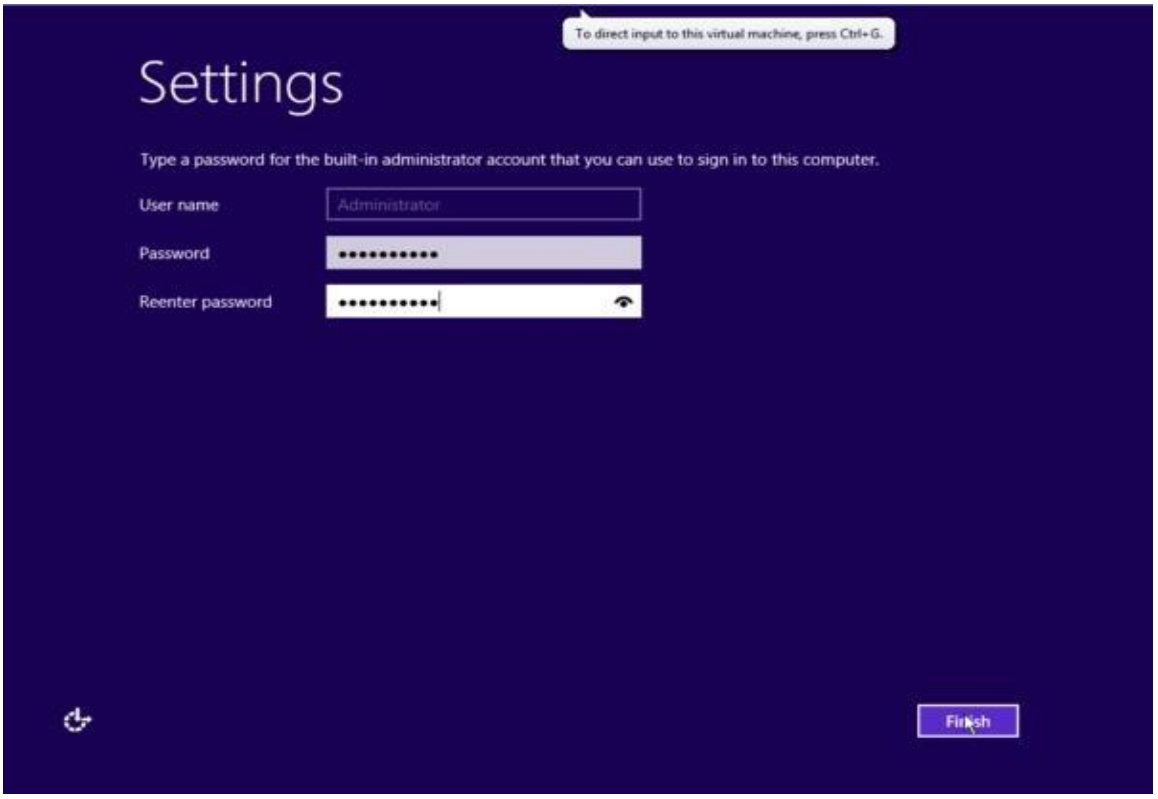
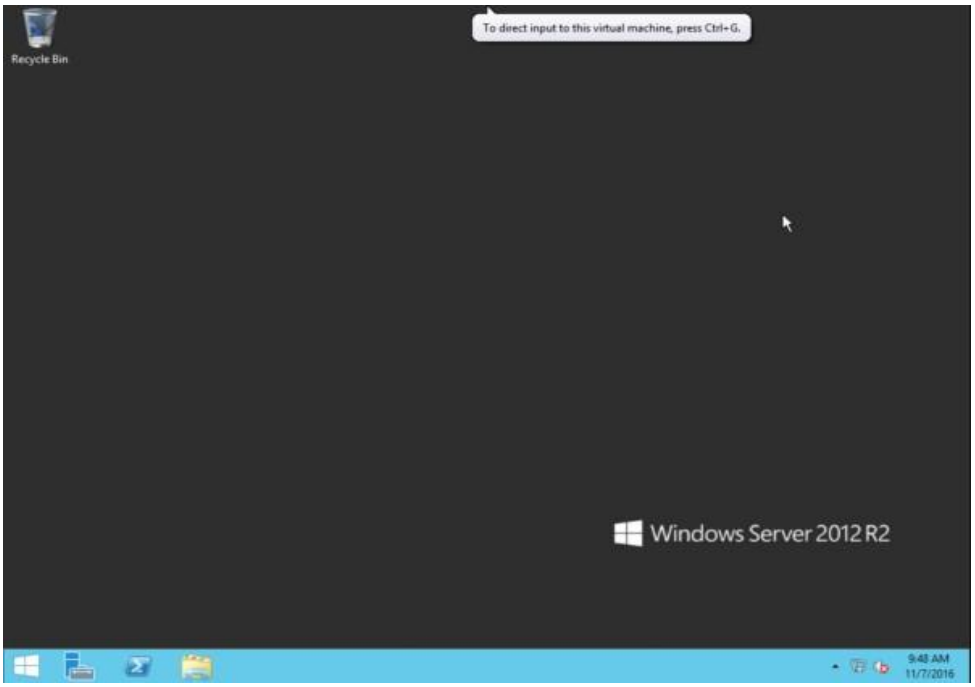


FIG 1.11 – SETTING PASSWORD

PROCEDURE FOR CONFIGURING:-

STEP-16: The windows server 2012 desktop screen appears with the server manager window launching automatically where the server can be configured.



RESULT:-

Thus we have installed and configured windows 2012 R2.

Ex.No 2 Setting up a Virtual network and transfer files between virtual machines

Aim

To setup virtual network and transfer files between virtual machines.

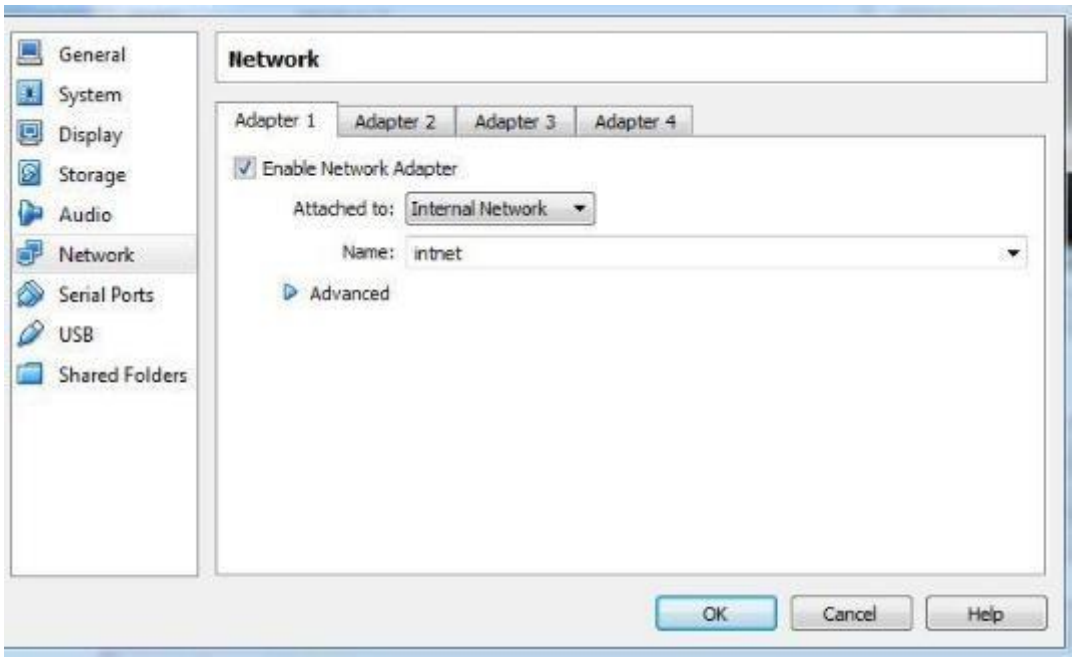
Components Required

1. PC
2. Oracle Virtualbox with Server and any OS.

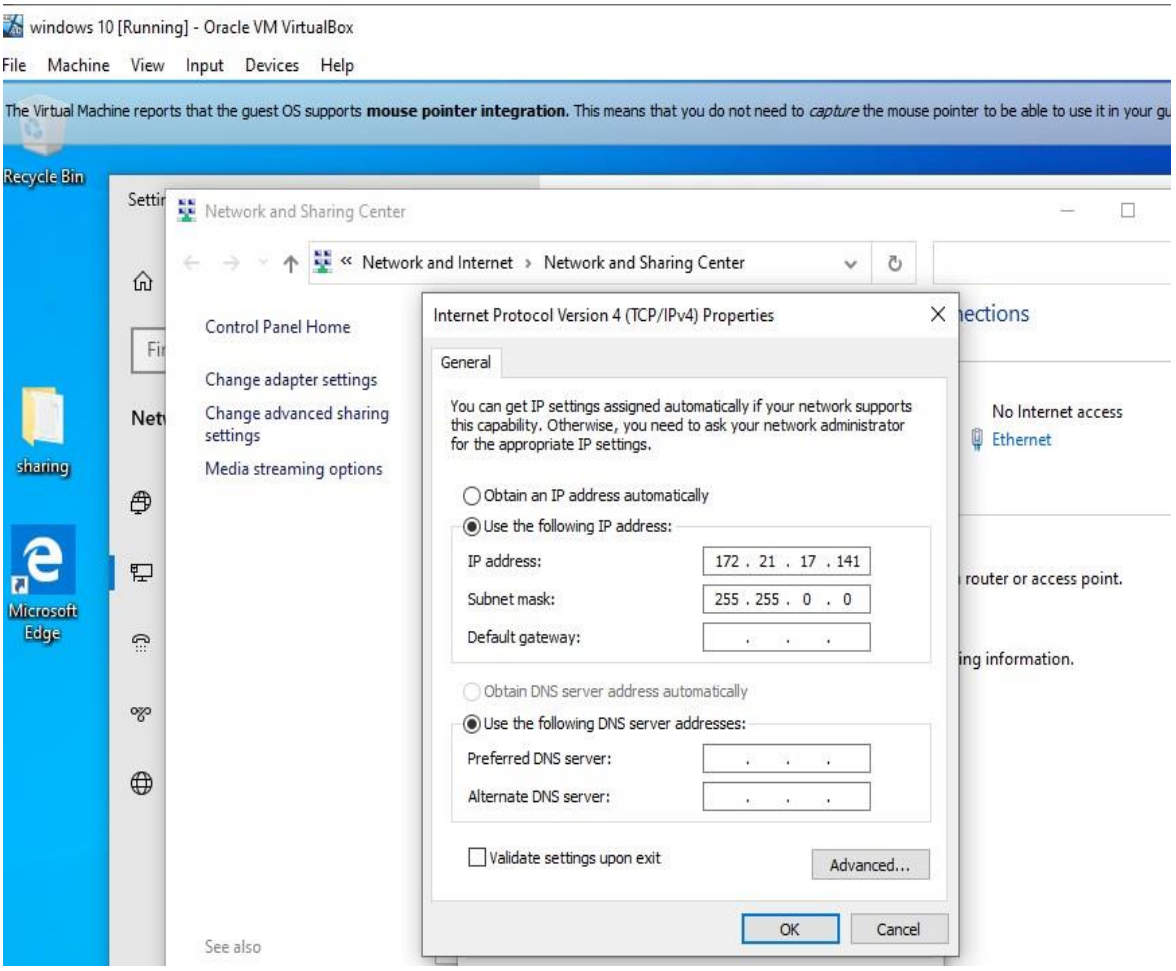
Setting up Virtual network

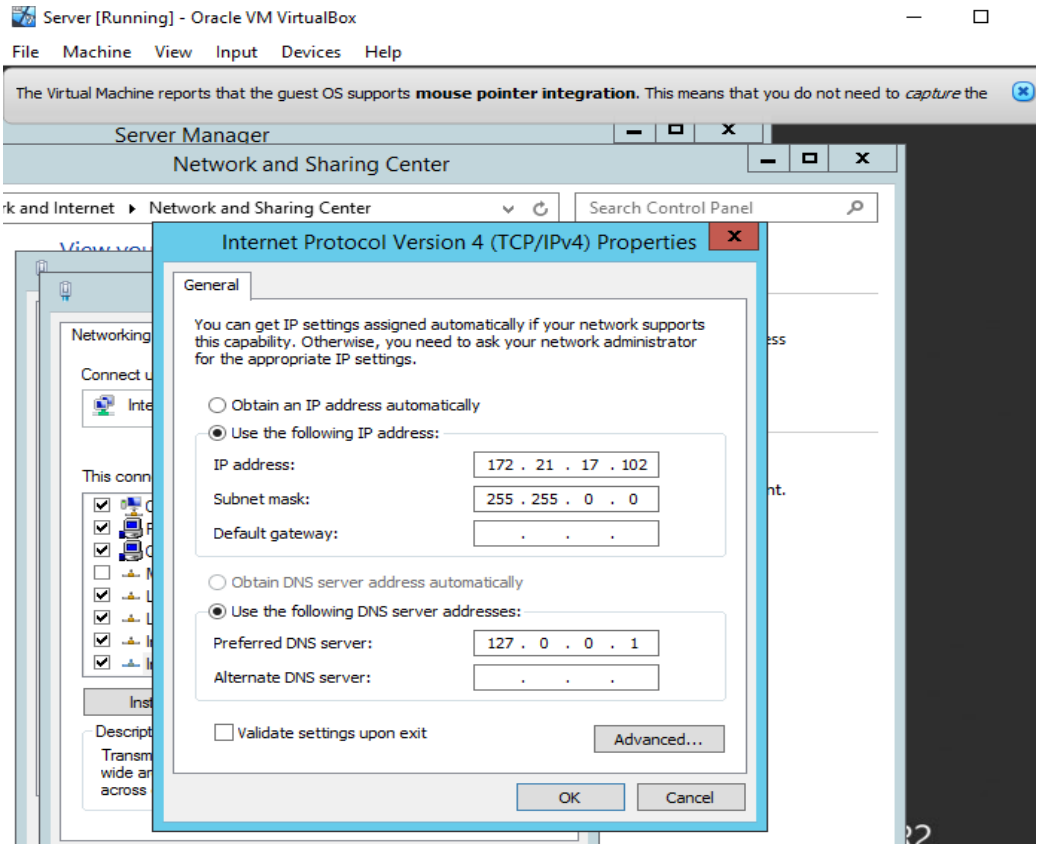
1. Go to Machines ----> Click settings

2. Select Network----> Enable Network Adapter -->Select Internal Network and Select Allow All.

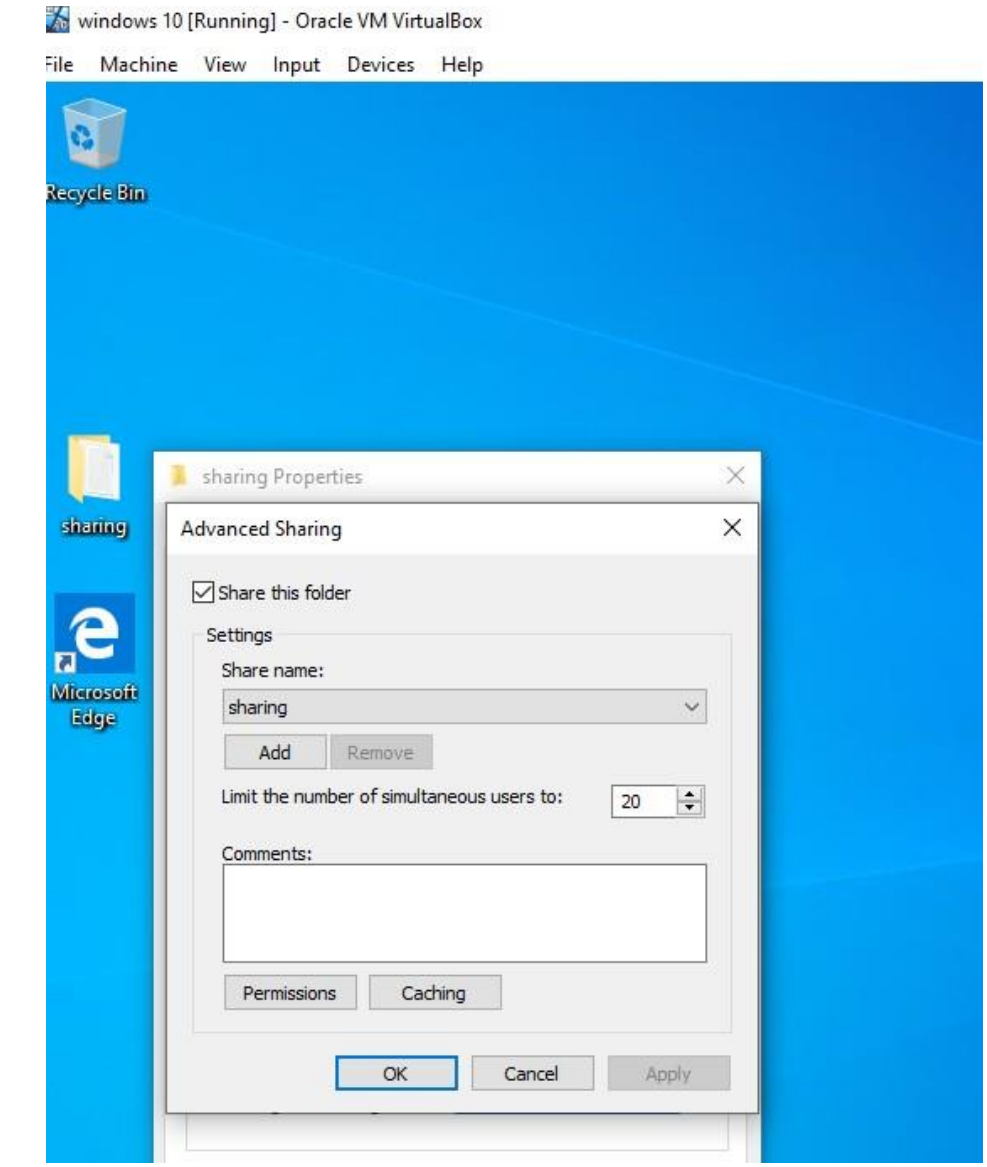


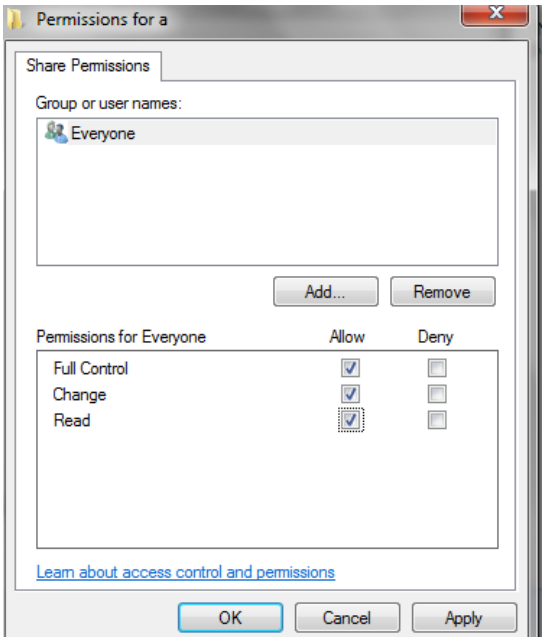
Setting up IP Address for both server and Windows 10

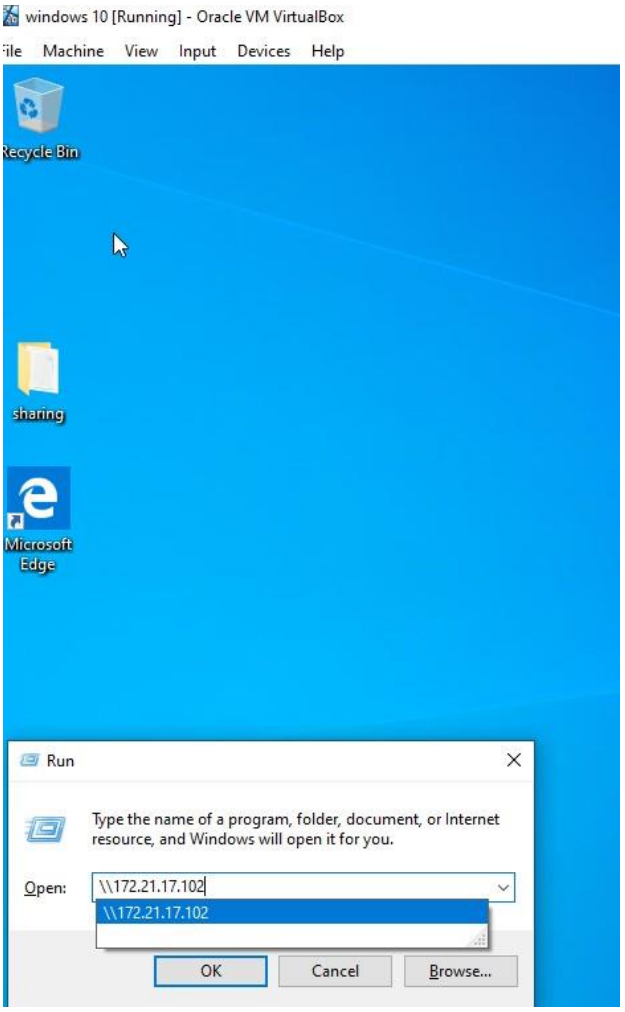


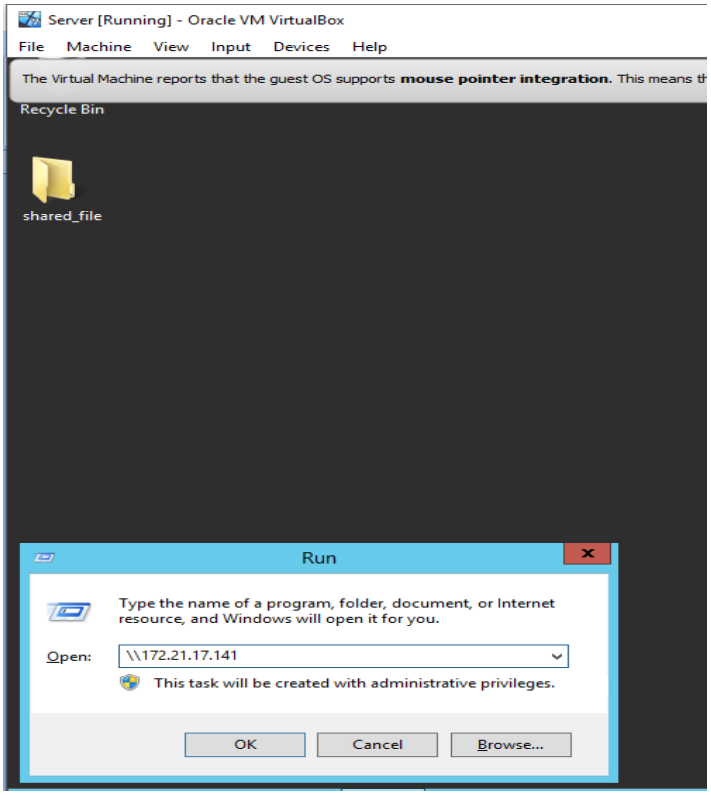


Sharing the folder

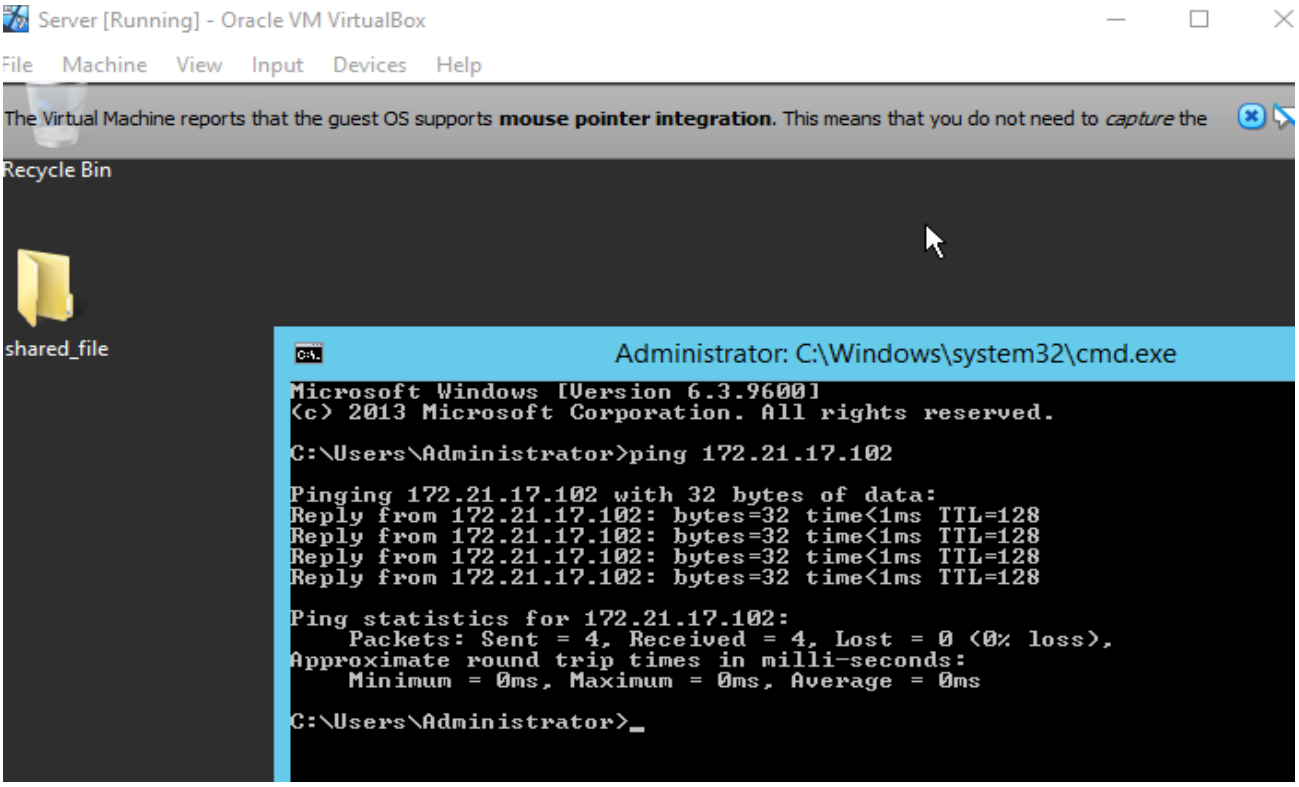

windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
sharing
Microsoft Edge
sharing Properties
Advanced Sharing
Share this folder
Settings
Share name:
sharing
Add
Remove
Limit the number of simultaneous users to:
20
Comments:
Permissions
Caching
OK
Cancel
Apply

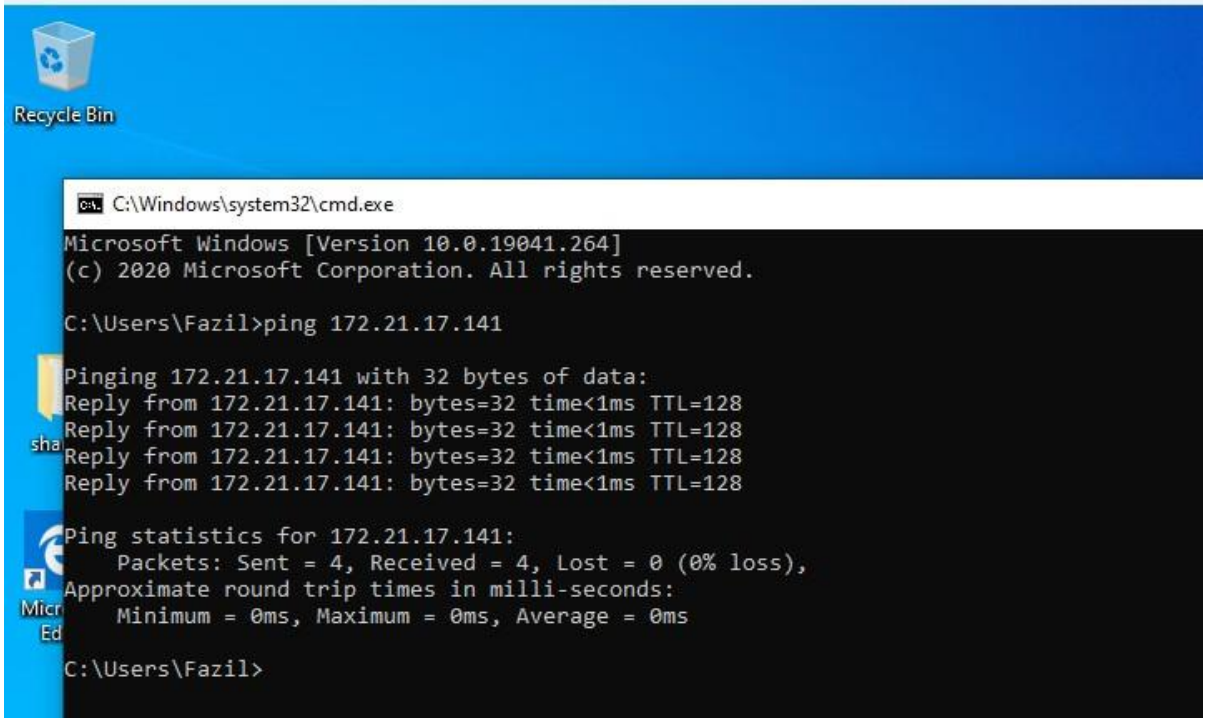

Permissions for a
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
Learn about access control and permissions
OK
Cancel
Apply

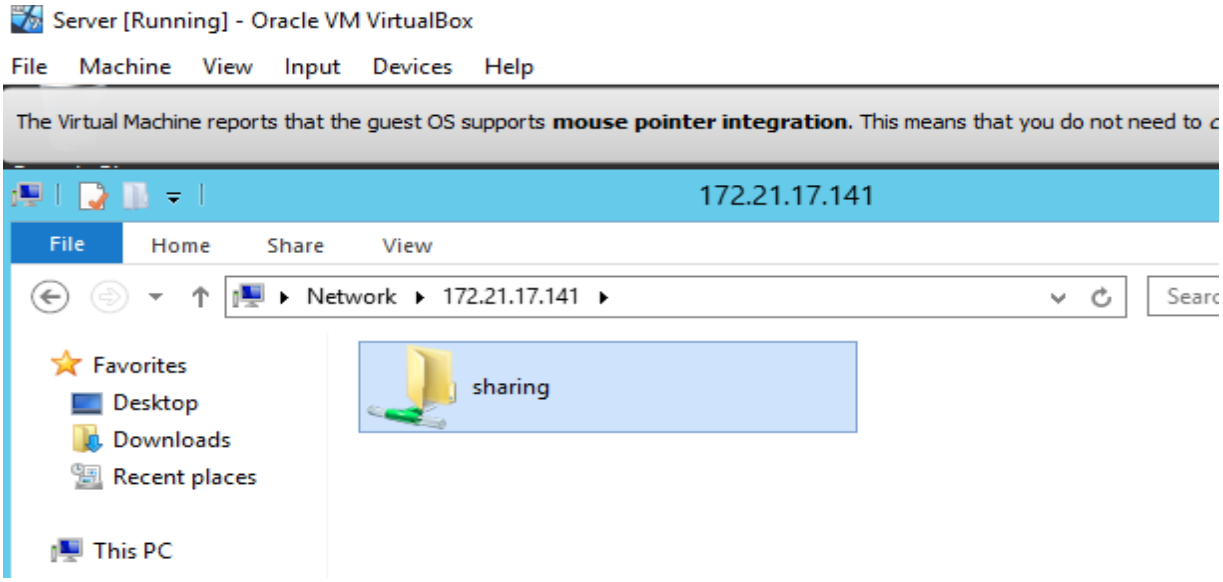


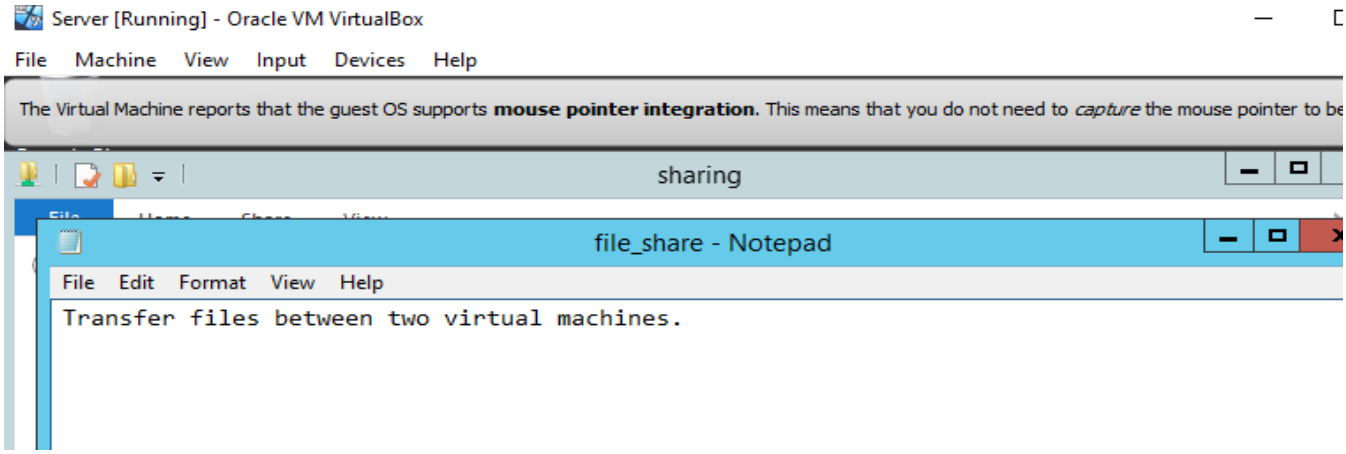


Test using ping command


Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the
Recycle Bin
shared_file
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 172.21.17.102
Pinging 172.21.17.102 with 32 bytes of data:
Reply from 172.21.17.102: bytes=32 time<1ms TTL=128
Reply from 172.21.17.102: bytes=32 time<1ms TTL=128
Reply from 172.21.17.102: bytes=32 time<1ms TTL=128
Reply from 172.21.17.102: bytes=32 time<1ms TTL=128
Ping statistics for 172.21.17.102:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Administrator>


Recycle Bin
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\Fazil>ping 172.21.17.141
Pinging 172.21.17.141 with 32 bytes of data:
Reply from 172.21.17.141: bytes=32 time<1ms TTL=128
Reply from 172.21.17.141: bytes=32 time<1ms TTL=128
Reply from 172.21.17.141: bytes=32 time<1ms TTL=128
Reply from 172.21.17.141: bytes=32 time<1ms TTL=128
Ping statistics for 172.21.17.141:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Fazil>





RESULT:
Thus,we have setting up virtual network and transfer files between virtual machines.

Ex.No 3 **Create and manage Windows Domain and Domain Controller**

Aim

To Create and manage Windows Domain and Domain Controller.

Components Required

1.PC

2.Window Server Software

Domain

A **domain** is defined as a logical group of network objects (computers, users, devices) that share the same **Active Directory** database.

A **Windows domain** is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers. Authentication takes place on domain controllers. Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain.

Domain controller

A **domain controller** is a server that responds to authentication requests and verifies users on computer networks. Domains are a hierarchical way of organizing users and computers that work together on the same network. The **domain controller** keeps all of that data organized and secured.

Step 1: Install Active Directory Domain Services (ADDS)

Log into Windows Server 2019 with administrative credentials. Open **Server Manager** → click on **Dashboard** → click on **Add roles and features**.

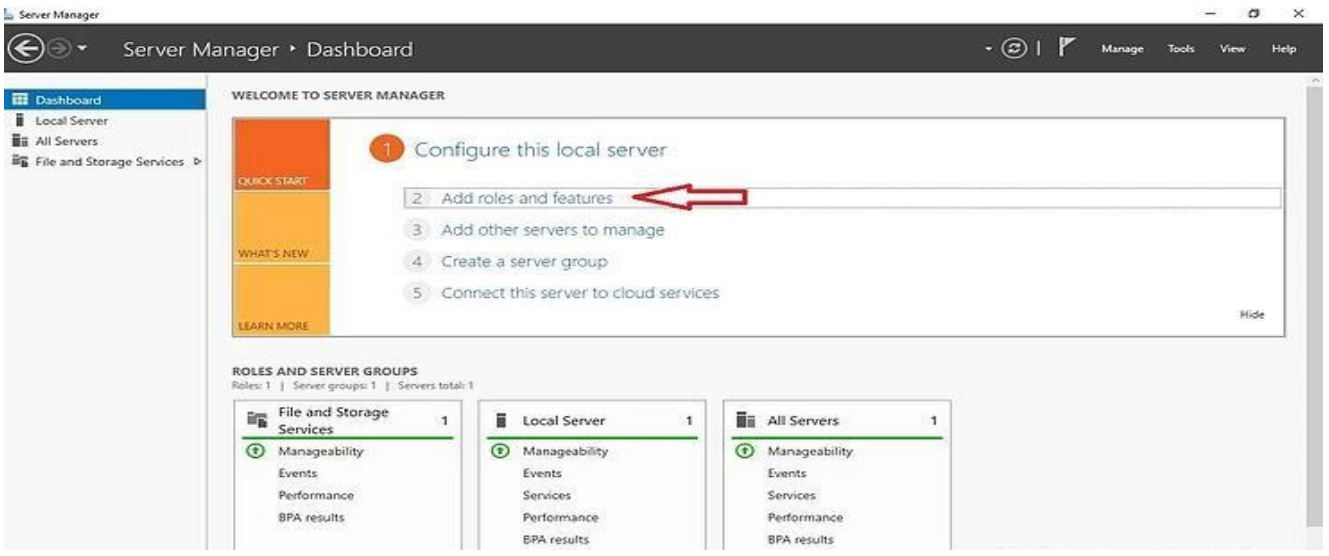


FIG 3.1 ADD ROLES AND FEATURES

The "**Before you begin**" tab contains some important information. Please go through it and click "**Next**".

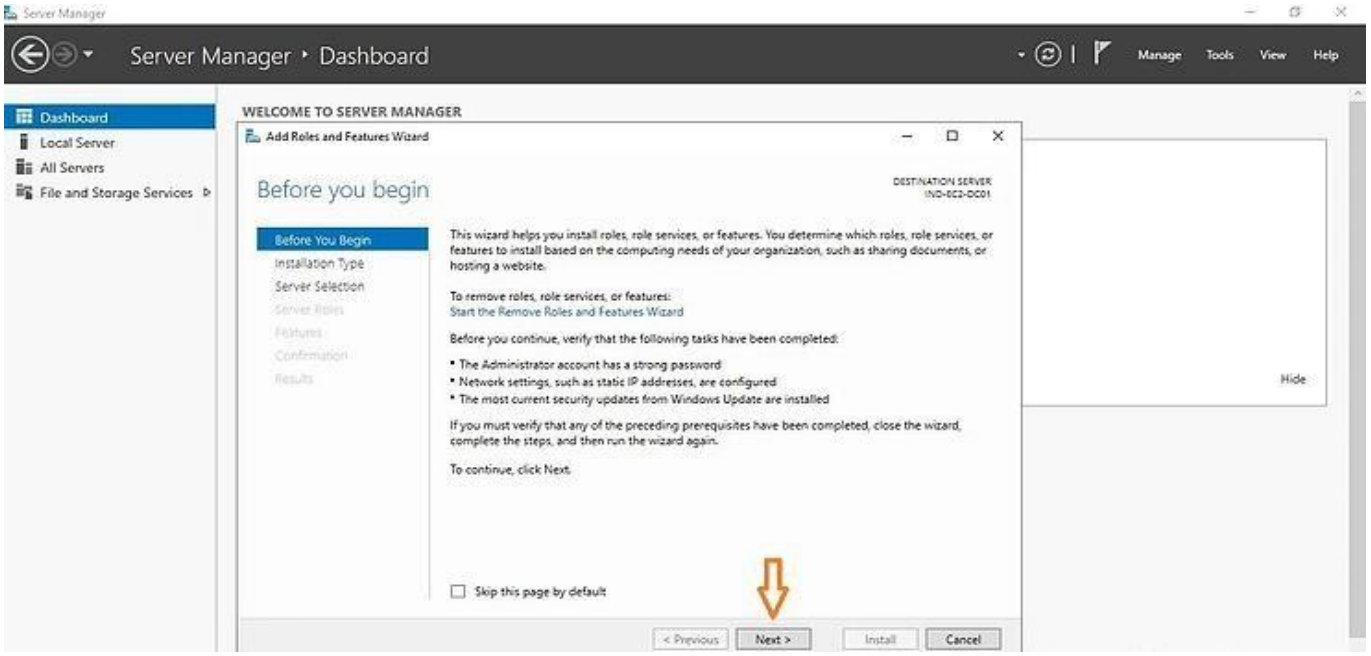


FIG 3.2 BEFORE YOU BEGIN WIZARD

In the "**Installation Type**" tab choose **Role-based or Feature-based installation** and click on the Next button.

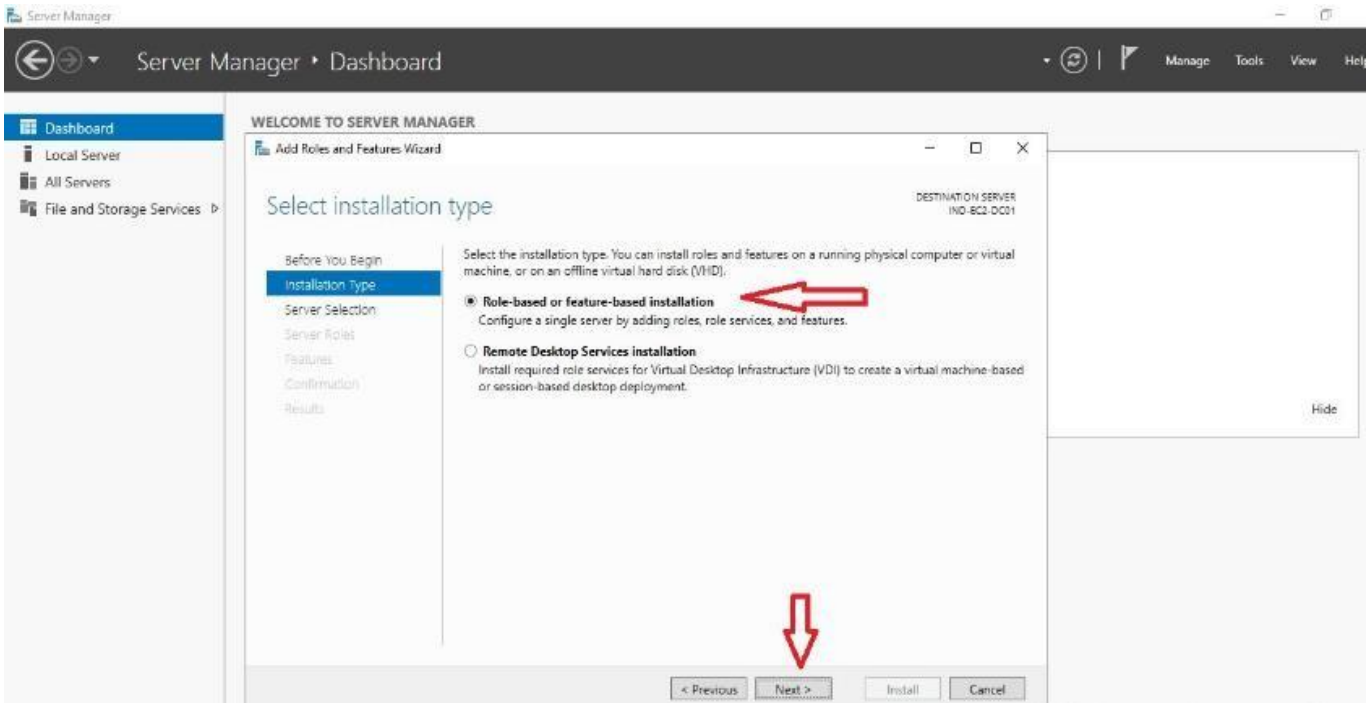


FIG 3.3 SELECT INSTALLATION TYPE

In the **Server Selection** tab, please select the destination server on which the role will be install. Please verify the hostname and the IP address points of the selected server. Click **Next** to continue.

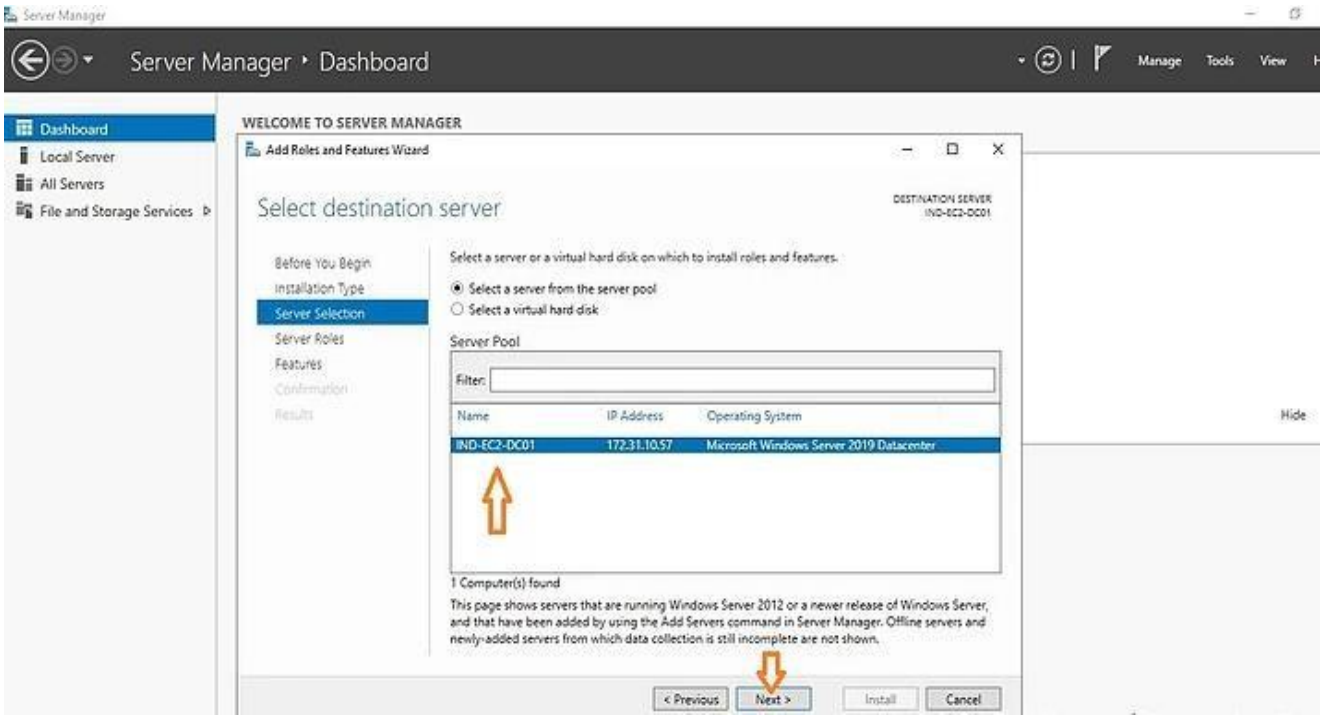


FIG 3.4 SELECT DESTINATION SERVER

In the **Server Roles** tab, put a tick mark for **"Active Directory Domain Services"** (select the **DNS Server** role as well, as we will configure AD integrated DNS server. If not selected, during installation it will automatically select and install the DNS Role).

Then, it will prompt to show the associated features for the role. Click on **Add Features** to add those. Then click **Next** to continue.

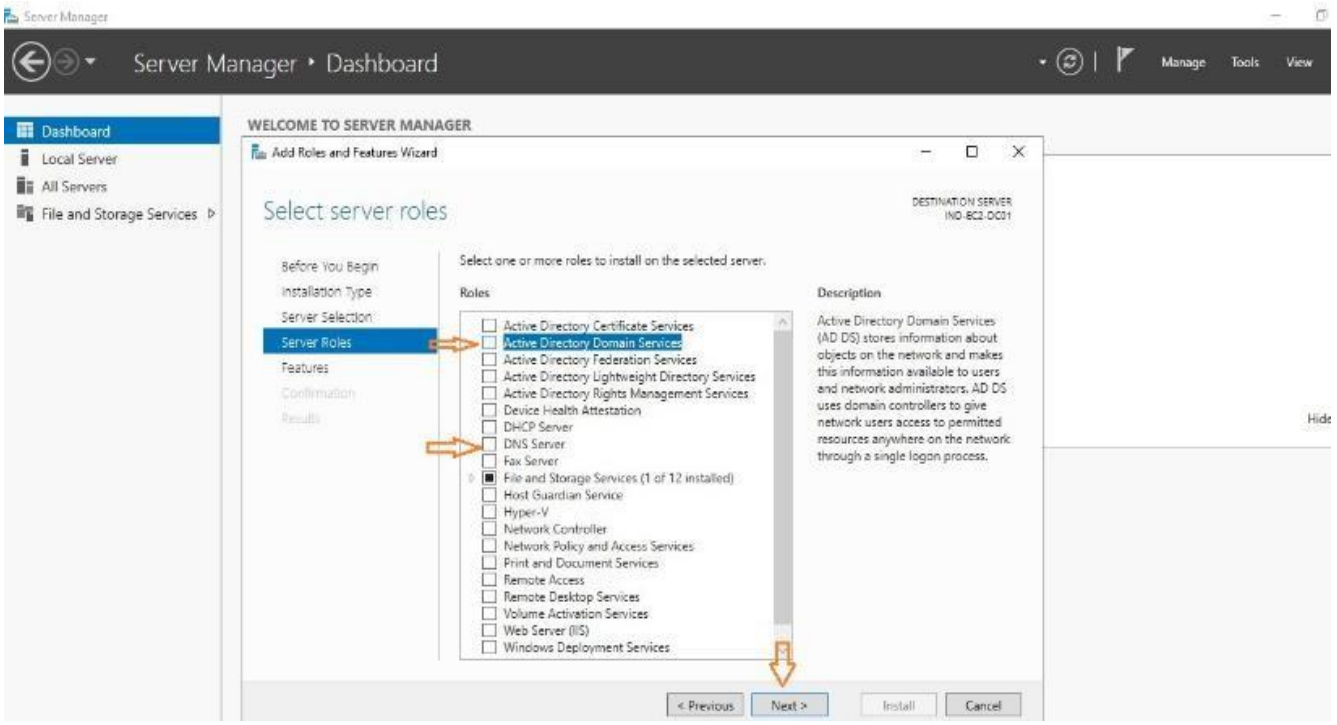


FIG 3.5 SELECT SERVER ROLES

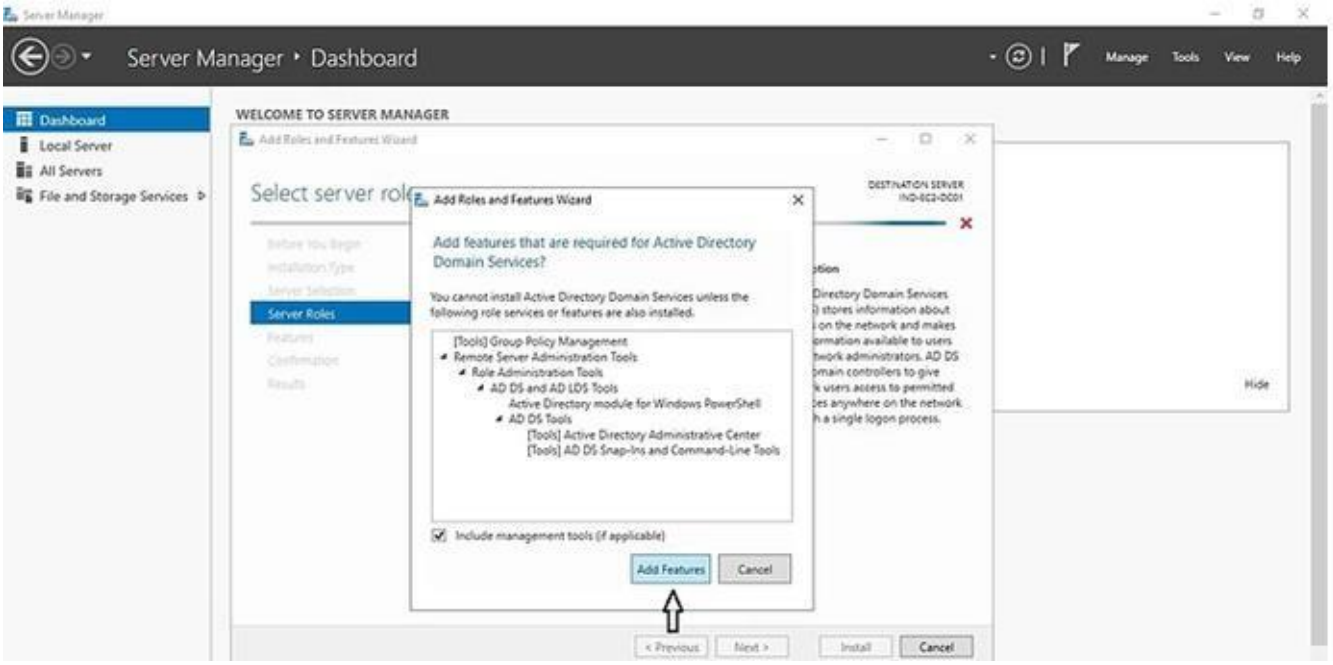


FIG 3.6 SELECT DESTINATION SERVER-ADD FEATURES

In the **Features** tab, the basic features for this required role are already selected by default. Click **Next** to install continue.

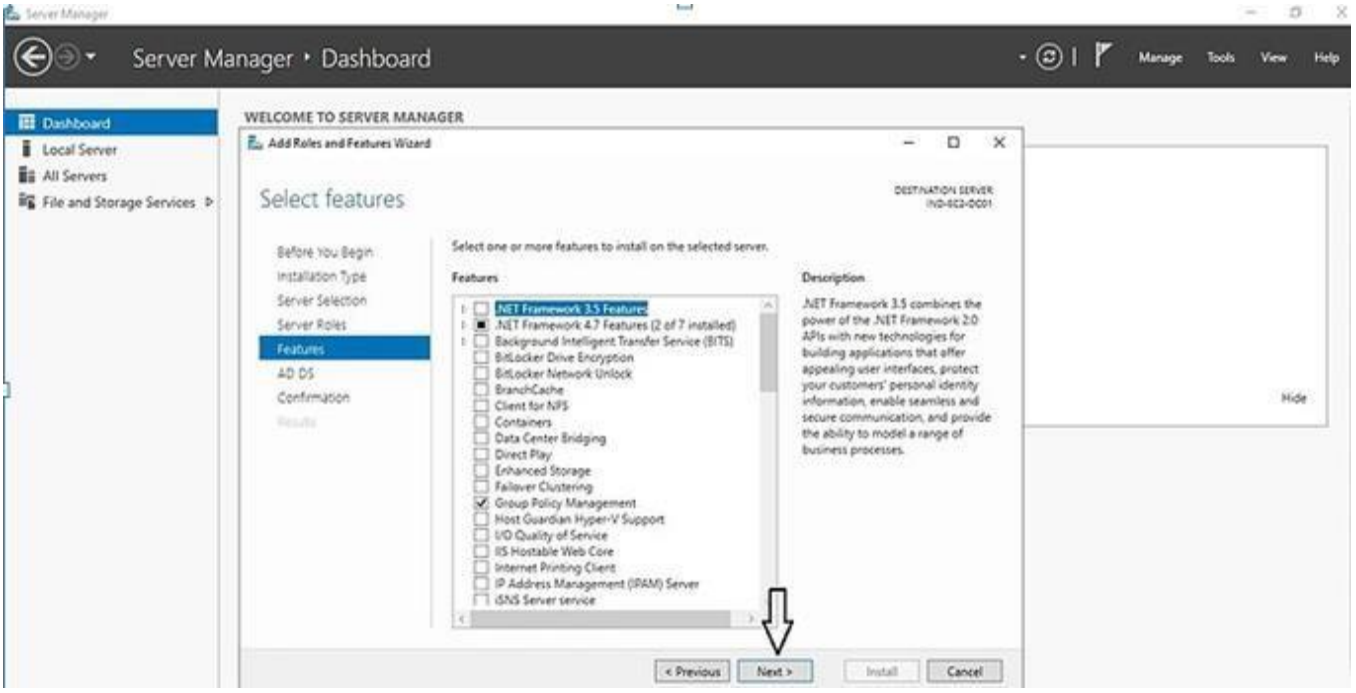


FIG 3.7 SELECT FEATURES

In the next window, it gives brief information about "**Active Directory Domain Services"** service. Click **next** to proceed.

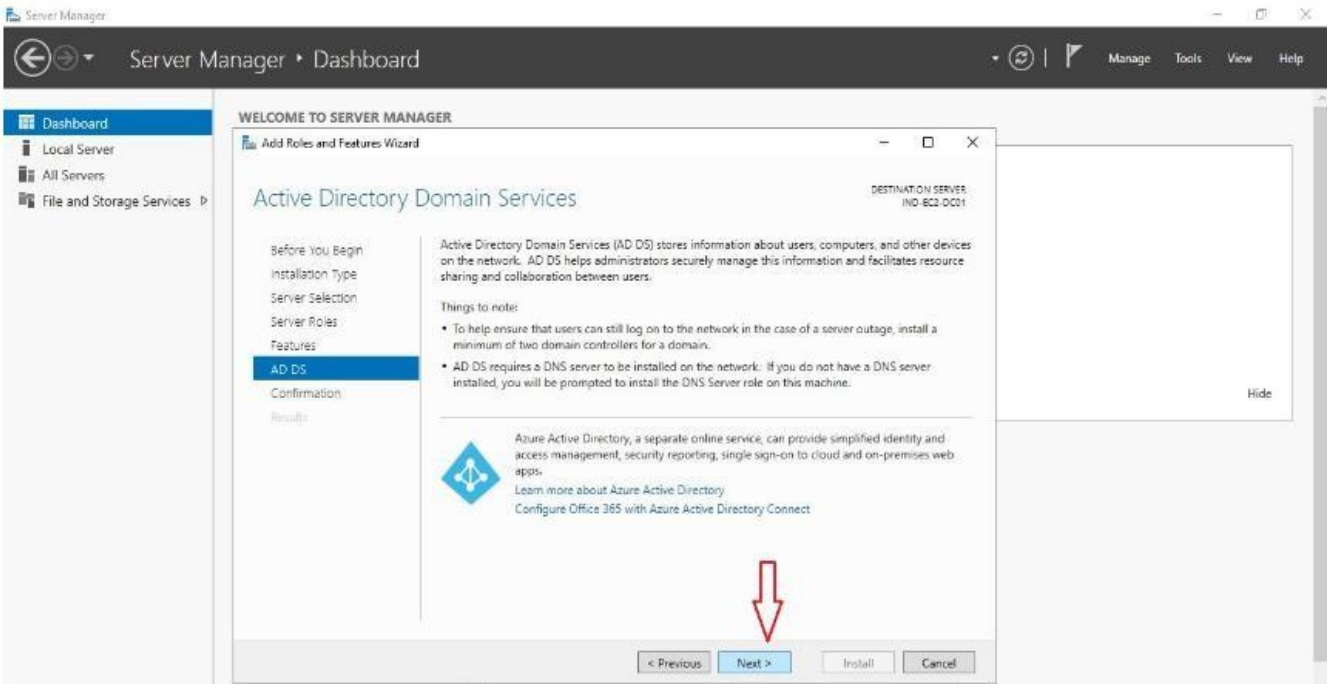


FIG 3.8 ACTIVE DIRECTORY DOMAIN SERVICES

In the **Confirmation** tab, verify the selections and click on the **Install** button.

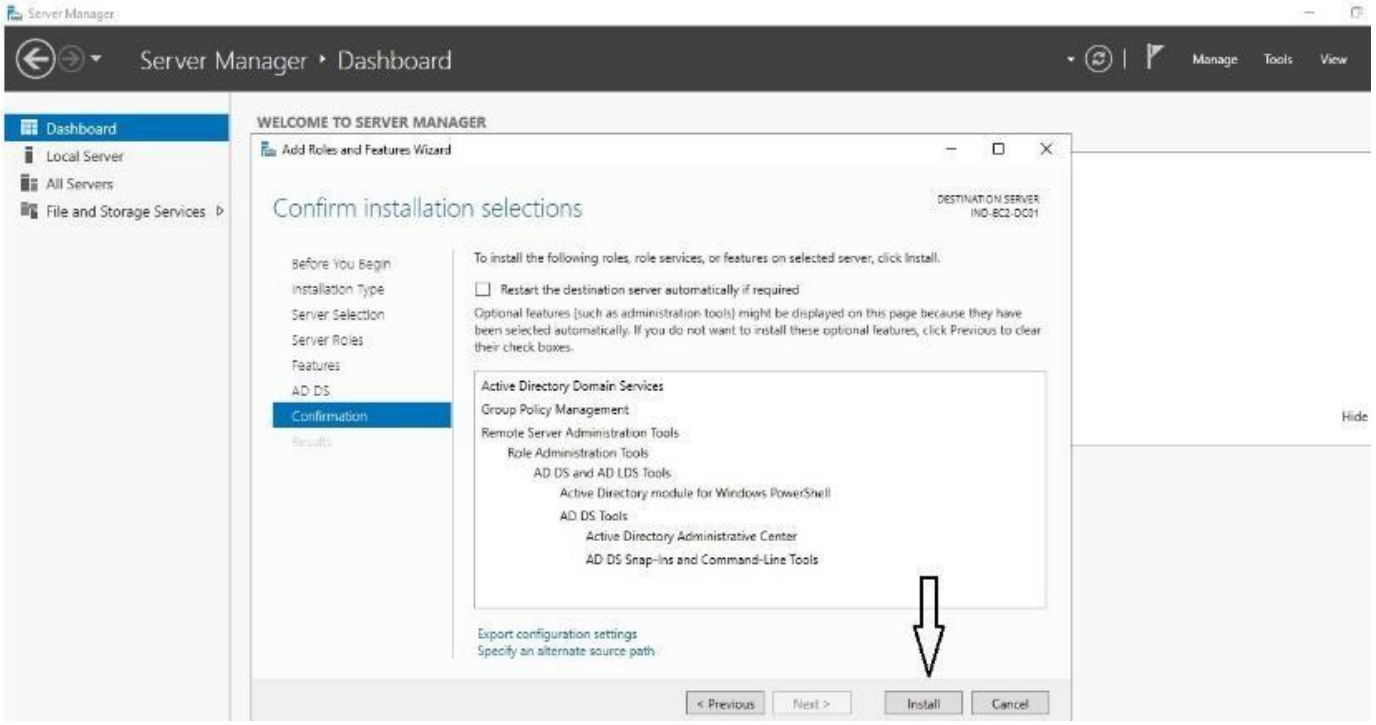
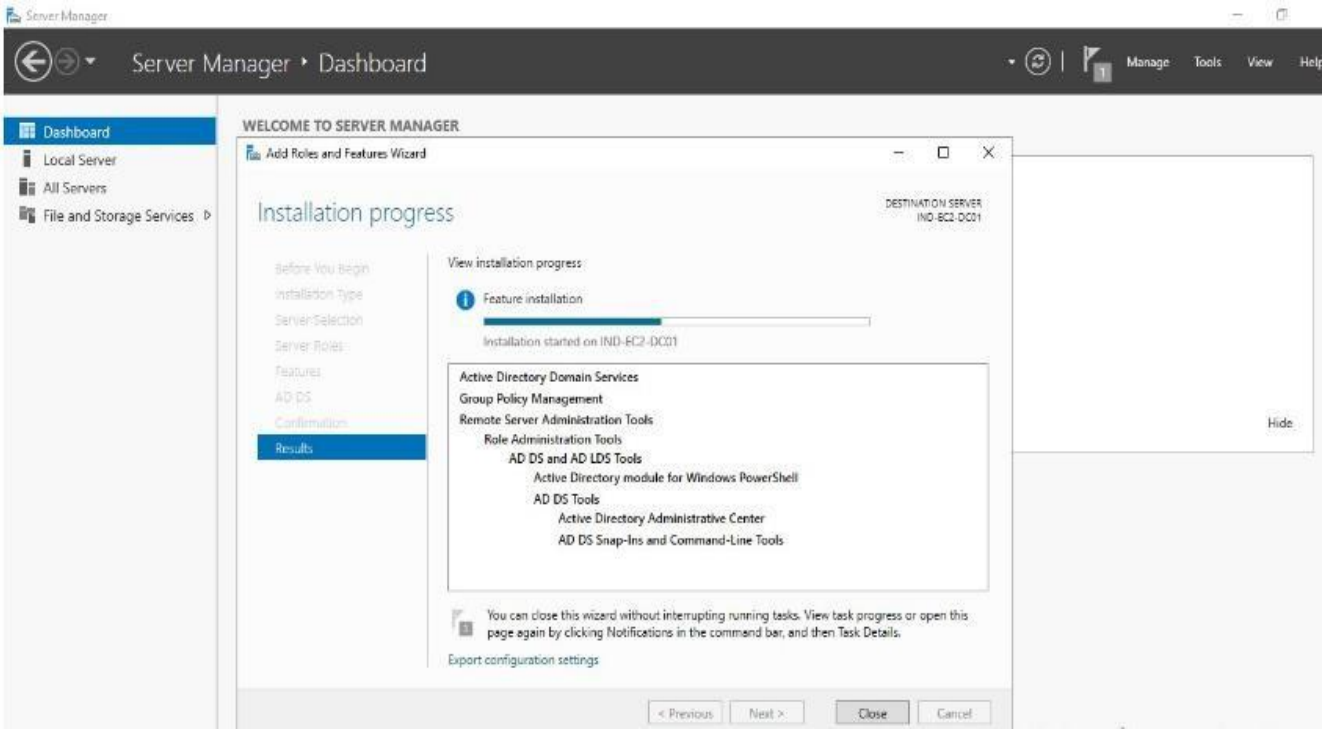


FIG 3.9 INSTALLATION

Once done, it will start the installation process and check the same in the **Results** tab.



Step 2: Promote the server into a Domain Controller

Once the **ADDS** role installation completes, click on the option **"Promote this server to a Domain Controller"** *(highlighted in below image)***.** select "Promote this server into a domain controller", this will start the configuration process.

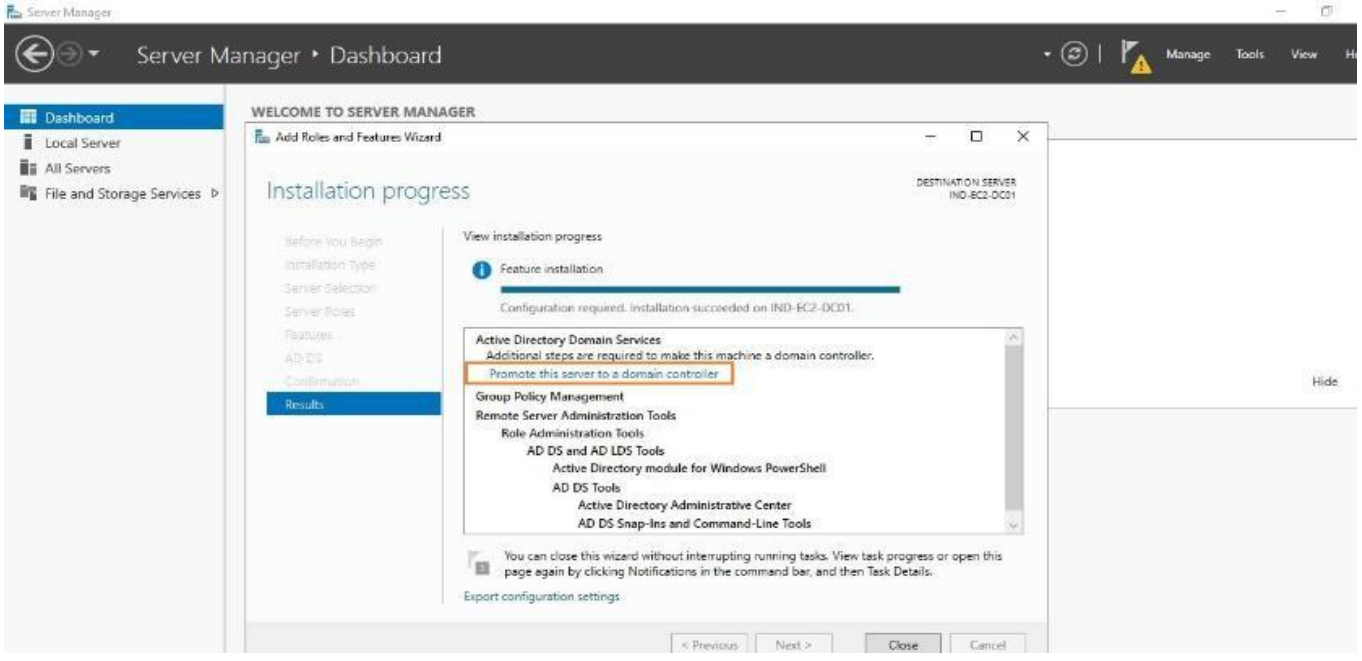


FIG 3.9 PROMOT THIS SERVER TO DOMAIN CONTROLLER

It will open the **"Active Directory Configuration Wizard"**. Now, from the Deployment Configuration tab, select **"Add a new forest"**. Provide a **Root Domain name**, then, click on **Next** to continue.

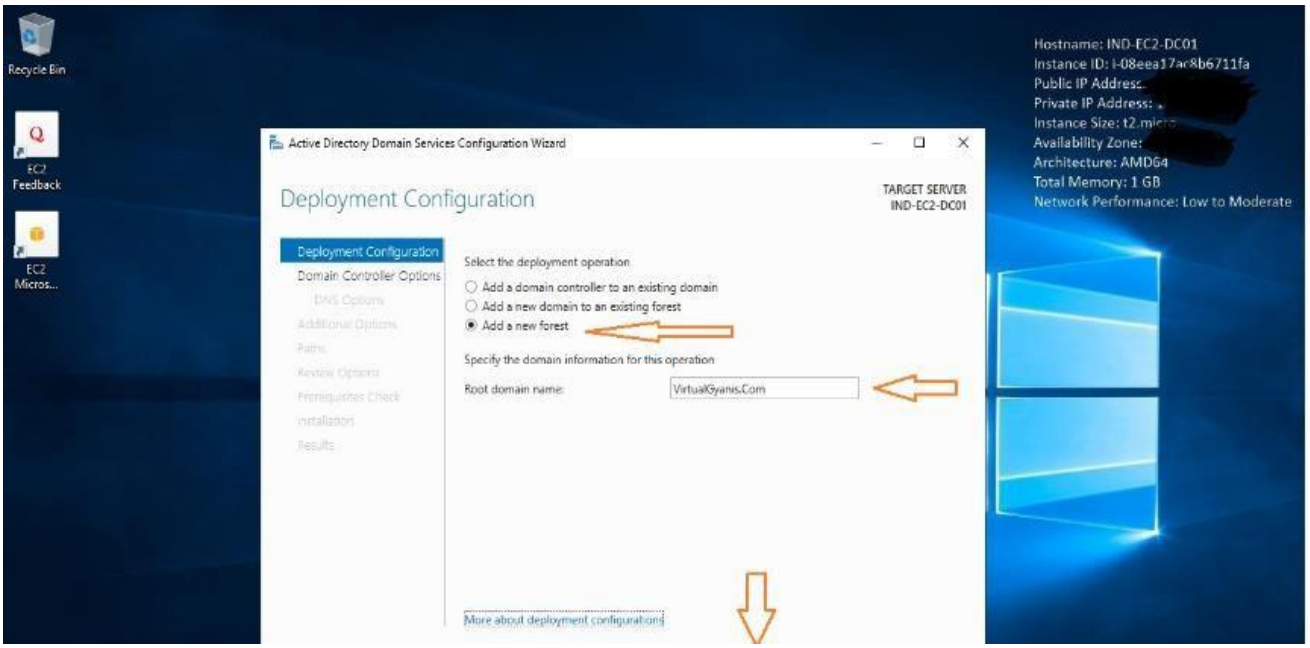


FIG 3.10 ACTIVE DIRECTORY CONFIGURATION WIZARD

In the **Domain Controller Option** tab, select a **Forest functional level** and a **Domain functional level**. Since this is the first domain controller in the forest, please select the **DNS Server.**

Then, enter the **Active Directory Restore Mode (DSRM)** password, this is used to retrieve/restore Active Directory data. Then, click **Next** to continue

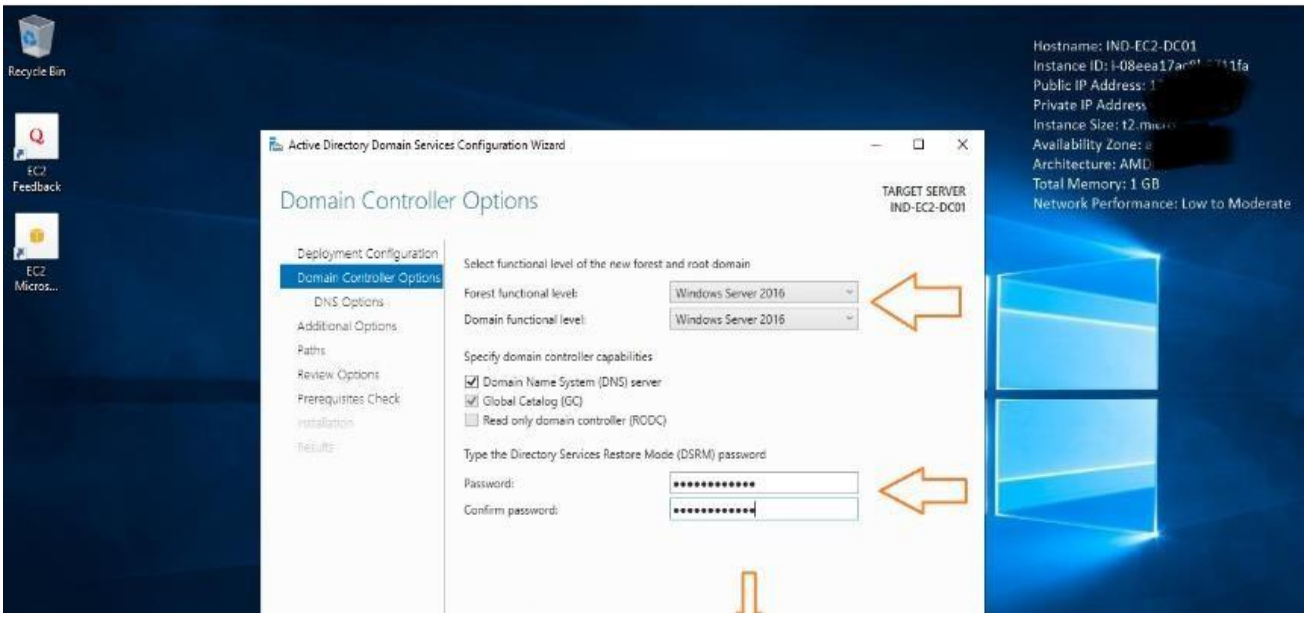


FIG 3.11 DOMAIN CONTROLLER

Since we have configured AD integrated DNS Server, user can ignore the DNS Delegation warning as shown in the below screen. Then, click **Next** to continue.

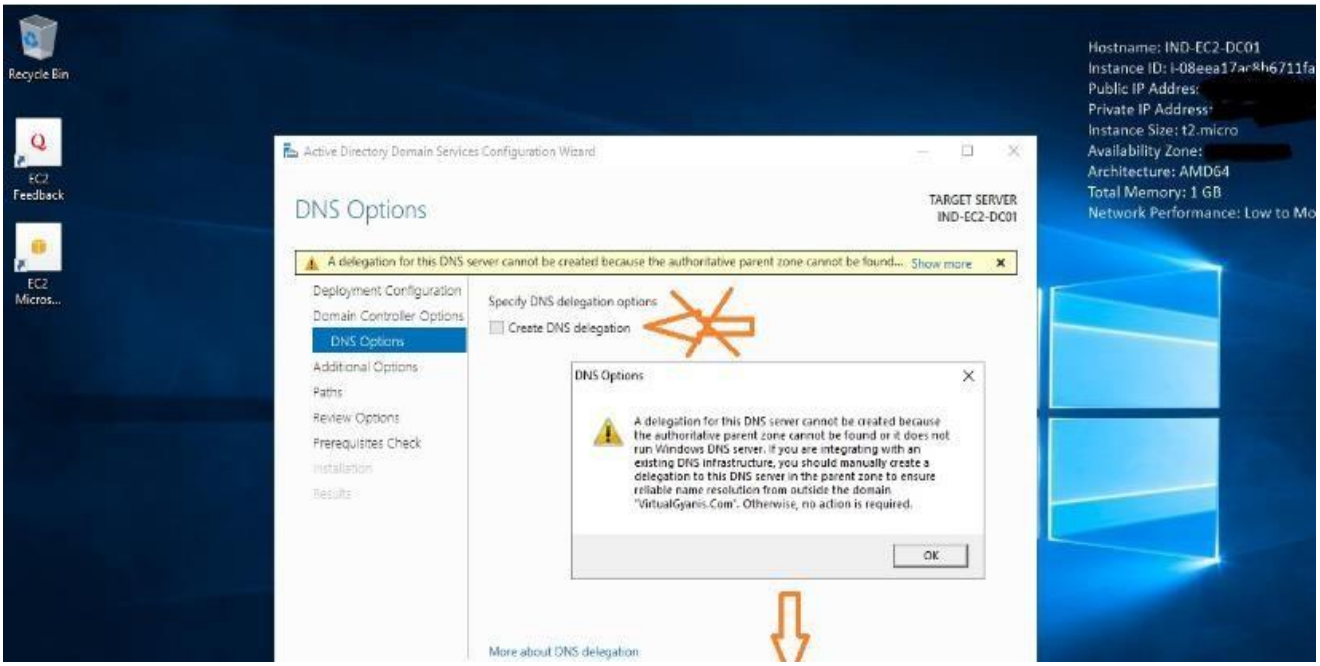


FIG 3.11 DNS

In the **Additional Options** tab, enter a NetBIOS name for the domain. It is suggested to keep the NetBIOS name same as the root domain name *(by default, it will fetch the domain name only)*. Then, click **Next** to continue.

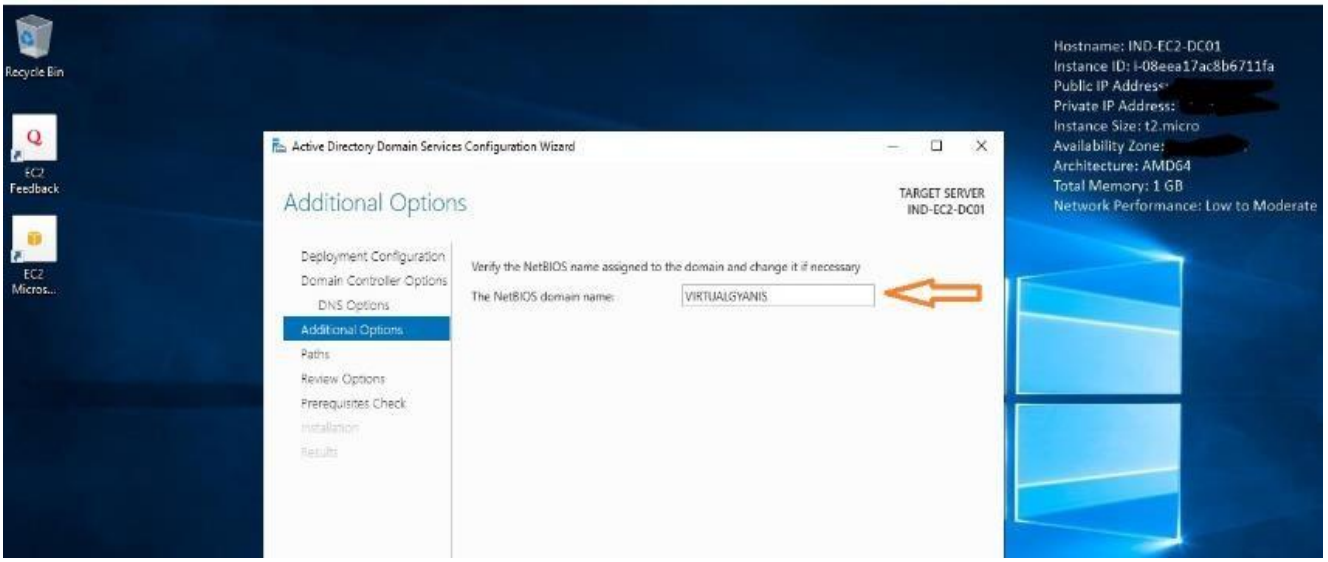


FIG 3.12 ADDITIONAL OPTIONS

In the **Path** tab, user have to mention the **Database (NTDS Database), LOG files and SYSVOL** folders path. User can change the default path as per the organization security policies. Now, click **Next** to continue.

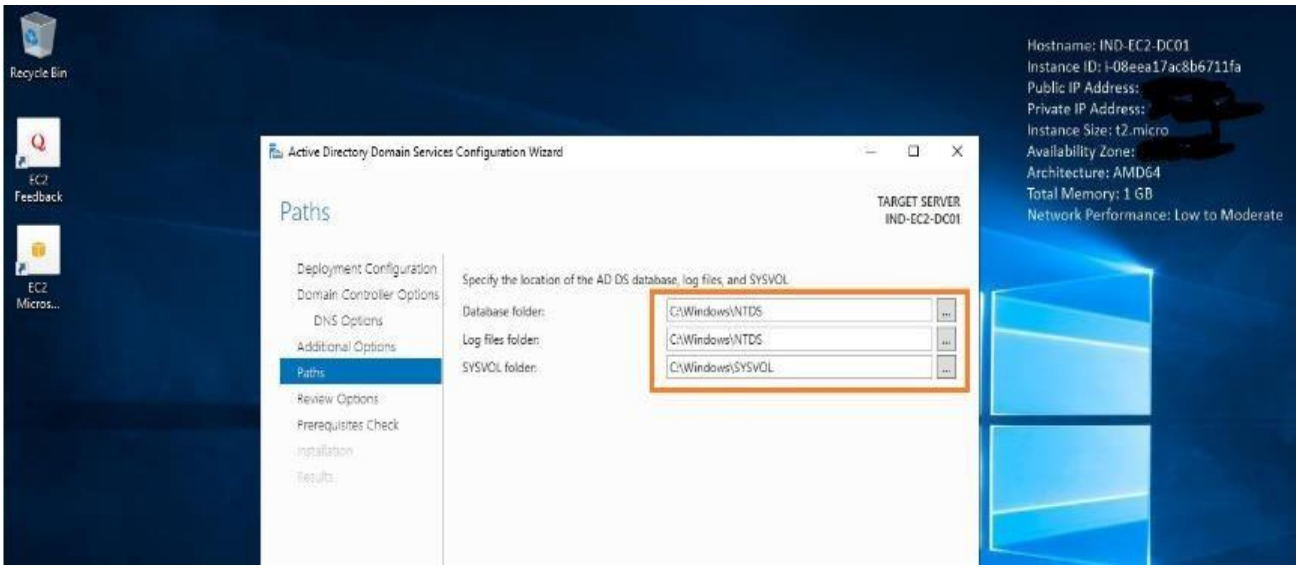


FIG 3.13 PATH

In the **Review Options** tab, user can review the configuration. Click **Next** to proceed or otherwise user can go back and change the required setting as per the need and then proceed further.

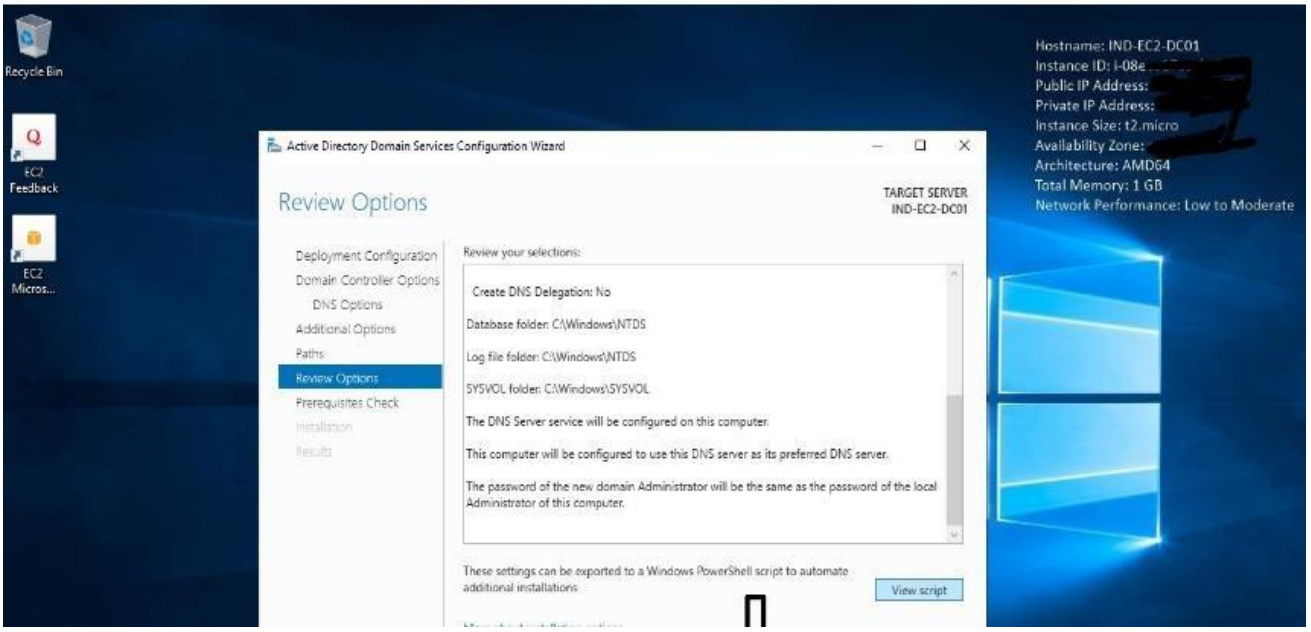


FIG 3.14 REVIEW OPTIONS

In the **Prerequisites Check** tab, it will do prerequisite check.

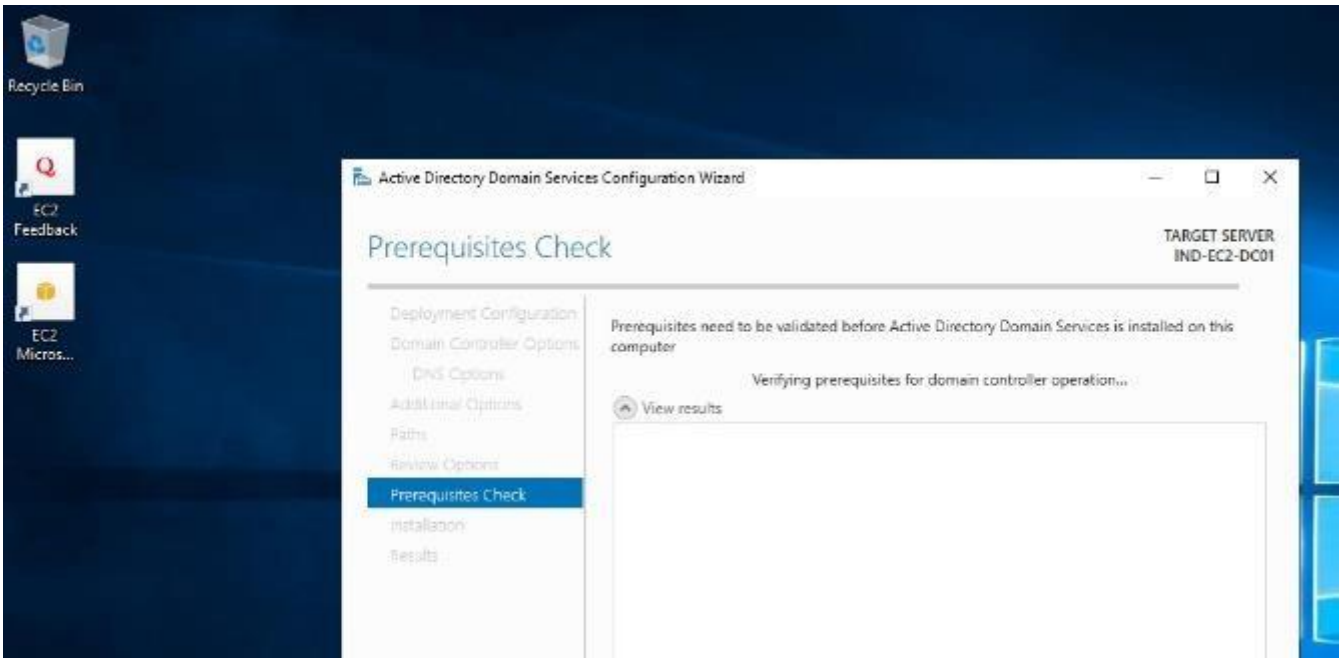
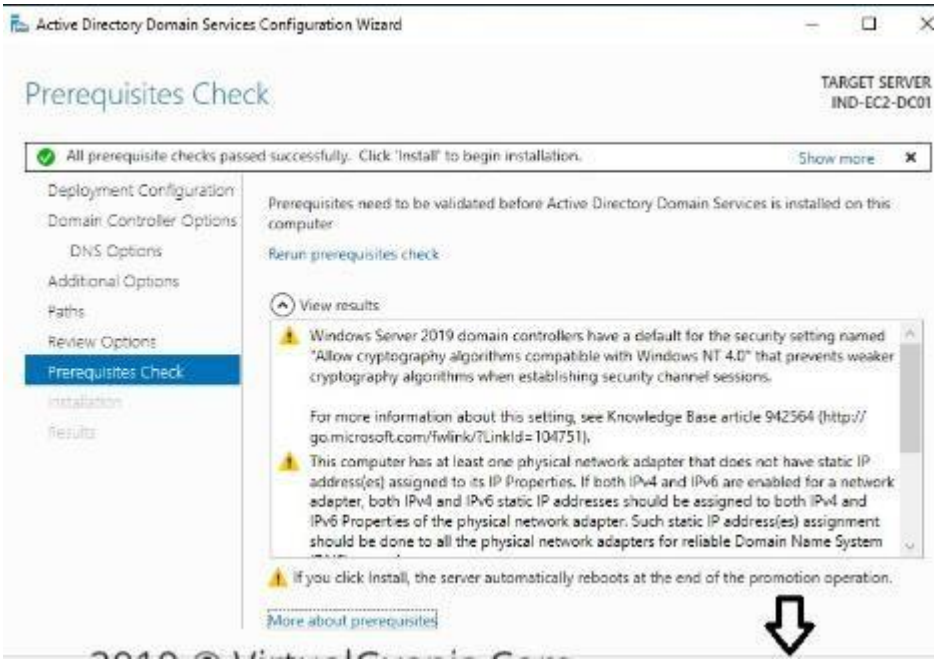


FIG 3.15 PREREQUISITES CHECK

Once prerequisite checks are completed successfully, it will enable/highlight the Install option. Then, click on the Install button to start the installation process.



Once installation completed successfully, user will get the below confirmation message. Close this window and restart the Server.

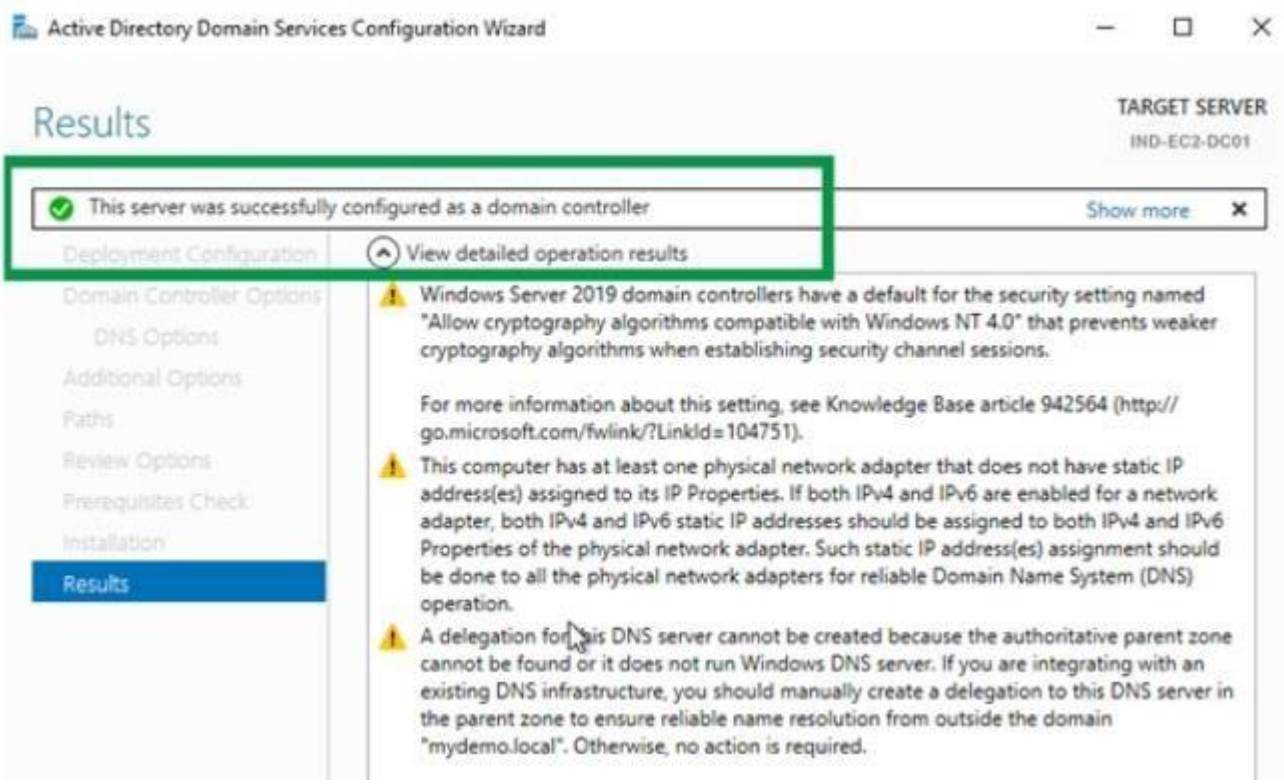


FIG 3.16 DOMAIN CONTROLLER

Once the server rebooted, user can login with the domain Admin credentials. By default, the local admin account will promoted as a Domain Admin account.

Result

Thus, The domain controller was created and managed.

Ex.No 4 **Designing an Active Directory and Managing adds objects**

Aim

To design an Active Directory and Managing ADDS objects.

ADDS Objects

Object is the basic element of Active Directory in Microsoft Windows Server family that represents something on the network, such as a user, a group, a computer, an application, a printer, or a shared folder. Real-world entities such as users, computers are represented as objects in Active Directory. Each object consists of a set of attributes which best describes it. For example, consider a user object. A user is described by attributes like Name, Address, and Telephone number and so on. Active Directory supports numerous types of objects. To unambiguously identify an object, a global unique identifier is associated with it.

Add Users and Computers to the Active Directory domain

After the new Active Directory domain is established, create a user account in that domain to use as an administrative account. When that user is added to the appropriate security groups, use that account to add computers to the domain.

1. To create a new user, follow these steps:
    1. Click **Start**, point to Administrative Tools, and then click **Active Directory Users and Computers** to start the Active Directory Users and Computers console.
    2. Click the domain name that you created, and then expand the contents.
    3. Right-click **Users**, point to **New**, and then click **User**.
    4. Type the first name, last name, and user logon name of the new user, and then click **Next**.
    5. Type a new password, confirm the password, and then click to select one of the following check boxes:
        - Users must change password at next logon (recommended for most users)
        - User cannot change password
        - Password never expires
        - Account is

        disabled Click

        Next.

    6. Review the information that you provided, and if everything is correct, click **Finish**.

FIG 4.1 Select Active Diretory Users and Computers

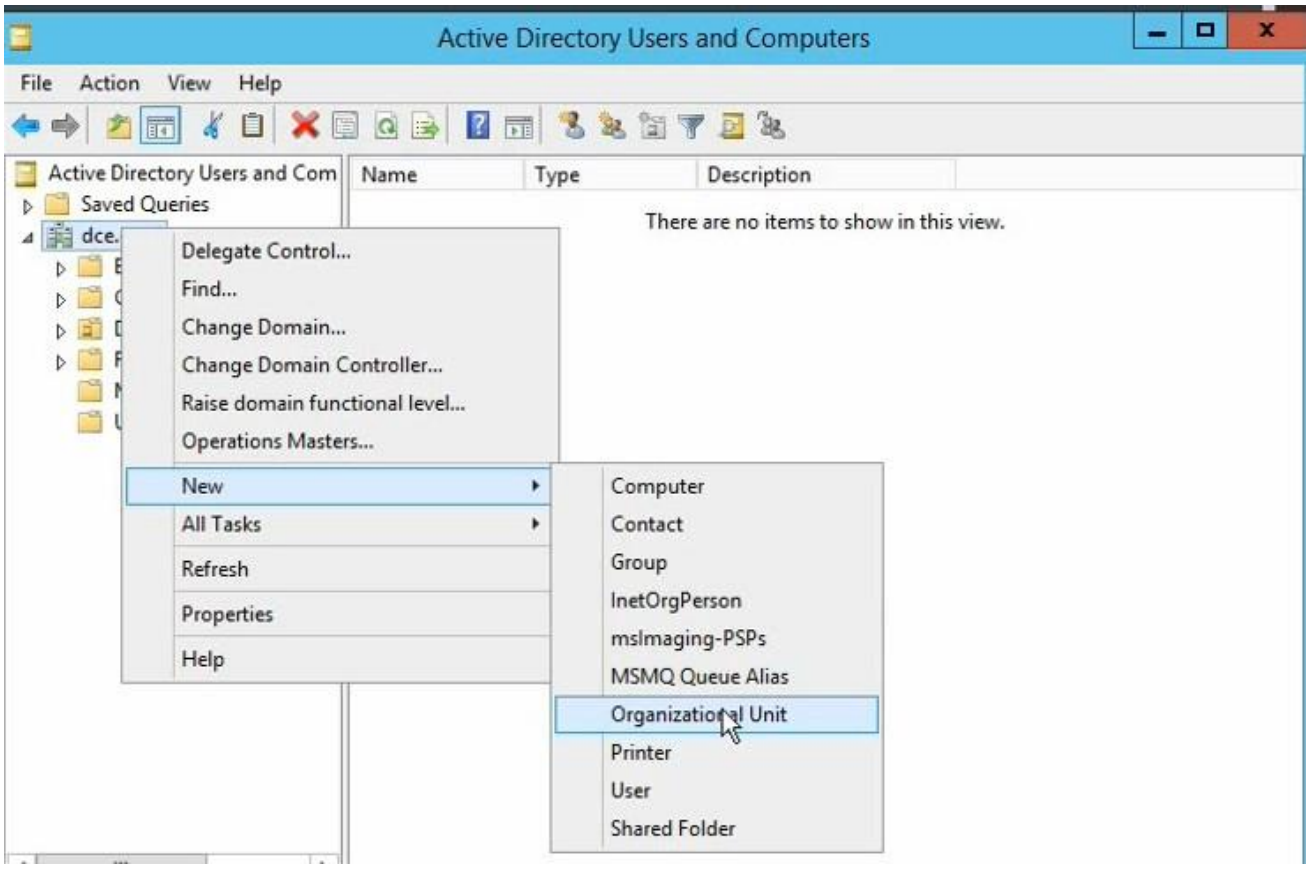


FIG 4.2 Create New Object (User)

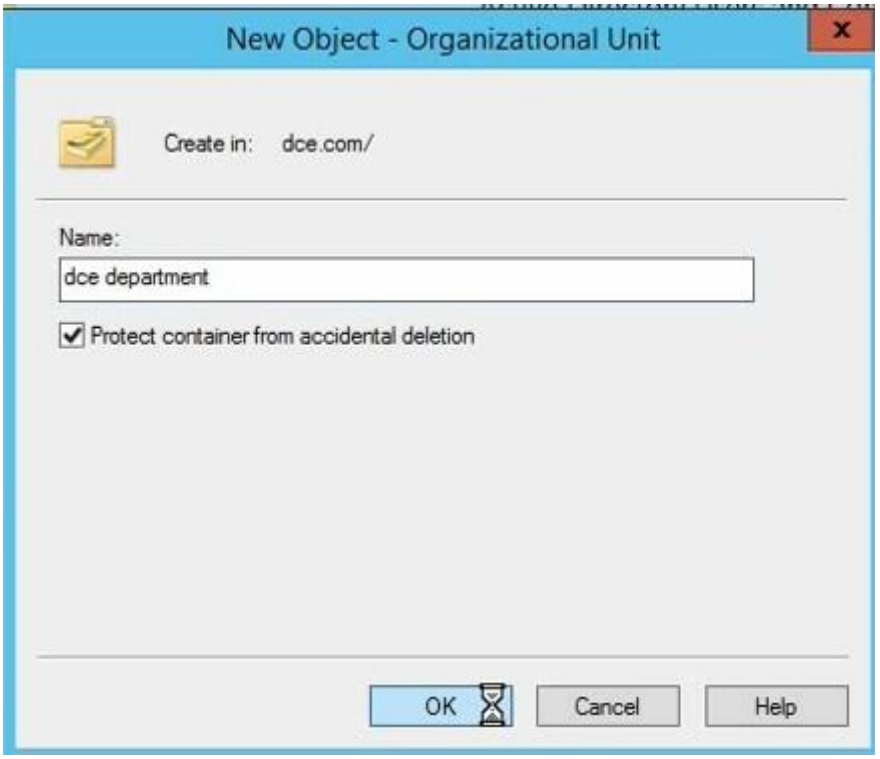
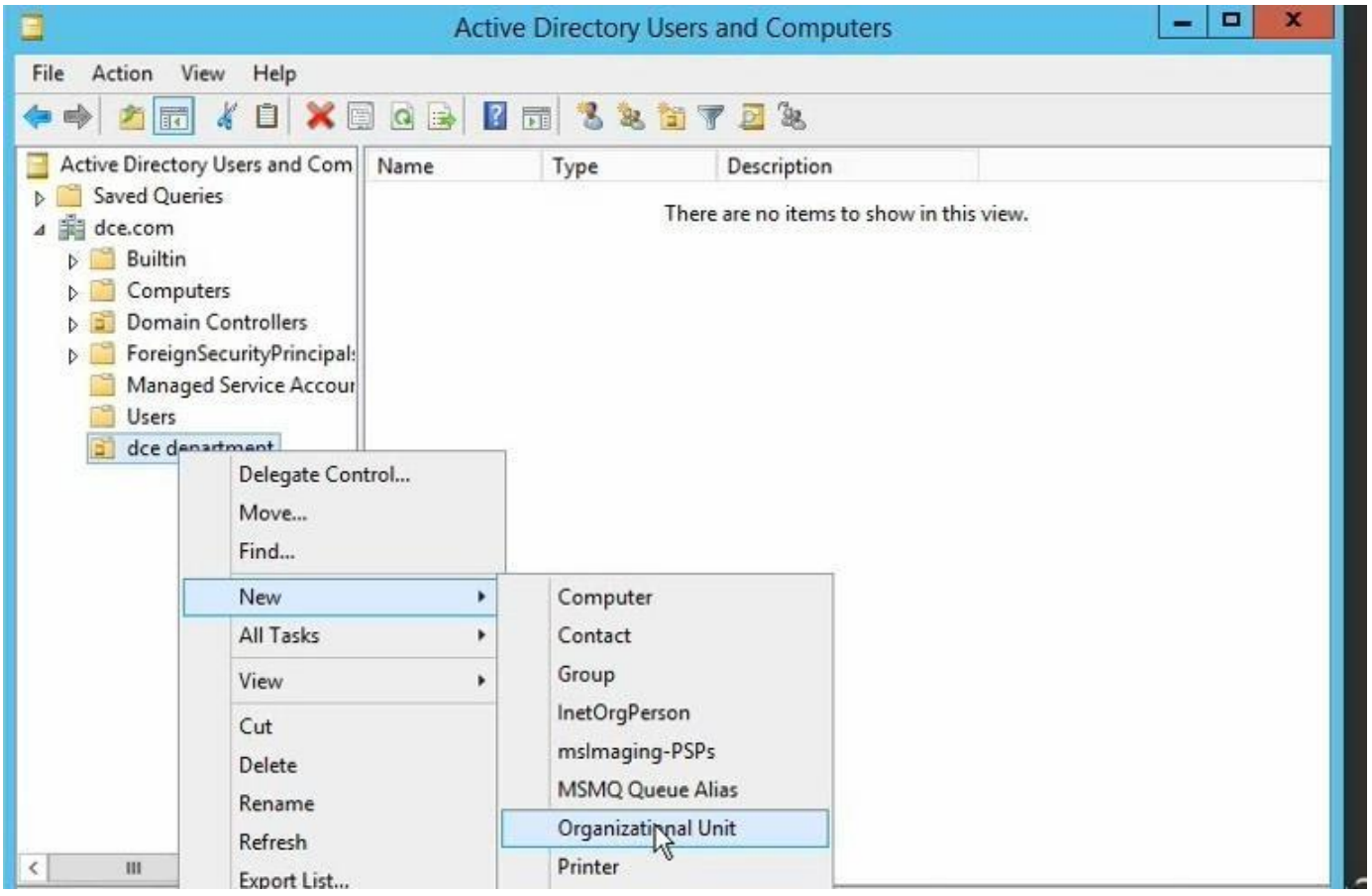


FIG 4.3 Create New Object (dce department)



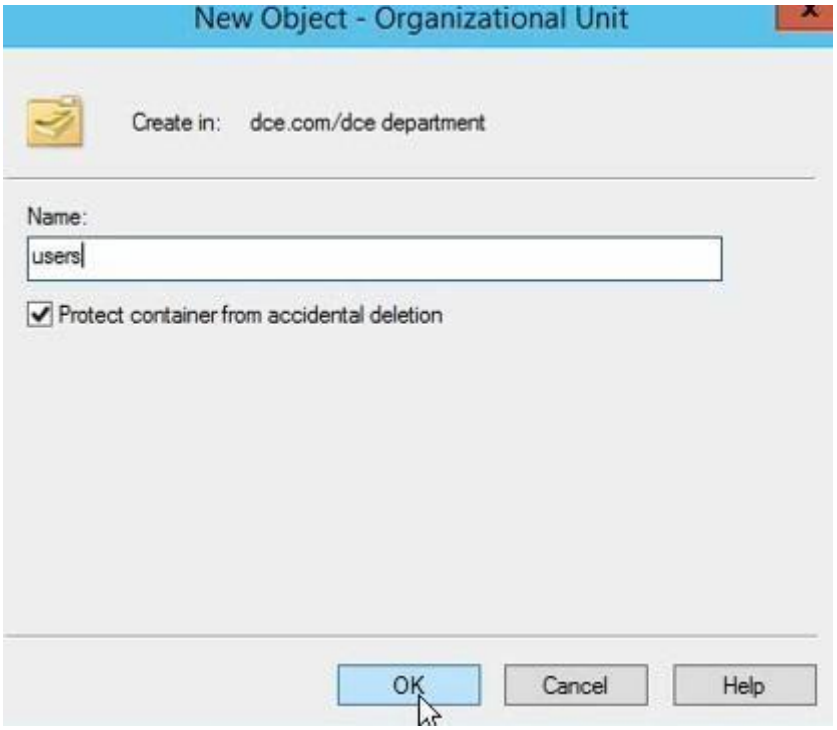


FIG 4.4 Create New Object (users)

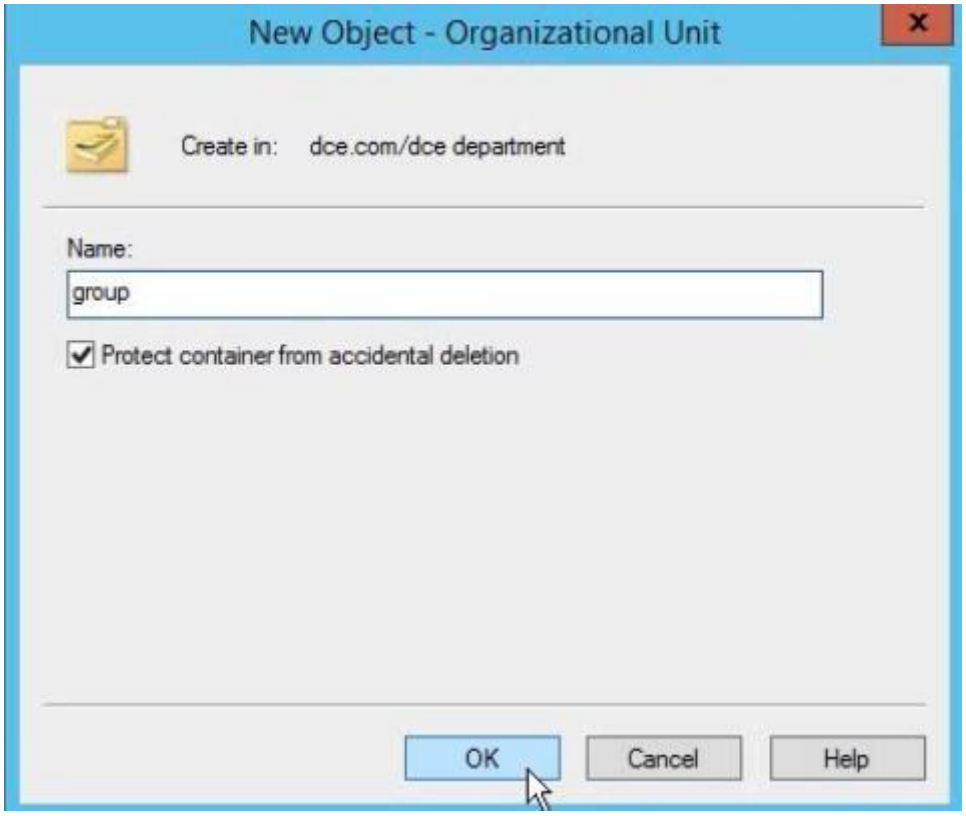


FIG 4.5 New Object (group)

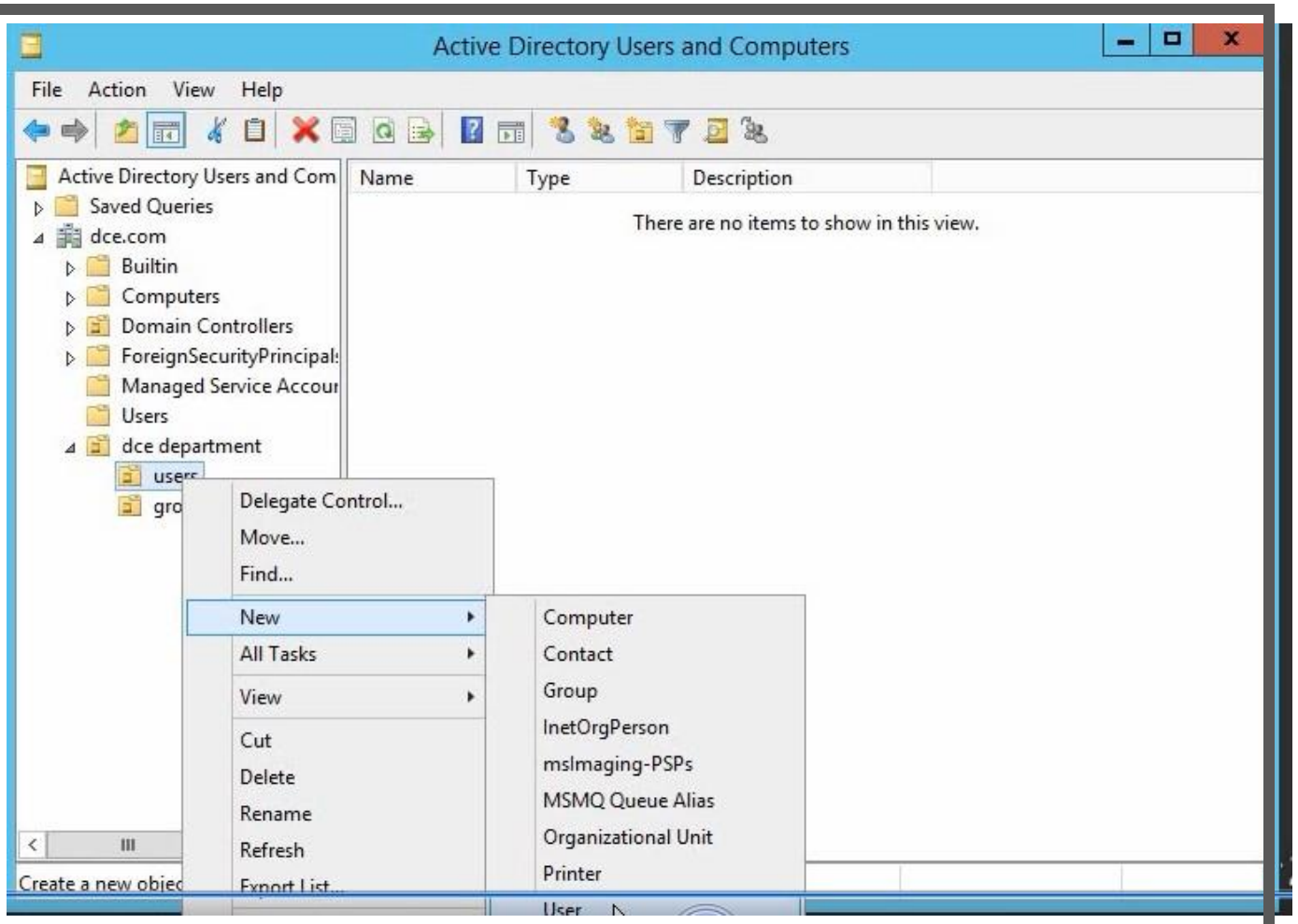
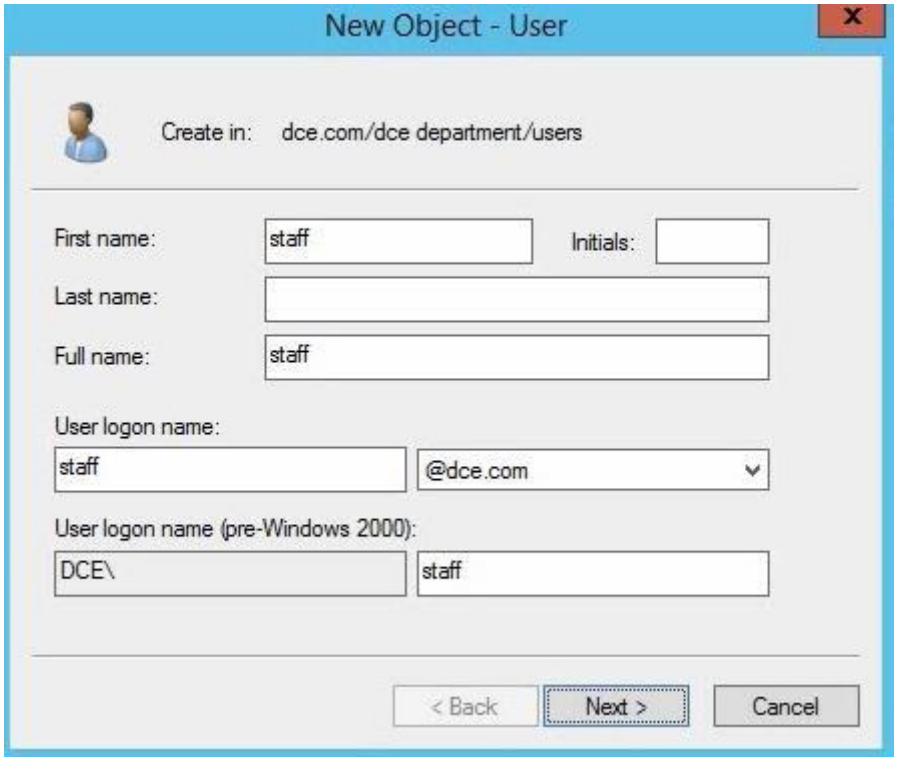


FIG 4.6 New UserCreation



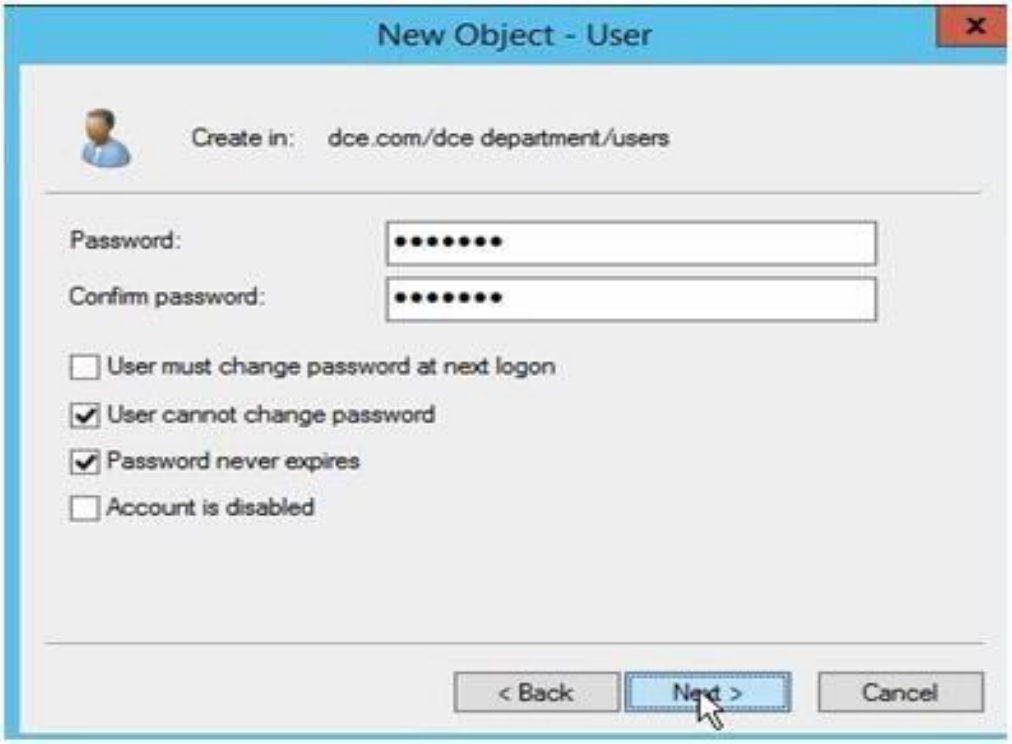
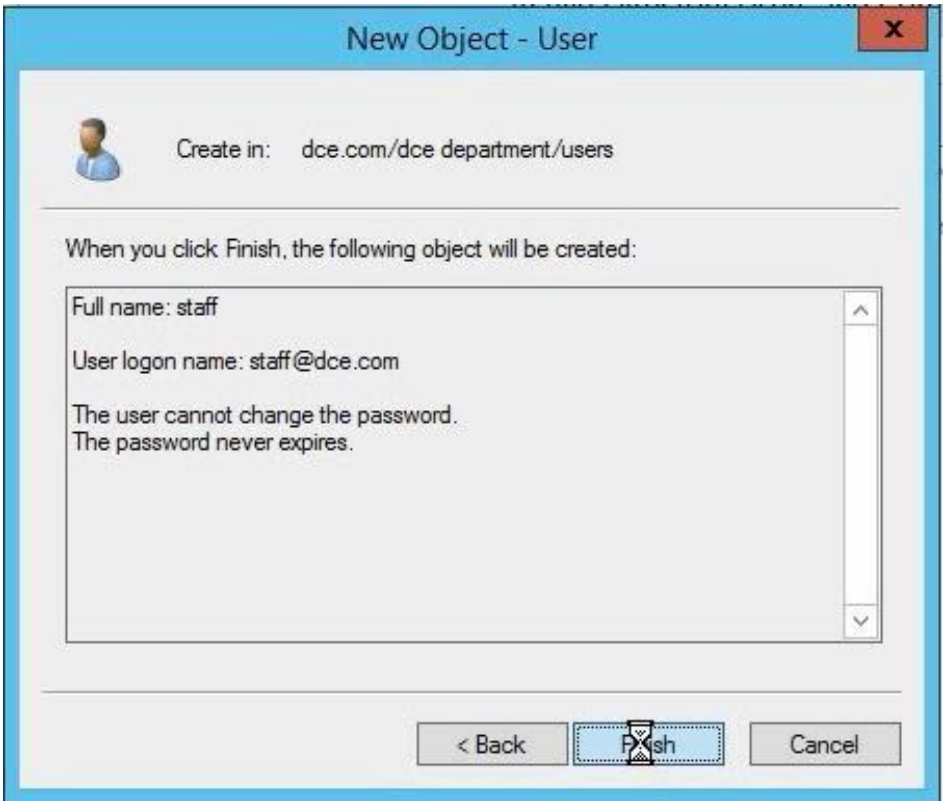
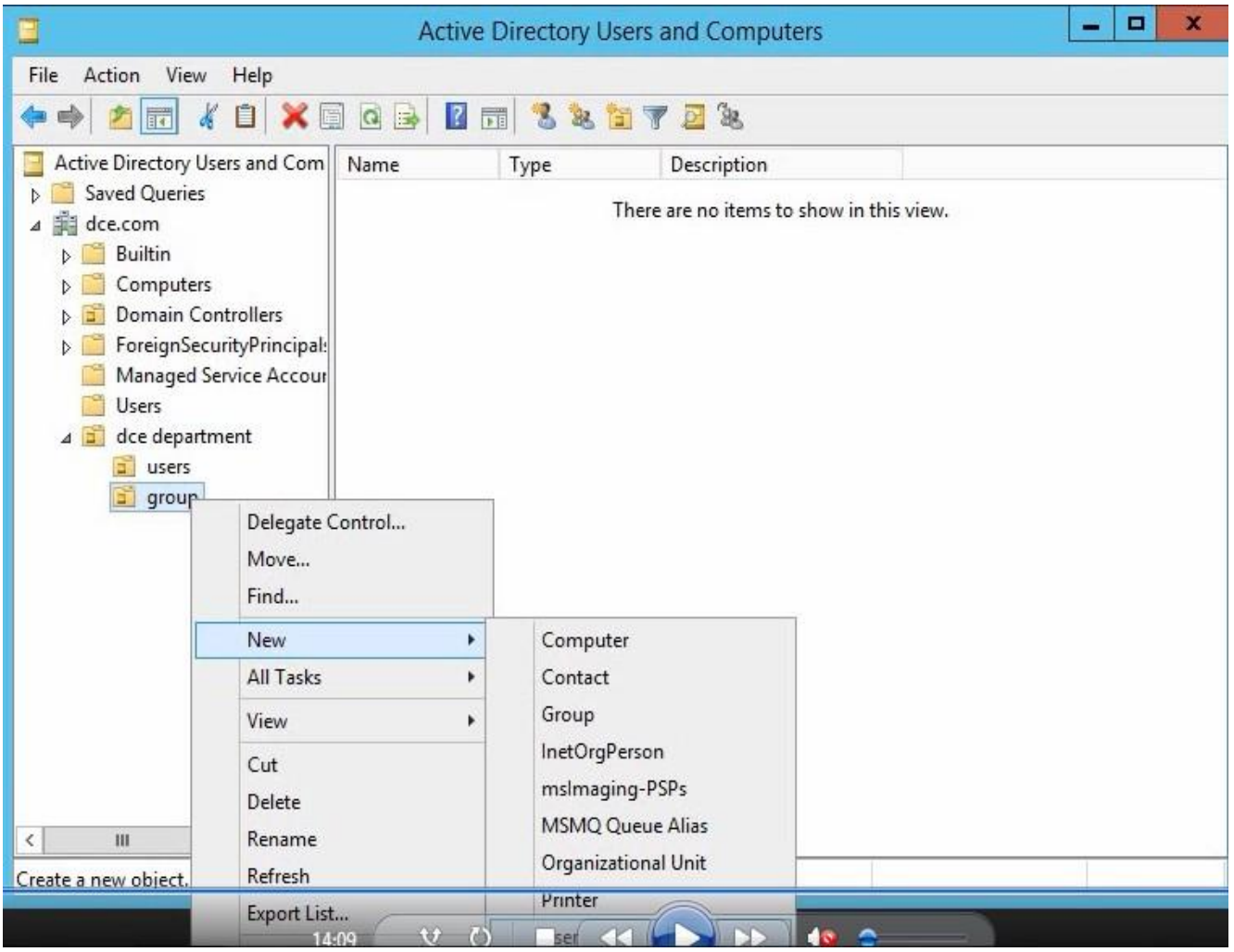


FIG 4.7 Selection of User Rights

FIG 4.8 Object Created




Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
dce.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
dce department
users
group
Name
Type
Description
There are no items to show in this view.
Delegate Control...
Move...
Find...
New
All Tasks
View
Cut
Delete
Rename
Refresh
Export List...
Computer
Contact
Group
InetOrgPerson
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
Create a new object.

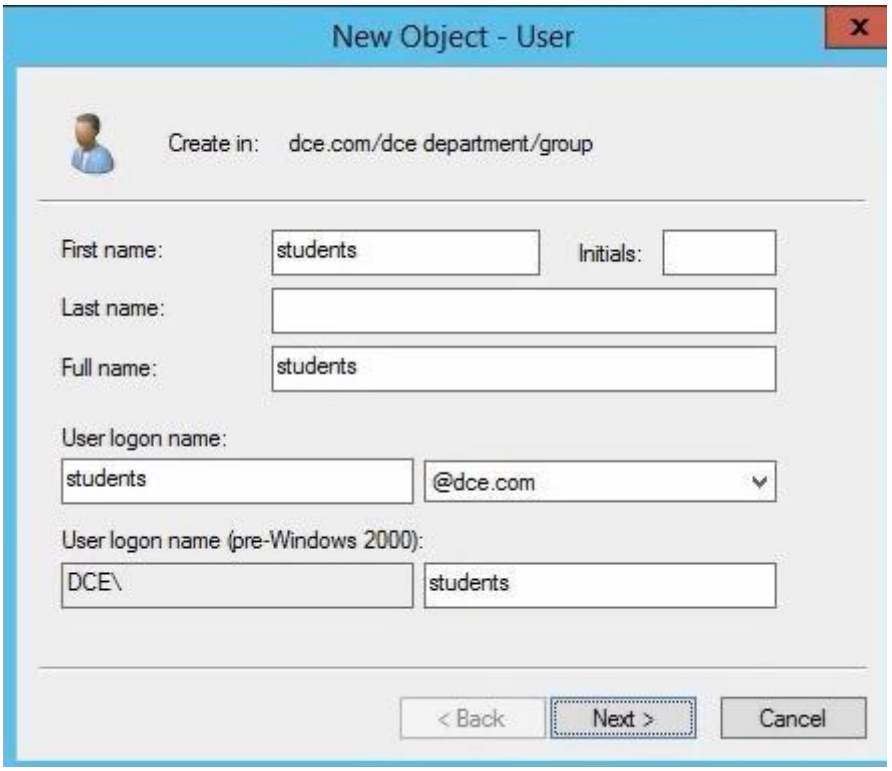
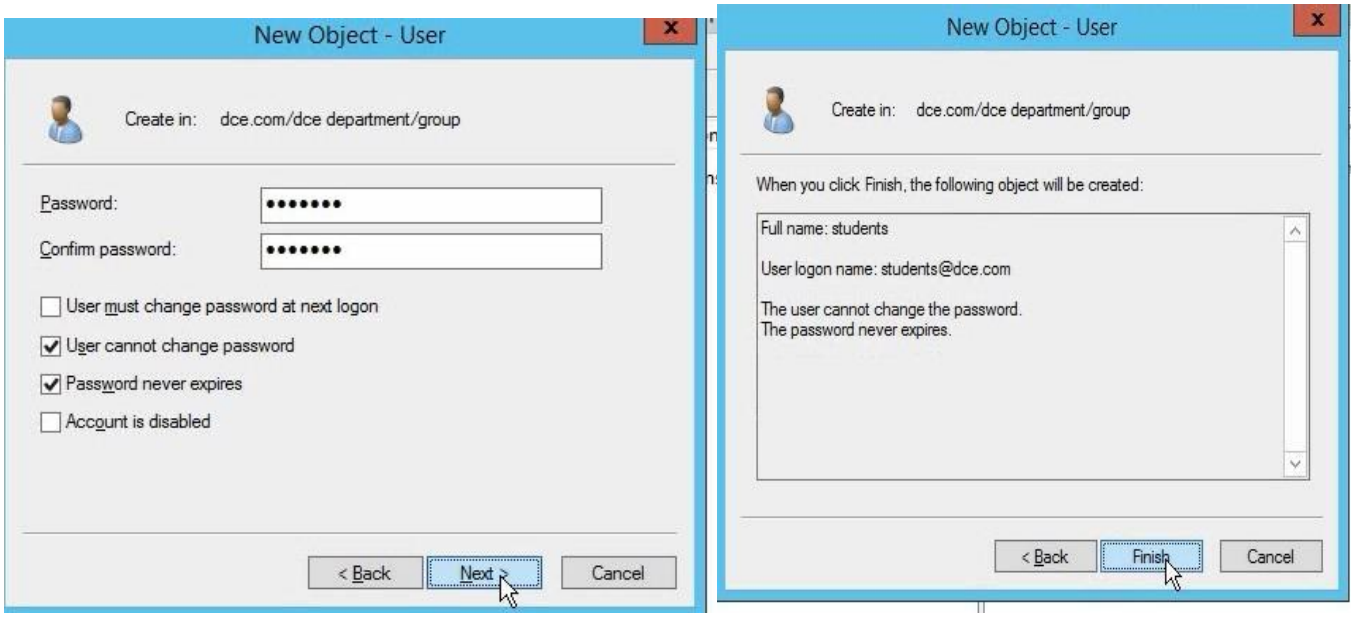

New Object - User
Create in: dce.com/dce department/group
First name: students
Initials:
Last name:
Full name: students
User logon name:
students
@dce.com
User logon name (pre-Windows 2000):
DCE\
students
< Back
Next >
Cancel

FIG 4.9 Students Object Created



Result:

Thus, the Active Directory Domain Service Object was created.

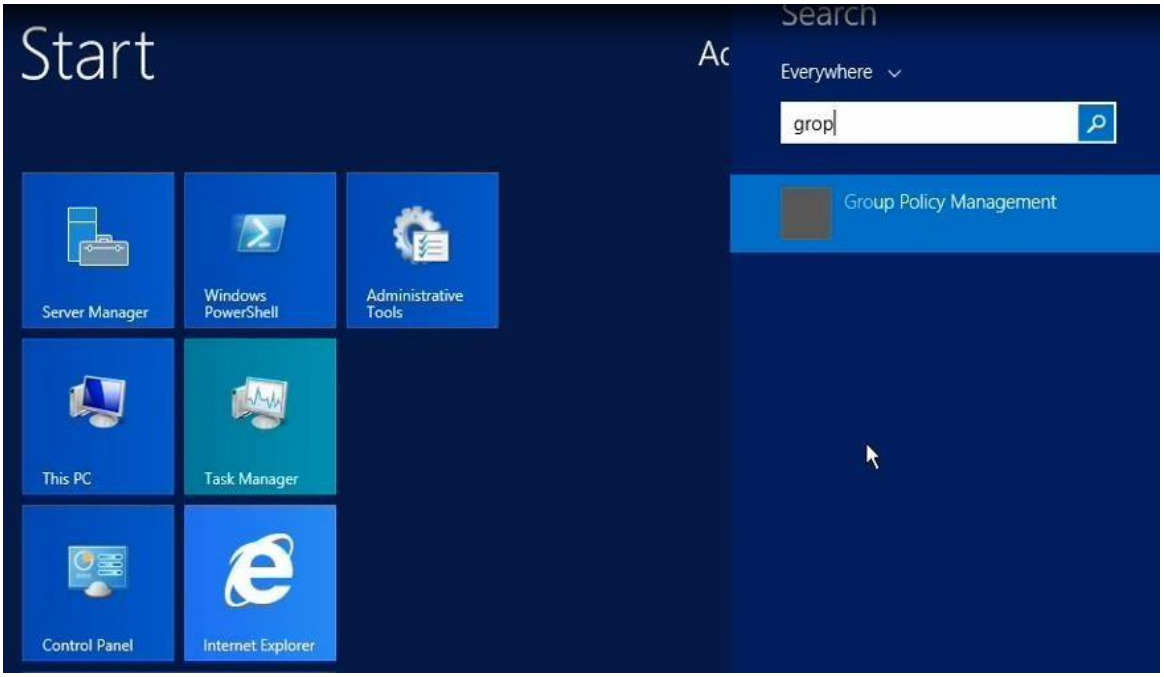
Ex.No 5 Implementing local policies and Group policies and user profiles

Aim

To implement local policies, Group policies and user profiles.

Components Required

1. A running PC
2. Windows sever 2012 with ADDS installed



Group Policy

A **Group Policy** is a computer or user setting that can be configured by administrators to apply various **computer specific** or **user specific registry settings** to computers that have joined the domain (active directory). A simple example of a group policy is the user password expiration policy which forces users to change their password on a regular basis.

A **Group Policy Object** (**GPO**) contains one or more group policy settings that can be applied to domain computers, users, or both. **GPO objects** are stored in **active directory**. You can open and configure GPO objects by using the **GPMC** (**Group Policy Management Console**) in Windows Server 2012:

Group Policy Settings are the actual configuration settings that can be applied to a domain computer or user. Most of the settings have three states, **Enabled**, **Disabled** and **Not Configured**.

Group Policy Management Editor provides access to hundreds of computer and user settings that can be applied to make many system changes to the desktop and server environment.

Group Policy Settings

Group Policy Settings are divided into **Computer Settings** and **User Settings**. **Computer Settings** are applied to computer when the system starts and this modifies the **HKEY Local Machine** hive of registry. **User Settings** are applied when the users log in to the computer and this modifies the **HKEY Local Machine** hive.

Computer Settings and **User Settings** both have policies and

preferences. These policies are:

Software Settings: Software can be deployed to **users** or **computer** by the administrator. The software deployed to users will be available only to those specific users whereas software deployed to a computer will be available to any user that on the specific computer where the **GPO** is applied.

Windows Settings: Windows settings can be applied to a user or a computer in order to modify the windows environment. Examples are: password policies, firewall policy, account lockout policy, scripts and so on.

Administrative Templates: Contains a number of user and computer settings that can be applied to control the windows environment of users or computers. For example, specifying the desktop wallpaper, disabling access to non-essential areas of the computers (e.g Network desktop icon, control panel etc), folder redirection and many more.

Preferences are a group policy extension that does the work which would otherwise require scripts. Preferences are used for both users and computers. You can use **preferences** to map network drives for users, map printers, configure internet options and more.

Creating and Applying Group Policy Objects
By default, GPOs **can be created and applied by** Domain Admins**,** Enterprise Admins **and** Group Policy Creator Owner **user groups. After creating the** GPO**, you can** apply **or** link **the GPOs to** sites**,** domains **or** Organizational Units **(**OUs**), however you cannot apply GPO to users, groups, or computers. GPOs are processed in following top to bottom order:**

1. **Local Group Policy**: Every windows operating system has local group policy installed by default. So this local group policy of the computer is applied at first.
2. **Site GPO**: The **GPOs** linked to the **Site** is then processed. By default, there is no site level group policy configured.
3. **Domain GPO**: Next, the **GPO** configured at **domain level** is processed. By default, GPO named

   default domain policy is applied at the domain level. This applies to all the objects of the domain.

If there is policy conflict between **domain** and **site level GPOs**, then GPO applied to **domain level**

takes the precedence.

4. **Organizational Unit GPO**: - In the end, **GPO** configured at **OU** is applied. If there is any conflict between previously applied GPOs, the GPO applied to **OU** takes the **most precedence** over **Domain**, **Site** and **Local Group Policy**.

set the **desktop wallpaper** for these two clients from a **group policy**:

Step 1: Open the **Group Policy Management Console** (**GPMC**) by going into **Server Manager>Tools**

and select **Group Policy Management** as shown.

Step 2: As the **GPMC** opens up, you will see the **tree hierarchy** of the **domain**. Now expand the domain, psg.com , and you will see the **Users OU** which is where our users reside. From here, **right-click** this **OU** and select the first option **Create a GPO in this domain and Link it here**:

Step 3: Now type the **Name** for this **GPO** object and click the **OK** button. We selected **WallPaper GPO**: Step 4: Next, **right-click** the **GPO object** and click **edit**:

Step 5: To find the **Desktop Wallpaper**, go to **Expand User Configuration> Policies> Administrative Templates> Desktop> Desktop**. At this point we should be able to see the setting in right window. **Right- click** the **Desktop Wallpaper** setting and select **Edit**:

Step 6: The settings of **Desktop Wallpaper** will now open. First we need to activate the policy by selecting the **Enabled** option on the left. Next, type the **UNC path** of shared wallpaper. Remember that we must **share the folder** that contains the wallpaper and configure the **share permission** so that users can access it. Notice that we can even select to **center** our wallpaper (**Wallpaper Style**). When ready click **Apply** and then **OK**:

Step 7: Now that we've configured our GPO, we need to apply it. To do so, we can simply log off and log back in the client computer or type following command in domain controller's command prompt to apply the settings immediately:

Step 8: As we can see below, our user's desktop now has the background image configured in the group policy we created:

PROCEDURE FOR SETTING PASSWORD POLICY:-

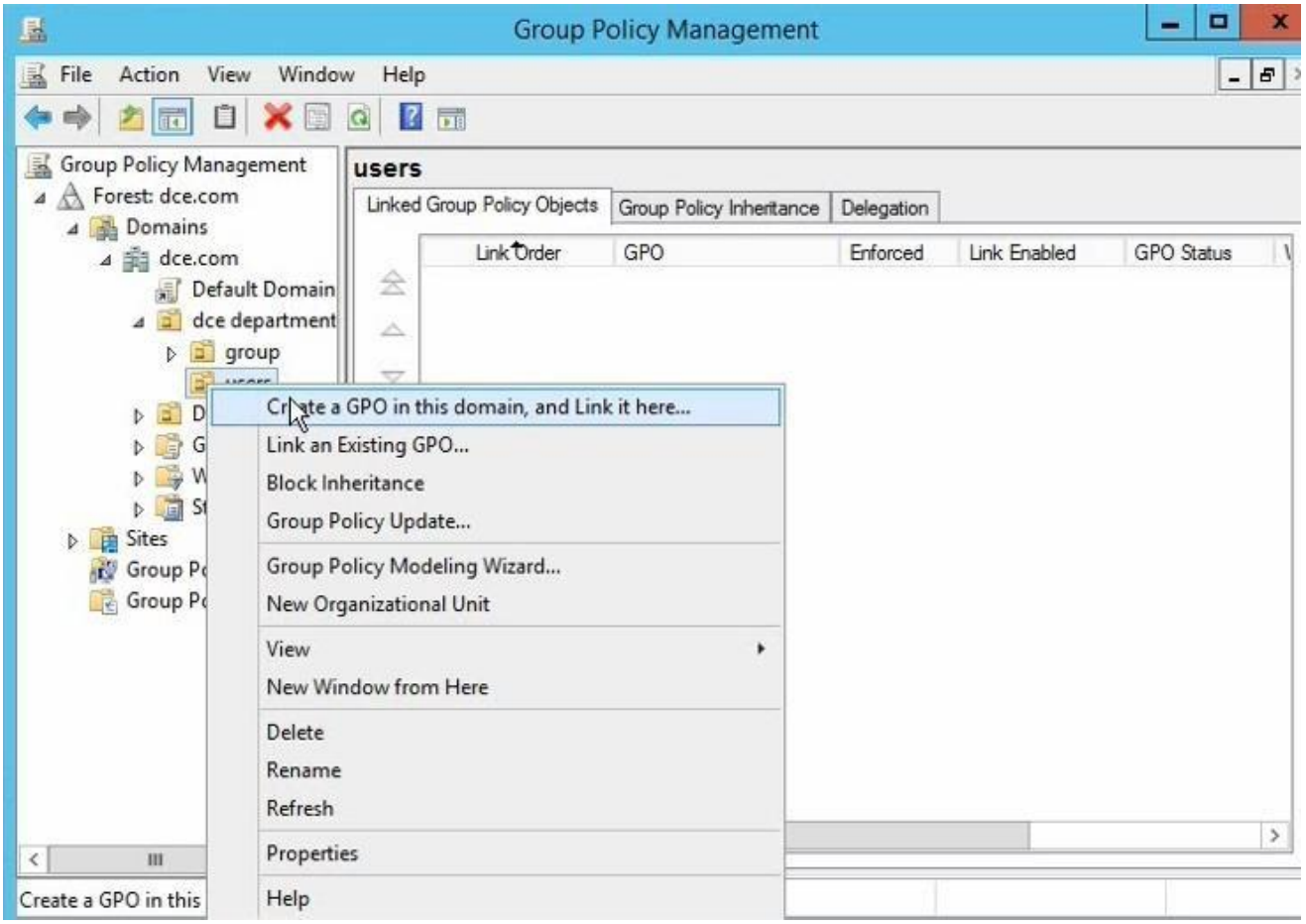
Password Policy ensures that a user password is strong and is changed in a periodic manner so that it becomes highly impossible for an attacker to crack the password.

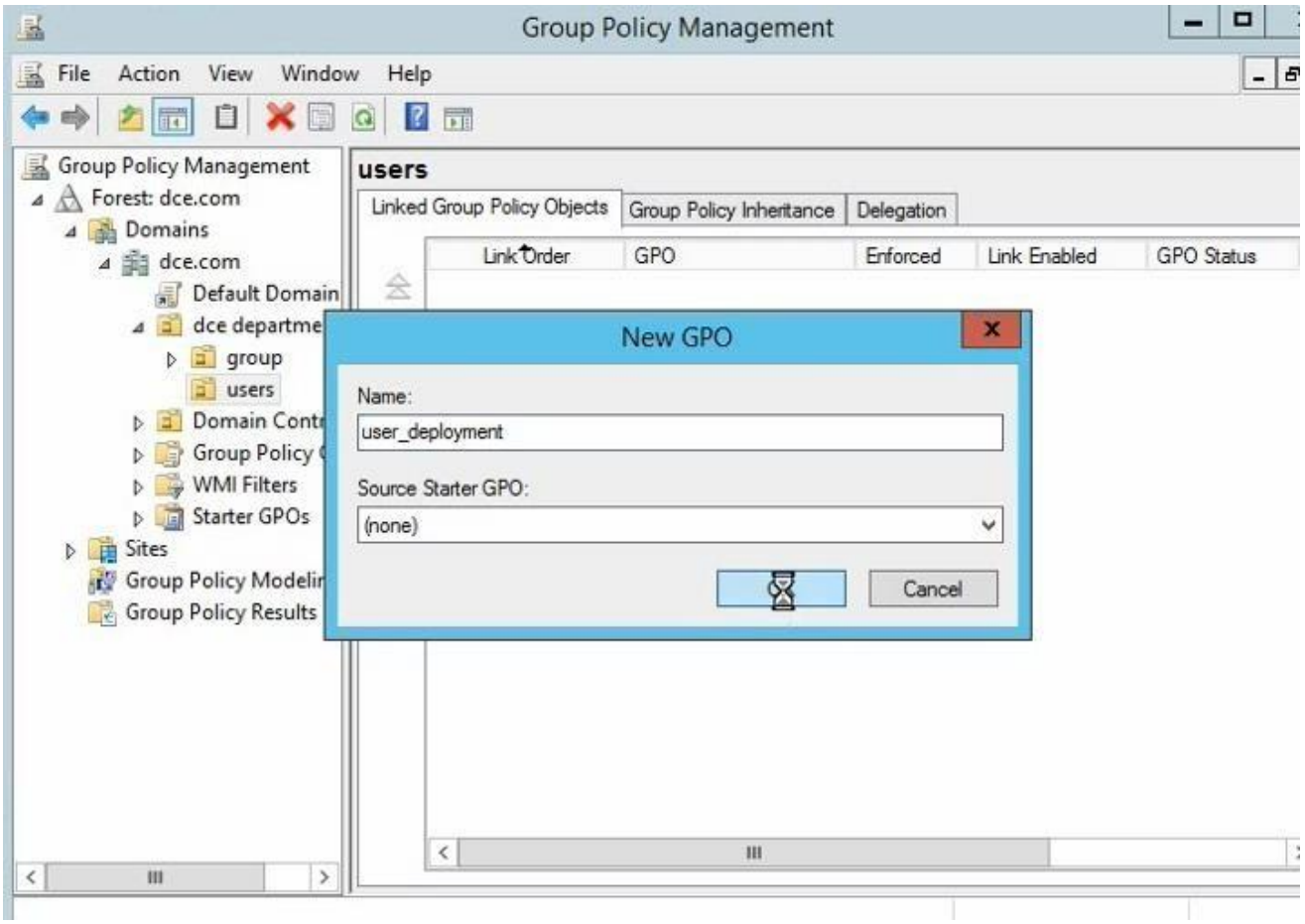
To edit Password Policy settings:

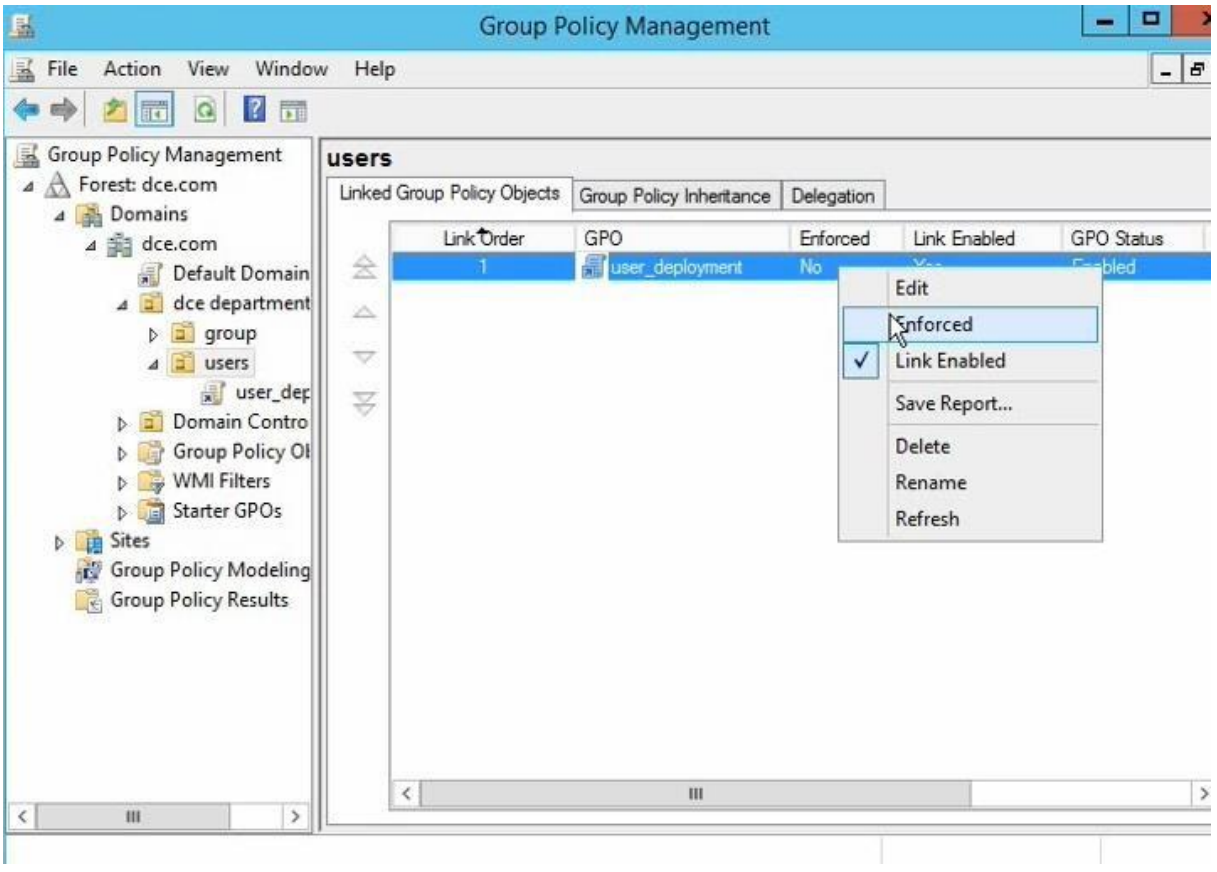
- Go to Start Menu → Administrative Tools → Group Policy Management
- In the console tree, expand the Forest and then Domains. Select the domain for which the Account policies have to be set
- Double-click the domain to reveal the GPOs linked to the domain.
- Right-click Default Domain Policy and select Edit. A Group Policy Editor console will open.

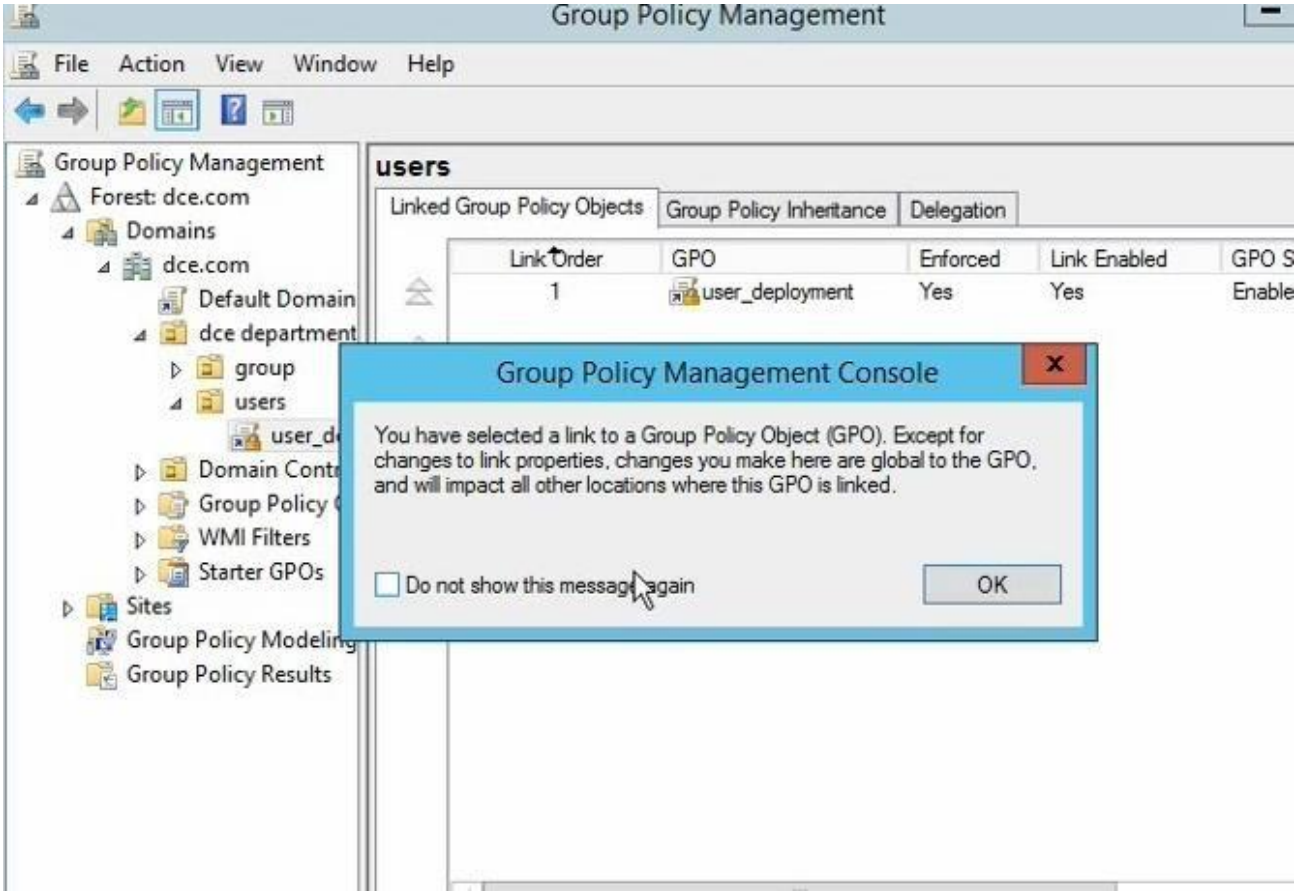
- Now, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy
- Double-click Password Policy to reveal the six password settings available in AD. Right-click any one of these settings and select Properties to define the policy setting
- The Properties dialog box of each policy setting will have two tabs. The Security Policy Setting tab is where the value for that setting is set. The Explain tab gives a brief description about the policy setting and its default values

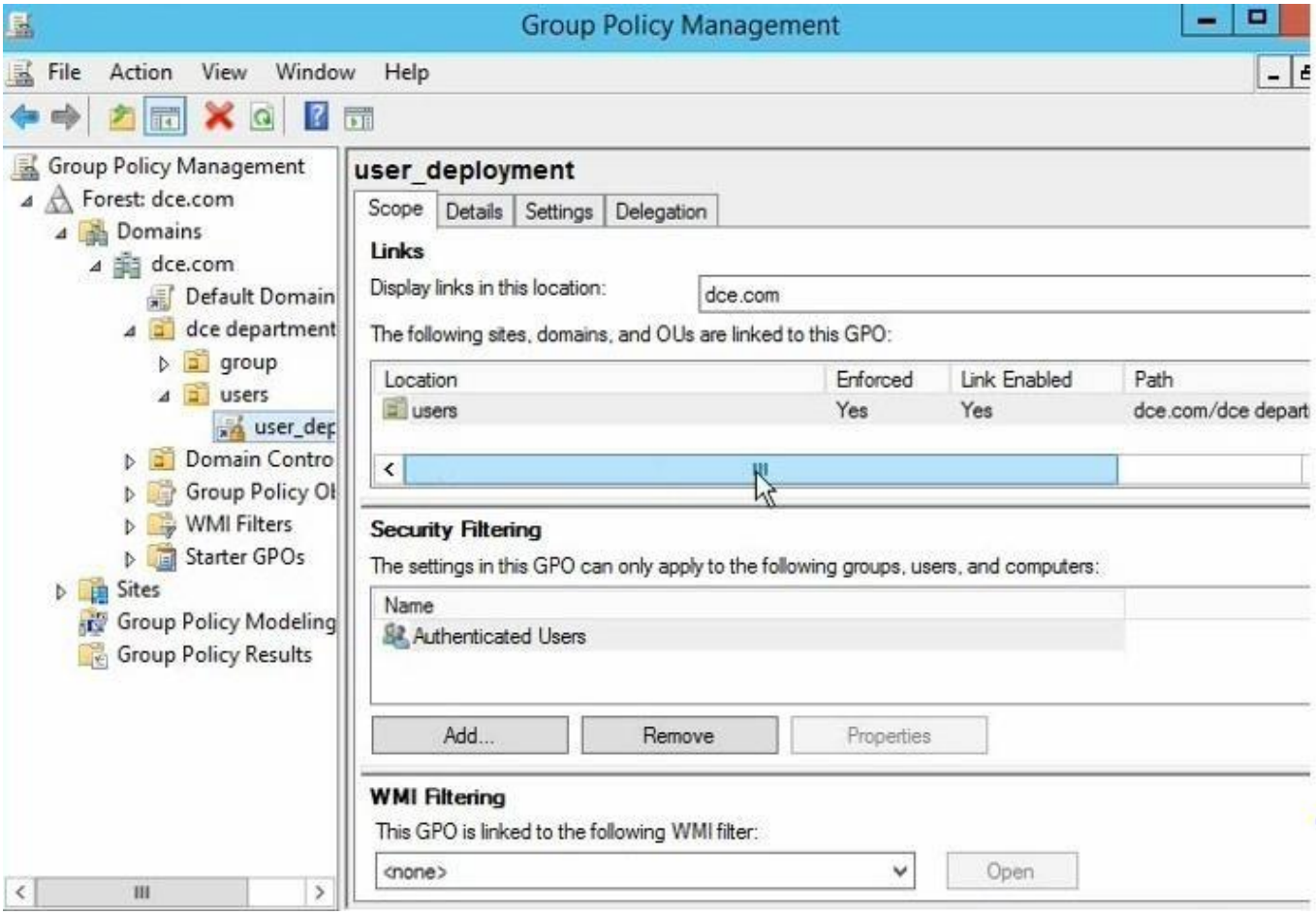
- In the Security Policy Setting tab, check the Define this Policy Setting check box and enter the desired value. Click Apply and then OK

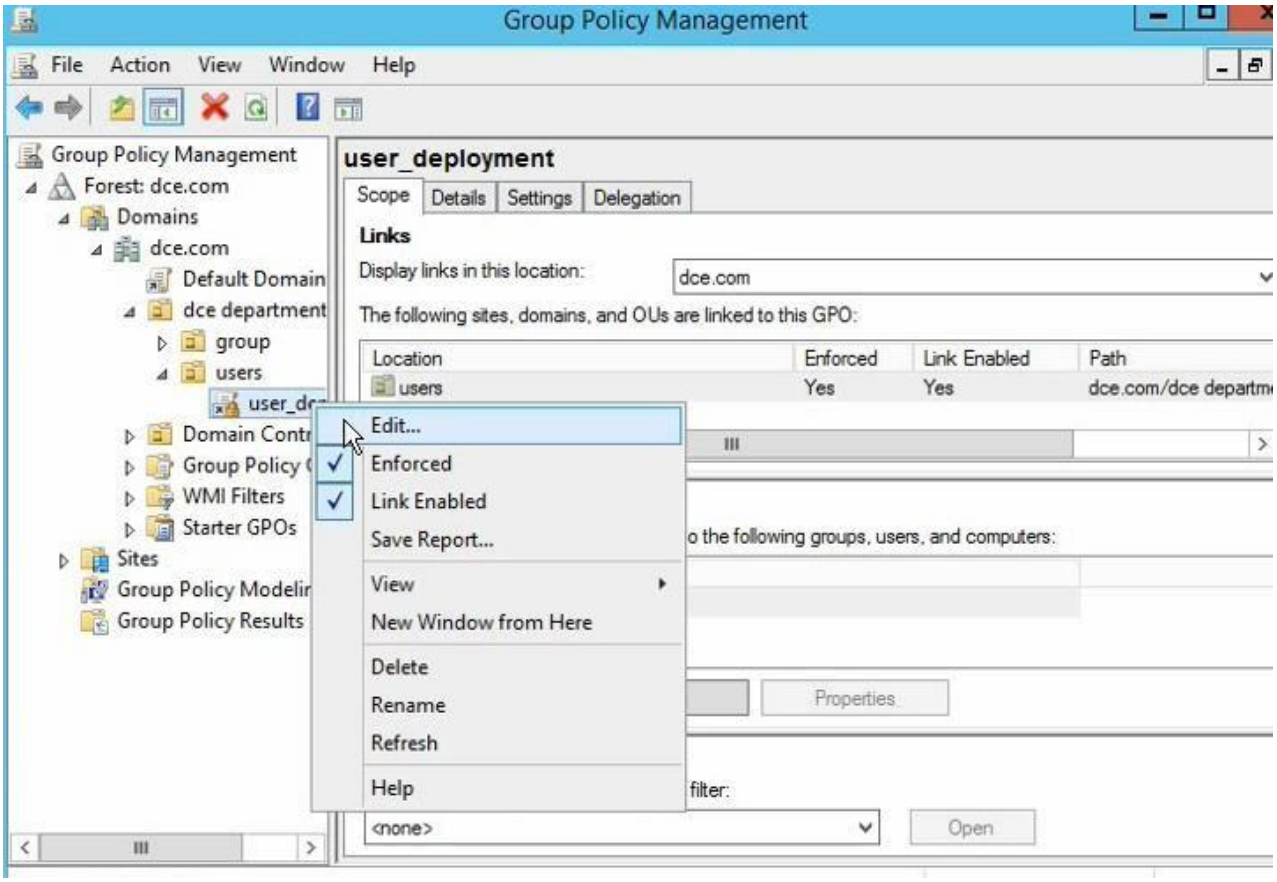


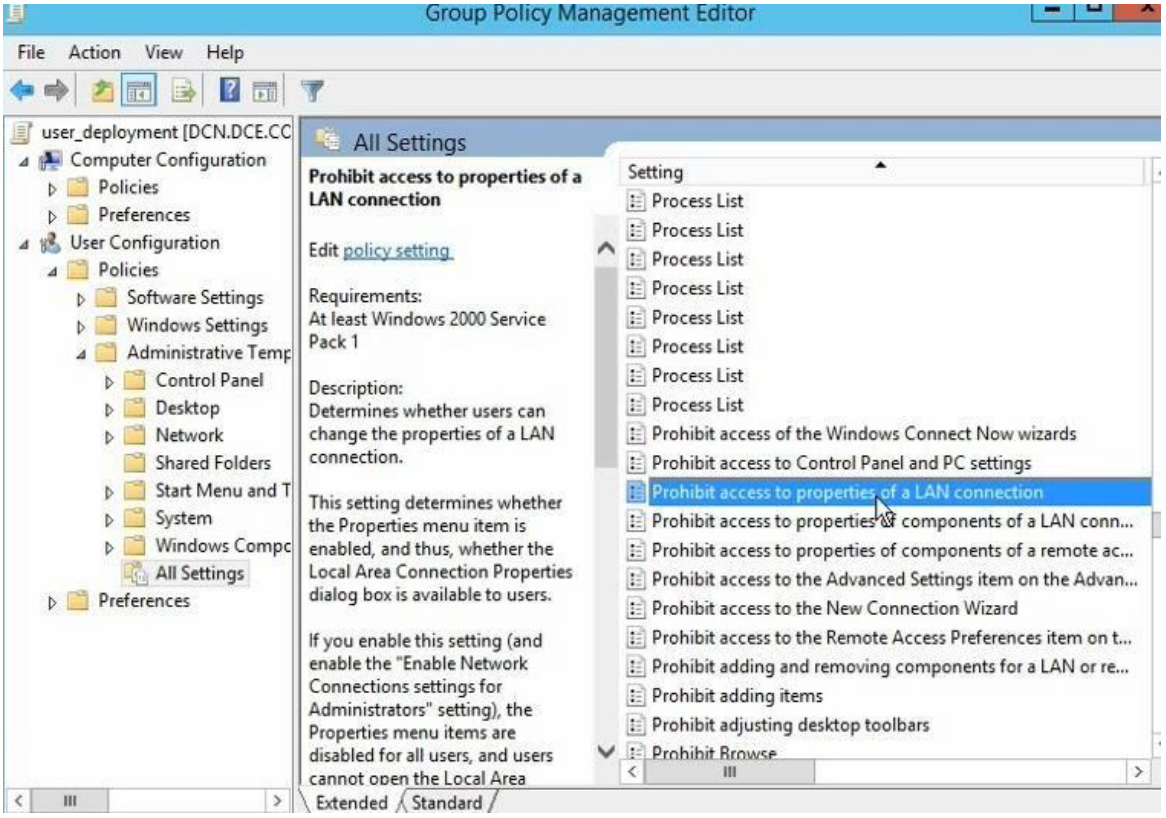

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dce.com
Domains
dce.com
Default Domain
dce departme
group
users
Domain Contr
Group Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modelir
Group Policy Results
users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
New GPO
Name:
user_deployment
Source Starter GPO:
(none)
Cancel

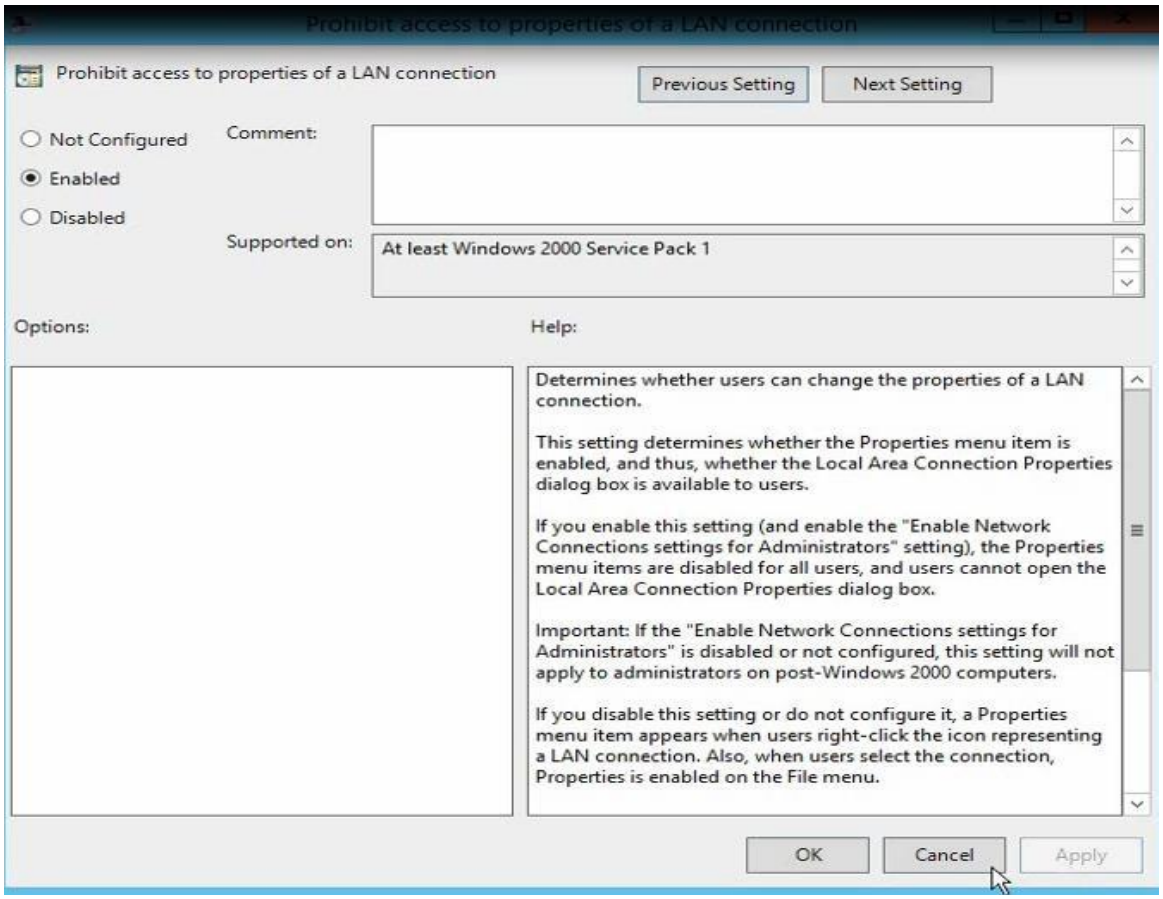

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dce.com
Domains
dce.com
Default Domain
dce department
group
users
user_dep
Domain Contro
Group Policy Ob
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1
user_deployment
No
Edit
Enforced
Link Enabled
Save Report...
Delete
Rename
Refresh

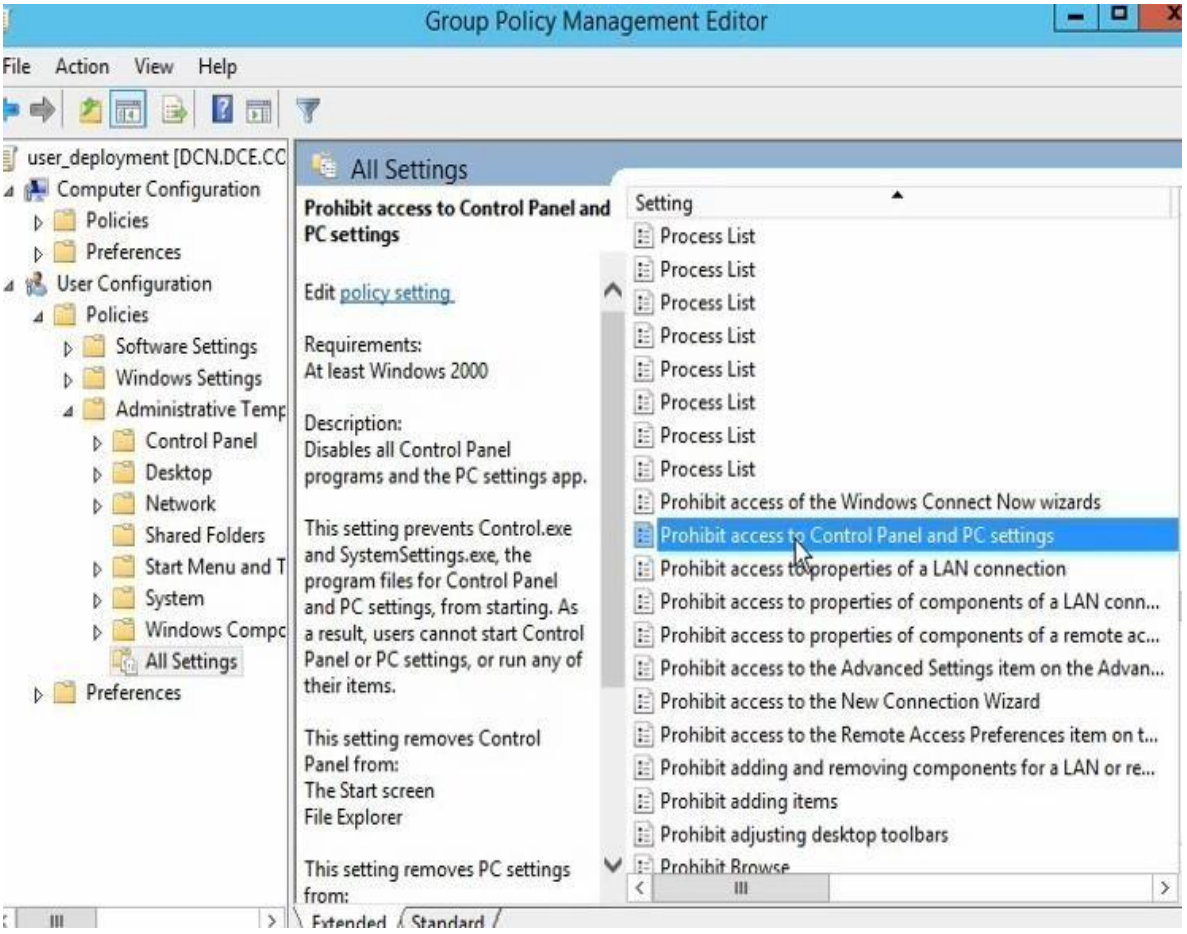

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dce.com
Domains
dce.com
Default Domain
dce department
group
users
Domain Cont
Group Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
users
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO S
1
user_deployment
Yes
Yes
Enable
Group Policy Management Console
You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO, and will impact all other locations where this GPO is linked.
Do not show this message again
OK

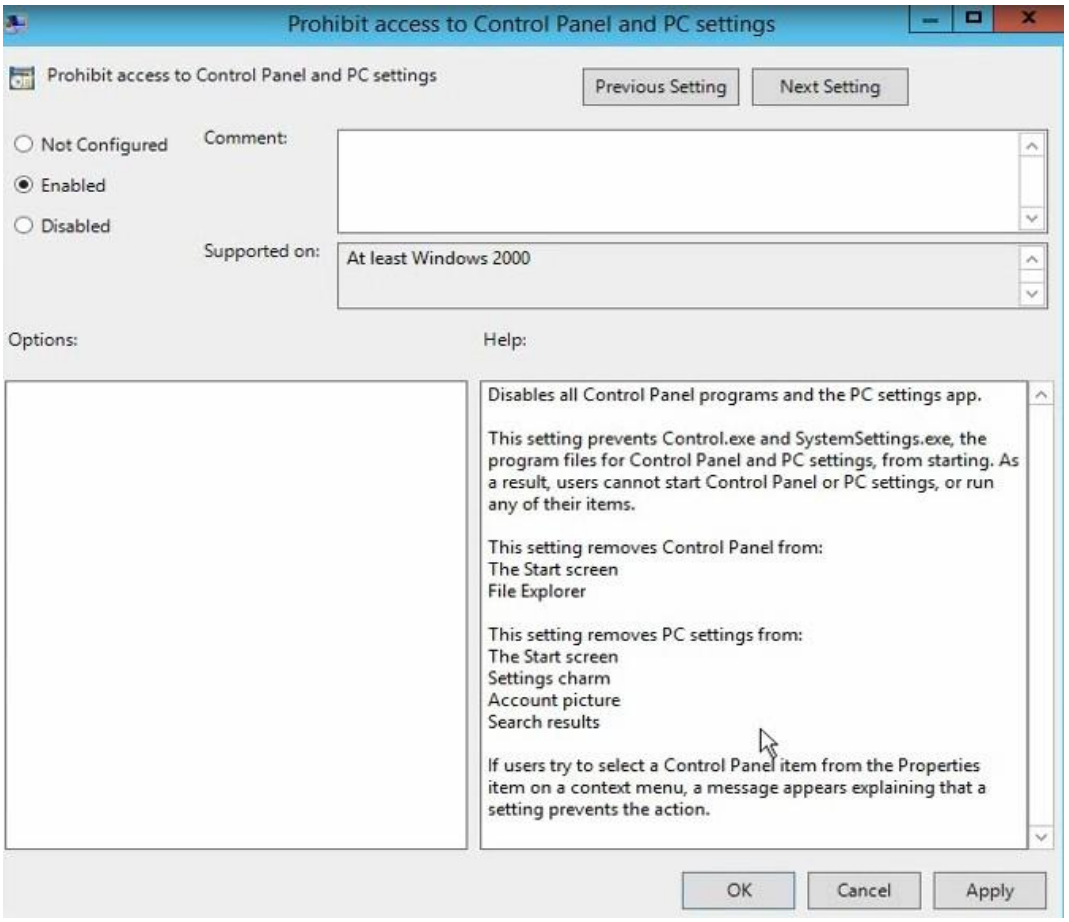

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dce.com
Domains
dce.com
Default Domain
dce department
group
users
Domain Contro
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
user_deployment
Scope
Details
Settings
Delegation
Links
Display links in this location:
dce.com
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
users
Yes
Yes
dce.com/dce depart
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open

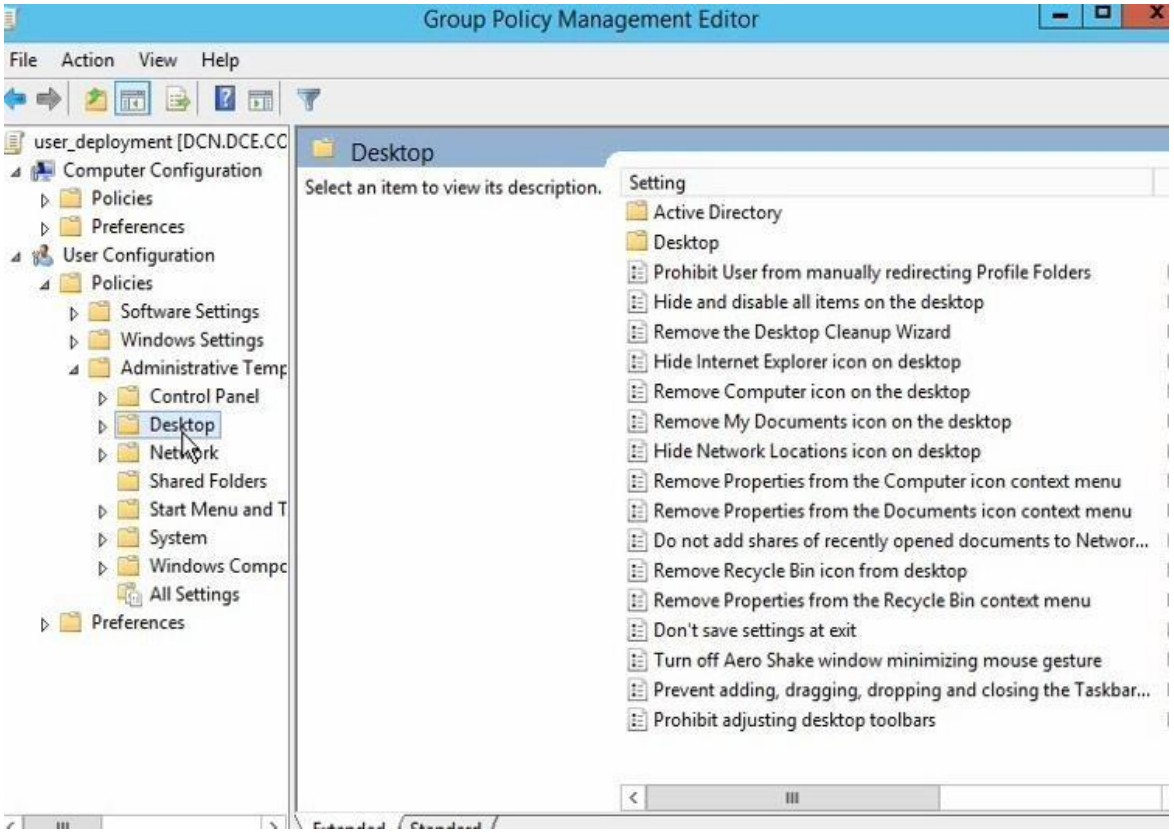

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dce.com
Domains
dce.com
Default Domain
dce department
group
users
Domain Contr
Group Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modelir
Group Policy Results
user_deployment
Scope Details Settings Delegation
Links
Display links in this location:
dce.com
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
users Yes Yes dce.com/dce departm
Edit...
Enforced
Link Enabled
Save Report...
View
New Window from Here
Delete
Rename
Refresh
Help
o the following groups, users, and computers:
Properties
filter:
<none>
Open

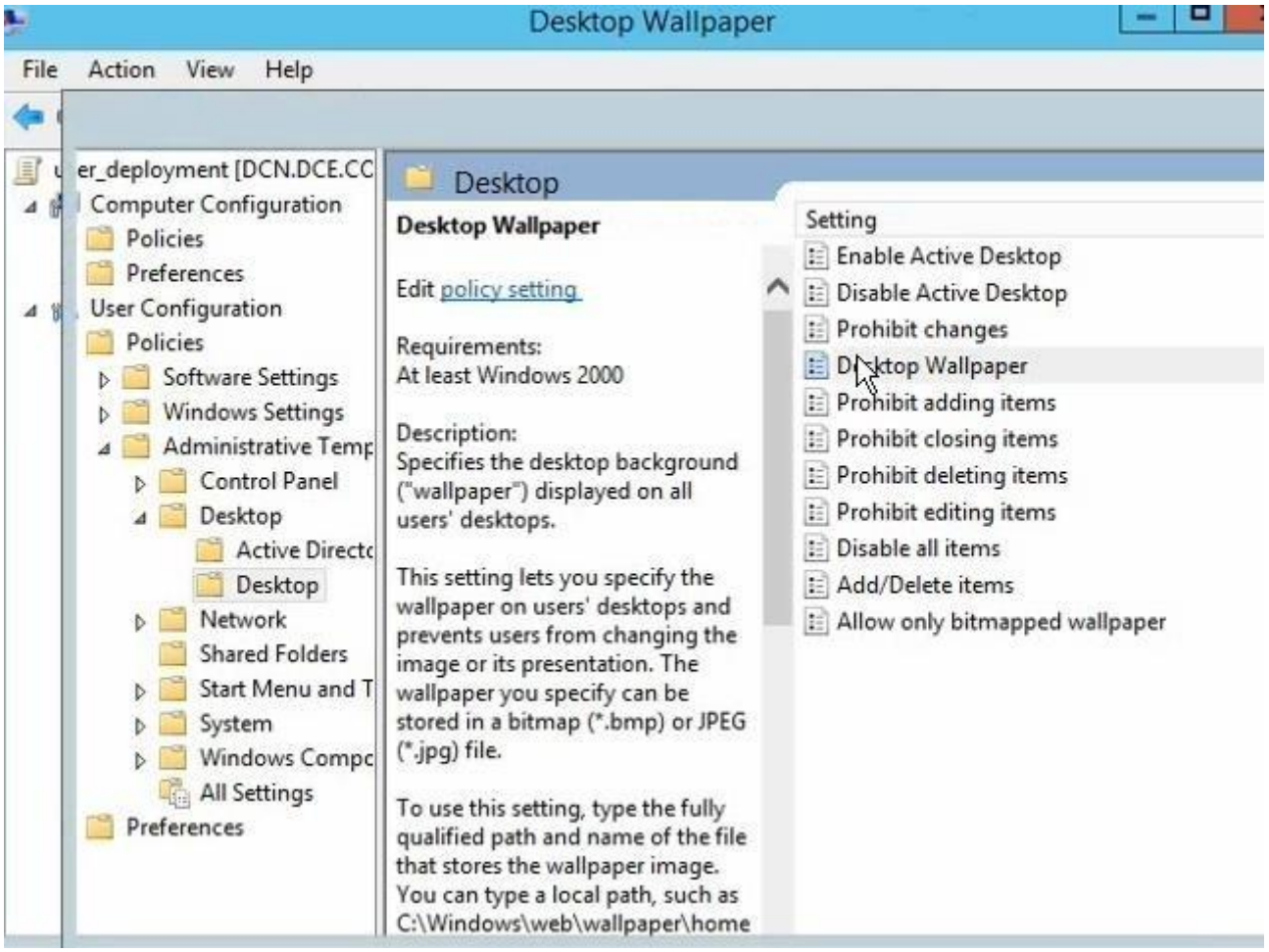

Group Policy Management Editor
File Action View Help
user_deployment [DCN.DCE.CC
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
All Settings
Prohibit access to properties of a LAN connection
Edit policy setting
Requirements:
At least Windows 2000 Service Pack 1
Description:
Determines whether users can change the properties of a LAN connection.
This setting determines whether the Properties menu item is enabled, and thus, whether the Local Area Connection Properties dialog box is available to users.
If you enable this setting (and enable the "Enable Network Connections settings for Administrators" setting), the Properties menu items are disabled for all users, and users cannot open the Local Area
Setting
Process List
Process List
Process List
Process List
Process List
Process List
Process List
Process List
Prohibit access of the Windows Connect Now wizards
Prohibit access to Control Panel and PC settings
Prohibit access to properties of a LAN connection
Prohibit access to properties of components of a LAN conn...
Prohibit access to properties of components of a remote ac...
Prohibit access to the Advanced Settings item on the Advan...
Prohibit access to the New Connection Wizard
Prohibit access to the Remote Access Preferences item on t...
Prohibit adding and removing components for a LAN or re...
Prohibit adding items
Prohibit adjusting desktop toolbars
Prohibit Browse
Extended Standard

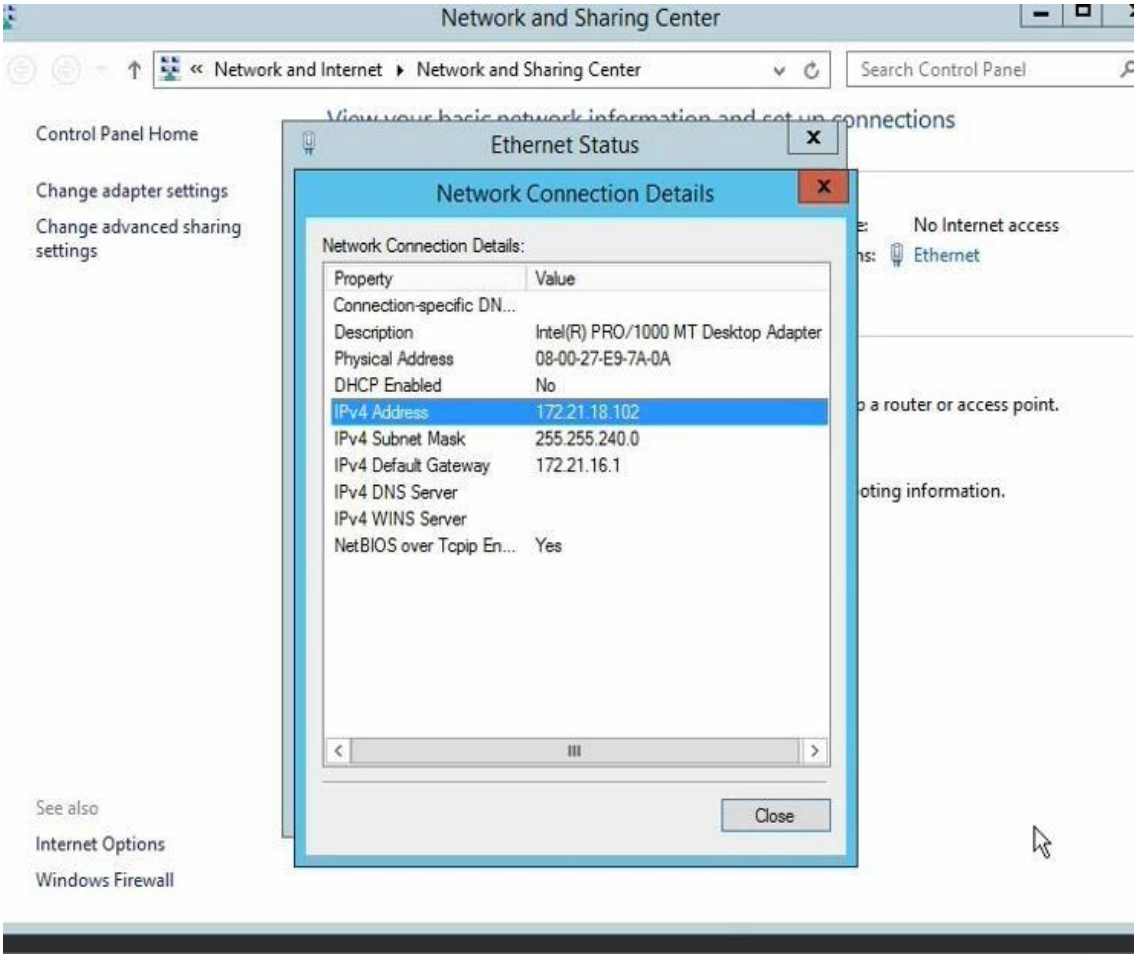

Prohibit access to properties of a LAN connection
Prohibit access to properties of a LAN connection
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000 Service Pack 1
Options:
Help:
Determines whether users can change the properties of a LAN connection.
This setting determines whether the Properties menu item is enabled, and thus, whether the Local Area Connection Properties dialog box is available to users.
If you enable this setting (and enable the "Enable Network Connections settings for Administrators" setting), the Properties menu items are disabled for all users, and users cannot open the Local Area Connection Properties dialog box.
Important: If the "Enable Network Connections settings for Administrators" is disabled or not configured, this setting will not apply to administrators on post-Windows 2000 computers.
If you disable this setting or do not configure it, a Properties menu item appears when users right-click the icon representing a LAN connection. Also, when users select the connection, Properties is enabled on the File menu.
OK
Cancel
Apply

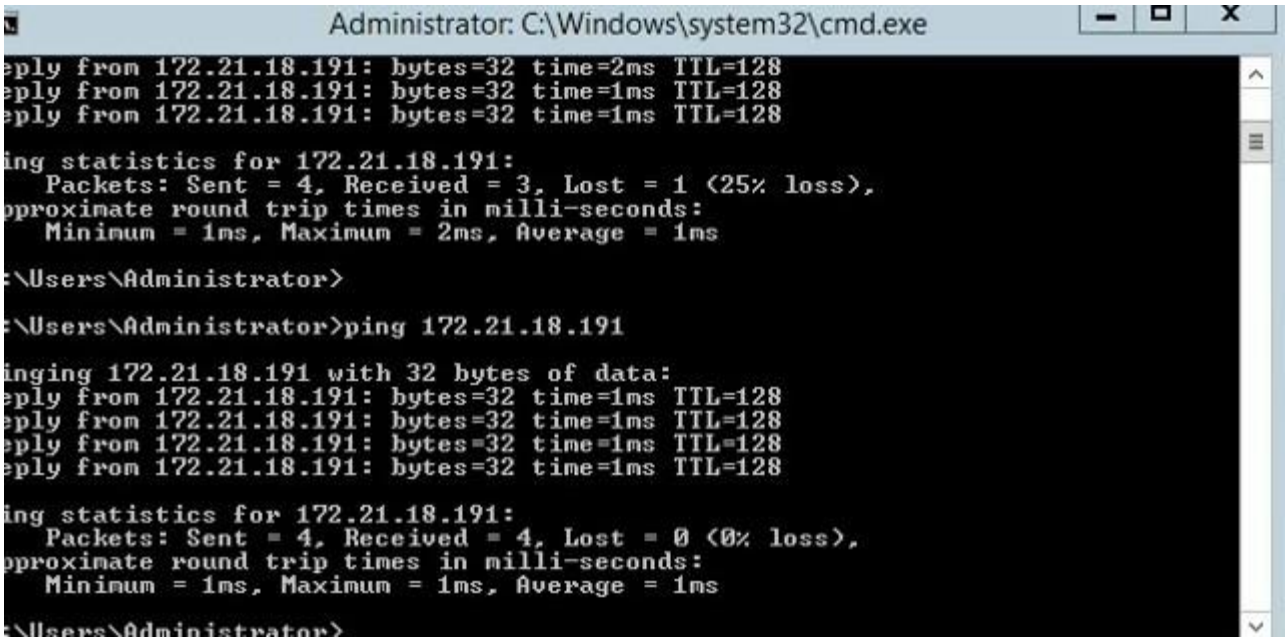

Group Policy Management Editor
File Action View Help
user_deployment [DCN.DCE.CC
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
All Settings
Prohibit access to Control Panel and PC settings
Edit policy setting
Requirements:
At least Windows 2000
Description:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control Panel from:
The Start screen
File Explorer
This setting removes PC settings from:
Setting
Process List
Process List
Process List
Process List
Process List
Process List
Process List
Process List
Prohibit access of the Windows Connect Now wizards
Prohibit access to Control Panel and PC settings
Prohibit access to properties of a LAN connection
Prohibit access to properties of components of a LAN conn...
Prohibit access to properties of components of a remote ac...
Prohibit access to the Advanced Settings item on the Advan...
Prohibit access to the New Connection Wizard
Prohibit access to the Remote Access Preferences item on t...
Prohibit adding and removing components for a LAN or re...
Prohibit adding items
Prohibit adjusting desktop toolbars
Prohibit Browse
Extended
Standard


Prohibit access to Control Panel and PC settings
Prohibit access to Control Panel and PC settings
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000
Options:
Help:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control Panel from:
The Start screen
File Explorer
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results
If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.
OK
Cancel
Apply


Group Policy Management Editor
File
Action
View
Help
user_deployment [DCN.DCE.CC
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
Desktop
Select an item to view its description.
Setting
Active Directory
Desktop
Prohibit User from manually redirecting Profile Folders
Hide and disable all items on the desktop
Remove the Desktop Cleanup Wizard
Hide Internet Explorer icon on desktop
Remove Computer icon on the desktop
Remove My Documents icon on the desktop
Hide Network Locations icon on desktop
Remove Properties from the Computer icon context menu
Remove Properties from the Documents icon context menu
Do not add shares of recently opened documents to Networ...
Remove Recycle Bin icon from desktop
Remove Properties from the Recycle Bin context menu
Don't save settings at exit
Turn off Aero Shake window minimizing mouse gesture
Prevent adding, dragging, dropping and closing the Taskbar...
Prohibit adjusting desktop toolbars


Desktop Wallpaper
File Action View Help
er_deployment [DCN.DCE.CC
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Active Directc
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
Desktop
Desktop Wallpaper
Edit policy setting
Requirements:
At least Windows 2000
Description:
Specifies the desktop background ("wallpaper") displayed on all users' desktops.
This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.
To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home
Setting
Enable Active Desktop
Disable Active Desktop
Prohibit changes
Desktop Wallpaper
Prohibit adding items
Prohibit closing items
Prohibit deleting items
Prohibit editing items
Disable all items
Add/Delete items
Allow only bitmapped wallpaper


Network and Sharing Center
Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Ethernet Status
Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DN...
Description
Intel(R) PRO/1000 MT Desktop Adapter
Physical Address
08-00-27-E9-7A-0A
DHCP Enabled
No
IPv4 Address
172.21.18.102
IPv4 Subnet Mask
255.255.240.0
IPv4 Default Gateway
172.21.16.1
IPv4 DNS Server
IPv4 WINS Server
NetBIOS over Tcpip En...
Yes
Close
No Internet access
Ethernet
See also
Internet Options
Windows Firewall



Result

Thus, the local policies and Group policies and user profiles was implemented.

Ex.No 6 **Implement Security using Encryption and Firewall**

Aim

To Implement Security using Encryption and Firewall.

Components Required

1.PC

File and Disk Encryption Using Bitlocker

BitLocker provides fix drive encryption, operating system drive encryption and Removable drive encryption. For OS drive encryption, Bitlocker uses a Trusted Platform Module (TPM). In case when the system doesn't have TPM, the user can use an additional method using USB or Network Unlock to enable Bitlocker. The Bitlocker to go is for removable drive.

BitLocker is Microsoft's disk encryption and security tool, integrated into Windows 10 Pro and Enterprise versions. The program enables Windows 10 users to encrypt an entire computer hard drive or removable storage disk, to protect the drive contents from malicious offline attacks. Windows BitLocker uses the AES algorithm with 256 or 128-bit key encrypt all the content in your disk.

This disk encryption prevents unauthorized users from reading, extracting, modifying or retrieving data in event of device theft or loss. To access and decrypt the data, the user must use the correct recovery key.

Install BitLocker Encryption

By default, the BitLocker is not installed in Windows Server. User should install it from the server manager, or using the install-WindowsFeature PowerShell command line.

1. From the **Server Manager dashboard**, click **Manage** then click **Add Roles and Features** to open the **Add Roles and Features Wizard**.

2. On the Before you begin page click Next.

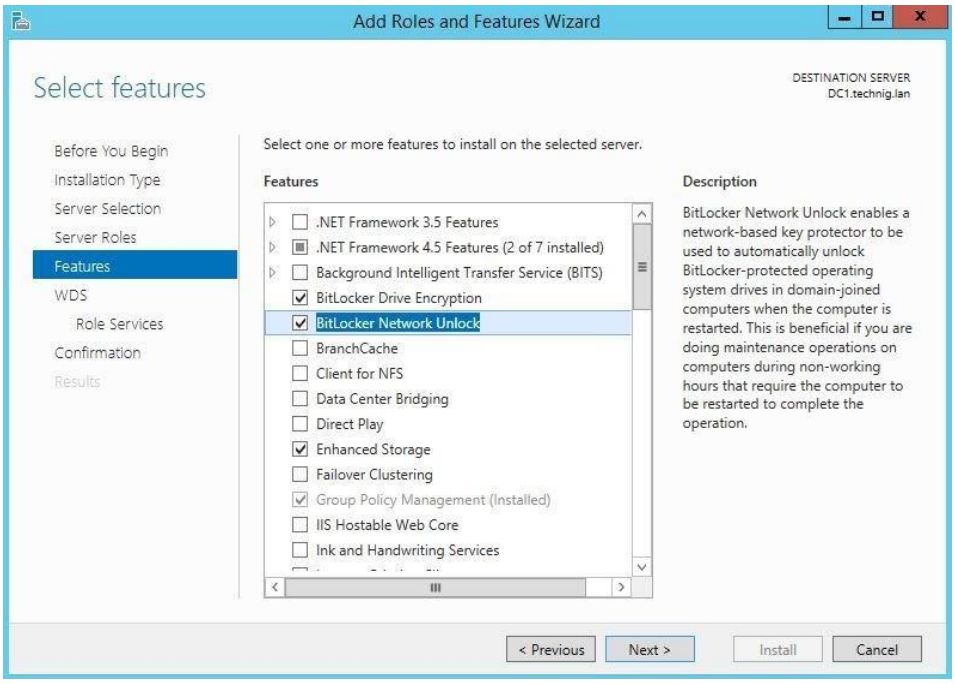
3. On the **Installation Type** page, select **Role-based or feature-based installation** and hit **Next**. On the

Server Selection page click **Next** also**.**

4. Leave the default and click **Next** on the **Server Roles** page.

5. On the **Features,** page select **BitLocker Drive Encryption** and **BitLocker Network Unlock.**

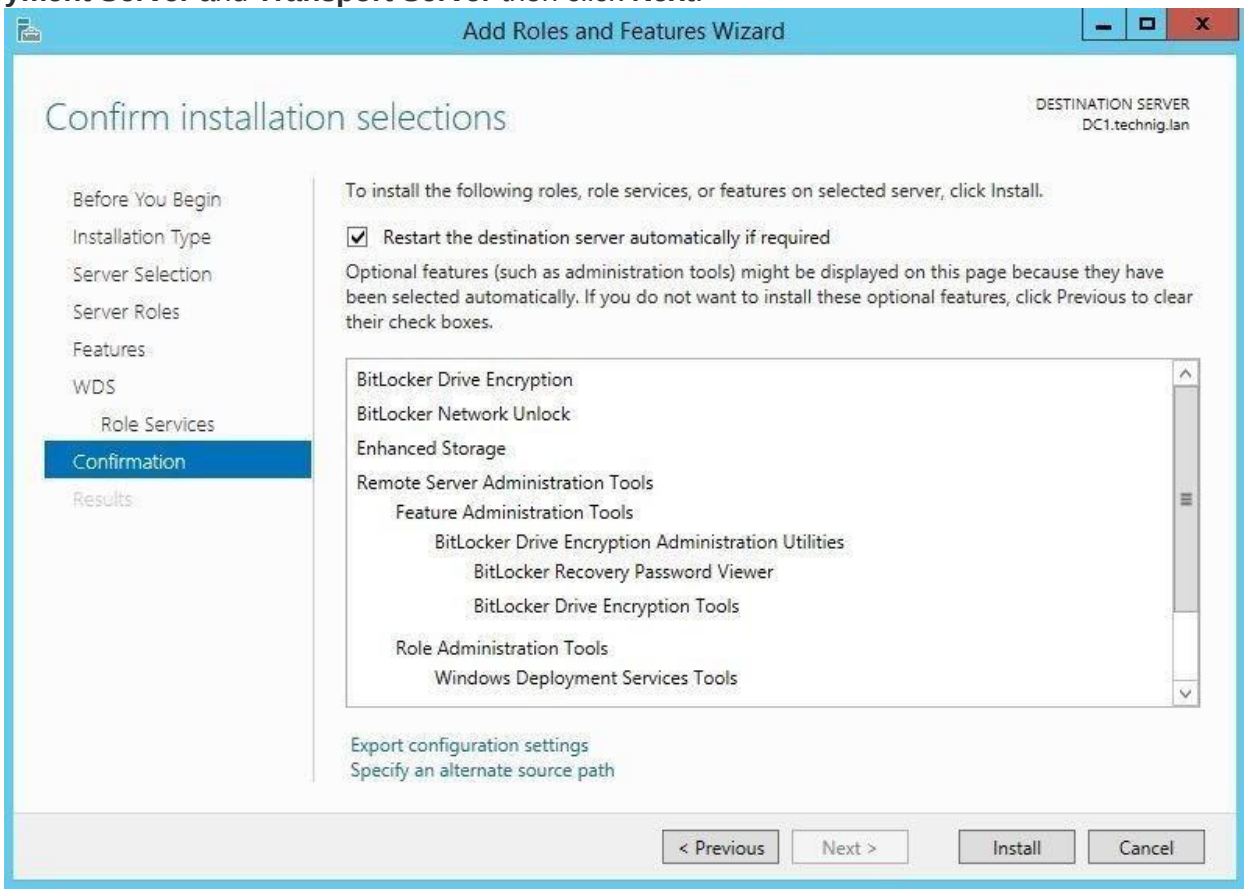
Add the required features also then click **Next**.



File and Disk Encryption Using BitLocker Drive Encryption

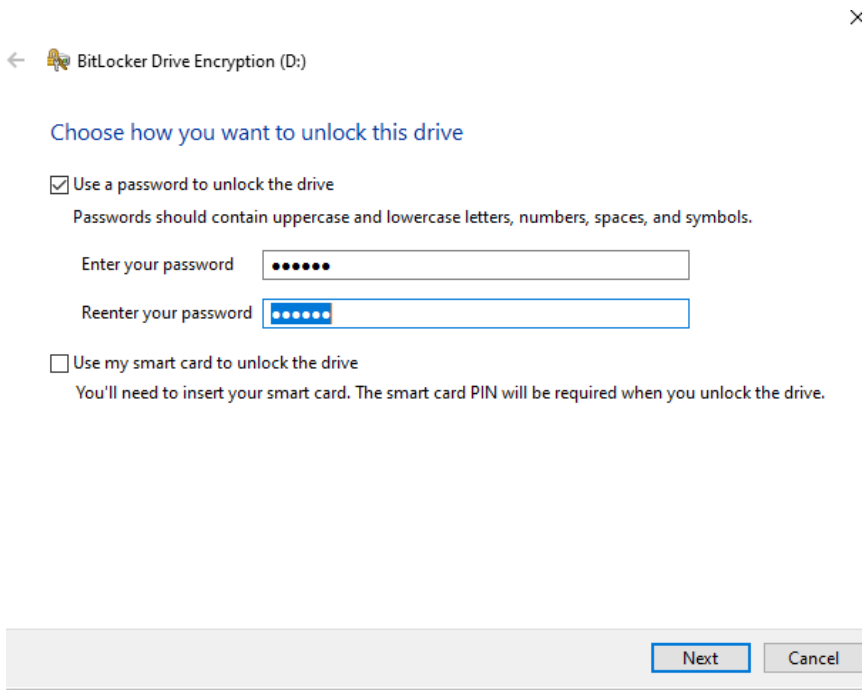
6. Click **Next** on the **WDS** page and go to the **Role Services** page, on the Role Services page select

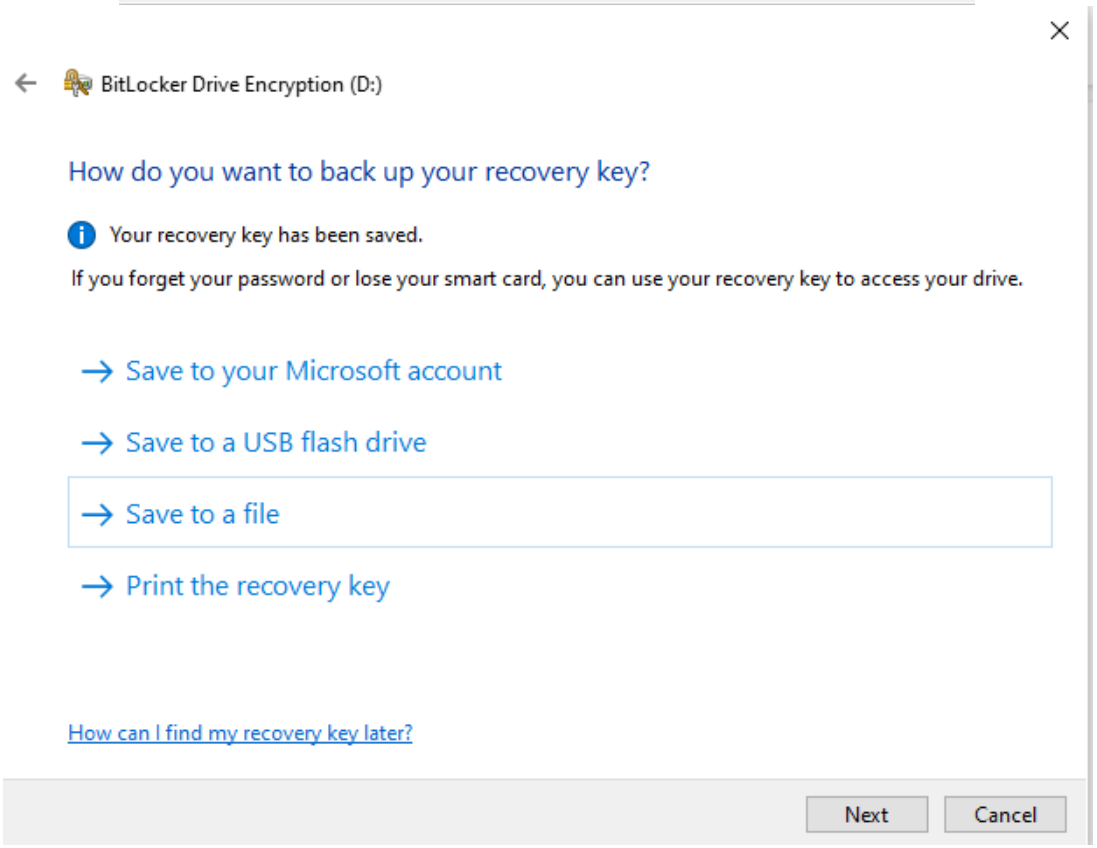
Deployment Server and **Transport Server** then click **Next**.

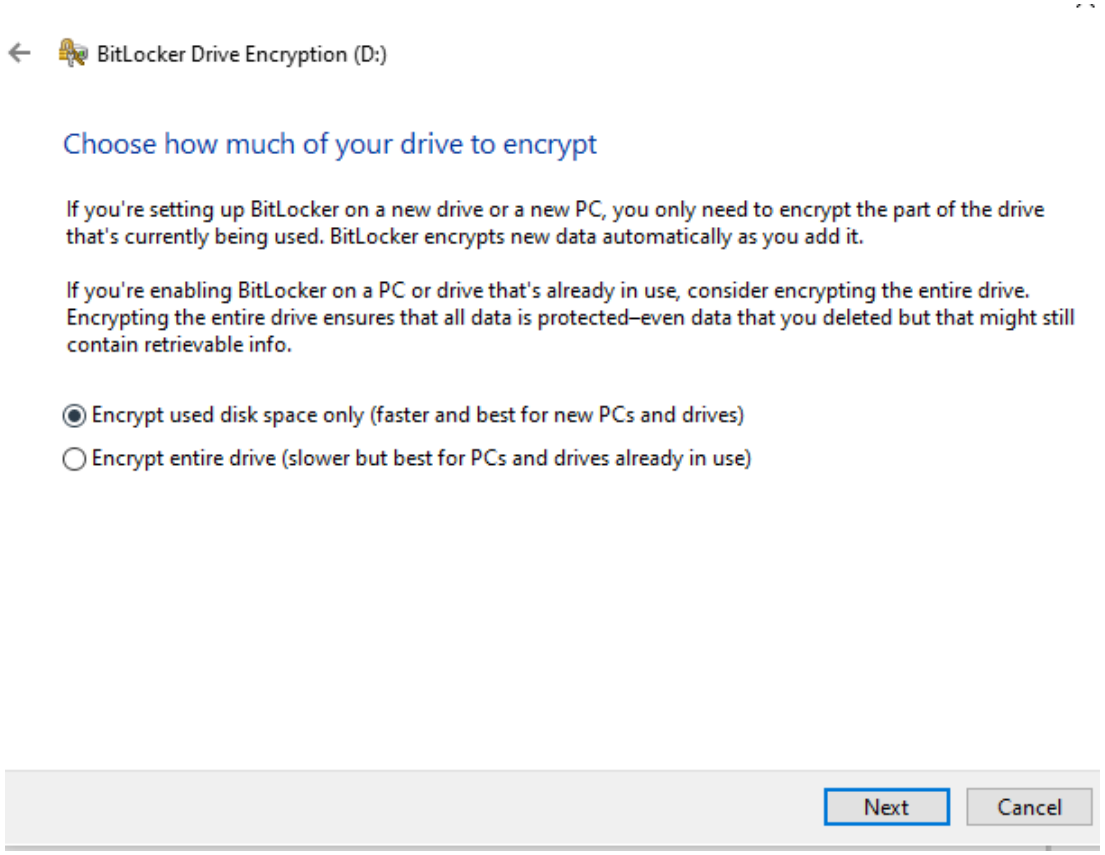


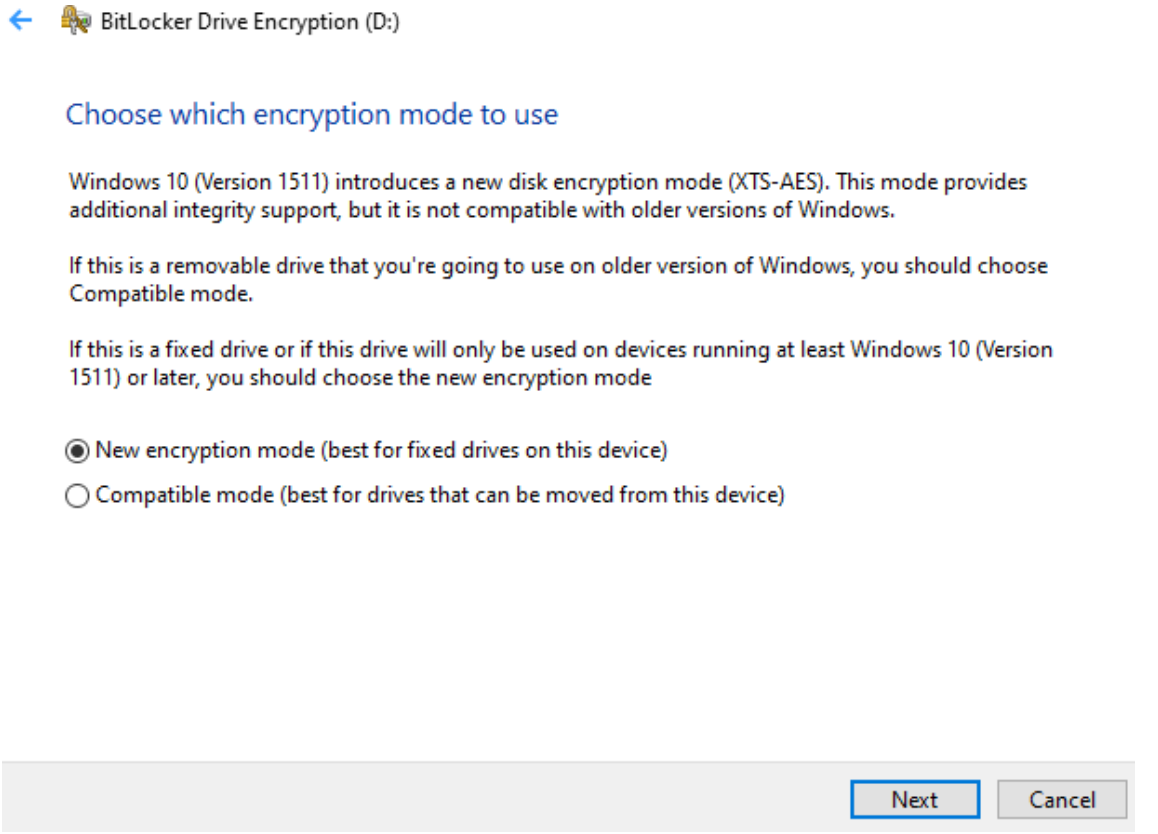
Disk Encryption Using BitLocker Network Unlock

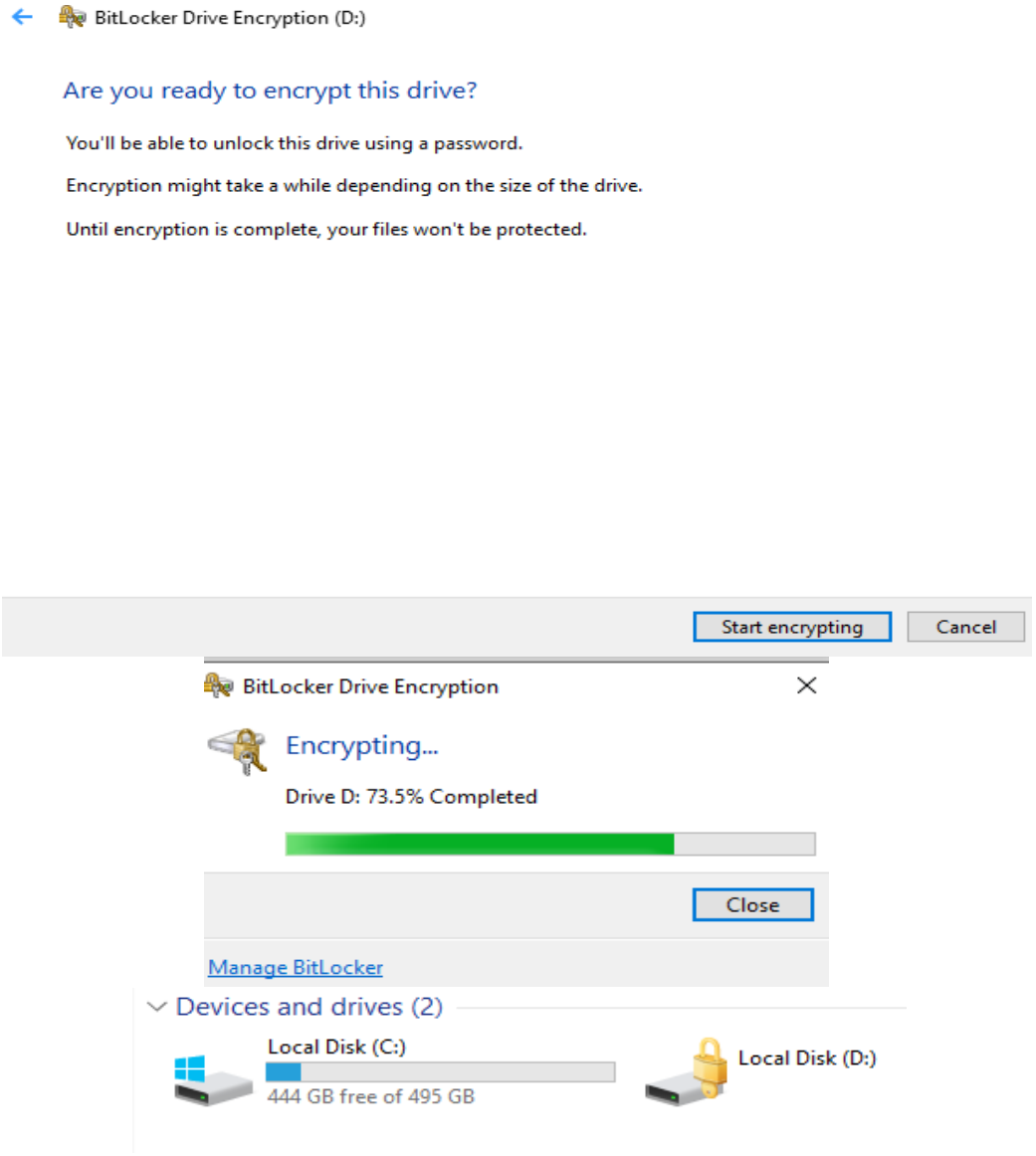
7. On the **Confirmation** page tick the **Restart the destination server automatically if required** option then clicks Install and let the installation process finished successfully. After the installation, the system will restart and Close the installation page.


BitLocker Drive Encryption (D:)
Choose how you want to unlock this drive
Use a password to unlock the drive
Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.
Enter your password
Reenter your password
Use my smart card to unlock the drive
You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.
Next
Cancel


BitLocker Drive Encryption (D:)
How do you want to back up your recovery key?
Your recovery key has been saved.
If you forget your password or lose your smart card, you can use your recovery key to access your drive.
Save to your Microsoft account
Save to a USB flash drive
Save to a file
Print the recovery key
How can I find my recovery key later?
Next
Cancel


BitLocker Drive Encryption (D:)
Choose how much of your drive to encrypt
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.
Encrypt used disk space only (faster and best for new PCs and drives)
Encrypt entire drive (slower but best for PCs and drives already in use)
Next
Cancel


BitLocker Drive Encryption (D:)
Choose which encryption mode to use
Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.
If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode
New encryption mode (best for fixed drives on this device)
Compatible mode (best for drives that can be moved from this device)
Next
Cancel



Firewall

A firewall is a piece of hardware or software that controls the flow of data packets, and it is critical on modern computer systems. It protects private networks and devices from malicious actions coming from public networks in the same way a physical firewall prevents fire from spreading from one area to another. A firewall acts as a defense mechanism which controls network traffic according to the implemented firewall rules.

Computers behind a firewall cannot receive data until the data passes all filters. This enhances security by a large margin and reduces the risk of unauthorized access to private networks. A proper firewall configuration

provides your system with a crucial layer of security and lowers the risk of successful hacking attacks. Firewalls can perform many tasks:

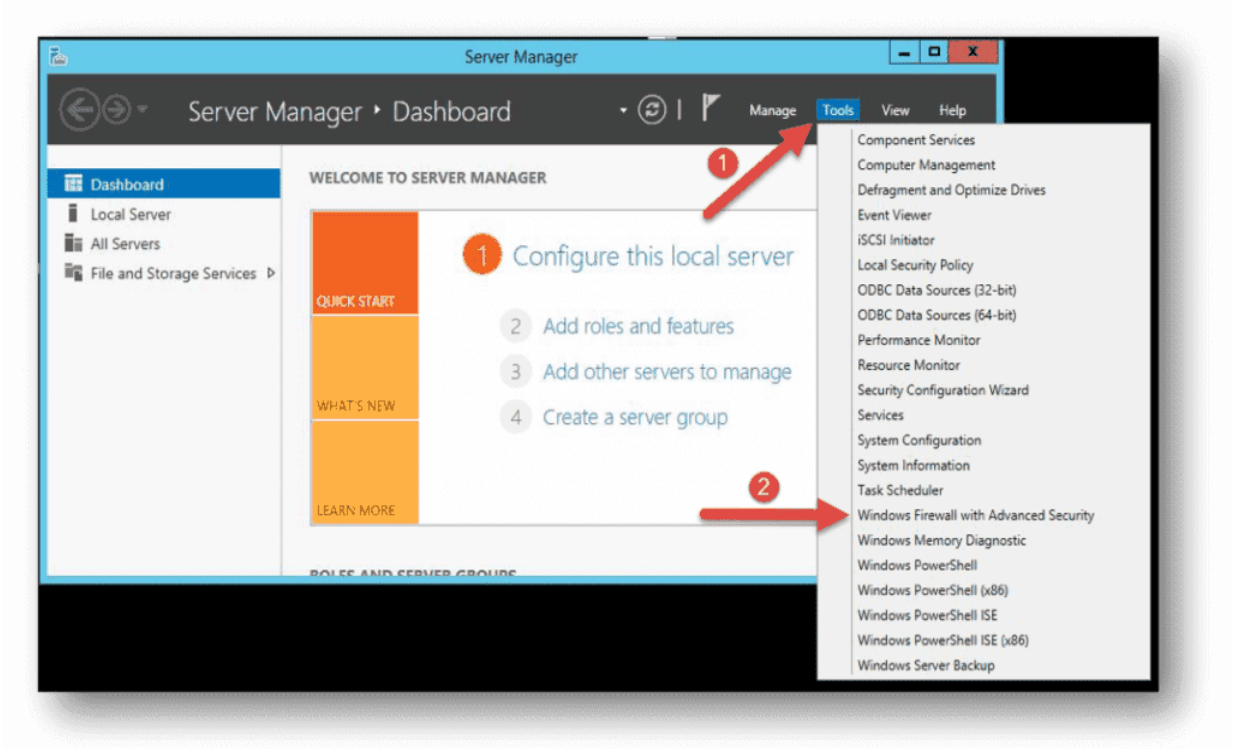
- Protect the data on your computer by creating a barrier that blocks any undesired incoming or outgoing traffic.
- Notify you if there are any connection requests from other computers.
- Log activity for later inspection and warn you if any application tries to connect to another computer.

Windows Firewall with Advanced Security provides safer inbound and outbound network communications by enforcing rules that control traffic flow for its local machine. There are three available firewall profiles:

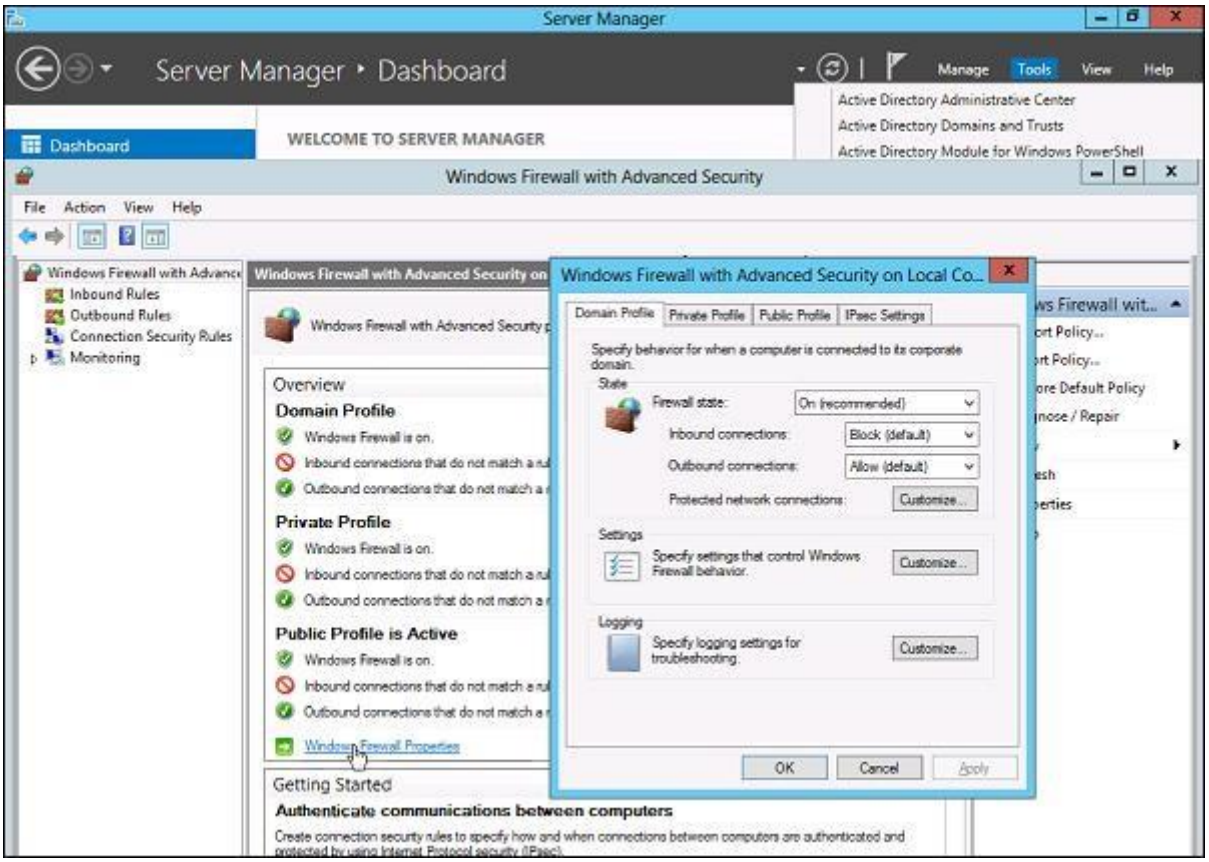
1. Domain. It is used when a computer connects to the corporate network. It is a network where the device can detect its domain controller.
2. Private. We use this profile for computers that connect to a private network, such as home or office. In private networks, the users are always behind a device and not directly exposed to the Internet.
3. Public. This profile is used when a computer connects to a public network, such as libraries, airports and other public hotspots. The firewall configurations should be the most restrictive for this profile since these networks are the least secure.

Launch Windows Firewall with Advanced Security

Step 1 − Click on the Server Manager from the task bar → Click the Tools menu and select Windows Firewall with Advanced Security.

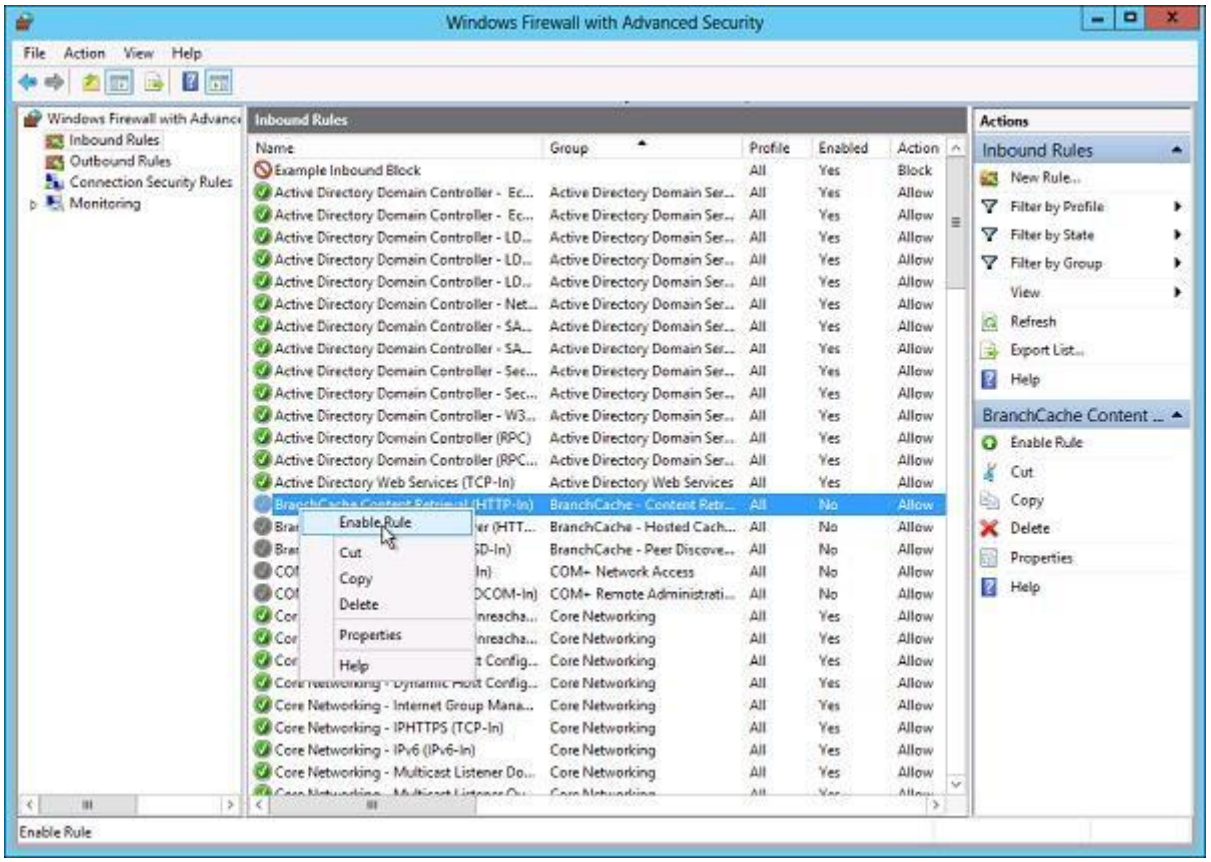


Step 2 − To see the current configuration settings by selecting Windows Firewall Properties from the MMC. This allows access to modify the settings for each of the three firewall profiles, which are – Domain, Private and Public and IPsec settings.



Step 3 − Applying custom rules, which will include the following two steps −

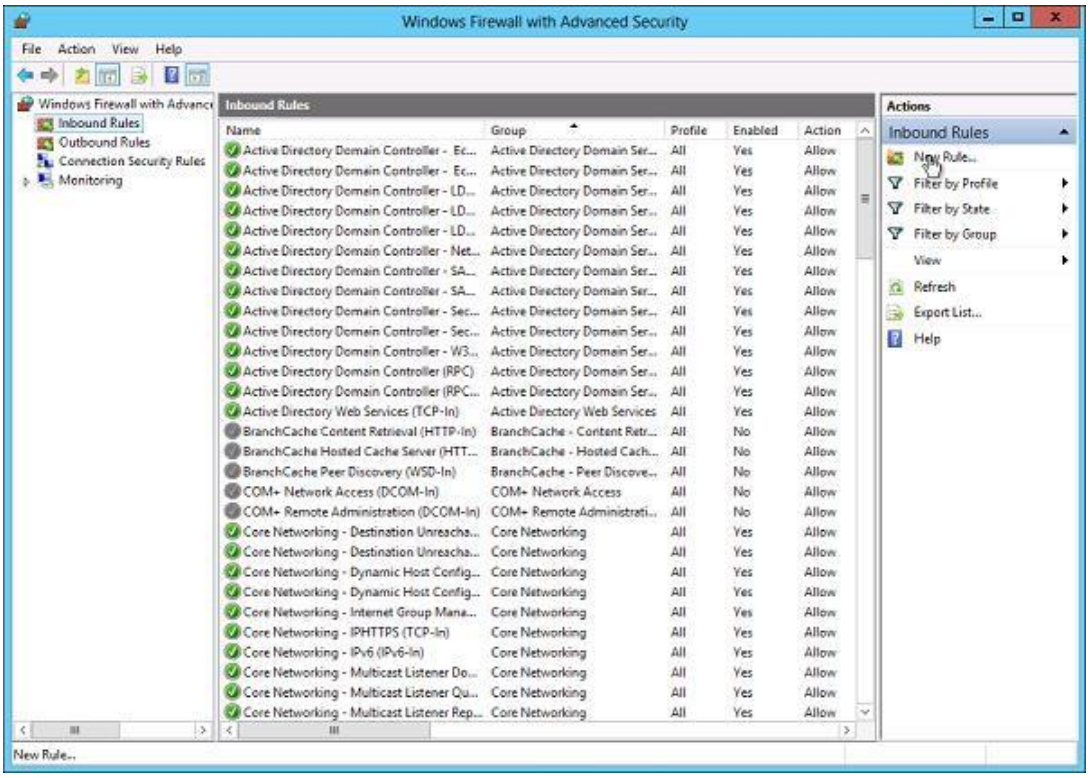
- Select either Inbound Rules or Outbound Rules under Windows Firewall with Advanced Security on the left side of the management console. (As you Know outbound traffic is the traffic generated from the server towards the internet and inbound traffic is vice versa). The rules that are currently enabled are denoted by a green checkbox icon, while disabled rules display a grey checkbox icon.
- Right-clicking a rule will allow you toggle enable/disable.



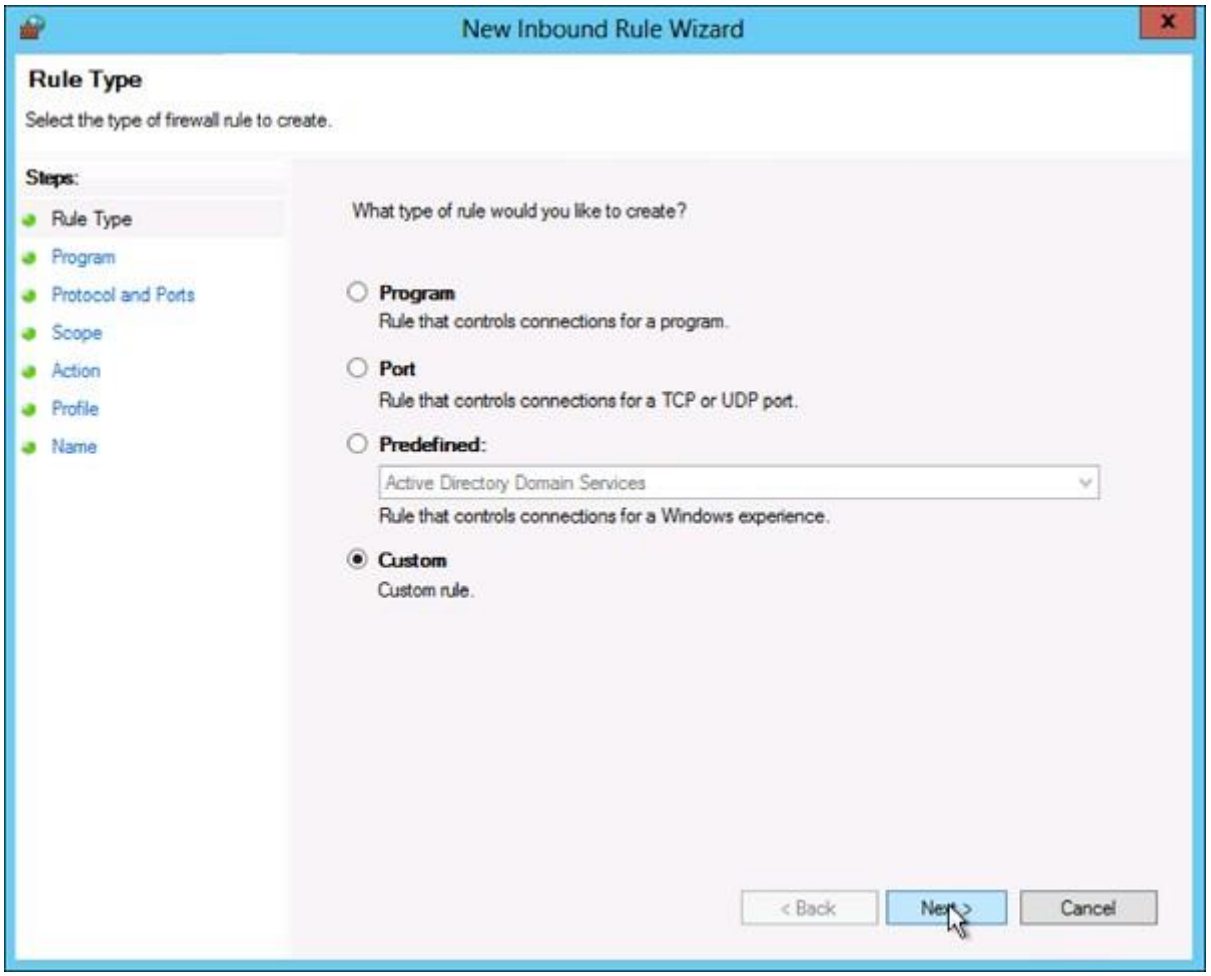
Create a New Firewall Rule

To create a new Firewall Rule, you have to adhere to the following steps −

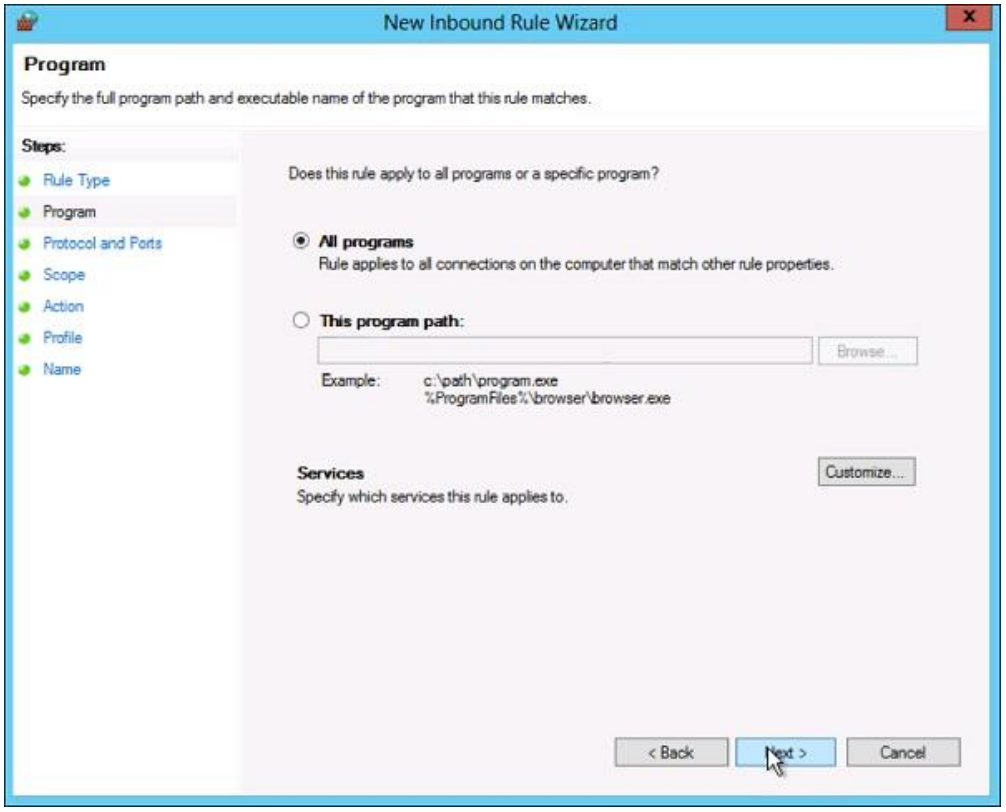
Step 1 − From the right side of either the Inbound Rules or Outbound Rules – click “New Rule”.



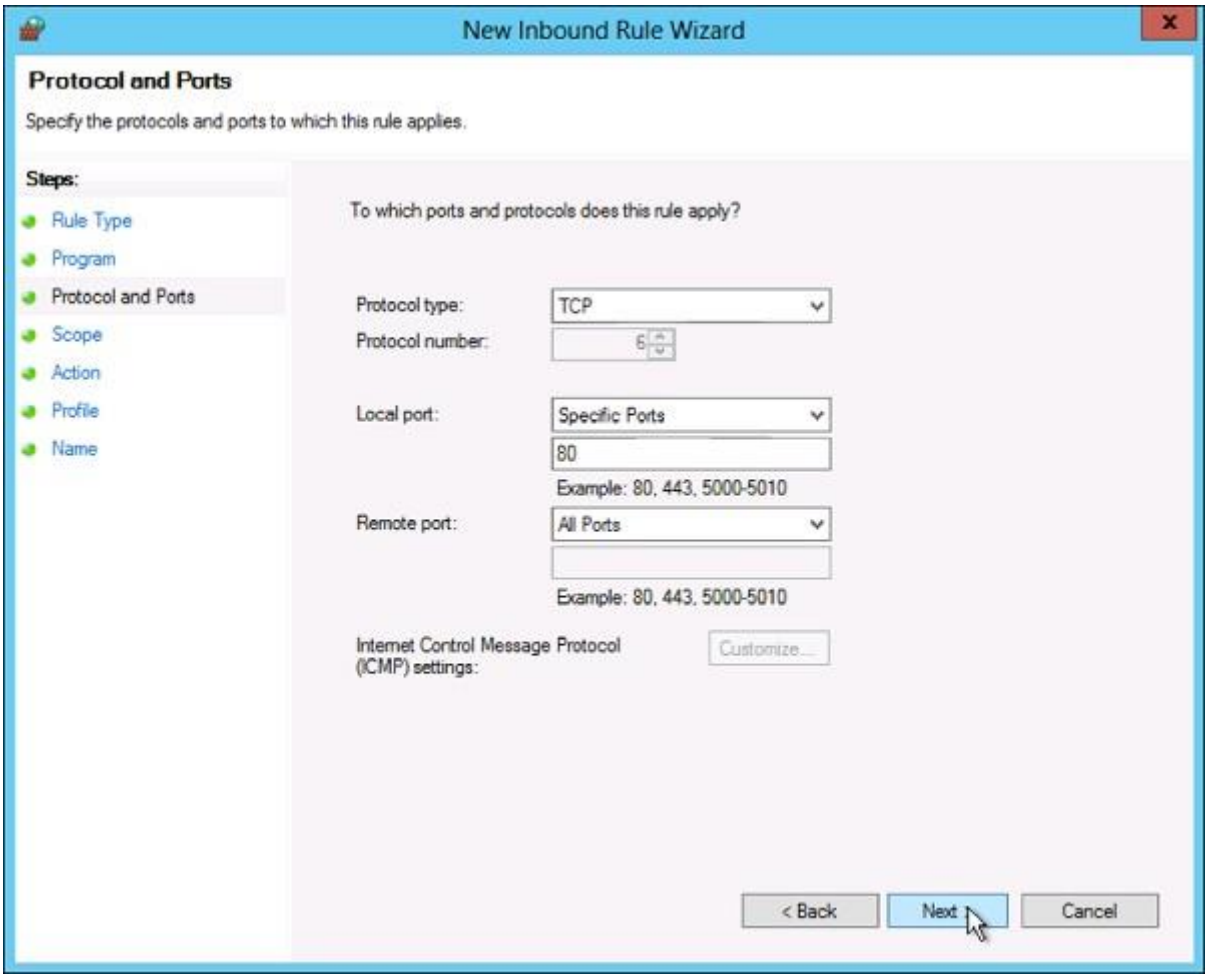
Step 2 − Custom from the Rule Type radial button → click Next.



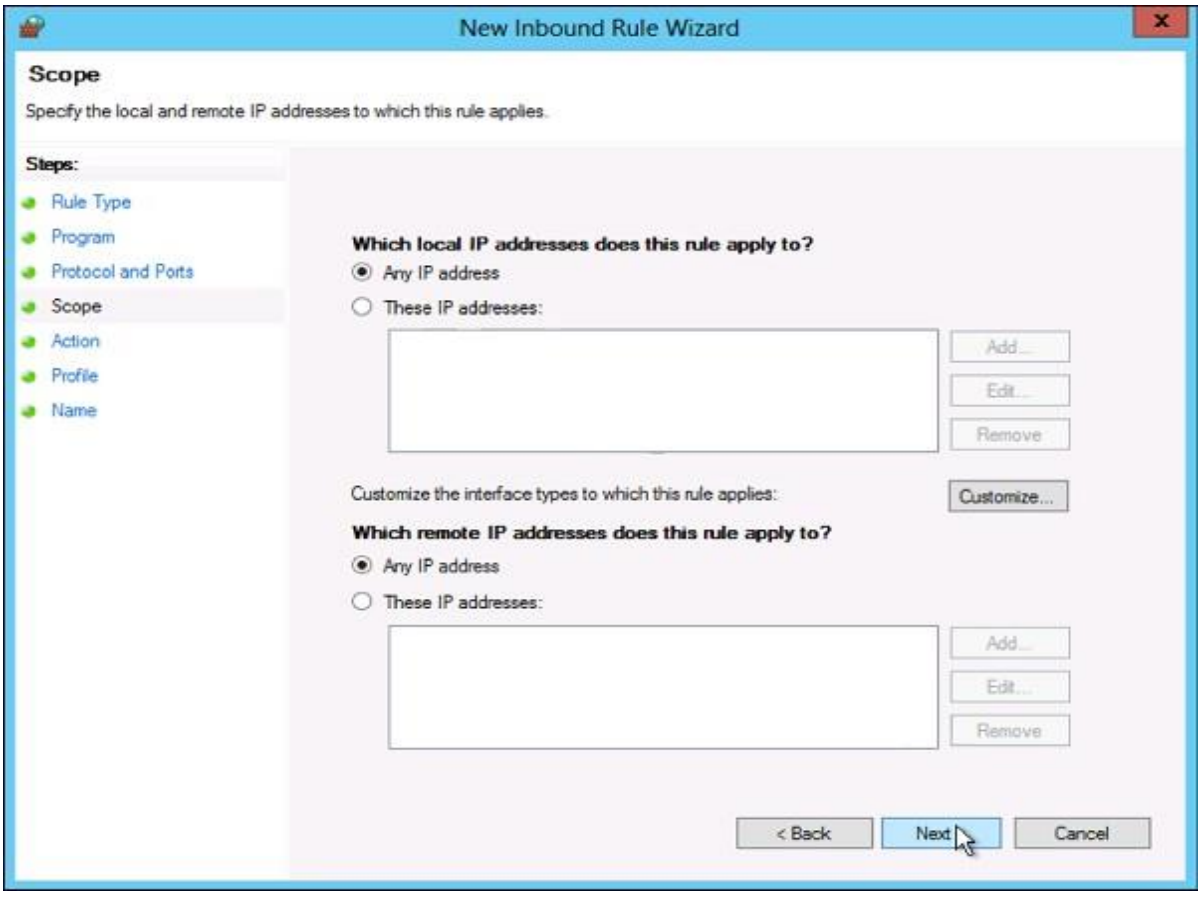
Step 3 − Select the Program association for the Custom Firewall Rule as either All programs or the path to a program → click Next.



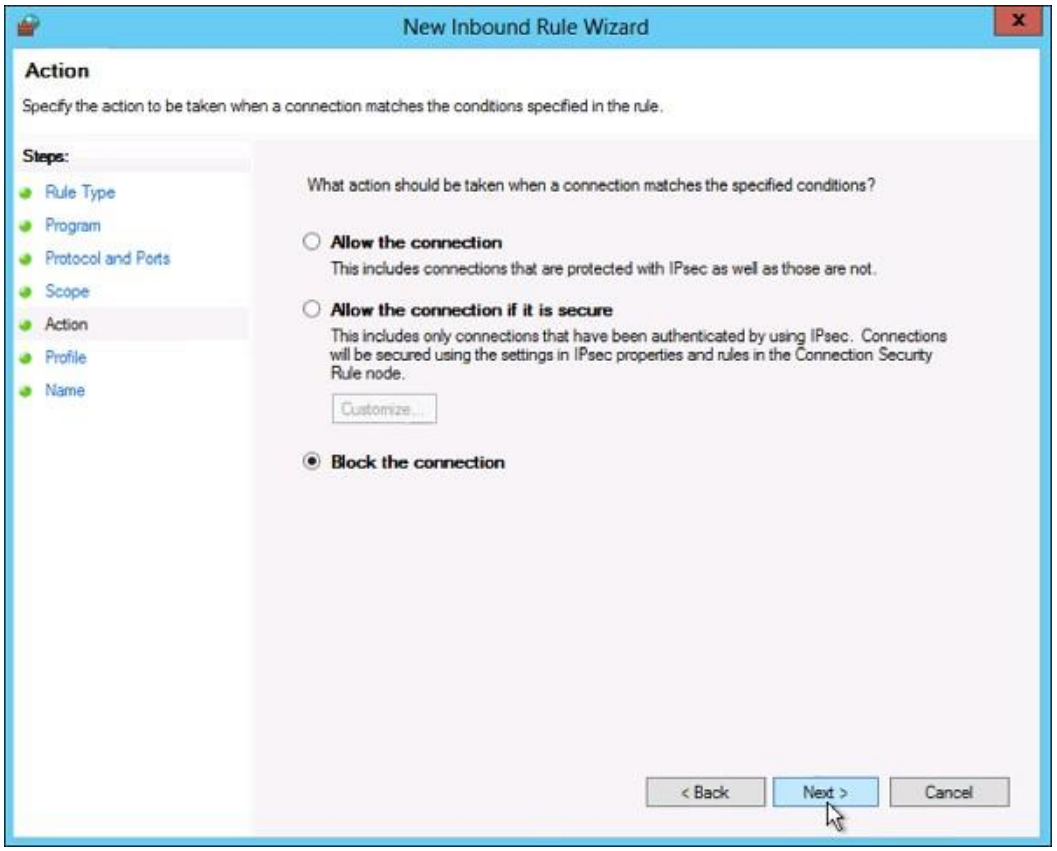
Step 4 − Protocol type field select the protocol type → click Next.



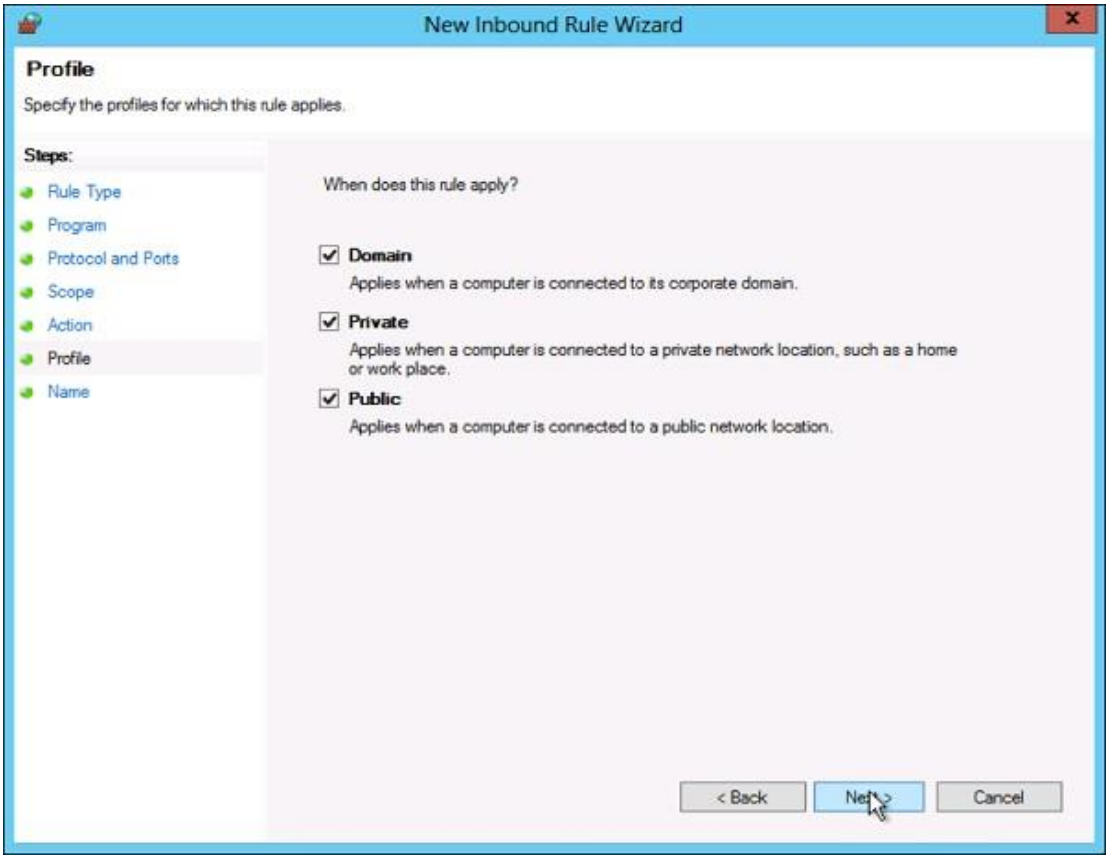
Step 5 − Select an IP address association for both local and remote addresses → click Next.



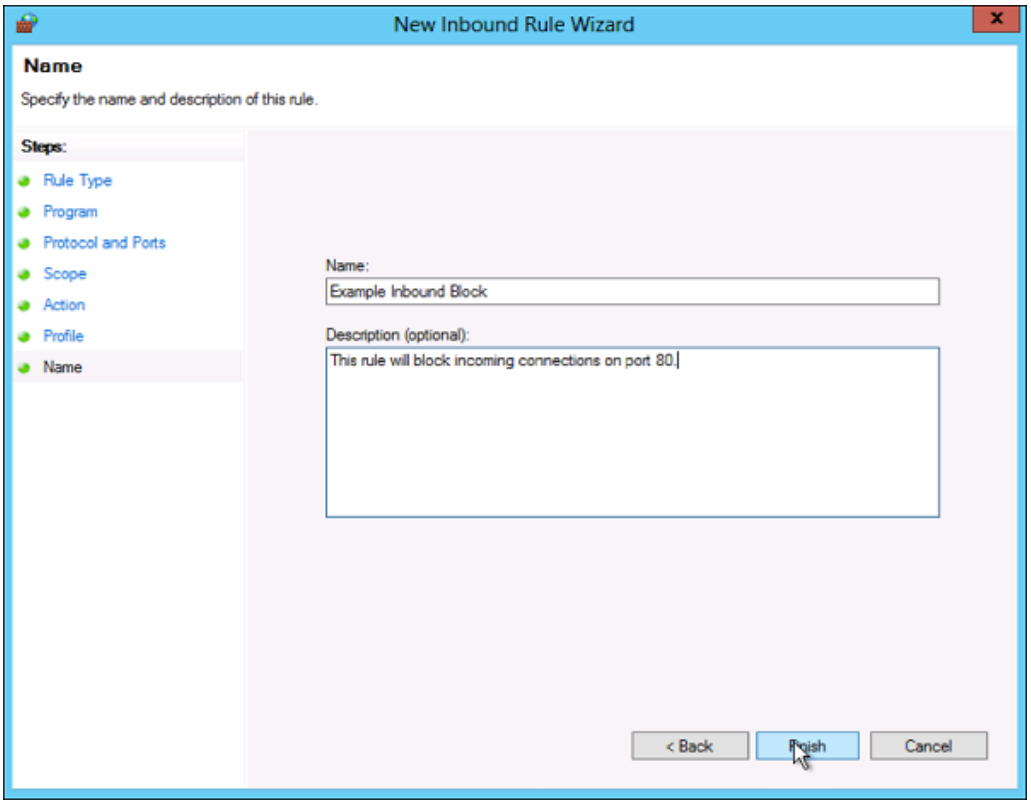
Step 6 − Select an action to take on matching traffic → click Next.



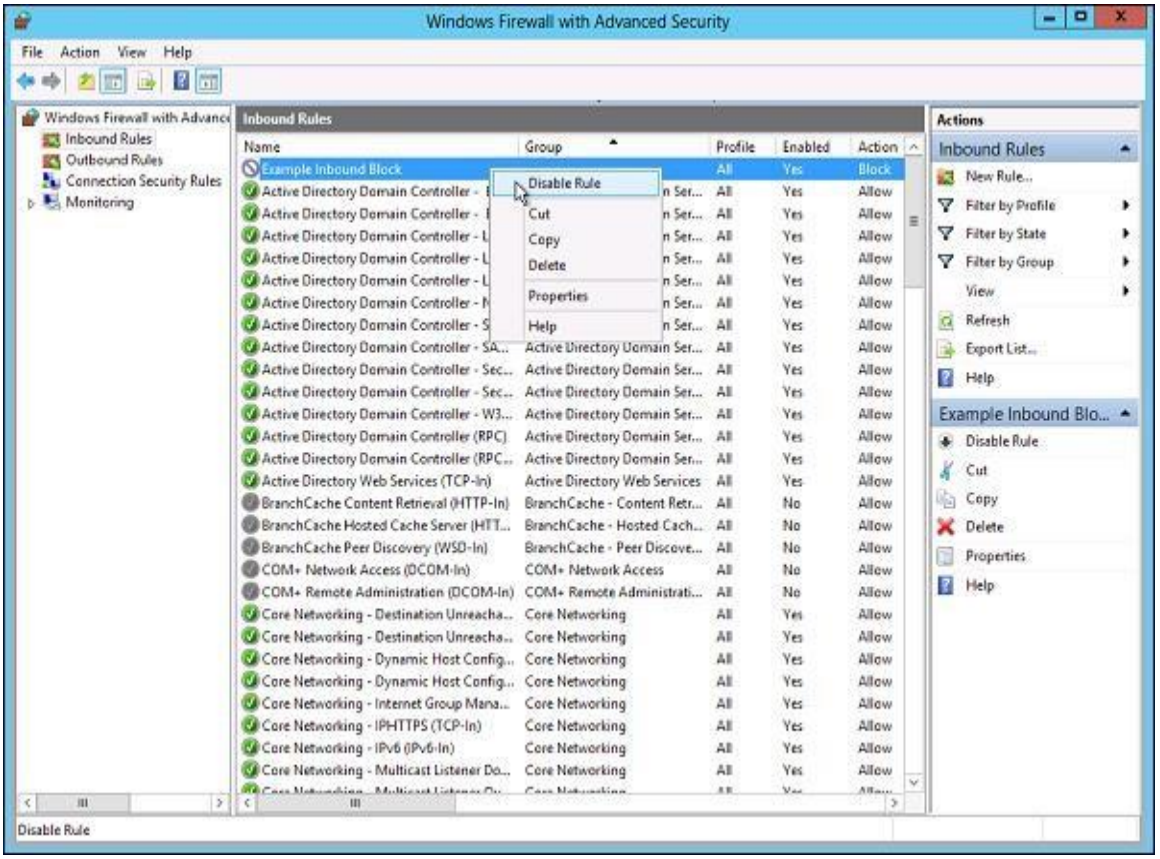
Step 7 − Select the profiles associated with the custom rule → click Next.



Step 8 − Put a name for your Firewall rule and an optional description → Finish.



Step 9 − The firewall rule can be found on the corresponding Rule tab, either inbound or outbound depending on the type created. To disable or delete the rule find the rule in the MMC, right-click it and select either Disable Rule or Delete.



Result

Thus the system security using encryption and windows firewall was implemented.

Ex.No 7 **Creating RAID sets: Mirroring and striping**

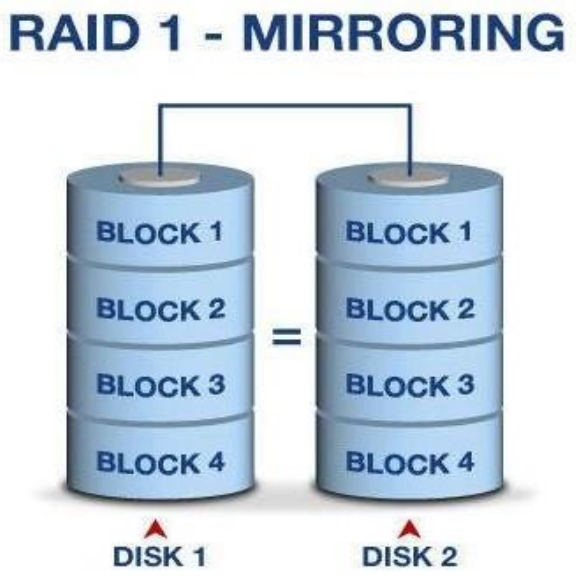
Aim

To create RAID set mirroring and striping.

Components Required

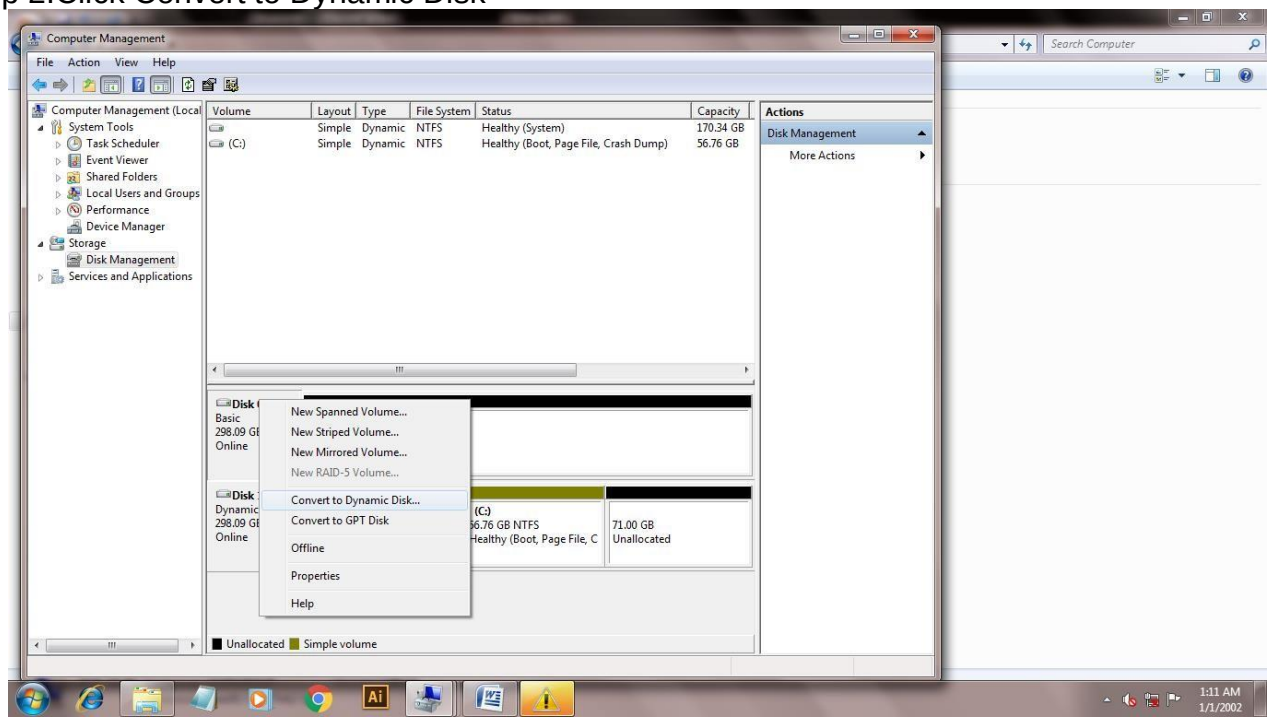
1. PC
2. External harddisk

RAID ("Redundant Array of Inexpensive Disks" or "Redundant Array of Independent Disks") is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. Disk mirroring, also known as RAID 1, is the replication of data to two or more disks. Disk mirroring is a good choice for applications that require high performance and high availability, such as transactional applications, email and operating systems. Disk mirroring also works with solid state drives so “drive monitoring” may be a better term for contemporary storage systems. Because both drives are operational, data can be read from them simultaneously, which makes read operations quite fast. The RAID array will operate if one drive is operational. Write operations, however, are slower because every write operation is done twice.

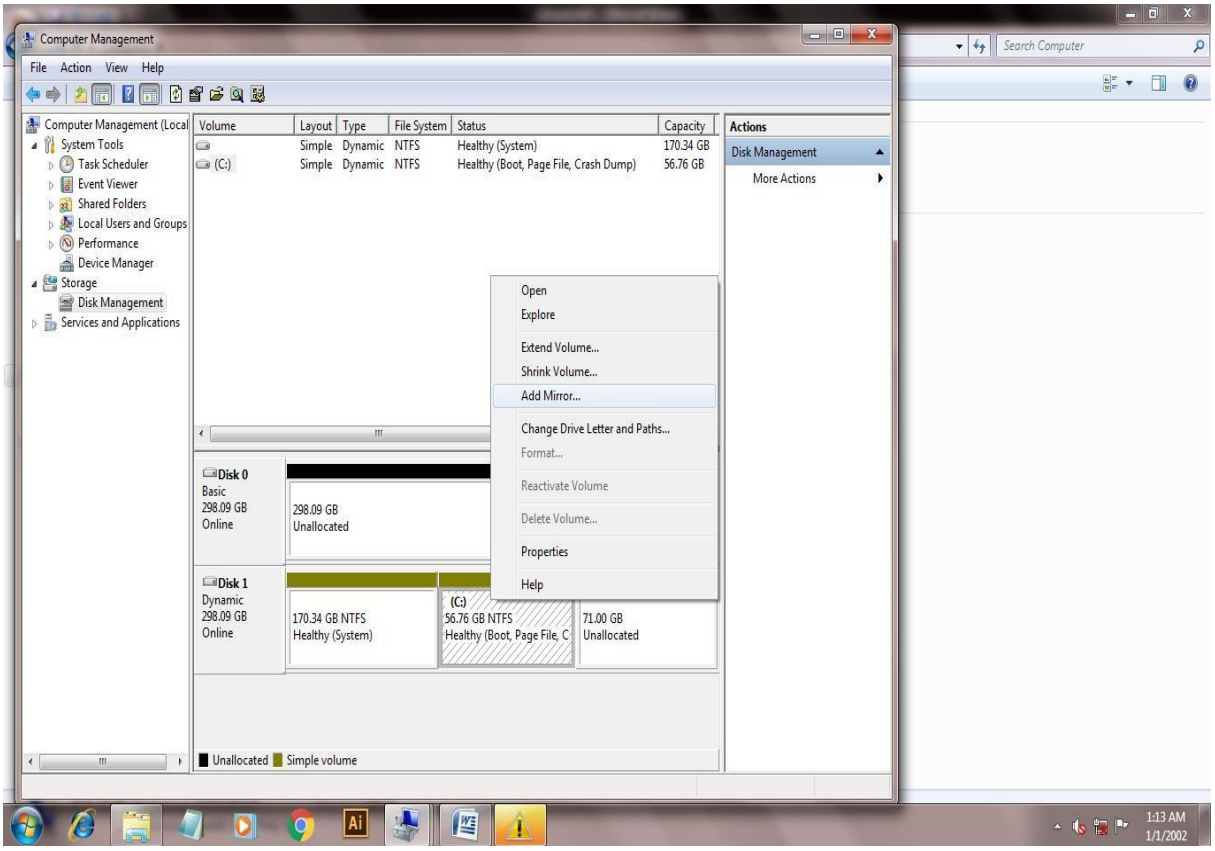


RAID levels:
RAID 0 – striping RAID 1 – mirroring
RAID 5 – striping with parity
RAID 6 – striping with double parity
RAID 10 – combining mirroring and striping Steps to create Mirroring and Stripping Step 1:Click Disk Management

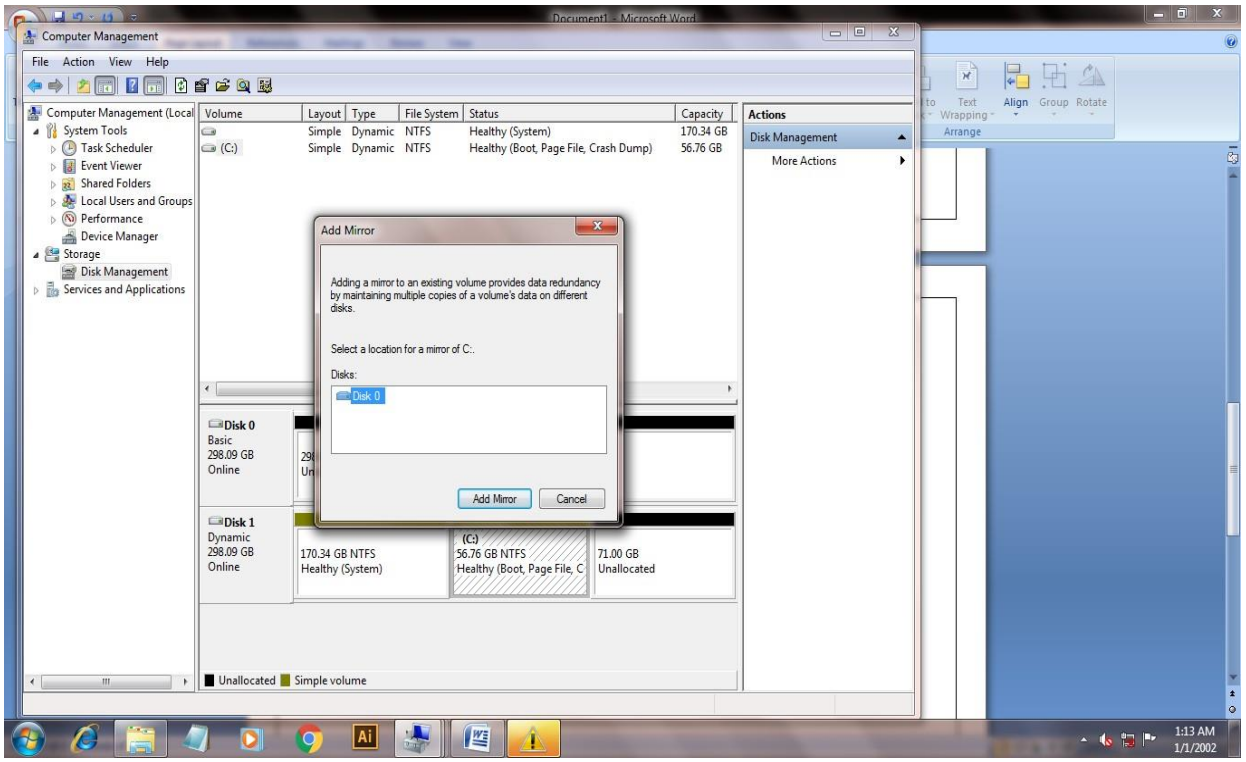
Step 2:Click Convert to Dynamic Disk

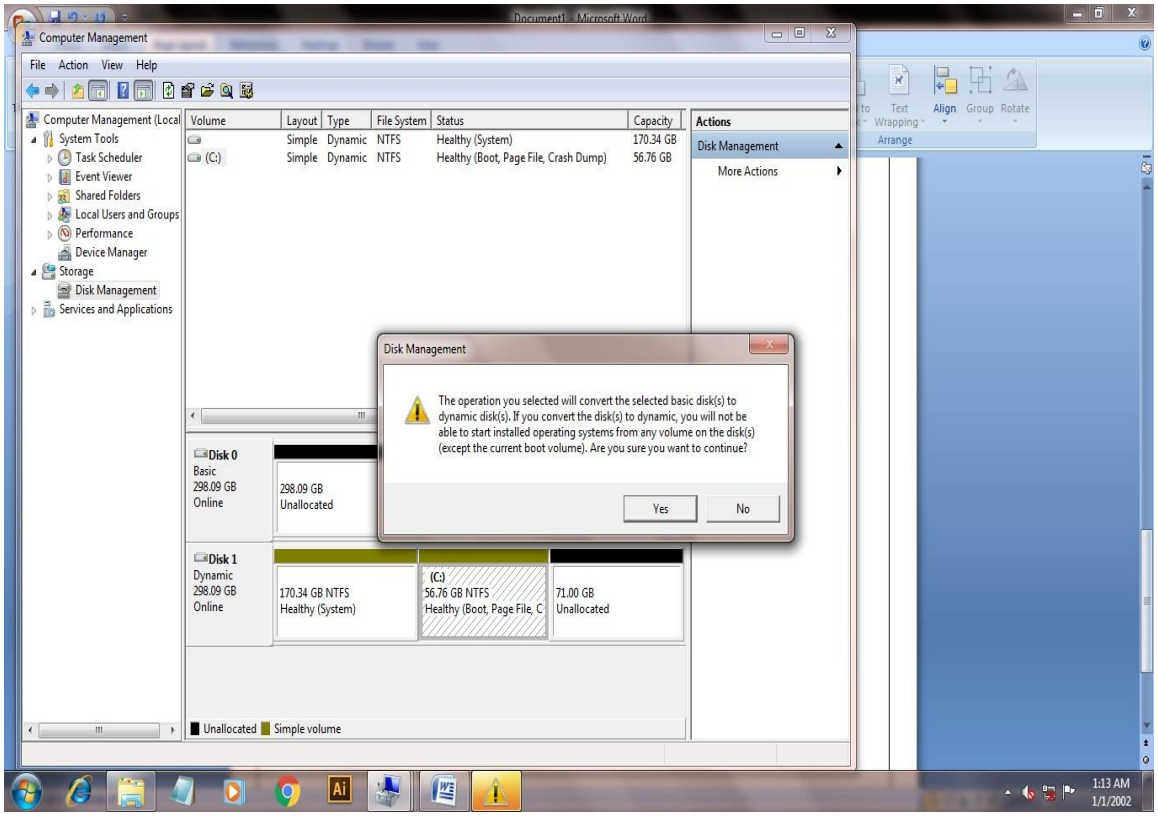


Step 3:Click Add Mirror

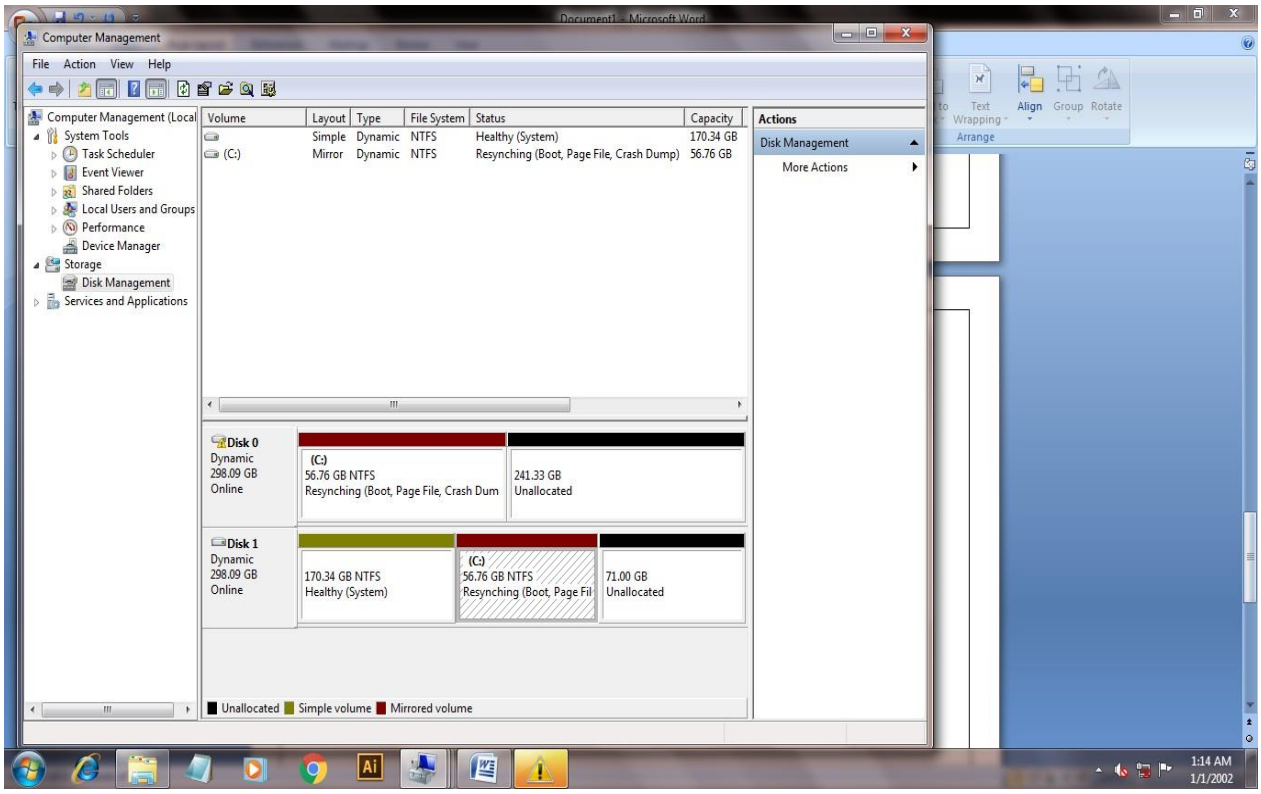


Step 4: Select the Disk 0





Step 5:Mirror Created



Result

Thus the RAID Mirroring and Stripping was created.

Ex.No 8 **Creating Network Back up and scheduling**

Aim

To create Network Back up and Scheduling.

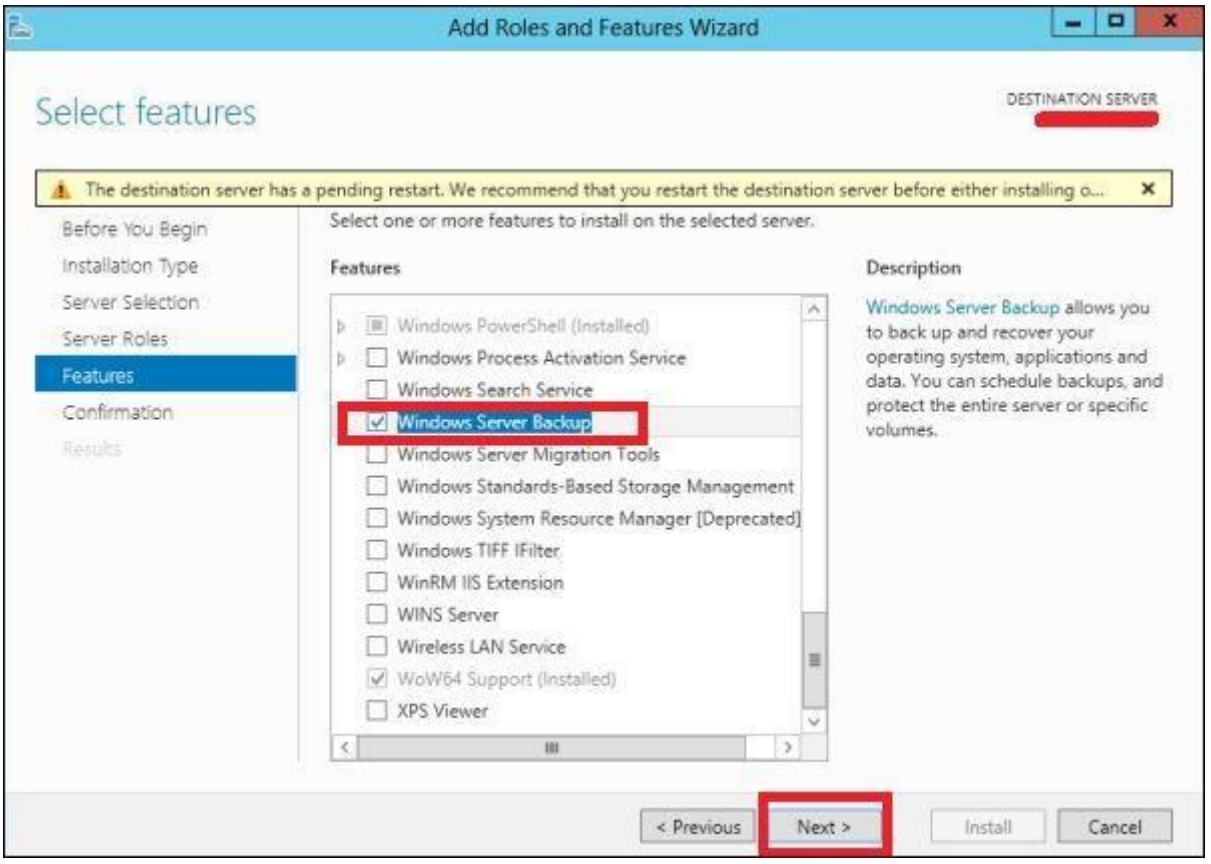
Components Required

1. PC
2. Windows server

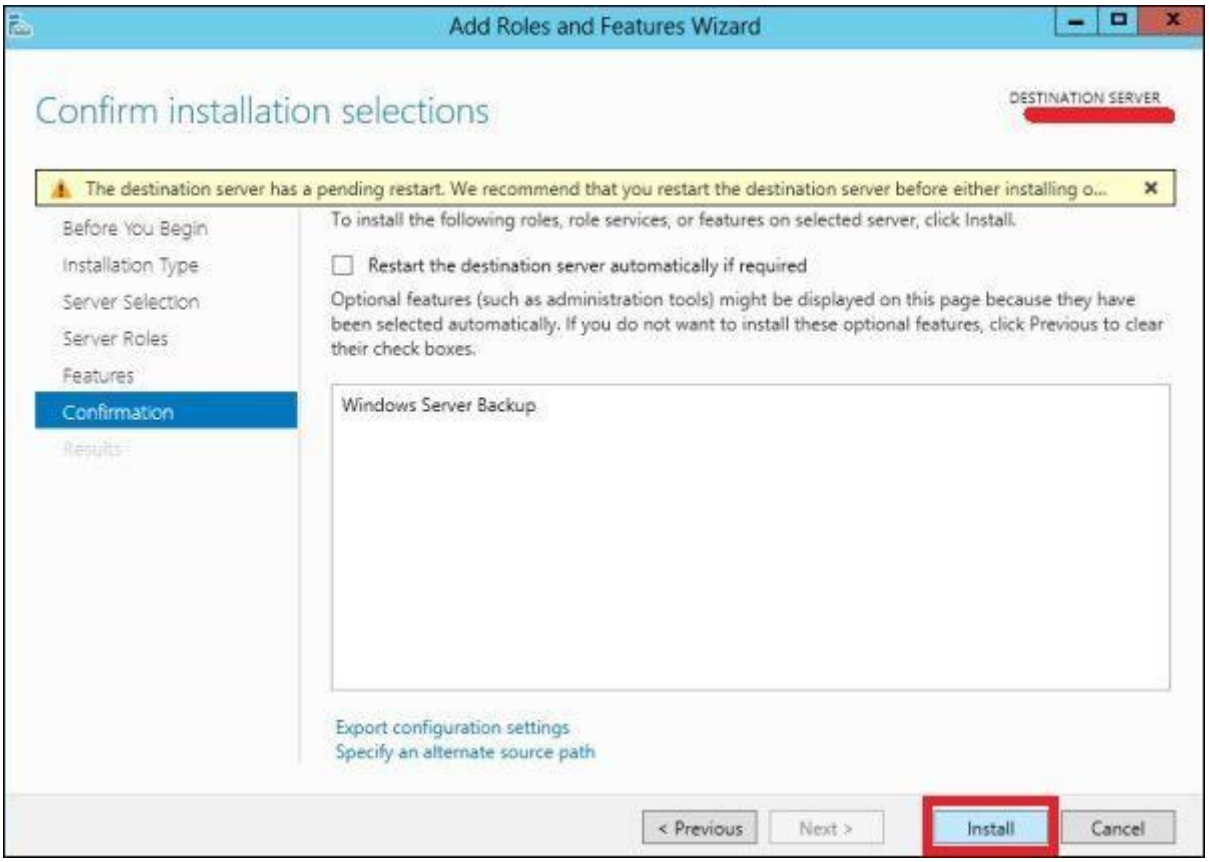
To **install the backup** feature

Step 1 − Go to Server Manager → Manage → Add Roles and Features → Next → Check the **Role-based** or **feature-based installation** box → then check on the **Select a server from the server pool** box and then click Next.

Once all this is done, check the **Windows Backup Server** box and then click on Next as shown in the following screenshot.

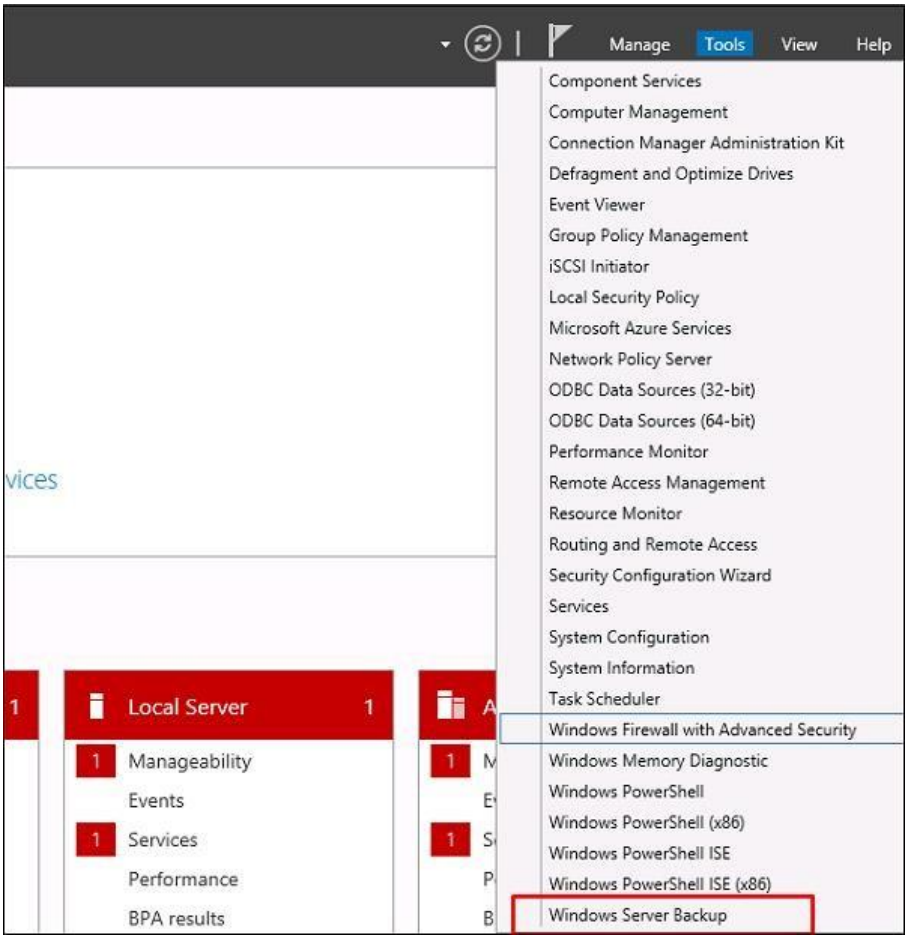


Step 2 − Click **Install** and then wait for the process to Finish.

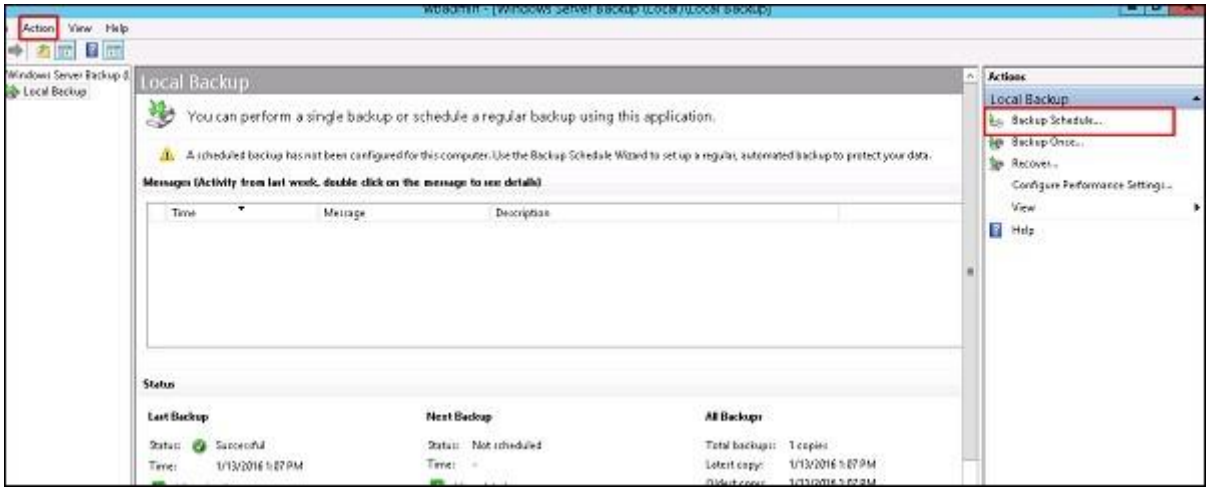


Now let us go and **configure the Backup** Feature it, for which user should follow the steps given below.

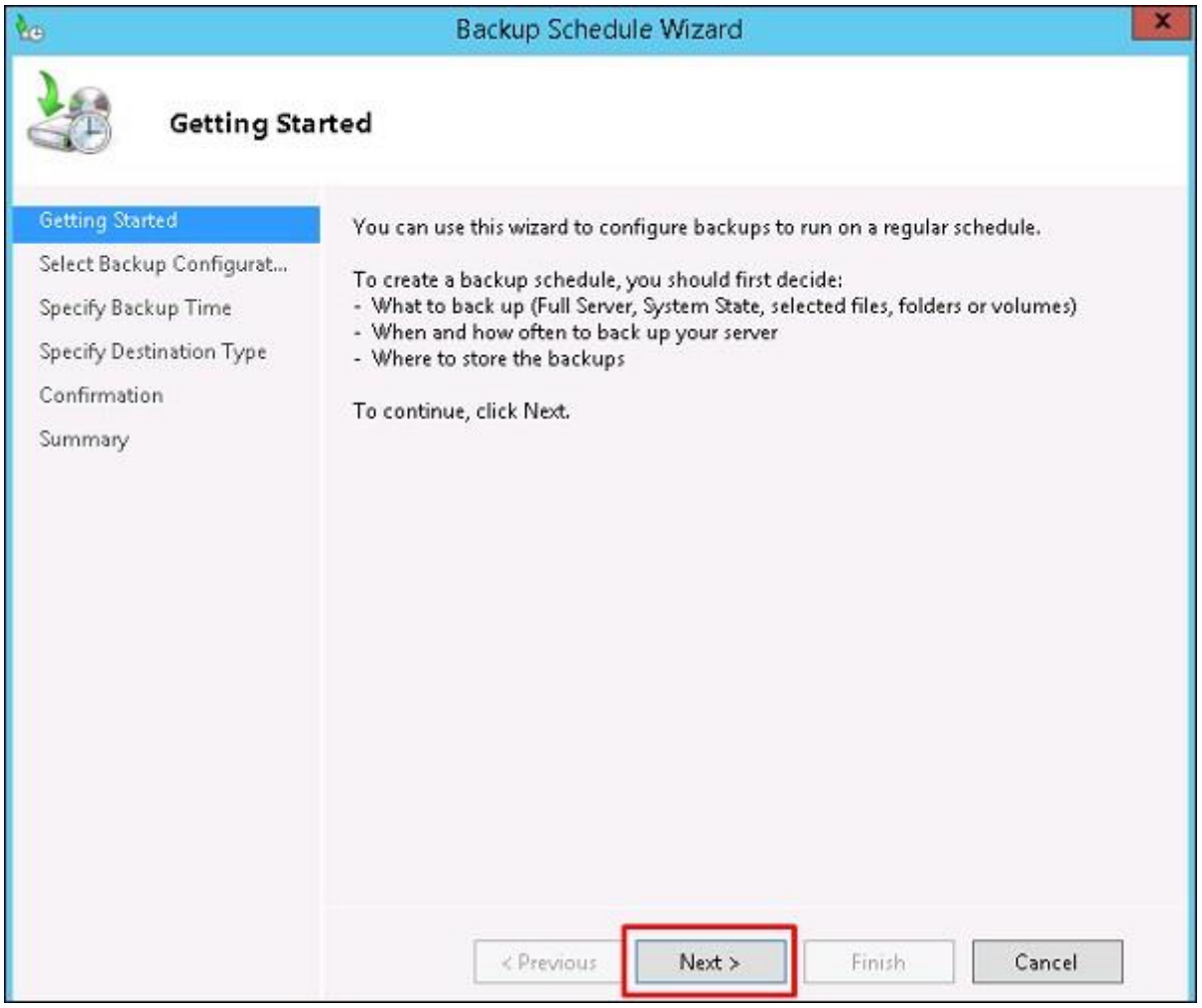
Step 1 − Go to **Server Manager** → Tools → Windows Server Backup.



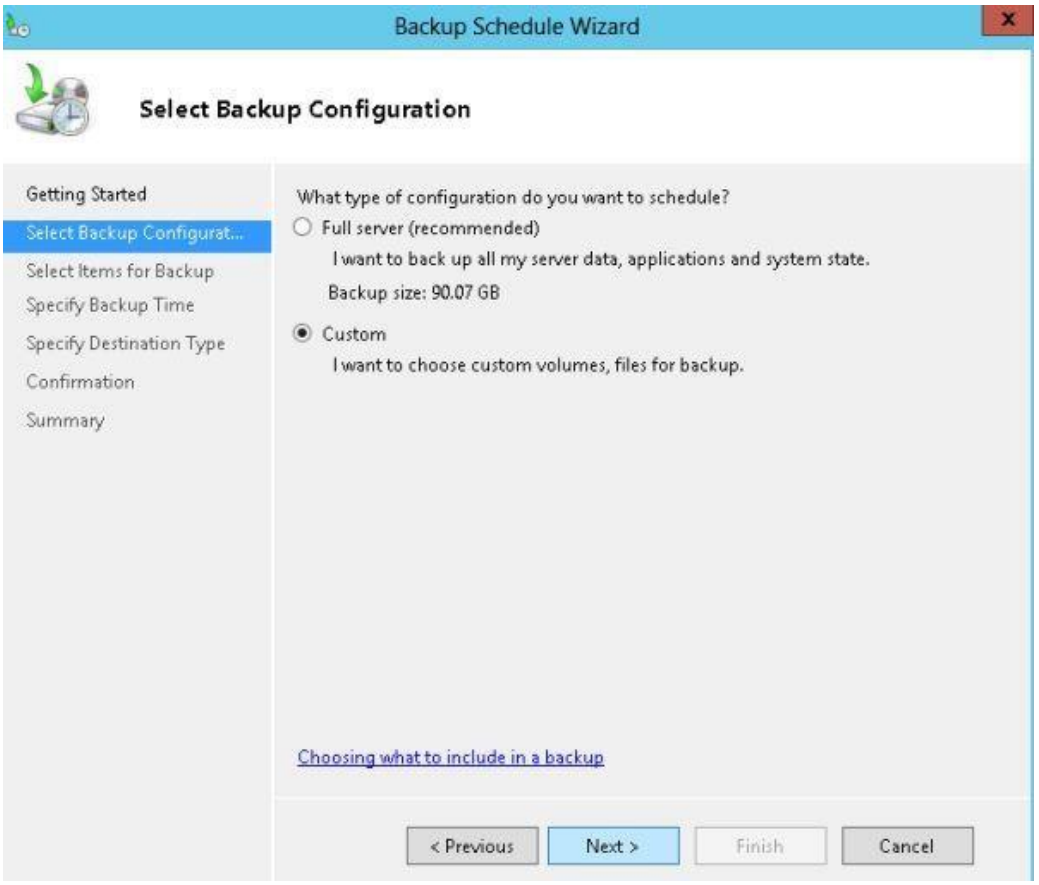
Step 2 − Click on **Backup Schedule** in the left side panel or click on **Action** at the top of the screen as shown in the following screenshot.



Step 3 − Click Next.

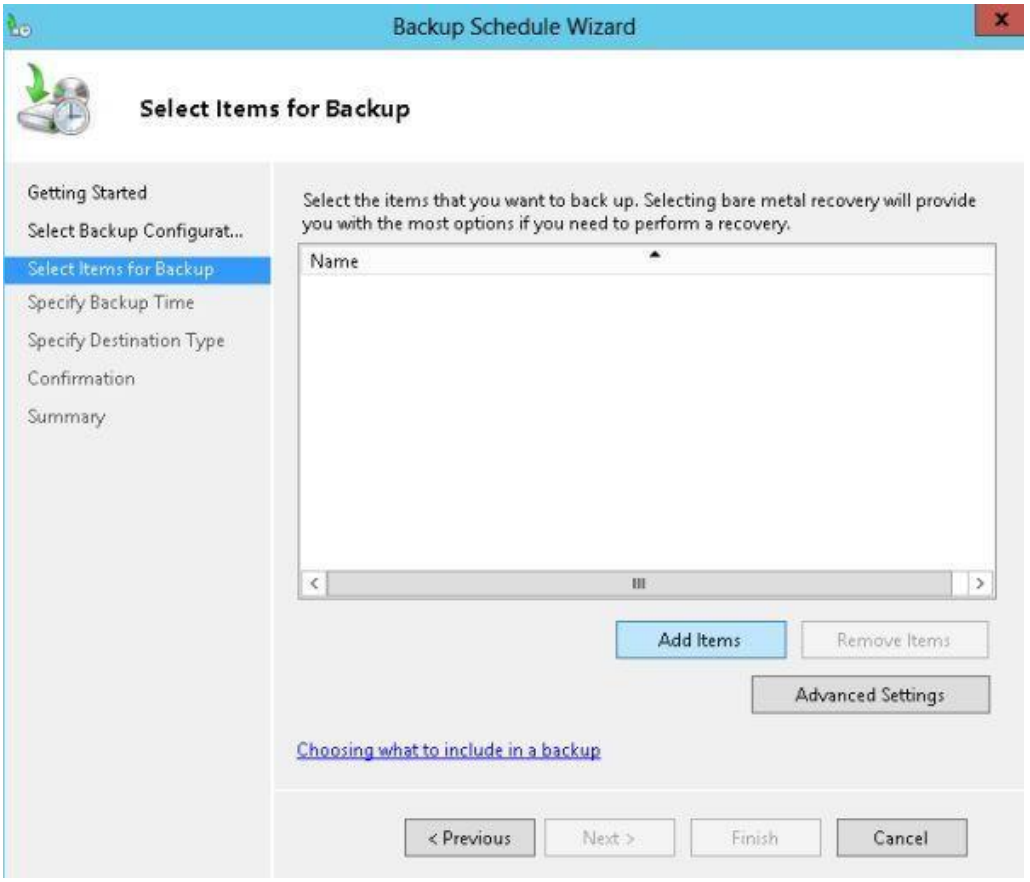


Step 4 − Now on the next page user can select "Backup Configuration" that can be either "Full Server" or "Custom". If user select Full Server then a backup of the Full Server will be created and if user select the Custom feature then get an option to select the item for which they want to create a backup.

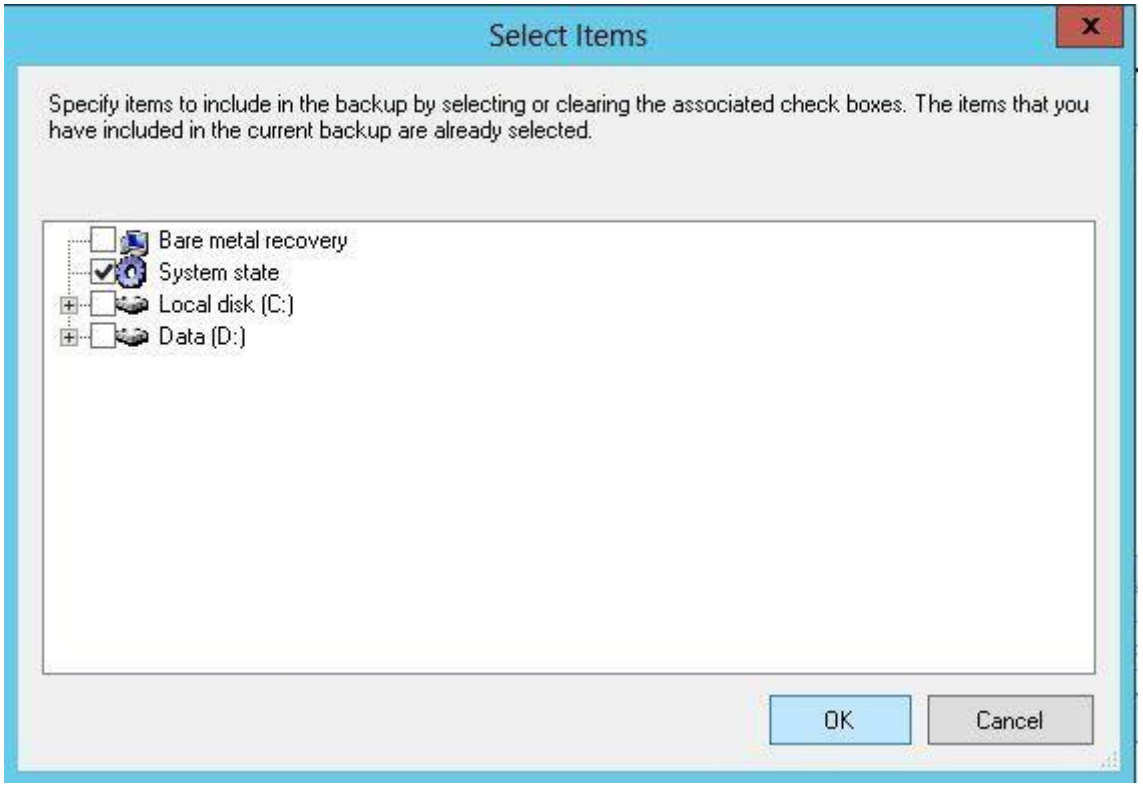


Step 5

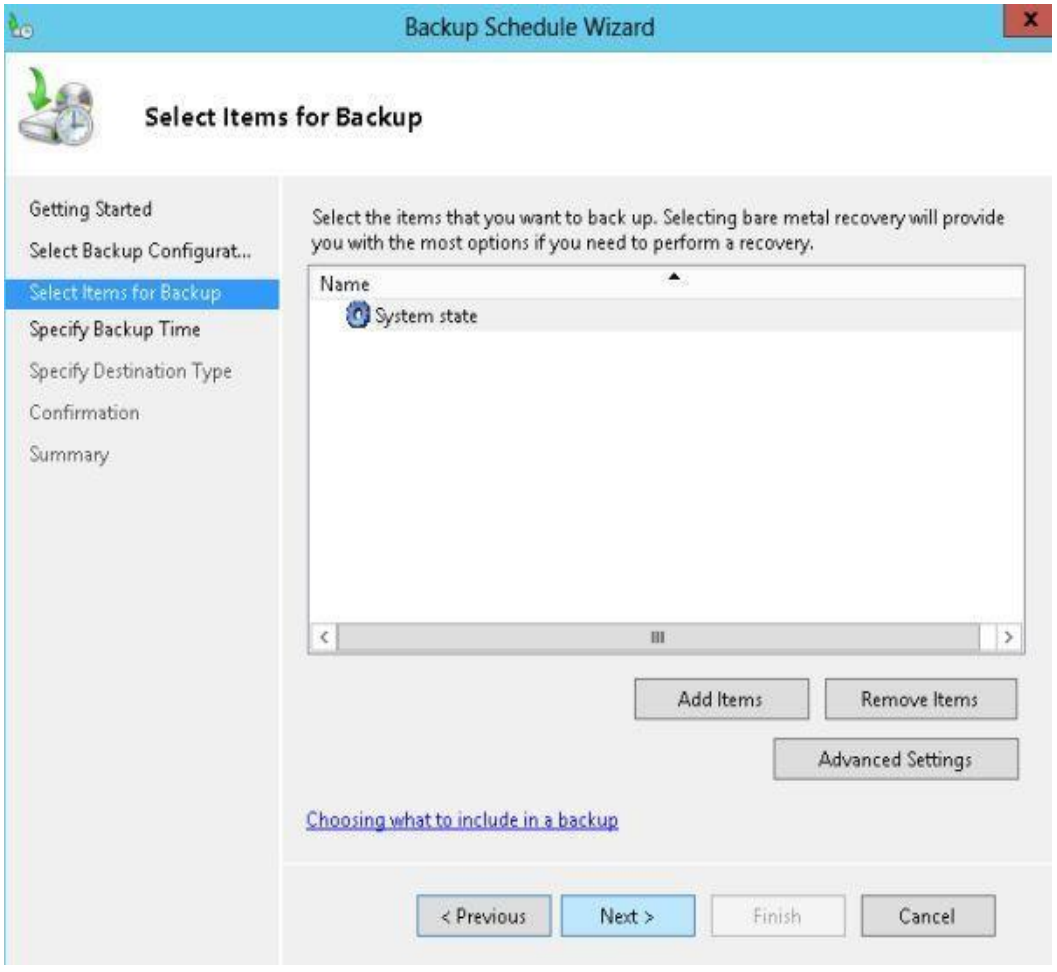
Now **select the item** for which the user want to create a backup. For that first click on "Add Items".



Select the Add Items a new window will be opened from which the user can select the items. Here, selected the System State.

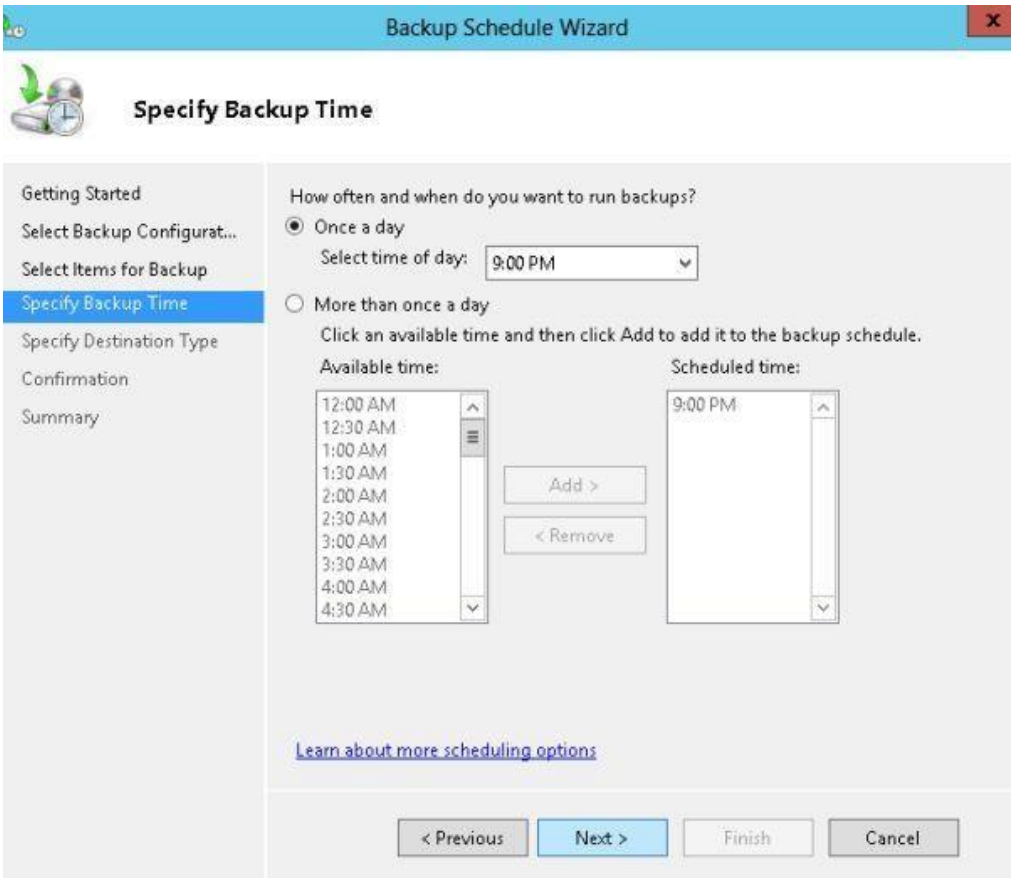


On clicking the "Ok" button.

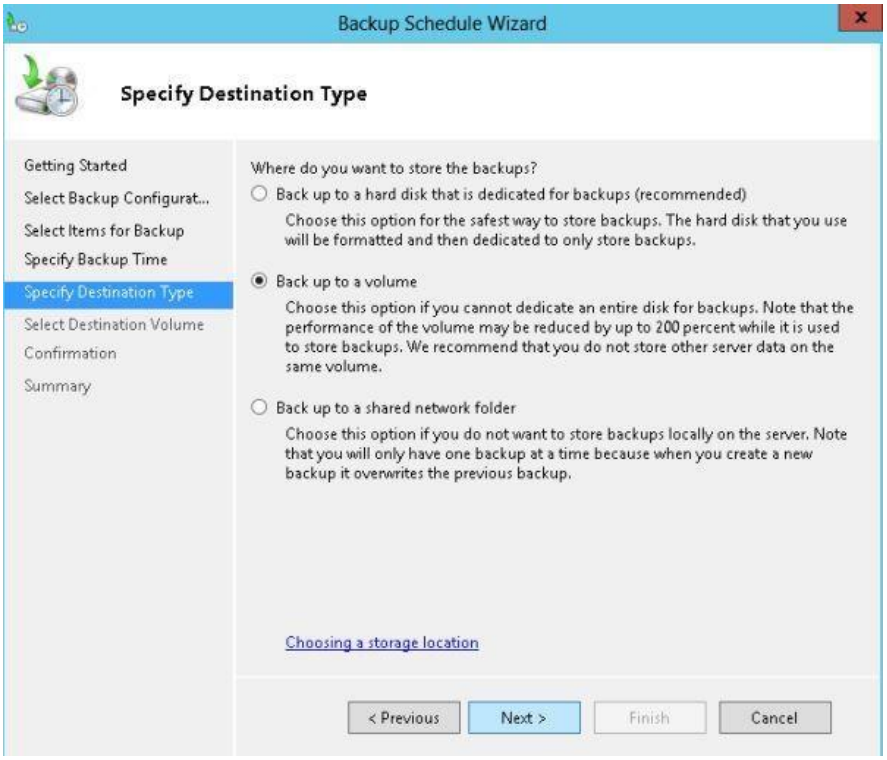


Step 4

Now specify the "Backup Time" for creating a backup either Once a Day or want to create the backup more than once, select the second option and specify the frequency of the backup.

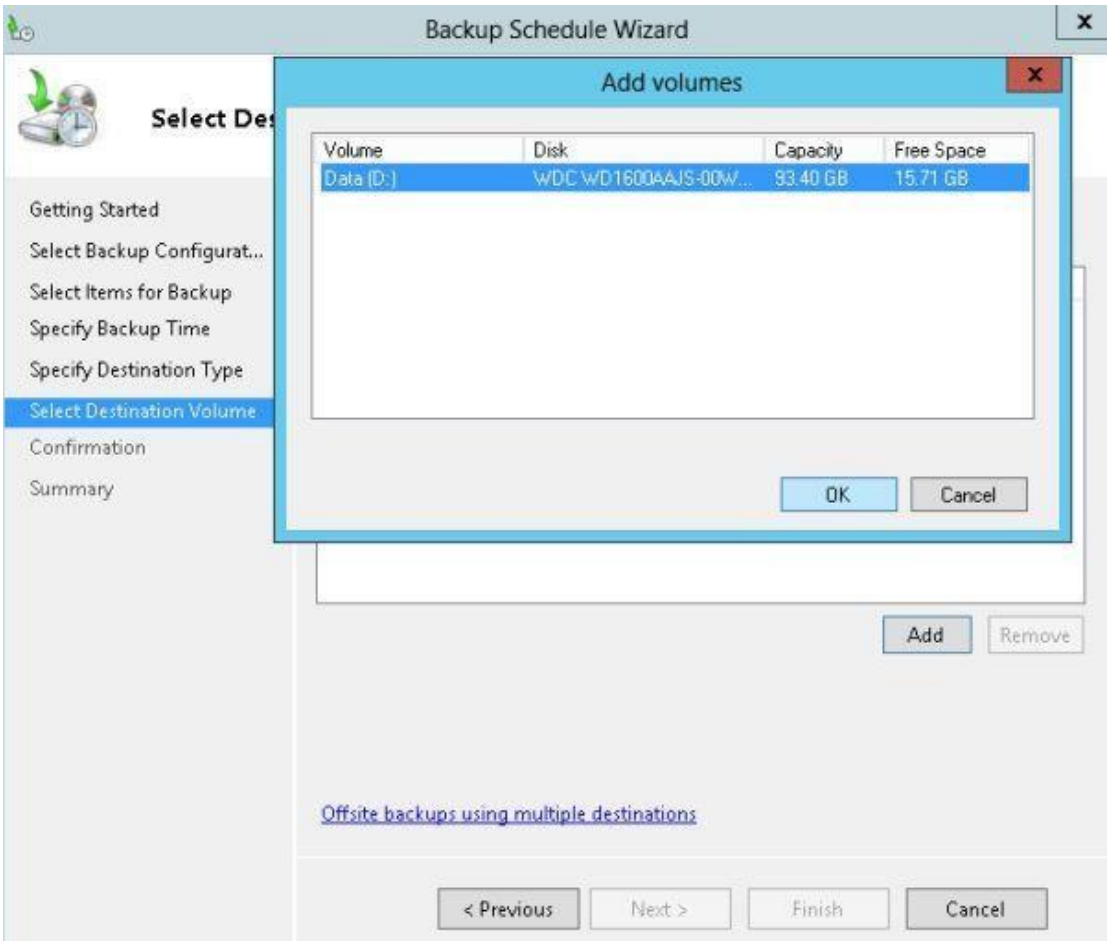


On the next page user must select the "Destination Type" that can be a volume of the computer, Hard Disk or any remote folder in the shared network. Here I have selected the second option, which is to create a backup on the volume of the computer.

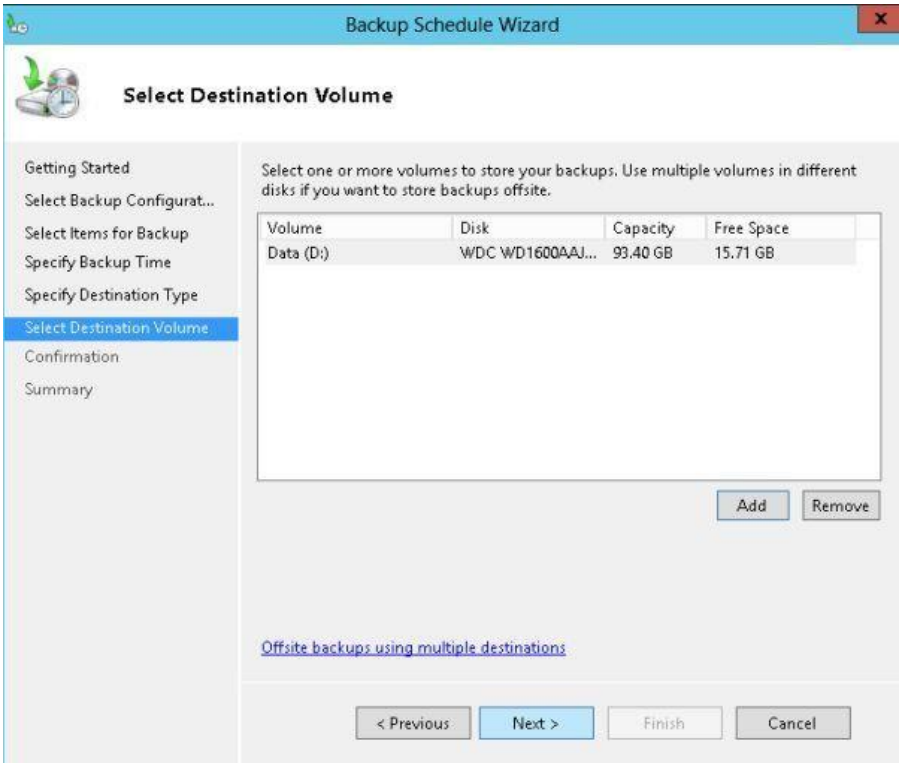


Step 5

On the next page user select the **Destination Volume** on which they want to create the backup. For that first click on the "Add" button and then select the destination volume.

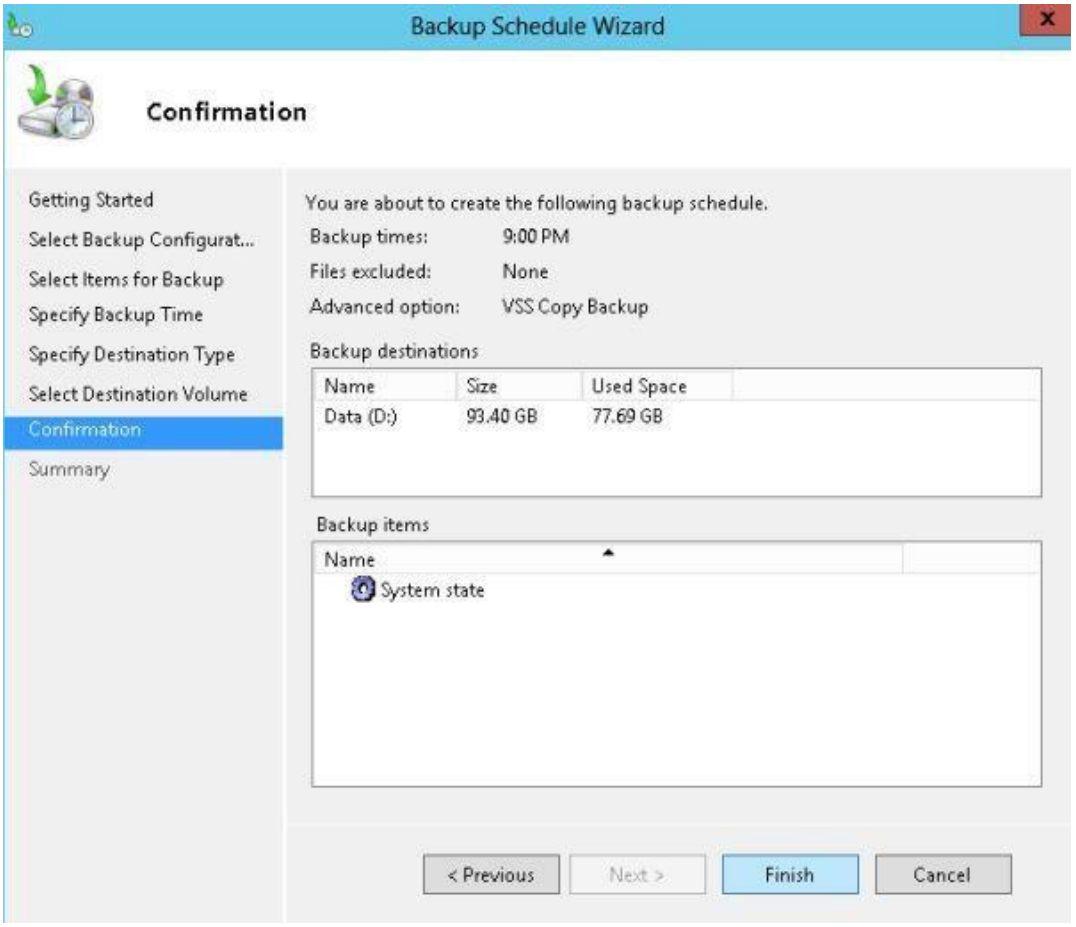


Now see the selection on the Wizard. After that click on Next.

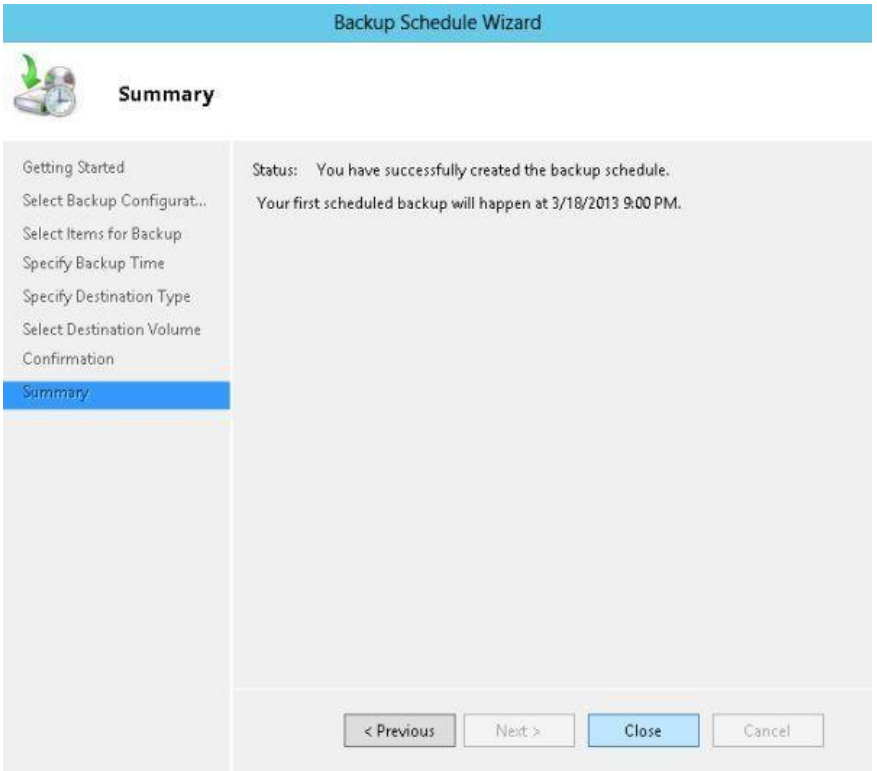


Step 6

Now a "Confirmation Page" will be opened that will show the full configuration of the selection made.



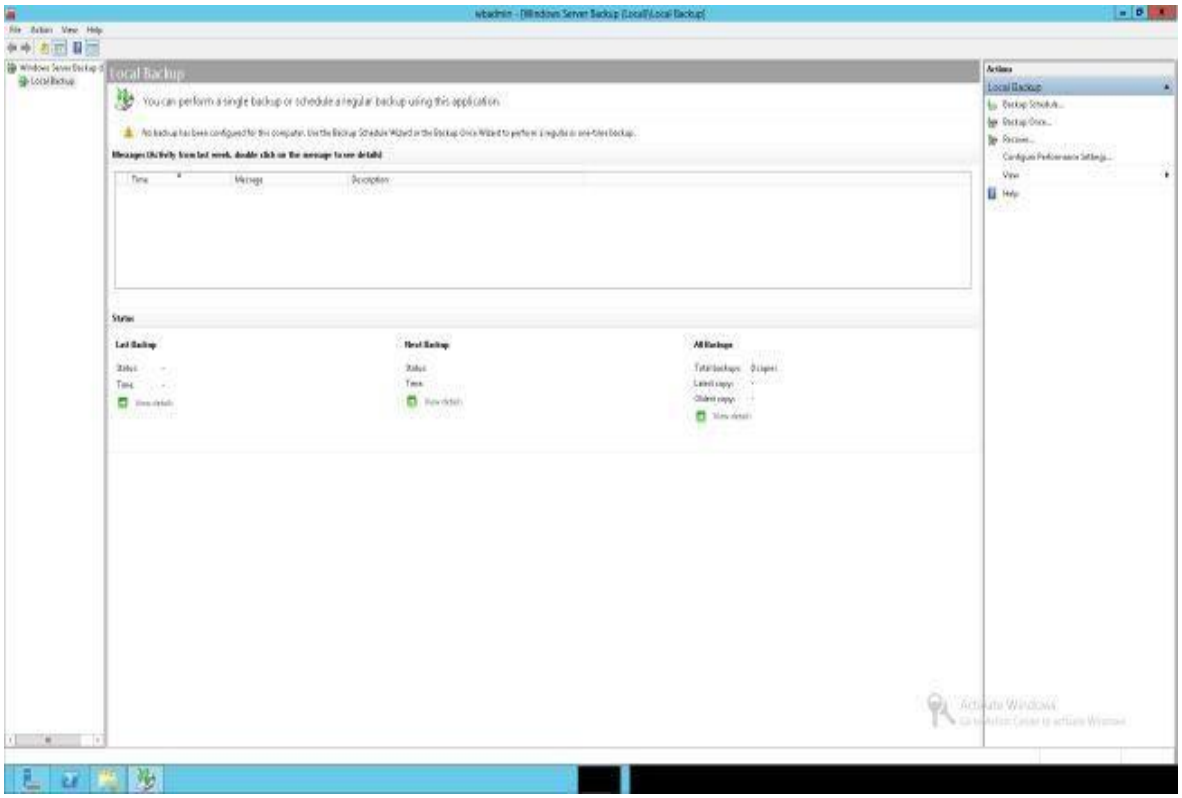
On clicking the "Finish" button a "Summary Page" will be opened that will show the status of the backup.



Step 1

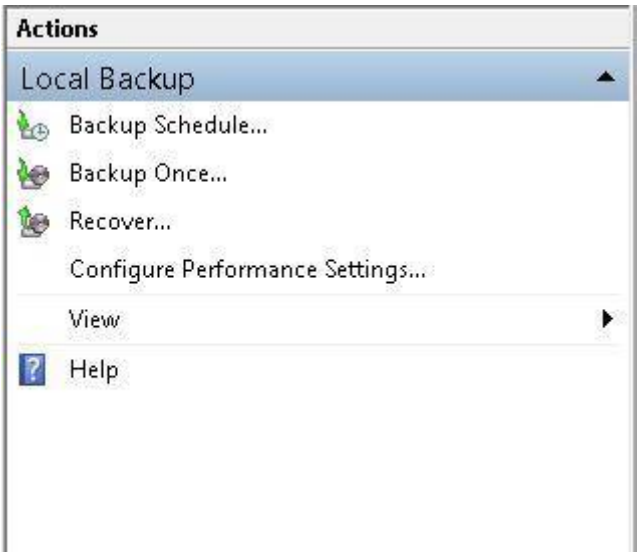
Go to the Tools option provided by the Server Manager, left-click on it and scroll down to the "Windows Server Backup" option.

Now this type of option will be opened:

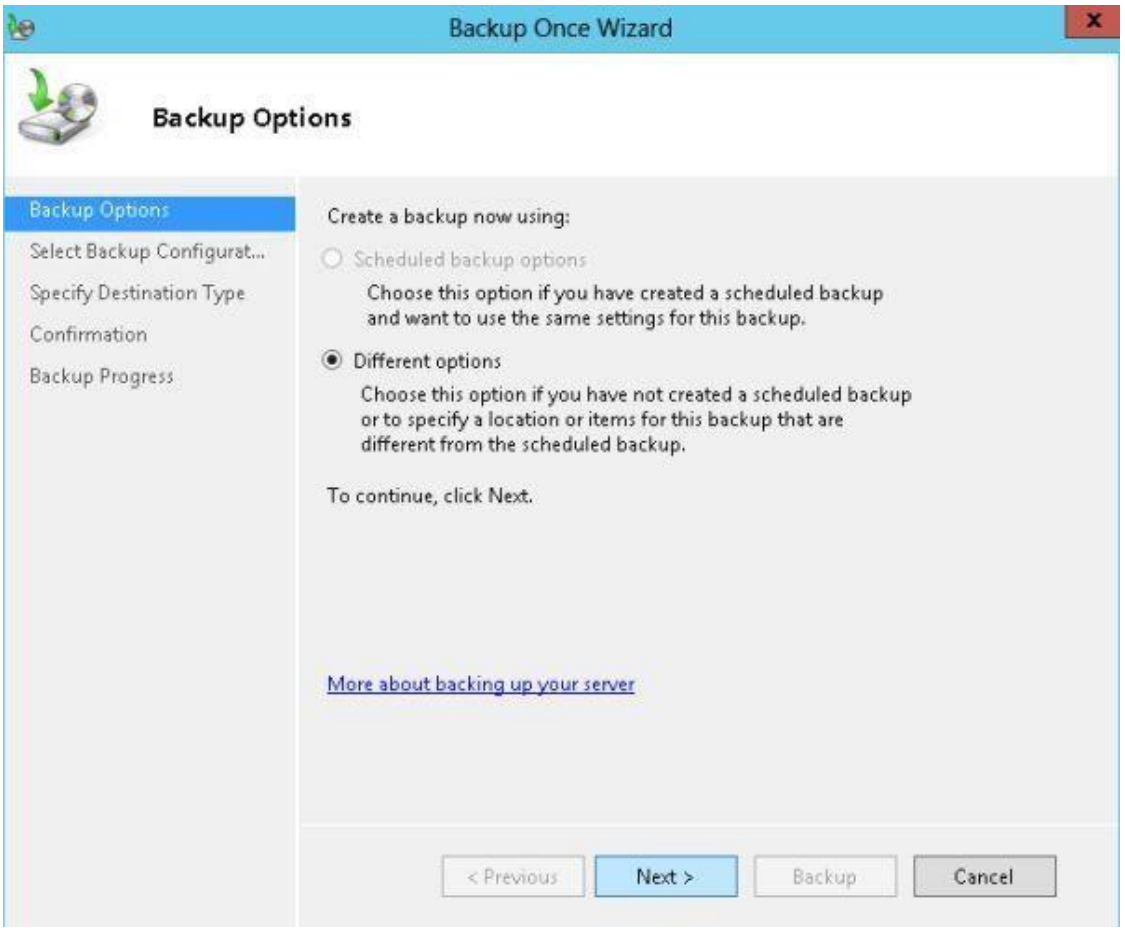


Step 2

In the Local Backup option user will get a few options like "Backup Schedule", "Backup Once", "Recover". So, here click on "Backup Once".

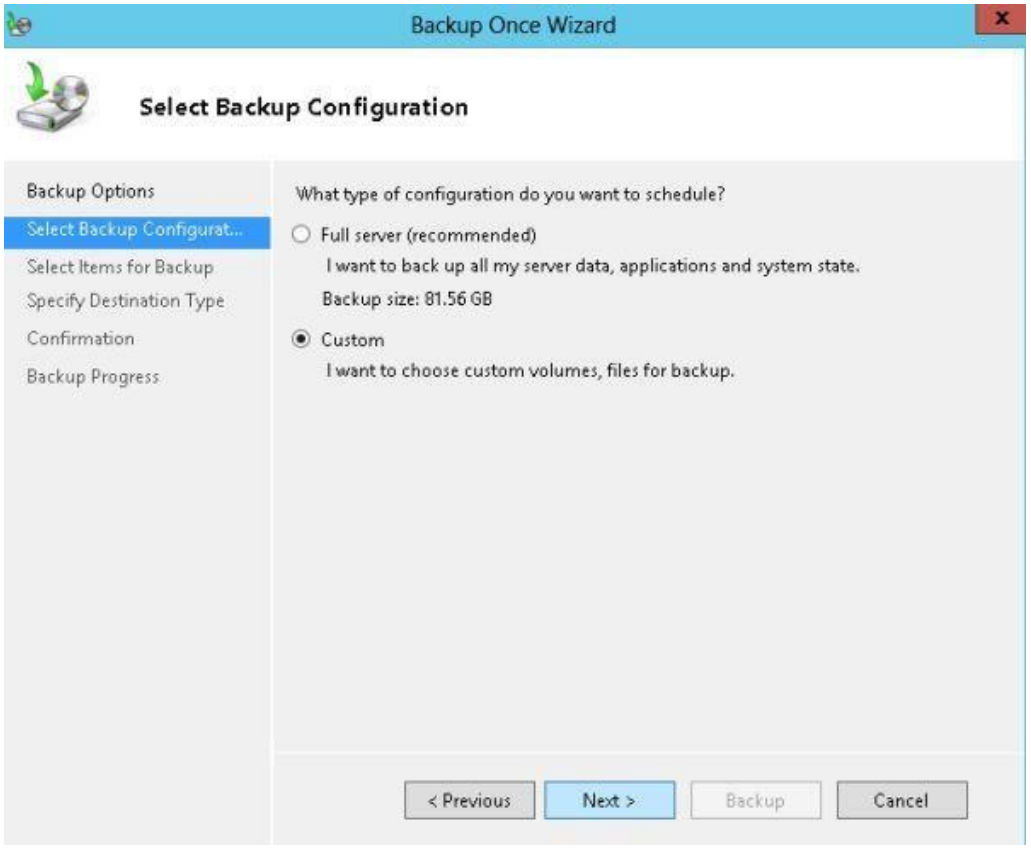


Now "Backup Options" will be available. "Different Options" and then click on "Next".

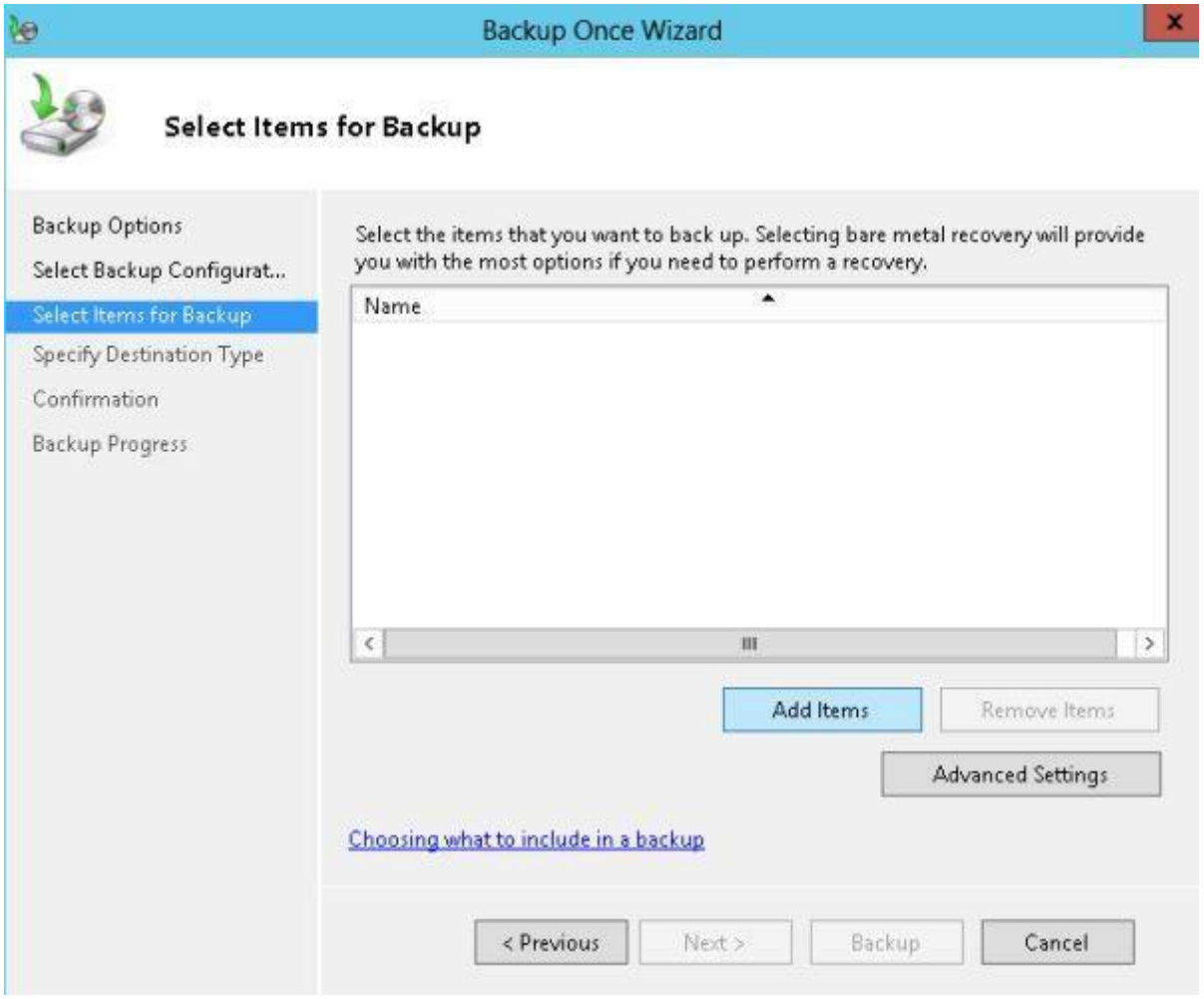


Step 3

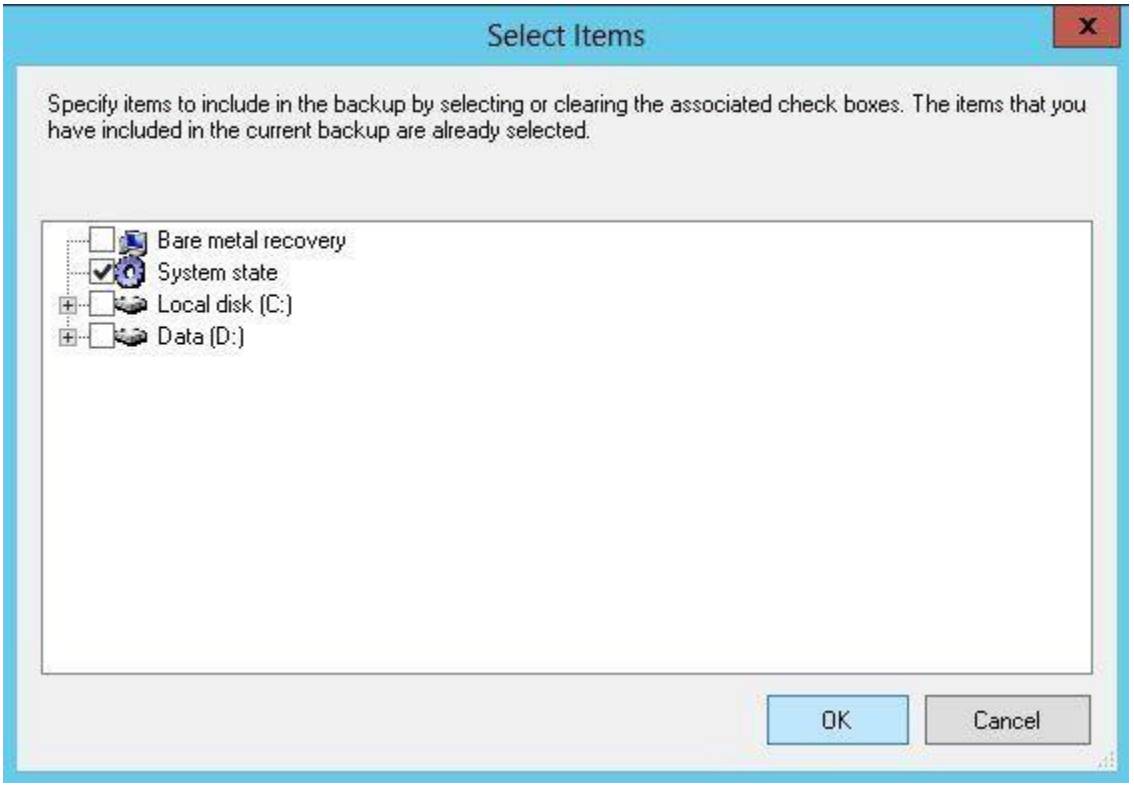
Now "Backup Configuration" will be available from which user can either select to create a backup of the "Full Server" or select the "Custom Option".



On the next page click on "Add Items".

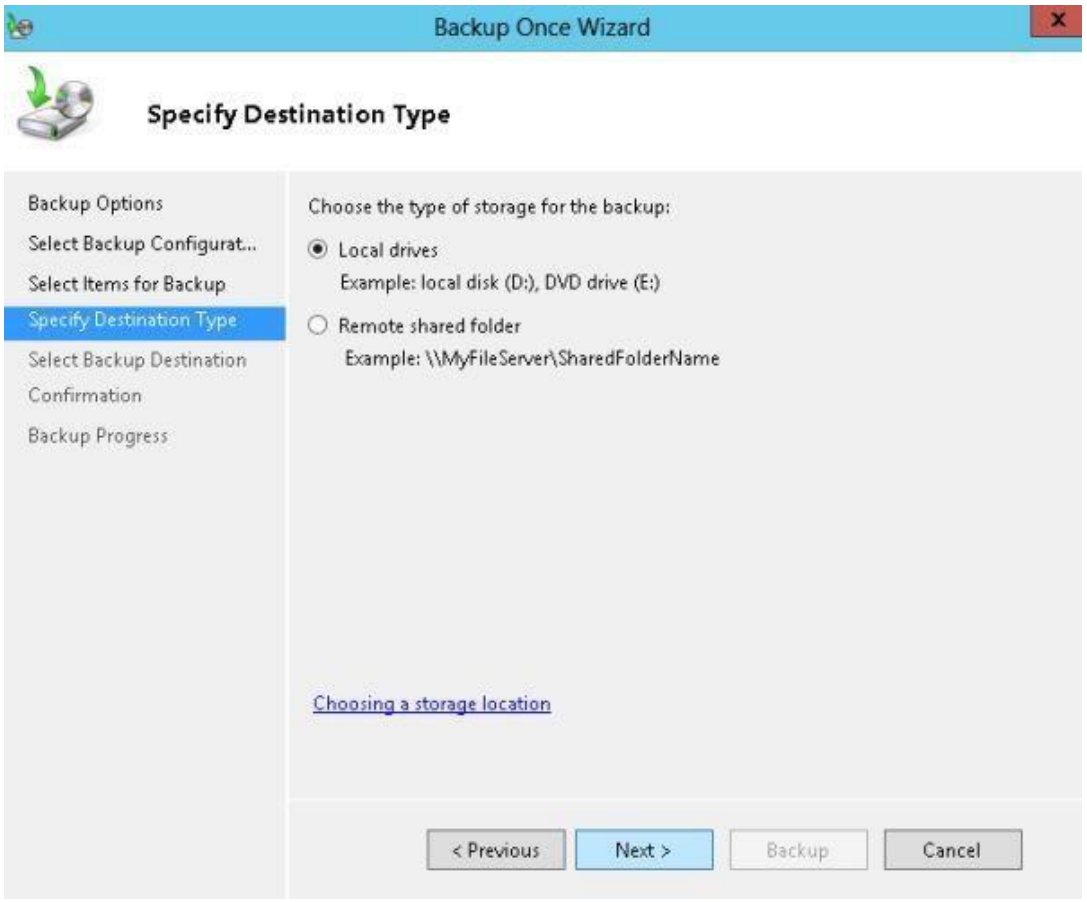


From the options user can select any Drive or System State or both. Here It will create a backup of only the System State so select it and click on the "OK" button.

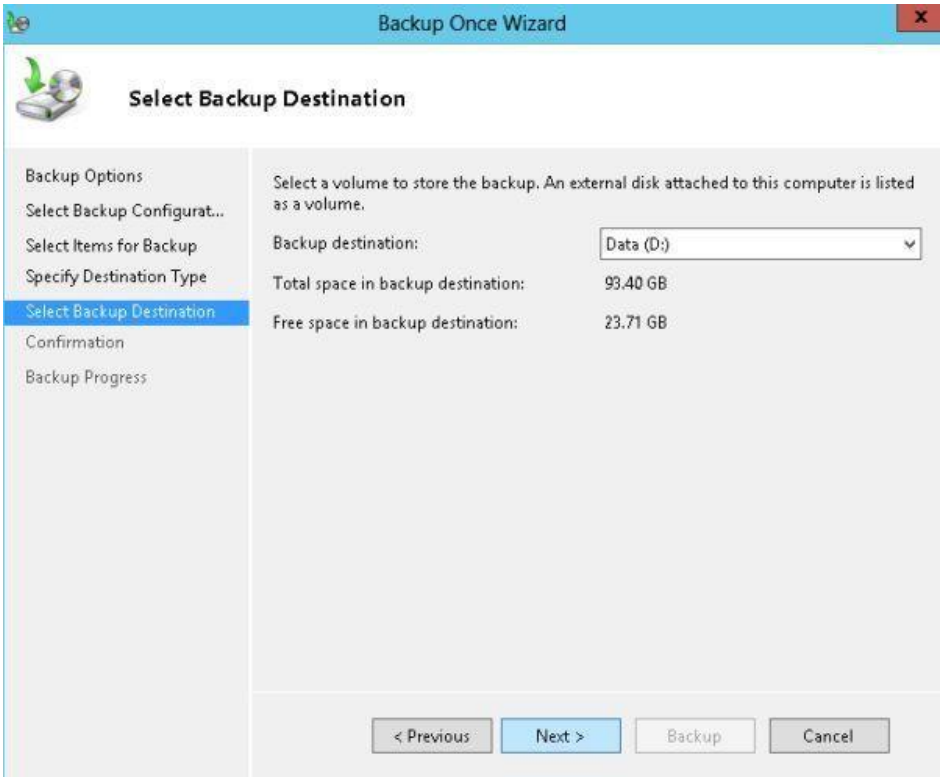


Step 4

Now user must select the "Destination Type" that can be either a "Local Drive" or any remotely shared folder.

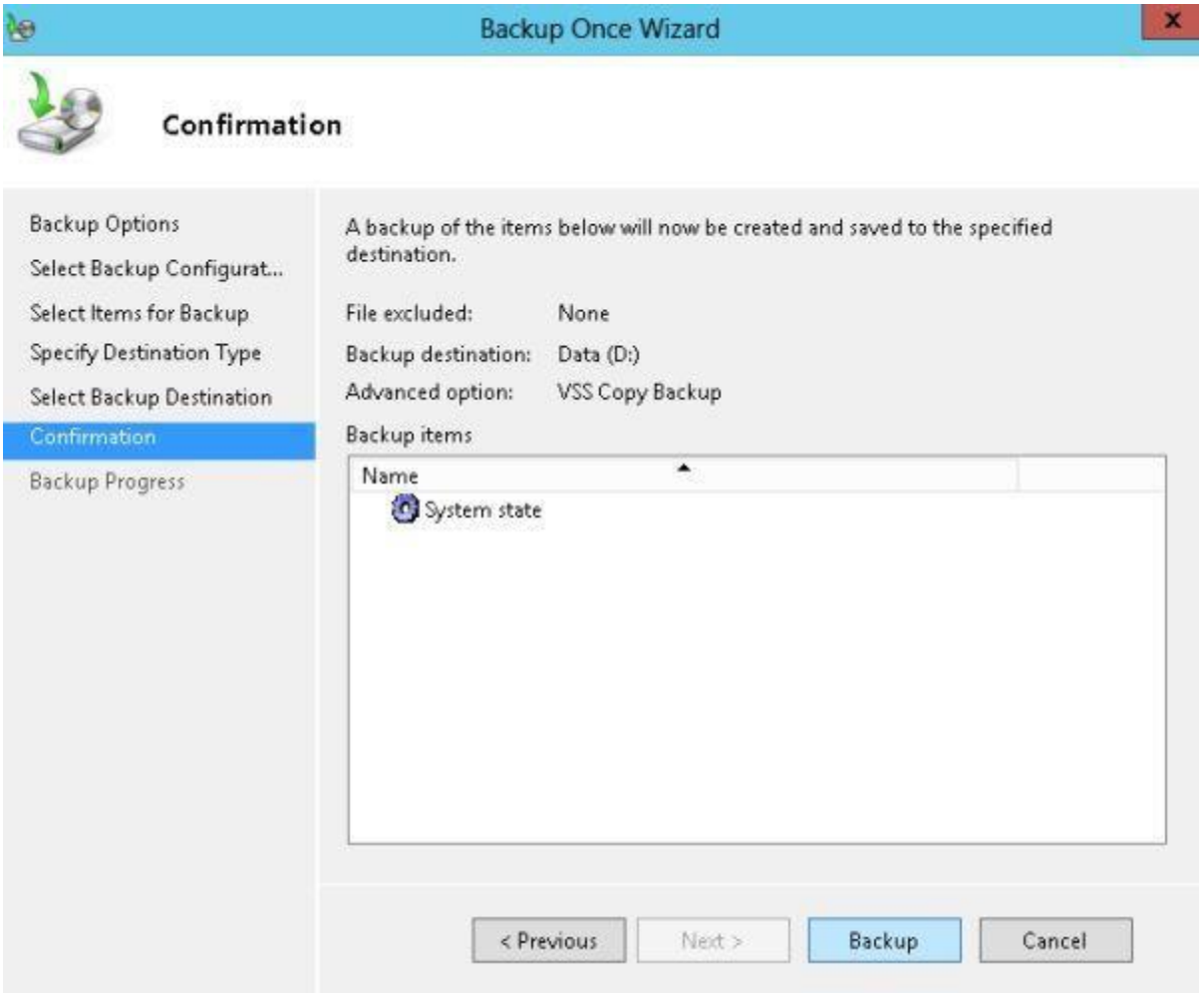


Since here I selected the Local Drive, it will ask me in which drive I would like to create the backup and how much space is available in that drive. After that click on "Next".

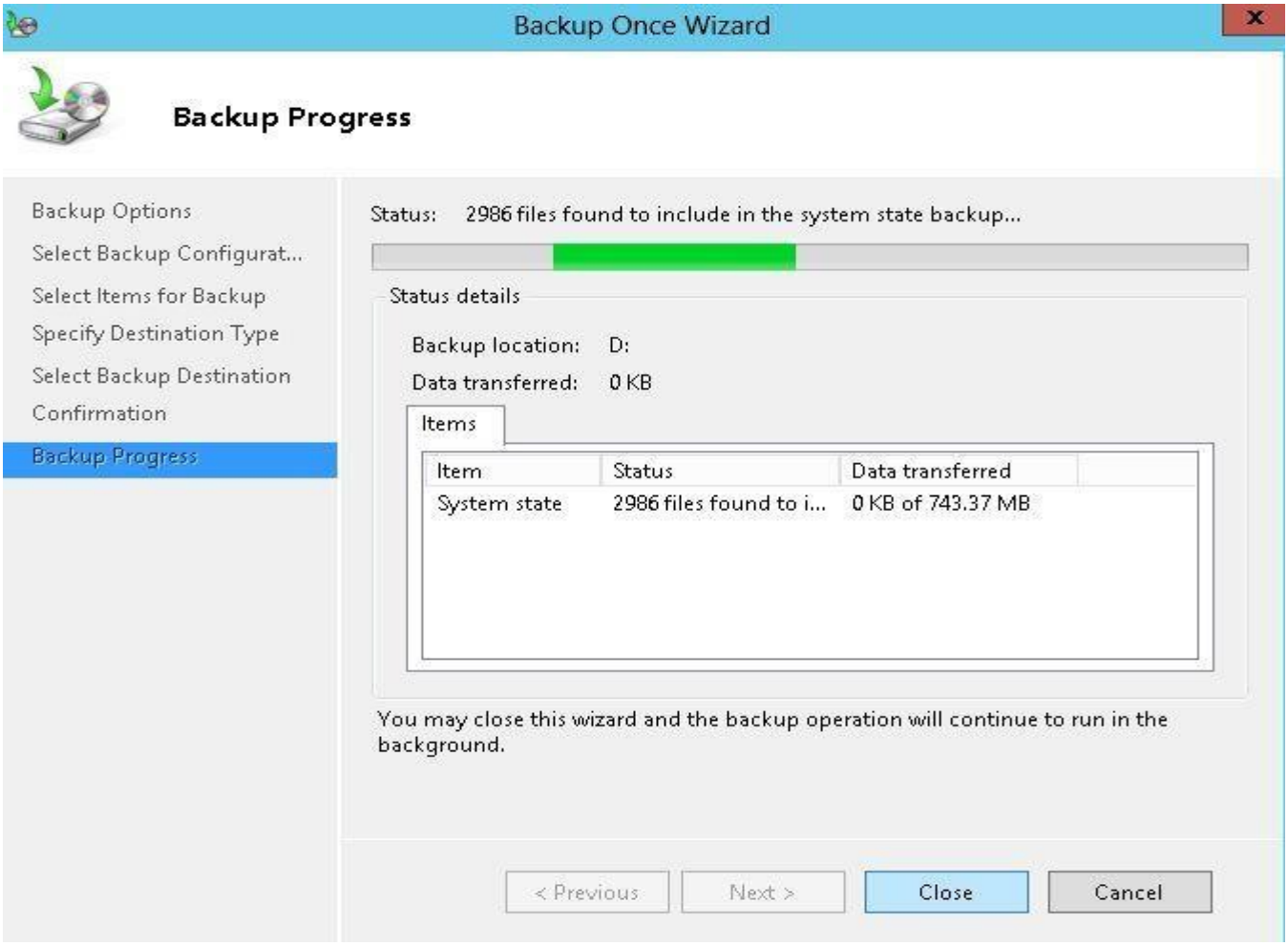


Step 5

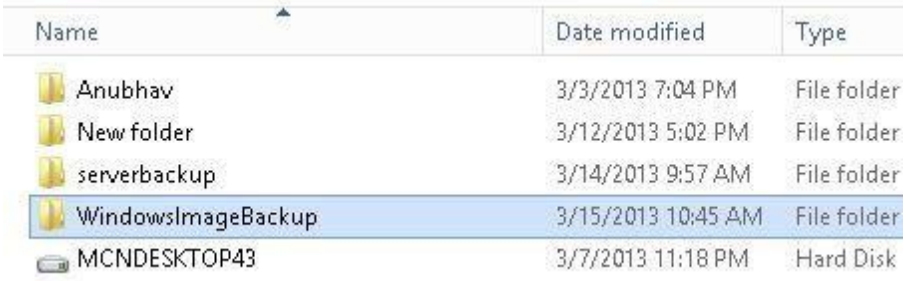
Now a Confirmation Page will be shown that will show the full details of whatever the user selected and will finally ask to give permission to create the backup. Click on "Backup" to start the backup.



Now the backup will begin and within a few minutes the backup will have been created.



Now specify the drive and ensure that the backup was created.



Result

Thus the Backup and Backup Schedule was created successfully.

Ex.No 9 Auditing File access on File server

Aim

To audit files and folders access on server.

Components Required

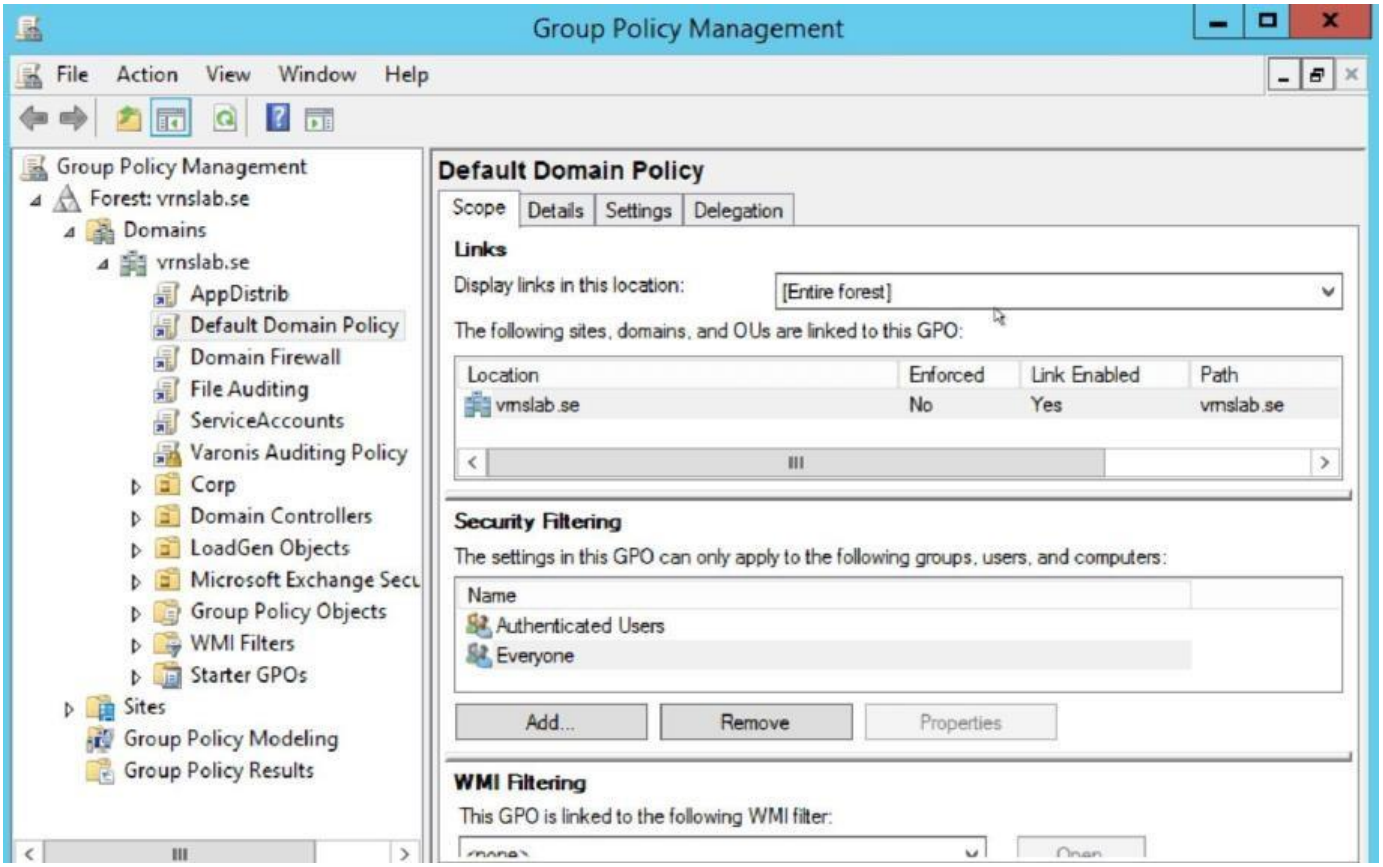
1. PC with server 2012

Auditing

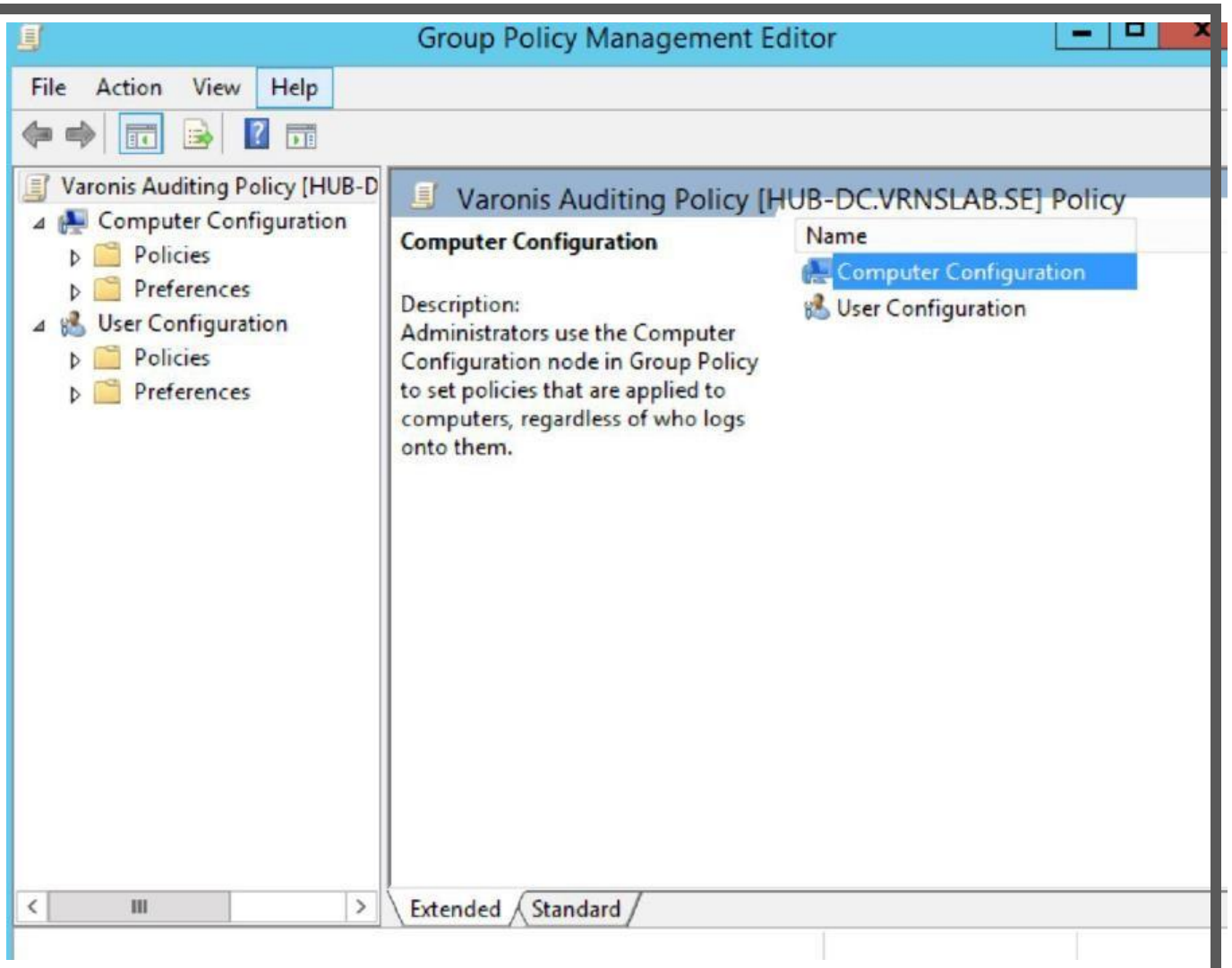
Windows file server auditing is a great way to monitor what is going on with all the files stored on your company's servers. You can find out who is accessing files, creating new files, deleting files, copying files, and moving files.

Step 1: Enable Audit Policy

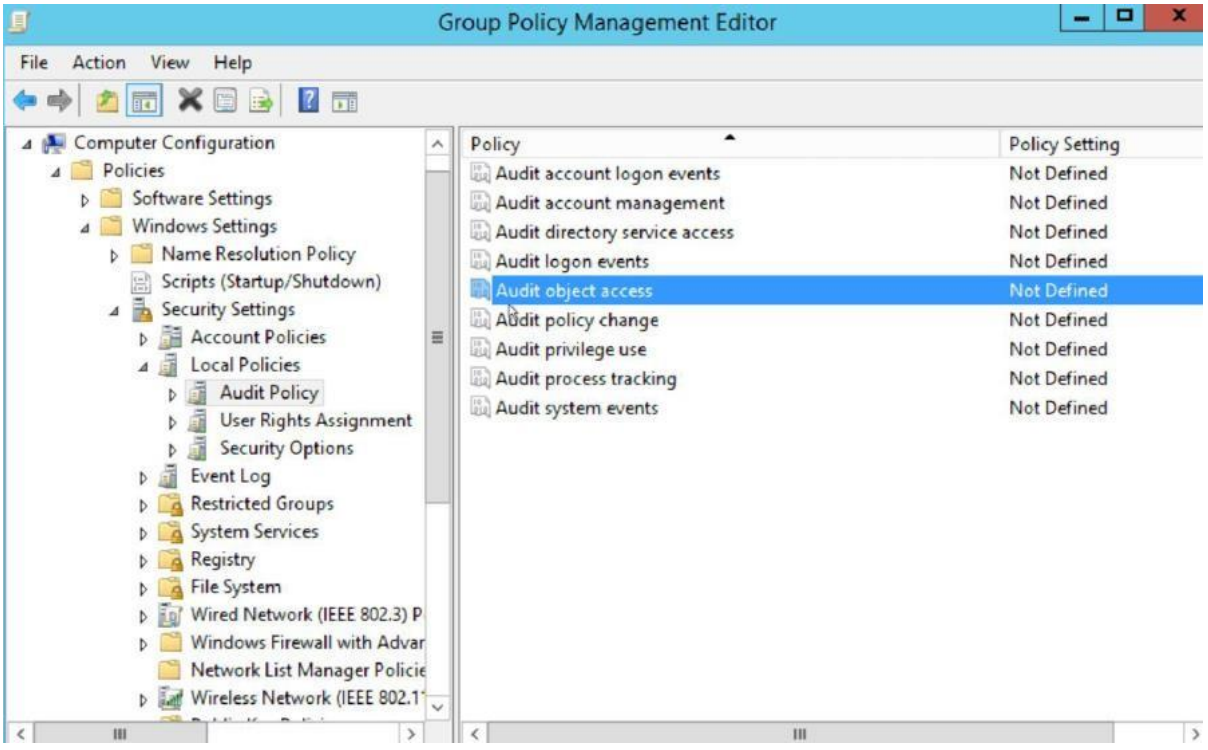
First, go to the Domain Controller (DC) and update the Group Policy (GPO) to enable file auditing.



Right click on the Group Policy that user want to update or create a new GPO for file auditing. In the right- click menu, select edit to go to the Group Policy Editor.

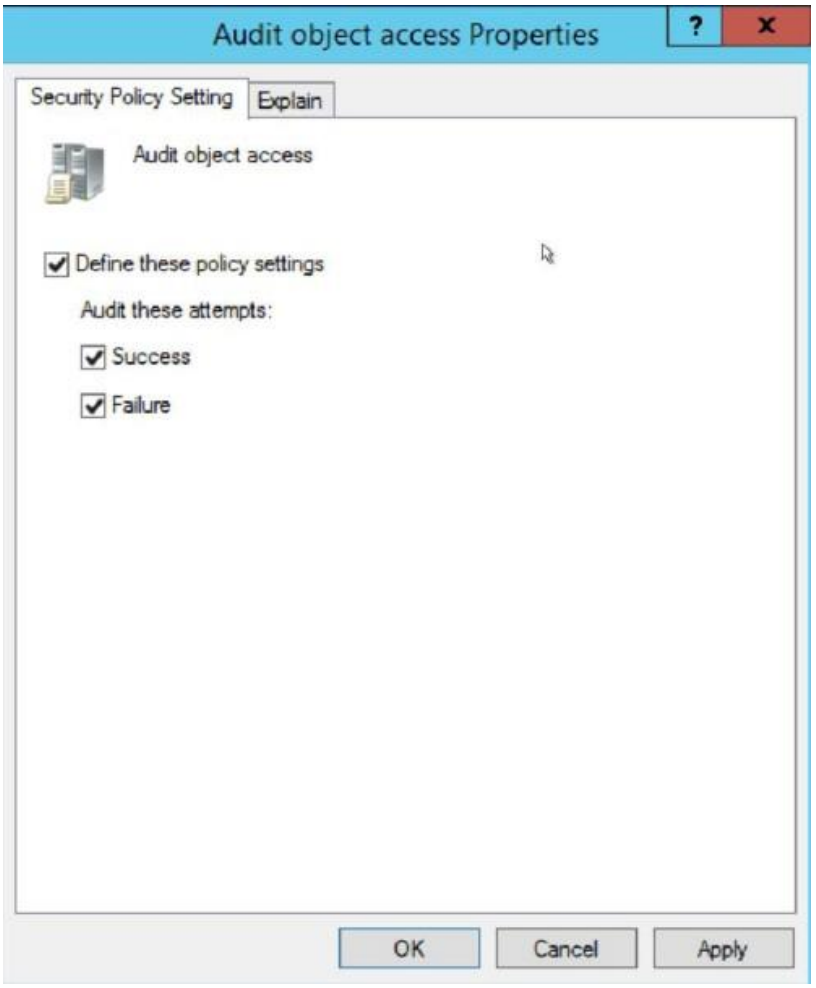


In the Group Policy editor, click through to Computer Configuration -> Policies -> Windows Settings -> Local Policies. Click on Audit Policy.

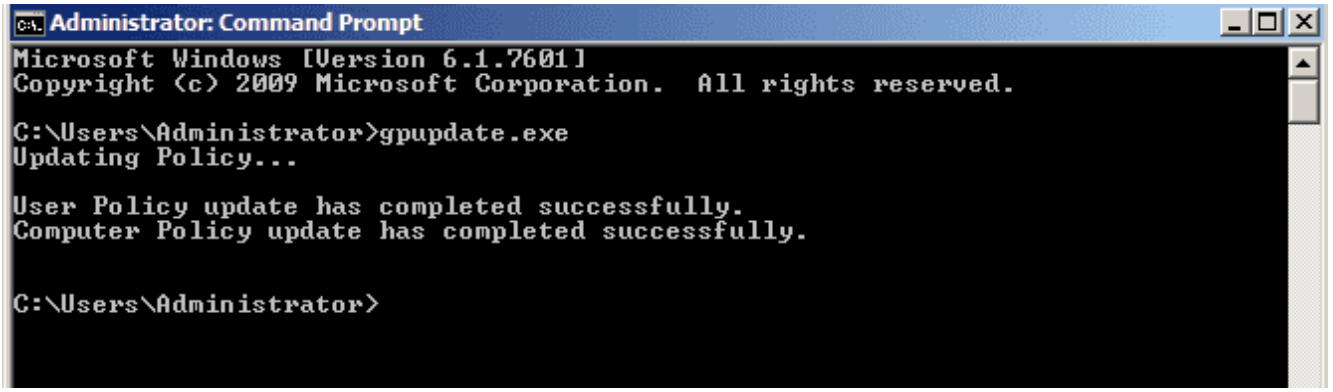


User can add many auditing options to Windows Event Log. The option for file auditing is the “Audit object access” option.

Double-click “Audit object access” and set it to both success and failure.

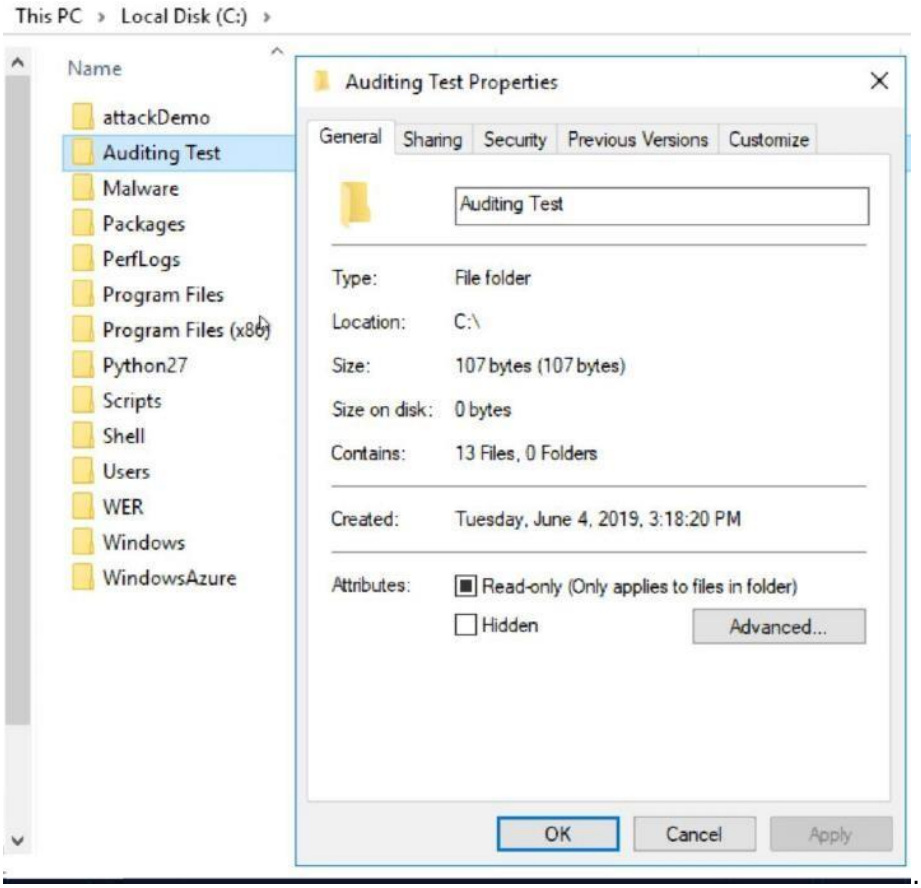


To enable the new GPO, go to a command line and run ‘gpupdate /force’.

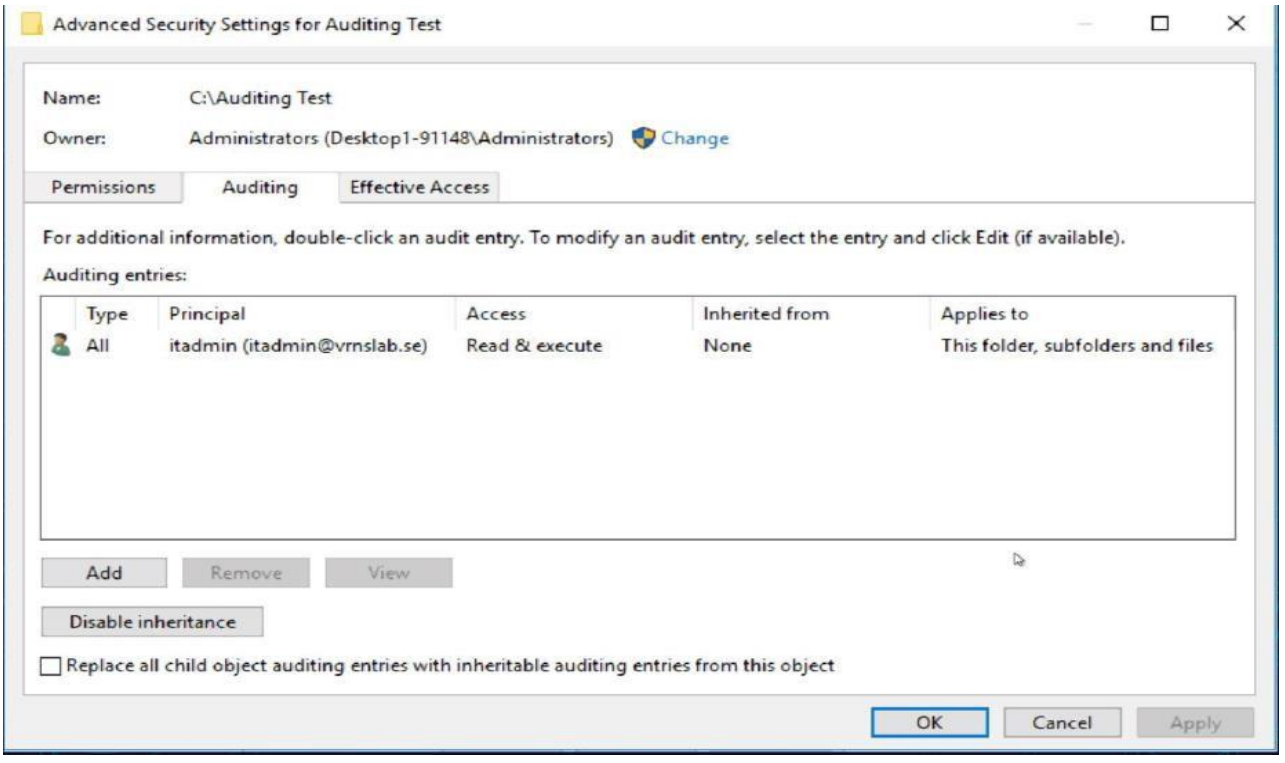


Step 2: Apply Audit Policy to Files and/or Folders

Right-click the file or folder in Windows Explorer. Select Properties

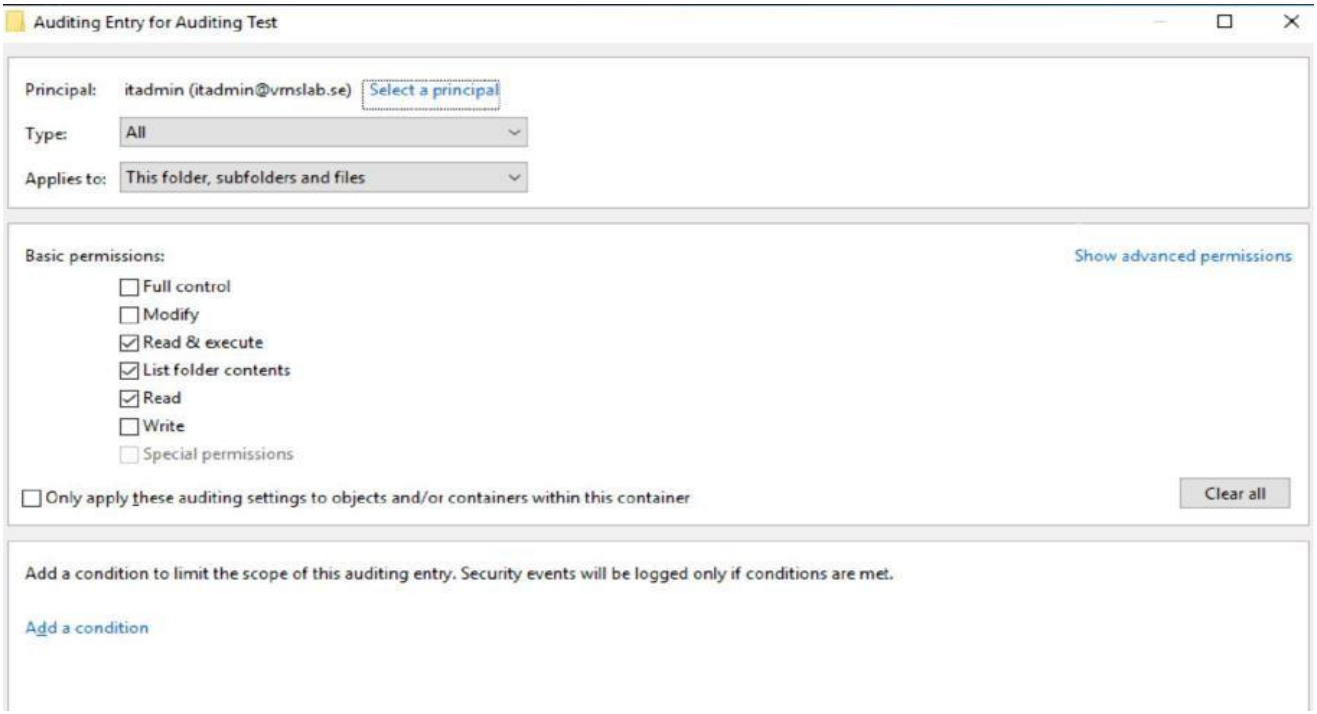


2. Change to the Security tab and click Advanced.



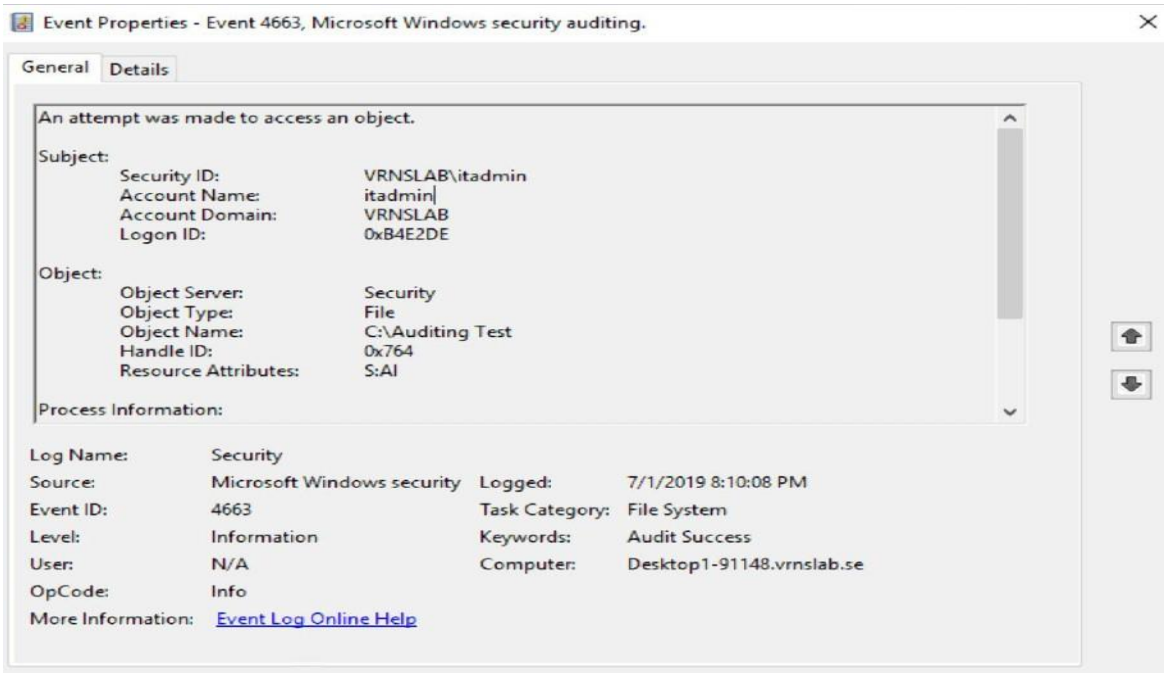
3. Click the Auditing tab and then Continue.

4. Add the Users or Groups that you want to audit and check all of the appropriate boxes.



Step 3: Open Event Viewer

Open Event viewer and click security in the Windows logs.



Result

Thus, the File auditing on File server was successfully completed.

Ex.No 10 Configuring Remote Server Administration

Aim

To Configure Remote Server Administration.

Components Required

1. PC with server

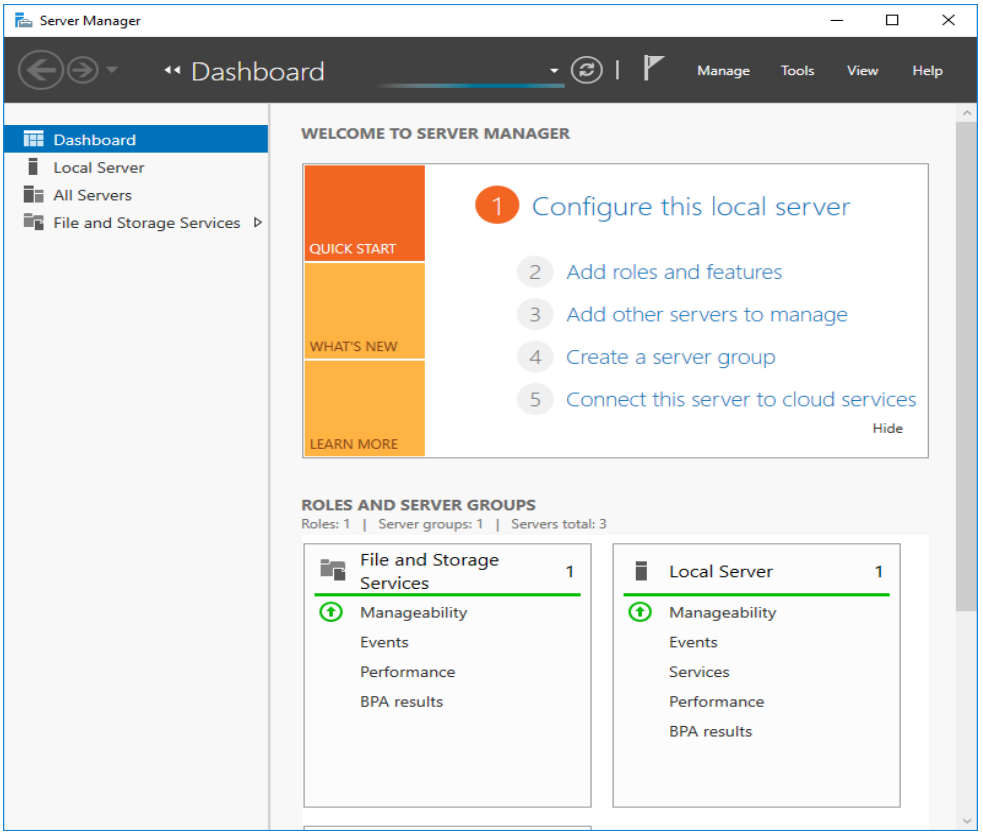
RSAT (**Remote Server Administration** Tools) is a Windows **Server** component for **remote** management of other computers also running that operating system. **RSAT** allows administrators to run snap-ins and tools on a **remote** computer to manage features, roles and role services.

It allows users to access the system they **need** when they can't be available physically for connecting. To put, users access the systems **remotely** through telecommunications or internet connection. **Remote** Access Services is effectively used by organizations for internally connecting networks and the system as well.

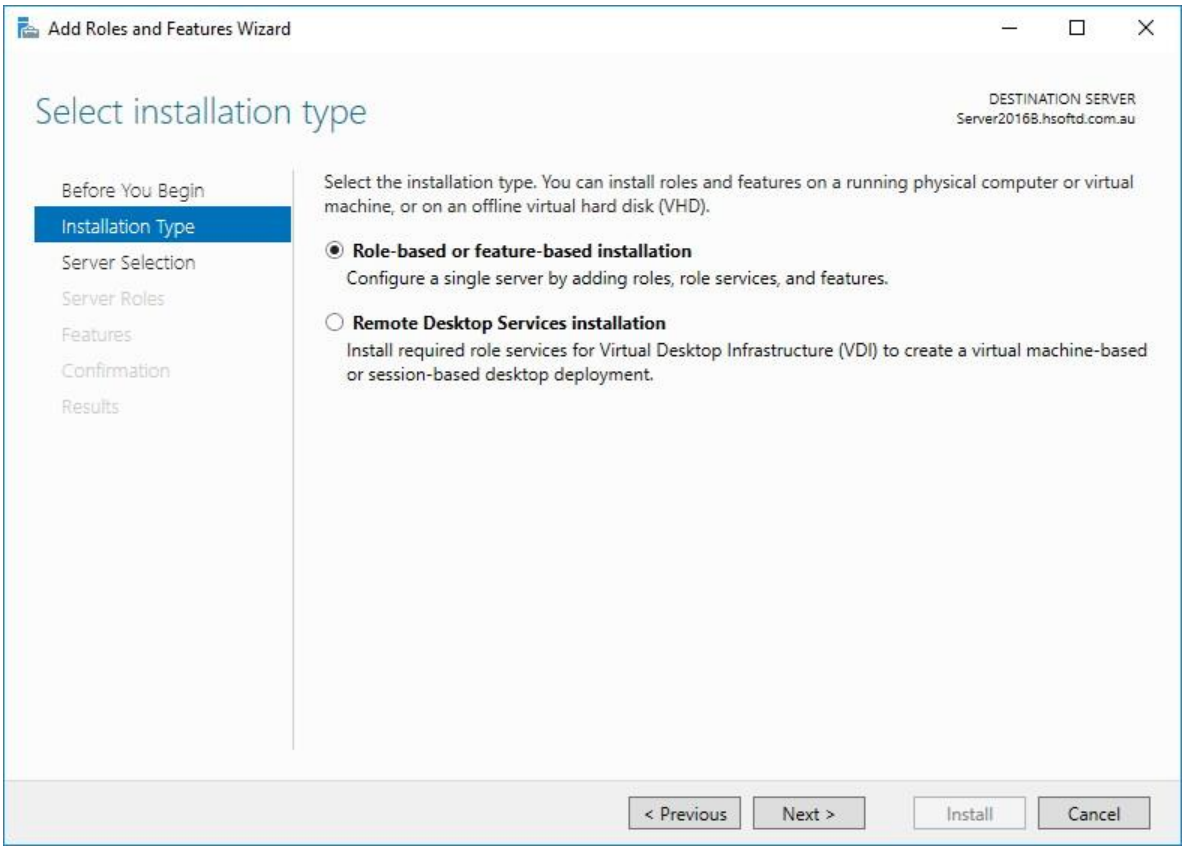
The following tools are included as part of the installation:

- SMTP Server Tools
- Hyper-V Management Tools
- Hyper-V Module for Windows PowerShell
- Hyper-V GUI Management Tools
- Windows Server Update Services Tools
- API and PowerShell cmdlets
- User Interface Management Console
- Active Directory Users and Computers Snap-in
- Active Directory Sites and Services Snap-in
- Active Directory Domains and Trusts Snap-in
- Active Directory Administrative Center Snap-in
- ADSI Edit Snap-in
- Active Directory Schema Snap-in (Not Registered)
- Active Directory Command Line Tools
- Active Directory Module for Windows PowerShell
- IIS Management Tools
- IIS Management Console
- IIS Management Compatibility

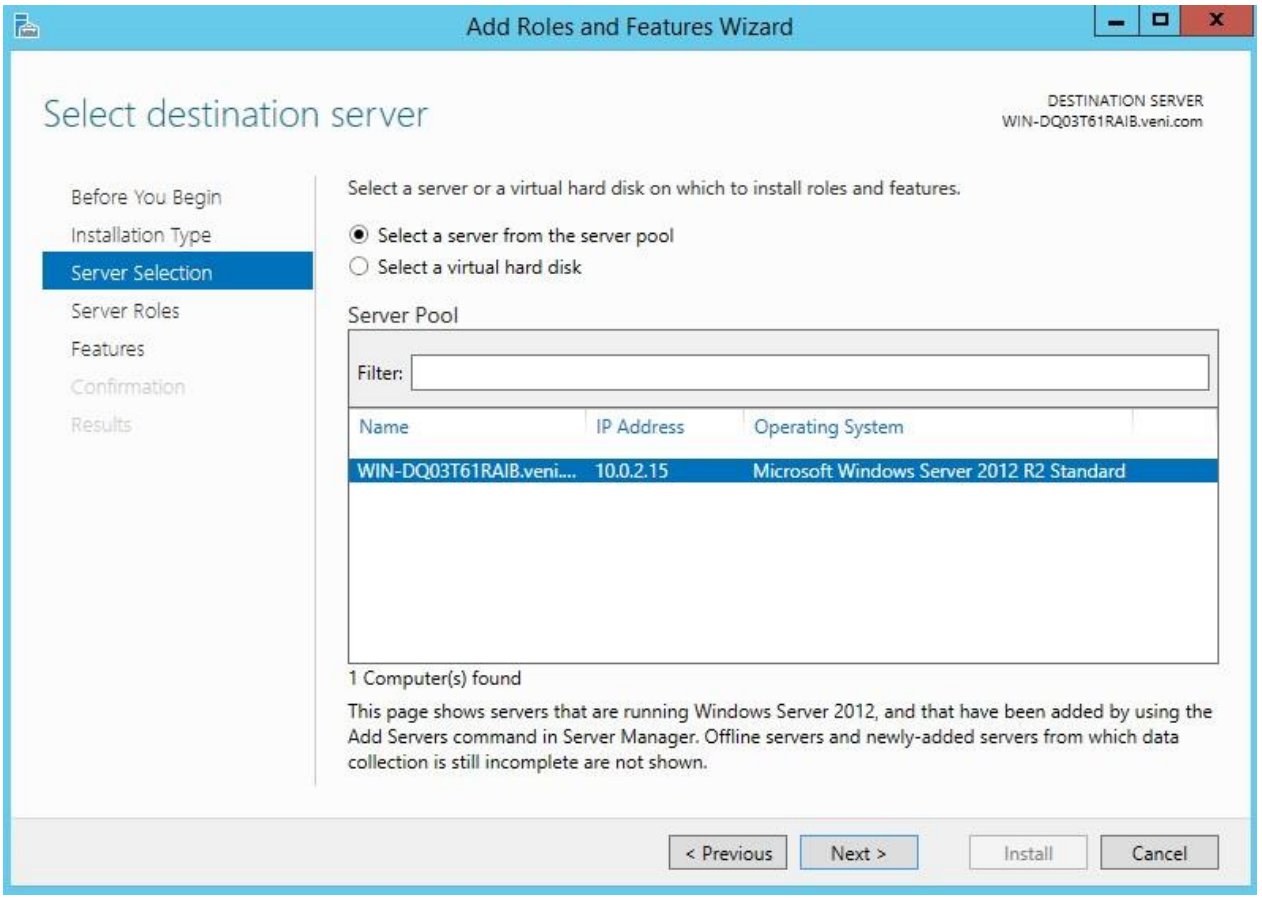
1. On the Server Manager main windows Click “Add roles and features”.



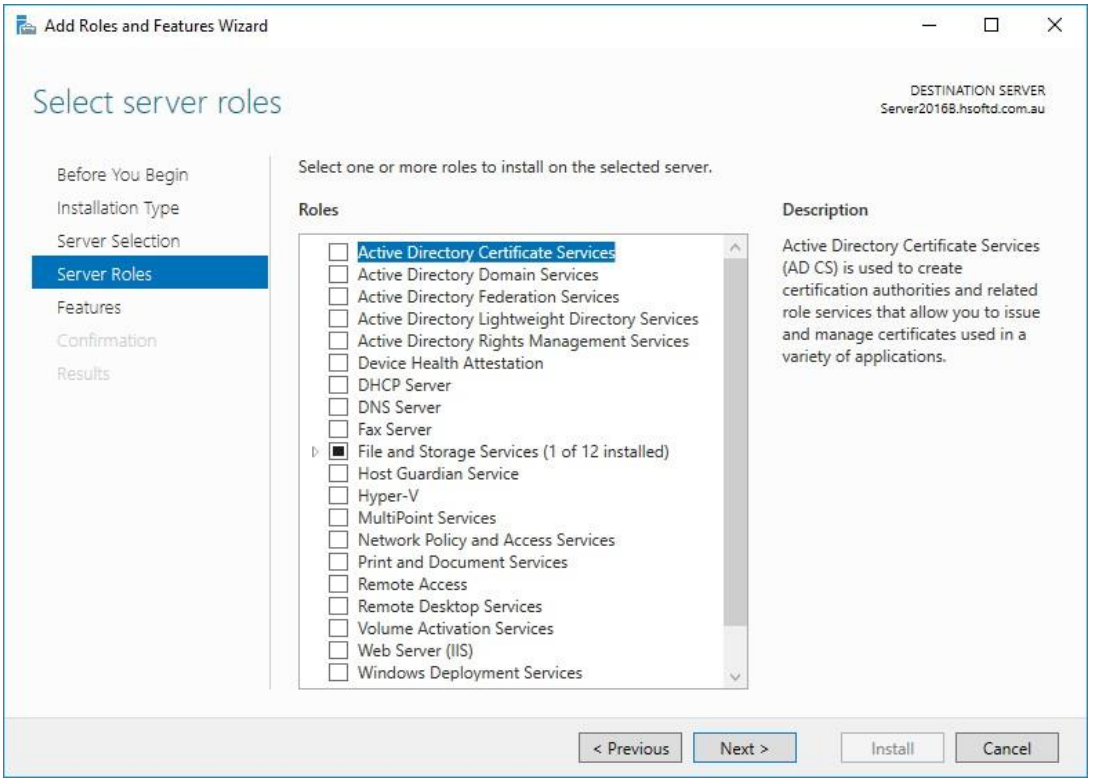
2. In the “Add Roles and Features Wizard” under “Installation Type” check the “Role-based or feature- based installation” radio button and click “Next”



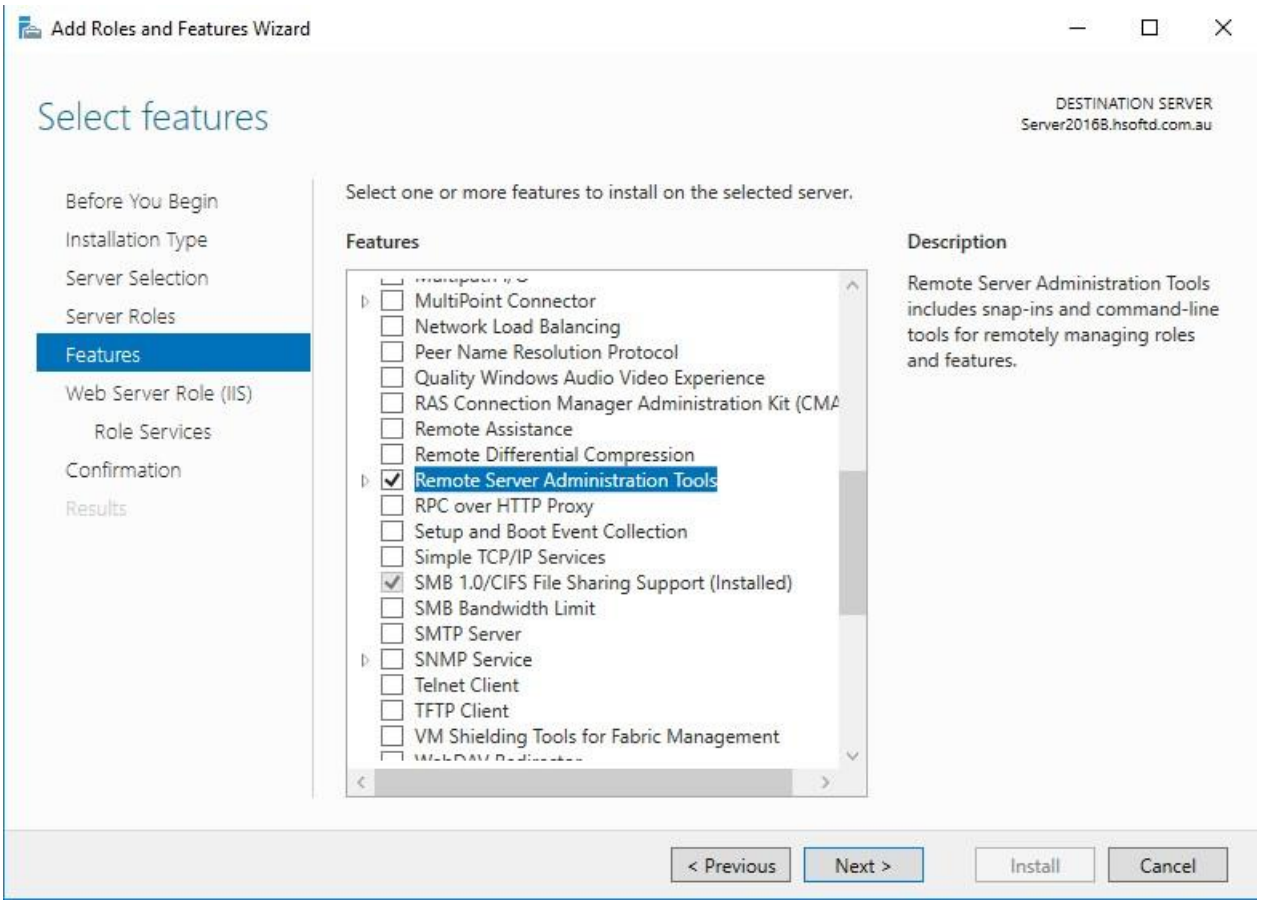
3. In the “Add Roles and Features Wizard” under “Server Selection” check the “Select a server from the server pool” radio button, select the server you want to install the Remote Server Administration Tools (RSAT) on and click “Next”



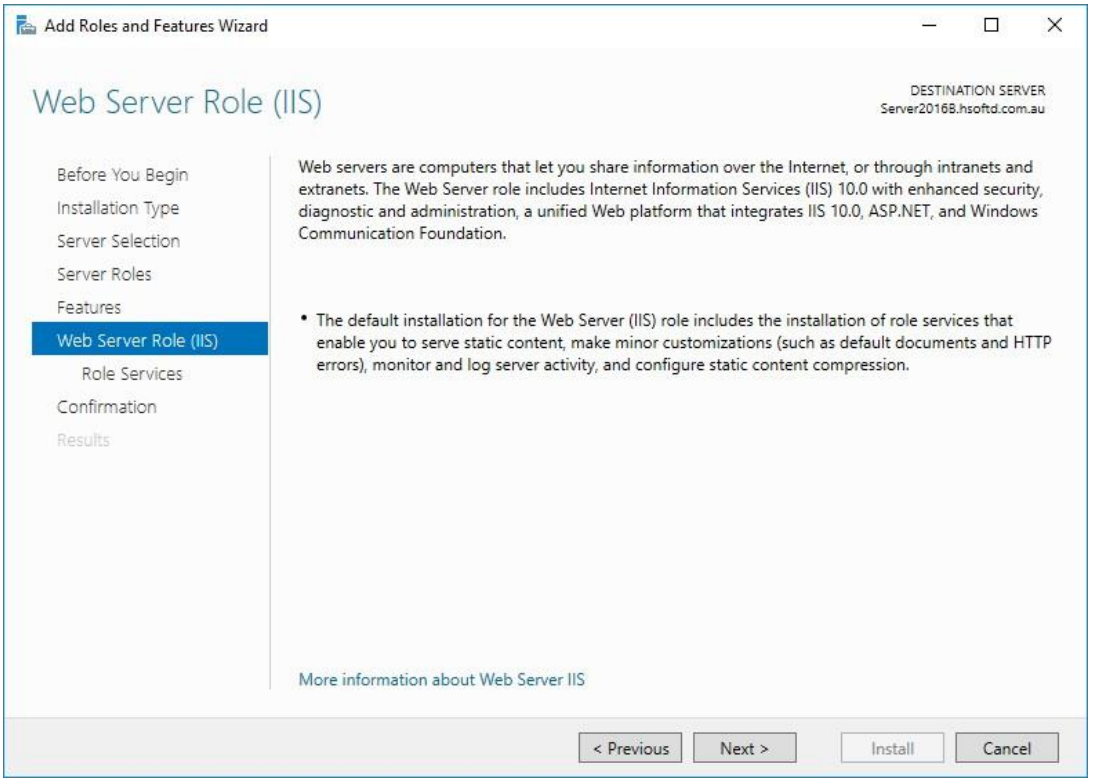
4. In the “Add Roles and Features Wizard” under “Server Roles” click “Next”



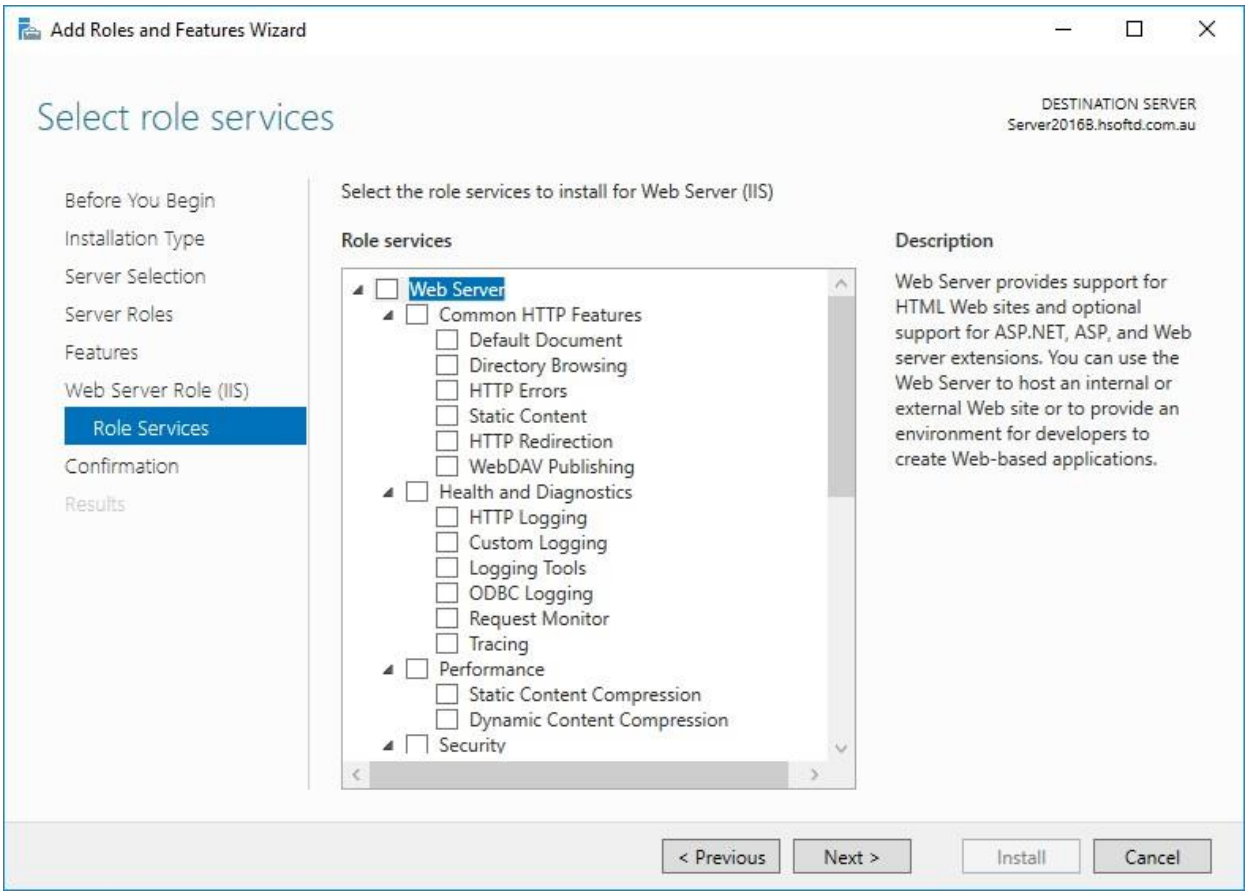
5. In the “Add Roles and Features Wizard” under “Features” scroll down and check the “Remote Server Administration Tools” check box. Click “Next”.



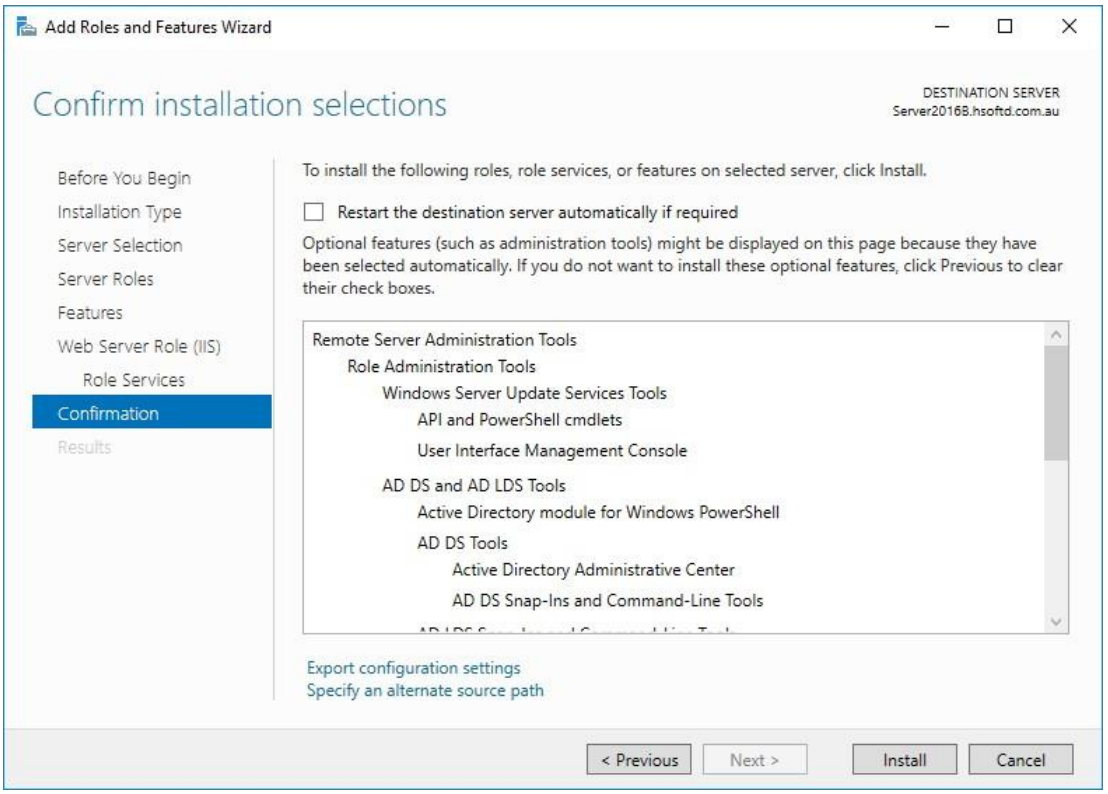
6. If prompted to add features accept the defaults and click “Add Features”, then click “Next”.



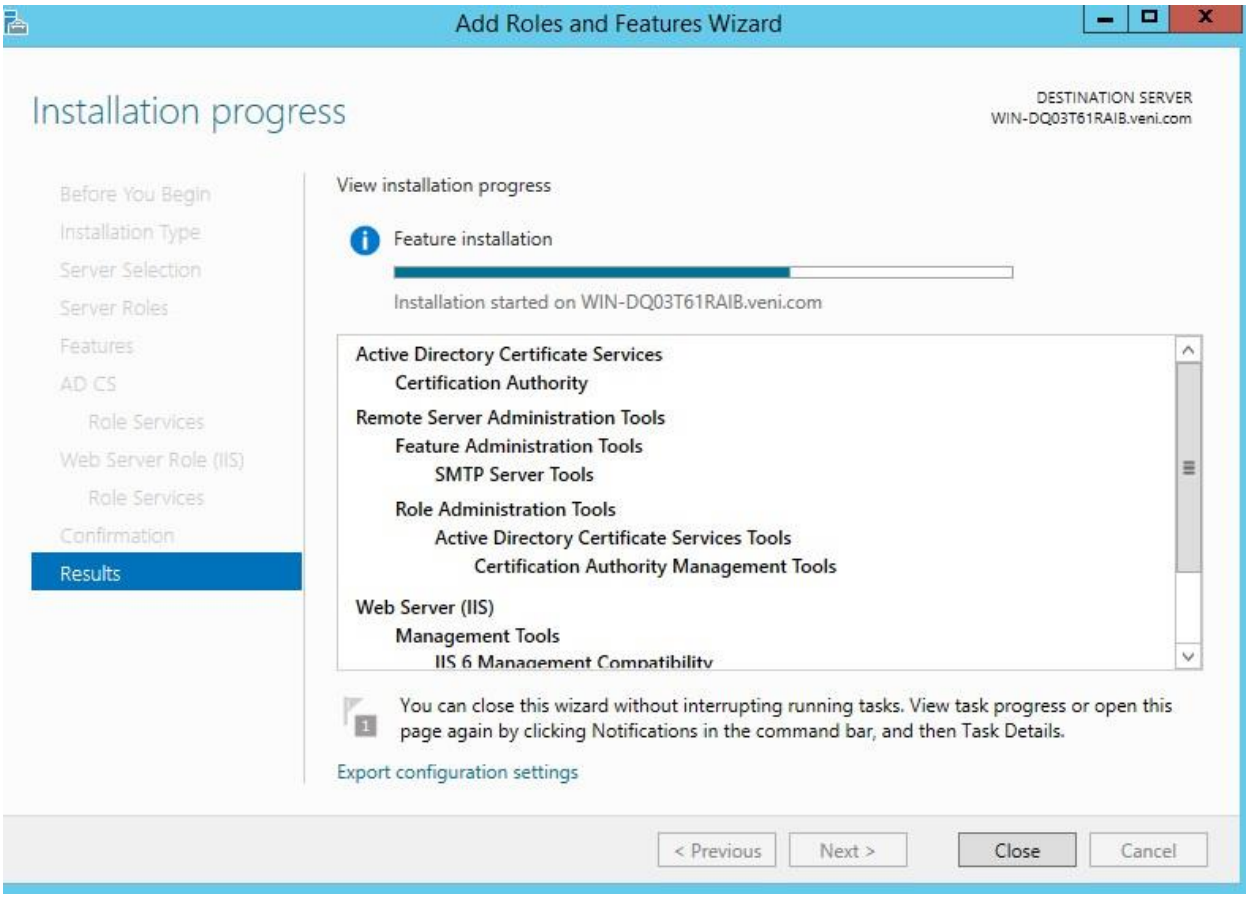
7. If the Web Server Role page displays, accept the defaults and click “Next”



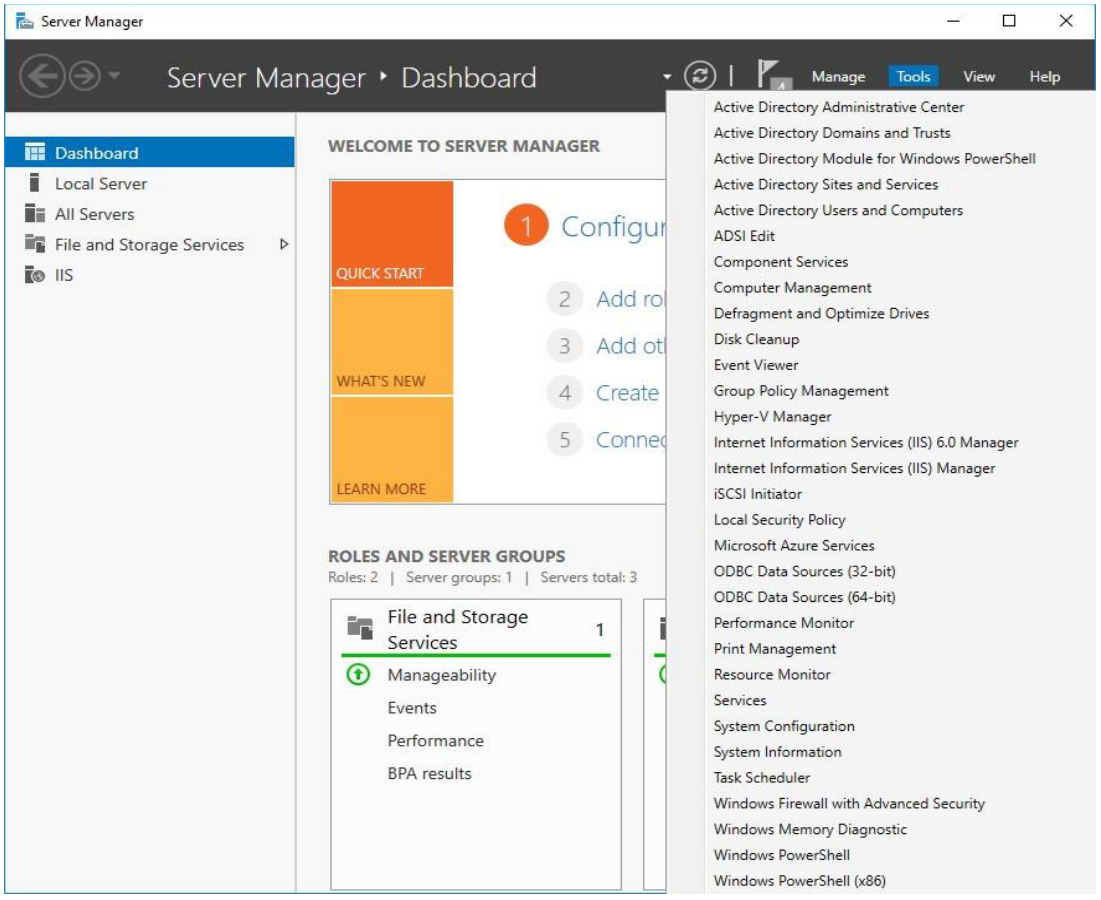
8. In the “Add Roles and Features Wizard” at the “Confirmation” page click “Install” to begin the installation of the Remote Server Administration Tools (RSAT)



9. The installation of the Remote Server Administration Tools (RSAT) will begin and the progress will be displayed. This installation should not require a restart of the server.



10 .When the installation of the Remote Server Administration Tools (RSAT) is complete you can find the RSAT tools under the “Tools” menu in “Server Manager”.



Result

Thus the Remote server administration was configured successfully.