

Windows Server® 2012

MICROSOFT CERTIFIED SOLUTIONS EXPERT (MCSE) THEORY & LAB

Student Name: _____

Faculty Name: _____ Aravinda Kumar V _____

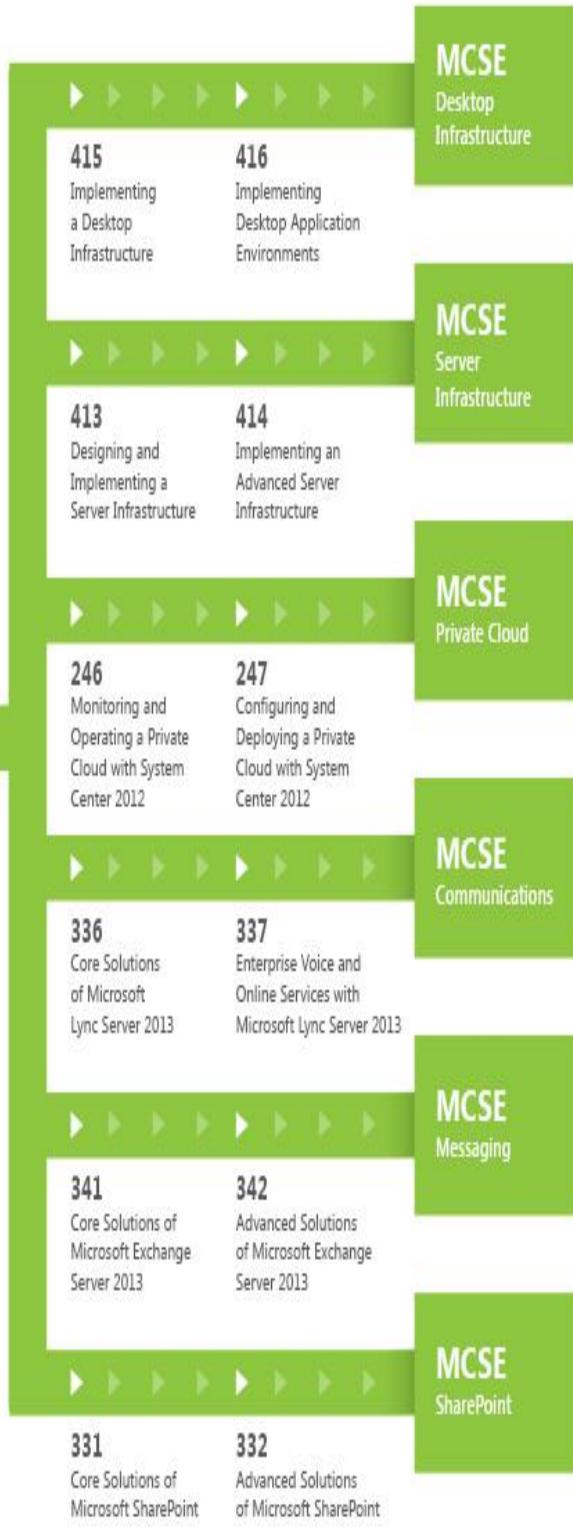
Branch Name: _____

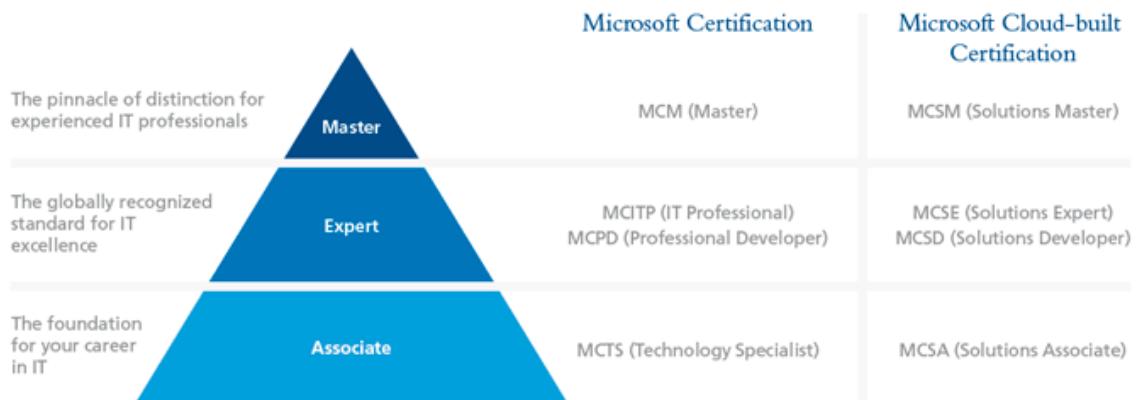
Batch Date : _____

Server Pathway



MTA IT Infrastructure 349, 365, 366, 367	410 Installing and Configuring Windows Server 2012	411 Administering Windows Server 2012	412 Configuring Advanced Windows Server 2012 Services	MCSA Windows Server 2012
---	---	---	--	---------------------------------------





INDEX

Sr. No.	Topic	Page No.
1	Installation Of Windows Operating System Lab – 1: Installing Windows Server 2012 Operating System Or Installing Windows 7 Operating System Lab – 2: Creating Local User Accounts Lab – 3: Conversion from GUI to Server Core Lab – 4: Conversion from Server Core to GUI	14 15 26 37 39 41
2	Ip address & Logical topologies & Active Directory Lab – 1: Assigning IP Address Lab – 2: Installing Active Directory	43 51 54
3	Member Server/Client and User Management Lab – 1: Configuring Client Or Configuring Member Server Lab – 2: Creating Domain User Accounts Lab – 3: Changing Default Password Policy Lab – 4: Enabling Account Lockout Policy Lab – 5: Configuring Log On To and Logon hours permissions Lab – 6: Changing Allow Logon Locally Policy	66 70 72 75 77 82 86 88
4	Permissions Lab – 1: Security Level Permissions Lab – 2: Share Level Permissions Lab – 3: Adding Mapped Drives Lab – 4: Verifying Access Based Enumeration	91 95 97 99 101
5	Profiles & File Server Resource Manager (FSRM) Lab – 1: Configuring Local Profiles Lab – 2: Configuring Roaming Profiles Lab – 3: Configuring Home Folder Lab – 4: Installing FSRM Role Service Lab – 5: Configuring Quota Limits using FSRM Lab – 6: Configuring File screening using FSRM Lab – 7: Configuring Storage Reports Management	103 109 110 113 114 119 122 126

6	Organizational Unit & Distributed File System (DFS)	129
	Lab – 1: Creating an Organizational Unit (OU)	133
	Lab – 2: Delegating Control to a User	135
	Lab – 3: Groups	137
	Lab – 4: Install DFS Namespace	140
	Lab – 5: Creating DFS Namespace	145
	Lab – 6: Creating DFS Folders	149
7	Logical Structure of Active Directory	152
	Lab – 1: Configuring Additional Domain Controller	155
	Lab – 2: Configuring Child Domain	165
	Lab – 3: Configuring New Domain Tree in Existing Forest	175
8	Roles of Active Directory	185
	Lab – 1: Transfer of Roles	190
	Lab – 2: Seizing of Roles	197
9	Group Policies	205
	Lab – 1: Applying Group Policy on OU Level	212
	Lab – 2: Applying Group Policy on Domain Level	216
	Lab – 3: Applying Group Policy on Site Level	220
	Lab – 4: Applying Group Policy Modeling	224
	Lab – 5: Applying Software Deployment Policy	227
	Lab – 6: Applying Scripts using Group Policy	232
	Lab – 7: Applying Folder Redirection	234
	Lab – 8: Applying Auditing Policy	238
	Lab – 9: Configuring Preferences using Item-level targeting	242
10	Trust Relationship	246
	Lab – 1: Creating Forest Trust	253
	Lab – 2: Active Directory Recycle Bin	264
11	Global Catalog, Sites and RODC	268
	Lab – 1: Configuring Global Catalog Server	274
	Lab – 2: Creating Active Directory Sites	275
	Lab – 3: Creating Active Directory Site-Links	279
	Lab – 4: Creating a Pre-Create RODC Account.	281
	Lab – 5: Configuring Read-Only Domain Controller	288

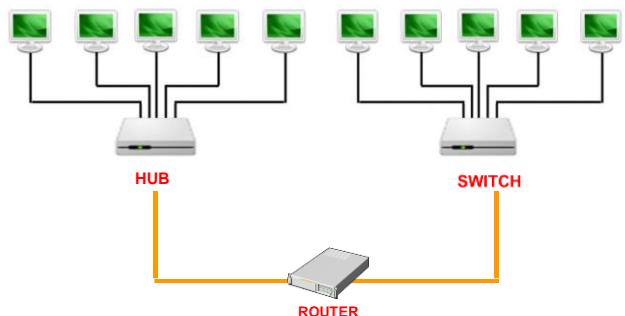
Sr. No.	Topic	Page No.
12	Dynamic Host Configuration Protocol (DHCP) Lab – 1: Installing DHCP Service Lab – 2: Creating a Scope Lab – 3: Creating DHCP Reservations Lab – 4: DHCP Server Backup and Restore Lab – 5: Configuring DHCP Server Failover	299 303 309 317 319 321
13	Domain Naming System (DNS) Lab – 1: Installing DNS Service Lab – 2: Creating Standard Primary Forward Lookup Zones Lab – 3: Creating Standard Primary Reverse Lookup Zones Lab – 4: Creating Secondary Zone Lab – 5: Creating Stub Zone Lab – 6: Creating Active Directory Integrated Primary zone Lab – 7: Conditional Forwarders Lab – 8: Forwarders Lab – 9: Root Hints Lab – 10: Cache Server	327 334 337 343 348 352 354 357 358 360 360
14	Internet Information Services (IIS)- Web & FTP Lab – 1: Installing Internet Information Service – Web & FTP Lab – 2: Creating a Website Lab – 3: Configuring Redirection of Websites Lab – 4: Creating Virtual Directory Lab – 5: Changing the Website IP address or Port no Lab – 6: Creating Do not Isolate User FTP Site	361 367 373 381 383 386 390
15	Windows Deployment Services (WDS) Lab – 1: Installing Windows Deployment Services Lab – 2: Configuring Windows Deployment Services Lab – 3: Adding Windows 2012 Boot Image to WDS Server Lab – 4: Adding Windows 2012 Install Image to WDS Server	391 394 400 404 407

16	Hyper – V	410
	Lab – 1: Installing Hyper – V	417
	Lab – 2: Configuring Virtual Machine on Hyper-V	424
	Lab – 3: Creating Fixed size Virtual Hard Disk	430
	Lab – 4: Creating Dynamically expanding Virtual Hard Disk	435
	Lab – 5: Creating Differencing Virtual Hard Disk	440
	Lab – 6: Configuring Virtual Networks	446
	Lab – 7: Configuring Hyper-V Replica	452
17	Routing	460
	Lab – 1: Assigning the IP Address to Configure Routing	464
	Lab – 2: Installing Routing Service on Router1 & Router2	469
	Lab – 3: Enabling Routing on Router1 & Router2	476
	Lab – 4: Configuring Static Routes	479
	Lab – 5: Configuring Network Address Translation	482
	Lab – 6: Configuring DHCP Relay Agent	486
18	Remote Access Services, Remote Desktop Services and HTTPS Web Sites	488
	Lab – 1: Configuring VPN Server	493
	Lab – 2: Establishing VPN Connection	498
	Lab – 3: Configure Remote Desktop Server in Remote Admin Mode	504
	Lab – 4: Creating Self-Signed Certificate for HTTPS Website	507
	Lab – 5: Creating a HTTPS Web Site	510
19	iSCSI and Storage	518
	Lab – 1: Configuring iSCSI Target Server	528
	Lab – 2: Configuring iSCSI Initiator	537
	Lab – 3: Creating Storage Pool and Simple Volume (RAID – 0)	552
	Lab – 4: Creating Mirror Volume (RAID – 1)	563
	Lab – 5: Creating Parity Volume (RAID – 5)	
20	Windows Server Backup	575
	Lab – 1: Configuring Windows Server Backup & Recovery	577
21	Advanced Topics - Groups	591
	Lab – 1: Configuring Network Load Balancing Cluster	598
22	Live Setup	608
	Documentation of Live Setup	609

Network & Networking

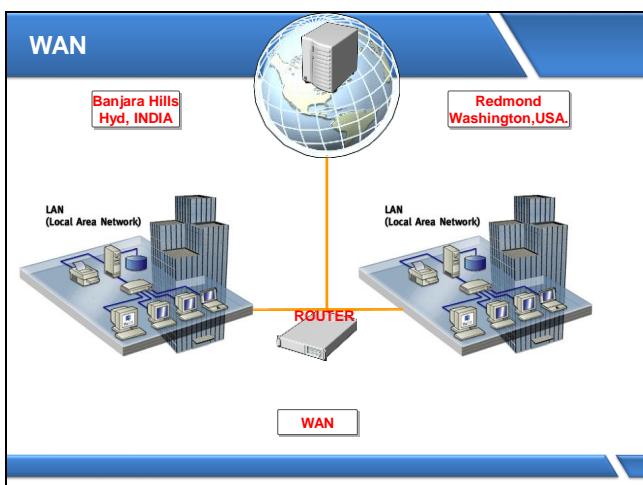
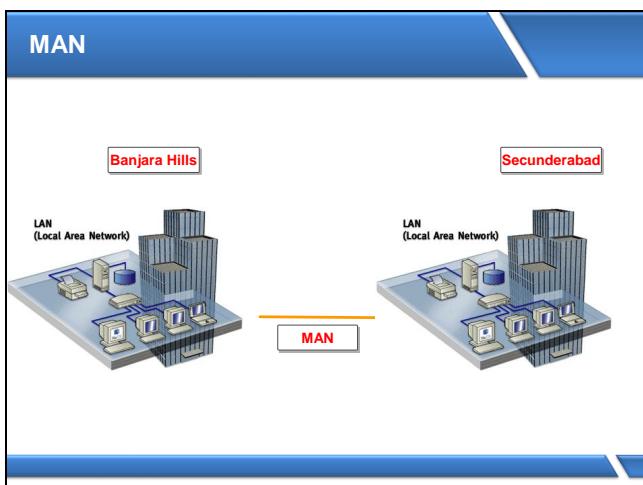
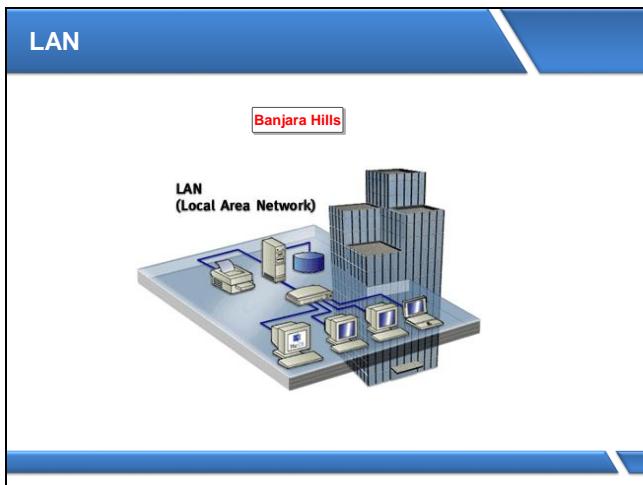
- **Network**
 - A Network is an Interconnection of devices.
- **Networking**
 - Networking is the communication between the interconnected devices.

What is Network ?



Types of Networks

- **Local Area Network**
 - Operate within a limited geographical location
 - Provides full-time connectivity to local services
- **Metropolitan Area Network**
 - Spans within a city
 - Provides full-time & part-time connectivity
- **Wide Area Network**
 - Operate over a large geographical location
 - Provides full-time & part-time connectivity



Network Devices

- **NIC**

The Network interface card is frequently called a NIC. It forms an interface between the networked device (Computer) and the Ethernet (LAN).
- **MAC ADDRESS**

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

Example - 01-23-45-67-89-ab

Network Devices

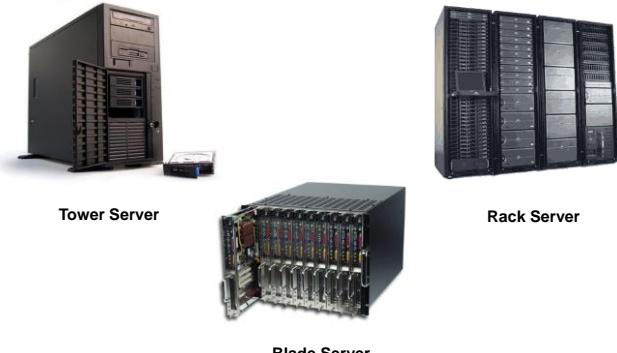
- **Hub**
 - It is generally used to connect all devices on a network so that they can communicate with each other. It always do broadcasting
- **Switch**
 - Like Hub, it is also used to connect all devices on a network so that they can communicate with each other. But first time it will do flooding and from second time onwards it will do unicast.
- **Router**
 - Router is device which allows communication between two or more different networks present in different geographical locations.

Operating System

Operating System

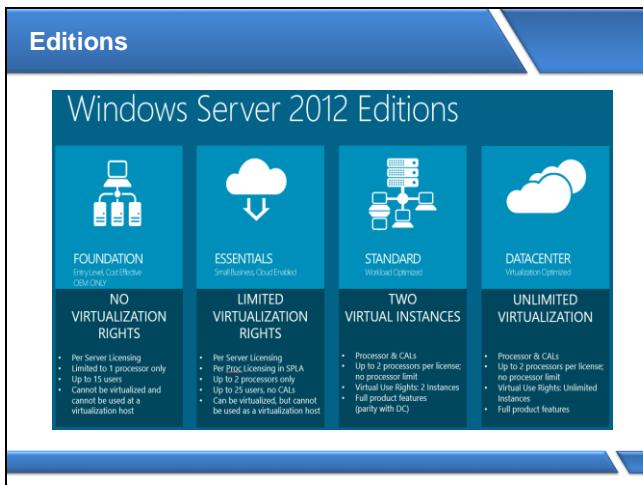
- An operating system is a software program that enables the computer hardware to communicate and operate with the computer software.
- Two types of Operating Systems
Client OS
Example-Windows Xp, Vista, Windows 7, Windows 8
Server OS
Example-Windows 2003, 2008, 2012

Types of Hardware Servers



The History of Microsoft N/w OS

- Windows NT 3.1 released in 1993
- Windows NT 3.5 released in 1994
- Windows NT 4.0 released in 1996
- Windows NT 5.0 was renamed as Windows 2000
- Windows .NET Server was renamed as Windows 2003
- Windows Server 2008
- Windows Server 2012



Windows 2012 Requirements

Component	Requirement
Processor	Minimum: 1 processor with 1.4 GHz. {{X64} 64bit processor} Maximum: 64 processors. Note: Hyper -V Compatible Processor is recommended for Standard and Data Center Editions. Intel VT or AMD – V.
Memory	Minimum: 512 MB RAM Maximum: 4 TB RAM
Available Disk Space	Minimum: 10 GB Recommended: 80 GB or greater
Drive	DVD-ROM drive

- ### Server Core
- Benefits of Server Core
 - Greater stability
 - Simplified management
 - Reduced maintenance
 - Reduced memory and disk requirements
 - Reduced attack surface

Features of Windows Server 2012

- **64 Bit operating System**
- **Easy Installation**
- **Cloud Infrastructure**
- **Improved Server Manager**
 - Customized Dash Board.
 - Remote Management of Server Core and Full.
- **Active Directory**
 - Administrative Center and Recycle Bin.
 - Domain Services.
 - Federation Services and Lightweight Directory Services.
 - Certificate Services and Rights Management Services.

Features of Windows Server 2012

- **In-built GPMC**
- **Centralized deployment of applications**
- **Disk Quotas**
- **Distributed File System**
- **Windows Server Backup**
- **DNS Dependency**
- **Internet Information services**
- **Improved Virtualization Features**
 - Live Migrations of Virtual Machines and Storage.
 - Hyper – V Replica.
 - Dynamic Memory.

Features of Windows Server 2012

- **Enhanced Windows Deployment Services**
 - Deploy OS with or without Active Directory.
- **Windows Server Core**
 - Anytime Conversion from Core to Full and Vice – Versa.
- **Network Access protection**
- **Improved DHCP Server**
 - Failover DHCP Server
 - Split Scope
- **Improved Security**
 - Kerberos Version5
 - Internet Protocol Security.

INSTALLATION OF WINDOWS OPERATING SYSTEM

Pre-requisites:

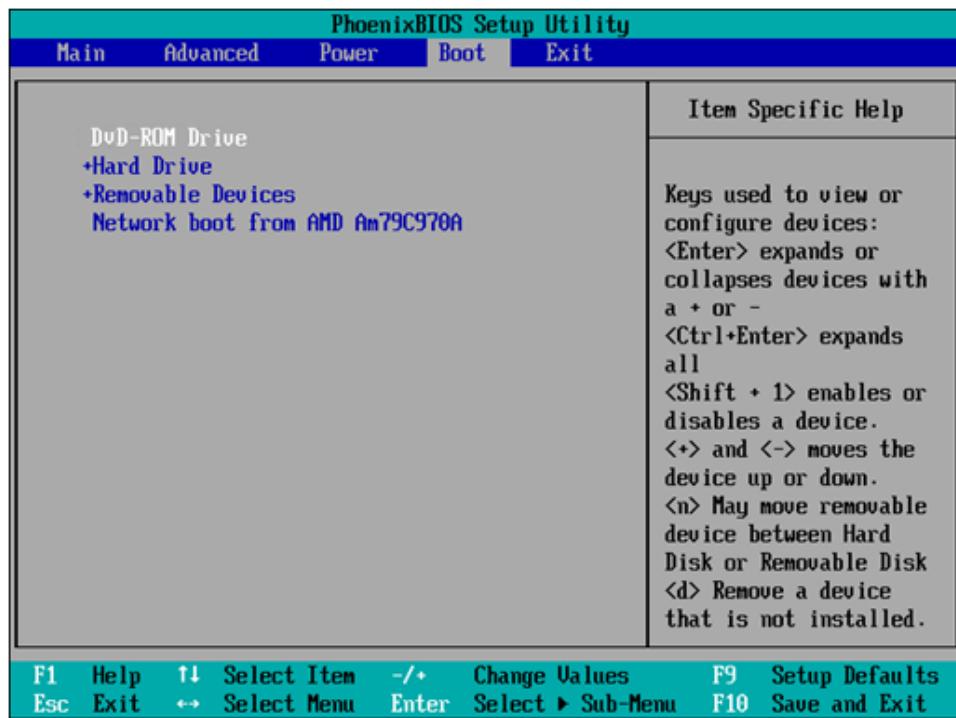
Before working on this lab, you must have

1. A Computer and Windows Server 2012 Operating System DVD.



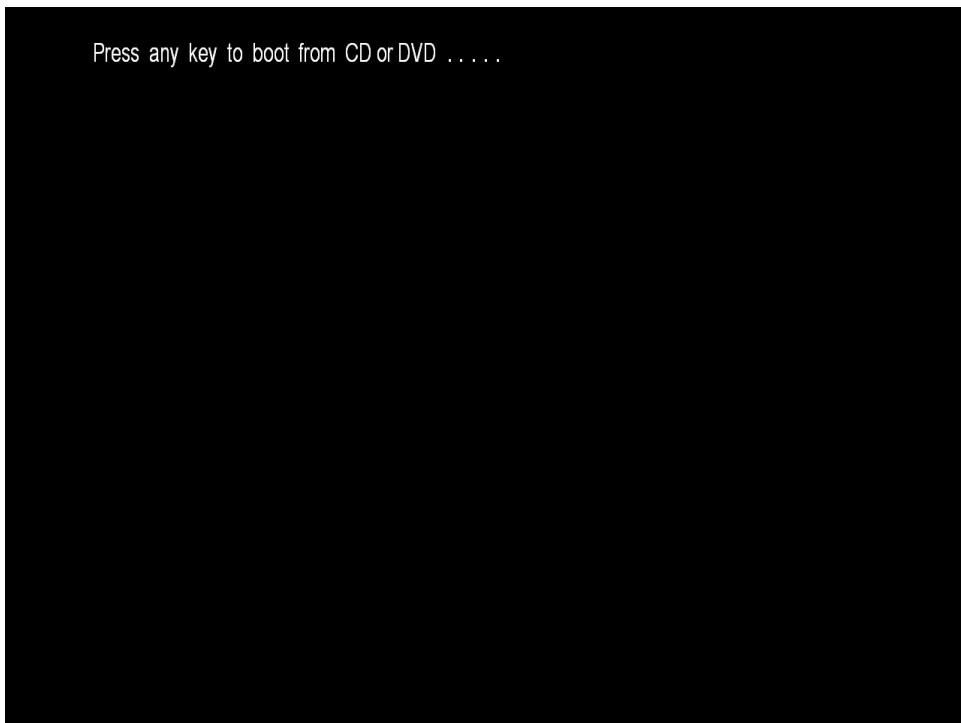
Lab – 1: Installing Windows Server 2012 Operating System

1. Restart the System and go to **BIOS**.
2. Set the First Boot Device as **DVD ROM**.

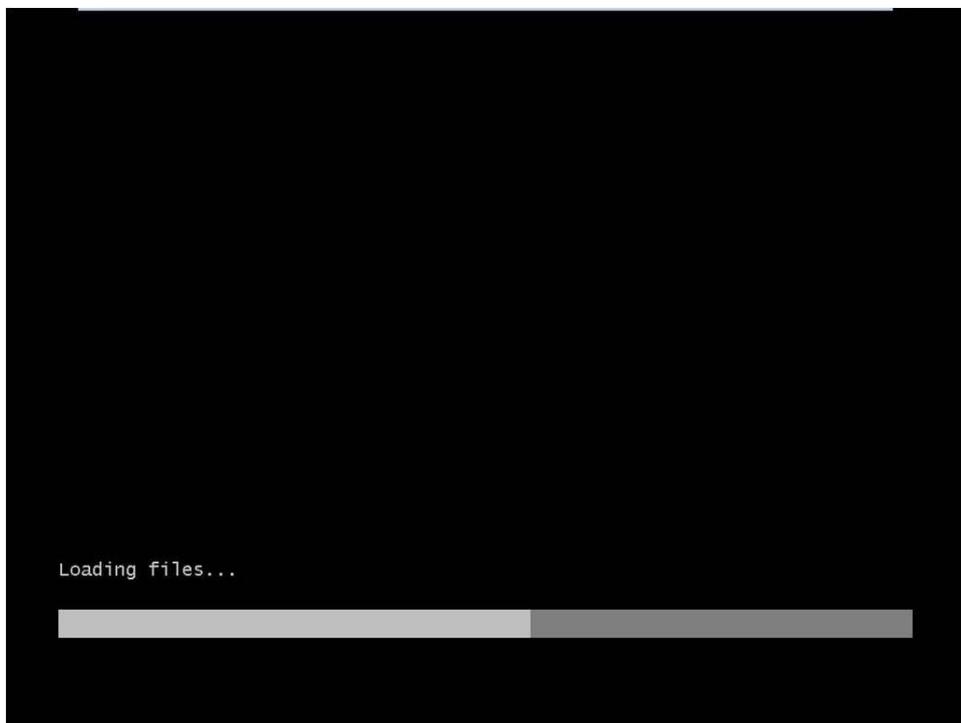


3. Save the settings by Pressing **F10** and click **YES**.
4. Insert **Windows Server 2012 DVD** and Restart the system.

5. Press any key to boot from the CD or DVD.



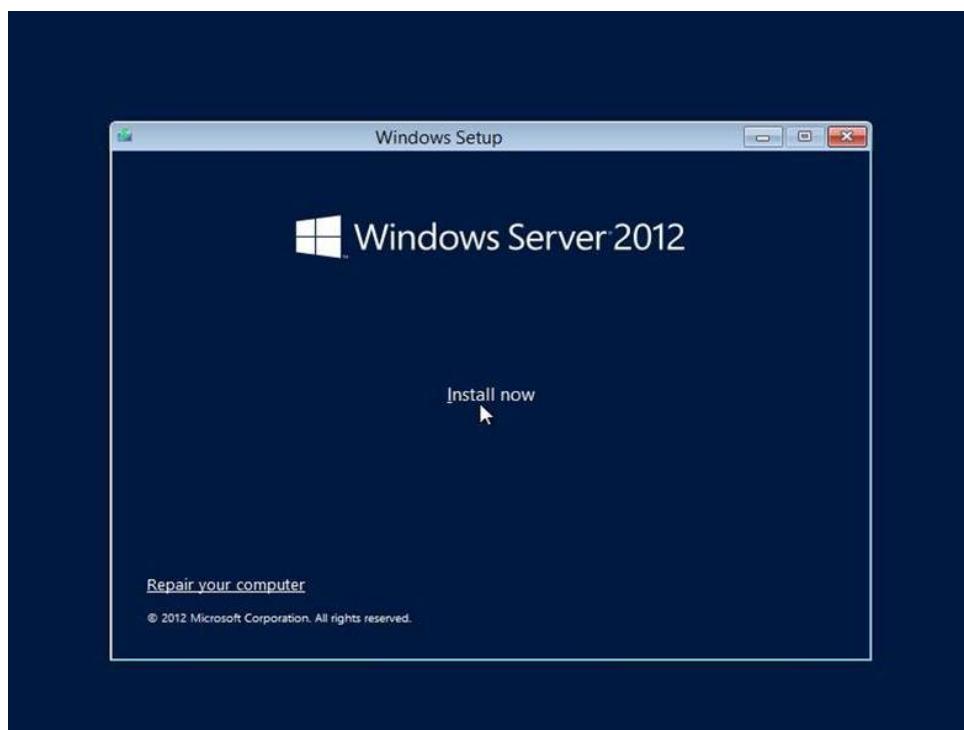
6. System copies the files from DVD.



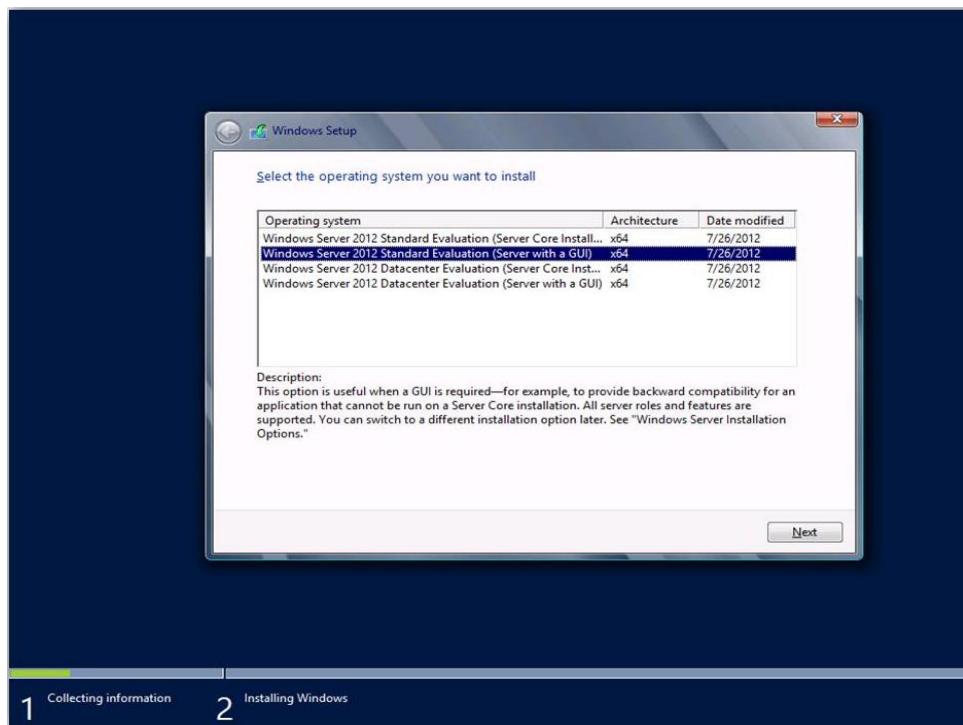
7. Select the language to install **English**.



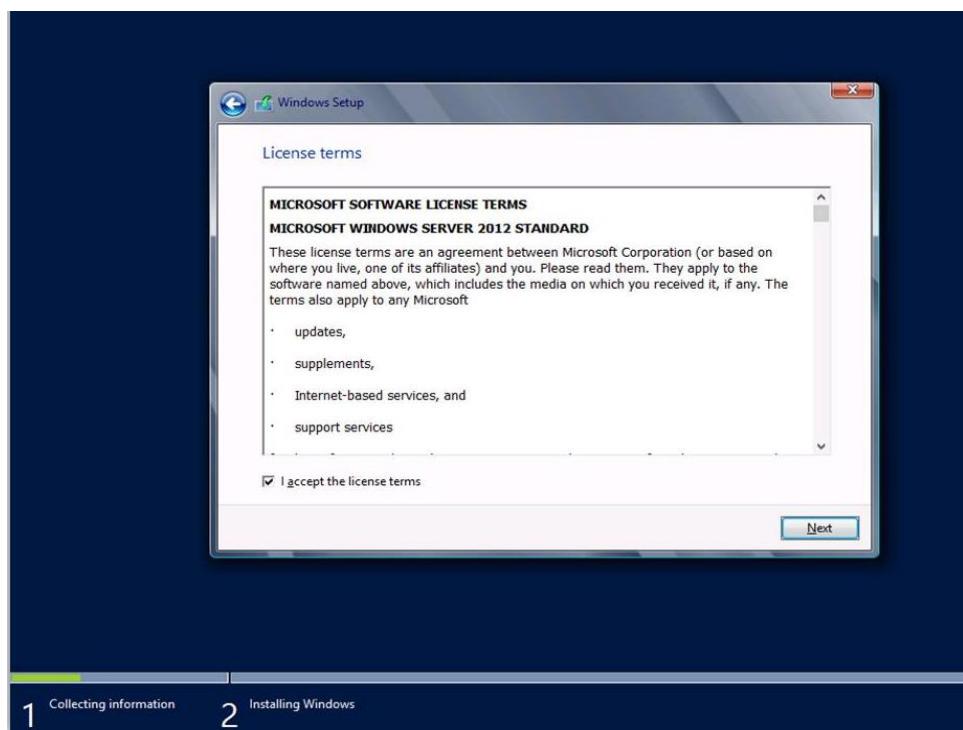
8. Click **Install now**.



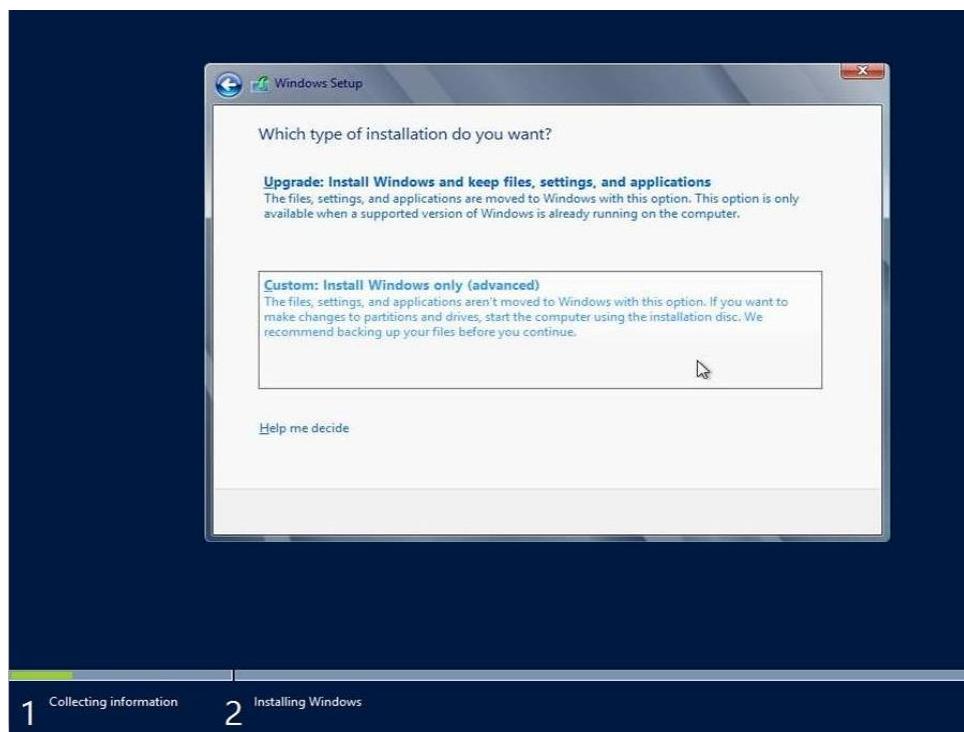
9. Select the edition **Windows Server 2012 Standard (Server with a GUI)**, click **Next**.



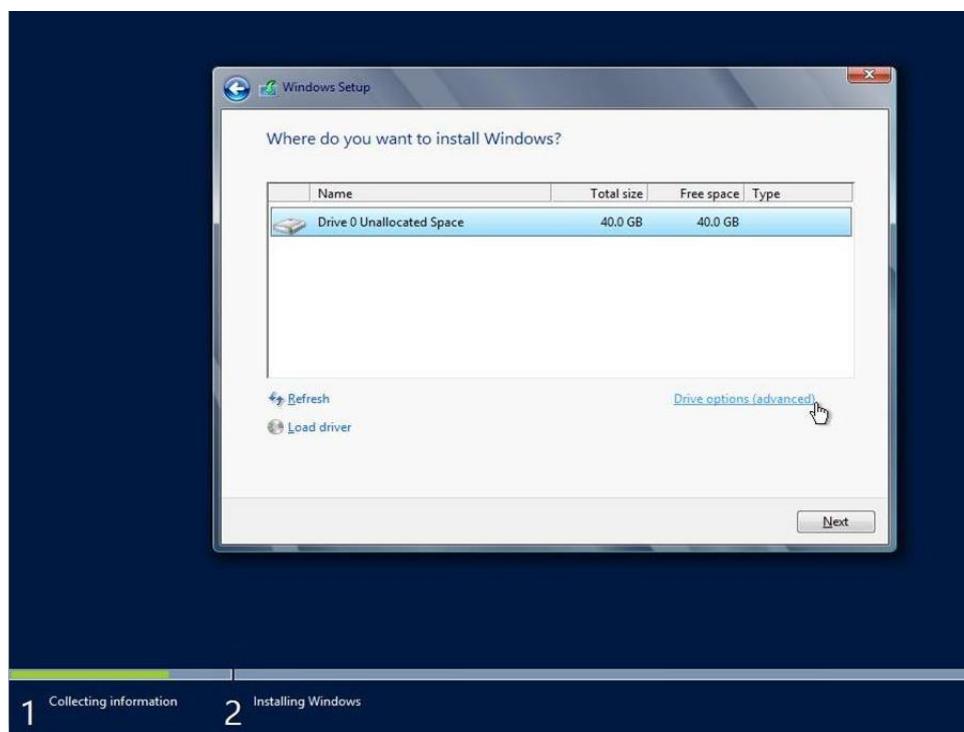
10. Check the box **I accept the license terms** and click **Next**.



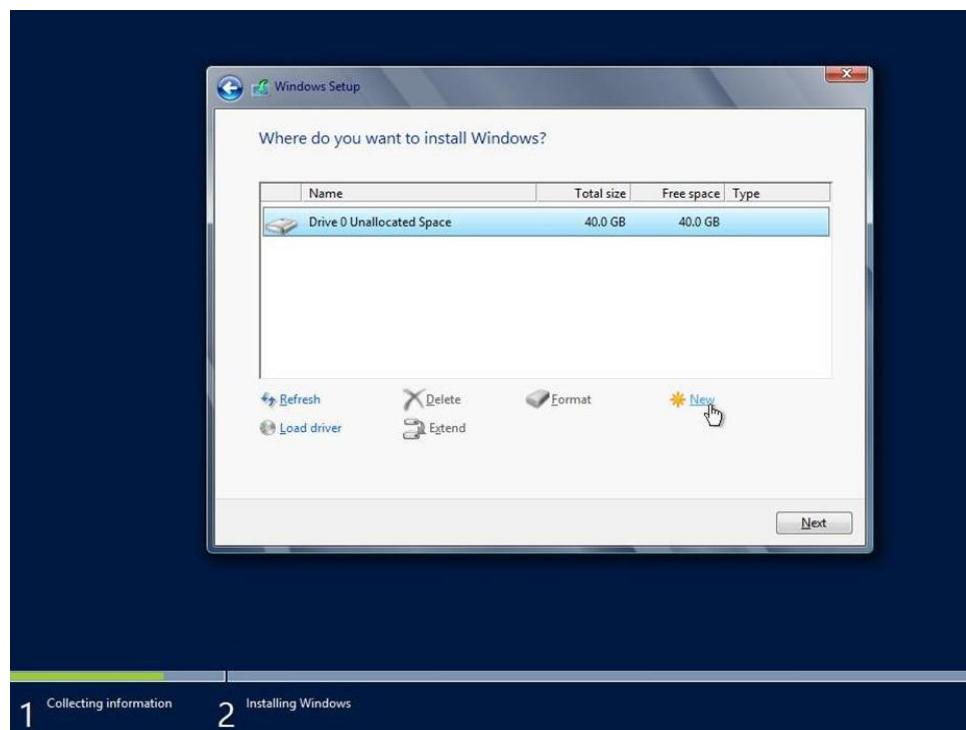
11. Select Custom Installation.



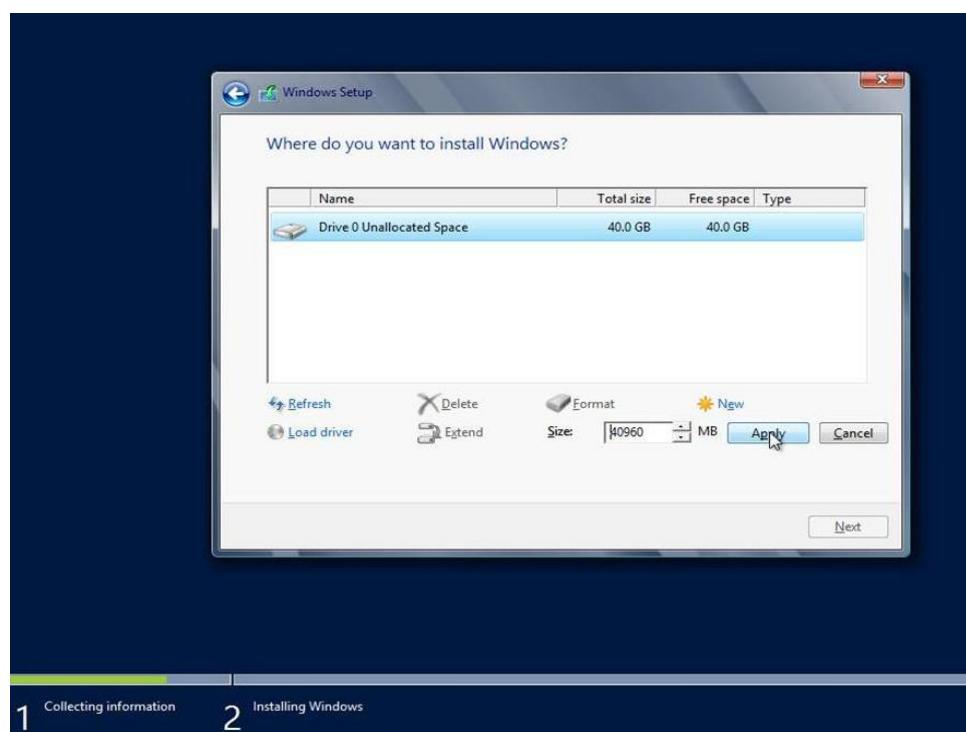
12. Click Drive options.



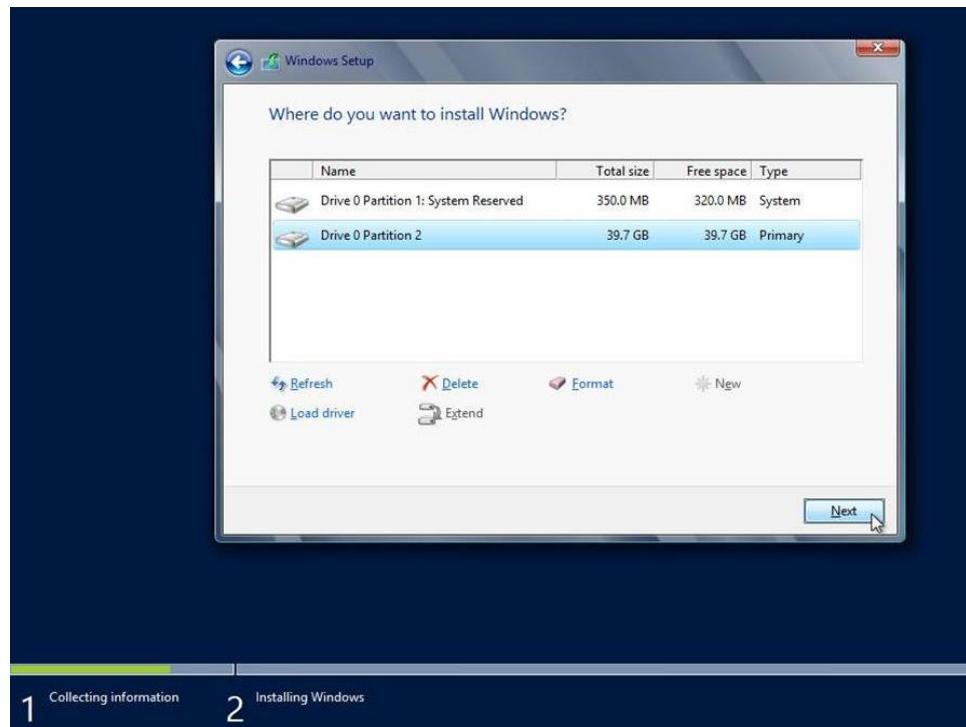
13. Select Unallocated Space and click **New**.



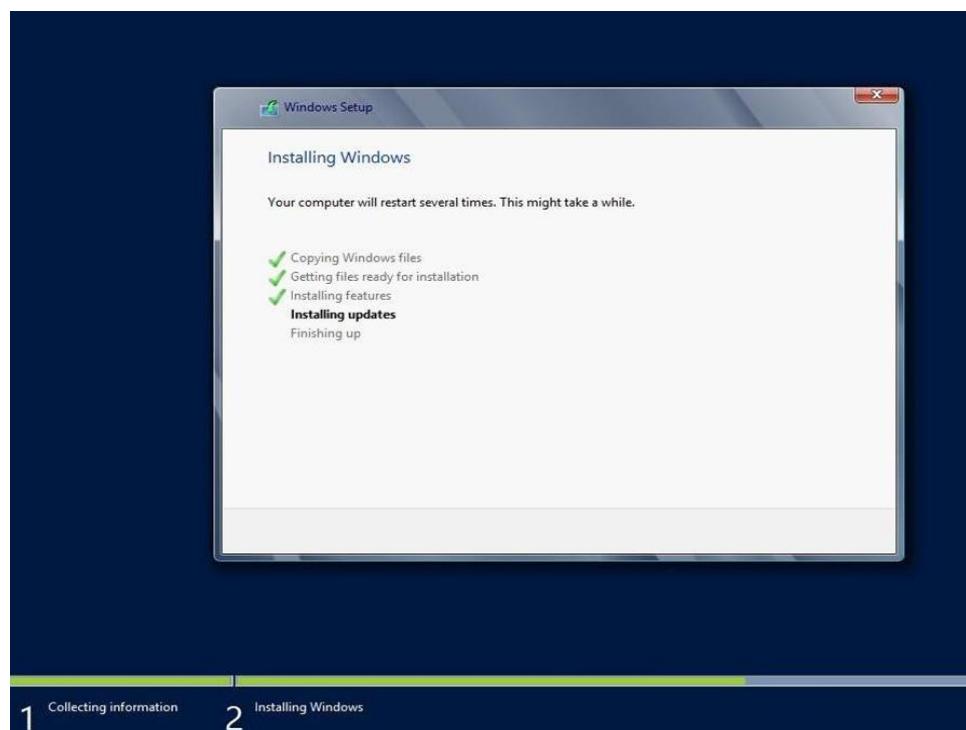
14. Enter the size for the partition, and click **Apply**.



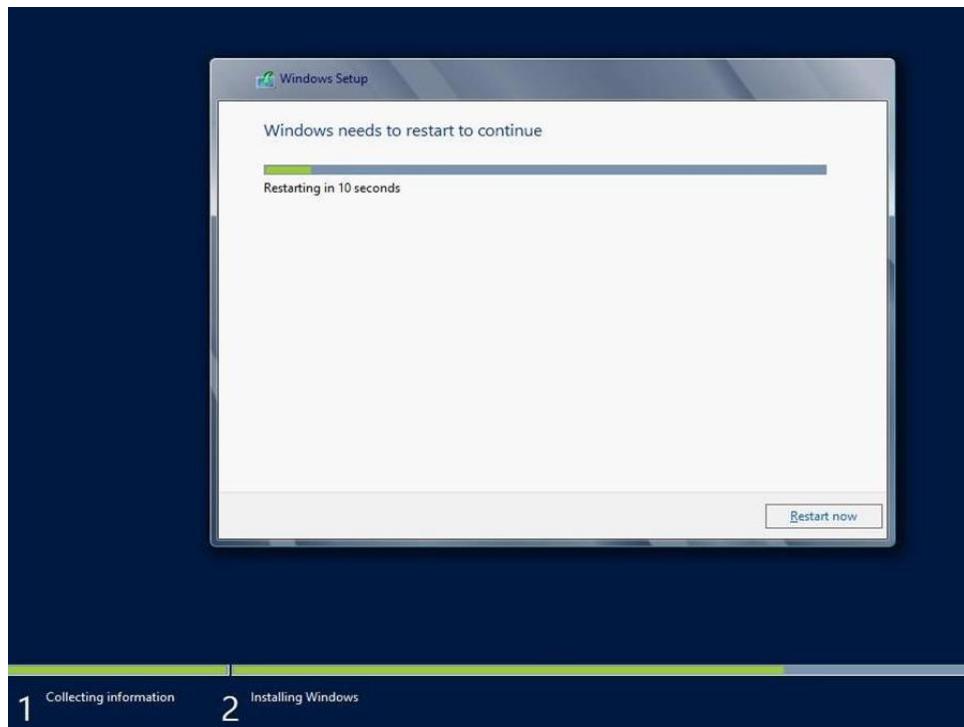
15. Select the **Partition** and click **Next**.



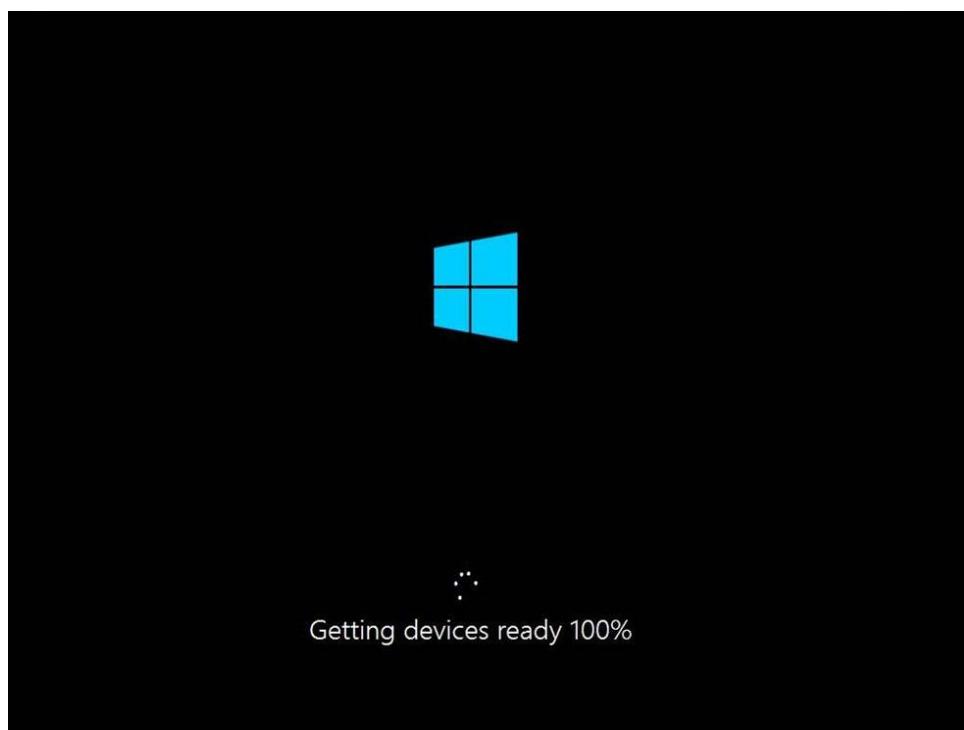
16. Windows Installation will start.



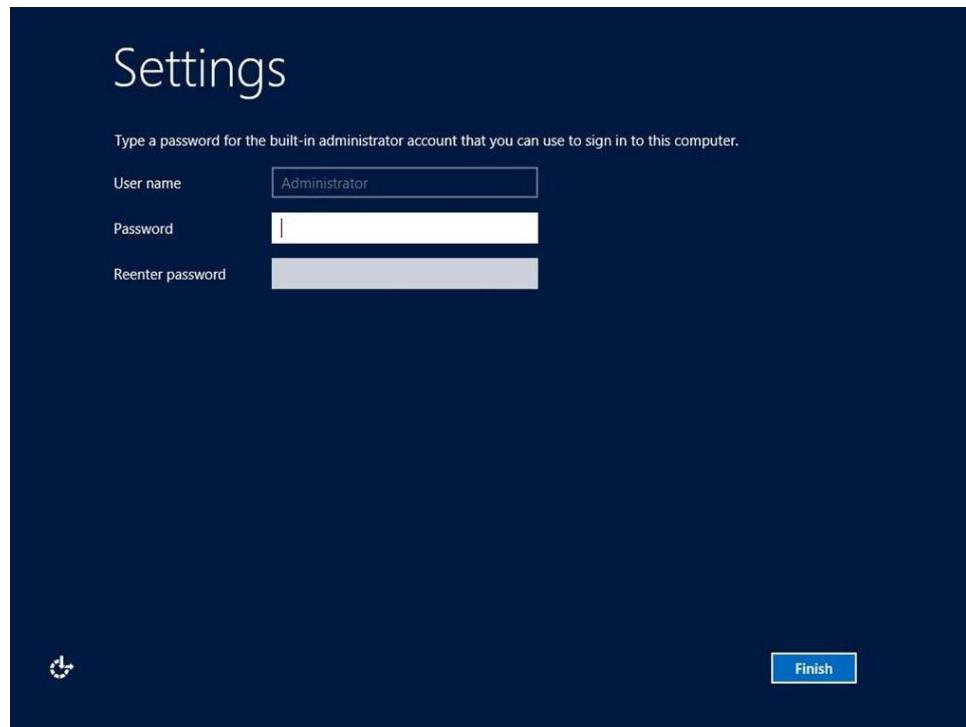
17. System Restarts.



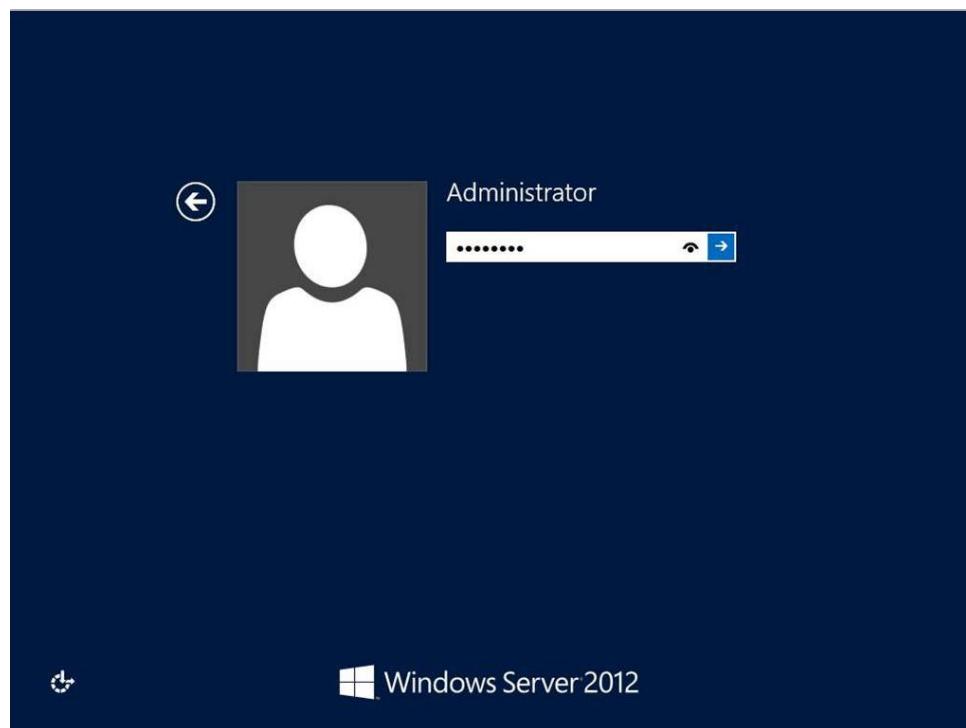
18. Completes the Installation, and system will be restarted.



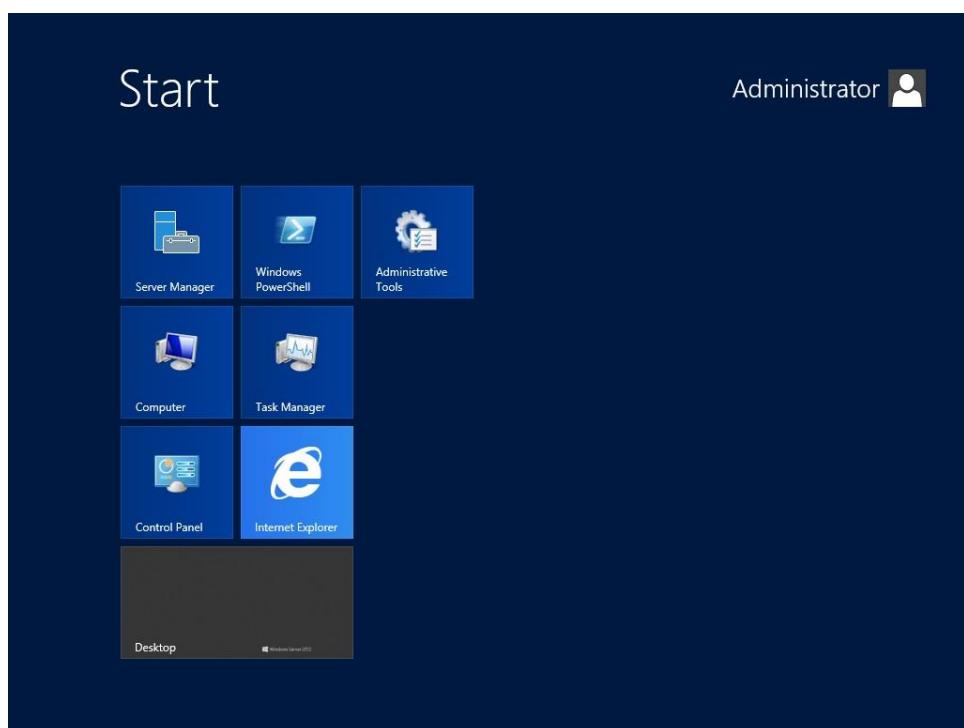
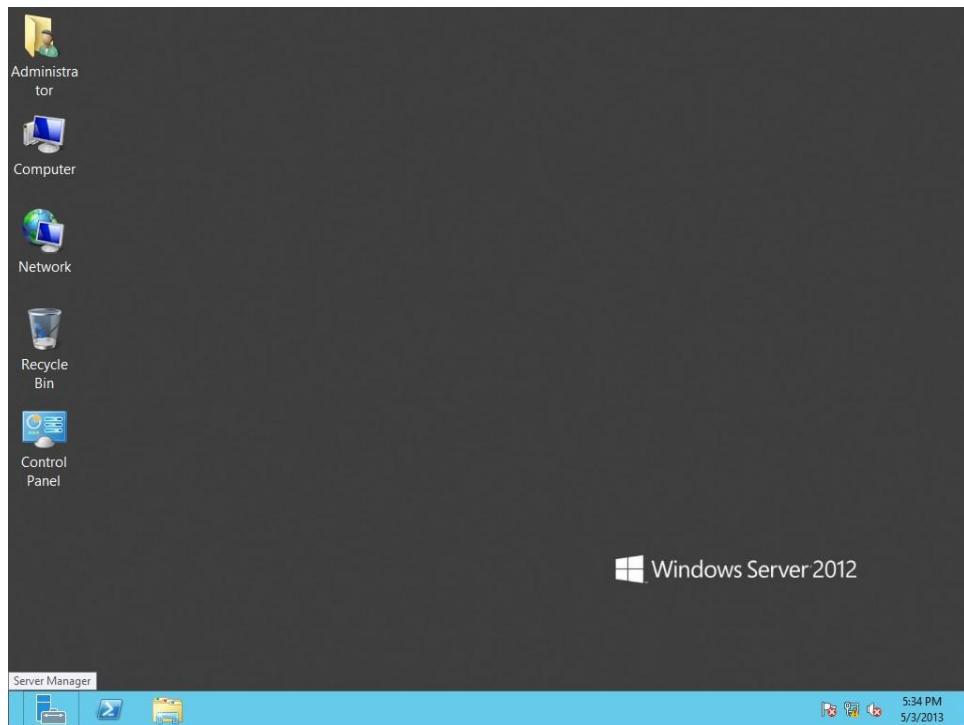
19. Enter Password and Re-enter Password for Administrator account, click **Finish**.



20. Enter Password and Logon using the Administrator account.



21. Finally Administrator has logged in.



INSTALLATION OF WINDOWS OPERATING SYSTEM

Pre-requisites:

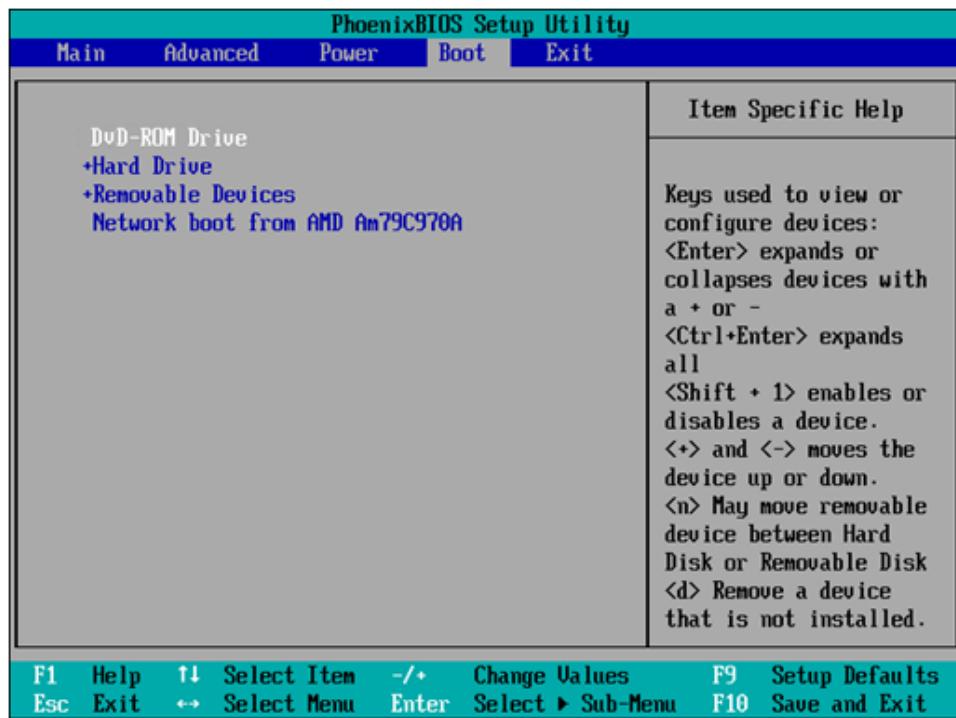
Before working on this lab, you must have

1. A Computer and Windows 7 Operating System DVD.



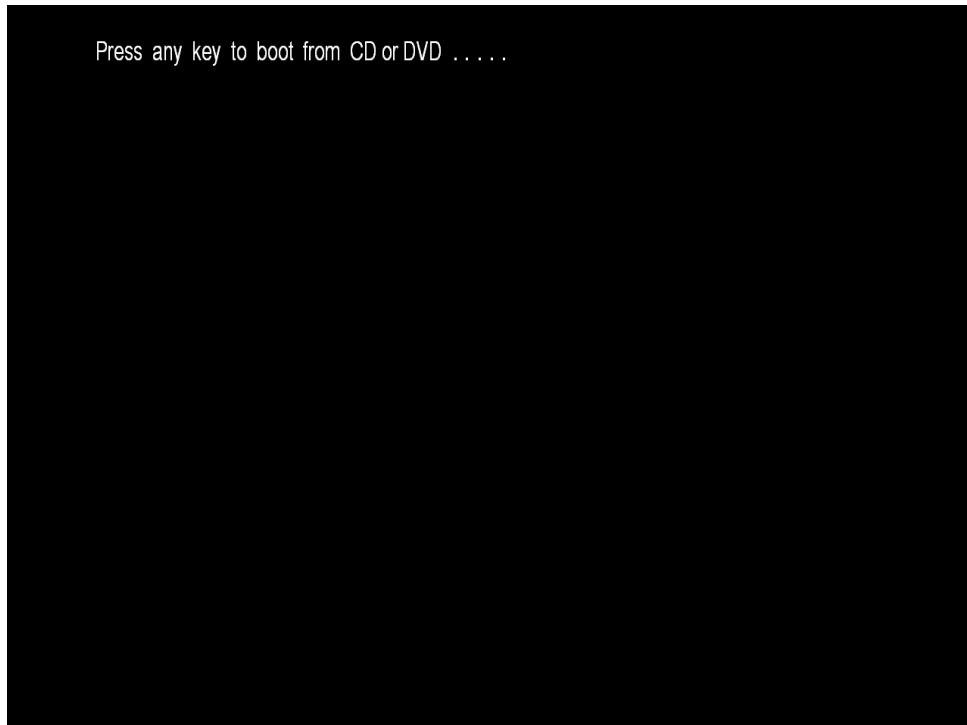
Installing Windows 7 Operating System

1. Restart the System and go to **BIOS**.
2. Set the First Boot Device as **DVD ROM**.

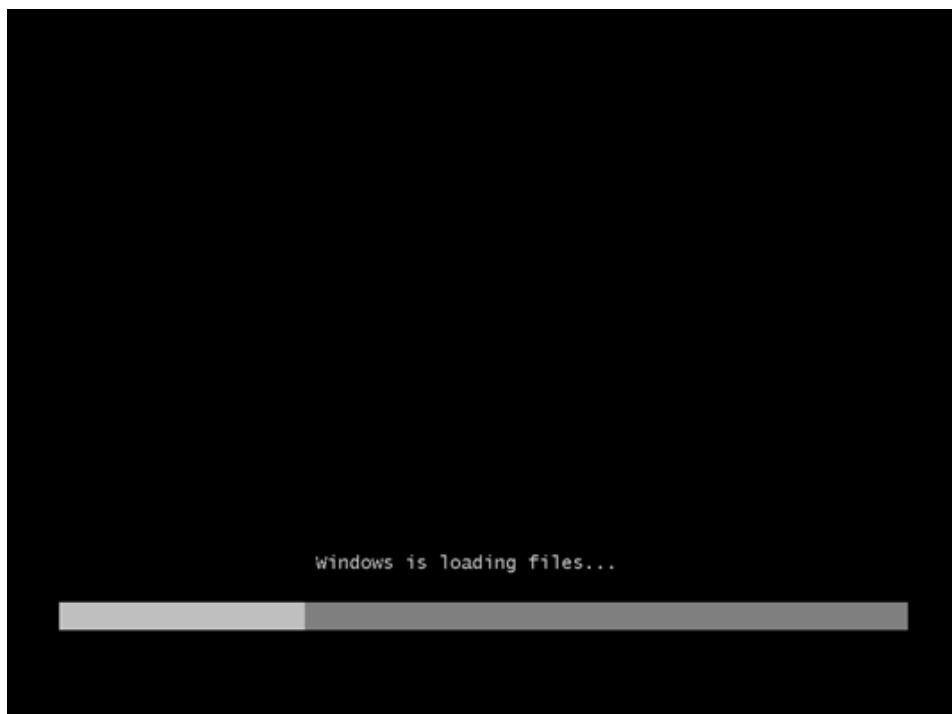


3. Save the settings by Pressing **F10** and click **YES**.
4. Insert **Windows 7DVD** and Restart the system.

5. Press any key to boot from the CD or DVD.



6. System copies the files from DVD.



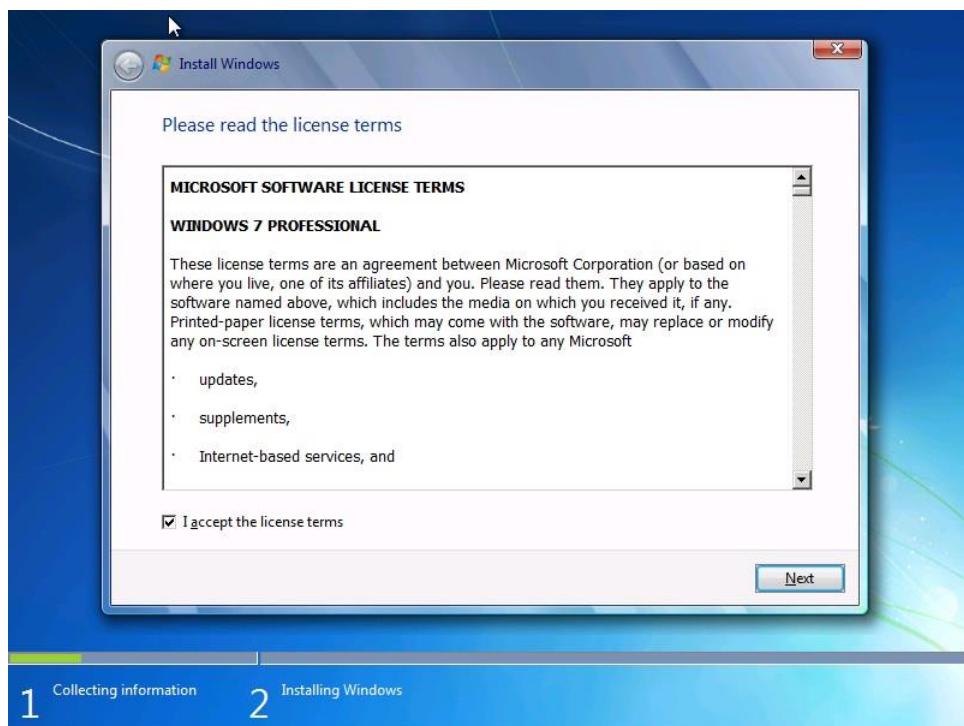
7. Select the language to install English and click **Next**.



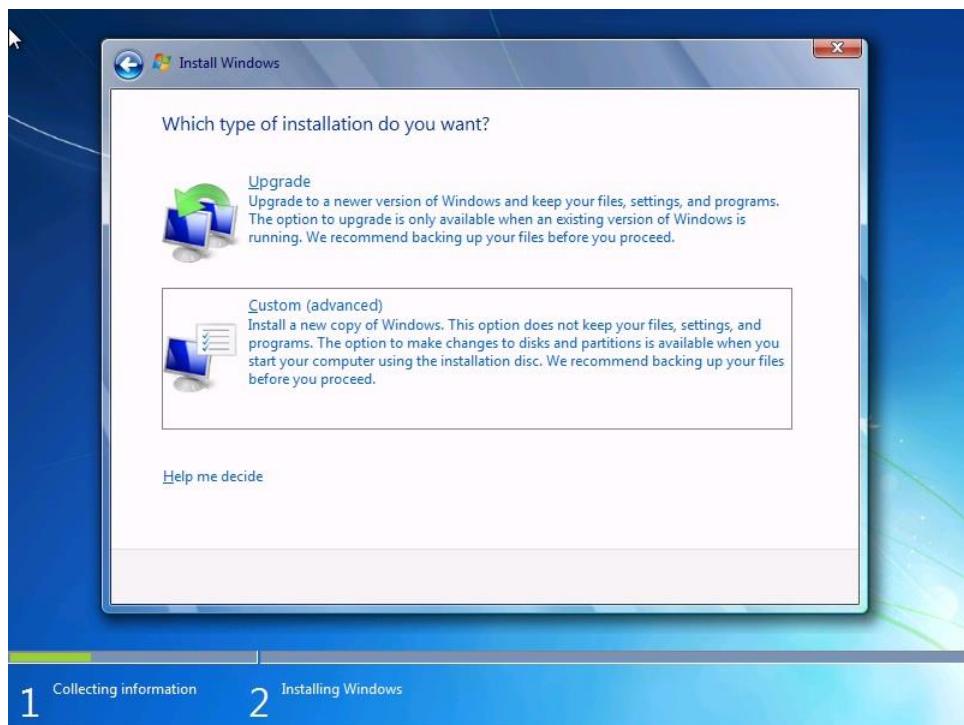
8. Click **Install now**.



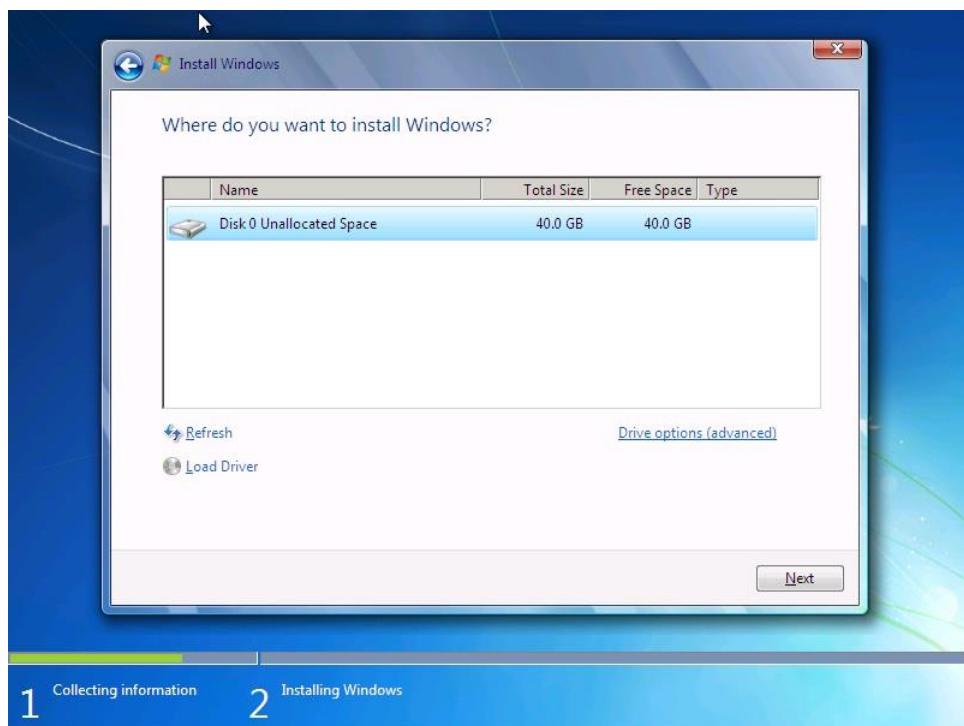
9. Check the box I accept the license terms



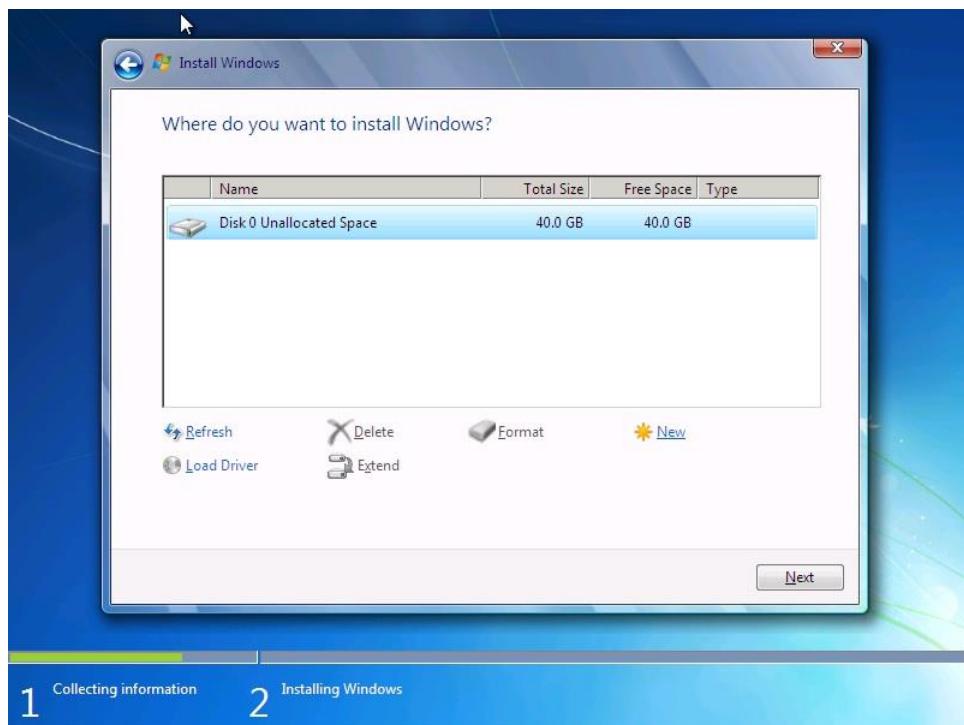
10. Select Custom Installation.



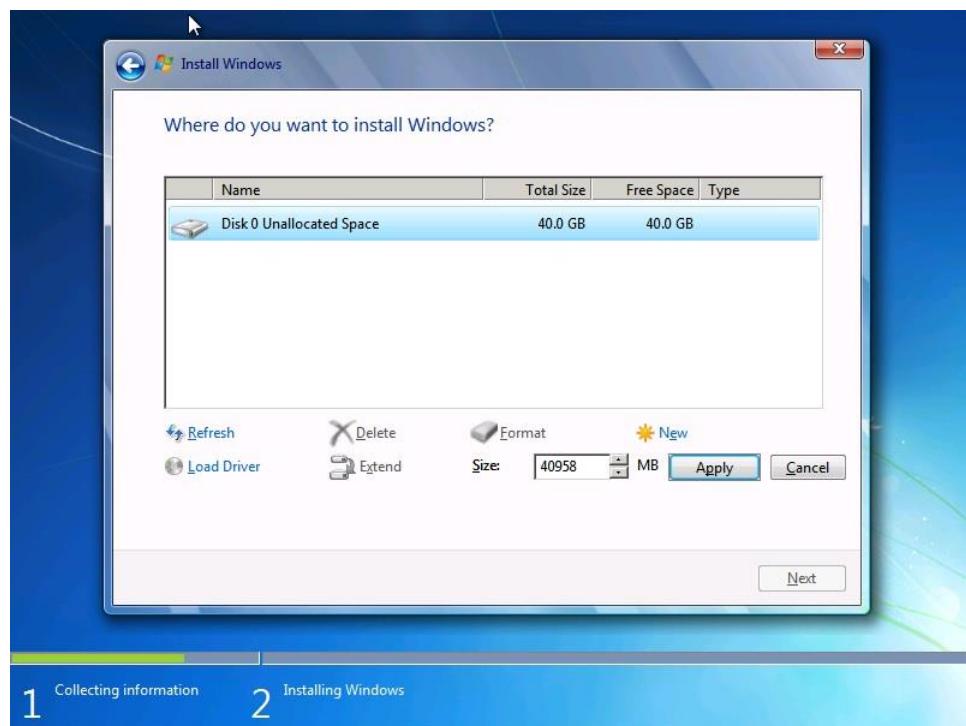
11. Click Drive options.



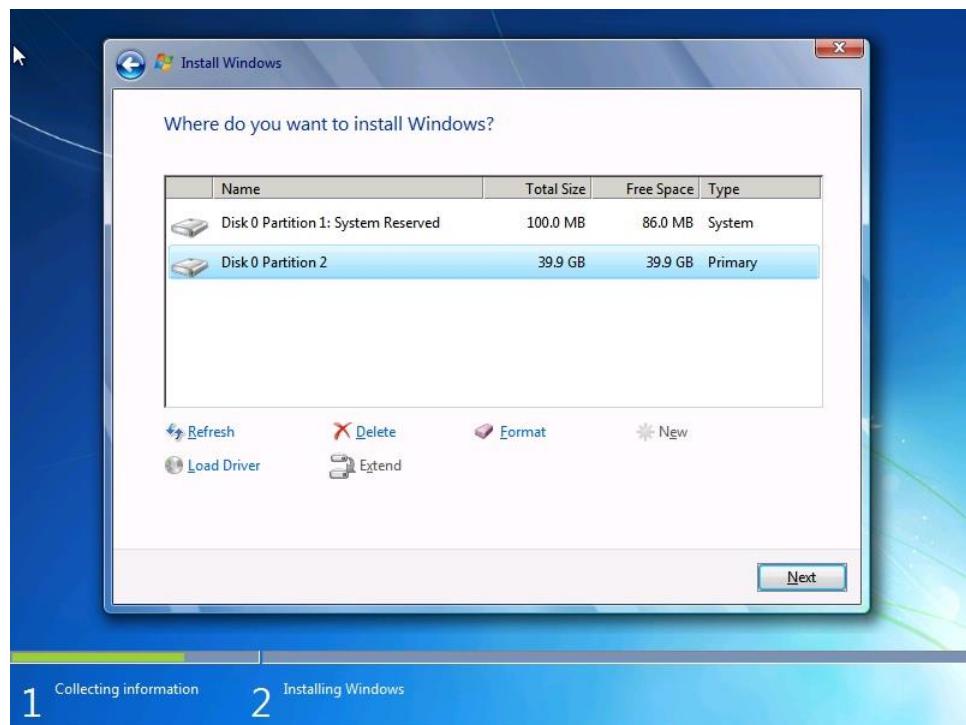
12. Select Unallocated Space and click New.



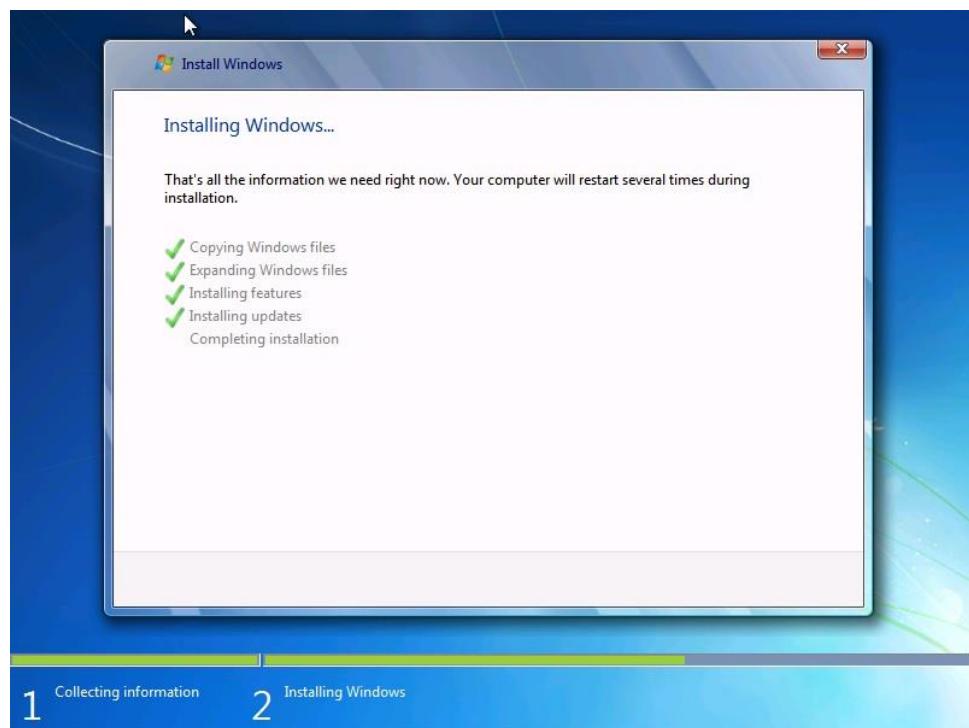
13. Enter the size for the partition, and click **Apply**.



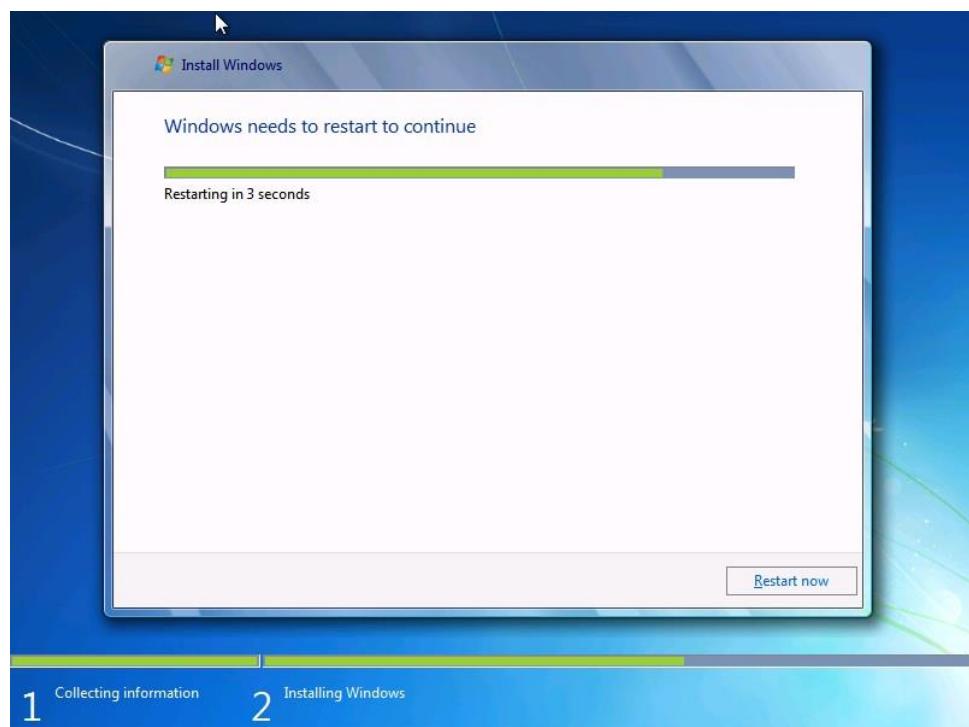
14. Select the **Partition** and click **Next**.



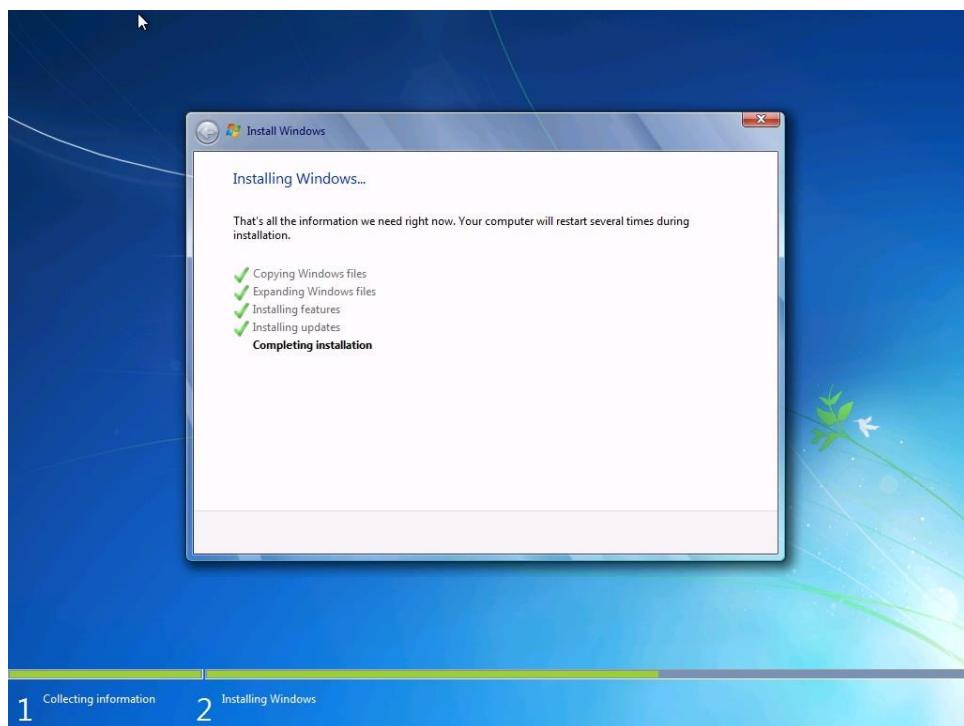
15. Windows Installation will start.



16. System Restarts.



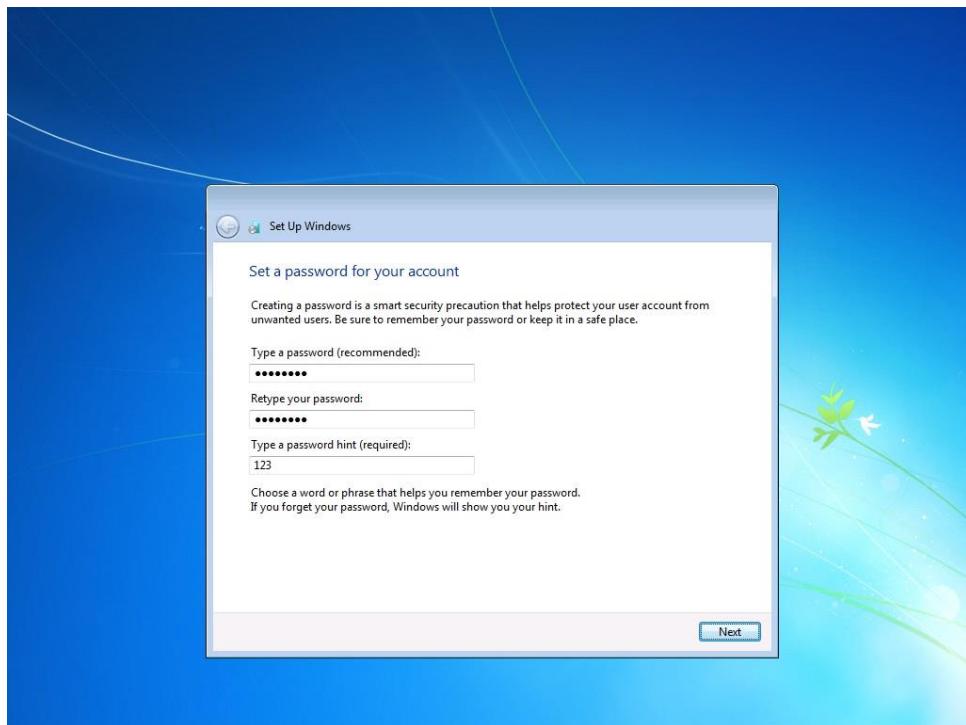
17. Completes the Installation, and system will be restarted.



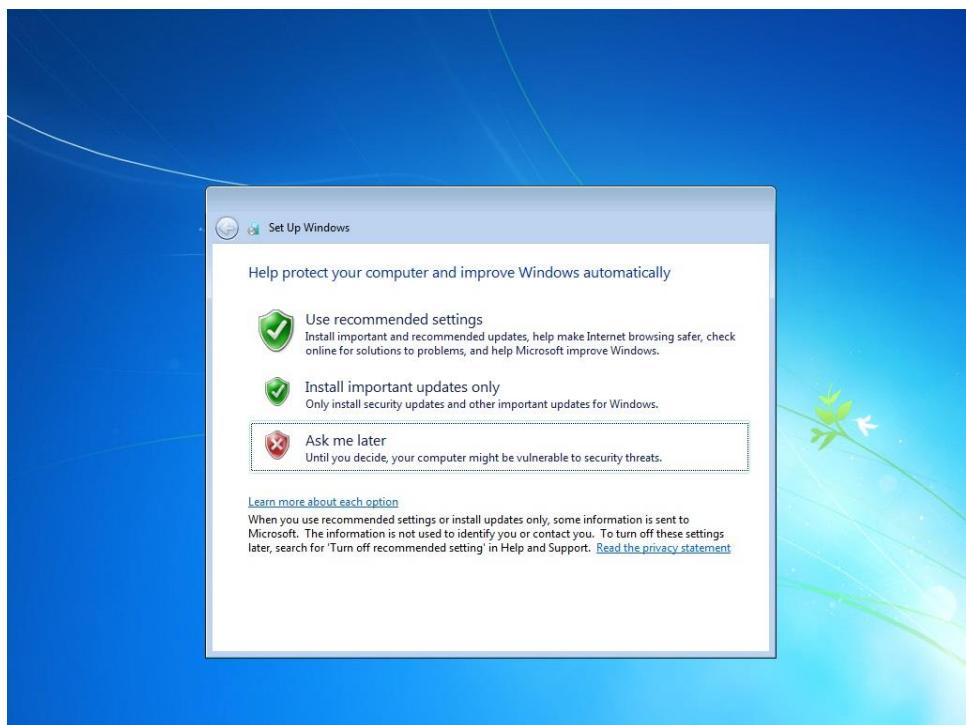
18. Enter the **User Name** and **Computer Name**, click **Next**.



19. Set a password for the account, and click **Next**.

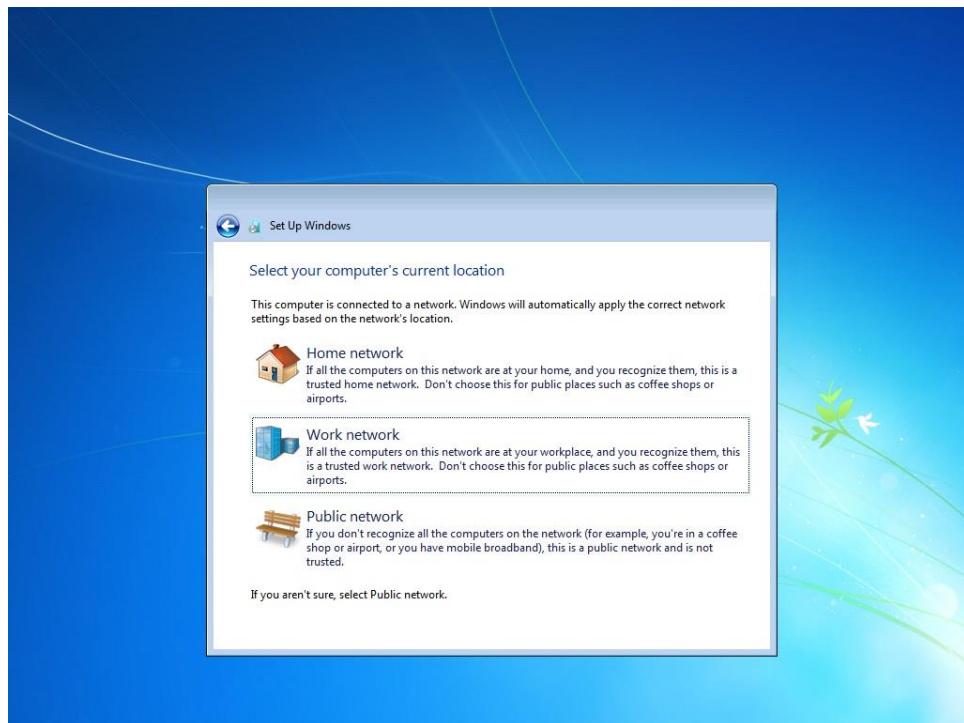


20. Configure Automatic Updates **Ask me later**.

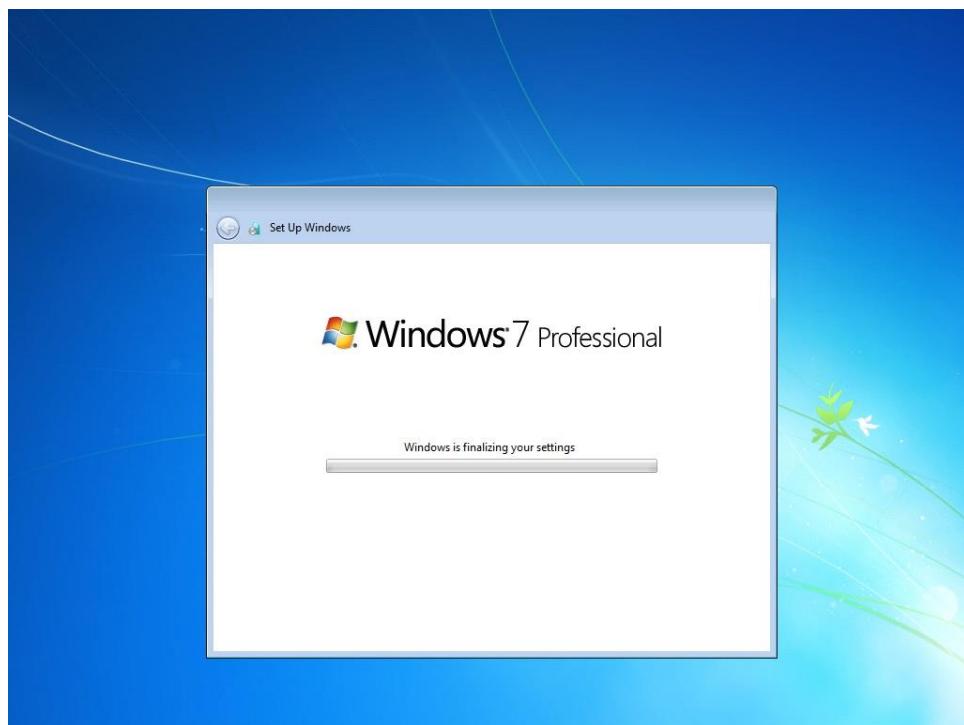


21. Select the **Time zone** and click **Next**.

22. Select the location of your computer **Work**.



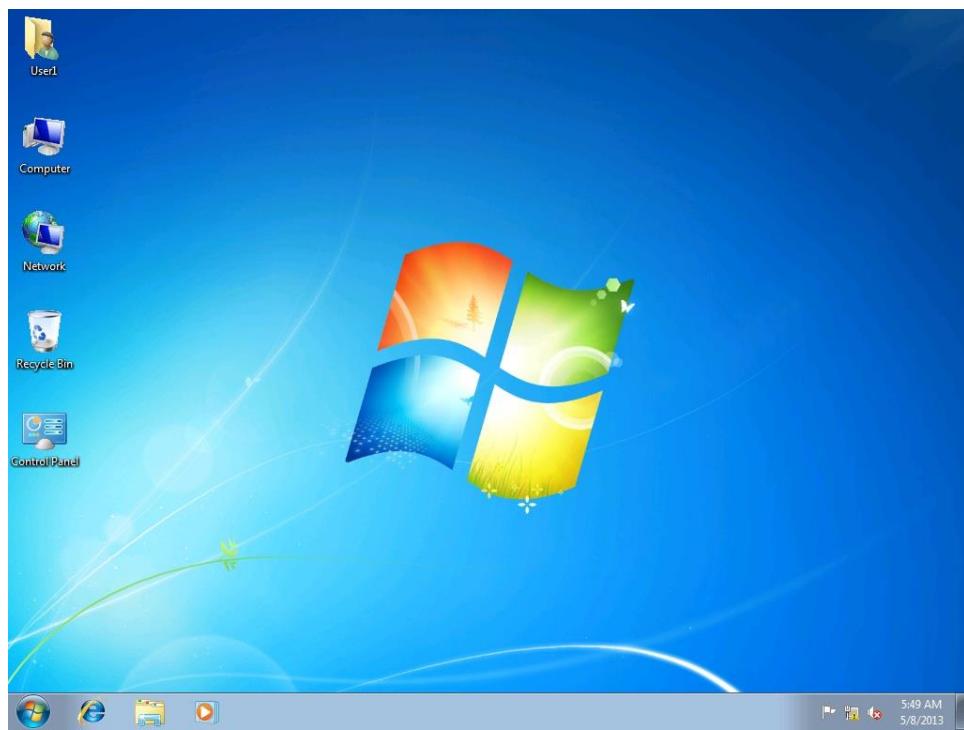
23. Windows finalize the settings.



24. Enter the **Password** to log on to the computer.

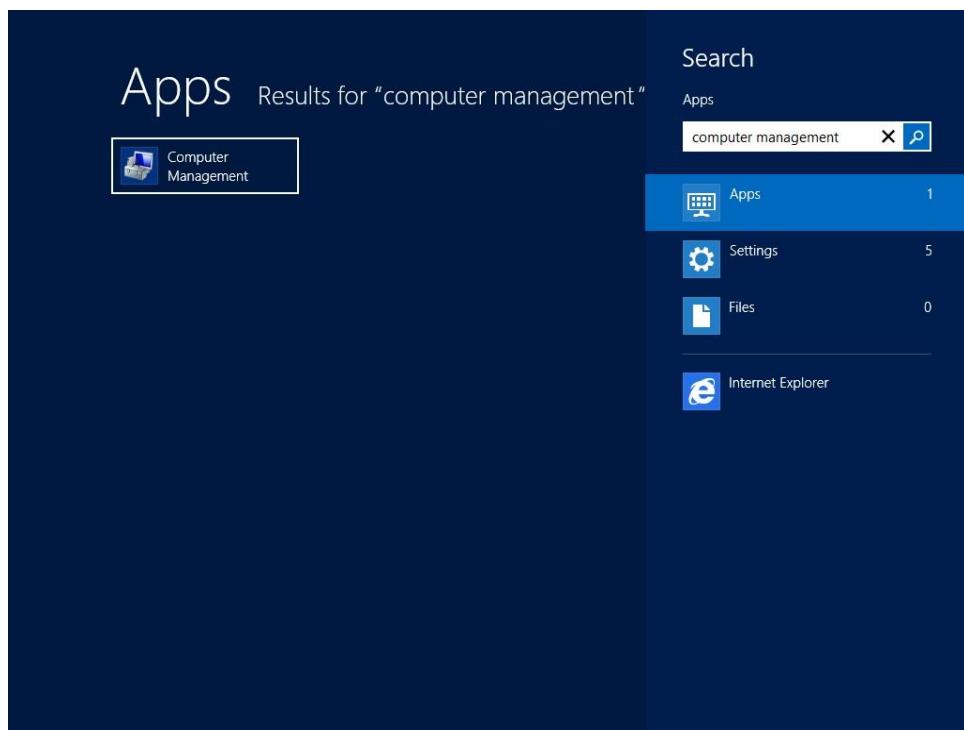


25. Finally Operating System is installed and the **User** has logged in.



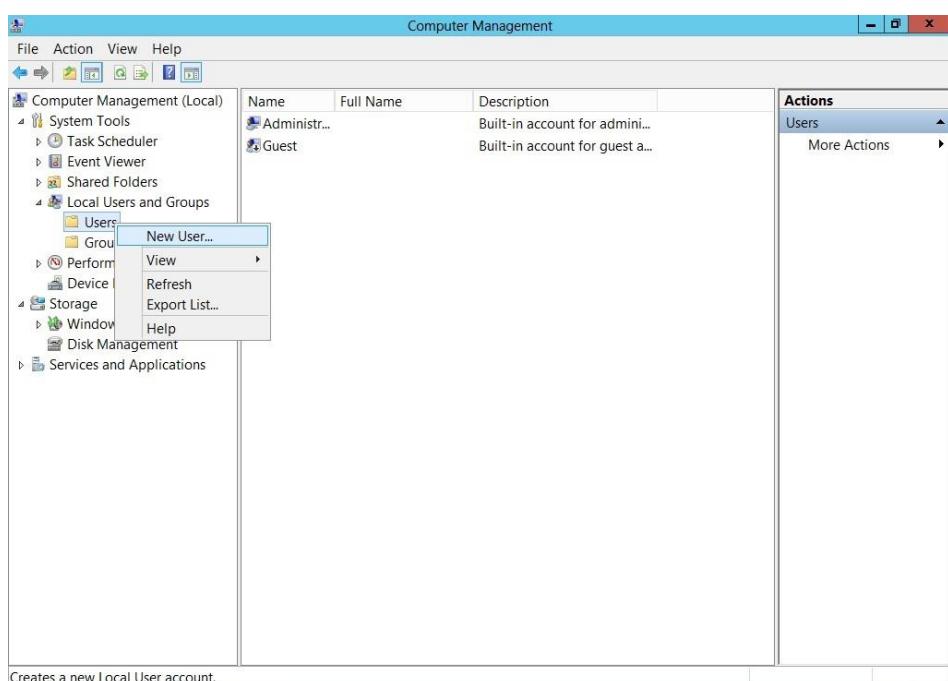
Lab – 2: Creating Local User Accounts

1. Login as the **Administrator** to the Computer.
2. Press Windows Key  to go to Start, type Computer Management in Search Apps, and select **Computer Management**.

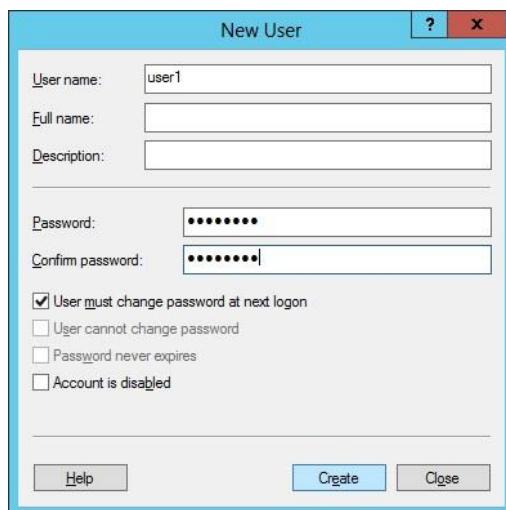


3. Expand **Computer Management** → Expand **System Tools** → Expand

Local Users and Groups → right click **Users** and then click **New User**.



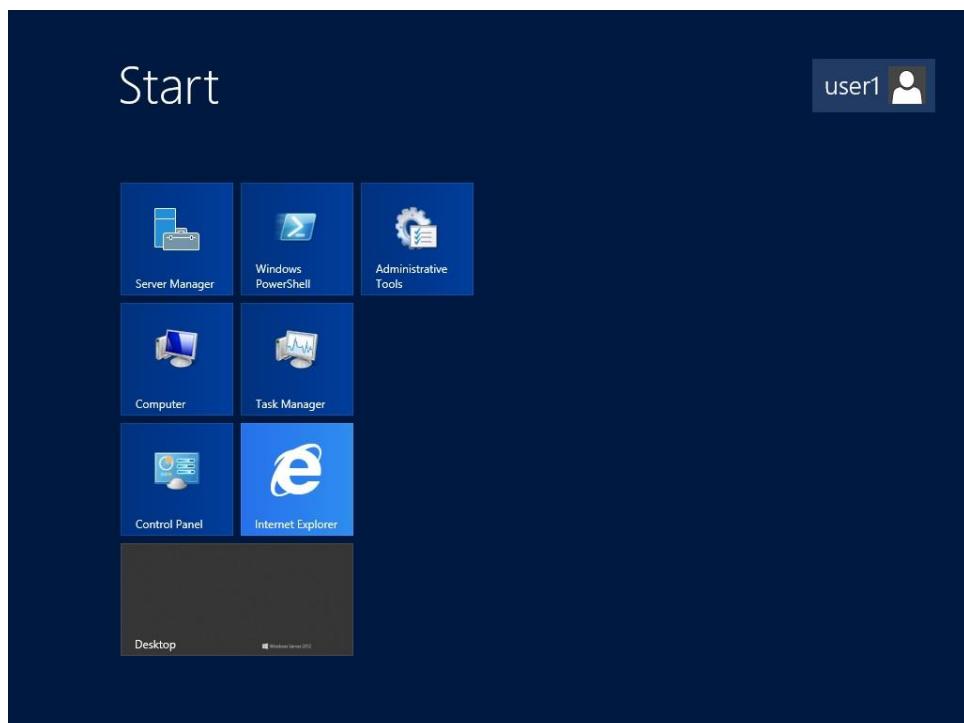
4. Enter **User Name** and set **Password, Confirm Password** and click **Create**.



5. Click **Close**, and then **Close Computer Management**.

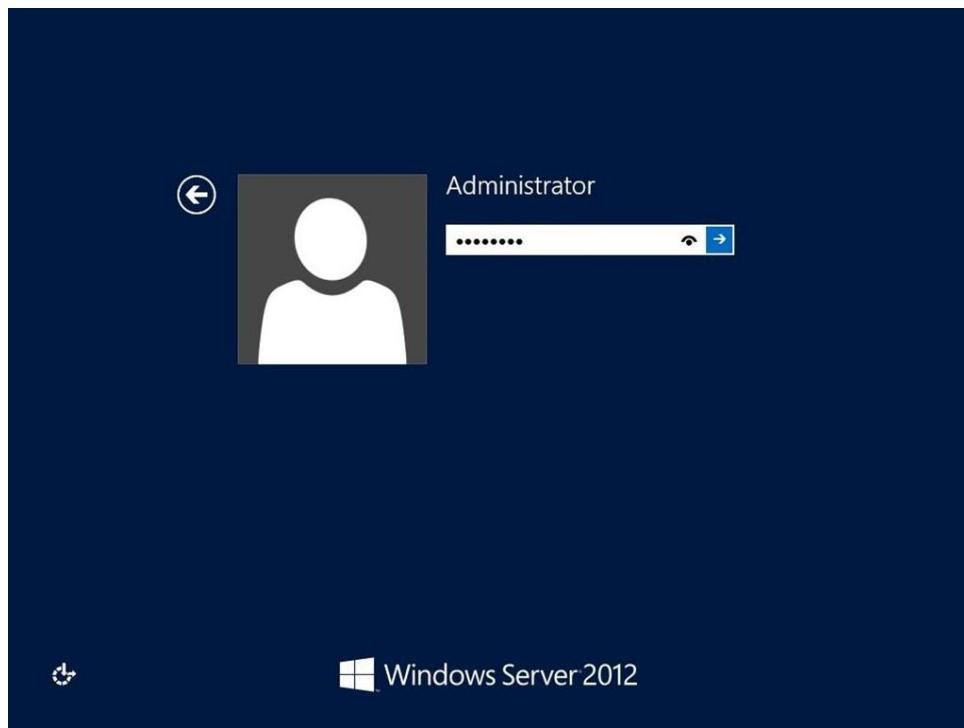
Verification:

1. Press **Ctrl + Alt + Del** → Click **Switch User or Logoff Administrator**.
2. Login as User (**User1**) on same computer.

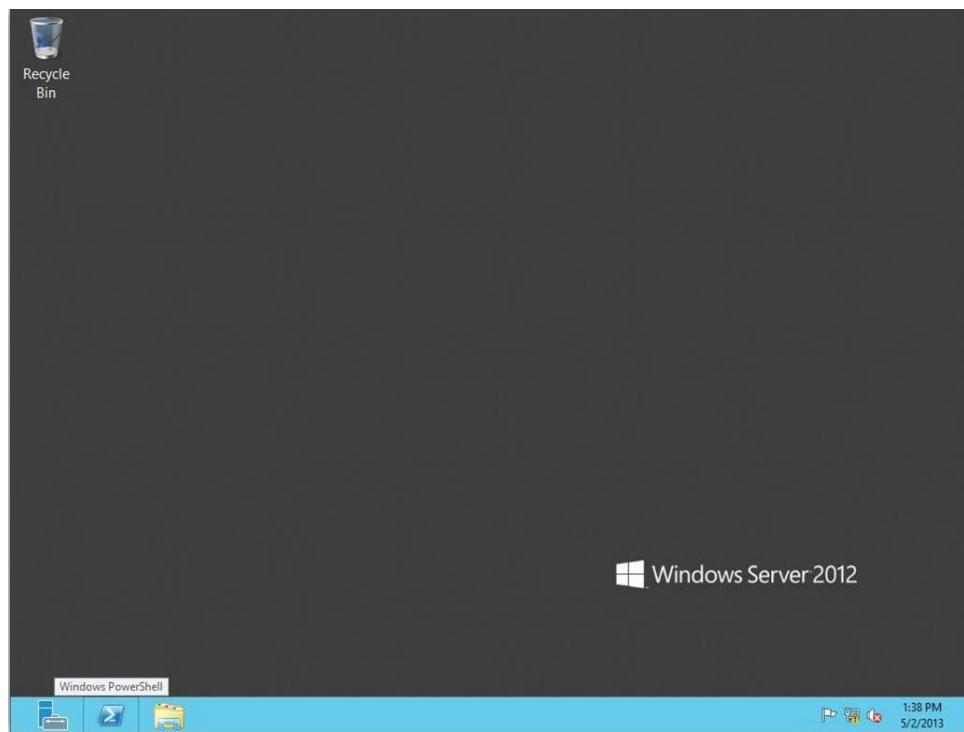


Lab – 3: Converting Windows Server 2012 GUI to Core

1. Login to Computer as Administrator



2. Click **Windows PowerShell**.

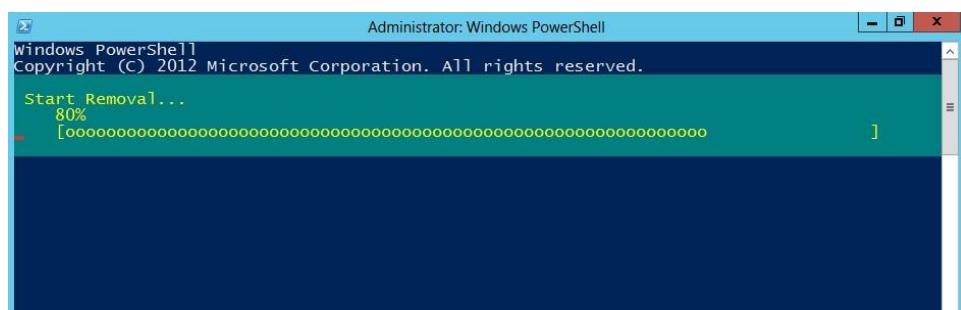


3. Type the following command

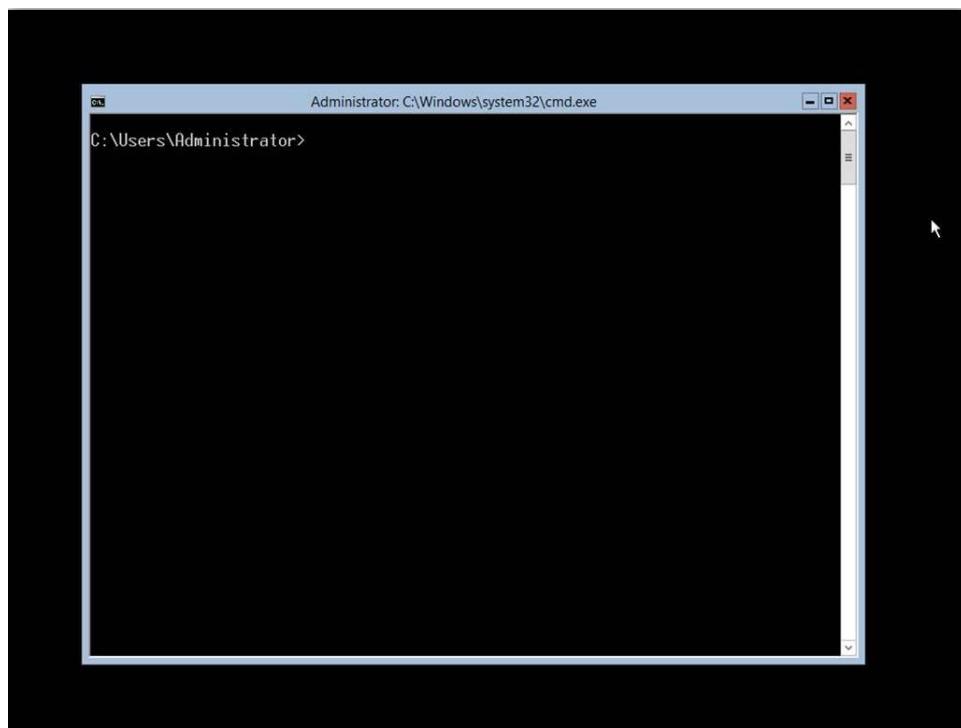
Uninstall-WindowsFeature Server-GUI-Mgmt-Infra, Server-GUI-Shell -Restart



4. The conversion starts and the computer restarts.

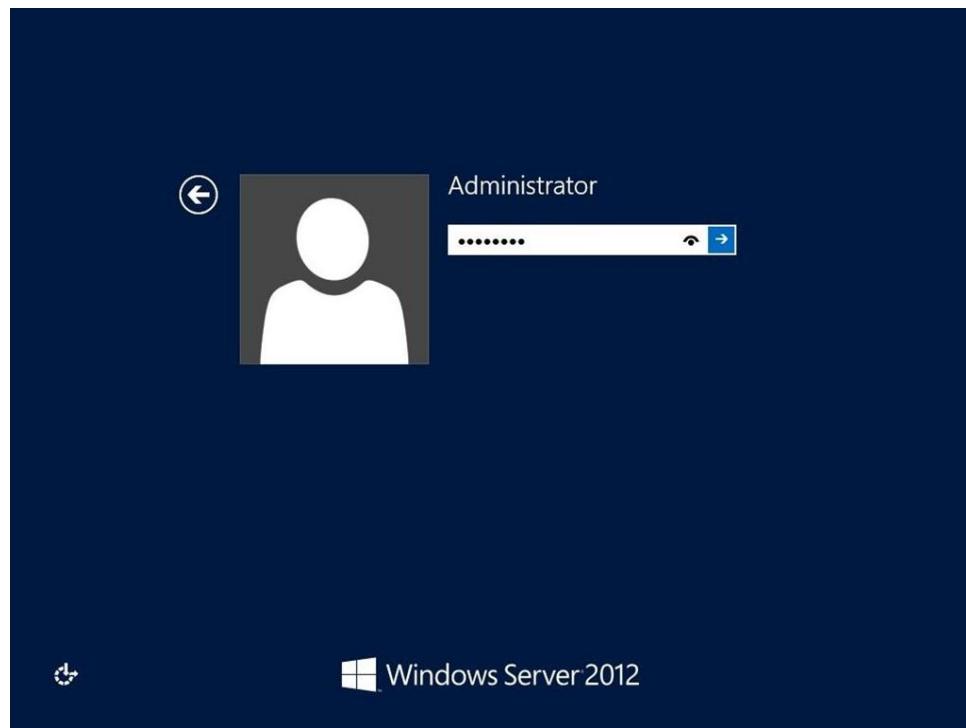


5. Login as Administrator and finally GUI is now converted to Server core.

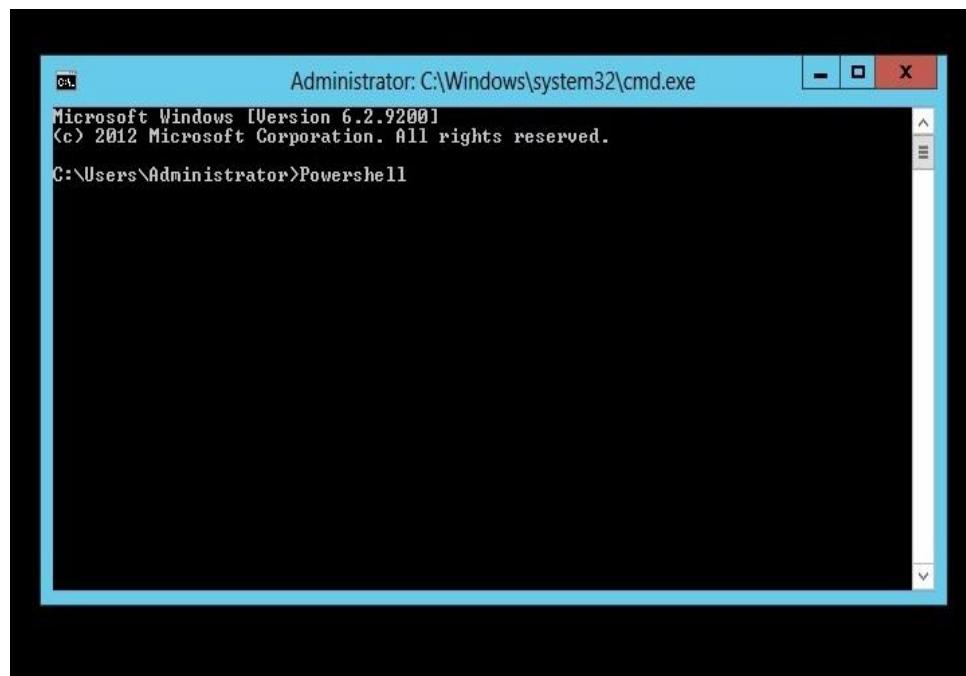


Lab – 4: Converting Windows Server 2012 Core to GUI

1. Login to Computer as Administrator

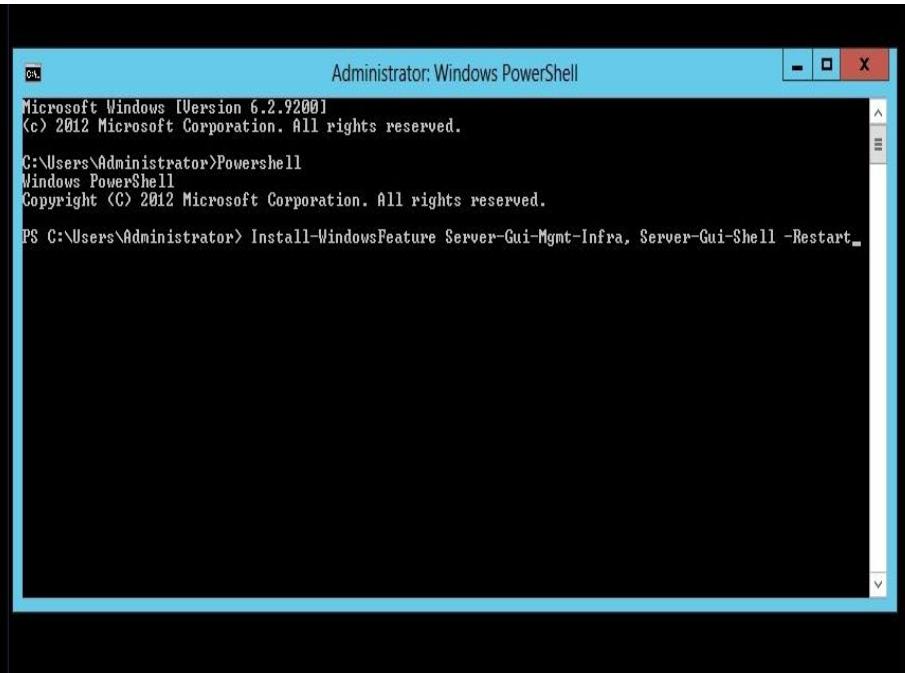


2. In Command Prompt, type **PowerShell**.



3. In PowerShell type the following command to convert Core to GUI.

Install-WindowsFeature Server-GUI-Mgmt-Infra, Server-GUI-Shell -Restart

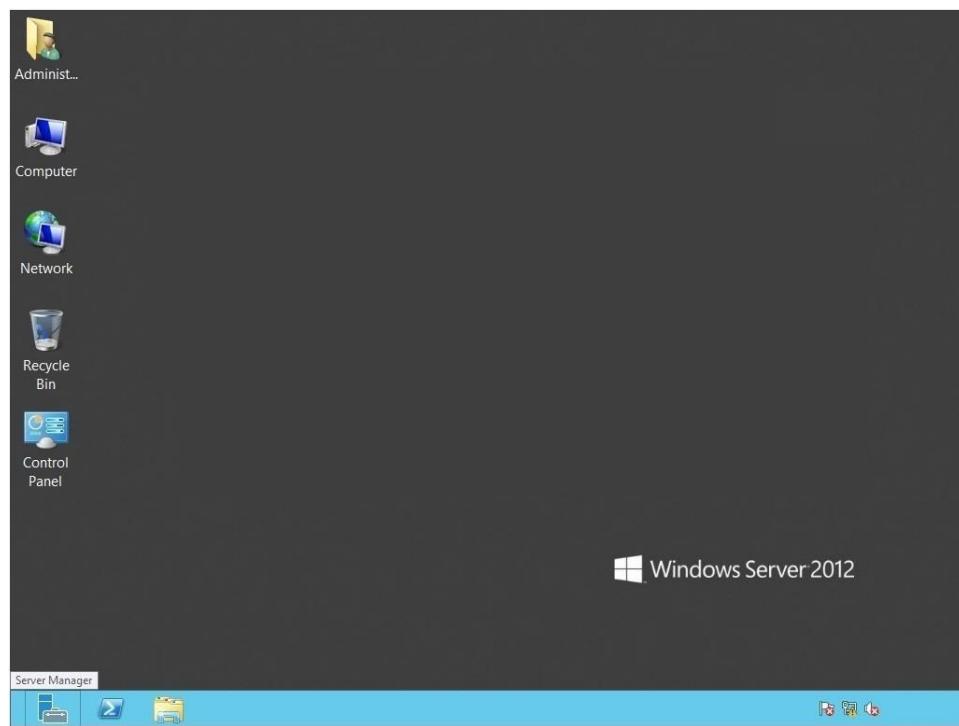


```
Administrator: Windows PowerShell
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>Powershell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Install-WindowsFeature Server-Gui-Mgmt-Infra, Server-Gui-Shell -Restart
```

4. It installs the required GUI features and restarts
5. Login as Administrator and finally Core is now converted to GUI.



IP ADDRESSING

IP Addressing

- Two Versions of Addressing Scheme
 - IP version 4 – 32 bit addressing
 - IP version 6 – 128 bit addressing

IP Address Classes

- Total IP Addressing Scheme is divided into 5 Classes
 - CLASS A
 - CLASS B LAN & WAN
 - CLASS C
 - CLASS D Multicasting
 - CLASS E Research & Development

Class Ranges

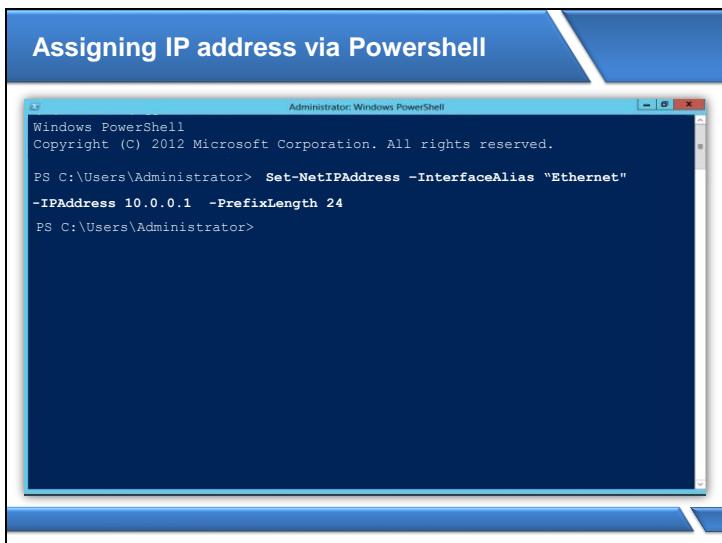
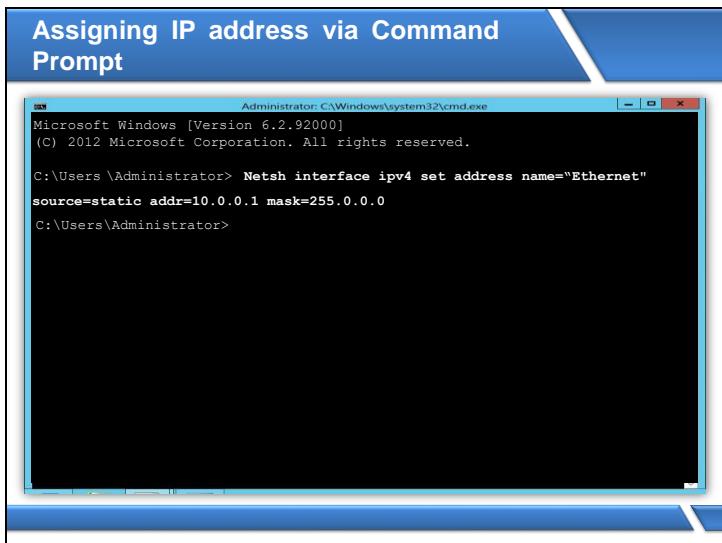
- CLASS A Range
 - 0.0.0.0 - 127.255.255.255
- CLASS B Range
 - 128.0.0.0 - 191.255.255.255
- CLASS C Range
 - 192.0.0.0 - 223.255.255.255
- CLASS D Range
 - 224.0.0.0 - 239.255.255.255
- CLASS E Range
 - 240.0.0.0 - 255.255.255.255

Octet Format

- IP address is divided into Network & Host Portion
 - CLASS A is written as N.H.H.H
 - CLASS B is written as N.N.H.H
 - CLASS C is written as N.N.N.H

Private and Public IP Address

- Private IP Address
 - CLASS A 10.0.0.0 - 10.255.255.255
 - CLASS B 172.16.0.0 - 172.31.255.255
 - CLASS C 192.168.0.0 - 192.168.255.255
- Public IP Address
 - Apart from the above specified IP addresses all other IP addresses are Public IP's



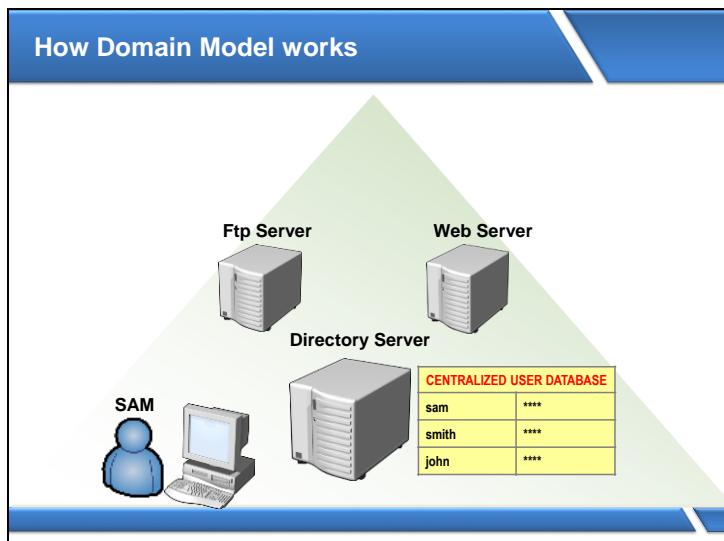
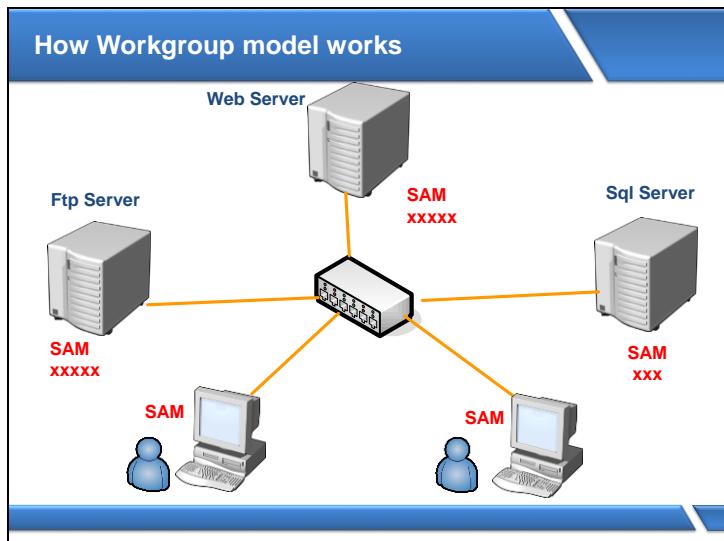
Logical Topologies

IN A WORKGROUP MODEL

- All computers are peers; no computer has control over another computer.
- Each computer has a set of user accounts. To use any computer in the workgroup, you must have an account on that computer

IN A DOMAIN MODEL

- One or more computers are servers. Network administrators use servers to control the security and permissions for all computers on the domain. This makes it easy to make changes because the changes are automatically made to all computers.



What Is Active Directory Domain Services ?

- The AD DS database stores information on user identity, computers, groups, services and resources.
- AD DS domain controllers also host the service that authenticates user and computer accounts when they log on to the domain

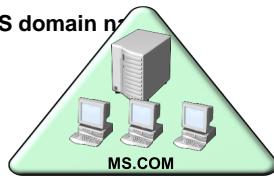


Purpose of Active Directory

- Provides User Logon and Authentication Services using Kerberos protocol.
- To Centralize and Decentralize the resource management.
- To centrally organize and manage:
 - User Accounts, Computers, Groups, Network Resources.
- Enables authorized Users to easily locate Network Resources.

Domain

- Domain is a logical grouping of user, computer, and group objects for the purpose of management and security.
- Creating the initial domain controller in a network also creates the domain—you cannot have a domain without at least one domain controller.
- Each domain is identified by a DNS domain name.



What is a Domain Controller ?

- A domain controller is a server that is configured to store a copy of the AD DS directory database (NTDS.DIT) and a copy of the SYSVOL folder.
- All domain controllers except RODCs store a read/write copy of both NTDS.DIT and the SYSVOL folder.
- NTDS.DIT is the database itself, and the SYSVOL folder contains all the template settings for GPOs.



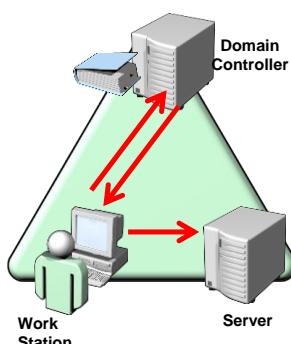
What is a Domain Controller ?

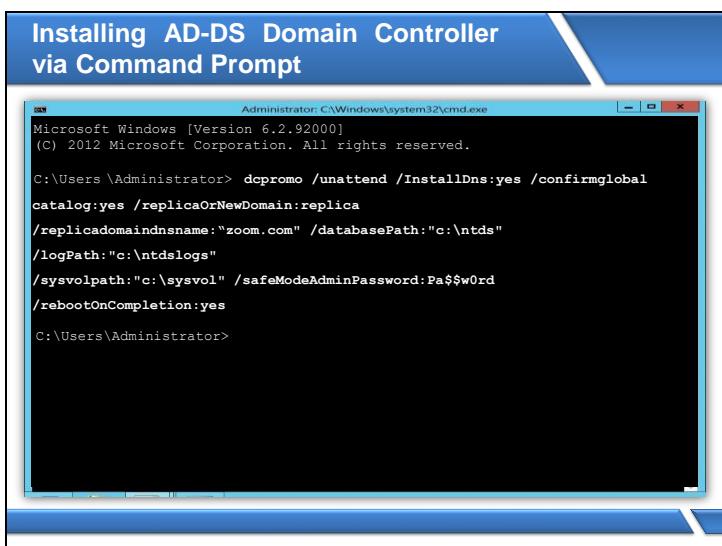
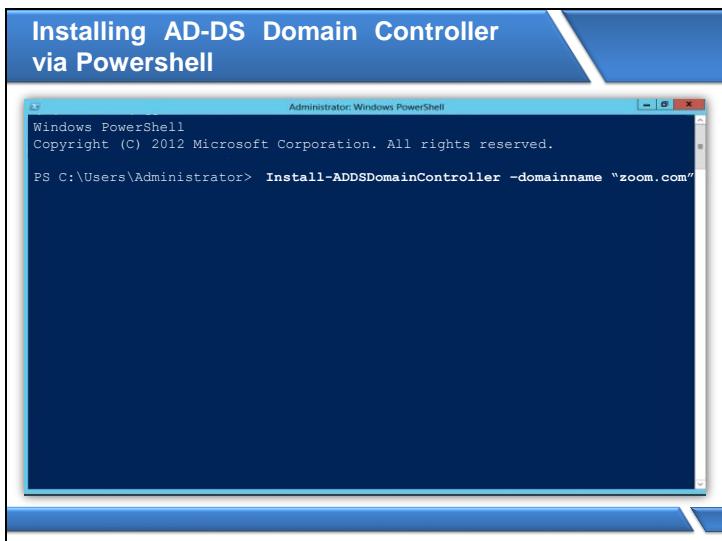
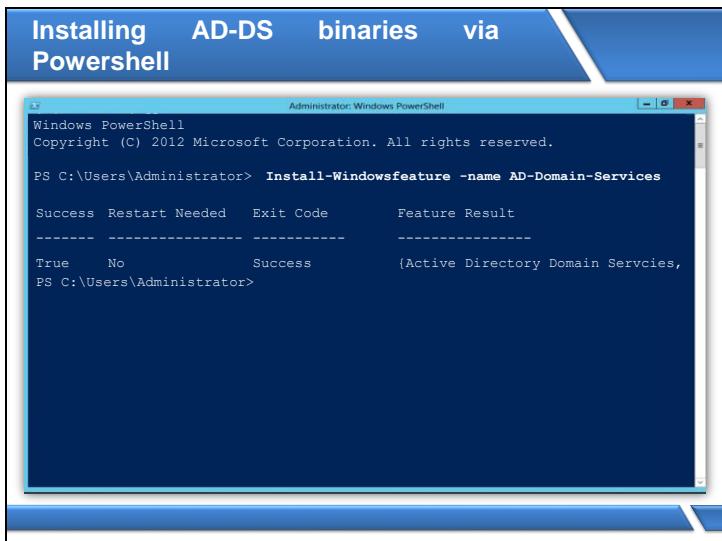
- Domain controllers host several other Active Directory-related services, including the Kerberos authentication service and the Key Distribution Center (KDC).
- Kerberos authentication service is used by User and Computer accounts for logon authentication
- KDC is the service that issues the ticket-granting ticket (TGT) to an account that logs on to the AD DS domain.



AD DS Logon Process

1. User Account is authenticated to Domain Controller
2. Domain Controller returns TGT back to Client
3. Client uses TGT to apply for access to Workstation
4. Domain Controller grants access to Workstation
5. Client uses TGT to apply for access to Server
6. Domain Controller returns access to Server



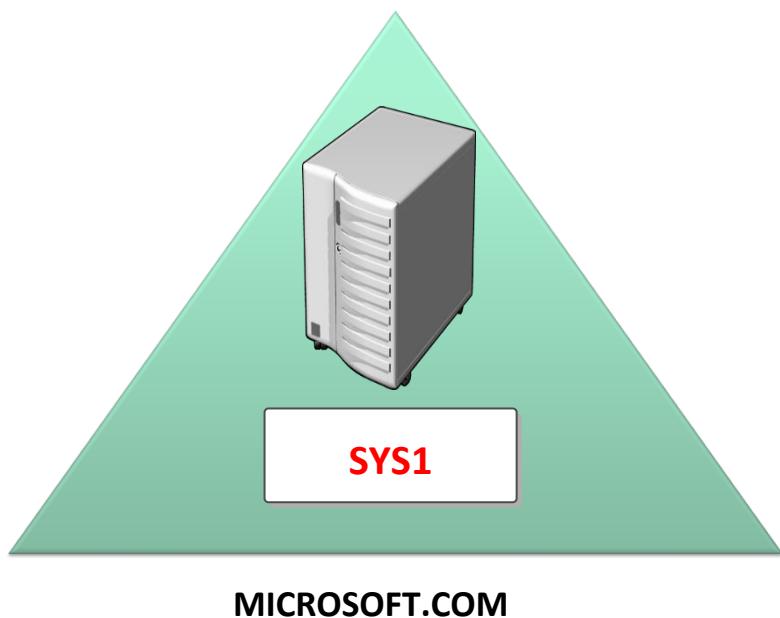


ACTIVE DIRECTORY

Pre-requisites:

Before working on this lab, you must have

1. A Computer with Windows Server 2012 Operating System and connected in the network.



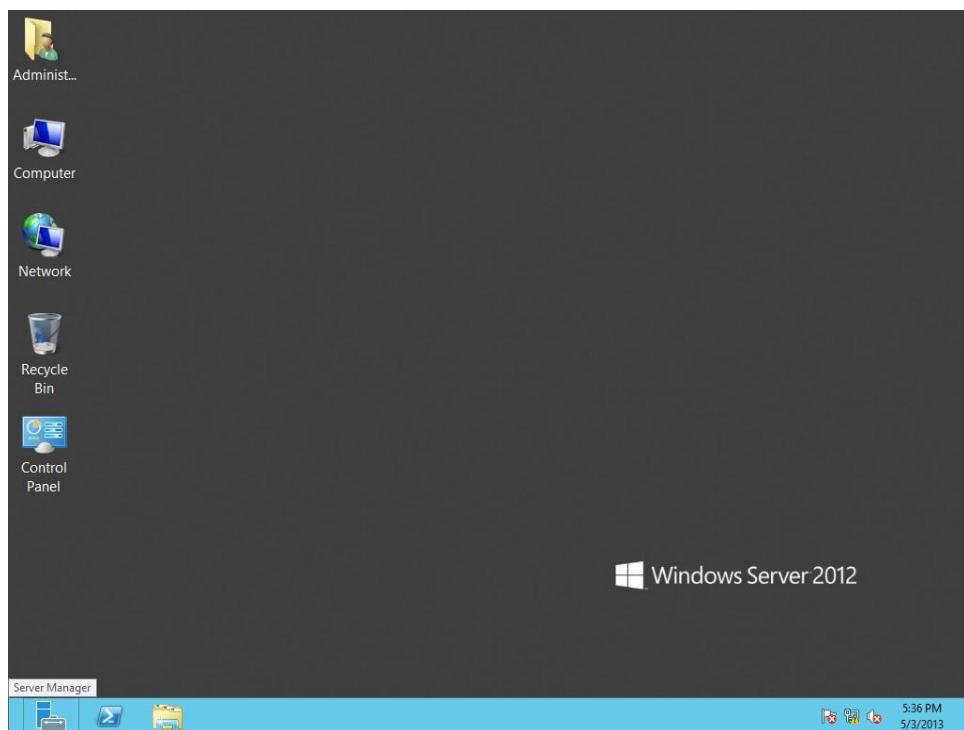
SYS1

Domain Controller

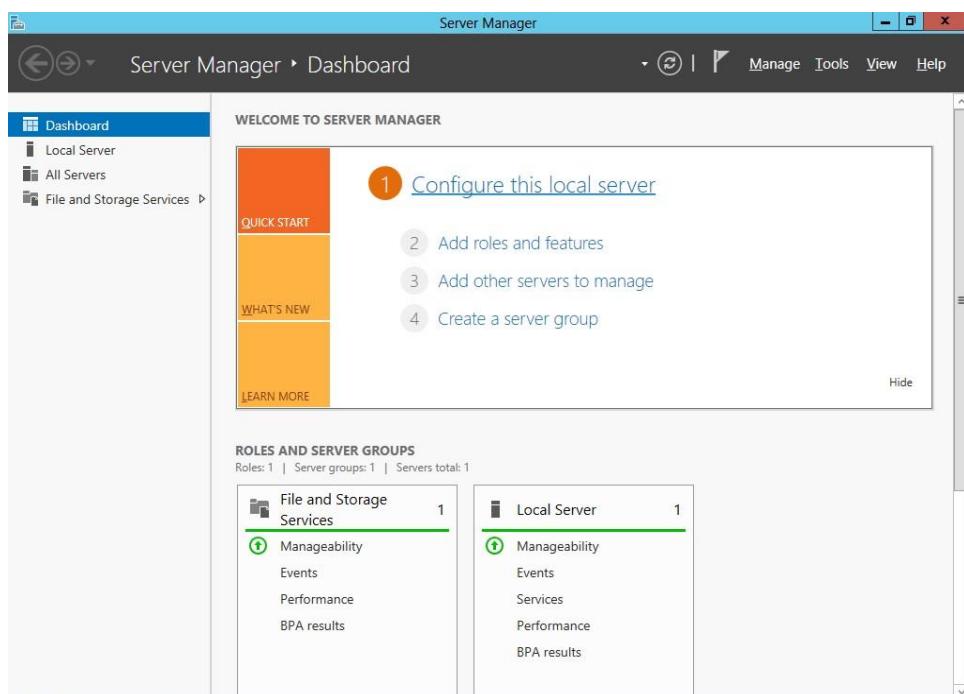
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1

Lab – 1: Assigning IP Address

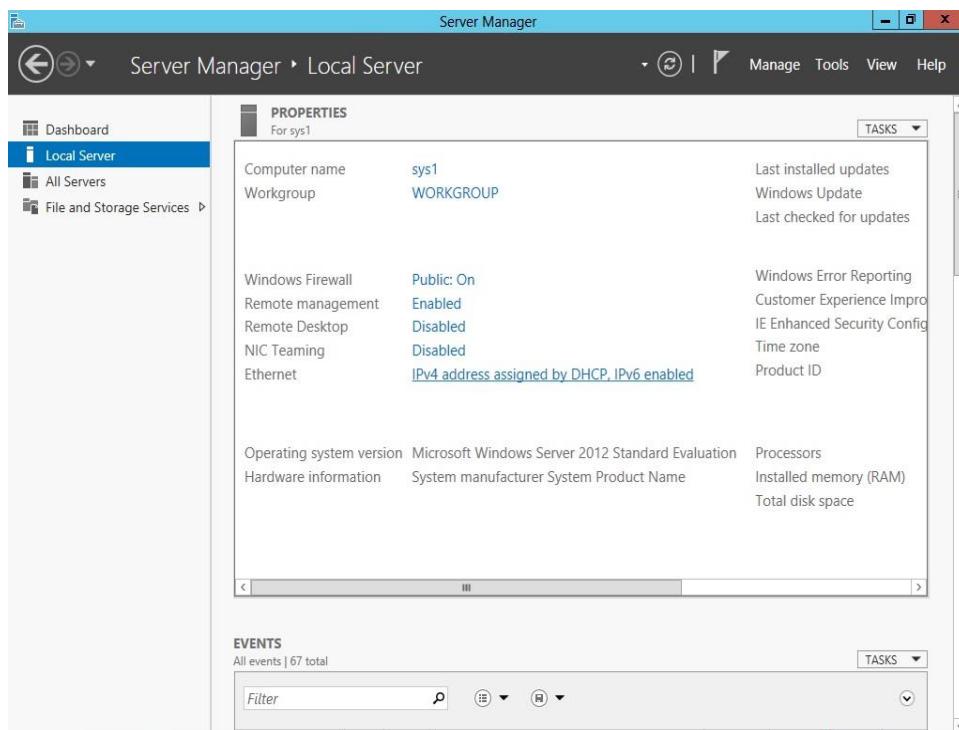
1. Click **Server Manager**.



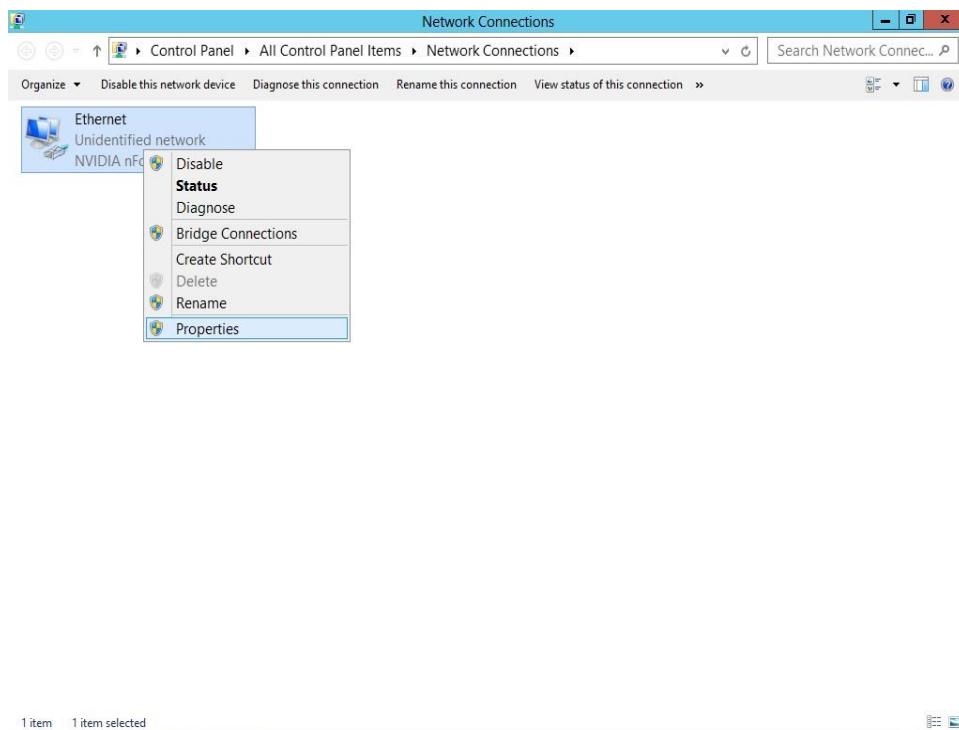
2. In Server Manager Dashboard, Click **Configure this local server**.



3. In Local Server, select Ethernet IPv4 address assigned by DHCP.

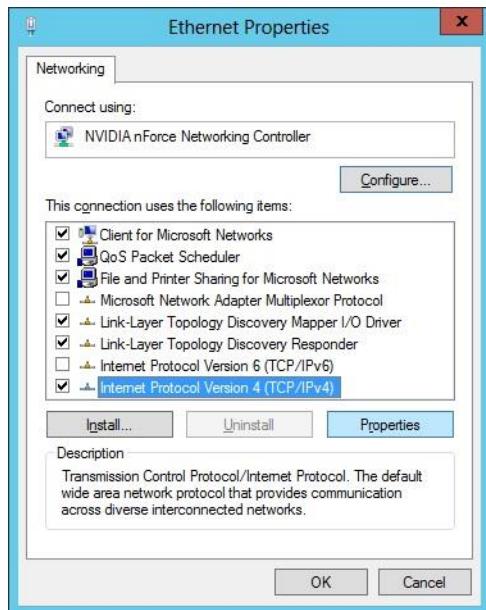


4. Right click **Ethernet**, select **Properties**.

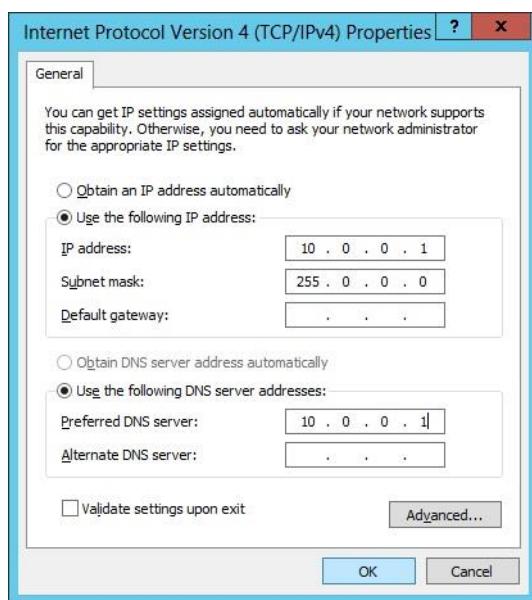


5. Select **Internet Protocol Version 6 (TCP/IPv6)** and **unchecked the box**.

6. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



7. Select **Use the following IP address** and enter the IP address and click Subnet mask, it will be entered automatically and select **Use the DNS Server addresses** and enter the **Preferred DNS Server address**



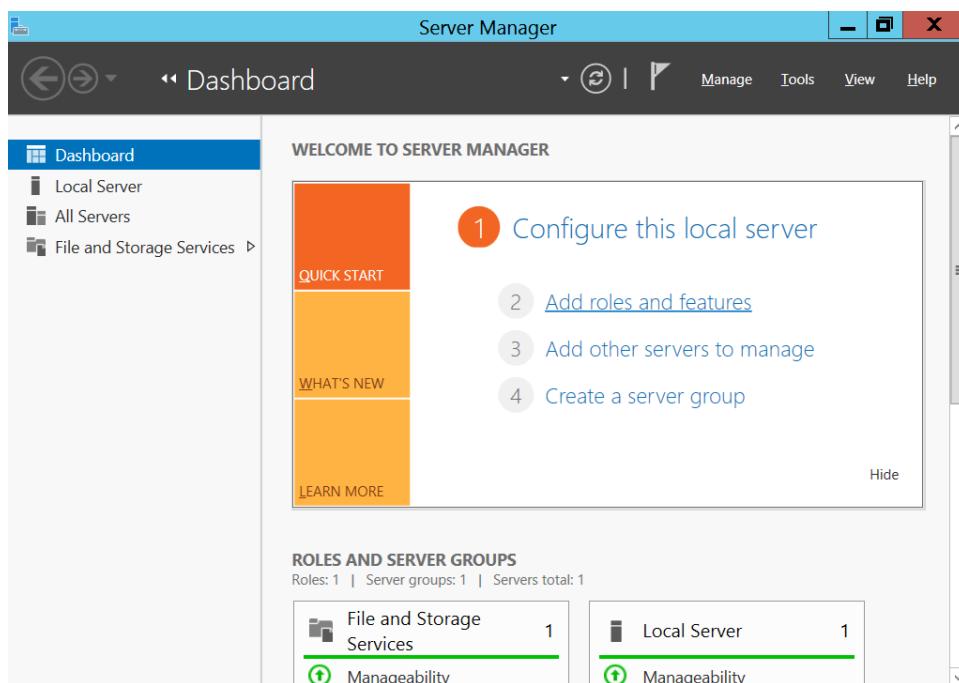
8. Click **OK**, and **OK**.

Lab – 2: Installing Active Directory

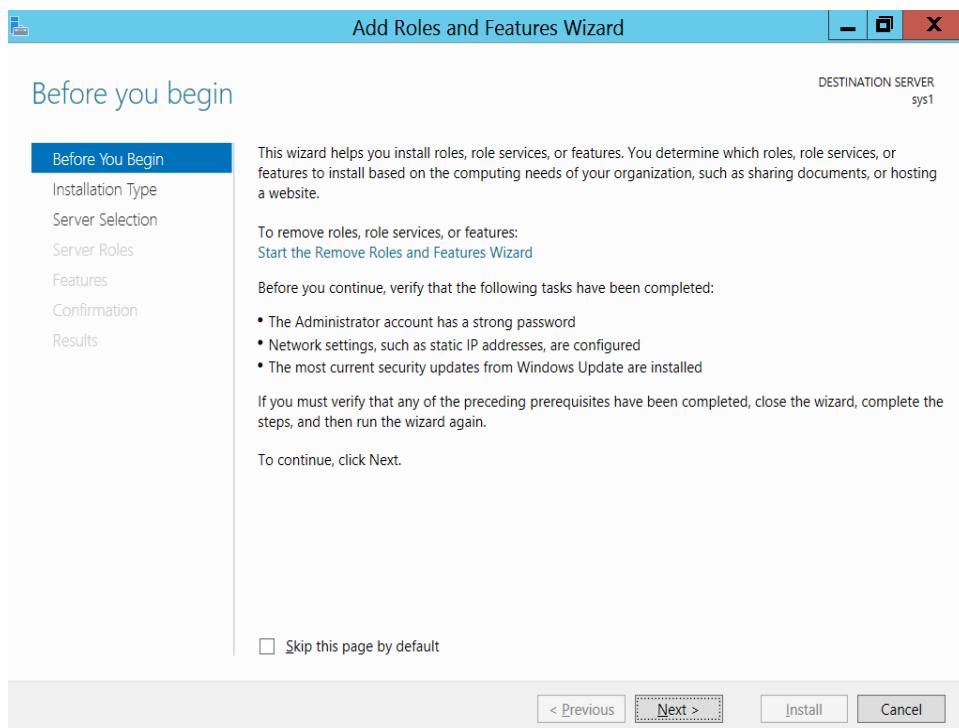
1. Log in as **Administrator** to the **Workgroup Computer**.
2. Assign **IP Address** and preferred **DNS Server Address**.
3. Click **Server Manager**



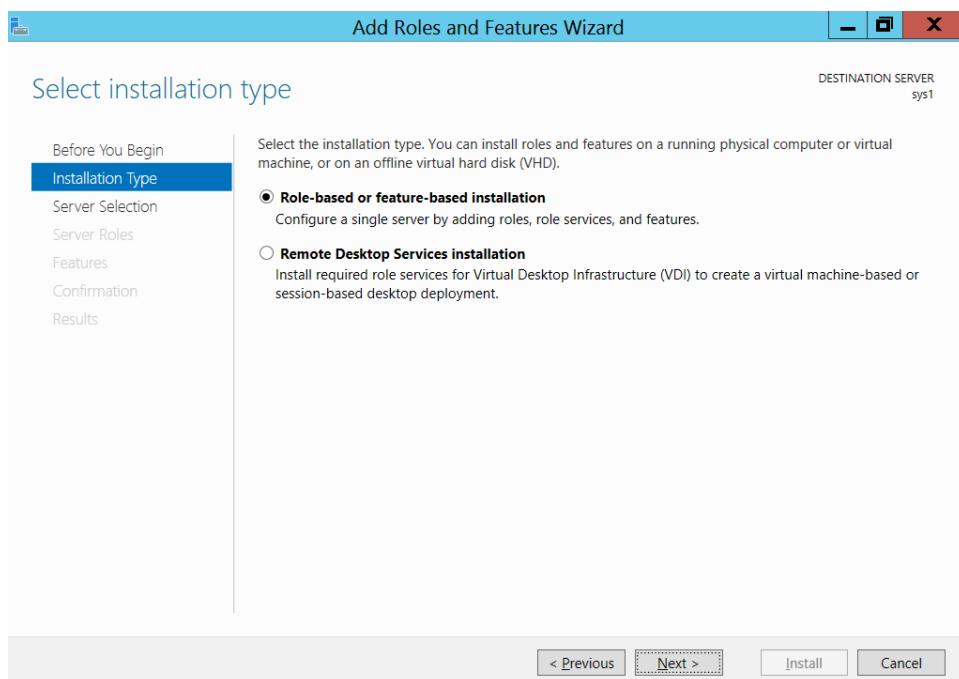
4. In Server Manager Dashboard, Click **Add roles and features**.



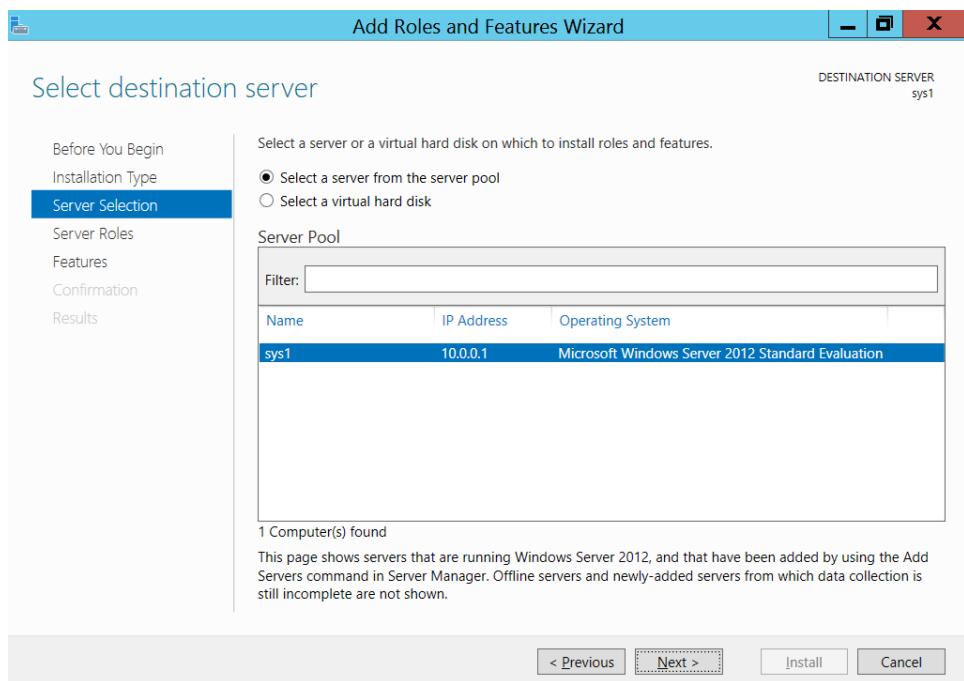
5. In Before you begin page, click **Next**.



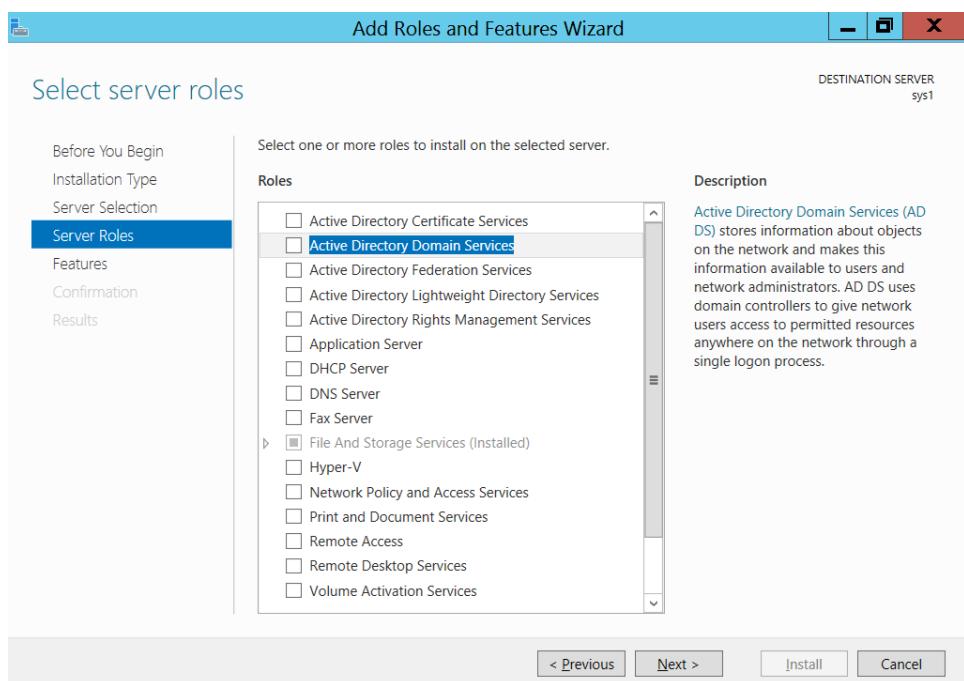
6. In Select installation type, select **Role-based or feature-based installation**, click **Next**.



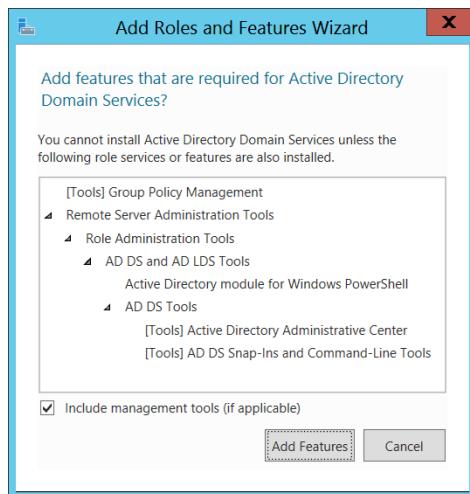
7. In Select destination server, from Server Pool select **SYS1, click **Next**.**



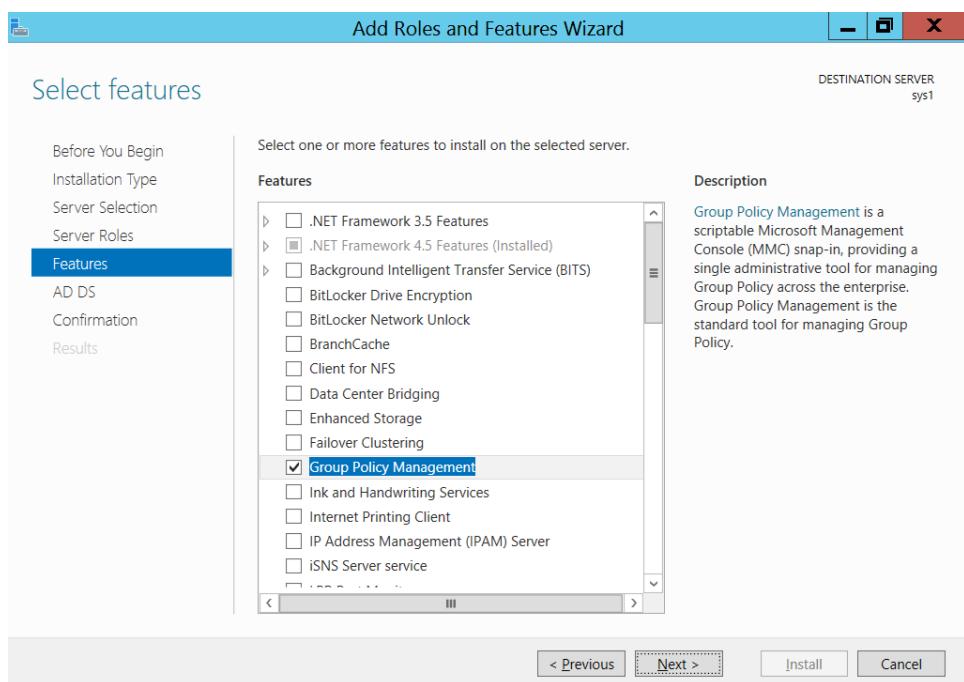
8. In Roles, check the box **Active Directory Domain Services.**



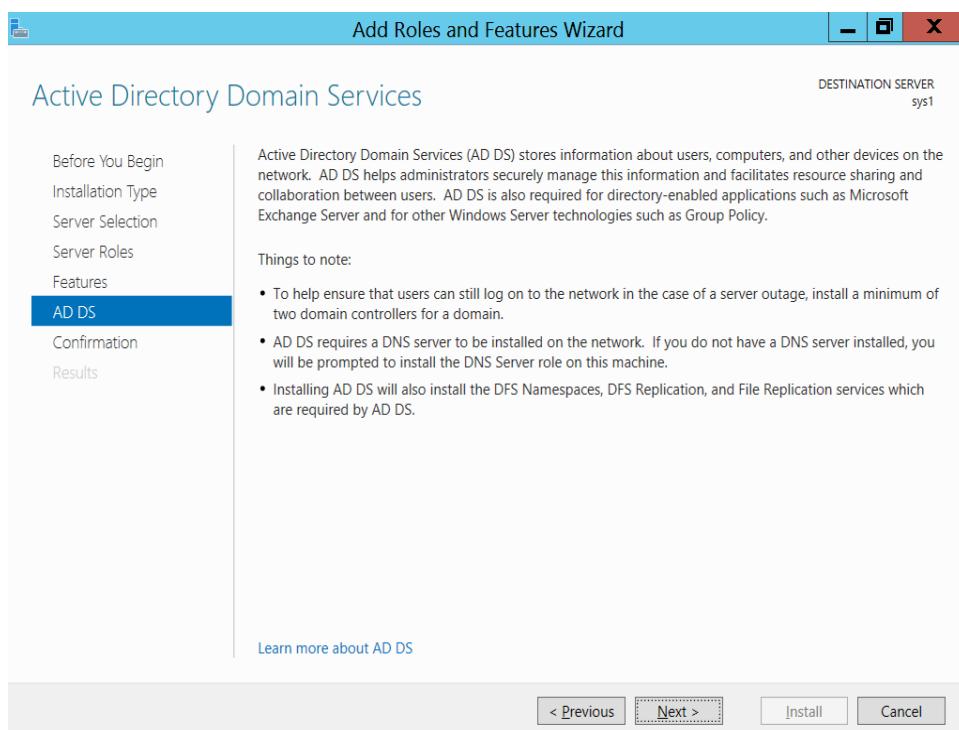
- 9.** Click **Add Features**, to install the required features for Active Directory Domain Services. Click **Next**.



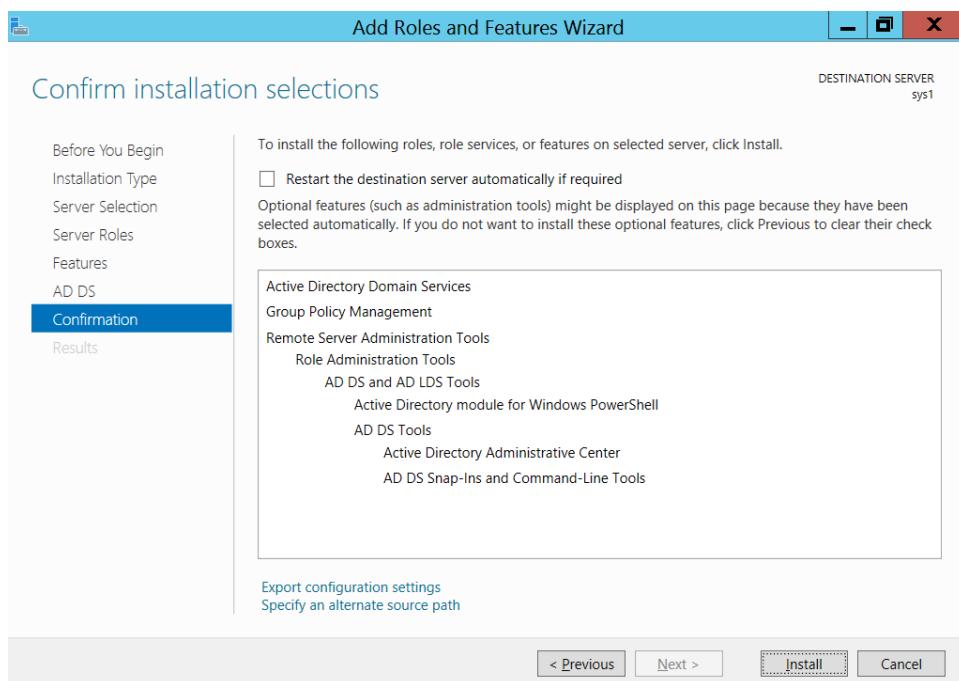
- 10.** In Select features wizard, click **Next**.



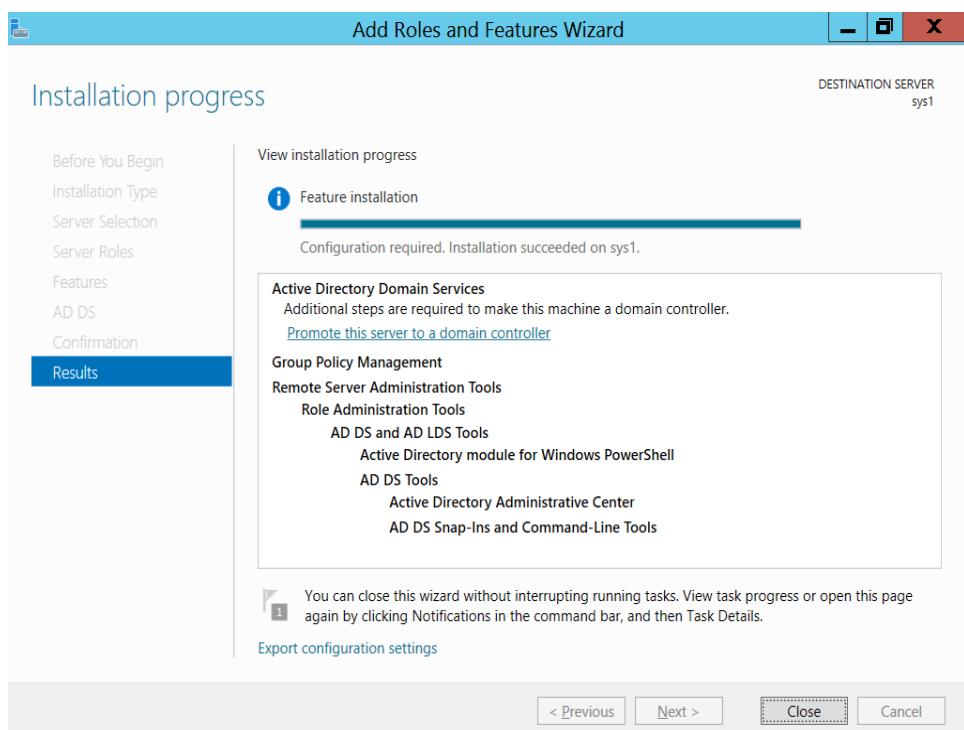
11. In Active Directory Domain Services wizard, click **Next.**



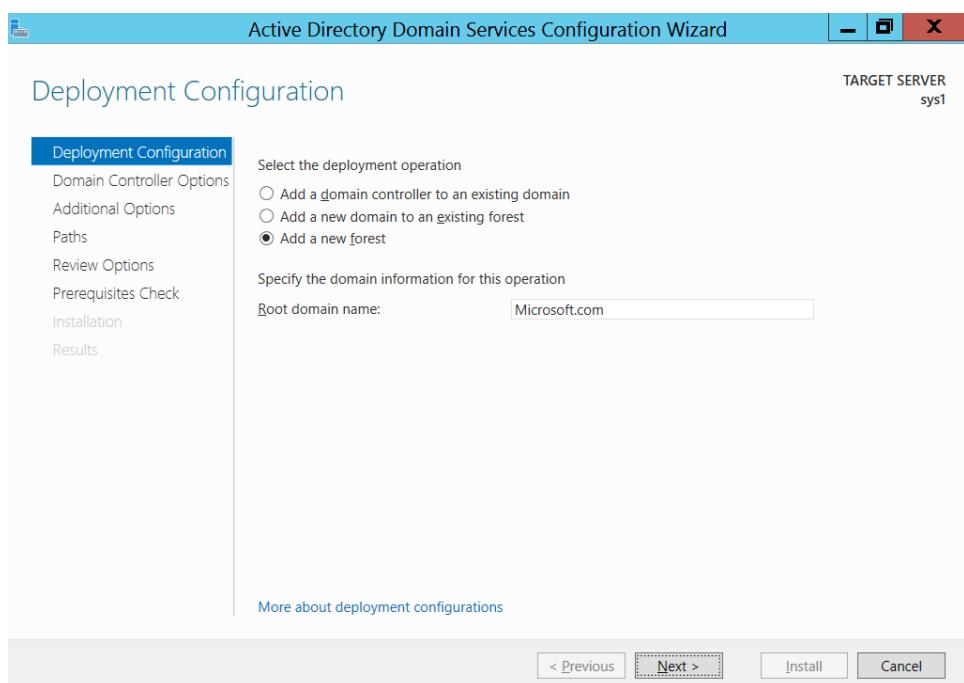
12. Check the box **Restart the destination server automatically if required. Click **Install**.**



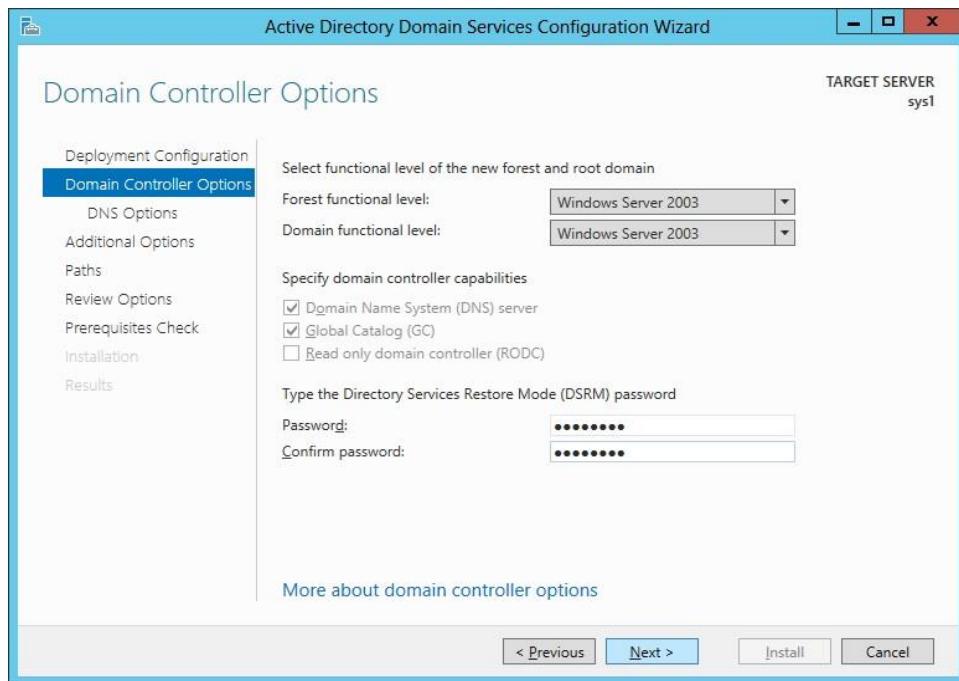
- 13. Click Promote this server to a domain controller.**



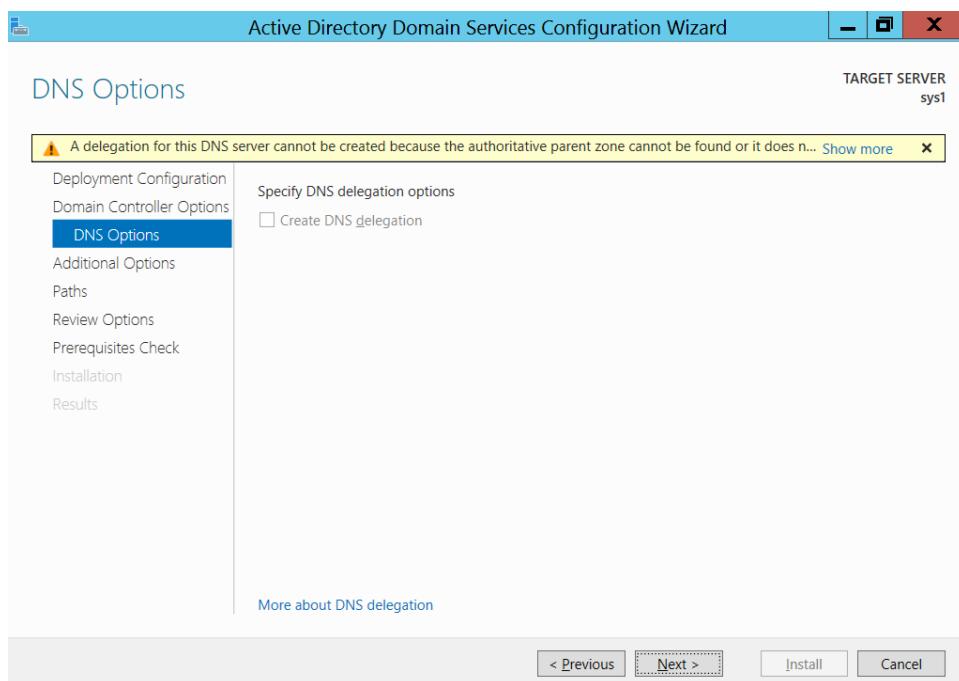
- 14. In Deployment Configuration wizard, select **Add a new forest**, enter the **Root domain name** (Ex: Microsoft.com) and click **Next**.**



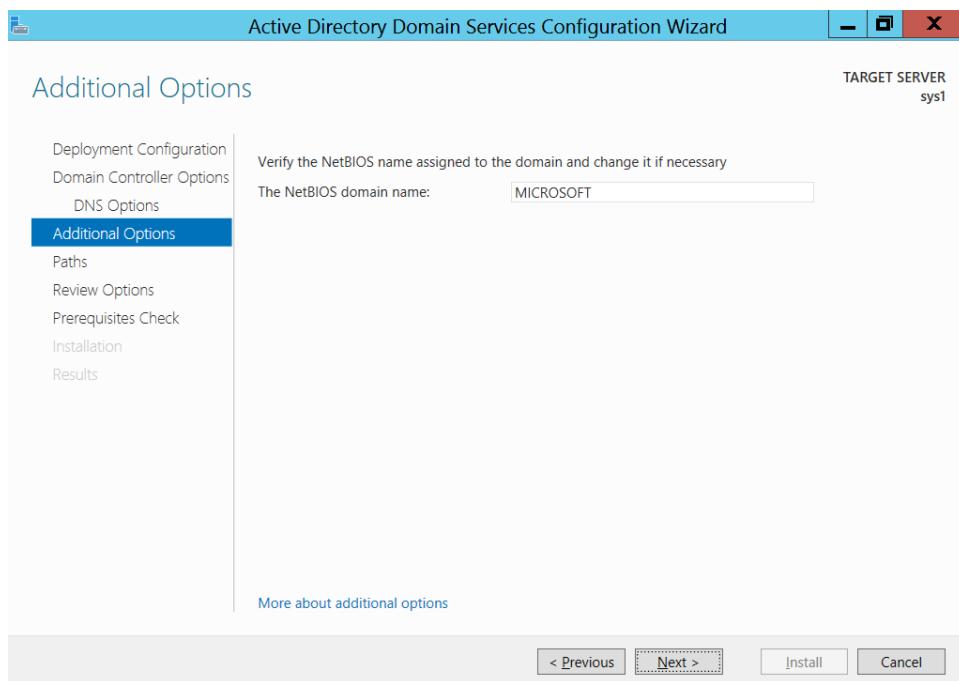
15. In Domain Controller Options, change **Forest** and **Domain functional level** to **Windows Server 2003**, and Domain Name System server. Type the Directory Services Restore Mode **Password** and **Confirm Password** and click **Next**.



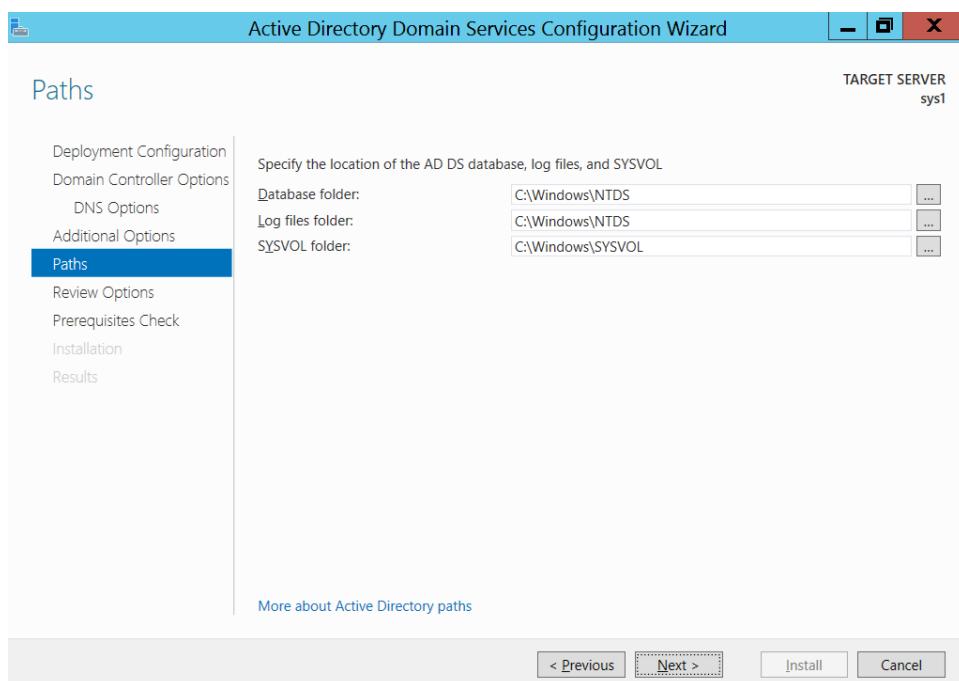
16. On DNS Options page, click **Next**.



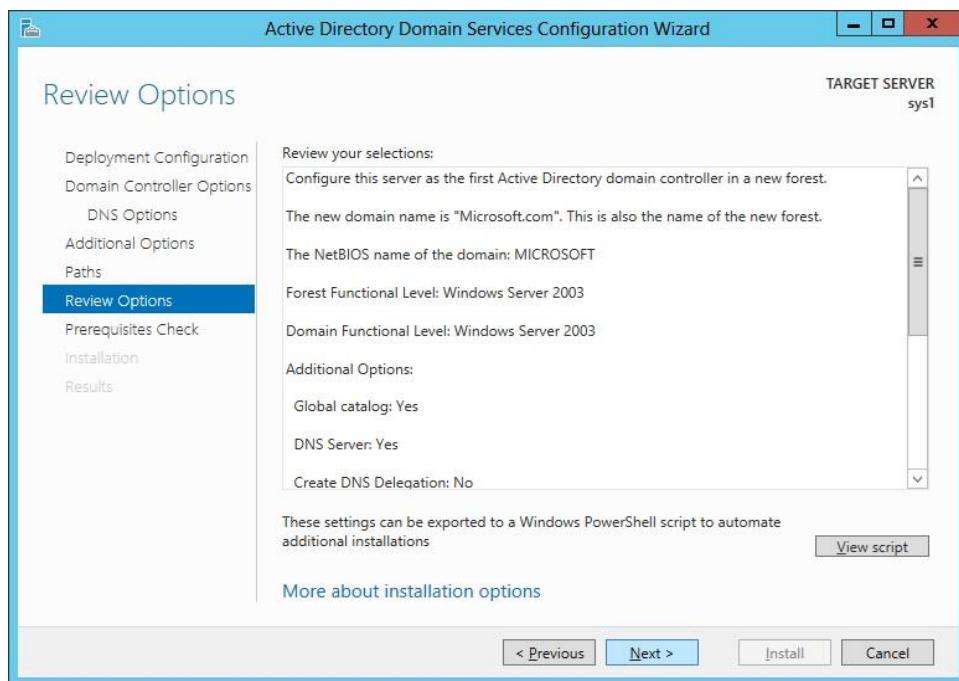
17. Verify the NetBIOS domain name (Ex: MICROSOFT), click **Next**.



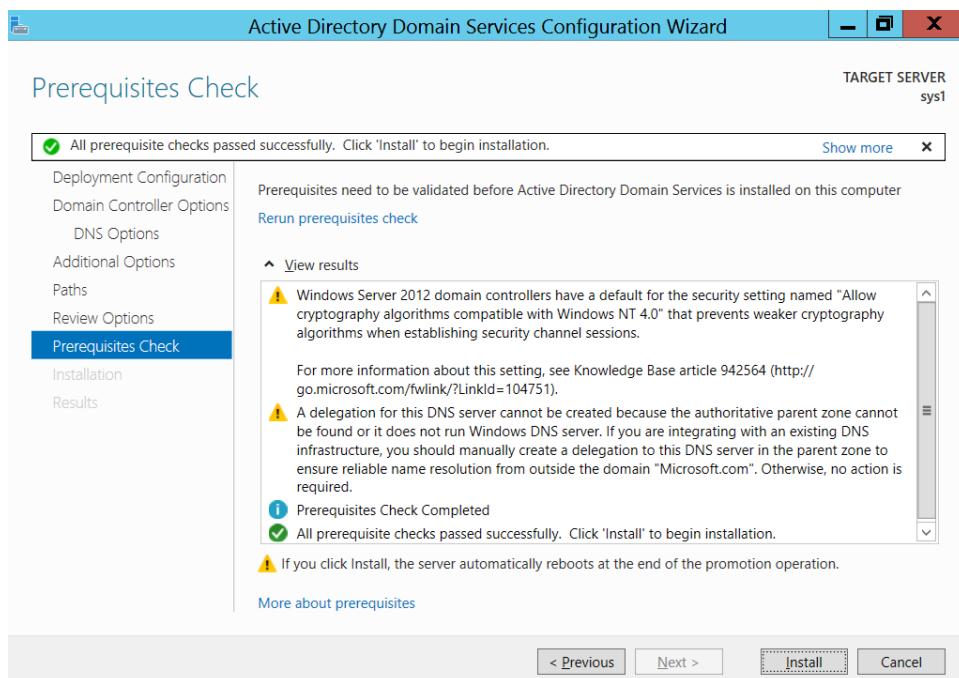
18. Verify the location of the AD DS database, log files, and SYSVOL, click **Next**.



19. Review the Summary and click **Next.**

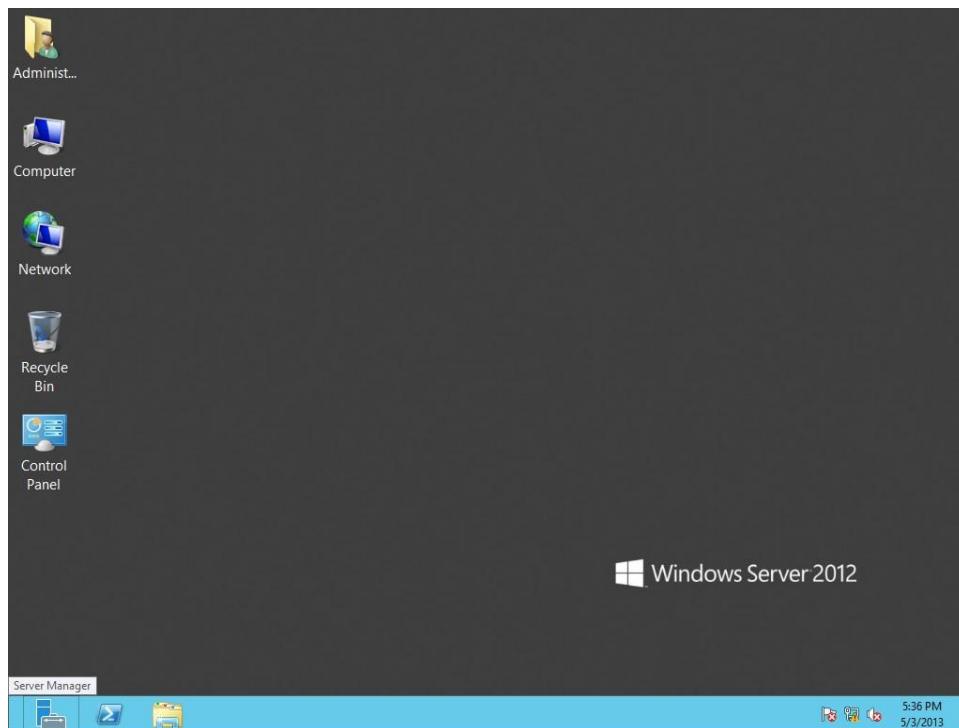


20. Click **Install to begin installation.**

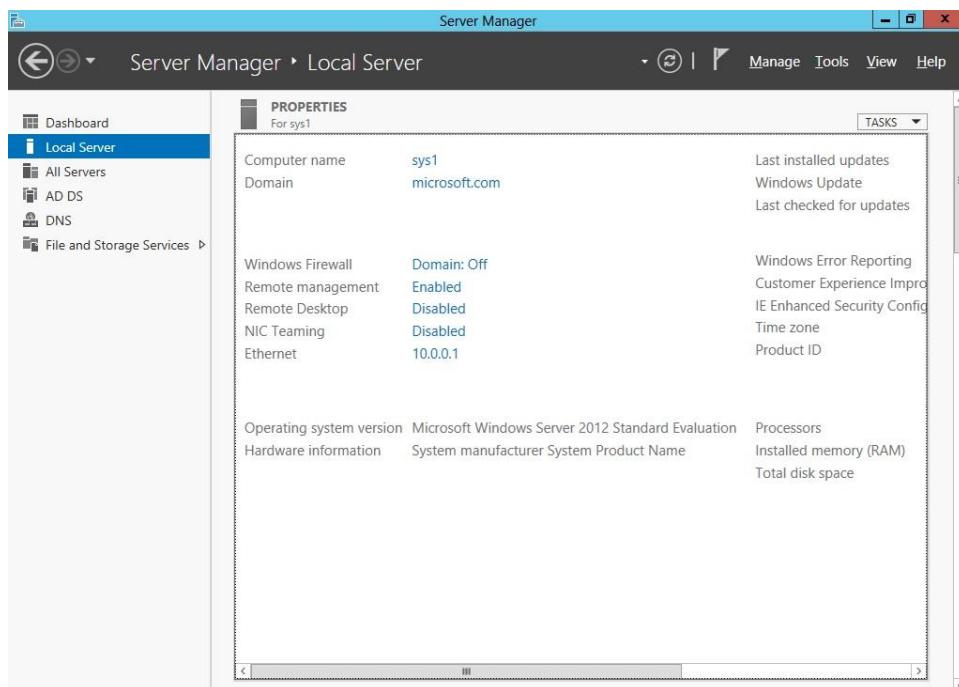


Verification:

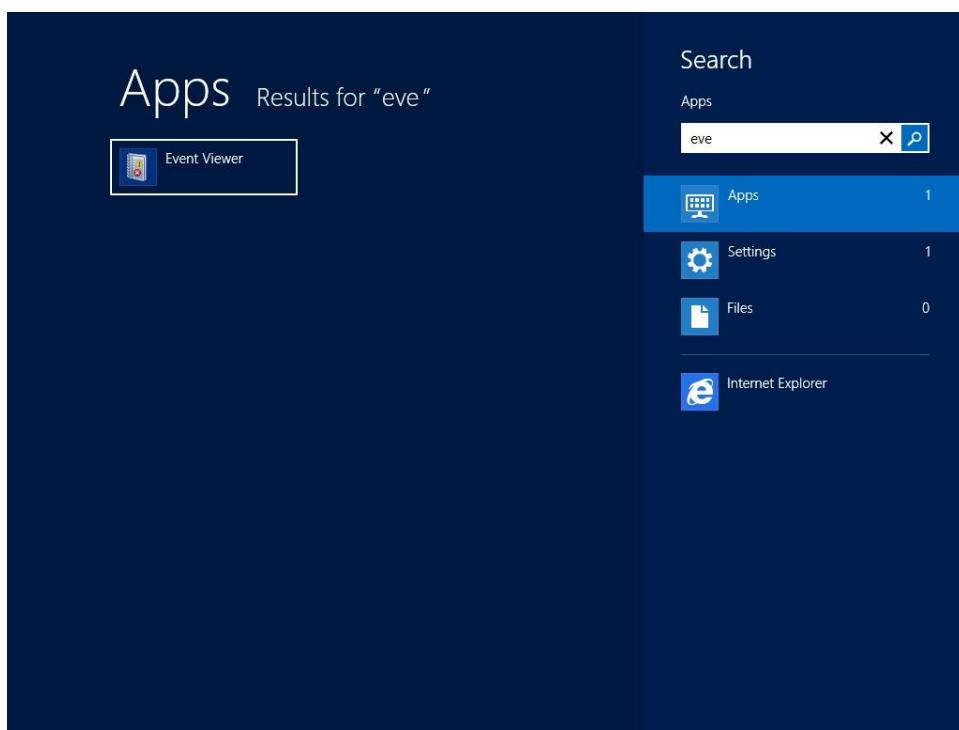
1. Click Server Manager.



2. In Server manager, select Local Server and verify for domain **Microsoft.com**.



3. Go to Start, type event in Search Apps, select **Event Viewer**.



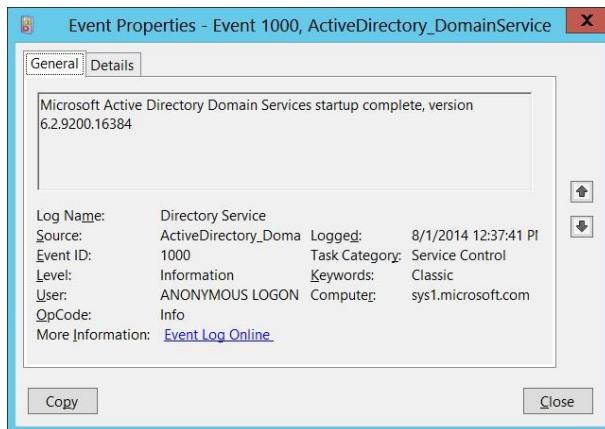
4. Expand Applications and Services Logs, select Directory Service, verify for the Event ids 1394 and 1000.

The screenshot shows the "Event Viewer" application window. The left pane shows a tree view of logs: "Event Viewer (Local)", "Custom Views", "Windows Logs", "Applications and Services Logs" (expanded to show "Active Directory Web Services", "DFS Replication", "Directory Service" [selected], "DNS Server", "File Replication Service", "Hardware Events", "Internet Explorer", "Key Management Service"), "Microsoft", "Windows PowerShell", and "Subscriptions". The main pane displays the "Directory Service" log with 1,544 events. A table lists columns: Level, Date and Time, Source, Event..., and Task Several entries are visible, including:

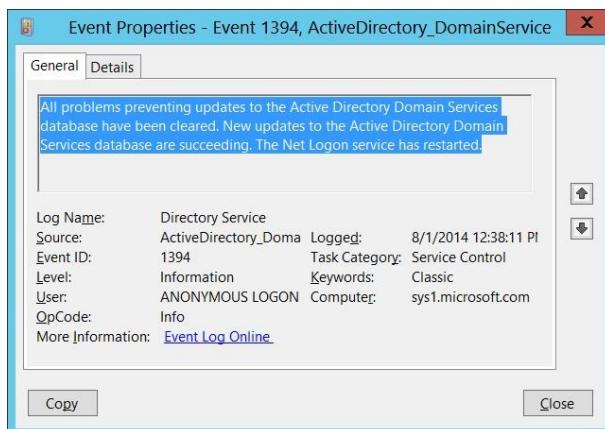
Level	Date and Time	Source	Event...	Task ...
Information	8/1/2014 12:52:42 ...	Activ...	1869	Glob...
Information	8/1/2014 12:38:11 ...	Activ...	1394	Servic...
Information	8/1/2014 12:37:41 ...	Activ...	1000	Servic...
Warning	8/1/2014 12:37:41 ...	Activ...	2886	LDAP...
Information	8/1/2014 12:37:31 ...	Activ...	2120	Intern...
Information	8/1/2014 12:37:31 ...	Activ...	2121	Intern...
Information	8/1/2014 12:29:08 ...	NTDS...	701	Onlin...
Information	8/1/2014 12:29:06 ...	Activ...	1869	Glob...
Information	8/1/2014 12:29:06 ...	NTDS...	700	Onlin...
Information	8/1/2014 12:29:06 ...	NTDS...	326	Gener...
Information	8/1/2014 12:29:06 ...	NTDS...	105	Gener...
Information	8/1/2014 12:29:06 ...	NTDS...	102	Gener...
Information	8/1/2014 12:14:35 ...	Activ...	1394	Servic...

The right pane shows the "Actions" menu, which includes options like "Open Save...", "Create Cust...", "Import Cus...", "Clear Log...", "Filter Curre...", "Properties", "Find...", "Save All Ev...", "Attach a Ta...", "View", "Refresh", "Help", "Selected Ev...", "Event Prop...", "Attach Tas...", "Copy", "Save Select...", and "Refresh".

5. Event 1000 displaying Active Directory Domain Services startup complete.



6. Event 1394 displaying Active Directory Domain Services updated successfully.





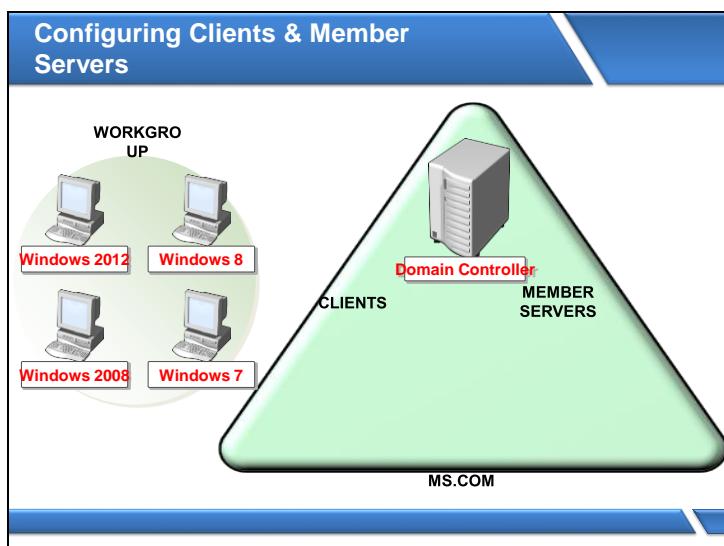
Clients & Member Servers

CLIENTS

- A computer joined in the domain with Client Operating system.
- Client Operating systems like
 - Windows 8, Windows 7, Windows XP professional . . .

MEMBER SERVERS

- A computer joined in the domain with Server Operating system.
- Server Operating systems like
 - Windows server 2012, Windows server 2008, Windows server 2003....





Local Users & Domain Users

Local User

- A user account created in local database of a computer.
- Local users are generally used in WORKGROUP model.
- Local users can login only on the respective computer.

Domain User

- A user account created in ACTIVE DIRECTORY database.
- Domain users are used in DOMAIN model.
- Domain users can logon to any computer in the DOMAIN.

Command	Description
DSadd	Creates AD DS objects
Dsget	Displays properties of AD DS objects
Dsquery	Searches for AD DS objects.
DSmod	Modifies AD DS objects
DSrm	Removes AD DS objects
Dsmove	Moves AD DS objects

DS Commands - Example

- **To modify the department of a user account, type:**
`Dsmod user "cn=vijay kumar, ou=users, dc=zoom, dc=com" –dept IT`
- **To display the email of a user account, type:**
`Dsget user "cn=vijay kumar, ou=users, dc=zoom, dc=com" –email`
- **To delete a user account, type:**
`Dsrm "cn=vijay kumar, ou=users, dc=zoom, dc=com"`
- **To create a new user account, type:**
`Dsadd user "cn=vijay kumar, ou=users, dc=zoom,dc=com"`

Manage User Accounts via PowerShell

Cmdlet	Description
New-ADUser	Creates user accounts
Set-ADUser	Modifies properties of user accounts
Remove-ADUser	Deletes user accounts
Set-ADAccountPassword	Resets the password of a user account
Set-ADAccountExpiration	Modifies the expiration date of a user account
Unlock-ADAccount	Unlocks a user account after it has become locked after too many incorrect login attempts

Powershell Cmdlets - Example

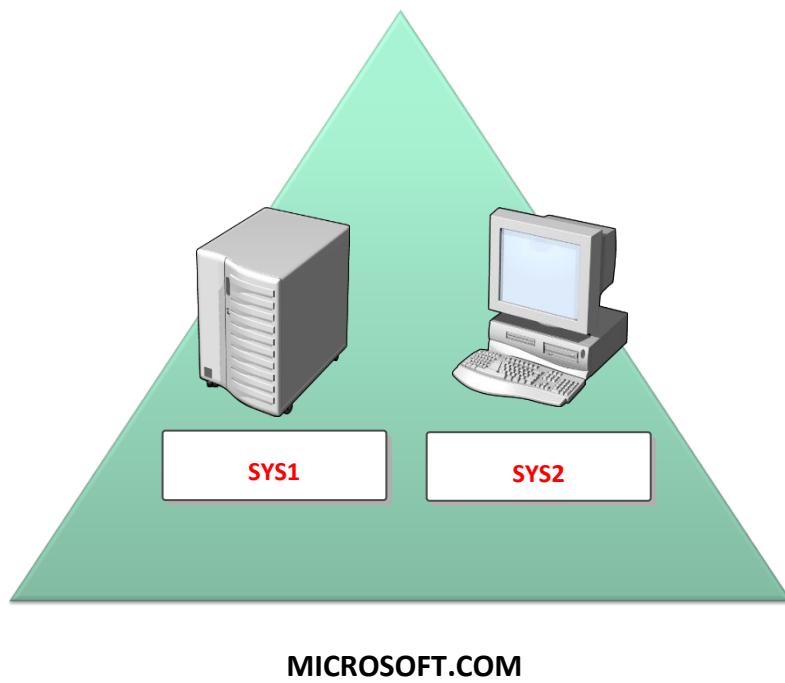
- **To create a new user account with Department IT, type:**
`New-ADUser "Vijay Kumar" –AccountPassword (Read-Host
–AsSecureString "Enter password") -Department IT`

MEMBER SERVER/CLIENT and USER MANAGEMENT

Pre-requisites:

Before working on this lab, you must have

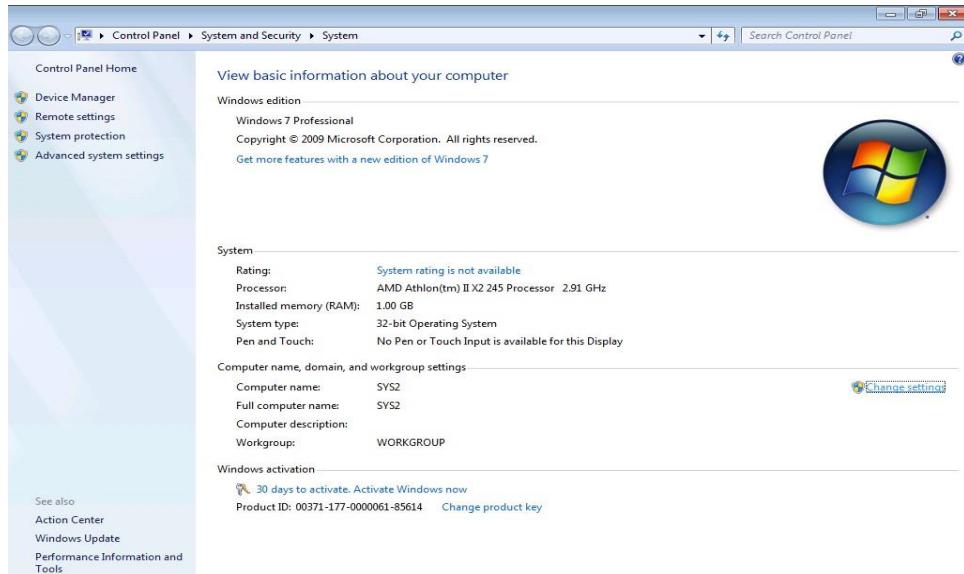
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server or windows 7.



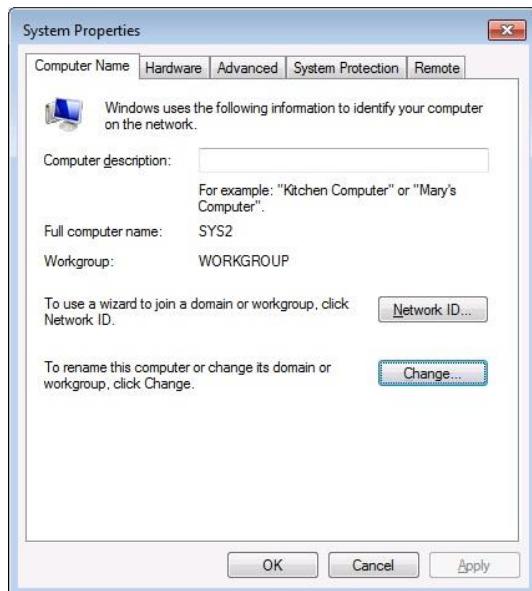
SYS1	SYS2
Domain Controller	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Member Server / Client	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1

Lab – 1: Configuring Client (Windows 7)

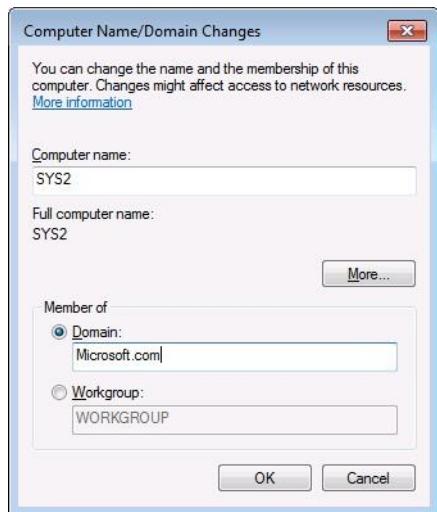
1. Log in as **Administrator** to **Workgroup Computer**.
2. Right click **Computer Icon** and click **Properties** and click **Change settings**.



3. In the System properties dialog box click **Change**.



4. Select the Member of **Domain** and enter the Domain Name (Ex:**Microsoft.com**).



5. Enter the user name **Administrator** and **Password**, click **OK**.



6. Welcome Message appears indicating that the computer was successful in joining the Domain, click**OK**and **OK**, It will ask for restart, click **Restart Now**.



7. After restarting the computer, it will become **Client**.

Verification:

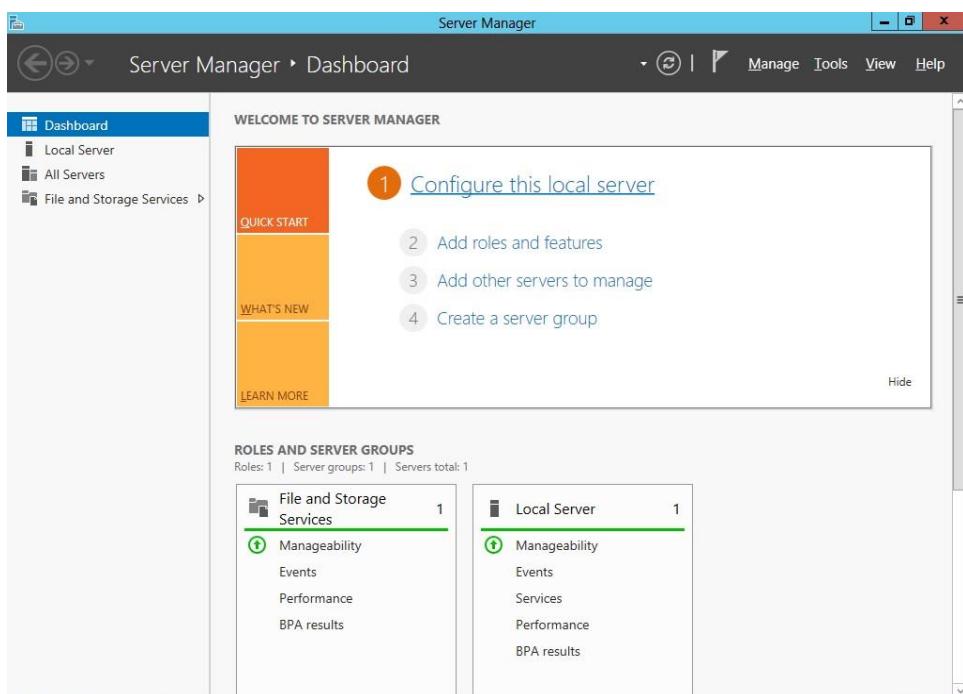
1. Right click **Computer Icon** → **Properties**.
2. Click Computer Name, domain, and workgroup settings and verify for the Domain Name**MICROSOFT.COM**.

Configuring Member server

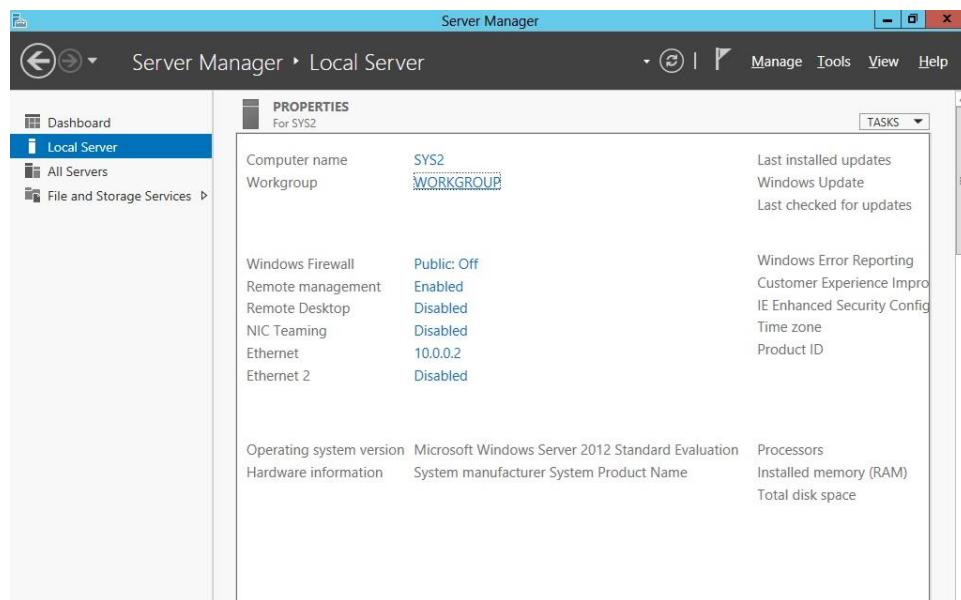
1. Log in as **Administrator** to **Workgroup Computer**.
2. Click **Server Manager**



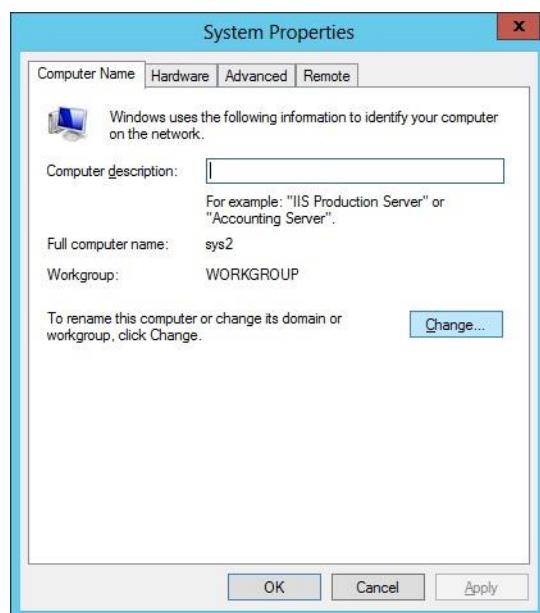
3. In Server Manager Dashboard, Click **Configure this local server**



4. In Local Server, select **WORKGROUP**.



5. In the System properties dialog box click **Change**.



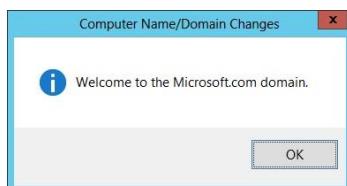
6. Select Member of **DOMAIN** and enter the Domain Name.(Ex:**Microsoft.com**)



7. Enter the user name **Administrator** and **Password**. Click **OK**.



8. Welcome Message appears indicating that the computer was successful in joining the Domain, click **OK**.



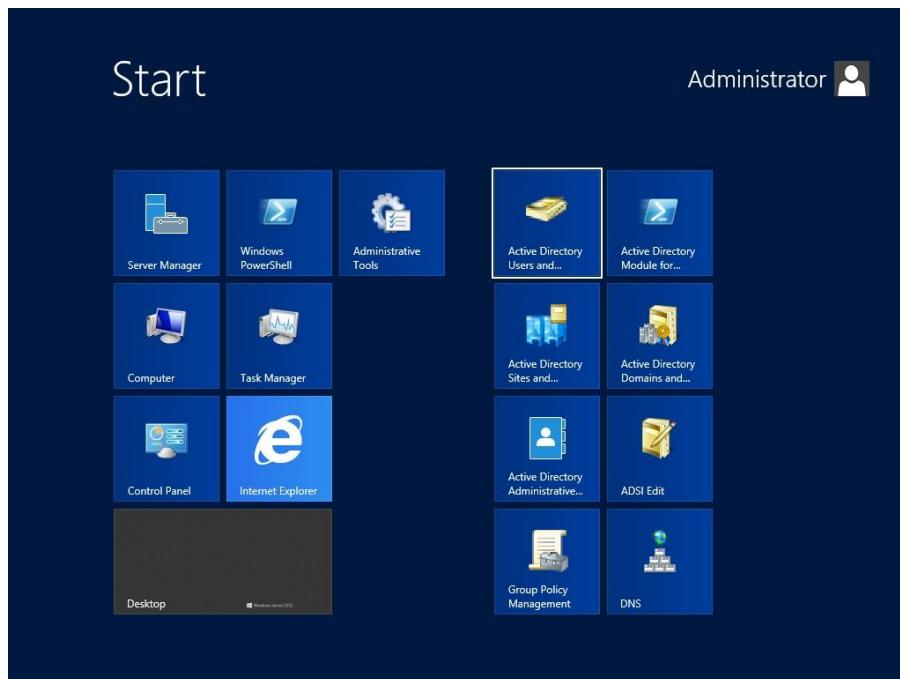
9. Click **OK** → click **OK**, and click **Close** to close the System Properties dialog box. It will ask for restart, click **Yes**.
10. After restarting the computer it will become **Member Server**.

Verification:

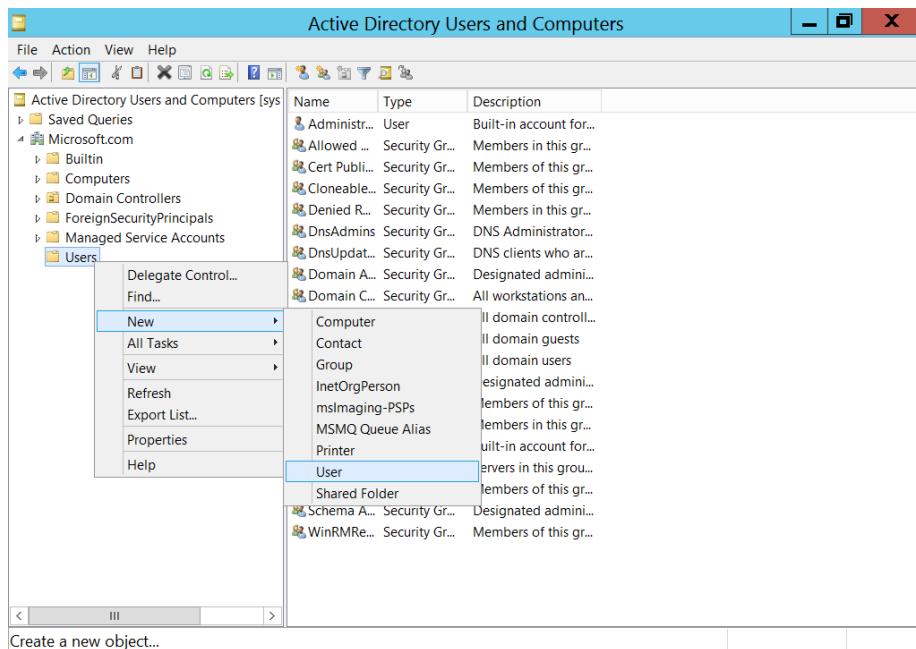
1. Go to Server Manager, select Local Server.
2. Verify for the Domain **MICROSOFT.COM**.

Lab – 2:Creating Domain User Accounts

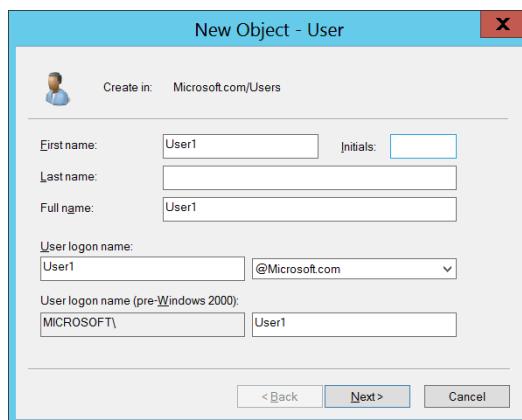
1. Log in as **Administrator** to the **Domain Controller**.
2. Press Windows Key to go to Start, select **Active Directory User and Computers**.



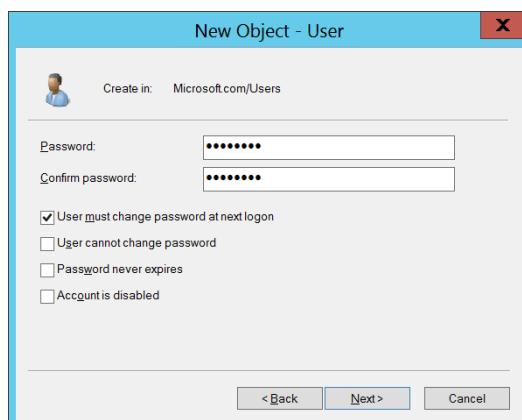
3. In the console tree, expand your domain **MICROSOFT.COM**, and then right click **Users Container**, select **New User**.



4. Specify the **First name** and **User Logon name** and then click **Next**.



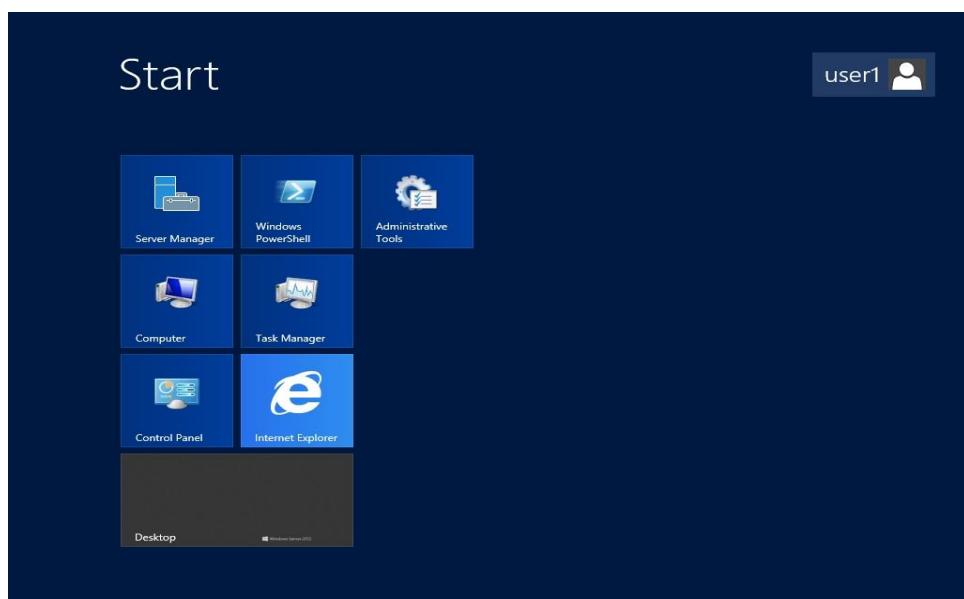
5. Enter the **Password** and **Confirm Password** for the User account, click **Next**.



6. Review the configuration settings for the User Account and then click **Finish**.

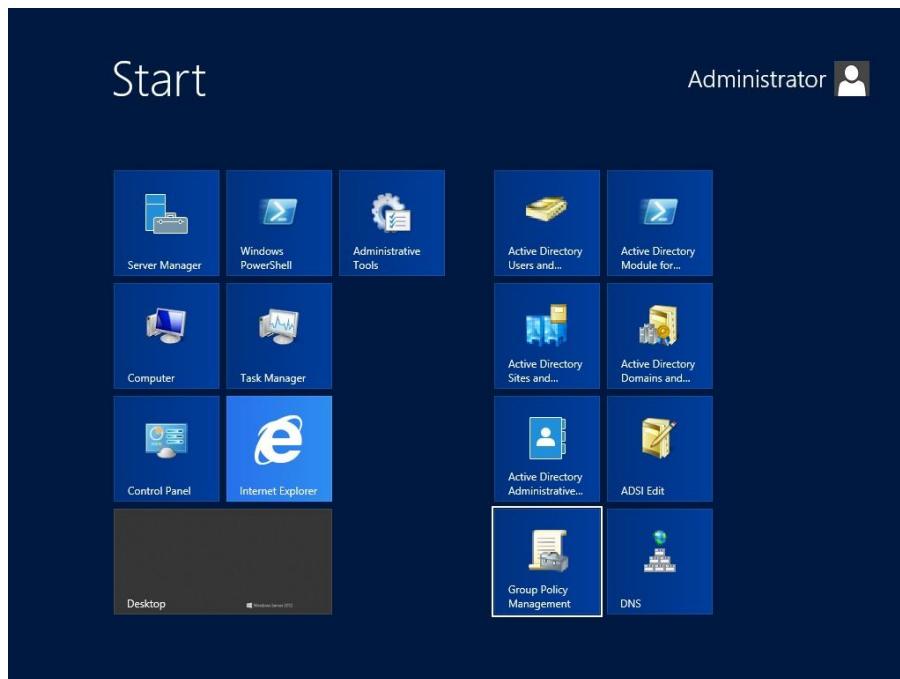
Verification:

1. Login as User (**User1@Microsoft.com**) in Member Server or Client.

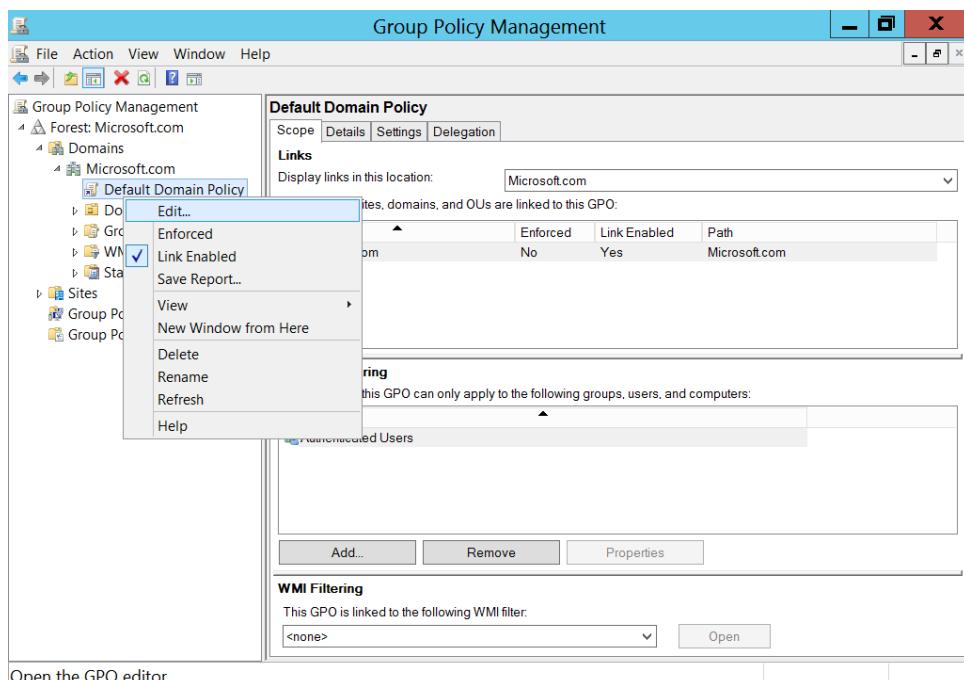


Lab – 3: Changing Default Password Policy

1. Log in as **Administrator** to the **Domain Controller**.
2. Press Windows Key to go to Start, select **Group Policy Management**.

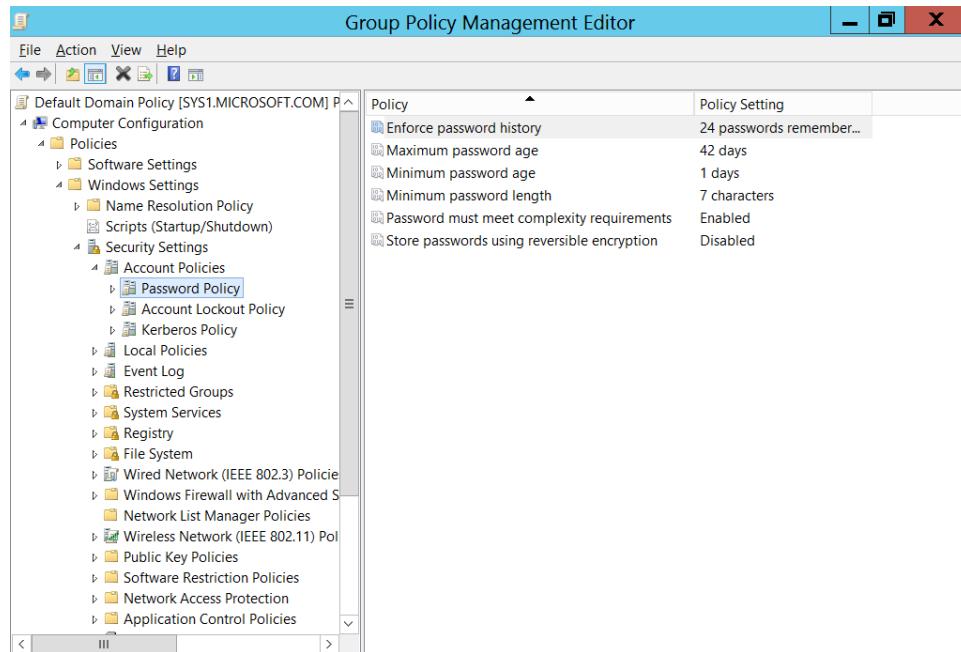


3. Expand Forest → Expand Domains → Expand Microsoft.com → right click **Default Domain policy** and select **Edit**.

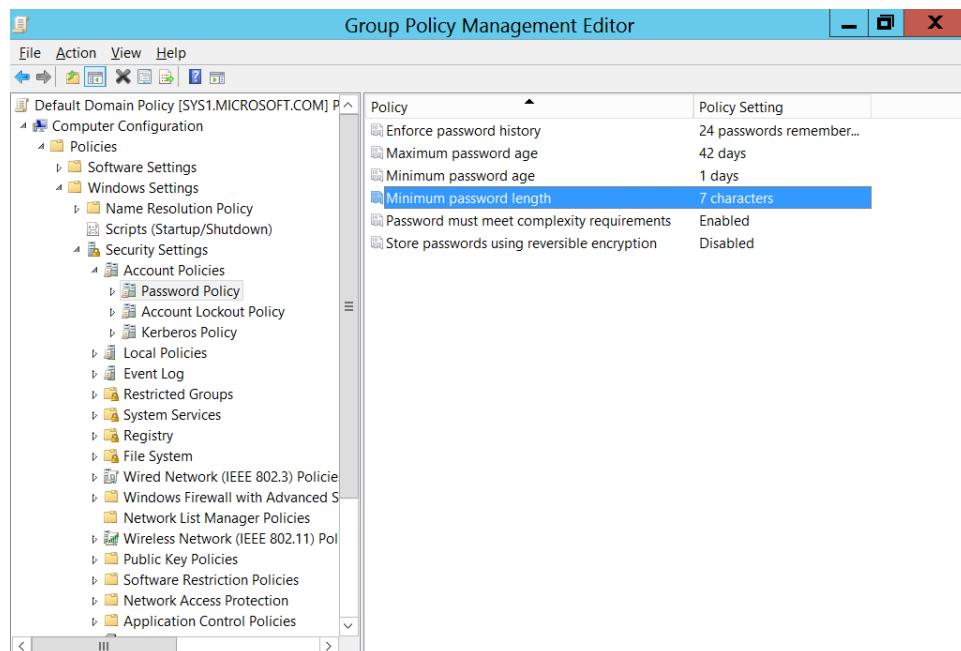


Open the GPO editor

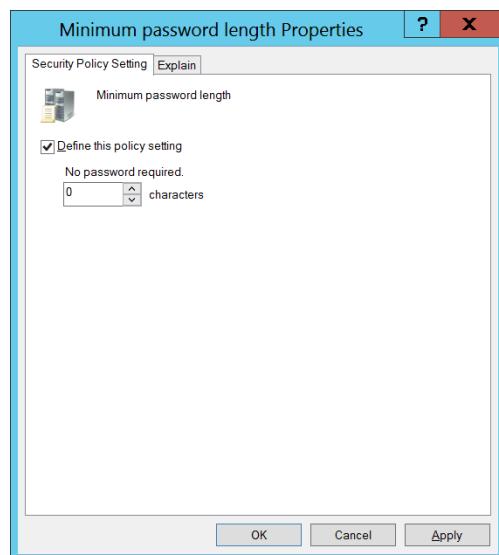
- 4. Expand Computer Configuration → Expand Policies → Expand Windows Settings
→ Expand Security Settings → Expand Account Policies → Open Password Policy.**



- 5. Double click Minimum Password Length.**



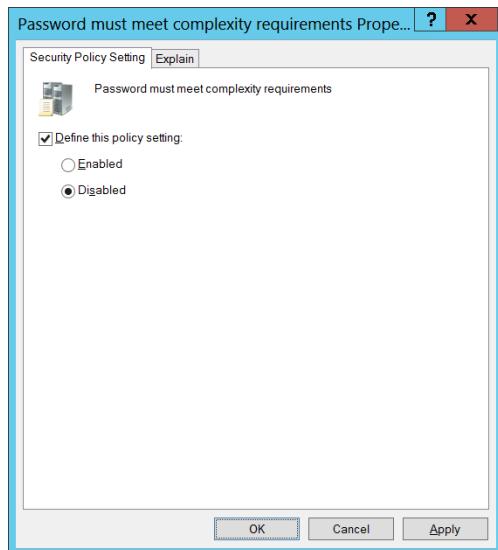
6. Change the length value from **(7 to 0)** and click **Apply** and **OK**.



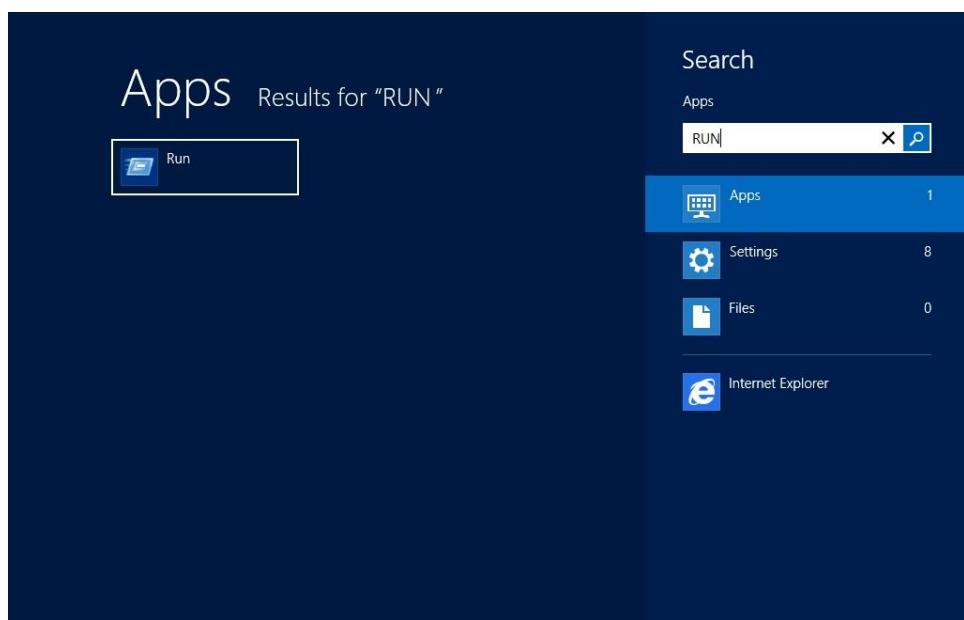
7. Double click **Password must meet complexity Requirements**.

Policy	Policy Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

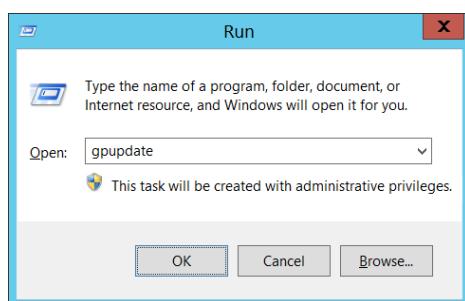
8. Select Disabled and Apply and OK.



9. Go to Start, type Run in Search Apps, and select Run



10. Type GPUPDATE and It refreshes the policy changes.

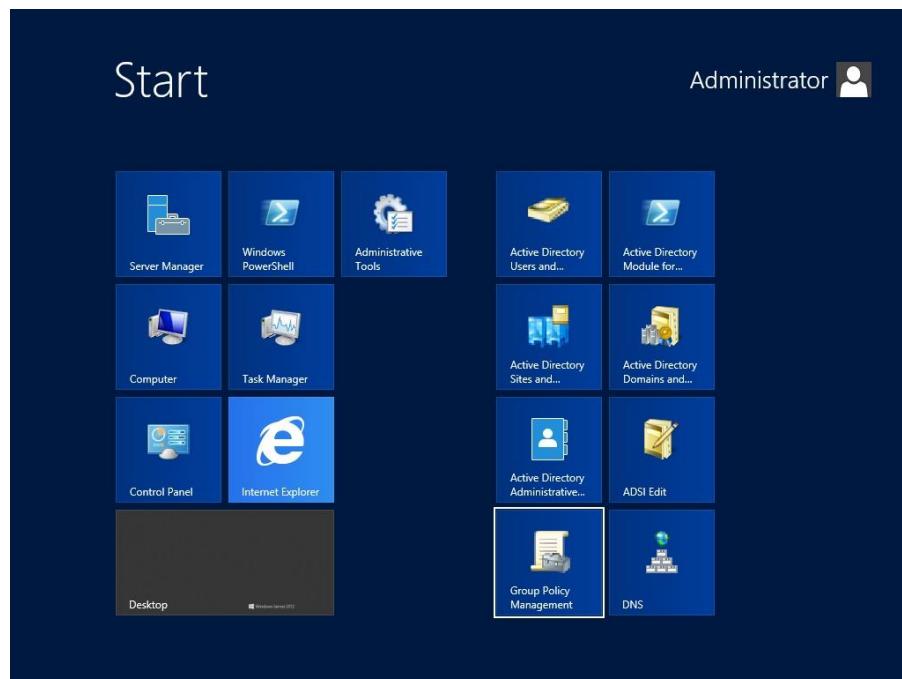


Verification:

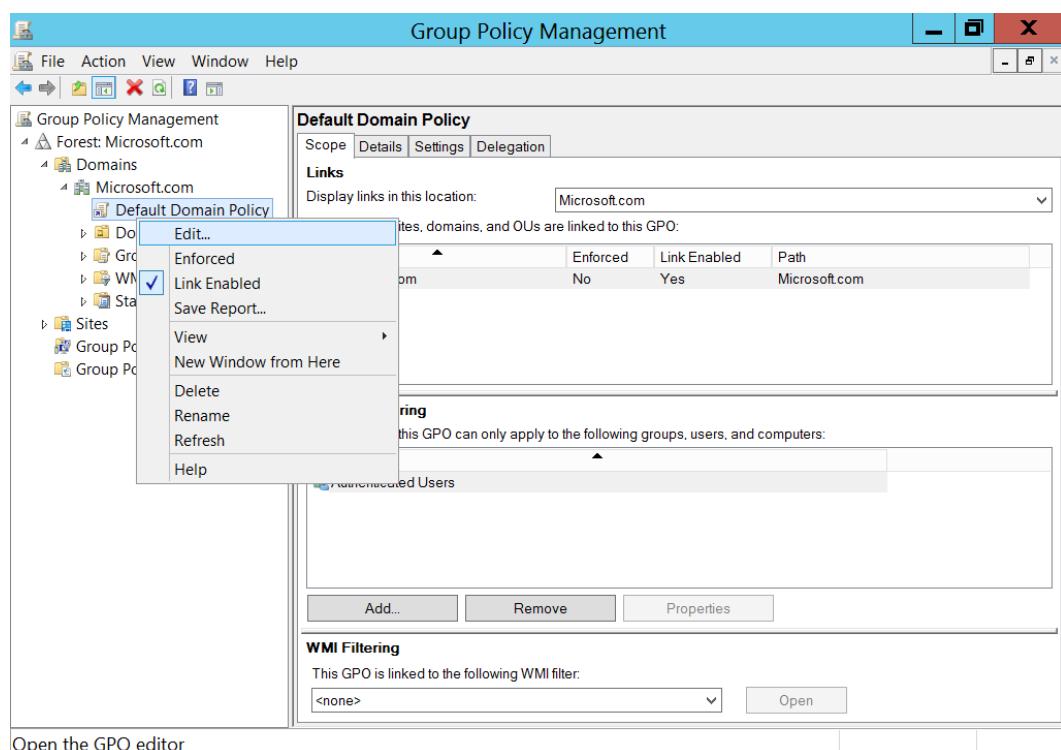
1. Go to **Active Directory Users and Computers** and Create a User **with any Password or without any Password.**

Lab – 4: Enabling Account Lockout policy

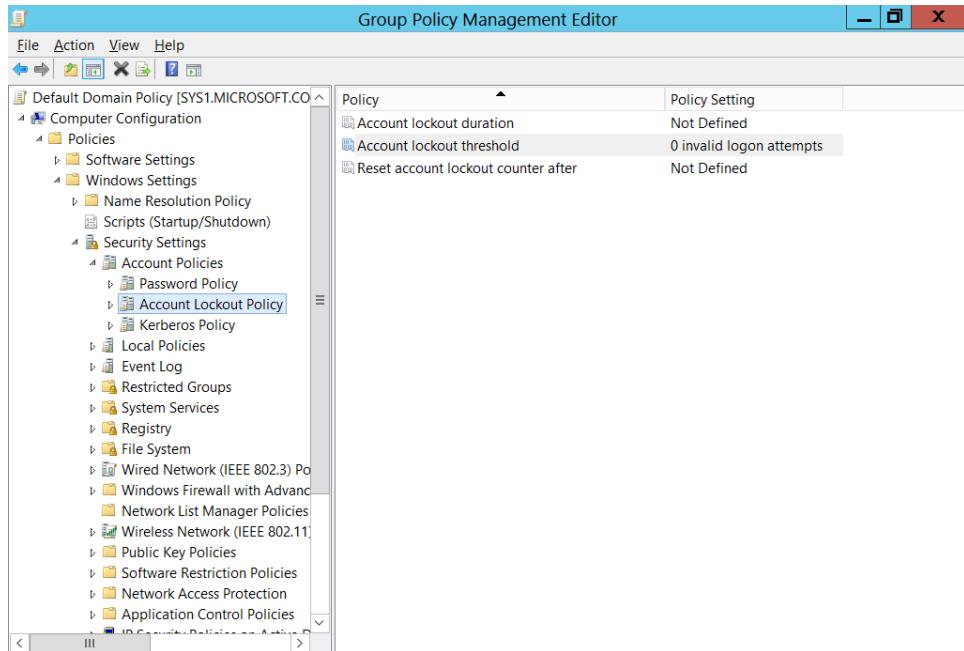
1. Log on to D.C as Administrator, click Press Windows Key to go to Start, select **Group Policy Management**.



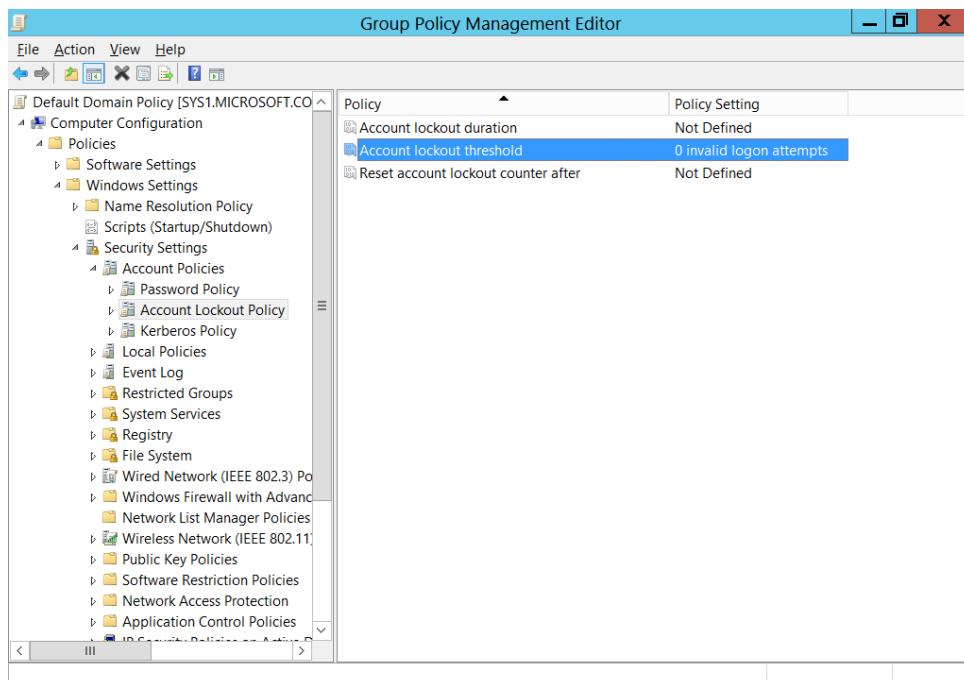
2. Expand **Forest** → **Expand Domains** → **Expand Microsoft.com** → right click **Default Domain policy** and select **Edit**.



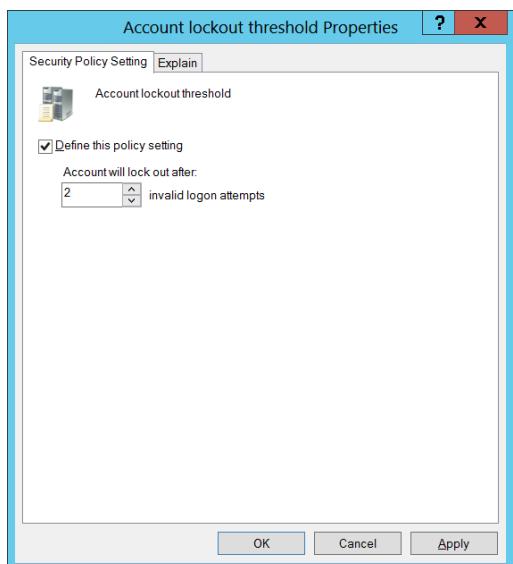
3. Expand **Computer Configuration** → Expand **Policies** → Expand **Windows Settings** → Expand **Security Settings** → Expand **Account Policies** → Open **Account Lockout Policy**.



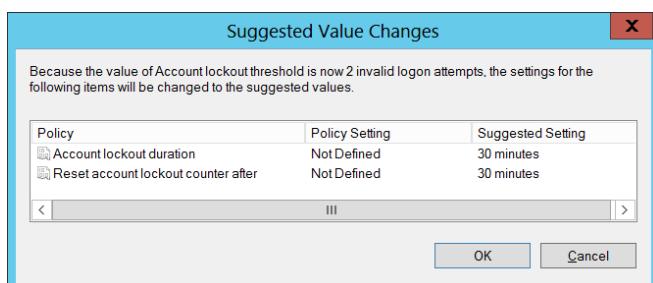
4. Double click, **Account lockout threshold**.



5. Enter the Value for Number of **invalid logon attempts**(Ex: 2)



6. Set the **Account lockout duration** and click**OK**.



7. Close the **Group Policy Management** Window.

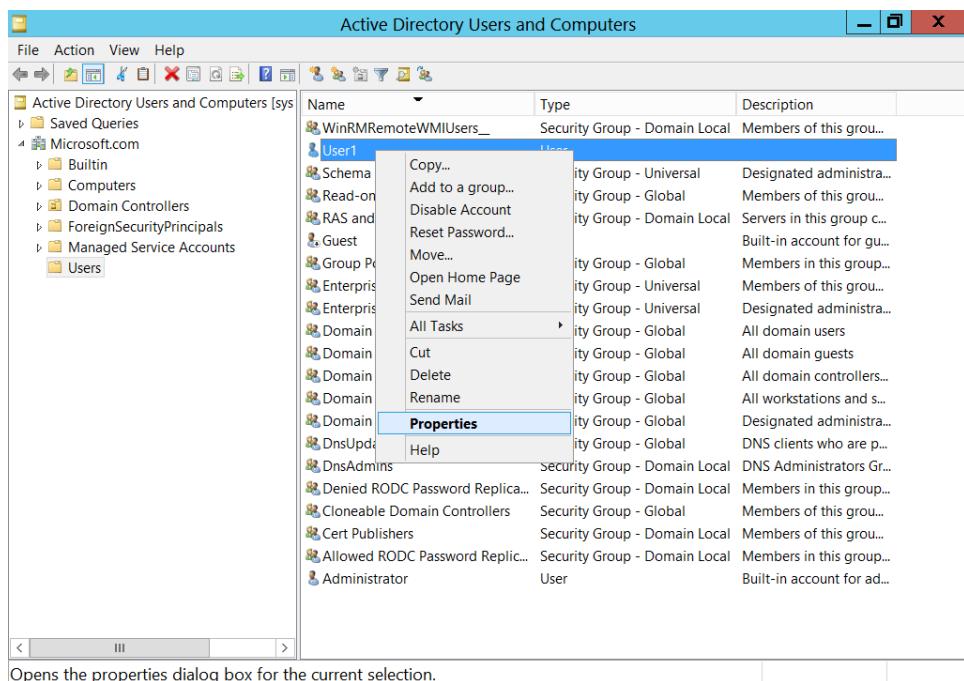
Verification:

1. Enter the password for **user (User1)** wrongly for 2 times while logging in and the user account will be locked.

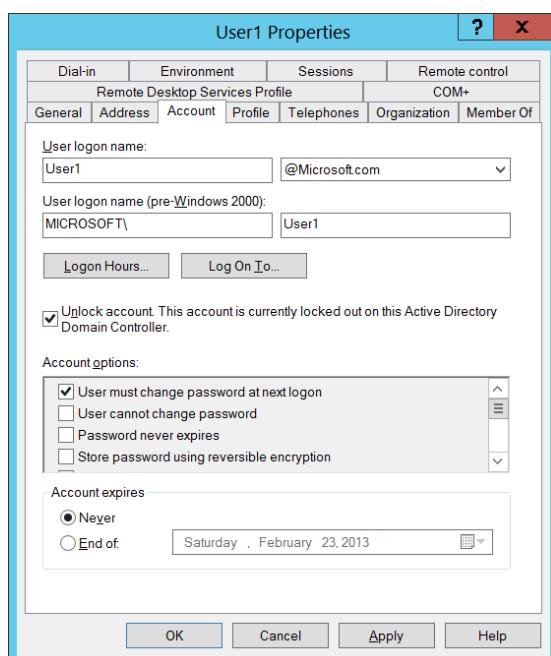
Unlocking the locked User account Manually

1. Log on to D.C as Administrator, click Start → Programs → Administrative Tools → **Active Directory Users and Computers**.

2. Right click the User (User1**) and select **Properties**.**



3. Check the box **Unlock account → click **Apply** and **OK**.**

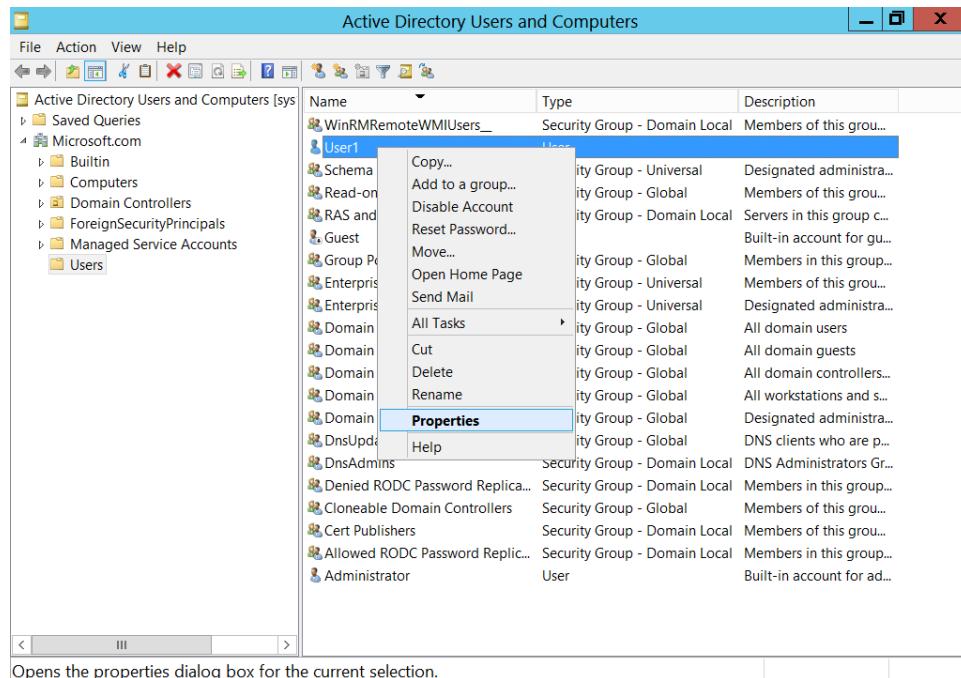


Verification:

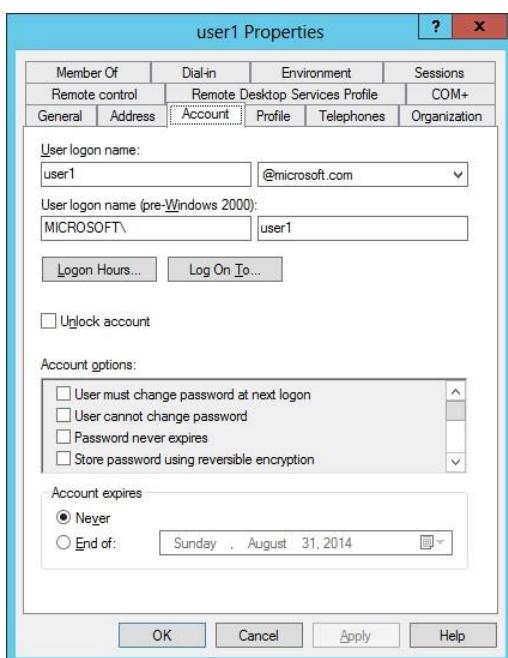
1. Log in as User (User1**) in client or Member Server.**

Lab – 5: Configuring Logon to and Logon hours permissions

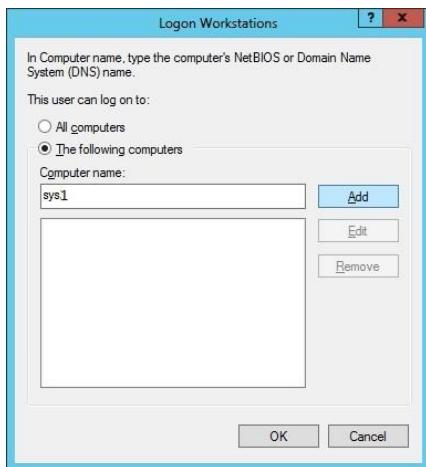
1. Log on to D.C as Administrator, click Start → Programs → Administrative Tools
→ Active Directory Users and Computers.
2. Right click the User (**User1**) and select **Properties**.



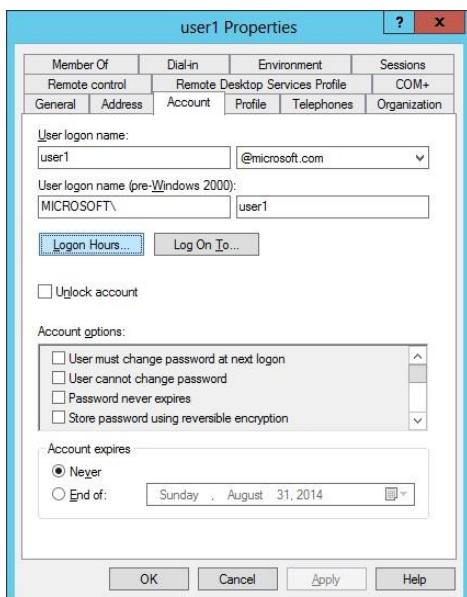
3. Select Account, click Log On To.



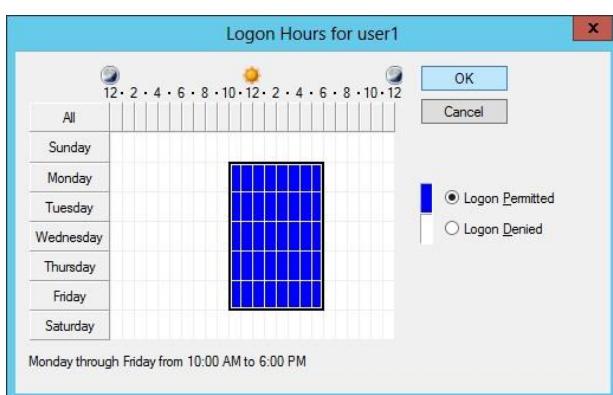
4. Select the following computers, Enter computer name (Ex: sys1), click Add and OK.



5. Click **Logon Hours**



6. Select the timing and select **Logon Permitted**.

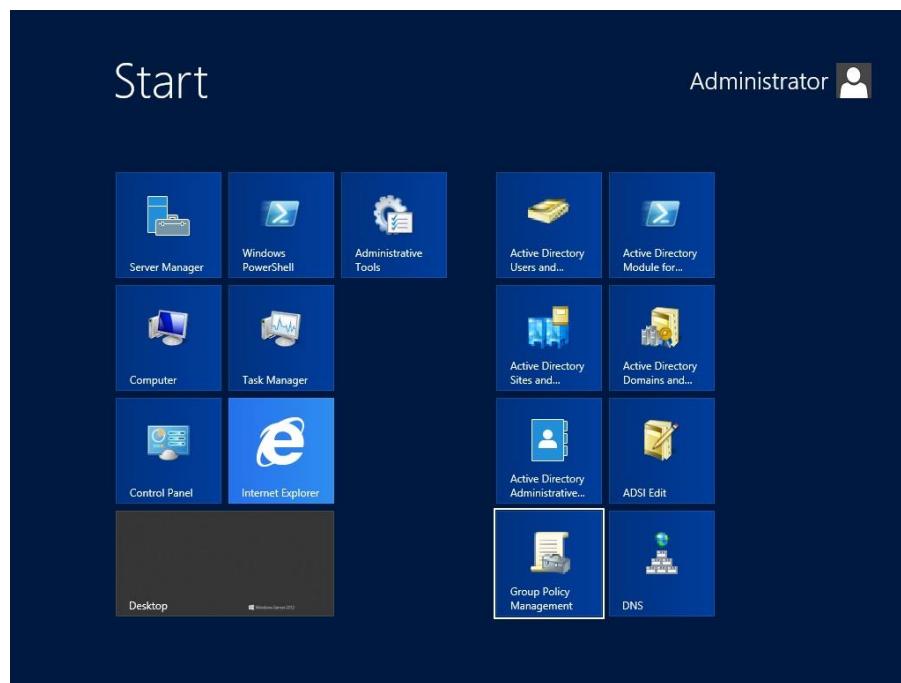


Verification:

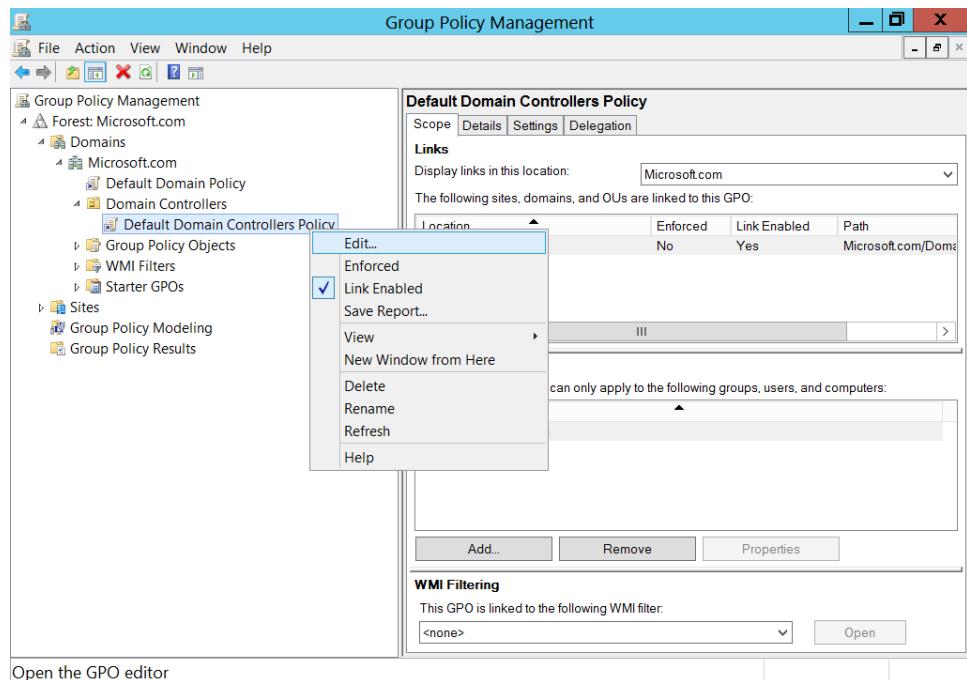
1. Try to Log in as User (**User1**) in client or Member server **sys2**

Lab – 6: Changing Allow Logon Locally Policy

1. Log in as **Administrator** to the **Domain Controller**, click Press Windows Key to go to Start, select **Group Policy Management**.

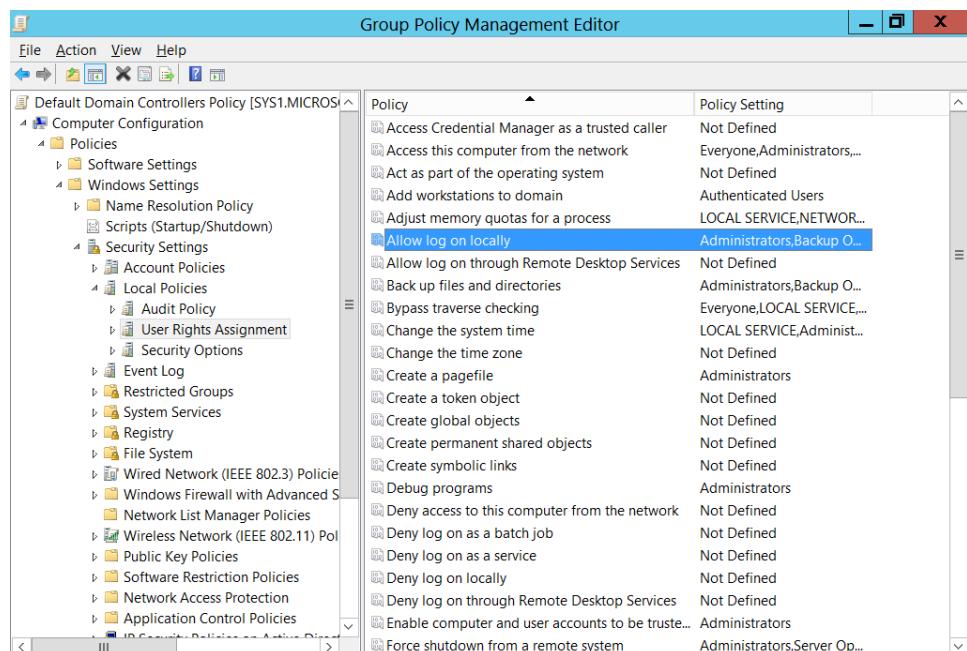


2. Expand **Forest** → **Expand Domains** → **Expand Microsoft.com** → **Expand Domain Controllers** → Right click **Default Domain Controller Policy** and select **Edit**.

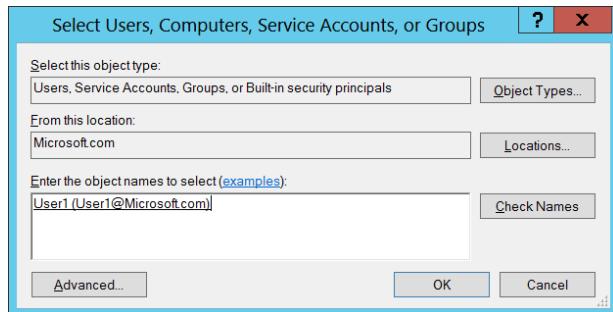


Open the GPO editor

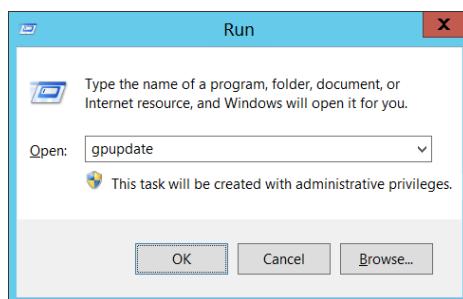
3. Expand **Computer Configuration** → Expand **Policies** → Expand **Windows Settings** → Expand **Security Settings** → Expand **Local Policies** → Select **User Rights Assignment** → Double click **Allow logon locally**.



4. Click **Add User or Group** → Click **Browse** → Enter the **Username** → Click **OK**.



5. Click **OK** → **OK** → **Apply** and **OK**.
6. Go to Start, type Run Type Control Panel in Search Apps, and select **Run**, type **GPUPDATE** and it refreshes the policy changes.



Verification:

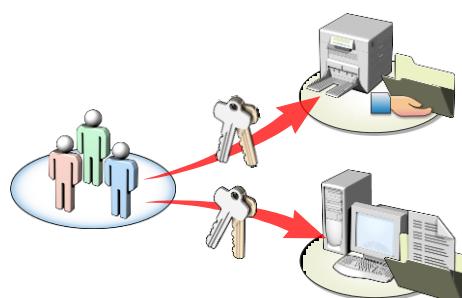
1. Log on to Domain Controller as **Domain User (User1)**.

PERMISSIONS

What are Permissions?

- Permissions define the type of access granted to a user, group, or computer to access resources.
- Permissions can be applied to resources such as files, folders, and printers.
 - Like: Privilege to read a file, delete a file, or to create a new file in folder.

What are Permissions?



Types of Permissions

- Security Level Permissions
- Share Level Permissions

Security Level Permissions

- Can be Implemented Only on NTFS partitions.
- Security or NTFS Permissions can be set on Drives, Folders and Files.
- By default, Security permissions will be inherited from its parent drive or folder.
- File permissions override folder permissions.
- Creators of files and folders are their owners.
- Different Security Permissions are
 - Full Control, Modify, Read & Execute, Write, Read, List Folder Contents.

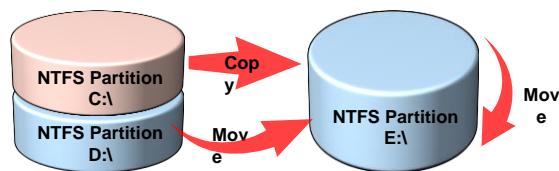
Share Level Permissions

- It can be implemented on NTFS and FAT partitions.
- It can be set on Drives and Shared Folders but not files.
- What are shared folders?
 - Shared folders can be accessed from network.
 - When you copy or move a shared folder, the folder will no longer be shared.
 - To hide a shared folder, include a \$ after the name of the shared folder & users access hidden shared folders by typing the UNC path.
- Different Share Permissions are
 - Read, Read/Write.

Effects on NTFS Permissions when Copying or moving files and folders

- When you copy files and folders within the same partition or different partition they inherit the permissions of the destination folder.
- When you move files and folders to a different partition, they inherit the permissions of the destination folder
- When you move files and folders within the same partition, they retain their previous permissions.

Effects on NTFS Permissions when Copying or moving files and folders



Access Based Enumeration (ABE)

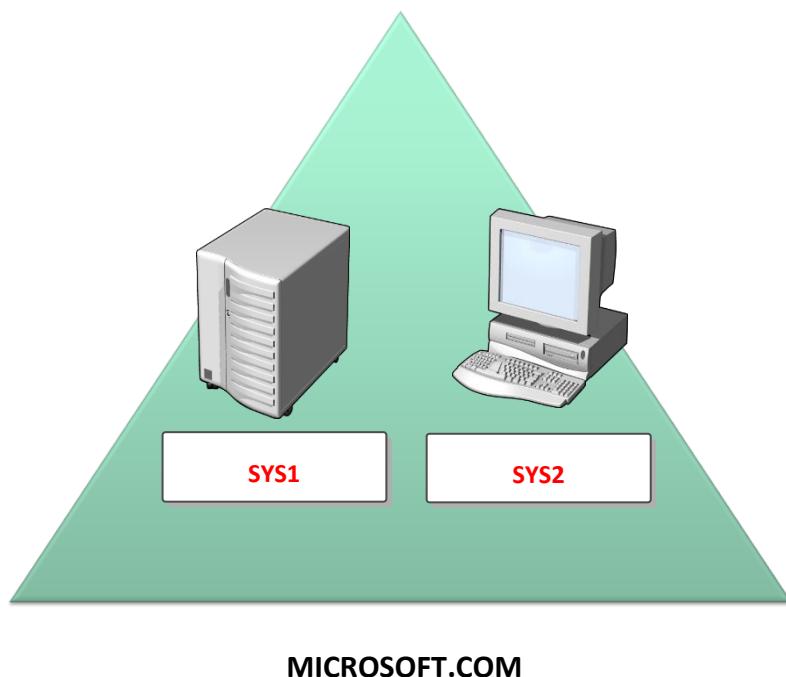
- Access Based Enumeration displays only the files and folders that a user has permissions to access.
- If a user does not have read permissions for a folder, windows hides the folder from the users view.

PERMISSIONS

Pre-requisites:

Before working on this lab, you must have

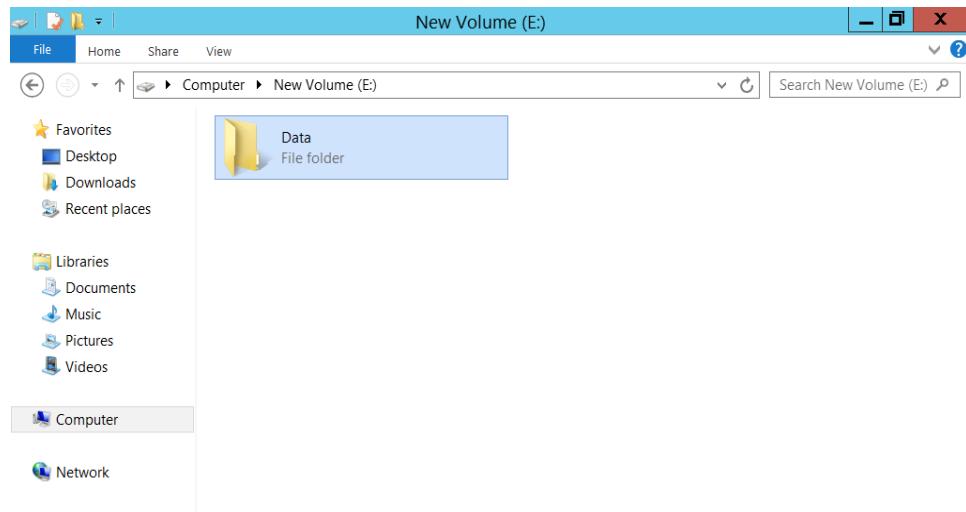
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server or windows 7.



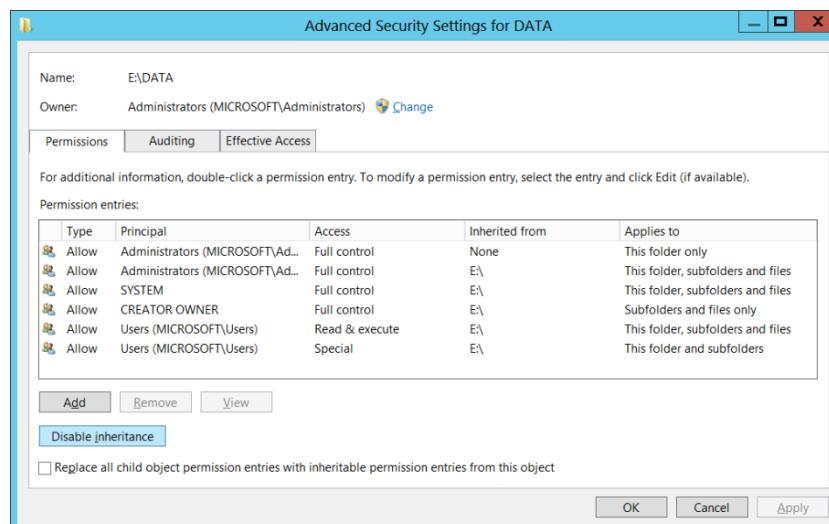
SYS1		SYS2	
Domain Controller		Member Server / Client	
IP Address	10.0.0.1	IP Address	10.0.0.2
Subnet Mask	255.0.0.0	Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1	Preferred DNS	10.0.0.1

Lab – 1: Security Level Permissions

1. Open Computer → Go to any NTFS partition and create a folder (**DATA**), along with some files in it.



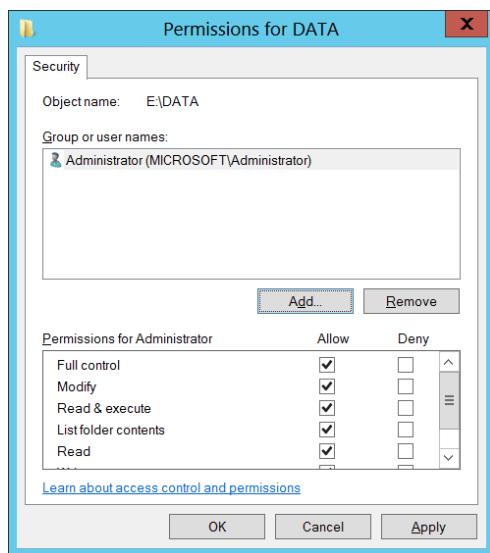
2. Right click the folder (**DATA**) and select properties and click **Security tab** → click **Advanced tab** → click **Edit** → click **Disable inheritance**.



3. Click **Remove** → **Apply** → **OK** → **OK**

4. Click **Edit**

5. Add **Administrator** or **Administrators** and allow **Full control** permission.

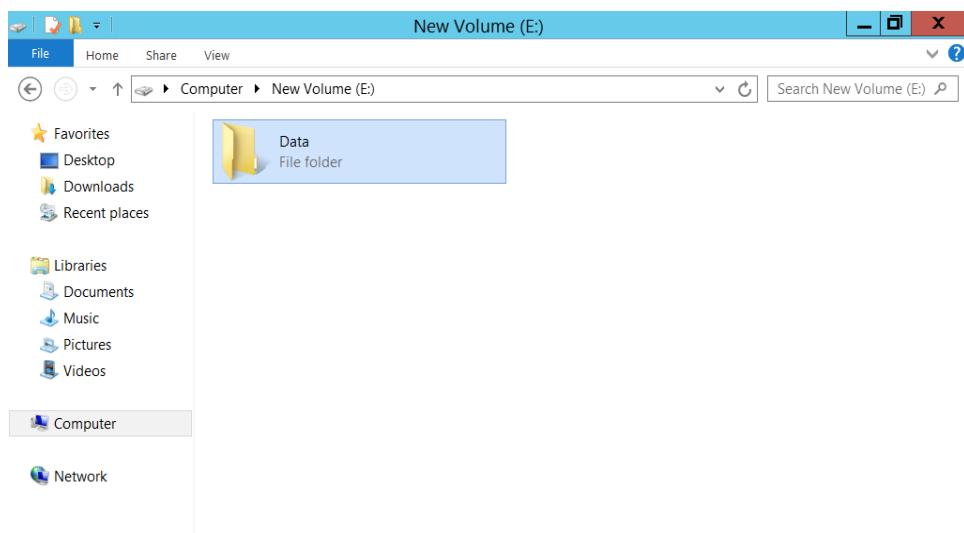


6. Then Add the **Users (User1)** and Allow **Read** permission.

7. Click **Apply → OK → OK**

Verification:

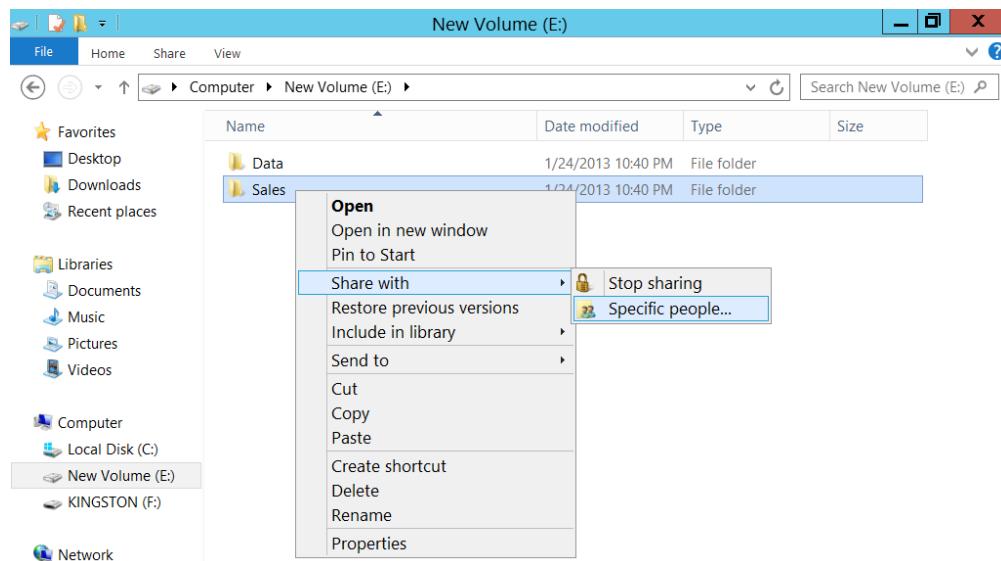
1. Login as User(**User1**) on the same computer, and Open Computer icon, and verify the respective permissions by accessing the folder.



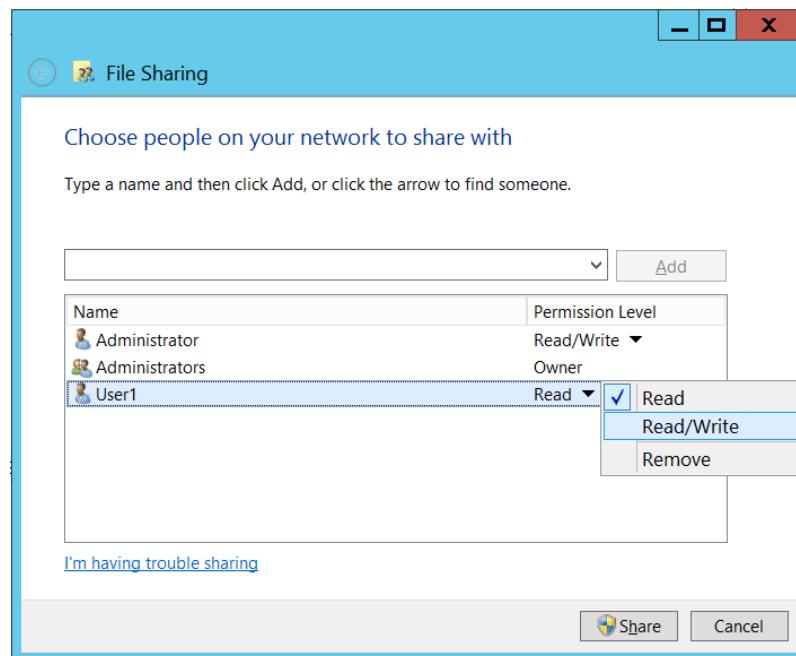
2. The User can just read the Files and Folders.

Lab – 2: Share Level Permissions

1. Logon to a Computer as **Administrator**, Open **Computer** → Open any drive and create a folder (**SALES**) along with some files in it.
2. Right click the folder (**SALES**) and Select **Share**



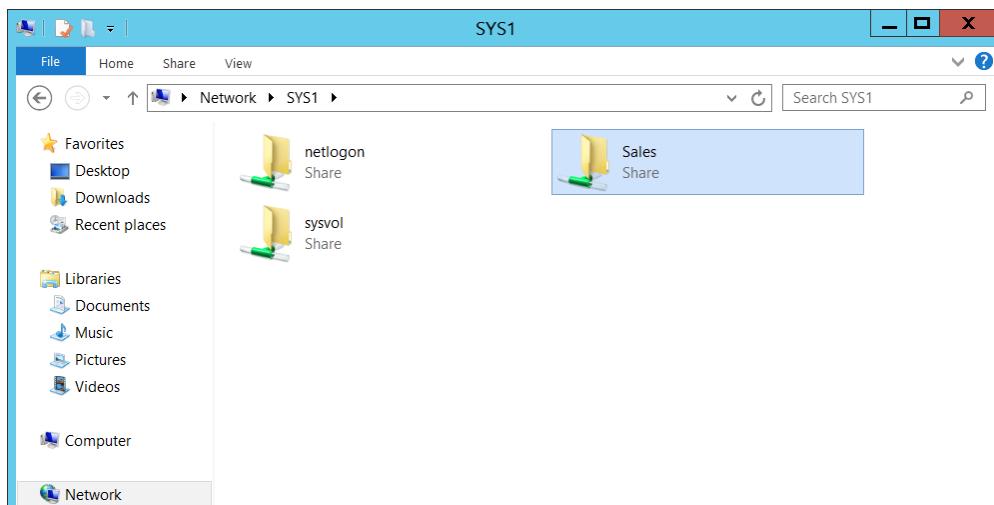
3. Select the drop down arrow mark and select **Find** → enter the User name (**User1**) → click **OK** → select the User(**User1**) and assign Permissions (Ex: **Read/Write**) → click **Share** → click **Done**.



Verification:

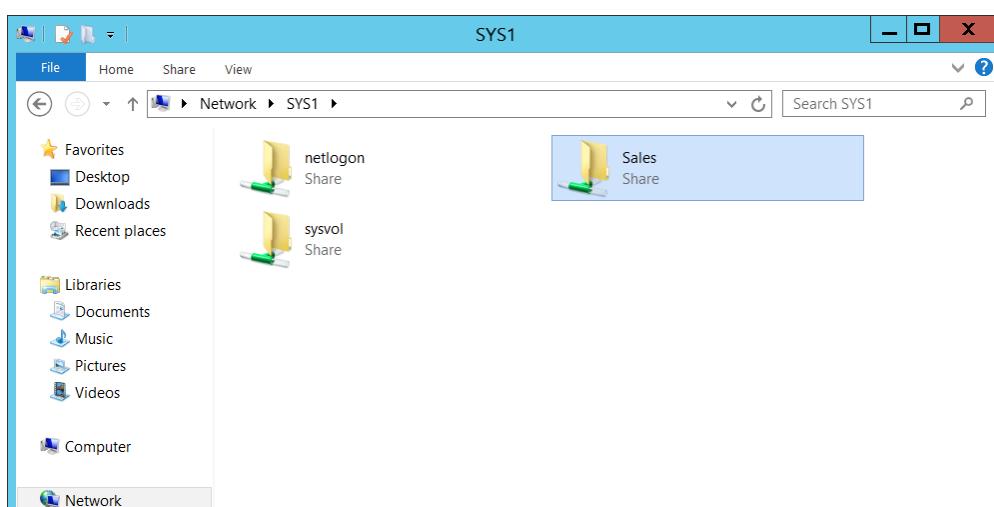
Access the Shared folder

1. Logon to Member Server or Client as User (**User1**) → Open Network.
2. Open **System Name** in which the shared folder is present.
3. Access the shared folder (**SALES**) & verify the permissions by creating some files.



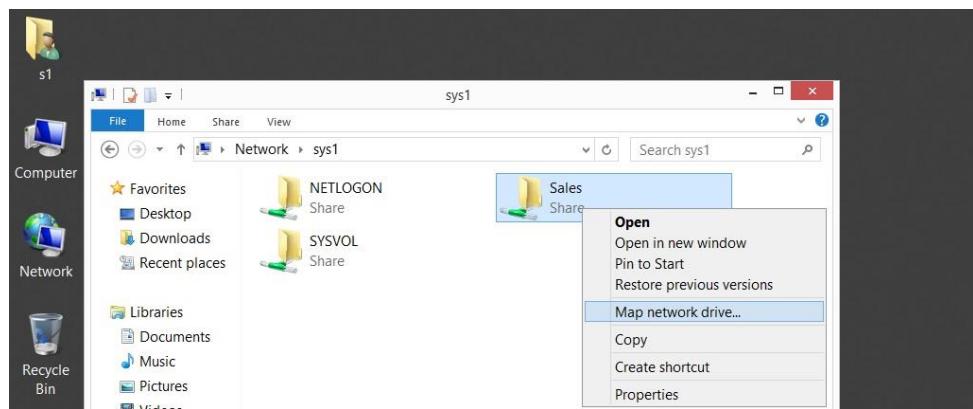
Accessing Shared folders using UNC Path:

1. Logon to Member server or Client as a User.
2. Click Start → click Run and type the Syntax **\Servername\Sharename**. Example:
\\SYS1\\SALES

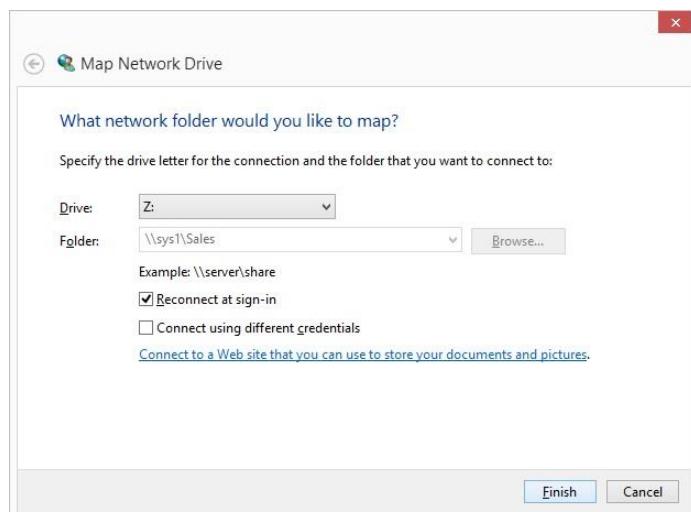


Lab – 3: Adding Mapped Drives

1. Logon to Member server or Client as a User.
2. Access the shared folder Sales, Right click on sales folder, select **Map network drive**.

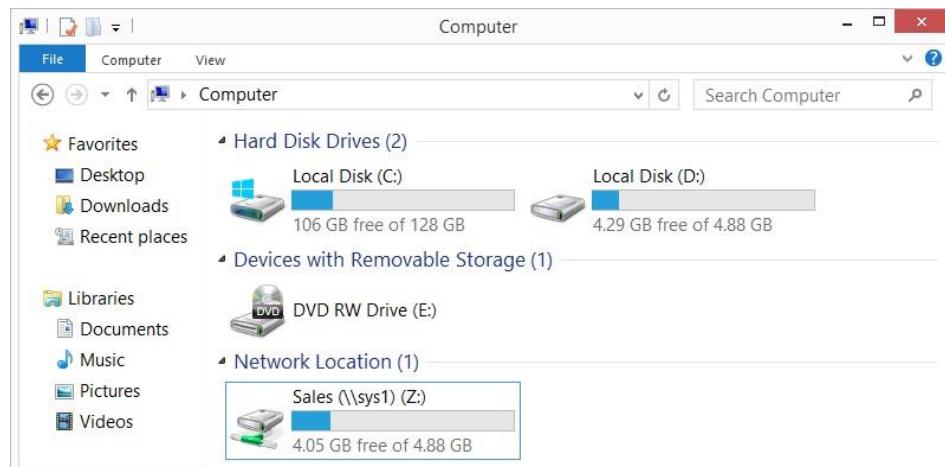


3. Select the Drive letter (Ex: Z:) and click **Finish**.



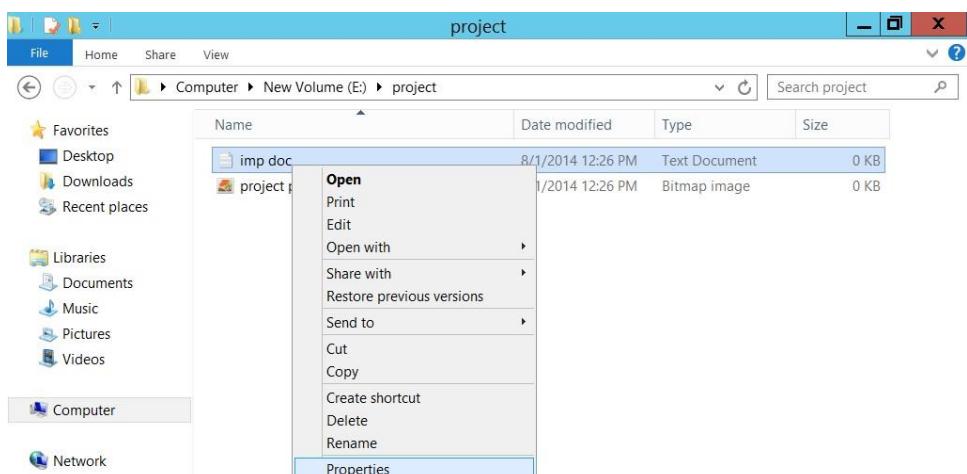
Verification:

1. Open Computer Icon and verify for Mapped network Drive

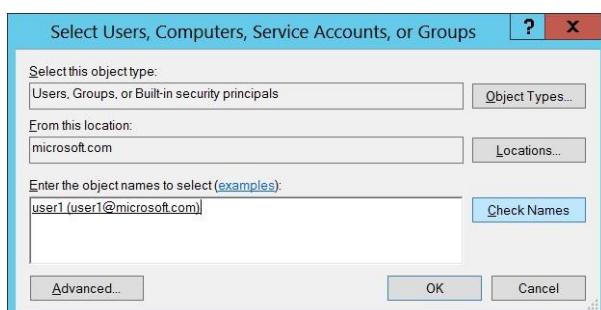


Lab – 4: Verifying Access Based Enumeration

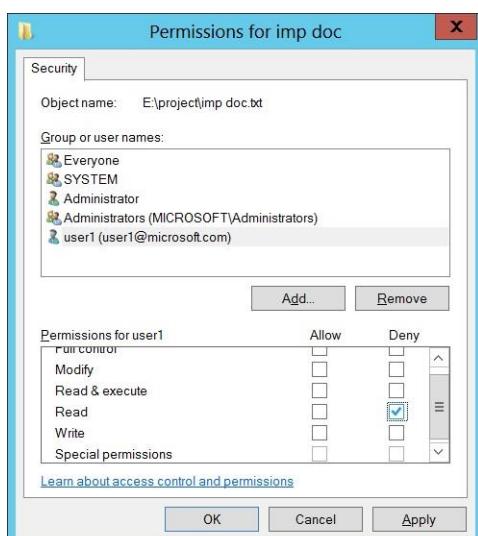
1. Logon to a Sys1 as **Administrator**, Open Computer → Open any drive and create a shared folder (**Ex: Project**) with everyone Read/Write permissions along with some files in it.
2. Right click on one of the file and select **Properties**



3. Select Security, click Edit and Add, Enter user1, click OK

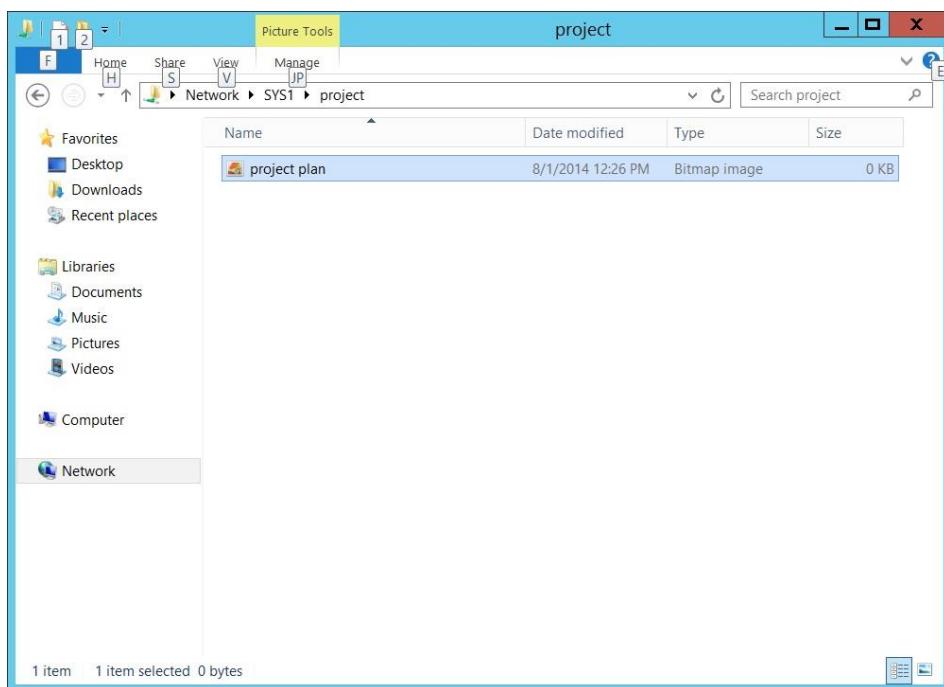


4. Select **user1** and set the permission Deny Read, click OK.



Verification:

1. Logon to Member Server or Client as User (**User1**).
2. Open **Network Icon**, Select SYS1, access the shared folder Project and verify for the files present.



PROFILES

Profiles

- **Profile is a User-State Environment.**
- **Profile contains Personal Settings of the User like**
 - Documents
 - Desktop Settings
 - Start Menu Icons
 - Shortcuts
 - Application Data
 - Downloads
 - Pictures, Music, Videos
 - Contacts
 - Favorites, etc

Types of Profiles

- **Local Profile**
- **Roaming Profile**

Local Profile

- A local user profile is created the first time you log on to a computer and is stored on a computer's local hard disk.
- Any changes made to your local user profile are specific to the computer on which you made the changes.

Location of Local Profile

- In 2012, 2008, Windows 8, Windows 7, Windows Vista is C:\Users
- In 2003, 2000, NT, XP, 2000 Professional is C:\Documents & Settings.

Roaming Profile

- A roaming user profile is created by your system administrator and is stored on a server.
- This profile is available every time you log on to any computer on the network.
- Changes made to your roaming user profile are updated on the server.

Home Folder

- Home Folder is a centralized location of the users files (data)
- Home Folder make it easier for an administrator to back up user files by collecting all user's files in one location
- Whenever the user logs on to any computer in a domain, Home Folder will be available in the form of Network Drive / Network Location.

File Server Resource Management

What Is FSRM?

- FSRM is intended to act as a capacity management solution for your Windows Server 2012 server.
- It provides a robust set of tools and capabilities that allow you to effectively manage and monitor your server's storage capacity.
- FSRM contains five components that work together to provide a capacity management solution

FSRM Functionality

- Storage quota management
- File screening management
- Storage reports management

What Is Quota Management?

- Quota management is a component that allows you to create, manage, and obtain information about quotas that are used to set storage limits on volumes or folders (and its contents).
- By defining notification thresholds, you can send email notifications, log an event, run a command or script, or generate reports when users approach or exceed a quota.
- Quota management also allows you to create and manage quota templates to simplify the quota management process.

Quota Management

- Quota management is used to limit disk space usage and provides notifications when thresholds are reached.
- Quota notifications can do any of the following:
 - Send email notifications
 - Log an event in Event Viewer
 - Run a command or script
 - Generate storage reports

File Screening Management

- File screen management provides a method for controlling the types of files that can be saved on file servers.
- When users attempt to save unauthorized files, file screening can block the process and notify the administrators to allow for proactive management.

Storage Reports

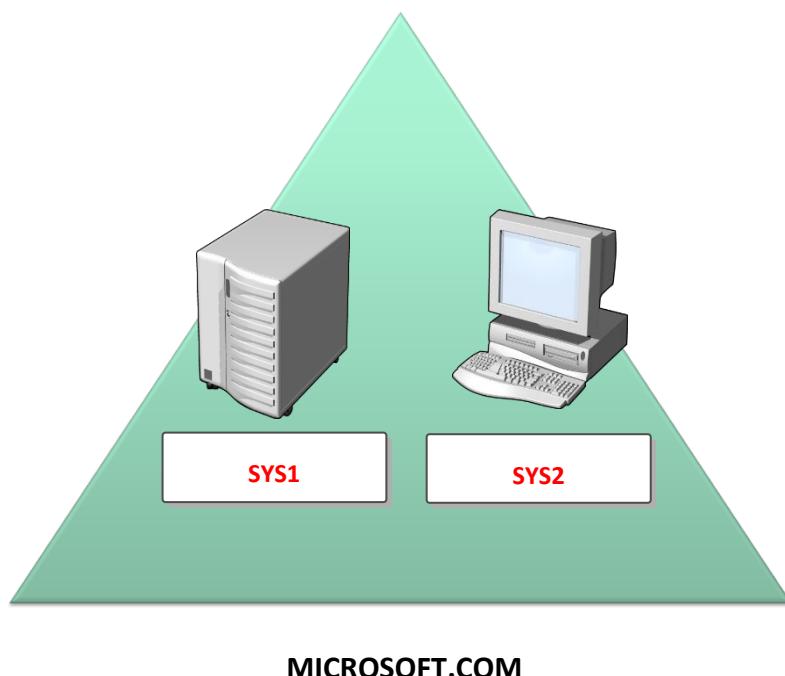
- Storage reports management is a component that allows you to schedule and configure storage reports about file usage on a file server.
- These reports provide information regarding following :
 - Quota usage.
 - File screening activity.
 - Files that may negatively affect capacity management, such as large files, duplicate files, or unused files.
 - List and filter files according to owner, file group, or a specific file property

PROFILES&FILE SERVER RESOURCE MANAGER

Pre-requisites:

Before working on this lab, you must have

1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server or windows 7.



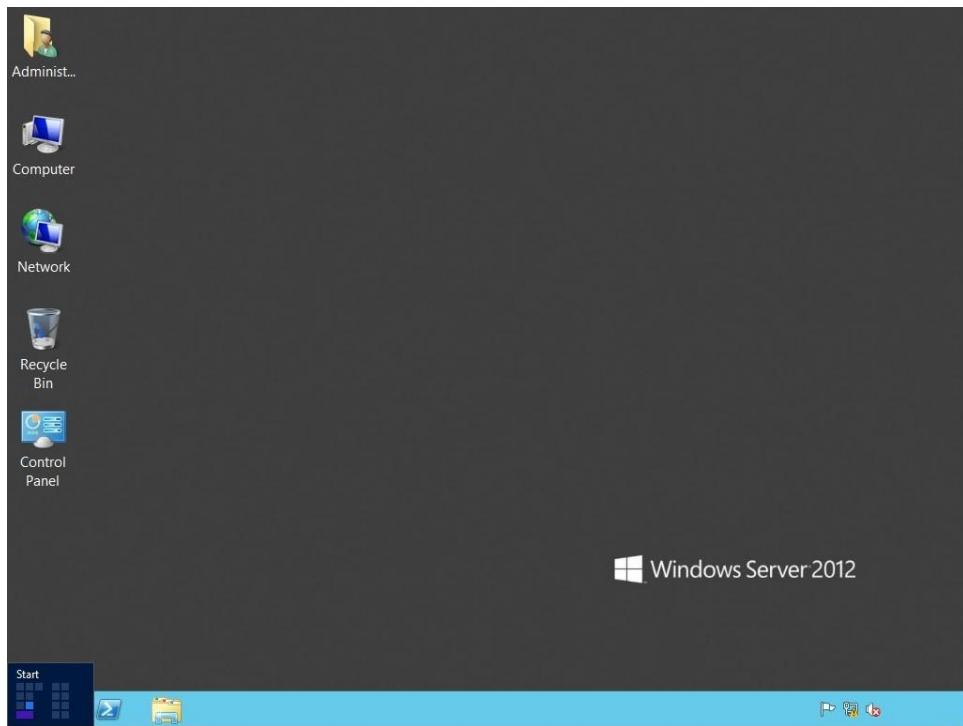
SYS1	SYS2
Domain Controller	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Member Server / Client	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1

Lab – 1: Configuring Local Profiles

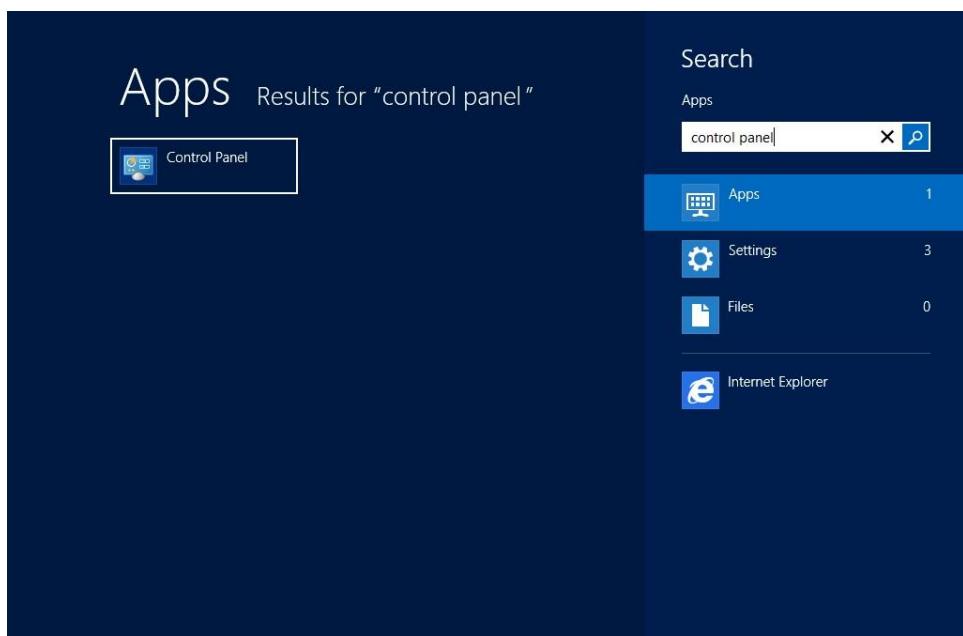
1. Log on to **Domain Controller** as **Administrator**.
2. Go to **Active Directory Users and Computers** and create **Users** (Ex: user1, user2).

Verification:

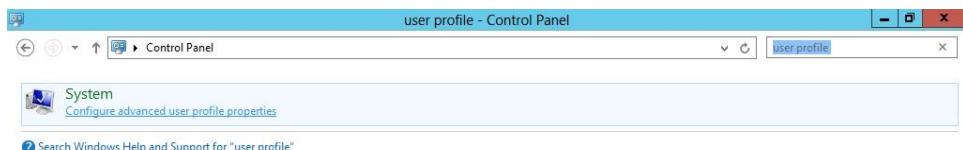
1. Login as **User (user1)** on **Client or Member Server**.
2. Press Windows key to go Start,



3. Type Control Panel in Search Apps, and select **Control Panel**.



4. In Control Panel search bar, type **user profile**, select **Configure advanced user profile properties**.



5. Verify for User Profile Type and Status to be Local.



6. Create some files on desktop and go to C: drive → Open Users → Open the user profile(user1) folder → open desktop folder → verify for the files created on Desktop.

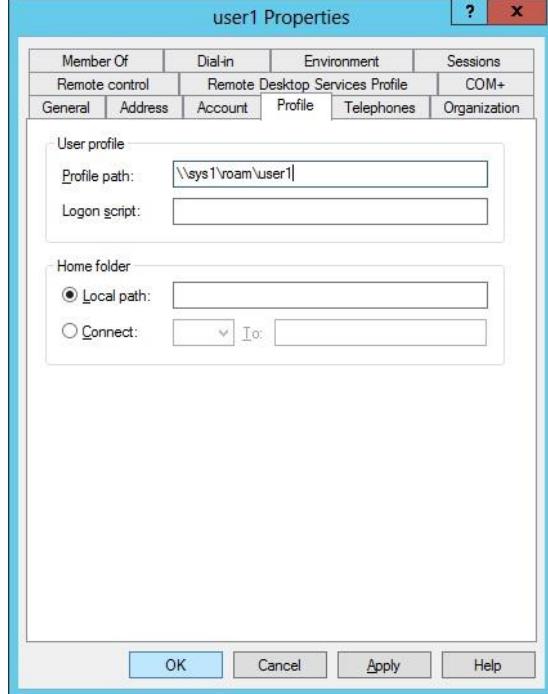
Lab – 2: Configuring Roaming Profiles

1. Log on to D.C as Administrator, Open **Computer** → Go to a drive and create a shared folder **roam** with **Everyone Read/Write** permission.

2. Go to Active Directory Users and Computers → Expand the Domain Name (MICROSOFT.COM) → click Users → Right click the User(user1) and select Properties and select the Profile tab.
3. Under User profile → enter profile path as

Syntax: \\Servername\Shared Folder Name\User Name

Example: \\SYS1\roam\user1.



4. Click Apply and OK.

Verification:

1. login as useruser1 on Client or Member Server and create some files on the Desktop.

2. In Control Panel search bar, type **user profile**, select **Configure advanced user profile properties**.



3. Verify for User Profile Type and Status to be Roaming.

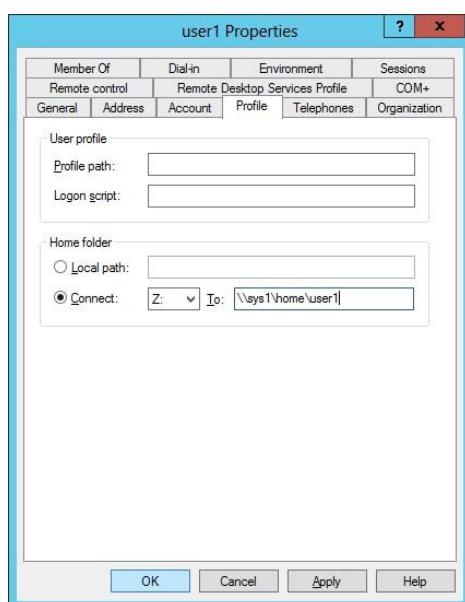


4. Logoff this user (**user1**) and login on another computer with the same user (**user1**), we can see the files which we have created on first computer.

Lab – 3: Configuring Home Folder

1. Log on to D.C as Administrator, Open **Computer** → Go to a drive and create a shared folder **home** with **Everyone Read/Write** permission.
2. Go to **Active Directory Users and Computers** → select **Users** and right click **User user1** and click **Properties**.
3. Select the **Profile tab** Under the **Home folder**, select **Connect** and Select a drive letter **Z:** and in **To:** enter **\Server Name\Share Name\User Name**.

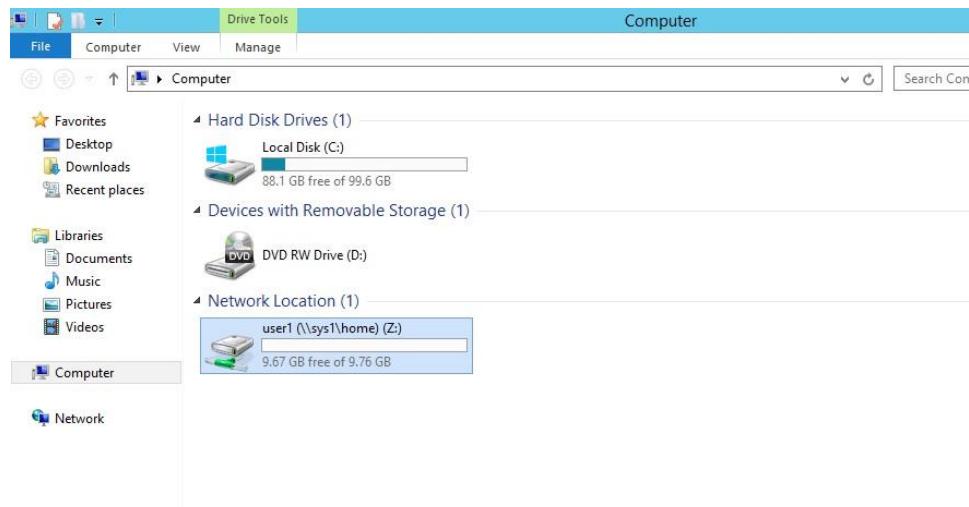
Example: **\SYS1\home\user1**.



4. Click **Apply** and **OK**.

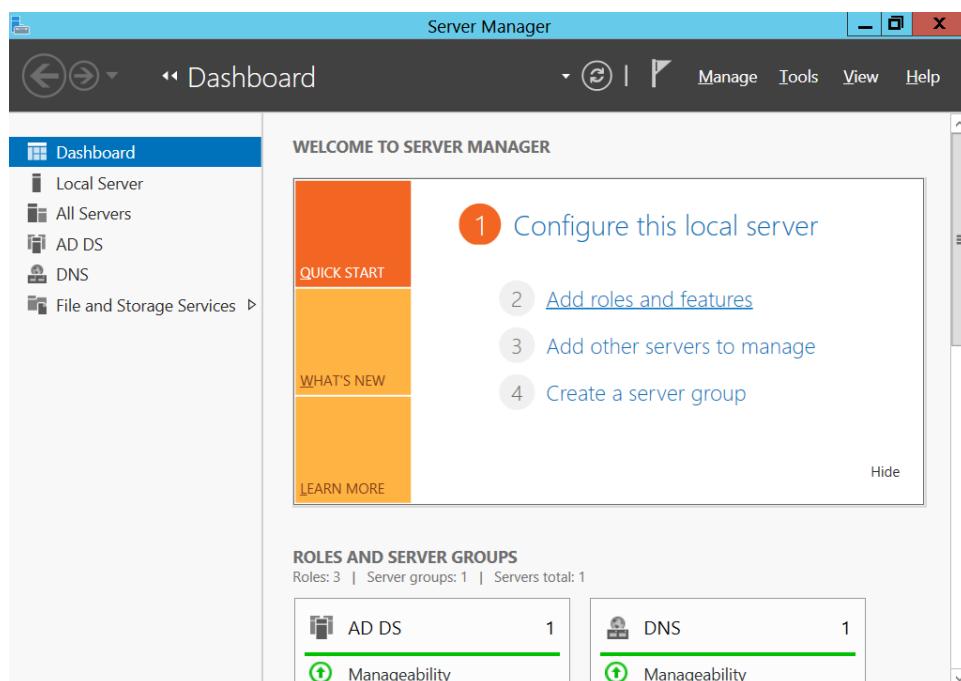
Verification:

1. Login as user (**user1**) on **Client or Member Server**.
2. Open **Computer**, Locate Home folder under network drives.

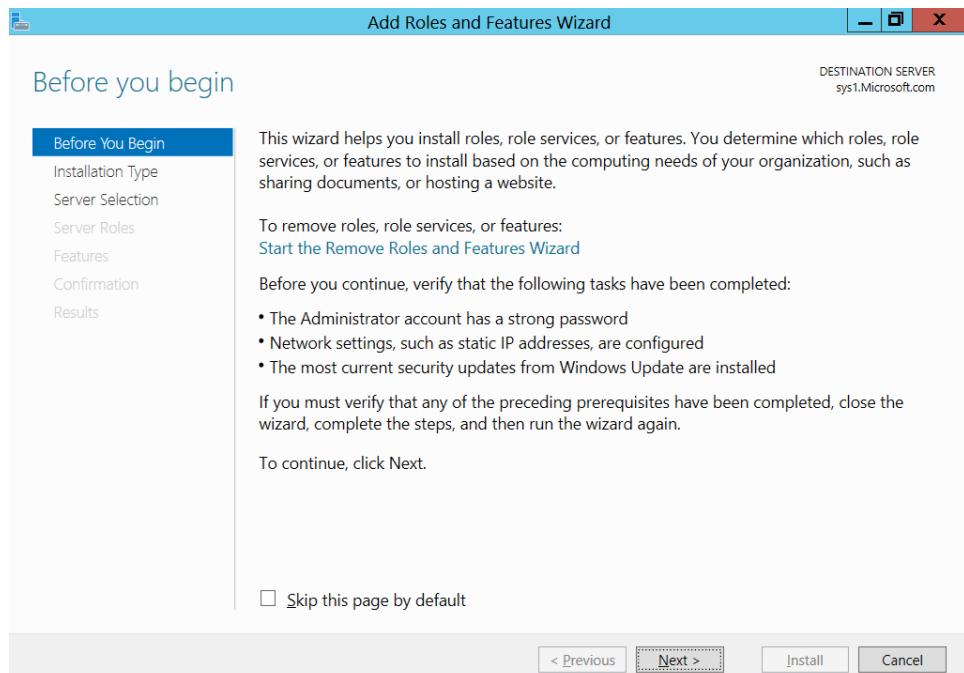


Lab – 4: Installing FSRM Role Service

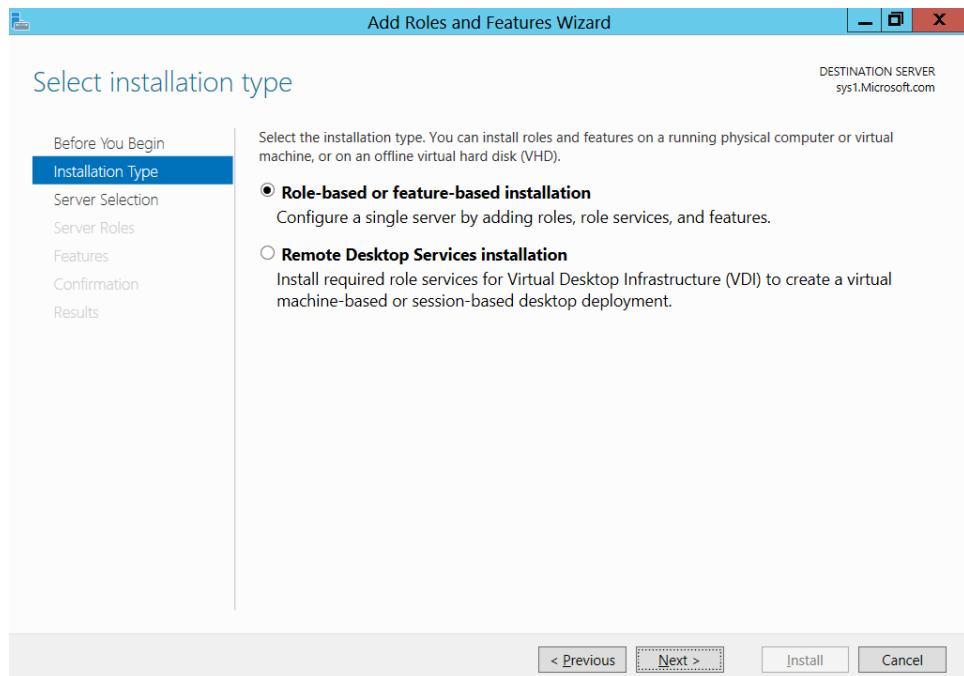
1. In Server Manager Dashboard, click **Add roles and features**.



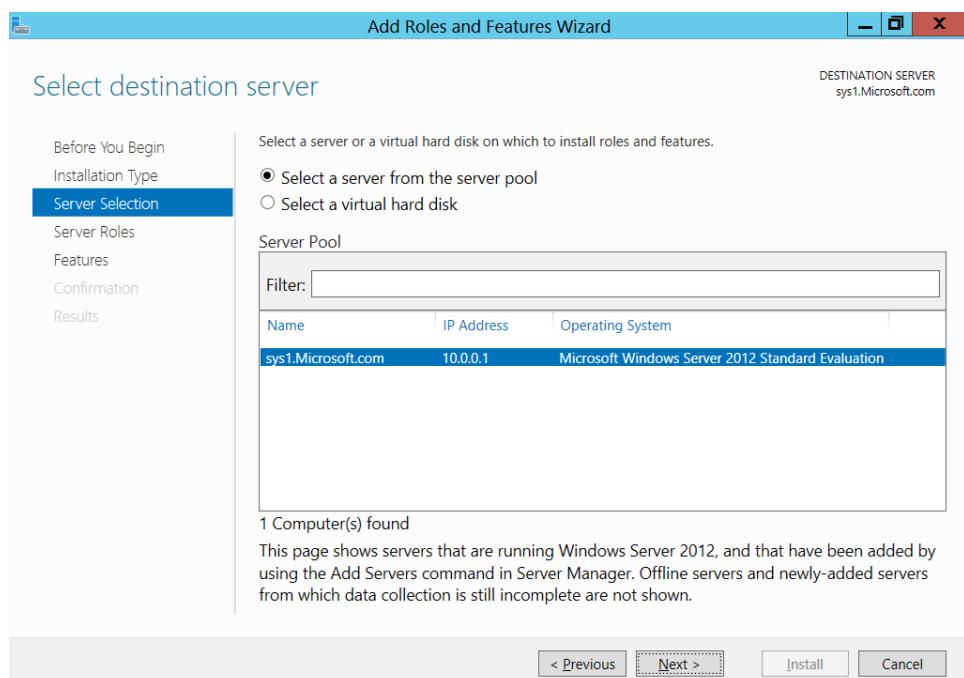
2. In Before you begin page, click **Next**.



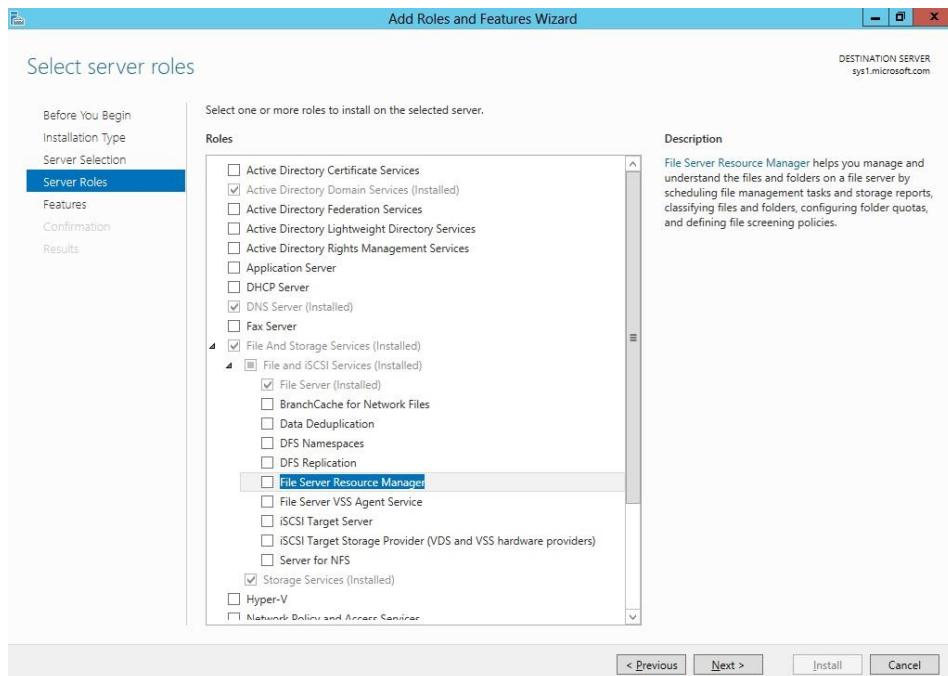
3. In Select installation type, select **Role-based or feature-based installation**, click **Next**.



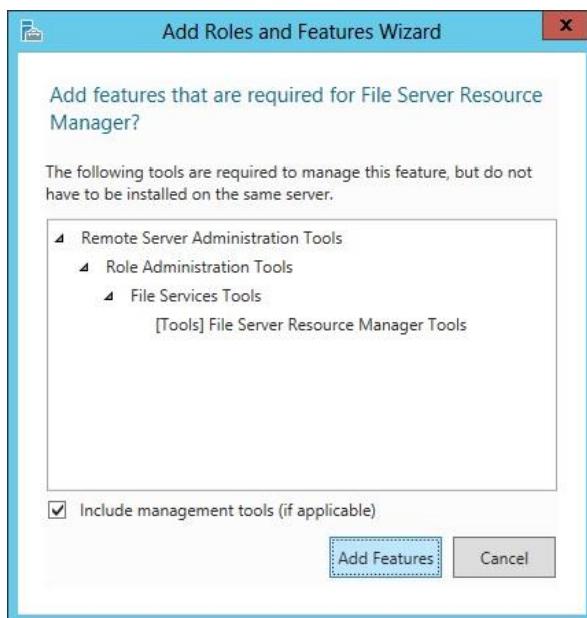
4. In Select destination server, from Server Pool select **SYS1**, click **Next**.



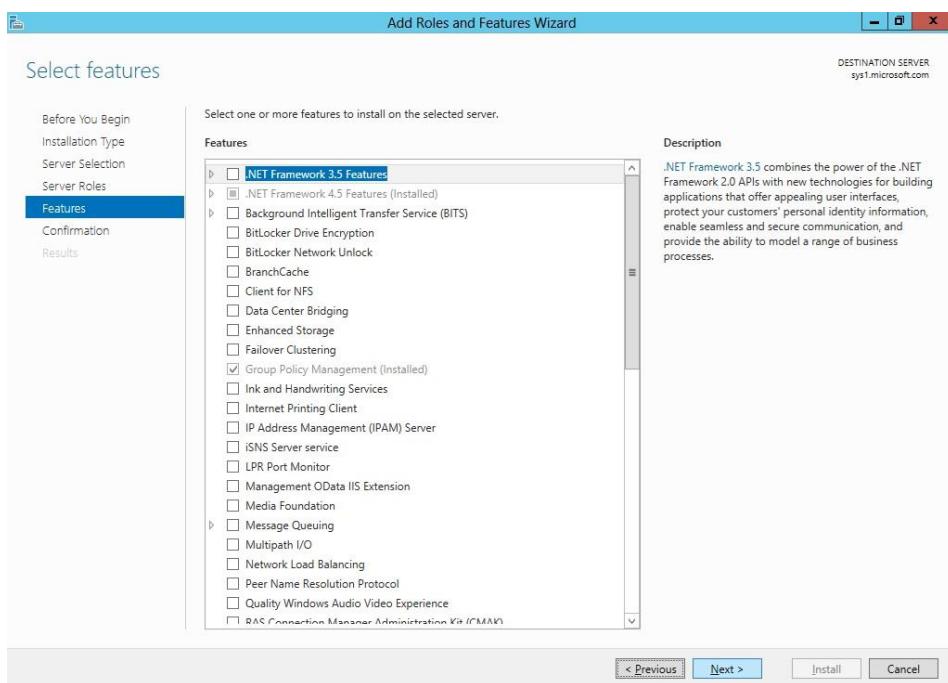
- 5.** In Roles, expand File and Storage Services, expand File and iSCSI Services, check the box **File Server Resource Manager**, click **Next**.



- 6.** Click **Add Features**, to install the required features for Active Directory Domain Services. Click **Next**.

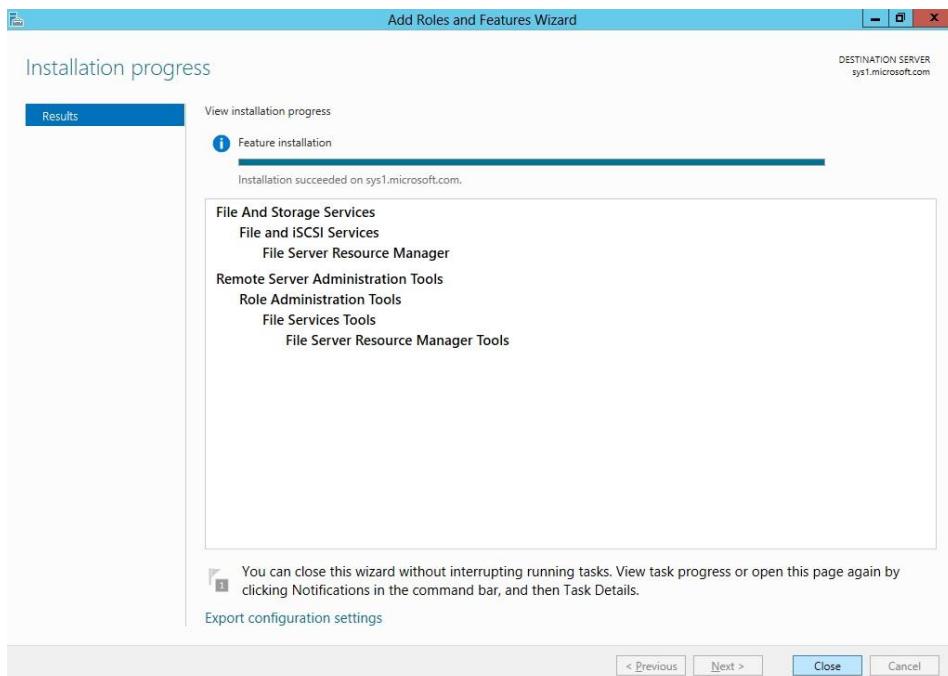


7. In Select features wizard, click **Next.**



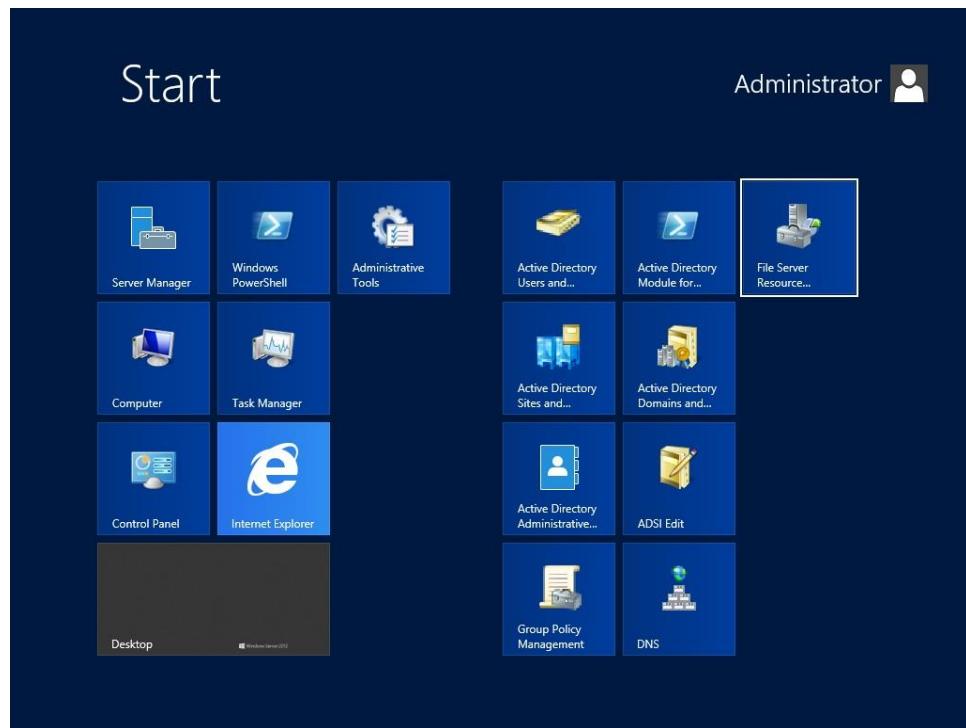
8. Check the box **Restart the destination server automatically if required. Click **Install**.**

9. Click **Close, to complete the installation**

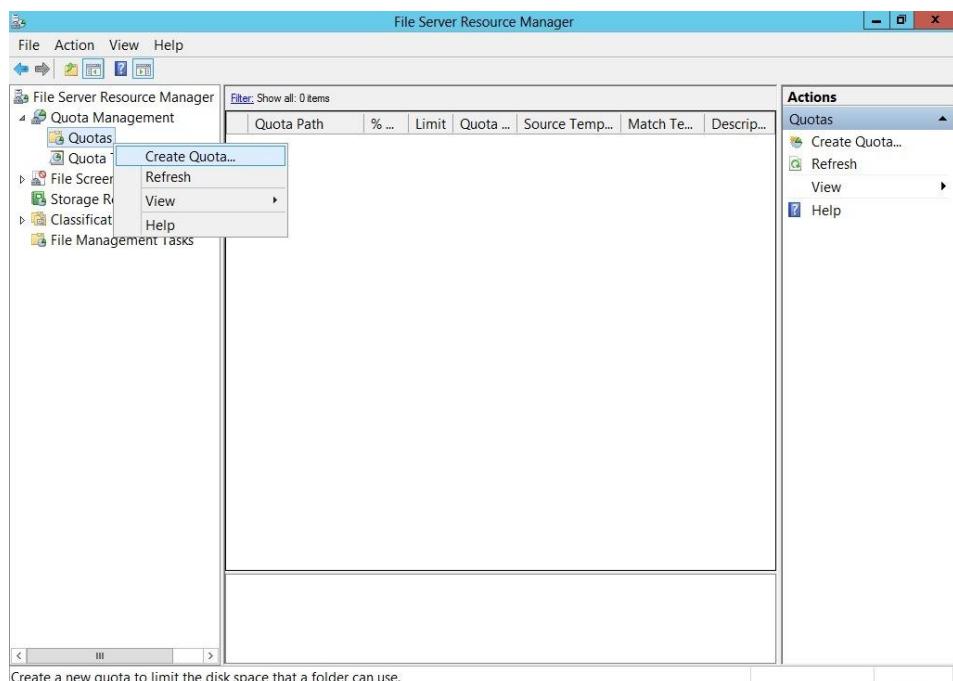


Lab – 5: Configuring Quota Management using FSRM

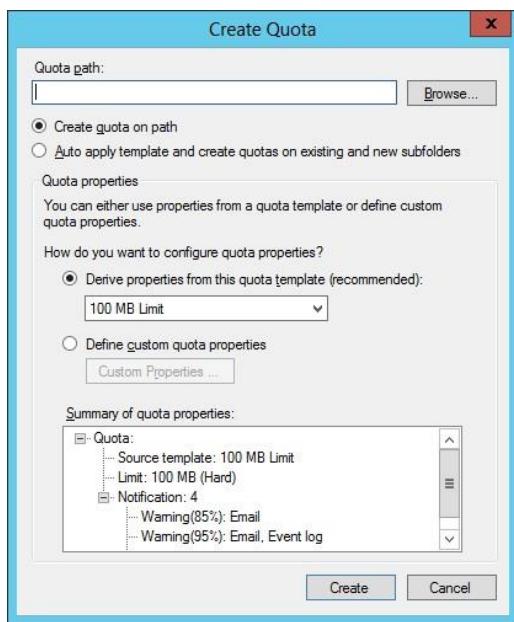
1. Go to Start, select **File Server Resource Manager**.



2. Expand Quota Management, right click Quotas, and select **Create Quota**.

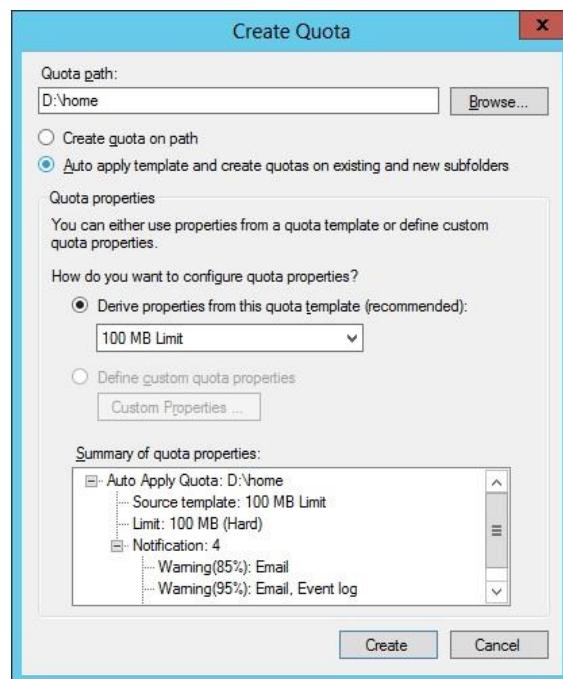


3. Click **Browse** and Select the Quota path (Ex: D:\Home)



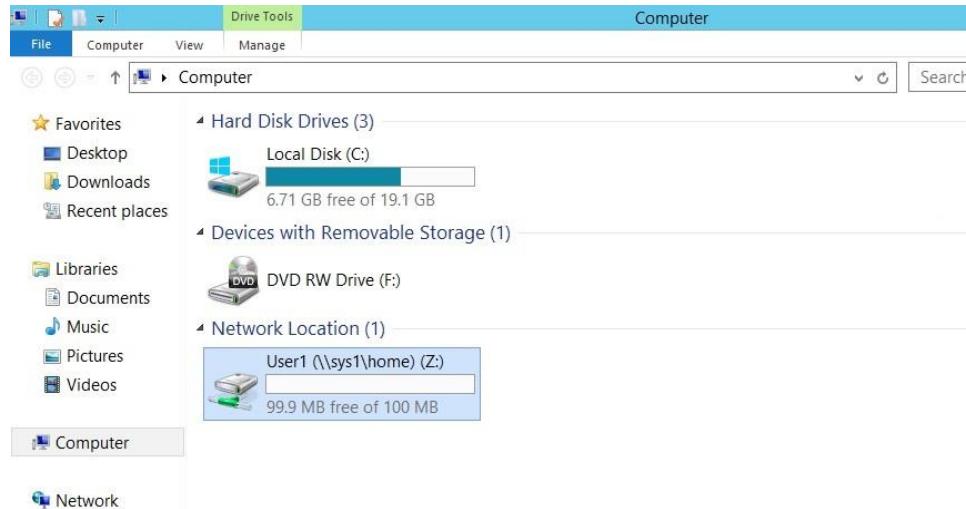
4. Select **Auto apply template and create quotas on existing and new subfolders**.

Select the limit and click **Create**.



Verification

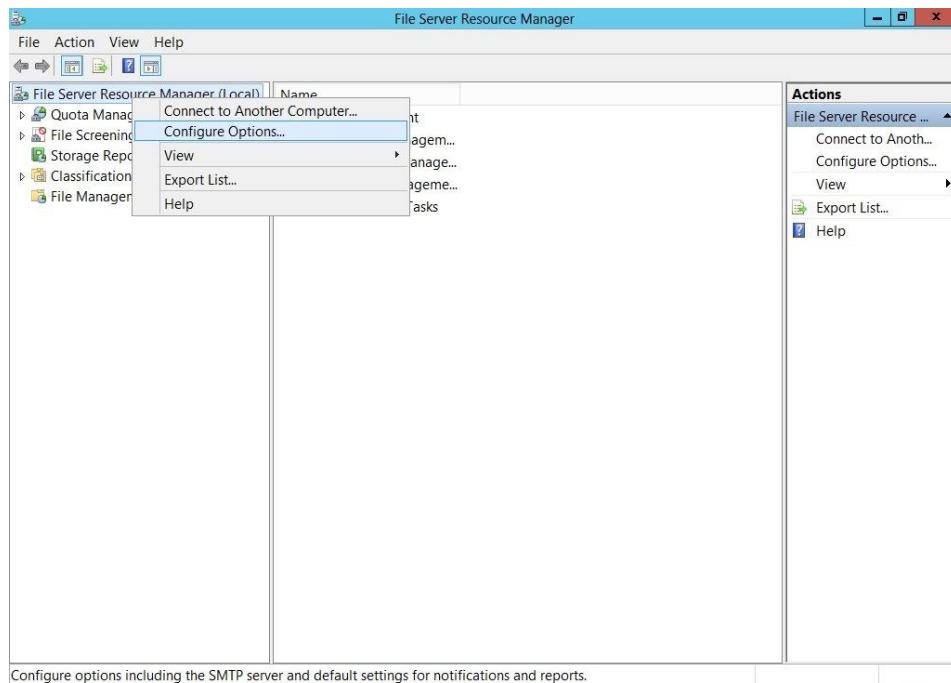
1. Log in as User (**User1**) on Client or Member Server (**SYS2**), Open Computer.
2. Verify the Size of the Network drive Z: (Home Folder).



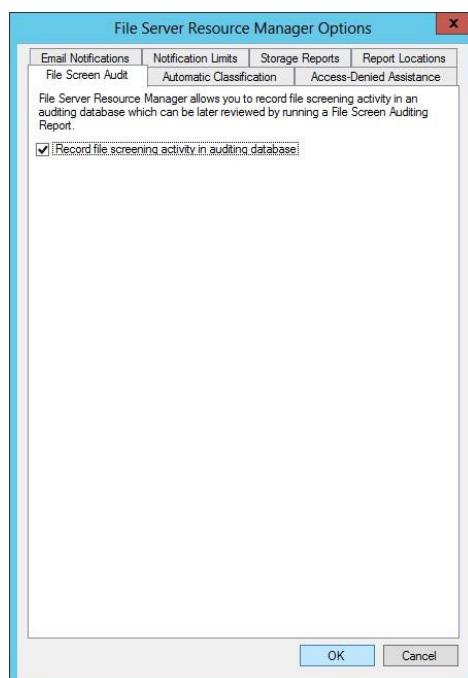
3. Login as other users and verify the size of the Home Folder.

Lab – 6: Configuring File Screening Using FSRM

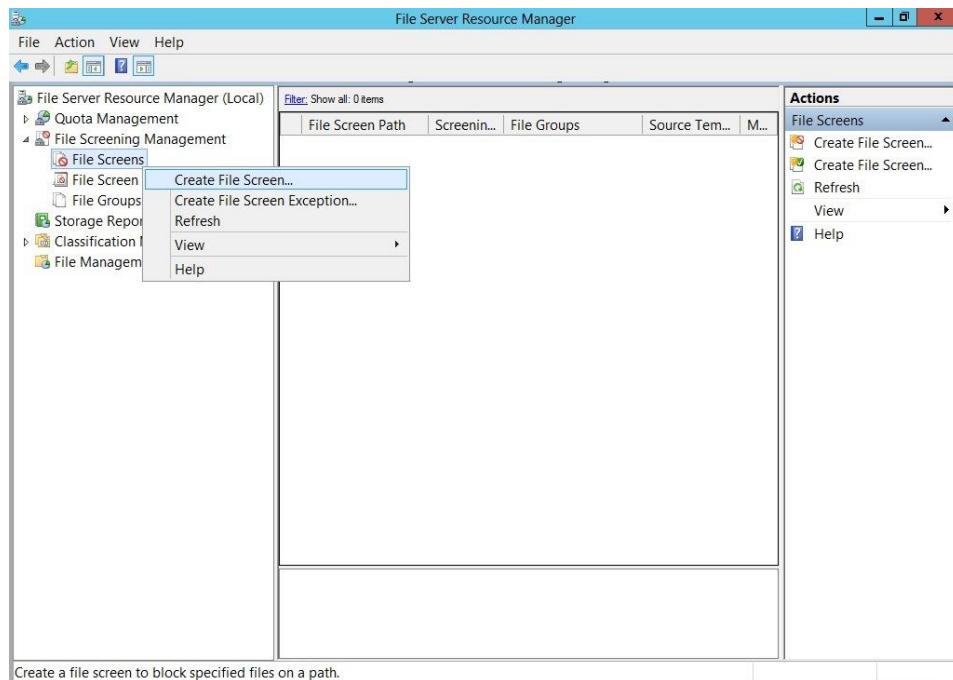
1. Go to Start, File Server Resource Manager, Right click on File Server Resource Manager and select **Configure Options**.



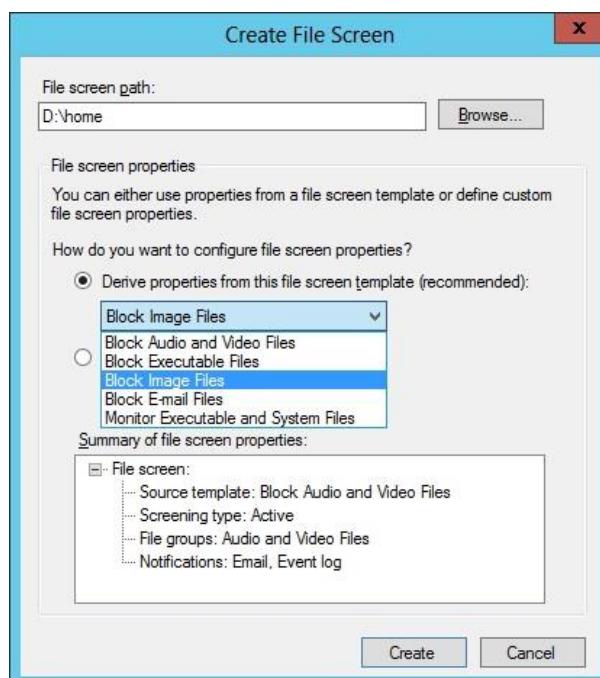
2. Check the box Record file screening activity in auditing database, click **OK**.



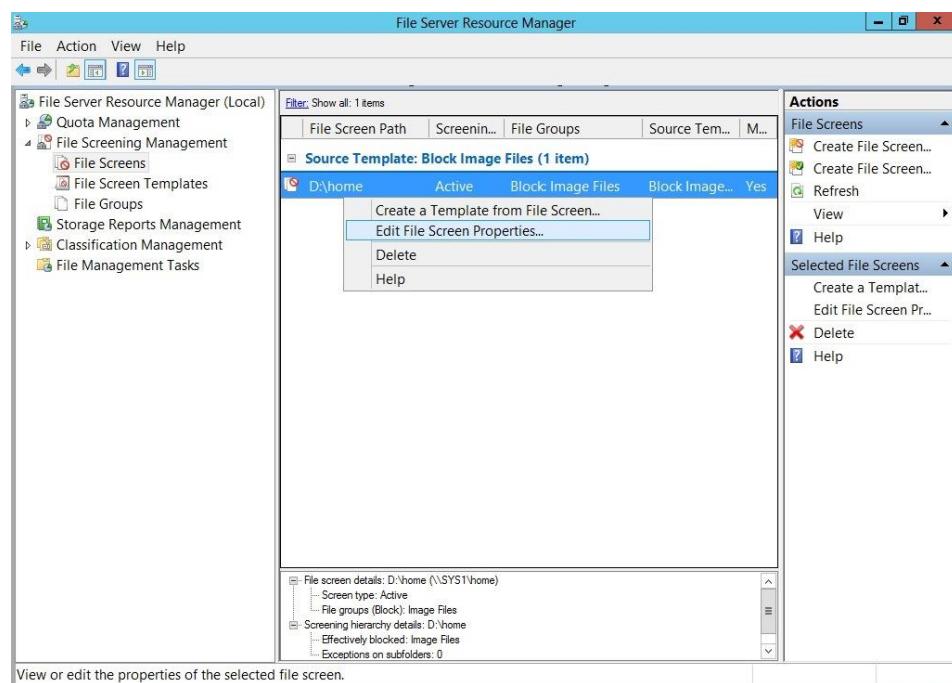
3. Expand File Screening Management, right click File Screens and select **Create File Screen**.



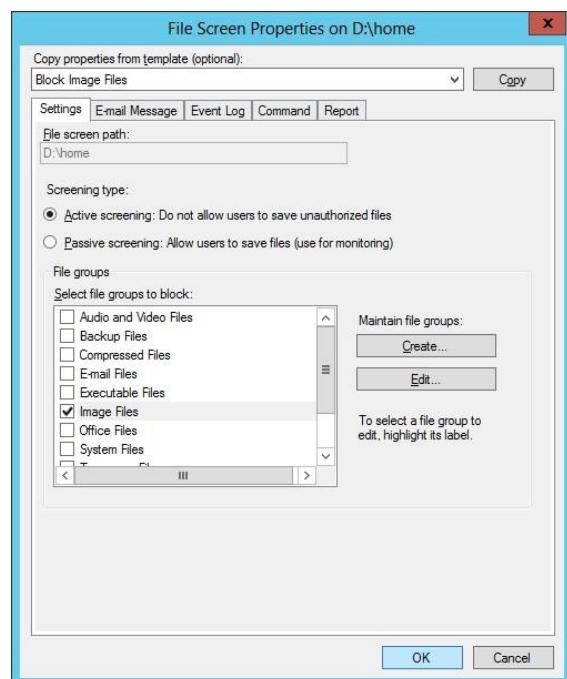
4. Click Browse to select the File screen path, select option **Block Image Files**, and click **Create**.



5. Right click on the created file screen, select **Edit File Screen Properties.**

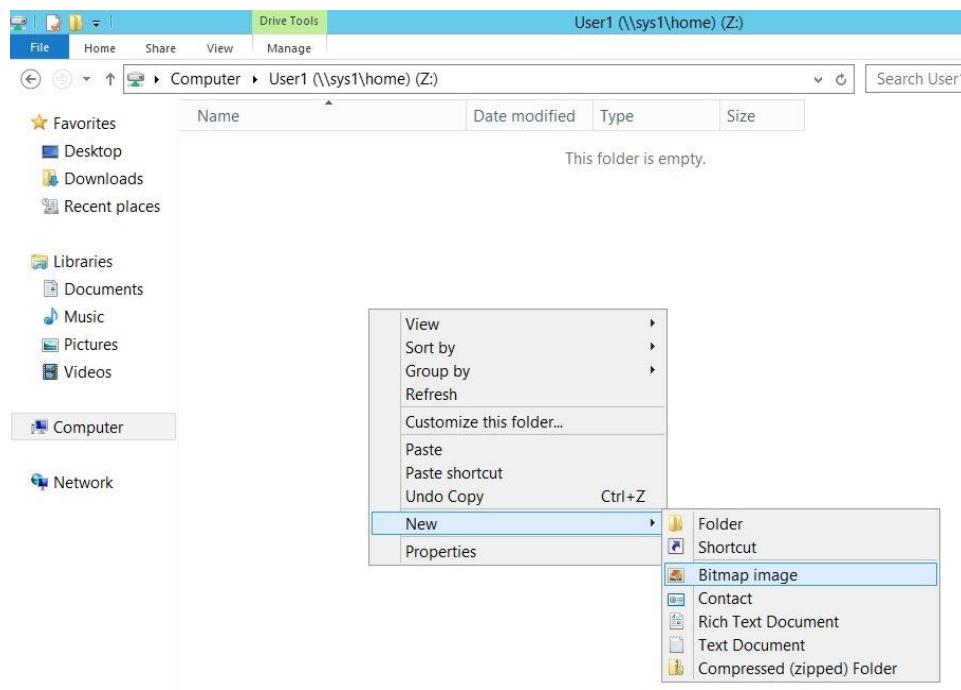


6. Select the Screening type Active screening, click **OK.**

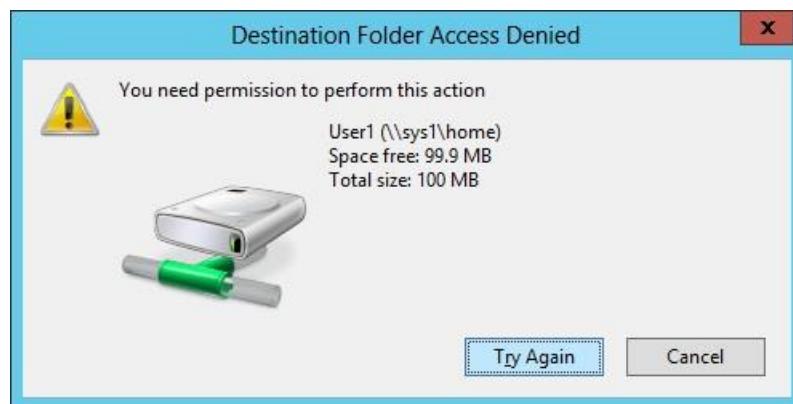


Verification

1. Log in as User (**User1**) on Client or Member Server (**SYS2**),
2. Open Computer, Network drive Z: (Home Folder) and try to create a **New Bitmap Image file**.

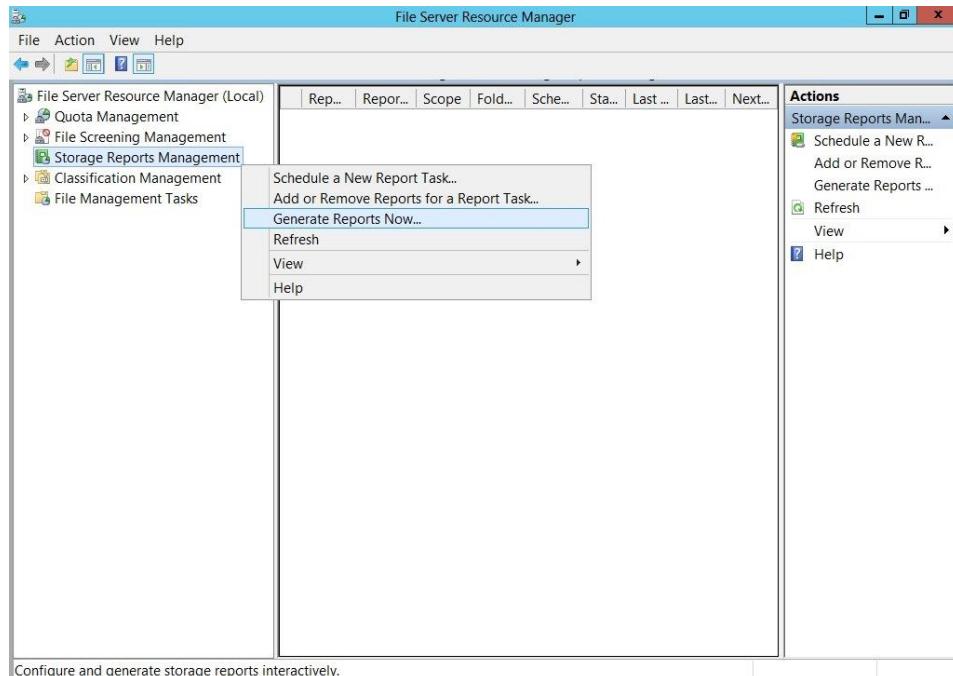


3. Verify for Access Denied Page.

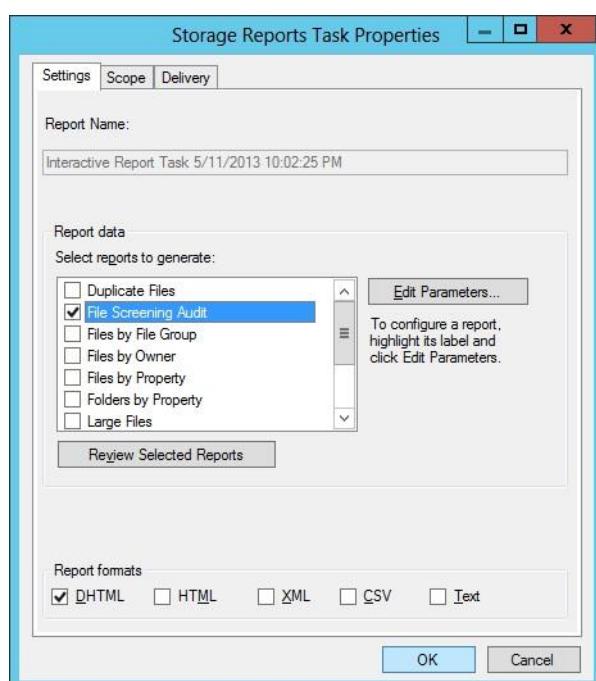


Lab – 7: Configuring Storage Reports Management using FSRM

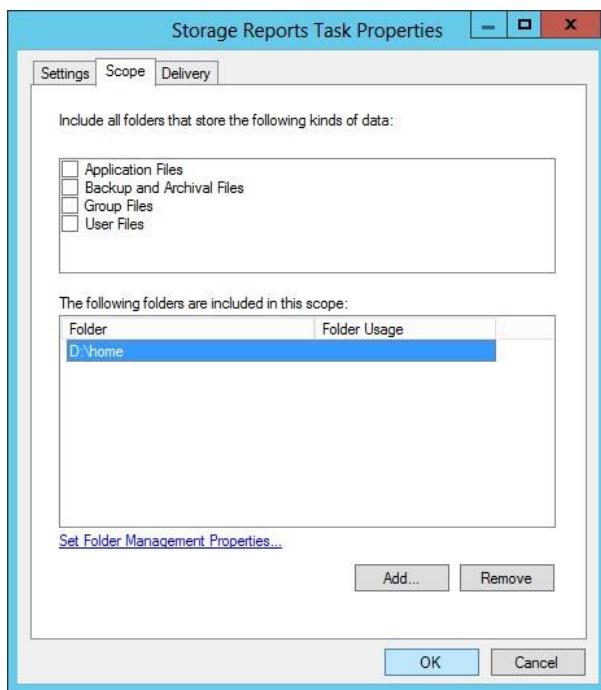
1. Go to Start, File Server Resource Manager, right click Storage Reports Management and select Generate Reports Now.



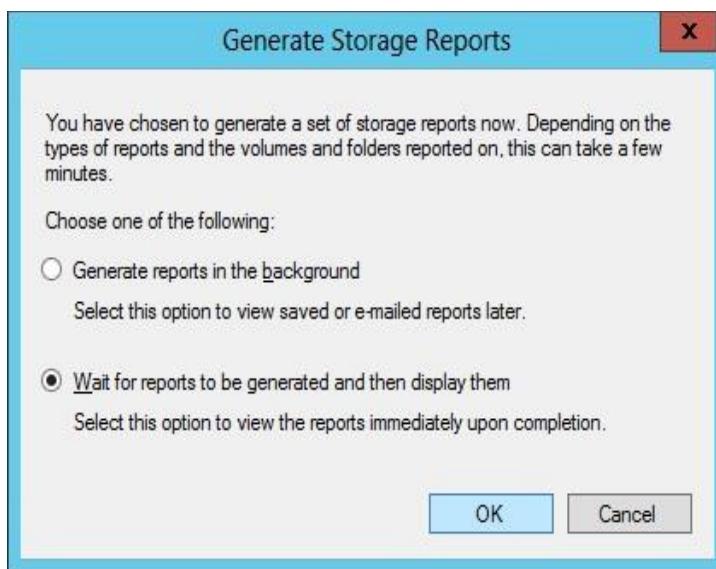
2. In settings page, check box **File Screening Audit**.



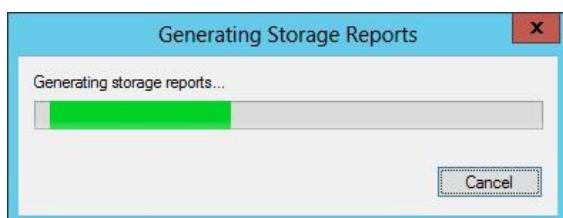
3. Select Scope, click **ADD**and select the home folder (Ex: D:\Home).



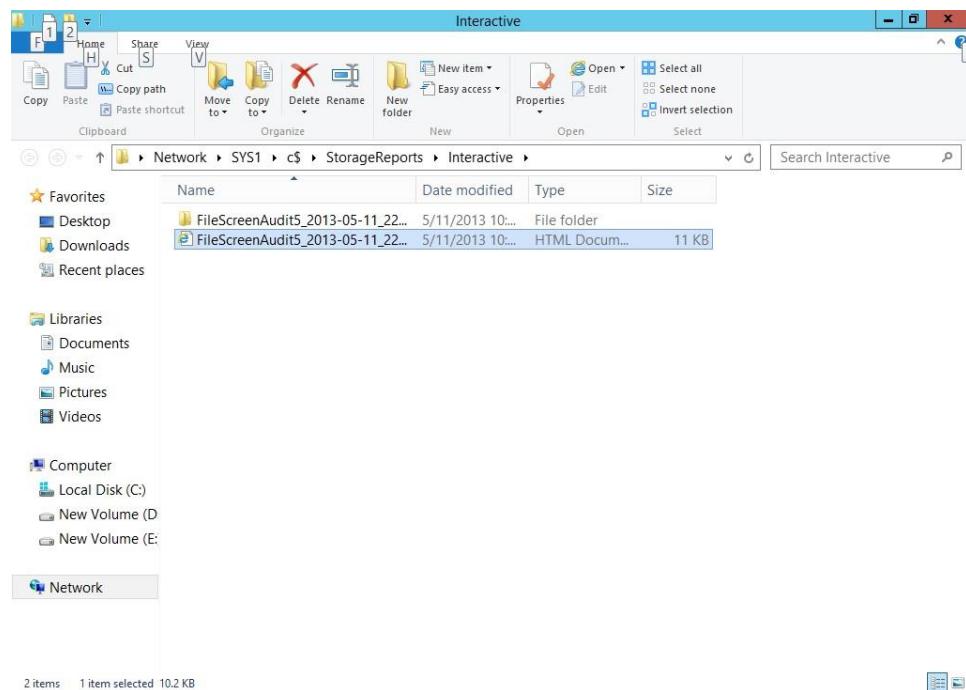
4. Select Wait for reports to be generated and then display them, click **OK**.



5. It Generates the Storage Reports



6. Select the File Screening Audit Report and Open the report.



7. Verify the Report for Blocked image file creation by the users.

The screenshot shows a report window titled 'File Screening Audit Report' generated at 5/11/2013 10:04:43 PM. It includes sections for 'Report Description' (Lists file screening audit events on the server for a specified period. Use this report to identify users or applications that violate screening policies.), 'Machine' (SYS1), and 'Report Folders' ('D:\home\'). Below this is a 'Report statistics' table:

Report statistics						
File name	Folder					
	File Group	Status	Time	User	Process	File Screen Path
new bitmap image.bmp	d:\home\user2	Image Files	Blocked	5/11/2013 10:00:12 PM	MICROSOFT\User2	Process ID (4)
new bitmap image.bmp	d:\home\user2	Image Files	Blocked	5/11/2013 10:00:12 PM	MICROSOFT\User2	Process ID (4)
new bitmap image.bmp	d:\home\user2	Image Files	Blocked	5/11/2013 10:00:12 PM	MICROSOFT\User2	Process ID (4)

Organizational Unit

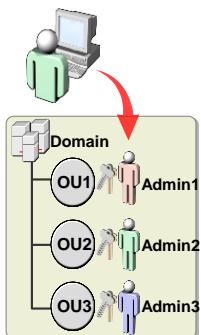
Organizational Unit

- It is a logical container which contain active directory objects (Users, Groups, OU & other objects)
- It is also called as SUBTREE
- It is used for Minimizing administrative tasks
- It is used for organizing and managing the active directory objects
- It is used for delegating the control to one or more users.

What Is Delegation of Control ?

- The process of decentralizing management of organizational units.
- Assigning management of an organizational unit to another user or group
- Eases administration by distributing routine administrative tasks to another user or group.

What Is Delegation of Control ?



Groups

- It is an object of Active Directory used for applying Permissions and Distribution of emails to its members.

Two types of Groups

- Security Group
- Distribution Group

Distributed File System

DFS

- DFS incorporates technologies that provide fault-tolerant access to geographically dispersed files.
- DFS namespaces enable a virtual representation of shared folder structures.

DFS Namespace (DFS-N)

- Allows administrators to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. The subfolders typically point to shared folders that are located on various servers in multiple geographical sites throughout the organization.

DFS - R

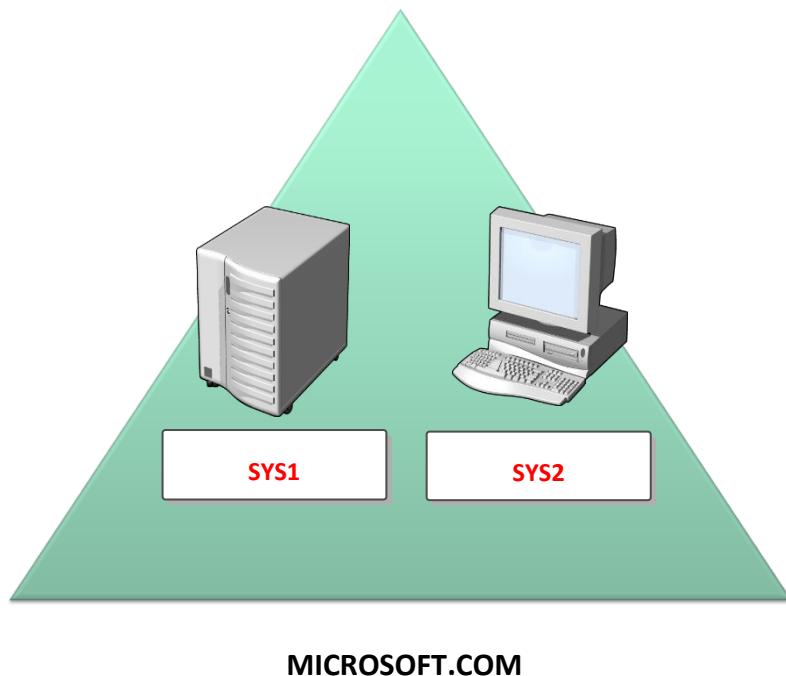
- A multimaster replication engine that synchronizes files between servers for local and WAN network connections. DFS Replication supports replication scheduling, bandwidth throttling, and uses remote differential compression (RDC) to update only the portions of files that have changed since the last replication. You can use DFS Replication in conjunction with DFS namespaces or as a standalone file replication mechanism.

OU&DISTRIBUTED FILE SYSTEM

Pre-requisites:

Before working on this lab, you must have

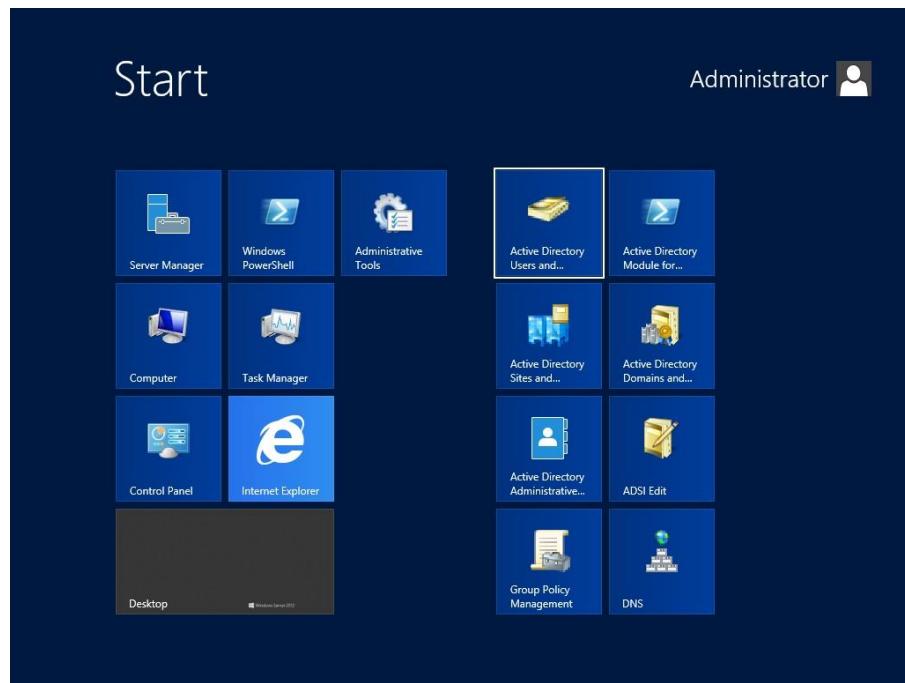
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server or windows 7.



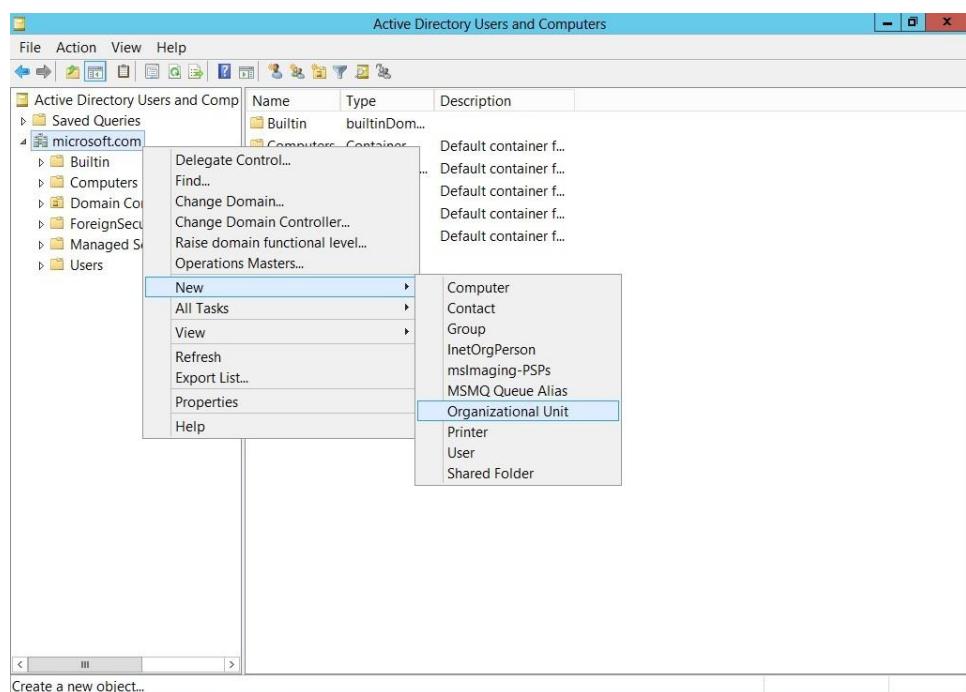
SYS1	SYS2
Domain Controller	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Member Server / Client	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1

Lab – 1: Creating an Organizational Unit (OU)

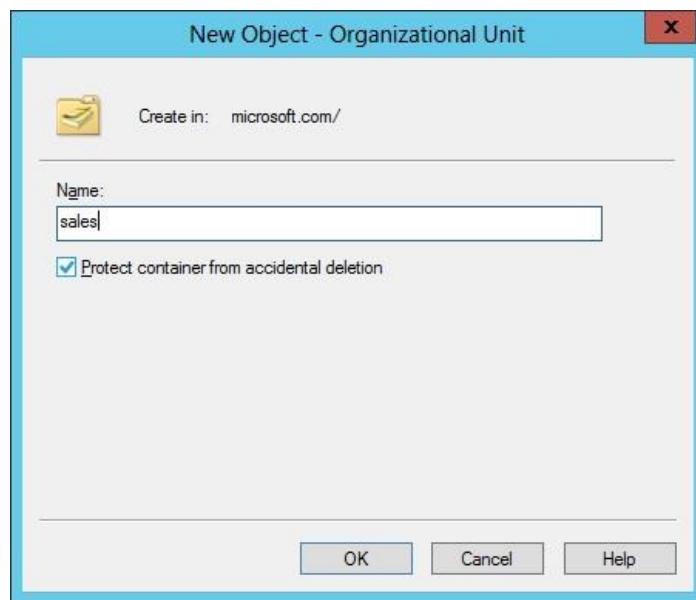
1. Press Windows Key to go to Start, select **Active Directory User and Computers**.



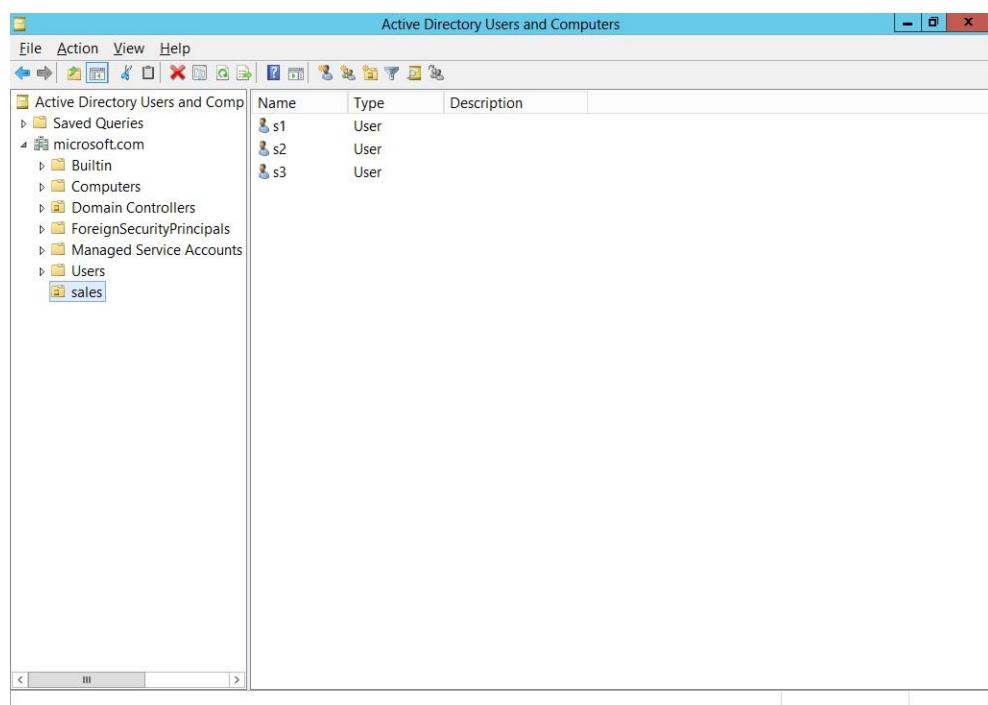
2. Right click **Domain Name** → **New** → **Organizational Unit**.



1. Enter the name for OU (Ex: **Sales1**) and click **OK**.

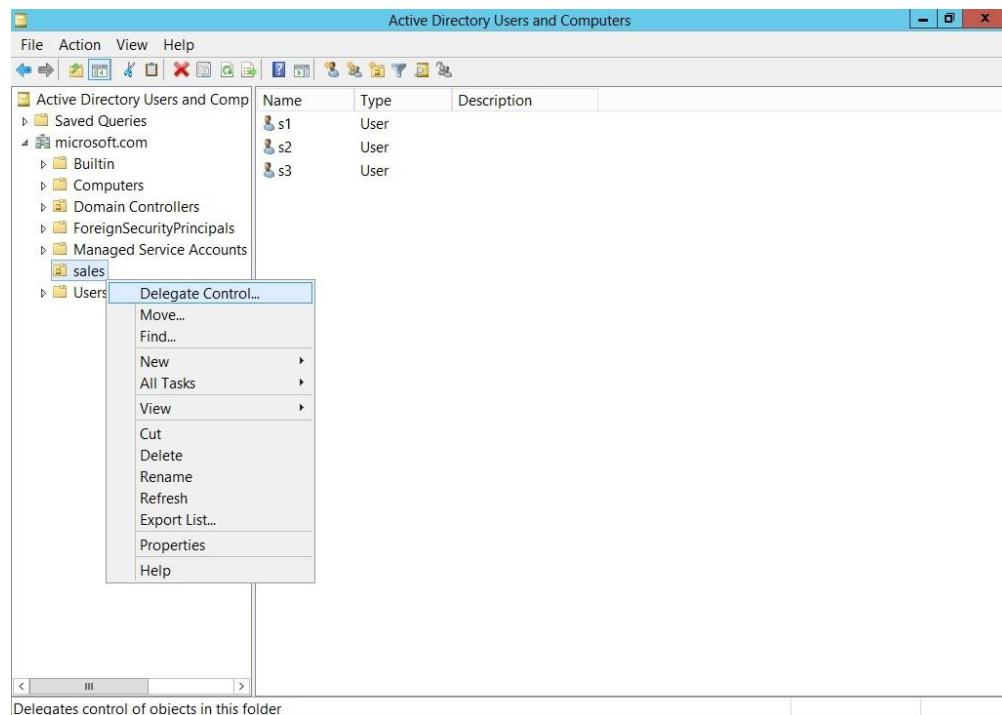


2. Create **Users** in the **Sales1** OU (Ex: **S1, S2, S3**)



Lab – 2: Delegating Control to a User

1. Go to Active Directory Users and Computers → right click OU → select **Delegate Control**



2. Click **Next**.



3. Click **Add** → Add the User (User1).



4. Check the Box **Create, delete and manage user accounts** and **Next**.



5. Click **Finish**.

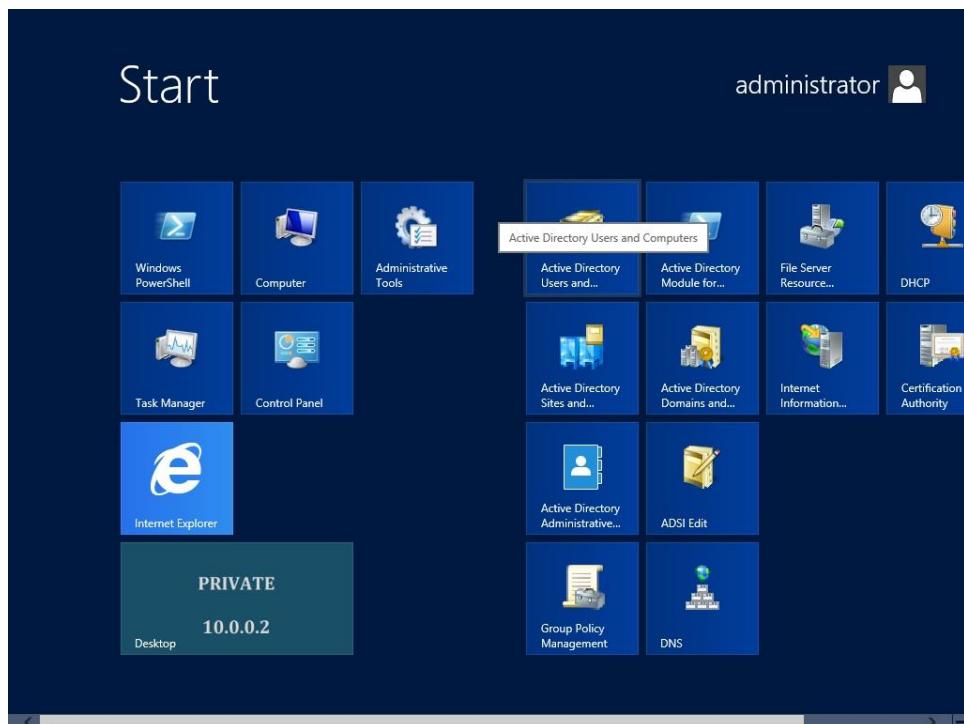


Verification:

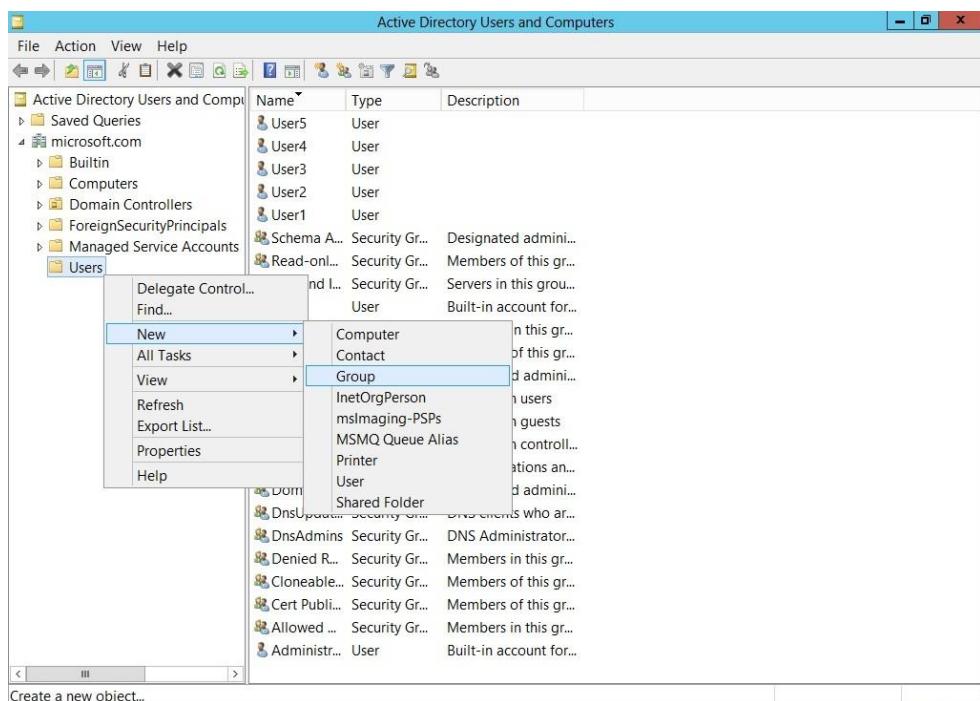
1. Log on to D.C as User (User1), Create User in OU.

Lab – 3: Creating Groups

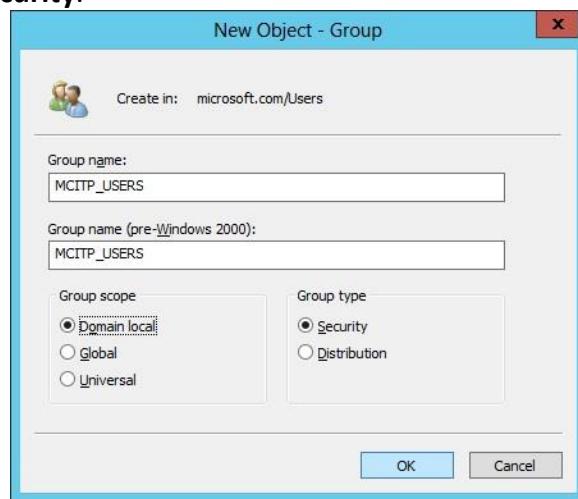
1. Login as **Administrator** on a **Domain Controller**.
2. Go to Start, select **Active Directory Users and Computers**.



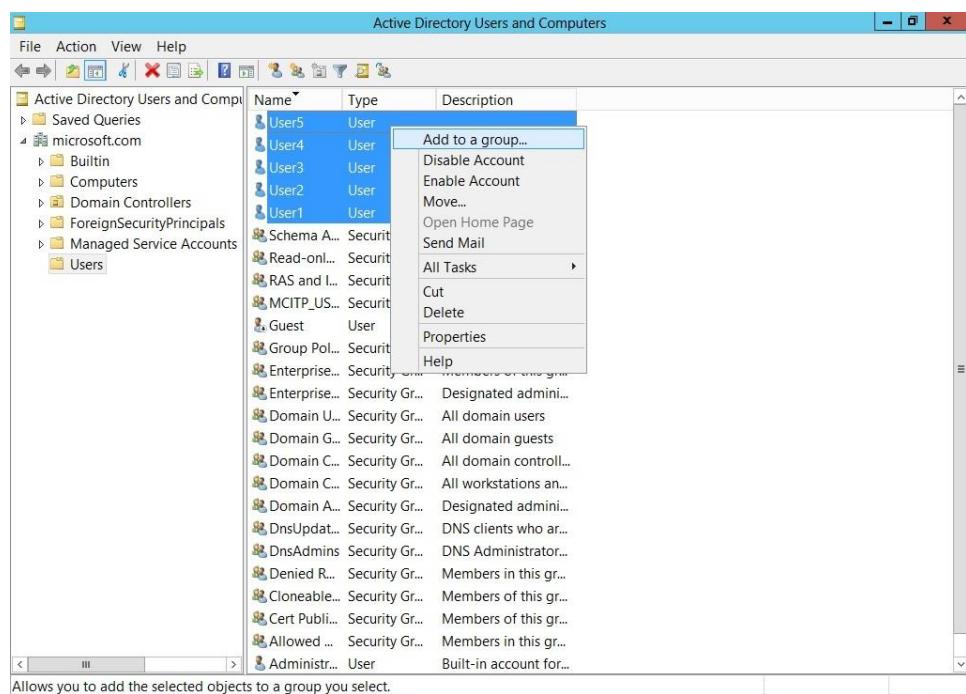
3. Right click **Users** → Select **New** → **Group**.



Mention the **Group name** and Select the Group Scope as **Domain Local** and Group type as **Security**.



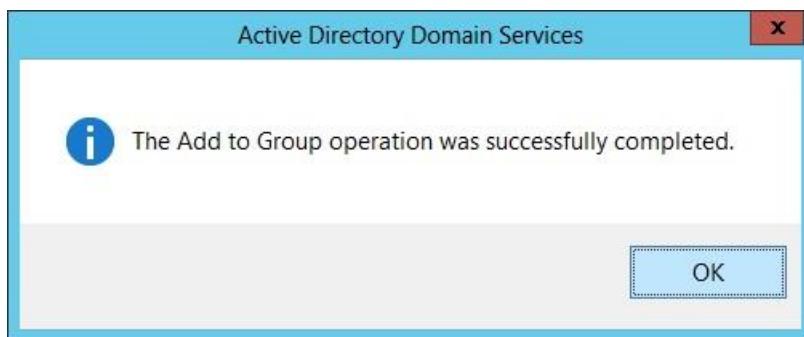
4. Group will be created successfully.
5. To add any users to this group, Right click on User account and Select **Add to a group**



6. Mention the group name as **MCITP_USERS** → click **OK**.

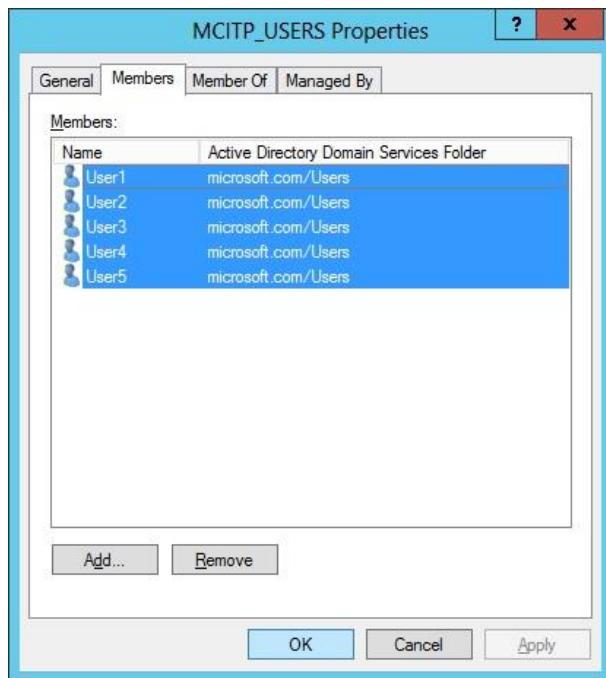


7. Add to Group operation was successfully completed.



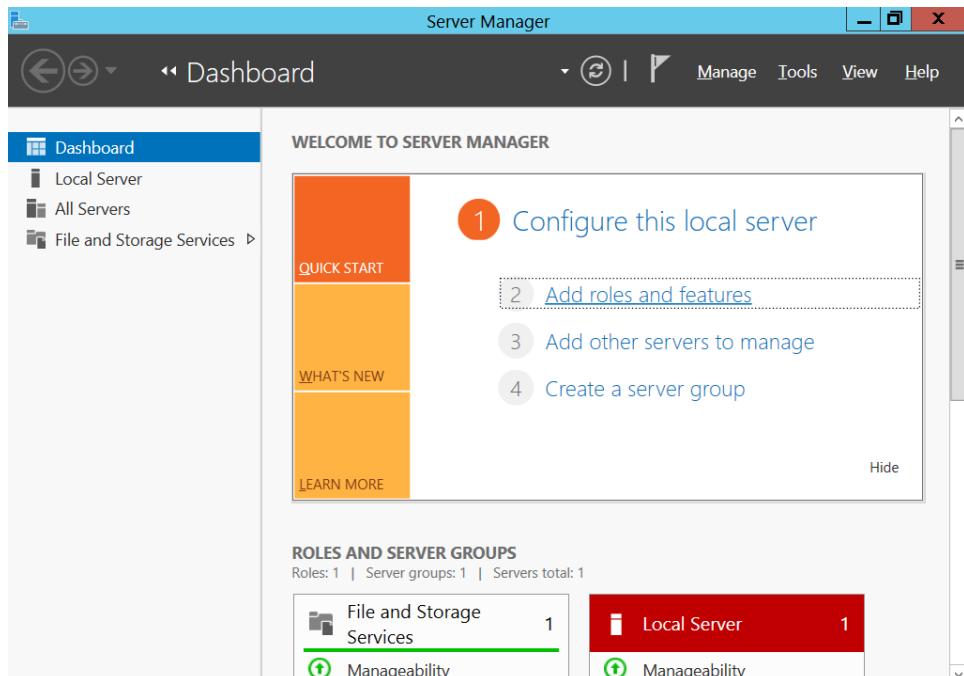
For Verification:

1. Go to **Active Directory Users and Computers** → Right click on **Group** → Select **Properties** → Select **Members Tab** → Verify for the User.

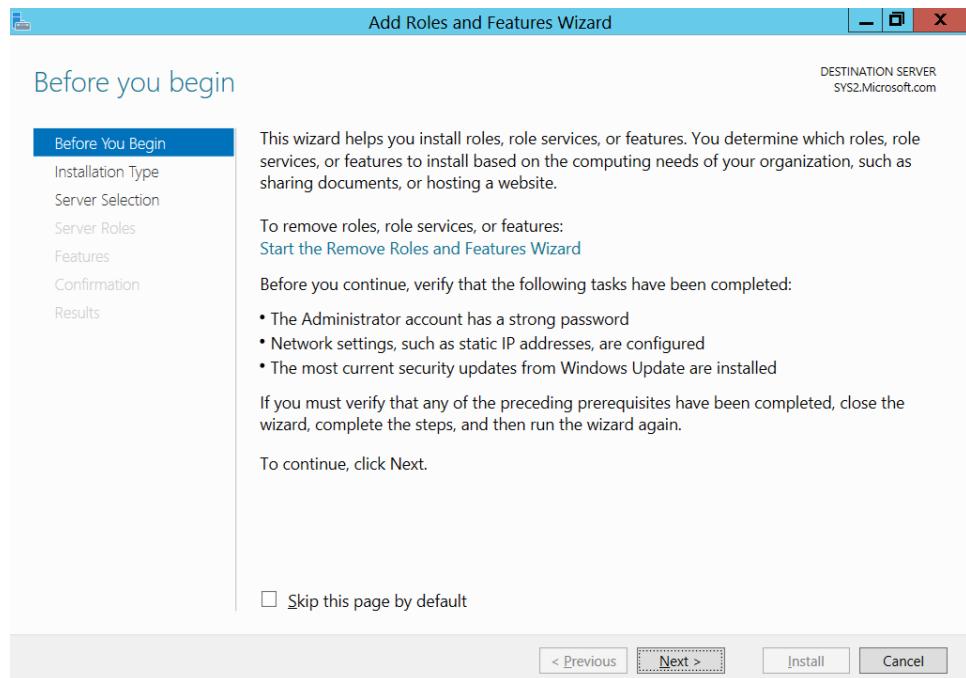


Lab – 4: Installing Distributed File System (DFS)

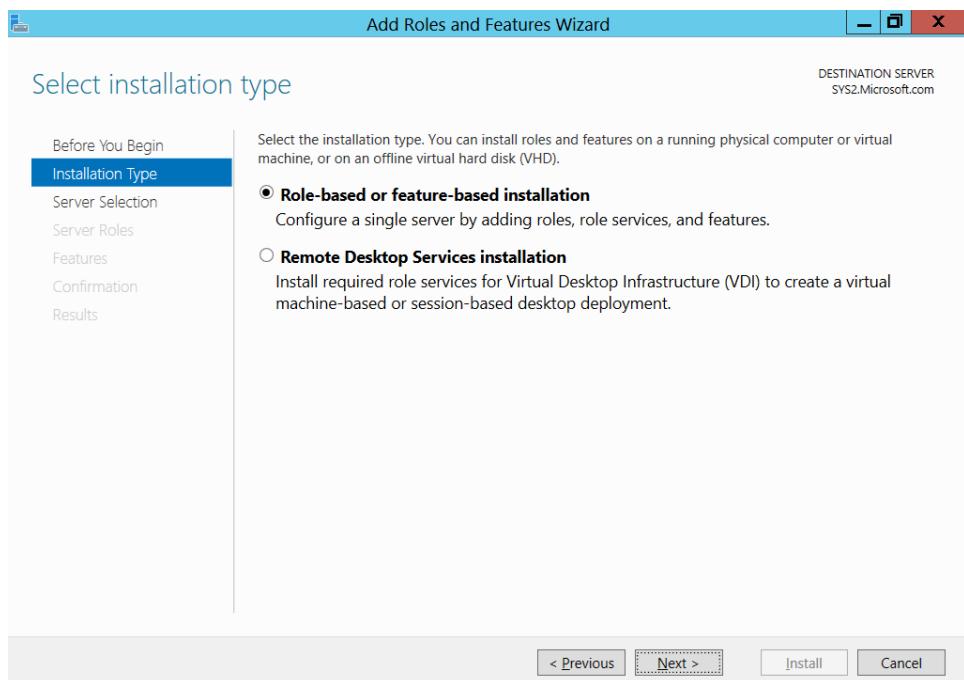
1. In **SYS2 (Member Server)**, Go to **Server Manager**. Click **Add roles and features**.



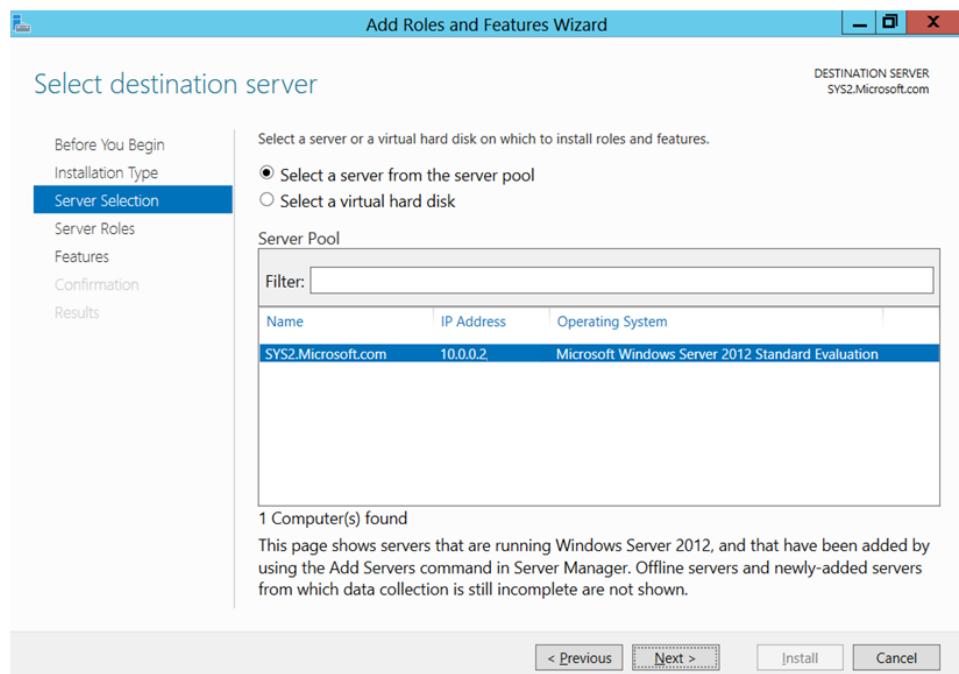
2. In Before you begin page, click **Next**



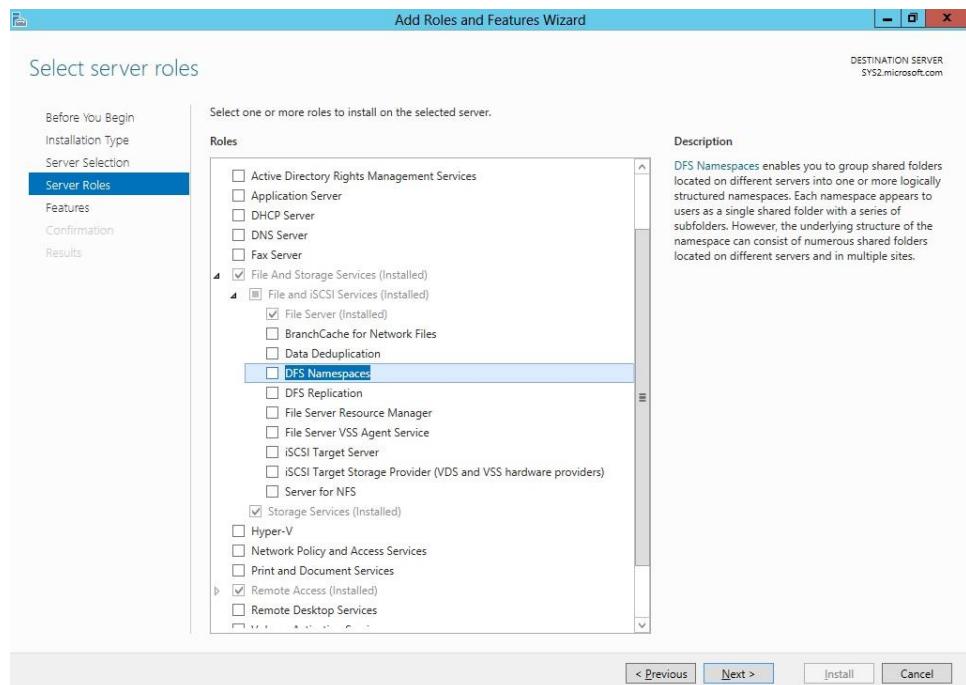
3. Installation.



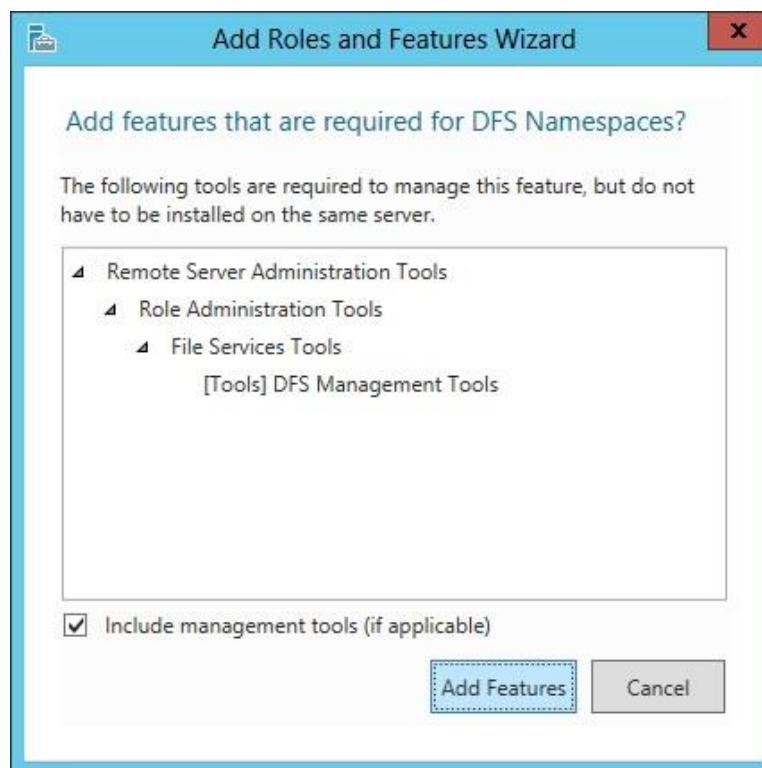
4. In Select destination server, from Server Pool select **SYS2.Microsoft.com**, click **Next**.



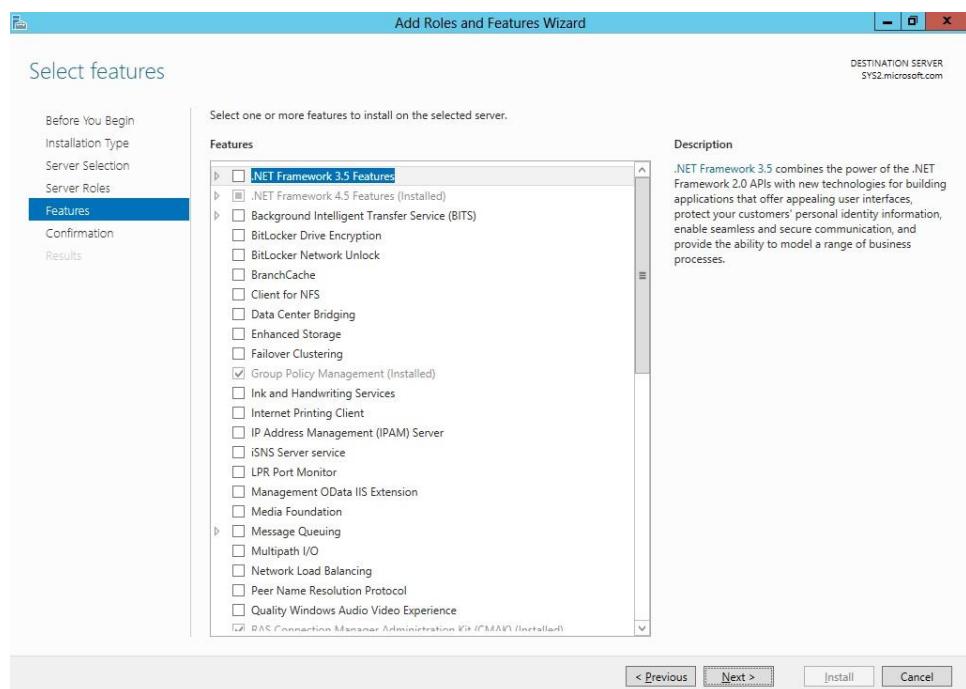
- 5. Expand File and Storage Services, Expand File and iSCSI Services, check box **DFS Namespaces**.**



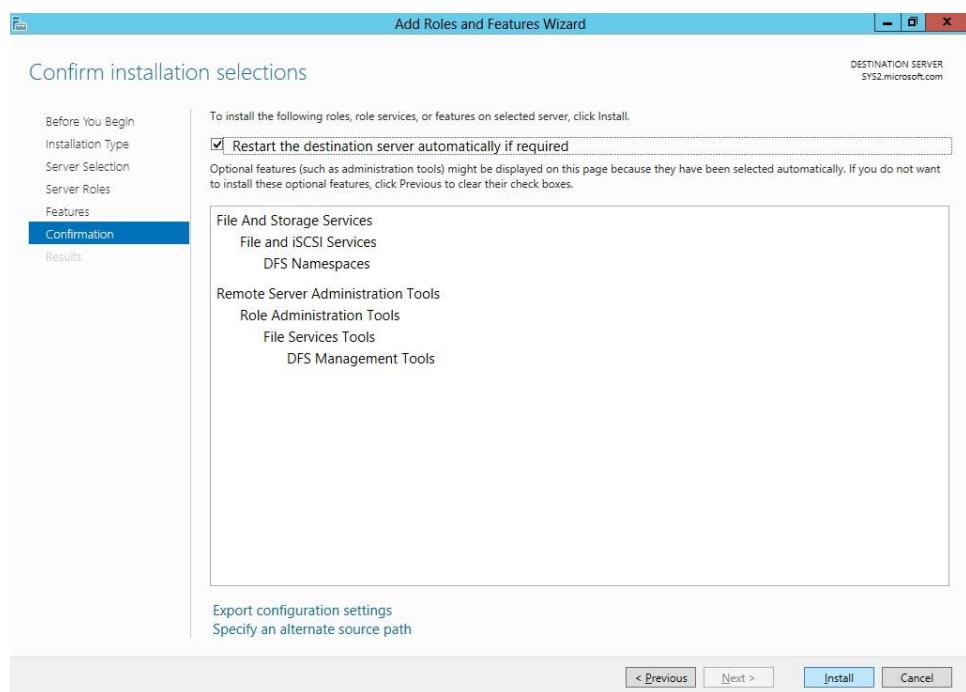
- 6. Click **Add Features**, to install the required features for DFS Namespaces, Click **Next**.**



7. In Select features wizard, click **Next.**



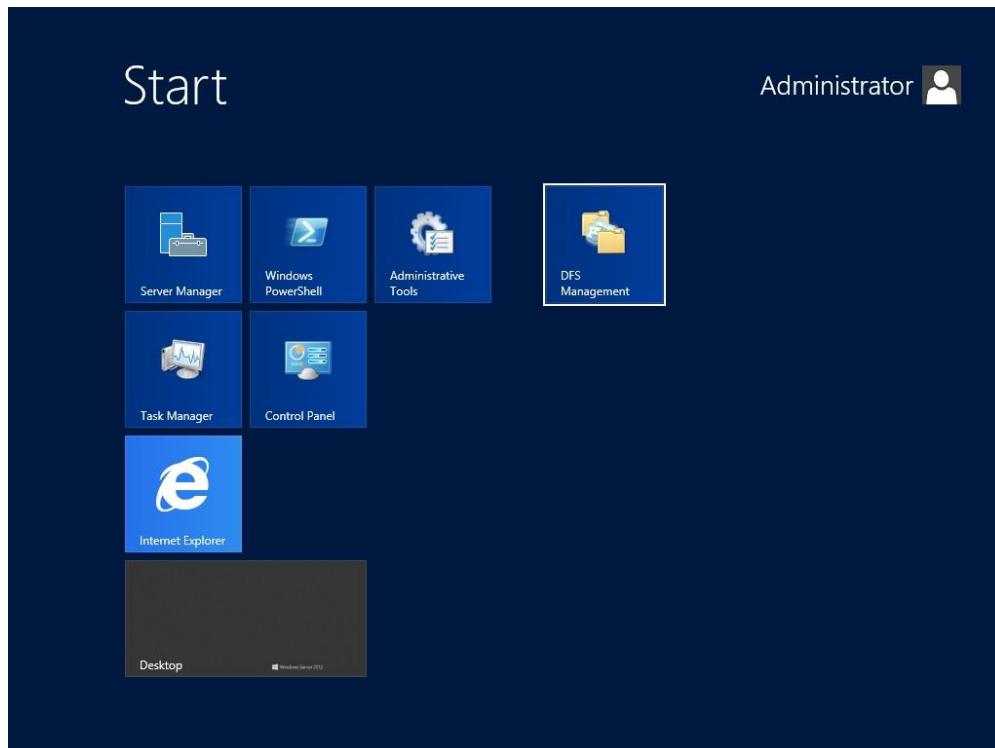
8. Check the box **Restart the destination server automatically if required. Click **Install**.**



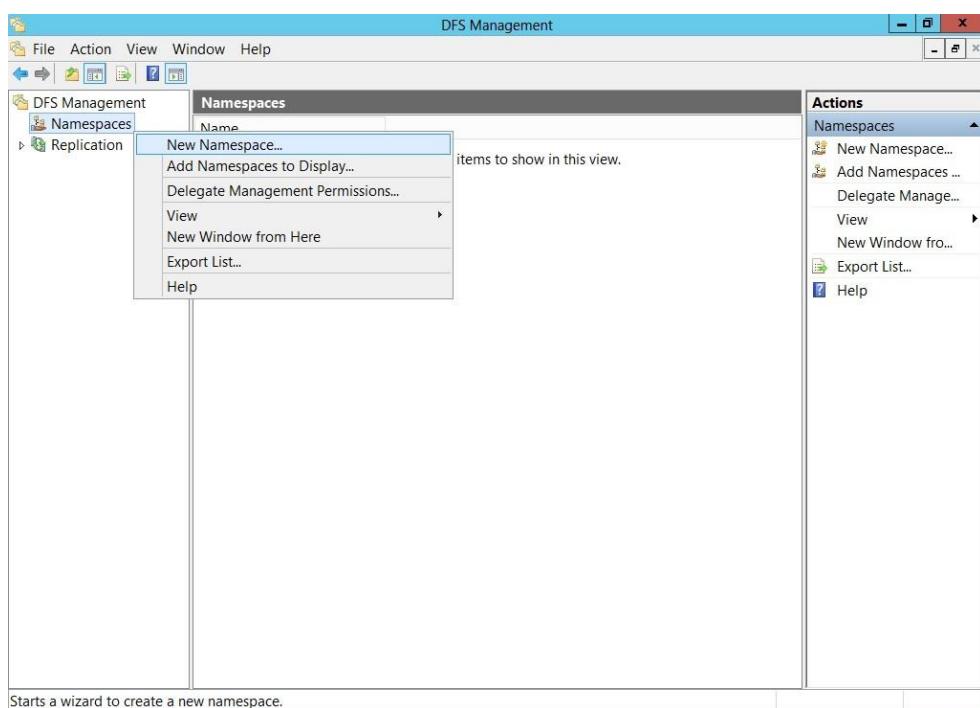
9. Click **Close.**

Lab – 5: Configuring Namespace In DFS

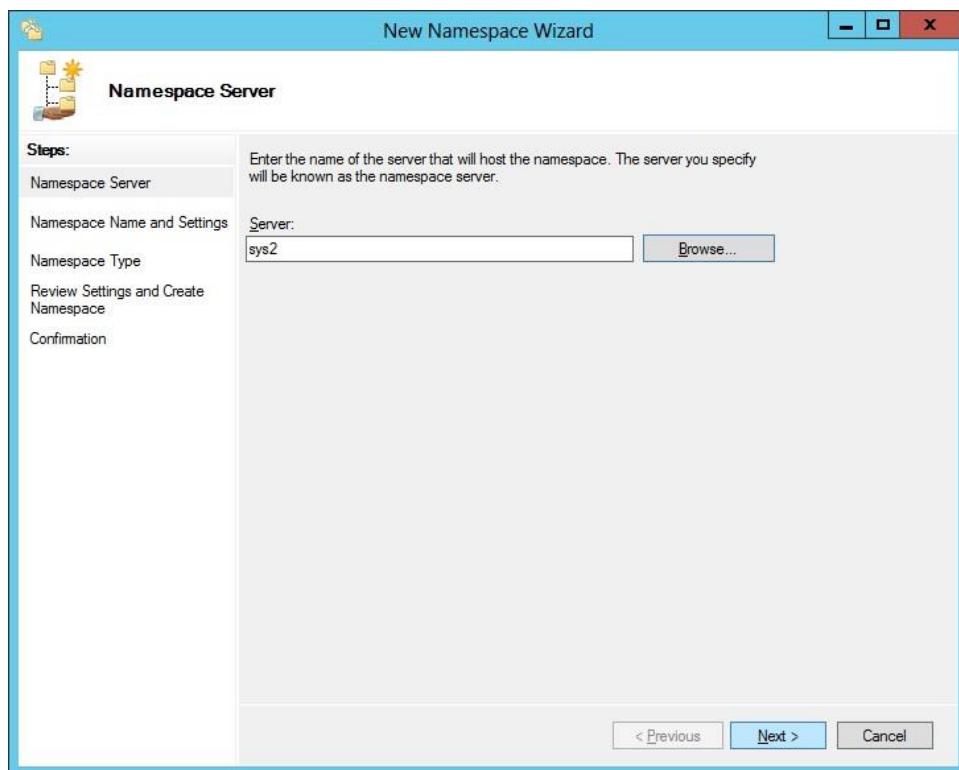
1. In **SYS2** (Member Server) Go to Start, select **DFS Management**.



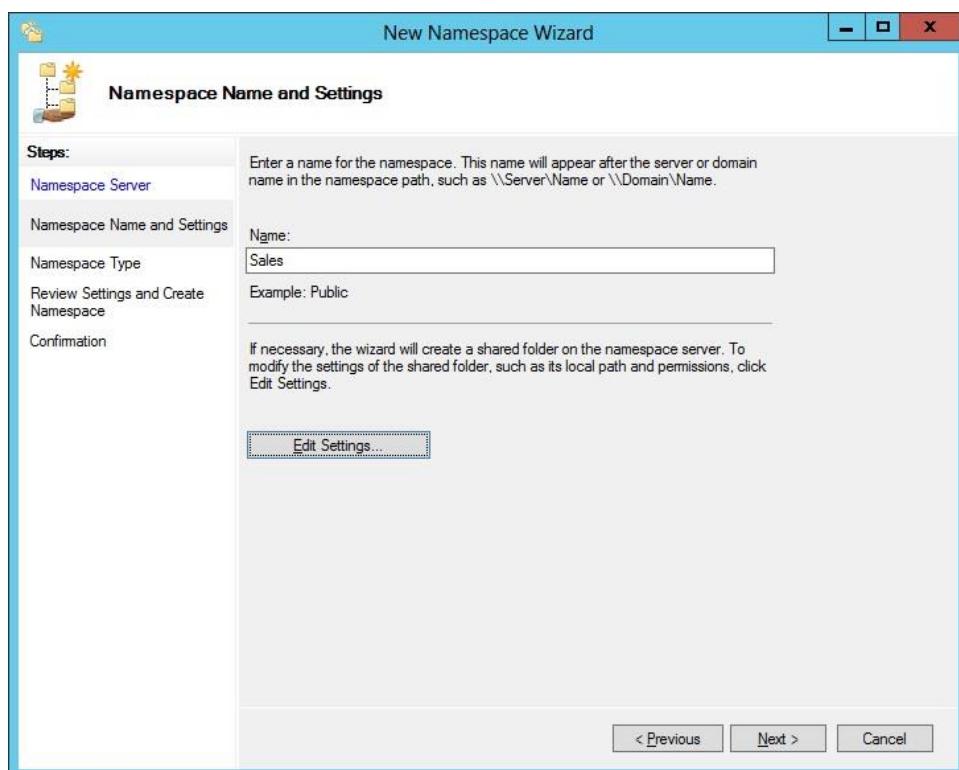
2. Right click Namespaces and Select **New Namespace**



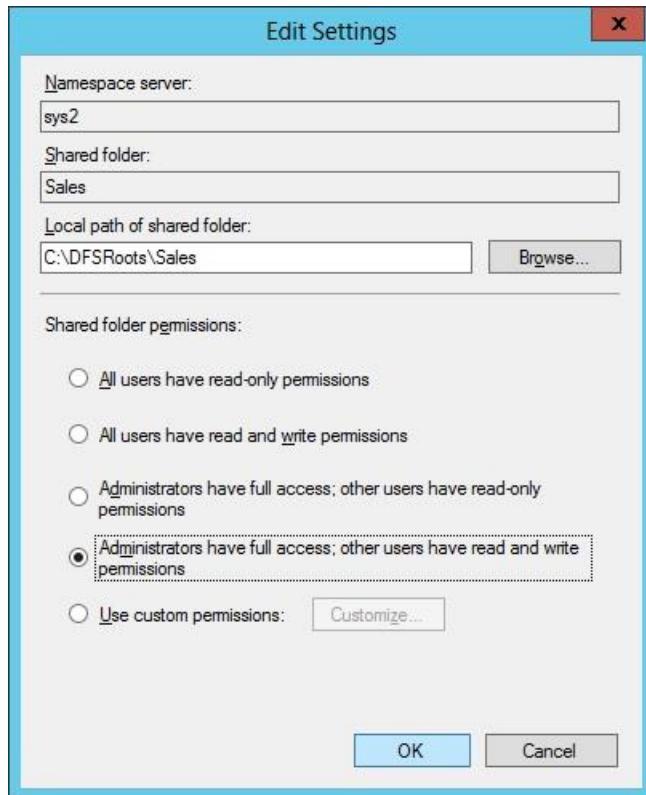
3. Enter the **Server Name** in which DFS Installed and Select **Next**.



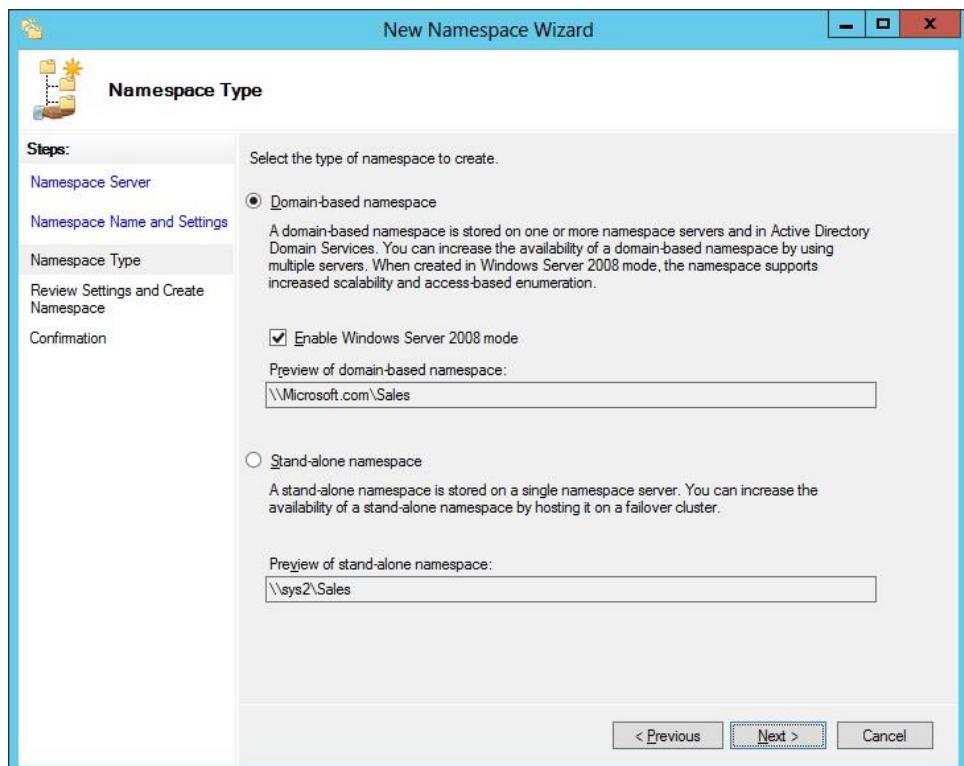
4. Enter Name for the **Namespace (Sales)**and click **Edit Settings**.

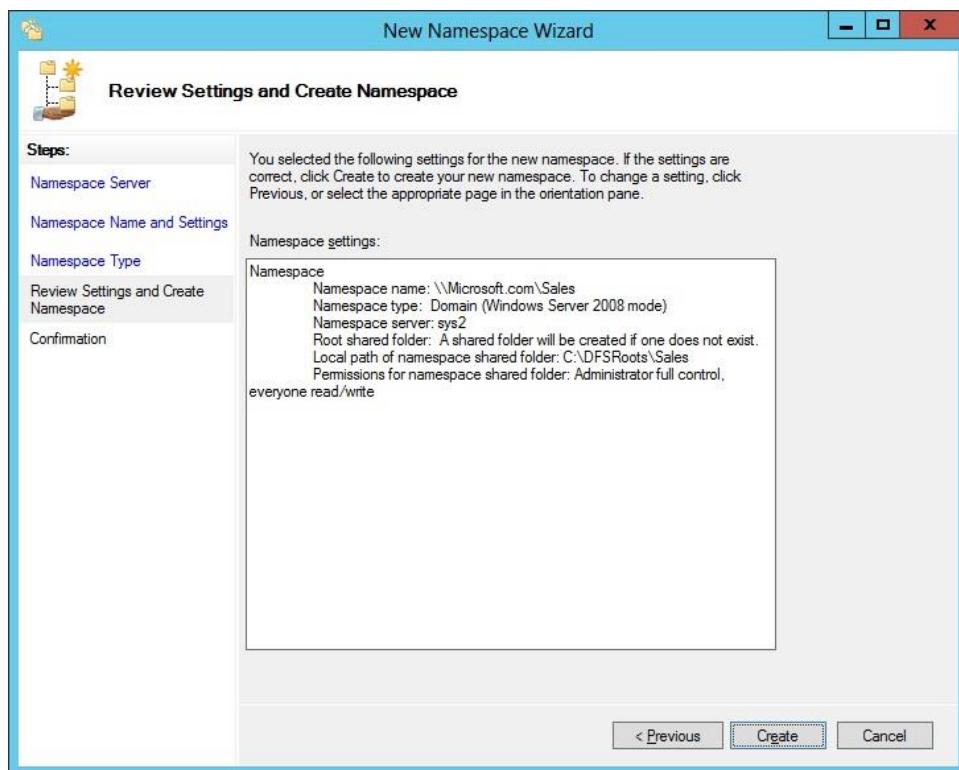
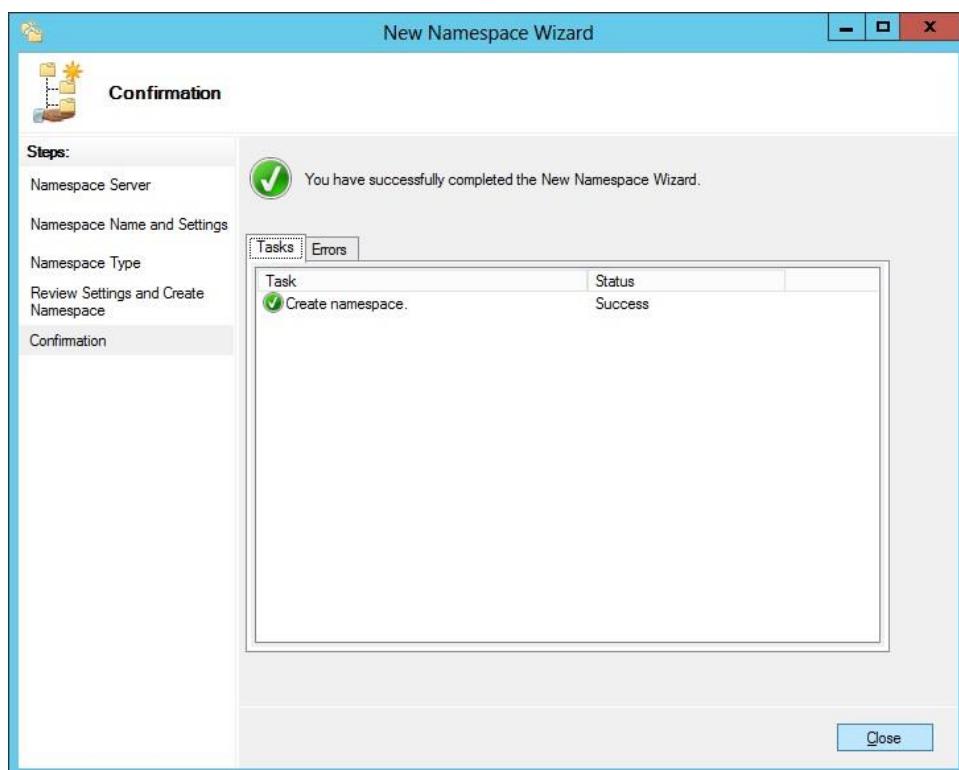


- 5. Select the Permissions **Administrators have full access, other users have read and write permissions**, and click Next.**



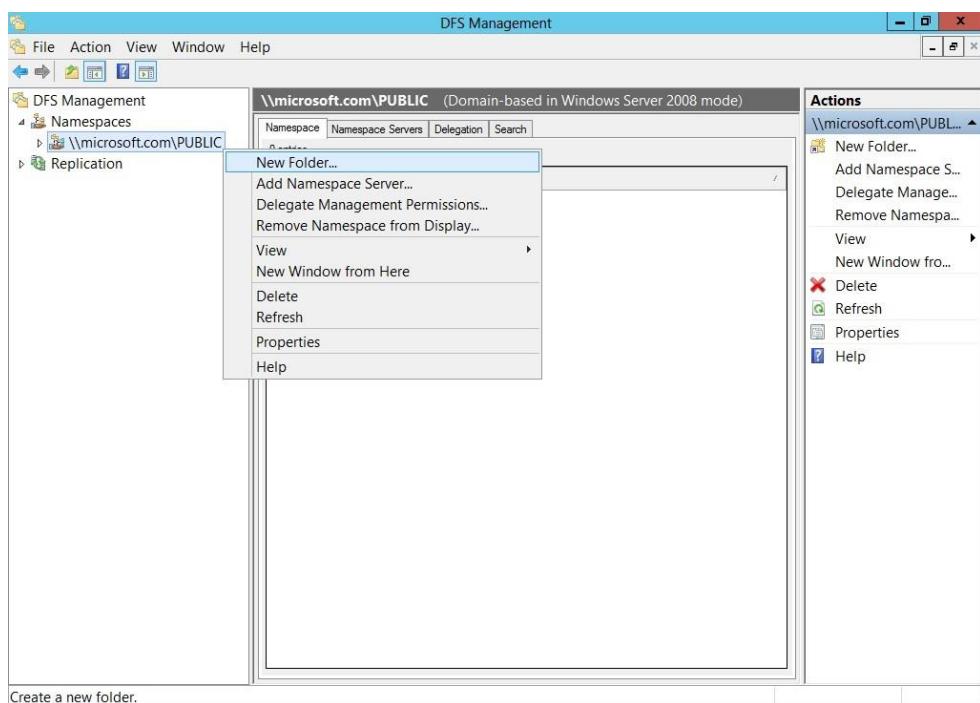
- 6. Select Domain Based Namespace → click Next**



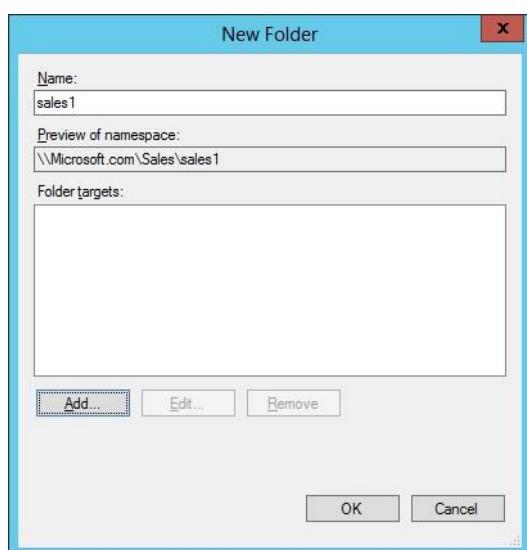
7. Click **Create**8. Select **Close**

Lab – 6: Configuring New Folder In Namespace

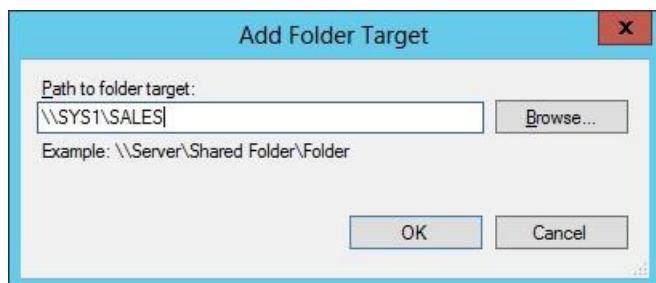
1. In **SYS1 (DC)** open any **Drive** which is formatted with **NTFS**
2. Create a shared folder (**Sales1**) and give permission (Ex:Read\Write for Everyone)
3. Similarly create a shared folder (**Sales2**) on **SYS2** and assign permission.
4. In **SYS2 (Member Server)** go to **DFS Management** and Expand Namespaces
5. Right click on namespace name and Select **New Folder**



6. Enter the Name (Ex: **Sales1**) and click Add.



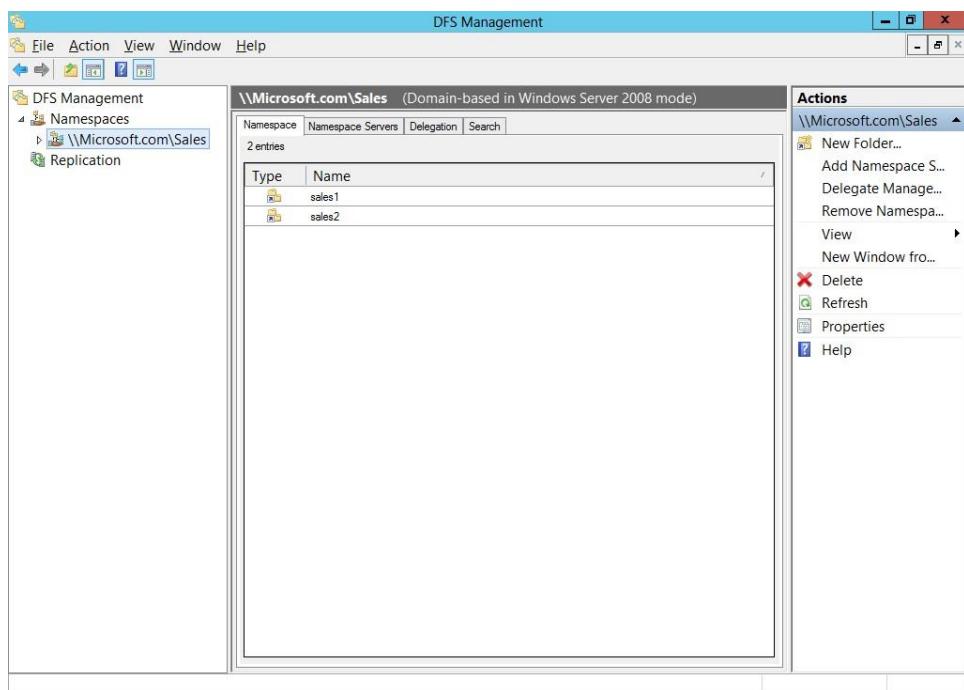
7. Enter the path for folder target (<\\SYS1\SALES>)&click OK.



8. Similarly add another DFS Folder (Ex: **Sales2**) and folder target <\\SYS2\Sales2>.

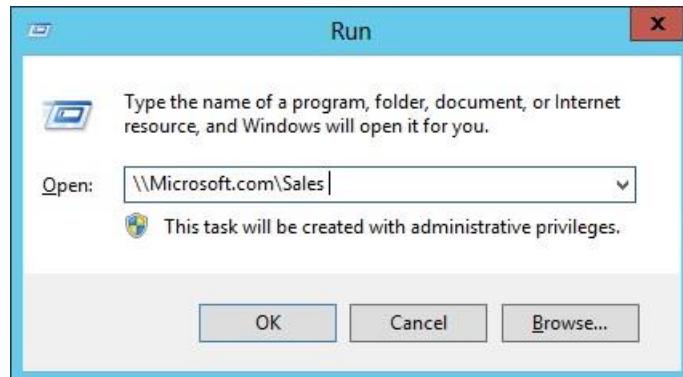


9. Go to DFS Management, Expand Namespaces, and select <\\Microsoft.com\Sales>.

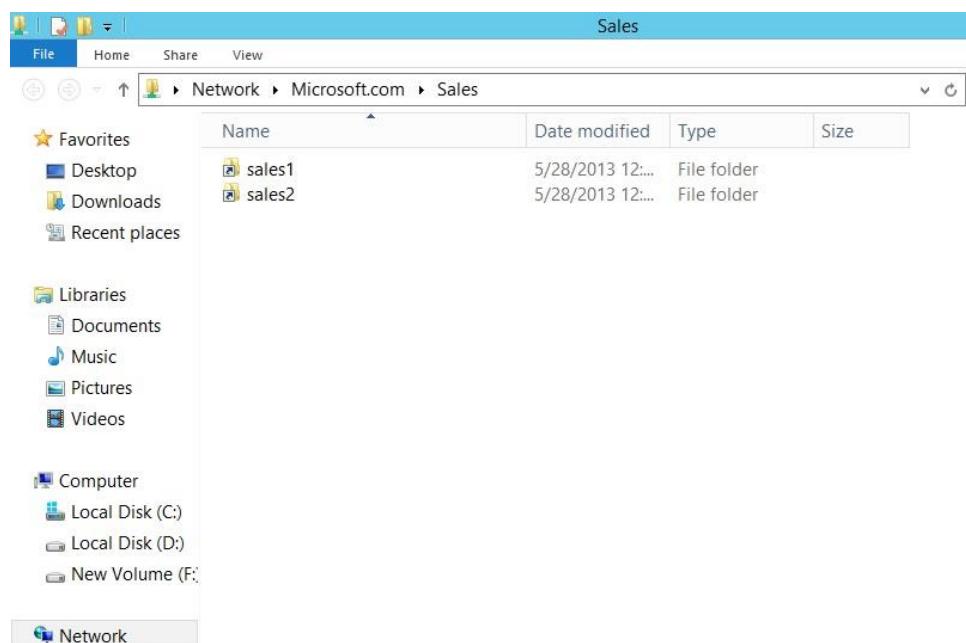


VERIFICATION:

1. In **SYS2** (Member Server), Go to Start, type Run in Search Apps, and select Run, type **\Domain name\Namespace Name** (Ex: **\Microsoft.com\Sales**)



2. It will display the contents (Folder) of Namespace.



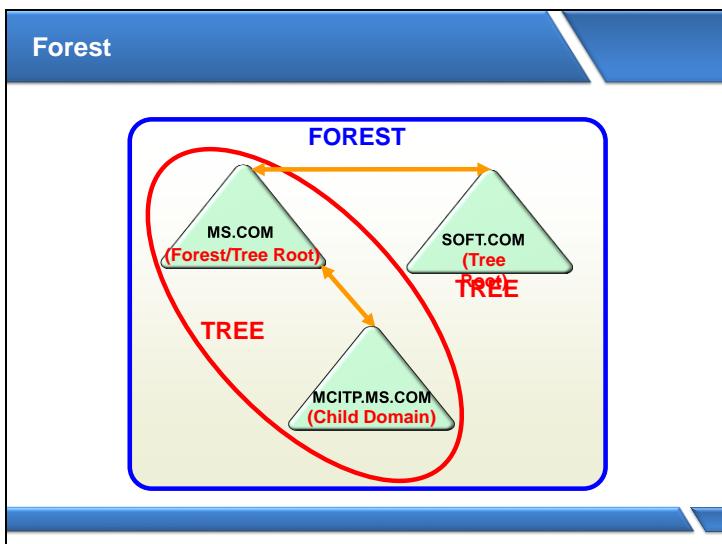
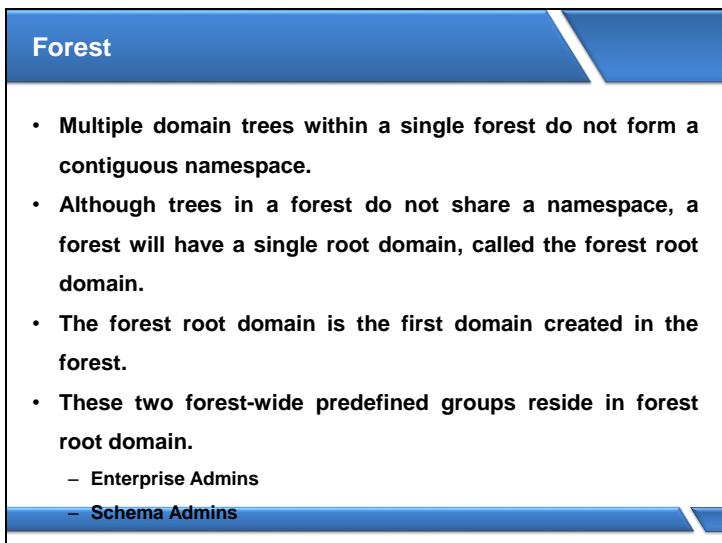
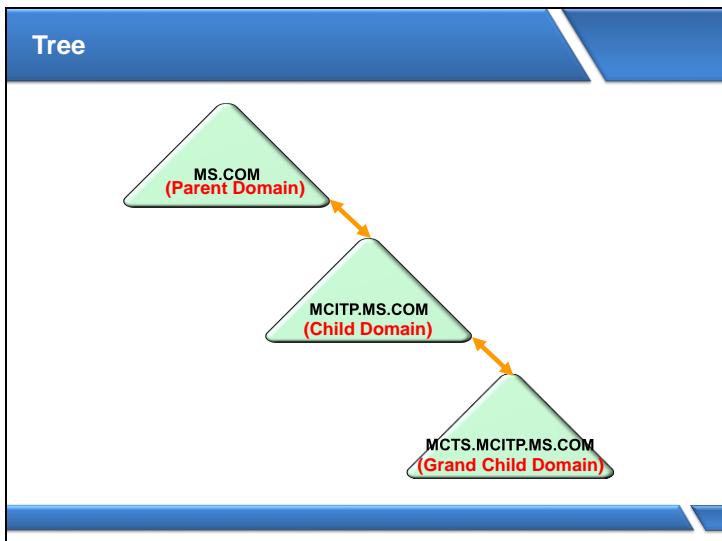
ACTIVE DIRECTORY

Additional Domain Controllers

- If you already have one domain controller in a domain, you can add additional domain controllers to the domain to improve the availability and reliability of network services.
- Adding additional domain controllers can help provide fault tolerance, balance the load of existing domain controllers, and provide additional infrastructure support to sites.
- The replication type between two read/write dc's is multi master replication.

Tree

- Tree is a set of one or more domains with contiguous names.
- If more than one domain exists, you can combine the multiple domains into hierarchical tree structures.
- The first domain created is the root domain of the first tree.
- Other domains in the same domain tree are child domains.
- A domain immediately above another domain in the same domain tree is its parent.



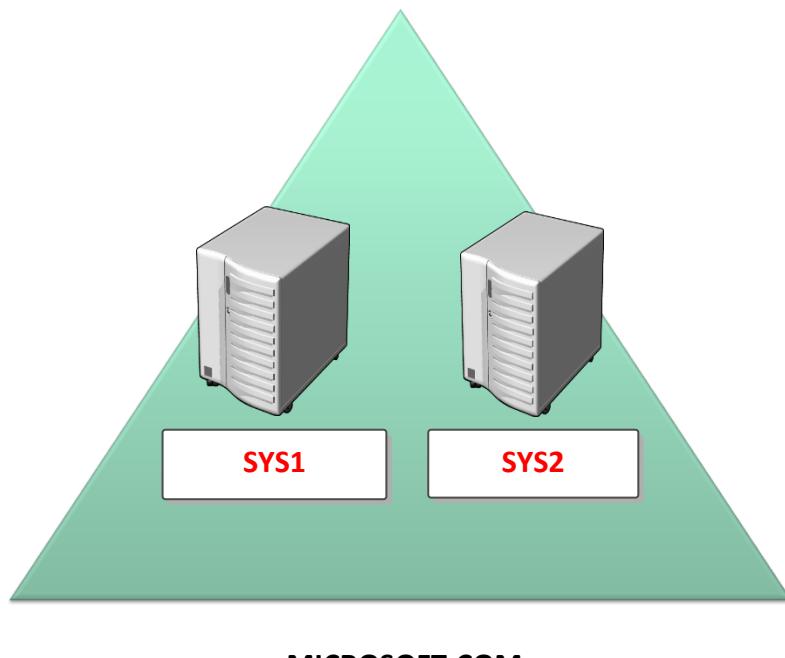
LOGICAL STRUCTURE OF ACTIVE DIRECTORY

CONFIGURING ADDITIONAL DOMAIN CONTROLLER

Pre-requisites:

Before working on this lab, you must have

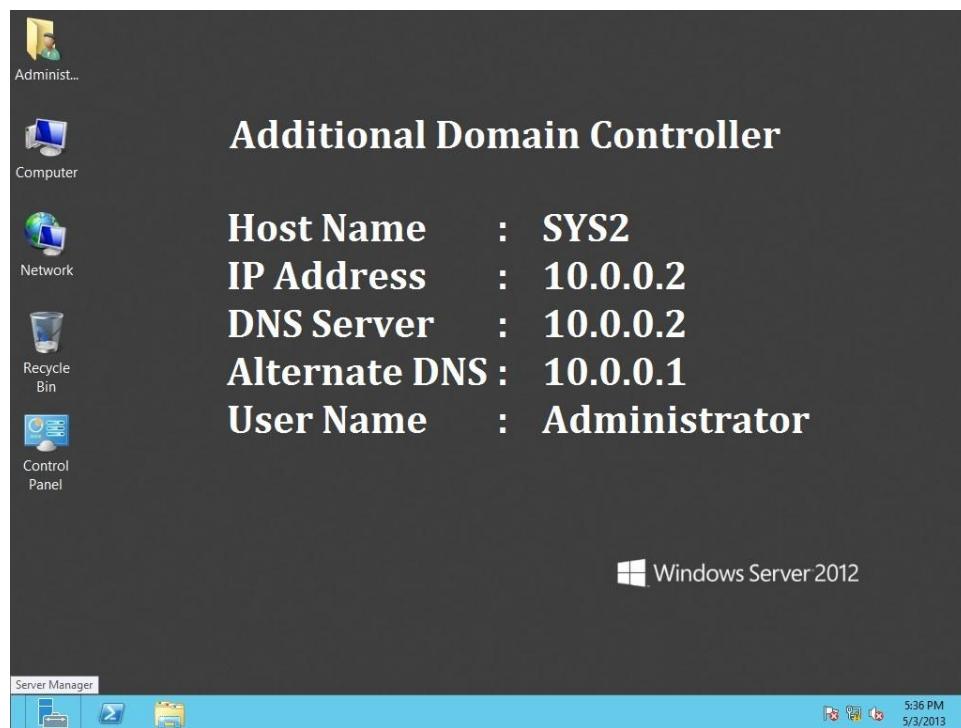
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server.



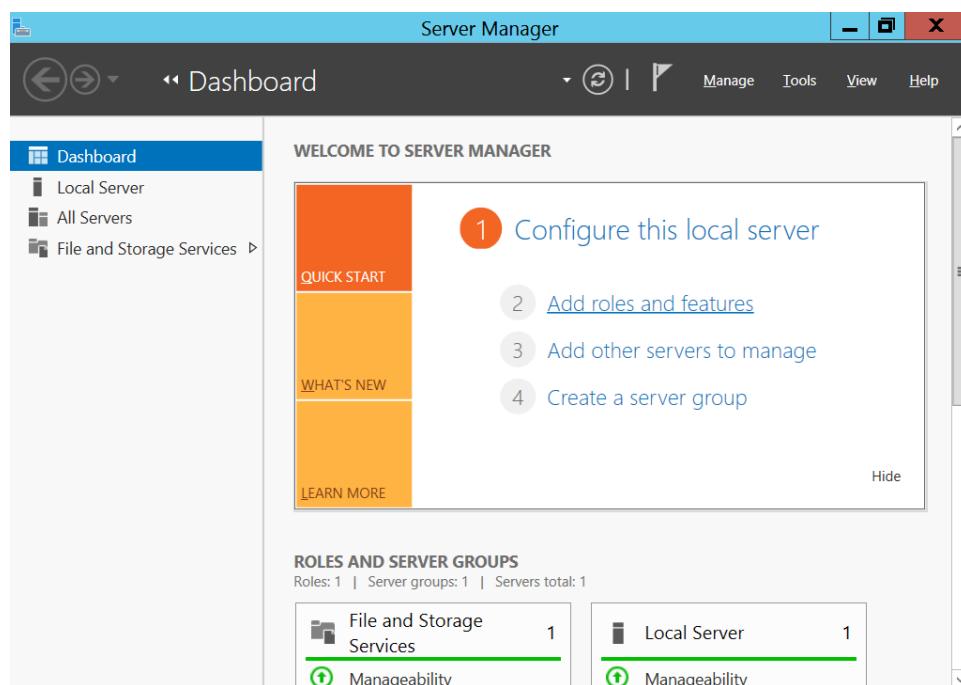
SYS1	SYS2
Domain Controller	Additional Domain controller
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Alternate DNS	-----
	10.0.0.2
	255.0.0.0
	10.0.0.2
	10.0.0.1

Lab – 1: Configuring Additional Domain Controller

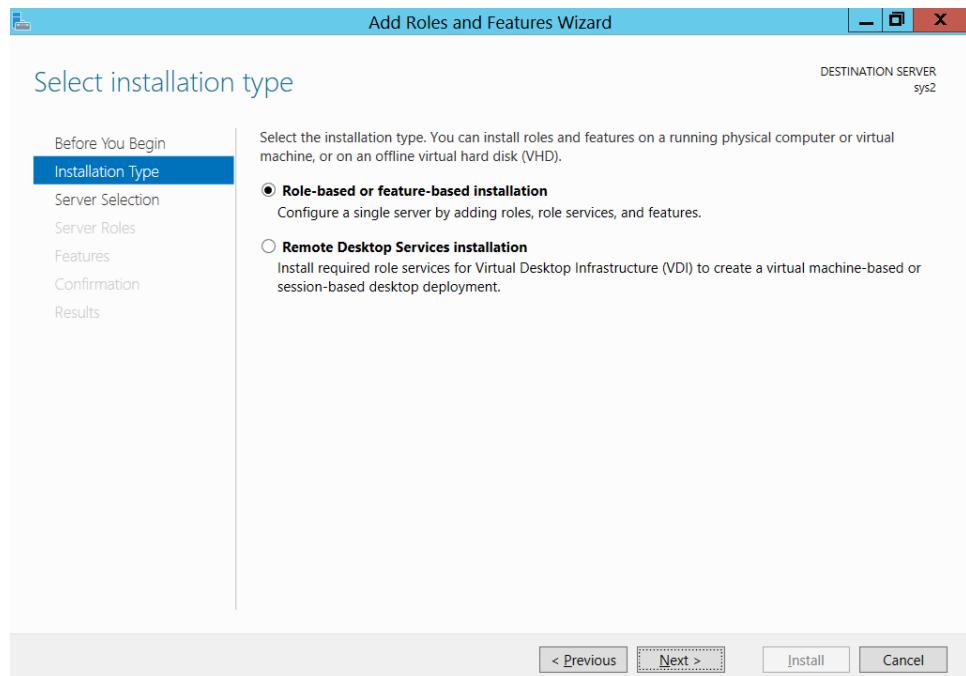
1. Log in as Administrator to the **Workgroup Computer**.
2. Assign **IP Address** and preferred **DNS Server Address**
3. Click Server Manager



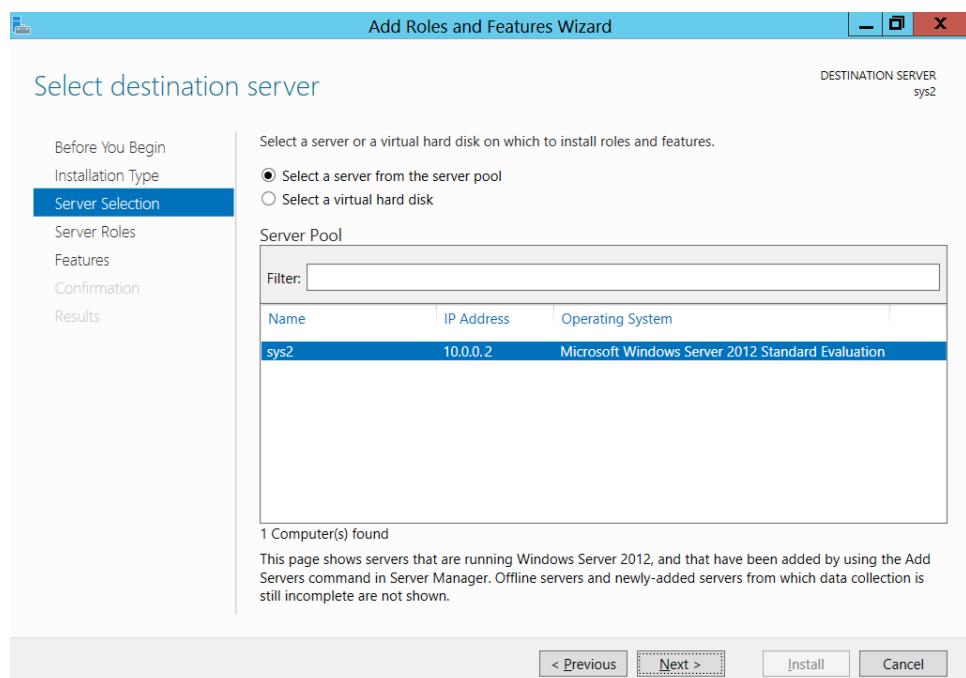
4. In Server Manager Dashboard, Click **Add roles and features**.



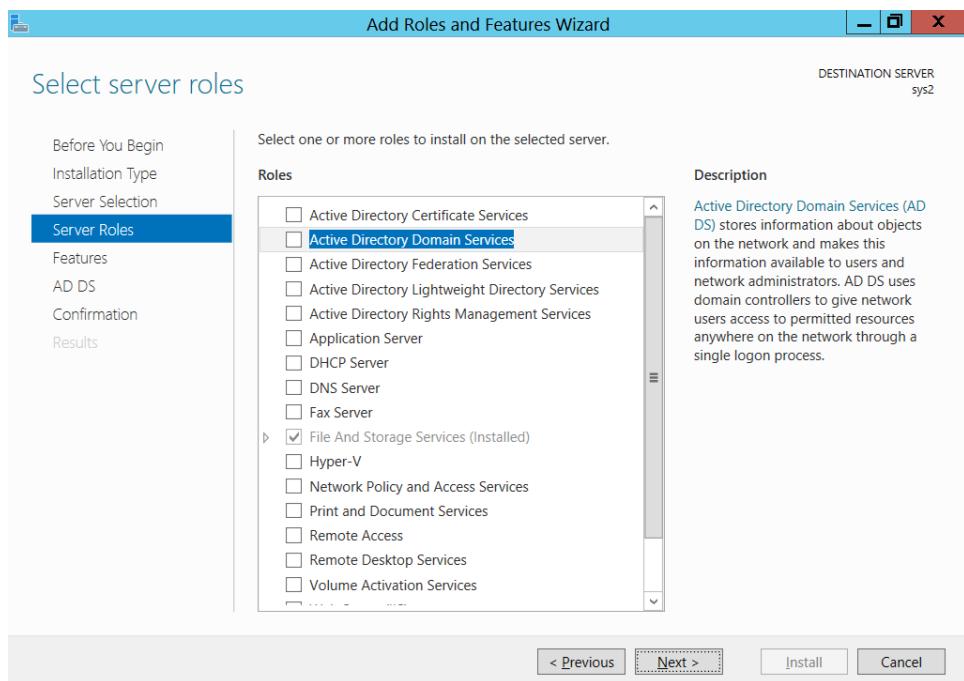
5. In Before you begin page, click **Next**, In Select installation type, select **Role-based or feature-based installation**, click **Next**.



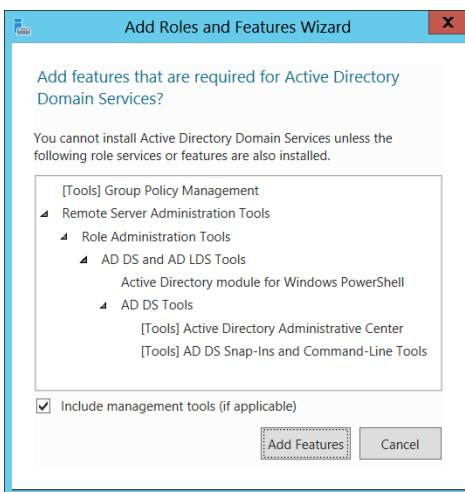
6. In Select destination server, from Server Pool select **SYS2**,click**Next**.



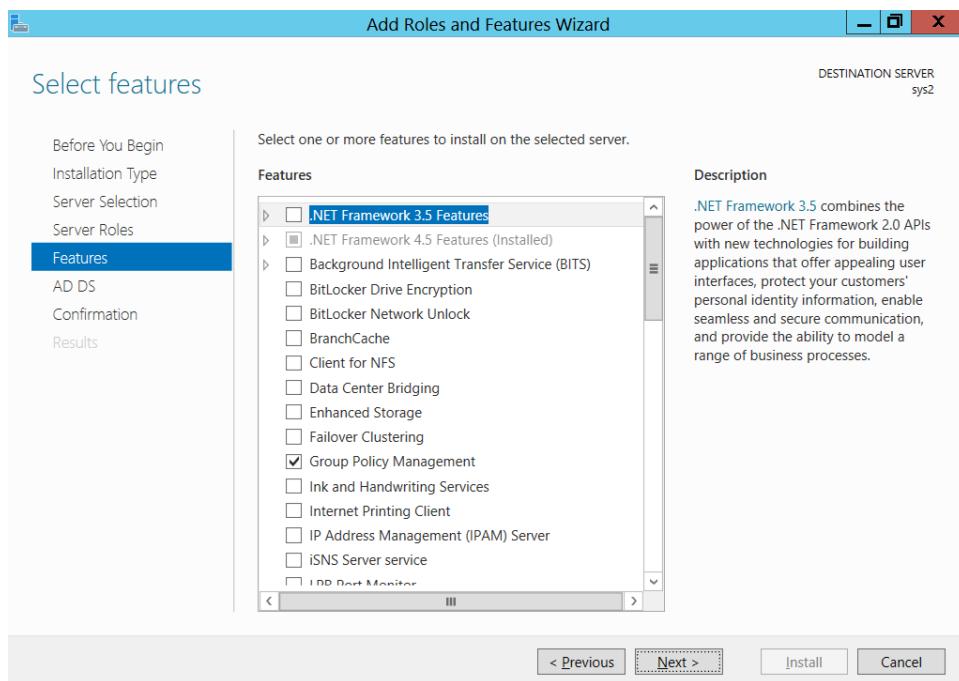
7. In Roles, check the box **Active Directory Domain Services**.



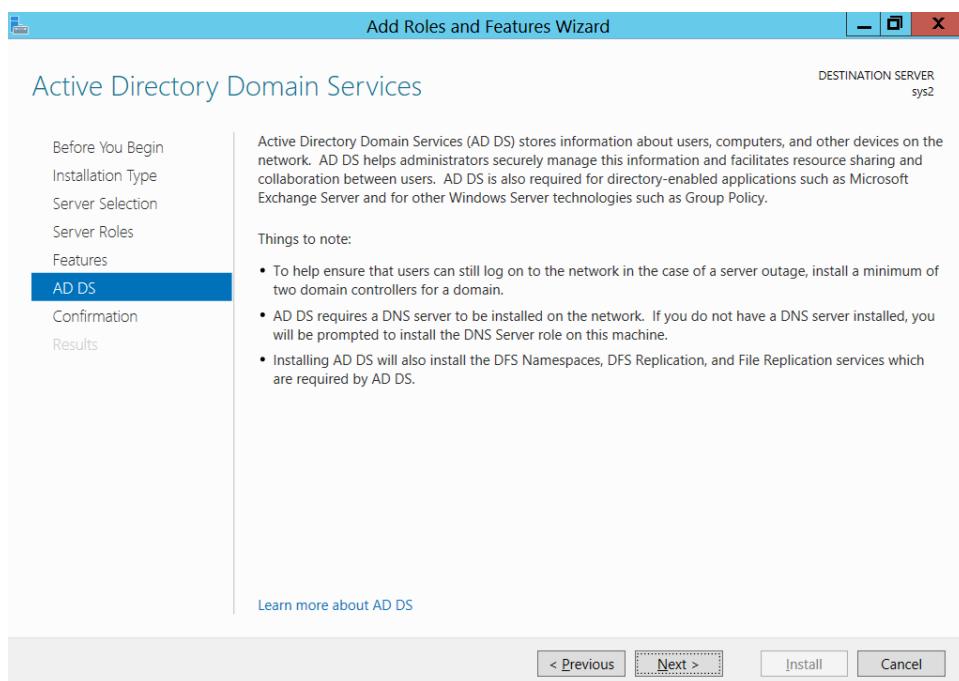
8. Click **Add Features**, to install the required features for Active Directory Domain Services. Click **Next**.



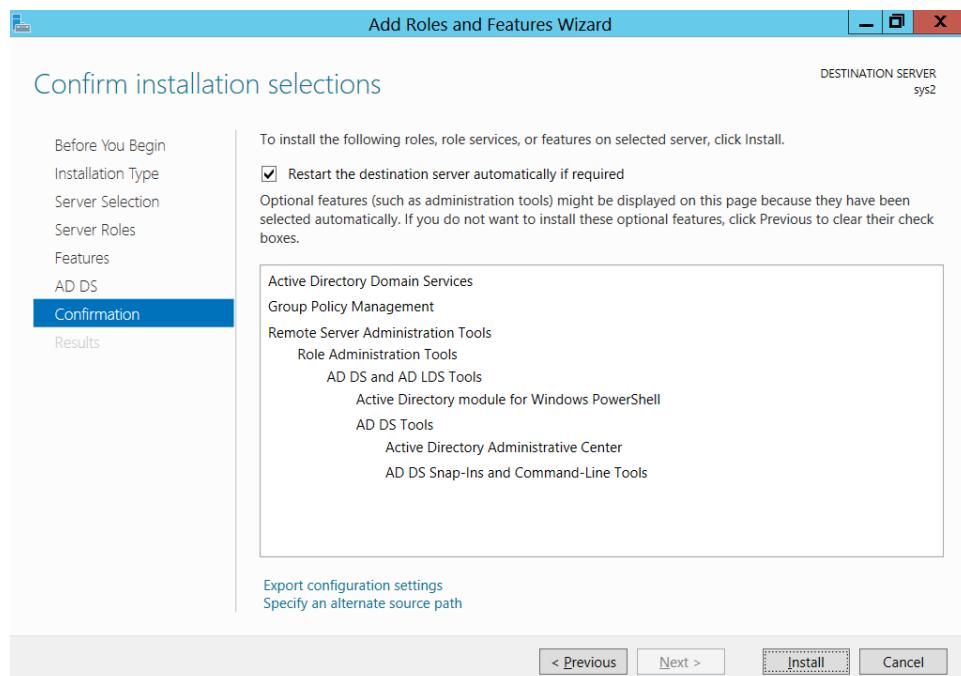
9. In Select features wizard, click **Next.**



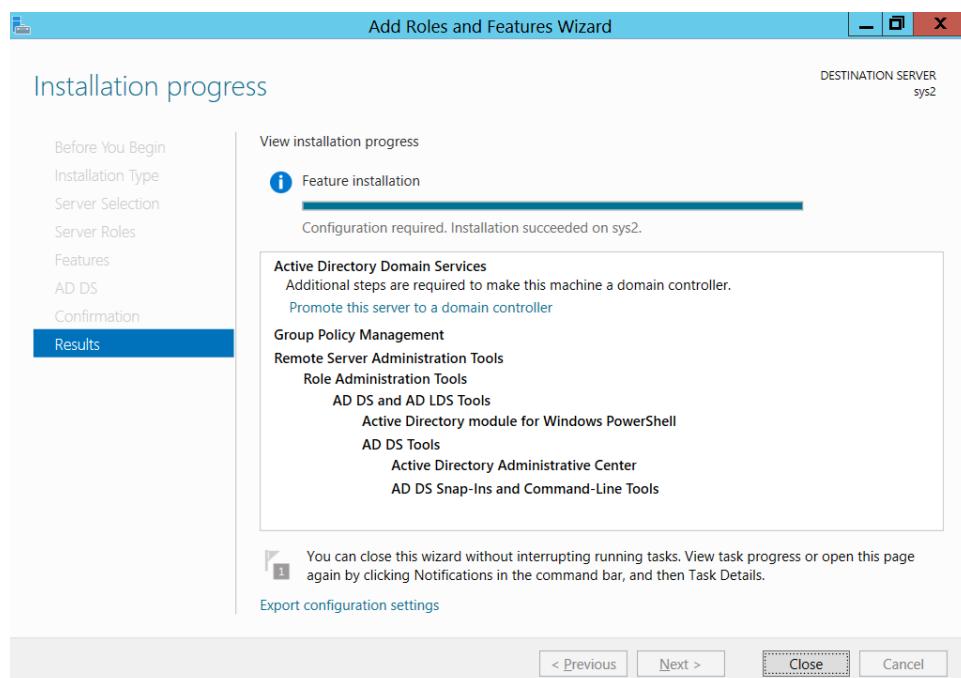
10. In Active Directory Domain Services wizard, click **Next.**



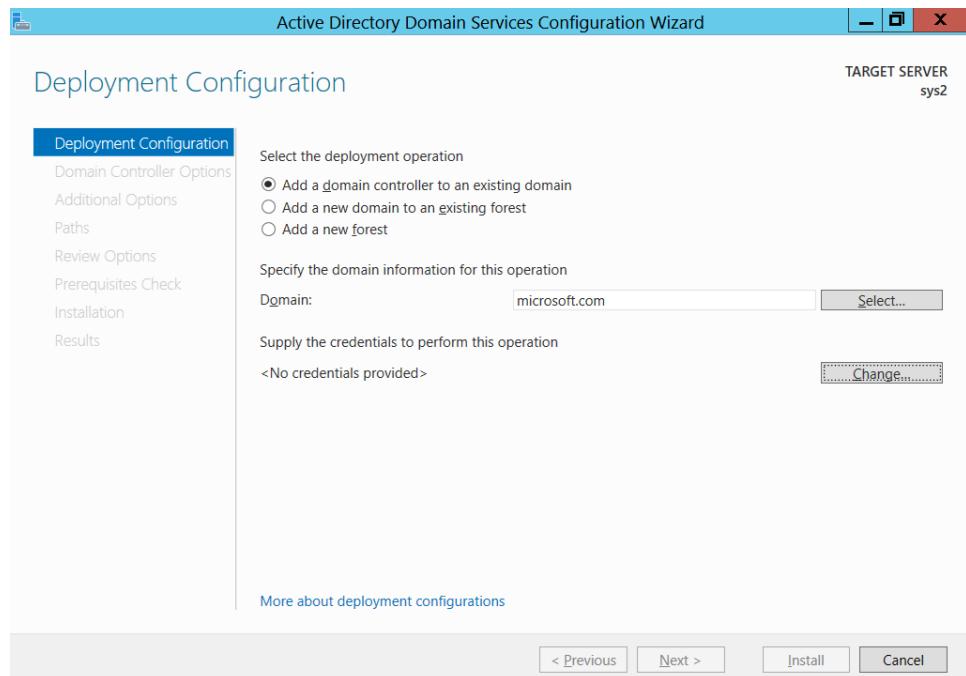
11. Check the box **Restart the destination server automatically if required. Click **Install**.**



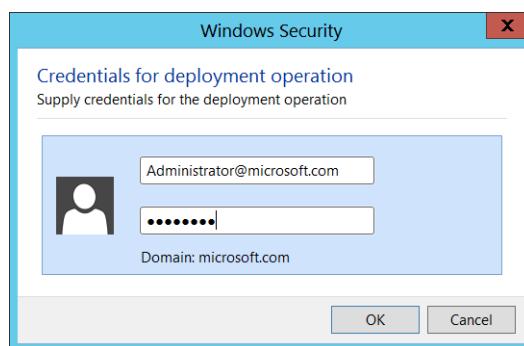
12. Click **Promote this server to a domain controller.**



13. In Deployment Configuration wizard, select **Add a domain controller to an existing domain**, enter the Domain (Ex: **Microsoft.com**) and click **Change**.

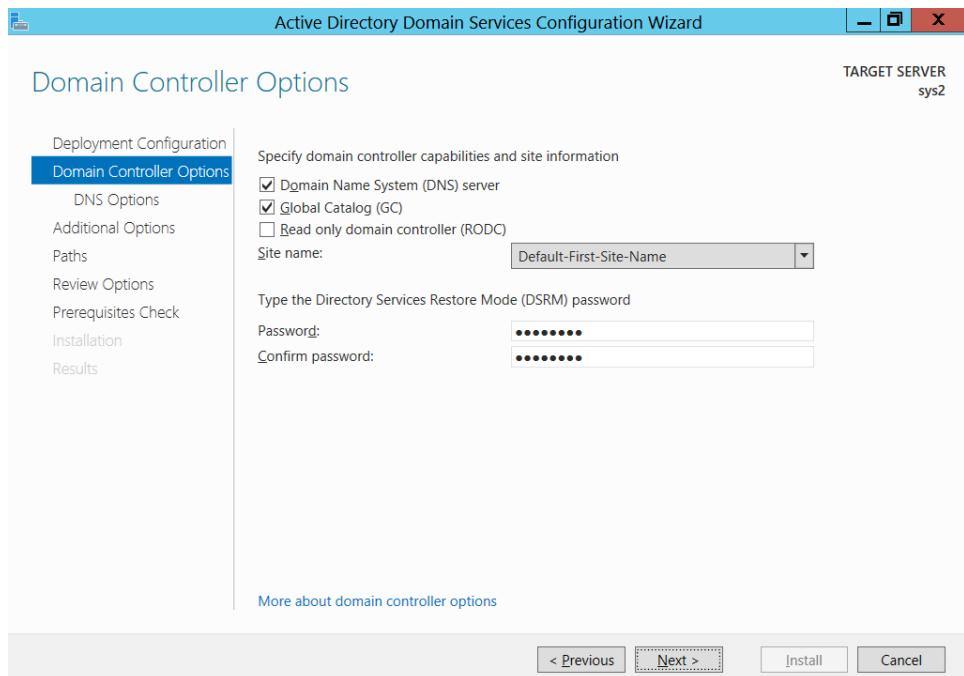


14. Enter User Name: **Administrator@microsoft.com** and Password, click **OK**.

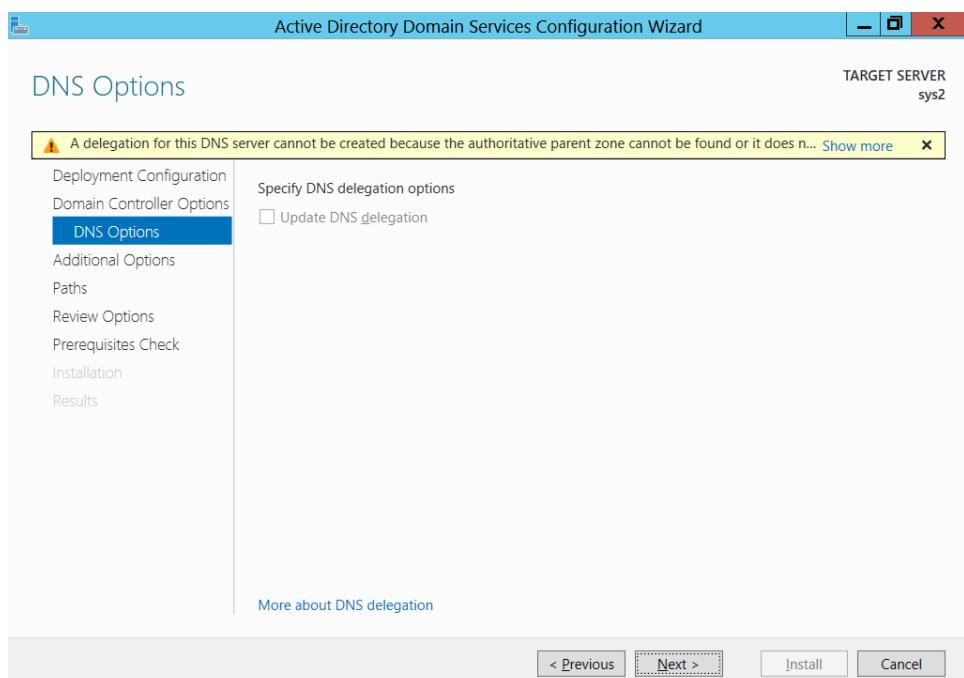


15. Click **Next**.

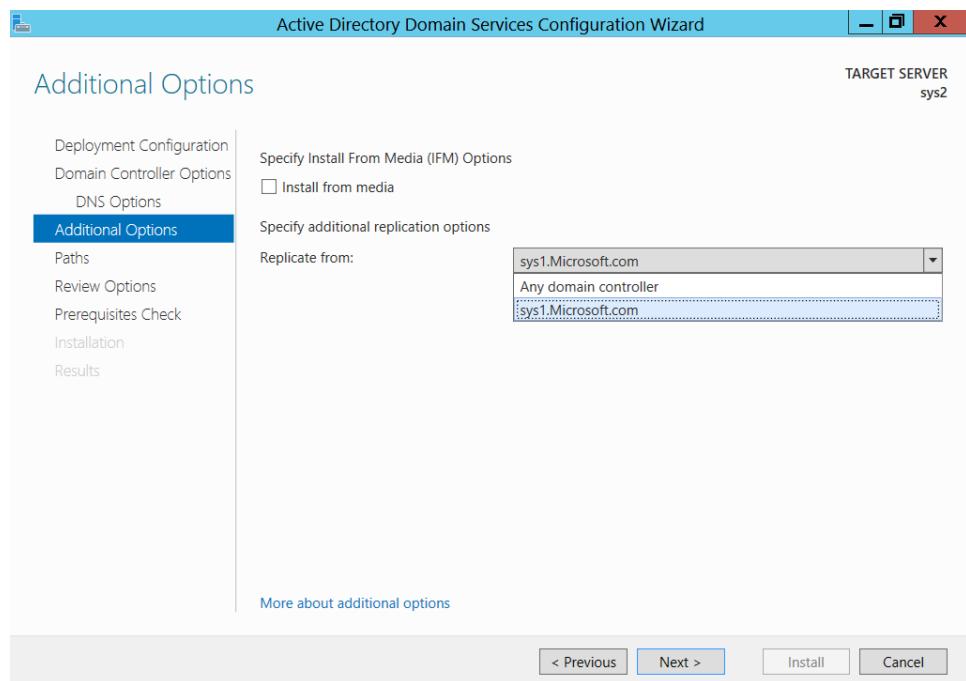
16. In Domain Controller Options, review the default settings, and type the Directory Services Restore Mode **Password** and **Confirm password** and click **Next**.



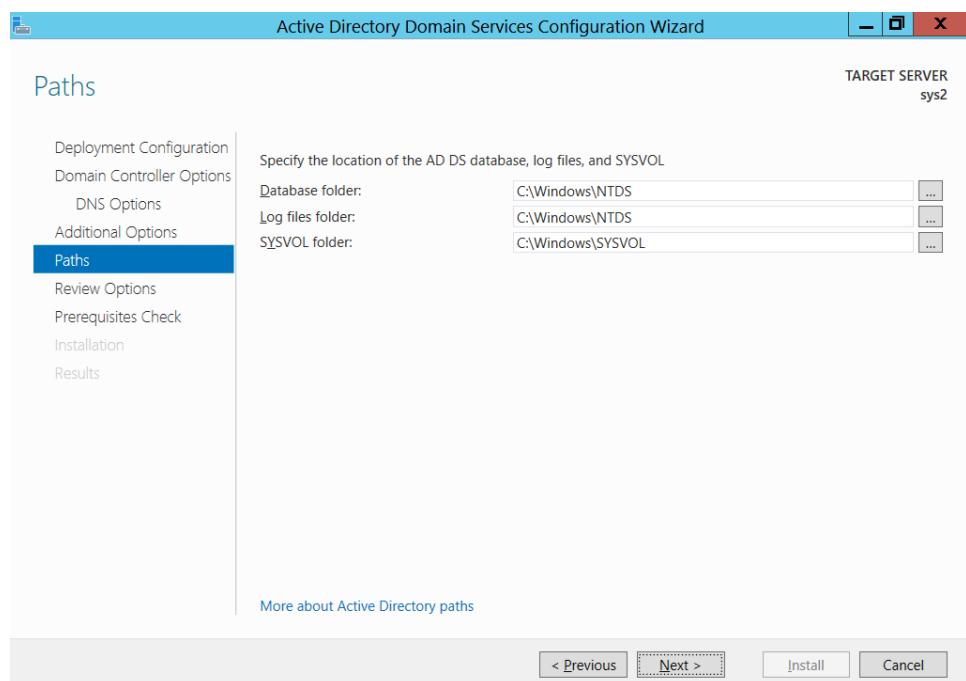
17. On DNS Options page, click **Next**.



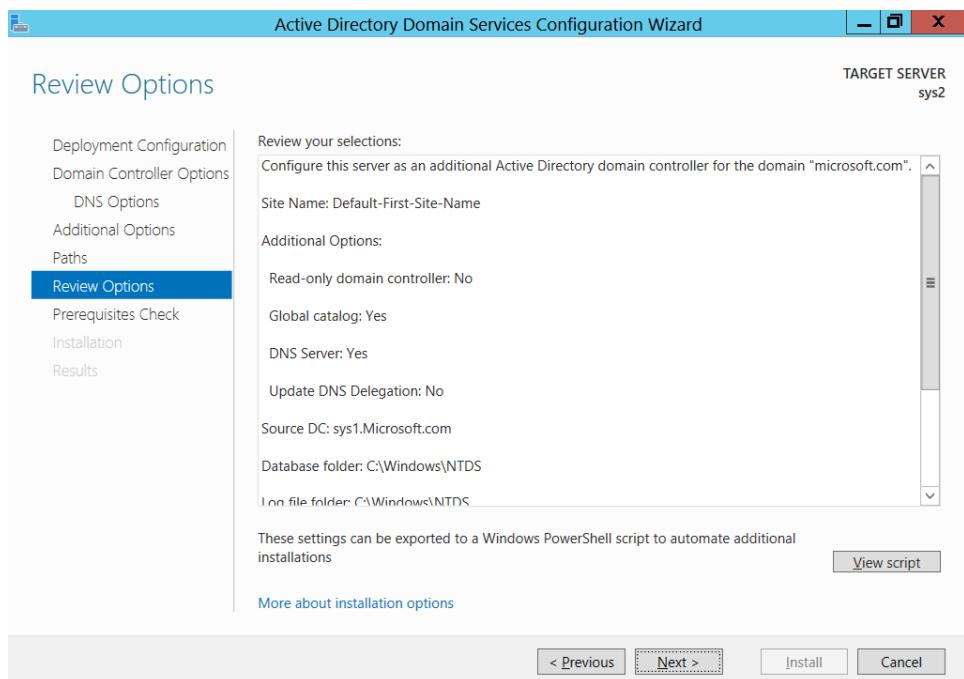
18. In Additional Options Page, select Replicate from **Sys1.Microsoft.com**, click **Next**.



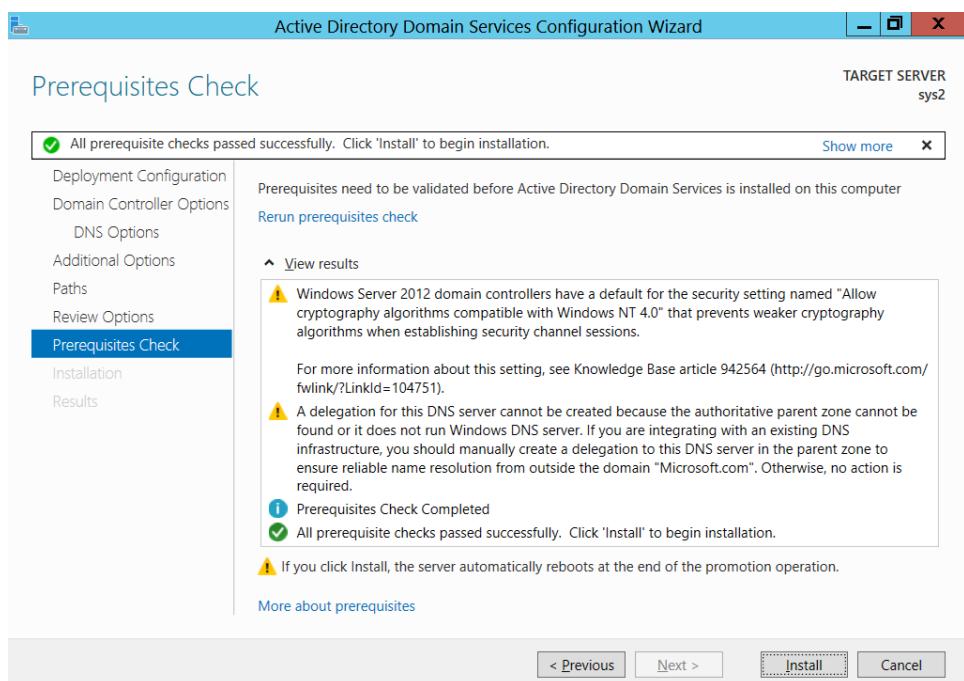
19. Verify the location of the AD DS database, log files, and SYSVOL, click **Next**.



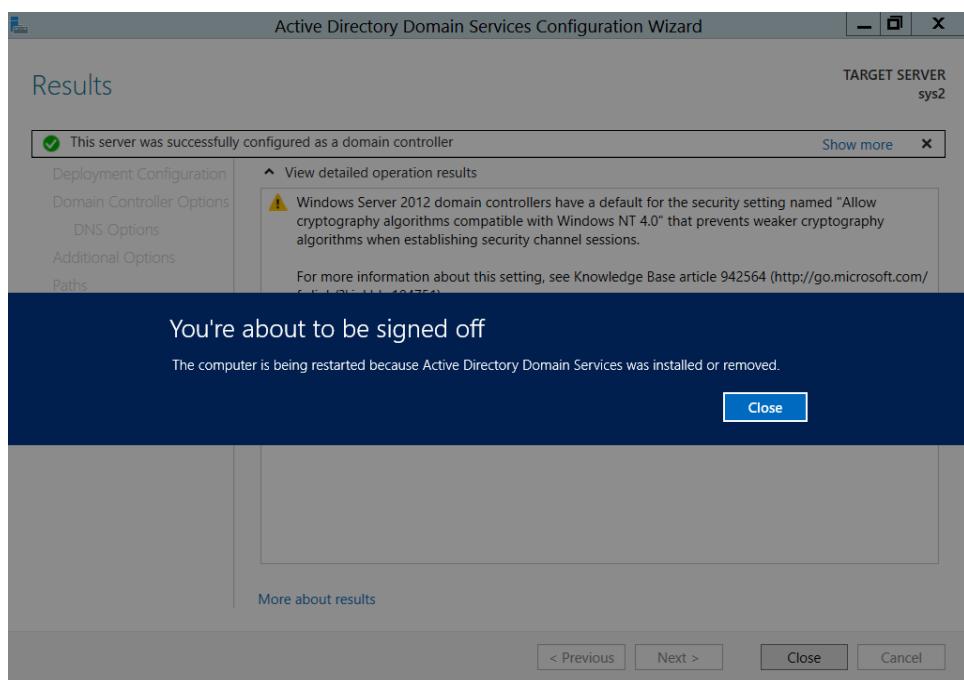
20. Review the Summary and click **Next.**



21. Click **Install to begin installation.**



22. The computer restarts as a part of Active Directory Domain Services installation.



23. After restarting the computer **Active directory** will be installed.

Verification:

1. Click Start → Run and type **CMD**.
2. Type **NET ACCOUNTS** and verify for **Backup** in Computer role.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.Micr0soft>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

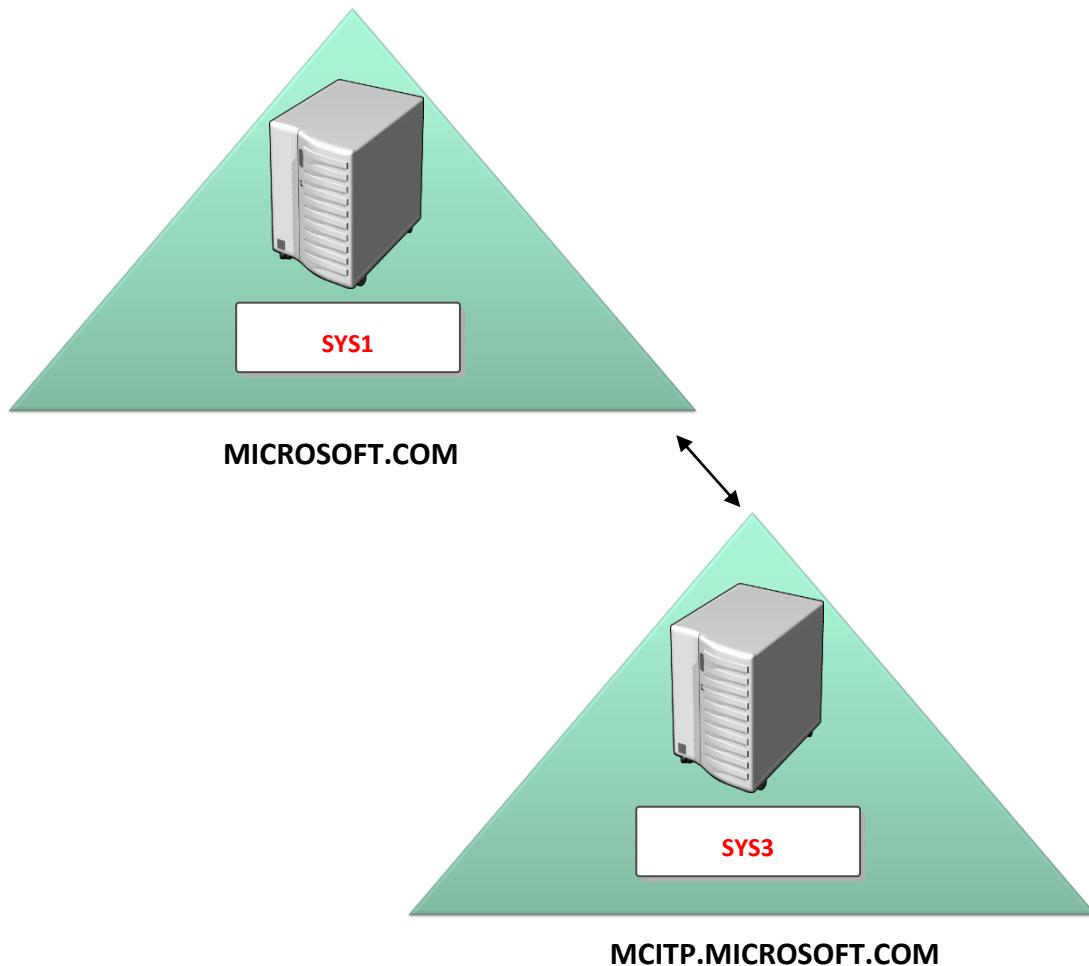
C:\Users\Administrator.Micr0soft>
```

CONFIGURING CHILD DOMAIN

Pre-requisites:

Before working on this lab, you must have

1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server.



SYS1

Domain Controller

IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Alternate DNS	-----

SYS3

Child Domain controller

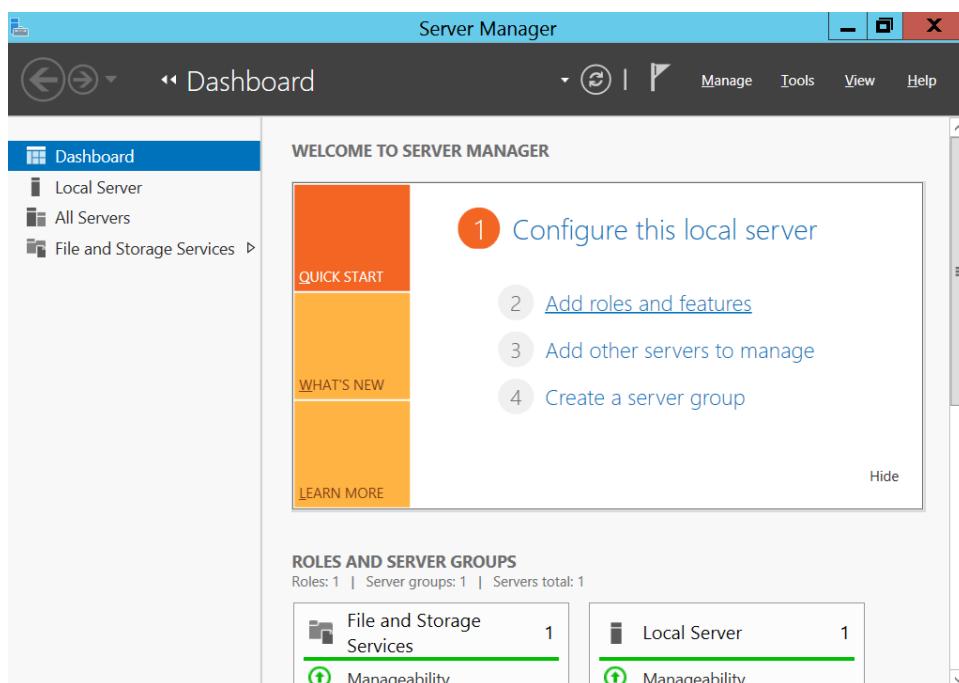
IP Address	10.0.0.3
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.3
Alternate DNS	10.0.0.1

Lab – 2: Configuring Child Domain

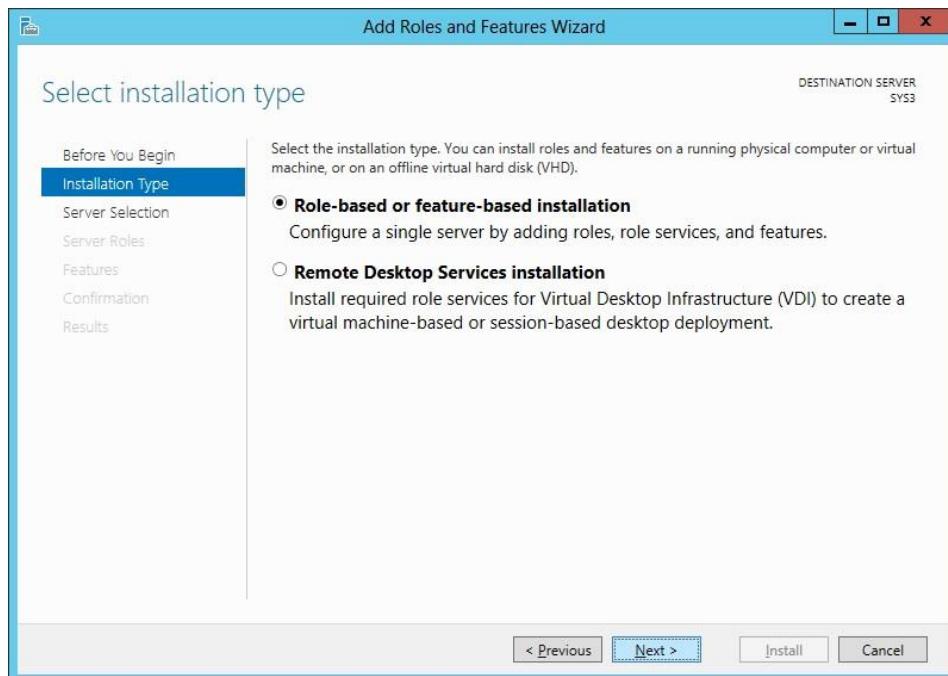
1. Log in as Administrator to the **Workgroup Computer**.
2. Assign **IP Address** and preferred **DNS Server Address**
3. Click **Server Manager**



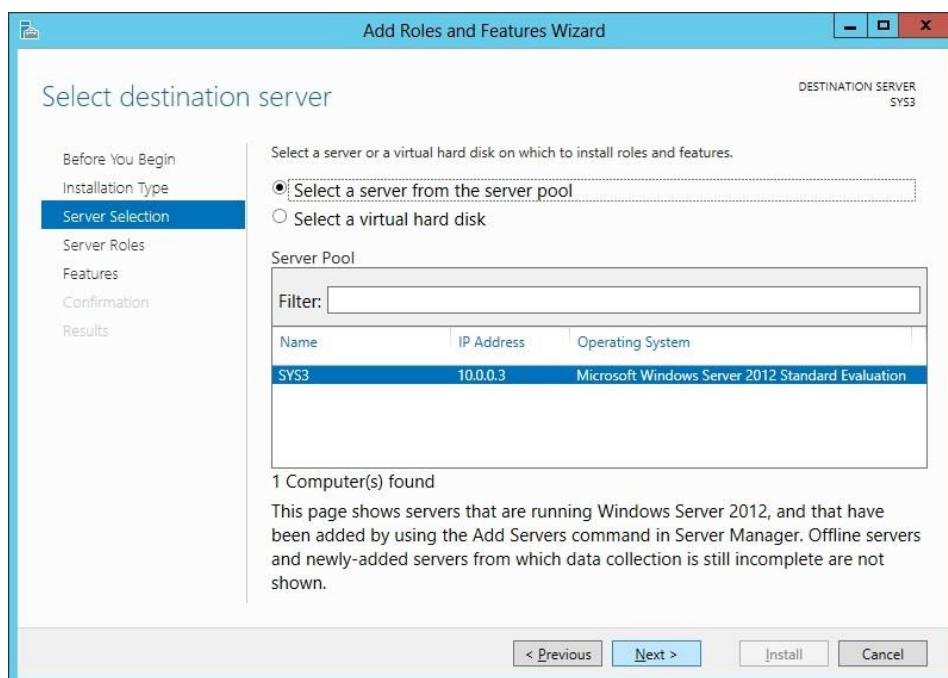
4. In Server Manager Dashboard, Click **Add roles and features**.



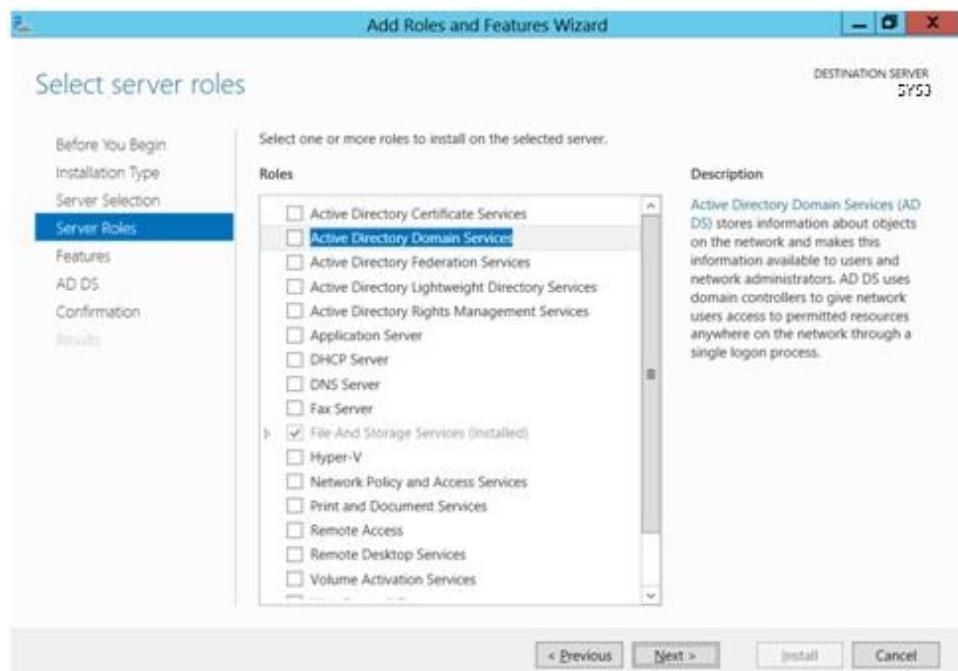
5. In Before you begin page, click **Next**, In Select installation type, select **Role-based or feature-based installation**, and click **Next**.



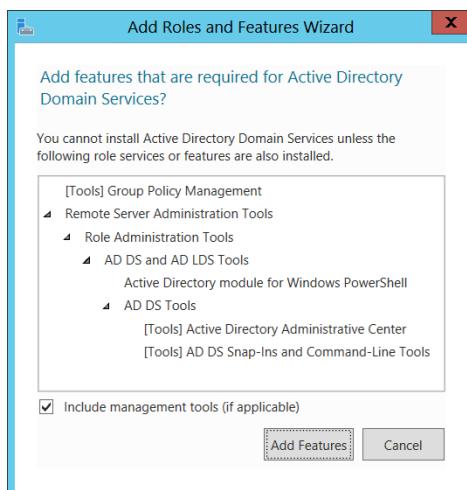
6. In Select destination server, from Server Pool select **SYS2**, click **Next**.

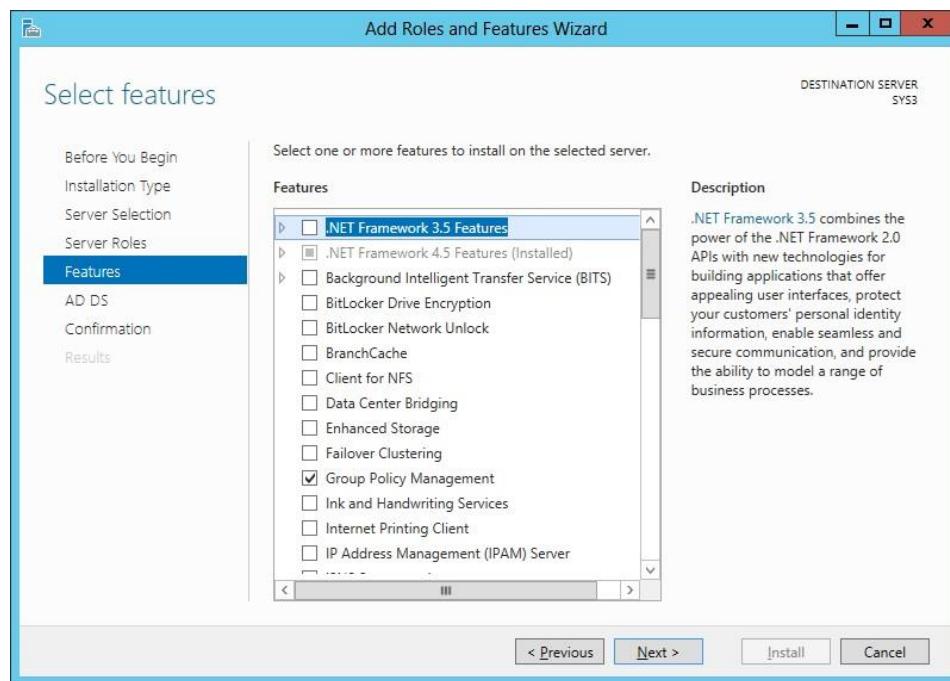
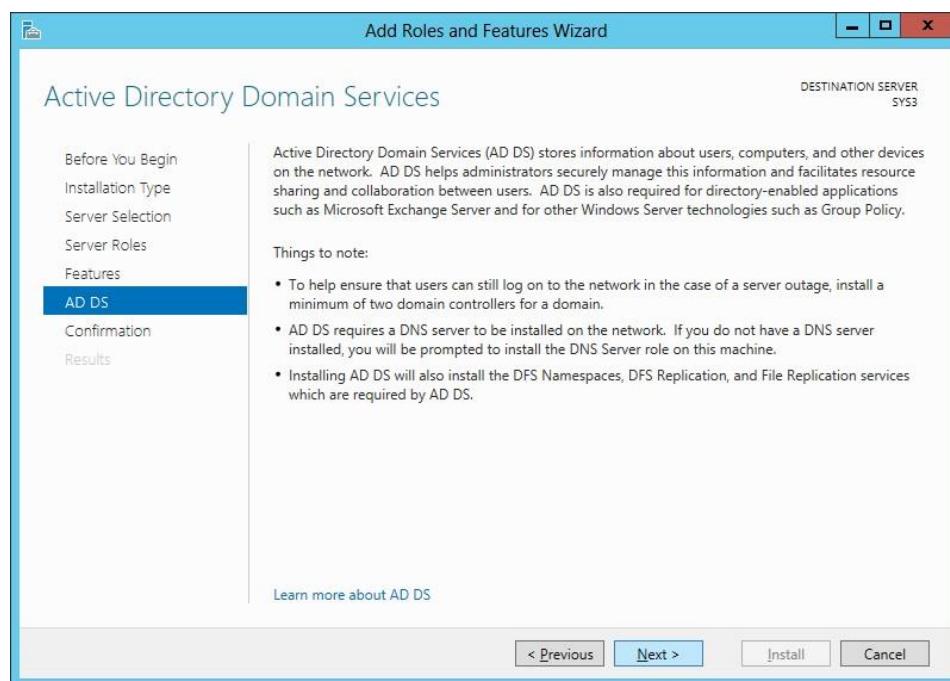


7. In Roles, check the box **Active Directory Domain Services**.

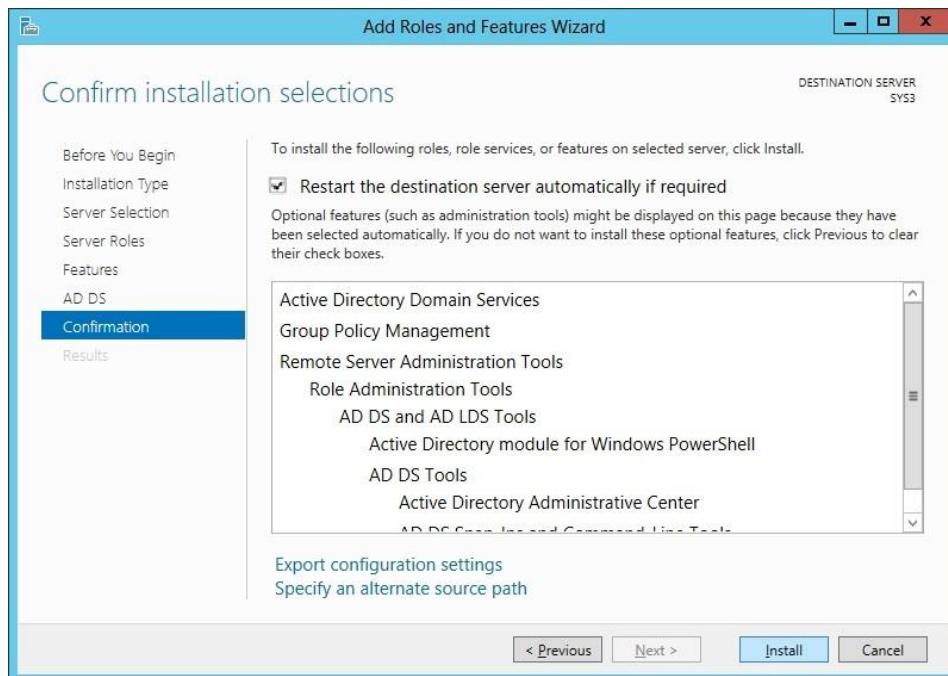


8. Click **Add Features**, to install the required features for Active Directory Domain Services. Click **Next**.

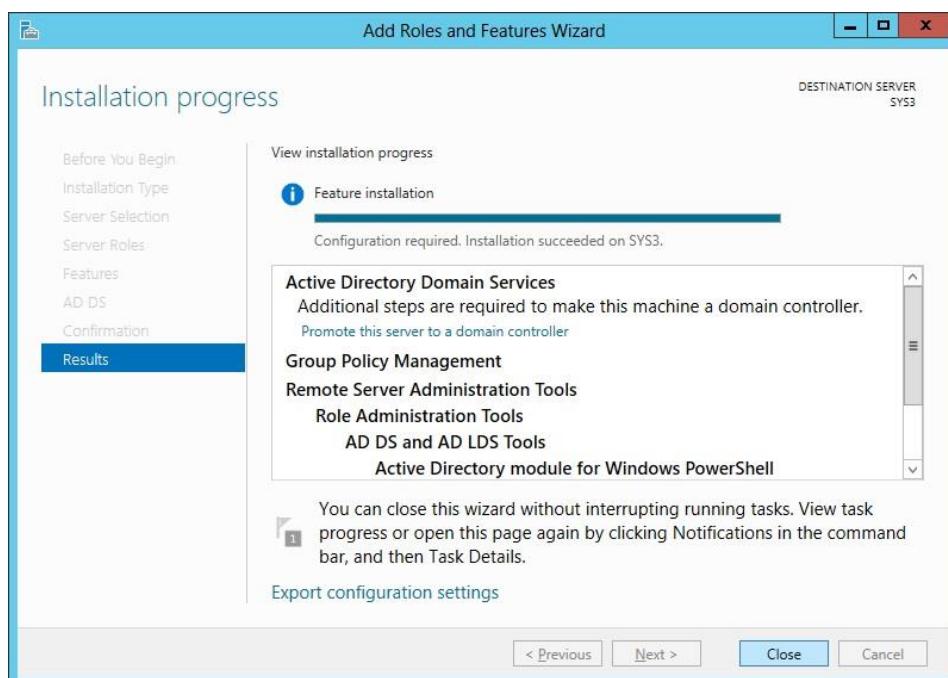


9. In Select features wizard, click **Next**.10. In Active Directory Domain Services wizard, click **Next**.

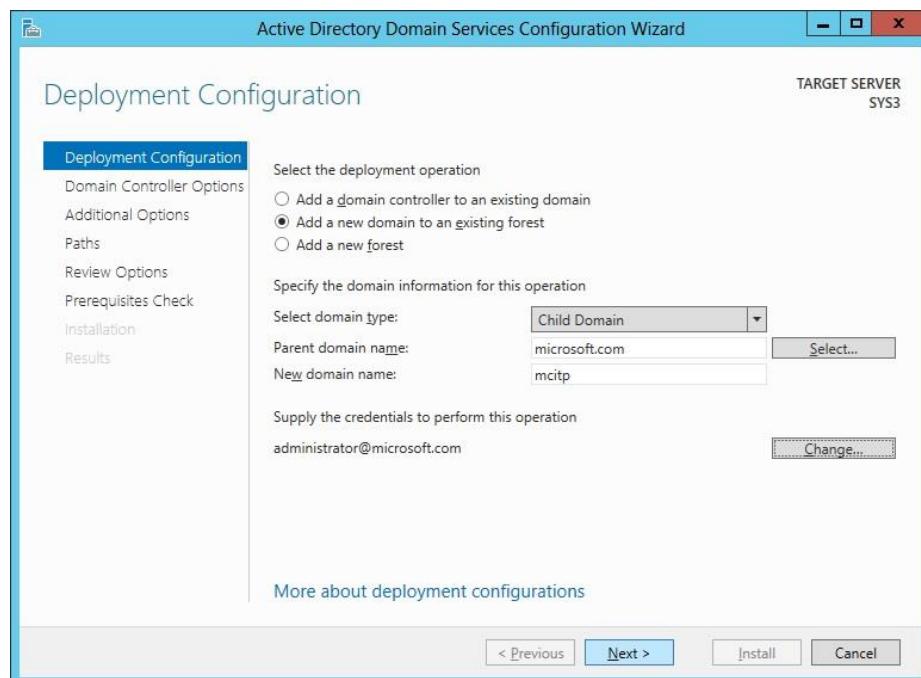
11. Check the box **Restart the destination server automatically if required**. Click **Install**.



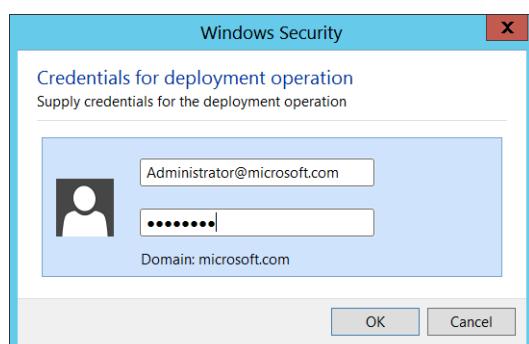
12. Click **Promote this server to a domain controller**.



13. In Deployment Configuration wizard, select **Add a new domain to an existing forest**, select domain type **Child Domain**, enter the Parent domain name (Ex: **Microsoft.com**) and New domain name (Ex: **mcitp**), and click **Change**.

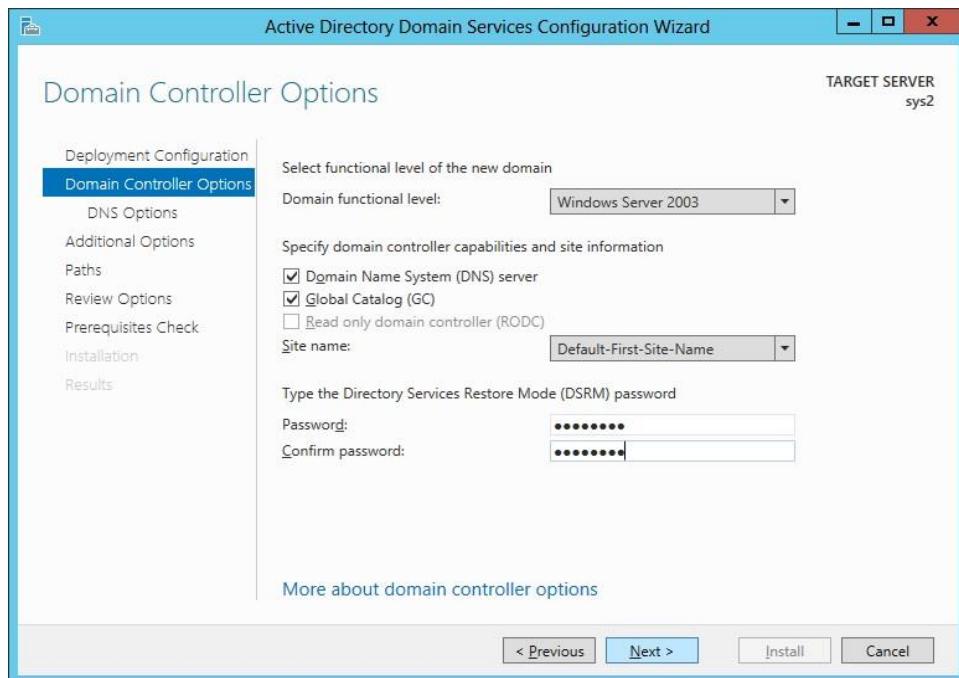


14. Enter User Name: Administrator@microsoft.com and Password, click **OK**.

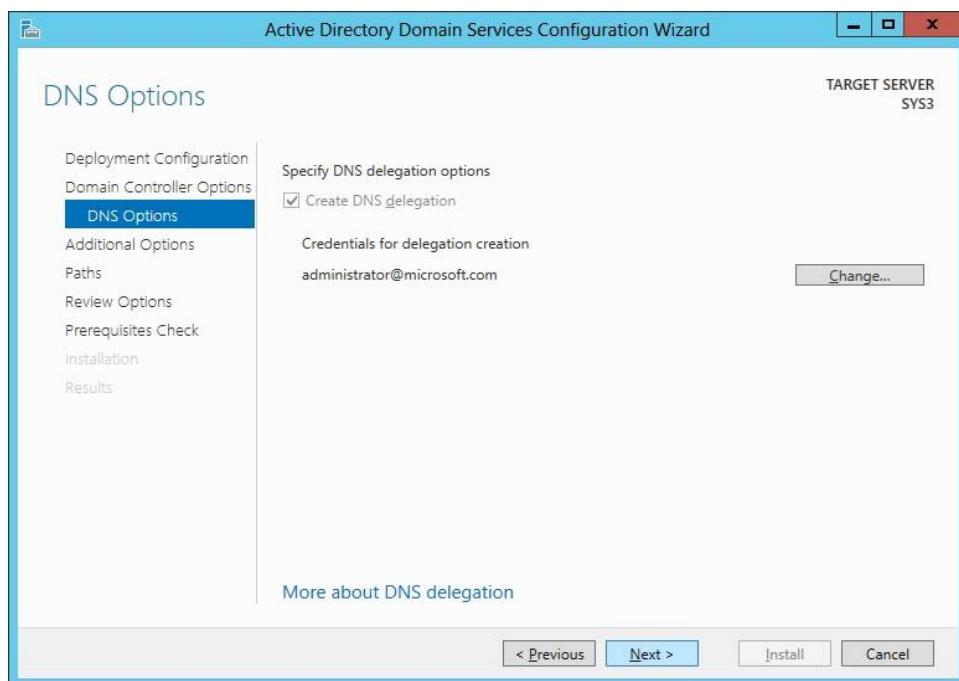


15. Click **Next**.

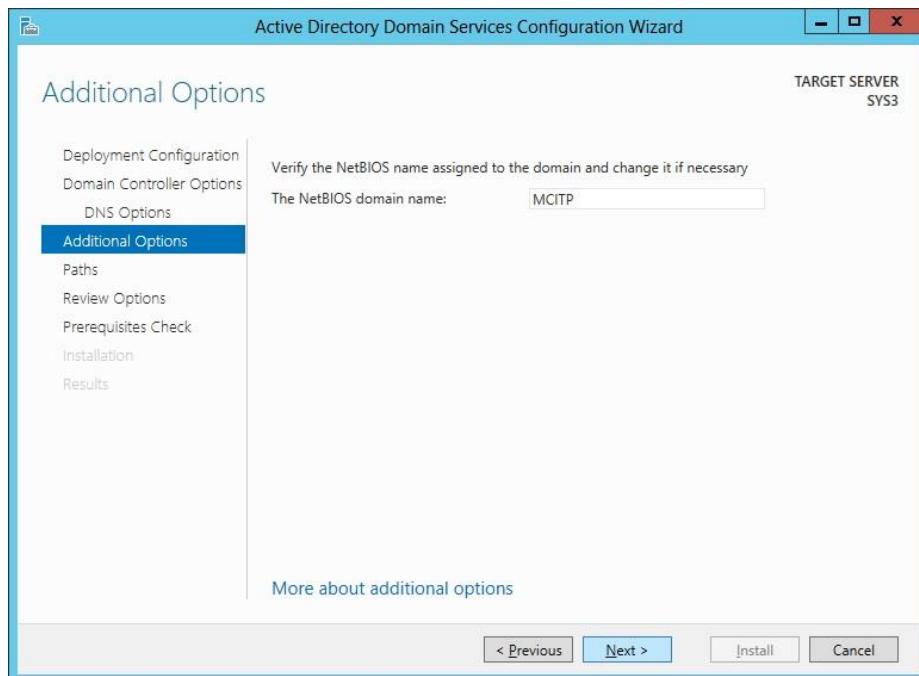
16. In Domain Controller Options, review the default settings, and type the Directory Services Restore Mode **Password** and **Confirm password** and click **Next**.



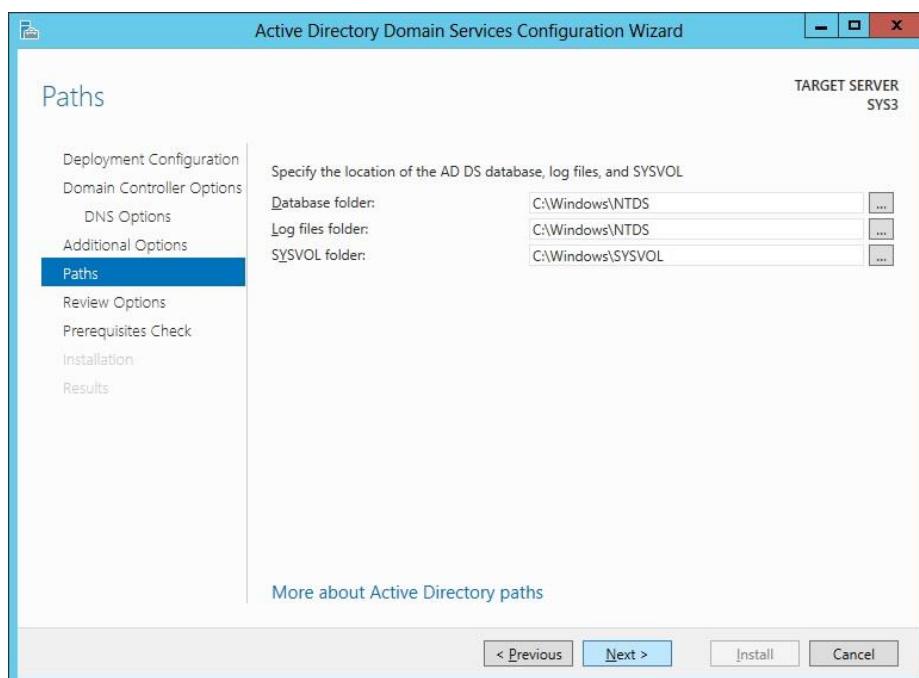
17. On DNS Options page, click **Next**.



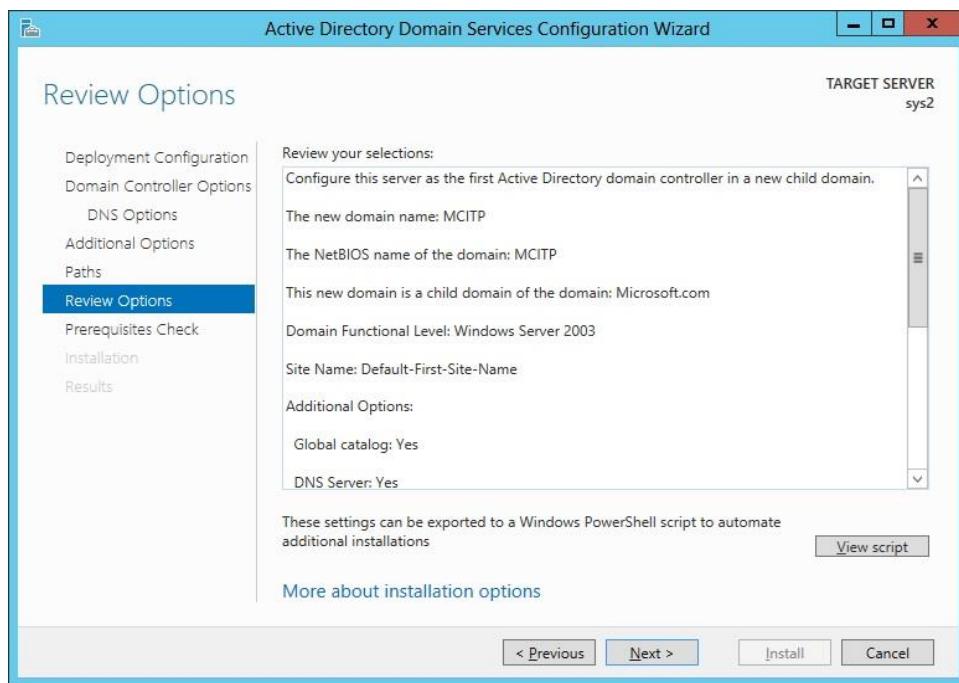
18. In Additional Options Page, Review the NetBIOS domain name (**MCITP**) click **Next.**



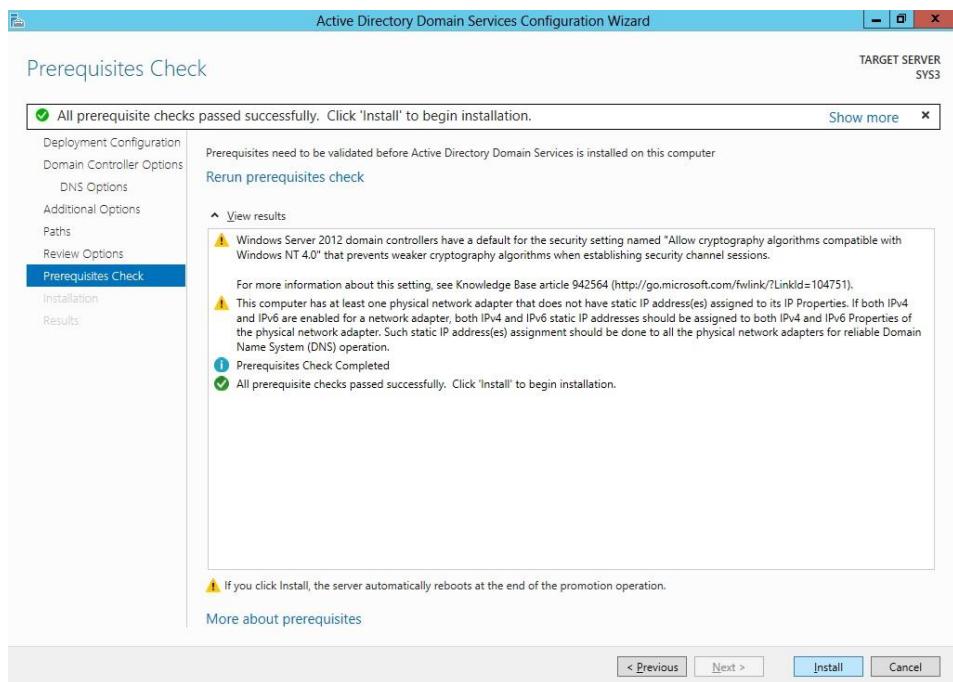
19. Verify the location of the AD DS database, log files, and SYSVOL, click **Next.**



20. Review the Summary and click **Next.**



21. Click **Install to begin installation.**



22. After restarting the computer **Active directory will be installed.**

Verification:

1. Go to Server Manager, Local Server verify for Domain **MCITP.MICROSOFT.COM**

2. Go to **Active Directory Domains and Trusts** verify for parent and child domain.

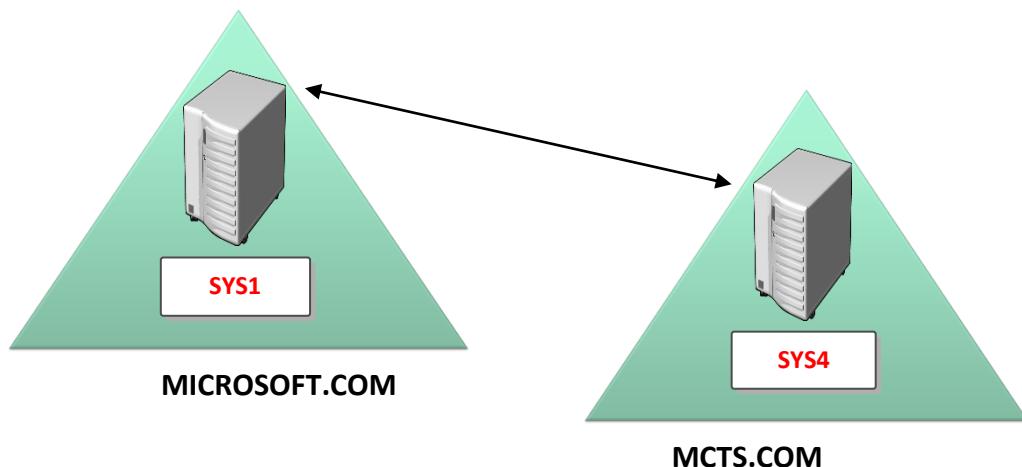
Example: **MICROSOFT.COM** and **MCITP.MICROSOFT.COM**.

CONFIGURING NEW DOMAIN TREE IN EXISTING FOREST

Pre-requisites:

Before working on this lab, you must have

1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server.



SYS1

Domain Controller

IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Alternate DNS	-----

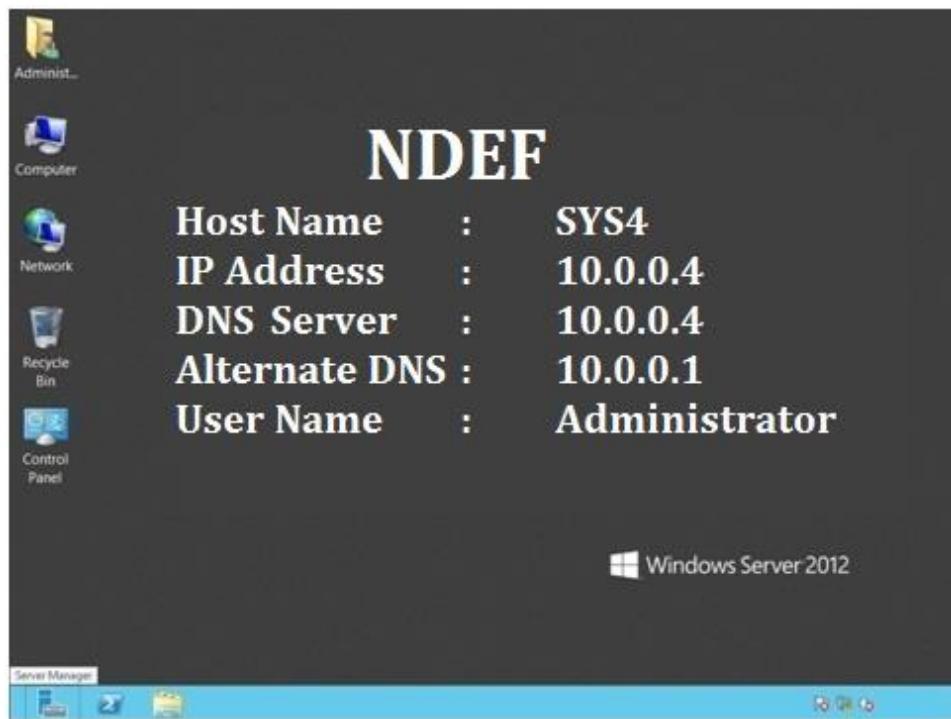
SYS4

New Domain Tree

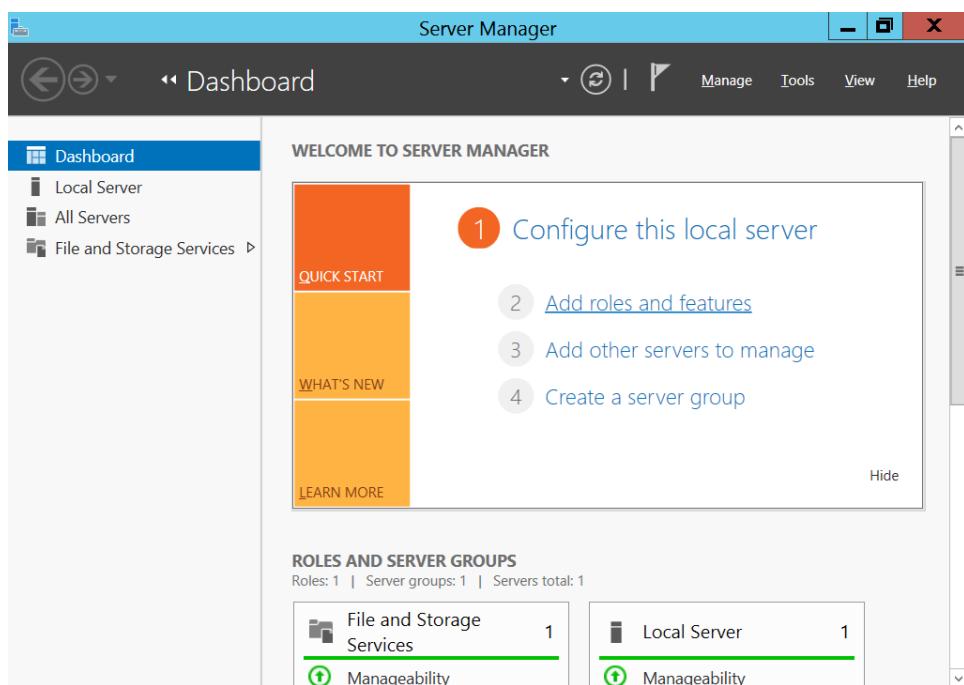
IP Address	10.0.0.4
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.4
Alternate DNS	10.0.0.1

Lab – 3: Configuring New Domain Tree in Existing Forest

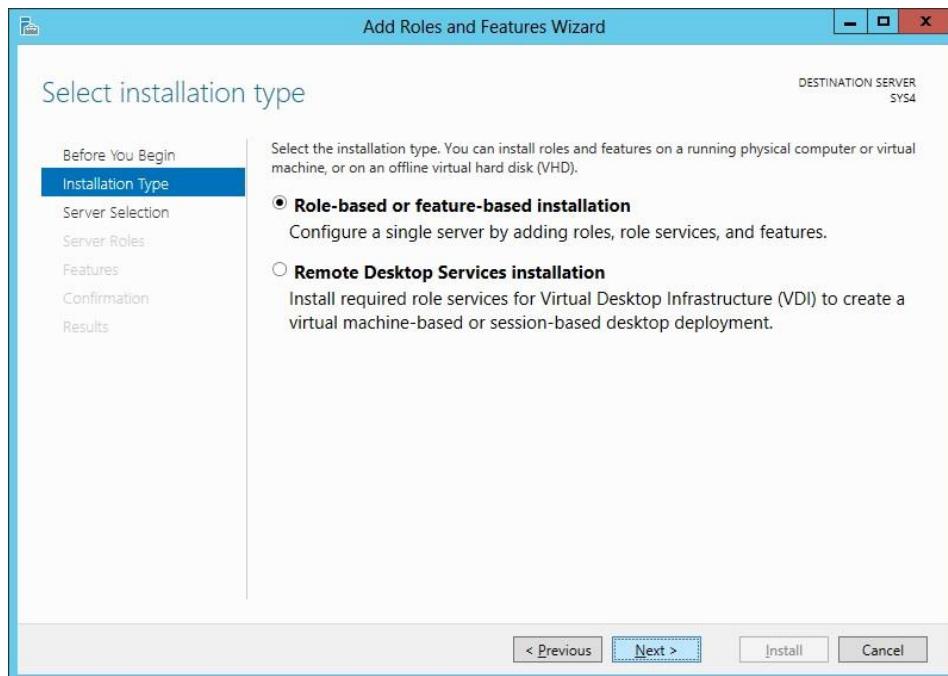
1. Log in as Administrator to the **Workgroup Computer**.
2. Assign **IP Address** and preferred **DNS Server Address**
3. Click Server Manager



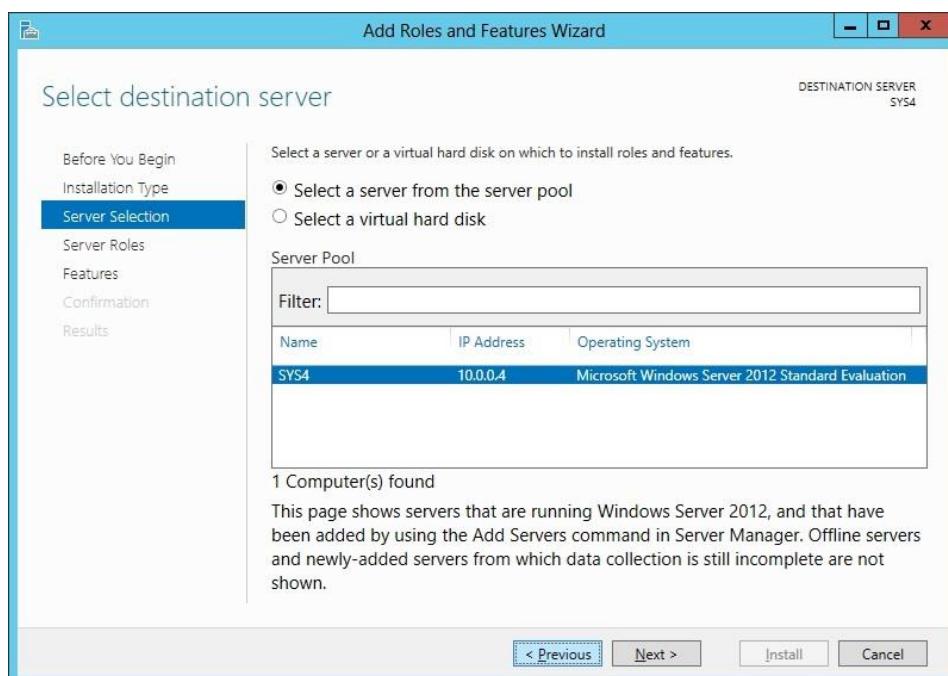
4. In Server Manager Dashboard, Click **Add roles and features**.



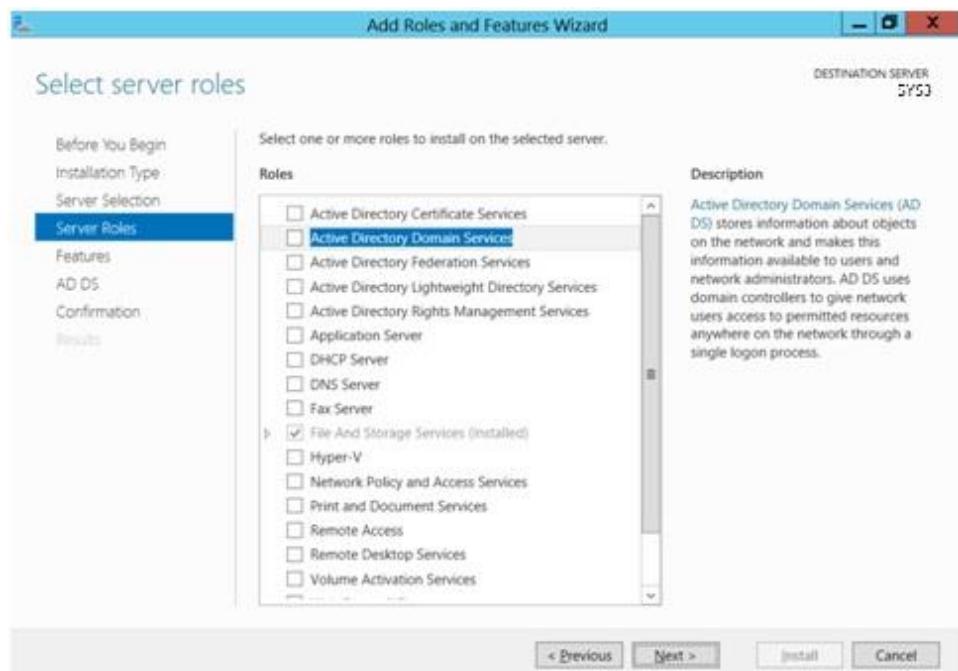
5. In before you begin page, click **Next**, In Select installation type, select **Role-based or feature-based installation**, and click **Next**.



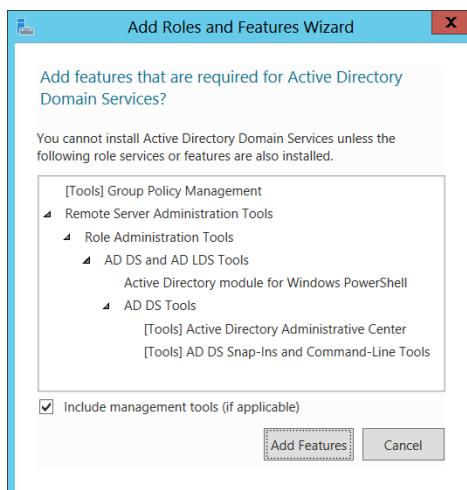
6. In Select destination server, from Server Pool select **SYS4**, click **Next**.

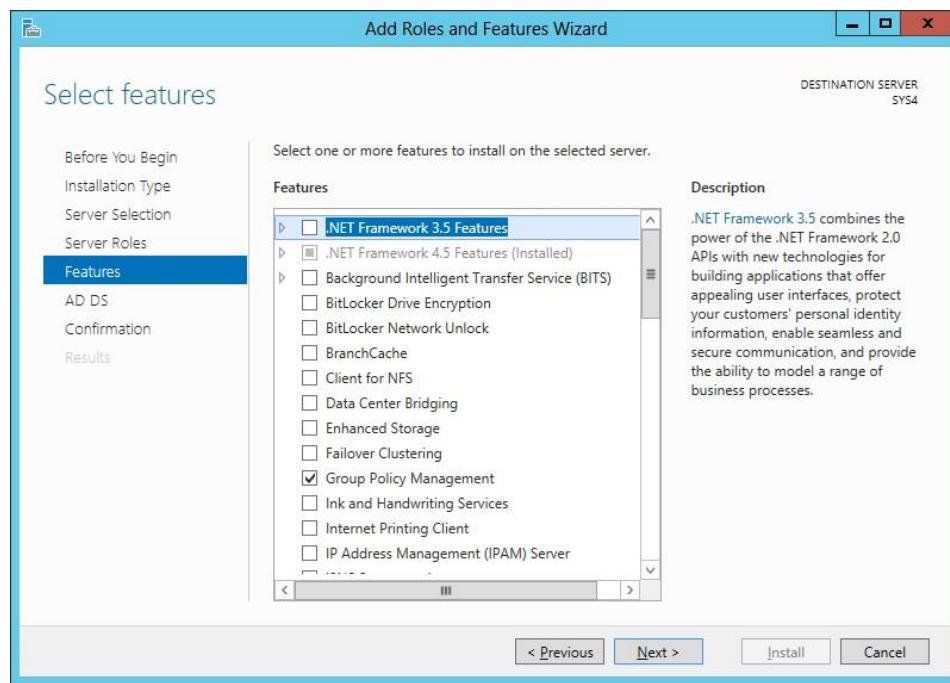
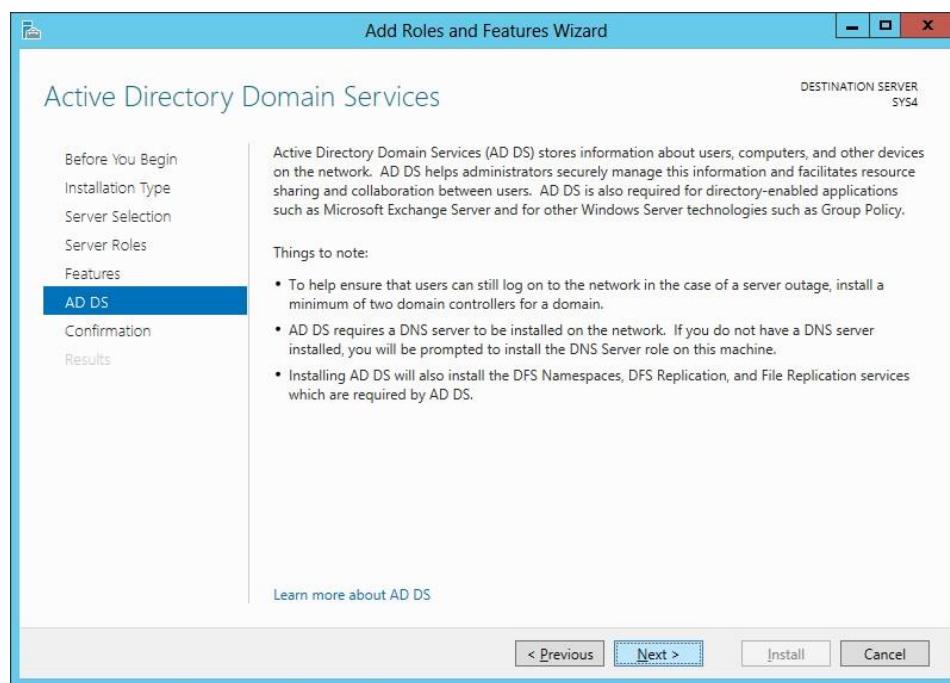


7. In Roles, check the box **Active Directory Domain Services**.

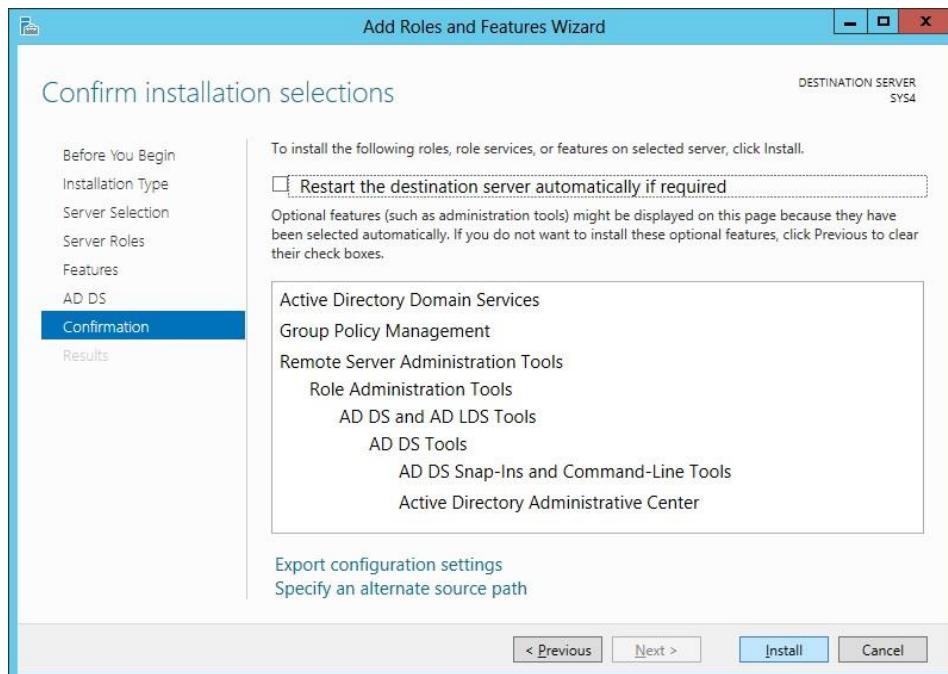


8. Click **Add Features**, to install the required features for Active Directory Domain Services. Click **Next**.

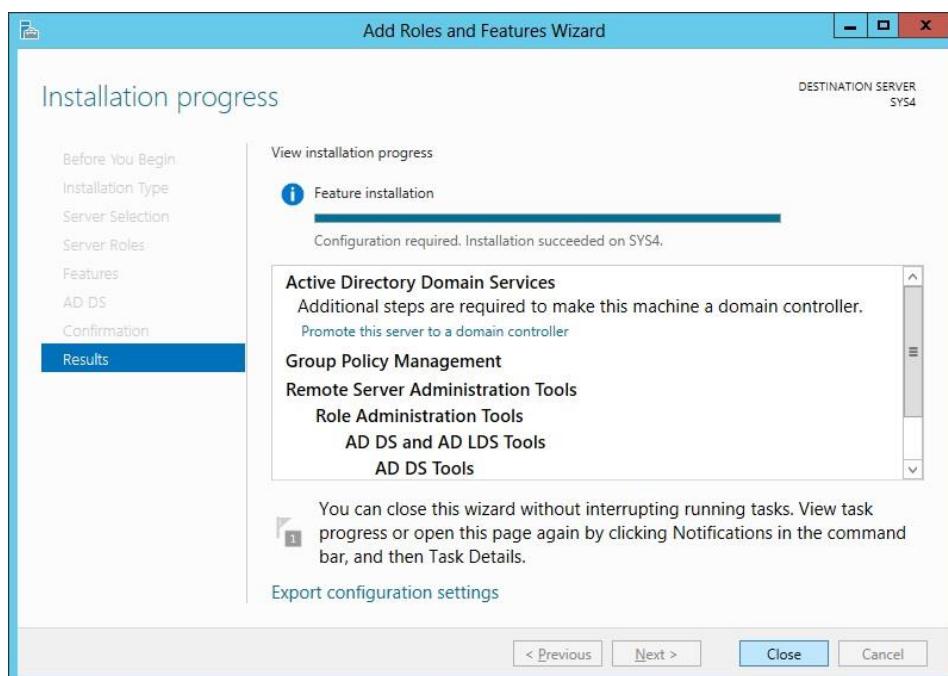


9. In Select features wizard, click **Next**.10. In Active Directory Domain Services wizard, click **Next**.

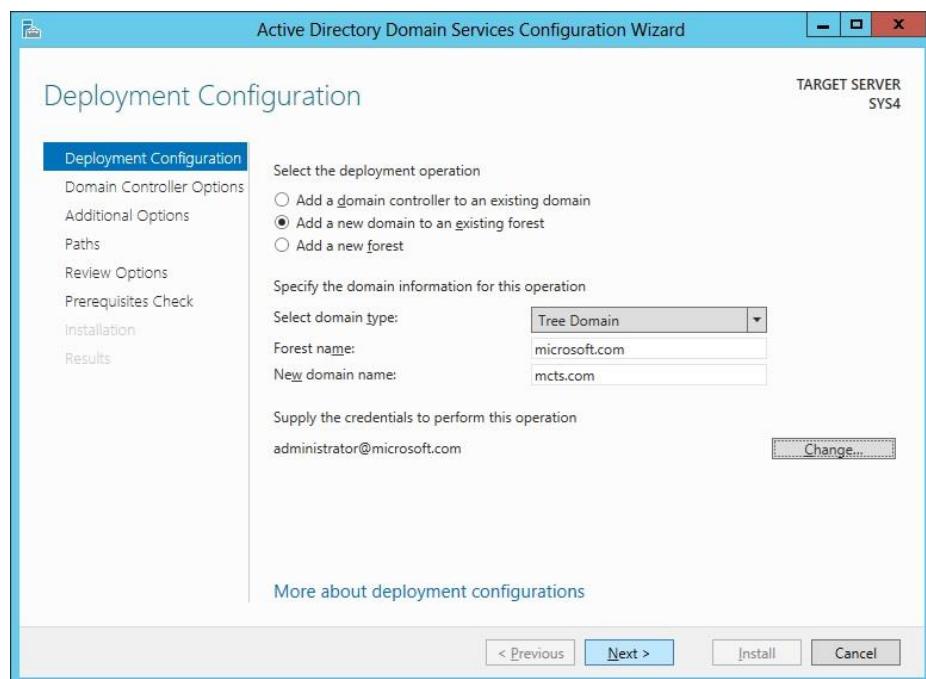
11. Check the box **Restart the destination server automatically if required**. Click **Install**.



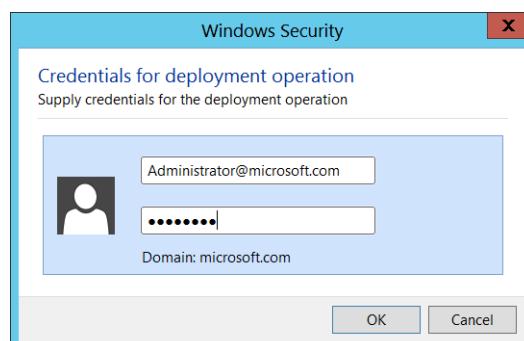
12. Click **Promote this server to a domain controller**.



13. In Deployment Configuration wizard, select **Add a new domain to an existing forest**, select domain type **Tree Domain**, enter the Forest name (Ex:**MICROSOFT.COM**) and New domain name (Ex: **MCTS.COM**), and click **Change**.

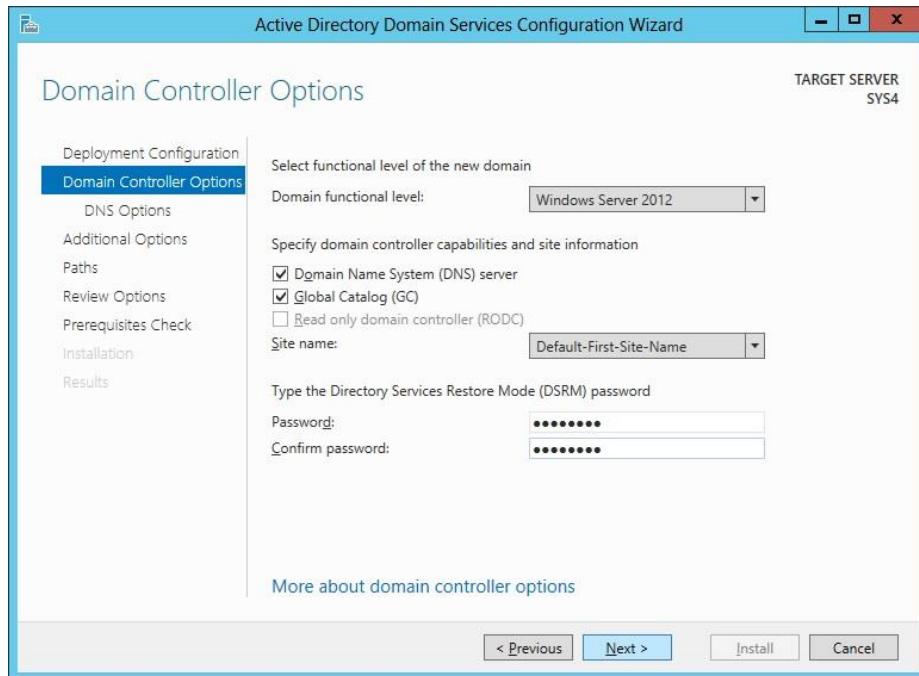


14. Enter User Name: Administrator@microsoft.com and Password, click **OK**.

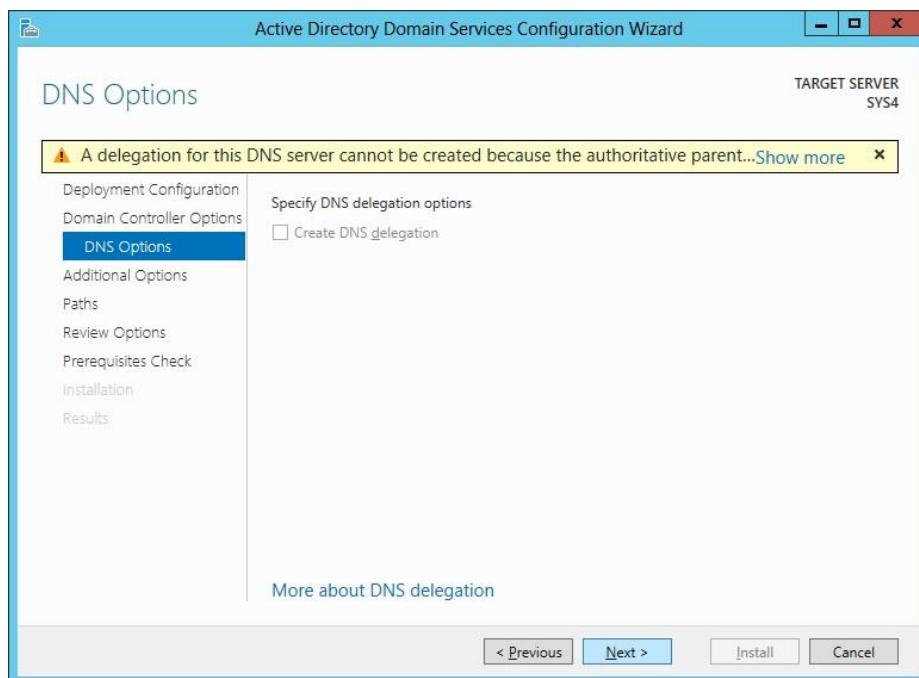


15. Click **Next**.

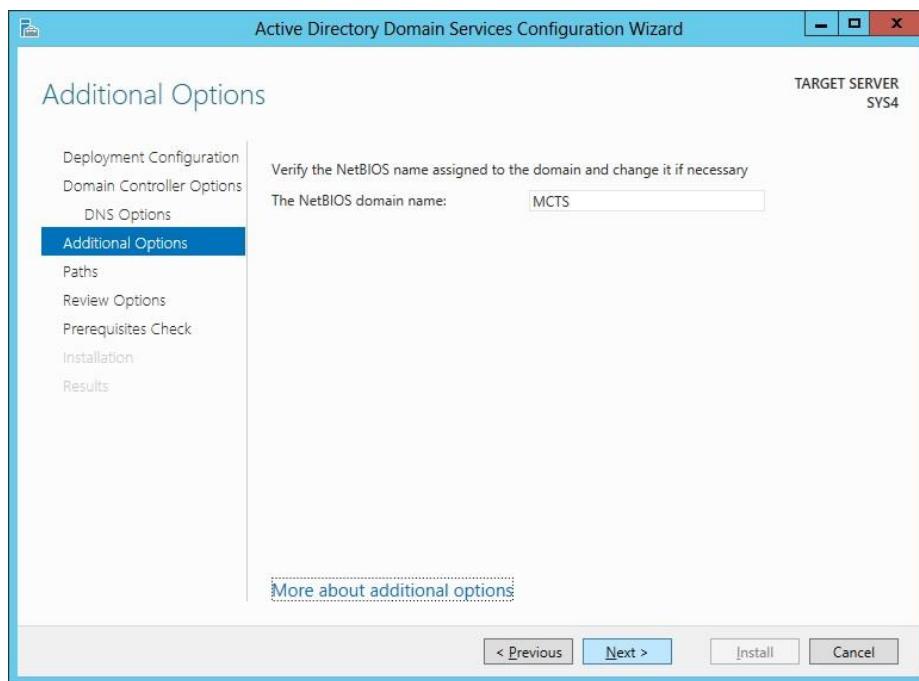
16. In Domain Controller Options, review the default settings, and type the Directory Services Restore Mode **Password** and **Confirm password** and click **Next**.



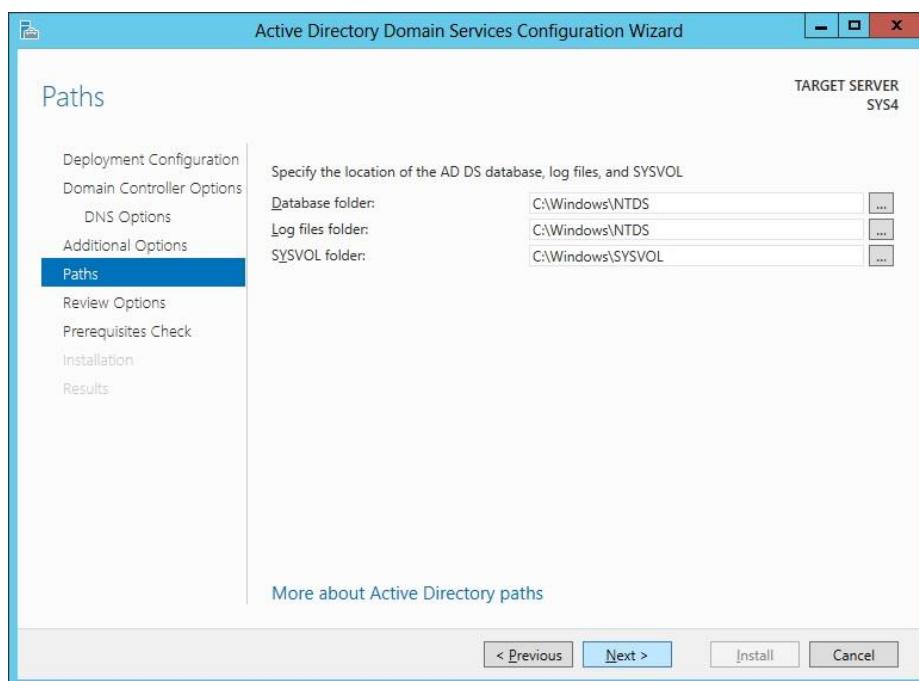
17. On DNS Options page, click **Next**.



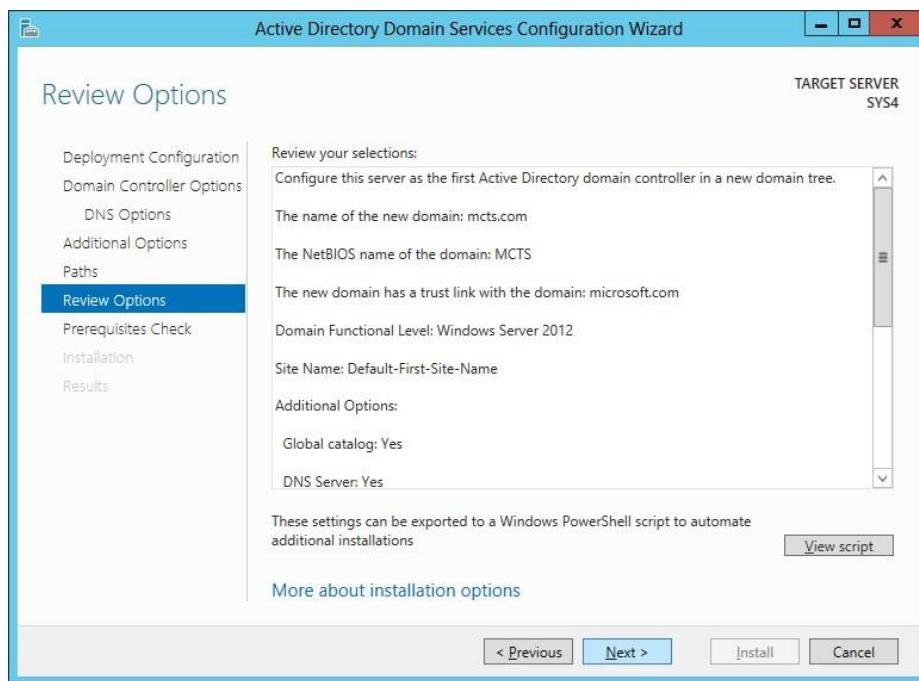
18. In Additional Options Page, Review the NetBIOS domain name (**MCTS**) click **Next**.



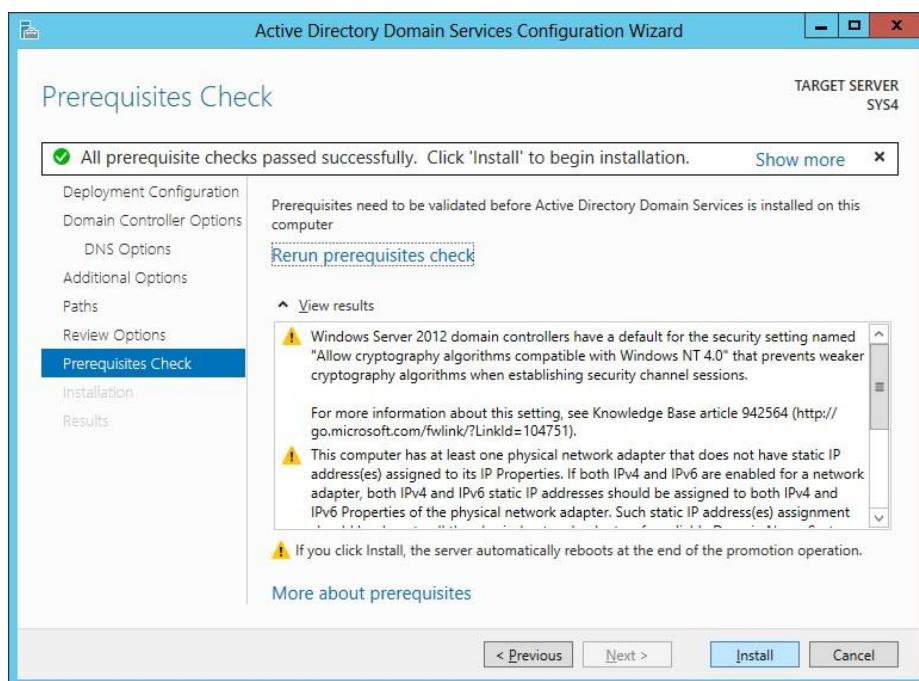
19. Verify the location of the AD DS database, log files, and SYSVOL, click **Next**.



20. Review the Summary and click **Next.**



21. Click **Install to begin installation.**



22. After restarting the computer **Active directory will be installed.**

Verification:

1. Go to Server Manager, Local Server verify for Domain **MCTS.COM**
2. Go to **Active Directory Domains and Trusts** verify for parent and child domain.
Example: **MICROSOFT.COM** and **MCTS.COM**.

ACTIVE DIRECTORY

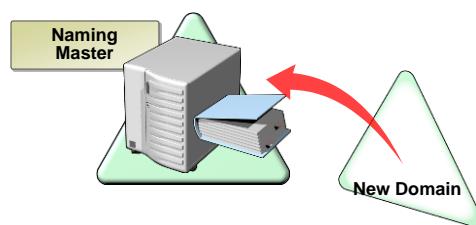
Roles of Active Directory

OPERATION MASTERS

- Naming Master
 - Schema Master
 - RID Master
 - PDC Emulator
 - Infrastructure Master
 - Global Catalog
- } Flexible Single Master Operation Roles (FSMO Roles)
- } Multi Master Operations Role

Naming Master

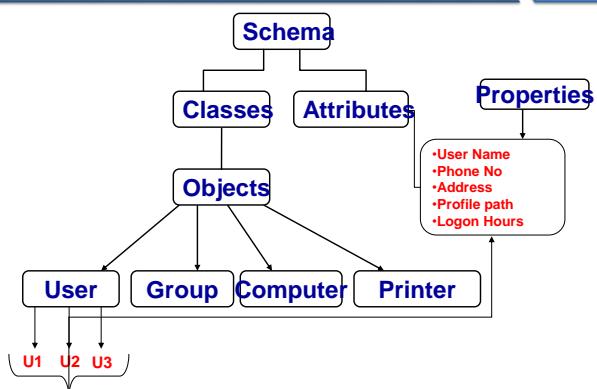
- Checks and Maintains the Uniqueness of the Domain Names in the Whole Forest.
- It is Responsible for Adding, Removing and Renaming the domain names in the whole Forest.



Schema Master

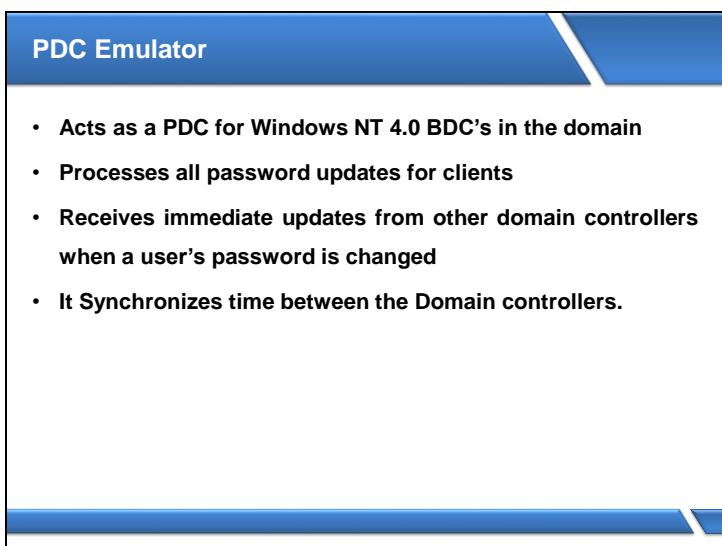
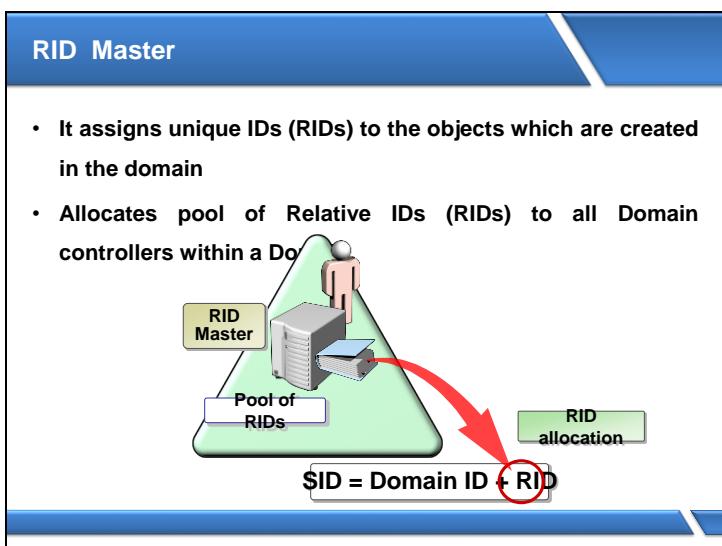
- Schema is a Set of Rules which is used to define the Structure of AD
- Schema contains Definitions of all the Objects which are stored in AD.
- Schema is further classified into:
 - **Classes**
 - Class is a Template which is used to Create an Object
 - **Attributes**
 - Attributes are Properties of an Object

Schema Master



Schema Master

- The Schema Master role owner is the DC responsible for performing updates to the directory schema.
- This DC is the only one that can process updates to the directory schema. Once the schema update is complete, it is replicated from the Schema Master FSMO role owner to all other DCs in the directory.
- There is only one Schema Master per forest.



Infrastructure Master

- Infrastructure Master Maintains and Updates the Universal Group Membership information
- It is Used for Inter-Domain Operations

Roles of Active Directory

OPERATION MASTERS

- Naming Master
- Schema Master
- RID Master
- PDC Emulator
- Infrastructure Master

Forest Wide Roles

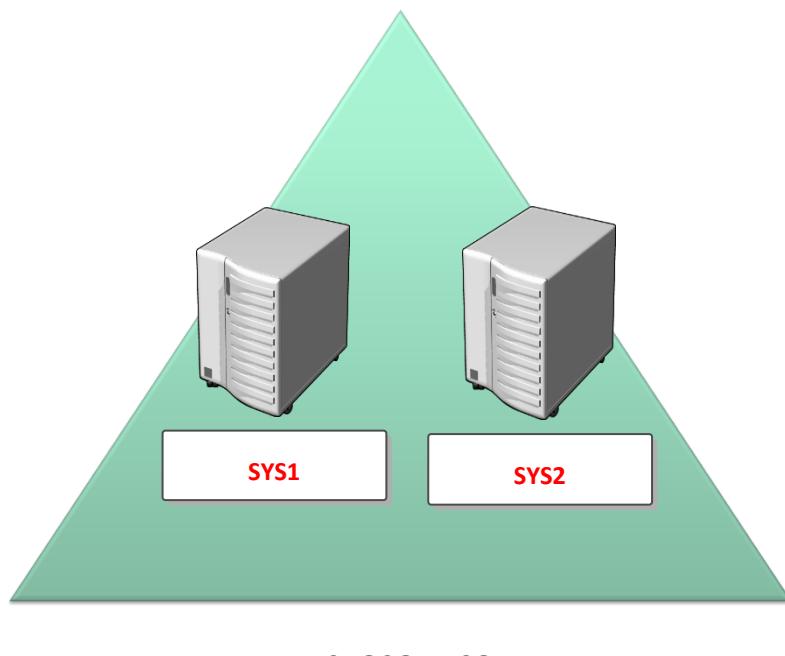
Domain Wide Roles

ROLES OF ACTIVE DIRECTORY

Pre-requisites:

Before working on this lab, you must have

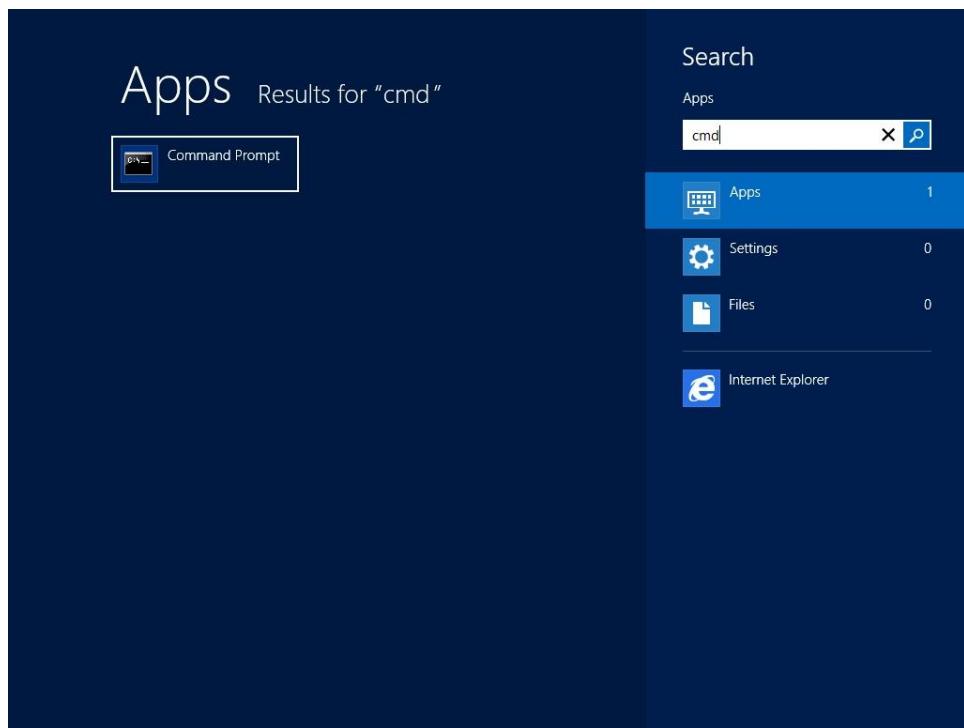
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server Additional Domain controller.



SYS1	SYS2
Domain Controller	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Alternate DNS	-----
Additional Domain controller	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.2
Alternate DNS	10.0.0.1

Lab – 1: Transfer of Roles

1. Log on to Domain Controller as Administrator
2. Go to Start, type cmd in Search Apps, and select **Command Prompt**



3. Type **Net accounts** and Verify for **Primary** in Computer role.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

C:\Users\Administrator>
```

4. Type **Ntdsutil** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

C:\Users\Administrator>ntdsutil
```

5. Type **Roles** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
```

6. Type **Connections** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
```

7. Type **Connect to server SYS2 (ADC System name)** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server sys2
```

8. Type: **Quit**

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server sys2
Binding to sys2 ...
Connected to sys2 using credentials of locally logged on user.
server connections: quit
```

9. Type **Help (or) ?**, to see the available syntax.

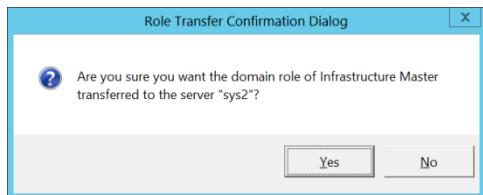
```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server sys2
Binding to sys2 ...
Connected to sys2 using credentials of locally logged on user.
server connections: quit
fsmo maintenance: ?
```

10. Type **Transfer infrastructure master** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
fsmo maintenance: ?
?
Connections - Show this help information
Help - Connect to a specific AD DC/LDS instance
Quit - Show this help information
Seize infrastructure master - Return to the prior menu
Seize naming master - Overwrite infrastructure role on connected server
Seize PDC - Overwrite Naming Master role on connected server
Seize RID master - Overwrite PDC role on connected server
Seize schema master - Overwrite RID role on connected server
Select operation target - Overwrite schema role on connected server
Transfer infrastructure master - Select sites, servers, domains, roles and naming contexts
Transfer naming master - Make connected server the infrastructure master
Transfer PDC - Make connected server the naming master
Transfer RID master - Make connected server the PDC
Transfer schema master - Make connected server the RID master
Transfer schema master - Make connected server the schema master

fsmo maintenance: Transfer infrastructure Master
```

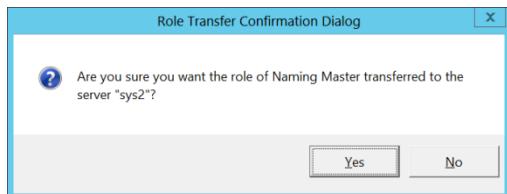
11. Click YES.



12. Type Transfer naming master and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Transfer schema master      - Make connected server the schema master
fsmo maintenance: Transfer infrastructure Master
Server "sys2" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name
,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name
,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site-Name
,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Transfer naming master
```

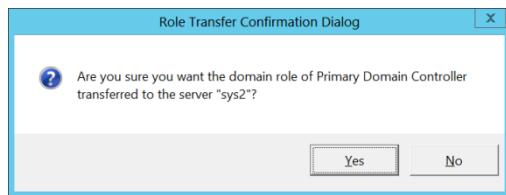
13. Click YES



14. Type Transfer PDC and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
fsmo maintenance: Transfer naming master
Server "sys2" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name
,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site-Name
,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name
,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name
,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site-Name
,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Transfer PDC
```

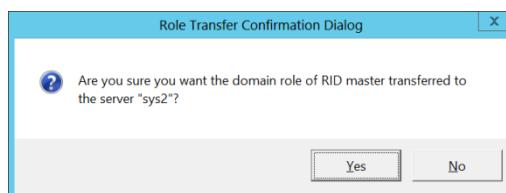
15. Click Yes



16. Type **Transfer RID Master** and Press Enter.

A screenshot of an Administrator Command Prompt window. The title bar says "Administrator: C:\Windows\system32\cmd.exe - ntdsutil". The command "fsmo maintenance: Transfer PDC" is entered, followed by a list of roles known by the server "sys2": Schema, Naming Master, PDC, RID, and Infrastructure. The command "fsmo maintenance: Transfer RID master" is then entered.

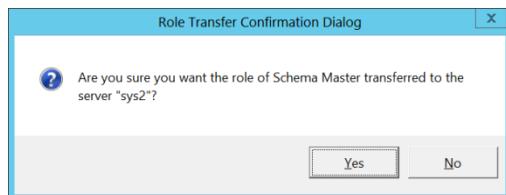
17. Click **YES**



18. Type **Transfer Schema Master** and Press Enter.

A screenshot of an Administrator Command Prompt window. The title bar says "Administrator: C:\Windows\system32\cmd.exe - ntdsutil". The command "fsmo maintenance: Transfer RID master" is entered, followed by a list of roles known by the server "sys2". The command "fsmo maintenance: Transfer schema master" is then entered.

19. Click **YES**



20. Type **Quit** and press **Enter**

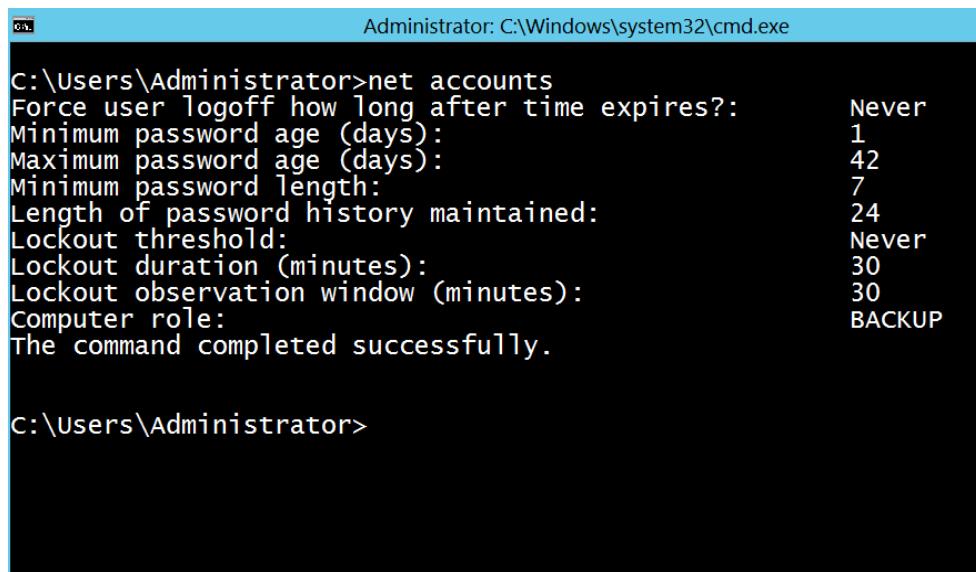
A screenshot of an Administrator Command Prompt window. The command "fsmo maintenance: Transfer schema master" has been run, followed by "fsmo maintenance: quit". The output shows that the server "sys2" knows about 5 roles, including Schema, Naming Master, PDC, RID, and Infrastructure.

21. Type **Quit** and Press Enter.

A screenshot of an Administrator Command Prompt window. The command "ntdsutil: quit" has been run. The output shows the same information as the previous screenshot, indicating that the server "sys2" knows about 5 roles.

Verification:

1. Type **Net accounts** and Press Enter
2. Computer role of **Domain Controller will be converted to Backup and Additional Domain Controller will be converted to Primary.**



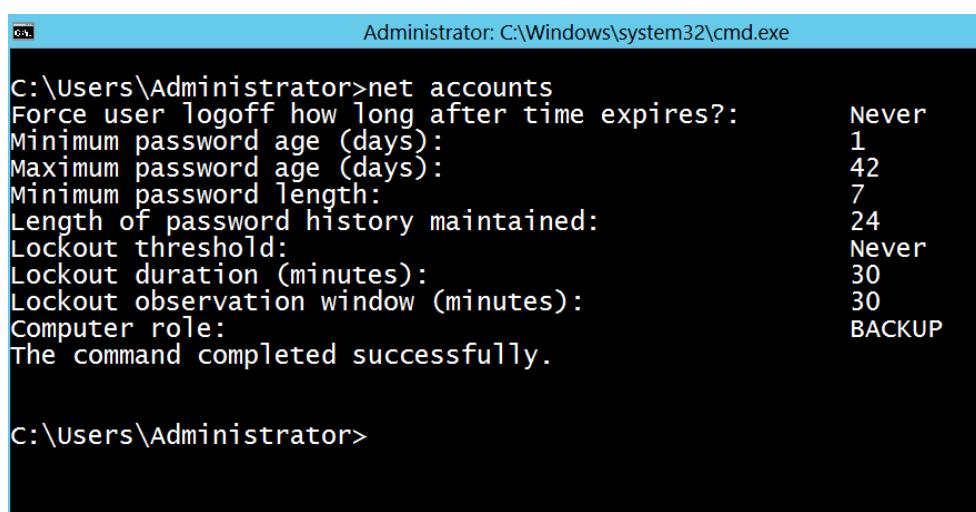
```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>
```

Lab – 2: Seizing of Roles

1. Log on to **Additional Domain Controller** as **Administrator**
2. **Shutdown the Domain Controller**
3. Go to Start, type cmd in Search Apps, and select **Command Prompt**
4. Type **Net accounts** and Verify for **BACKUP** in Computer role.



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>
```

5. Type **Ntdsutil** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>ntdsutil
```

6. Type **Roles** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
```

7. Type **Connections** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
```

8. Type **Connect to server SYS1 (ADC System name)** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server sys1
```

9. Type: **Quit**

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP
The command completed successfully.

C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server sys1
Binding to sys1 ...
Connected to sys1 using credentials of locally logged on user.
server connections: quit
```

10. Type **Help(or)?** To view the available syntax.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
fsmo maintenance: ?

?                                     - Show this help information
Connections                         - Connect to a specific AD DC/LD
Help                                  - Show this help information
Quit                                 - Return to the prior menu
Seize infrastructure master          - Overwrite infrastructure role
er
Seize naming master                  - Overwrite Naming Master role o
r
Seize PDC                            - Overwrite PDC role on connecte
Seize RID master                     - Overwrite RID role on connecte
Seize schema master                 - Overwrite schema role on connec
Select operation target              - Select sites, servers, domains
                                         naming contexts
Transfer infrastructure master       - Make connected server the inf
r
Transfer naming master               - Make connected server the nami
Transfer PDC                          - Make connected server the PDC
Transfer RID master                  - Make connected server the RID
Transfer schema master               - Make connected server the sche

fsmo maintenance:
```

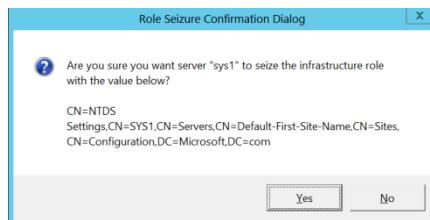
11. Type **Seize infrastructure master** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
fsmo maintenance: ?

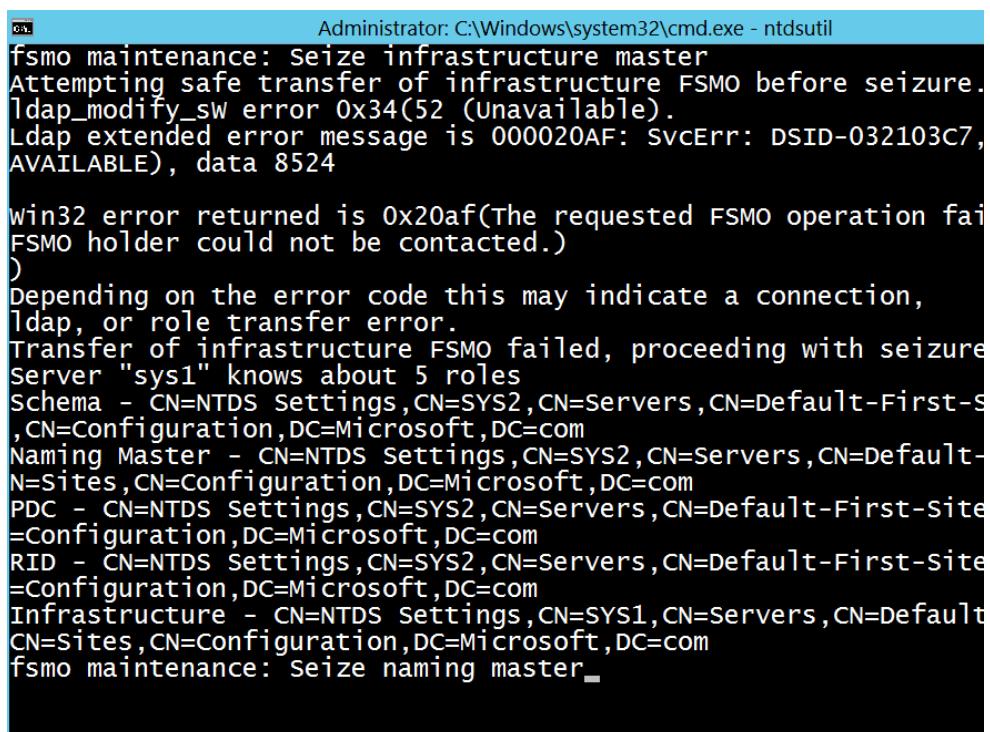
?                                     - Show this help information
Connections                         - Connect to a specific AD DC/LD
Help                                  - Show this help information
Quit                                 - Return to the prior menu
Seize infrastructure master          - Overwrite infrastructure role
er
Seize naming master                  - Overwrite Naming Master role o
r
Seize PDC                            - Overwrite PDC role on connecte
Seize RID master                     - Overwrite RID role on connecte
Seize schema master                 - Overwrite schema role on connec
Select operation target              - Select sites, servers, domains
                                         naming contexts
Transfer infrastructure master       - Make connected server the inf
r
Transfer naming master               - Make connected server the nami
Transfer PDC                          - Make connected server the PDC
Transfer RID master                  - Make connected server the RID
Transfer schema master               - Make connected server the sche

fsmo maintenance: seize infrastructure master_
```

12. Click **YES**.



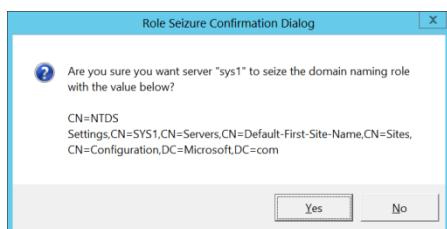
13. Type **Seize naming master** and Press Enter.



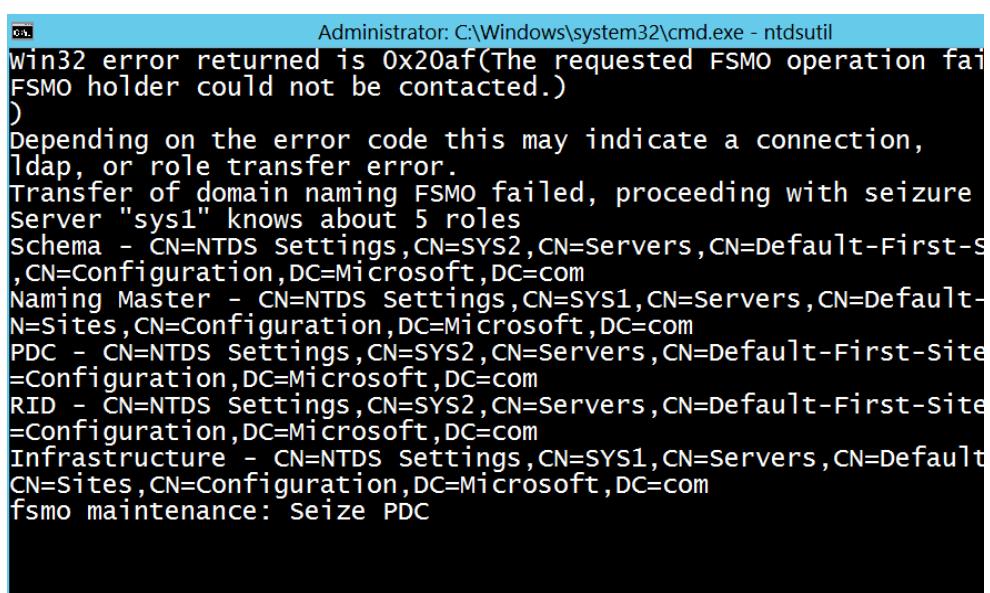
```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
fsmo maintenance: seize infrastructure master
Attempting safe transfer of infrastructure FSMO before seizure.
ldap_modify_sw error 0x34(52) (Unavailable).
Ldap extended error message is 000020AF: SvcErr: DSID-032103C7,
AVAILABLE), data 8524

Win32 error returned is 0x20af(The requested FSMO operation failed
FSMO holder could not be contacted.)
)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of infrastructure FSMO failed, proceeding with seizure
Server "sys1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Seize naming master
```

14. Click **YES**

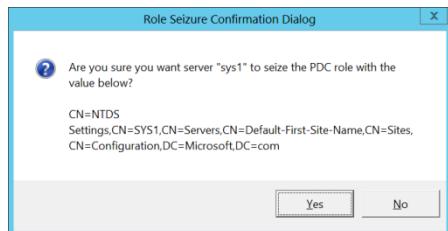


15. Type **Seize PDC** and Press Enter.



```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Win32 error returned is 0x20af(The requested FSMO operation failed
FSMO holder could not be contacted.)
)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of domain naming FSMO failed, proceeding with seizure
Server "sys1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Seize PDC
```

16. Click Yes

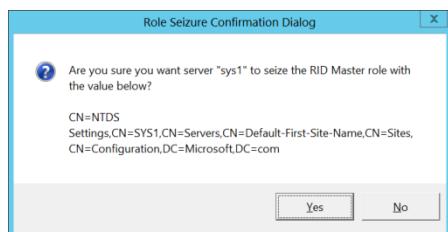


17. Type Seize RID Master and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-
CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Seize PDC
Attempting safe transfer of PDC FSMO before seizure.
ldap_modify_sw error 0x34(52) (Unavailable).
Ldap extended error message is 000020AF: SvcErr: DSID-032105B1,
AVAILABLE), data 8524

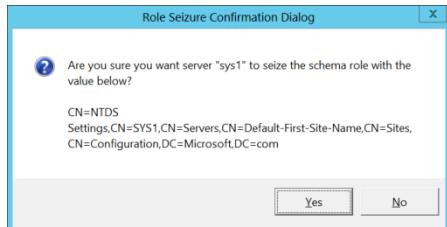
Win32 error returned is 0x20af(The requested FSMO operation failed.
FSMO holder could not be contacted.)
)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of PDC FSMO failed, proceeding with seizure ...
Server "sys1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Seize RID master.
```

18. Click YES



19. Type Seize Schema Master and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Tldap, or role transfer error.
Transfer of RID FSMO failed, proceeding with seizure ...
Searching for highest rid pool in domain
Server "sys1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS2,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: Seize Schema master
```

20. Click **YES**21. Type **Quit** and press Enter

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Depending on the error code this may indicate a connection, Tldap, or role transfer error.
Transfer of schema FSMO failed, proceeding with seizure ...
Server "sys1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: quit
```

22. Type **Quit** and Press Enter.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Server "sys1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: quit
ntdsutil: quit
```

Verification:

1. Type **Net accounts** and Press Enter
2. Computer role of **Additional Domain Controller will be converted to Primary.**

```
Administrator: C:\Windows\system32\cmd.exe
Naming Master - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
PDC - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
RID - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Configuration,DC=Microsoft,DC=com
Infrastructure - CN=NTDS Settings,CN=SYS1,CN=Servers,CN=Default-First-Site,CN=Sites,CN=Configuration,DC=Microsoft,DC=com
fsmo maintenance: quit
ntdsutil: quit

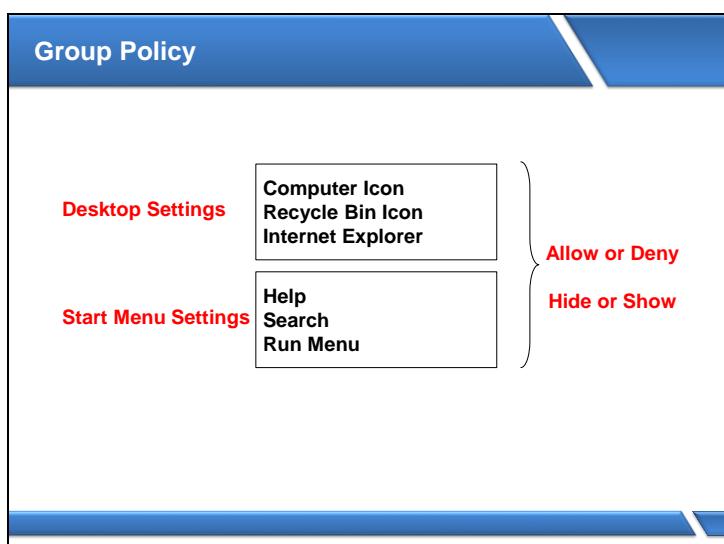
C:\Users\Administrator>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.

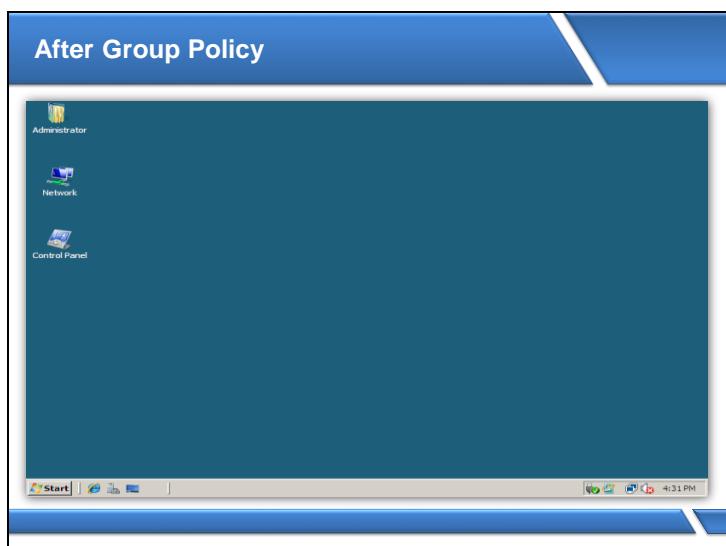
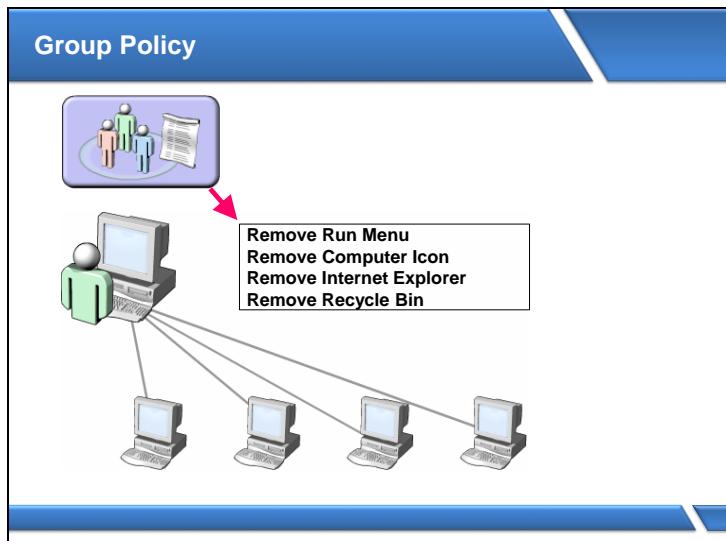
C:\Users\Administrator>
```

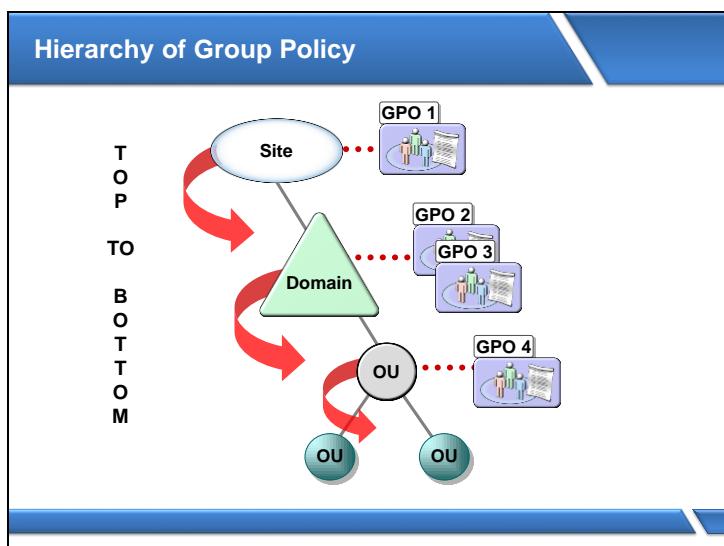
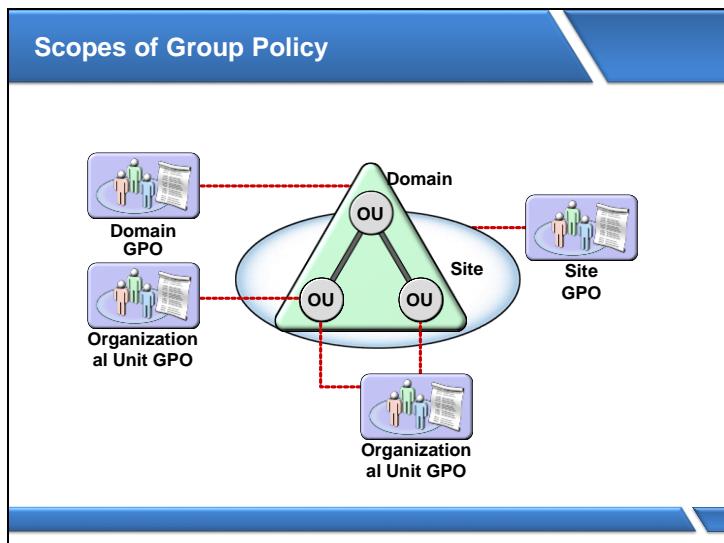
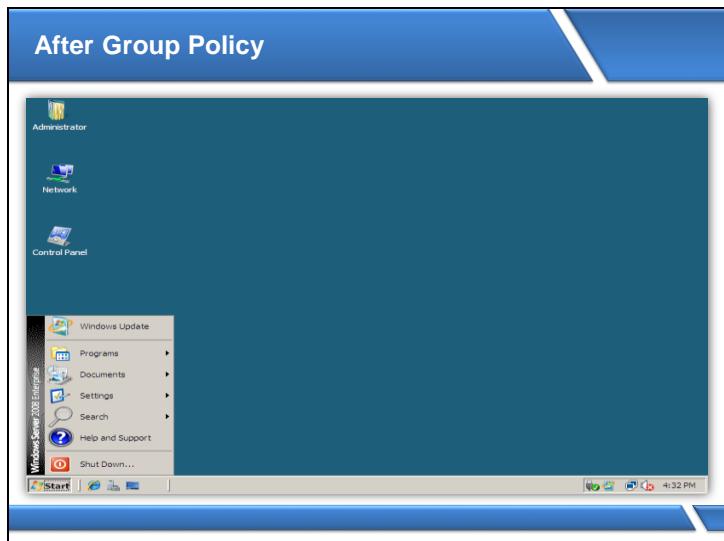
GROUP POLICY

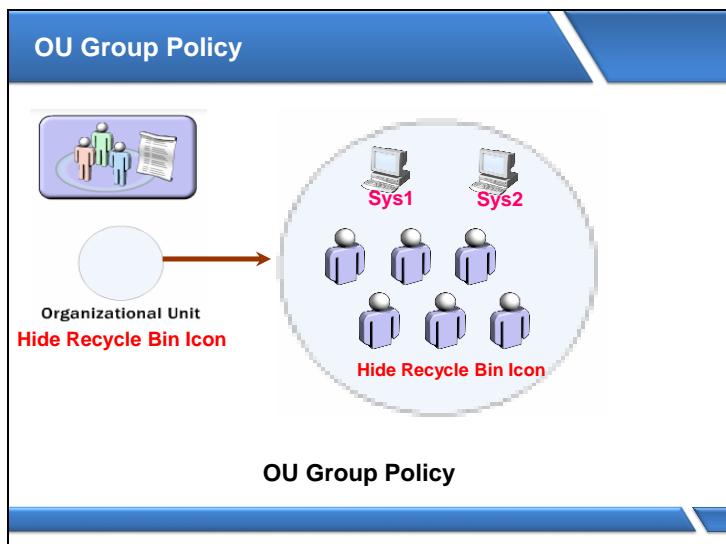
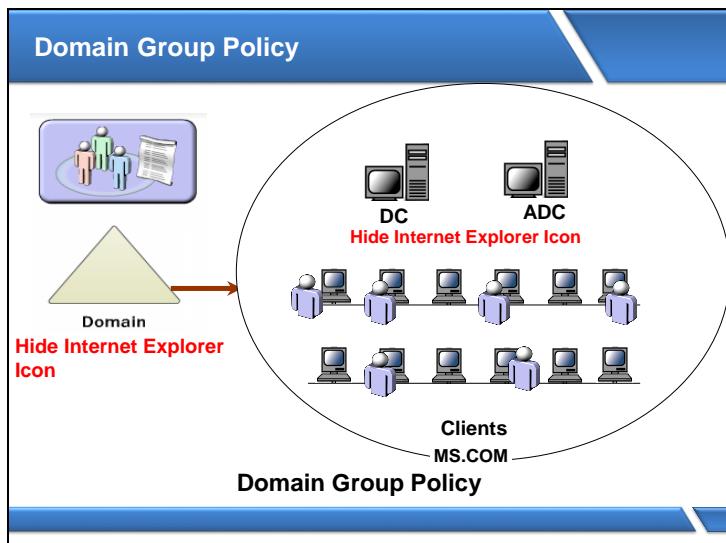
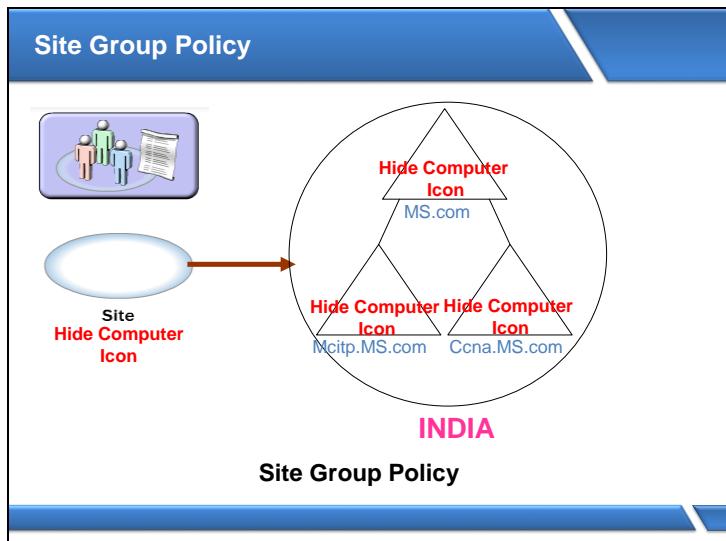
Group Policy

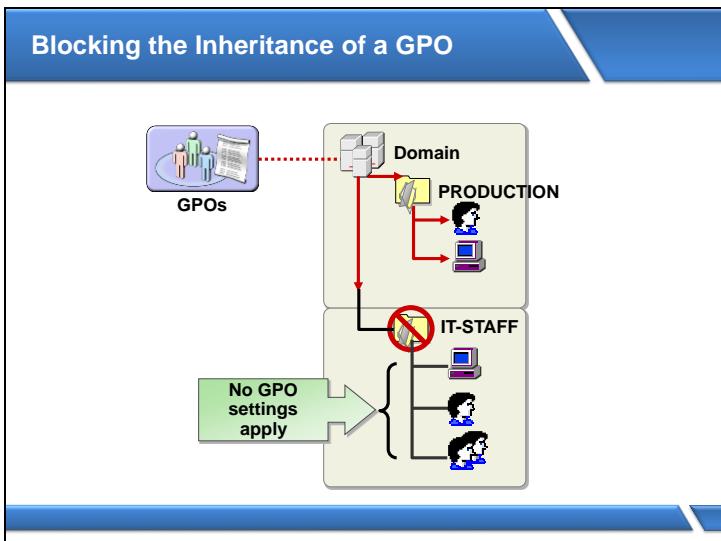
- Group policy is a collection of settings which can be applied on computers and users.
- With group policy administrator can centrally manage the computers and users.
- Eases administration using group policy.











- ### Software Deployment
- It is to deploy software (Applications) on all the computers in the domain from one central location by applying the Group Policies.
 - Supports the deployment of ".MSI" but not ".EXE" applications.

- ### Folder Redirection
- Redirection of folders on the local computer or on a Shared folder.
 - Folders on a server appear as if they are located on the local drive.
 - Fastens the User logon process in case if the profile is large.

Auditing

- Audit policy configures a system to audit categories of activities. If audit policy is not enabled, a server will not audit those activities
- Audit events categories are as below :
 - Access to NTFS files and folders
 - Account or object changes in AD DS
 - Logon
 - Assignment of use of user rights

Group Policy preferences

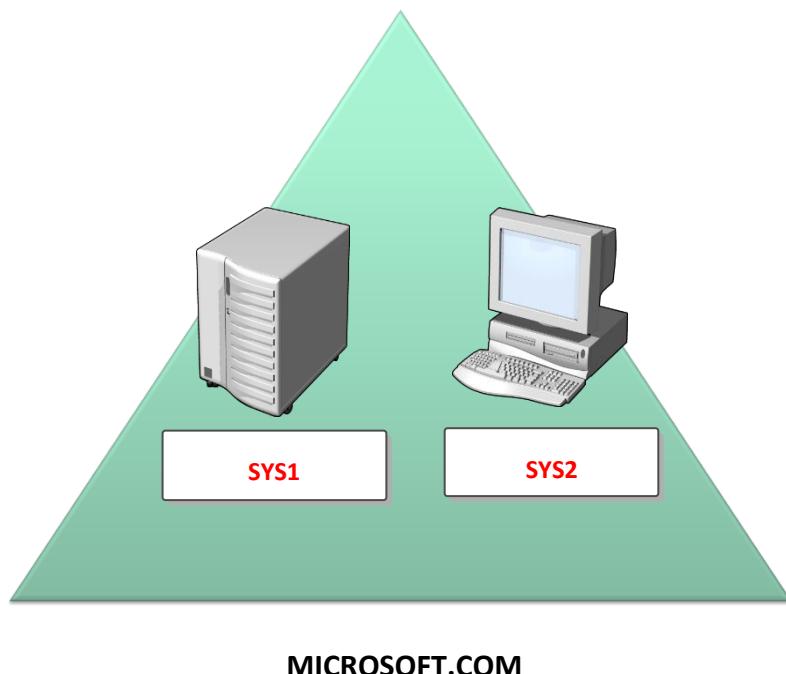
- Group Policy preferences provide better targeting, through item-level targeting and action modes. Additionally, rich user interfaces and standards-based XML configurations provide you with more power and flexibility over managed computers when you administer GPOs.
- Examples of the new Group Policy preference extensions include folder options, mapped drives, printers, scheduled tasks, services, and Start menu settings.

GROUP POLICIES

Pre-requisites:

Before working on this lab, you must have

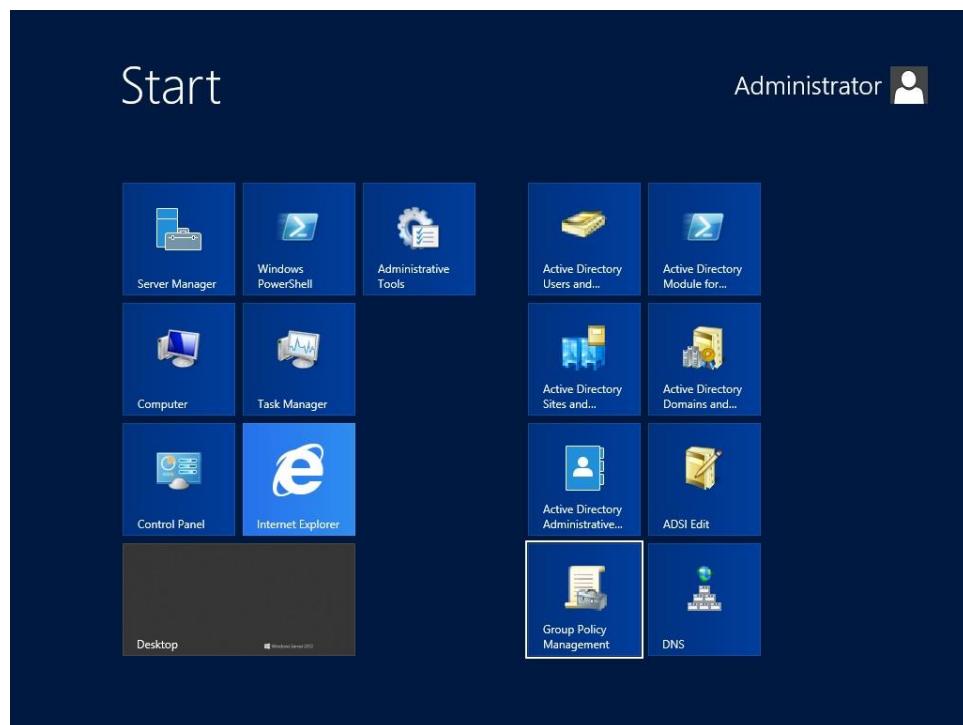
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server or Windows 7.



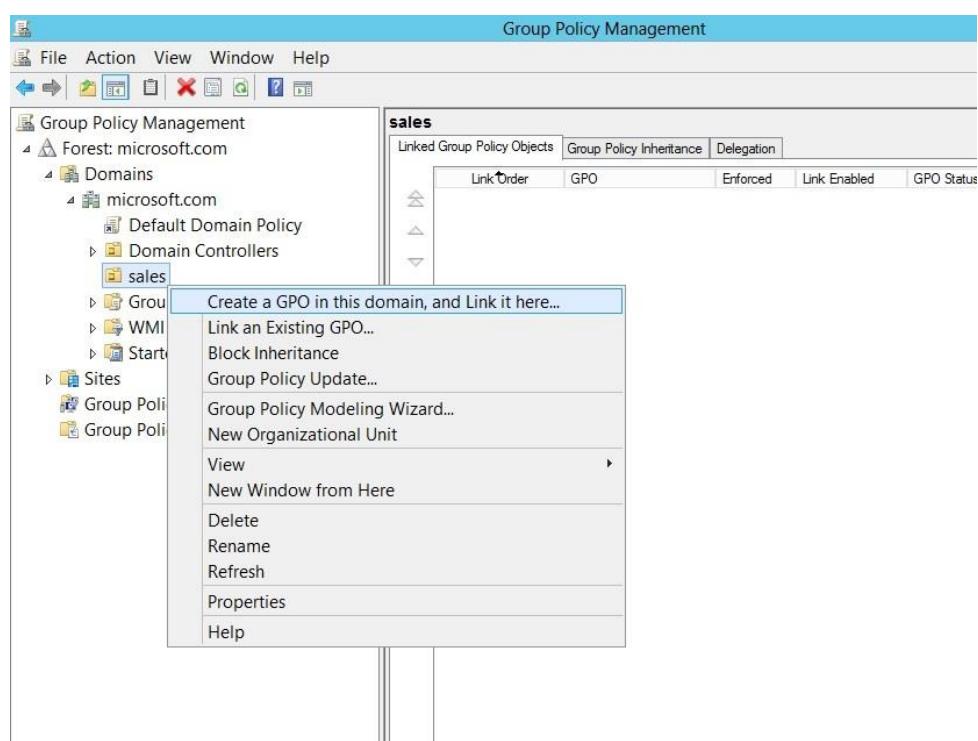
SYS1	SYS2
Domain Controller	Member Server / Client
IP Address 10.0.0.1	IP Address 10.0.0.2
Subnet Mask 255.0.0.0	Subnet Mask 255.0.0.0
Preferred DNS 10.0.0.1	Preferred DNS 10.0.0.1

Lab – 1: Applying Group Policy on Organizational Unit Level

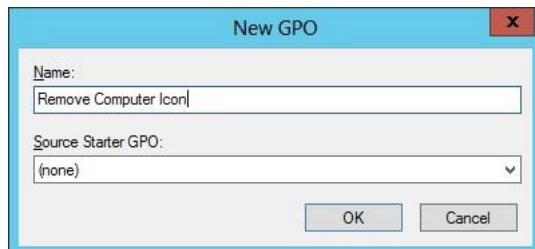
1. Press Windows Key to go to Start, select **Group Policy Management**.



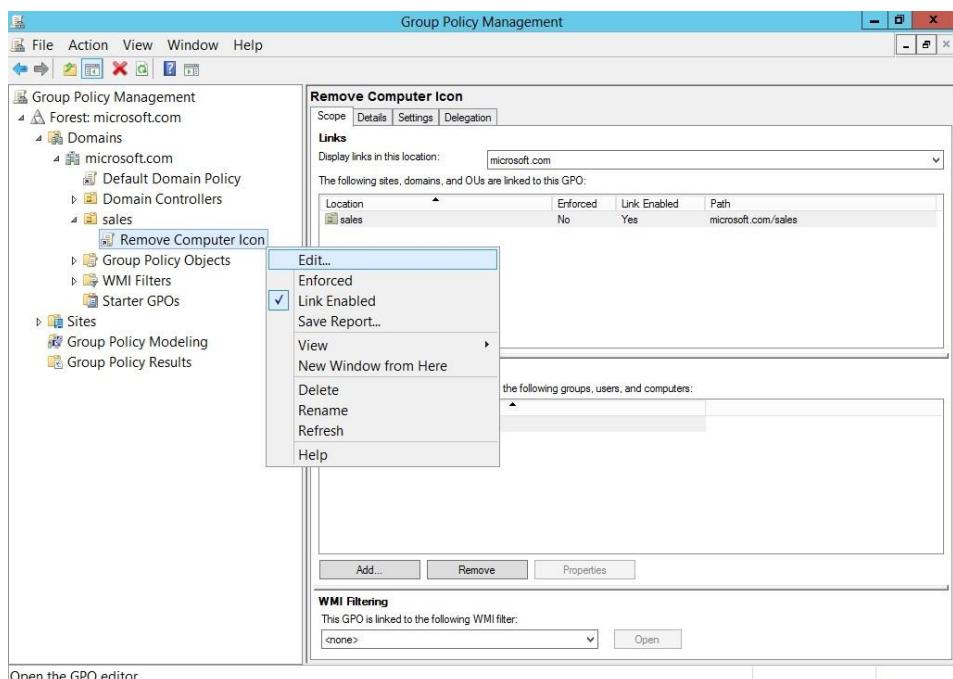
2. Right click OU (Sales) → Create a GPO in this domain and Link it here.



3. Enter any name to GPO Link (Ex: Remove Computer Icon) and click OK.

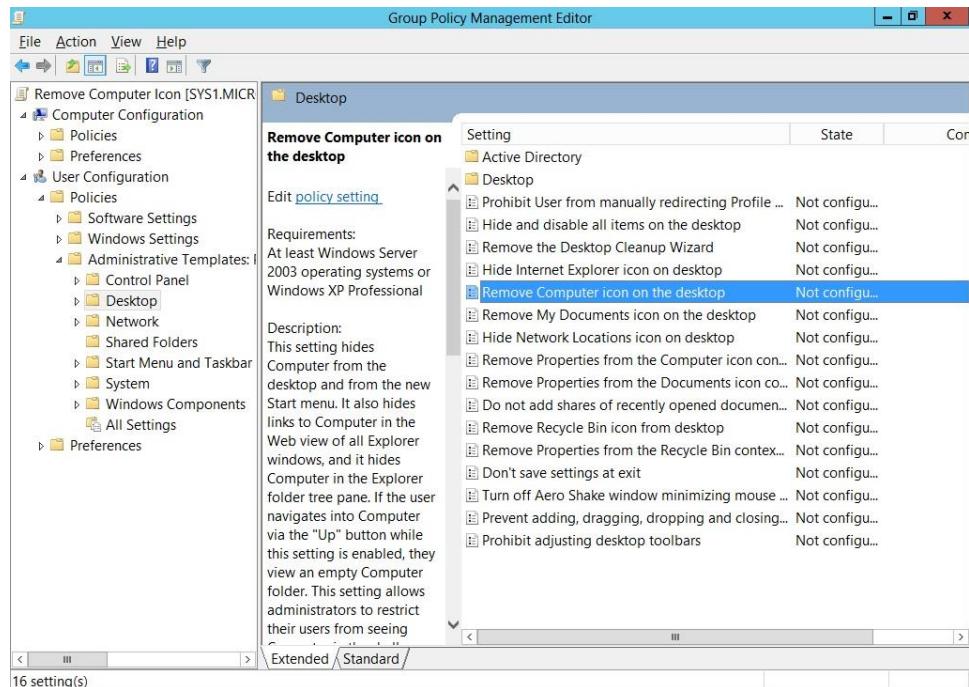


4. Right Click created GPO Link → Edit

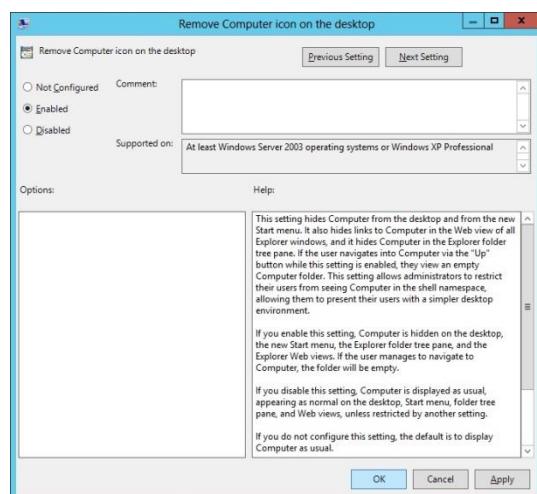


5. In Group Policy Management Editor Window, Go to **User Configuration** → **Policies** → **Administrative Templates** → **Desktop**.

- 6. Select a policy (**Remove Computer icon on the Desktop**) on right side of the screen, Right Click and select **Properties**.**

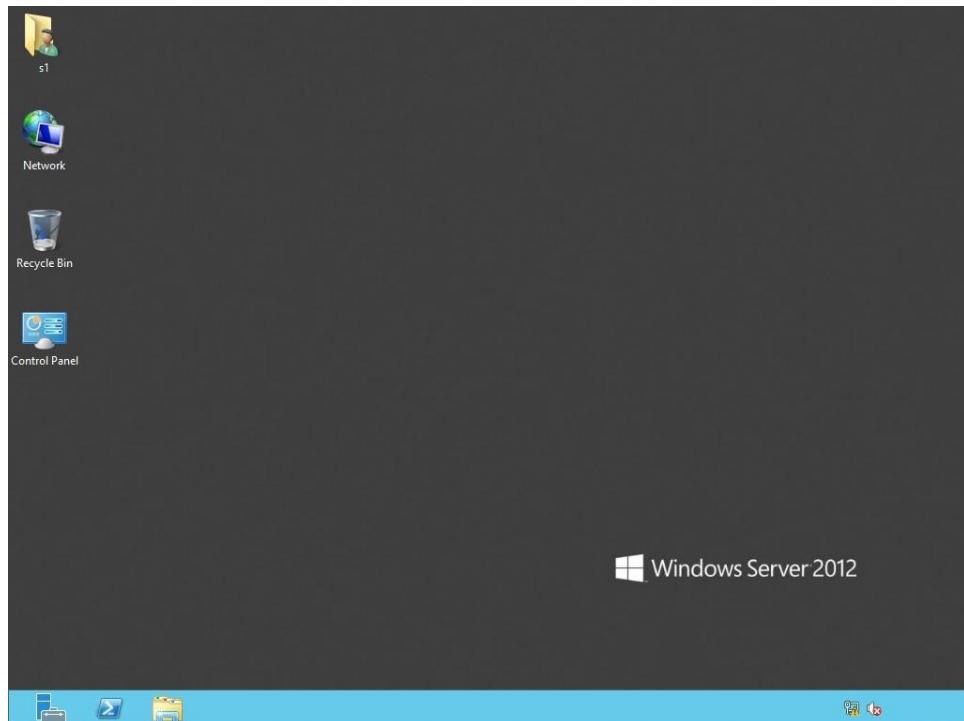


- 7. Select **Enabled** option and click **Apply** and **OK**.**



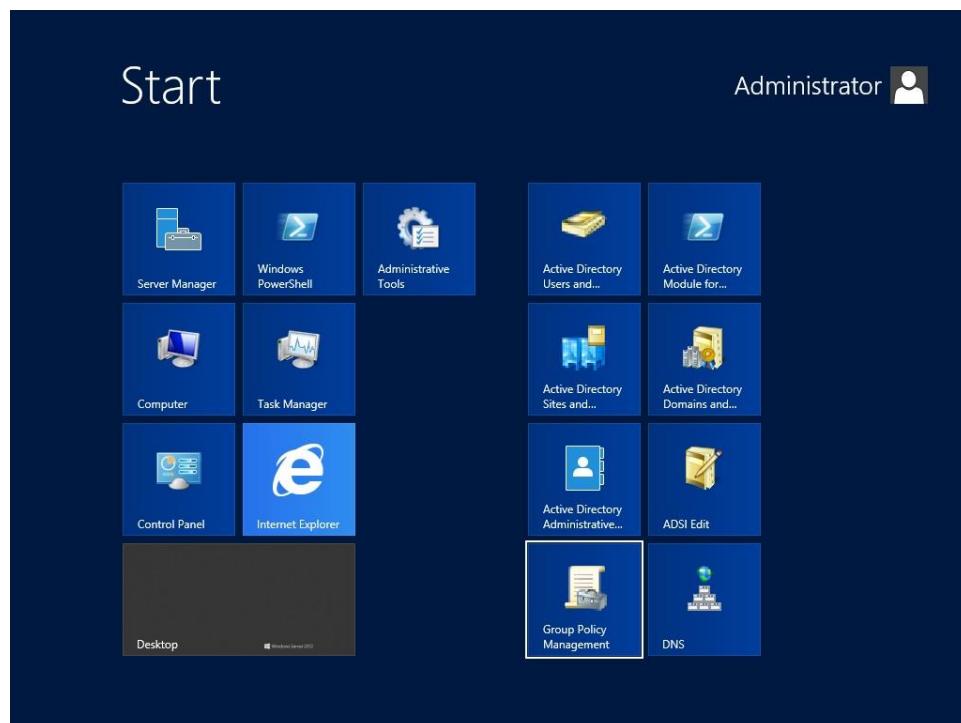
Verification:

1. Logon to client system as sales OU user (**s1**) and verify the changes because of the policy.

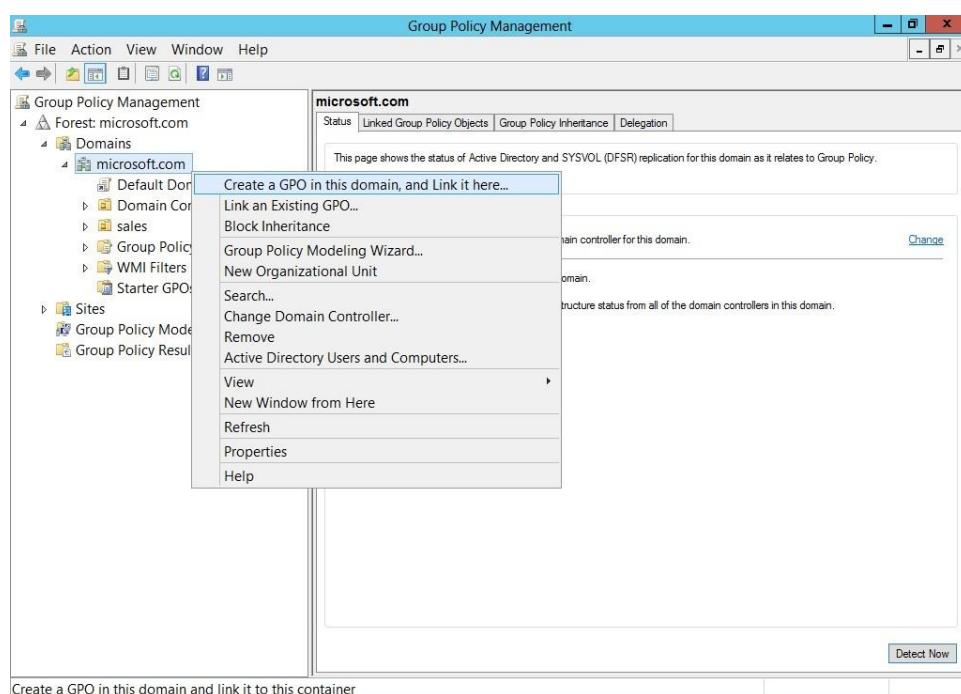


Lab – 2: Applying Group Policy on Domain Level

1. Press Windows Key to go to Start, select **Group Policy Management**.



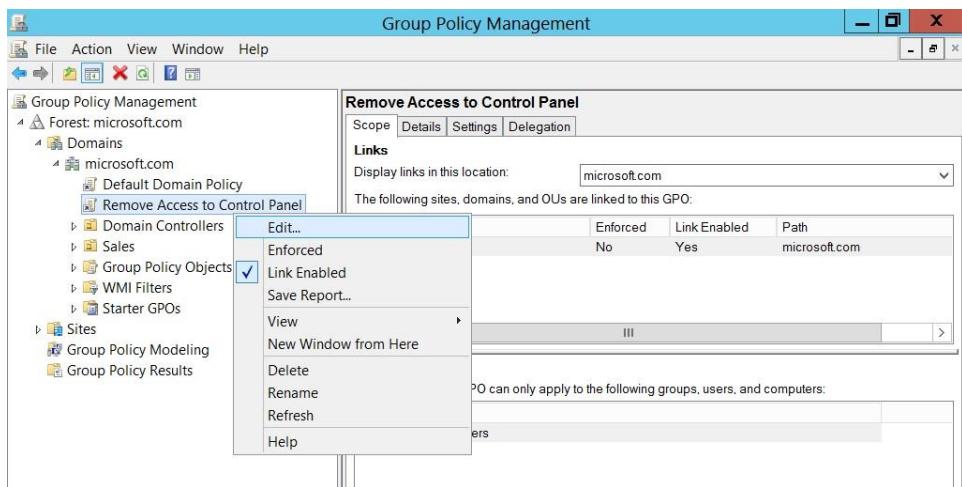
2. Right click Domain name (**MICROSOFT.COM**) and select **Create a GPO in this domain and Link it here.**



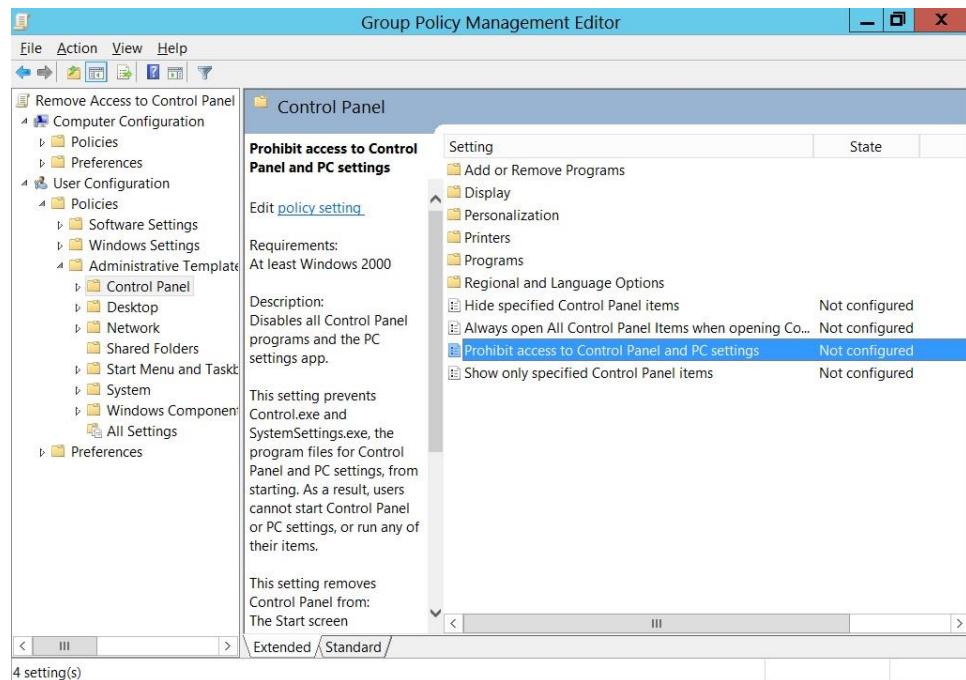
3. Enter New GPO Link name Ex: **Remove Network Icon** and click **OK**.



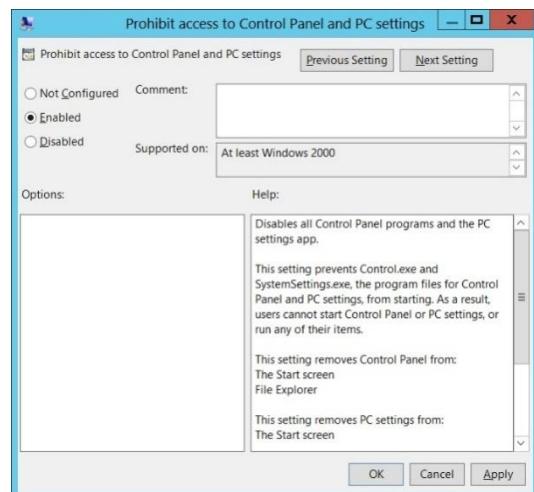
4. Select the Created GPO → Right Click Created GPO → Select **Edit**.



5. In the Group Policy Management editor window, Go to **User Configuration** → **Policies** → **Administrative Templates** → **Control Panel**
6. Select a policy (**Prohibit Access to Control Panel and PC Settings**) right side of the screen, Right Click and select **Properties**.

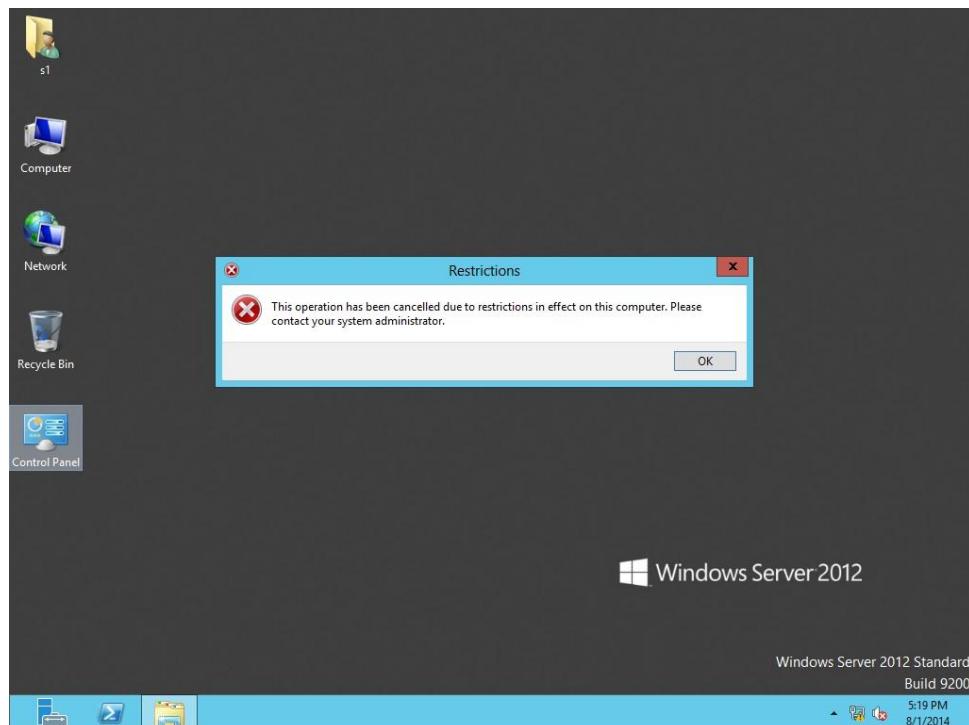


7. Select Enabled option and click Apply and OK



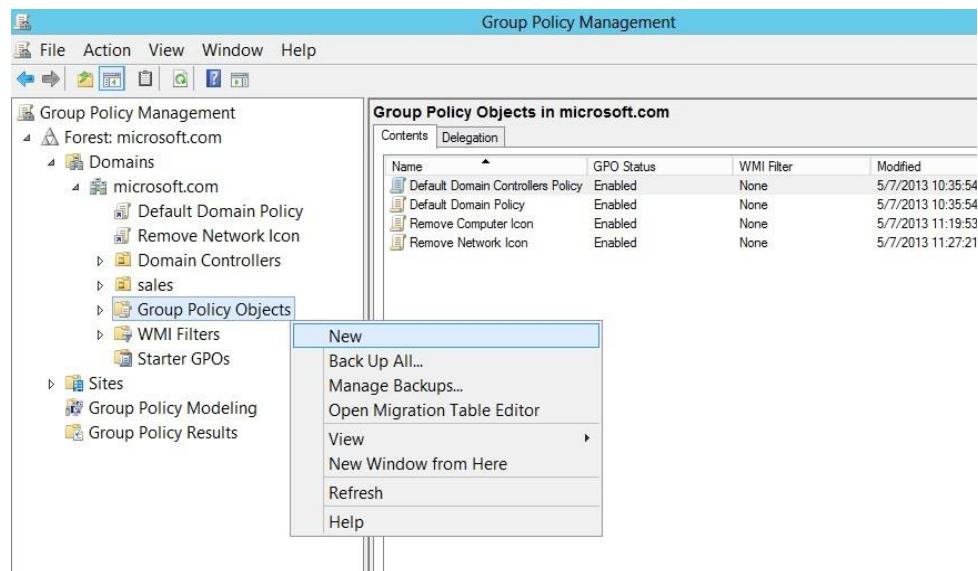
Verification:

1. Login as User (**S1**) to Client or Member Server and try to access Control Panel.

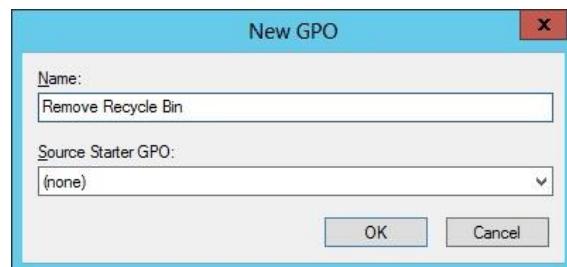


Lab – 3: Applying Group Policy on Site Level

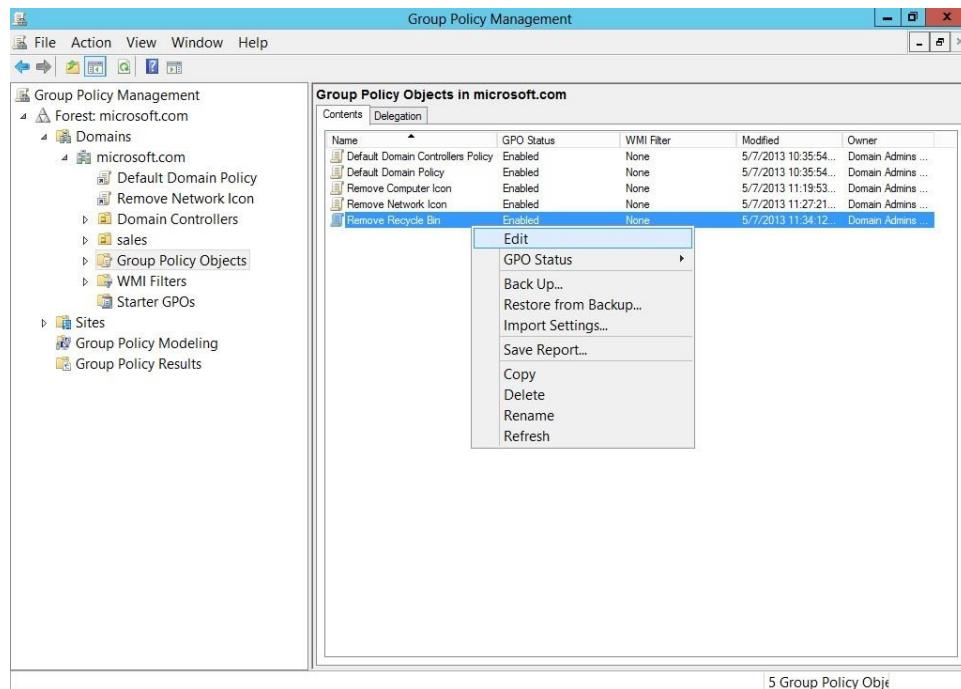
1. Go to Start, **Group Policy Management** → Right click **Group Policy Objects** → Select **New**.



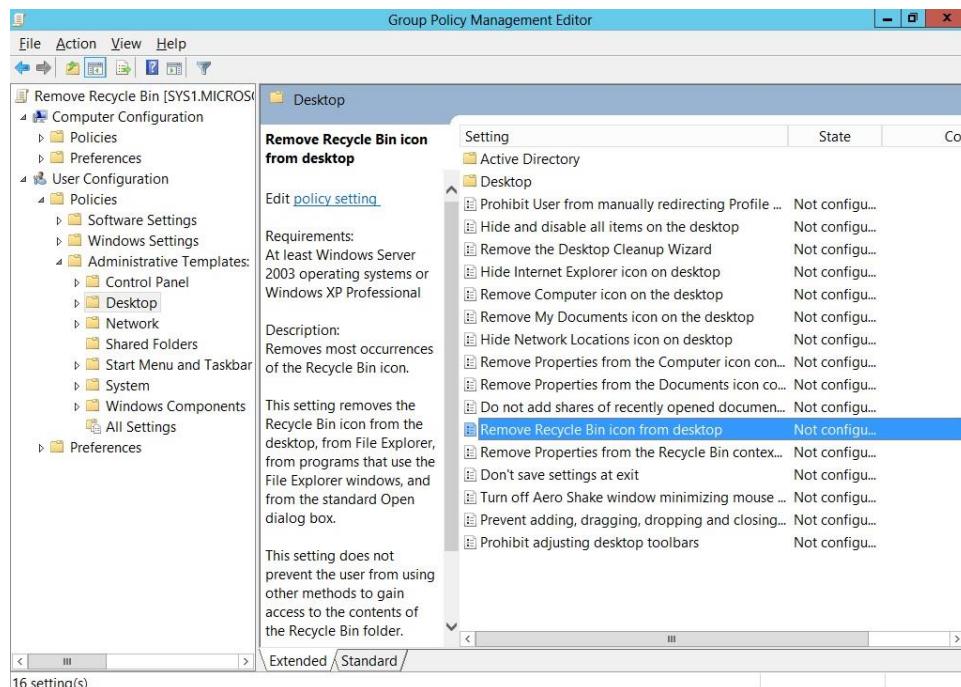
2. Enter New GPO Link name Ex: **Remove Recycle Bin** and click **OK**.



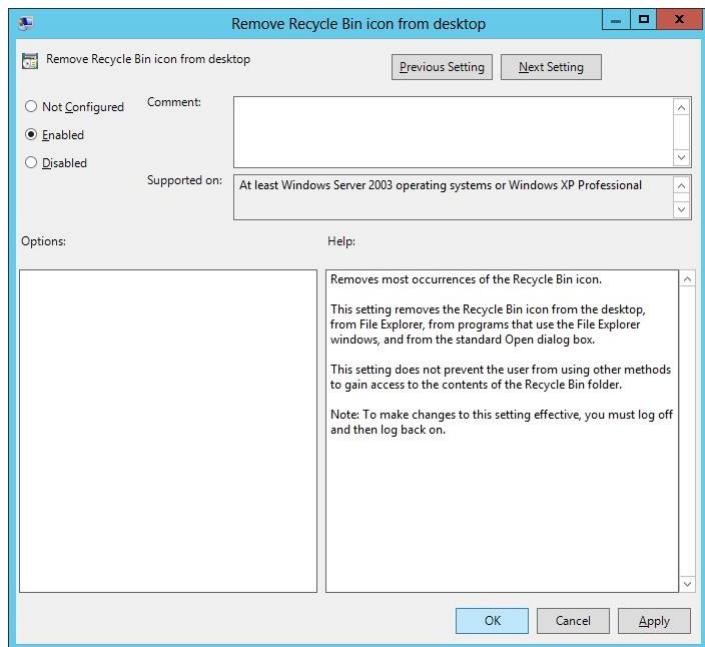
3. Select the Created GPO → Right Click Created GPO → Select **Edit**.



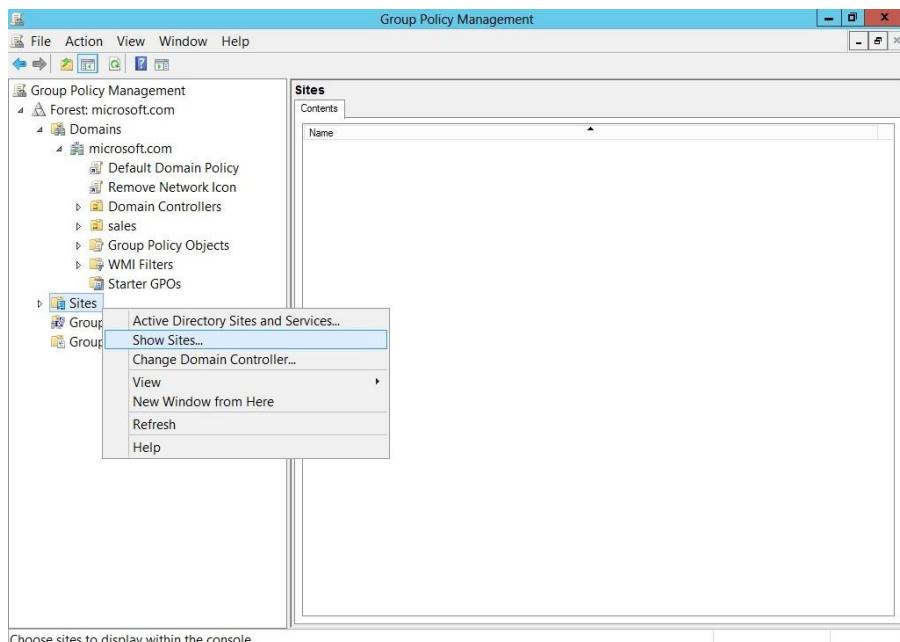
4. Select User Configuration → Policies → Administrative Templates → Desktop, select **Remove Recycle Bin icon from desktop**.



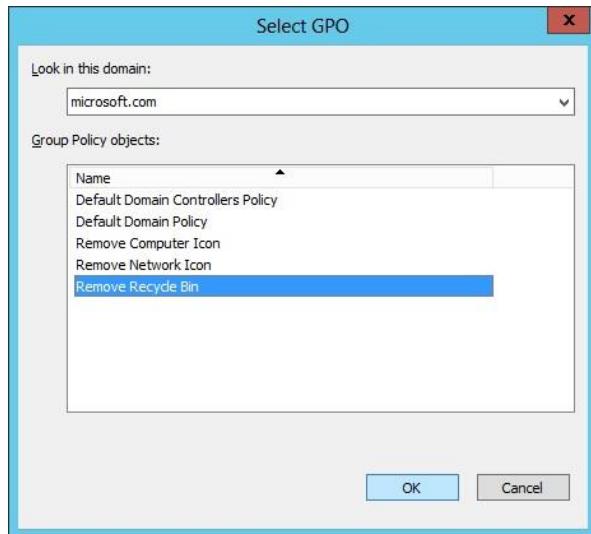
5. Right click Remove Recycle Bin icon from desktop → Properties, select **Enabled** → OK → Close.



6. Right click **Sites** → select **Show Sites** → check **Default-First-Site-Name** → click **OK**
→ Right Click **Default-First-Site-Name** → select **Link an Existing GPO....**



7. Select an existing GPO, (**Remove Recycle Bin**) click **OK**.

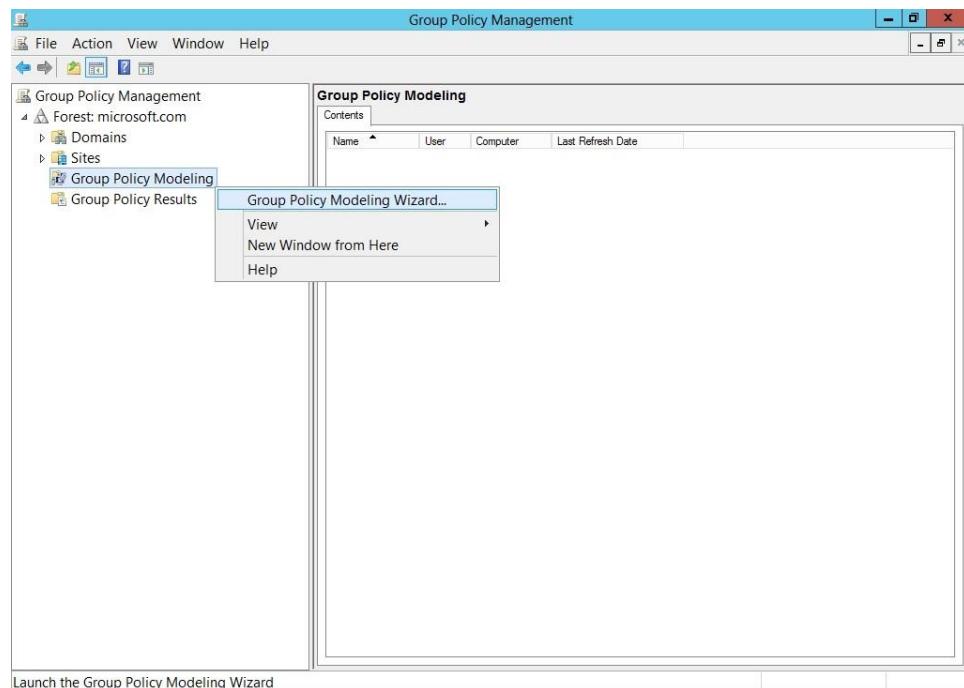


Verification:

1. Login as a user to **Client or Member Server**, and Verify for the changes.

Lab – 4: Applying Group Policy Modeling

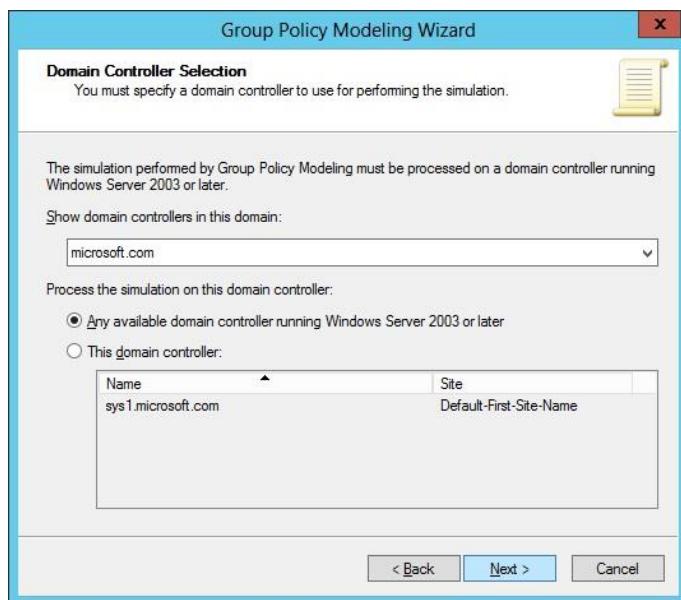
1. Go to Group Policy Management → Right Click **Group Policy Modeling** and Select **Group Policy Modeling Wizard**.



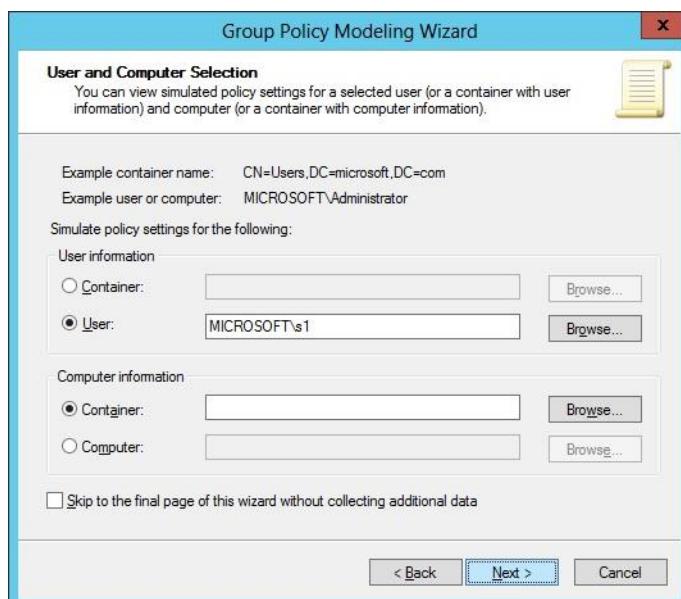
2. Click **Next**.



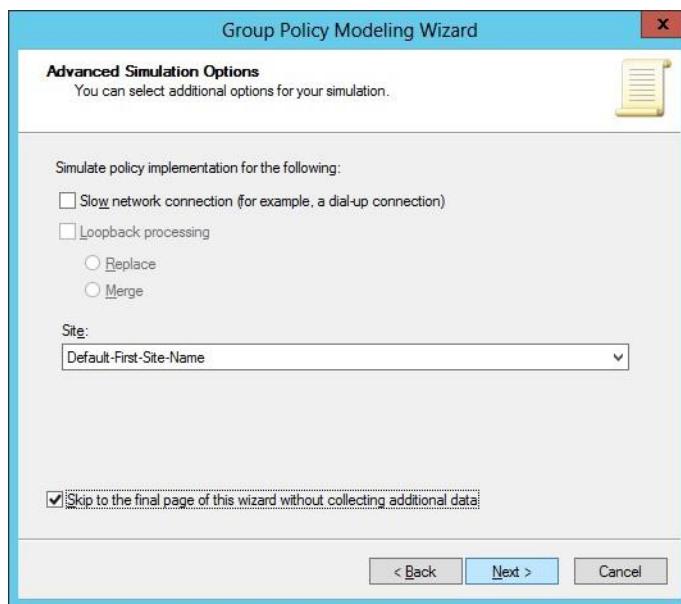
3. Select the domain name and click **Next**.



4. Select User and click Browse → enter the Username (**S1**)→click **OK** and **Next**.



- 5. Select the site (**Default-First-site-Name**) and check skip to final page, click **Next**.**



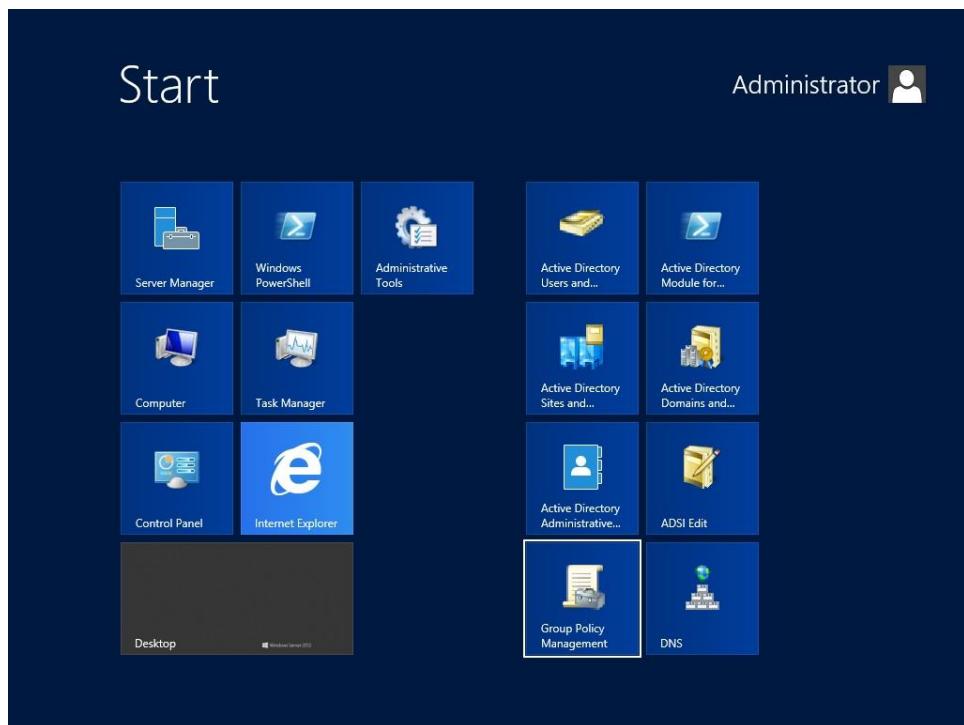
- 6. Click **Next** → **Finish**.**

Verification:

- 1. Click Details on the summary page and verify the policies applied on the User.**

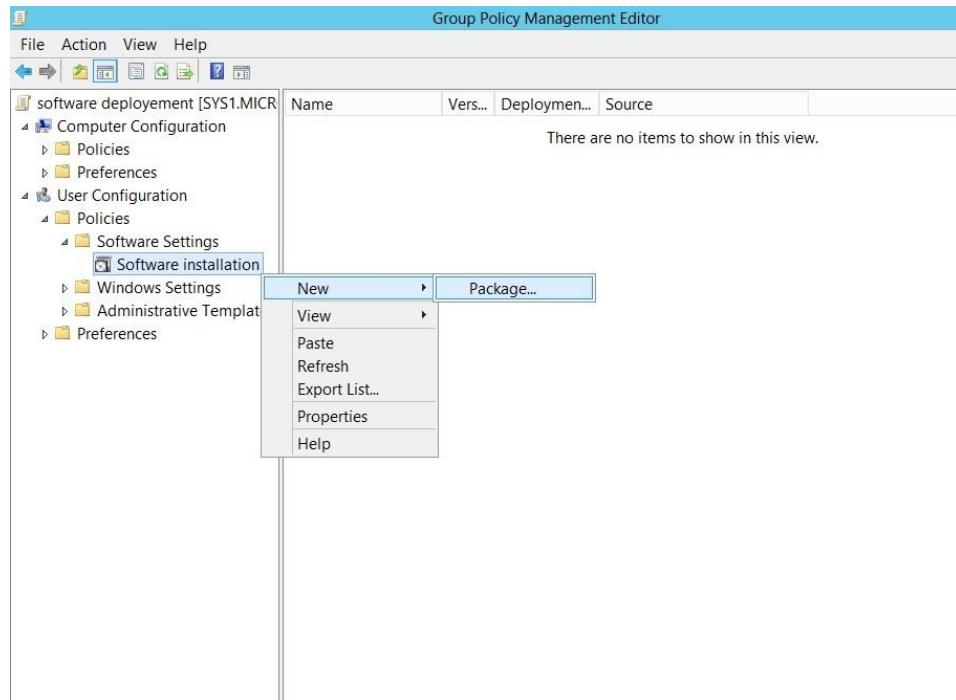
Lab – 5: Applying Software Deployment Policy

1. Logon to D.C as Administrator, Create a Shared folder with (.msi) applications in it
2. Go to **Group Policy Management**.

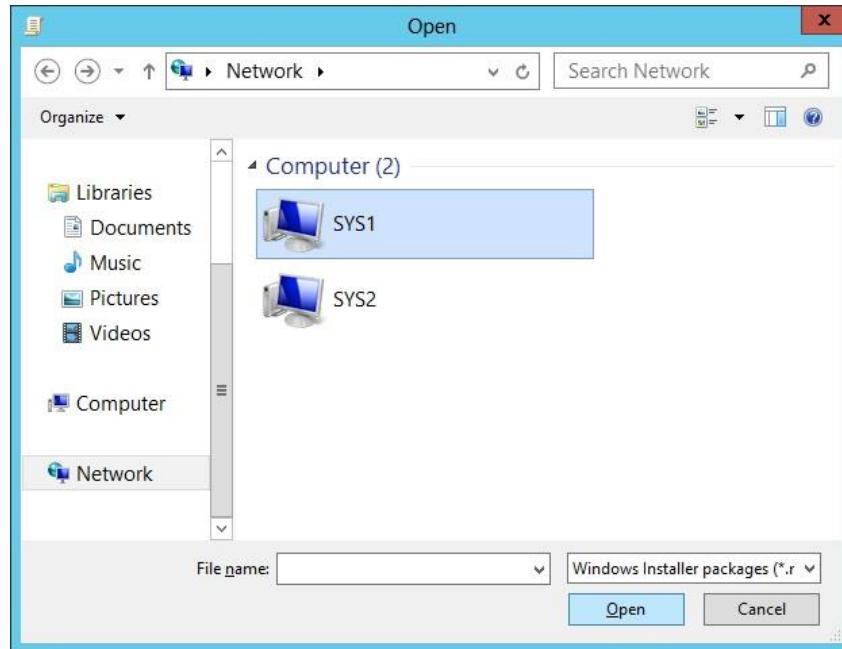


3. Right click OU (**Sales1**) →Create a GPO in this domain and Link it here → Enter the name (Software Deployment) →click OK, Right click the policy and click **Edit**.

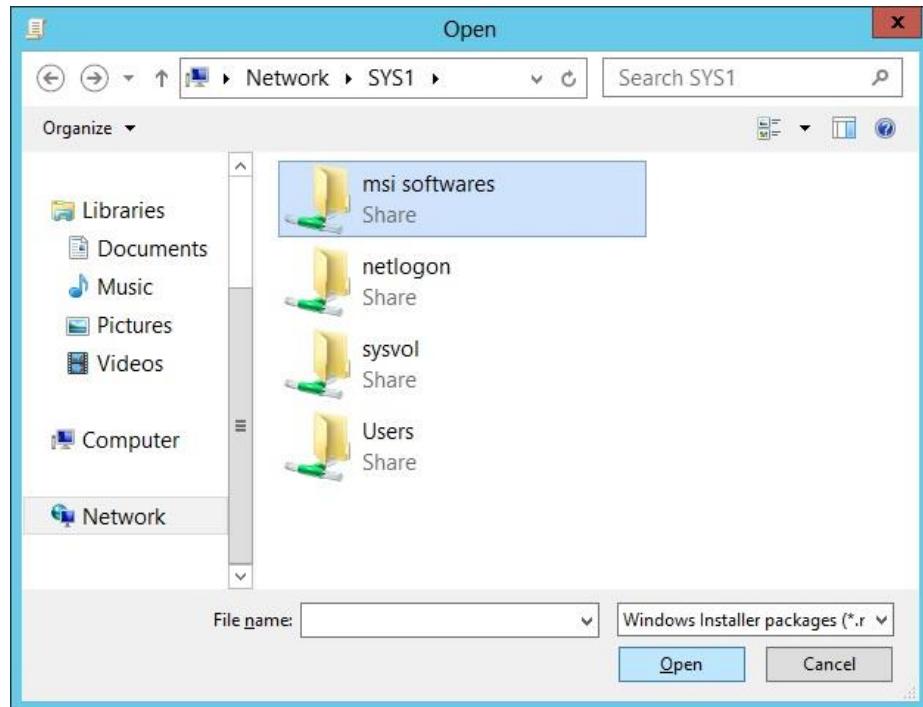
4. User Configuration → Expand Policies → Expand Software settings → Right click Software Installation → Select New → Package



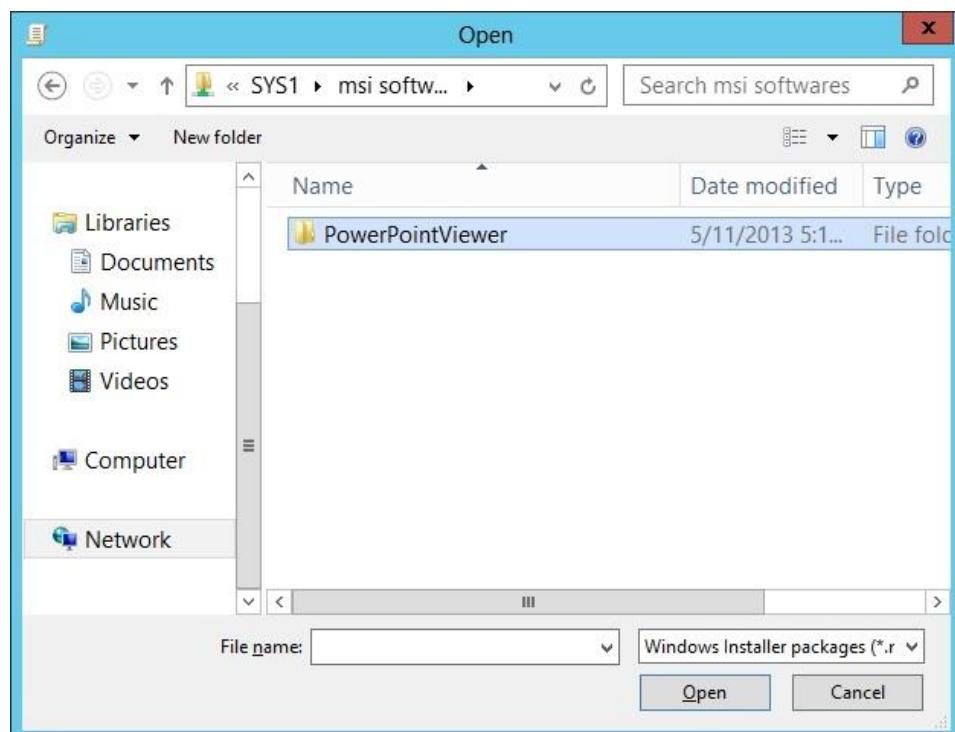
5. From the left pane, select Network, Open **SYS1** (Server containing shared folder).



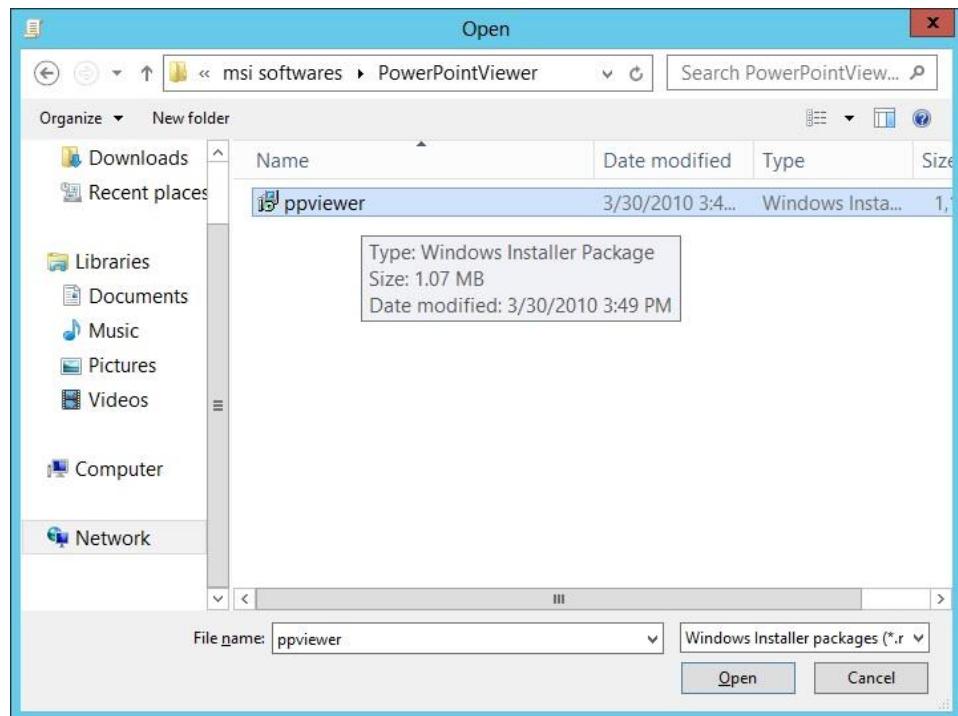
6. Select the **MSI Softwares** Shared Folder → click **Open**.



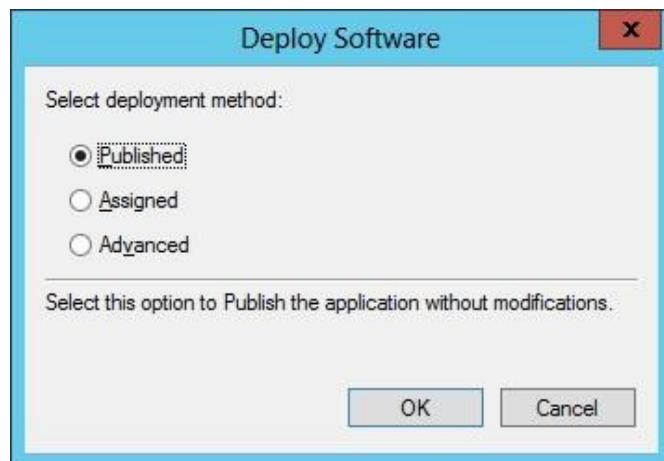
7. Select the Application Folder (**Power Point Viewer**) → click **Open**.



8. Select the Application (**PPVIEWER**) → click **Open**.

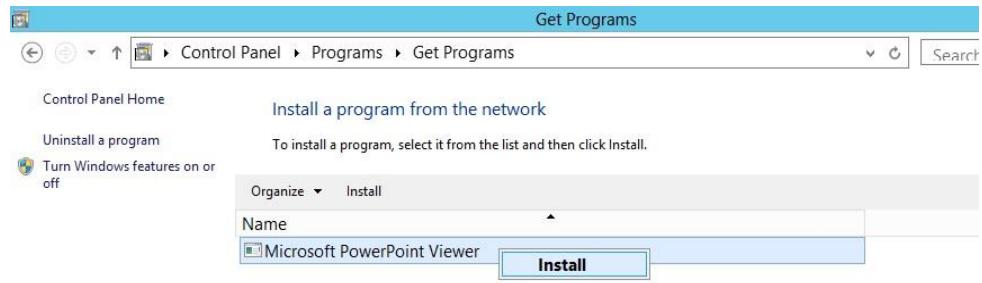


9. Select the **Method to Deploy Application (Published)** and click **OK**.



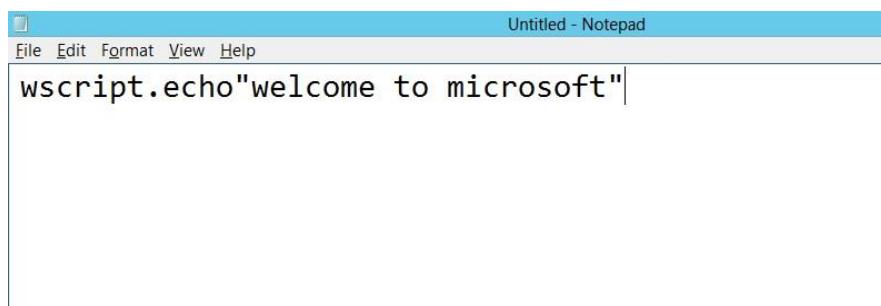
Verification:

1. Go to Member Server and login as **user1**.
2. Go to Control Panel, click **Programs and Features**.
3. Click **Install a Program from the Network**, Select the **Application** and **Install**



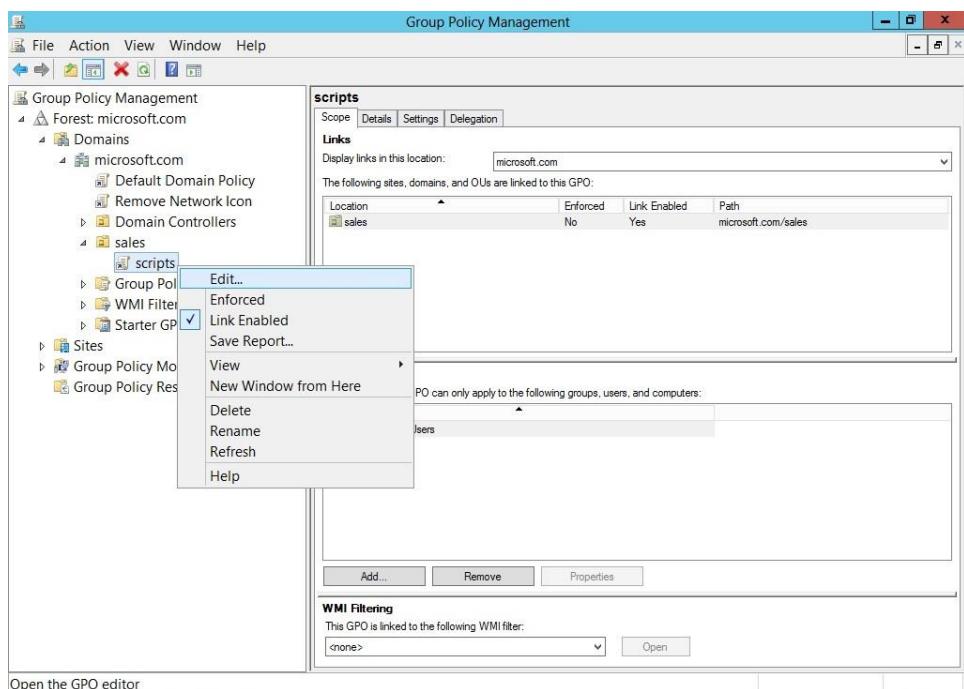
Lab – 6: Applying Scripts using Group Policy.

1. Log on to D.C, create a Shared Folder **User Scripts** with Everyone as Read/write.
2. Go to Start, type Notepad in Search Apps, and select **Notepad**.
3. Enter the text **wscript.echo "Welcome to Microsoft"**

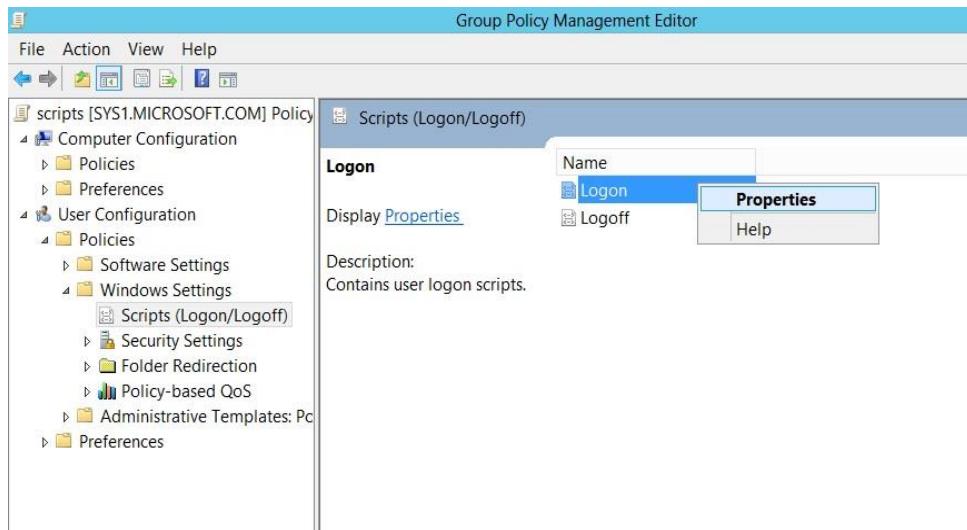


```
wscript.echo"welcome to microsoft"
```

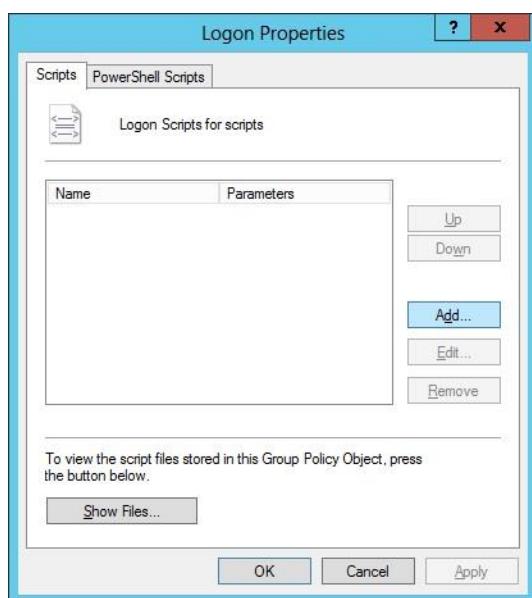
4. Save the file in the Shared folder **User Scripts** as **Logon.vbe**
5. Go to Group Policy Management → Right click **OU (Sales1)** → **Create a GPO in this domain and Link it here** and enter the name **Script**, click **OK**, Select the GPO Right Click and select **Edit**.



6. Expand User Configuration → Expand Policies → Windows Settings → Scripts
→ Logon → Properties.



7. Click Add.



8. Enter the UNC path for the Script in the shared folder
\SYST\Userscripts\logon.vbe and click OK → Apply and OK.

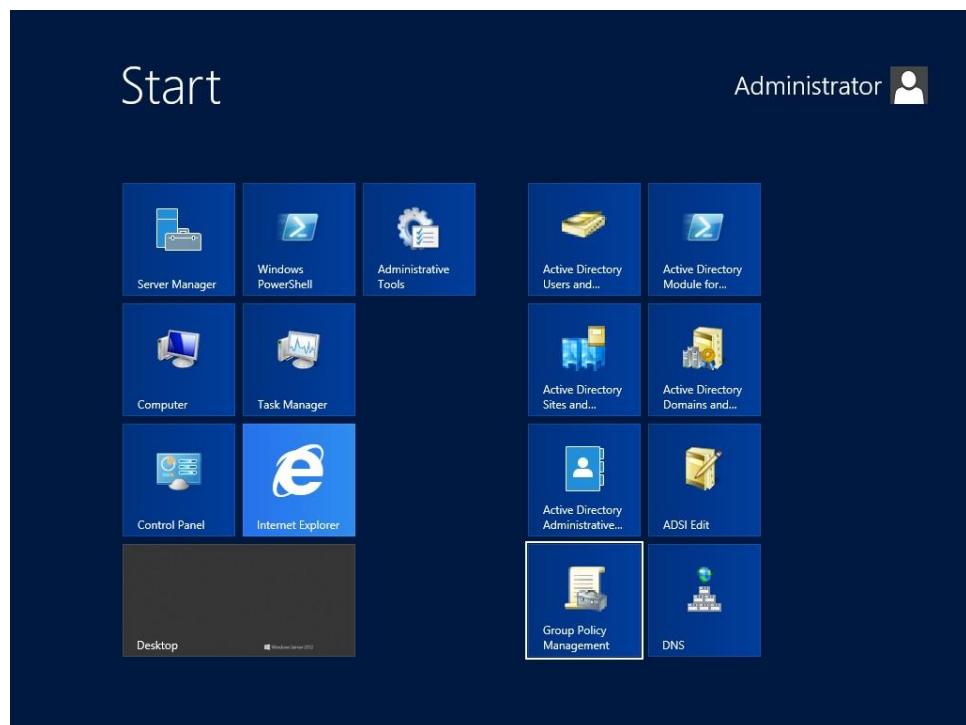
Verification:

1. Go to Member Server and login as USER1 and verify for the Message.

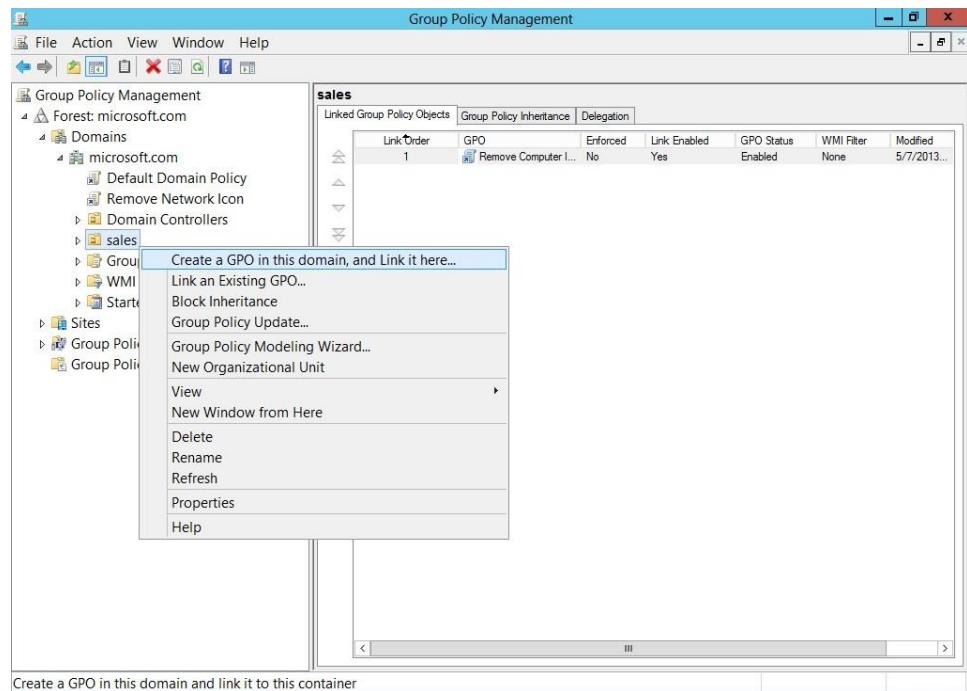


Lab – 7: Applying Folder Redirection

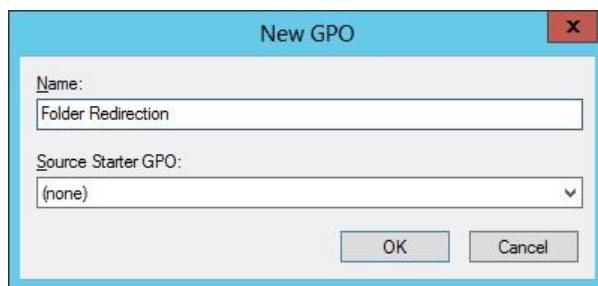
1. Go to D.C, create a Shared Folder (Folder Redirection) with everyone Read/Write.
2. Press Windows Key to go to Start, select **Group Policy Management**.



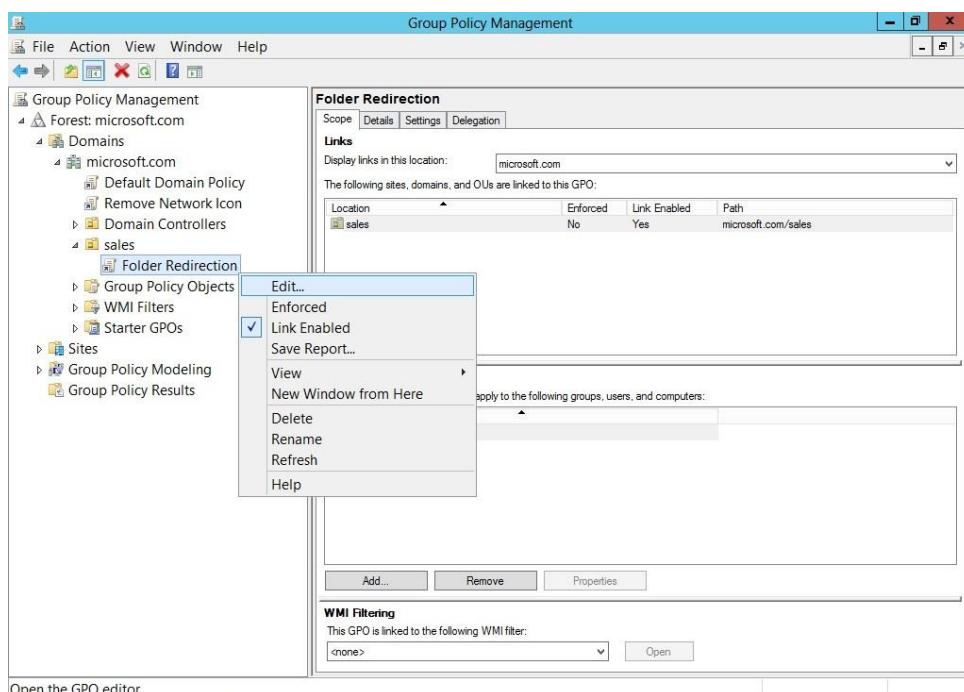
3. Right click OU (**Sales**) → Select **Create a GPO...**



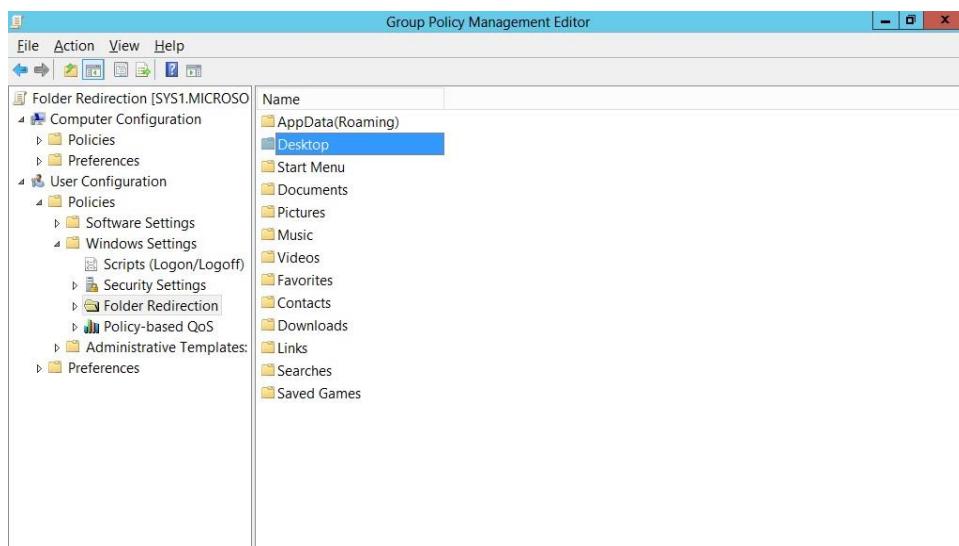
4. Enter name (Ex: **Folder Redirection**) and click **OK**.



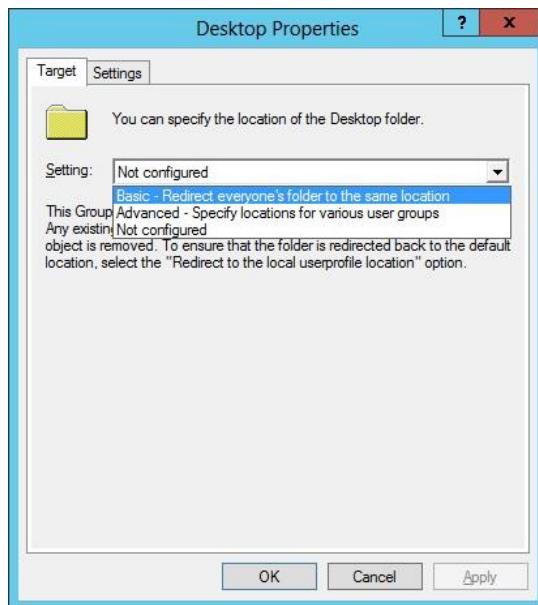
5. Right Click created GPO, select **Edit**.



6. Expand User configuration → Policies → Windows Settings → Folder Redirection → Select Desktop → Right click Desktop → Select Properties

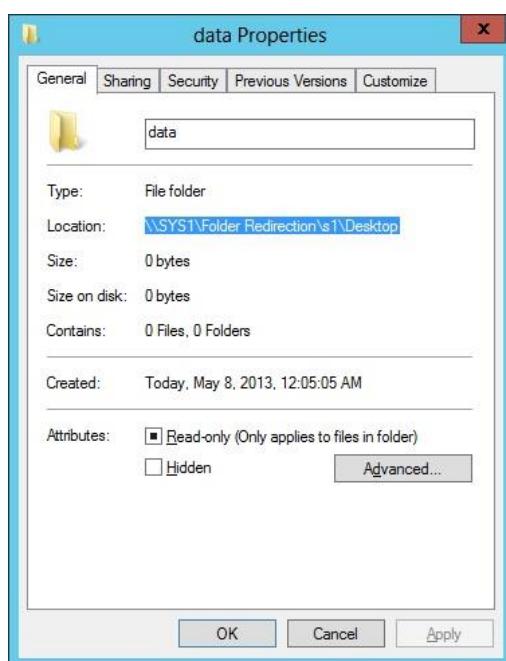


7. Select **Basic** Redirection, select **Create a folder for each user under the root path**, click **Browse** →select the shared folder from Network, **\\\SYS1\\Folder Redirection**, click **Apply** and **OK**.



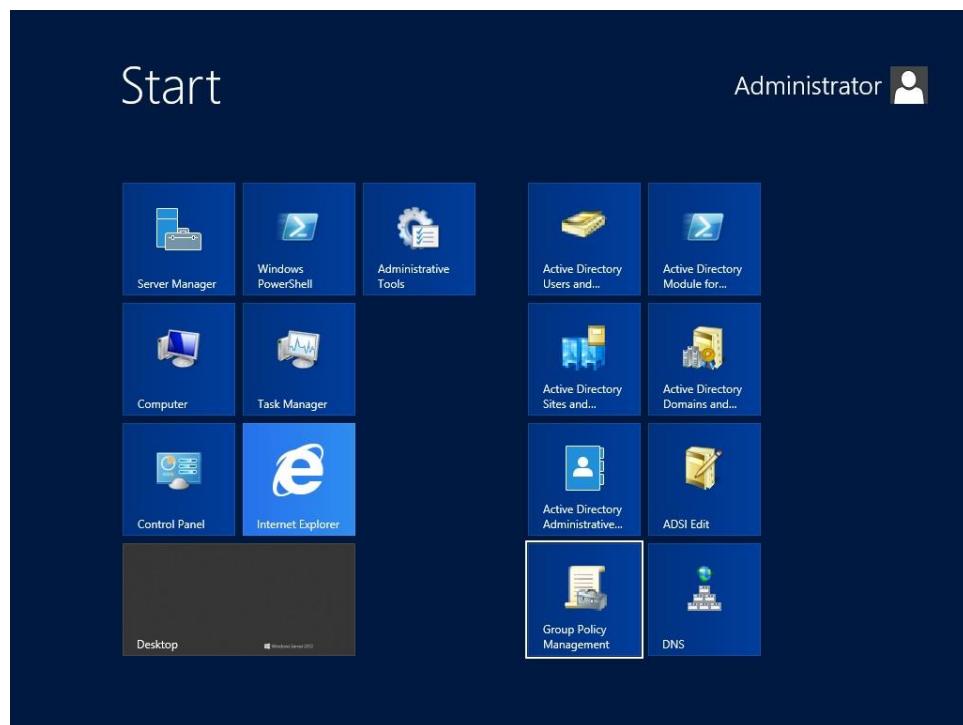
Verification:

1. Login as user (**S1**) in client system.
2. Create a folder on desktop, Right Click on the folder →**properties** and check the path, it should show **Network path (\\\SYS1\\FolderRedirection\\S1\\Desktop)**.

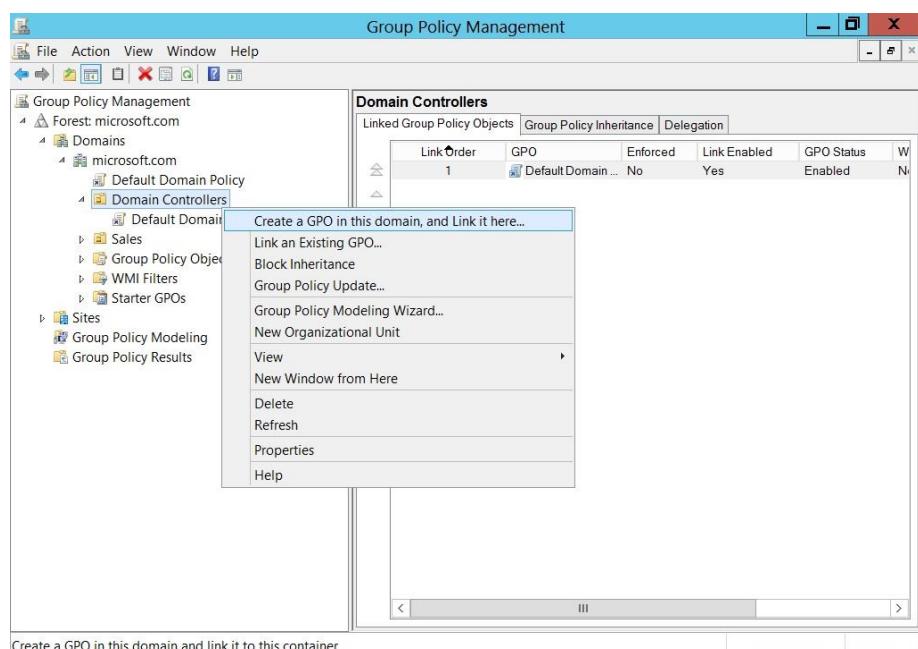


Lab – 8: Applying Auditing Policy

1. Press Windows Key to go to Start, select **Group Policy Management**.



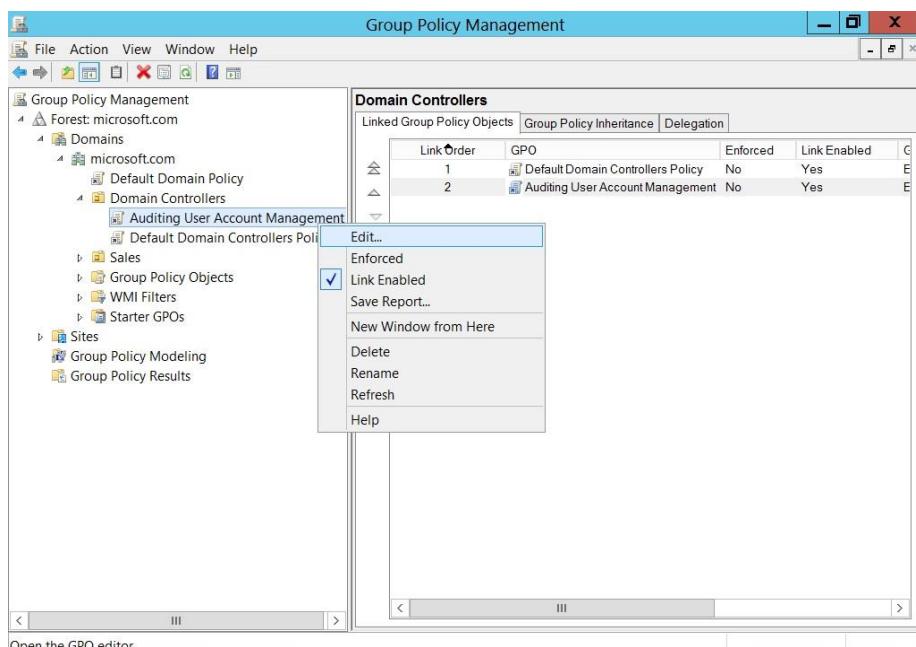
2. Right click Domain Controllers →Select **Create a GPO...**



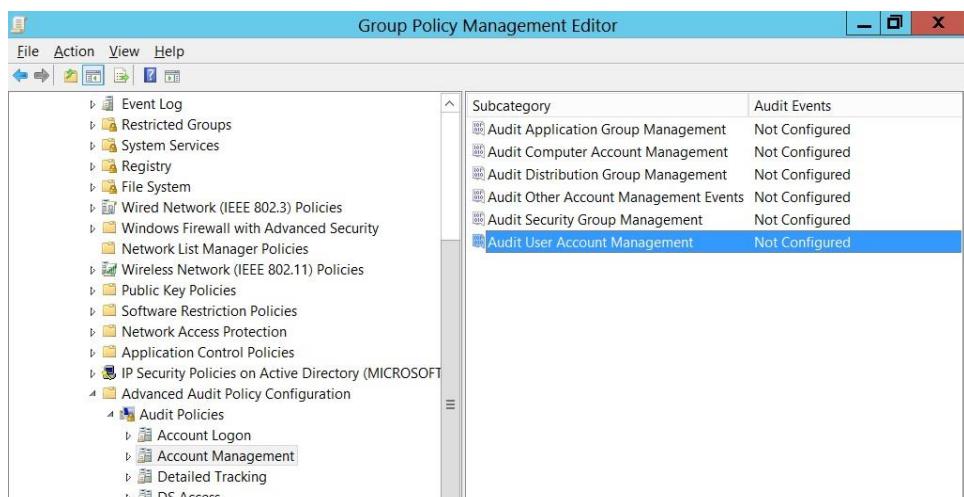
3. Enter name (Ex: **Auditing User Account Management**) and click **OK**.



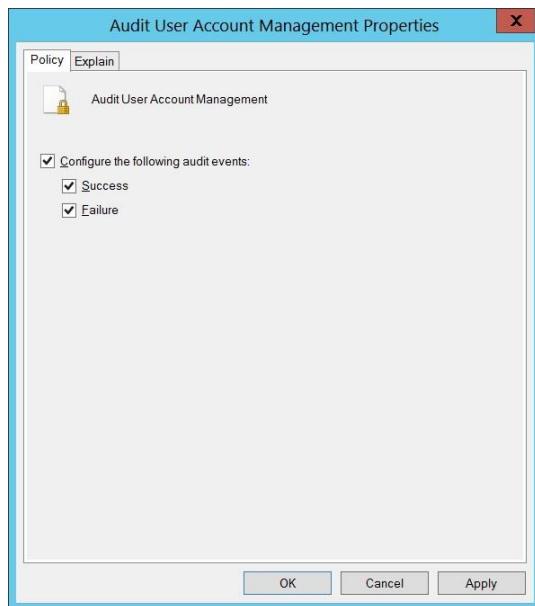
4. Right Click created GPO, select **Edit**.



5. Expand Computer configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Management → Right click **Audit User Account Management** → Select **Properties**

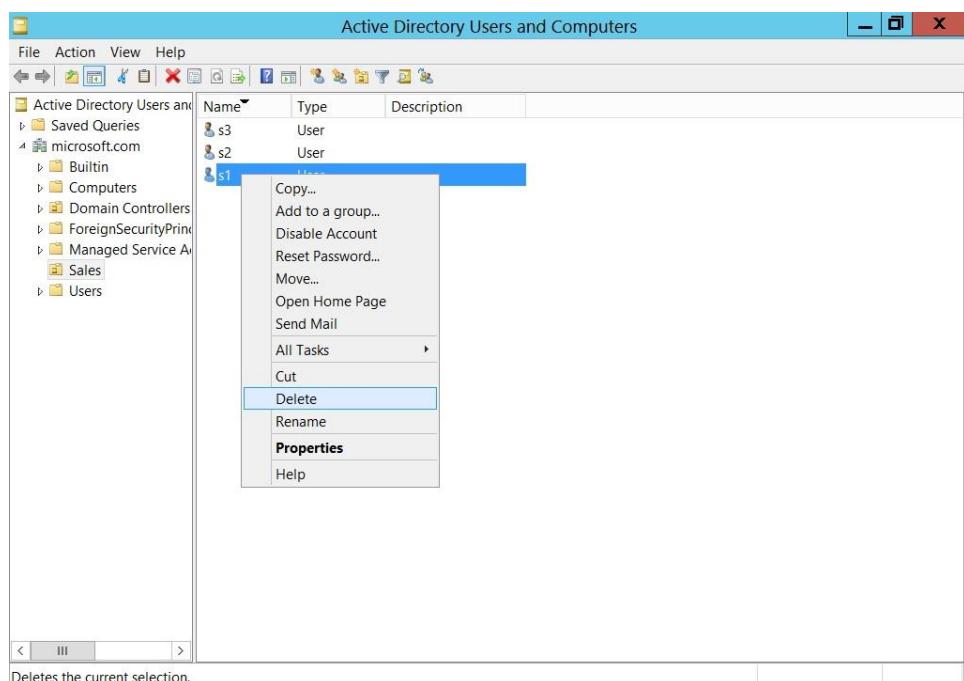


6. Check the box, **Configure the following audit events** and Select **Success** and **Failure**.

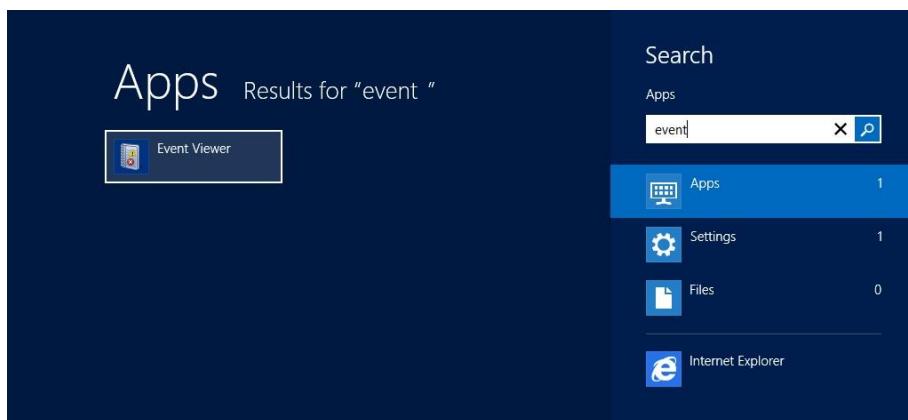


Verification:

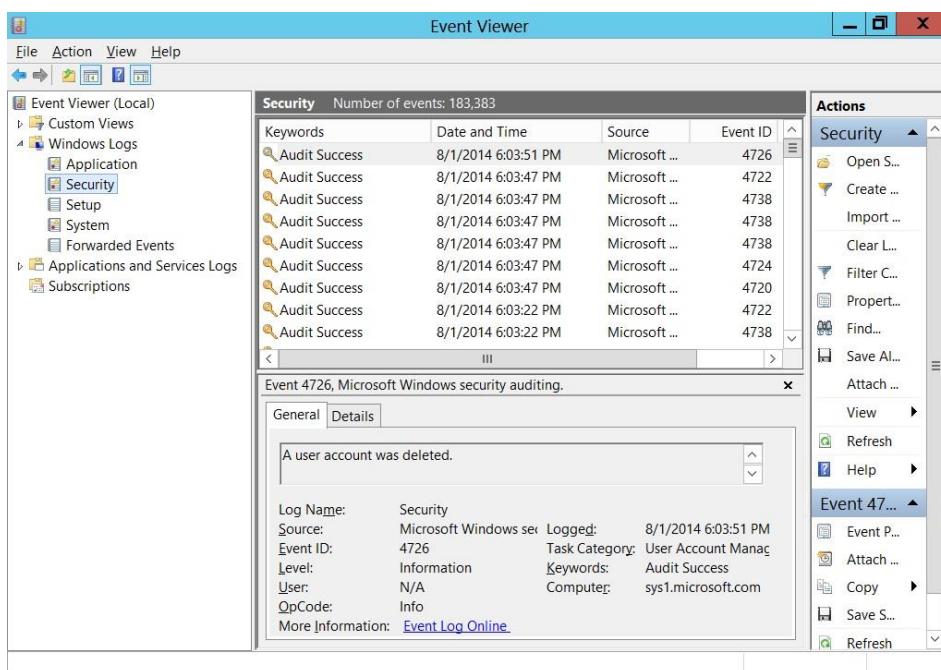
1. Login as Administrator on D.C, go to Active Directory Users and Computers and delete a user (S1).



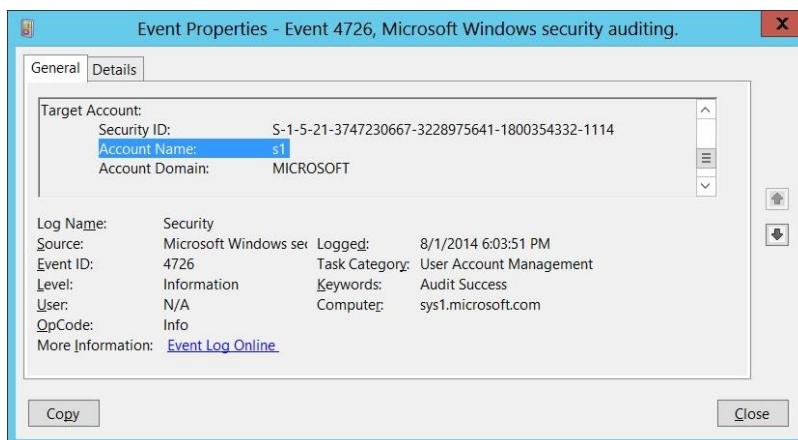
2. Go to Start, Type Event in Search Apps and select Event Viewer



3. Expand Windows Logs → Security and select the Event Audit Success Properties.

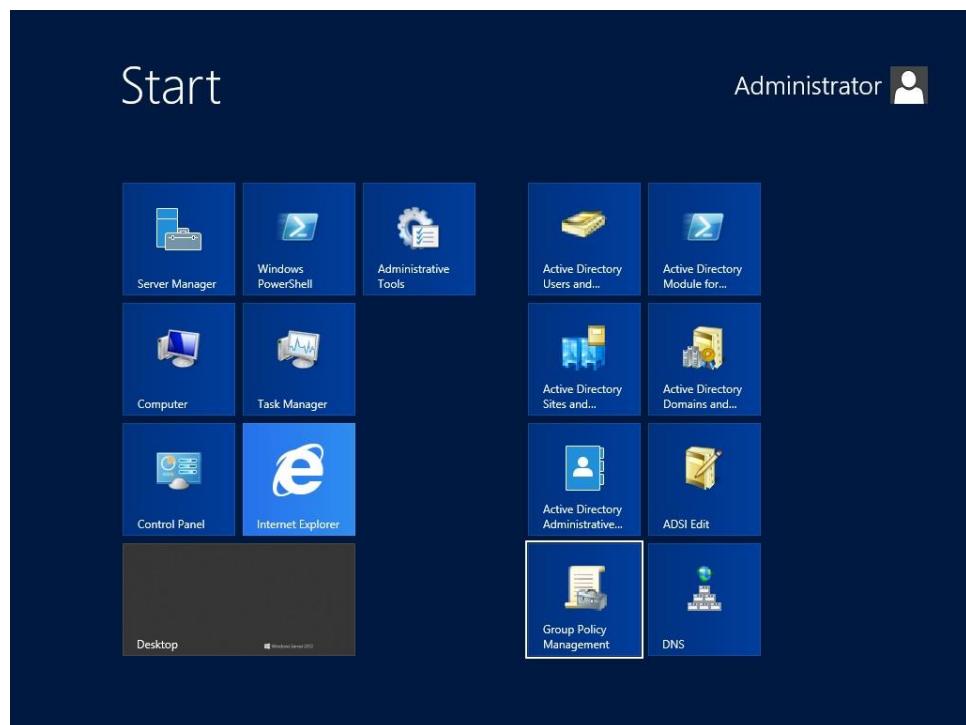


4. Verify the event displaying user s1 deleted by Administrator.

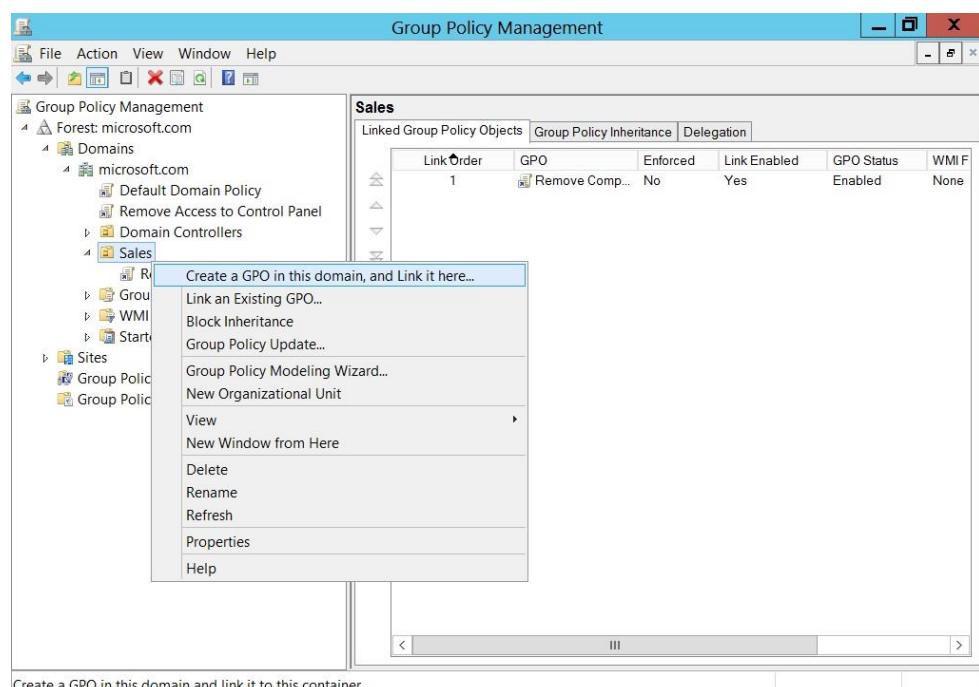


Lab – 9: Configuring Preferences using Item-level targeting

1. Press Windows Key to go to Start, select **Group Policy Management**.



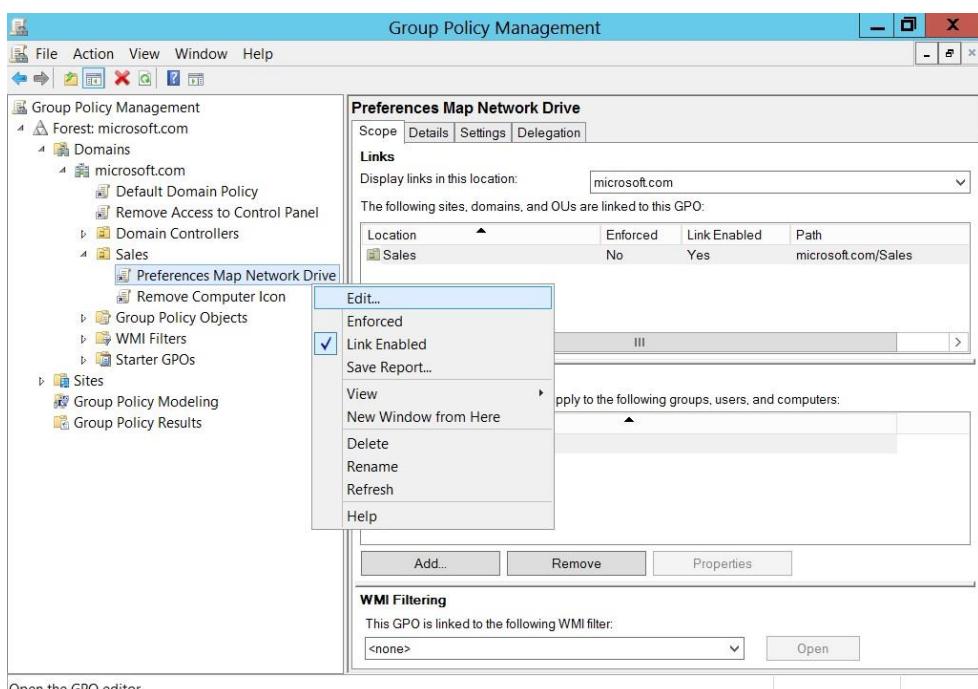
2. Right click Sales ou → Select **Create a GPO...**



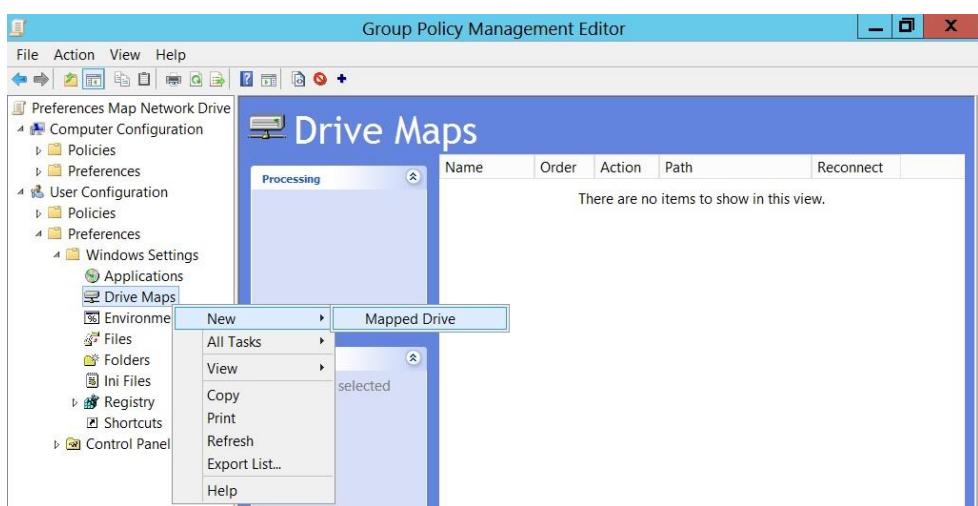
- 3. Enter name (Ex: Preferences Map Network Drive) and click OK.**



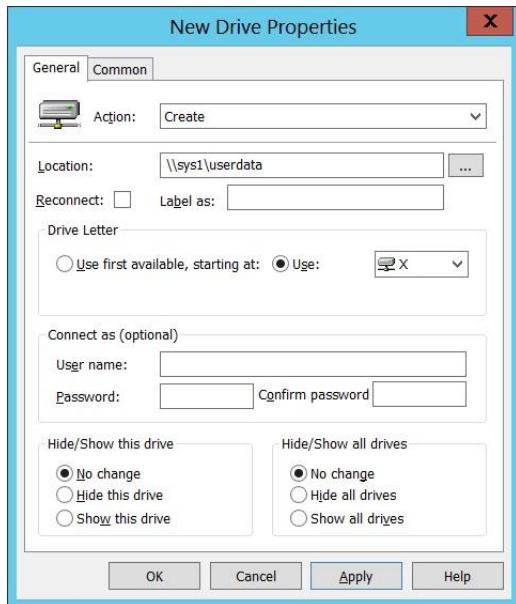
- 4. Right Click created GPO, select Edit.**



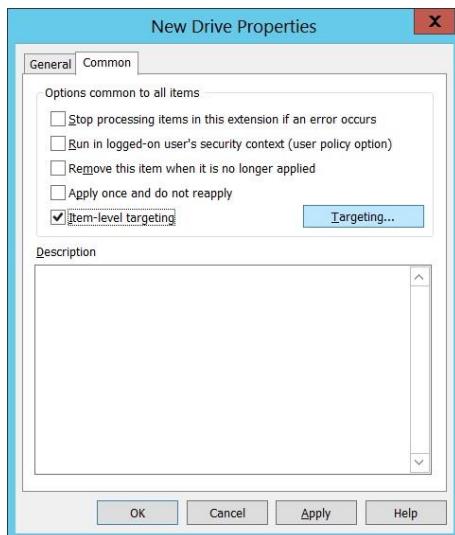
- 5. Expand User configuration → Preferences → Windows Settings → Right click Drive Maps → Select New Mapped Drive**



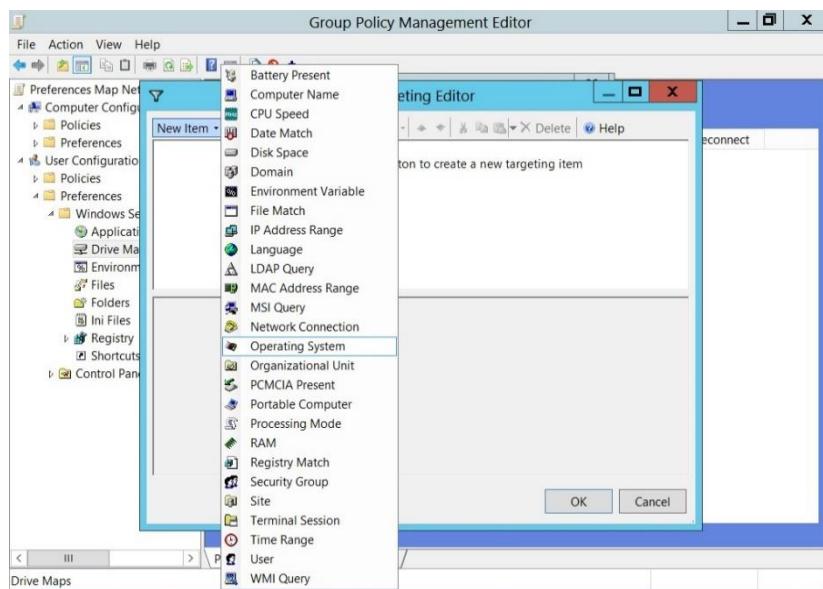
6. In Action select Create, Enter Location: (<\\sys1\\userdata>), select Drive Letter X:**→OK**



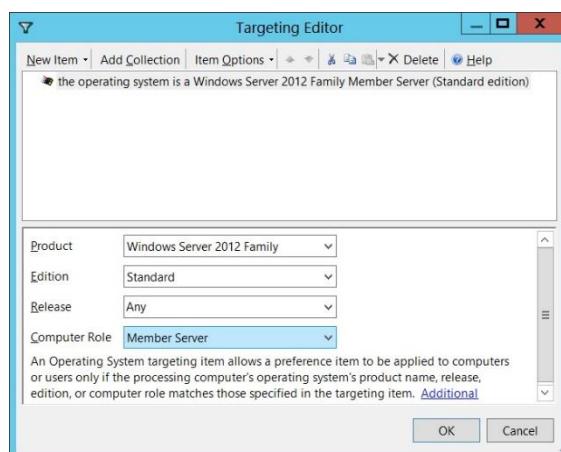
7. Select Common tab and check box Item-level targeting, click Targeting...



8. Select New Item → select Operating System

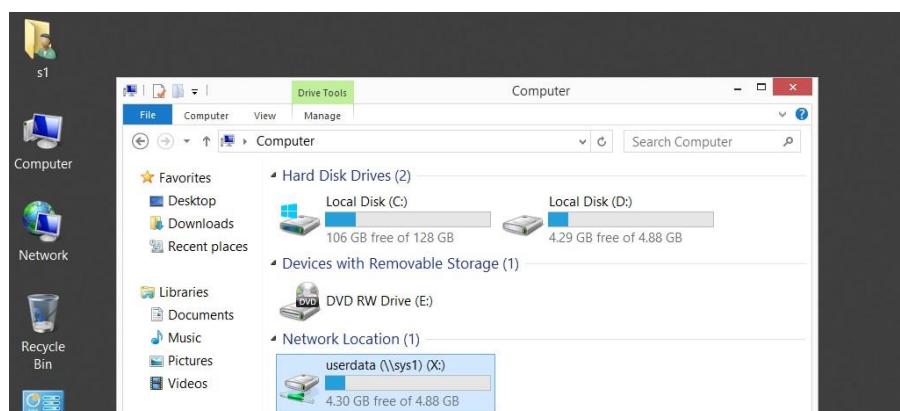


9. Select Product: WindowsServer2012Family, Edition: Standard, Computer Role: MemberServer, click OK.



Verification:

1. Login as user (S1) to Member Server.



ACTIVE DIRECTORY

Trust Relationships

- Secure communication paths that allow objects in one domain to be authenticated and accepted in other domains
- Some trusts are automatically created.
 - Parent-child domains trust each other
 - Tree root domains trust forest root domain
- Other trusts are manually created
- Forest-to-Forest transitive trust relationships can be created in Windows Server 2003, 2008 and Windows server 2012 forests only.

Trust Relationships

Trust categories	<ul style="list-style-type: none">• Transitive trusts• Nontransitive trusts
Trust directions	<ul style="list-style-type: none">• One-way incoming trust• One-way outgoing trust• Two-way trust
Trust types	<ul style="list-style-type: none">• Five types of trusts: Default, Shortcut, External, Forest and Realm

Types of Trusts

DEFAULT: Two-way-transitive Kerberos trusts (Intraforest)

SHORTCUT: One or two-way transitive Kerberos trusts (Intraforest) Reduce authentication requests

EXTERNAL: One way non-transitive NTLM trusts. Used to connect to/from Windows NT or external 2000 domains Manually created

FOREST: One or two-way transitive Kerberos trusts. Only between 2003,2008 or 2012 Forest Roots, Creates transitive domain relationship

REALM: One or two-way – non-transitive Kerberos trusts Connect to/from UNIX Kerberos realms

Transitive Trust

In this category,

If Domain A trust Domain B and Domain B trust Domain C then Domain A automatically trust Domain C

```

    graph TD
        A((DOMAIN A)) -- "Transitive Trust" --> B((DOMAIN B))
        B -- "Transitive Trust" --> C((DOMAIN C))
        A -- "Automatic Transitive Trust" --> C
    
```

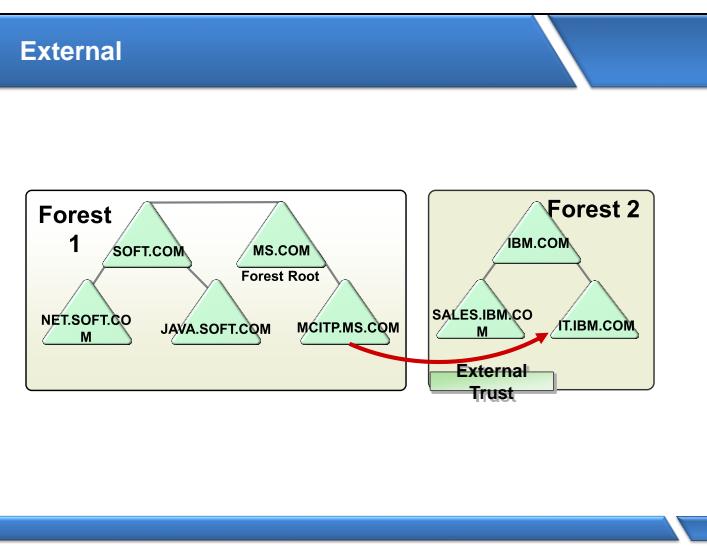
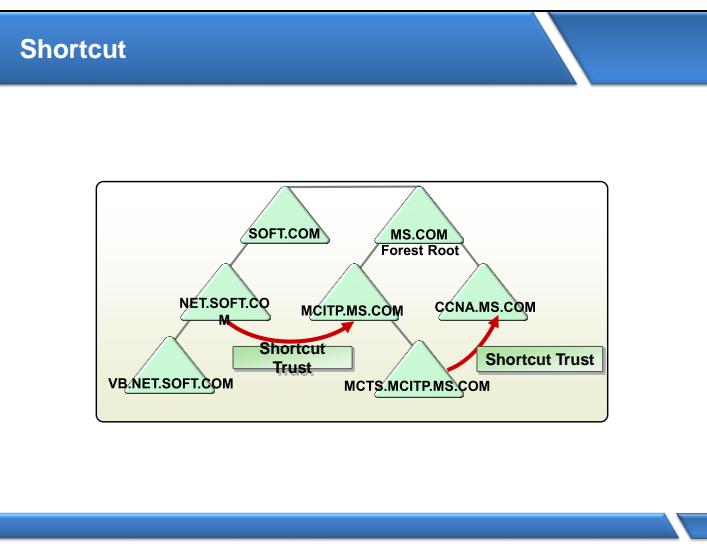
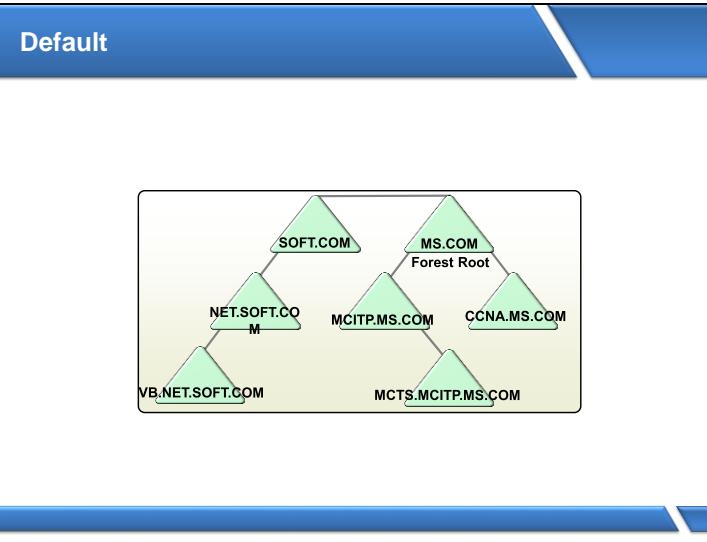
Non-Transitive Trust

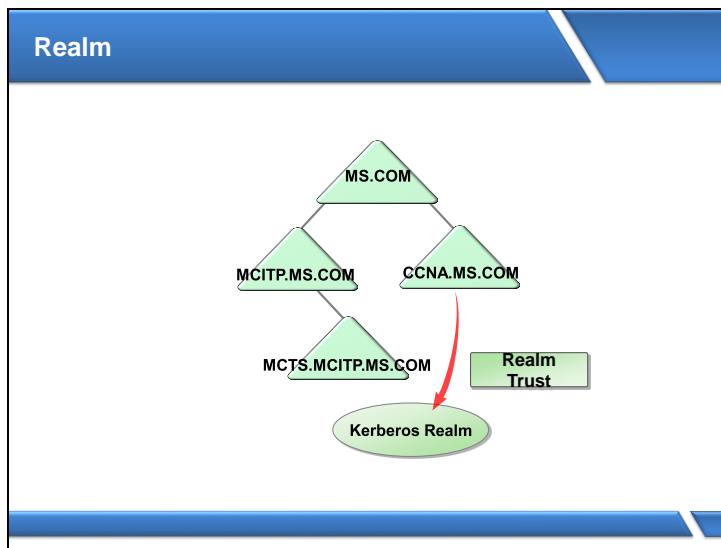
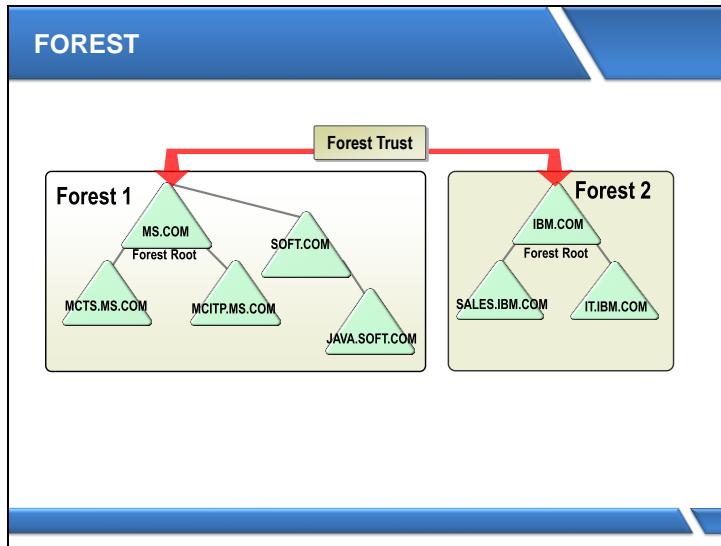
In this category,

If Domain A trust Domain B and Domain B trust Domain C then Domain A does not trust Domain C

```

    graph TD
        A((DOMAIN A)) -- "Non-Transitive Trust" --> B((DOMAIN B))
        B -- "Transitive Trust" --> C((DOMAIN C))
        A -- "No Automatic Trust" --> C
    
```





FUNCTIONAL LEVELS

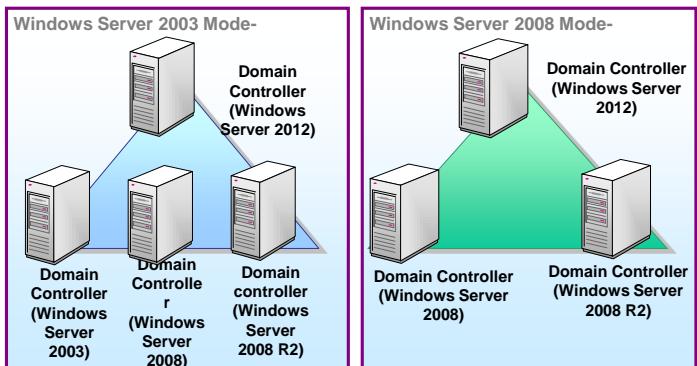
Functional Levels

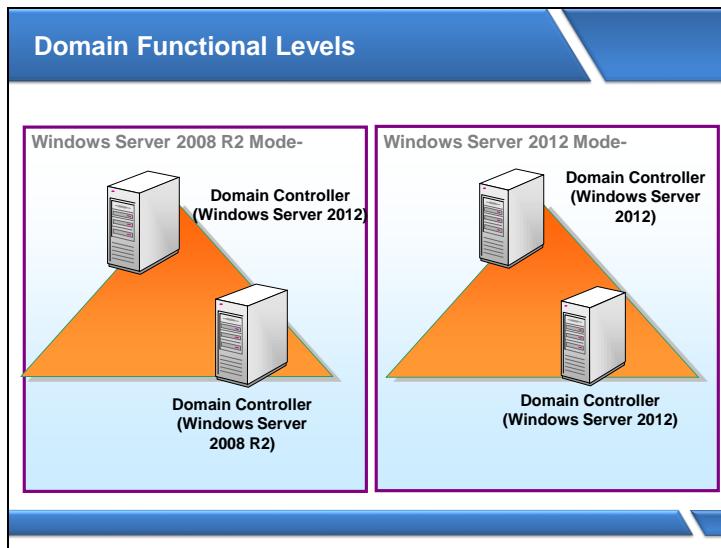
- Functional levels determine
 - Supported domain controller operating system
 - Active Directory features will be available

Domain Functional Levels

Domain Functional Levels	Operating systems Supported on Domain controllers
Windows Server 2003	Windows Server 2003 OS, Windows Server 2008 OS, Windows Server 2008 R2 OS, Windows Server 2012 OS
Windows Server 2008	Windows Server 2008 OS, Windows Server 2008 R2 OS, Windows Server 2012 OS
Windows Server 2008 R2	Windows Server 2008 R2 OS, Windows Server 2012 OS
Windows Server 2012	Only Windows Server 2012 OS

Domain Functional Levels





Forest Functional Levels

Forest Functional Levels	Supported Domain Functional Levels
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012
Windows Server 2012	Only Windows Server 2012

Domain & Forest Functional Levels

- Domain functional levels can be raised independently of other Domains
- Raising forest functional level is performed by Enterprise Admin
 - Requires all Domain Functional levels to be at Windows Server 2003 or Windows Server 2008 functional levels

Active Directory Recycle Bin

- Active Directory Recycle Bin provides a way to restore deleted objects without AD DS downtime
- Uses Windows PowerShell with Active Directory Module or the Active Directory Administrative Center to restore objects

The diagram illustrates the object lifetime cycle in the Active Directory Recycle Bin:

- Live**: The initial state of the object.
- Deleted**: Reached by performing a **Delete** operation on the Live object.
- Recycled**: Reached by performing a **Recycle** operation on the Deleted object.
- Physically deleted**: Reached by performing a **Garbage-collect** operation on the Recycled object.

Annotations provide additional context:

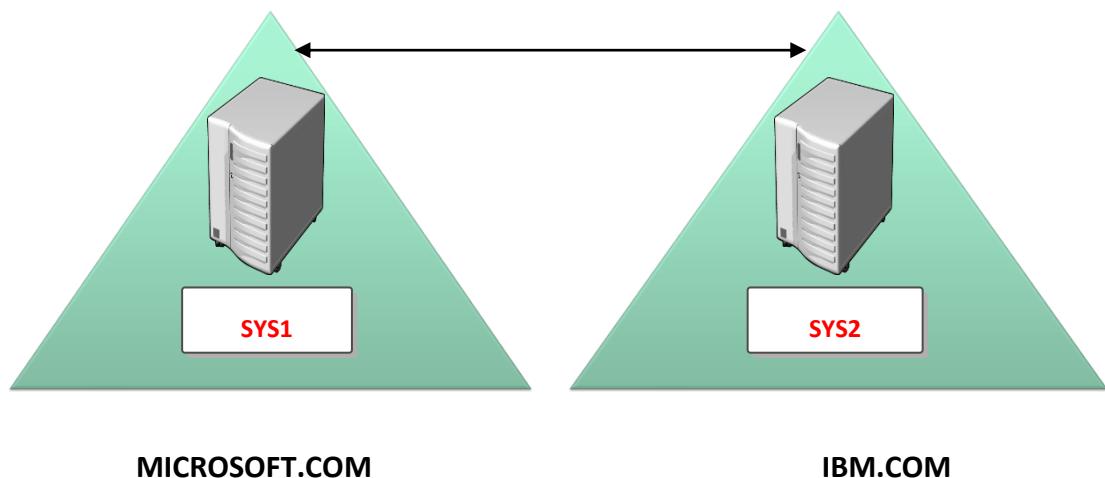
- A curved arrow from **Deleted** back to **Live** is labeled **Undelete/authoritative restore**.
- A horizontal dashed line below the **Deleted** and **Recycled** states is labeled **Deleted object lifetime**.
- A horizontal dashed line below the **Recycled** and **Physically deleted** states is labeled **Recycled object lifetime**.

TRUST RELATIONSHIP

Pre-requisites:

Before working on this lab, you must have

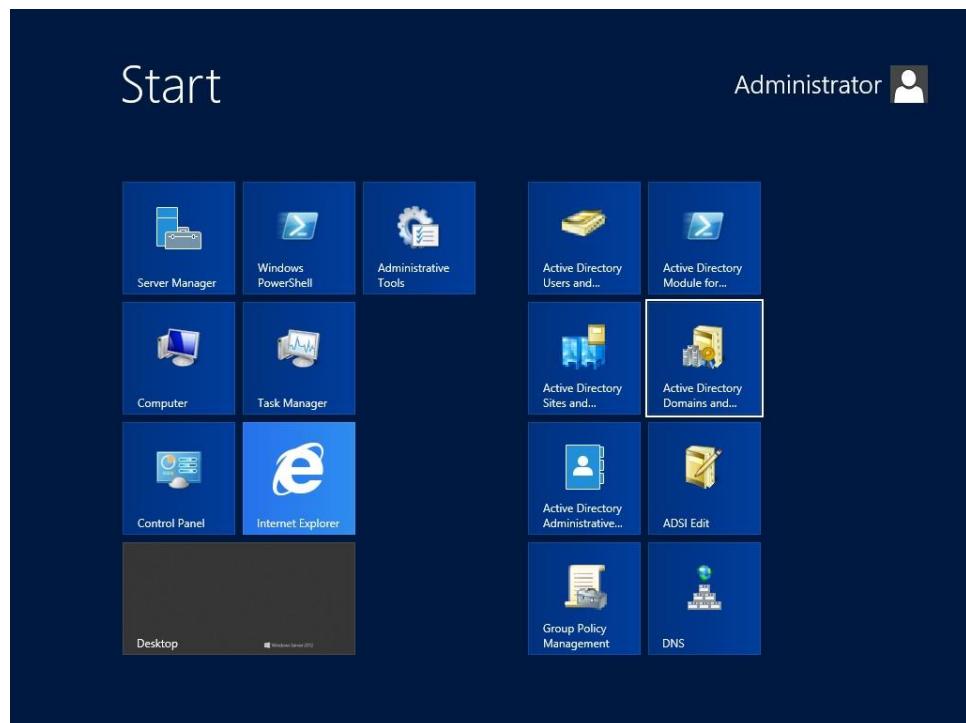
1. A computer running Windows Server 2012 Domain Controller for MICROSOFT.COM.
 2. A computer running Windows Server 2012 Domain Controller for IBM.COM.



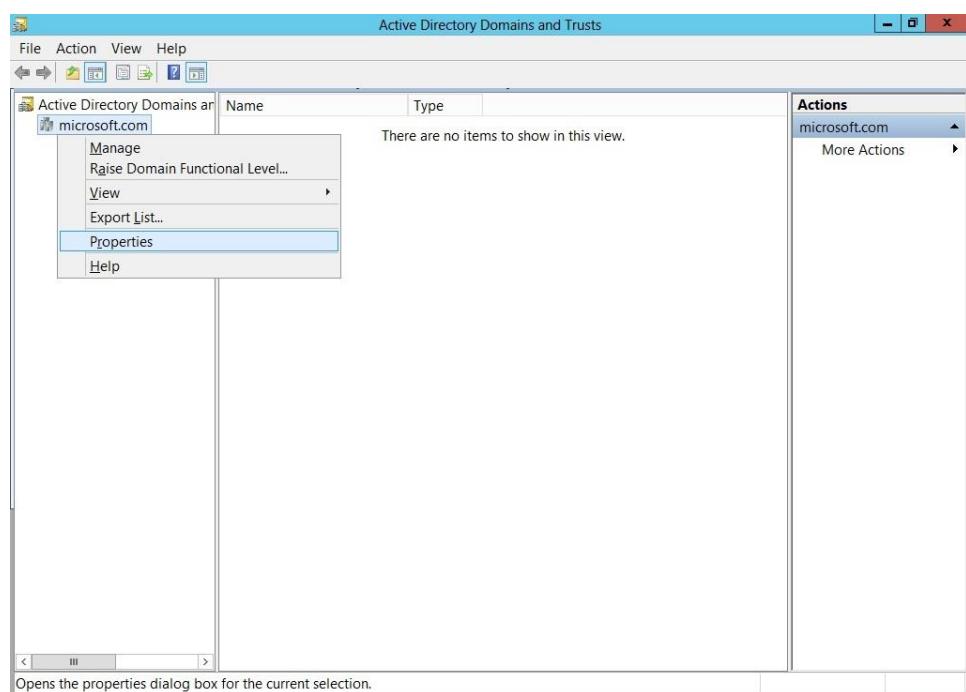
SYS1	SYS2		
Domain Controller-MICROSOFT.COM		Domain Controller-IBM.COM	
IP Address	10.0.0.1	IP Address	10.0.0.2
Subnet Mask	255.0.0.0	Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1	Preferred DNS	10.0.0.2
Alternate DNS	10.0.0.2	Alternate DNS	10.0.0.1

Lab – 1: Creating Forest Trust

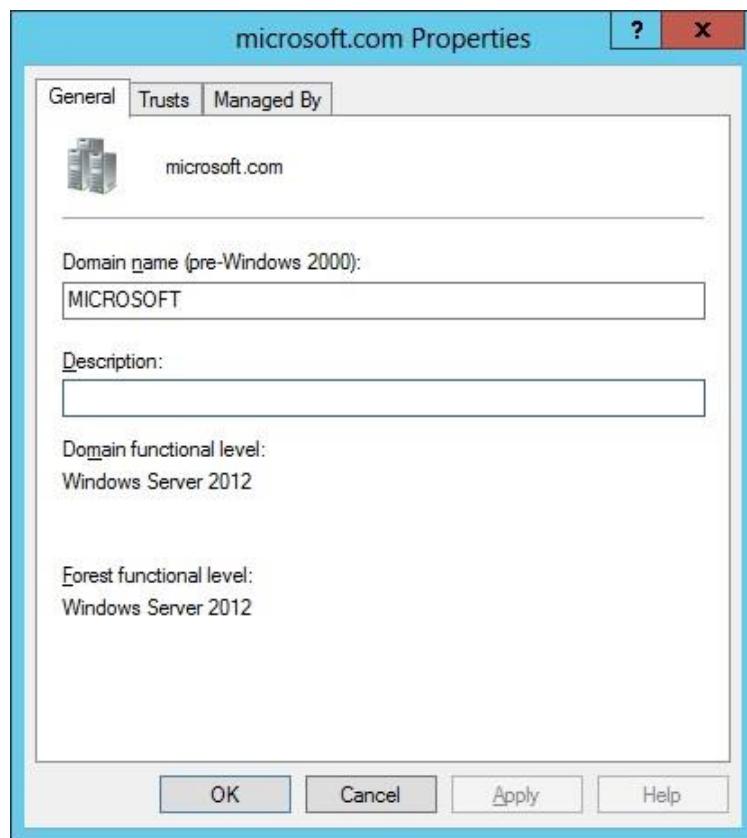
1. Go to Active Directory Domains and Trusts,



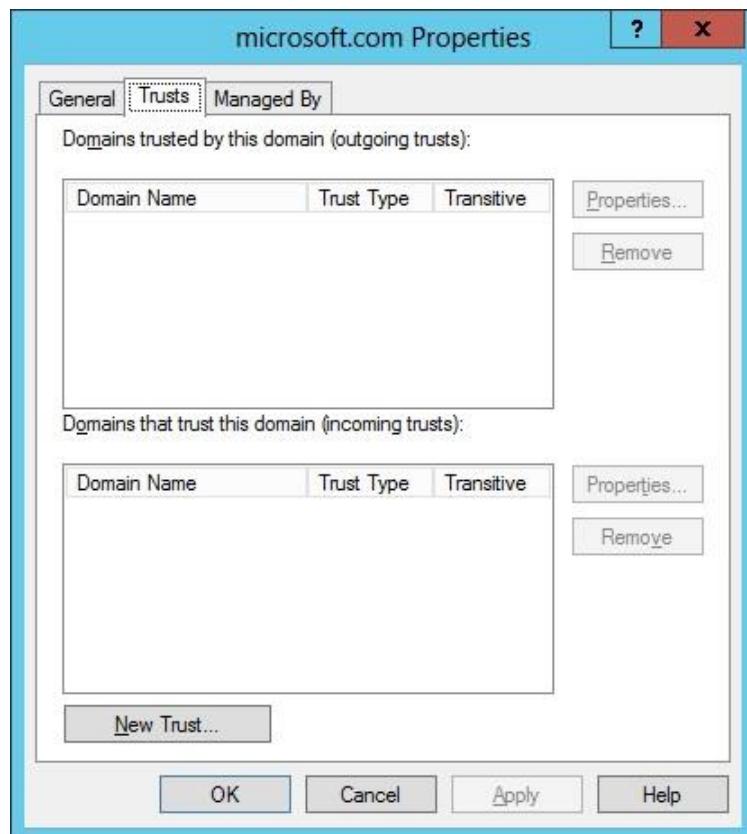
2. Right click the Domain name and select Properties.



3. Verify Domain and Forest functional level to be Windows Server 2012.



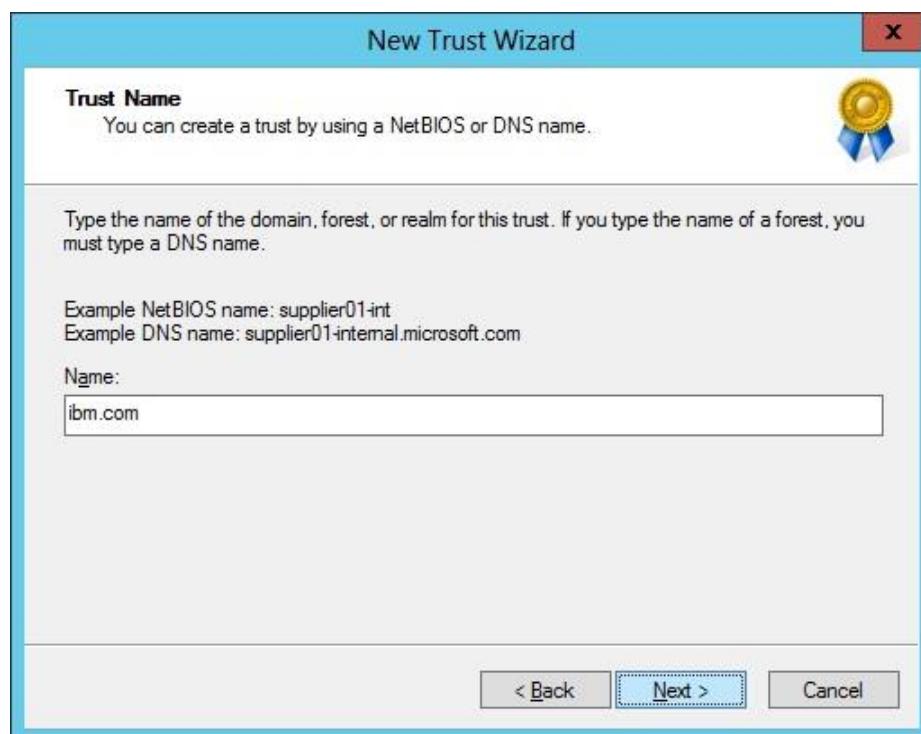
4. Select **Trusts** tab, Click **New Trust**.

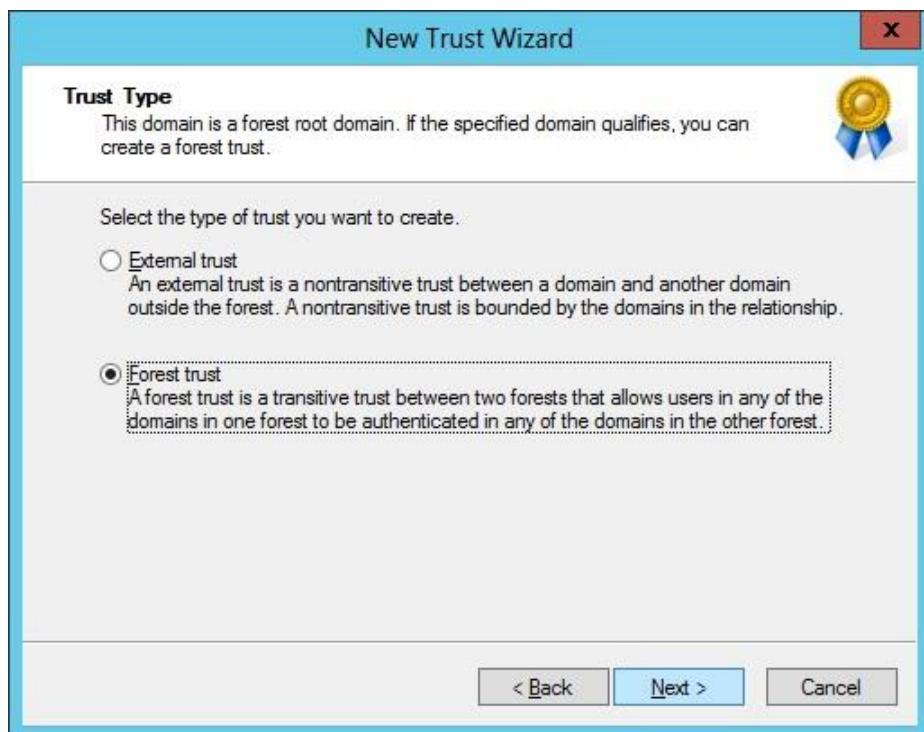
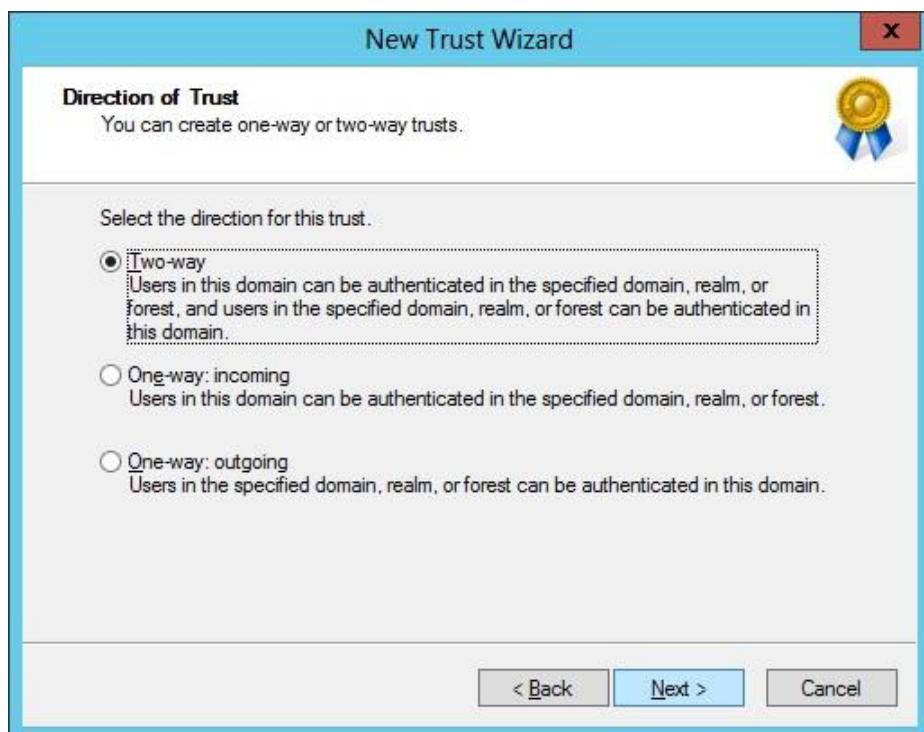


5. On Welcome wizard, click **Next**.

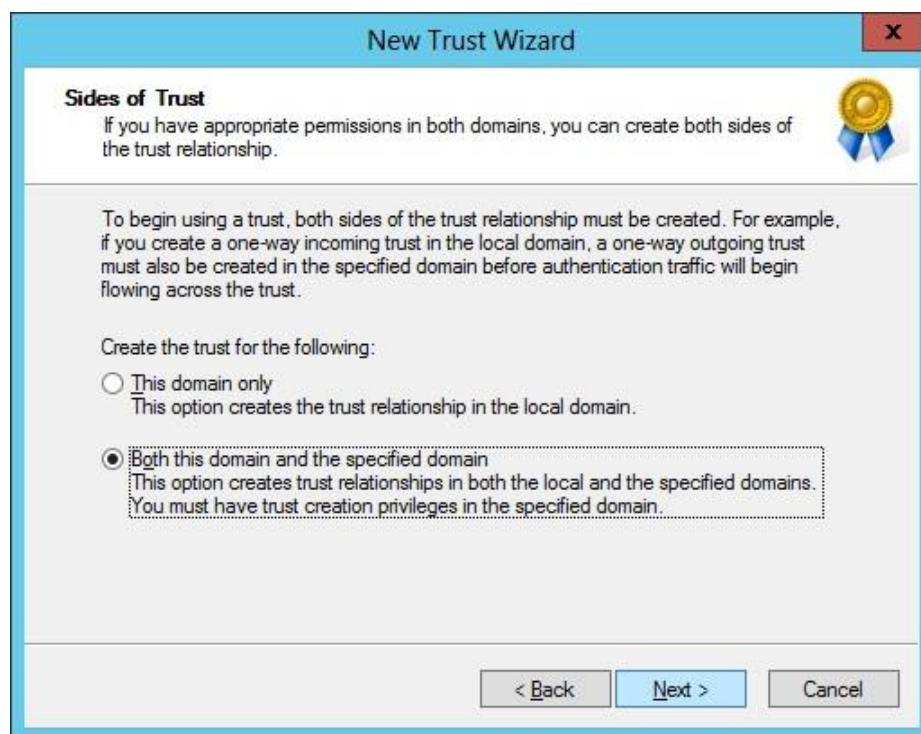


6. In Trust Name, enter name of other Forest **IBM.COM** and click **Next**.



7. Select **Forest trust** and click **Next**8. Select **Two-way** and click **Next**.

9. Select **Both this domain and the specified domain** and click **Next**.



10. Enter **Administrator** and **Password of Specified domain:IBM.COM** and click **Next**



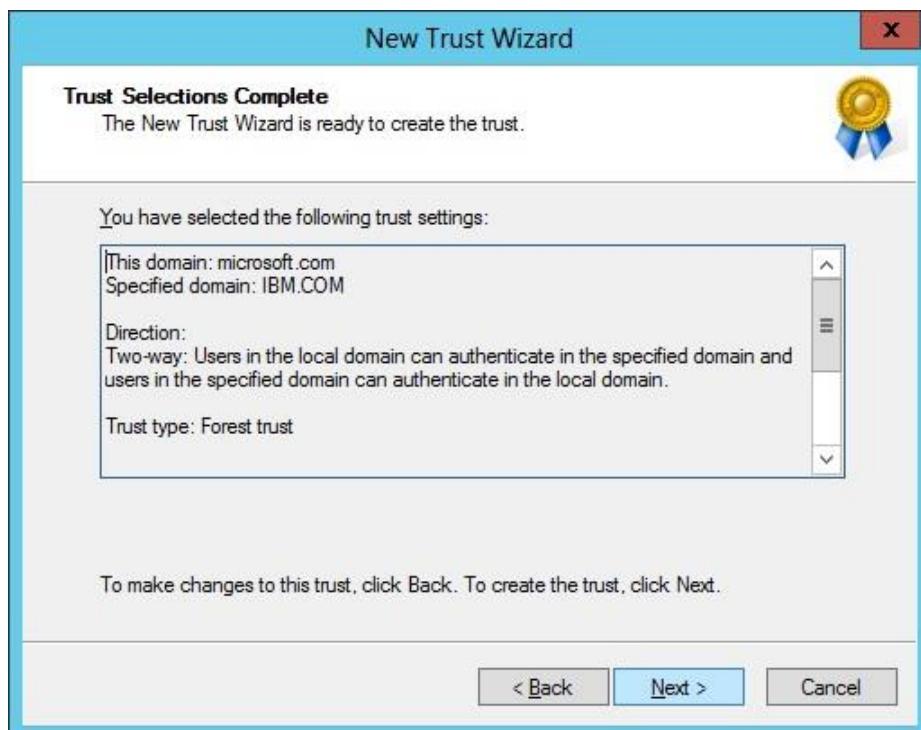
11. Select **Forest-wide authentication** for **Local Forest** and click **Next**.



12. Select **Forest-wide authentication** for **Specified Forest** and click **Next**.



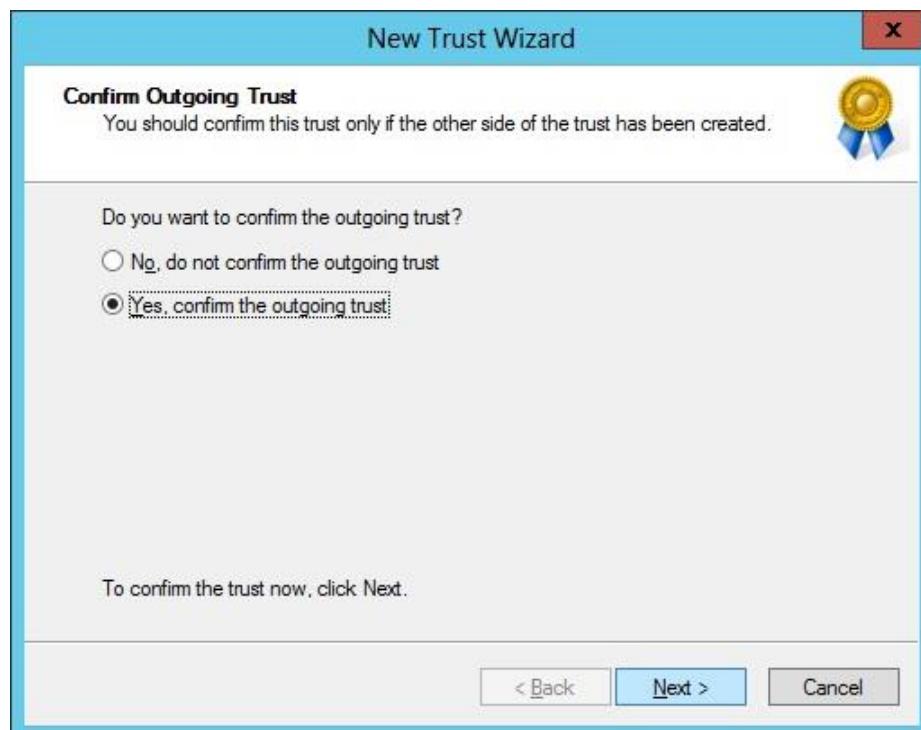
13. Verify the **Trust Selections** and click **Next**.



14. Verify the **Summary** and click **Next**.



15. Select Yes, confirm the outgoing trust and click Next.



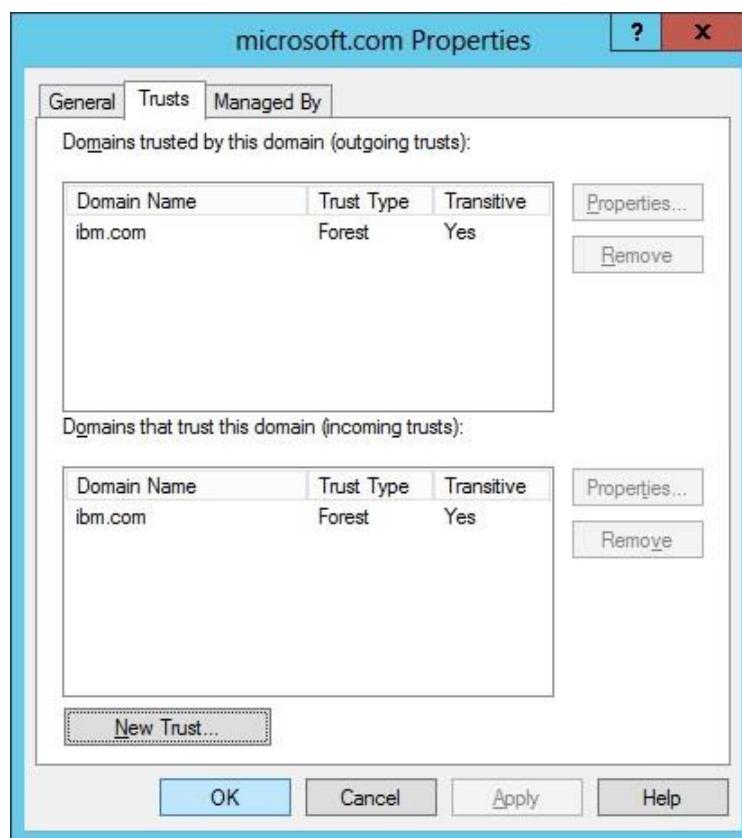
16. Select Yes, confirm the incoming trust and click Next.



17. Click **Finish**.



18. Check Outgoing and Incoming Trusts and click **OK**.



Verification:

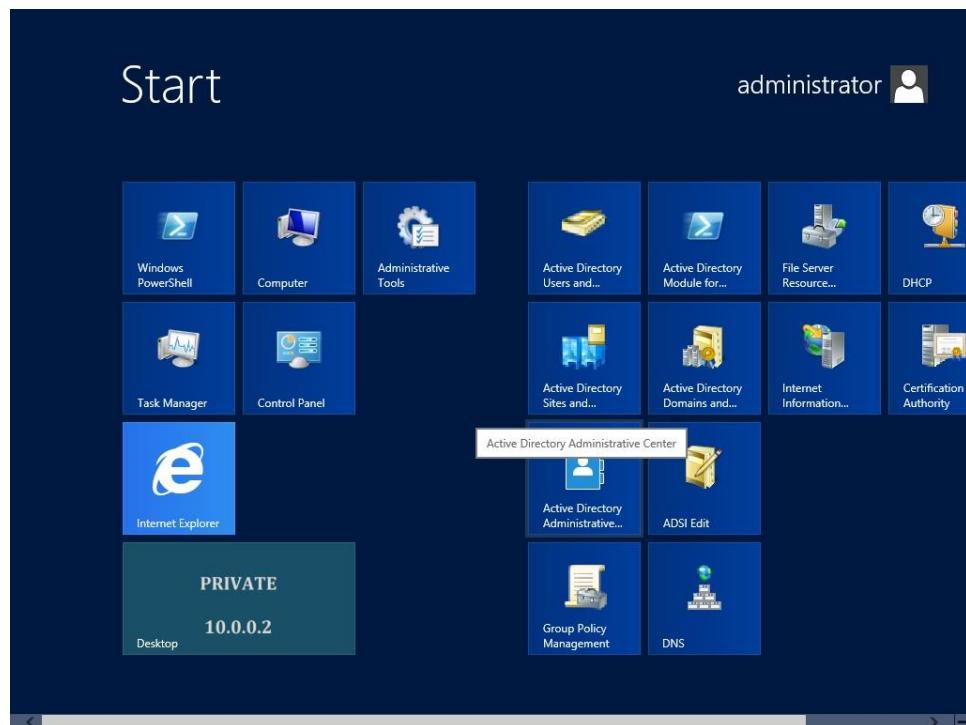
1. Try to Logon on to MICROSOFT.COM domain computers or IBM.COM domain computers as other Domain Users.

Note:By default Users cannot log on to D.C.

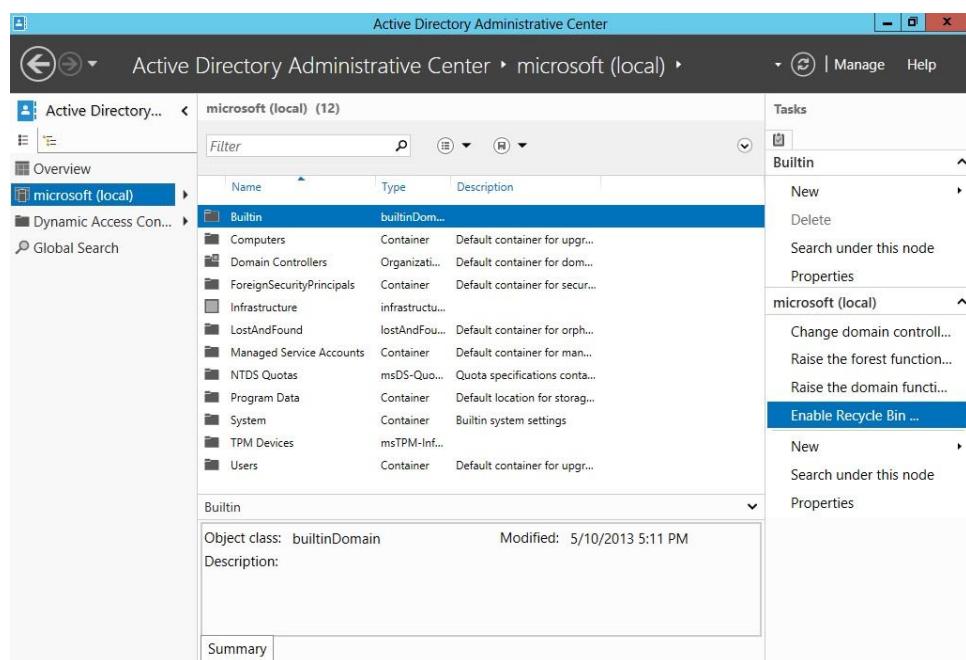
2. Log in as MICROSOFT Administrator to MICROSOFT.COM D.C and allow IBM users to log on to D.C using **Domain Controller Security Policy** in **Group Policy Management.(Allow Logon Locally Policy)**
3. Similarly allow MICROSOFT.COM users to log on to IBM.COM D.C using Domain Controller Security Policy of IBM.COM D.C.

Lab – 2:Active Directory Recycle Bin

1. Log in as Administrator to the Domain Controller (SYS1).
2. Go to Start, select Active Directory Administrative Center.



3. In Active Directory Administrative Center, select Microsoft (Local), Click Raise Domain Functional Level, select Windows Server 2012.
4. Click Raise Forest Functional Level, select Windows Server 2012 and refresh.
5. Click Enable Recycle Bin



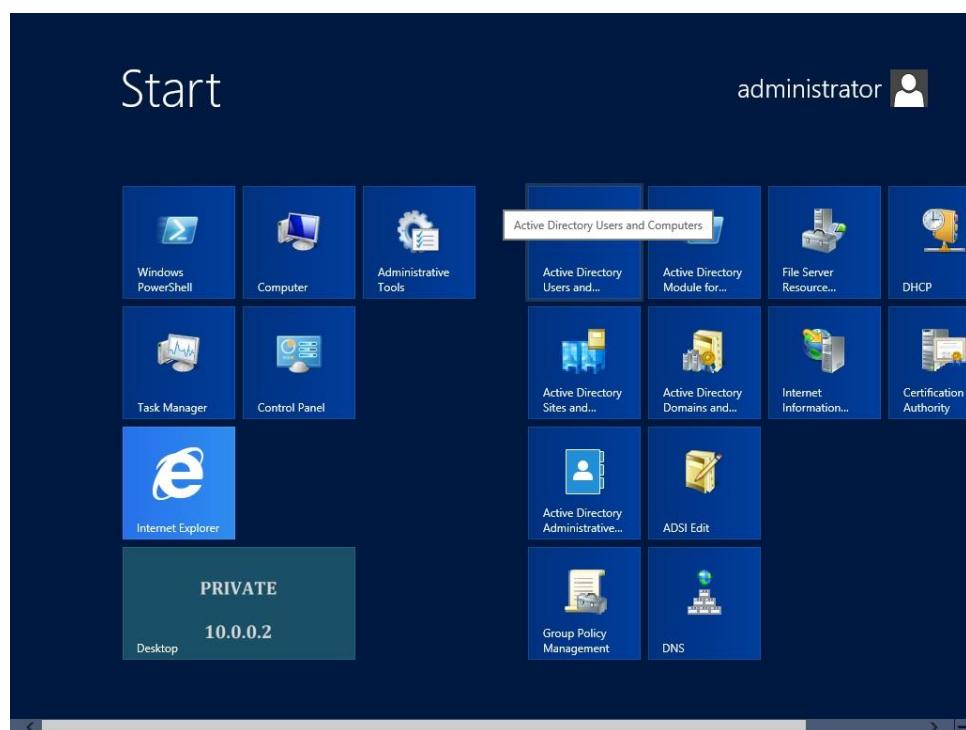
6. Click **OK** to confirm the Enable Recycle Bin feature.



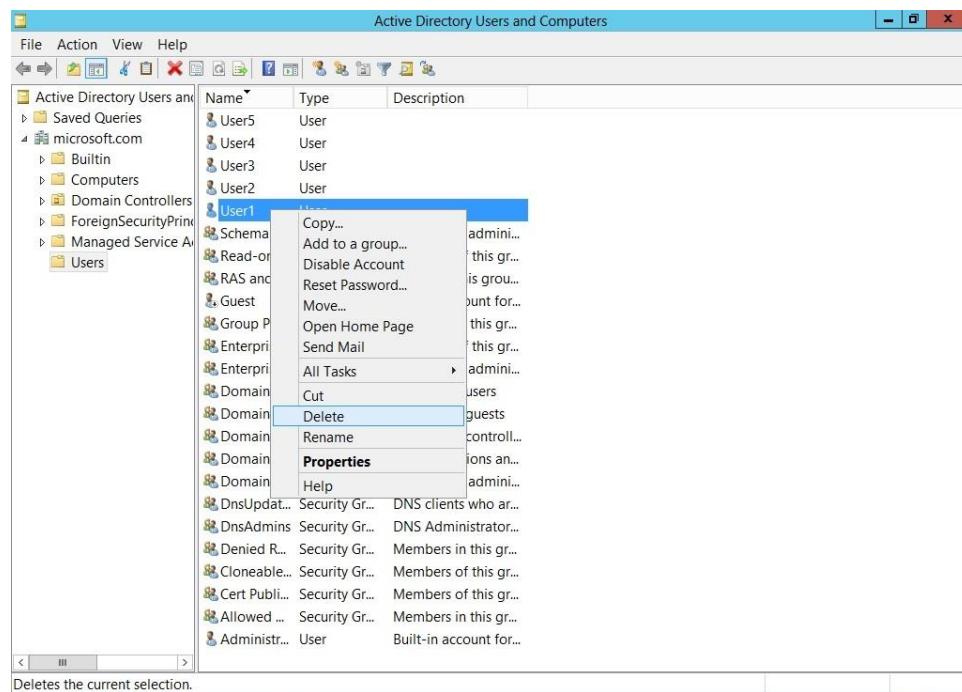
7. Click **OK**, and Refresh Active Directory Administrative Center now.



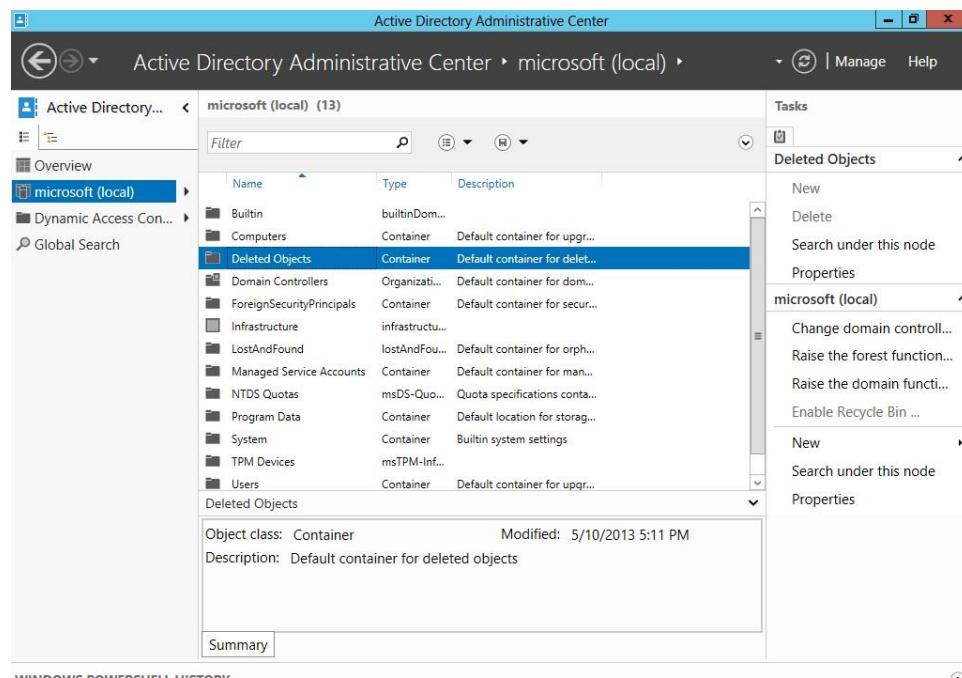
8. Go to Start, select **Active Directory Users and Computers**.



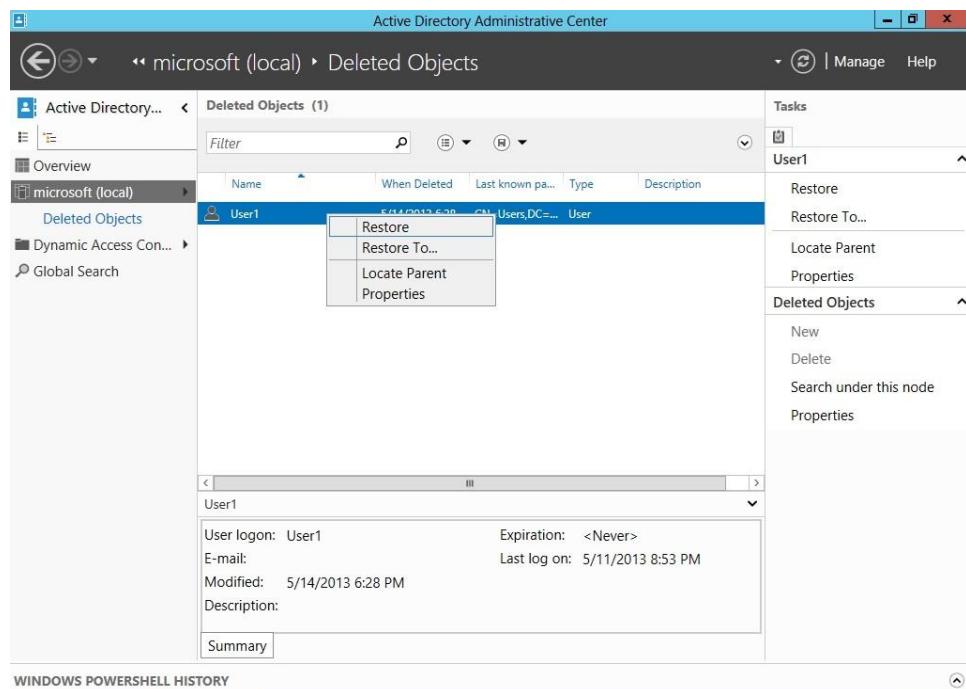
9. Right click User (User1) and select **Delete**, click **Yes** to confirm the deletion.



10. Go to Active Directory Administrative Center, select Microsoft (local), **Deleted Objects Container**

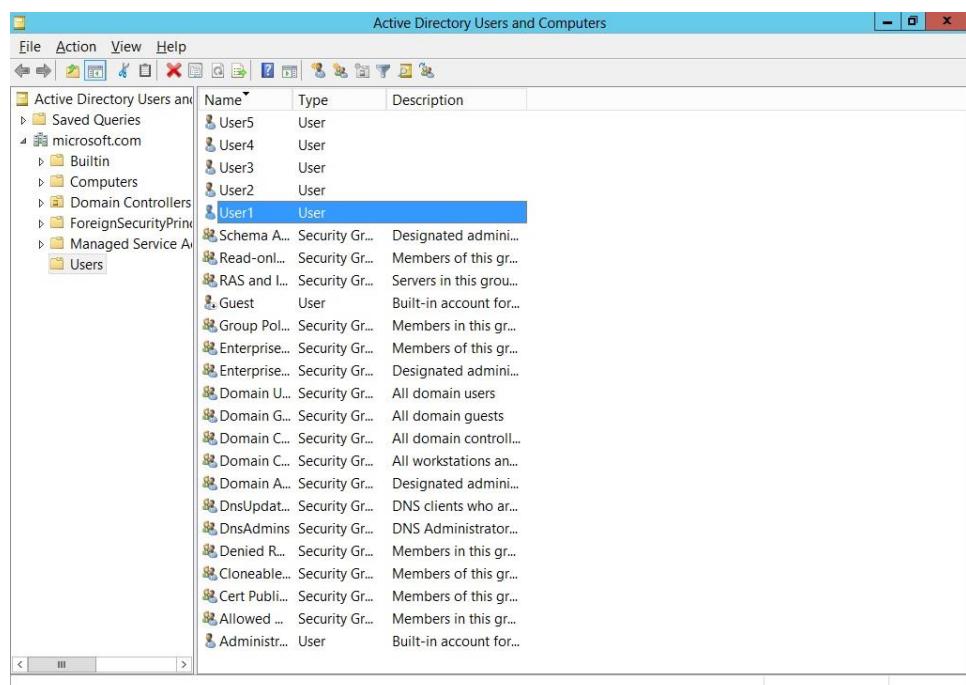


- 11. Select the User account (User1) to be restored, right click and select **Restore**.**

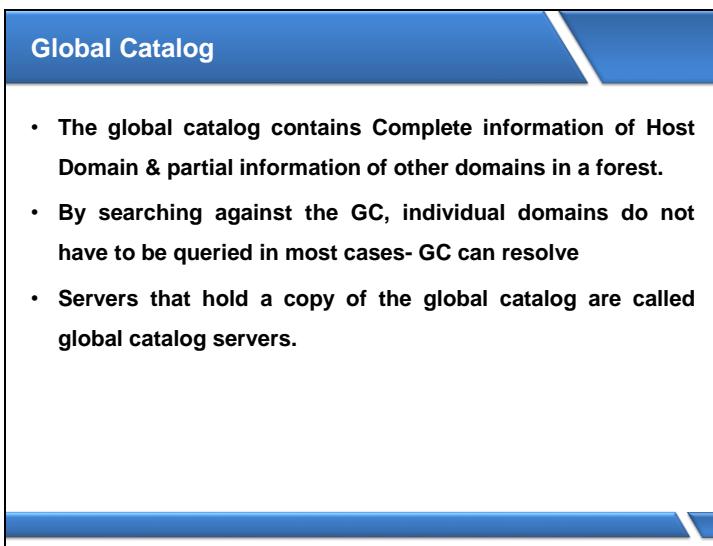
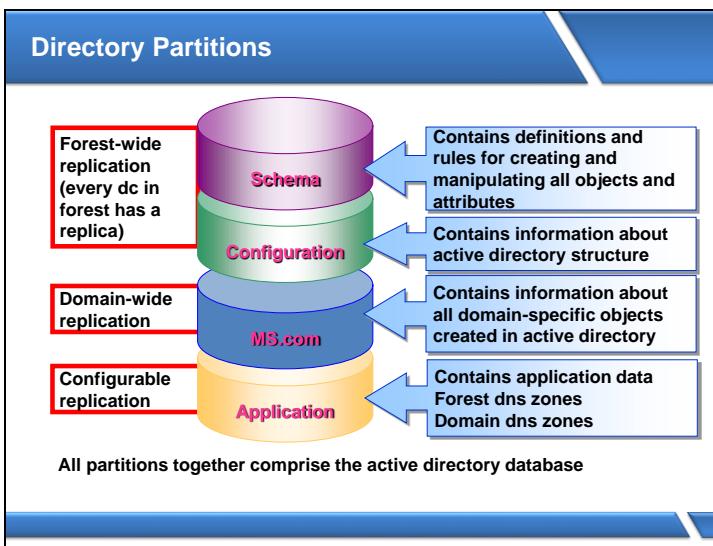


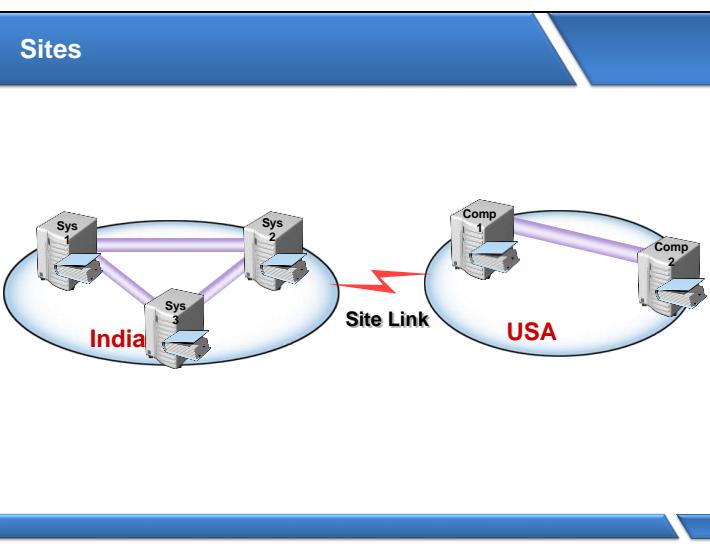
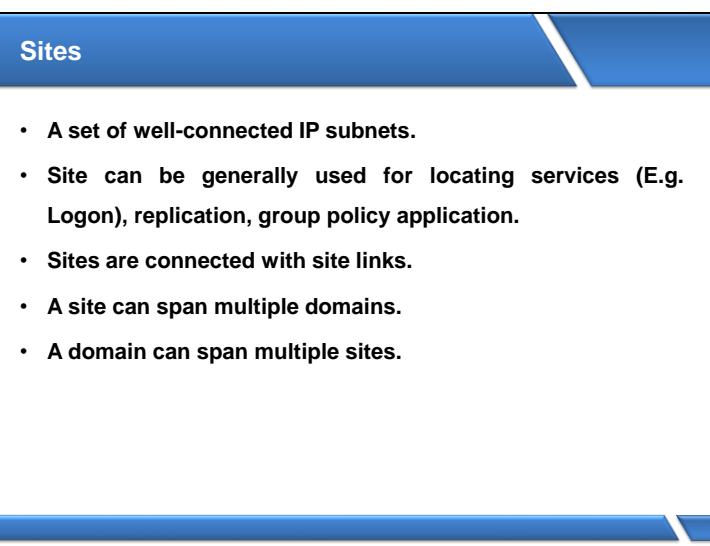
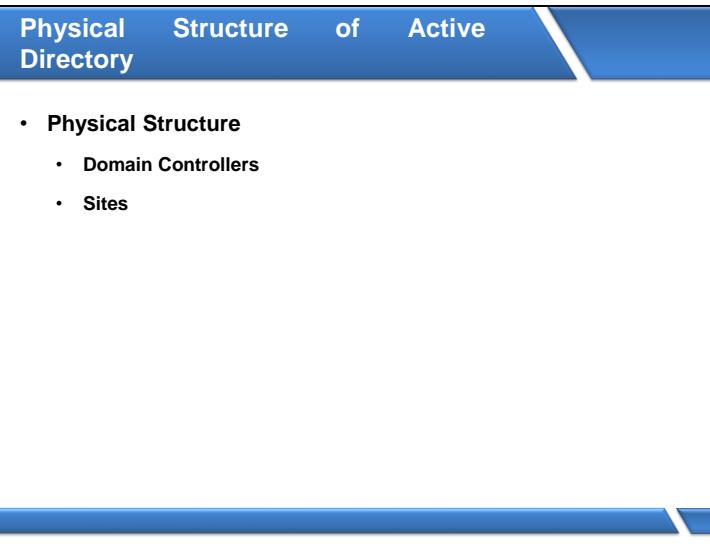
Verification

- 1. Go to Start, Select Active Directory Users and Computers, and verify for the restored user account.**



ACTIVE DIRECTORY



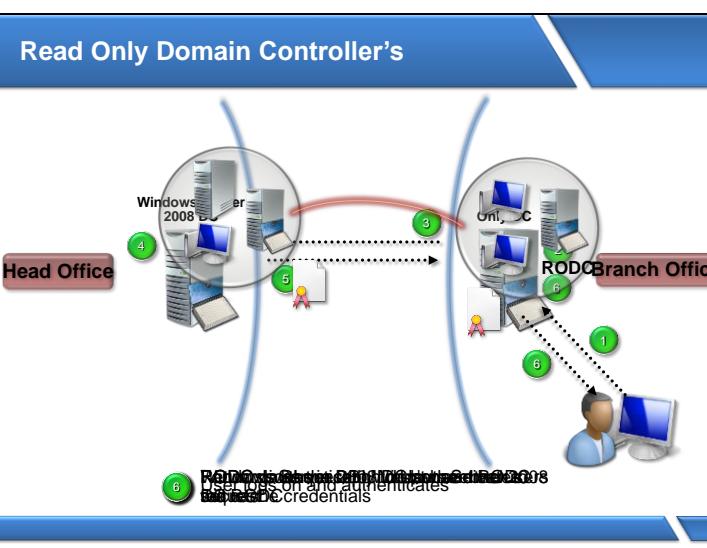


Read-Only Domain Controllers (RODCs)

- RODC addresses some of the problems that are commonly found in branch offices.
- These locations might not have a DC, Or they might have a writable DC but no physical security to that DC, low network bandwidth, or inadequate expertise to support that DC.

Functionality of RODCs

- Read-only AD DS database
- Uni-directional replication
- Credential caching
- Administrator role separation



Read-only AD DS Database

- Except for account passwords, an RODC holds all the Active Directory objects and attributes that a writable domain controller holds.
- However, changes cannot be made to the database that is stored on the RODC. Changes must be made on a writable domain controller and then replicated back to the RODC.

Uni-directional Replication

- Because no changes are written directly to the RODC, no changes originate at the RODC. Accordingly, writable DCs do not have to pull changes from the RODC. This means that any changes or corruption that a malicious user might make at branch locations cannot replicate from the RODC to the rest of the forest.

Credential Caching

- By default, an RODC does not store any user credentials.
- You must explicitly allow any credential to be cached on an RODC.

Administrator Role Separation

- You can delegate local administrative permissions for an RODC to any domain user without granting that user any user rights for the domain or other domain controllers.
- In this way, the branch user can be delegated the ability to effectively manage and perform maintenance work on the server, such as upgrading a driver in the branch office RODC only, without compromising the security of the rest of the domain

Install From Media

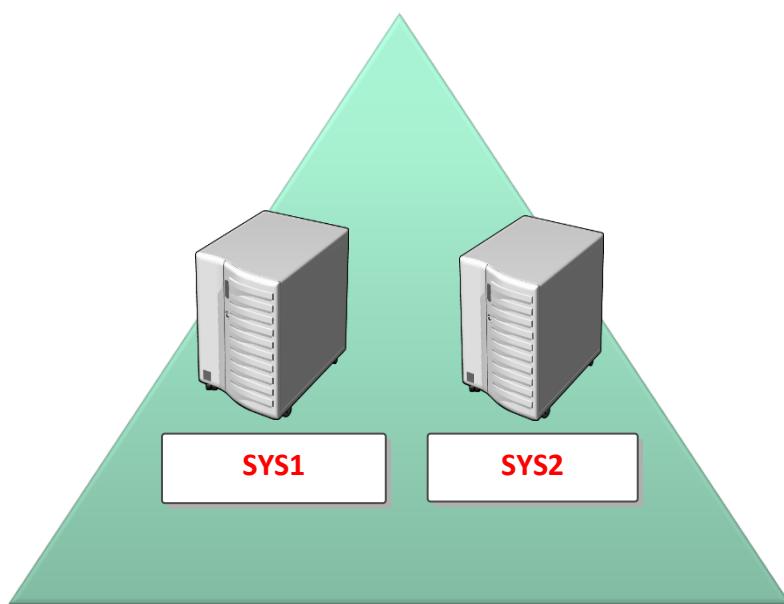
- If you have a network that is slow, unreliable, or costly, you might find it necessary to add another domain controller at a remote location or branch office.
- IFM process must take place over a potentially unreliable WAN connection. As an alternative, and to significantly reduce the amount of traffic copied over the WAN link
- Most of the copying is then done locally (perhaps from a USB drive), and the WAN link is used only for security traffic and to ensure that the new domain controller receives any changes that are made after you create the IFM backup

GLOBAL CATALOG, SITES, and READ ONLY DOMAIN CONTROLLER

Pre-requisites:

Before working on this lab, you must have

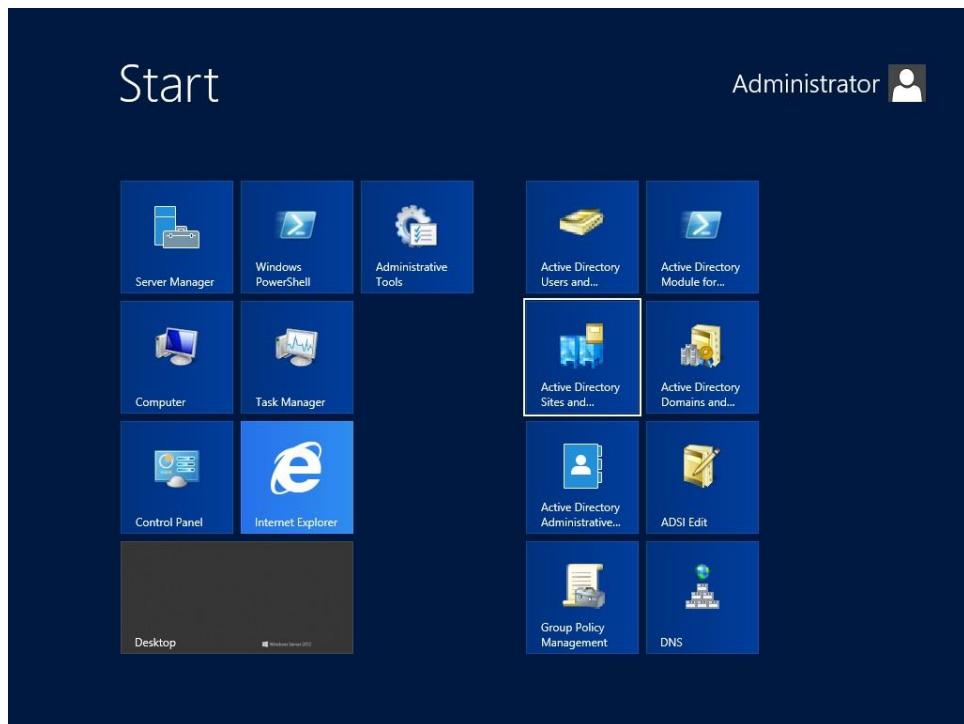
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server.



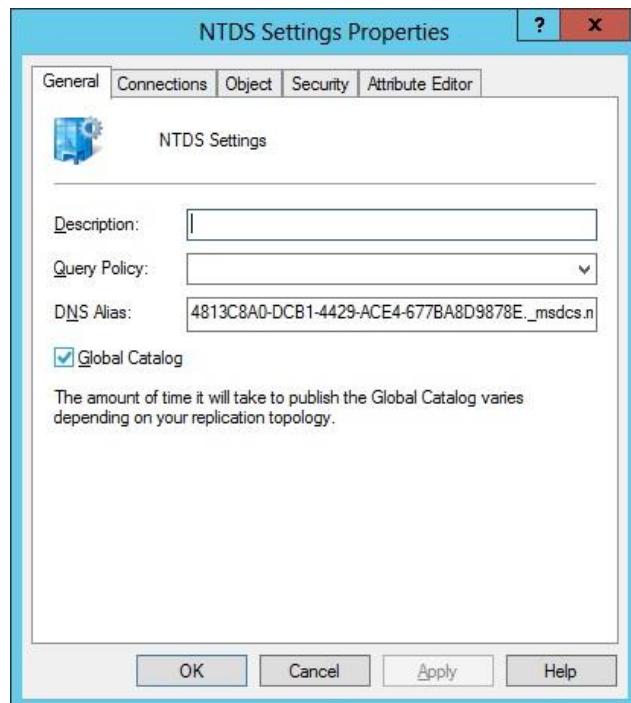
SYS1	SYS2
Domain Controller	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Alternate DNS	-----
Read Only Domain controller	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.2
Alternate DNS	10.0.0.1

Lab – 1: Configuring Global Catalog Server

1. Go to Active Directory Sites and Services.

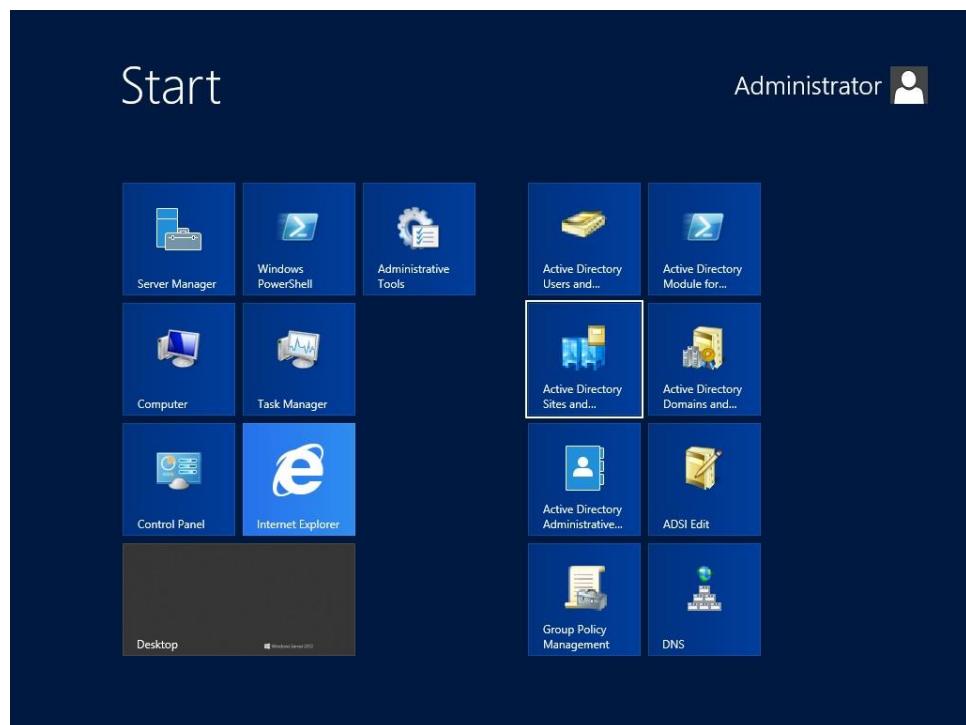


2. Expand the Sites → Default-First-Site-Name → Servers → Server Names → NTDS Settings.
3. Right click NTDS Setting and Properties, If the checkbox Global Catalog is checked, then it is a GlobalCatalogServer.

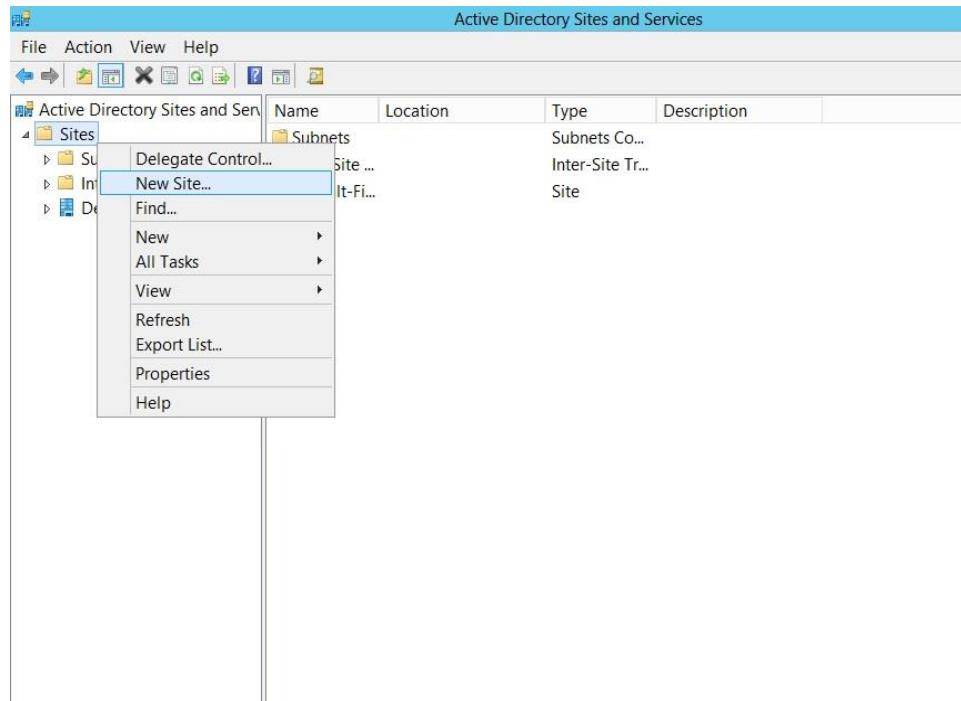


Lab – 2: Creating Active Directory Sites

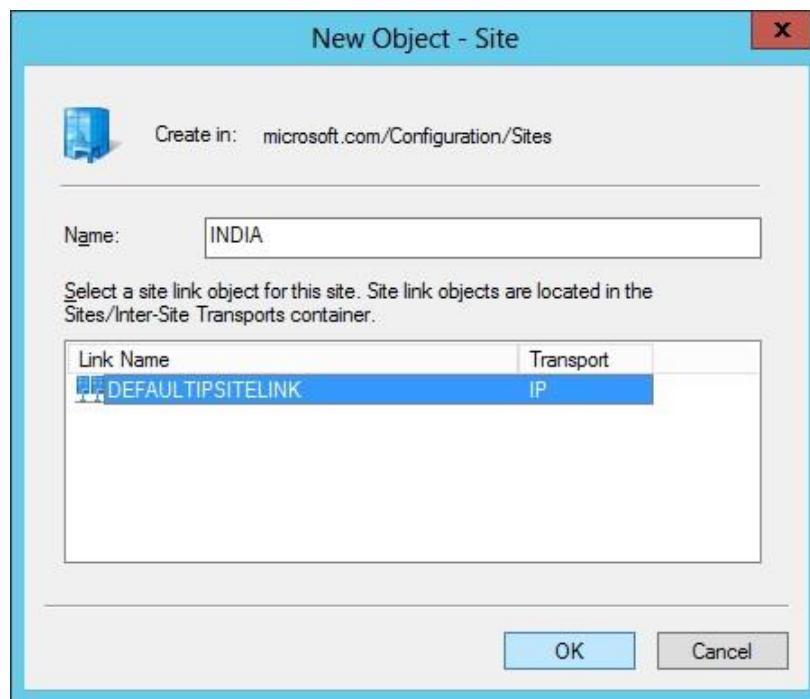
1. Logon to D.C as Administrator, go to Start, Active Directory Sites and Services.



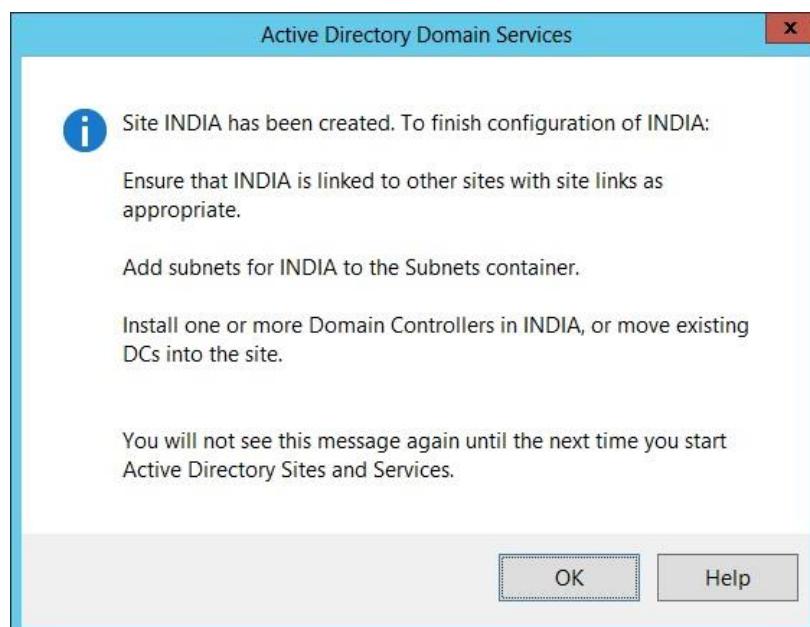
2. Right click **Sites**→**New Site**.



3. Enter the site name (**INDIA**) and select **DEFAULTIPSITELINK** and click **OK**.

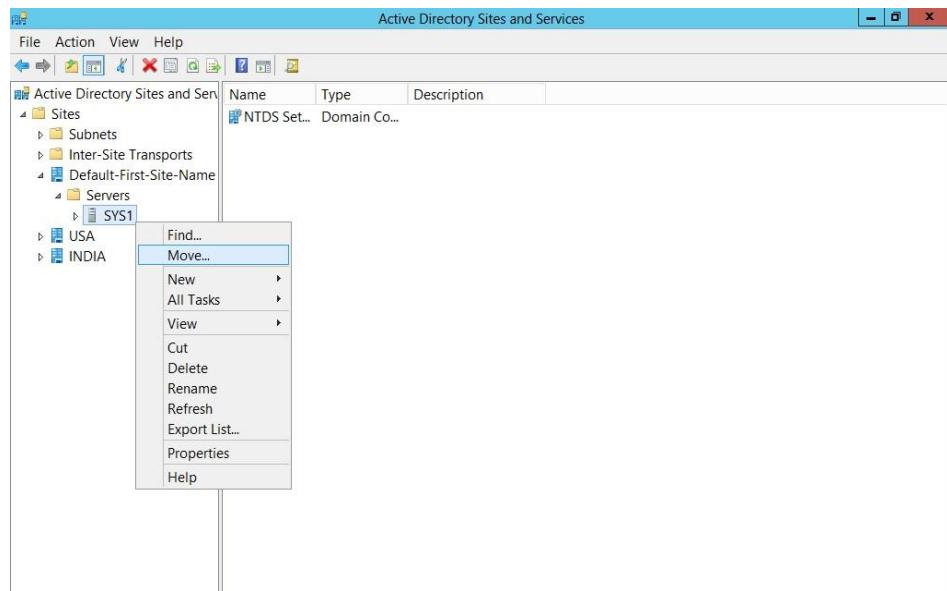


4. Site INDIA will be created, click **OK**.

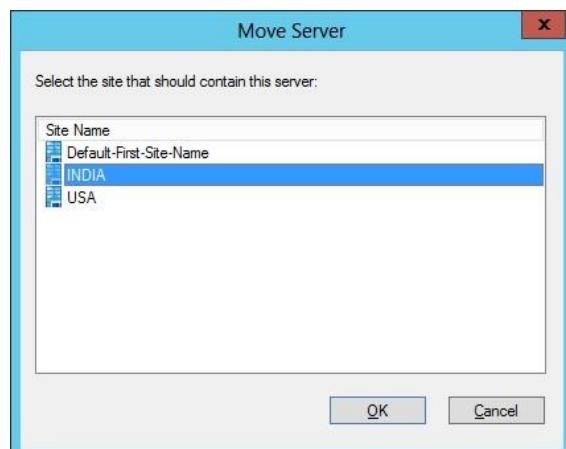


5. Similarly create another site (**USA**)

6. Expand **Default-First-Site-Name** → Expand **Servers** → Right click **Server (SYS1)** → **Move**



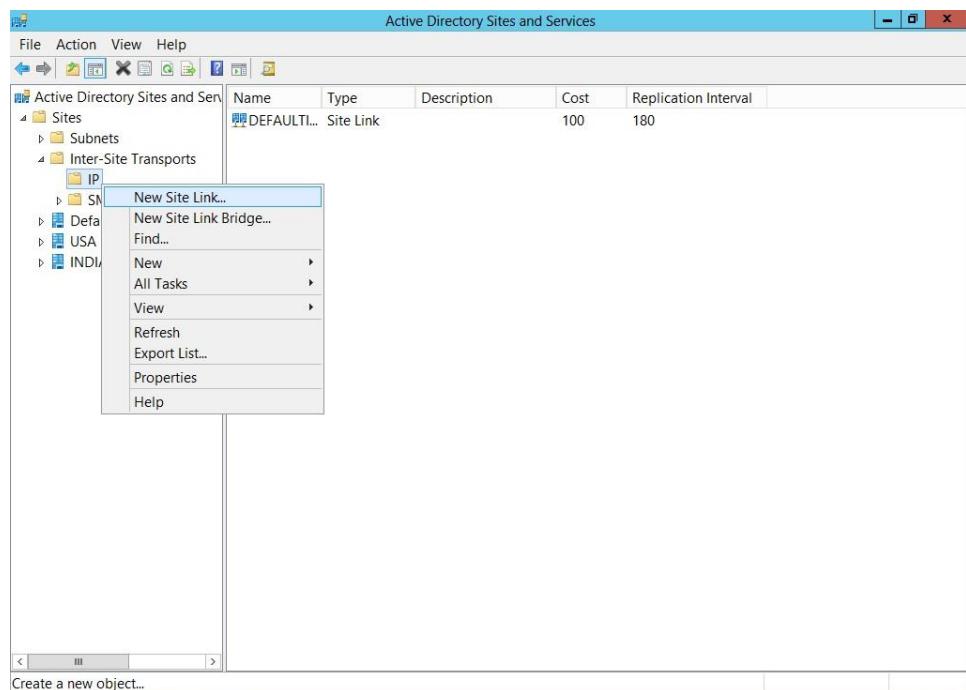
7. Select the Site (**INDIA**) and click **OK**.



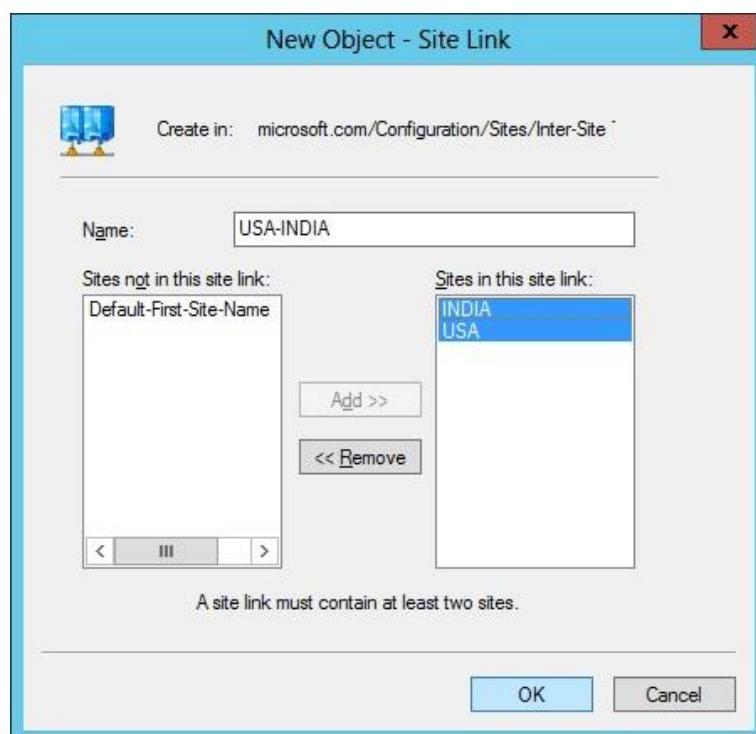
8. Server is now moved under **INDIA** site.

Lab – 3: Creating Active Directory Site-Links

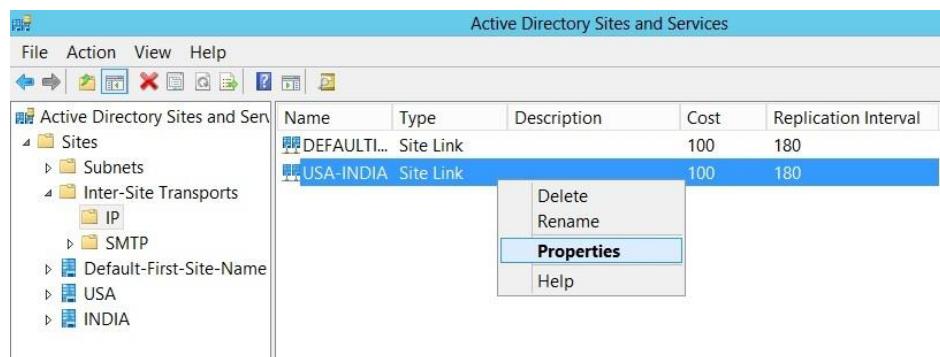
1. Log on to D.C as Administrator
2. Go to **Active Directory Site sand Services** → Expand **Sites** → Expand **Inter-Site Transports** → Right click **IP** → select **New Site Link**.



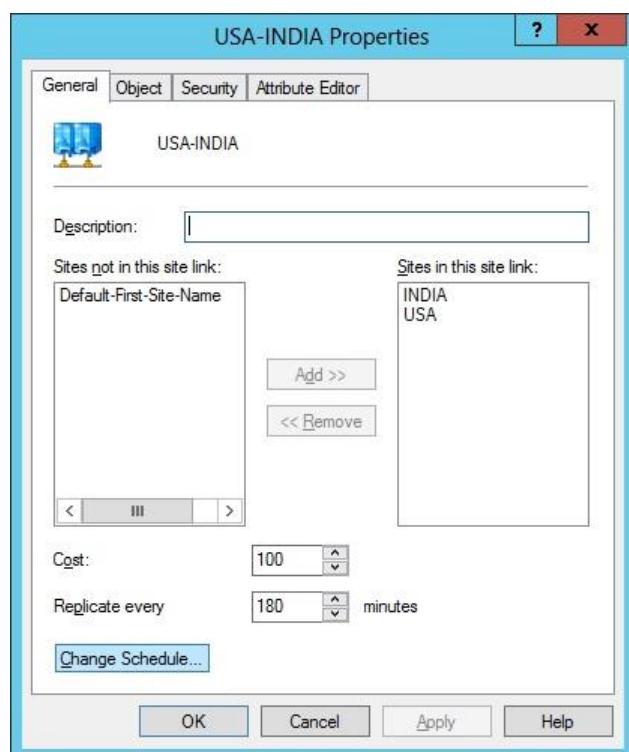
3. Enter the name (**INDIA-USA Link**), select INDIA and USA sites and click **Add**→click **OK**.



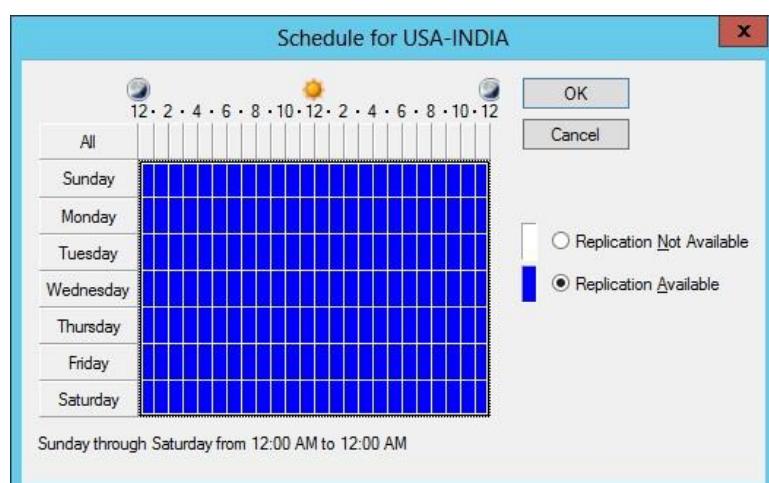
- 4. Right click INDIA-USA Link, select Properties.**



- 5. Click Change Schedule.**

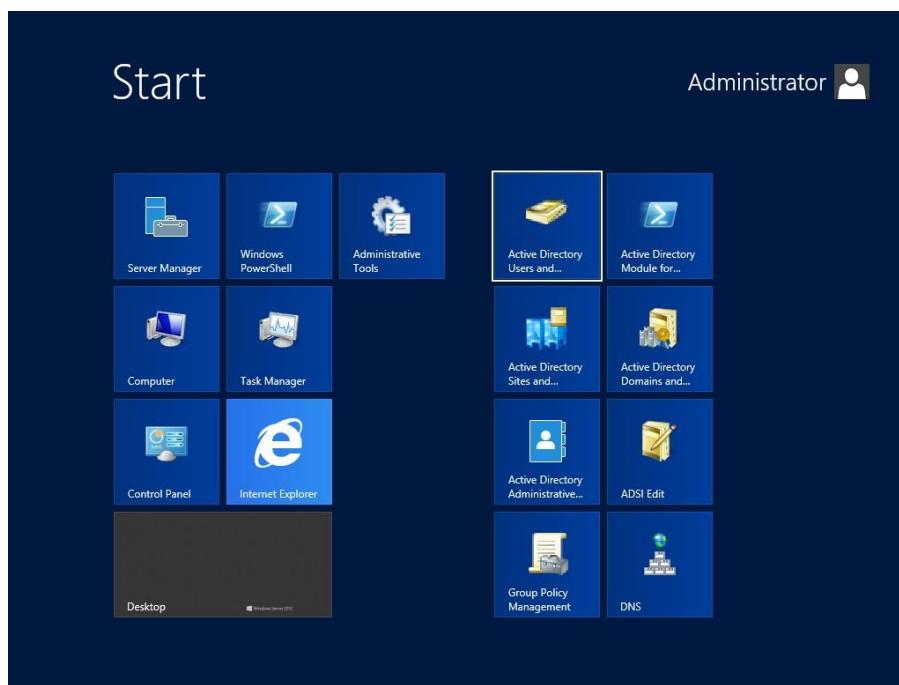


- 6. Select the Interval of Time for ReplicationAvailable, click OK→OK.**

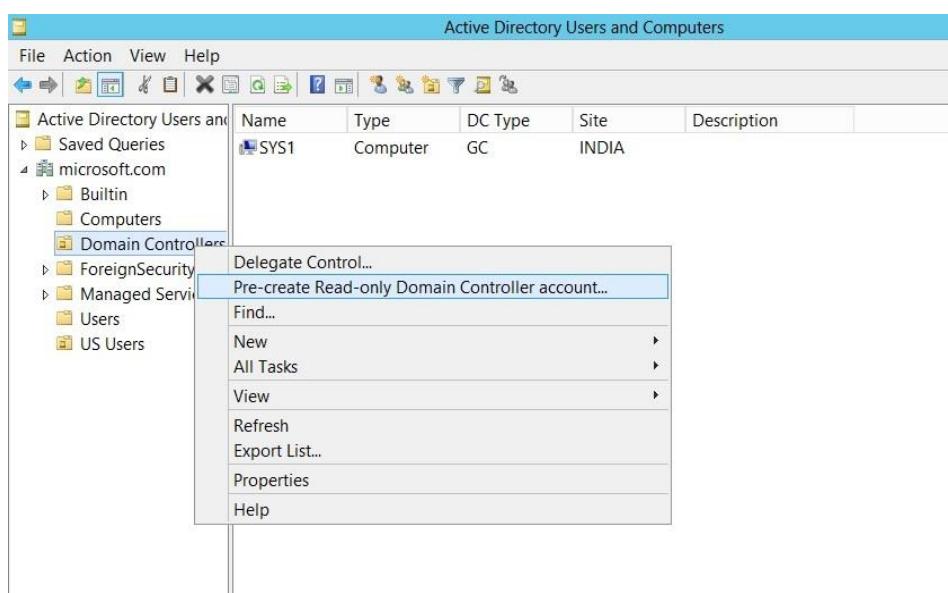


Lab – 4: Creating a Pre-Create Read Only Domain Controller Account

1. Log in as **Administrator** to the **Domain Controller (SYS1)**.
2. Verify Domain and Forest Functional Levels to **Windows Server 2008 or later**.
3. Go to **Active Directory Users and Computers**.



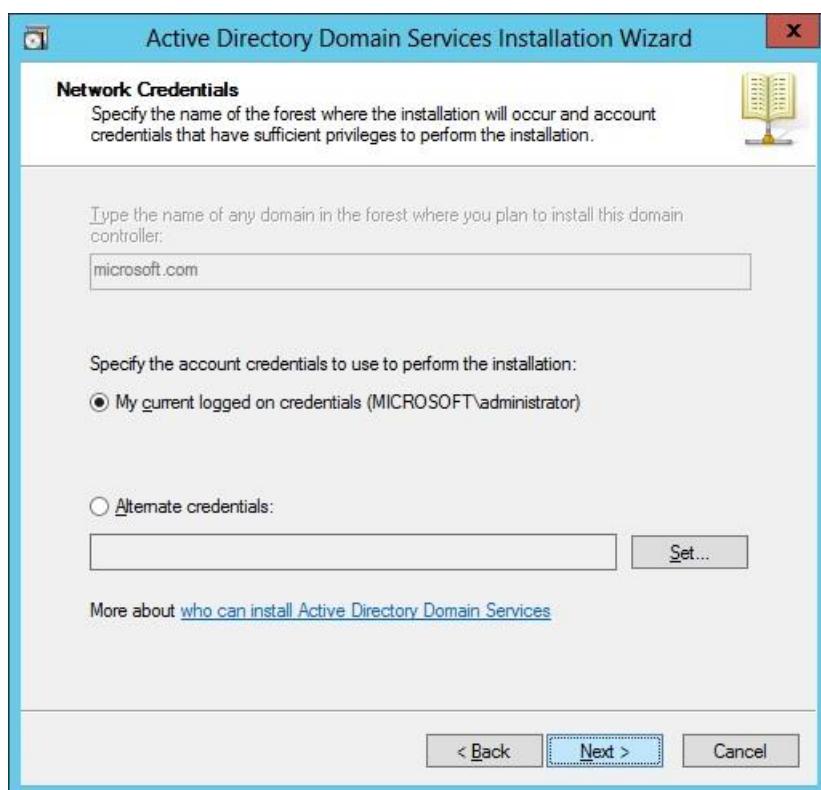
4. Create **Users** (Ex: **User1, User2, User3, User4, User5**).
5. Right click Domain Controllers, Select **Pre-create Read-only Domain Controller account**.



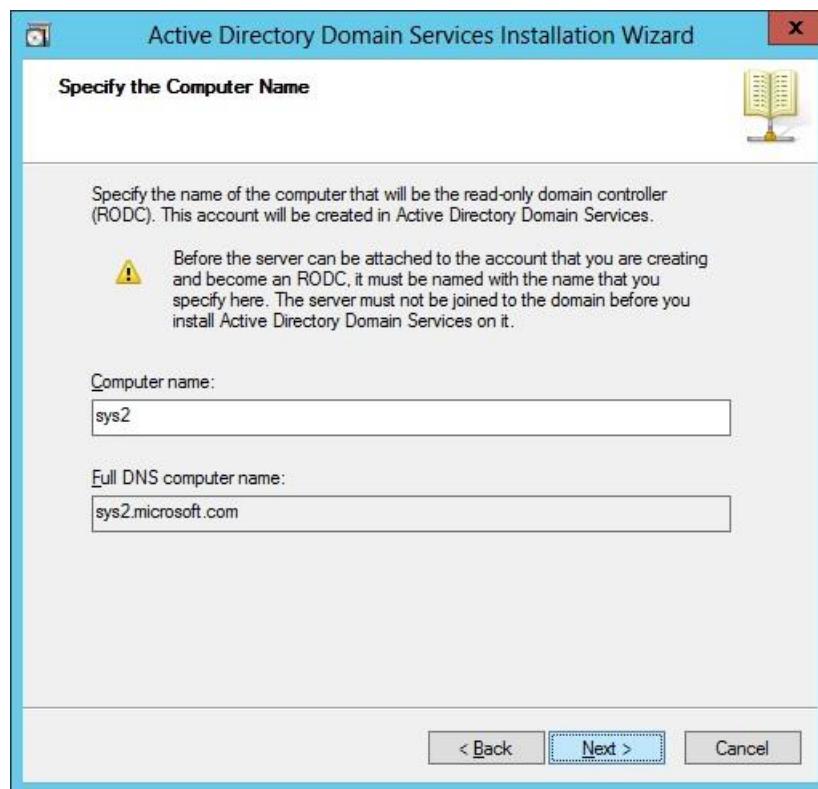
6. In Welcome Screen, click **Next**.



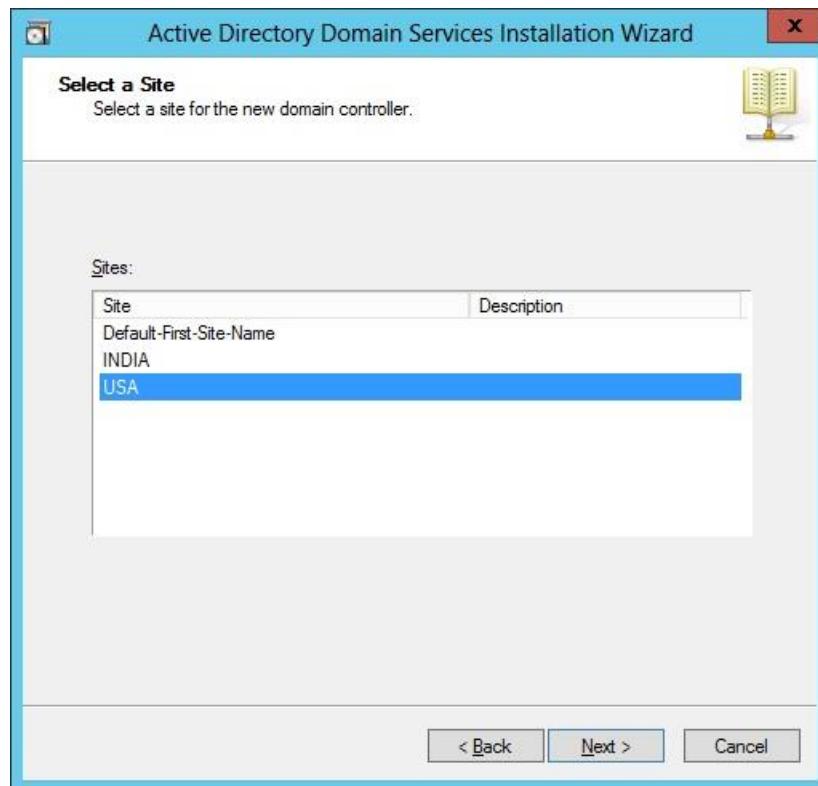
7. Select **My current logged on credentials (MICROSOFT\Administrator)** and click **Next**.



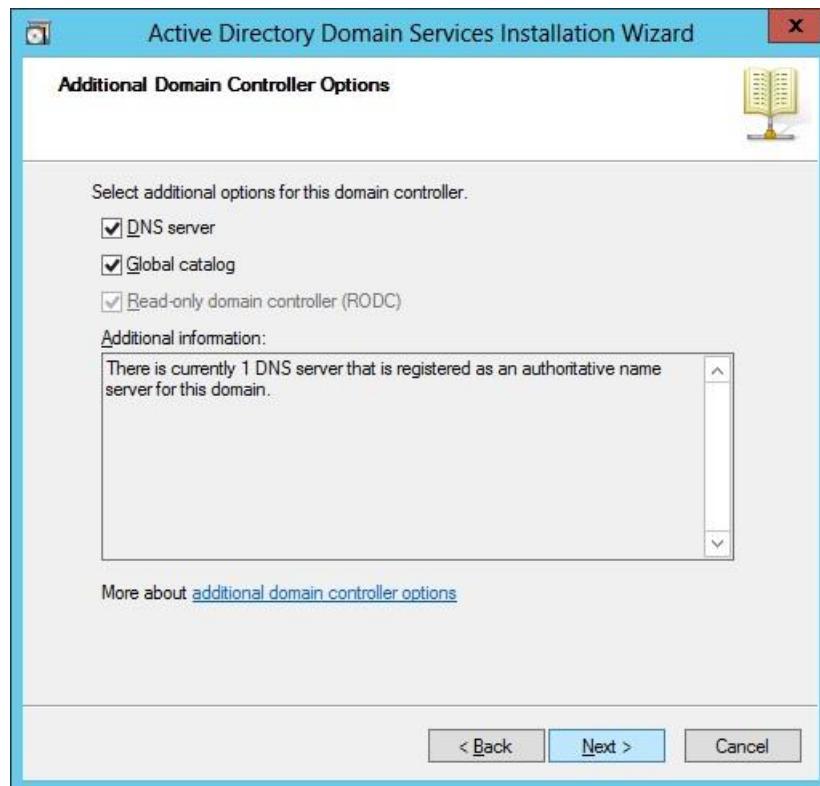
8. Enter the **Computer Name(SYS2)** of Read Only Domain Controller.



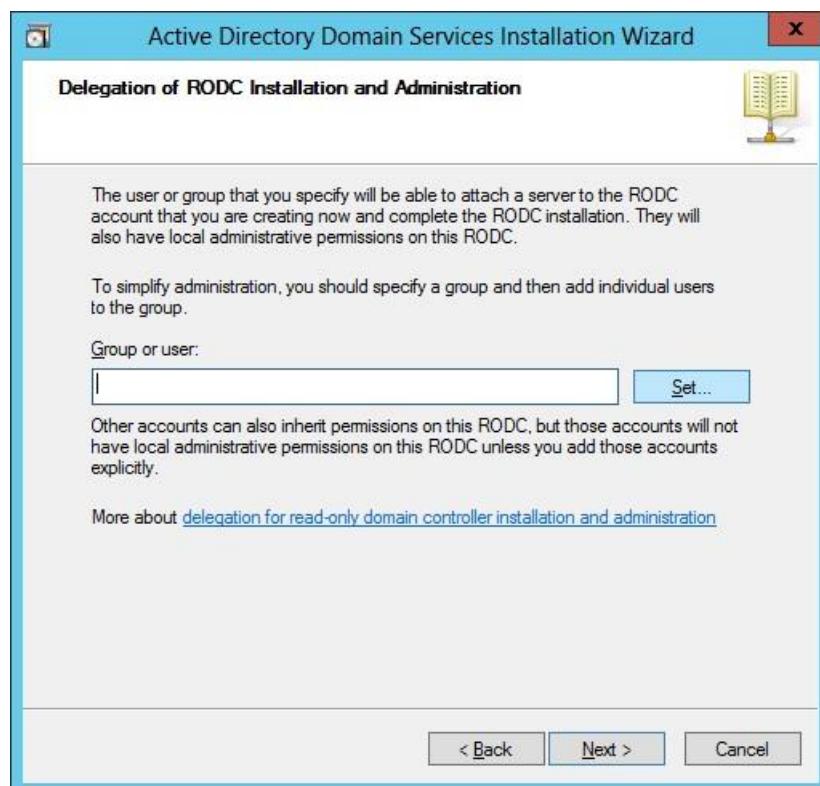
9. Select the Site (**USA**) for the Read-only Domain Controllers and click **Next**.



10. Verify the **DNS**, **Global Catalog** and **Read-only Domain Controller (RODC)** checkboxes and click **Next**.



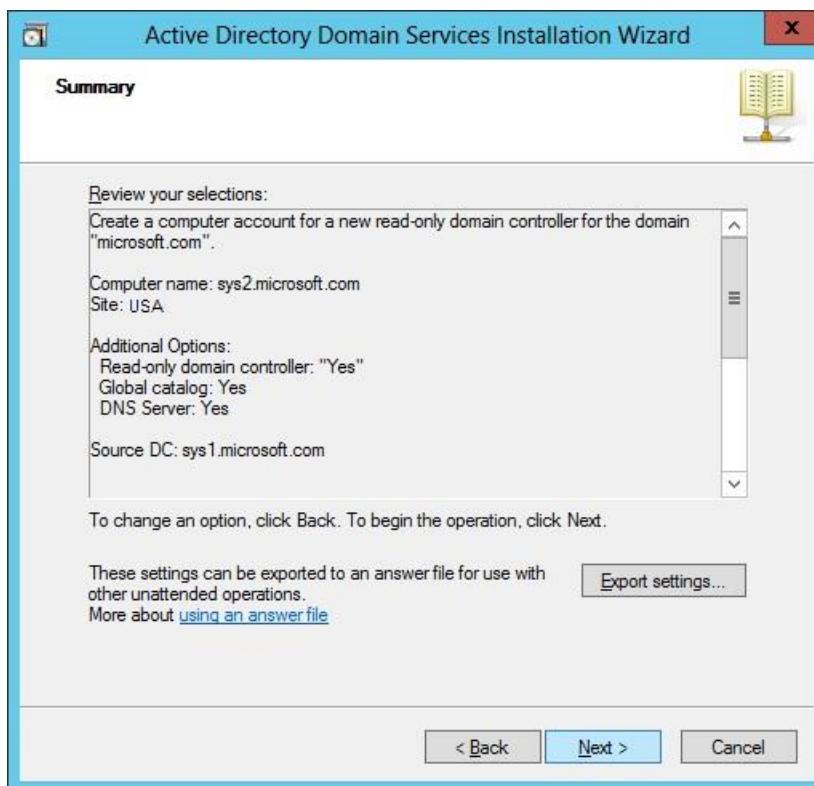
11. Click **Set**.



12. Enter the User name (**User1**) and click **OK** and click **Next**.



13. Review the Summary, and click **Next**.



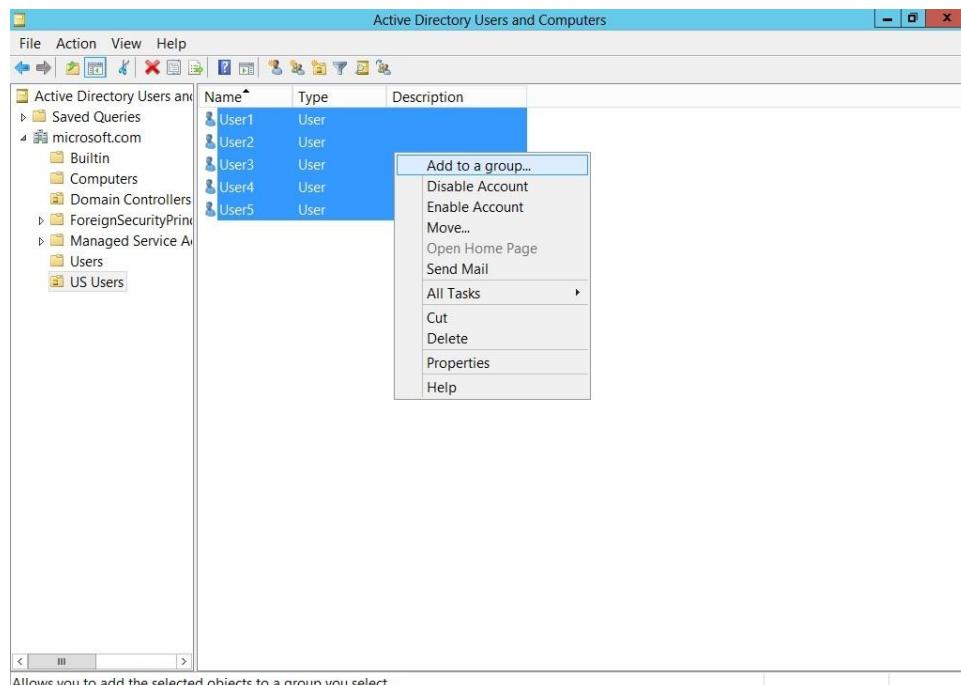
14. Click **Finish**.



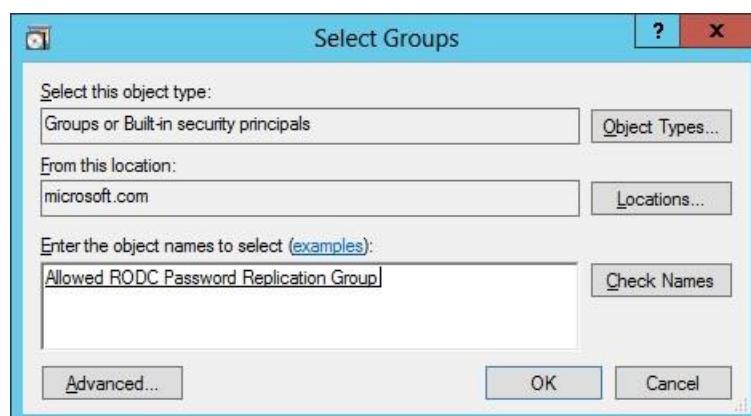
15. Account of Read-only Domain Controller will be created in Domain Controllers.

Name	Type	DC Type	Site
SYS1	Computer	GC	INDIA
SYS2	Computer	Unoccupied DC Account (Read-only, GC)	USA

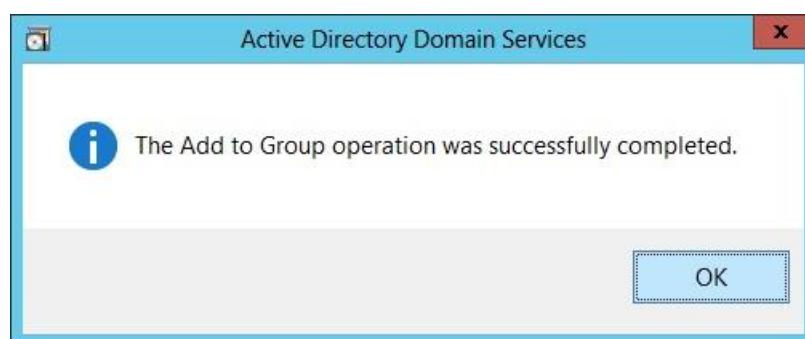
- 16. To cache the user account password on RODC, Select the Users (User1, User2, User3, User4, User5) Right click and select Add to a Group.**



- 17. Enter the Group Name Allowed RODC Password Replication Group and click OK.**

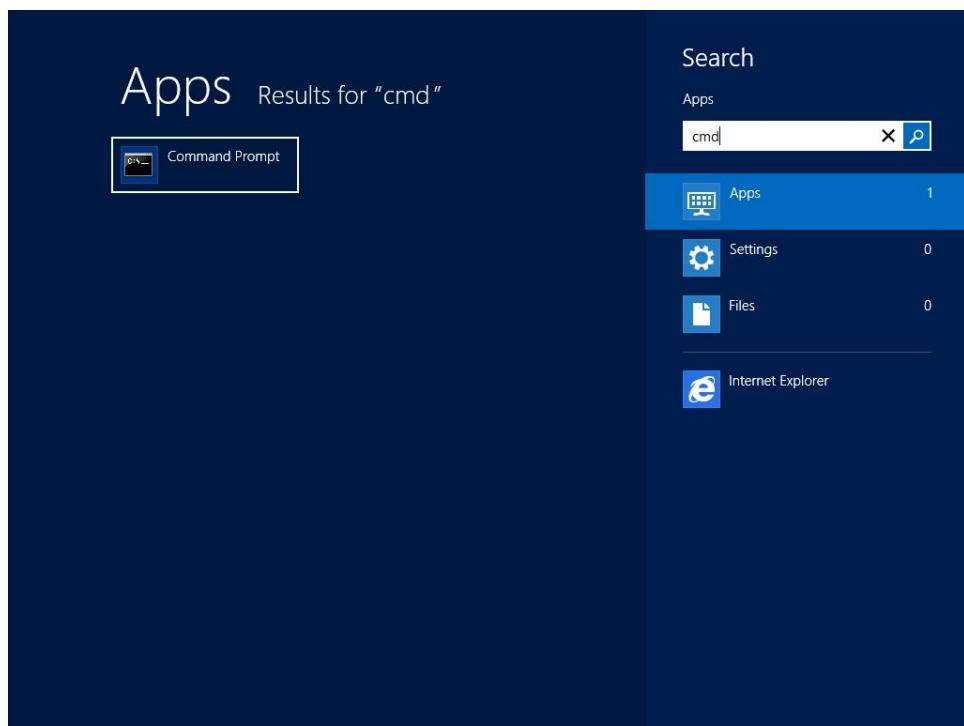


- 18. The Users will be added to the Group, click OK.**

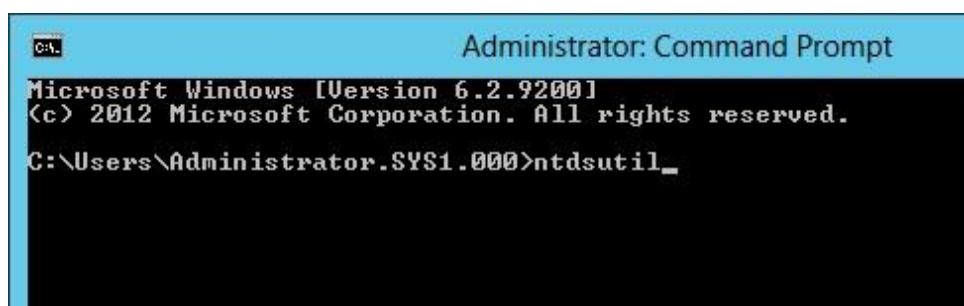


Lab – 5:Configuring Read-Only Domain Controller using IFM

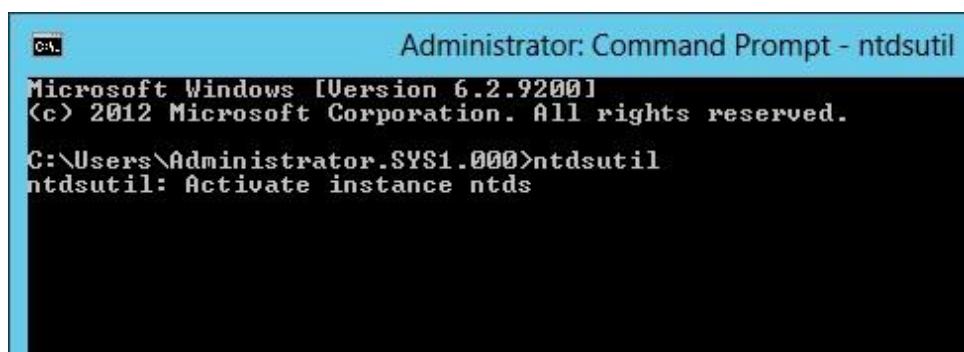
1. Log in as **Administrator** to the **Domain Controller (SYS1)**.
2. Create a Shared folder (Ex: **ifm**) in C drive.
3. Go to Start, type cmd in Search Apps, and select **Command Prompt**



4. Type **Ntdsutil**



5. Type **Activate instance ntds**.



6. Type **ifm**.



```
Administrator: Command Prompt - ntdsutil
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SYS1.000>ntdsutil
ntdsutil: Activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
```

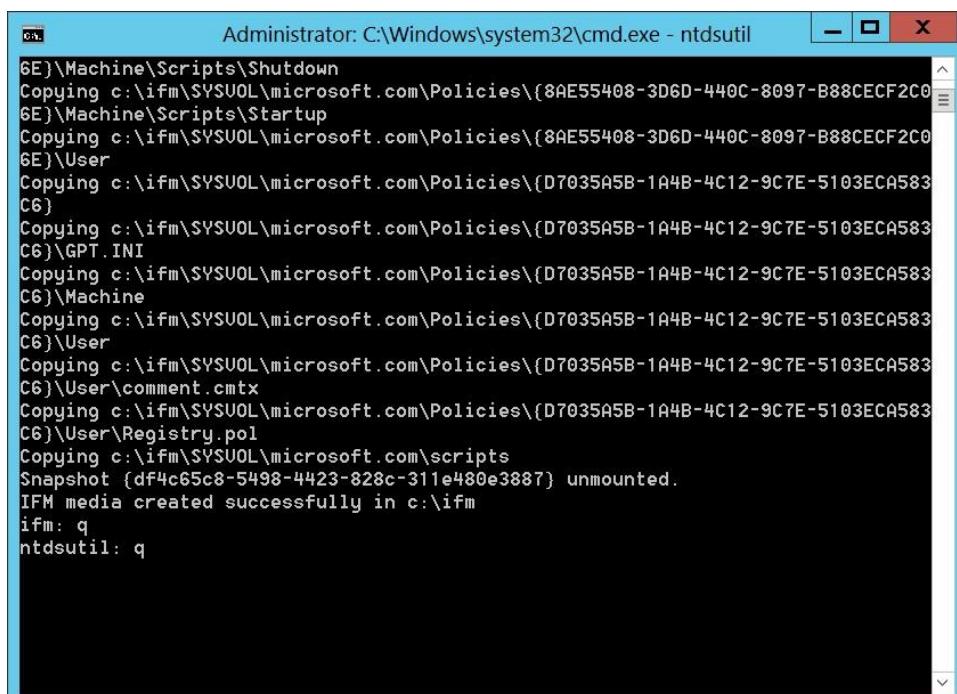
7. Type **createsysvolRODCC:\ifm**



```
Administrator: C:\Windows\system32\cmd.exe - n

C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create sysvol rodc c:\ifm
Creating snapshot for RODC media...
```

8. Verify for the **snapshot generated successfully** then type **quit**, and again **quit**.



```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
6E)\Machine\Scripts\Shutdown
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{8AE55408-3D6D-440C-8097-B88CECF2C0
6E)\Machine\Scripts\Startup
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{8AE55408-3D6D-440C-8097-B88CECF2C0
6E)\User
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{D7035A5B-1A4B-4C12-9C7E-5103ECA583
C6}
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{D7035A5B-1A4B-4C12-9C7E-5103ECA583
C6}\GPT.INI
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{D7035A5B-1A4B-4C12-9C7E-5103ECA583
C6}\Machine
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{D7035A5B-1A4B-4C12-9C7E-5103ECA583
C6}\User
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{D7035A5B-1A4B-4C12-9C7E-5103ECA583
C6}\User\comment.cmtx
Copying c:\ifm\SYSUOL\microsoft.com\Policies\{D7035A5B-1A4B-4C12-9C7E-5103ECA583
C6}\User\Registry.pol
Copying c:\ifm\SYSUOL\microsoft.com\scripts
Snapshot {df4c65c8-5498-4423-828c-311e480e3887} unmounted.
IFM media created successfully in c:\ifm
ifm: q
ntdsutil: q
```

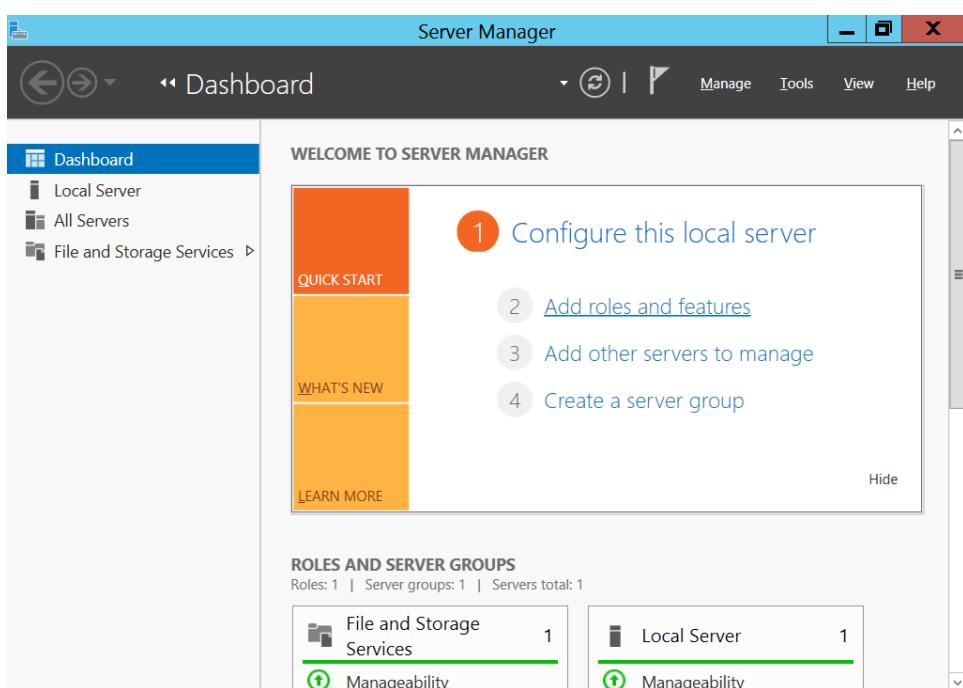
9. Log in as Administrator to the **Workgroup Computer(SYS2)**

10. Assign **IP Address** and Preferred **DNS Server Address**.

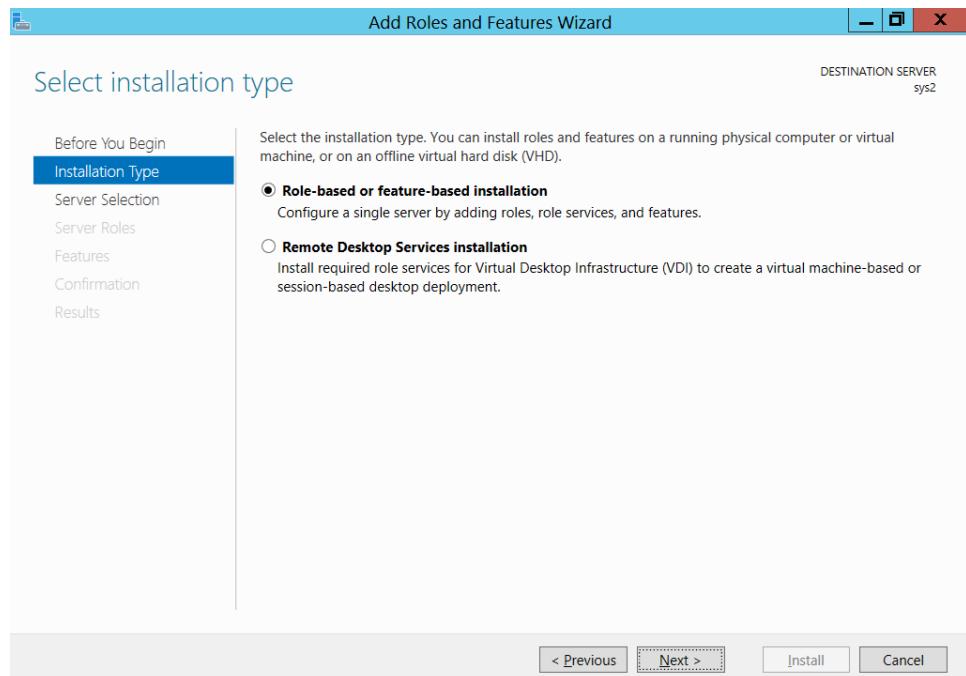
11. Access the shared folder (Ex: ifm) on Domain Controller and copy it to local hard disk drive (Ex: C drive).
12. Click **Server Manager**



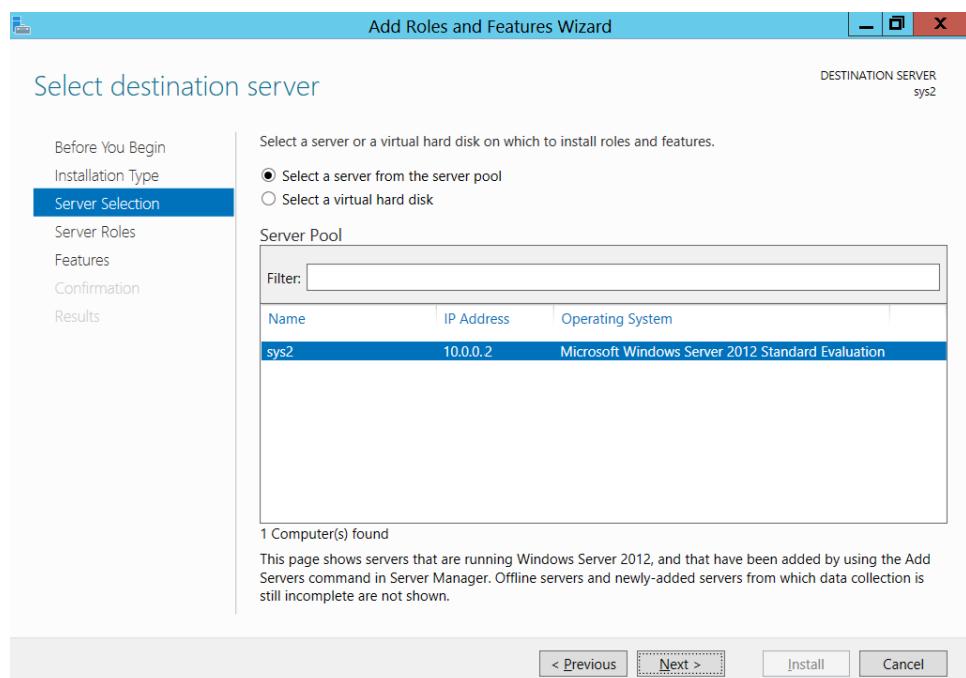
13. In Server Manager Dashboard, Click **Add roles and features**.



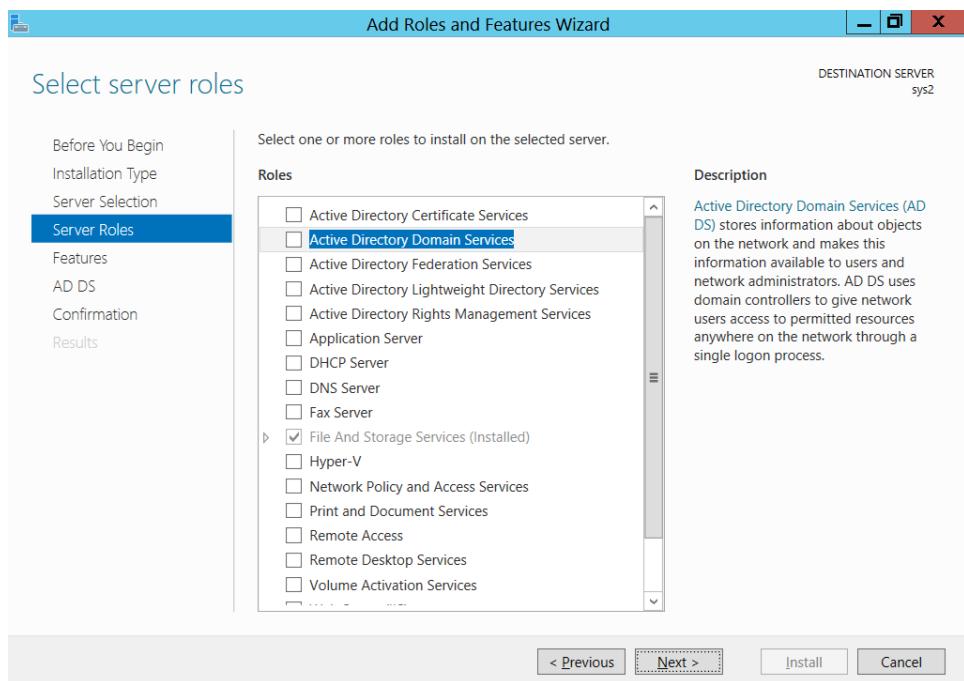
14. In Before you begin page, click **Next**, In Select installation type, select **Role-based or feature-based installation**, click **Next**.



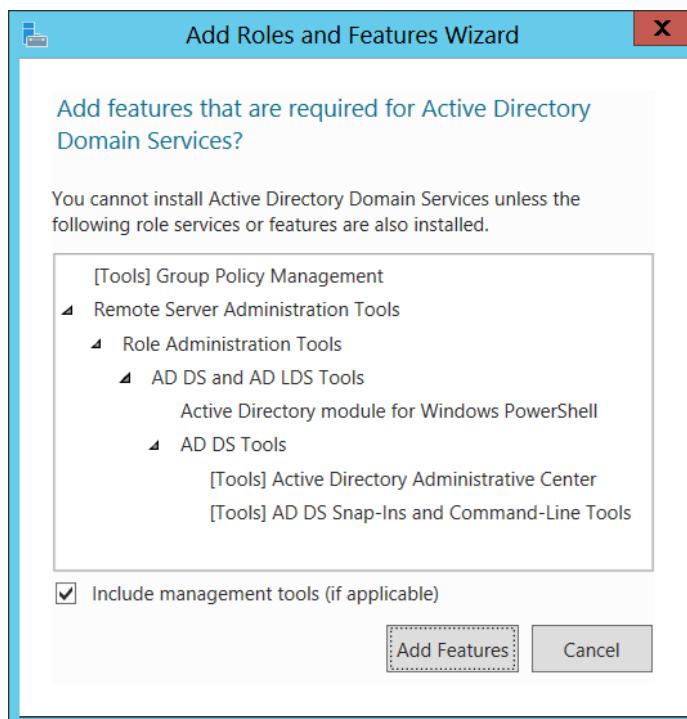
15. In Select destination server, from Server Pool select **SYS2**,click**Next**.



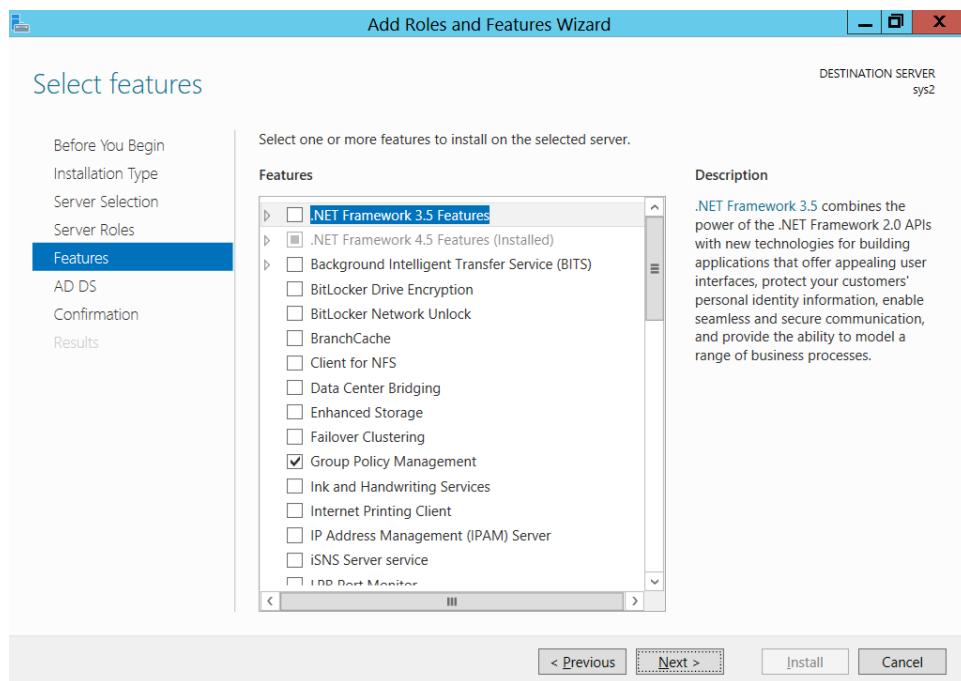
16. In Roles, check the box Active Directory Domain Services.



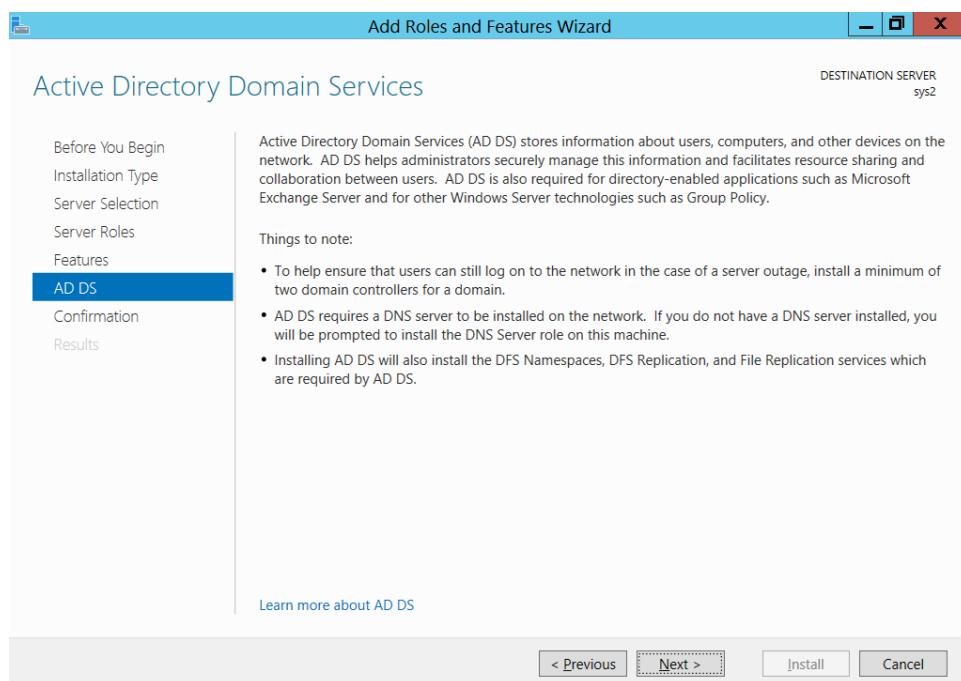
17. Click **Add Features, to install the required features for Active Directory Domain Services. Click **Next**.**



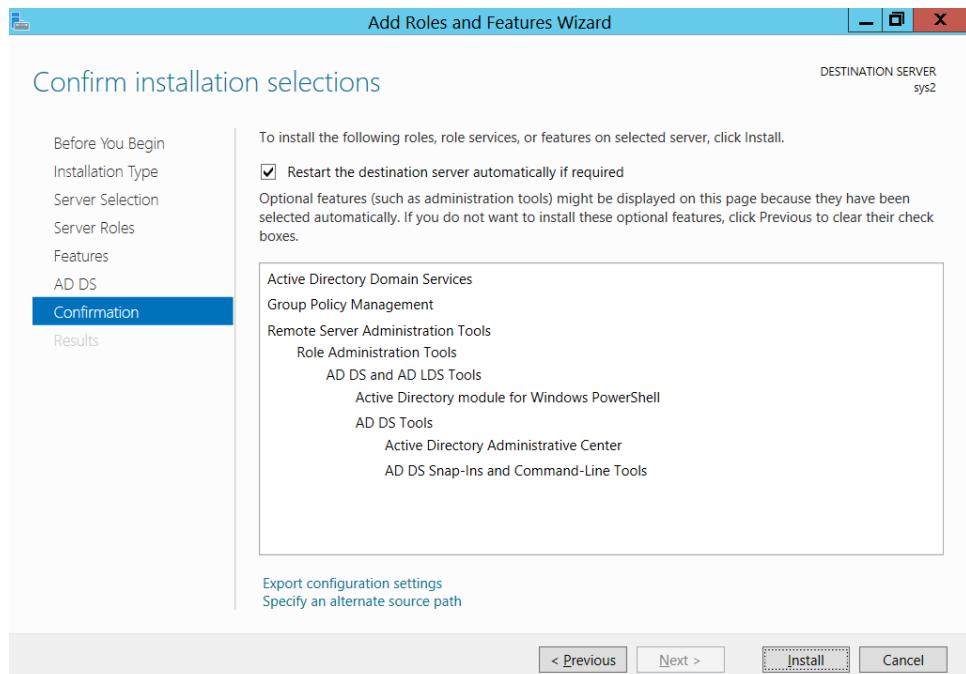
18. In Select features wizard, click **Next.**



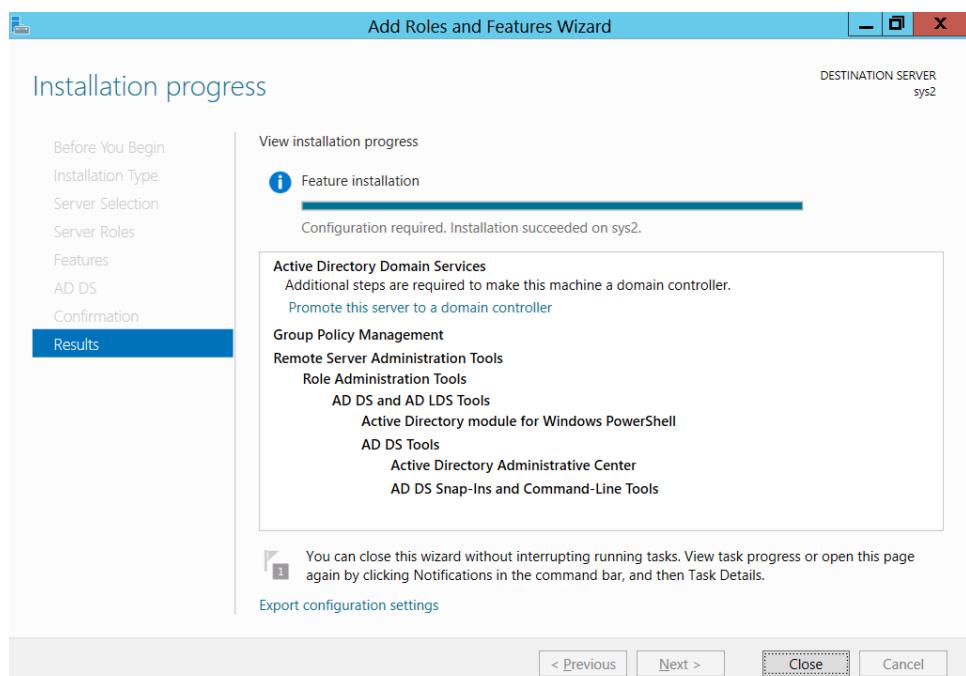
19. In Active Directory Domain Services wizard, click **Next.**



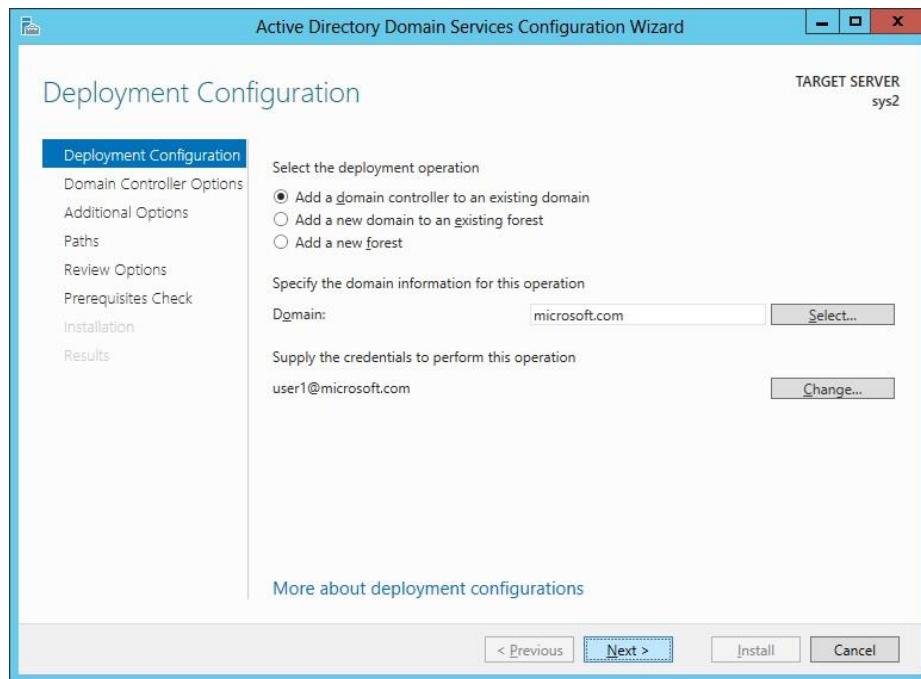
- 20. Check the box **Restart the destination server automatically if required**. Click **Install**.**



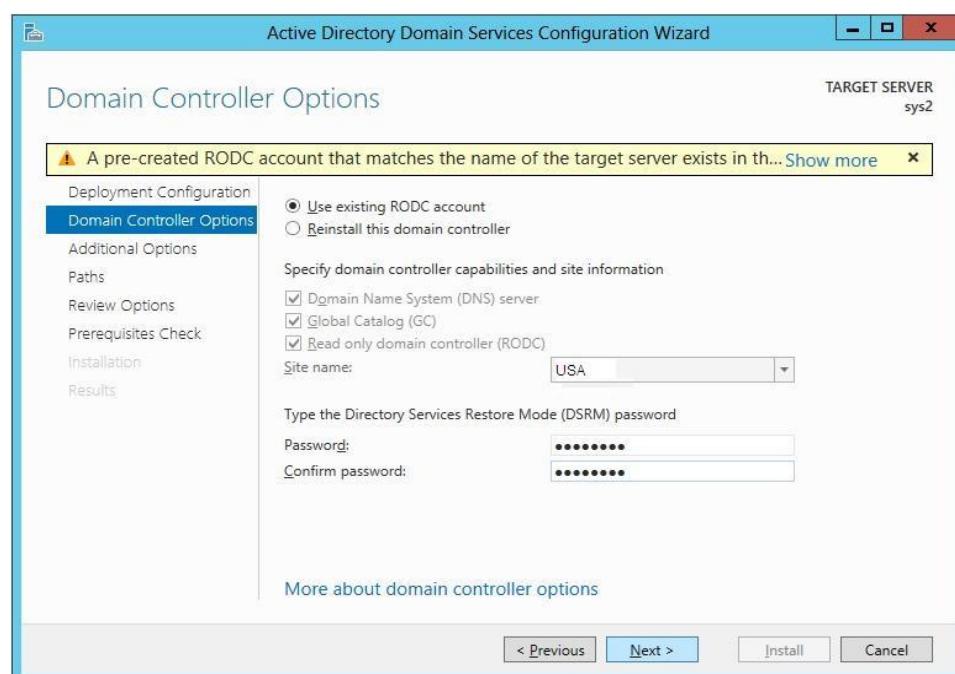
- 21. Click **Promote this server to a domain controller**.**



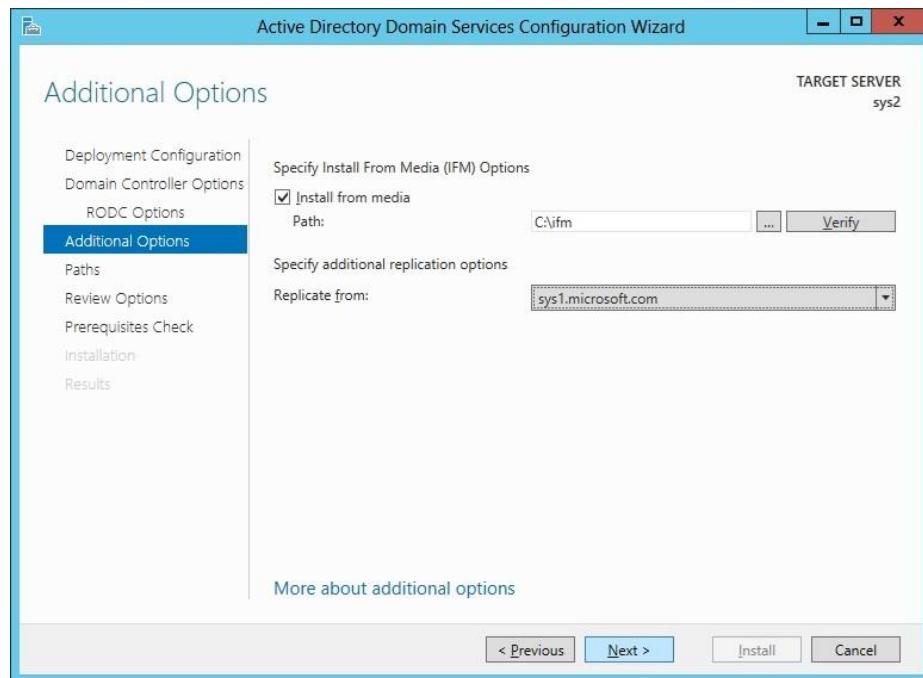
22. In Deployment Configuration wizard, select **Add a domain controller to an existing domain**, enter the Domain (Ex: Microsoft.com)
23. Click **Change**, enter User Name: user1@microsoft.com and Password, click **OK→Next.**



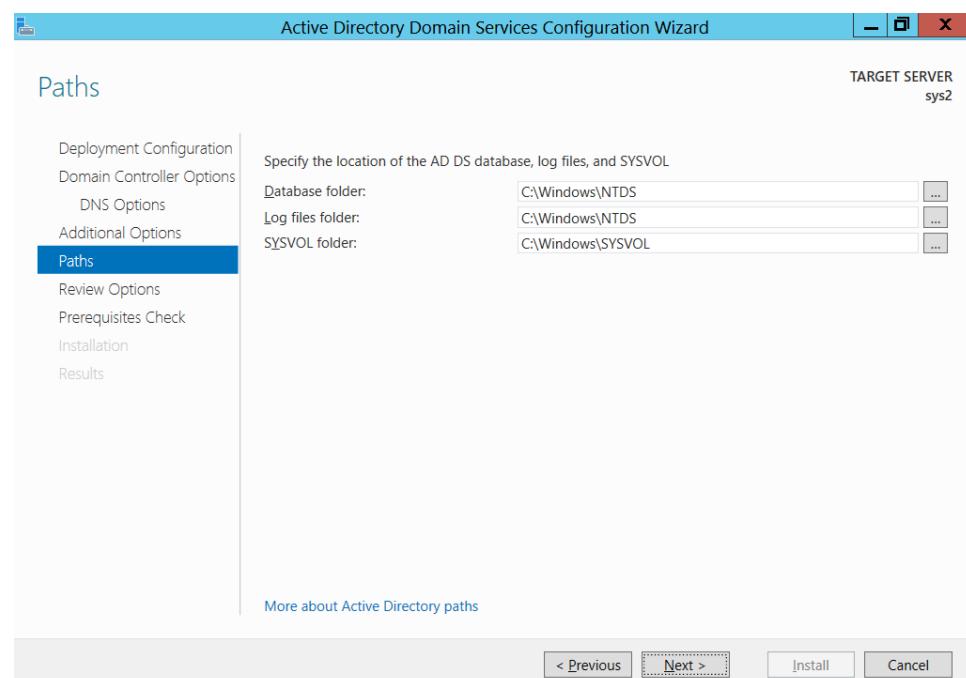
24. In Domain Controller Options, review the default settings, and type the Directory Services Restore Mode **Password** and **Confirm password** and click **Next**.



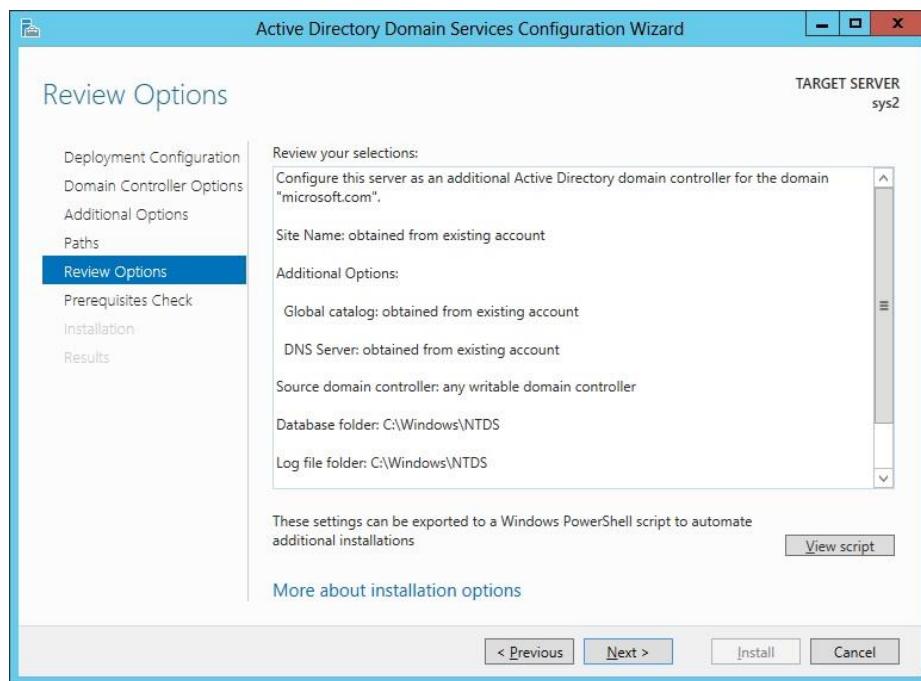
25. In Additional Options Page, check box Install from media, browse and select the folder C:\ifm → select Replicate from **Sys1.Microsoft.com**, click **Next**.



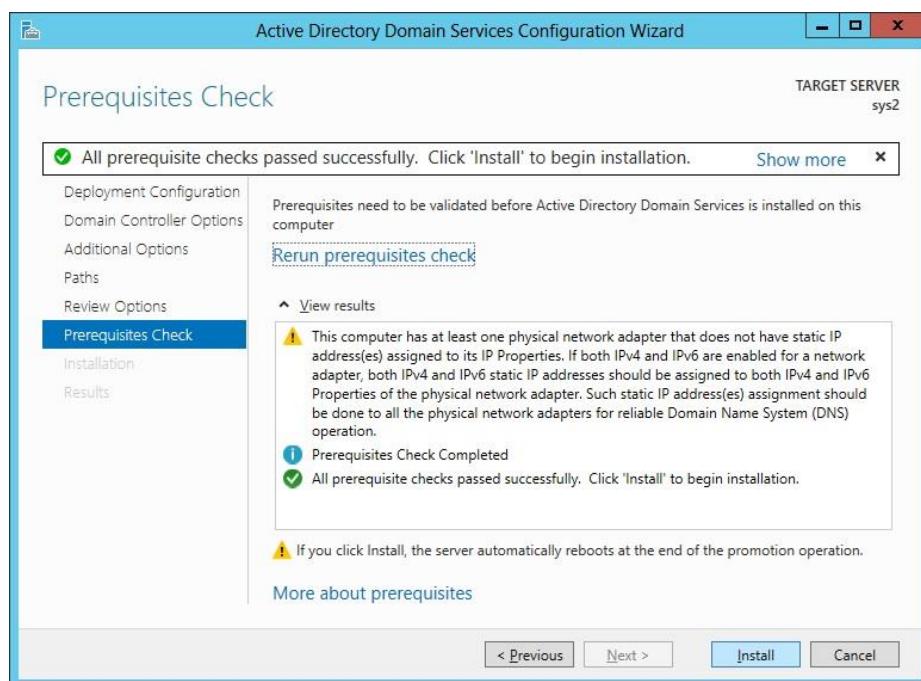
26. Verify the location of the AD DS database, log files, and SYSVOL, click **Next**.



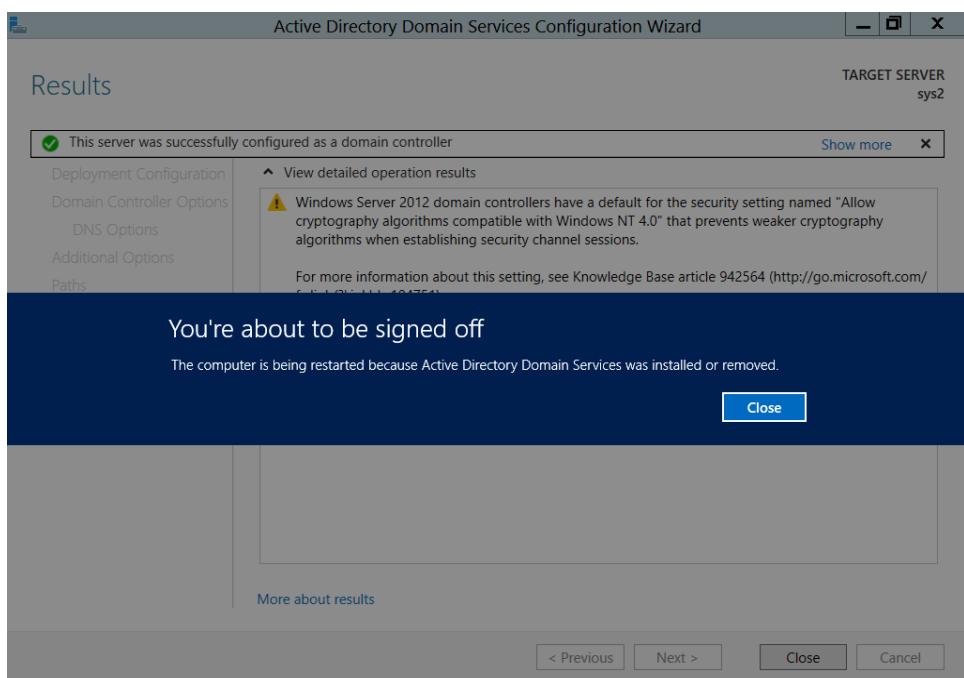
27. Review the Summary and click **Next**.



28. Click **Install** to begin installation.



29. The computer restarts as a part of Active Directory Domain Services installation.



30. After restarting the computer **Active directory** will be installed.

Verification:

1. Log on to **Domain Controller (SYS1)** as **Administrator**
2. Go to Active Directory Users and Computer, Expand Domain Controllers OU and verify for **SYS2** as **Read Only Domain Controller**.

Name	Type	DC Type	Site	Description
SYS1	Computer	GC	INDIA	
SYS2	Computer	Read-only, GC	USA	

DYNAMIC HOST CONFIGURATION PROTOCOL

Types of IP addresses

IP addresses can be

- **Static IP address**
 - Addresses that are manually assigned and do not change over time
- **Dynamic IP address**
 - Addresses that are automatically assigned for a specific period of time and might change

What is DHCP?

- It gives IP Addresses automatically to the clients who is requesting for an IP Address
- Centralized IP Address management
- DHCP prevents IP address conflicts and helps conserve the use of client IP Address on the network
- DHCP reduces the complexity and amount of administrative work by assigning TCP/IP configuration automatically to the Clients.

DHCP

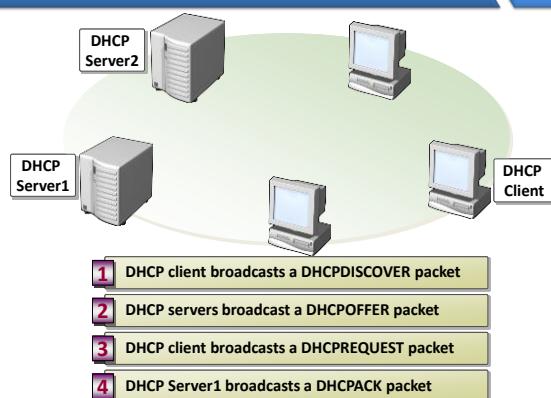
AUTHORIZATION

- In Domain model the DHCP server should be authorized to assign the IP Addresses to clients.
- It is a security precaution that ensures that only authorized DHCP servers can run in the network. To avoid computers running illegal DHCP servers in the network.

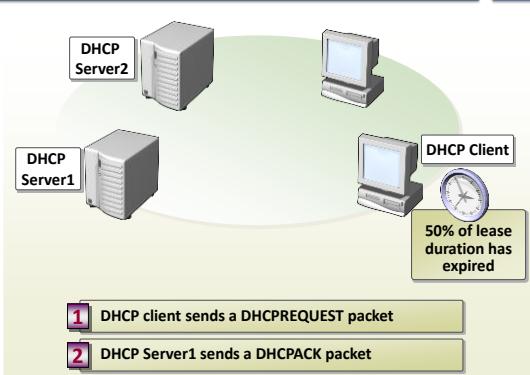
SCOPE

- A scope is a range of IP addresses that are available to be leased to clients.

DHCP Lease Generation Process

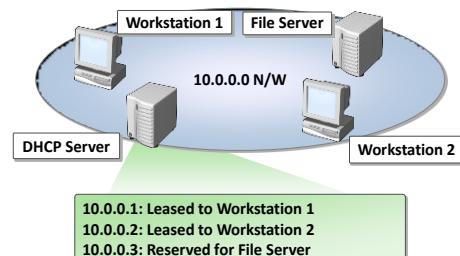


DHCP Lease Renewal Process



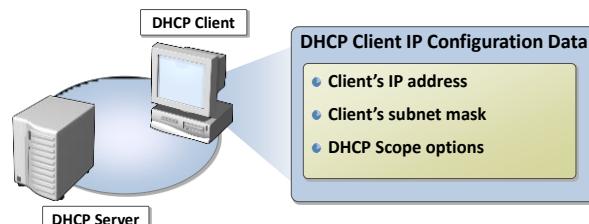
What is DHCP Reservation?

- A reservation is a specific IP address, within a scope, that is permanently reserved to a specific DHCP client



What are DHCP options?

- DHCP Scope options are other server addresses given to clients along with IP Configuration.



DHCP Failover

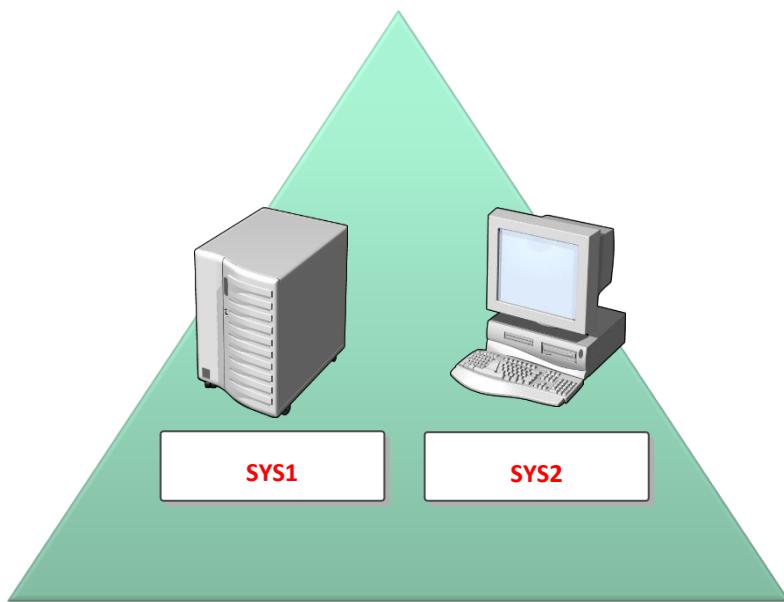
- DHCP failover is a new feature available in Windows Server® 2012 ensuring continuous availability of DHCP service to clients.
- With DHCP failover, two DHCP servers share DHCP scope and lease information, enabling one server to provide DHCP leases to DHCP clients if the other server is unavailable
- Hot stand-by mode: This mode provides redundancy for DHCP services.
- Load balance mode: This mode allocates DHCP client leases across two servers.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Prerequisites:

Before working on this lab, you must have

3. A computer running windows 2012 server or Domain Controller.
4. A computer running windows 2012 server or windows 7.



MICROSOFT.COM

SYS1	SYS2
Domain Controller / DHCP Server	Member Server / Client
IP Address 10.0.0.1	IP Address 10.0.0.2
Subnet Mask 255.0.0.0	Subnet Mask 255.0.0.0
Preferred DNS 10.0.0.1	Preferred DNS 10.0.0.1

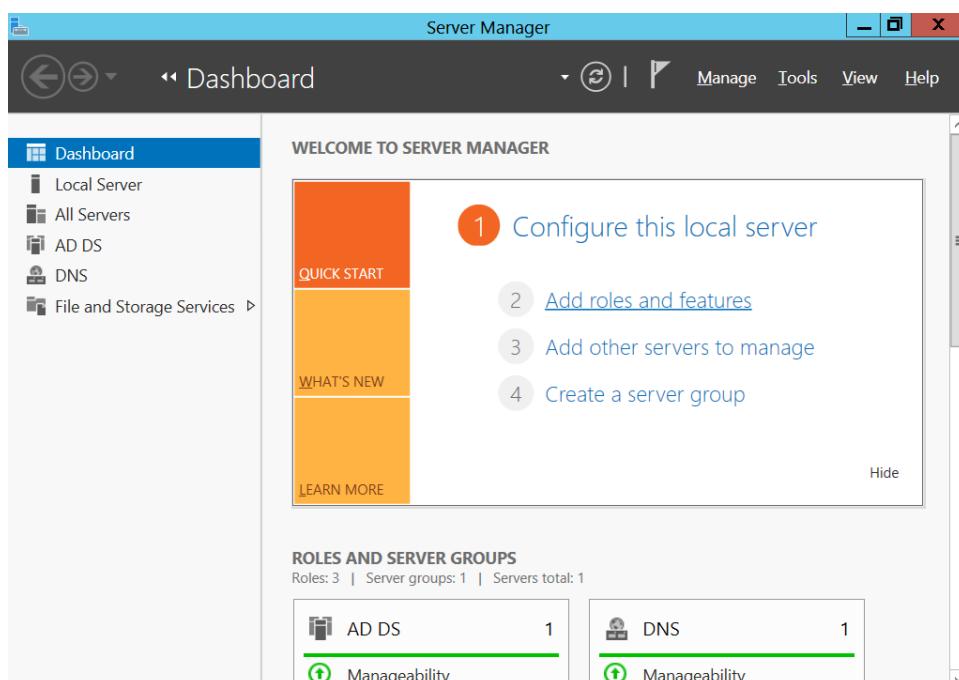
Lab – 1: Installing DHCP Service

SYS1 - CONFIGURATION

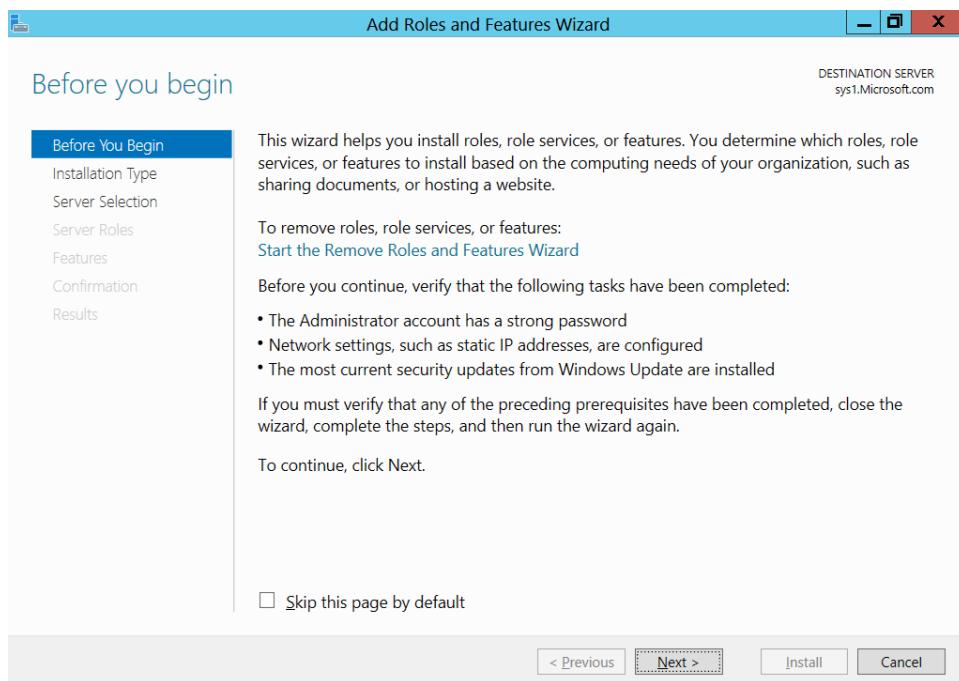
1. Click **Server Manager**.



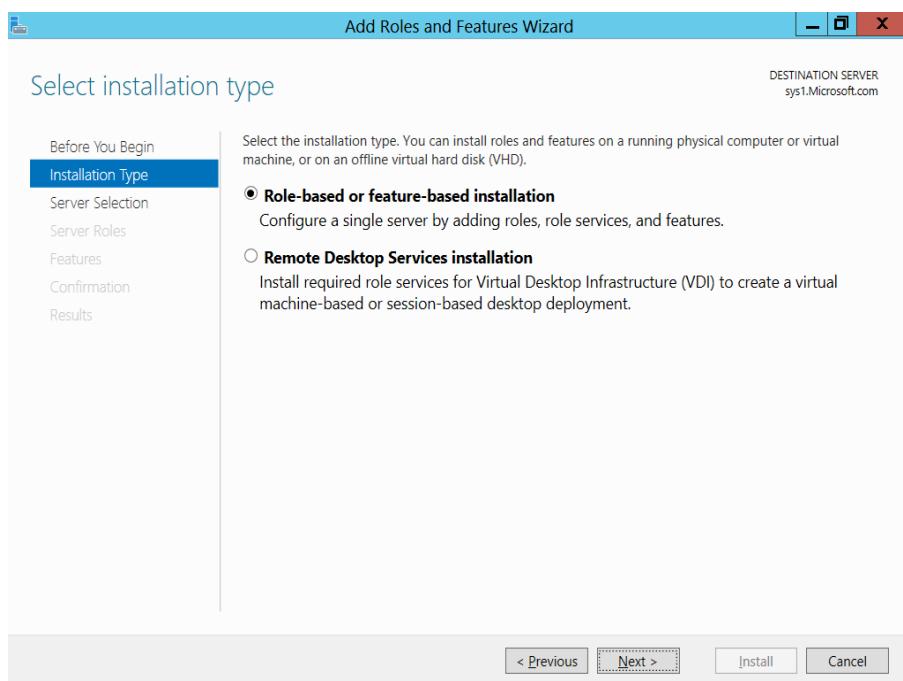
2. In the Server Manager Console, Select **Add roles and features**



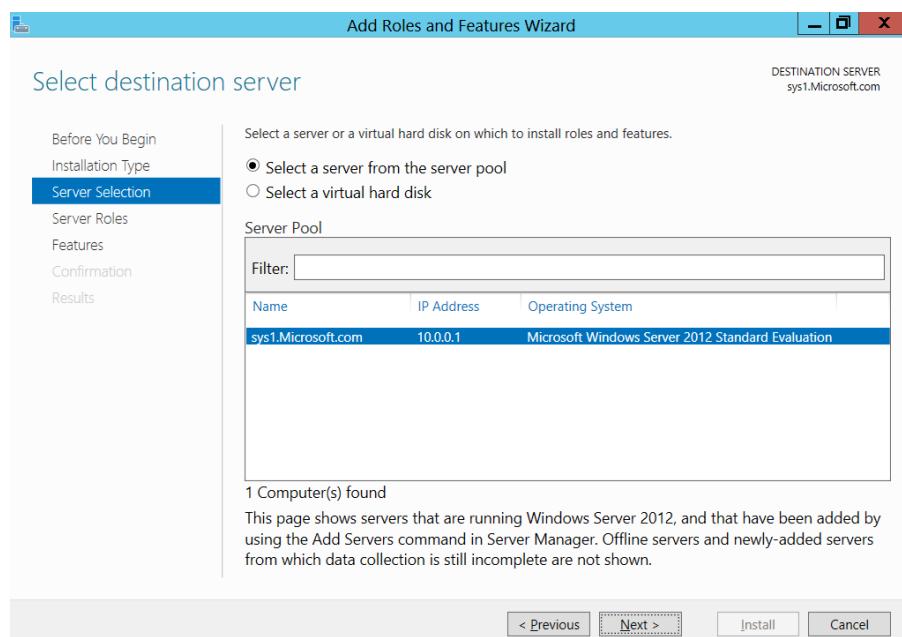
3. In before you begin page, click **Next**.



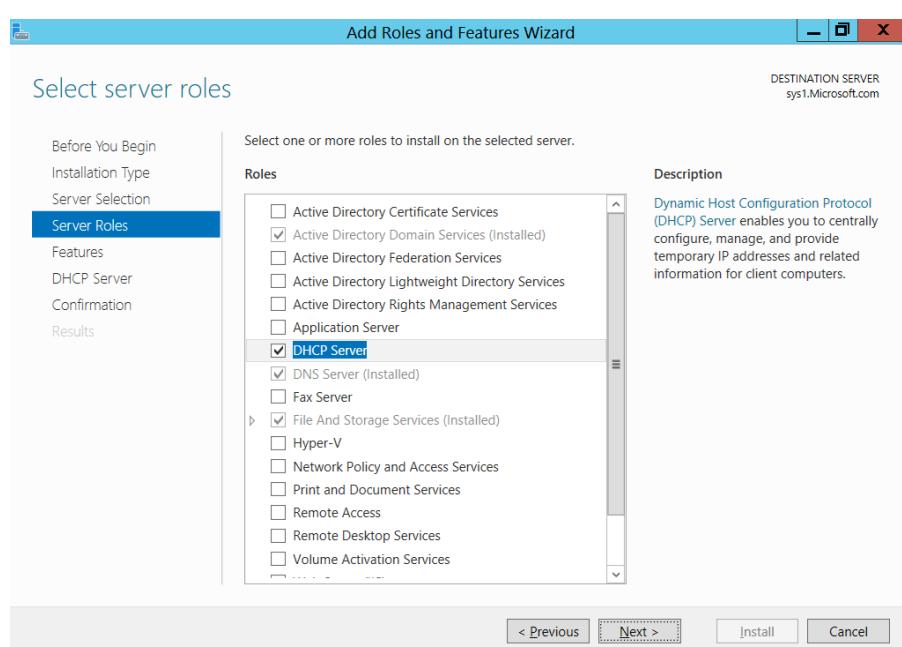
4. Select **Role-based or feature-based installation**, click **Next**.



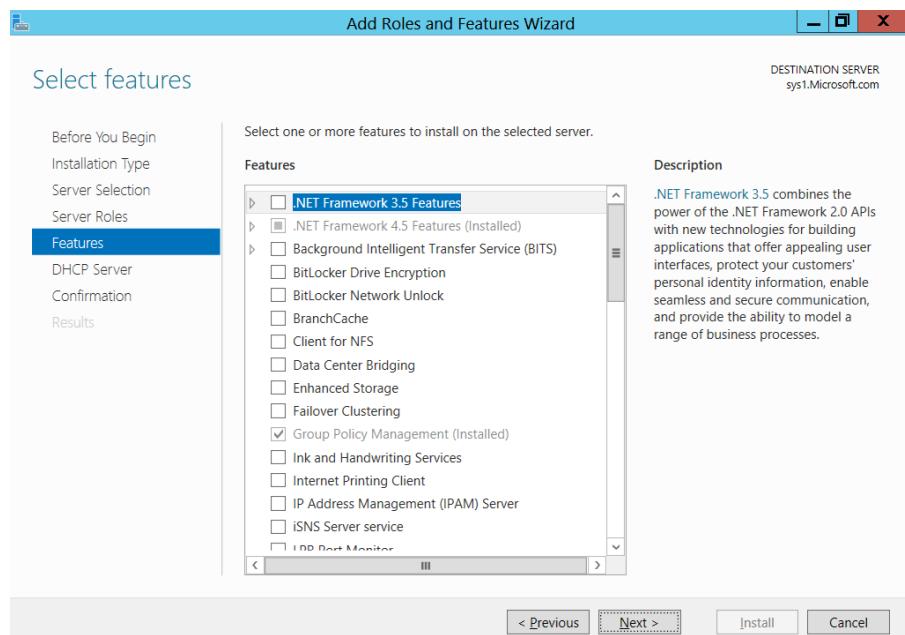
- 5. Select a server (**sys1.Microsoft.com**) from the server pool and click **Next**.**



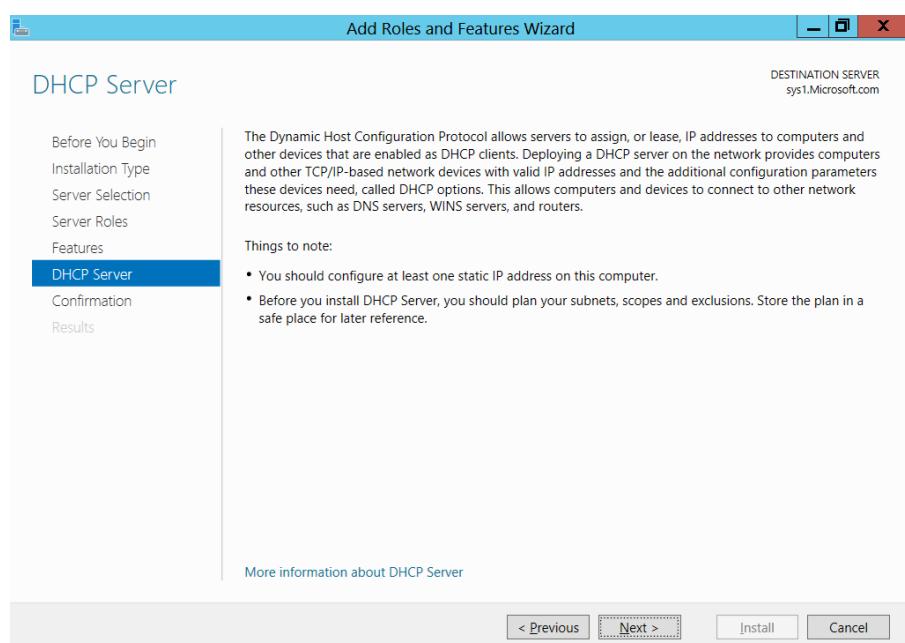
- 6. In select server roles, check the box DHCP Server and click **Next**.**

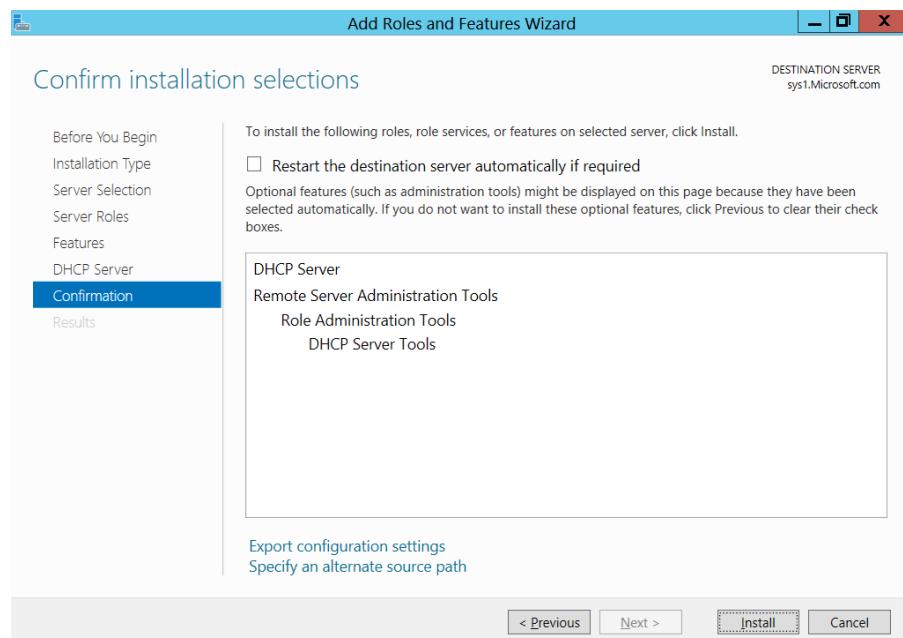
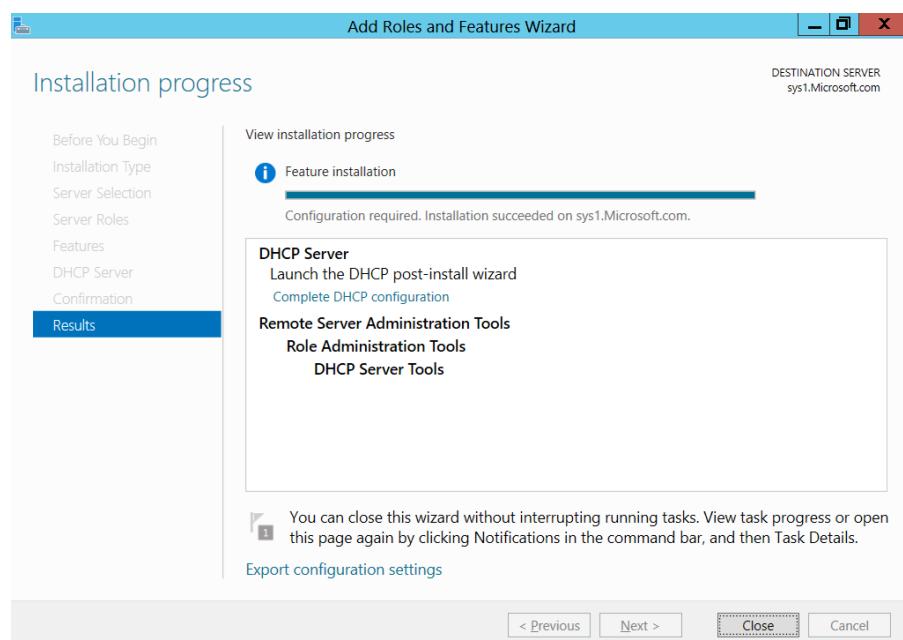


7. In select features, click **Next**.

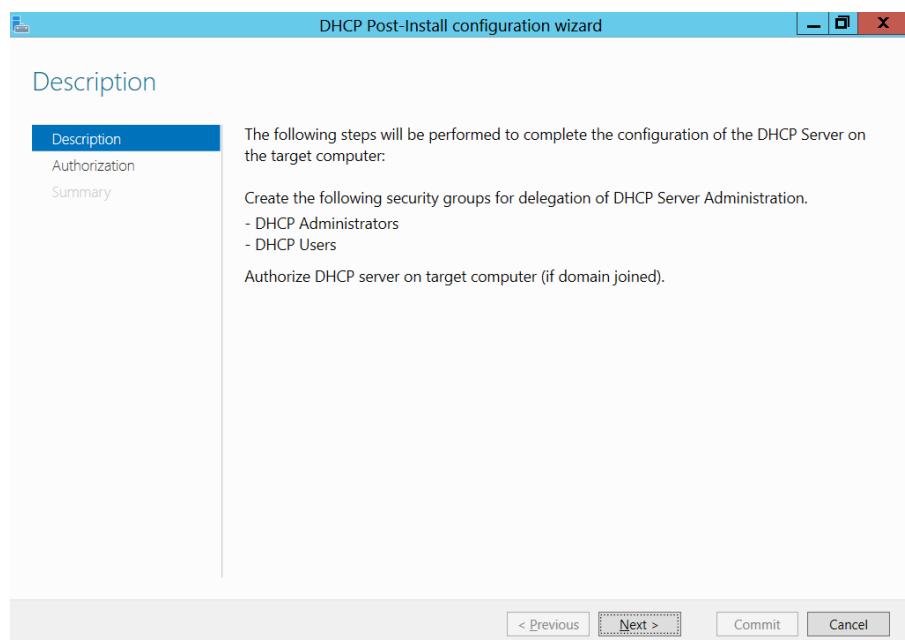


8. Click **Next**.

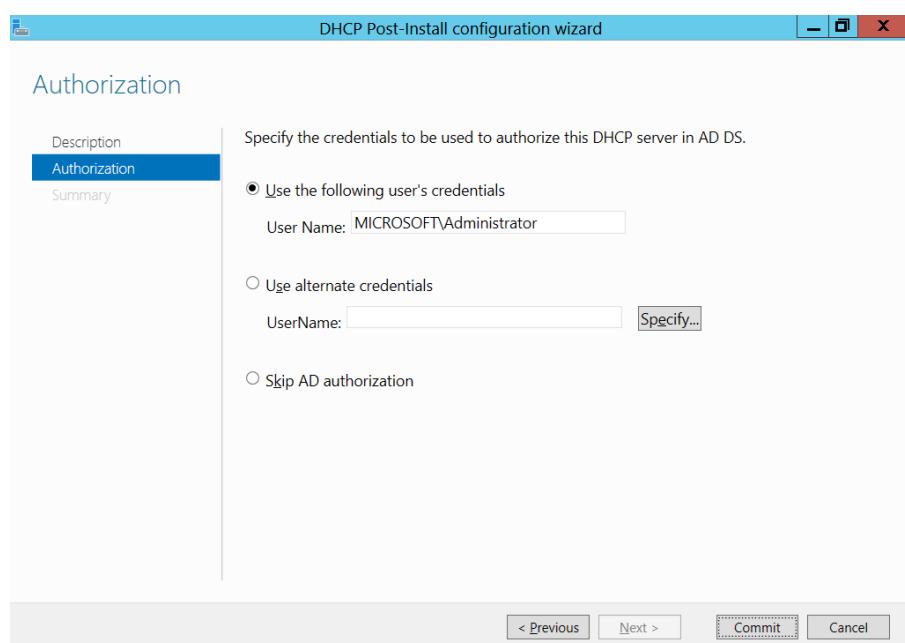


9. Check Restart the destination server automatically if required and click **Install.****10. Select Complete DHCP configuration.**

11. In DHCP Post-install configuration wizard, click **Next**.



12. Click **Commit** to Authorize the DHCP Server.



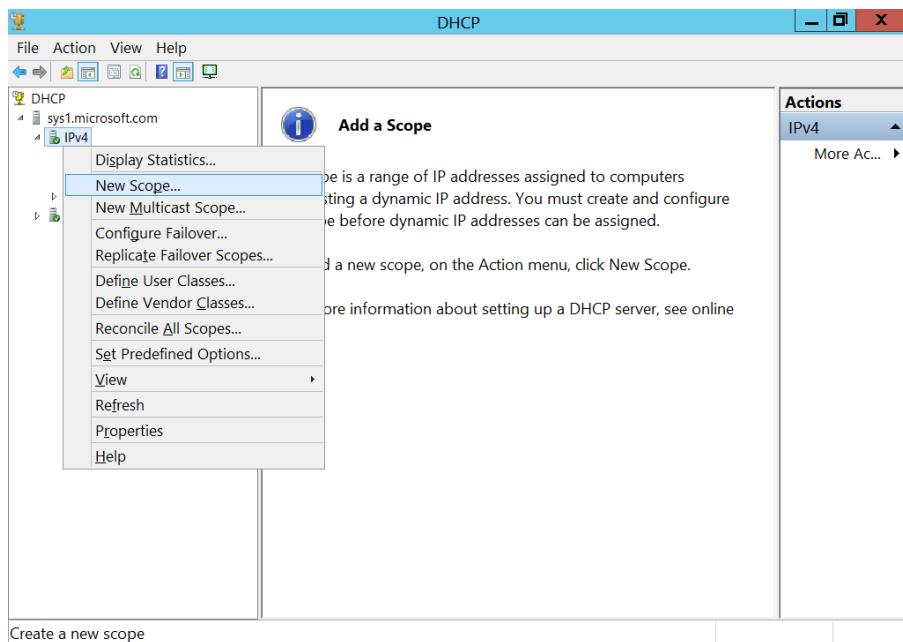
13. Click **Close** to Complete the Authorization of DHCP Server.

Lab – 2: Creating a scope

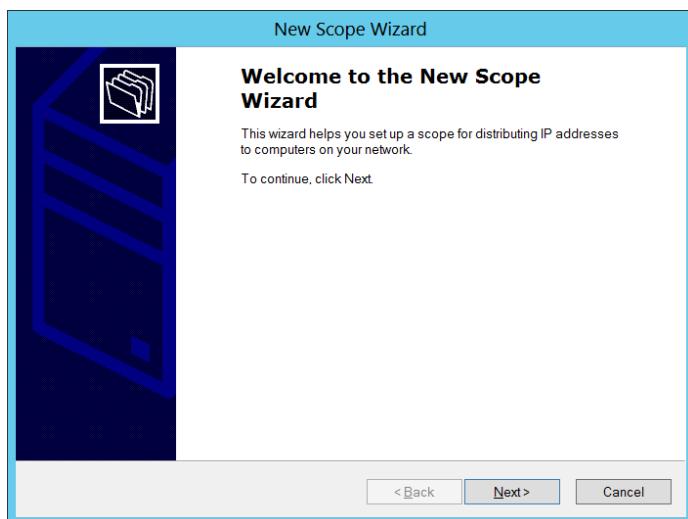
1. Go to Start, select **DHCP**.



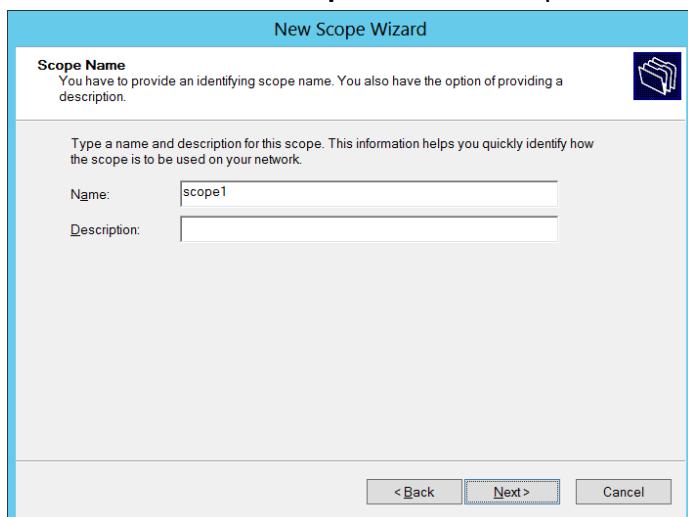
2. Expand the System name → right click IPv4 → select **New Scope**



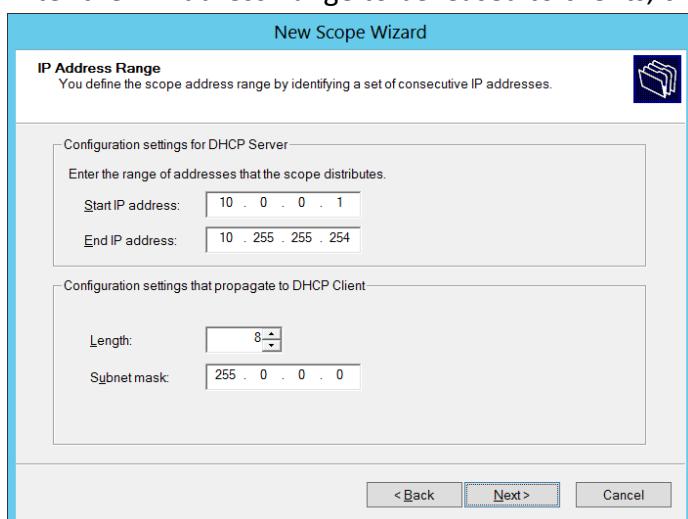
3. The New Scope wizard starts, click **Next**.



4. Enter **Name** and a **Description** for the scope and click **Next**.

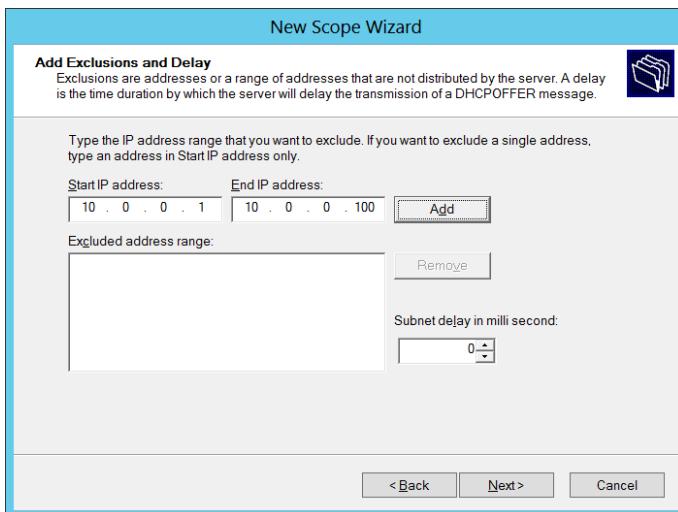


5. Enter the IP Address Range to be leased to clients, click **Next**.

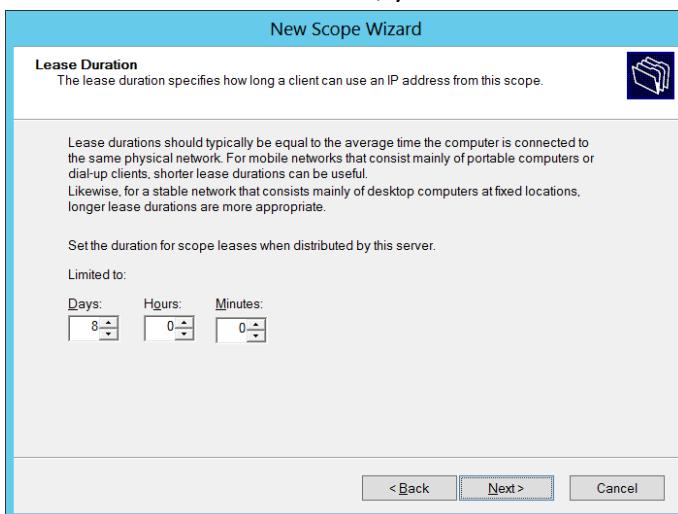


Note: Mention the scope range in the same network of DHCP server.

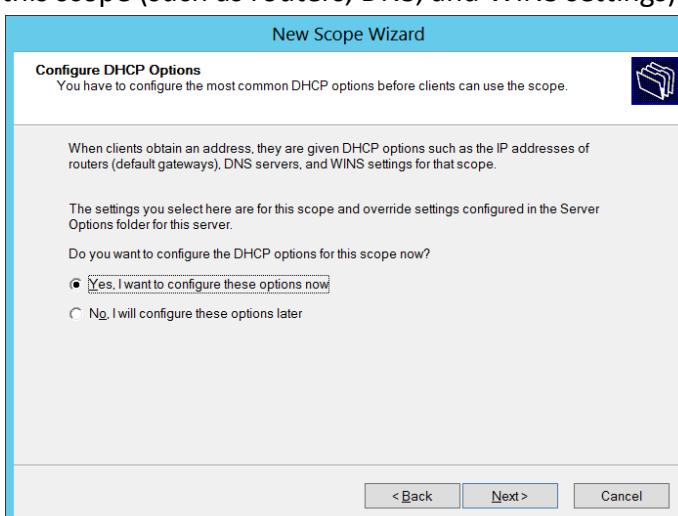
6. To exclude IP addresses, enter the **Start and end IP address**, click **Add**. Click **Next**.



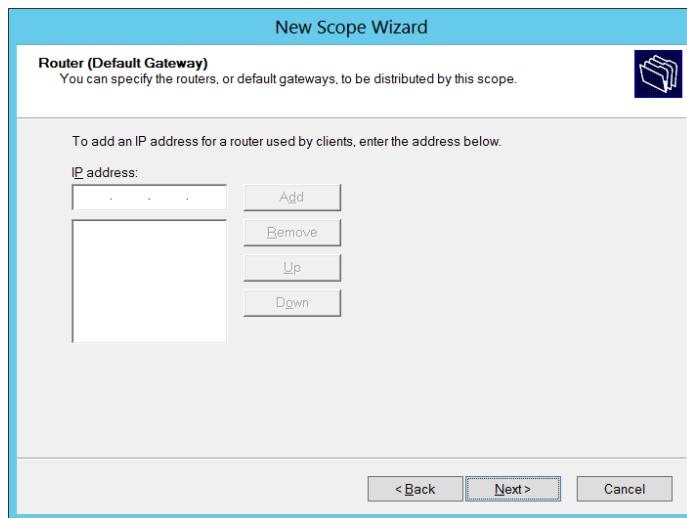
7. In the **Lease Duration** screen, you can Increase or Decrease the value, click **Next**.



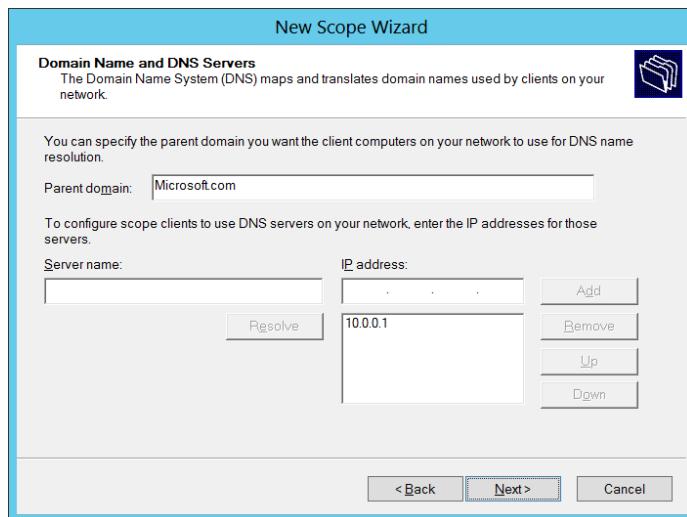
8. In the **Configure DHCP Options** screen, choose **Yes**, to configure DHCP options for this scope (such as routers, DNS, and WINS settings) now. Click **Next**.



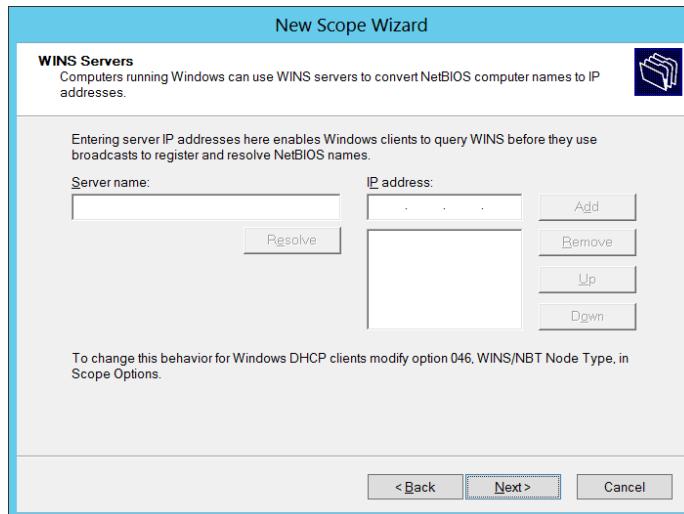
9. In the **Router (Default Gateway)** screen, enter the IP address of the **router** that will function as the **default gateway** for this scope clients and click **Add**. Or, if you don't have a **Router** in your network, just click **Next**.



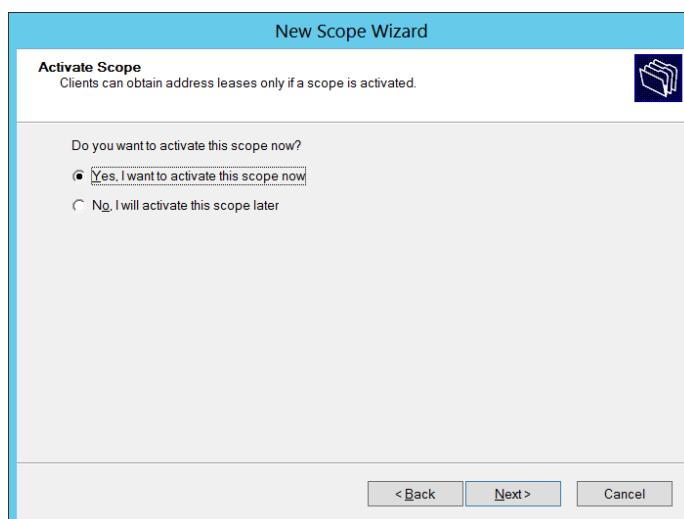
10. In the **Domain Name** and **DNS Servers** screen enter the name of the Parent Domain & IP address of the DNS server, click **Add** → click **Next**.



11. In the WINS Servers screen enter the IP address of the WINS server, click **Add** click **Next**, if you don't have a WINS server on your network, just click **Next**.

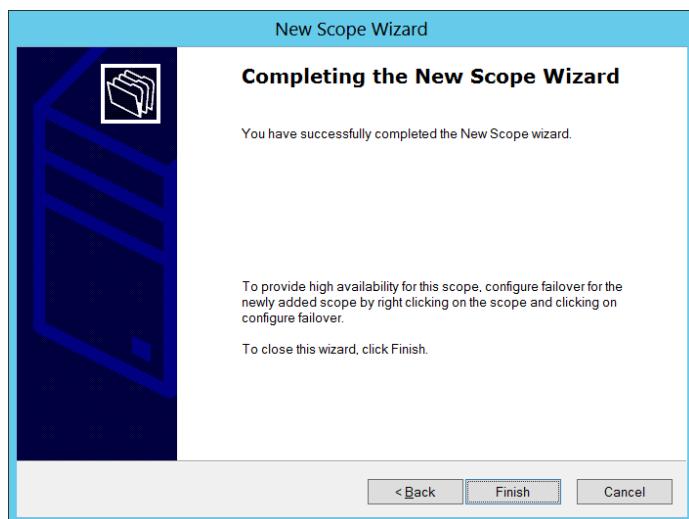


12. In the Activate Scope screen, select **YES** and click **Next**.



Note: A DHCP server can't assign IP addresses until the scope is activated.

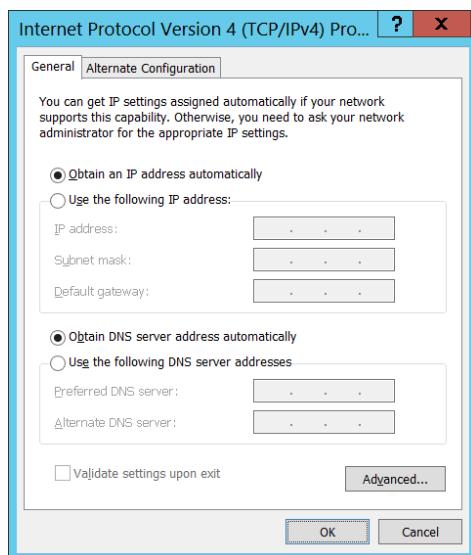
13. Click **Finish** to complete the creation of Scope.



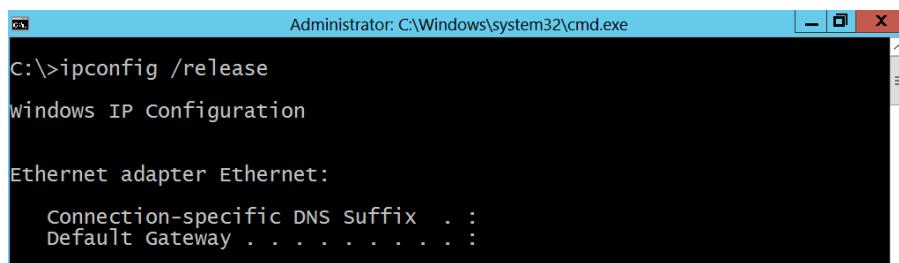
SYS2 - CONFIGURATION

Verification: In DHCP Client

1. Right click network Icon → Select properties → click View Status and select properties → Select Internet protocol Version 4 (TCP/IPv4) Properties and select **Obtain an IP Address automatically** and **Obtain an DNS Server Address Automatically** → OK



2. Open the **Command Prompt** → and type **Ipconfig /release**

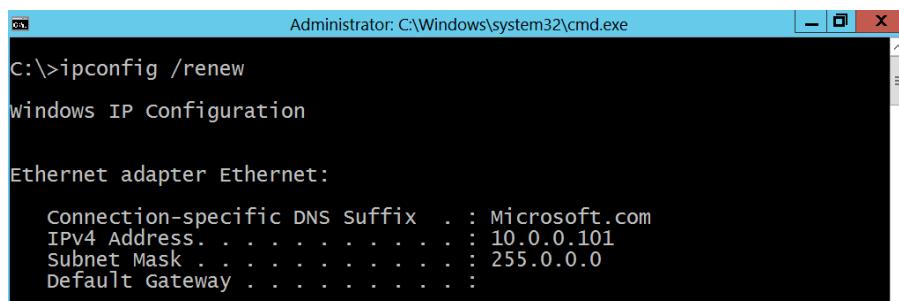


```
Administrator: C:\Windows\system32\cmd.exe
C:\>ipconfig /release
Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . .
  Default Gateway . . . . .
```

3. Then type **Ipconfig/renew**

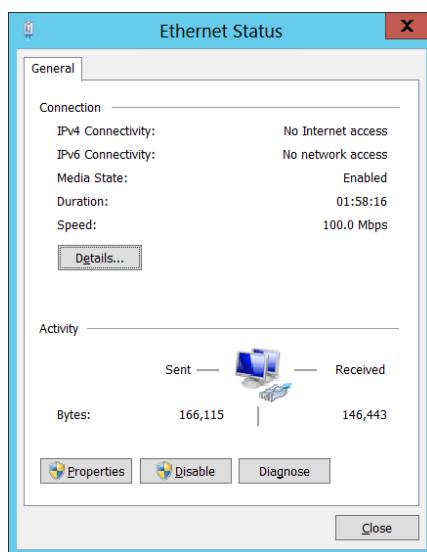


```
Administrator: C:\Windows\system32\cmd.exe
C:\>ipconfig /renew
Windows IP Configuration

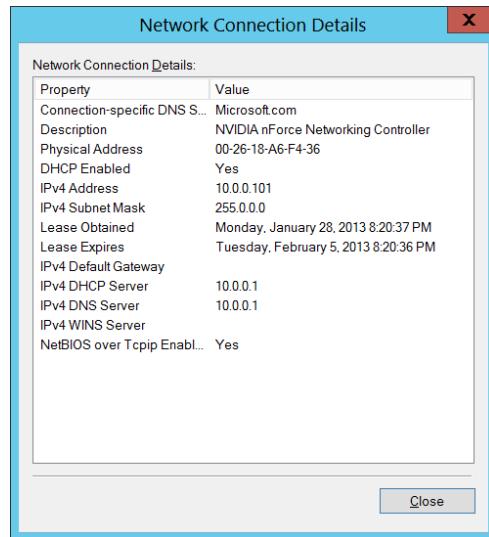
Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . : Microsoft.com
  IPv4 Address. . . . . : 10.0.0.101
  Subnet Mask . . . . . : 255.0.0.0
  Default Gateway . . . . .
```

4. After that Right click on network Icon → Select properties → click View Status and click **Details.**



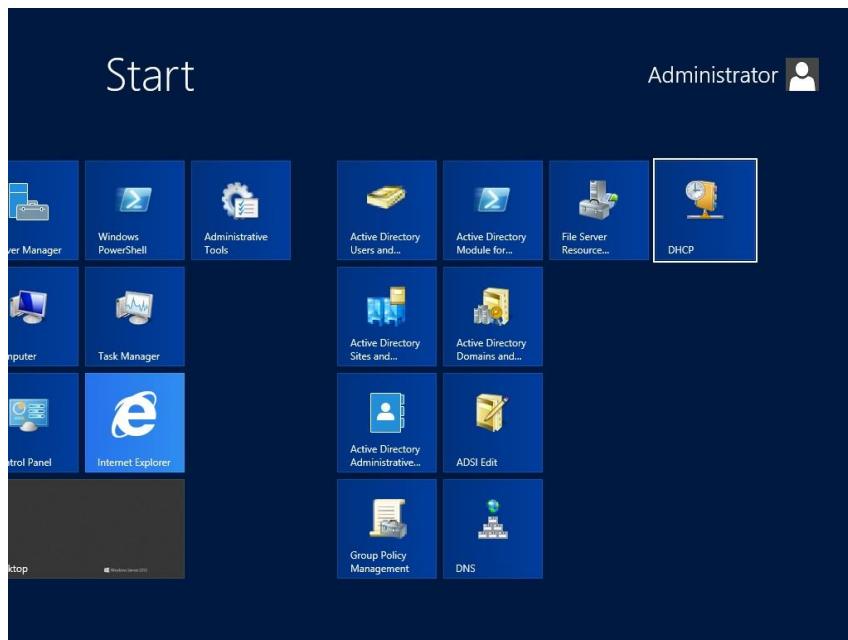
5. Verify the IP Address leased by the DHCP Server along with the lease duration and DHCP Server and DNS Server details.



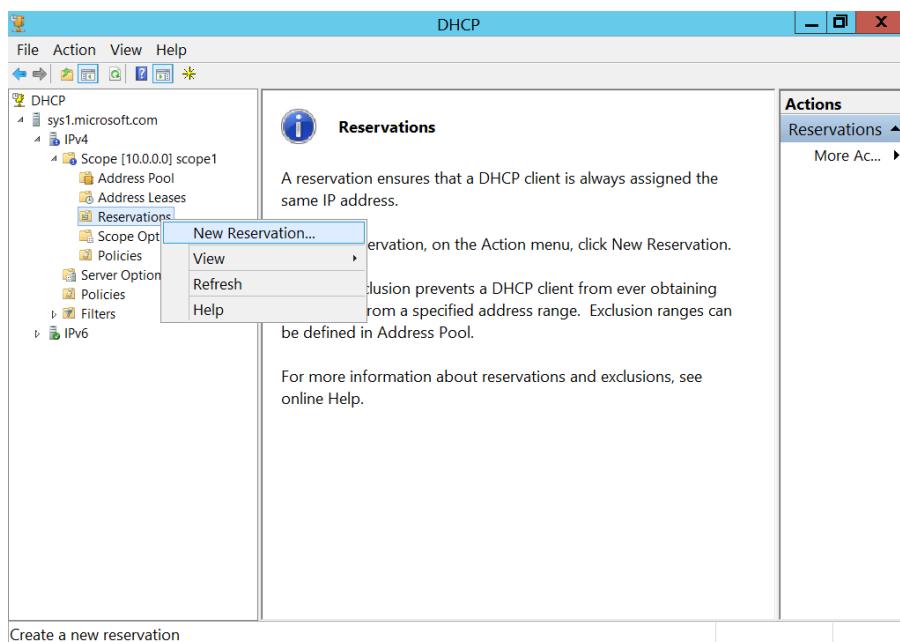
Lab – 3: Creating DHCP Reservations

SYS1 - CONFIGURATION

1. Go to Start, select **DHCP**.

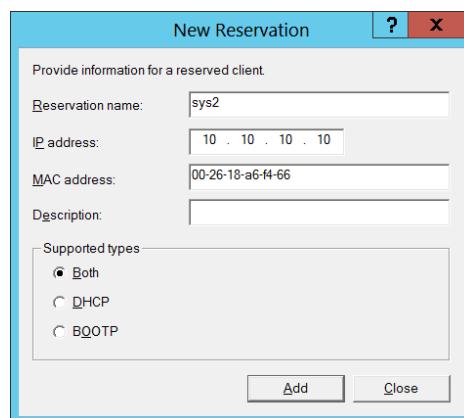


2. In the left pane of the DHCP Console, expand the Scope → Right click **Reservation** → Select **New Reservation**



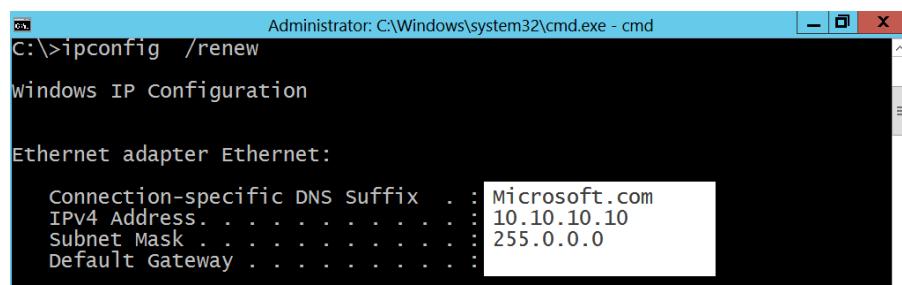
3. Type in a name for the reservation in the “**Reservation name**” text box. Then, in the “**IP address**” text box, mention the IP address that you want to be reserved. Then, enter the MAC address of the network adapter of the computer for which the reservation is being made in the box provided → click **Add** → click **Close**.

Note: To Know the MAC or Physical address of the client type **Ipconfig /all** or **getmac** in command prompt of client computer.



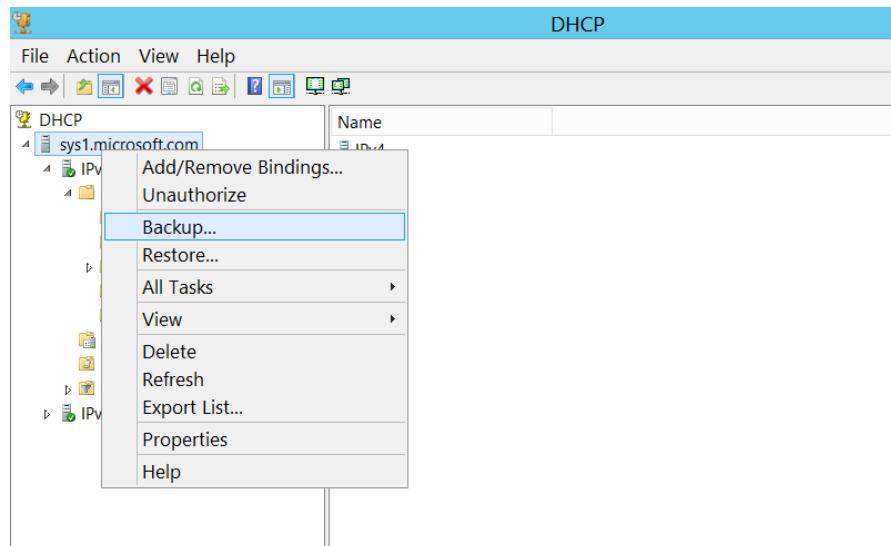
Check the output in the client computer (SYS2).

4. In the command prompt type **Ipconfig /release** and **Ipconfig /renew**.

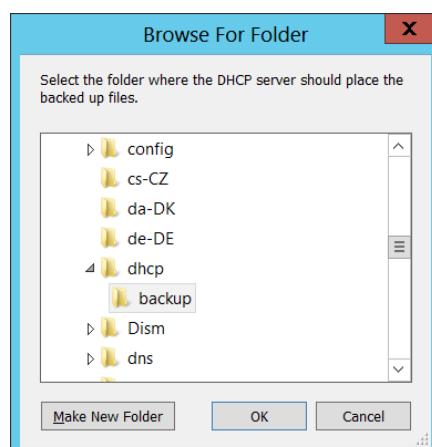


Lab – 4: DHCP Server Backup and Restore

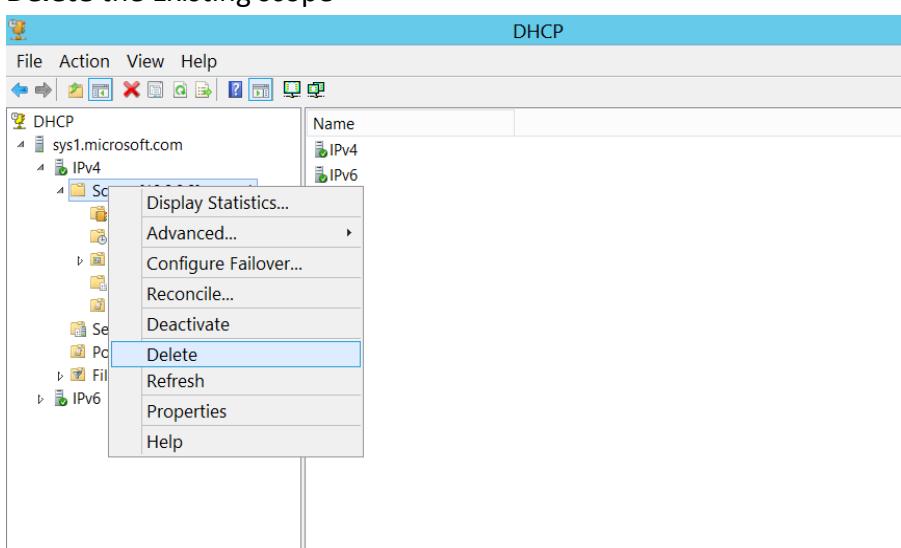
1. Go to DHCP console → right click the server name → select **Backup**



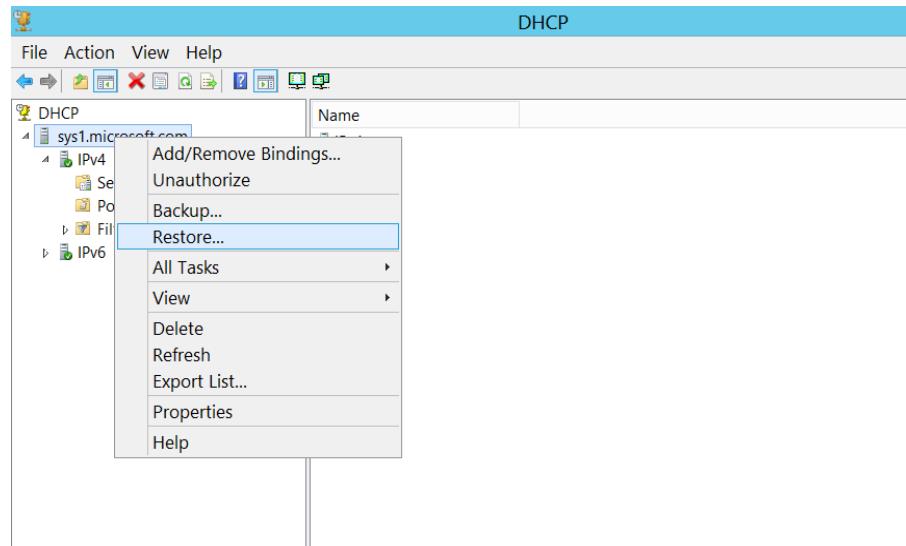
2. Select the Location to save the **backup file** → OK



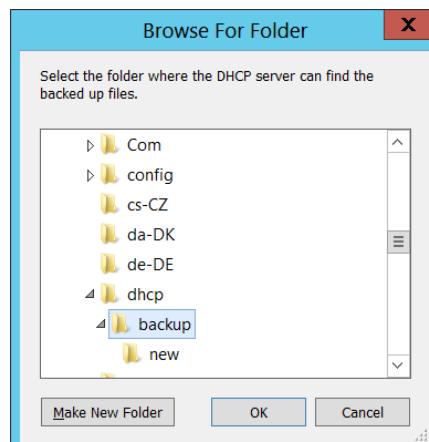
3. **Delete the Existing scope**



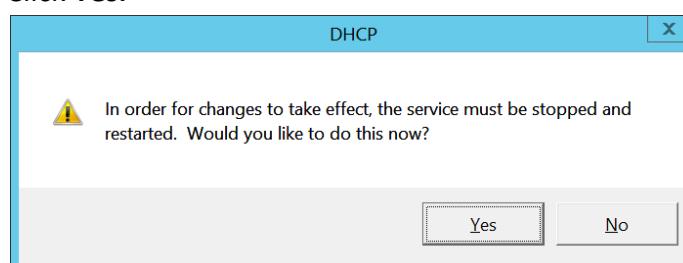
4. In DHCP Console → right click the server name → select **Restore**.



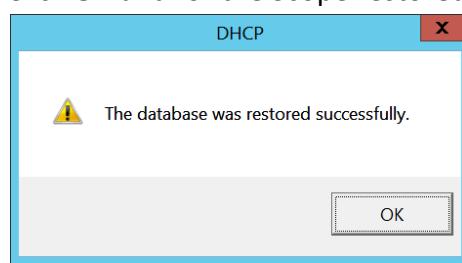
5. Select the location of file for **Restoration**.



6. Click **Yes**.



7. Click **OK** and for the Scope restored in DHCP Console.



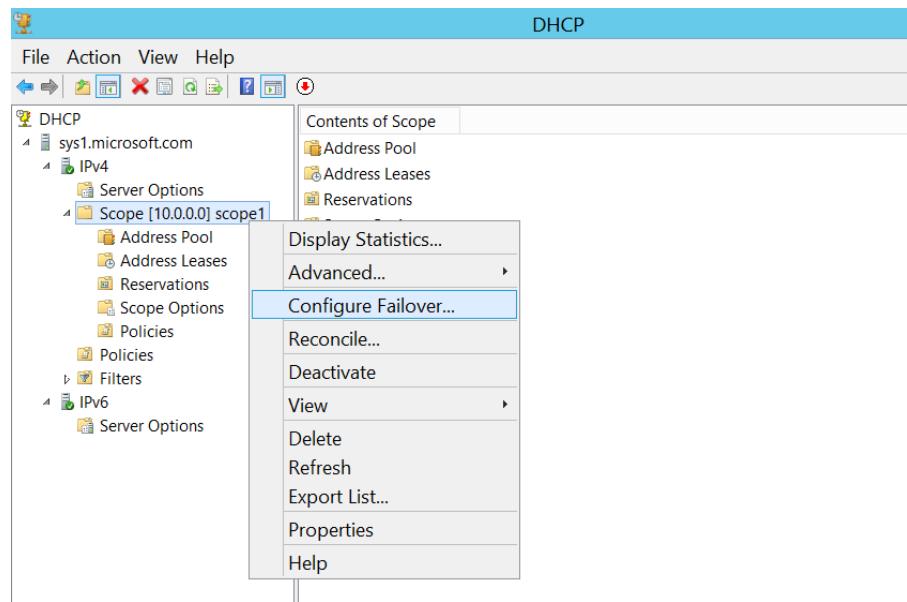
Lab – 5:Configuring DHCP Server Failover

SYS2 - CONFIGURATION

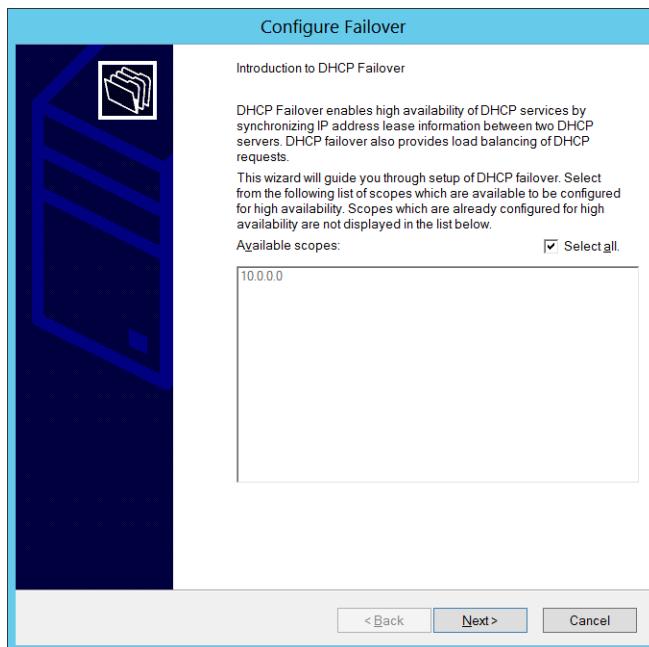
1. Install DHCP Server Role on SYS2 and Do not Authorize the Server.

SYS1 - CONFIGURATION

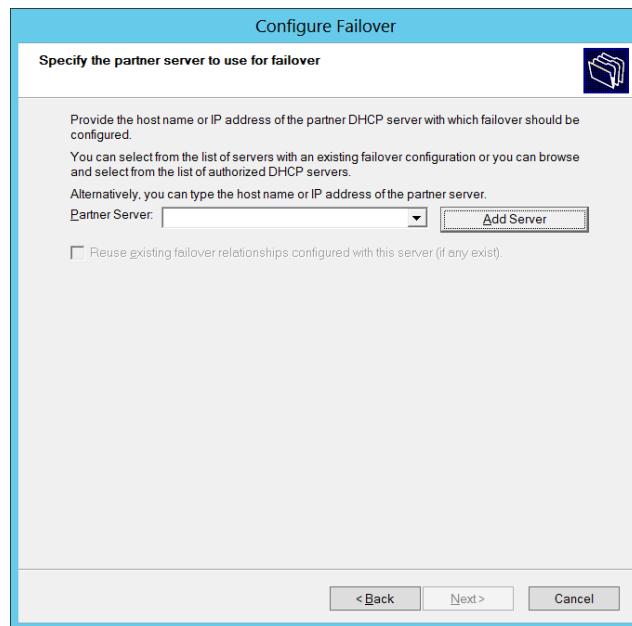
2. Go to DHCP console → In left pane, expand Server name → Expand IPv4 → right click Scope → select **Configure Failover**



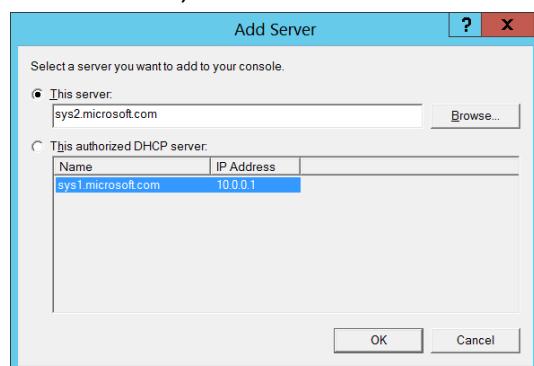
3. In Introduction to DHCP Failover wizard, click **Next**.



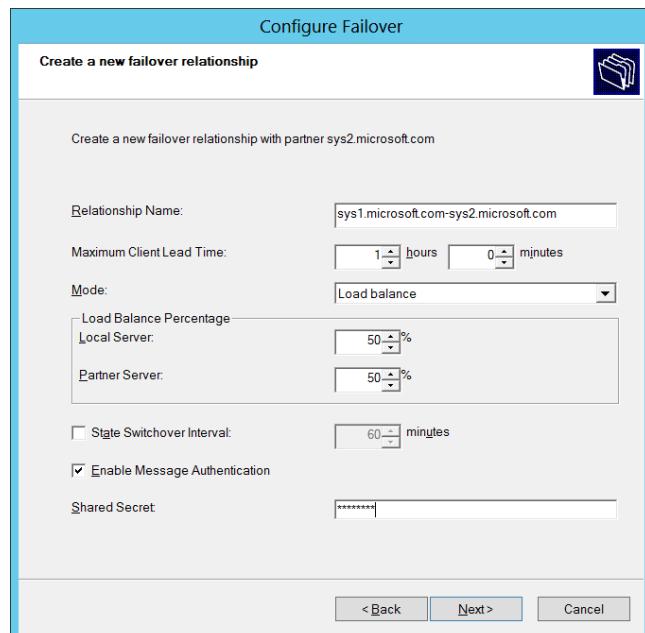
4. Click **Add Server** to add the Failover Server.



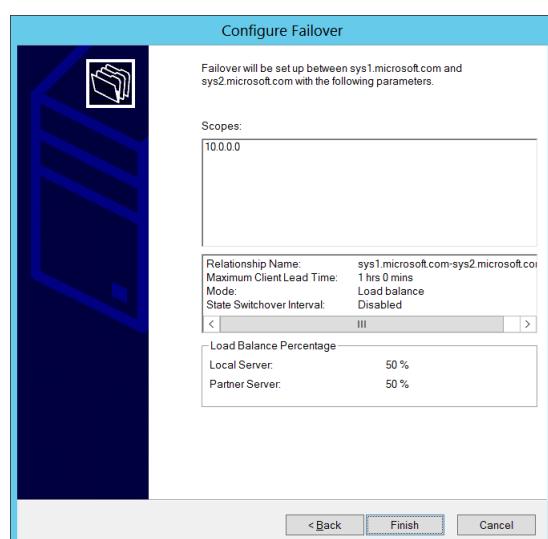
5. In Add Server, Browse and Select the server (**sys2.microsoft.com**), click **OK**.



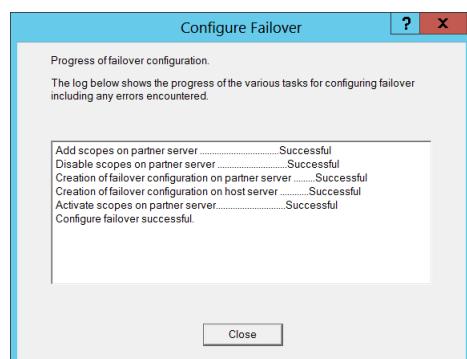
6. Select the Mode, **Enable Message Authentication** and enter Shared Secret, **Next**.



7. To Complete the Failover, click **Finish**.

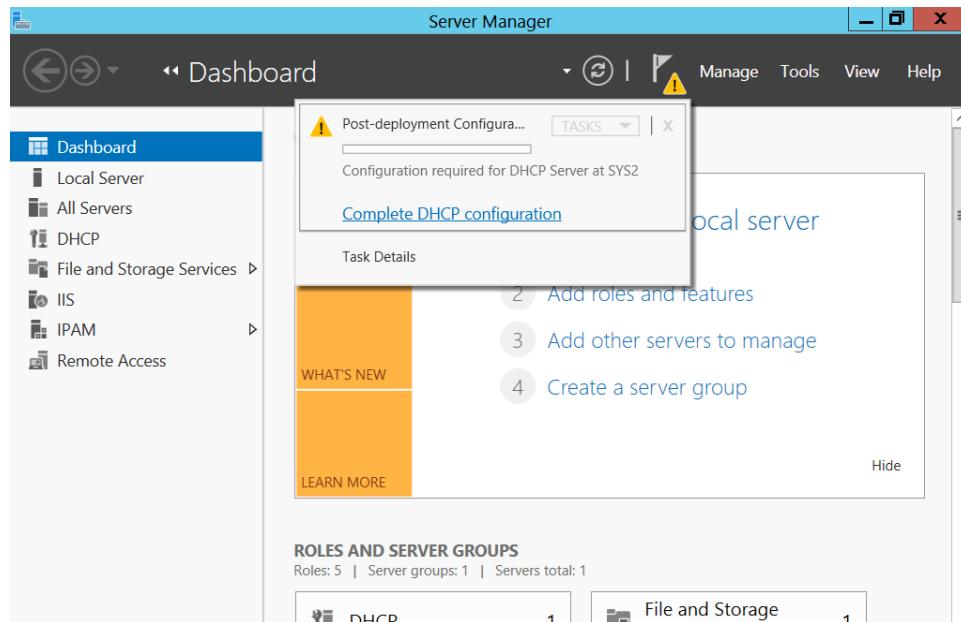


8. Verify the Summary to be **Successful**.

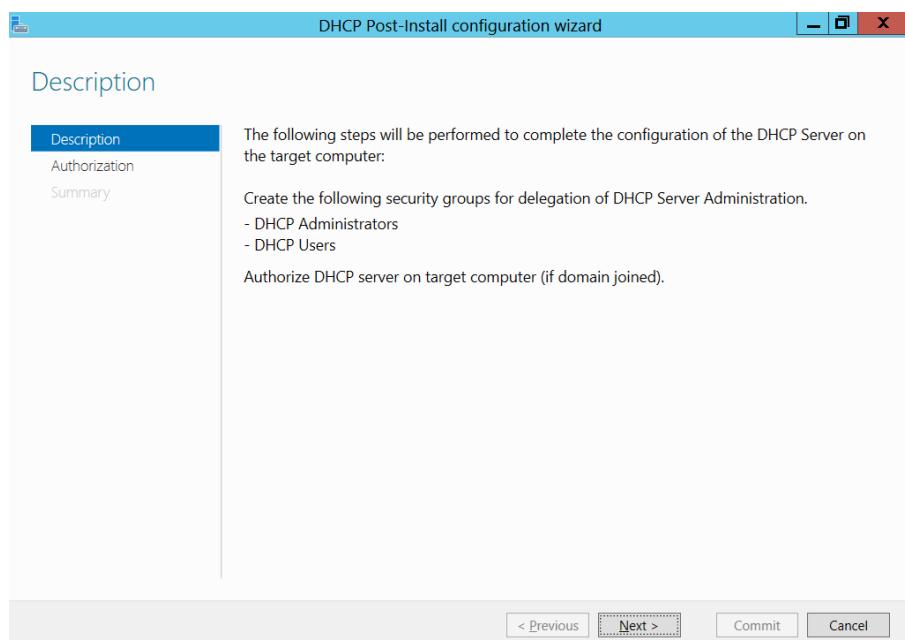


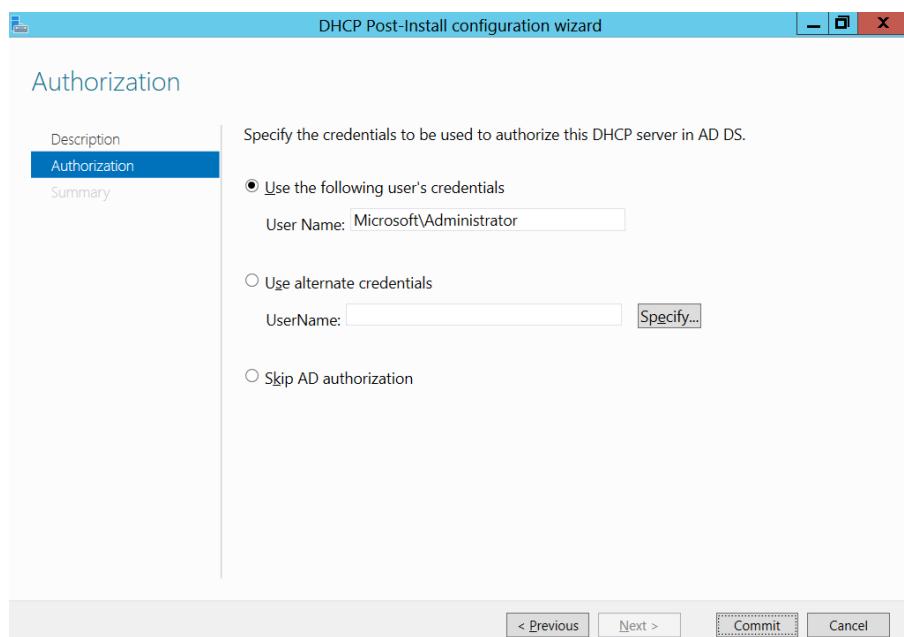
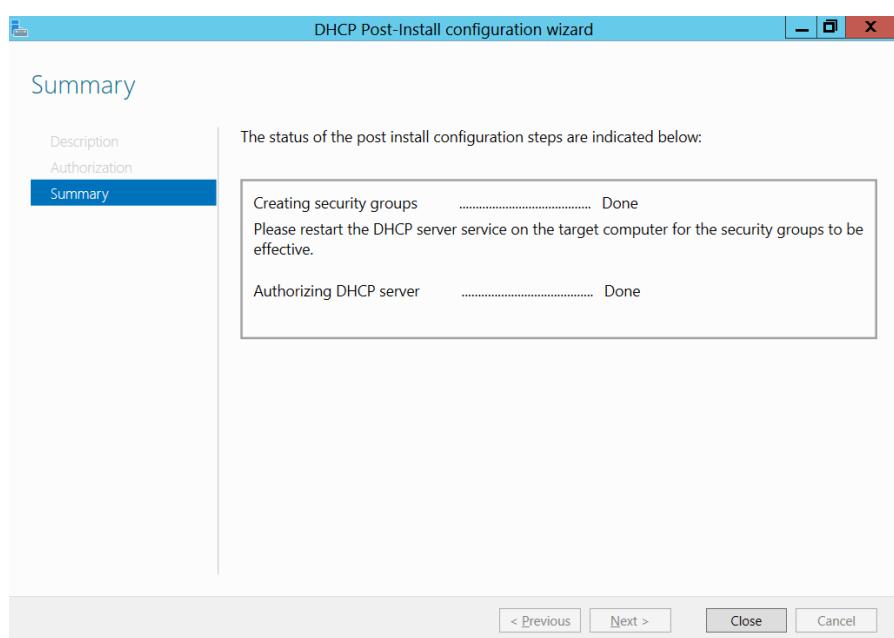
SYS2 - CONFIGURATION

1. Go to Server Manager Dashboard, select notification flag, **Complete DHCP Configuration.**



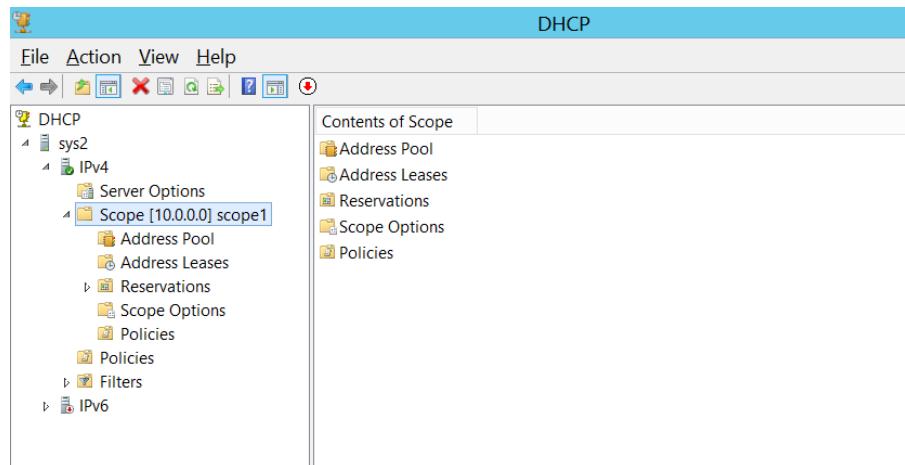
2. In DHCP Post-Install configuration wizard, click **Next**.



3. Click **Commit**, to Authorize the DHCP server **sys2.microsoft.com**4. Verify the summary and click **Close**.

Verification:

1. Go to DHCP console and verify the scope replicated from sys1

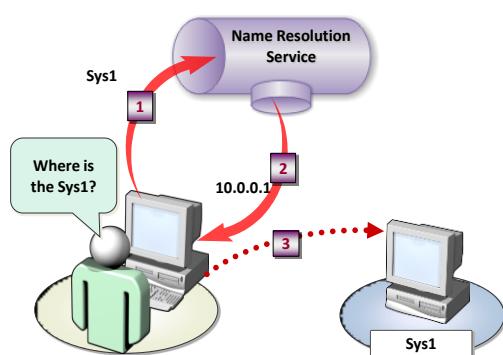


DOMAIN NAMING SYSTEM

What is DNS

- Domain Name Service/Domain Name System
- Provides resolution of names to IP addresses and resolution of IP addresses to names
- Defines a hierarchical namespace where each level of the namespace is separated by a “.”

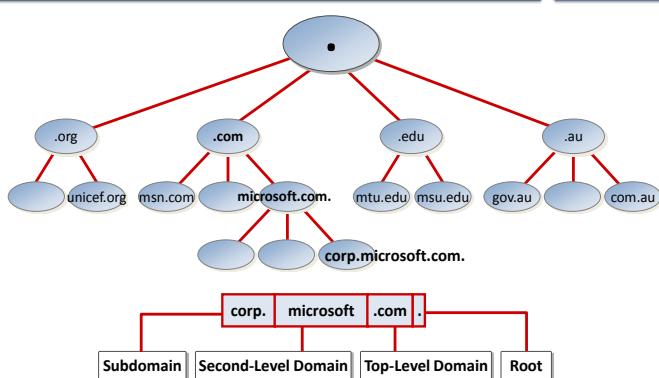
How names are mapped to IP Addresses



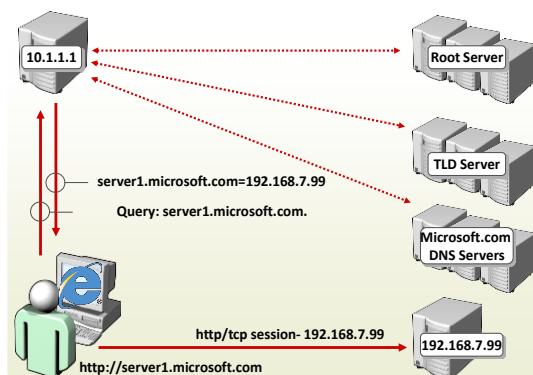
DNS

- Computer running DNS service can be:
 - Microsoft® Windows® Server 2012
 - Microsoft® Windows® Server 2008
 - Microsoft® Windows® Server 2003
 - Microsoft® Windows® 2000 Server
 - Microsoft® Windows® NT 4
 - UNIX
 - Linux
 - NetWare Etc.

DNS Namespace



How DNS Queries Works



Authoritative & Non-authoritative DNS server

- **An authoritative DNS server will either:**
 - Return the requested IP address
 - Return an authoritative “No”
- **An Non-authoritative DNS server will either:**
 - Check its cache
 - Use forwarders
 - Use root hints

Fully Qualified Domain Name (FQDN)

- Identifies a host's name within the DNS namespace hierarchy
- Host name + DNS domain name = FQDN
- Example:
 - Host name: Sys1 & Domain name: MS.com
 - Then FQDN = Sys1.MS.com

Lookup Types

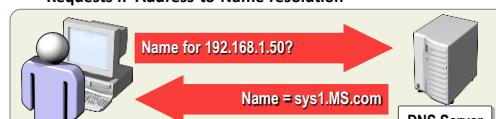
- **Forward Lookup**

– Requests Name-to-IP Address resolution



- **Reverse Lookup**

– Requests IP Address-to-Name resolution



ZONE

Zone is a storage database which contains all zone Records

- **Forward Lookup Zone**
 - Used for Resolving Host Names to IP-Address
 - It maintains Host to IP Address Mapping Information
- **Reverse Lookup Zone**
 - Used for Resolving IP-Address to Host Names
 - It maintains IP Address to Host Mapping Information

Types of Records

- **SOA Record**
 - The first record in any zone file
- **N S Record**
 - Identifies the DNS server for each zone
- **Host Record**
 - Resolves a host name to an IP address
- **Alias Record**
 - Resolves an alias name to a host name

Types of Records

- **Pointer Record**
 - Resolves an IP address to a host name
- **MX Record**
 - Used by the mail server
- **SRV Records (Service Records)**
 - Resolves names of servers providing services

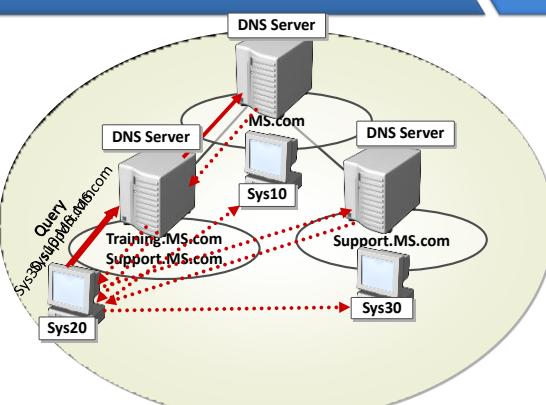
Zone Types

- **Standard Primary**
 - It is the Master Copy of all Zone Information. It is Read/Write copy
- **Standard Secondary**
 - It is Backup to Primary zone. It is Read Only
- **Stub Zone**
 - It contains only NS ,SOA & possibly Glue (A) Records which are used to locate name servers
- **Active Directory Integrated**
 - It stores the information of Zone in ACTIVE DIRECTORY DATABASE

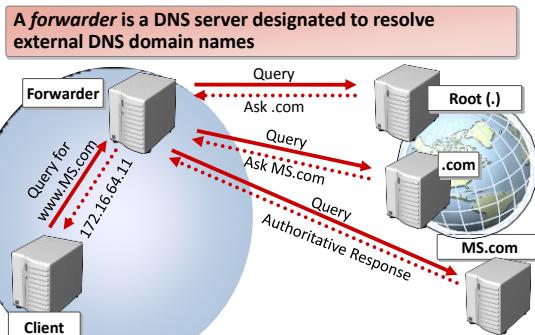
What are Service Records

- SRV records allow DNS clients to locate TCP/IP-based Services.
- SRV records are used when:
 - A domain controller needs to replicate
 - A client searches Active Directory
 - A user attempts to change her password
 - An administrator modifies Active Directory

How Stub Zone works

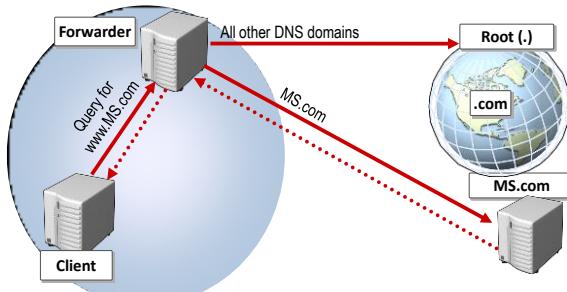


How Forwarders works



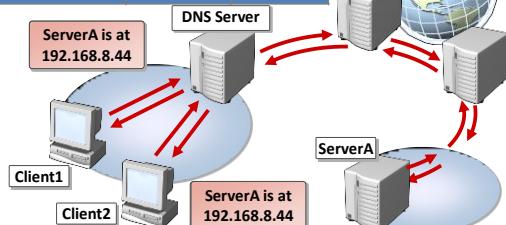
How Conditional Forwarders works

Conditional forwarding forwards requests using a domain name condition



How DNS Server Caching Works

DNS server cache		
Host name	IP address	TTL
ServerA.MS.com	192.168.8.44	28 seconds

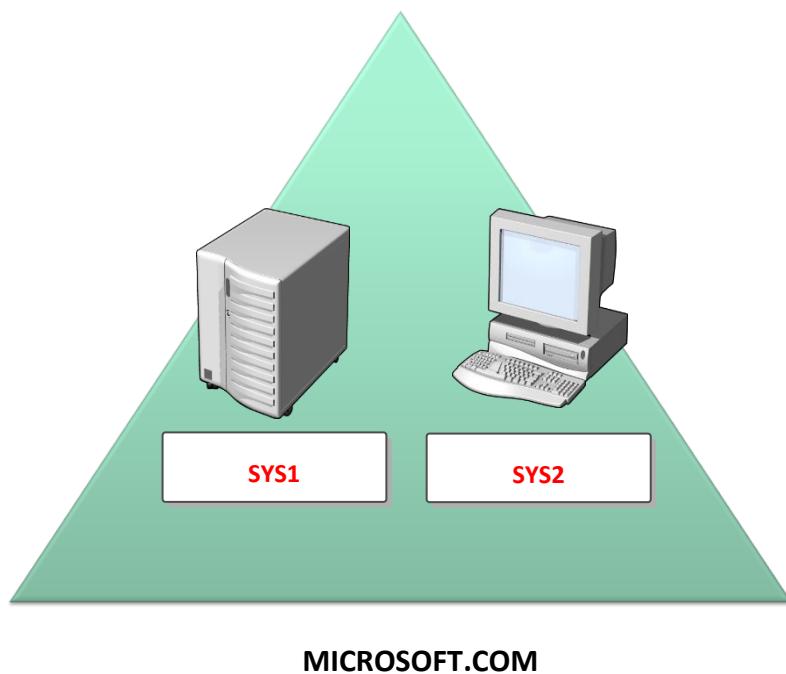


DOMAIN NAMING SYSTEM (DNS)

Prerequisites:

Before working on this lab, you must have

1. A computer running windows 2012 server or Domain Controller.
2. A computer running windows 2012 server.



SYS1

Domain Controller / DNS Server

IP Address 10.0.0.1

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

SYS2

Member Server / DNS Server

IP Address 10.0.0.2

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.2

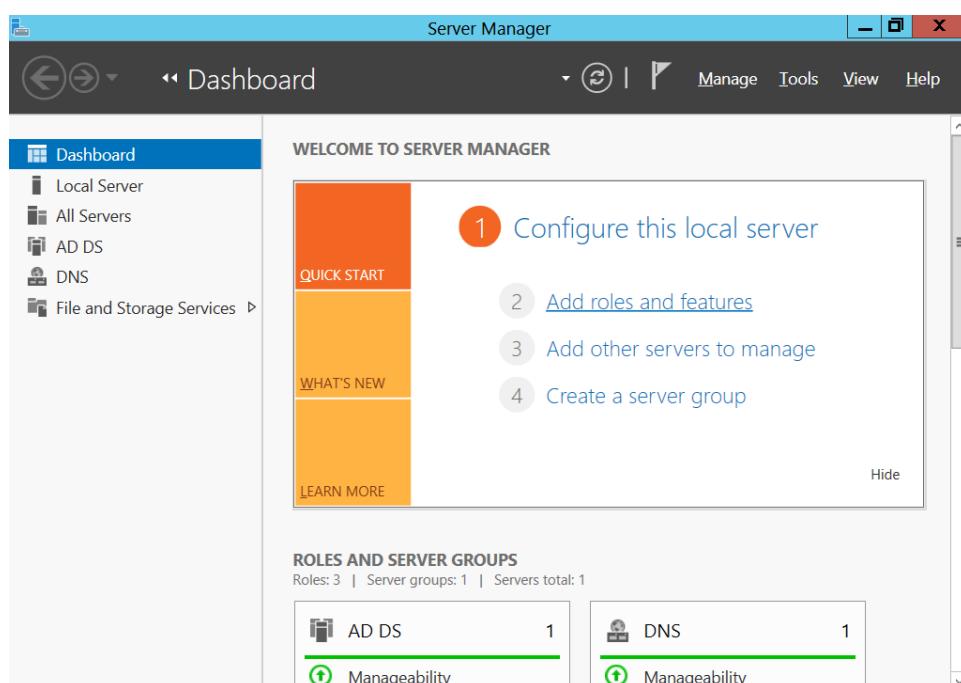
Lab – 1: Installing DNS Service

SYS1 -CONFIGURATION

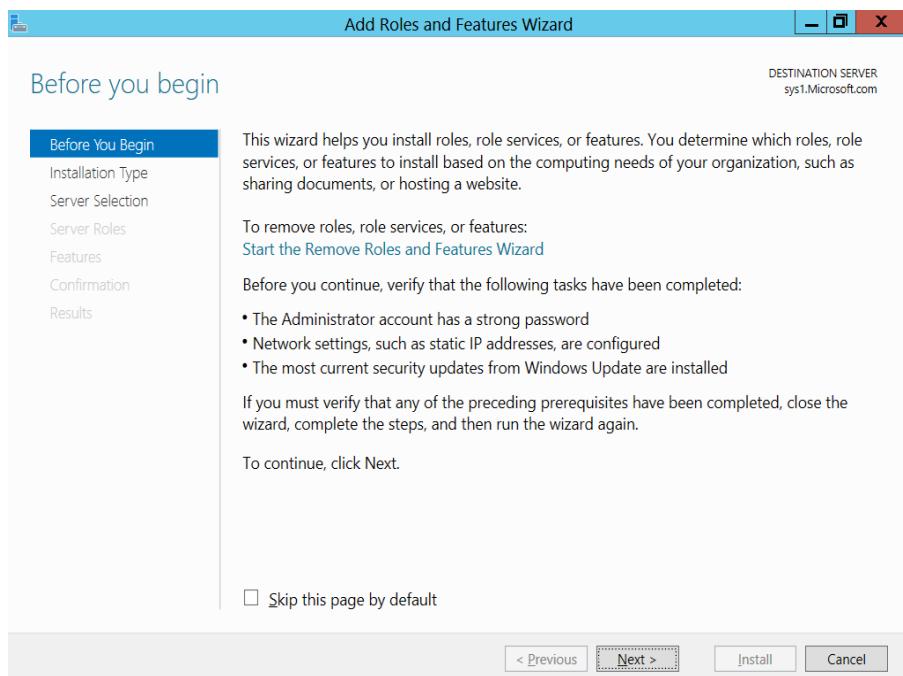
1. Select Click **Server Manager**.



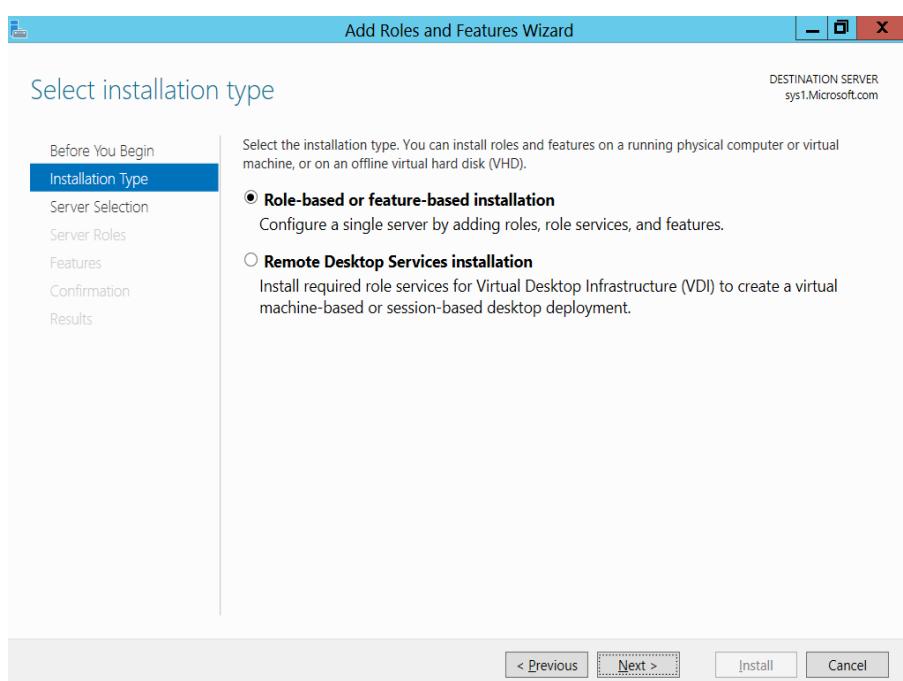
2. In the Server Manager Console, Select **Add roles and features**



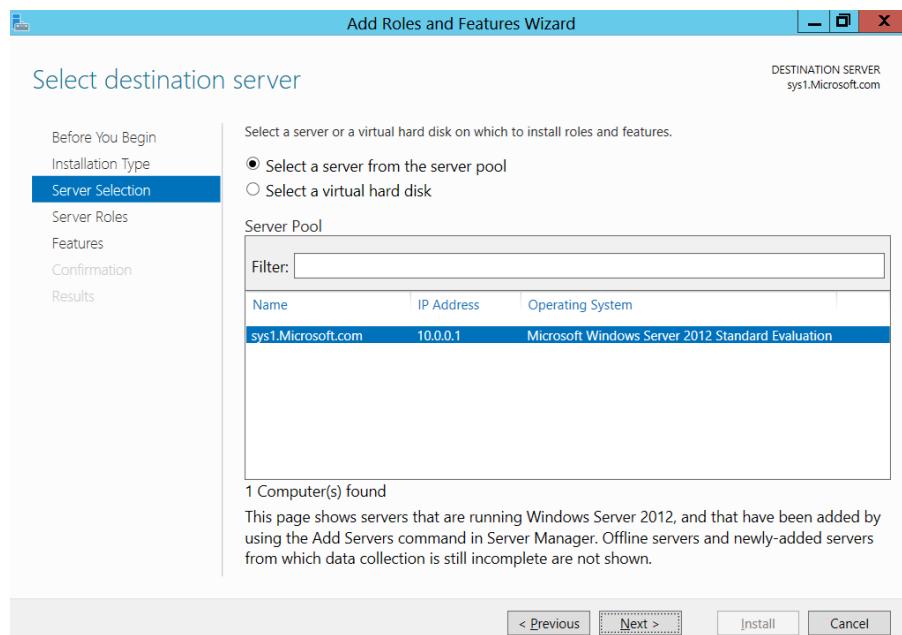
3. In Before you begin page, click **Next**.



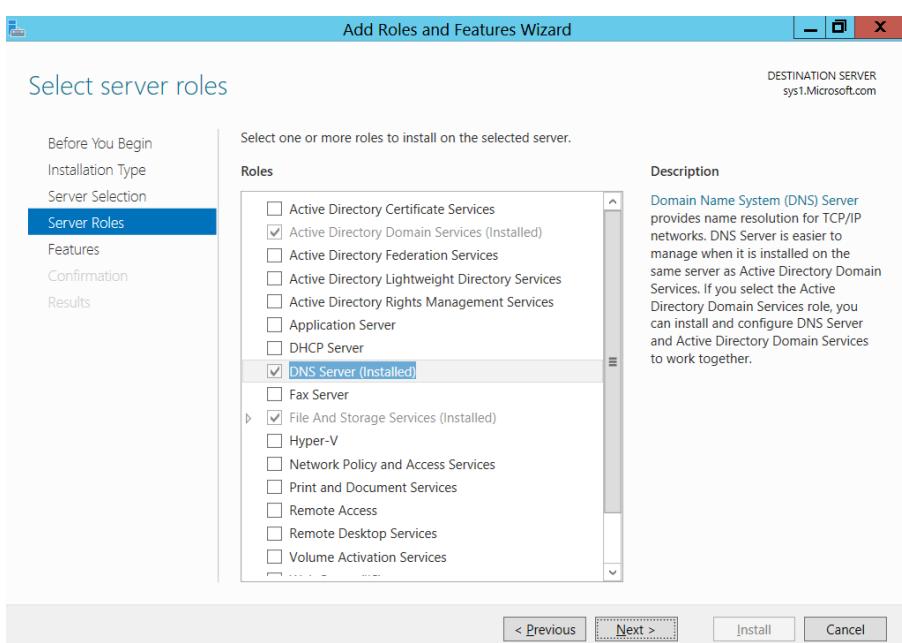
4. Select Role-based or feature-based installation and click **Next**.



- 5. Select a server (**sys1.Microsoft.com**) from the server pool and click **Next**.**



- 6. Check box **DNS Server**, click **Next** → **Next** → **Install** → **Finish**.**

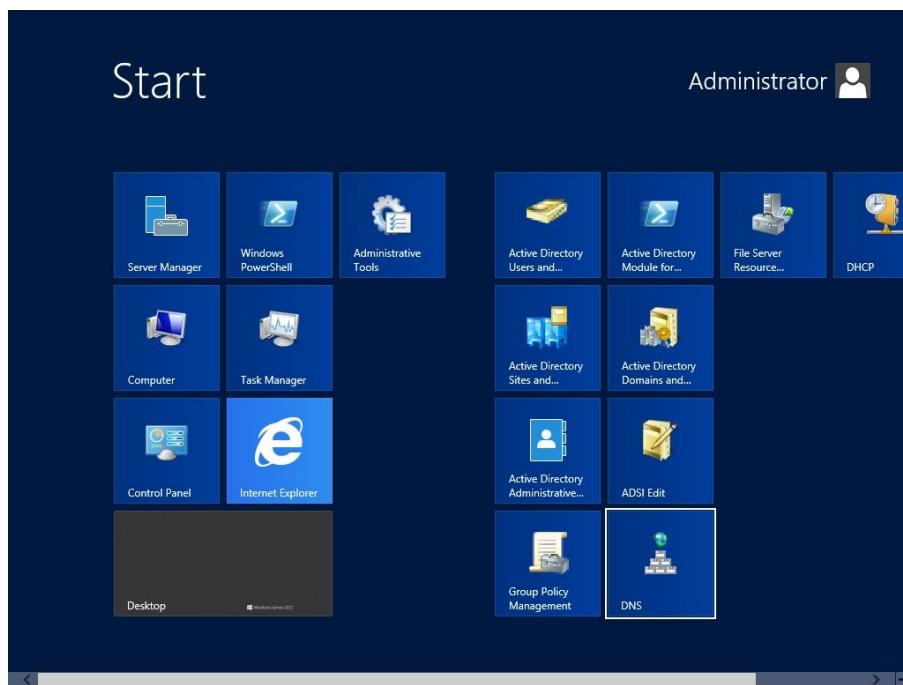


Note: On Domain Controller, by default DNS Server Role will be installed.

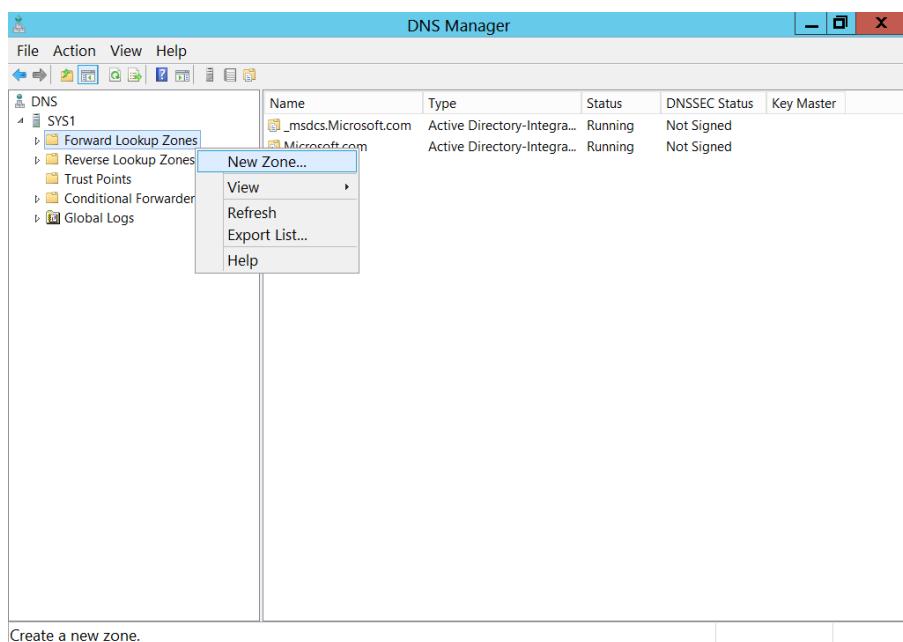
On Member Server we have to install the DNS Server Role Manually using the same process.

Lab – 2: Creating Standard Primary - Forward Lookup Zone

1. Go to Start, select DNS.



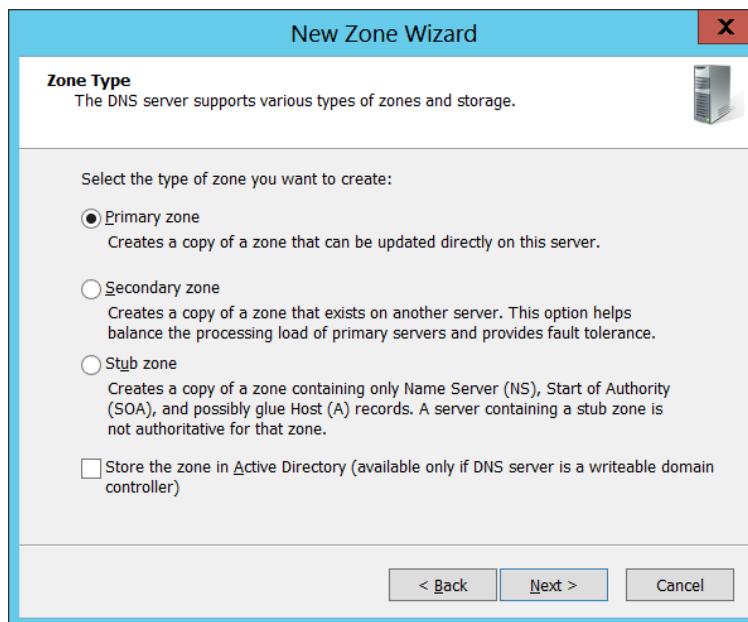
2. In the DNS dialog box, Expand the **DNS→Server name** in the left pane, right click the **Forward Lookup Zones** →select **New Zone**



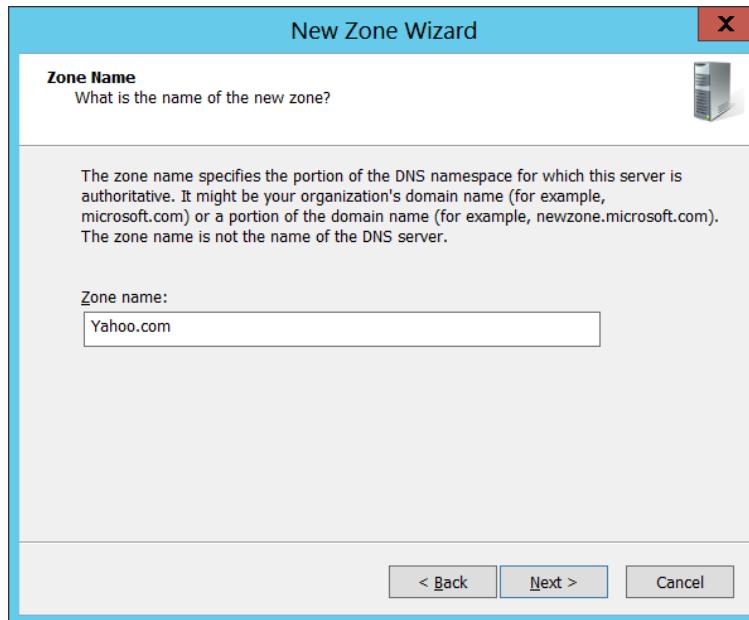
3. In the welcome to new zone wizard click **Next**



4. Select “**Primary Zone**” and Remove the check box for “**Store the zone in Active Directory**”, click **Next**.



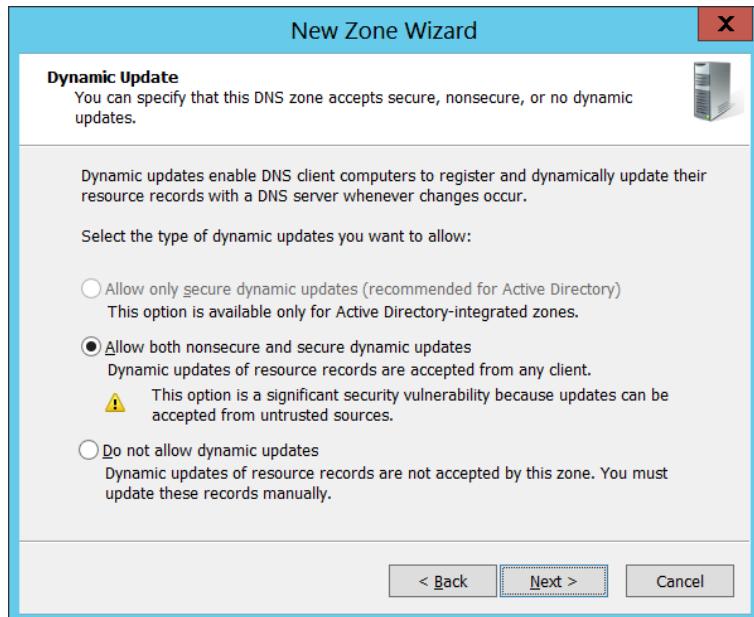
5. In the Zone Name screen, type in the name of the zone you are creating. This name is usually the FQDN of the DNS domain that the zone will contain, such as **YAHOO.COM** → click **Next**.



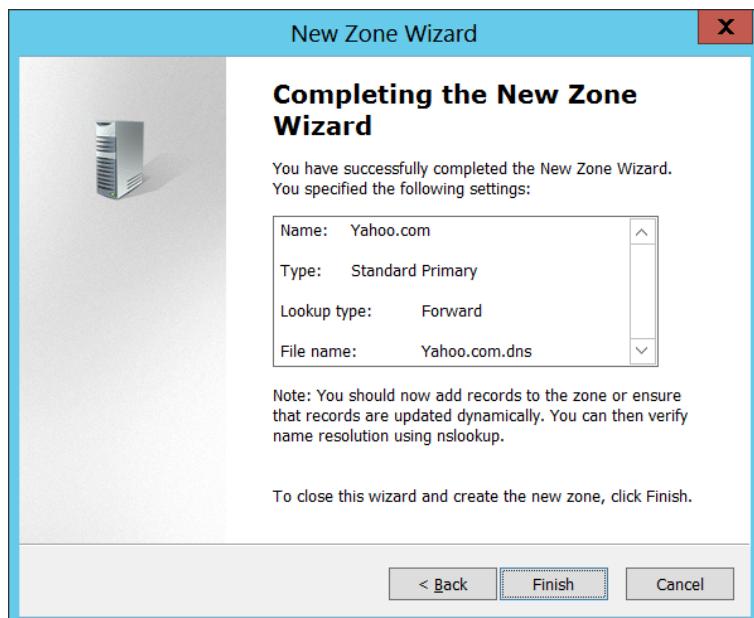
6. The Zone File screen appears. In this screen, you can either create a new zone file for the new zone, or configure the new zone to use an existing file. Click **Next**.



7. In dynamic Update Select "Allow both non-secure and secure dynamic update" → click Next.



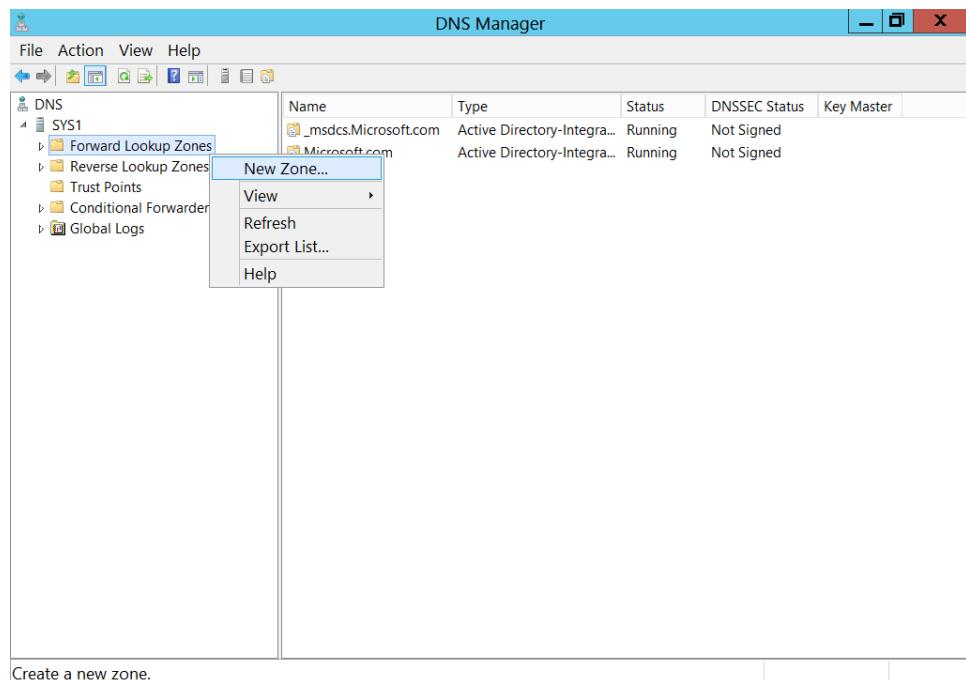
8. The Completing the New Zone Wizard screen appears. Click **Finish**.



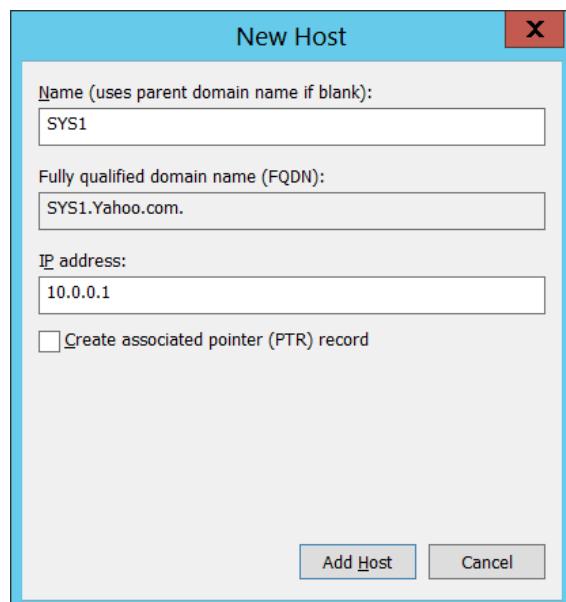
9. In the DNS Console, the new zone you created appears in the right pane.

Creating Host Records for the standard primary zone

1. Go to Start, select **DNS**.
2. Right click the zone and select **New Host**.

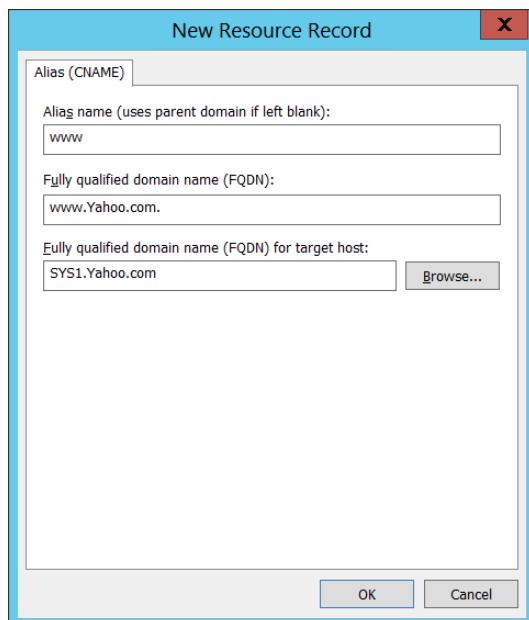


3. Enter the **Host name** for which you are configuring the record Ex: **SYS1**, enter the corresponding **IP address of the host** → click **Add Host** → **OK** → **Done**.



Creating an Alias record for the host record

1. Go to Start, select **DNS**.
2. Right click the zone and select **New Alias**.
3. Enter the name in the '**Alias Name**' dialog box Ex: www
4. Click **Browse** → Double click system name → double click Forward Lookup Zone → double click the zone name → select the host name → click **OK** → **OK**



VERIFICATION:

1. Open **Command Prompt** → type **ping FQDN** (Fully Qualified Domain Name)
Ex: Ping SYS1.YAHOO.COM (or) Ping WWW.YAHOO.COM
2. Name should be resolved into IP Address.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping www.yahoo.com

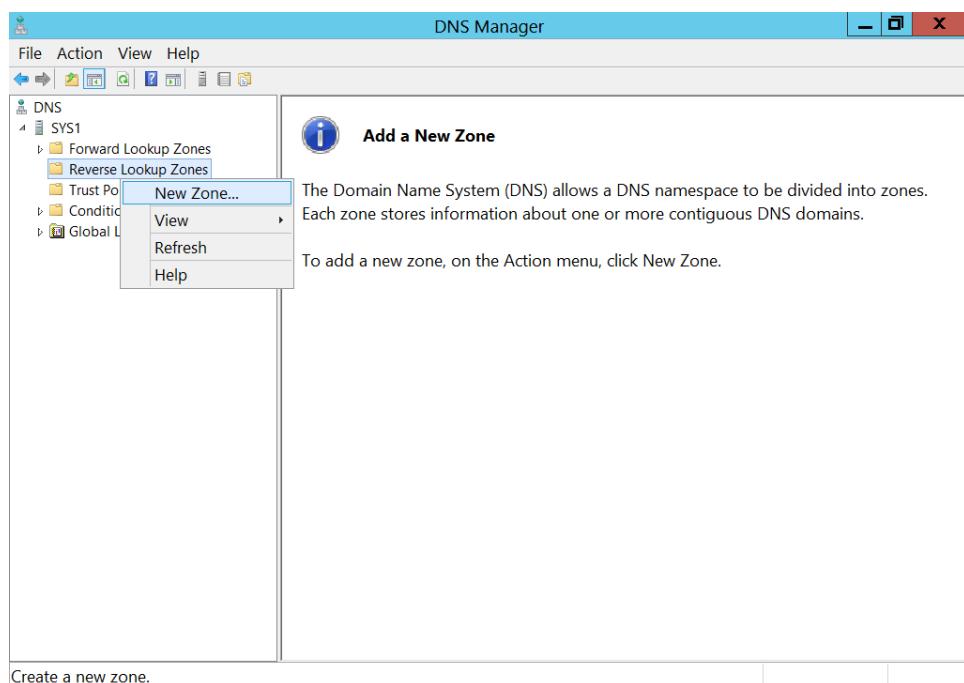
Pinging sys1.yahoo.com [10.0.0.1] with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    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>
```

Lab – 3: Creating Standard Primary - Reverse Lookup Zone

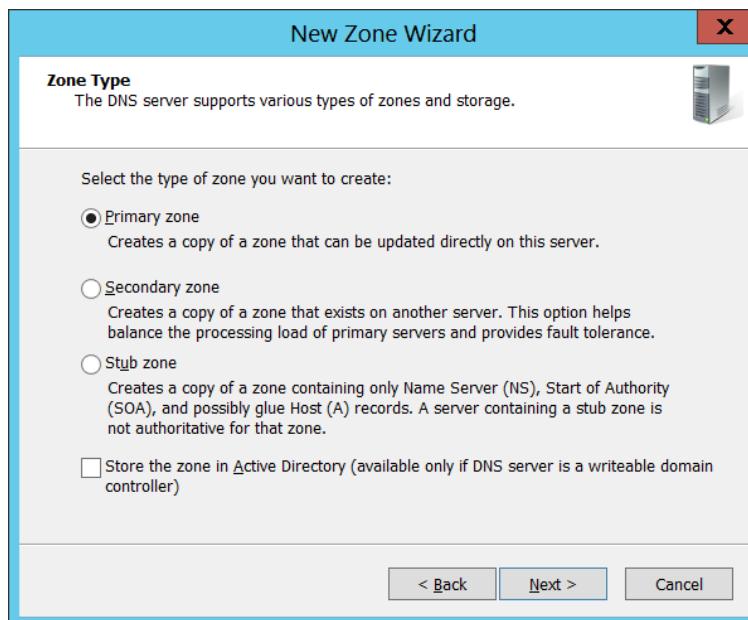
1. Go to Start, select **DNS**.
2. In the DNS dialog box, expand the **DNS server's name** in the left pane → right click the **Reverse Lookup Zones** → Select **New Zone**.



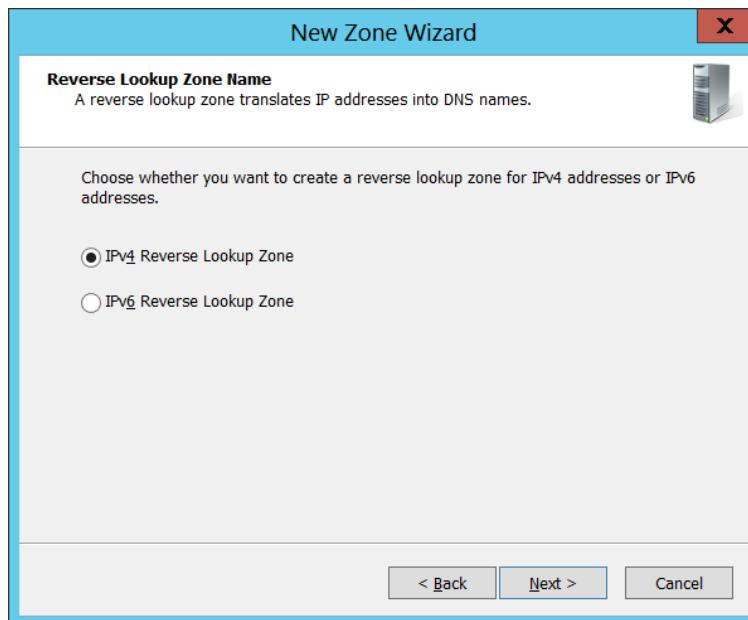
3. Click **Next**



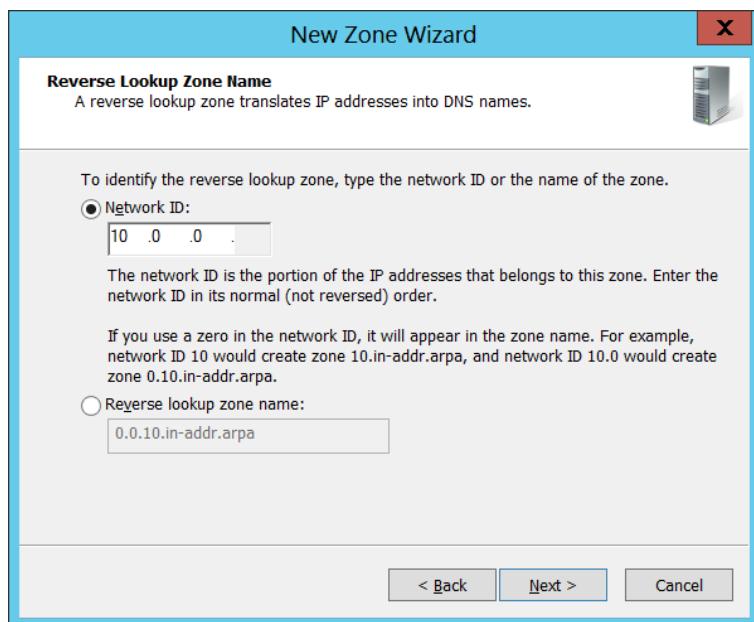
4. Select “Primary Zone” and Remove the check box for "Store the zone in Active Directory", click Next.



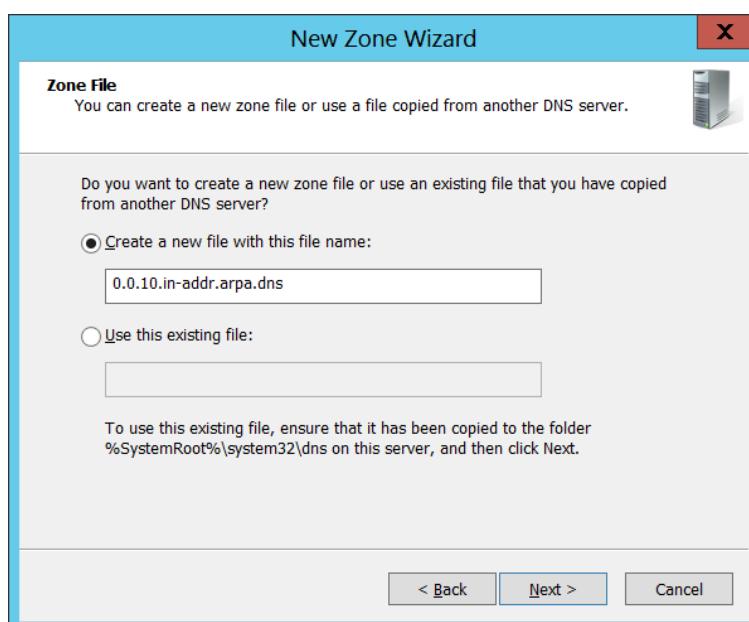
5. Check IPv4 Reverse Lookup Zone



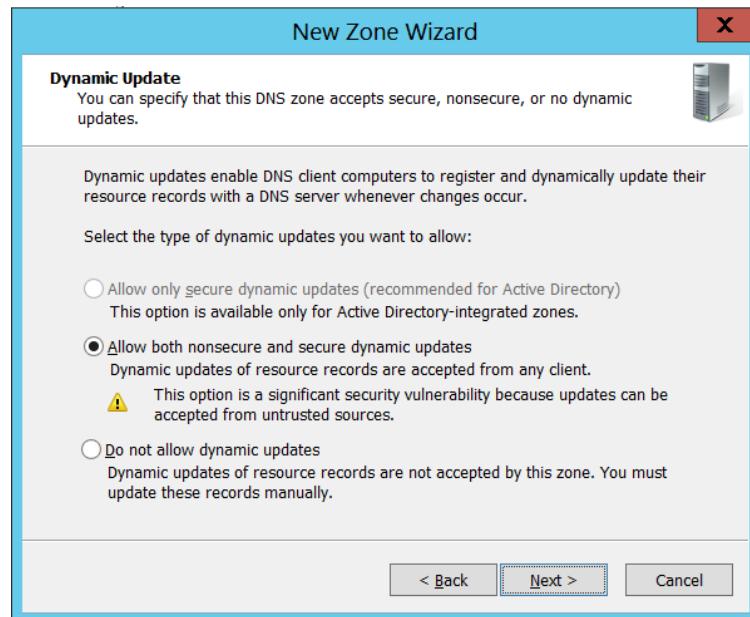
6. In the network ID give the first three octets Ex: 10.0.0 → **Next**



7. Click **Next**

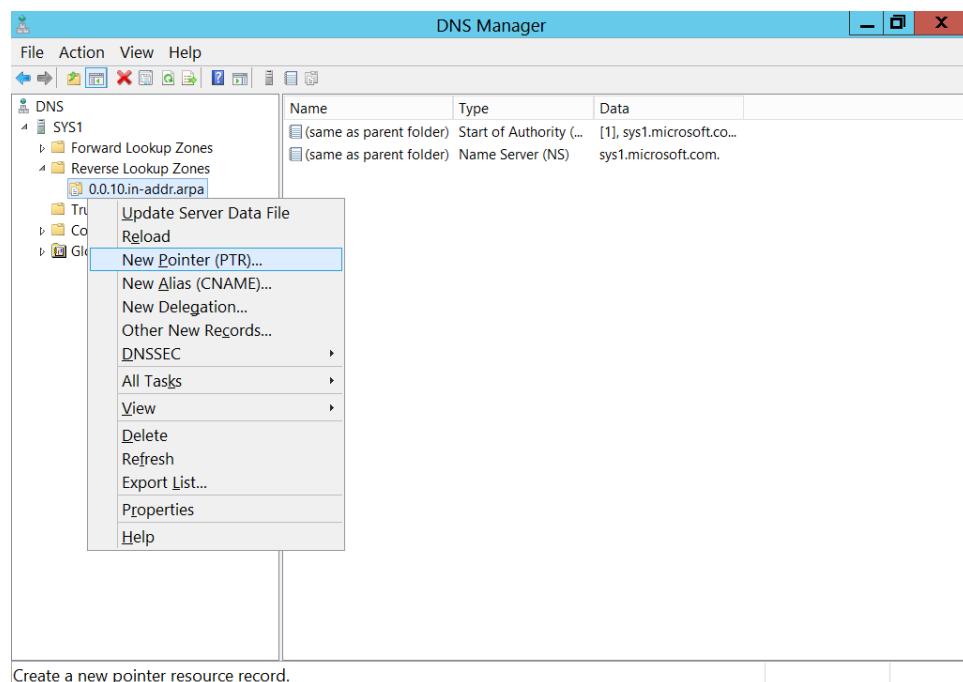


8. In dynamic Update Select "Allow both non-secure and secure dynamic update" → click **Next** → **Finish**

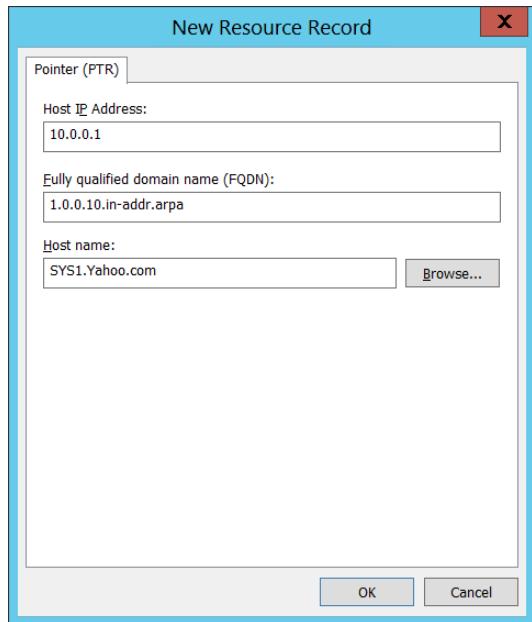


Creating pointer record

1. Go to Start, select **DNS**.
2. Expand Reverse lookup zone and Right click the zone → select **New Pointer**



3. In the pointer record give the fourth octet → click browse → double click server name (SYS1) → double click Forward Lookup Zone → double click the zone name(Yahoo.com) → double click the host name (SYS1) → OK



Verification:

1. Open the command prompt and type **nslookup 10.0.0.1**

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup 10.0.0.1
Server: sys1.yahoo.com
Address: 10.0.0.1

Name: sys1.yahoo.com
Address: 10.0.0.1

C:\Users\Administrator>
```

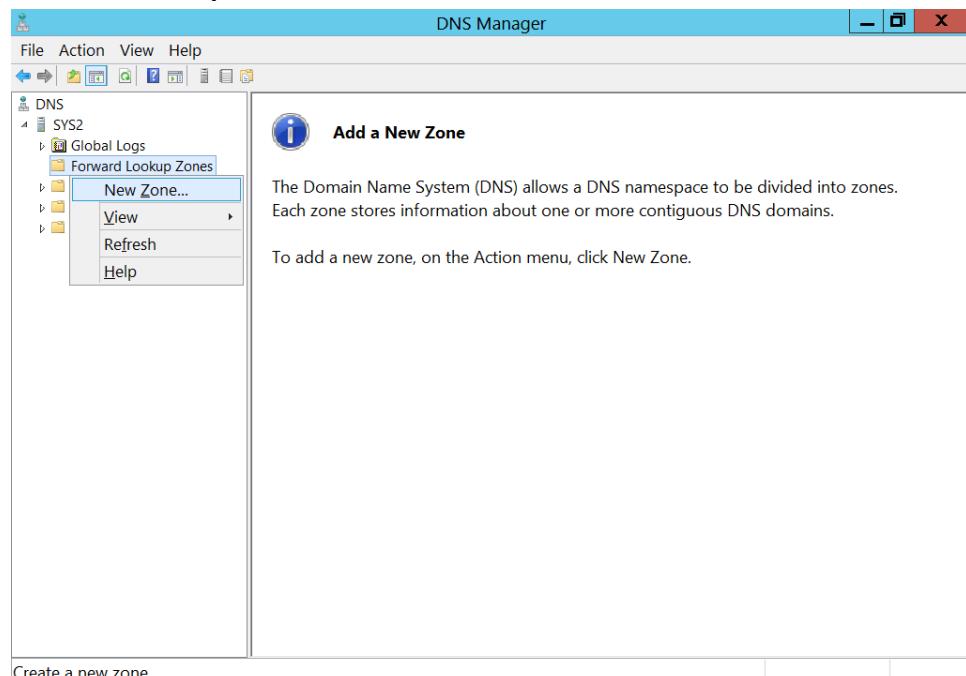
Lab – 4: Creating secondary zone

SYS1 - CONFIGURATION

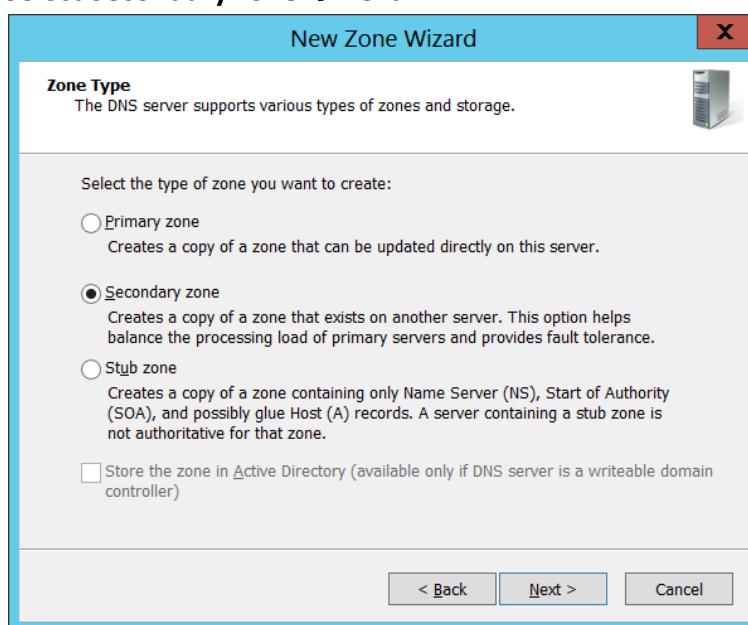
1. In **SYS1** one primary zone should be present. E.g.: Yahoo.com

SYS2 - CONFIGURATION

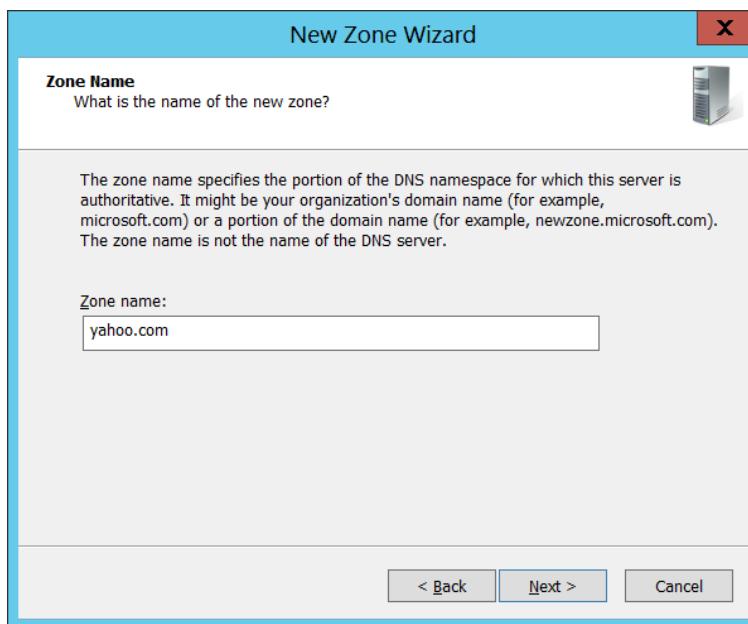
2. Go to Start, select **DNS**.
3. In the DNS dialog box, expand the DNS server's name in the left pane. Right click **Forward Lookup Zones** → select **New Zone** → **Next**



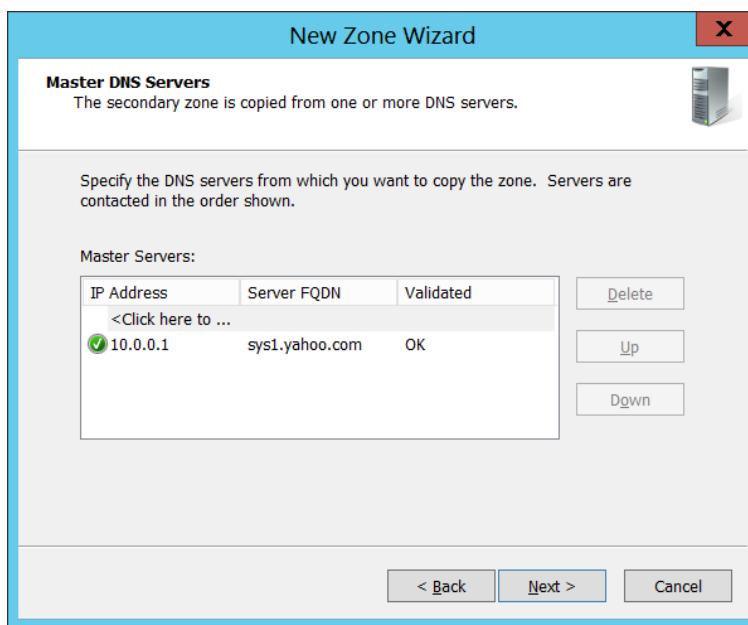
4. Select **Secondary zone** → **Next**.



5. Give the name of **primary zone** → click **Next**.



6. Give the **IP address of primary zone** Ex: 10.0.0.1 → click **Next**.



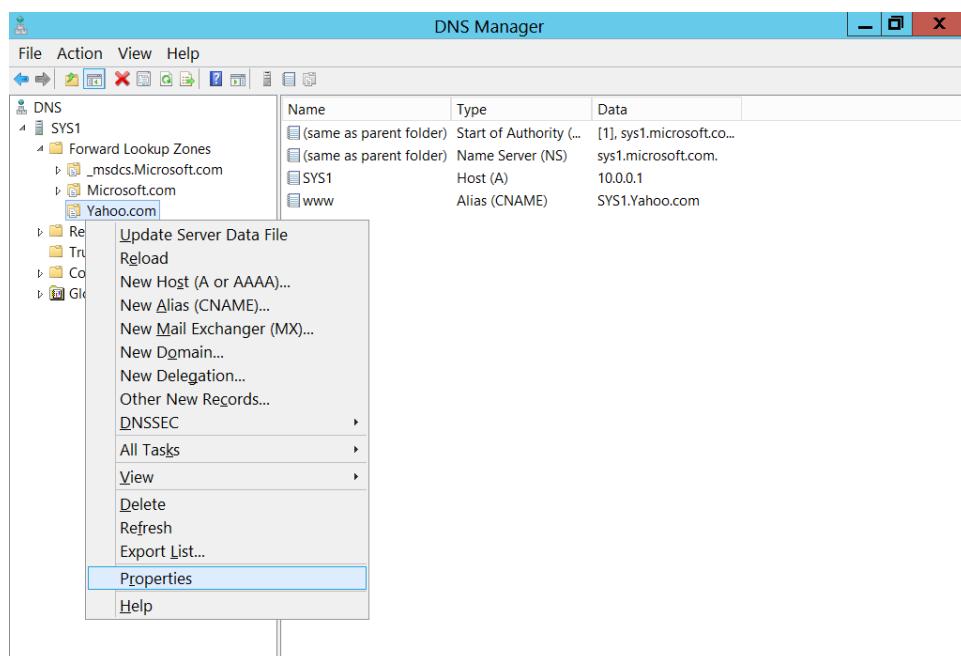
7. Click **Next →Finish**.



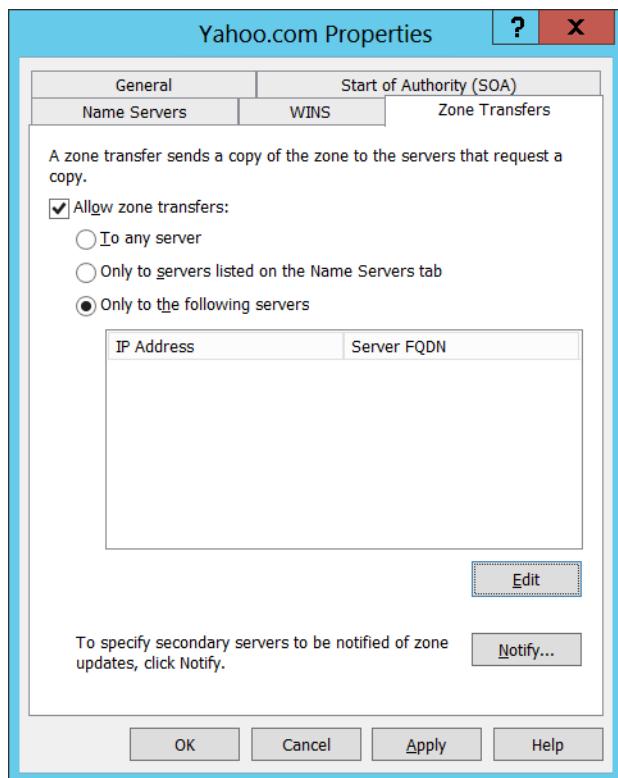
Allow zone transfers to secondary zone

SYS1-CONFIGURATION

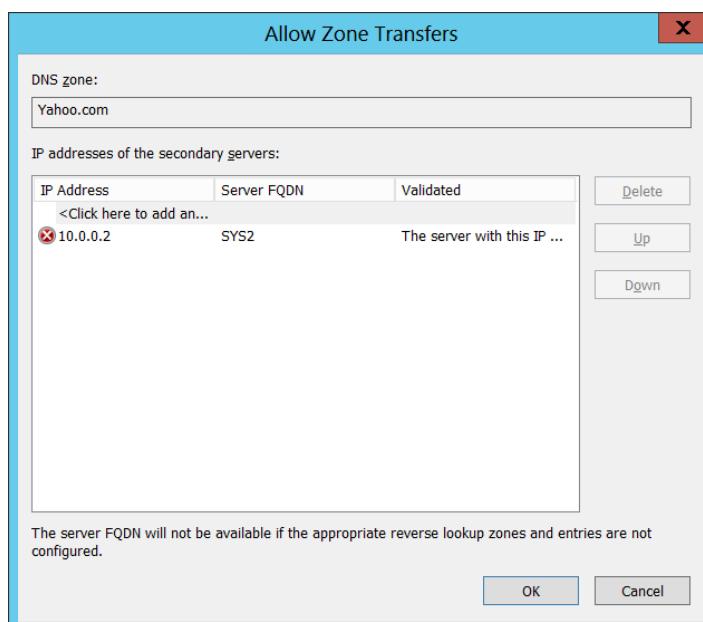
1. Go to Start, select **DNS**.
2. In the DNS dialog box, expand the DNS server's name in the left pane → Expand **Forward Lookup Zone** → right click **primary zone** → select **Properties**.



3. Select **Zone Transfers** Tab → check the box for **Allow zone transfers** → select **Only to the following servers**.



4. Click **Edit** and mention the **Computer IP Address of secondary zone**. Click **Notify** → Select **to the following servers** → and mention the **Computer IP Address of secondary zone**.



5. Click **Apply** → **OK** → Again Click **Apply** → **OK**.

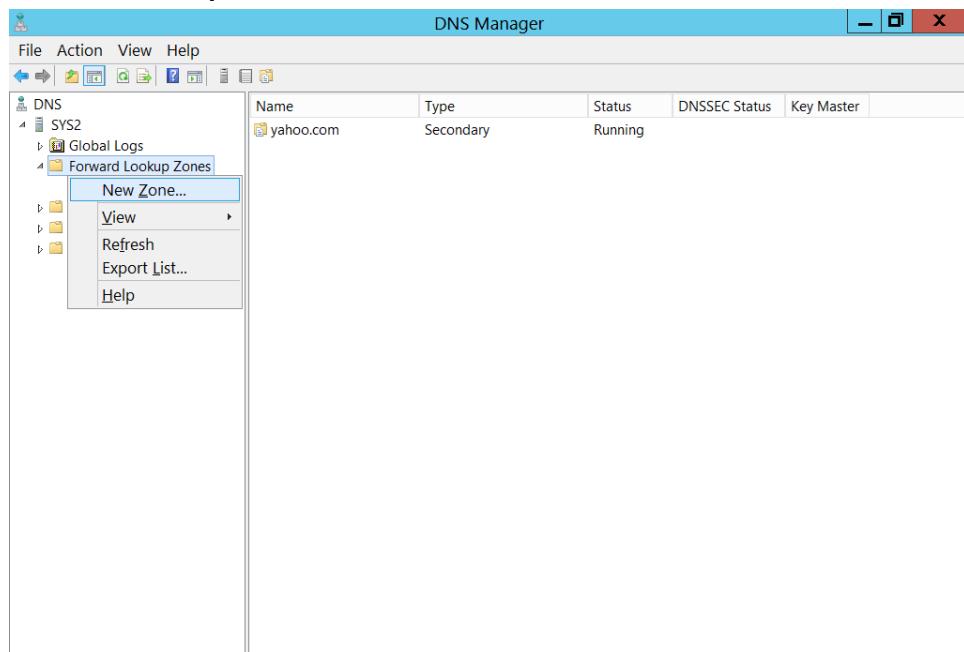
Lab – 5: Creating Stub zone

SYS1-CONFIGURATION

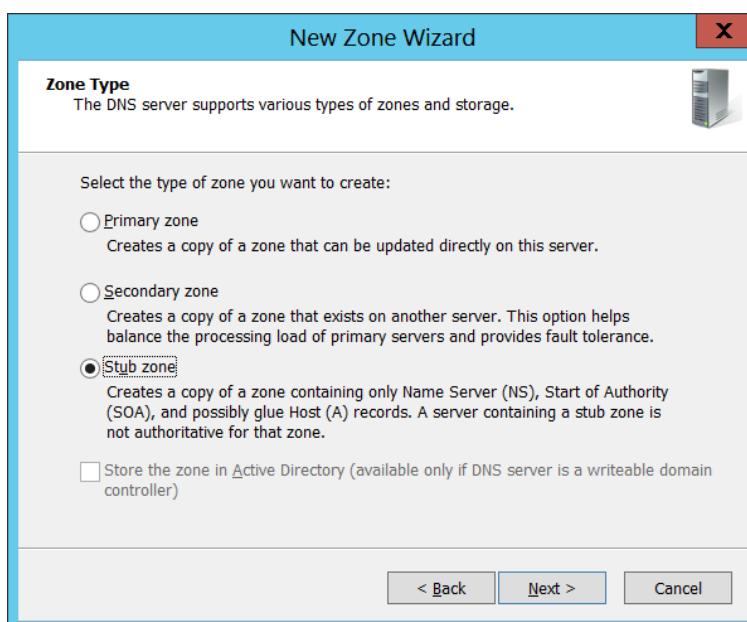
1. Log on to **SYS1** and create a primary zone **Msn.com** along with host and alias records.

SYS2-CONFIGURATION

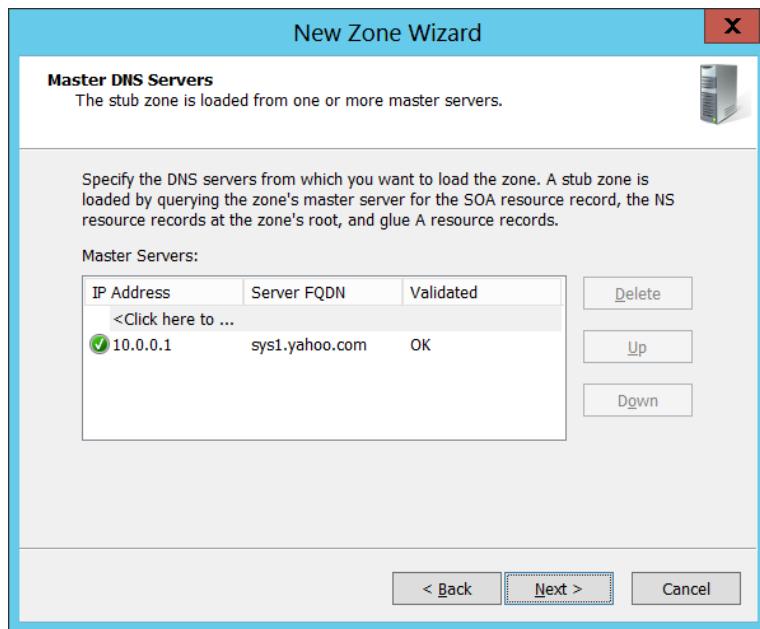
1. Log on to **SYS2** and Go to Start, select **DNS**.
2. In the DNS dialog box, Expand **DNS Server name** in the left pane, right click **Forward Lookup Zones** →Select **New Zone** →Next



4. Select **Stub zone** →Next

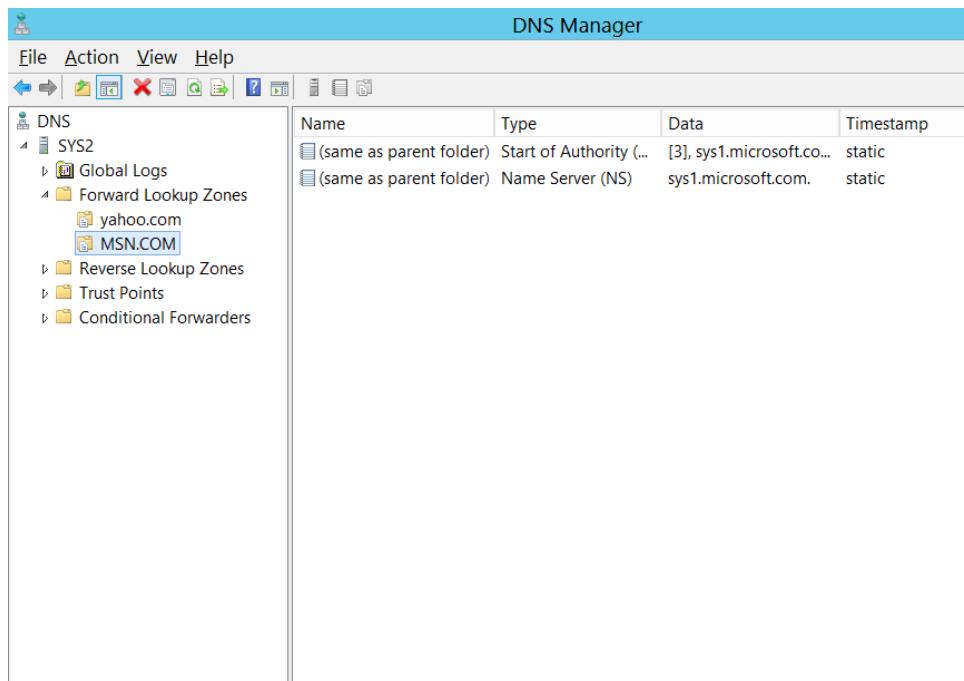


5. Give the name of **primary zone (Msn.com)** →click **Next**.
6. Give the **IP address of primary zone** Ex: 10.0.0.1 →click **Next**.



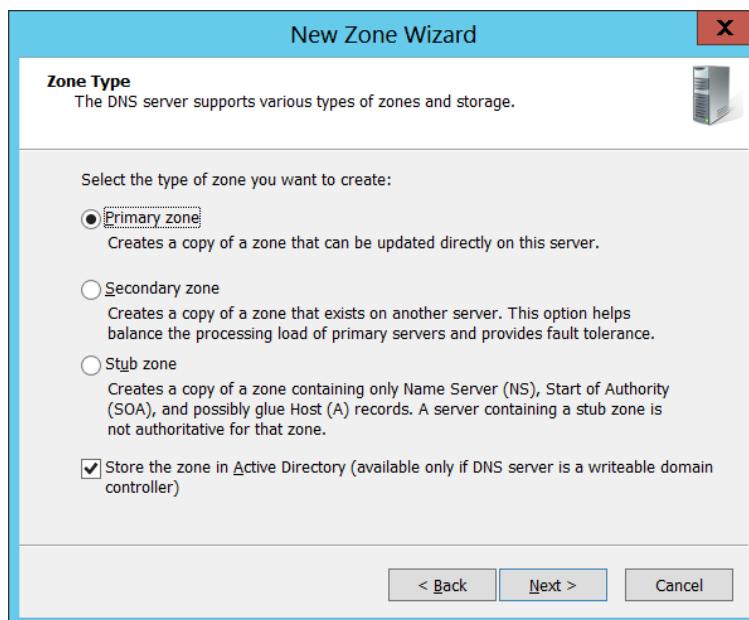
8. Click Next →Finish.

9. Refresh the stub zone and verify for records.

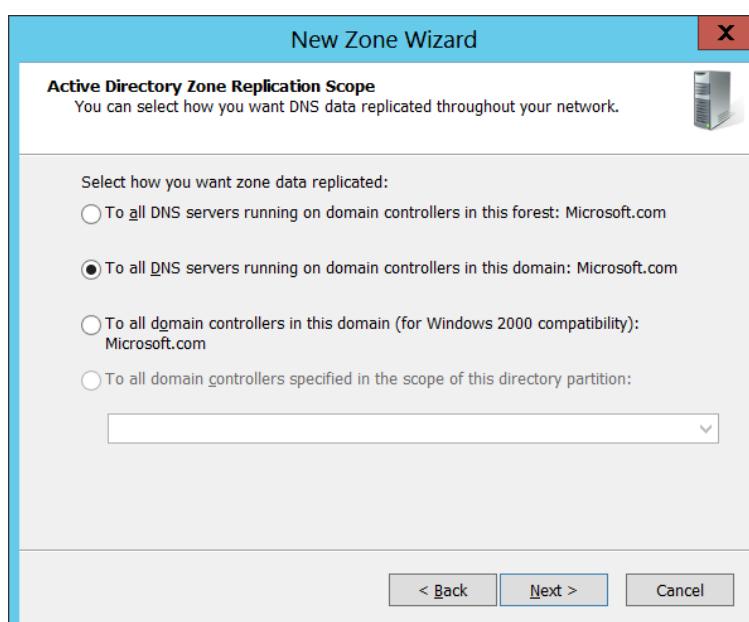


Lab – 6: Creating Active Directory Integrated Primary zone

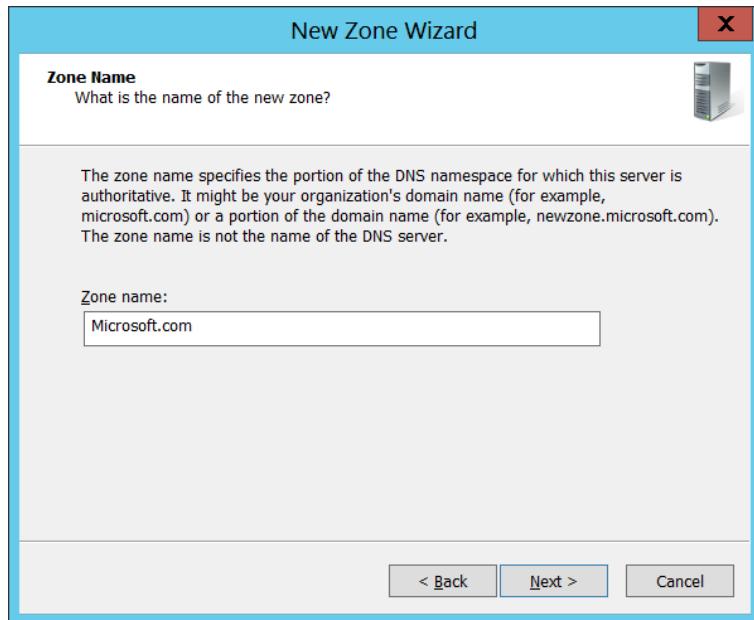
1. Go to Start, select **DNS**.
2. In the DNS dialog box, expand the DNS server's name in the left pane, right click **Forward Lookup Zones** → select **New Zone**
3. Click **Next** → Accept the default option of “**Primary Zone**” and Select the check box for “**Store the zone in Active Directory**” → click **Next**.



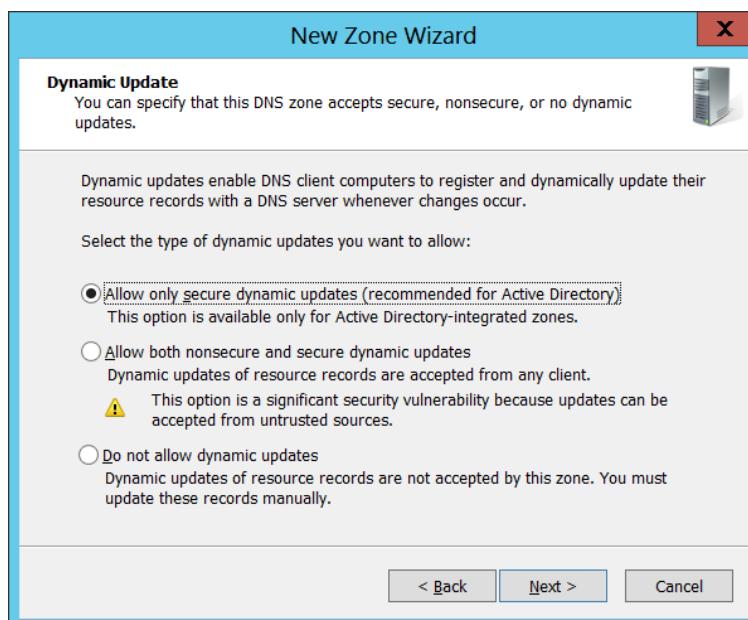
4. In AD Zone Replication Scope, Select the “**To all DNS servers in Active directory domain**”→click **Next**.



5. Give the Zone Name same as the **Domain Name** (Ex: Microsoft.com),click **Next**.



6. Select “Allow only secure and dynamic update” → click Next → Finish.

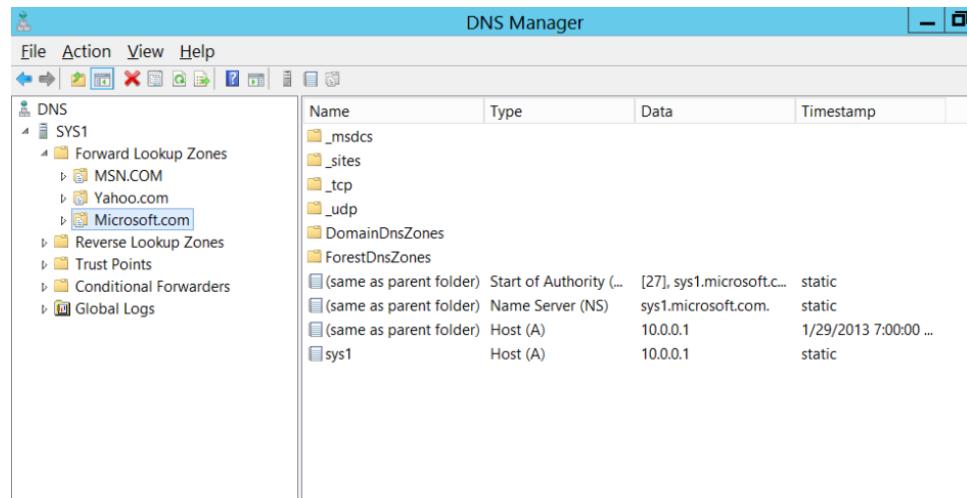


Verification:

- Verify for the Service records in Microsoft.com zone.

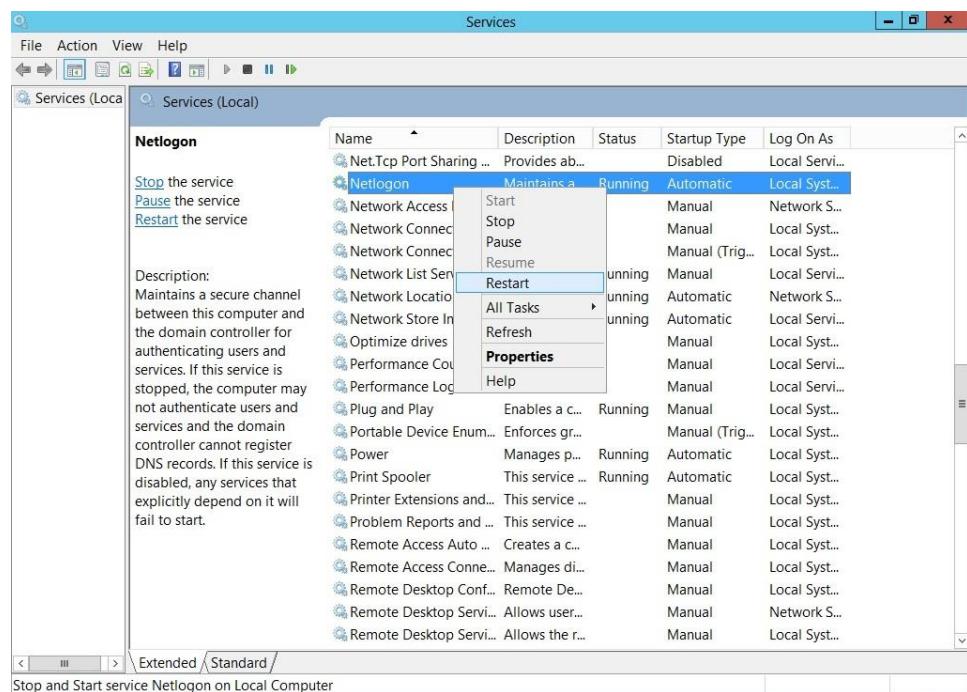
NOTE: Service records are available only for the zone with the domain name.

- In DC by default the service records are created in the DNS server in the zone with domain name.



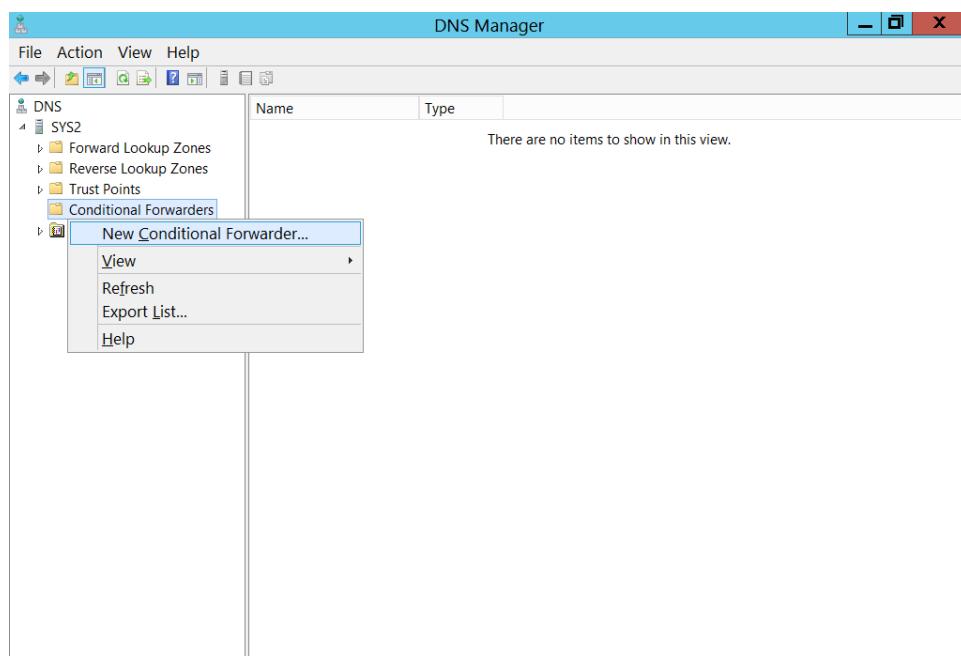
Note: To get the missing records restart the services **Netlogon and DNS Server**.

- Go to Start, type Services in Search Apps, and select Services
- Right click **Netlogon** and click **Restart**, Right click **DNS Server** and click **Restart**.

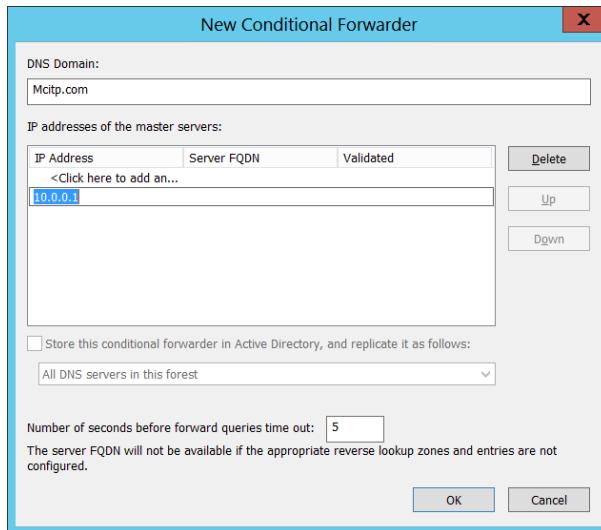


Lab – 7: Conditional Forwarders

1. In **SYS1** create a zone with the name Ex: **MCITP.COM** with host and alias records.
2. In **SYS1** open the command prompt and type ping www.MCITP.COM
3. There will be a reply from 10.0.0.1
4. In **SYS2** assign the **IP Address** and **Preferred DNS** as **10.0.0.2**
5. In **SYS2** open the command prompt and type ping www.MCITP.COM
6. There will not be any reply because the information is in 10.0.0.1
7. If **SYS2** has to resolve the query then configure forwarders in **SYS2** properties.
8. Go to DNS dialog box in **SYS2** → Right click **conditional forwarders** → select **New conditional forwarders**



9. Mention the DNS Domain as **MCITP.COM** and add the IP address of primary zone.



10. In **SYS2** open the command prompt and type ping www.MCITP.COM

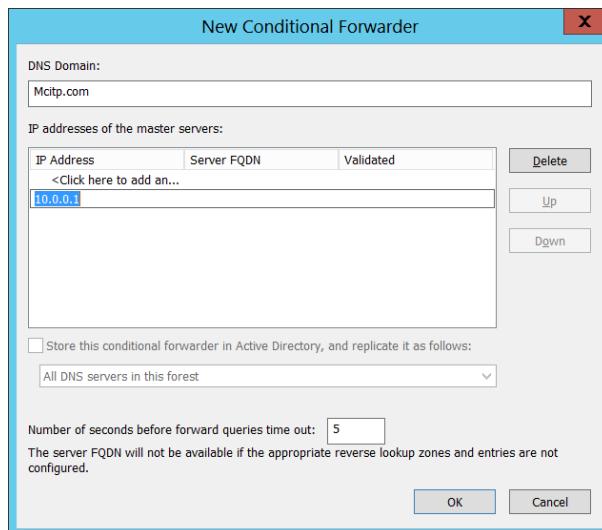
11. There will be a reply from 10.0.0.1

Note: Only MCITP.COM names can be resolved with the above process.

Lab – 8: Forwarders

1. In **SYS1** create a zone with the domain name Ex: **Microsoft.com** with host and alias records.
2. In **SYS1** open the command prompt and type ping www.Microsoft.com
3. There will be a reply from 10.0.0.1
4. In **SYS2** assign the **IP Address** and **Preferred DNS** as **10.0.0.2**
5. In **SYS2** open the command prompt and type ping www.Microsoft.com
6. There will not be any reply because the information is in 10.0.0.1
7. If **SYS2** has to resolve the query then configure forwarders in **SYS2** properties.
8. Open DNS in **SYS2** → Right click **SYS2** → select properties → select forwarders → click Edit.

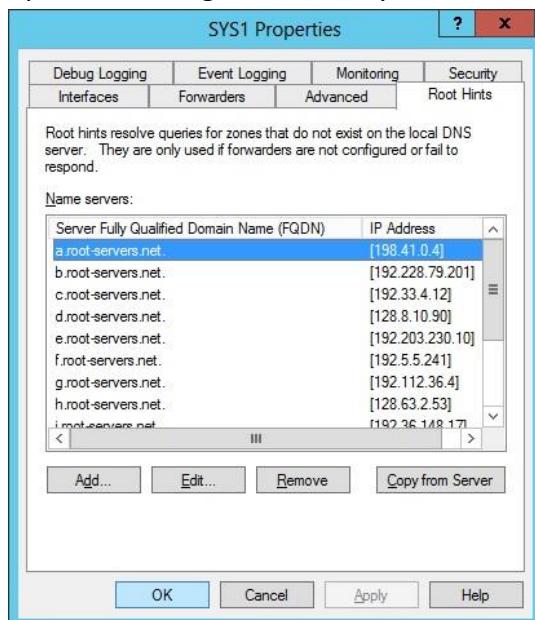
9. Mention the IP address of primary zone → click **OK** → click **OK**.



10. In **SYS2** open the command prompt and type ping www.Microsoft.com
11. There will be a reply from 10.0.0.1

Lab – 9: Root Hints

1. Root hints contain the information of 13 root servers
2. Open DNS → Right click the system name → select Properties → select **Root Hints**



Lab – 10: Cache server

1. To see the information present in the cache type the command
“Ipconfig /displaydns”
2. To clear the cache information type the command
“Ipconfig /flushdns”

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator>

```

INTERNET INFORMATION SERVICES

Internet Information Services (IIS)

- IIS is a service which is used to host the information over internet.
- It provides integrated, reliable, scalable and manageable Web server capabilities over an intranet / internet.

Versions of IIS

- IIS 2.0 in Windows NT 4.0 Operating System
- IIS 5.0 in Windows 2000 Operating System
- IIS 6.0 in Windows 2003 Operating System
- IIS 7.0 in Windows 2008 Operating System
- IIS 8.0 in Windows 2012 Operating System

Features Of IIS 8.0

- Supports IPv6
- Backup & Restoration of website configuration is automatic.
- Support for Application Developers & Programmers

IIS 8.0 Services

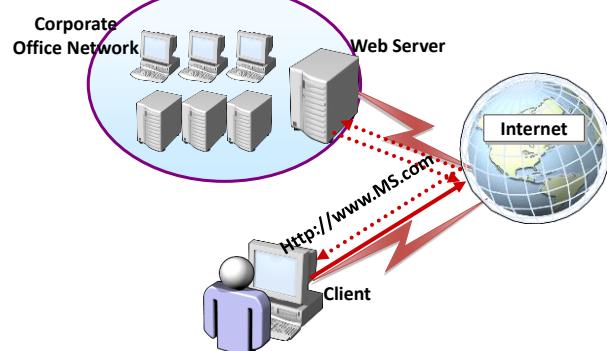
- World Wide Web (WWW) publishing service (HTTP)
- File Transfer Protocol (FTP) service

Hyper-Text Transfer Protocol

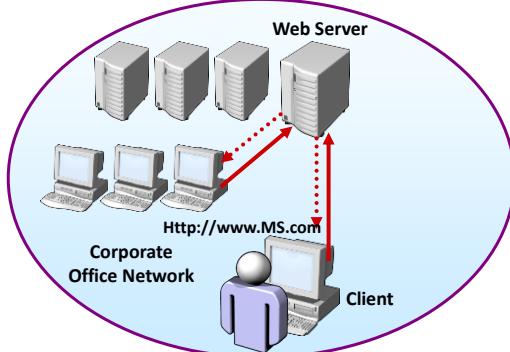
World Wide Web (WWW) publishing service (HTTP)

- Http service is used to publish data to World Wide Web quickly & easily.
- This protocol is easily configurable and it supports security and encryption to protect sensitive data.
- Default Port No is 80

Internet Web Server



Intranet Web Server



Requirements to Host WEB SERVER

- Static IP Address (Public IP if published over Internet)
- Domain name (Registered Domain name if Published over Internet)
- Name Resolution Service like DNS
- Home Directory
 - Required for each Web site
 - Central location of published pages

Virtual Directory

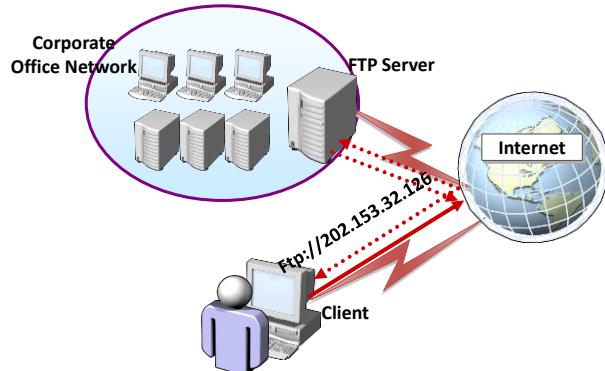
- Virtual Directories are sub directories of the root of the web site.
- By using Virtual directories we can create alias or pointer to a directory somewhere else in the same system or another system on the network.

FTP

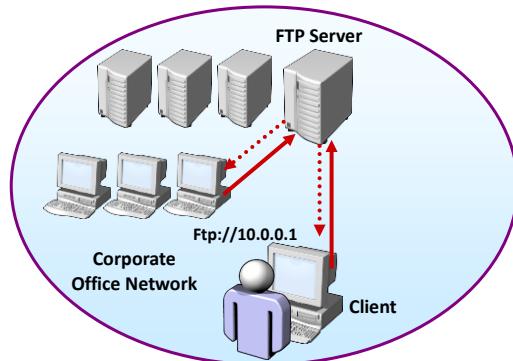
File Transfer Protocol (FTP) service

- It is a protocol used to download and upload the files over the internet.
- Default Port No is 21

Internet FTP Server



Intranet FTP Server



Requirements to Host FTP SERVER

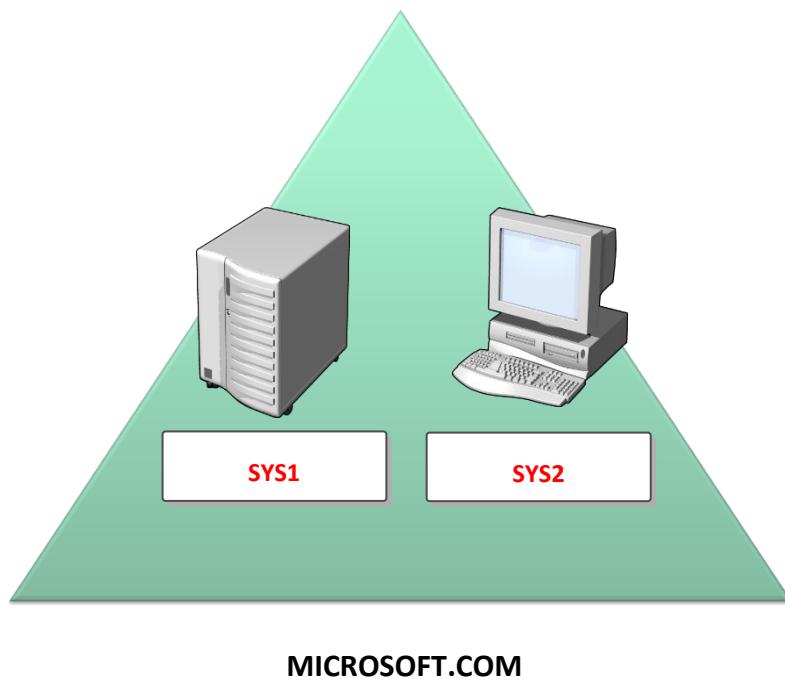
- Static IP Address (Public IP if published over Internet)
- Home Directory
 - Required for each FTP site
 - Central location of published pages

INTERNET INFORMATION SERVICES (IIS) –WEB& FTP SERVER

Prerequisites:

Before working on this lab, you must have

1. A computer running windows 2012 server or Domain Controller.
2. A computer running windows 2012 server or Windows 7.



SYS1

Domain Controller/DNS/Web Server

IP Address 10.0.0.1

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

SYS2

Member Server / Client

IP Address 10.0.0.2

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

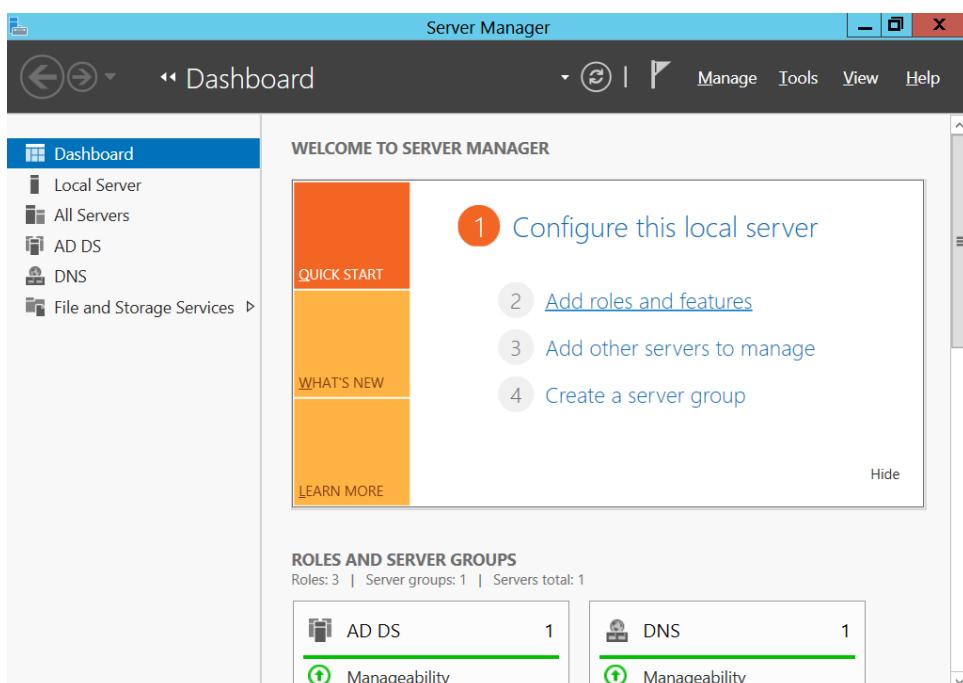
Lab – 1: Installing Internet Information Services - Web & FTP Server

SYS1- CONFIGURATION

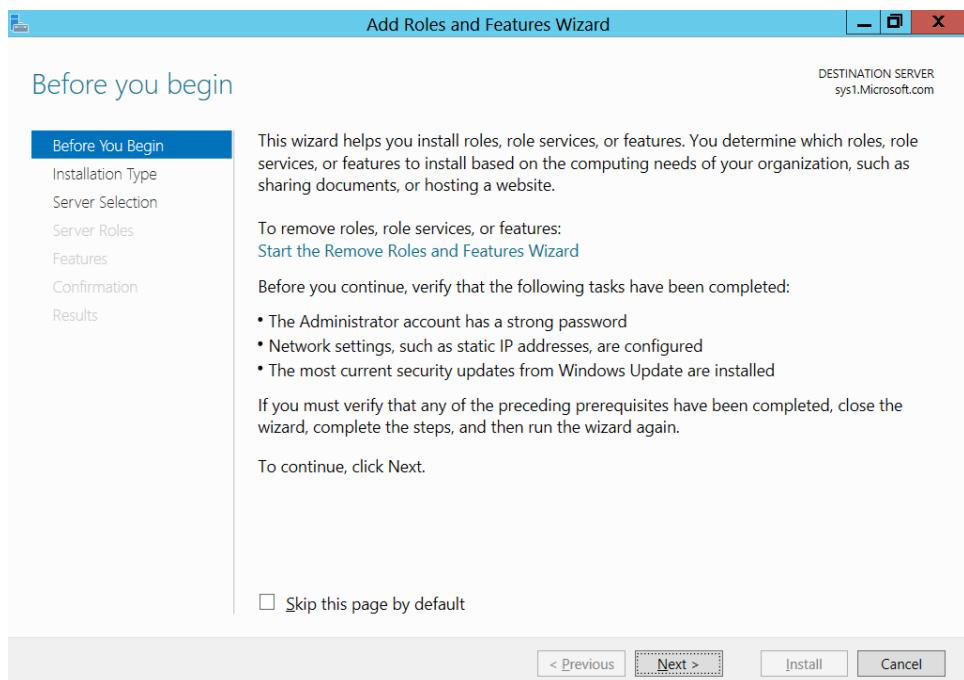
1. Click **Server Manager**.



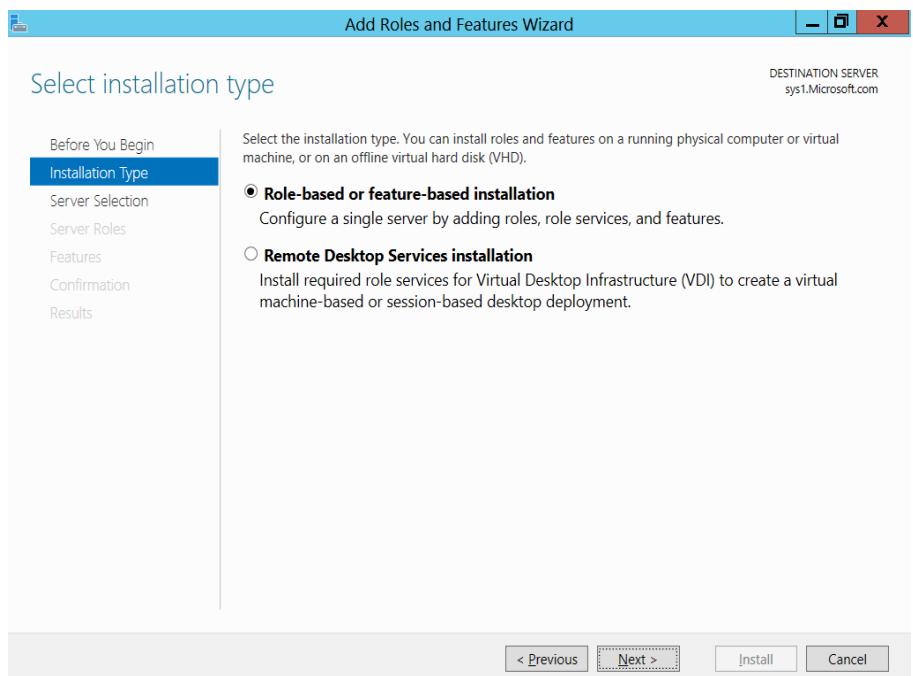
2. In the Server Manager Dashboard → select **Add roles and features**.



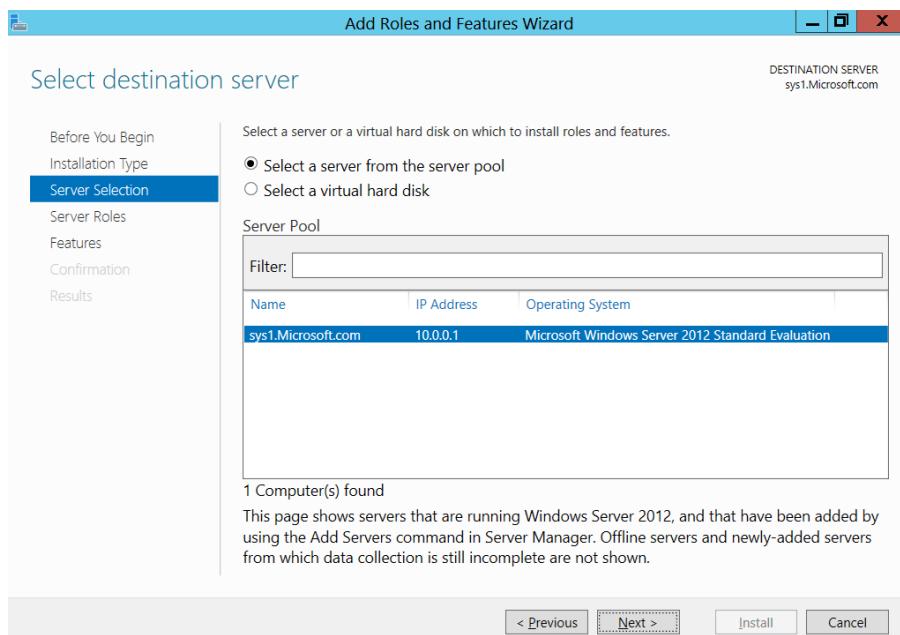
3. In Before you begin page, click **Next**.



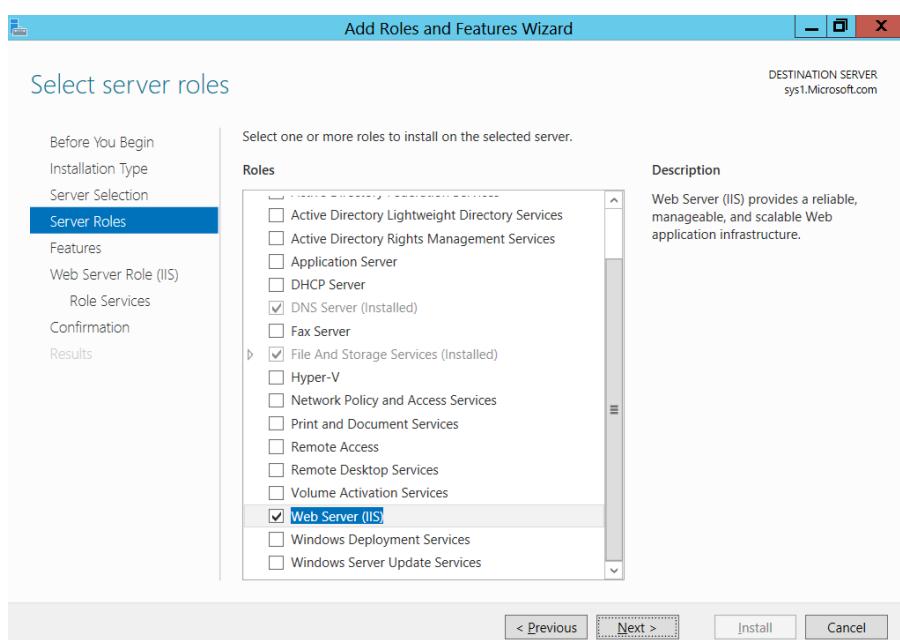
4. Select **Role-based or feature-based installation**, click **Next**.



- 5. Select a server (**sys1.Microsoft.com**) from the server pool and click **Next**.**

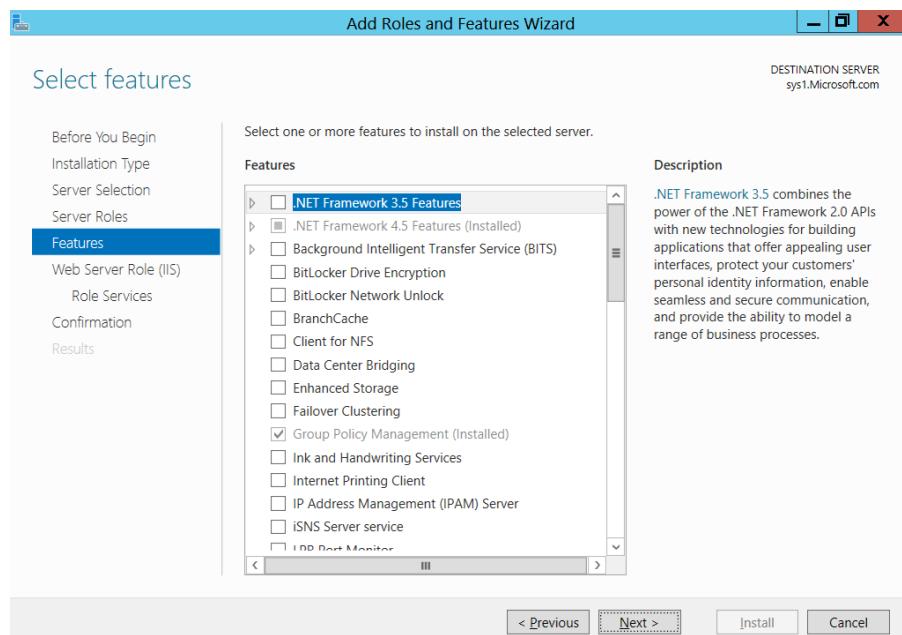


- 6. In select server roles, check the box Web Server and click **Next**.**

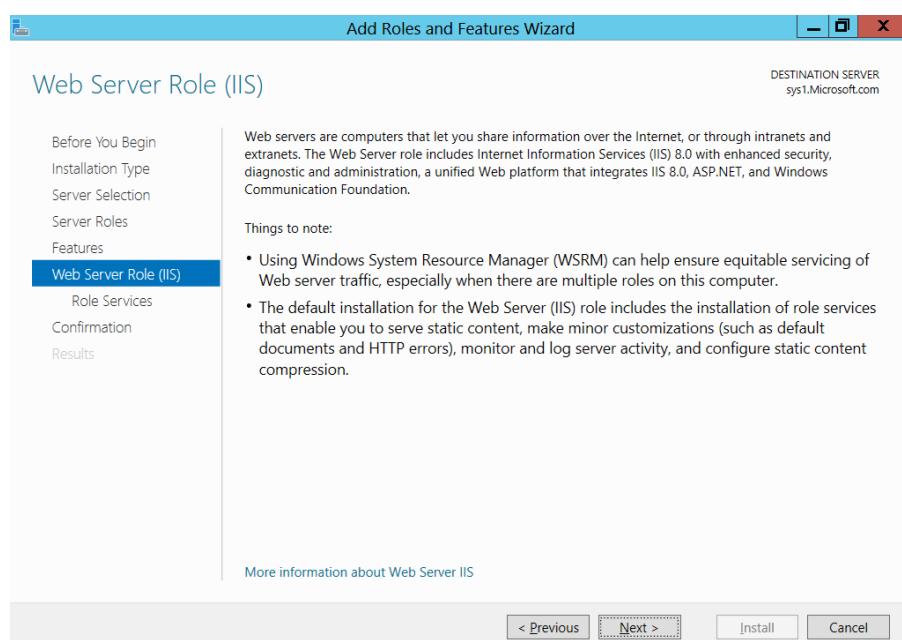


- 7. In Add required features for Web Server (IIS), click **Add Features**.**

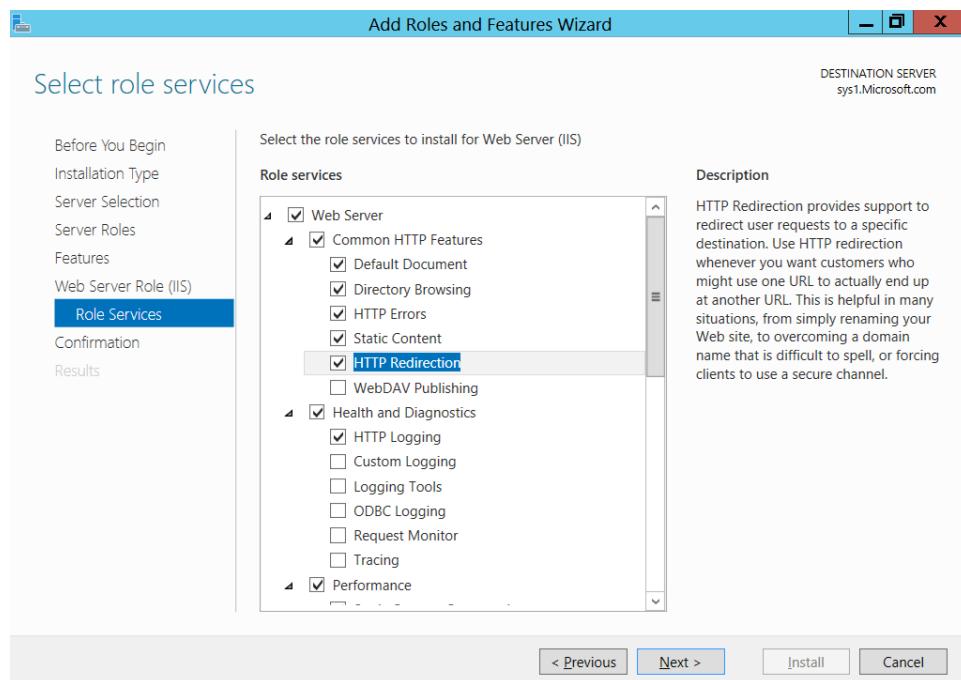
8. In select features, click **Next.**



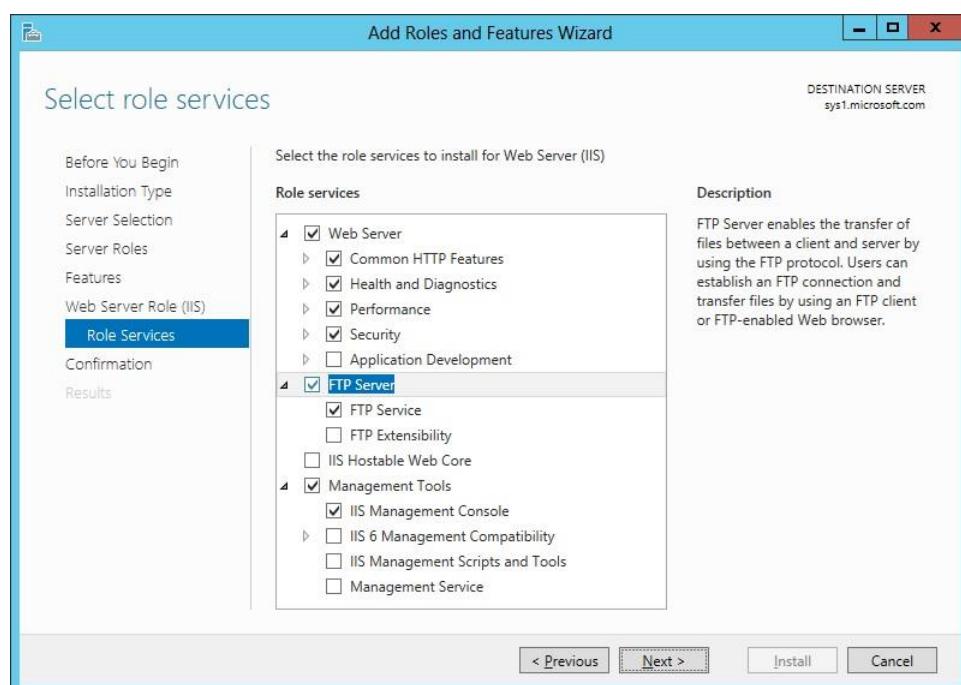
9. Click **Next.**

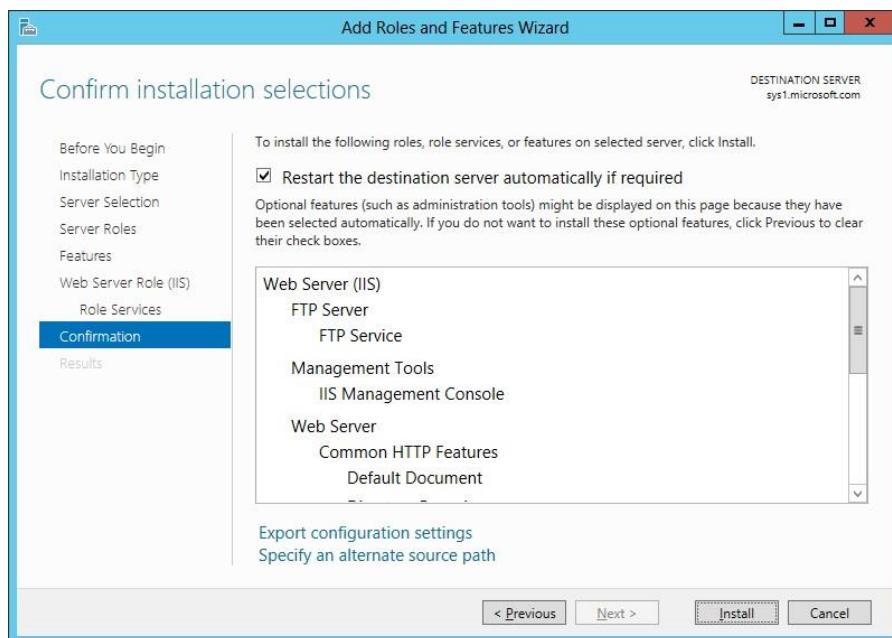


10. Check the box **HTTP Redirection, under Common HTTP Features.**

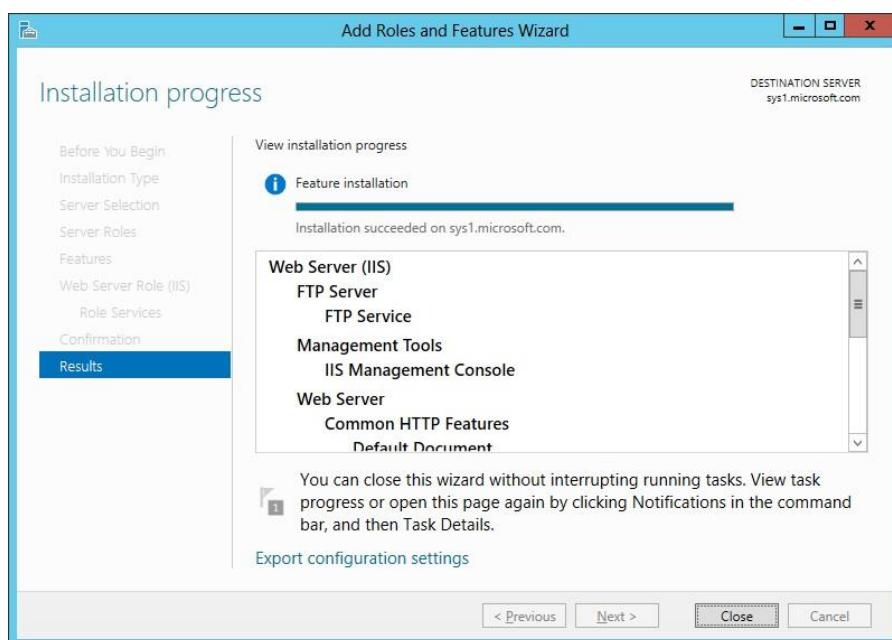


11. Check the box **FTP Service, under FTP Server.**



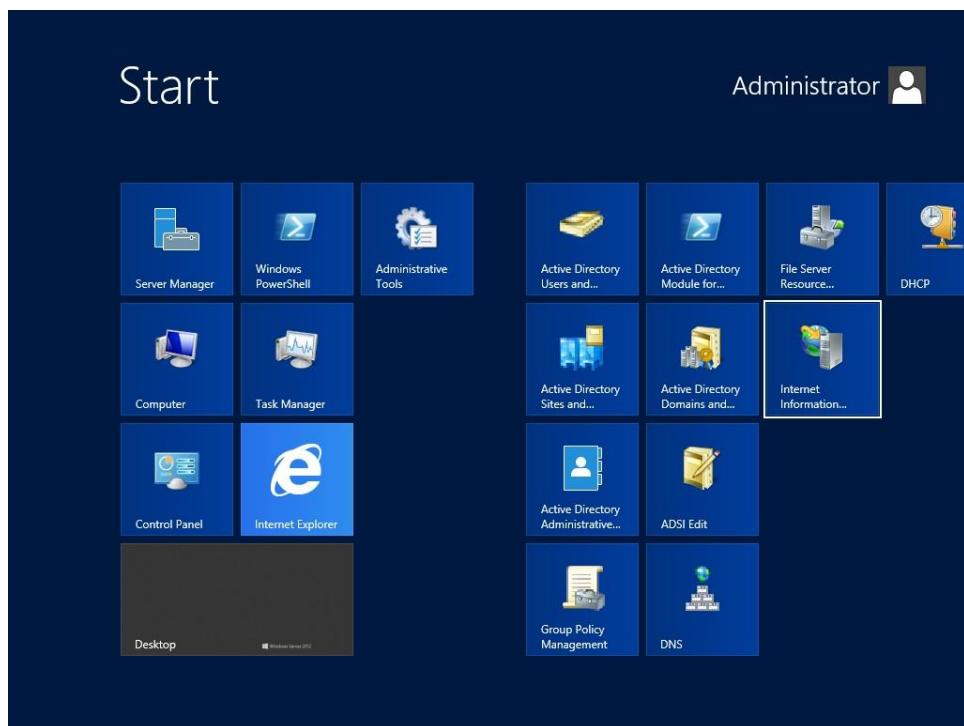
12. Check Restart the destination server automatically if required and click **Install**.

13. Select Complete DHCP configuration.

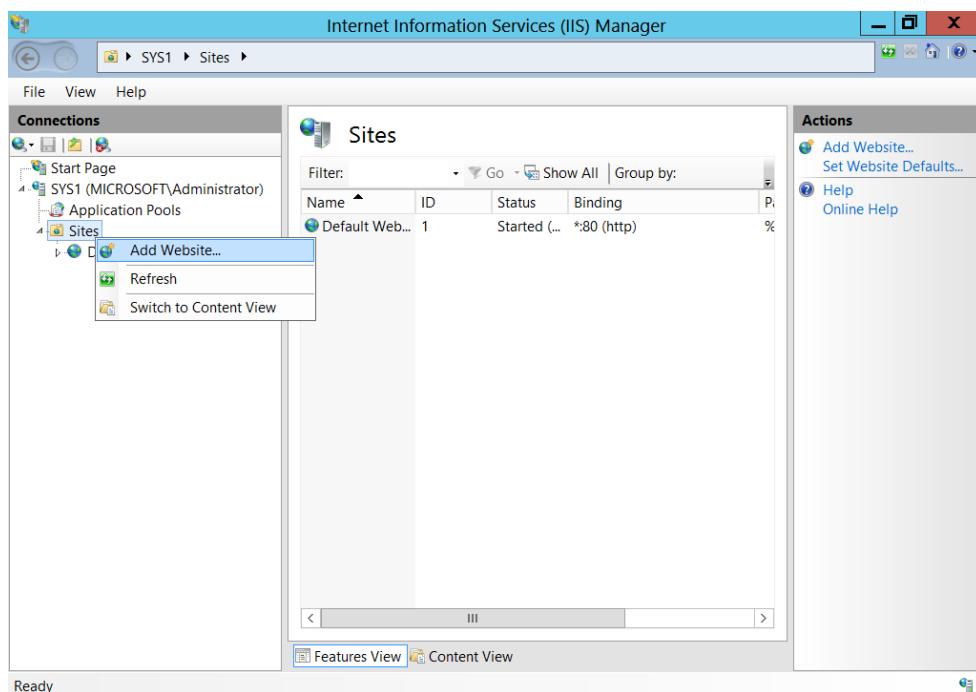


Lab – 2: Creating a Web Site

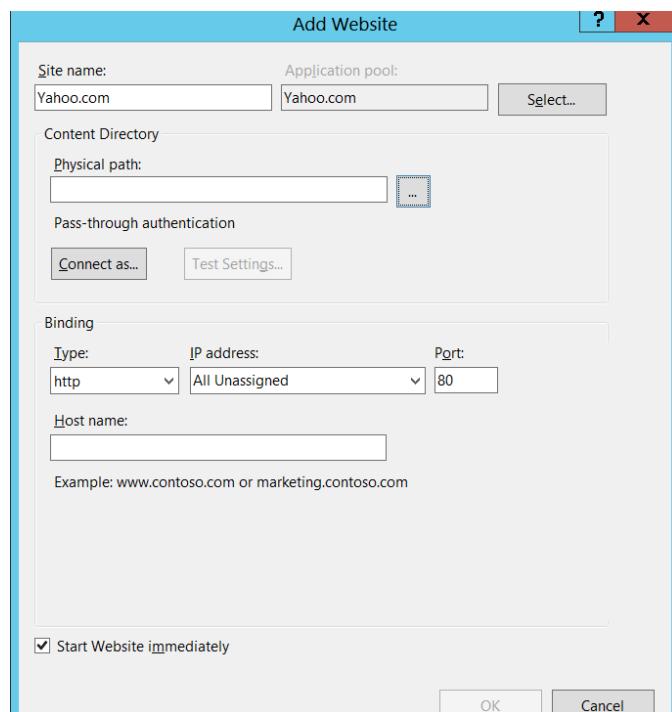
1. Go to Start, select **Internet Information Services Manager**.



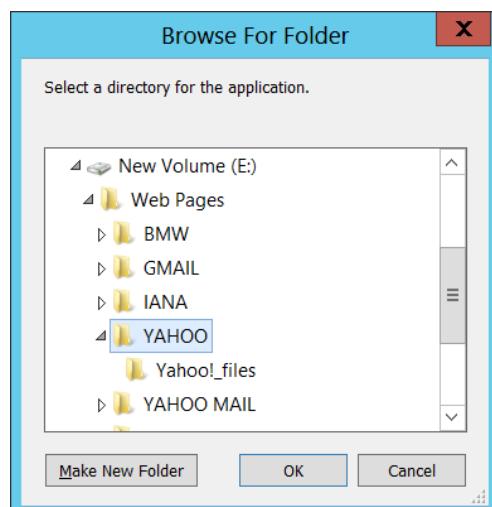
2. In the left pane of the **Internet Information Services**, Expand the server → Right click on sites and select **Add Web Site**.



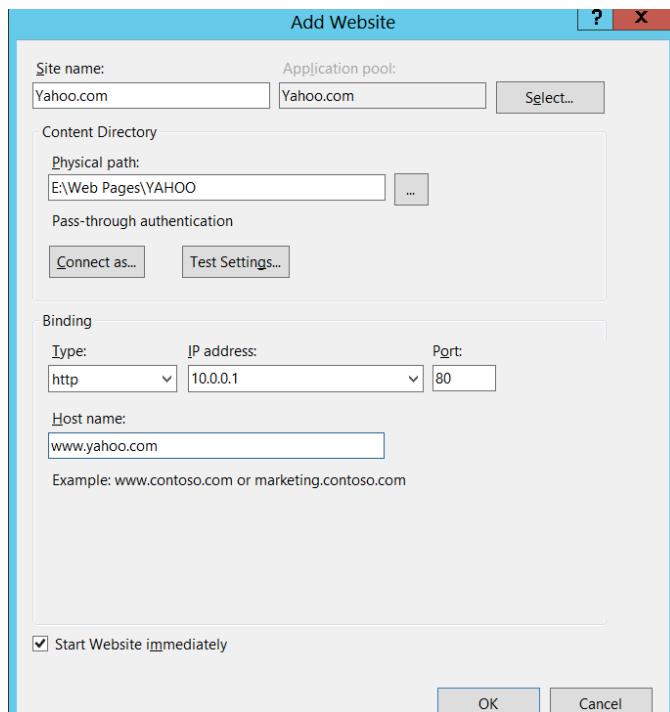
3. Add Web Site wizard opens → In the Site name type a Name for the Website
Ex:YAHOO.COM



4. In Physical path, browse and select the location of Home Directory (webpage)



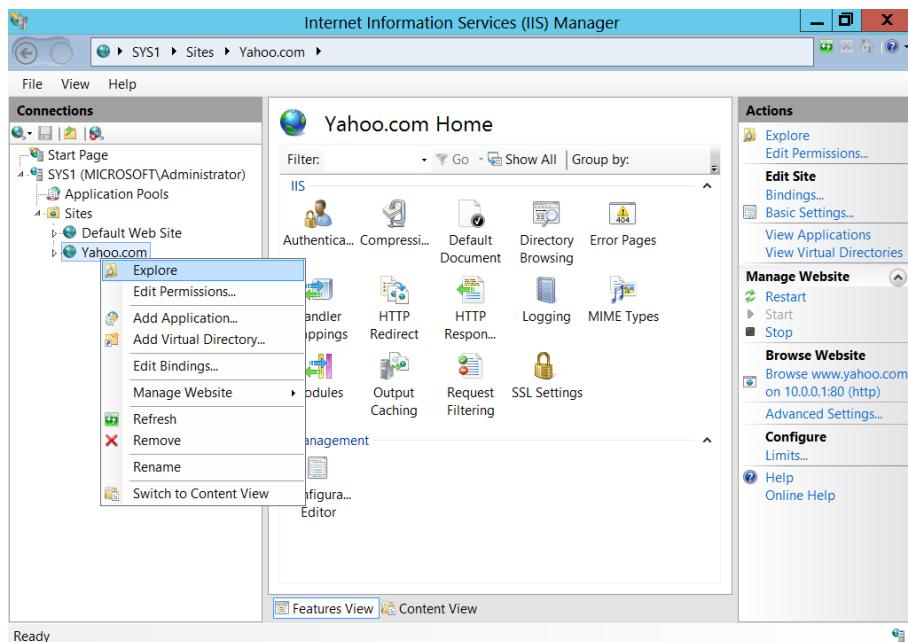
5. Select one **IP address (10.0.0.1)** from the drop-down list.
6. Specify the Host name Ex: [WWW.YAHOO.COM](http://www.yahoo.com) & click**OK**.



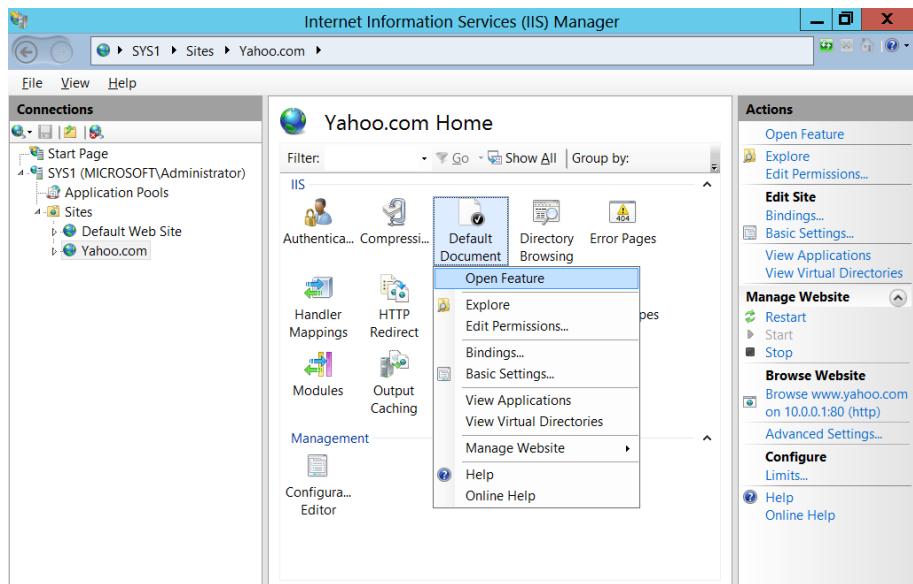
7. **Web Site** will be successfully added.

Adding the Default Document for the website

1. Open IIS → expand sites → select website → right click and select **Explore**.

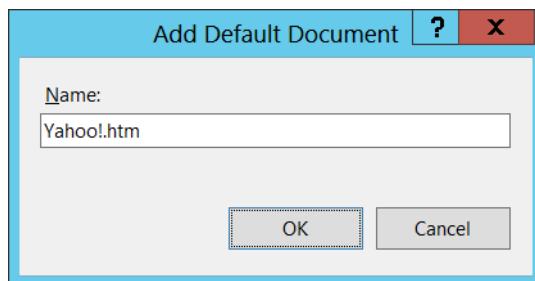


2. Select the **Webpage** → Right click & select **Rename** → Copy the webpage name
3. In IIS → expand sites → select website → Open **Default Document** feature.



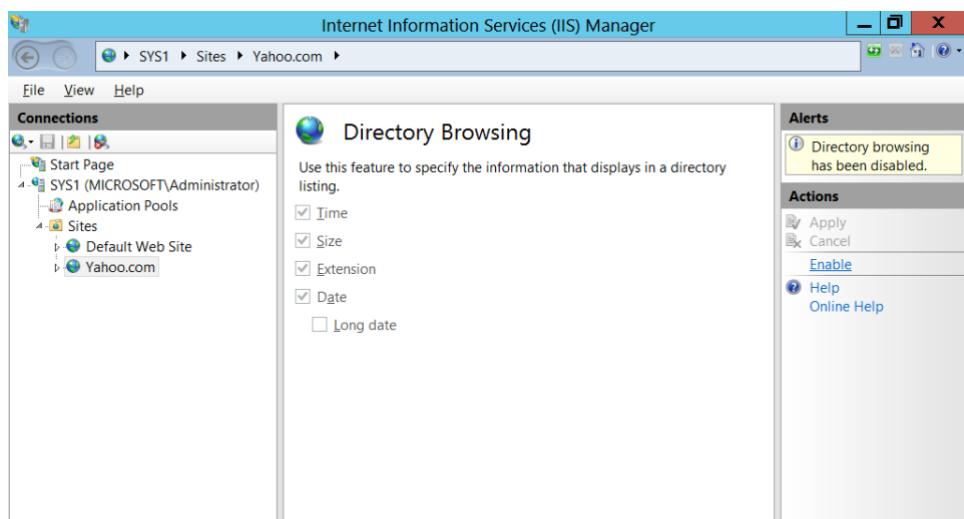
- Click **Add**, Mention (Paste) the html file name (with Extension of file)

Ex:Yahoo!.htm → click **OK**.



Enable Directory Browsing for the web site

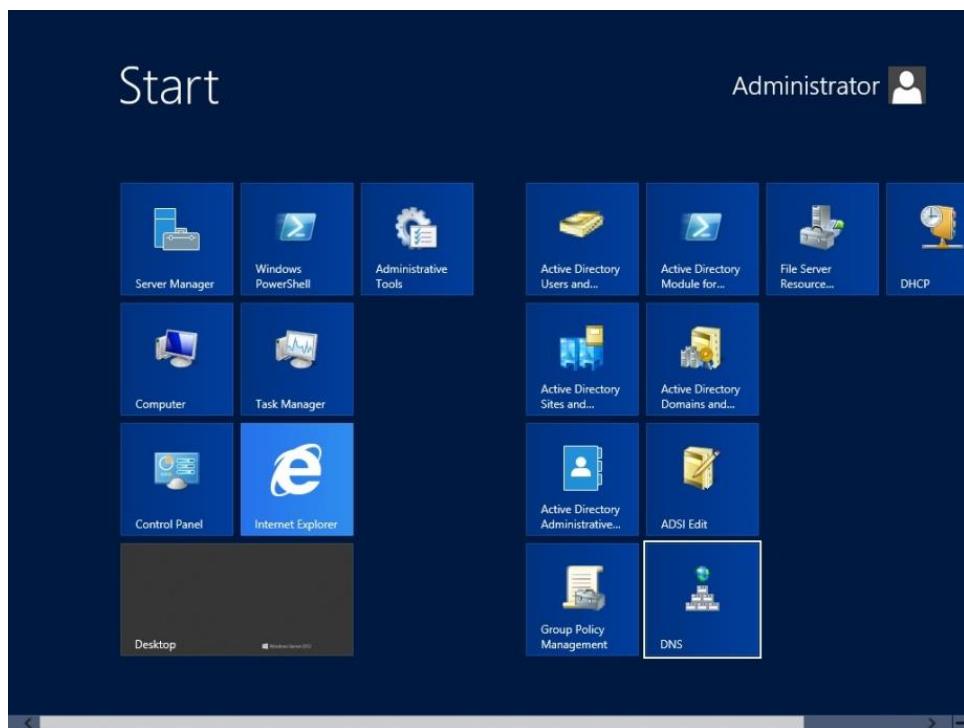
- Open IIS → expand sites and select the website (YAHOO.COM)



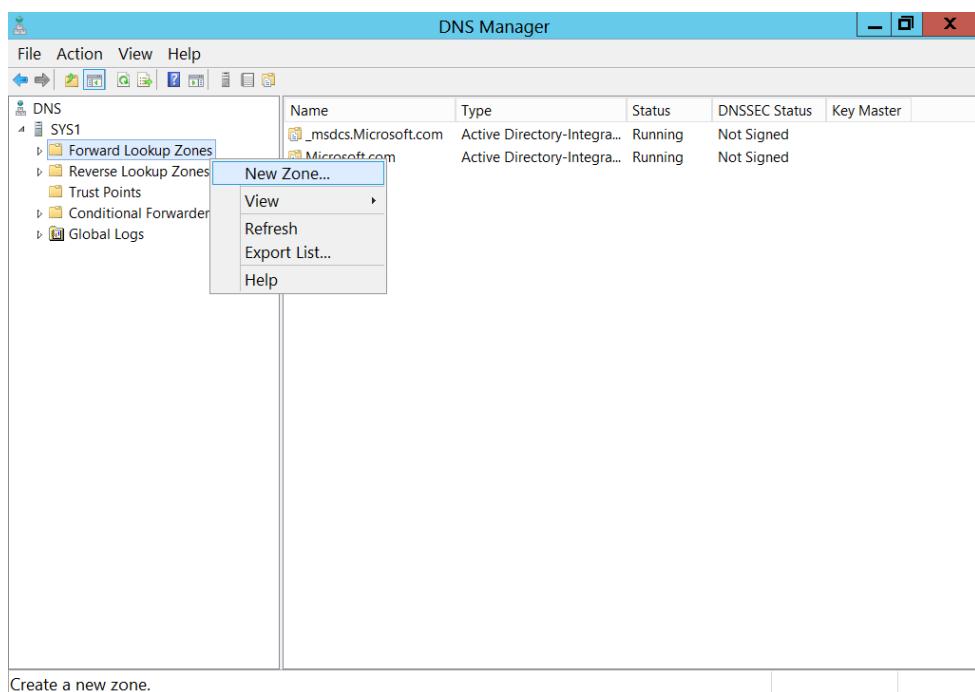
- Open Directory Browsing Feature → click **Enable**. (on Actions pane)

DNS Configuration for the Website

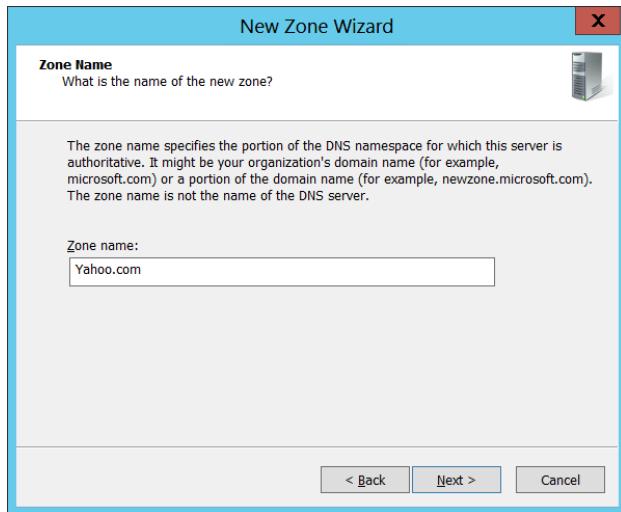
1. Go to Start, select DNS



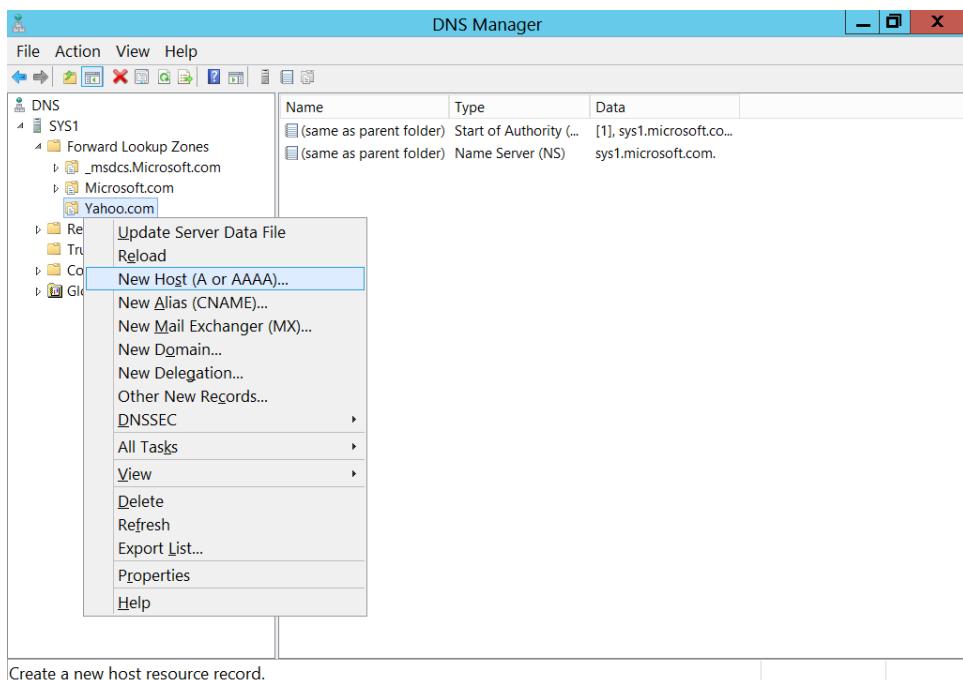
2. Select Forward Lookup Zone → Right click select New Zone



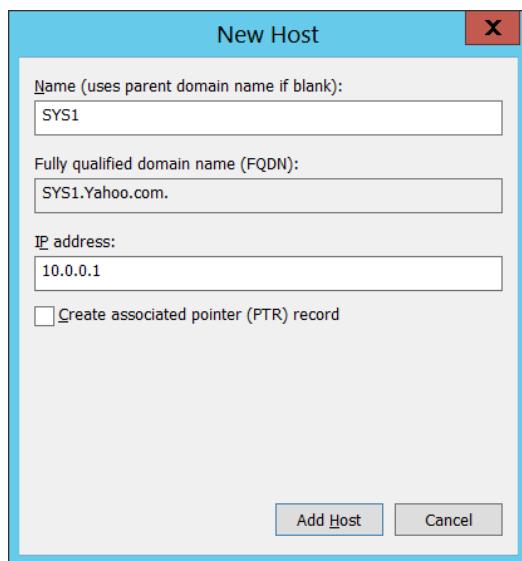
3. Create a new primary zone in **Forward Lookup Zone** and mention the website **Domain Name (Ex:YAHOO.COM)**



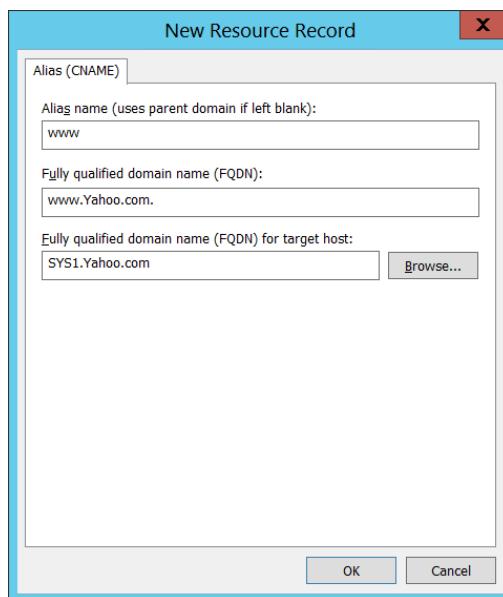
4. Select the zone → Right click select **New Host**



5. Mention the **Web Server name and IP Address** →Add Host →OK →Done.



6. Select the zone →Right click select **New Alias** & Create an **Alias** (E.g: www) for the host, which you specified in the host header for the site →click **OK**.



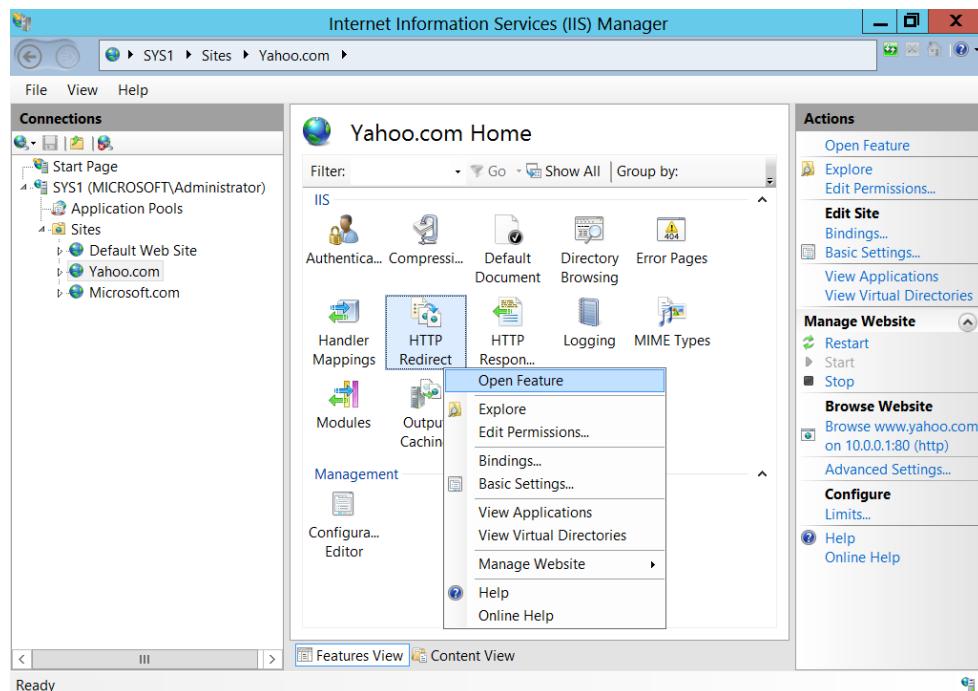
VERIFICATION:

1. Open Internet Explorer or any browser and access the website

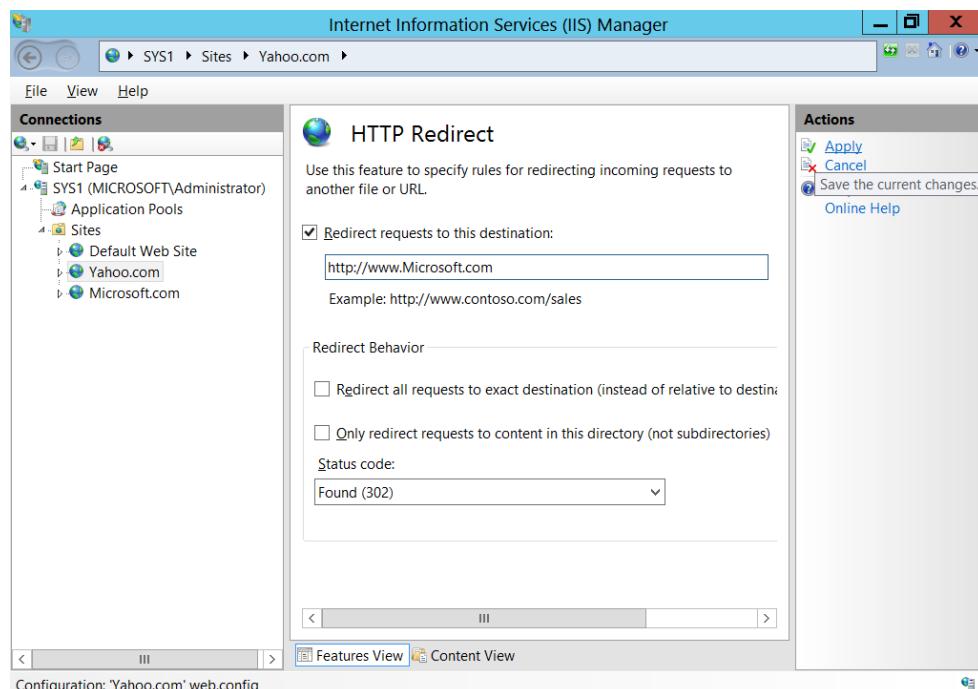


Lab – 3: Configuring redirection of Websites

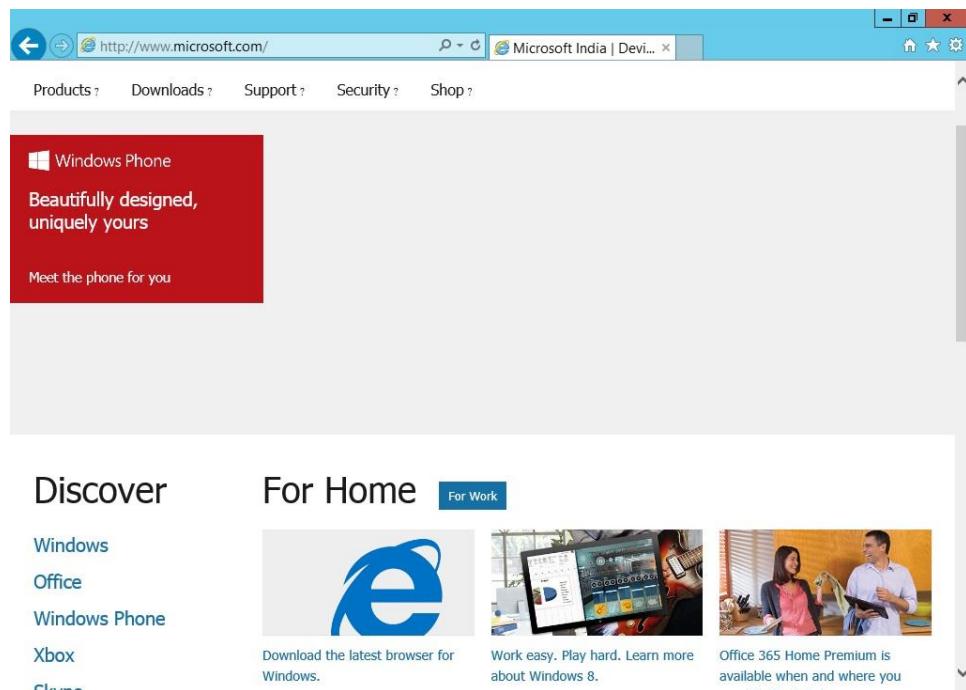
1. Go to Start select **Internet Information Services Manager**,
2. Create **two websites**, Ex:**YAHOO.COM** and **MICROSOFT.COM**
3. If YAHOO has to be redirected to MICROSOFT then Select **YAHOO.COM** → Open **HTTP Redirect feature**



4. Select the check box **Redirect requests to this destination** give the destination as <http://www.MICROSOFT.com> and click **Apply** in the actions Pane.

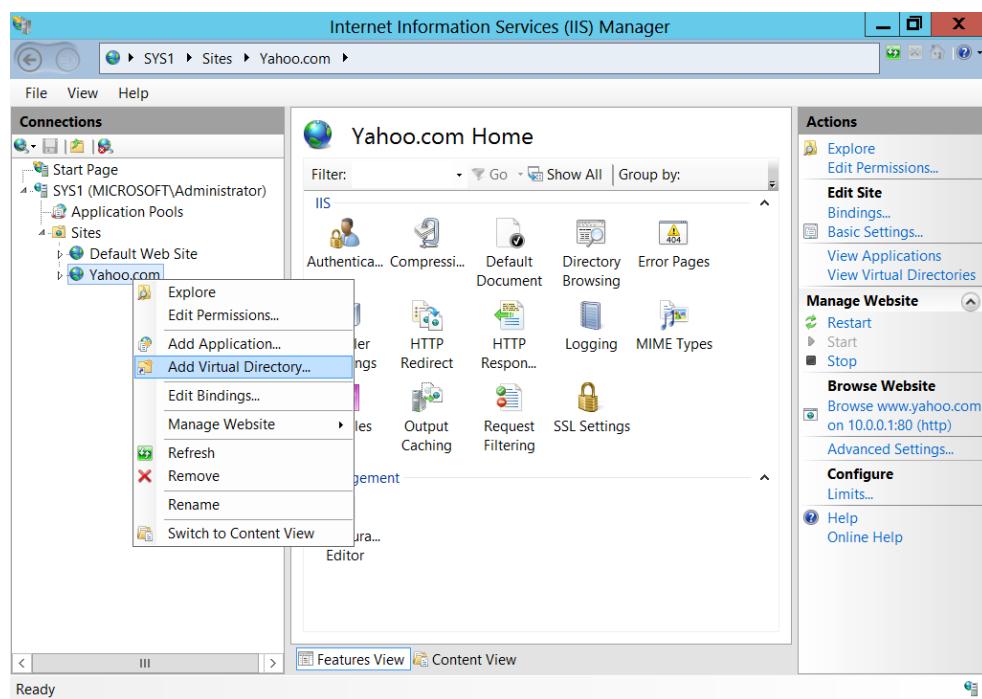


5. Open Internet Explorer or any browser and access **Yahoo** (www.yahoo.com) and it will be automatically redirected to **MICROSOFT** (www.MICROSOFT.com).

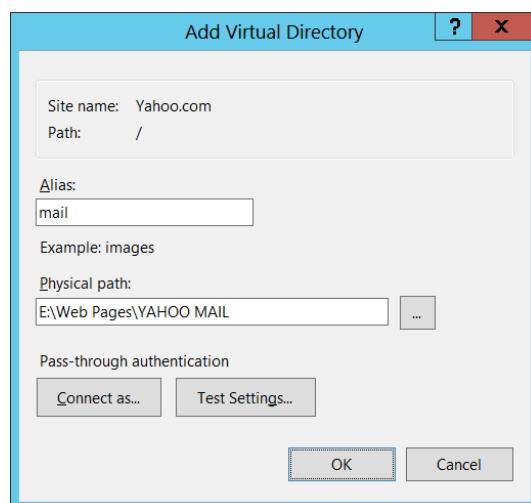


Lab – 4: Creating Virtual Directory

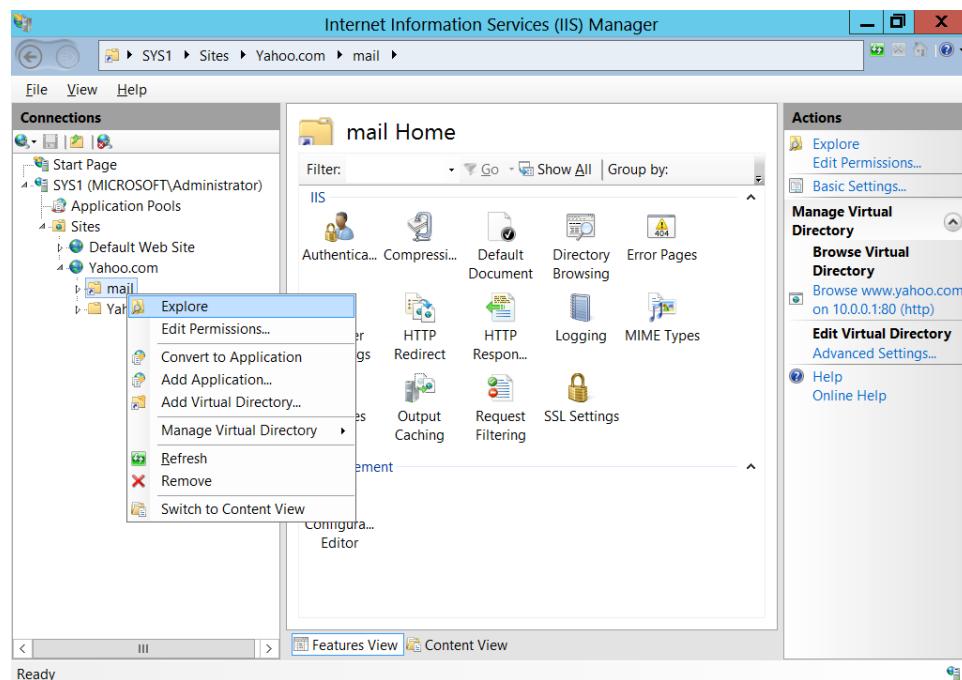
1. Go to Start, select **Internet Information Services Manager**.
2. Expand the system name, Select the Web Site (Yahoo) for which you want to create Virtual Directory → Right click and select **Add Virtual Directory**.



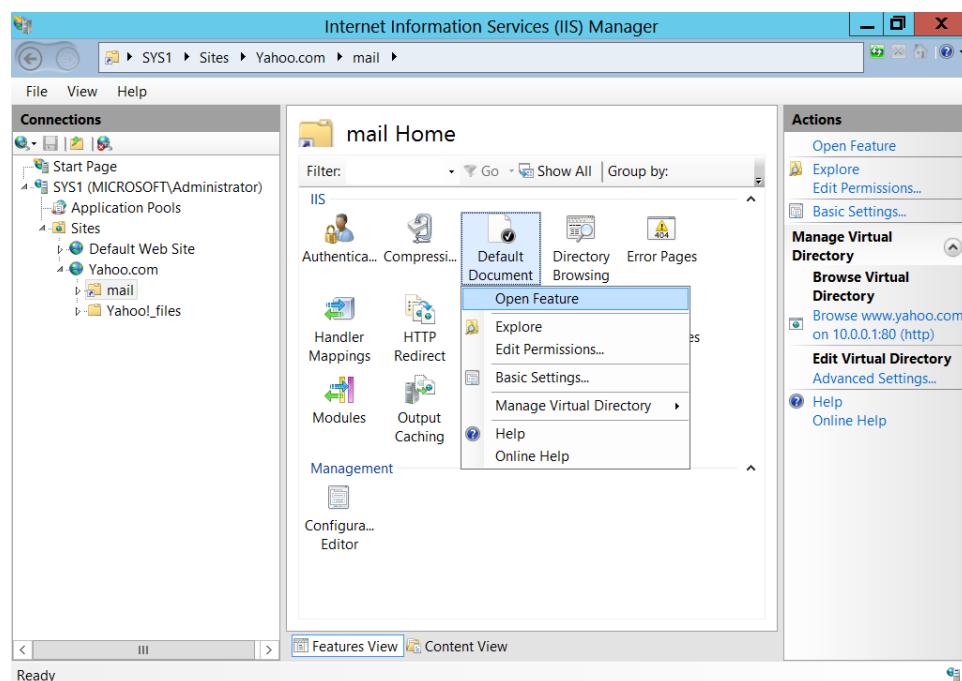
3. Specify the **Alias** name to the **Virtual Directory** (Ex: mail), and **Browse** to select the physical path Ex:(D:\Yahoomail) → click **OK**.



4. Virtual Directory will be created.



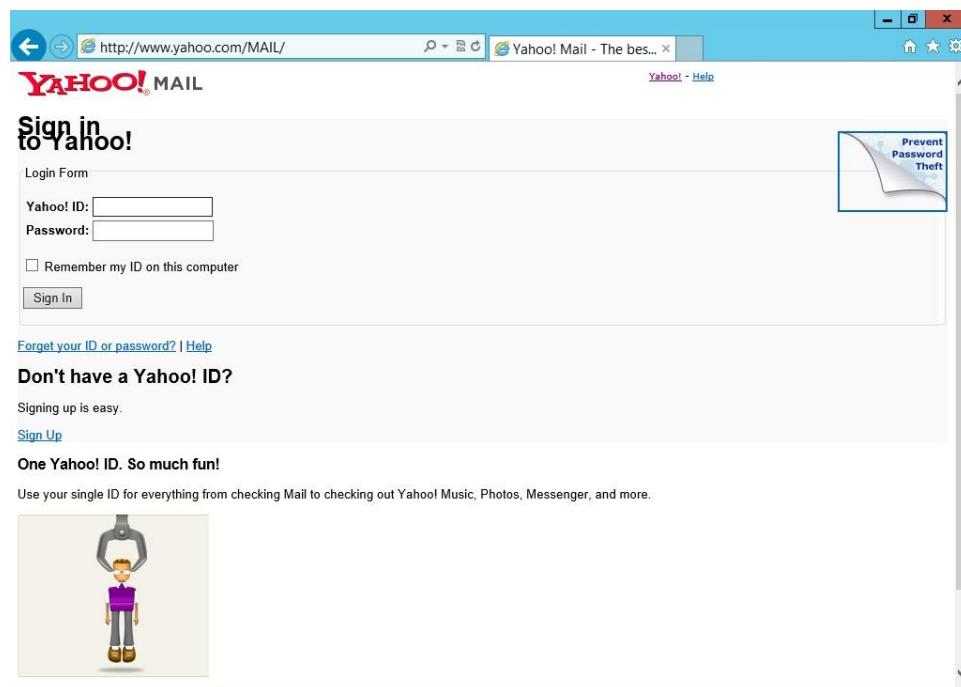
5. Add the Default Document for the Virtual Directory →OK



6. To access the virtual directory specify the syntax in **Internet Explorer**

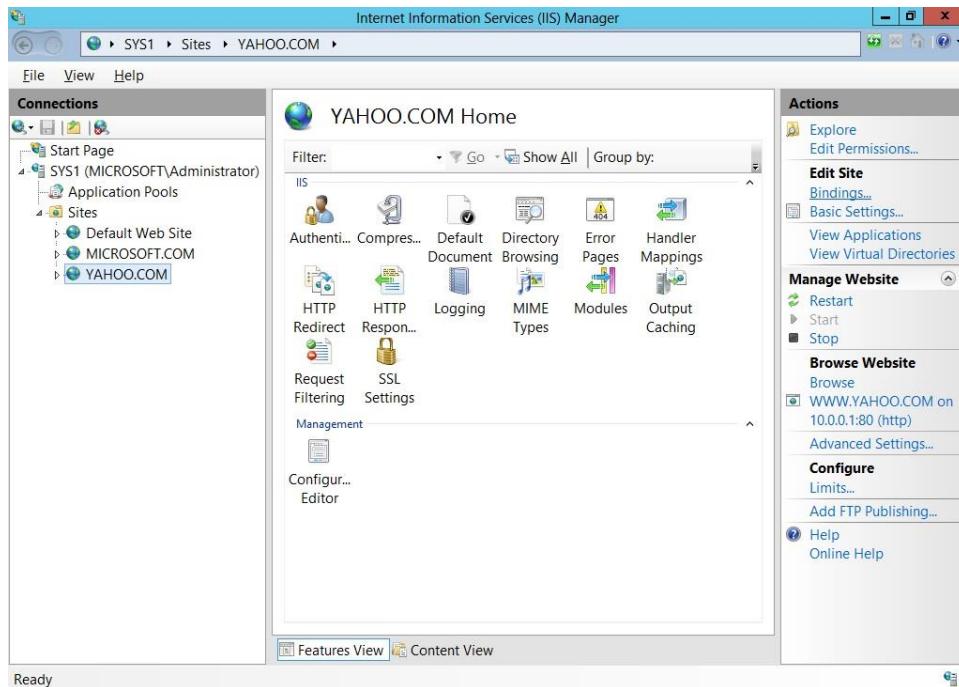
<http://websitename/virtualdirectoryname>

Ex: <http://www.Yahoo.com/mail>



Lab – 5: Changing the Web Site IP address or Port no

1. Go to Start, select **Internet Information Services Manager**.
2. Select the Web site → click **Bindings** in the Actions Pane.

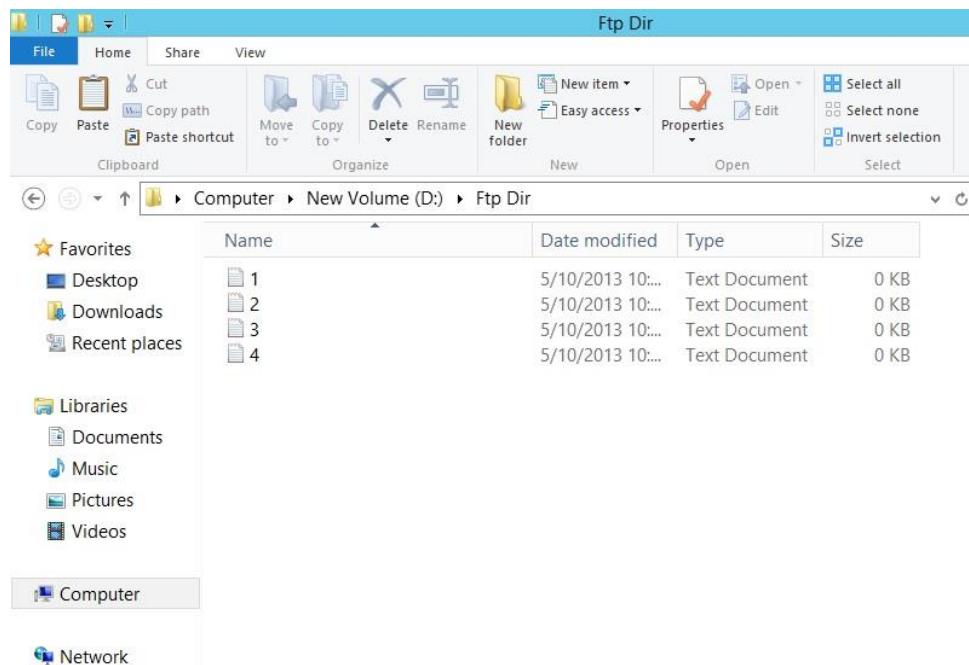


3. Click **edit** and change the **IP address or port number or host name**.
4. If the port number is changed then the website can be accessed only by specifying the port number [http://www.yahoo.com:port number](http://www.yahoo.com:port_number)

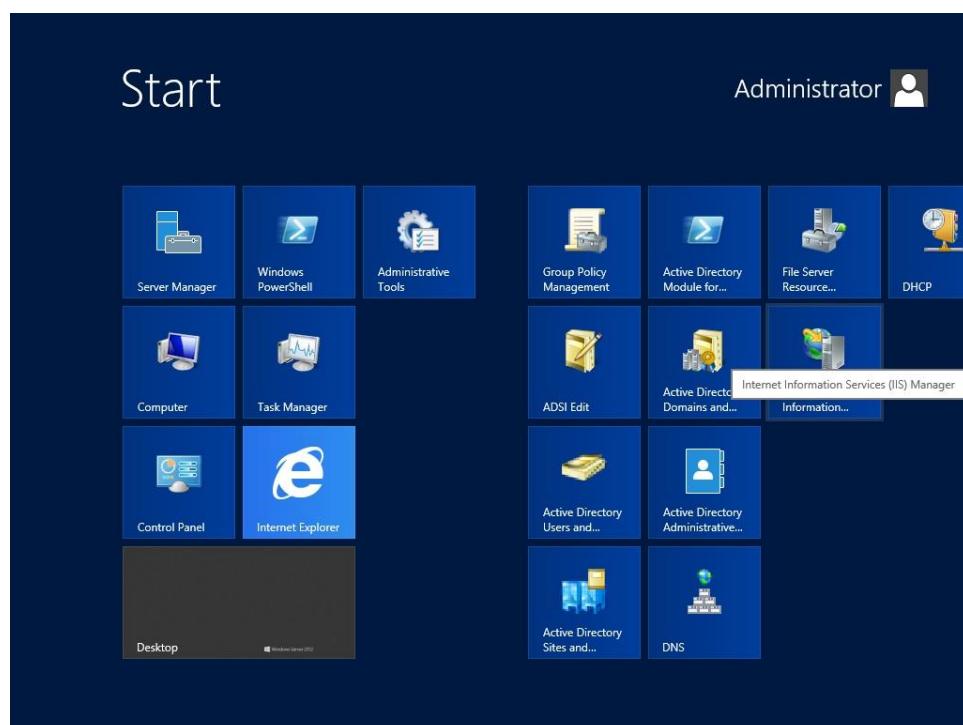


Lab – 6: Creating Do not Isolate user FTP Site

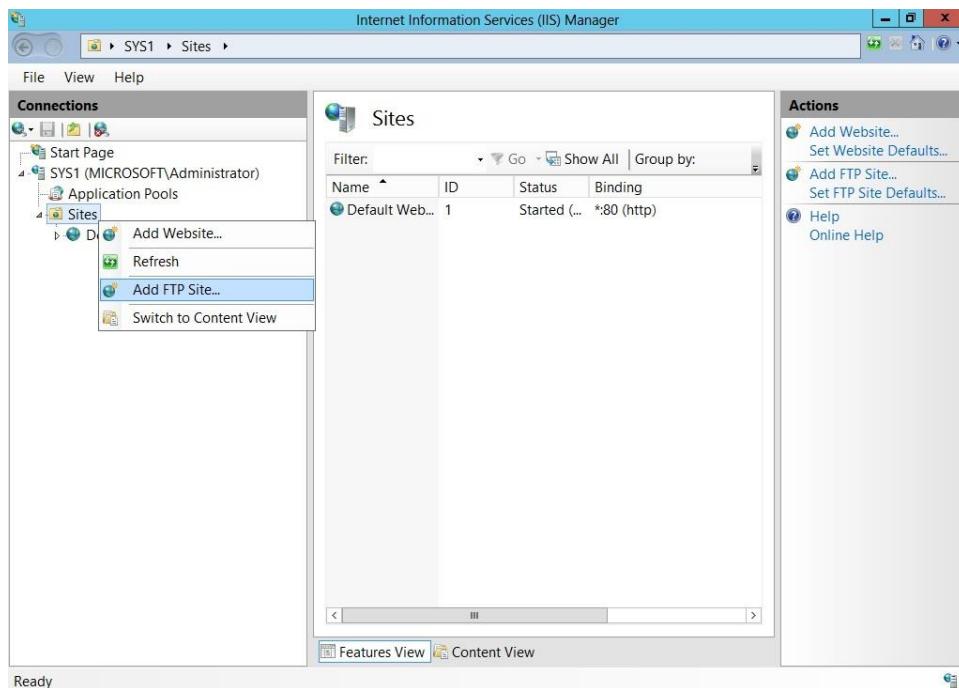
1. Open any drive and **create a folder (Ex: FTP Dir)** → Open the folder and **create some files** Ex: 1.txt, 2.txt, 3.txt, 4.txt.



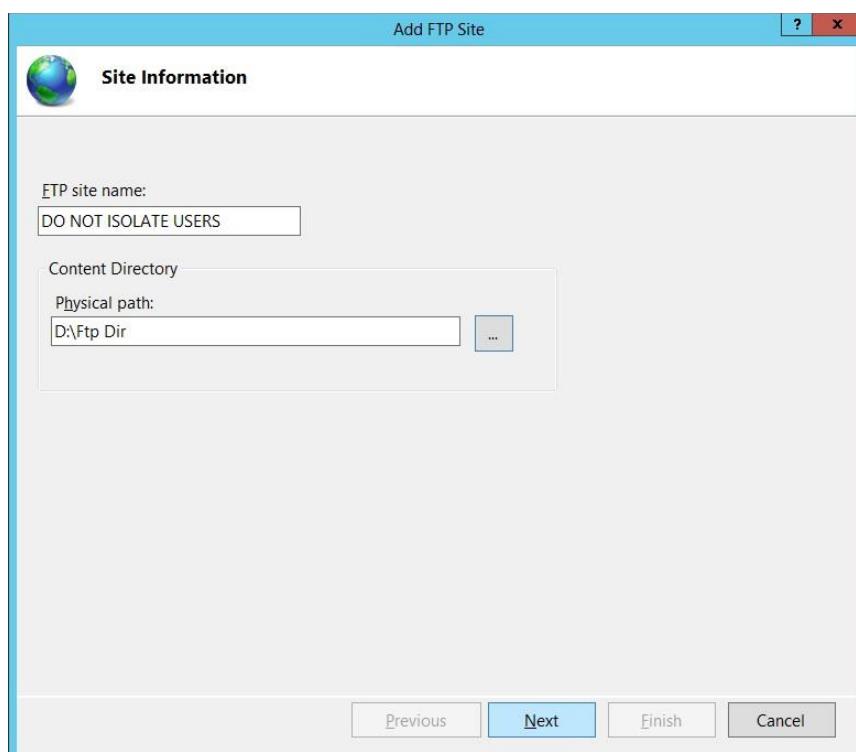
2. Go to Start, select **Internet Information Services (IIS) Manager**.



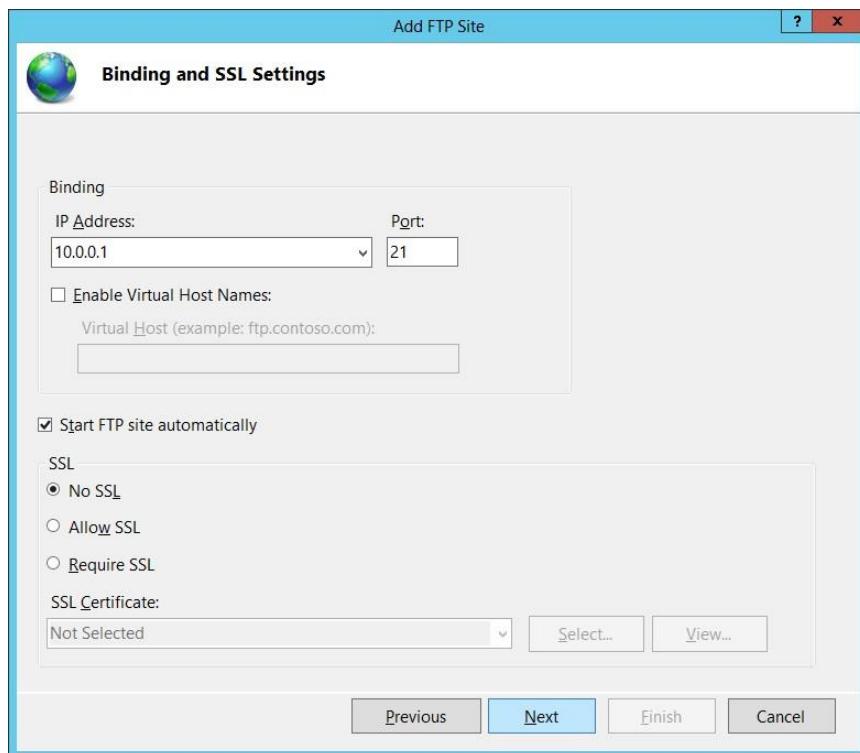
3. In the left pane of the **Internet Information Services** dialog box → Expand the server → Right click on **Sites** and select **ADD FTP Site**



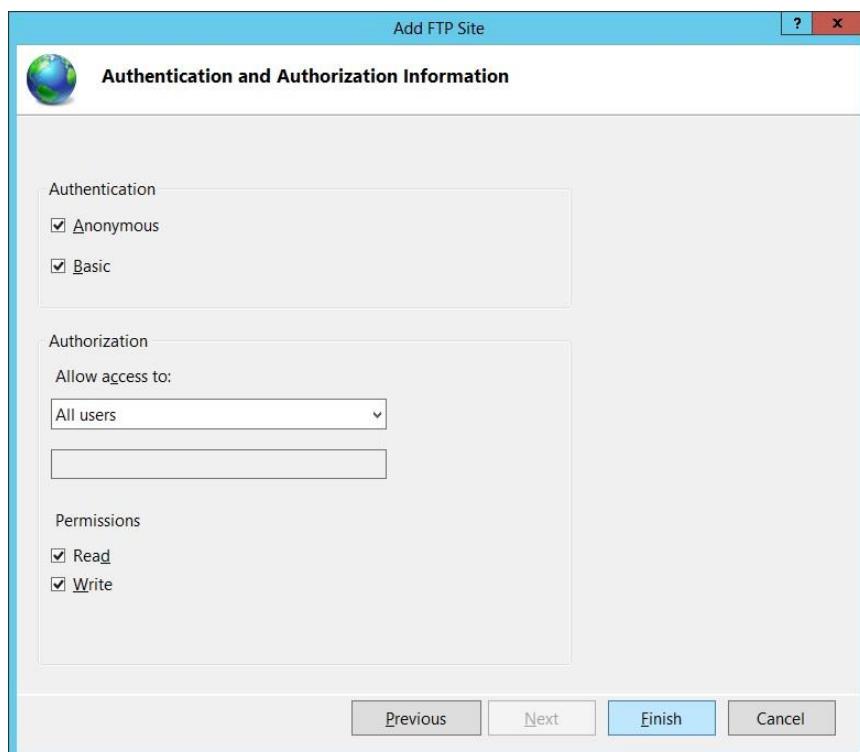
4. In Site Information screen, enter the FTP site name, and enter the path to the home folder (Content Directory) you want to assign to this FTP site. This can be either a local path or a UNC path of the shared folder → you can **browse for this folder** if you need to → click **Next**.



5. In the **Bindings and SSL Settings** dialog box select the IP address and port no. and select “**NO SSL**”.



6. In Authentication and Authorization Information dialog box, Check the box for **Anonymous and Basic**, Select **All Users**, Check the box for **Read and Write** → click **Finish**.

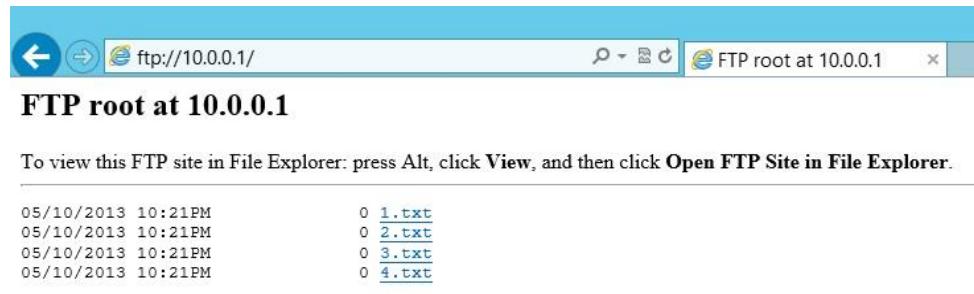


Accessing the FTP site from the Client systems

SYS2 – CONFIGURATION

1. Go to any Computer → Open Internet Explorer and type <ftp://10.0.0.1> and Press Enter.

Ex: <ftp://10.0.0.1>



FTP root at 10.0.0.1

To view this FTP site in File Explorer: press Alt, click View, and then click Open FTP Site in File Explorer.

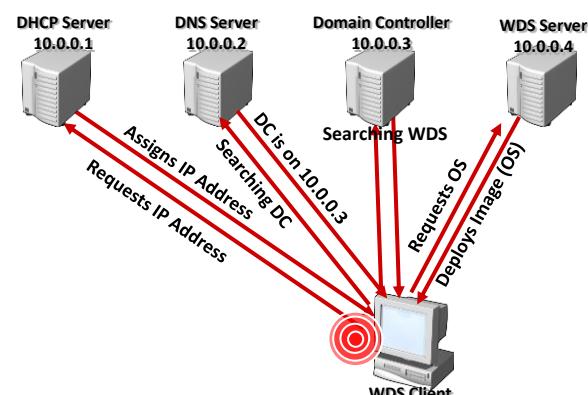
Date	Time	File Name
05/10/2013	10:21PM	0 1.txt
05/10/2013	10:21PM	0 2.txt
05/10/2013	10:21PM	0 3.txt
05/10/2013	10:21PM	0 4.txt

WINDOWS DEPLOYMENT SERVICES (WDS)

Requirements of WDS- Deployment Server

- DHCP Server
- DNS Server
- Active Directory – Domain Services
- An NTFS Partition to Store Images

How WDS Works?



Types of Clients

- **Known Clients**
 - A Known Client Computer is one whose computer account has been pre-created (Pre-Staged) in Active directory.
- **Un-Known Clients**
 - An un-known Client Computer is one whose computer account has not been pre-staged in Active directory.

Types of Images

- **Boot Image**
 - It is a WIM file you can use to boot a computer to begin the deployment of an O.S to the computer.
- **Install Image**
 - It is a image of Windows Vista or Windows server 2008 O.S itself that you want to deploy onto the client computer.

Types of Images

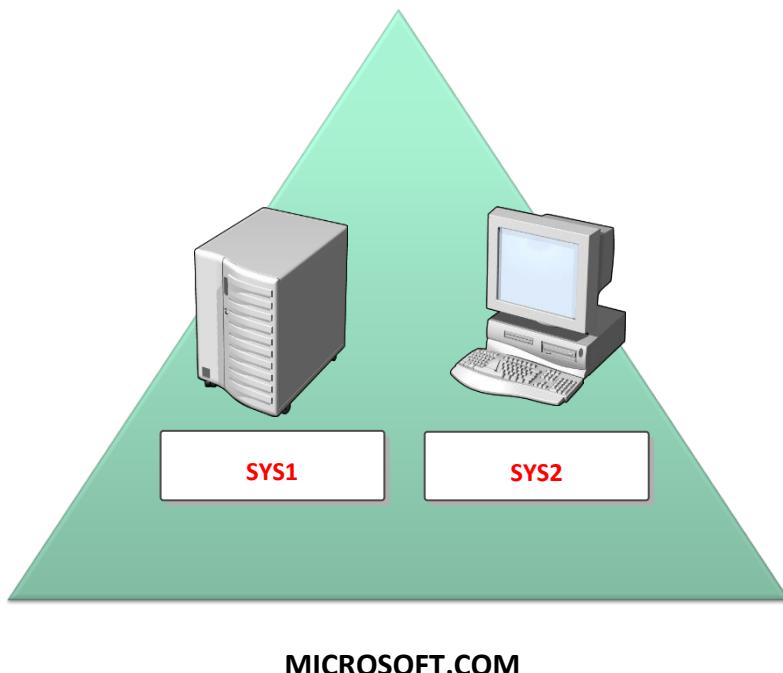
- **Capture Image**
 - It is a special boot image that you use to boot a master computer and upload an image to a WDS server.
- **Discover Image**
 - It is a boot image that you use to deploy an install image onto a computer that is not PXE enabled.

WINDOWS DEPLOYMENT SERVICES (WDS)

Prerequisites:

Before working on this lab, you must have

1. A computer running windows 2012 server Domain Controller, DHCP with Scope, DNS with Services records.
2. A computer with or without any Operating system.



SYS1	SYS2
Domain Controller / WDS Server	WDS Client
IP Address 10.0.0.1	IP Address -----
Subnet Mask 255.0.0.0	Subnet Mask -----
Preferred DNS 10.0.0.1	Preferred DNS -----

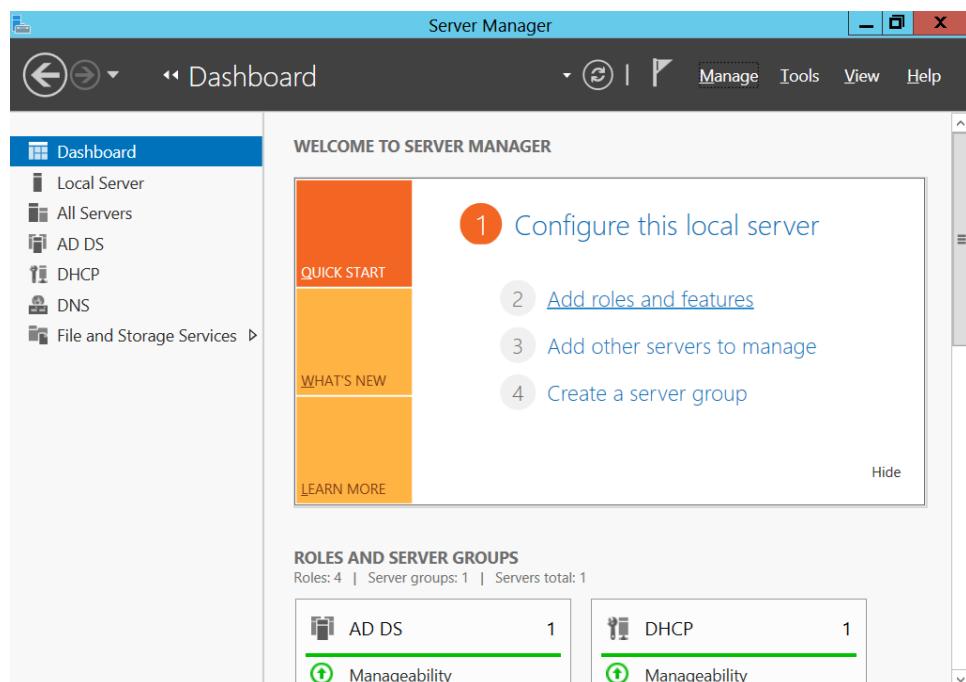
Lab – 1: Installing Windows Deployment Services

SYS1 – CONFIGURATION

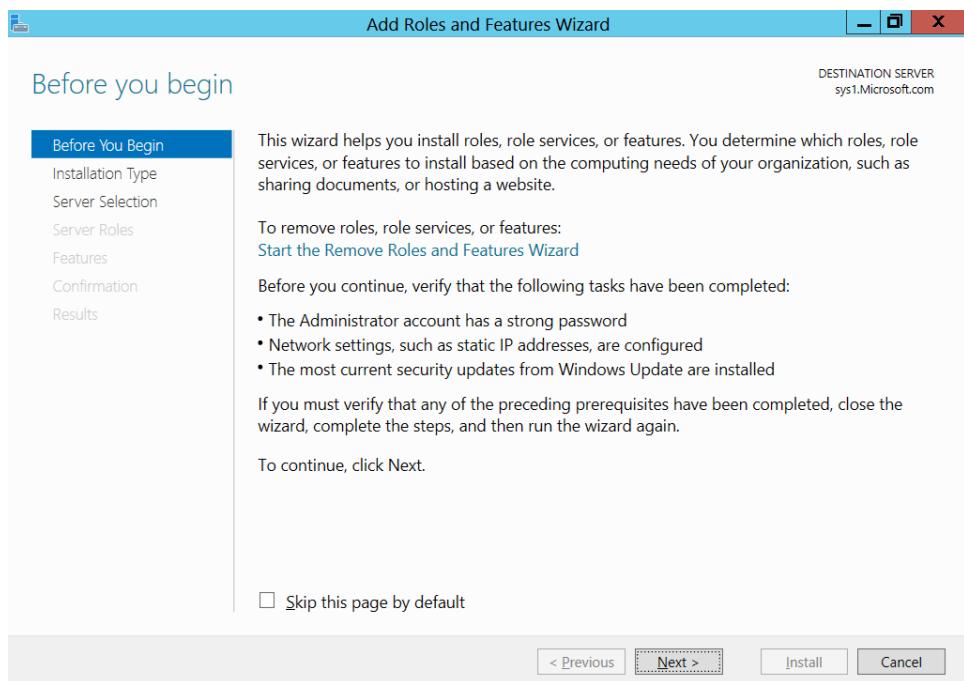
1. Go to Start, click Server Manager



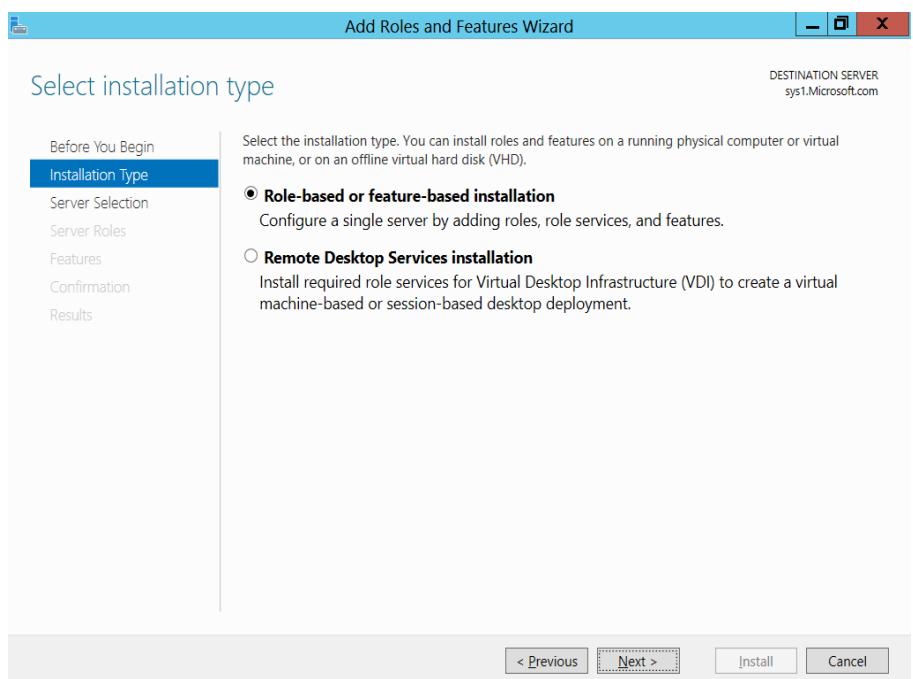
2. In the Server Manager Console, Select **Add roles and features**



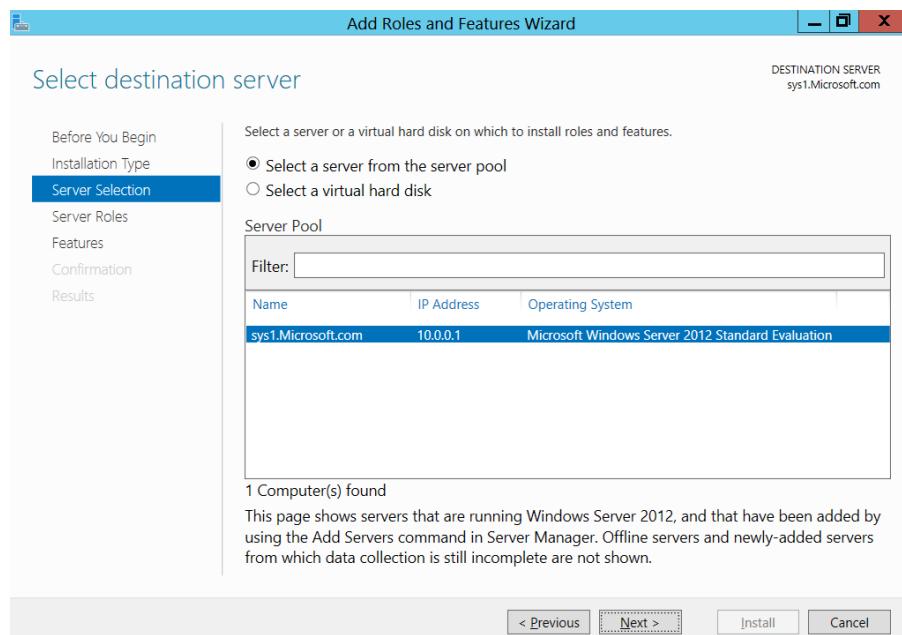
3. In Before you begin page, click **Next**.



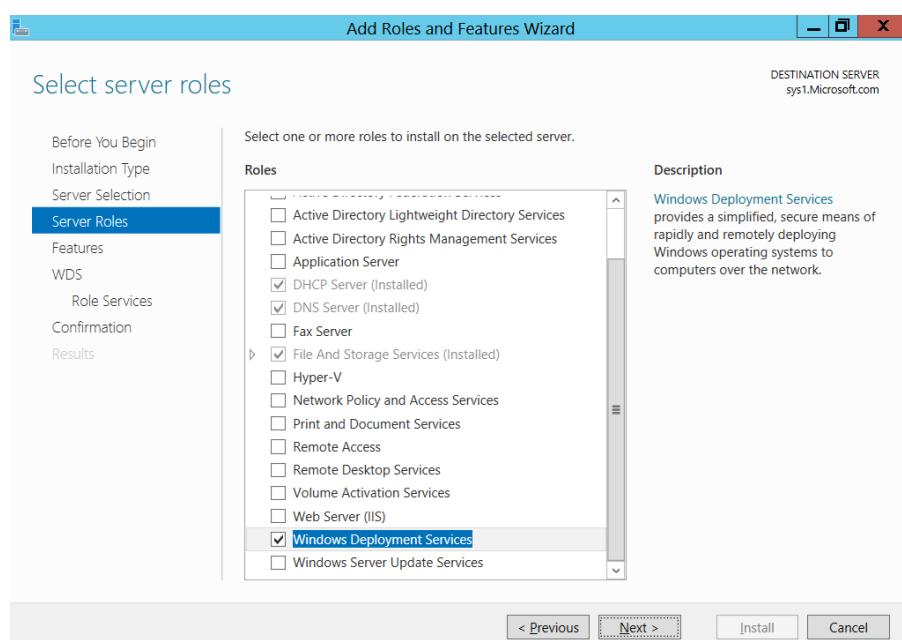
4. Select **Role-based or feature-based installation**, click **Next**.



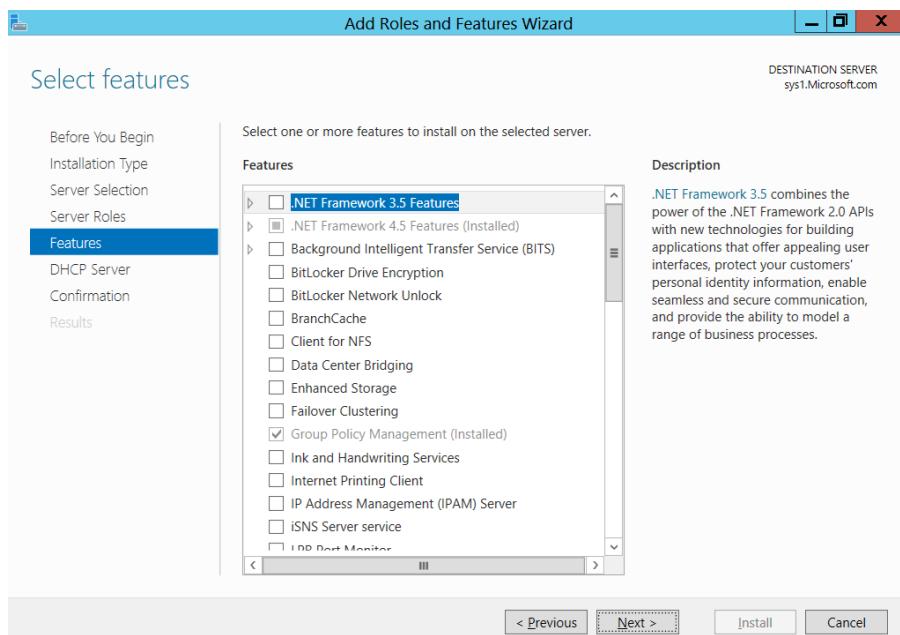
- 5. Select a server (**sys1.Microsoft.com**) from the server pool and click **Next**.**



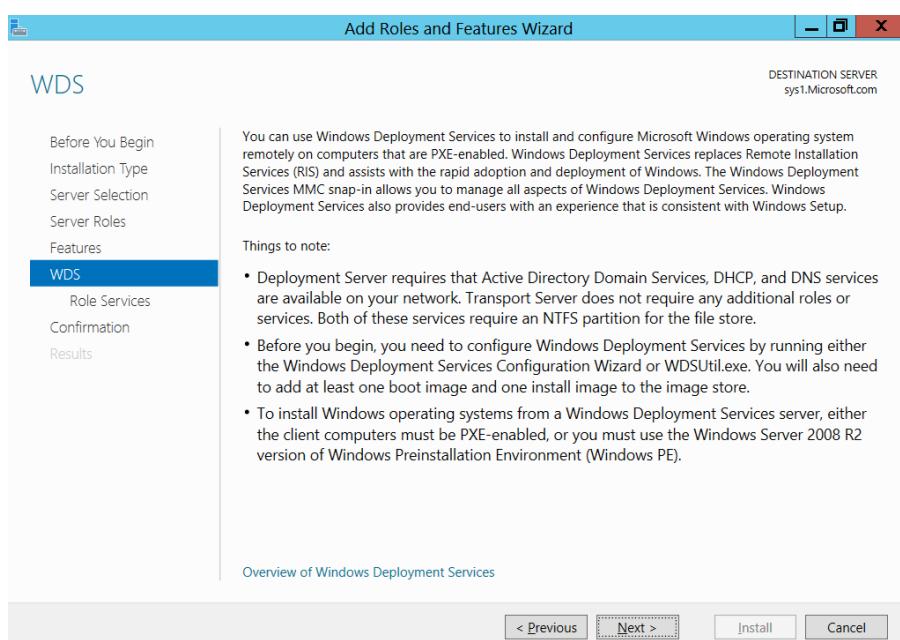
- 6. In select server roles, check the box **Windows Deployment Services**, click **Next**.**



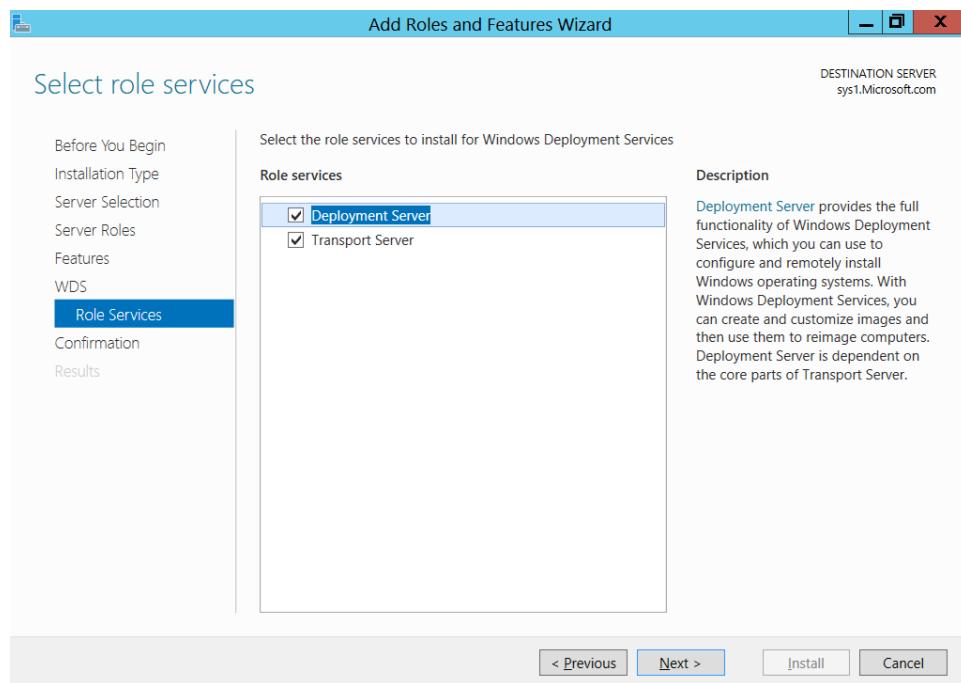
7. In select features, click **Next.**



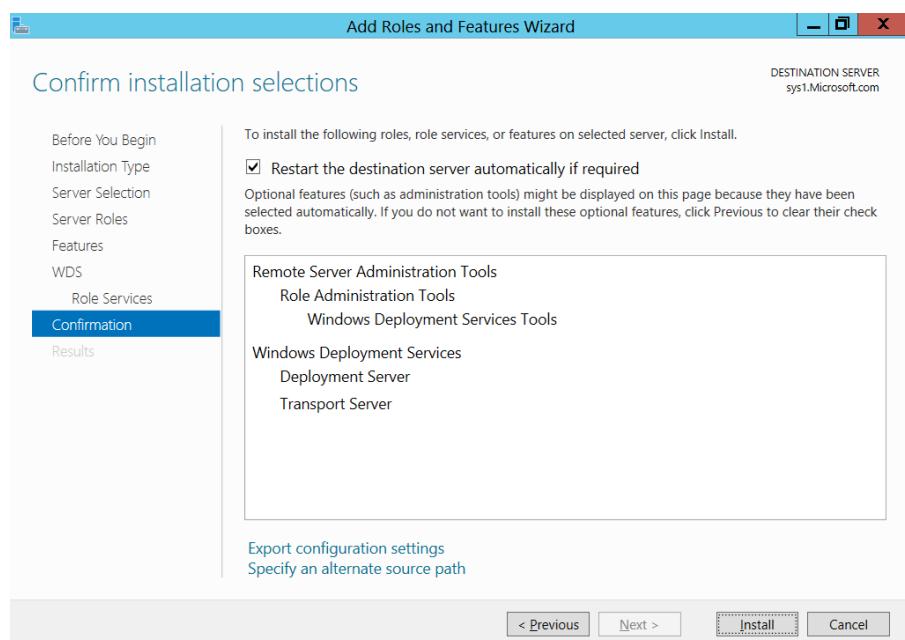
8. Click **Next.**



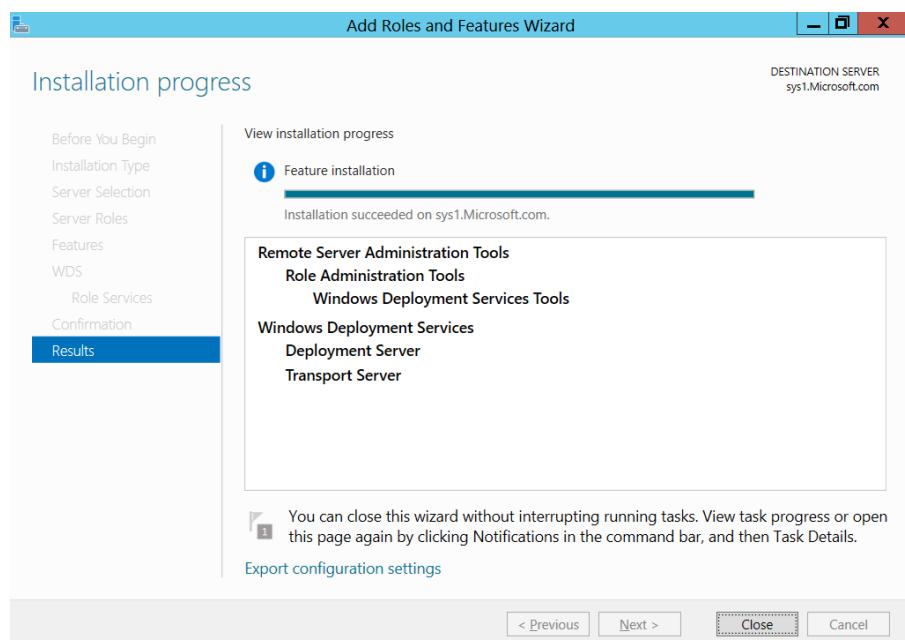
- 9.** In Select role services, Deployment and Transport Server is selected, click **Next**.



- 10.** Check Restart the destination server automatically if required and click **Install**.



11. Click Close to complete the Installation.



Note: SYS1 – CONFIGURATION

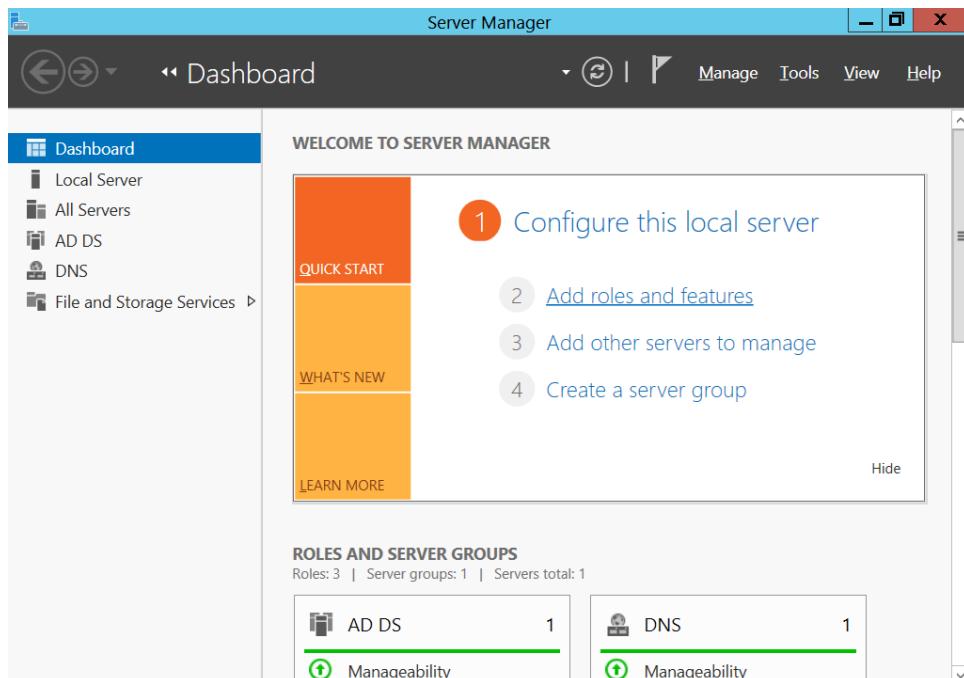
Install the DHCP Service (If not installed) and create a scope in the DHCP.

Give the range (10.0.0.10 – 10.0.0.100), and in the DHCP scope options mention the Domain name (Microsoft.com) and mention the DNS server IP address (10.0.0.1).

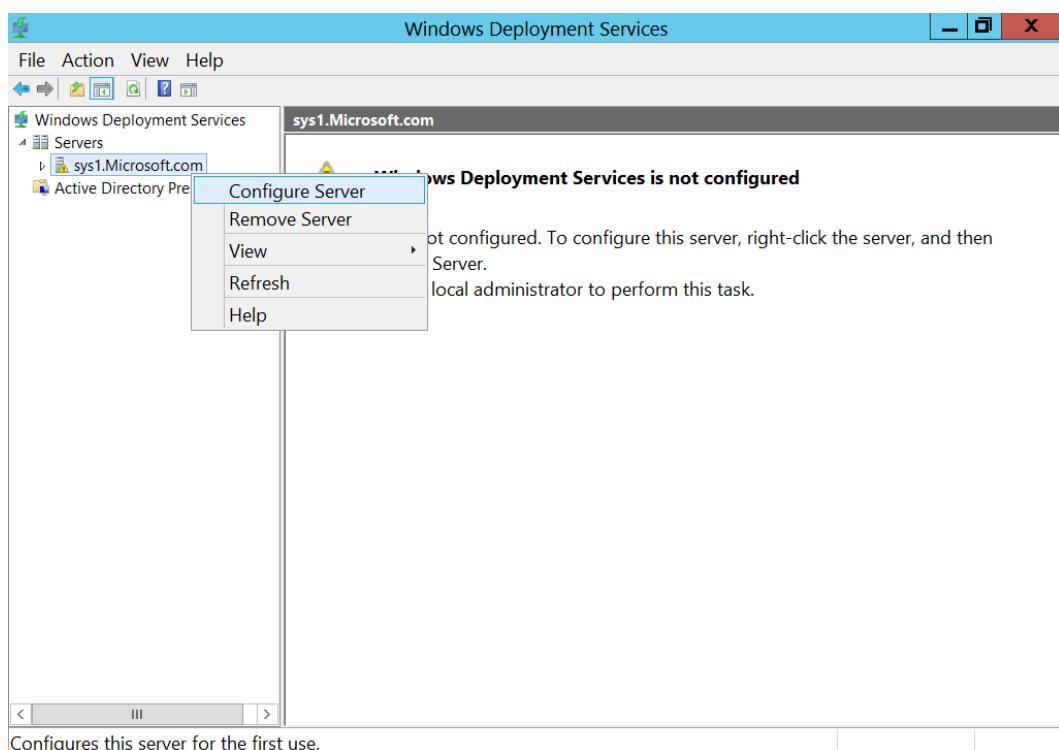
Lab – 2: Configuring Windows Deployment Services

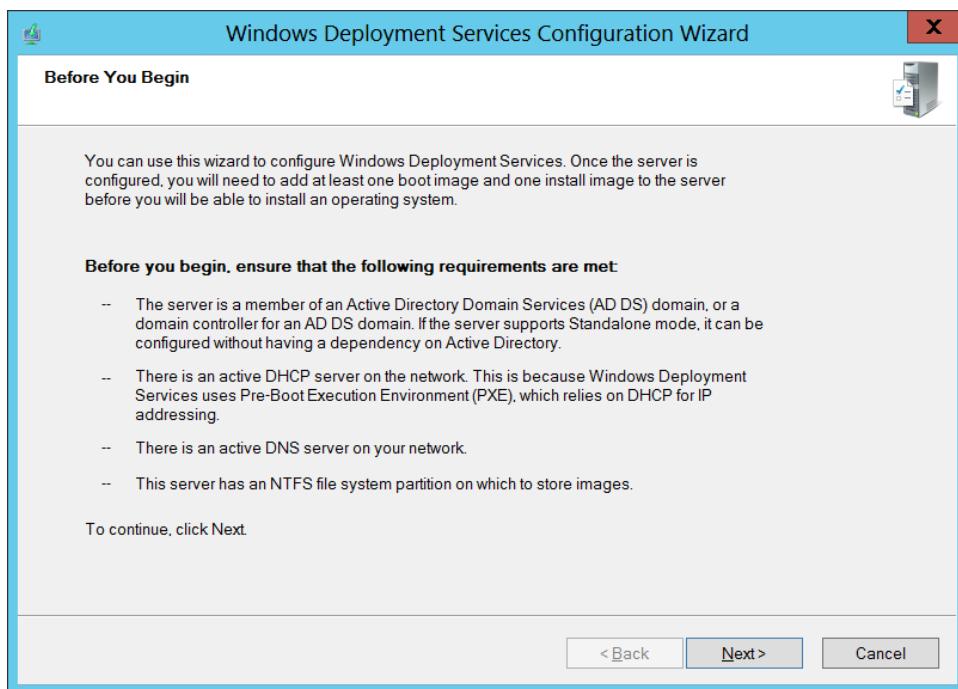
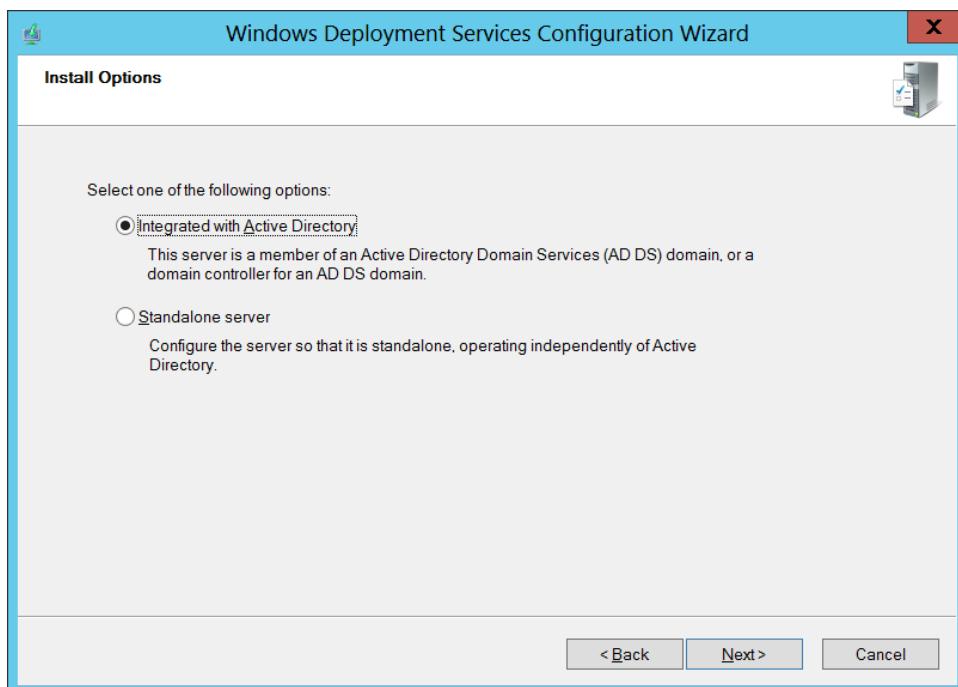
SYS1 – CONFIGURATION

1. Go to Start, select Windows Deployment Services.

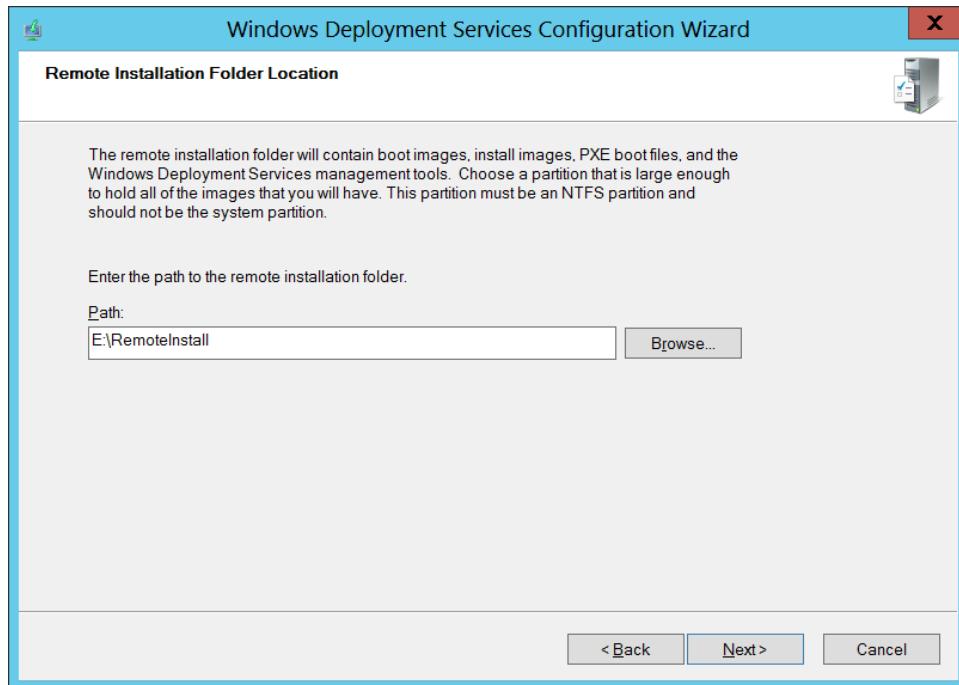


2. Right click Server Name, Select Configure Server.



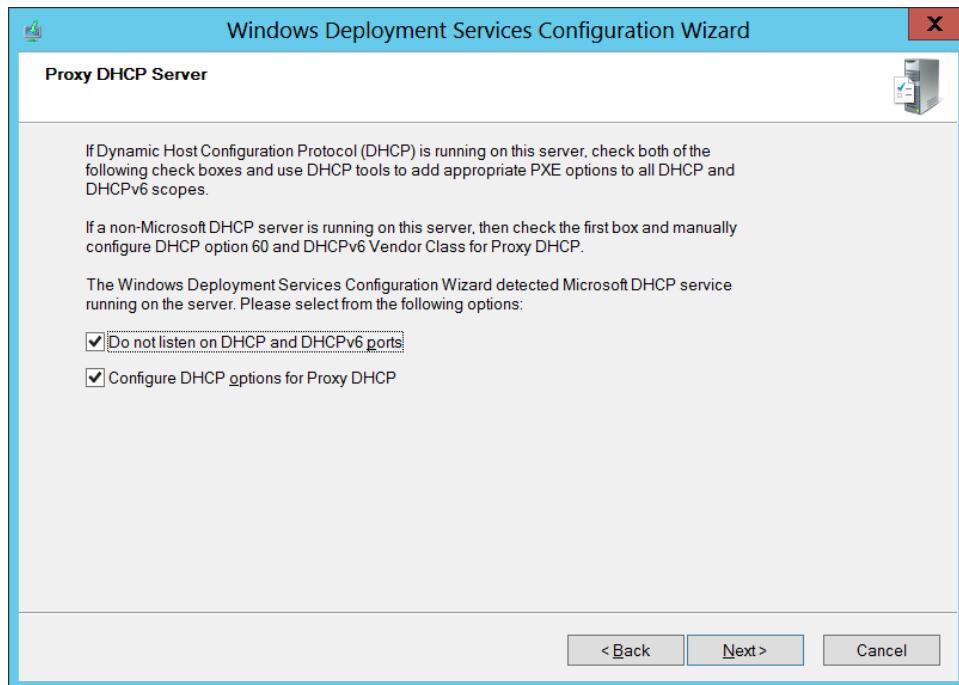
3. In Before You Begin Page, click **Next**.4. In Install Options, in Domain Model select **Integrated with Active Directory**, click **Next**.

5. Browse and select any empty drive to store **Image Folder** (or) change the Drive letter click **Next**.

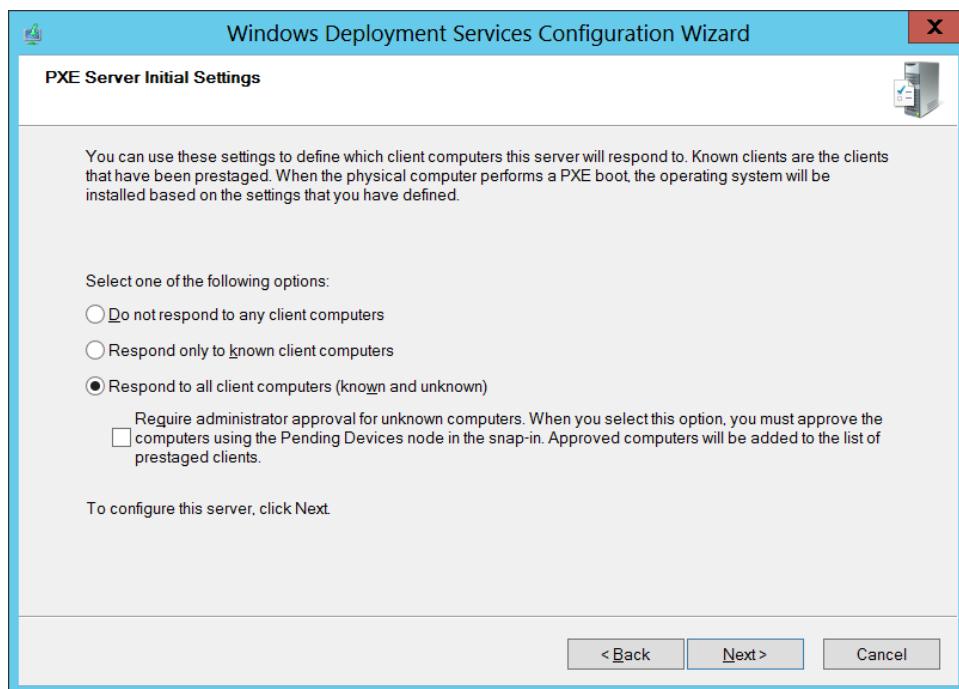


Note: If the WDS server is a DHCP server also then one more wizard will be displayed indicating that the WDS service should not listen on port 67.

So, we have to check the boxes, **Do not listen on port 67** and **Configure DHCP option tag 60 in all DHCP scope options to PXE Client**.



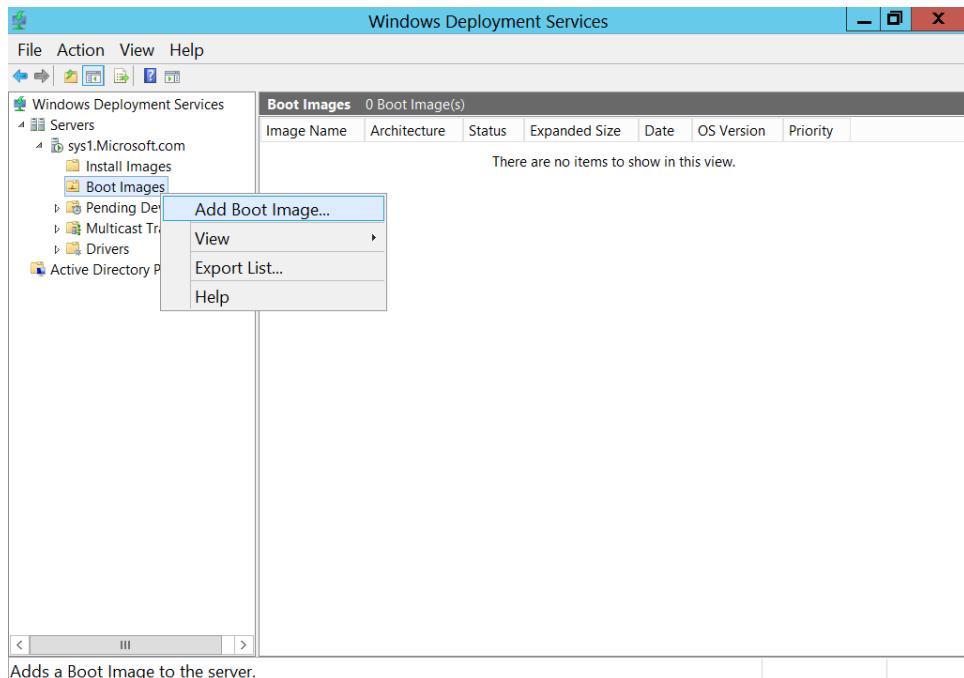
6. Select **Respond to all Known and Unknown Client Computers**, and click **Next**.



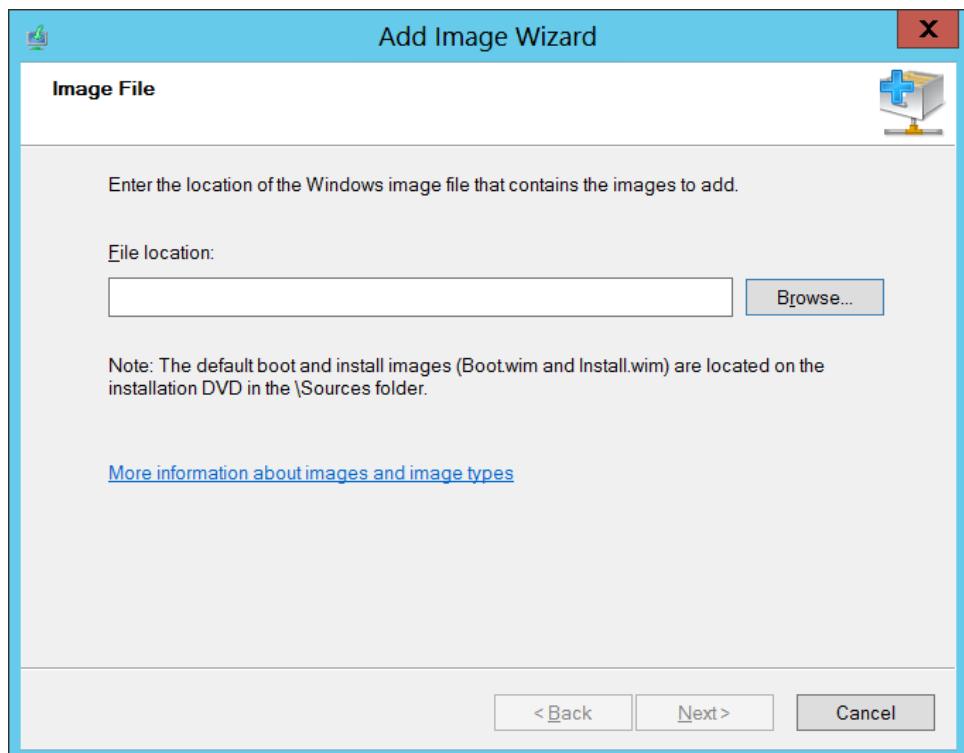
7. Wizard will Configure the **WDS Server**
8. Uncheck the box **Add Images** to Windows Deployment Server now, and **click Finish**.
9. **WDS Server Service** configured successfully and started.

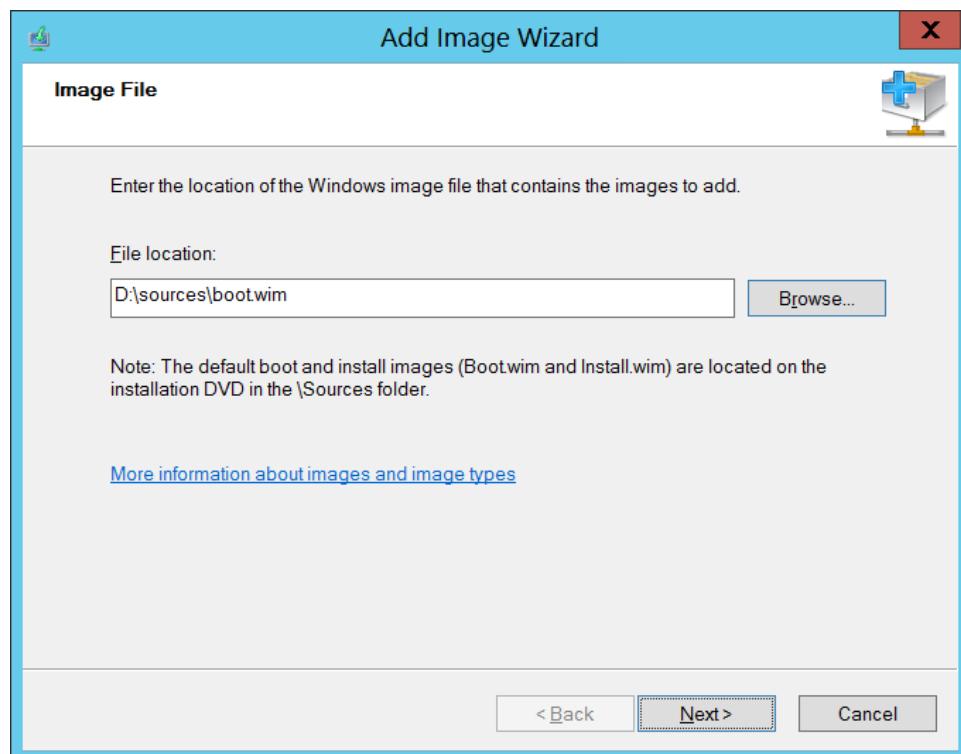
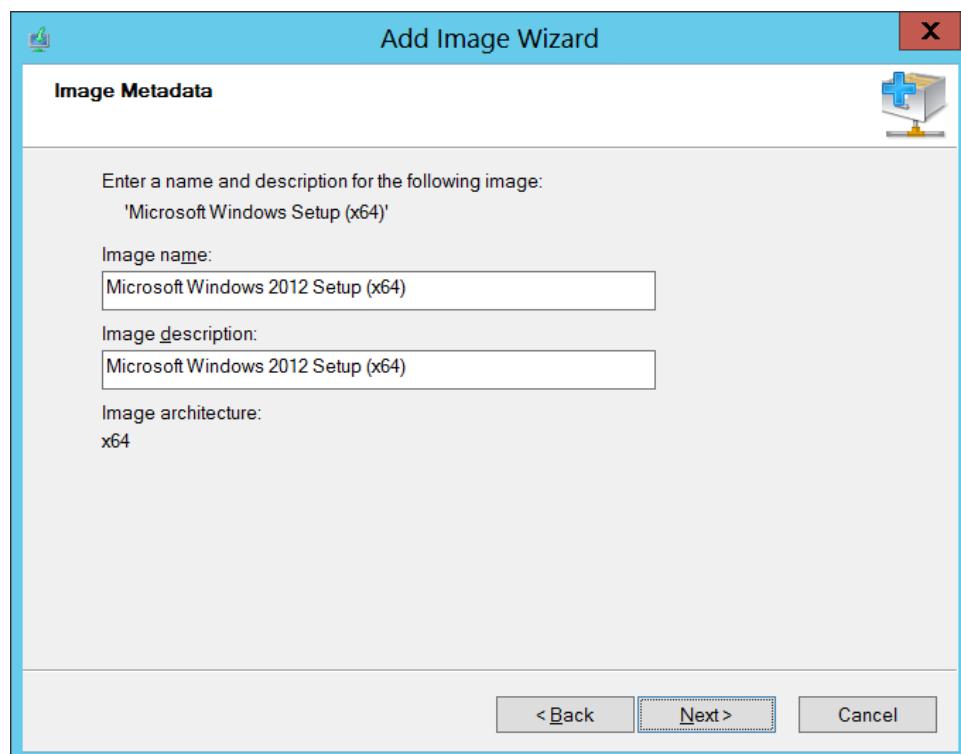
Lab – 3: Adding Windows 2012 Boot Image to WDS Server

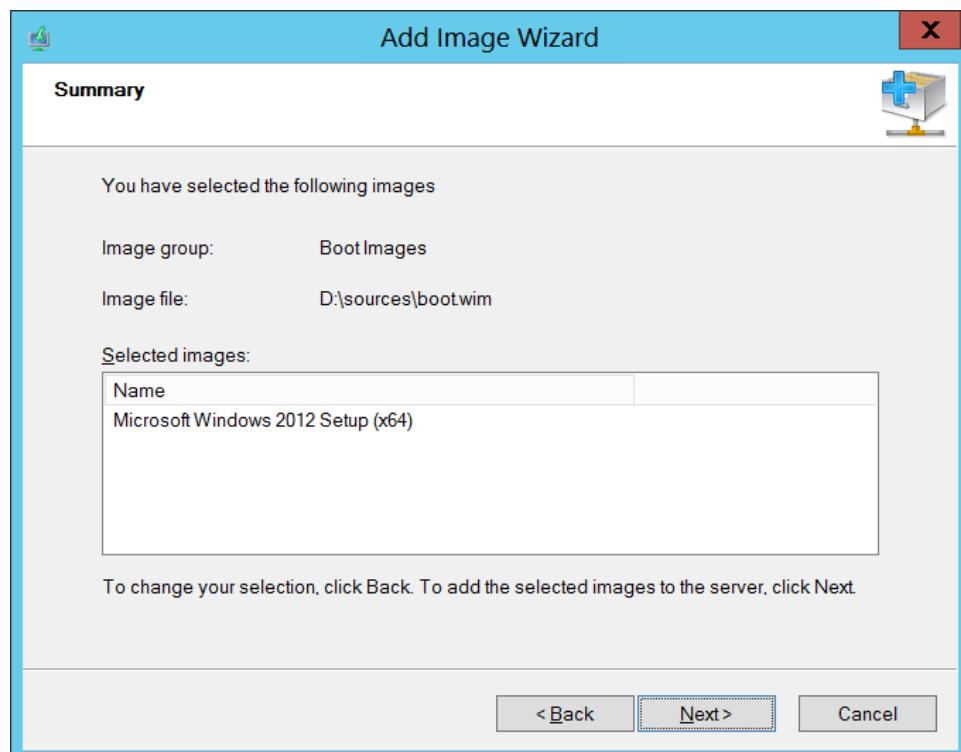
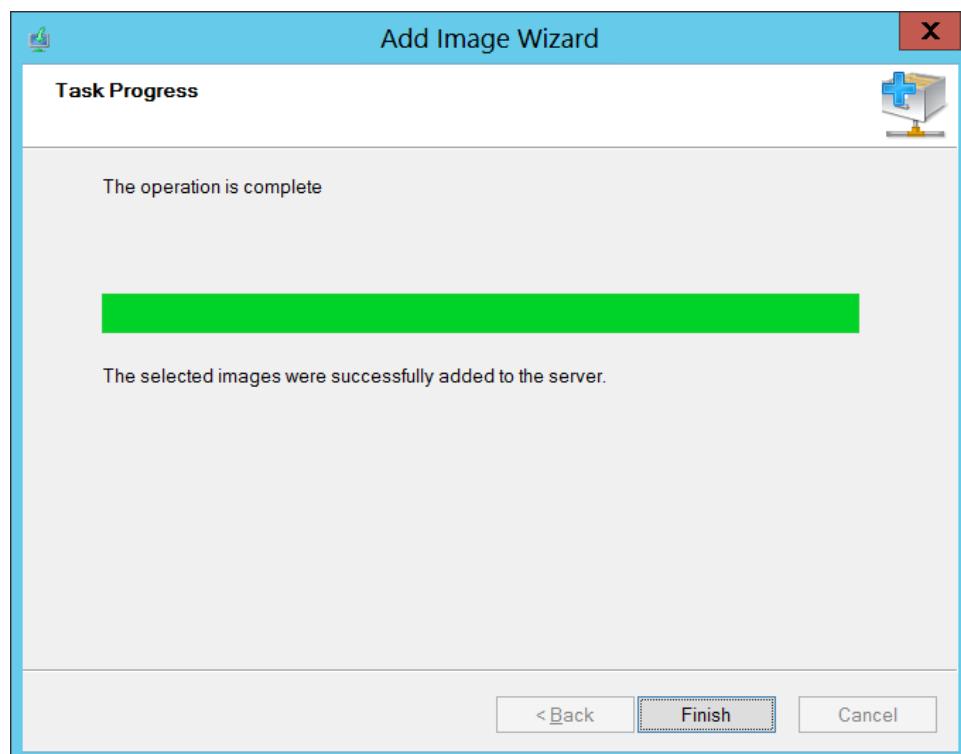
1. Right click Boot Images Select **Add Boot Image**.



2. Browse and Select **boot.wim** file from 2012 OS DVD (Ex: D:\Sources\boot.wim)

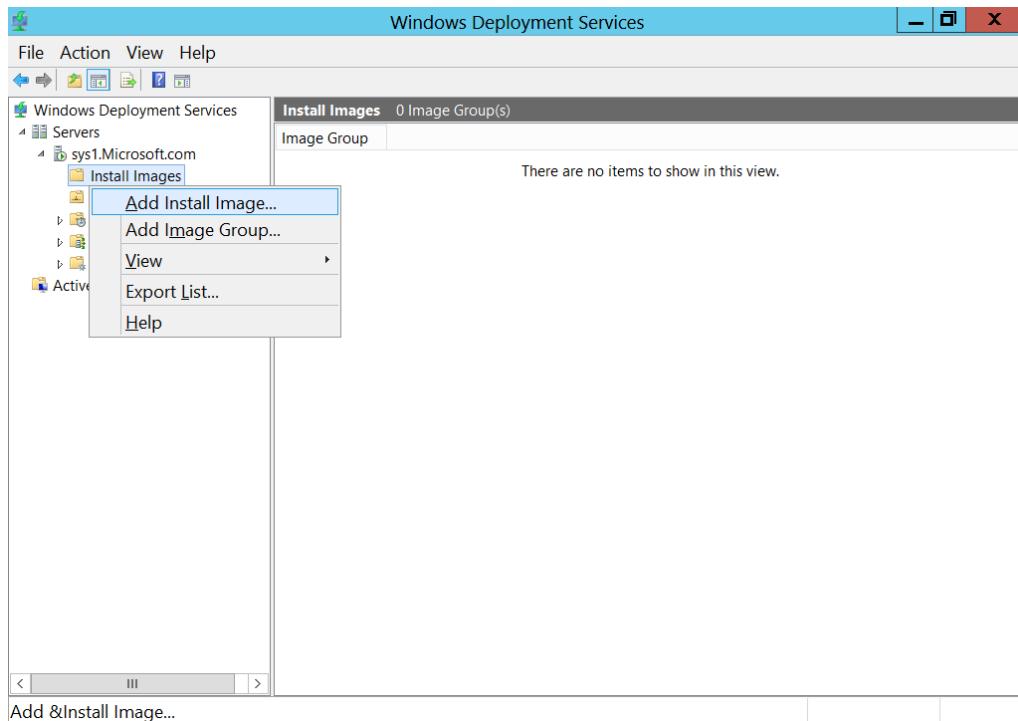


3. Click **Next**.4. Give Name to image Ex: **Windows Server 2012**.

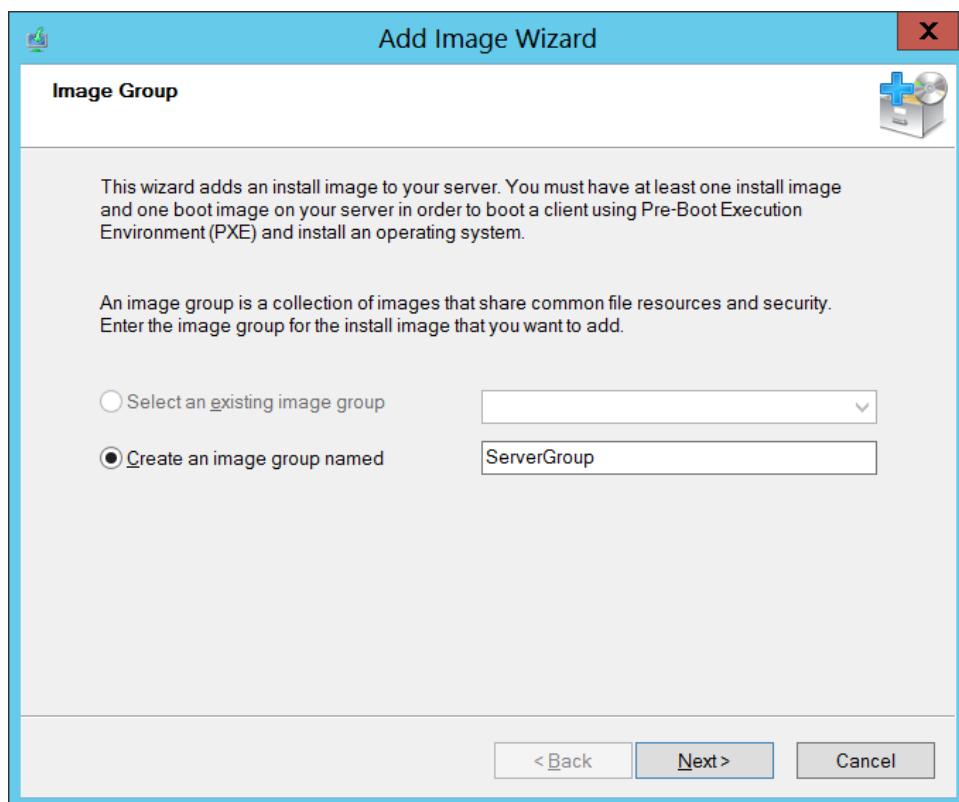
5. Click **Next**.6. Image will be added → click **Finish**.

Lab – 4: Adding Windows2012 Install Image to WDS Server

- Right click Install Images Select **Add Install Image**.

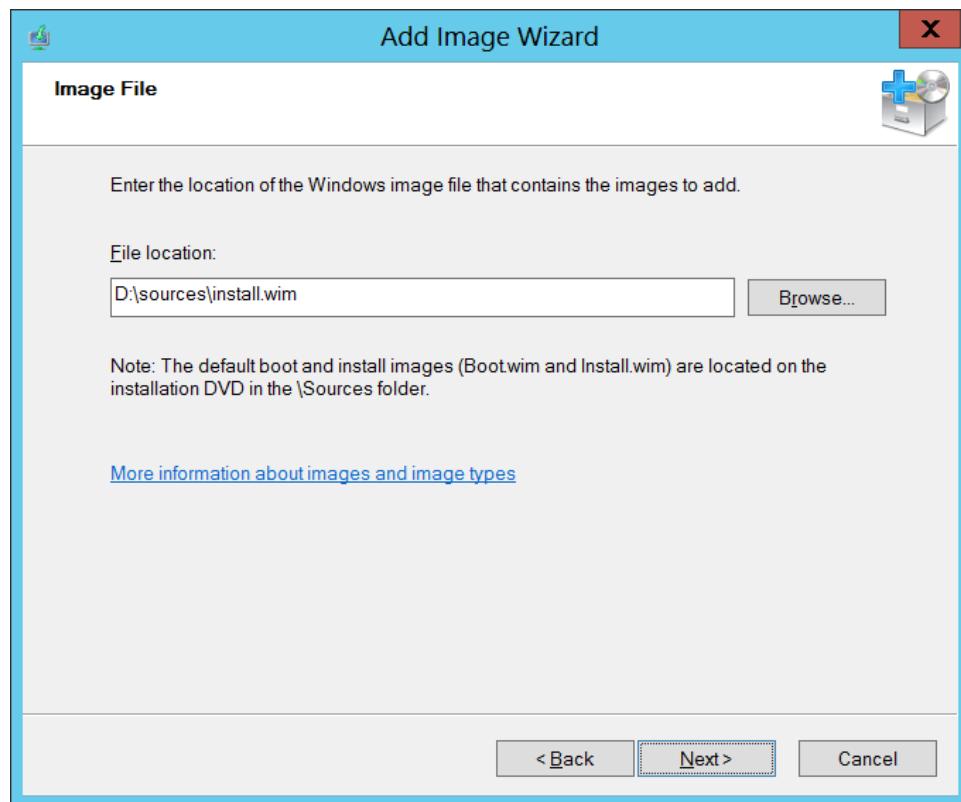


- Give Name to Image Group Ex: **Server Group** and click **Next**.

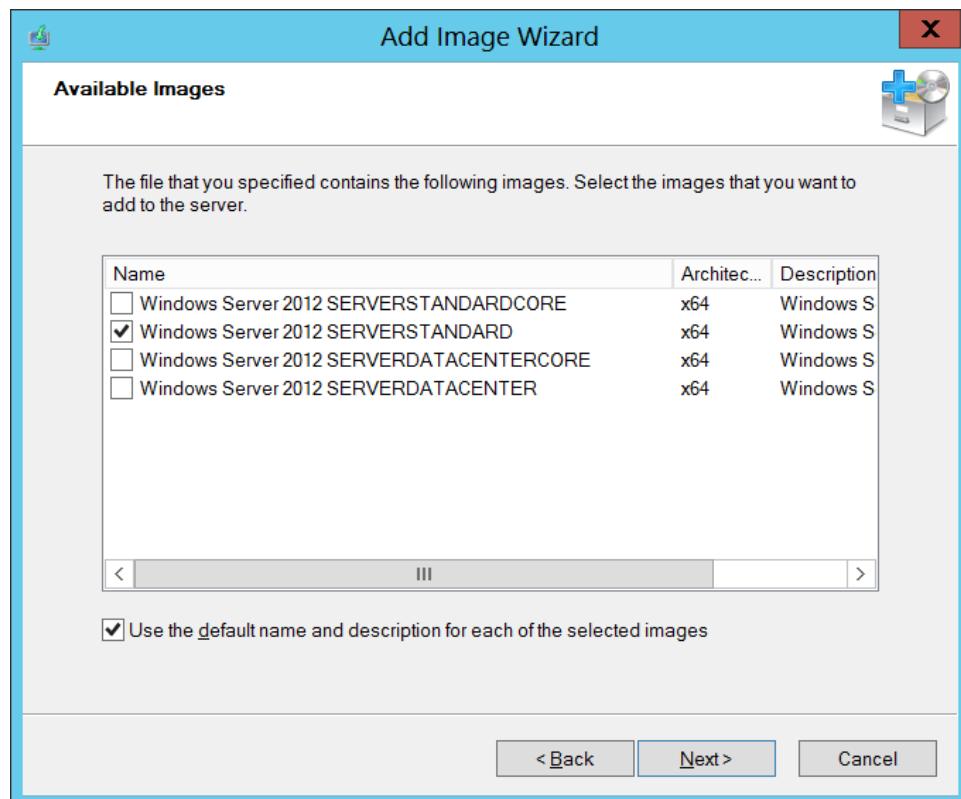


3. Browse and select **Install.wim** file from 2012 OS DVD (Ex: D:\Sources\install.wim)

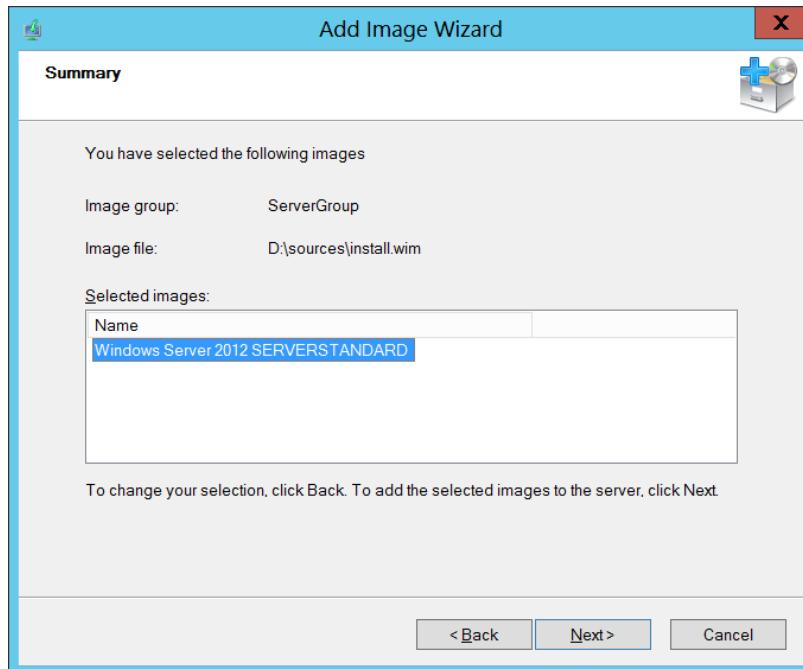
→ click **Next**.



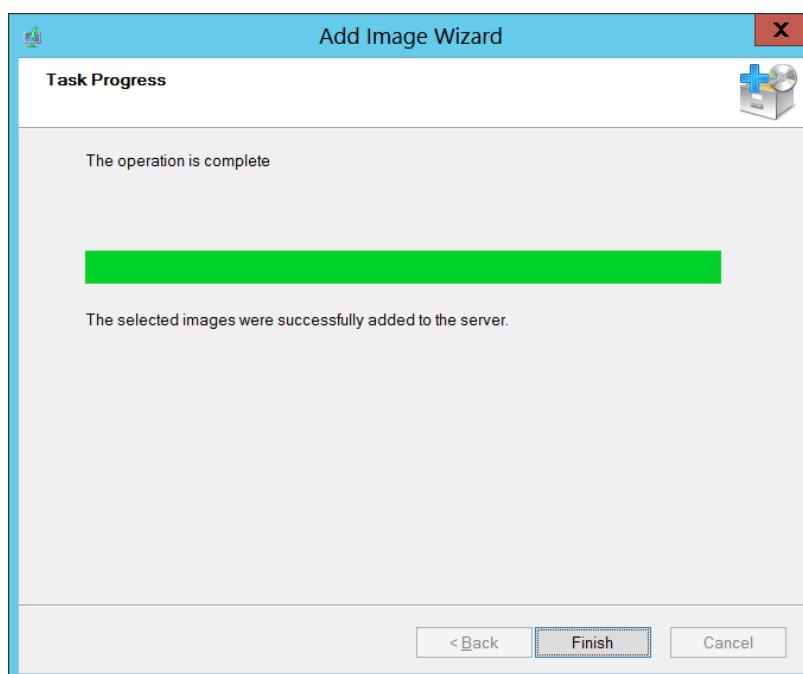
4. Select **Windows Server 2012 STANTARD** and click **Next**.



5. Click **Next**



6. Click **Finish**.



Verification:

1. Boot the **Client system** with **PXE NIC Card**
2. Press **F12key** when prompted to start the **Installation**.
3. Then mention the **Administrator Credential**.
4. Select the Operating System which you want to install.
5. Select the Partition to install the O.S and follow the instructions.

HYPER-V

WINDOWS SERVER 2012

Hyper-V

- Hyper-V is the hardware virtualization role that is available in Windows Server 2012.
- Hardware virtualization provides virtual machines with direct access to the virtualization server's hardware.
- This is in contrast to software virtualization products such as Microsoft Virtual Server 2005 R2, that use the virtualization server's operating system to provide indirect access to the server's hardware.

Type-I Hypervisor

- Also called as bare metal virtualization.
- Hypervisor is directly installed on hardware.
- Robust
- Used in production environment.

Company Name	Hypervisor Name
Microsoft	Hyper-V
VM Ware	vSphere
Citrix	XenServer

Type-II Hypervisors

- Hosted virtualization.
- Slow
- Testing and lab.

Company Name	Hypervisor Name
Microsoft	Virtual PC
VM Ware	Workstation
Oracle	Oracle Virtual Box

Hardware Requirements

- The server must have an x64 platform that supports hardware assisted virtualization and Data Execution Prevention.
- The server must have enough CPU capacity to meet the requirements of the guest virtual machines.
 - A virtual machine hosted on Hyper-V in Windows Server 2012 can support up to 64 virtual processor

Hardware Requirements

- The server must have enough memory to support all of the virtual machines that must run concurrently, plus enough memory to run the host Windows Server 2012 operating system.
 - The server must have at least 4 GB of RAM.
 - A virtual machine hosted on Hyper-V in Windows Server 2012 can support a maximum of 1 terabytes (TB) of RAM

Hardware Requirements

- The storage subsystem performance must meet the input/output (I/O) needs of the guest virtual machines. Whether deployed locally or on storage area networks (SANs), you may have to place different virtual machines on separate physical disks, or you may have to deploy a high performance redundant array of independent disks (RAID), solid-state drives (SSD), hybrid-SSD, or a combination of all

Hardware Requirements

- The virtualization server's network adapters must be able to support the network throughput needs of the guest virtual machines. You can improve network performance by installing multiple network adapters and using multiple Network Interface Cards (NICs).

Virtual Machine Hardware

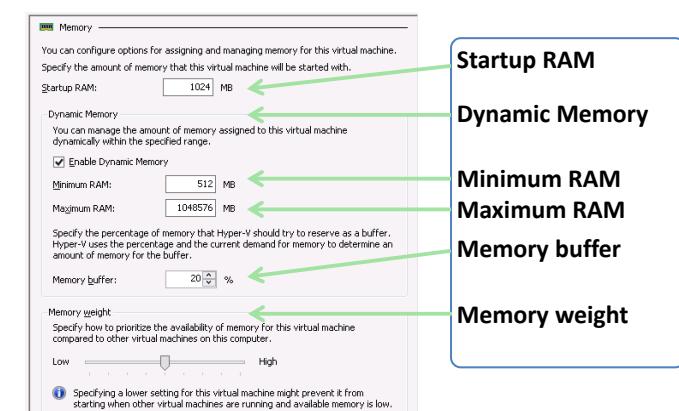
Virtual machines have the following simulated hardware by default:

- BIOS
- Memory
- Processor
- IDE Controller 0 and 1
- SCSI Controller
- Synthetic Network Adapter
- COM 1 and 2
- Diskette Drive

You can add the following hardware to a virtual machine:

- SCSI Controller (up to 4)
- Network Adapter
- Legacy Network Adapter
- Fibre Channel adapter
- RemoteFX 3D video adapter

Dynamic Memory for Virtual Machines



What Is a VHD?

- A virtual hard disk is a file that represents a traditional hard disk drive
- VHDX format has the following benefits over the VHD format:
 - The disks can be larger (64 TB versus 2 TB)
 - The disk is less likely to become corrupted
 - The format supports better alignment when deployed to a large sector disk
 - The format supports larger block size for dynamic and differencing disks

Creating Virtual Disk Types

- Dynamically expanding VHDs
- Fixed-size VHDs
- Differencing VHDs
- Pass Through Disks

Pass Through Disks

- Hyper-V allows virtual machines to access storage mapped directly to the Hyper-V server without requiring the volume be configured.
- The storage can either be a physical disk internal to the Hyper-V server or it can be a Storage Area Network (SAN) Logical Unit (LUN) mapped to the Hyper-V server.
- To ensure the Guest has exclusive access to the storage, it must be placed in an Offline state from the Hyper-V server perspective.

Differencing VHDs

- Differencing disks reduce space used by storage at the cost of performance
- You can link multiple differencing disks to a single parent disk
- You cannot modify parent disk
- You can use Inspect Disk tool to reconnect a differencing disk to a missing parent

Virtual Switch

- External
Used to map a network to a specific network adapter or network adapter team
- Internal
Used to communicate between the virtual machines on the host and between the virtual machines and the host itself
- Private
Used to communicate between virtual machines, but not between the virtual machines and the host itself

Hyper-V Replica

- With Hyper-V Replica, administrators can replicate their Hyper-V virtual machines from one Hyper-V host at a primary site to another Hyper-V host at the Replica site.
- Additionally, administrators can use Hyper-V Replica to test the Replica virtual machine without disrupting the ongoing replication. If a failure occurs at the primary site, administrators can quickly restore their business operations by bringing up the replicated virtual machine at the Replica site.

Prerequisites for Hyper-V Replica

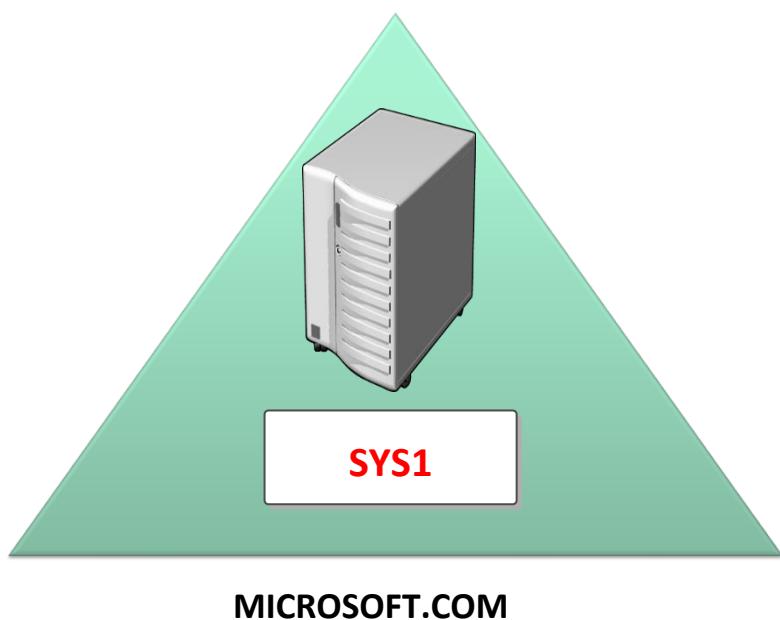
- Windows Server 2012 with Hyper-V role
 - Hyper-V Replica is part of the Hyper-V role
 - At least two servers, usually in different sites
- Sufficient storage to host virtual machines
 - Local and replicated virtual machines
- Connectivity between primary and replica sites
- Windows firewall configured to allow replication
 - Hyper-V Replica HTTP and Hyper-V Replica HTTPS
- X.509v3 certificate for mutual authentication
 - If certificate authentication is used
 - Otherwise, Hyper-V hosts must be in the same AD DS forest

HYPER – V

Pre-requisites:

Before working on this lab, you must have

2. A Computer with Windows Server 2012 Operating System and connected in the network.



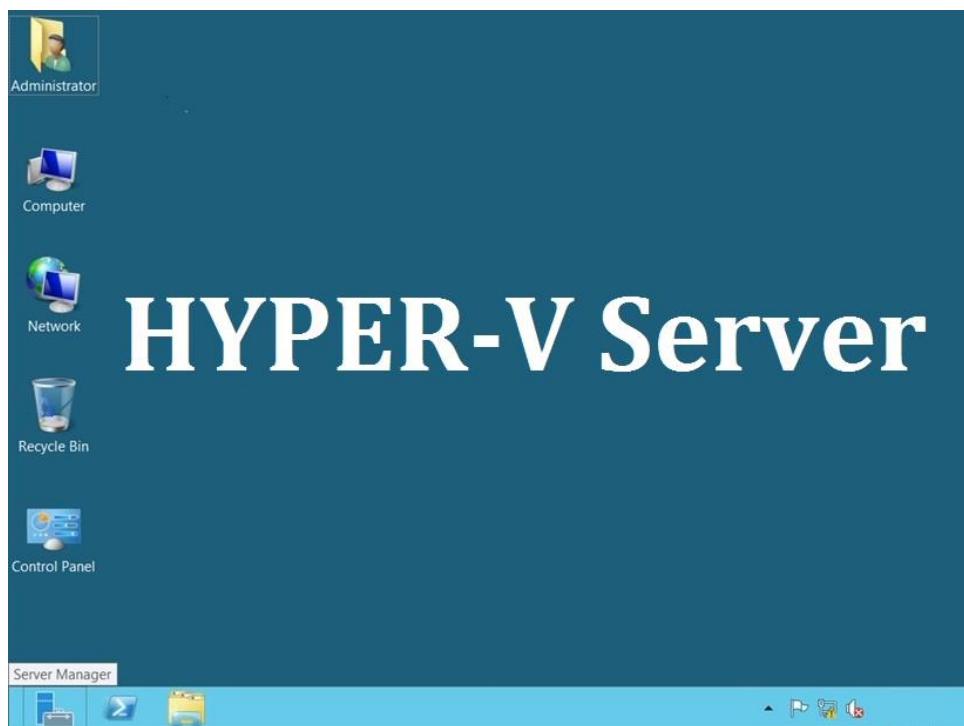
SYS1

Domain Controller

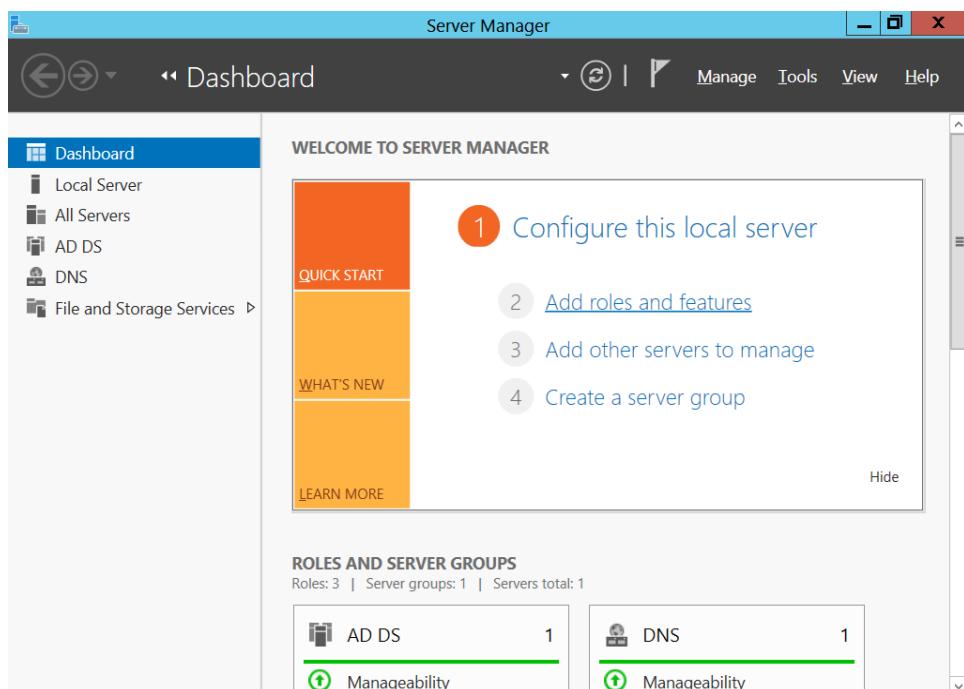
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1

Lab – 1: Installation of HYPER – V

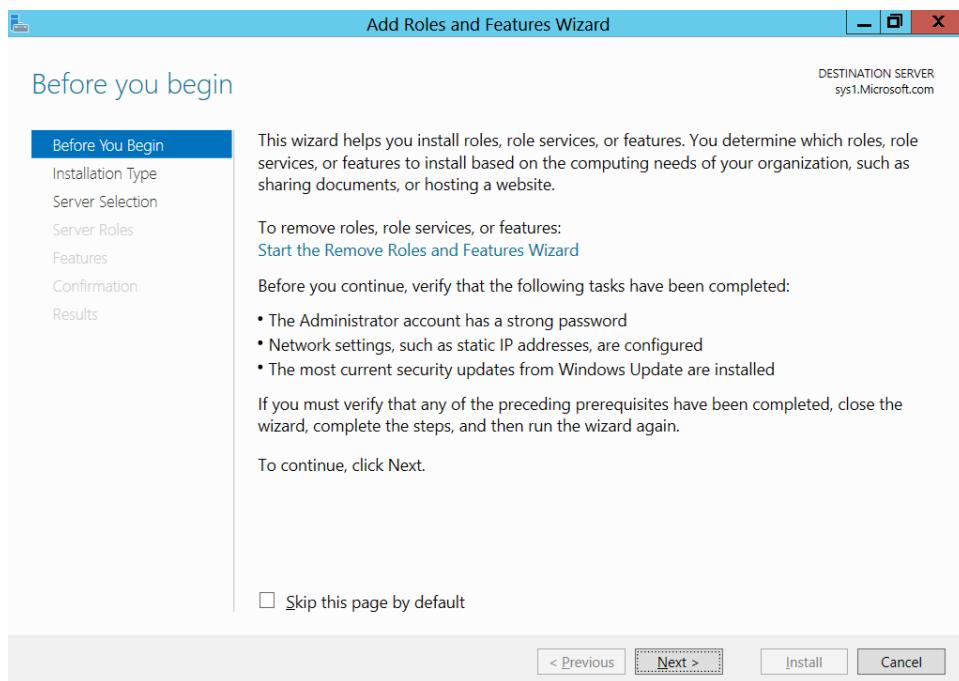
9. Click **Server Manager**.



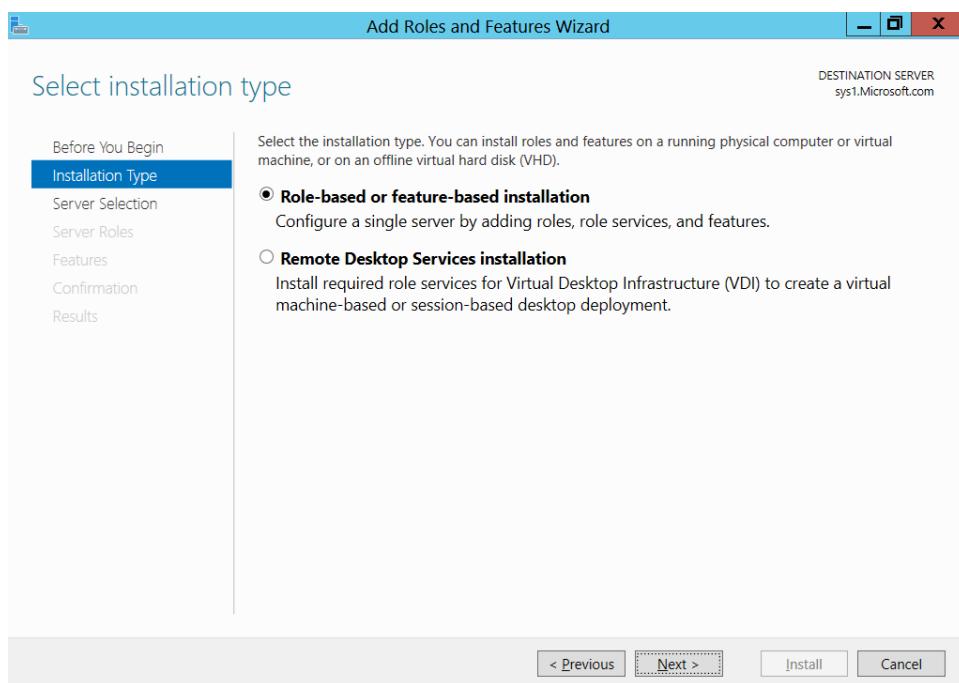
10. In Server Manager Dashboard, Click **Add roles and features**.



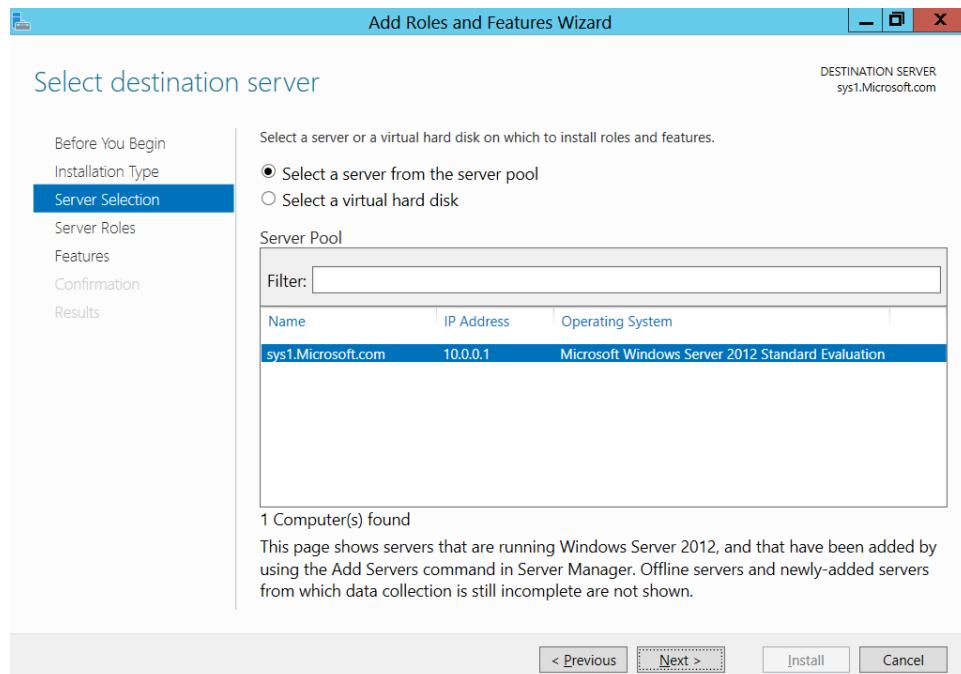
11. In Before you begin page, click **Next**.



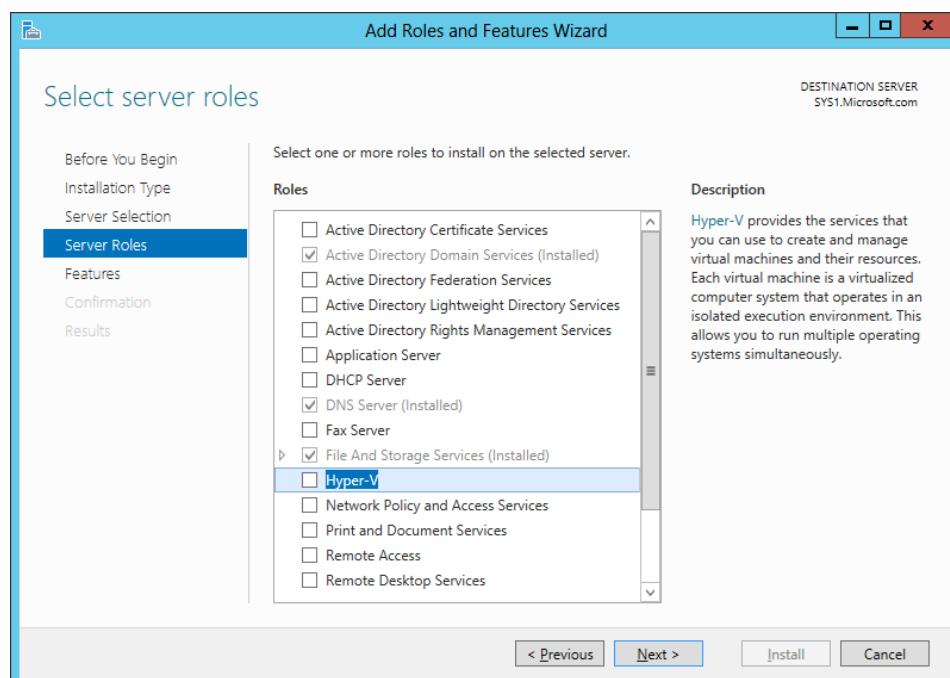
12. In Select installation type, select **Role-based or feature-based installation**, click **Next**.



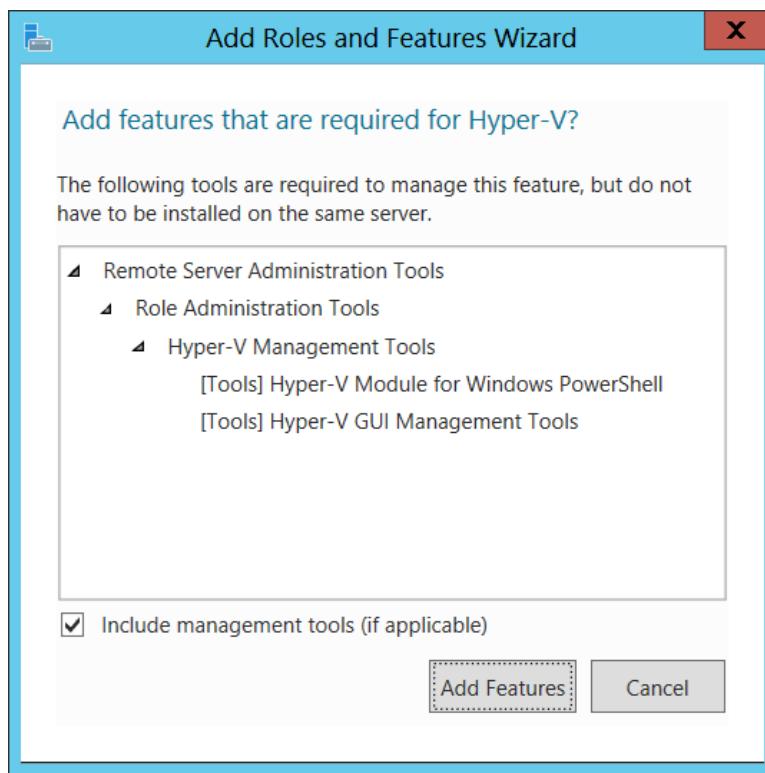
13. In Select destination server, from Server Pool select **SYS1.Microsoft.com**, click **Next**.



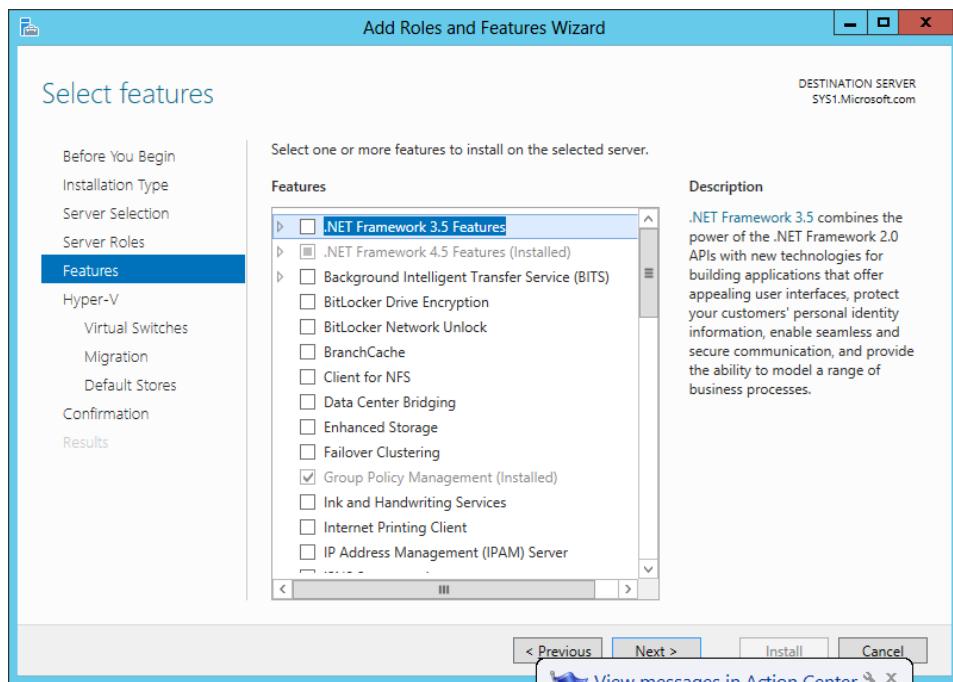
14. In Roles, check the box **Hyper-V**.



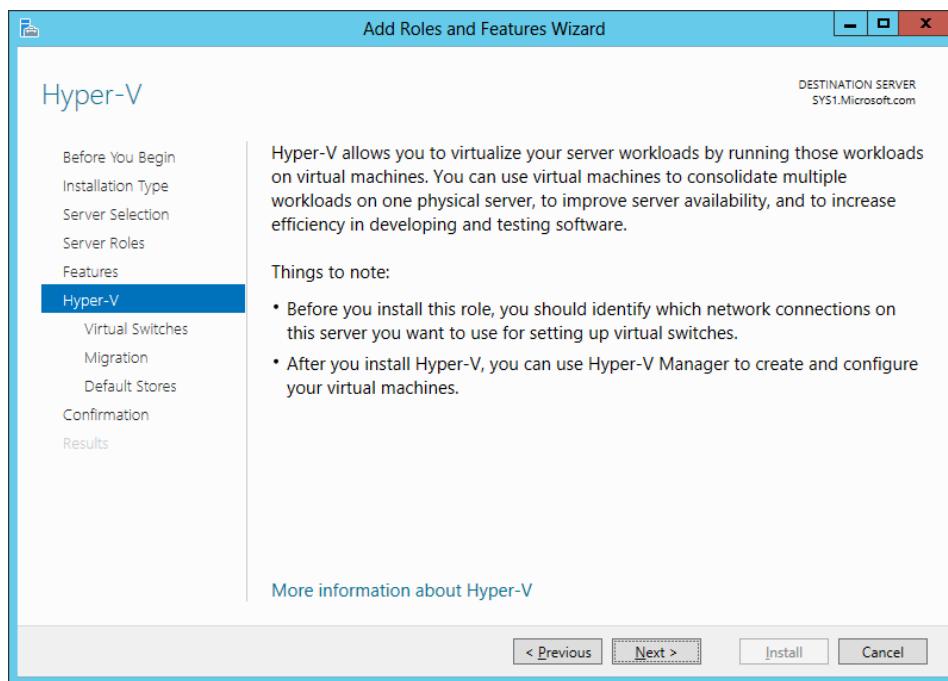
15. Click **Add Features**, to install the required features for Hyper-V. Click **Next**.



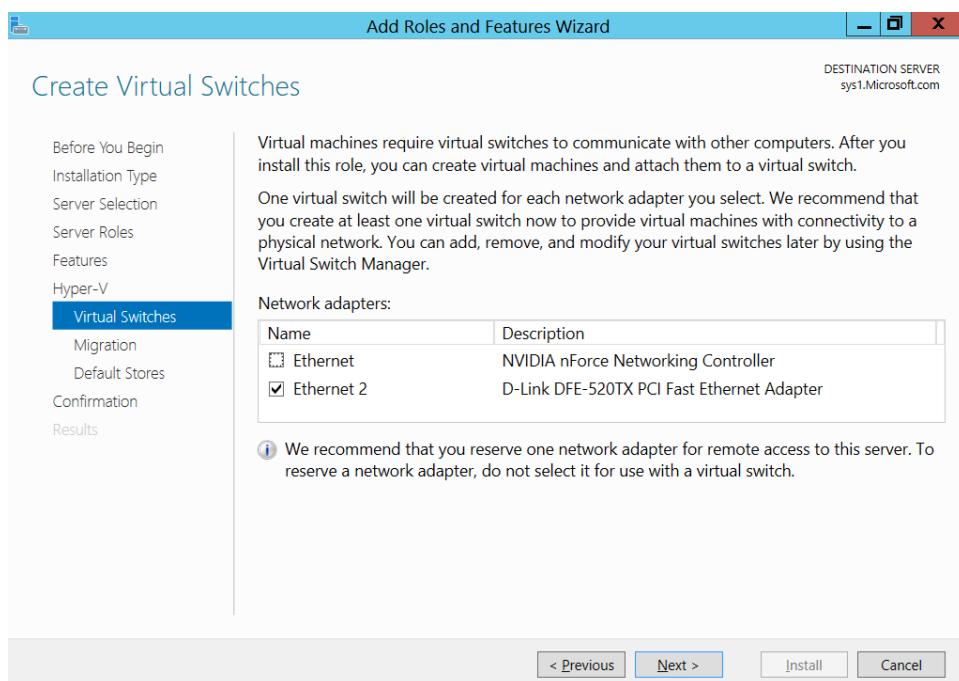
16. In Select features wizard, click **Next**.

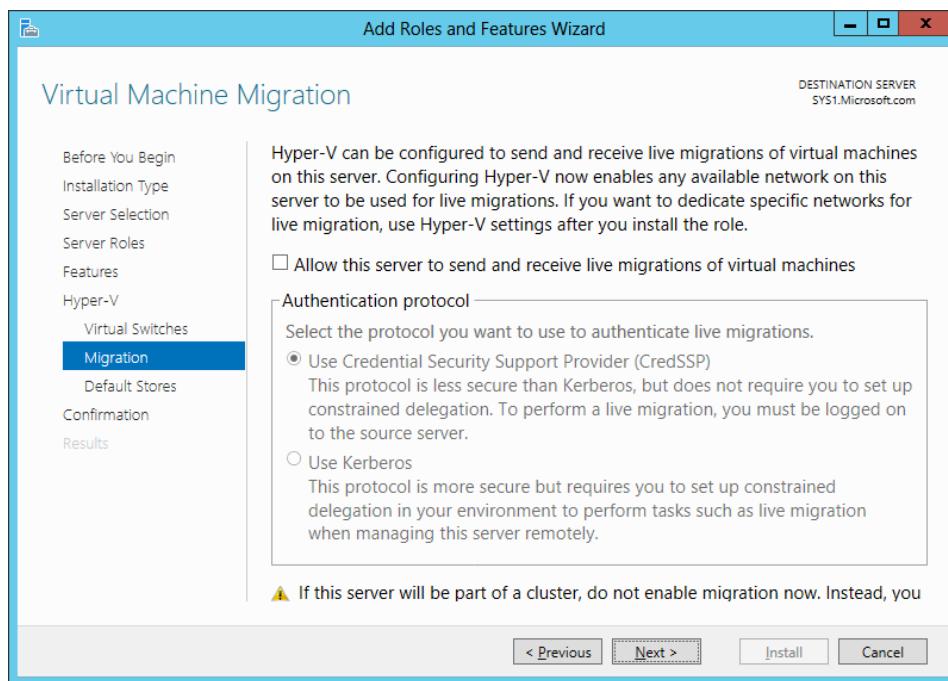
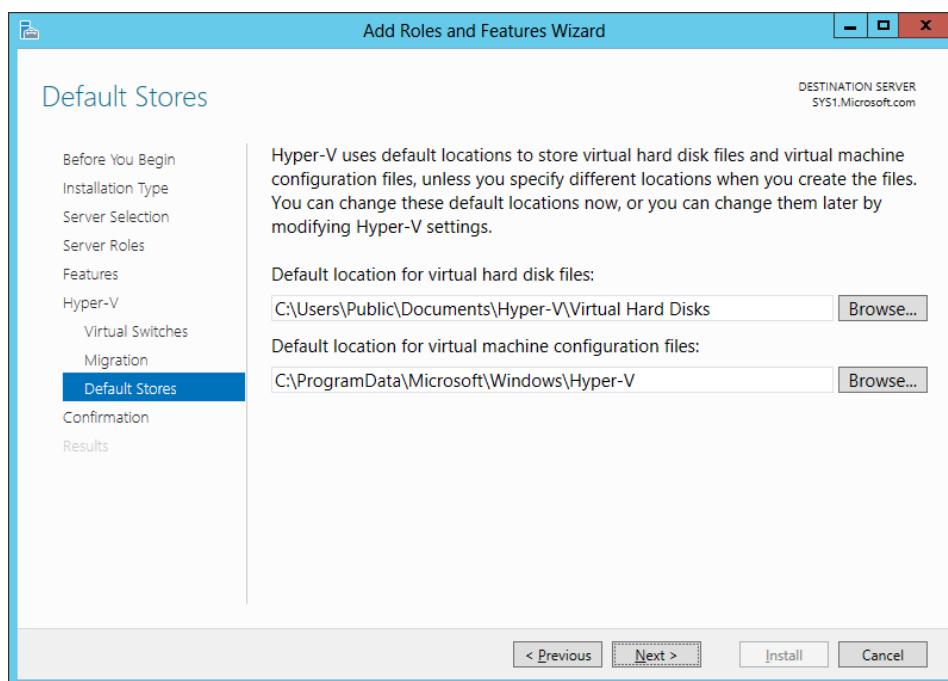


17. In Hyper-V wizard, click Next.

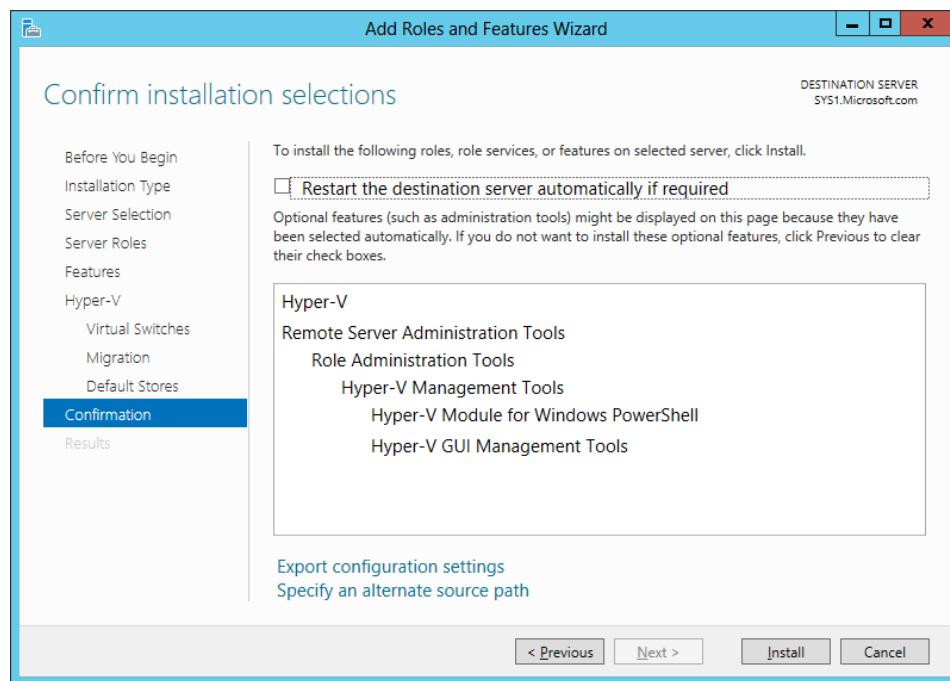


18. Check the box **Ethernet 2 to work as Virtual Switch. Click Next.**



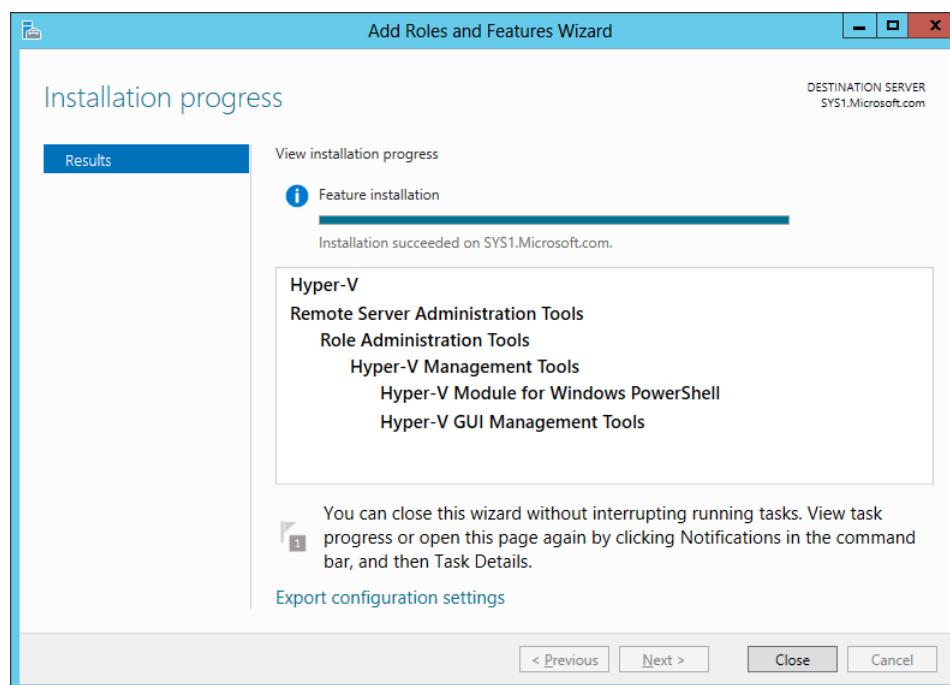
19. In Virtual Machine Migration Page, click **Next**.20. In Default Stores Page, click **Next**.

21. Check box Restart the destination server automatically if required, click **Install**.



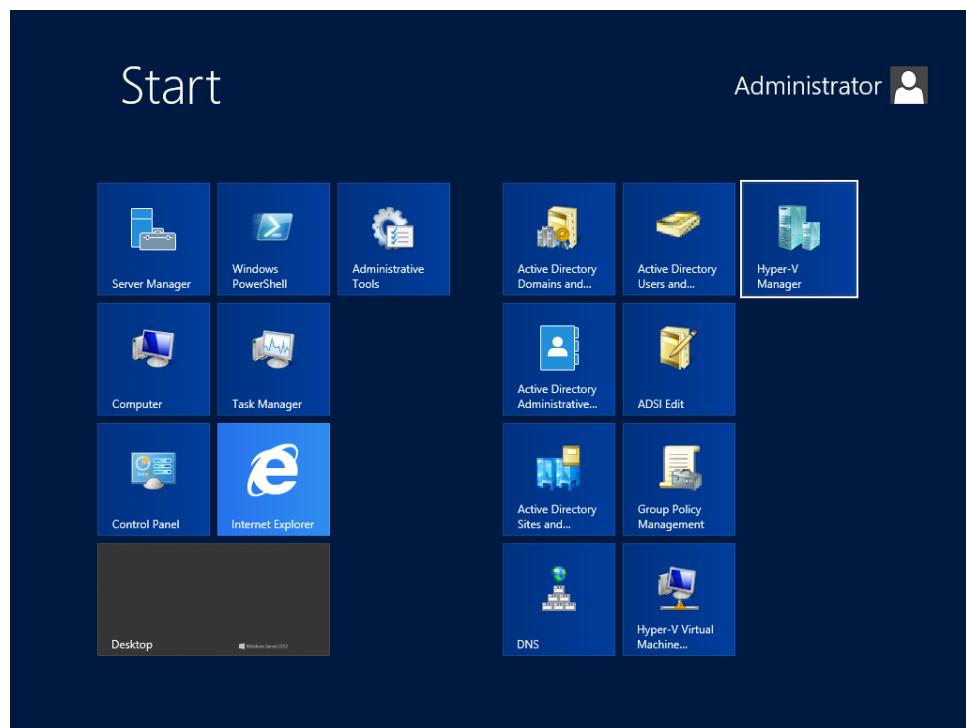
22. Computer Restarts and completes the installation of Hyper-V Role.

23. Click **Close**.

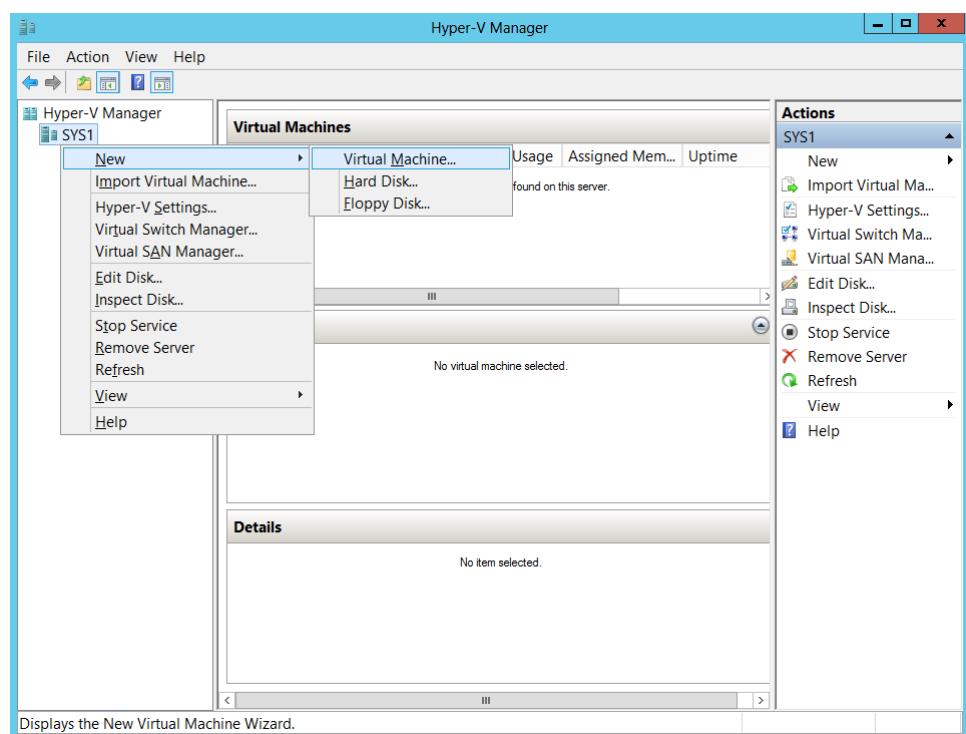


Lab – 2: Creating Virtual Machine on Hyper-V

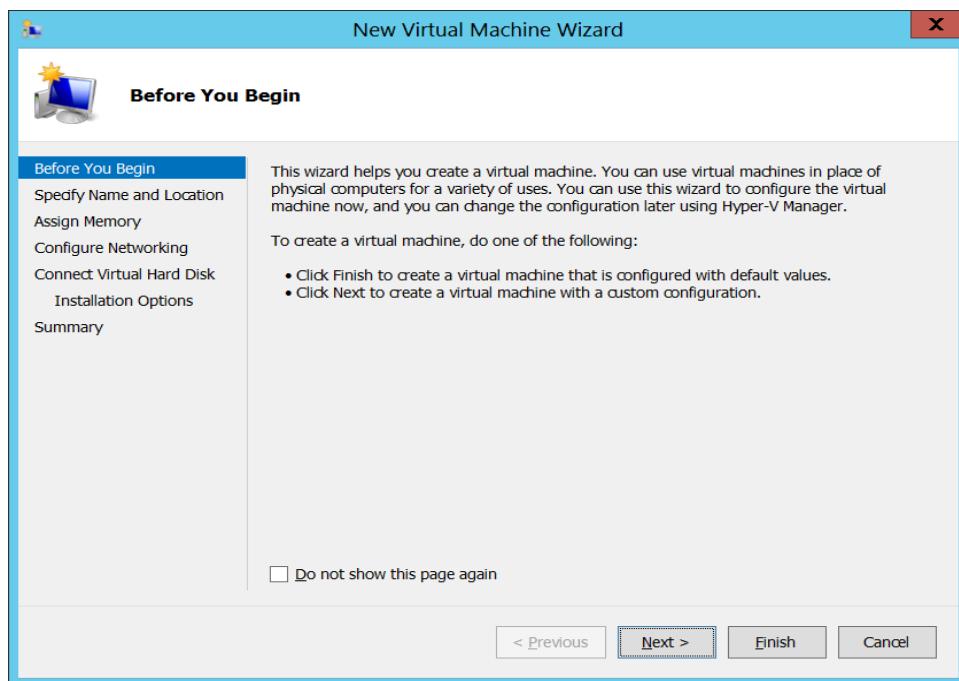
1. Go to Start, select **Hyper-V Manager**.



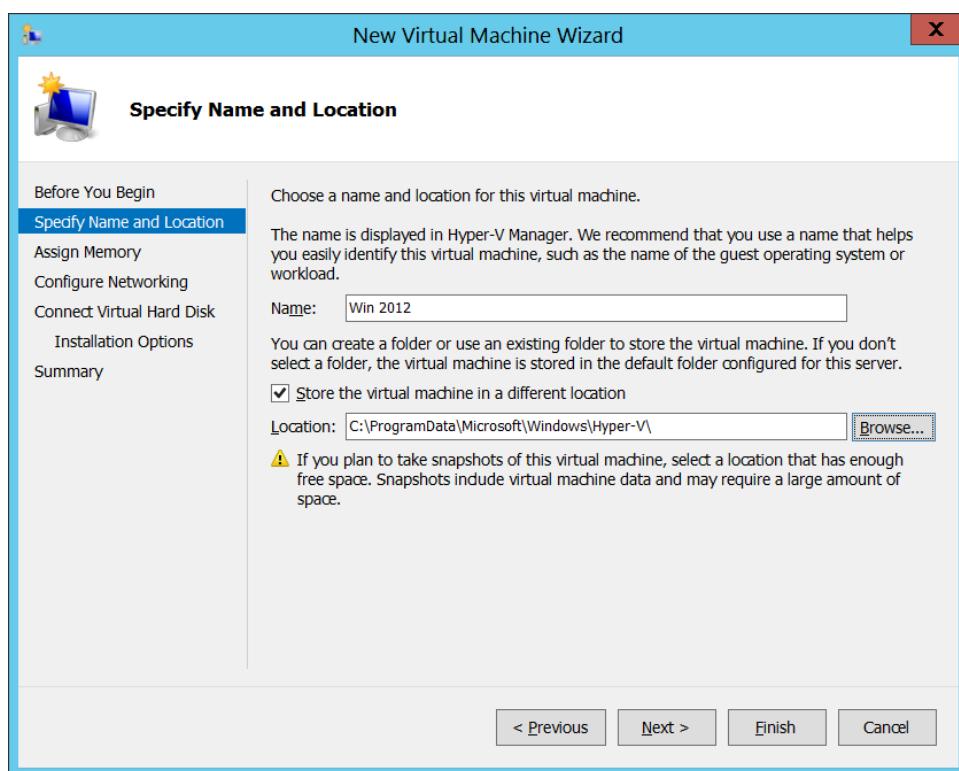
2. In Hyper-V Manager, right click on Server Name (**SYS1**) and select **New Virtual Machine**.



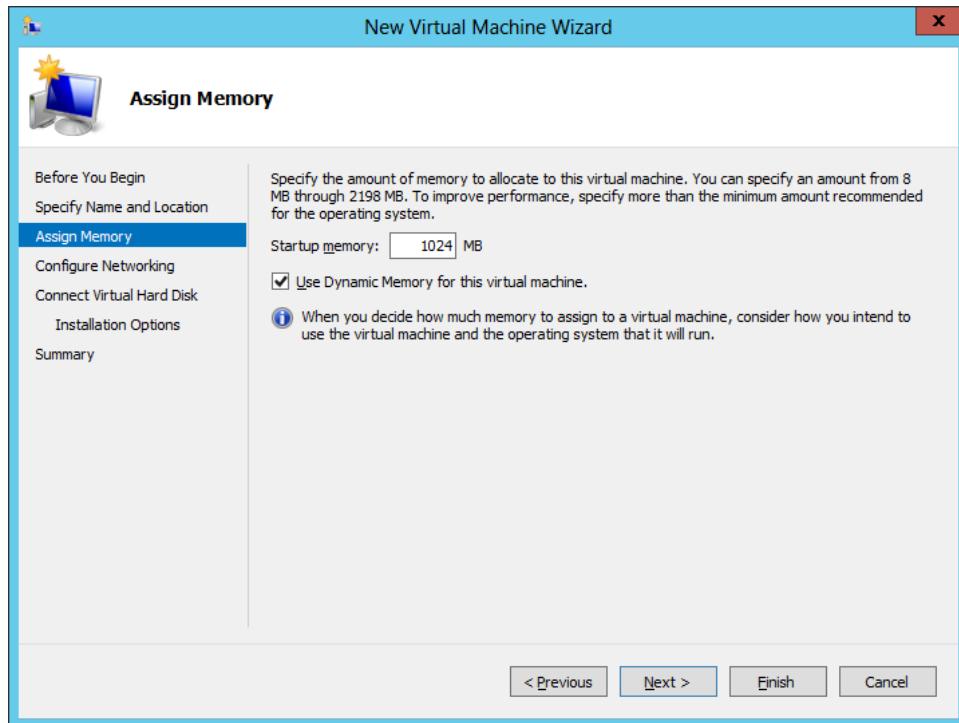
3. In Before you begin page, click **Next**.



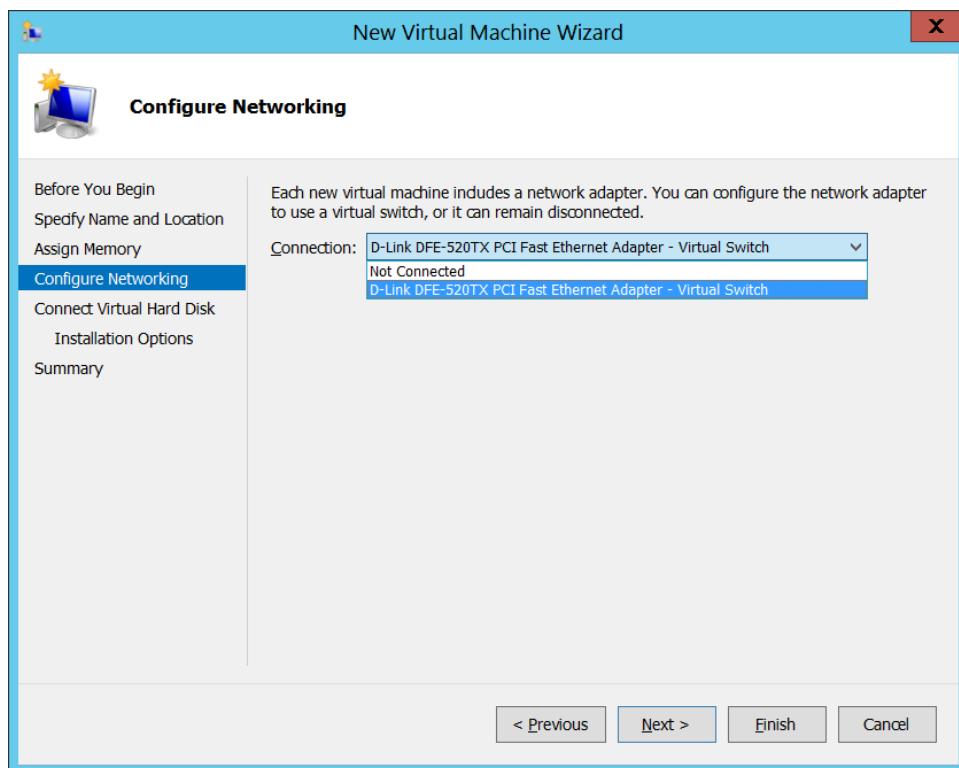
4. Enter Name and Location for the Virtual Machine (Ex: Win 2012) and click **Next**.



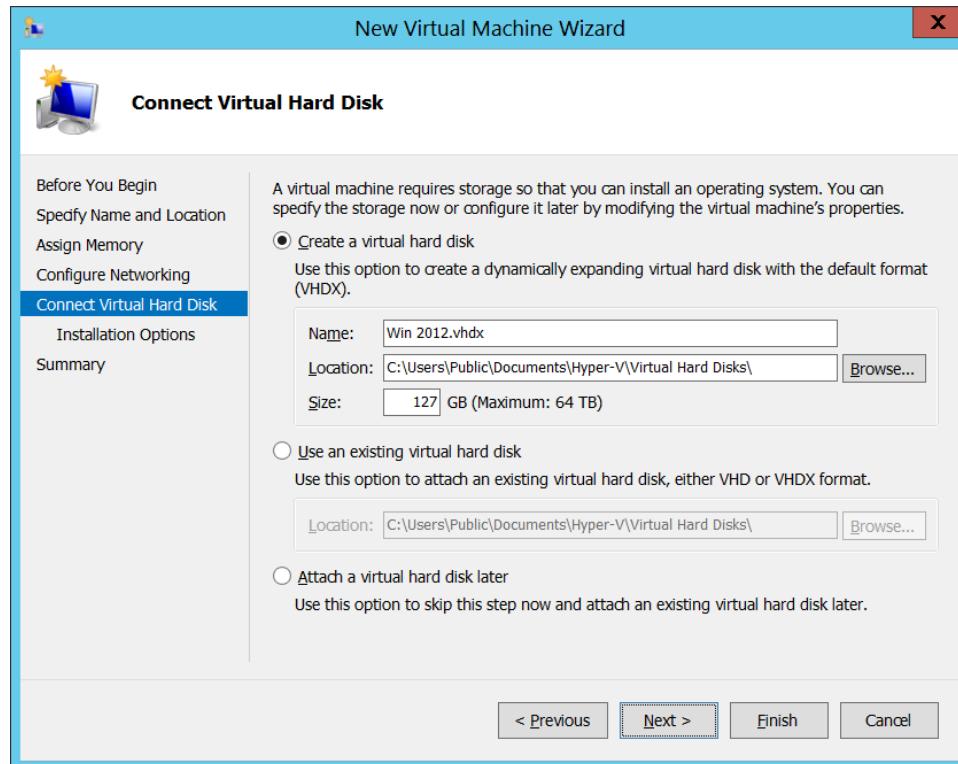
5. In Assign Memory Page, Enter the amount of RAM for the virtual machine (Ex: 1024 MB) and select Use Dynamic Memory for this virtual machine.



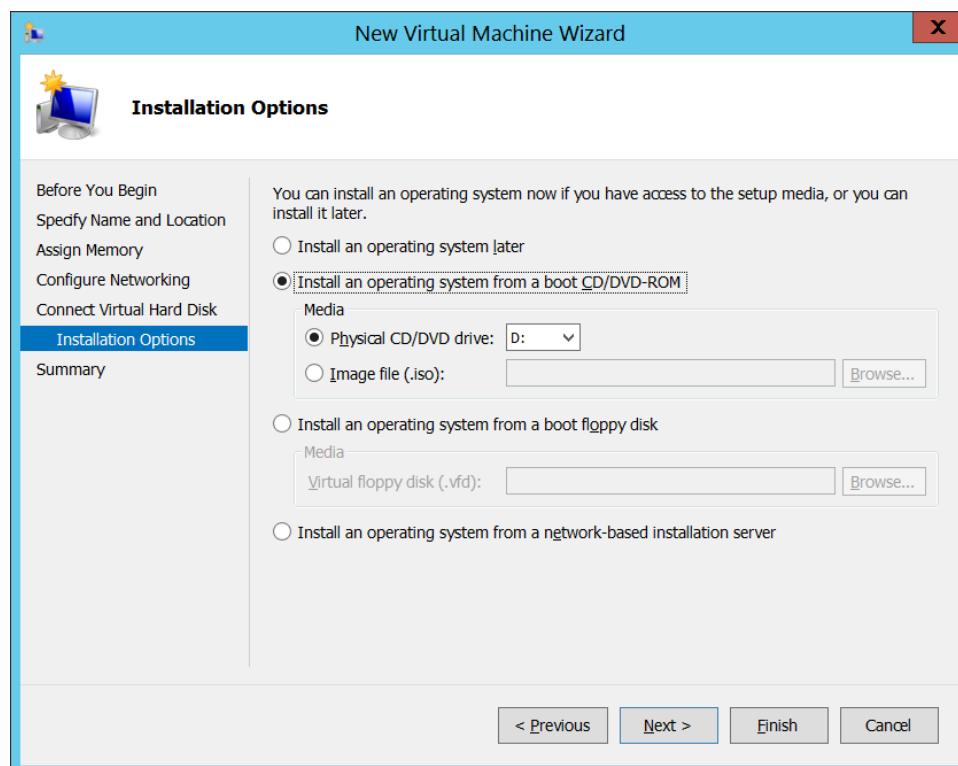
6. In Configure Networking Page, select Virtual Switch Adapter click **Next**.



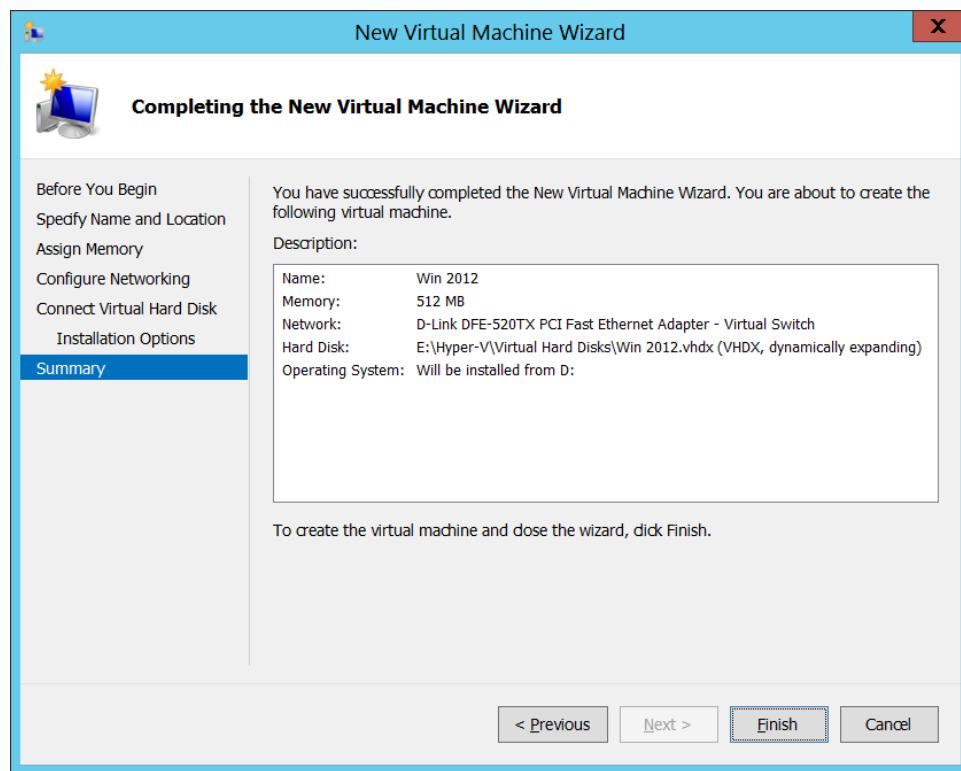
7. In Connect Virtual Hard Disk Page, select **Create a virtual hard disk** and enter the **Name**, **Location** and **Size** of the virtual hard disk. Click **Next**.



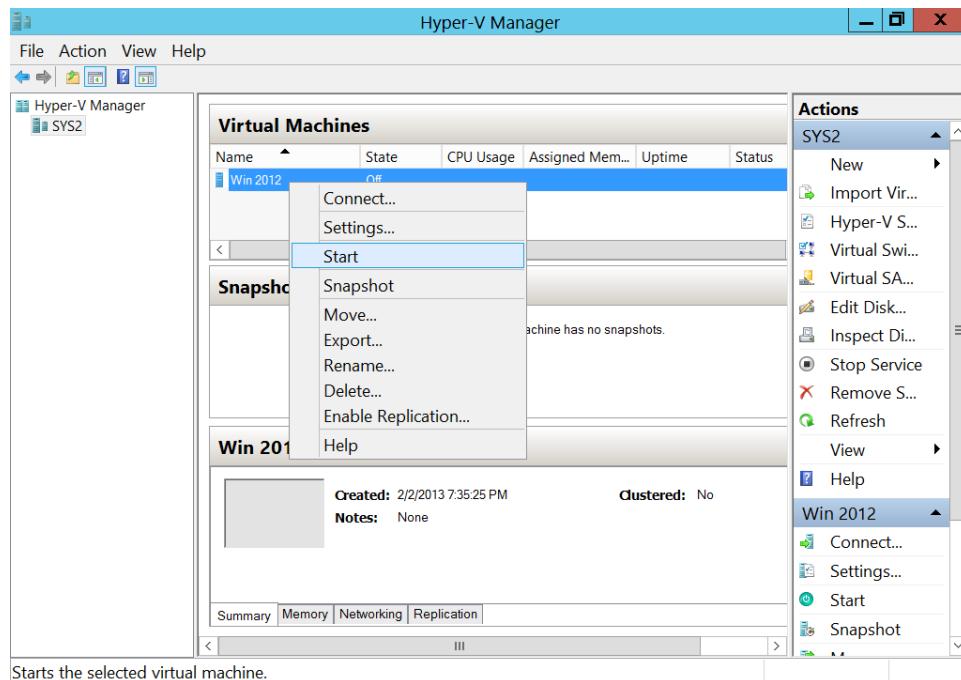
8. In Installation Options, select **Install an operating system from a boot CD/DVD-ROM**, click **Next**.

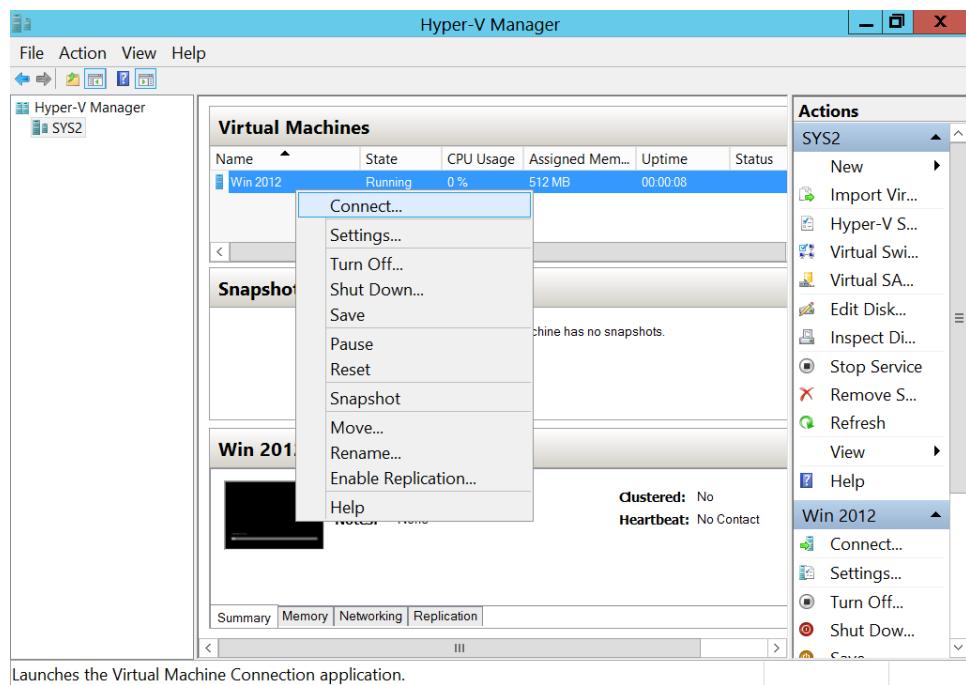


9. In Completing the New Virtual Machine Wizard, click **Finish**.

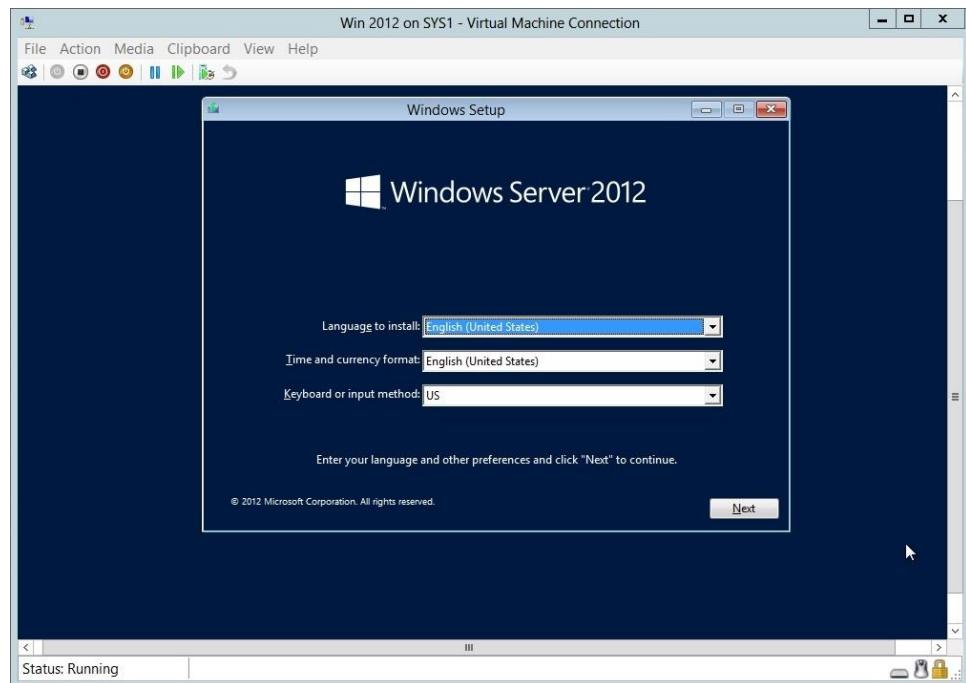


10. In Hyper-V Manager console, right click virtual machine (Ex: win 2012), click **Start**.



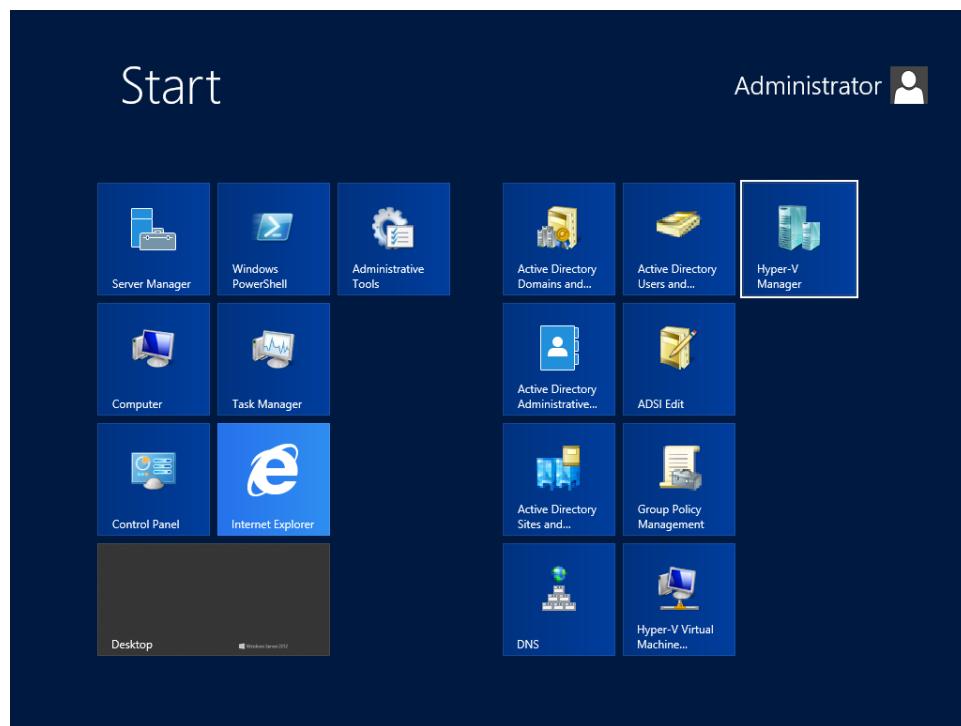
11. Right click virtual machine (Ex: win 2012), click **Connect**.

12. Install the Operating System on Virtual Machine.

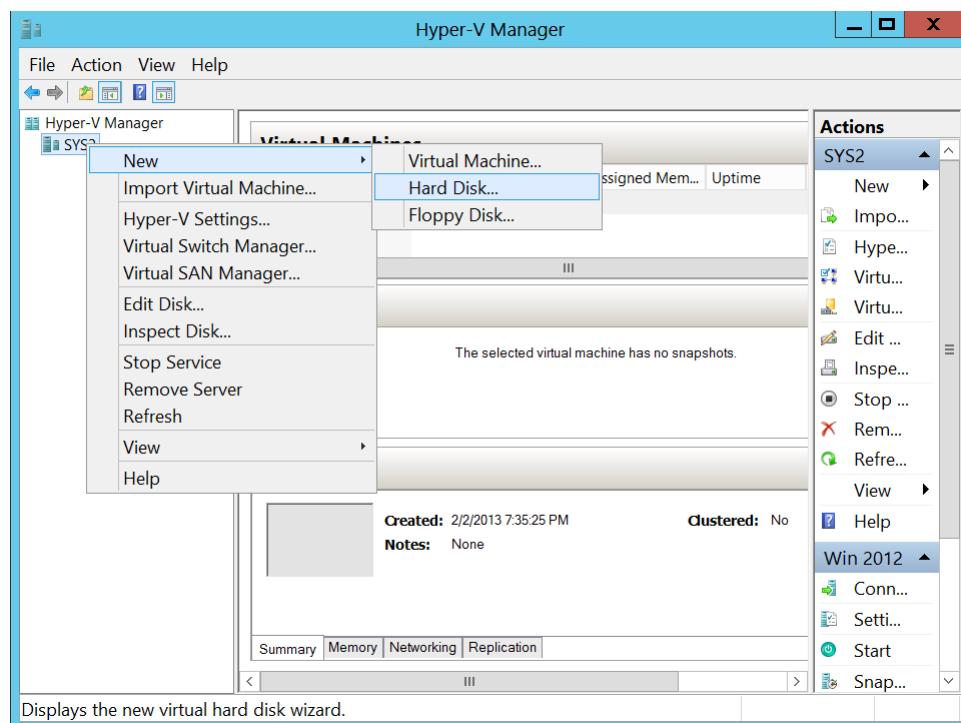


Lab – 3: Creating Fixed Size Virtual Hard Disk

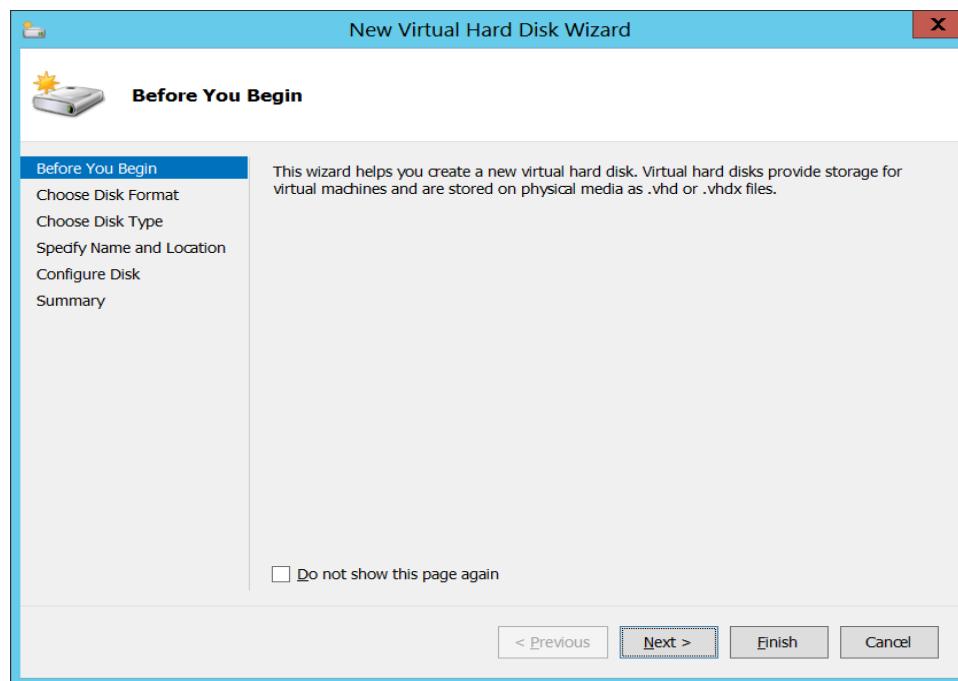
1. Go to Start, select **Hyper-V Manager**.



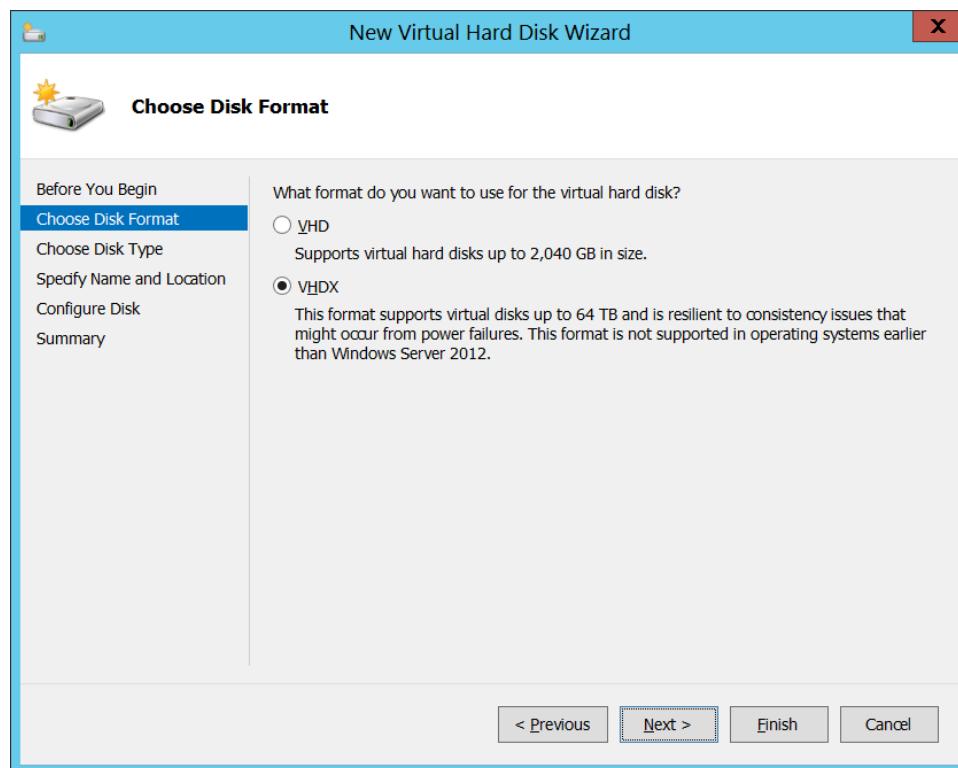
2. In Hyper-V Manager, right click on Server Name (**SYS1**) and select **New Hard Disk**.



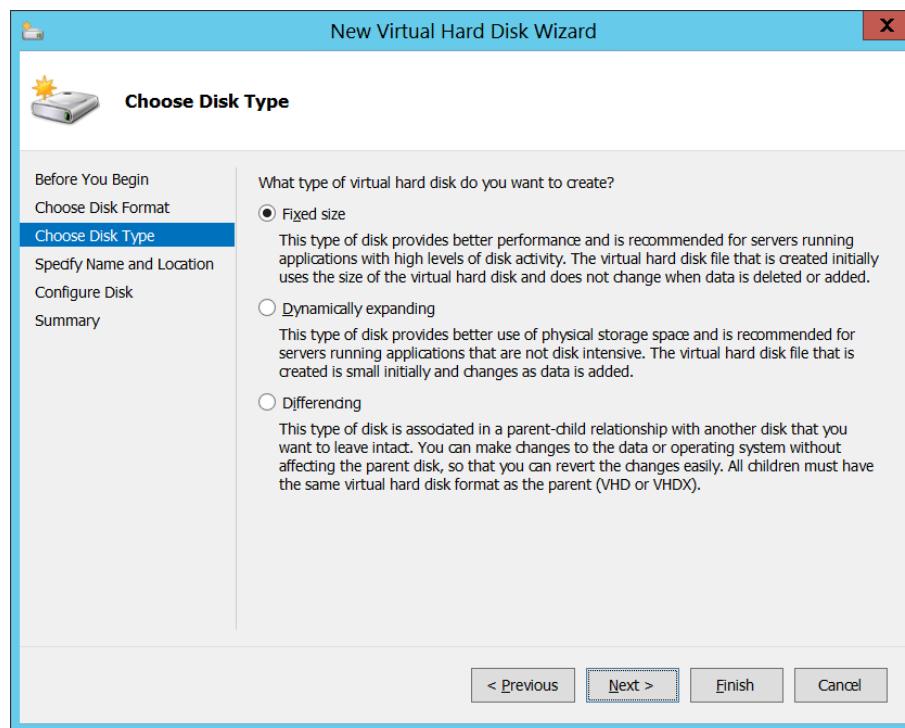
3. In Before you begin page, click **Next**.



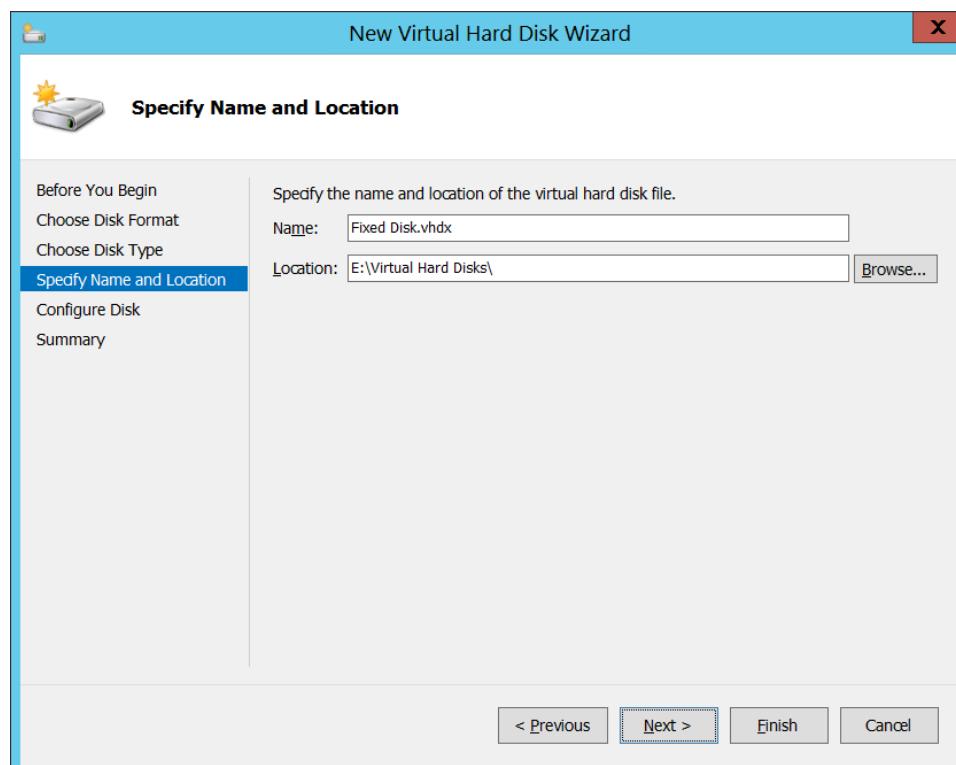
4. In Choose Disk Format Page, select **VHDX** and click **Next**.



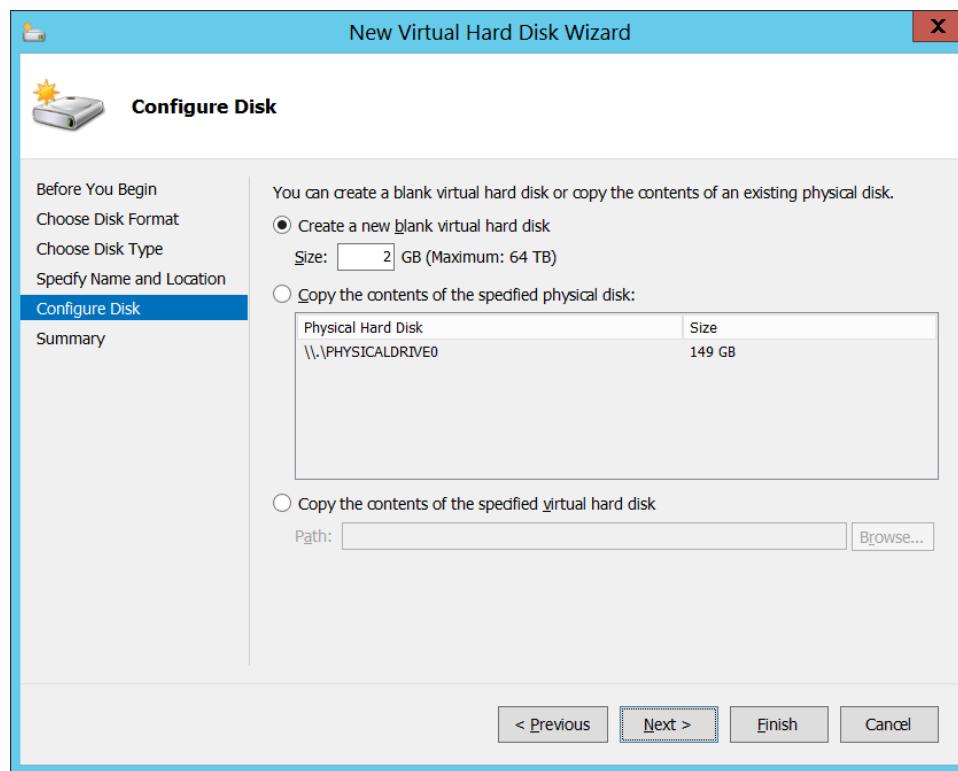
5. In Choose Disk Type, select **Fixed size** and click **Next**.



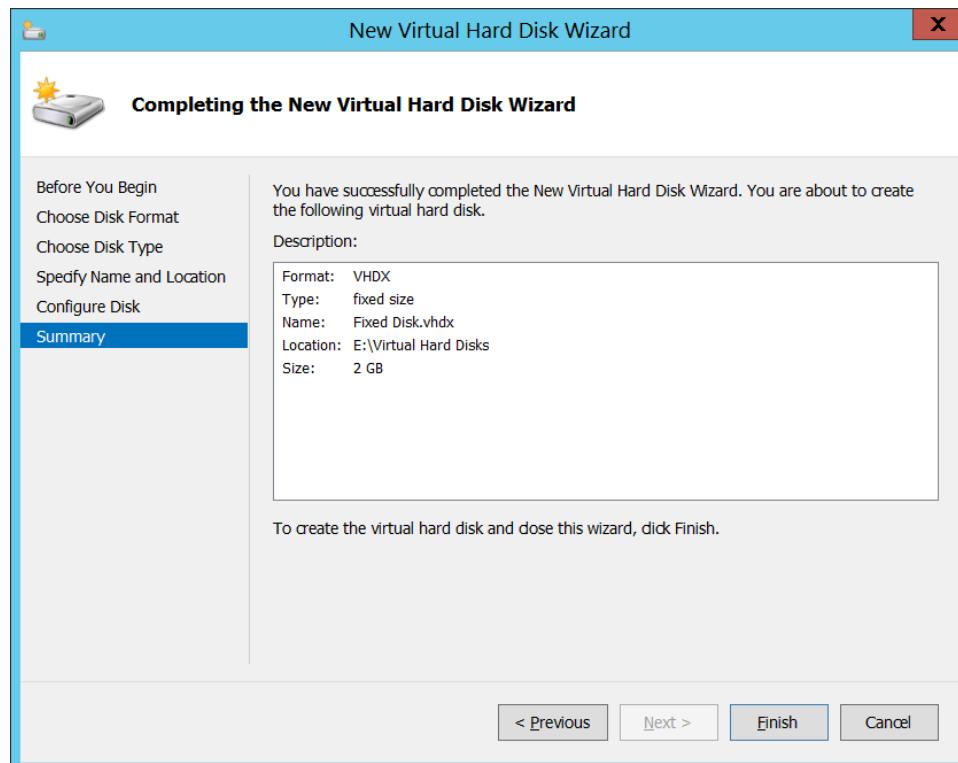
6. Enter **Name**, **Browse** and select **Location** for virtual hard disk, click **Next**.



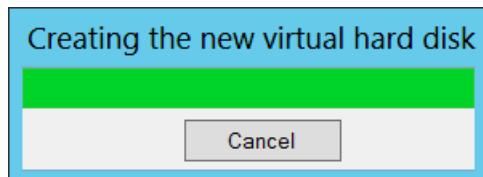
7. Select **Create a new blank virtual hard disk**, **Sizeofvirtual hard disk**. Click **Next**.



8. Click **Finish** to create the New Virtual Hard Disk.

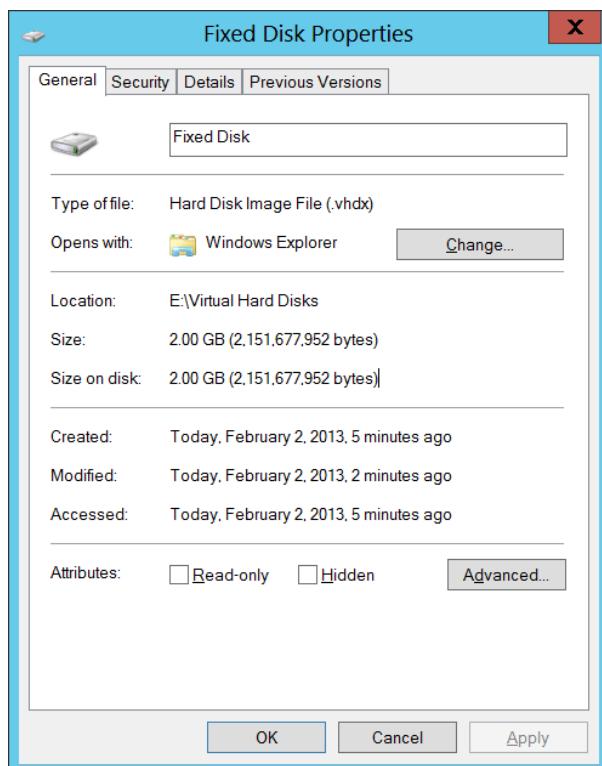


9. It creates a new Fixed size virtual hard disk.



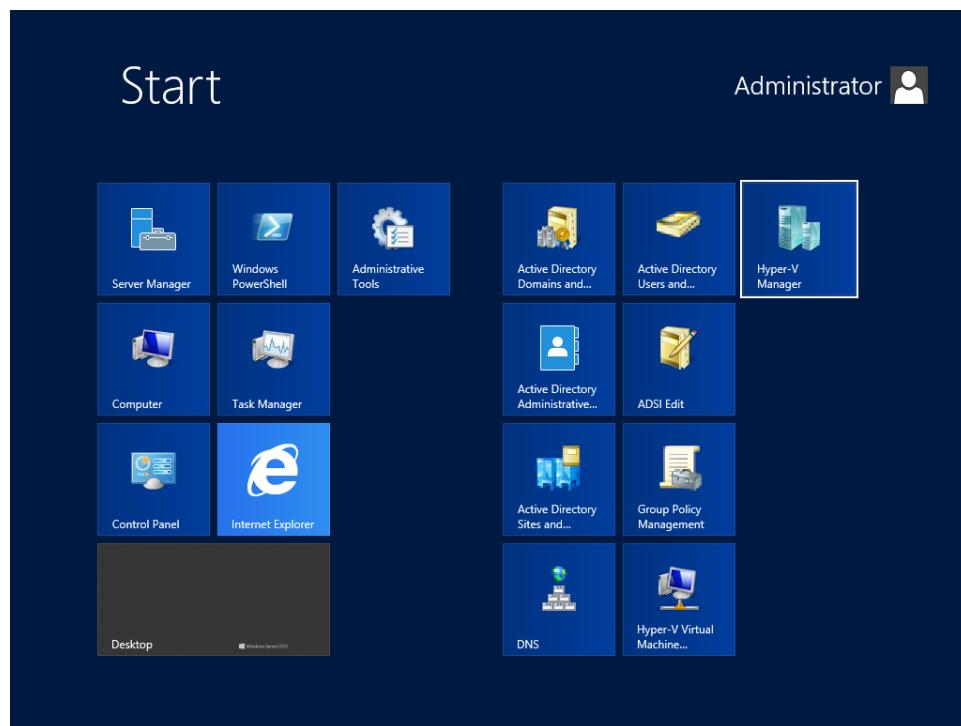
Verification:

1. Go to the location of the Fixed size virtual hard disk (Ex: E:\Virtual Hard Disks), select Fixed Disk.vhdx file → Properties and verify the Size and Size on disk.

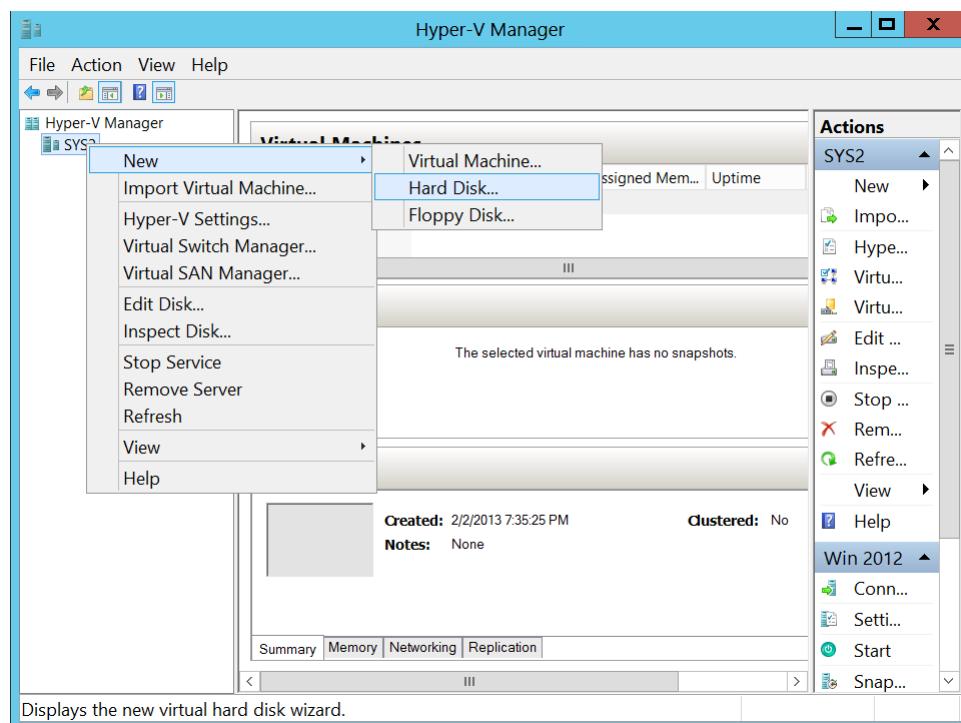


Lab – 4: Creating Dynamically Expanding Virtual Hard Disk

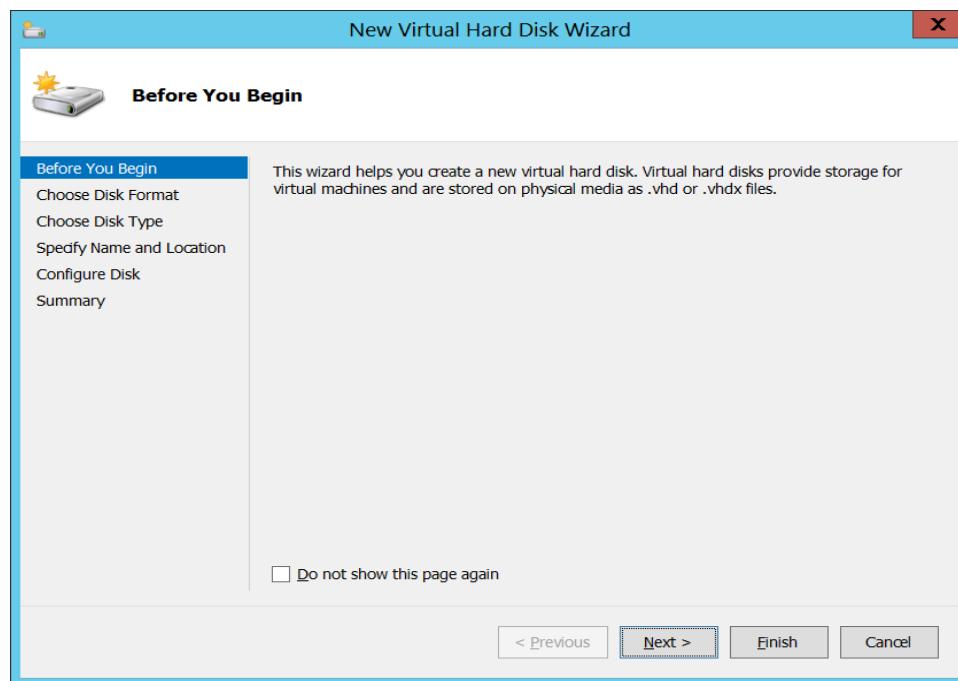
1. Go to Start, select **Hyper-V Manager**.



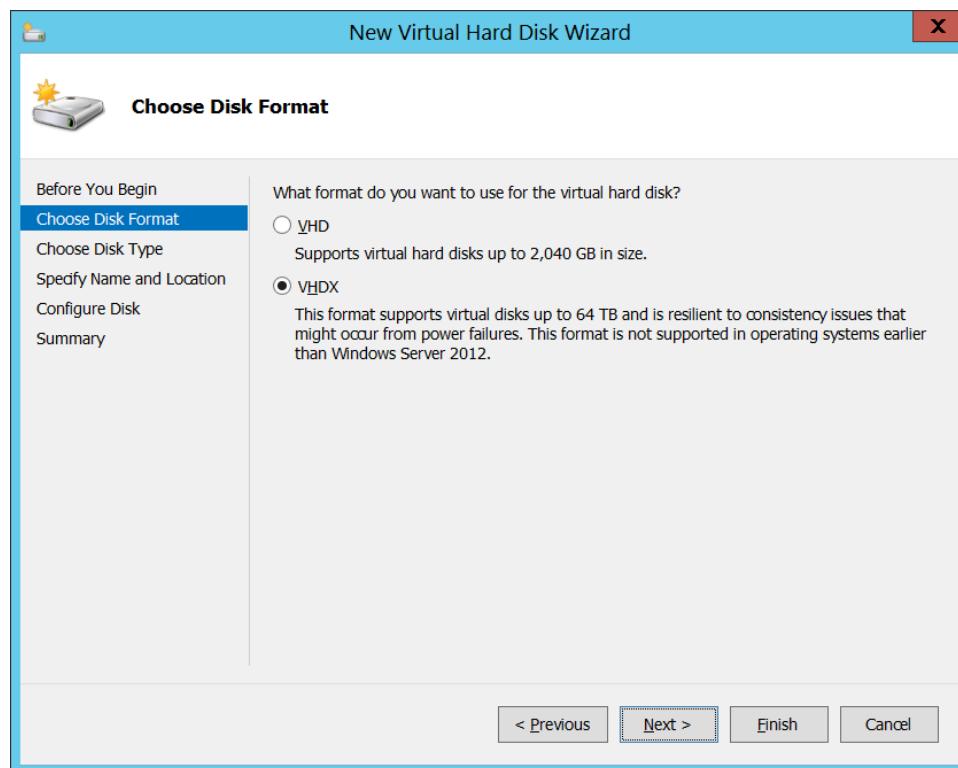
2. In Hyper-V Manager, right click on Server Name (**SYS1**) and select **New Hard Disk**.



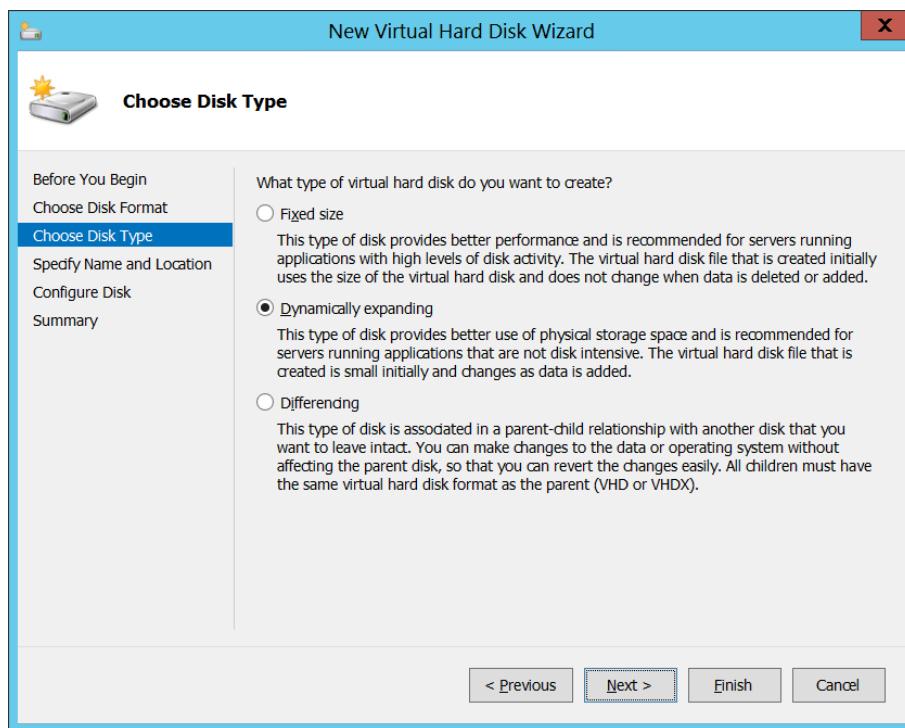
3. In Before you begin page, click **Next**.



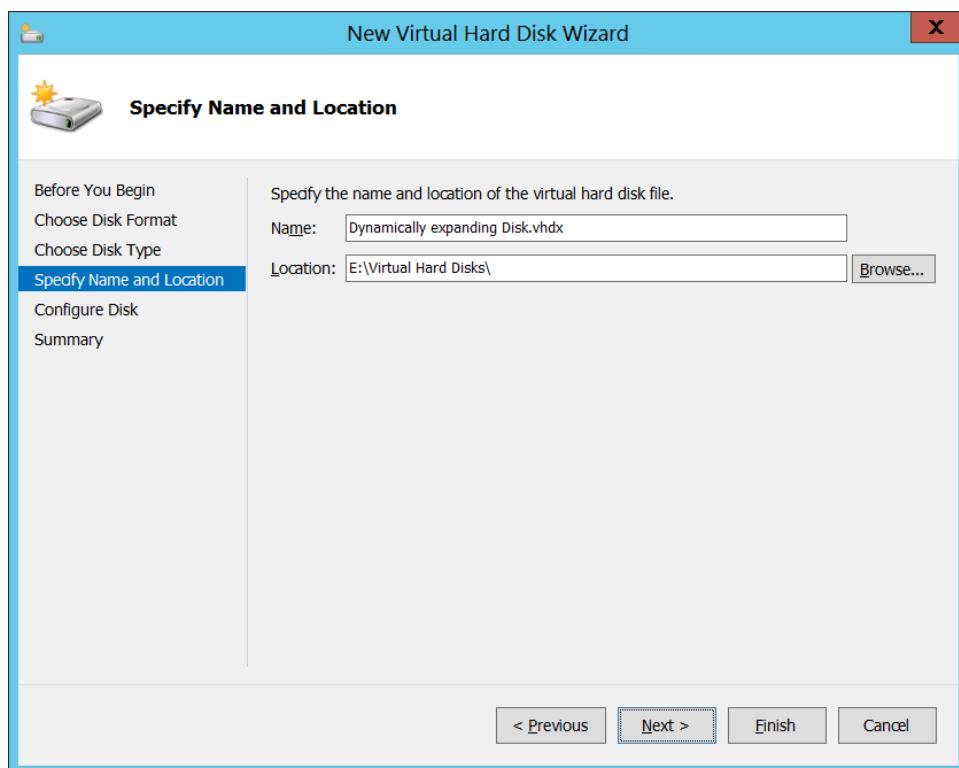
4. In Choose Disk Format Page, select **VHDX** and click **Next**.



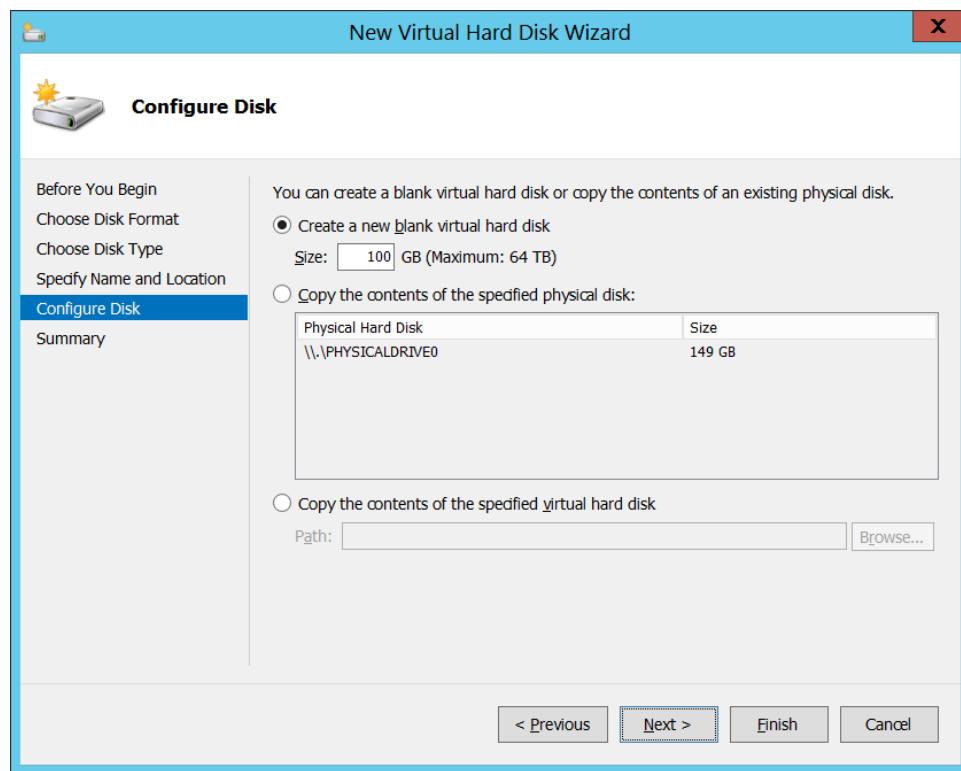
5. In Choose Disk Type, select **Dynamically expanding** and click **Next**.



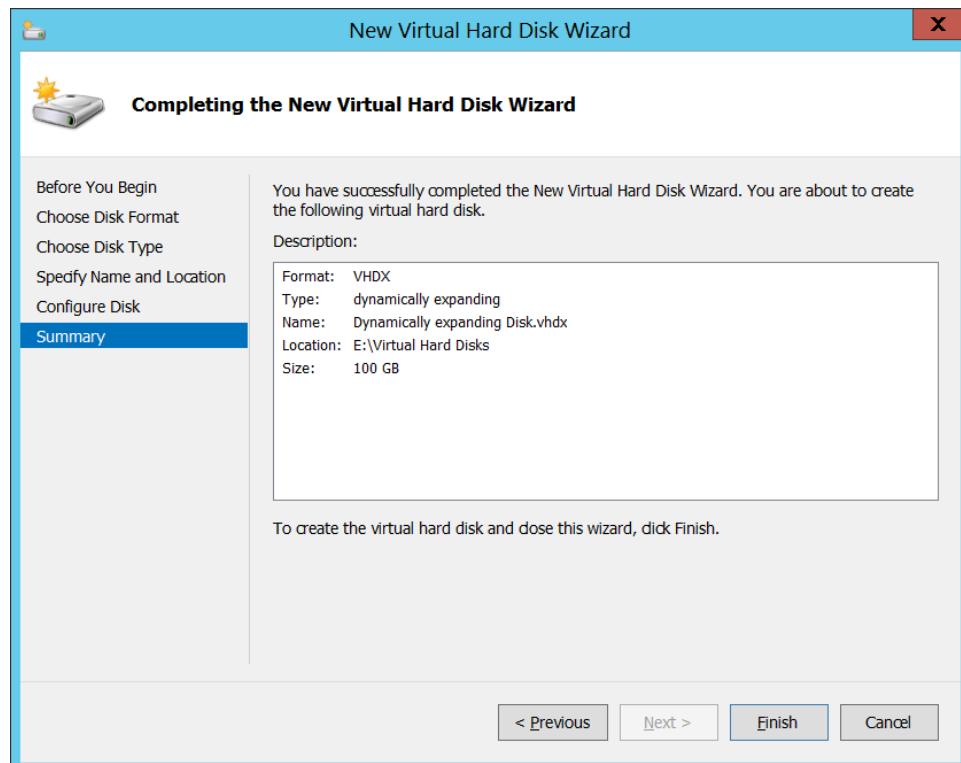
6. Enter **Name**, **Browse** and select **Location** for virtual hard disk, click **Next**.



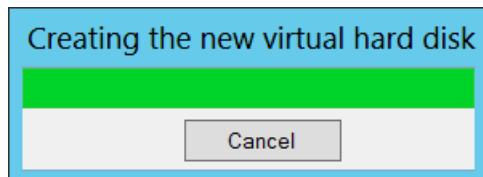
7. Select **Create a new blank virtual hard disk**, **Size of virtual hard disk**. Click **Next**.



8. Click **Finish** to create the New Virtual Hard Disk.

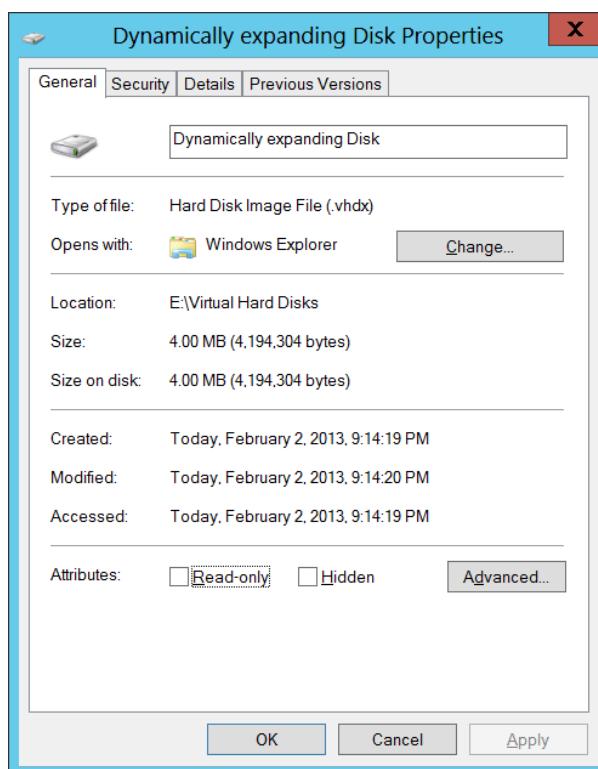


9. It creates a new Fixed size virtual hard disk.



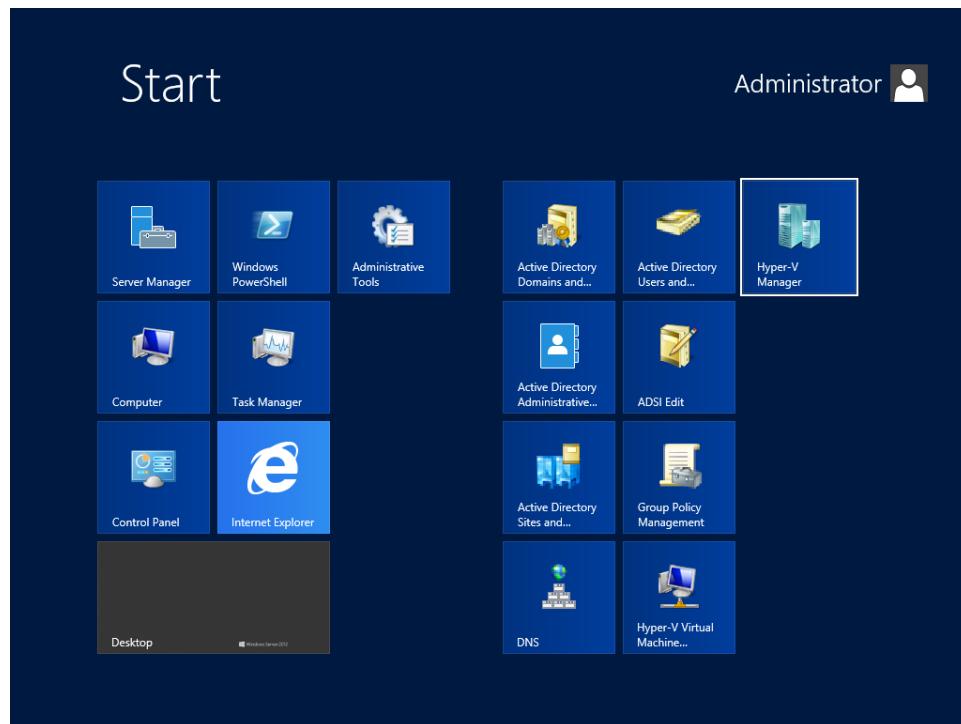
Verification:

1. Go to the location of the Dynamically expanding virtual hard disk (Ex: E:\Virtual Hard Disks), select Dynamically expanding Disk.vhdx file → Properties and verify the Size and Size on disk.

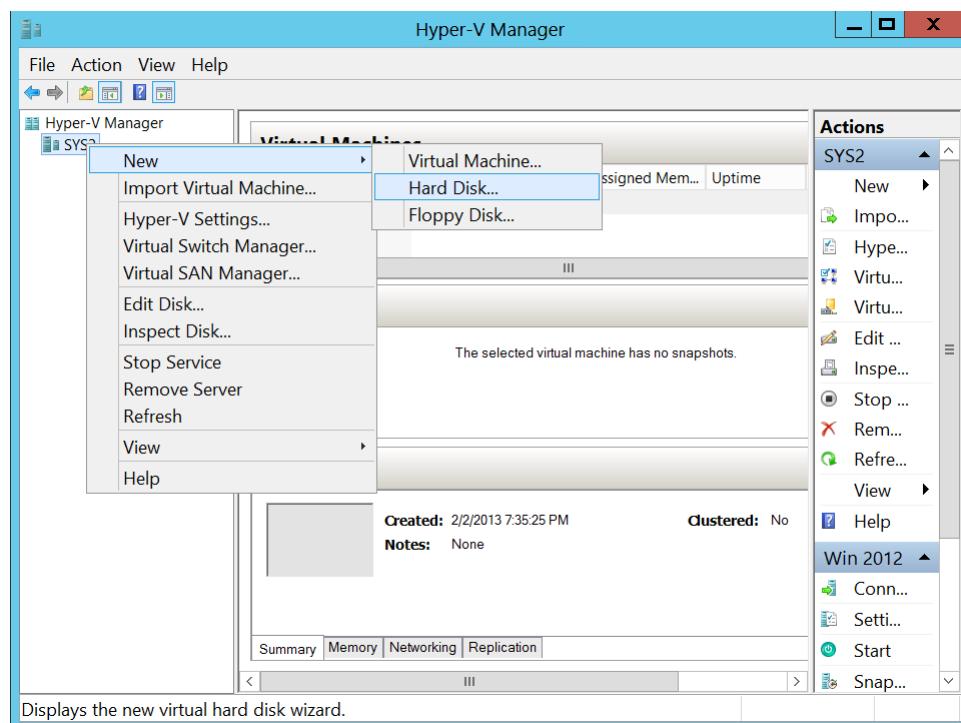


Lab – 5: Creating Differencing Virtual Hard Disk

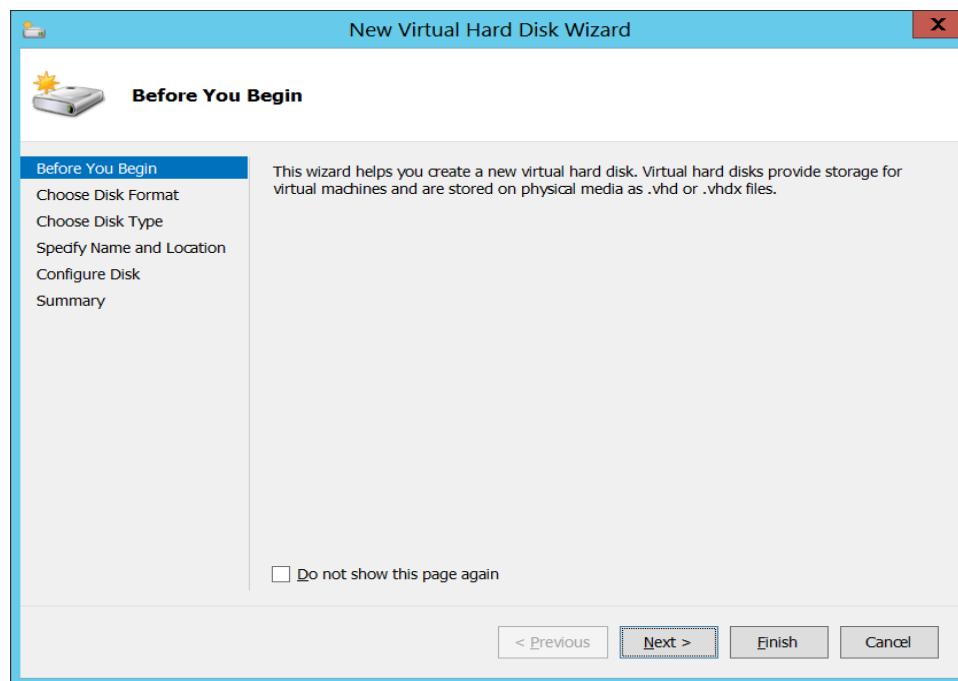
1. Go to Start, select **Hyper-V Manager**.



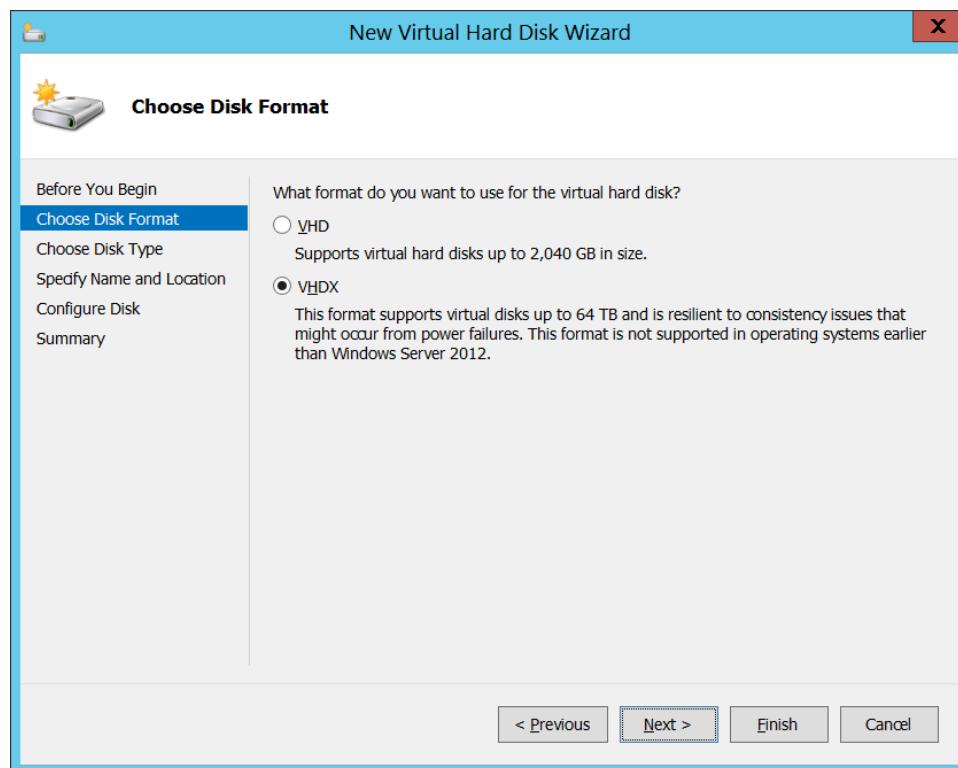
2. In Hyper-V Manager, right click on Server Name (**SYS1**) and select **New Hard Disk**.



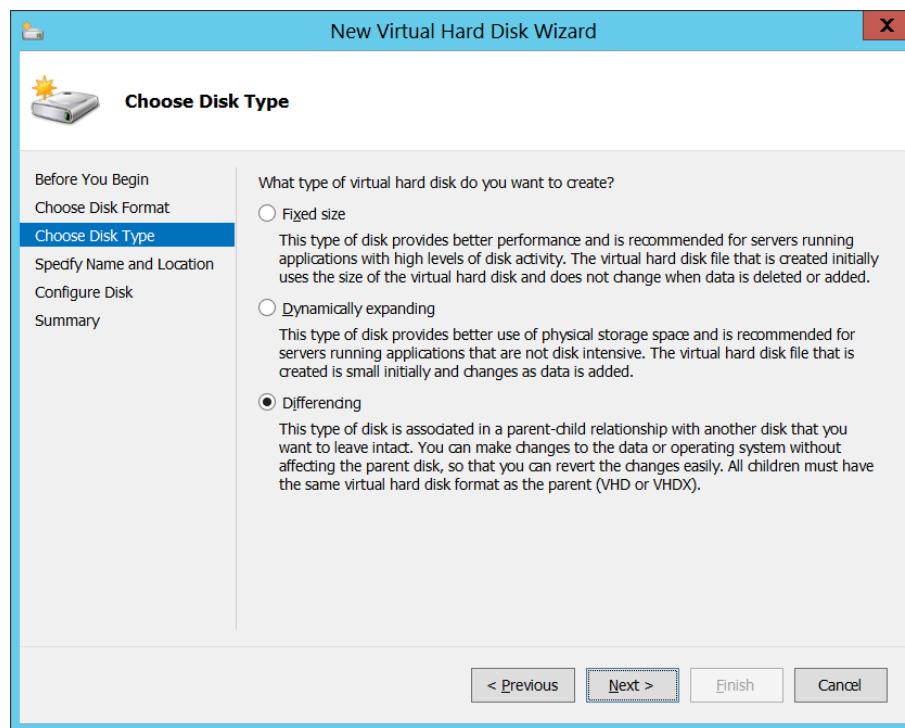
3. In Before you begin page, click **Next**.



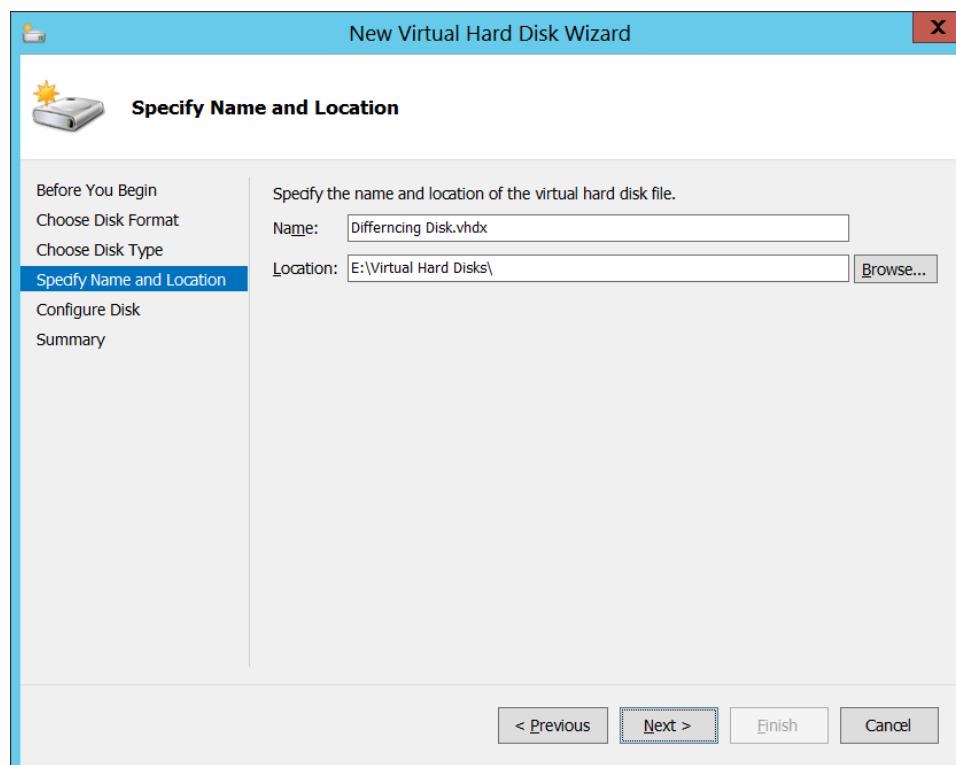
4. In Choose Disk Format Page, select **VHDX** and click **Next**.



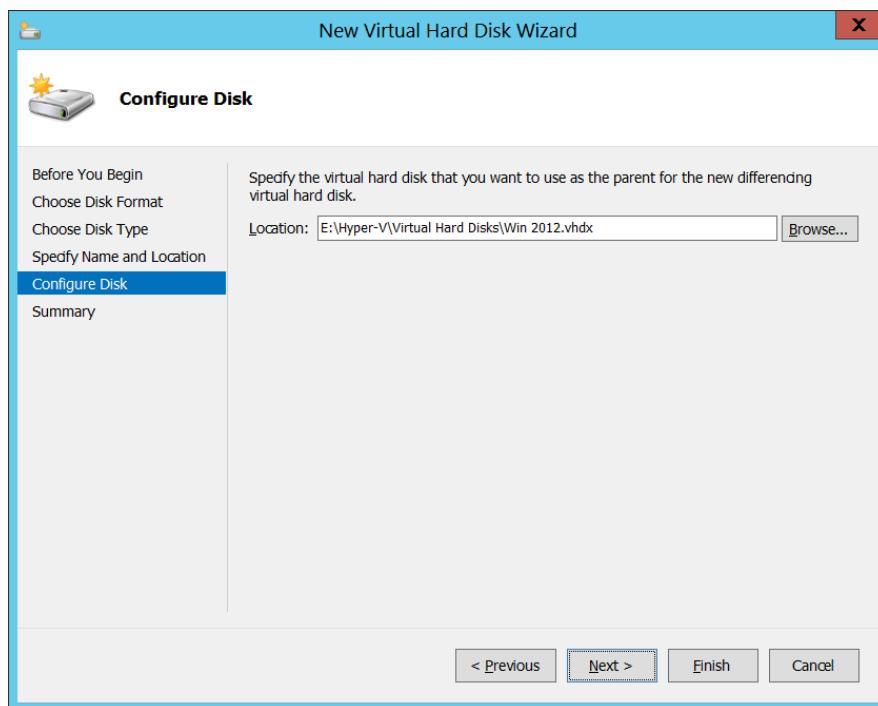
5. In Choose Disk Type, select **Differencing** and click **Next**.



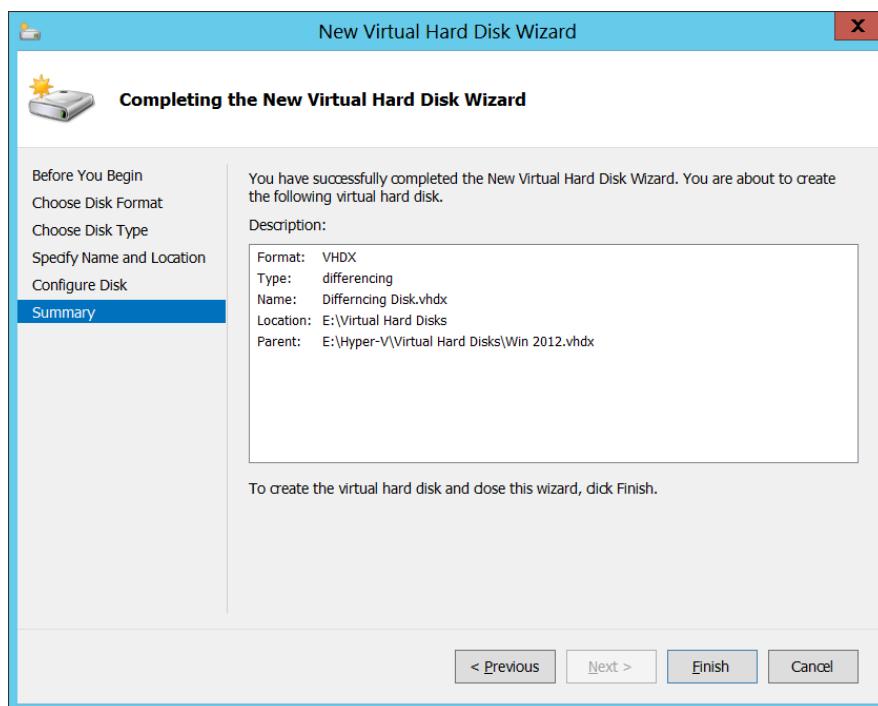
6. Enter **Name**, **Browse** and select **Location** for virtual hard disk, click **Next**.



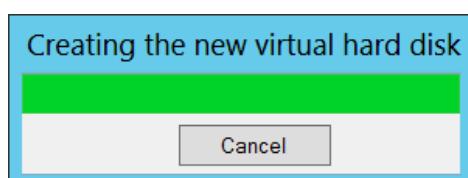
7. In Configure Disk Page, Browse and select the Parent Disk, click **Next**.



8. Click **Finish** to create the New Virtual Hard Disk.

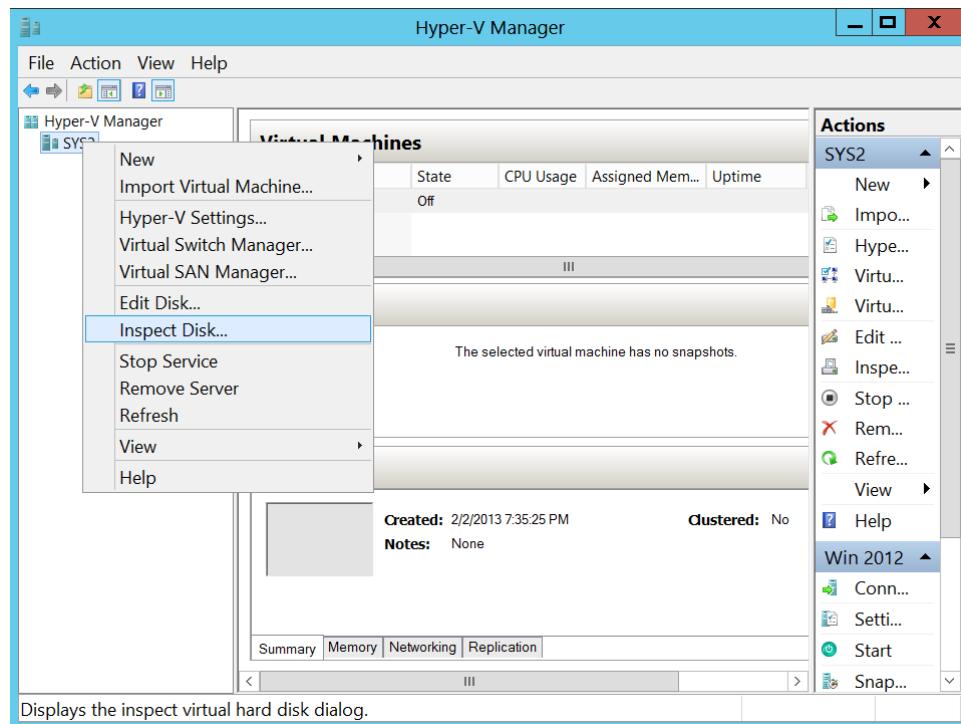


9. It creates a new Differencing virtual hard disk.

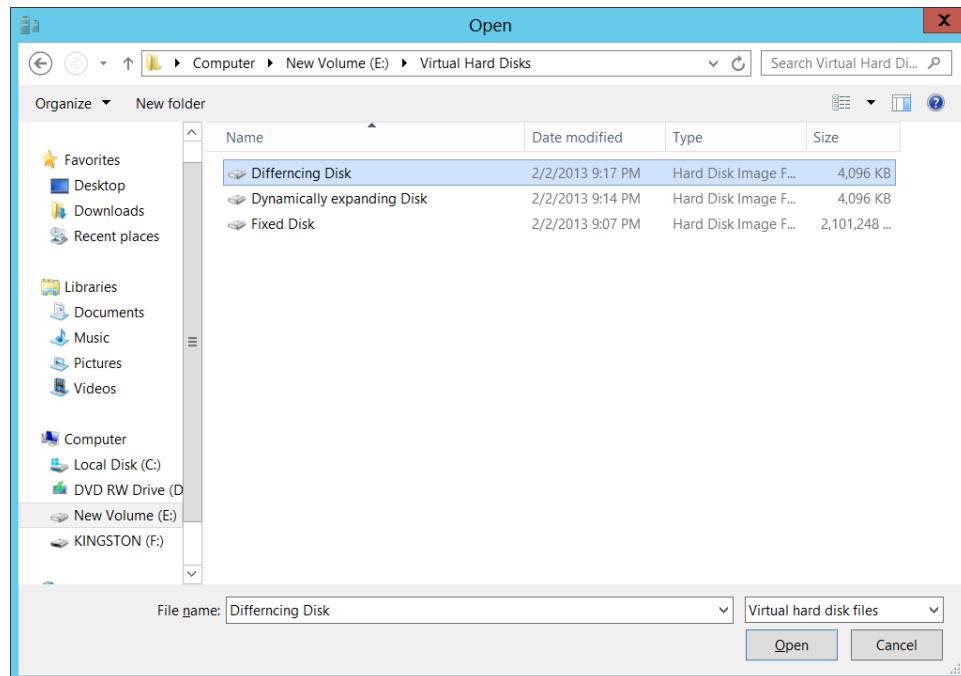


Verification:

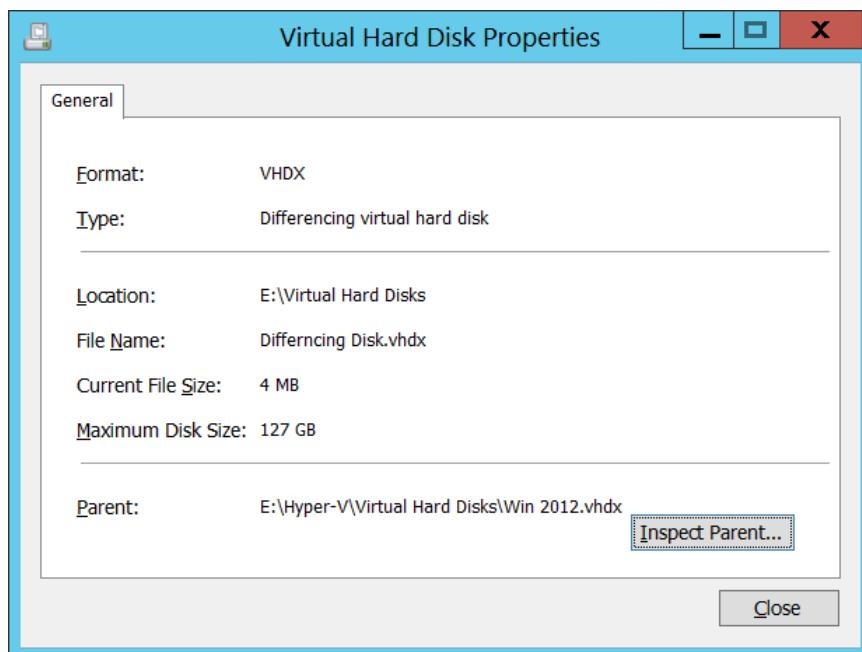
1. Go to Hyper-V Manager Console, right click Server, select **Inspect Disk**.



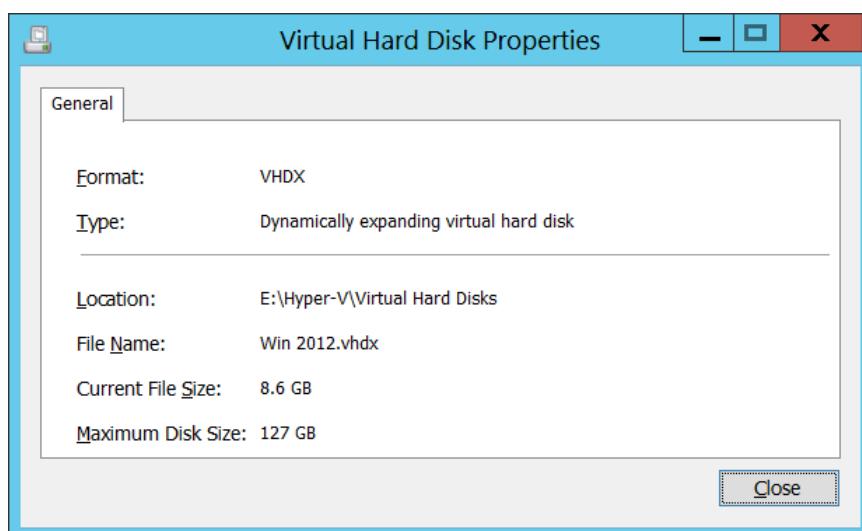
2. Browse and select the **Differencing Disk** from (E:\Virtual Hard Disks).



3. In Virtual Hard Disk Properties, select **Inspect Parent**.

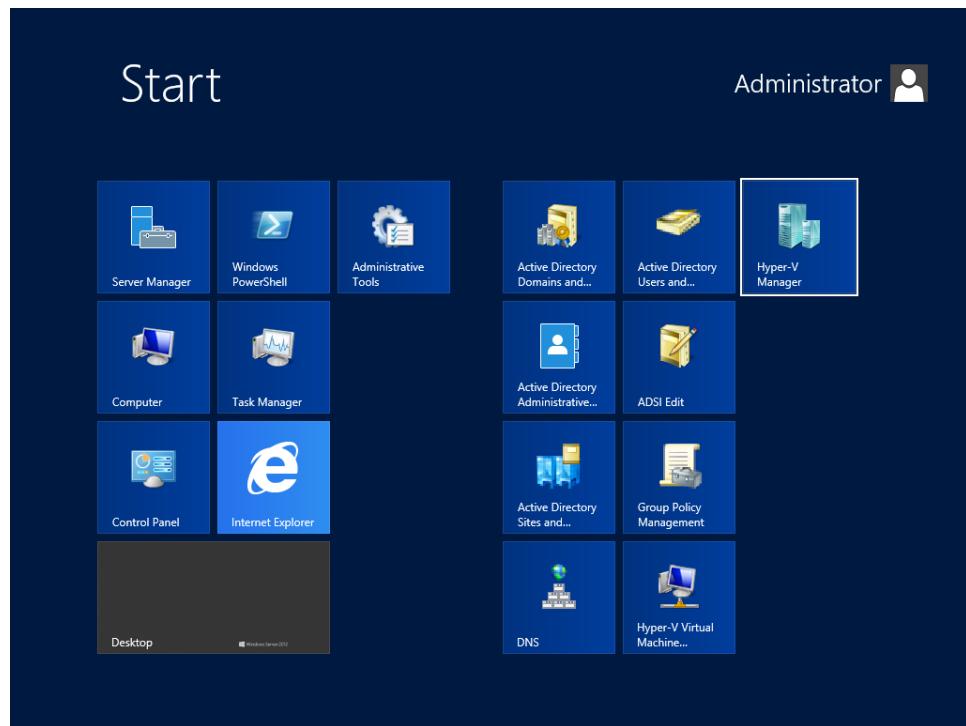


4. Verify the Parent Virtual Hard Disk Properties and click **Close**.

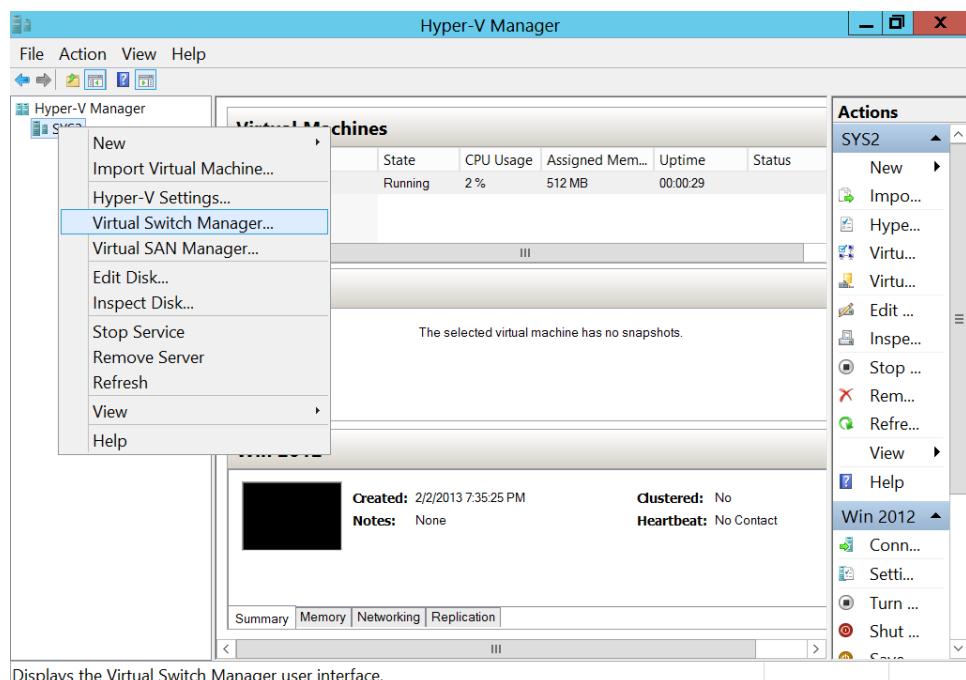


Lab – 6: Configuring Virtual Networks

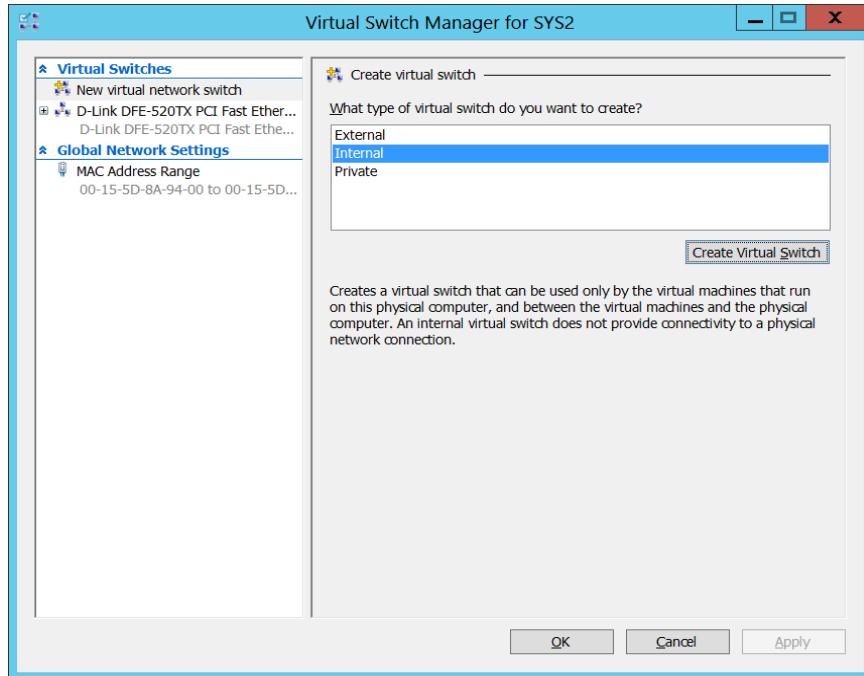
1. Go to Start, select **Hyper-V Manager**.



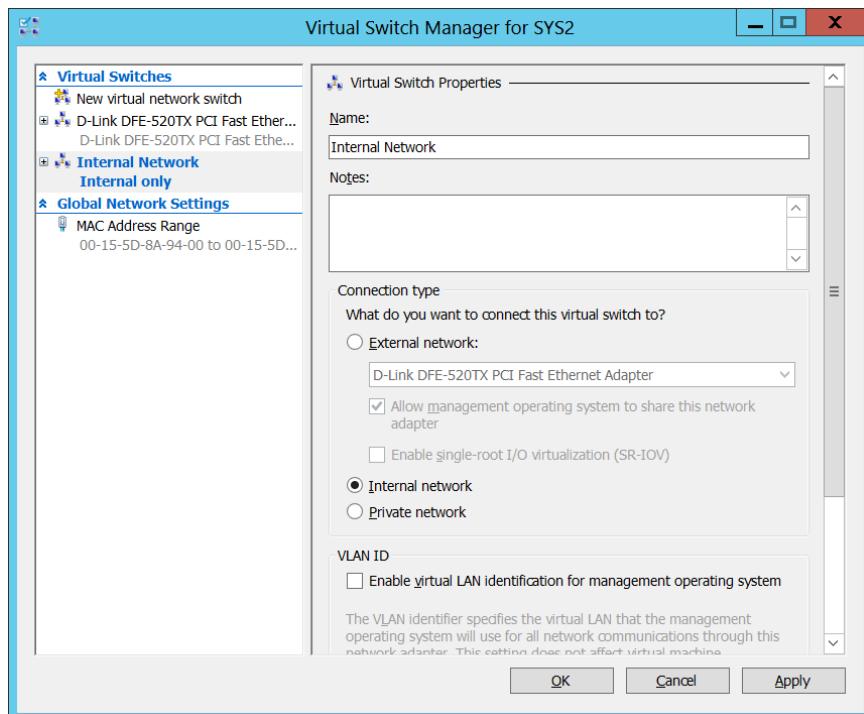
2. In Hyper-V Manager, right click Server(SYS1) and select **Virtual Switch Manager**.



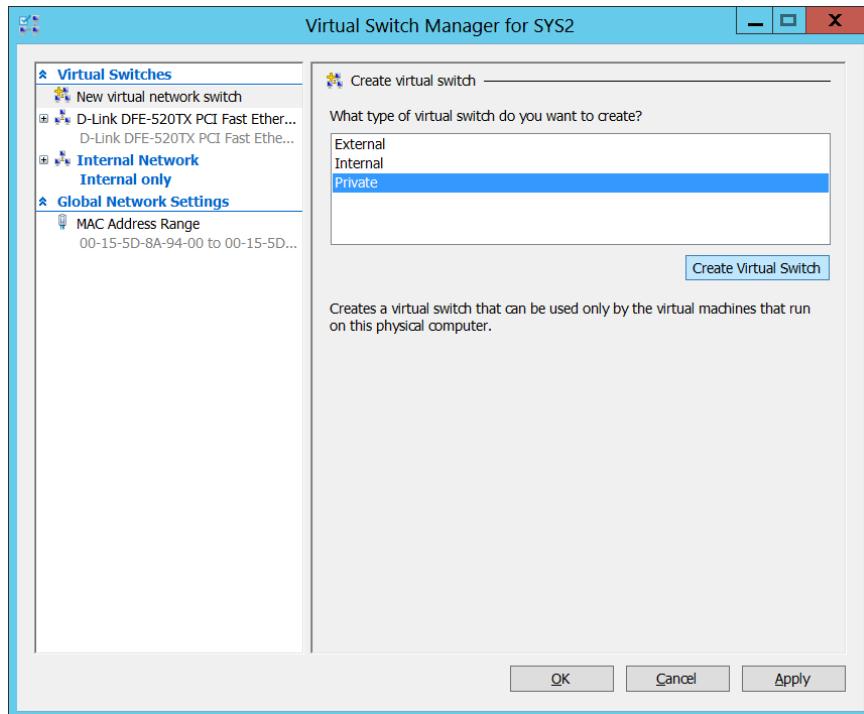
3. In Virtual Switch Manager Page, select New virtual network switch, select Internal, and click **Create Virtual Switch**.



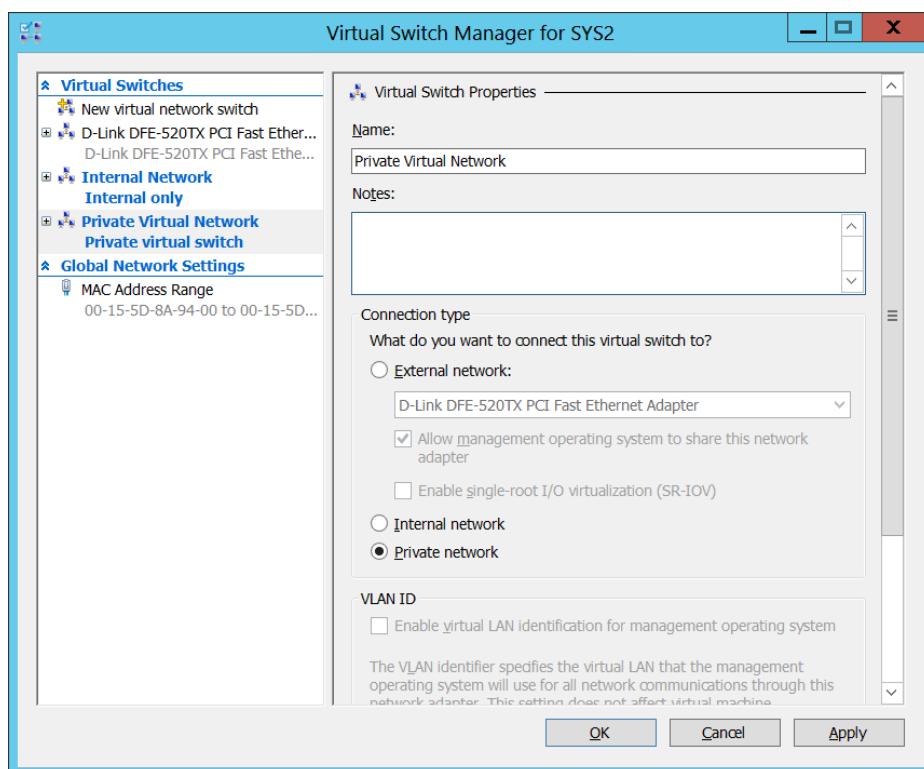
4. Select Internal Network, enter the Name (Ex: Internal Network) and in Connection type select Internal network, click **OK**.



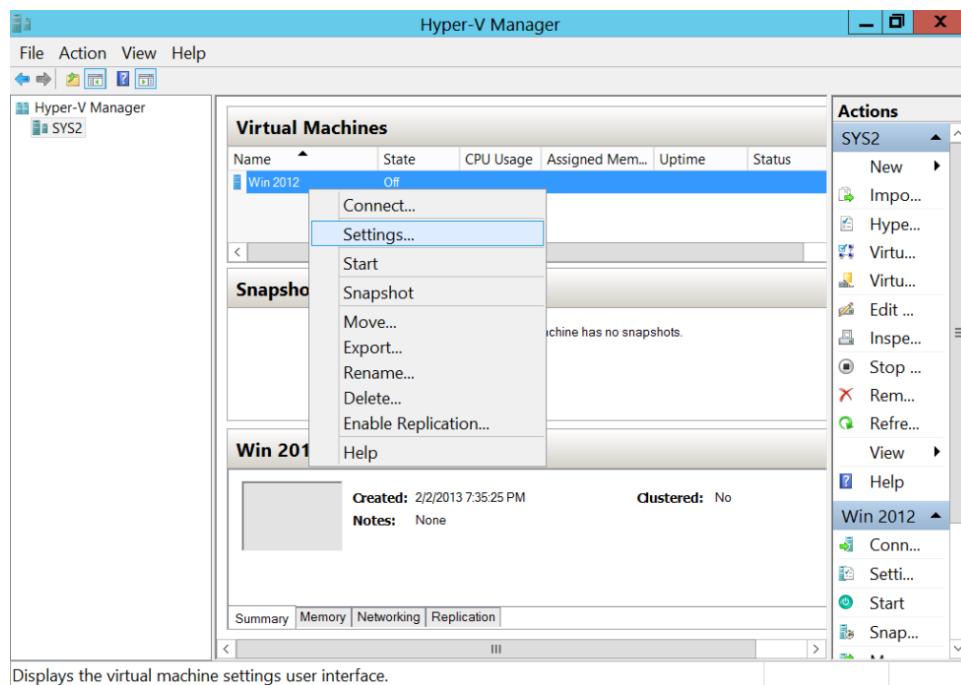
5. In Virtual Switch Manager Page, select New virtual network switch, select **Private**, and click **Create Virtual Switch**.



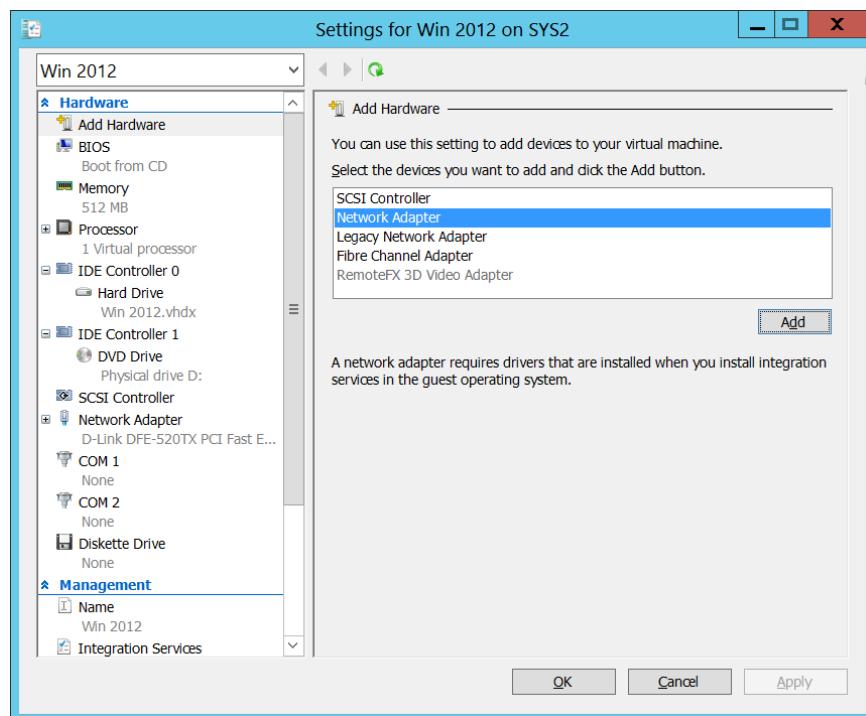
6. Select Private Virtual Network, enter the Name (Ex: Private Virtual Network) and in Connection type select Private network, click OK.



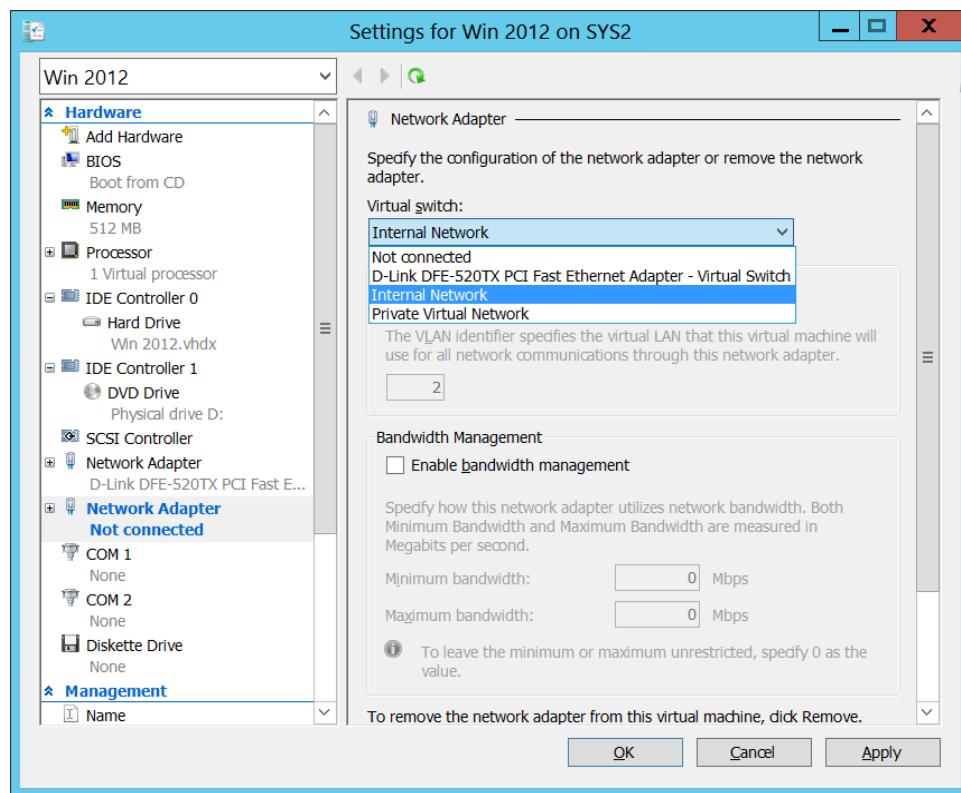
7. Go to Hyper-V Manager, right click Virtual Machine (Ex: win 2012) select **Settings**.



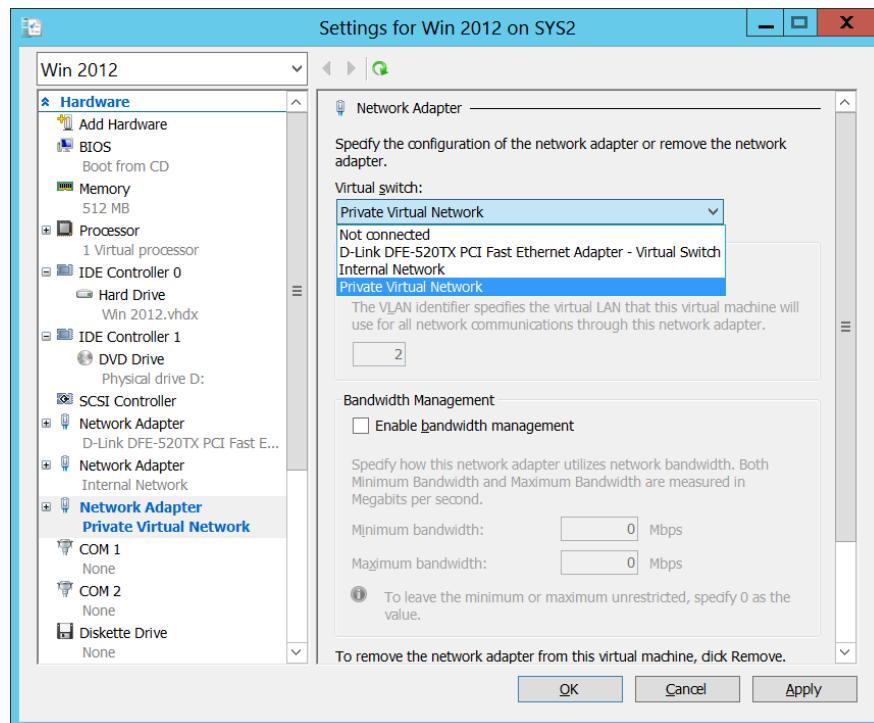
8. Select Add Hardware, select Network Adapter, and click Add.



9. Select Network Adapter and select Internal Network.

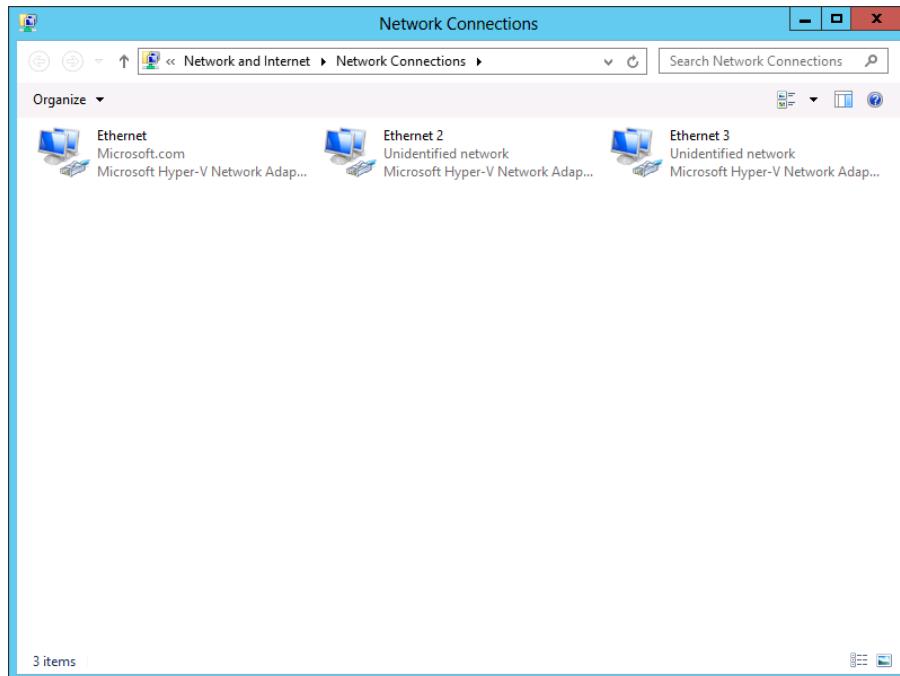


10. Select Network Adapter and select Private Virtual Network.

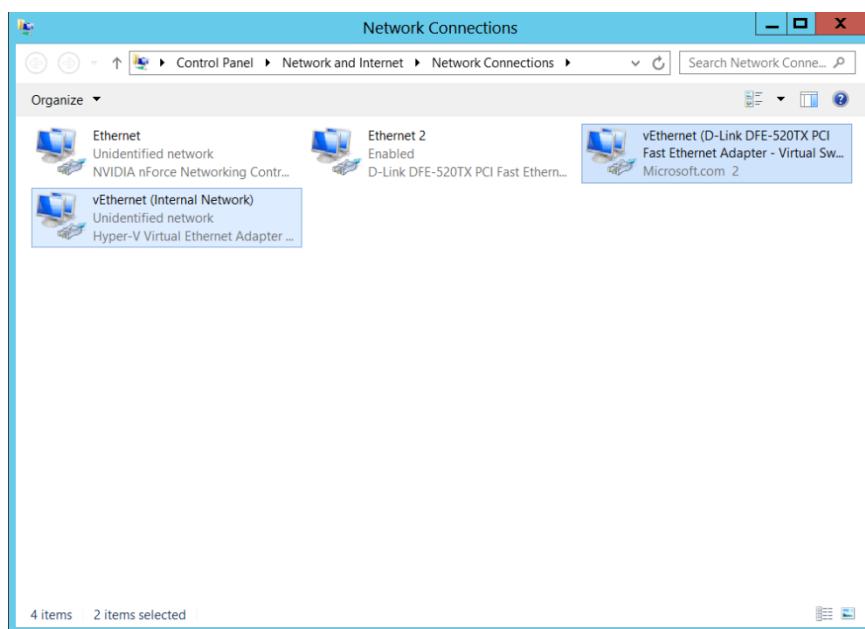


Verification:

1. Log on to Virtual Machine, go to Network Connection and verify for 3 network adapters External, Internal and Private Virtual Networks respectively.



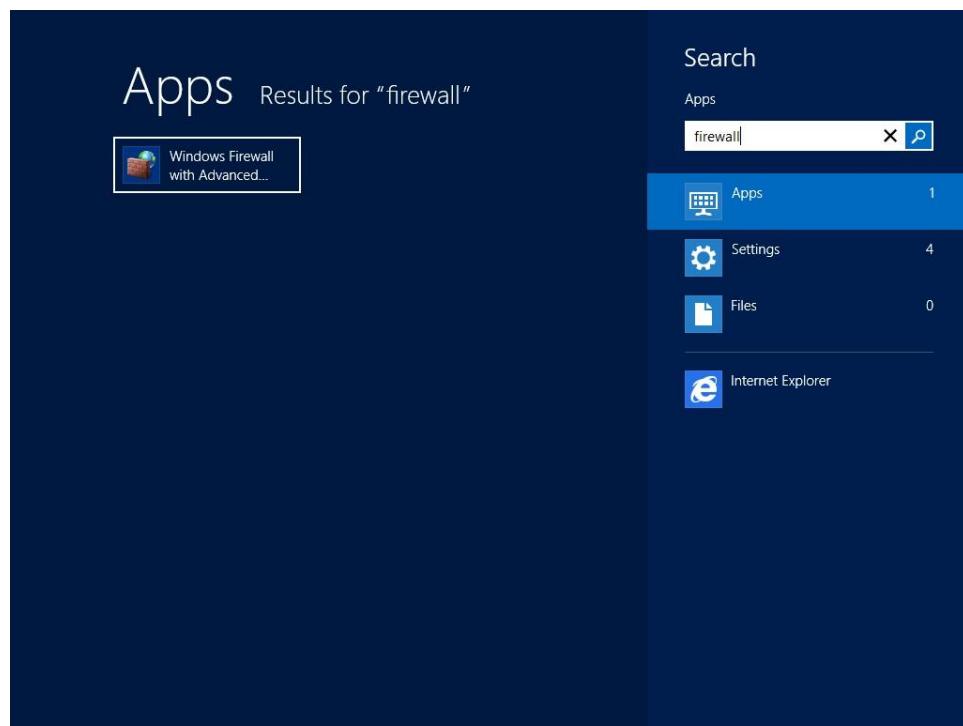
2. Go to Network connection on Host machine and verify 2 virtual network adapters connected to External and Internal networks respectively.



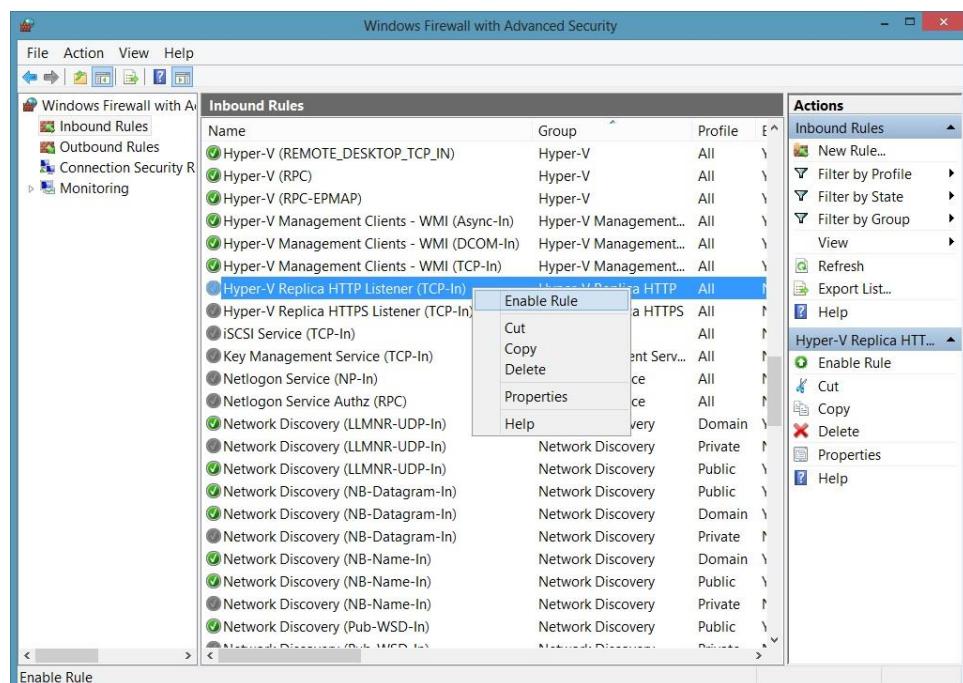
Lab – 7: Configuring Hyper-V Replica

SYS2 – CONFIGURATION

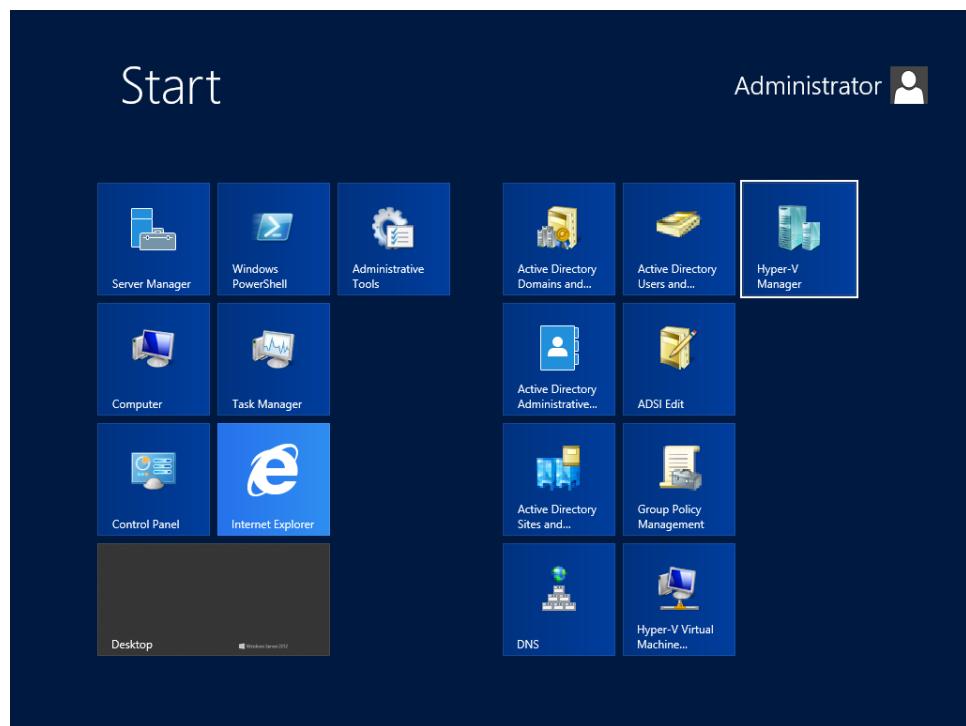
1. Log on to Member Server **SYS2** as Domain Administrator and Install Hyper-V.
2. Go to Start, type Firewall, select **Windows Firewall with Advanced...**



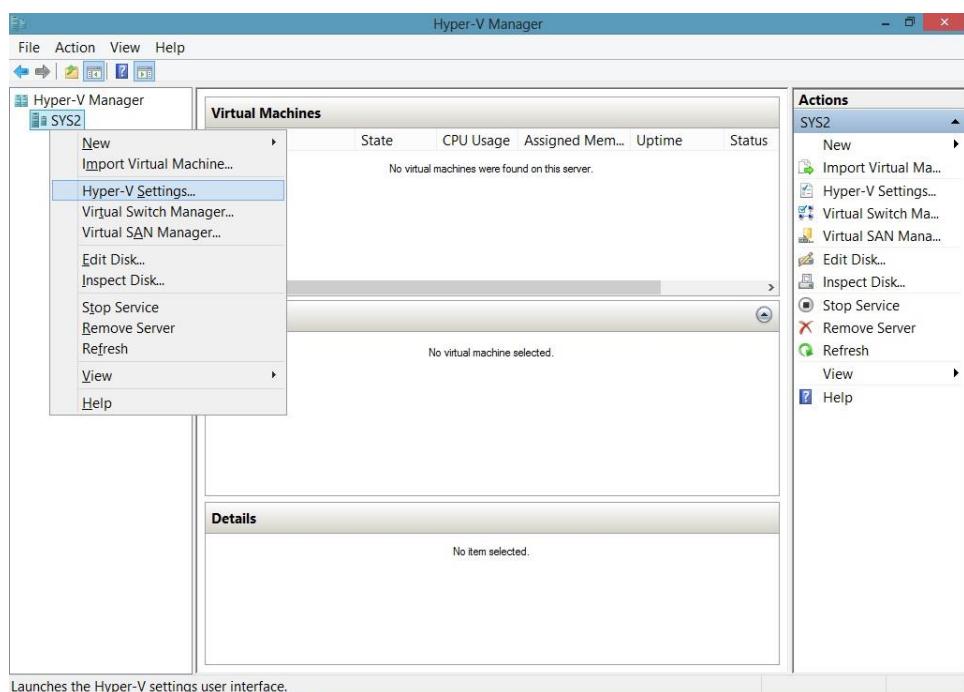
3. Select Inbound Rules, Right click **Hyper-V Replica HTTP Listener (TCP-In)**, Enable Rule and **Hyper-V Replica HTTPS Listener (TCP-In)** and Enable Rule.



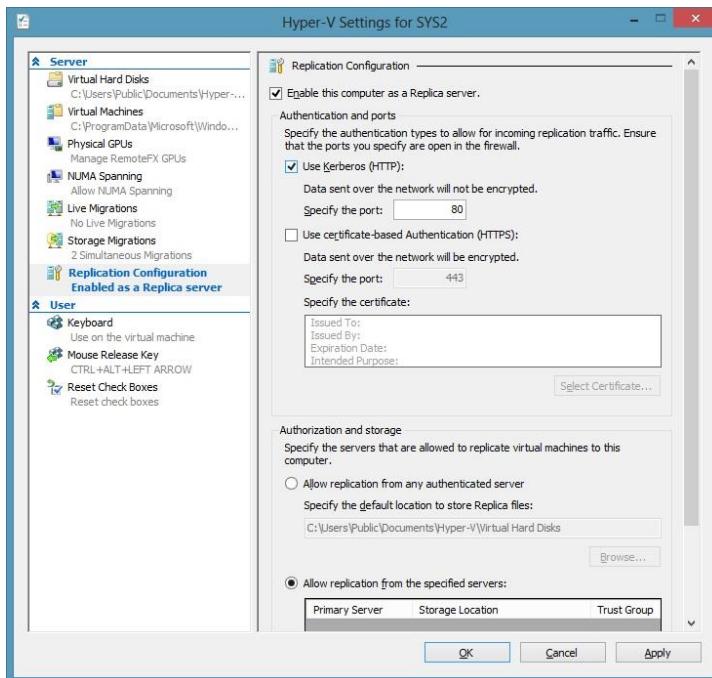
4. Go to Start, select **Hyper-V Manager**.



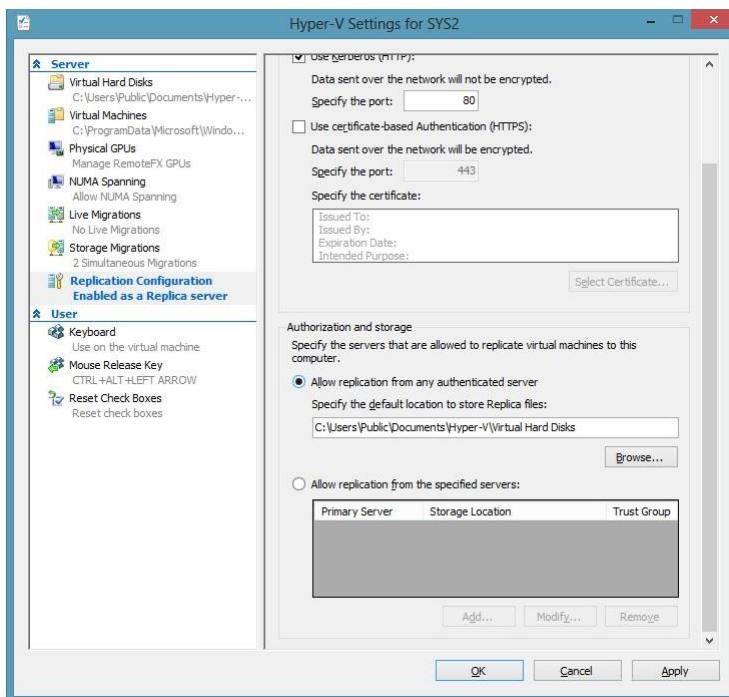
5. In Hyper-V Manager, right click on Server Name (**SYS2**) and select **Hyper-V Settings**



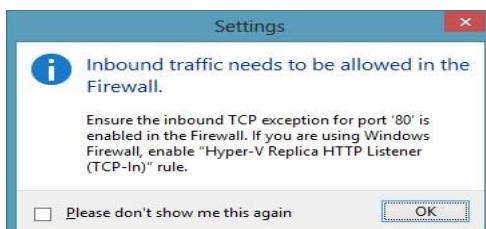
- 6. Select Replication Configuration, check box **Enable this Computer as a Replica server** and check **Use Kerberos (HTTP)****



- 7. In Authorization, select **Allow replication from any authenticated server****

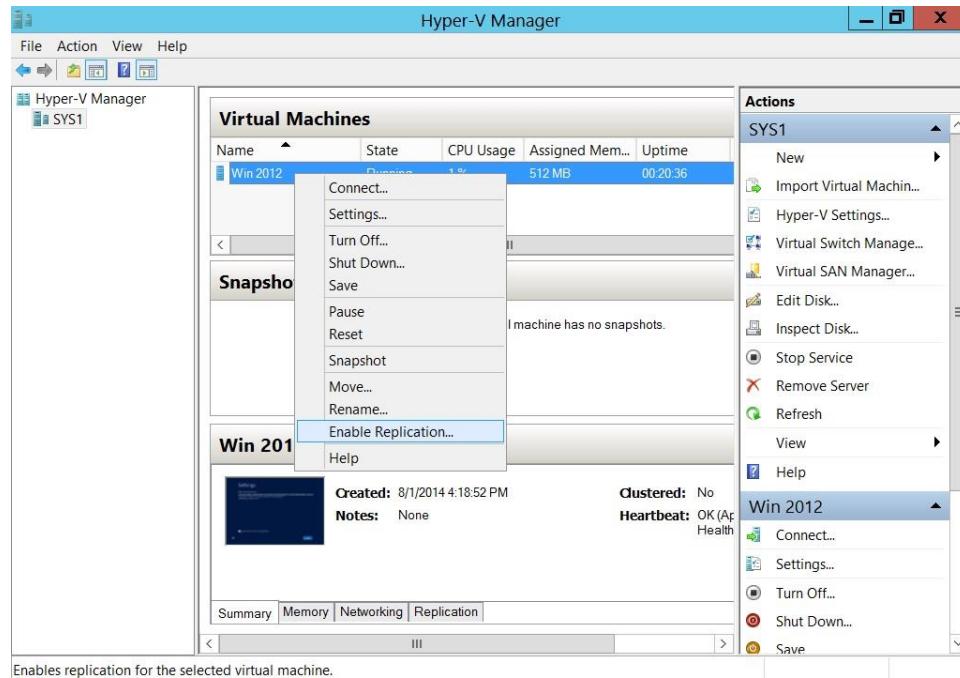


- 8. Click **OK**.**

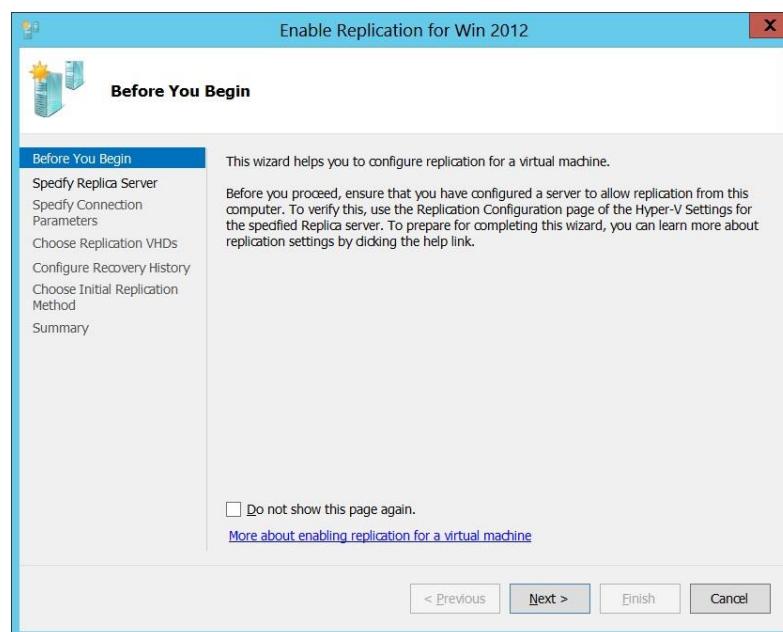


SYS1 – CONFIGURATION

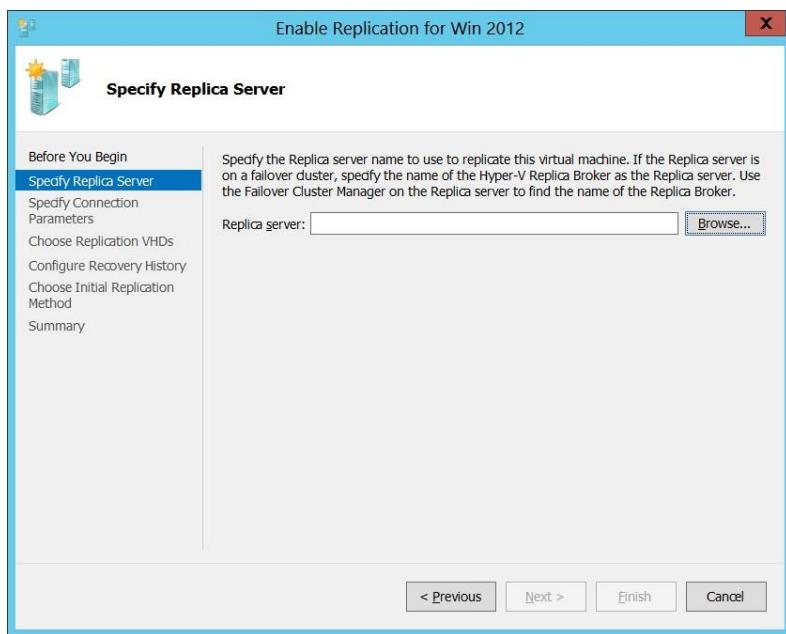
1. Go to Start, Hyper-V Manager, right click on virtual machine (Win 2012) and select **Enable Replication**.



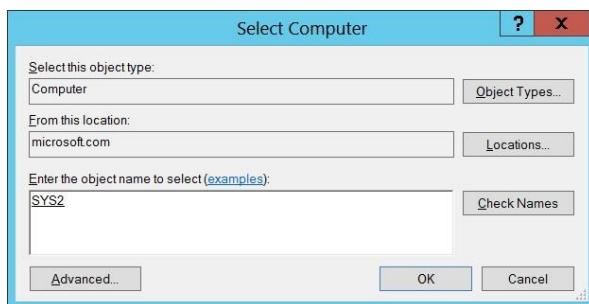
2. In Before you Begin Page, click **Next**.



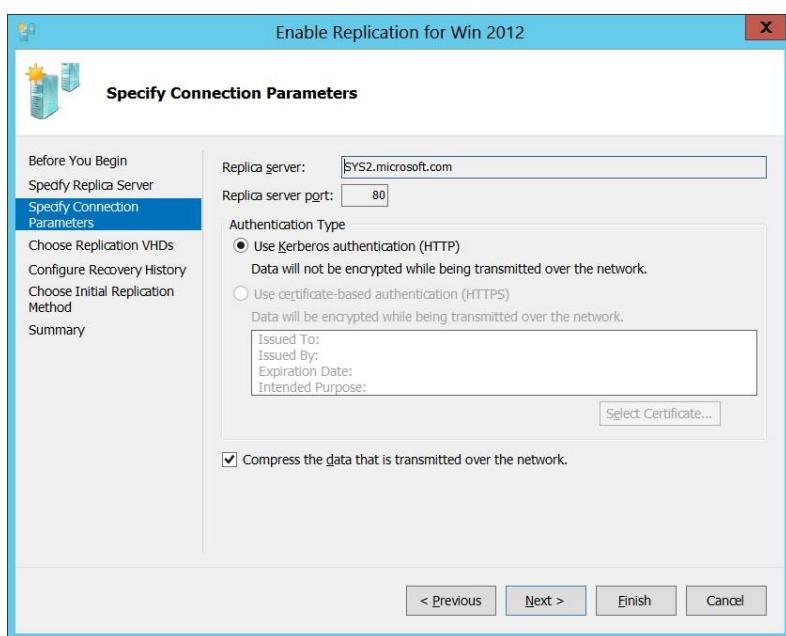
3. Click **Browse**.

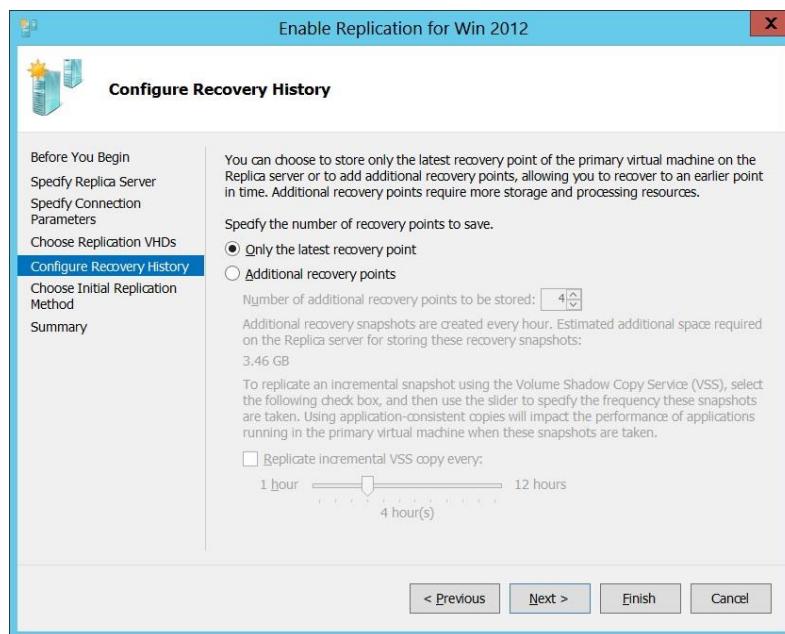
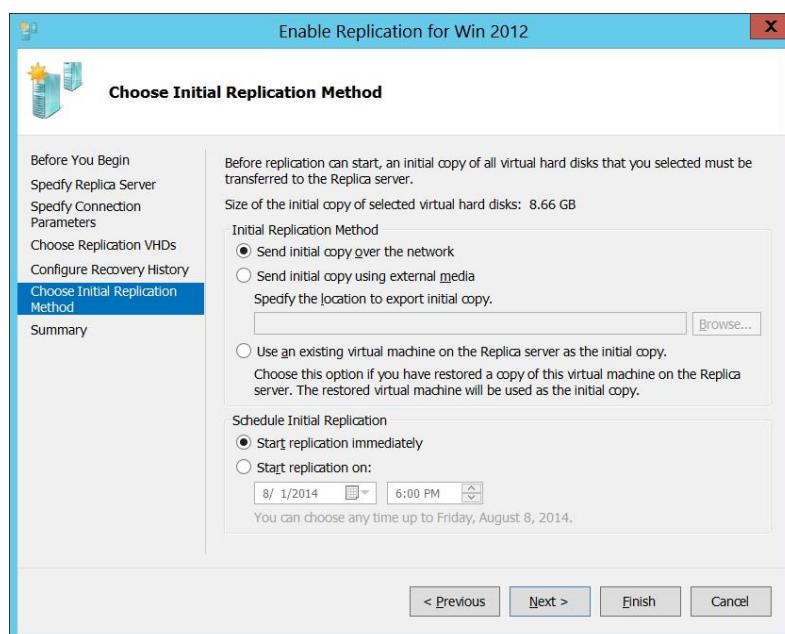


4. Enter the server name **SYS2**, click **OK**.

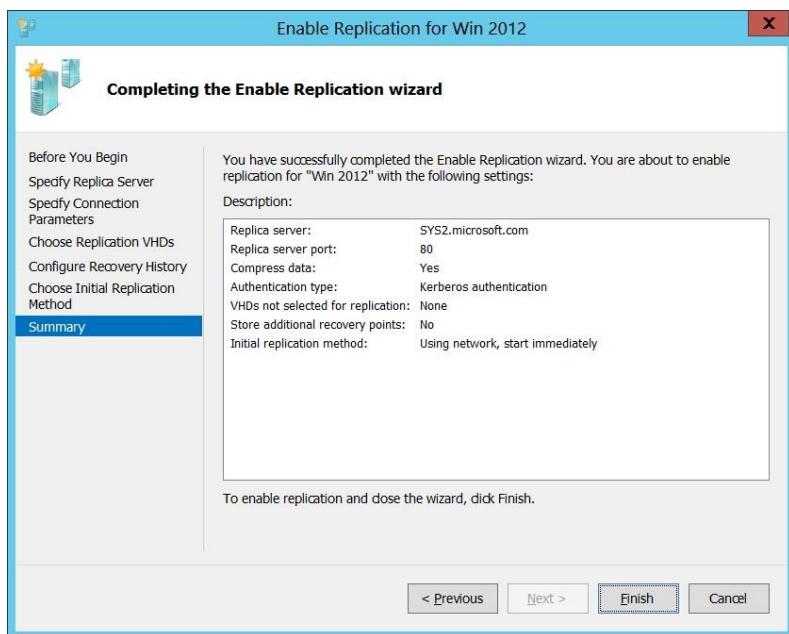


5. Click **Next**, accept the defaults click **Next**.

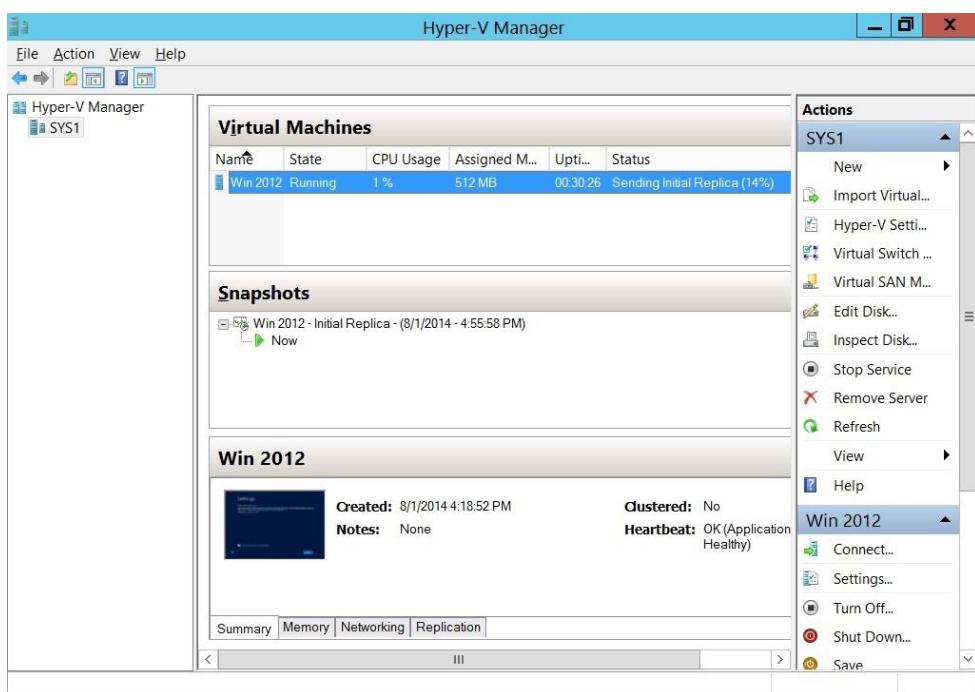


6. Click **Next**.7. Select **Initial Replication Method**, click **Next**.

8. Click Finish.

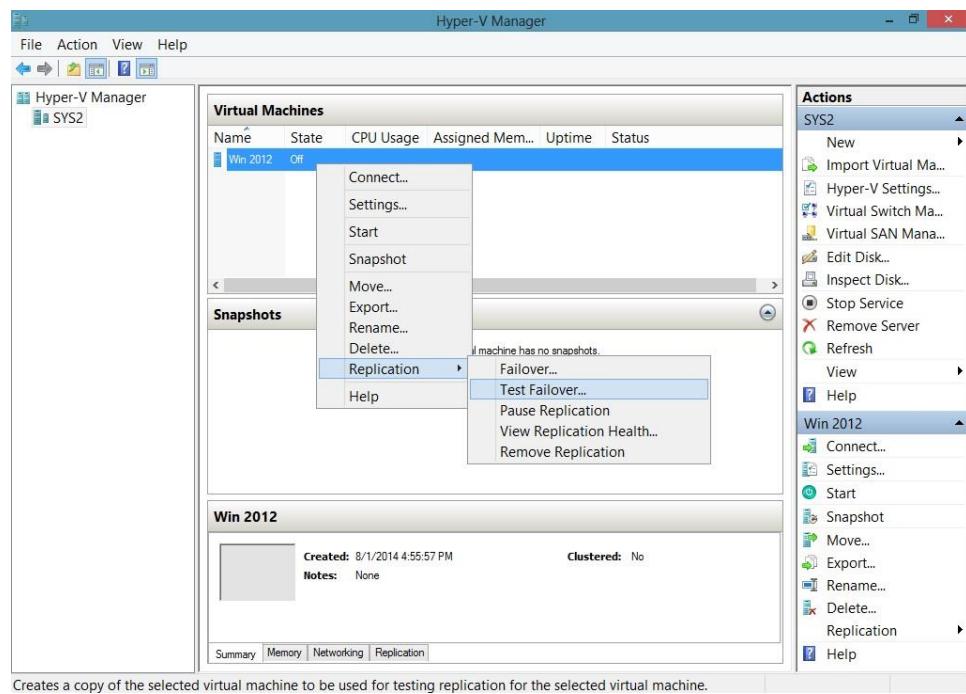


9. Verify for Sending Initial Replication.



Verification:

1. Go to Hyper-V Manager Console, and verify for replicated Virtual Machine.
2. To Test Failover, right on the virtual machine → select Replication and click Test Failover.



ROUTING

Definition

ROUTER

It is a device used to communicate between two different networks.

ROUTING

It is a process of sending the data packets through the best path to reach the destination.

DEFAULT GATEWAY

It gives the exit point (or) entry point to reach the destination.

Types of Routing

Static Routing

Routes should be added manually on the router by the administrator.

Dynamic Routing

Routes will be added automatically by the router with the help of routing protocols

Types of Routers

Software Router

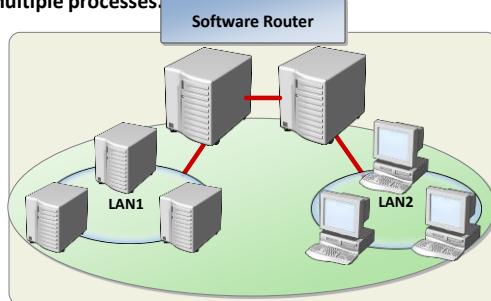
It is a computer which performs routing task as one of its multiple tasks.

Hardware Router

It is a Dedicated HARDWARE DEVICE which works only as a router.

Routing and Remote Access Service (RRAS)

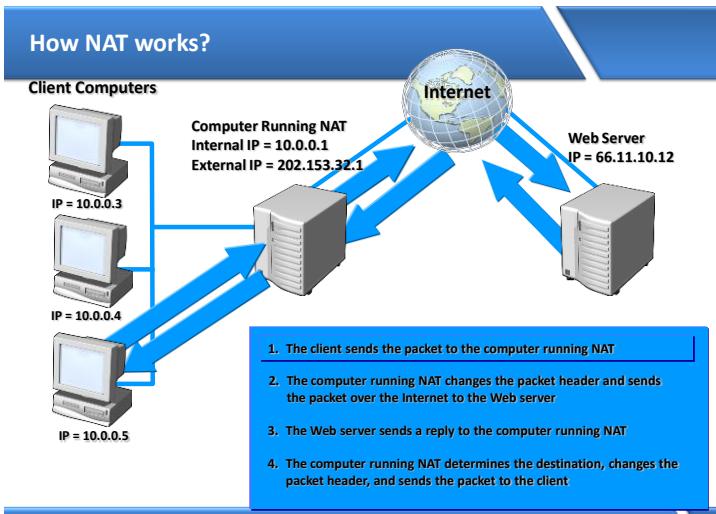
- Routing and Remote Access is a service that performs routing as one of its multiple processes.



NAT

NETWORK ADDRESS TRANSLATION

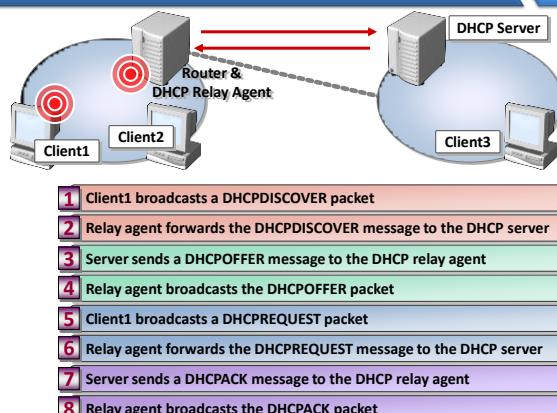
- Provides access to Internet from a protected private address range
- Translates Private IP's to Public IP's & vice-versa for outgoing and incoming traffic
- Hides private IP address range from the Internet
- Can be used with DHCP or can be configured to assign IP to Client



DHCP Relay Agent

- A DHCP Relay agent is a computer or router that listens for DHCP Broadcasts from DHCP clients and then relays(sends) those messages to DHCP Servers on the another network.

How a DHCP Relay Agent Works?

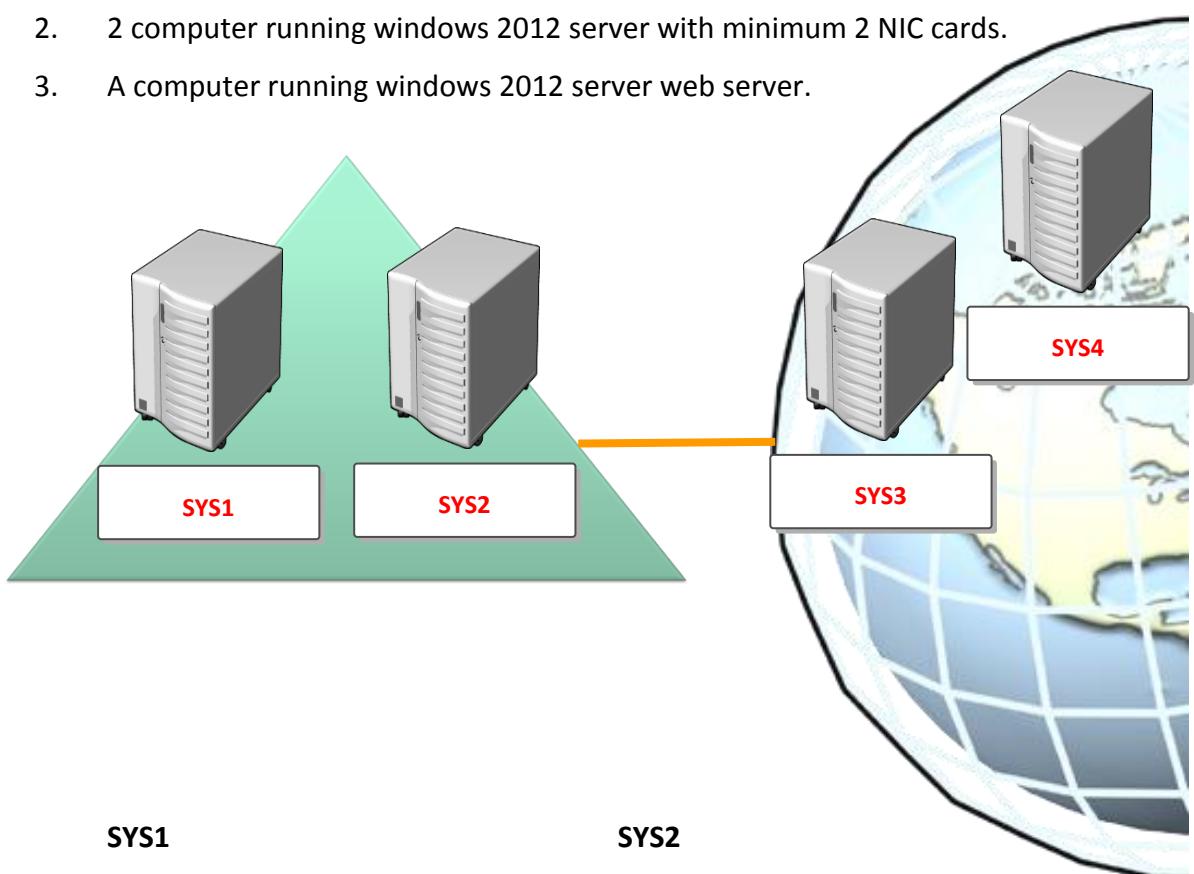


ROUTING

Prerequisites:

Before working on this lab, you must have

1. A computer running windows 2012 server Domain Controller.
2. 2 computer running windows 2012 server with minimum 2 NIC cards.
3. A computer running windows 2012 server web server.

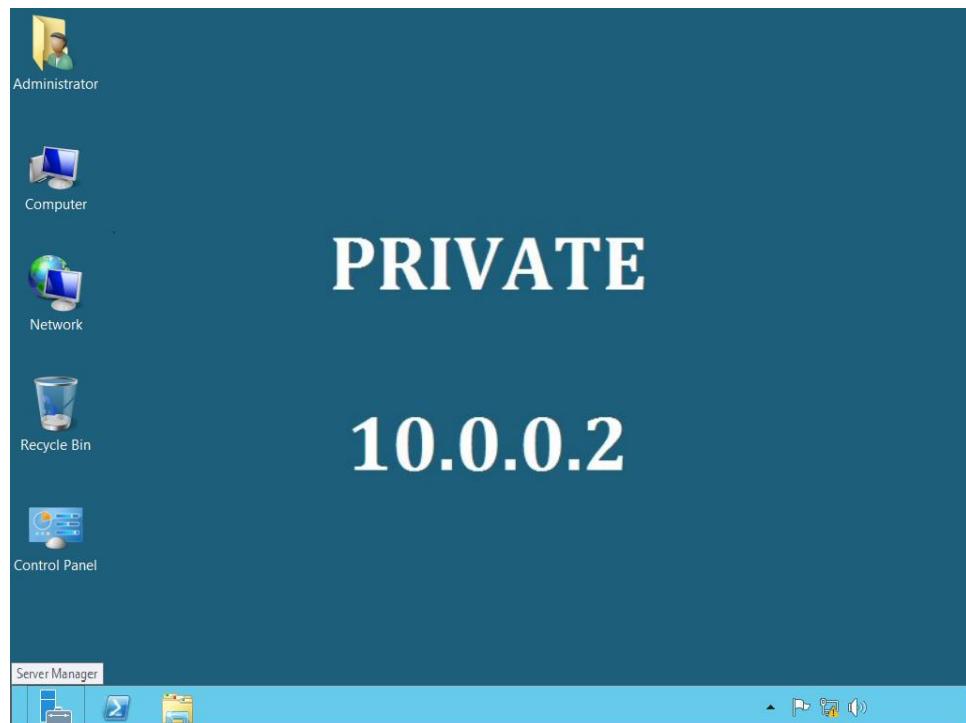


SYS1		SYS2	
Domain Controller / DNS Server		Router - I	
IP Address	10.0.0.2	IP Address	10.0.0.1, 11.0.0.1
Subnet Mask	255.0.0.0	Subnet Mask	255.0.0.0
Gateway	10.0.0.1	Gateway	-----
DNS Server	10.0.0.2, 12.0.0.2	DNS Server	10.0.0.2
SYS3		SYS4	
Router – II		Web server / DNS Server	
IP Address	11.0.0.2, 12.0.0.1	IP Address	12.0.0.2
Subnet Mask	255.0.0.0	Subnet Mask	255.0.0.0
Gateway	-----	Gateway	12.0.0.1
DNS Server	12.0.0.2	DNS Server	12.0.0.2, 12.0.0.1

Lab – 1: Assigning the IP Address to Configure Routing

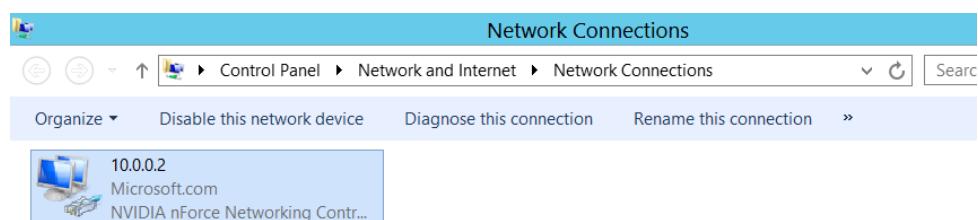
ON PRIVATE:

1. Logon to **Private**.

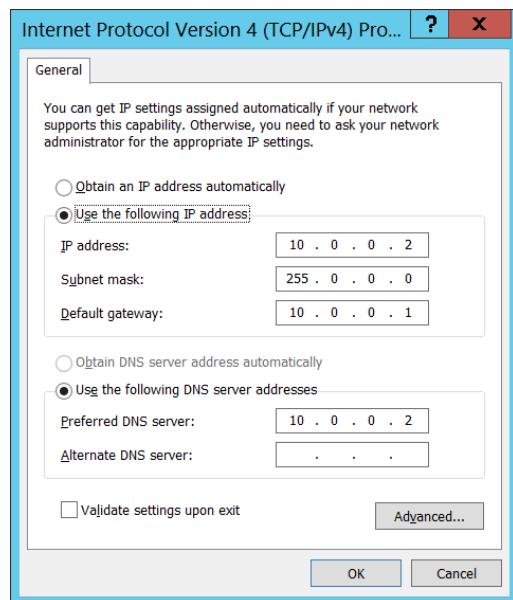


2. Check the IP settings:

Go Server Manager → Local Server → click 10.0.0.2, Right click **NIC card** → click **Properties**

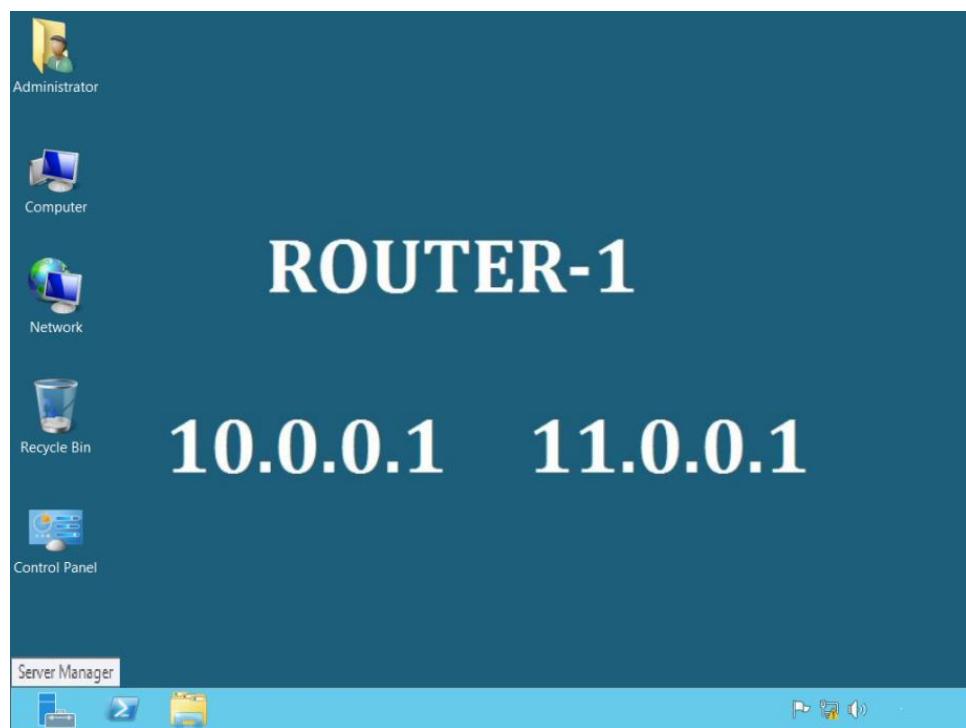


3. Right click NIC card → click Properties → Internet Protocol Version4 (TCP/IPv4) → Properties → Define the IP address as mentioned below.



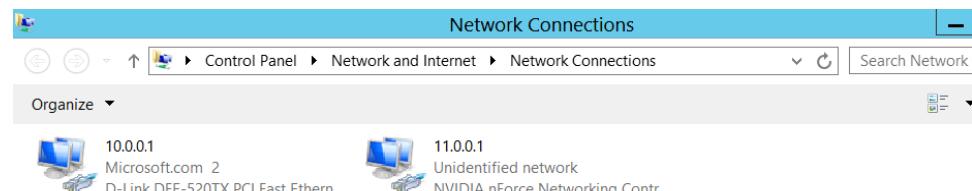
ON ROUTER 1:

1. Logon to **Router1**



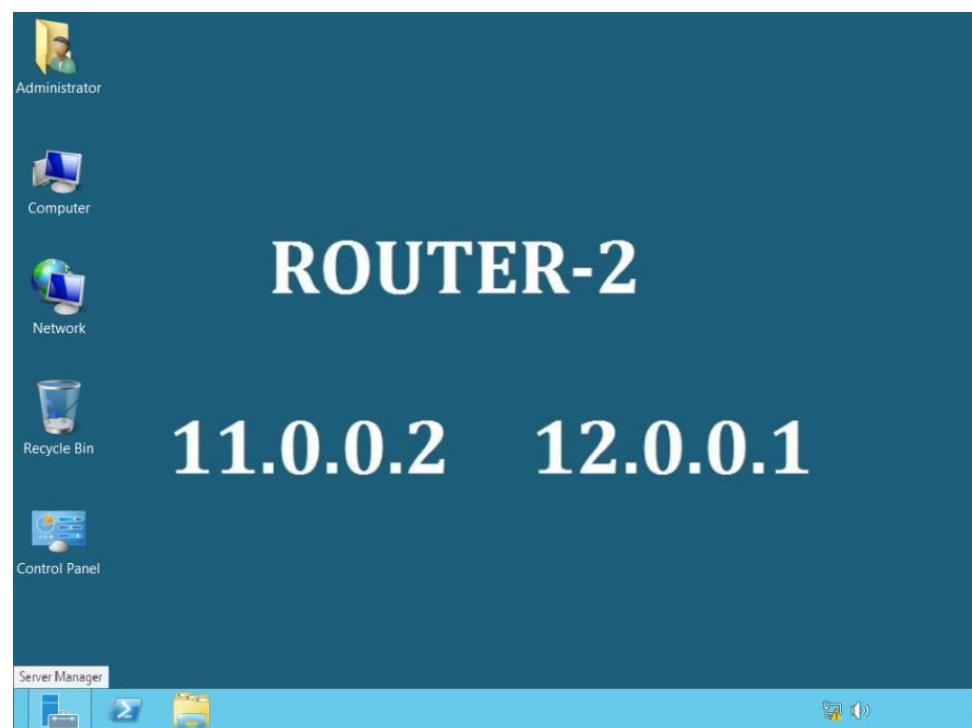
2. **Check the IP settings:**

Go Server Manager → Local Server → click 10.0.0.1, Right click NIC card → click Properties → Internet Protocol Version 4 (TCP/IPv4) → Properties → Define the IP address as mentioned below.



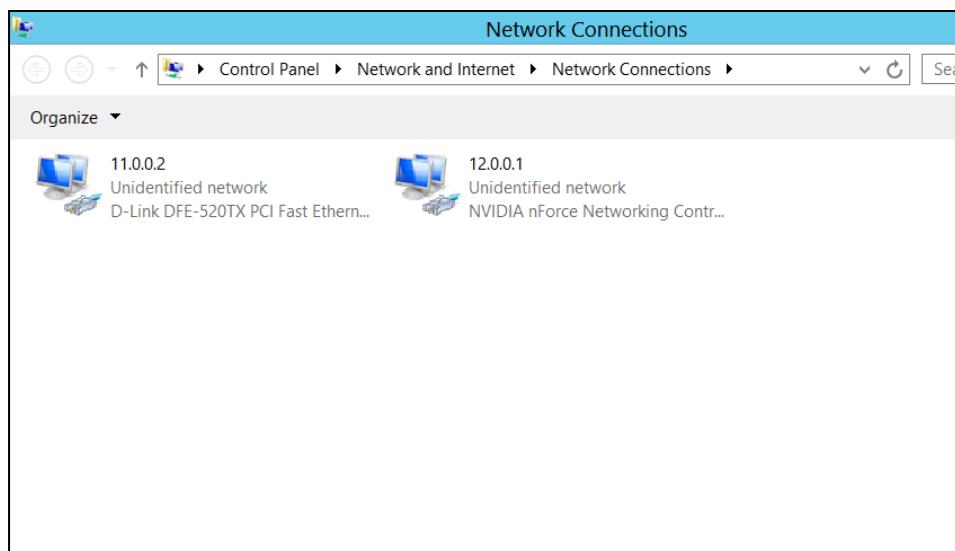
On ROUTER 2:

1. Log on to Router2



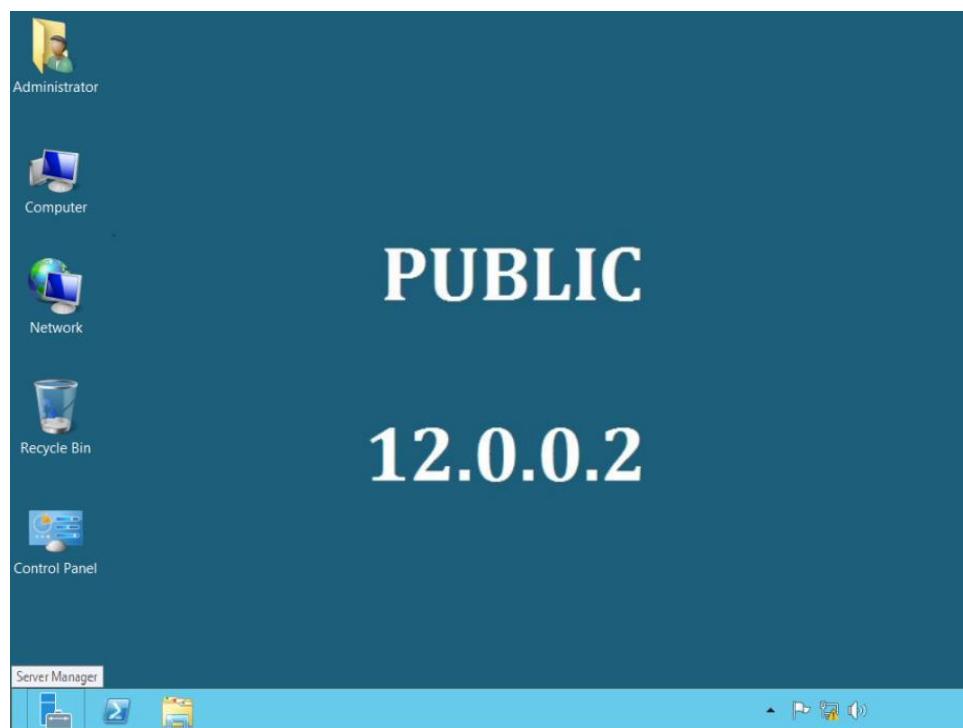
2. **Check the IP settings:**

Go Server Manager → Local Server → click 11.0.0.2, Right click NIC card → click Properties → Internet Protocol Version 4 (TCP/IPv4) → Properties → Define the IP address as mentioned below.



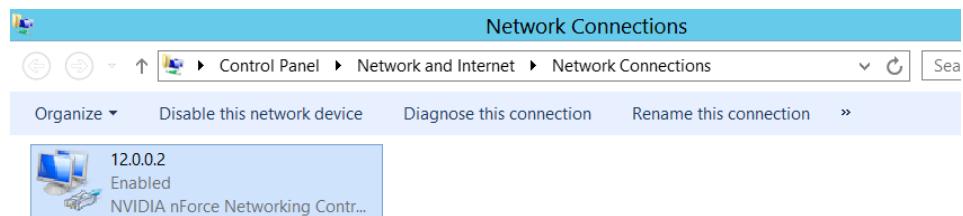
On PUBLIC:

1. Logon to **Public**

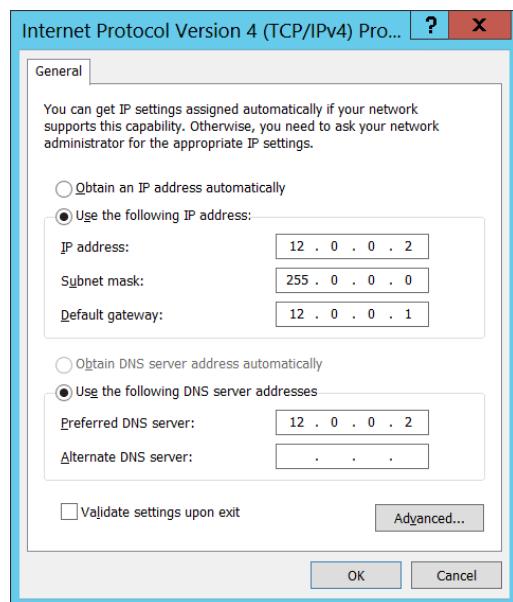


2. Check the IP settings:

Go Server Manager → Local Server → click 12.0.0.2,

**3. Right click on NIC card → click Properties → Internet Protocol Version 4 (TCP/IPv4)**

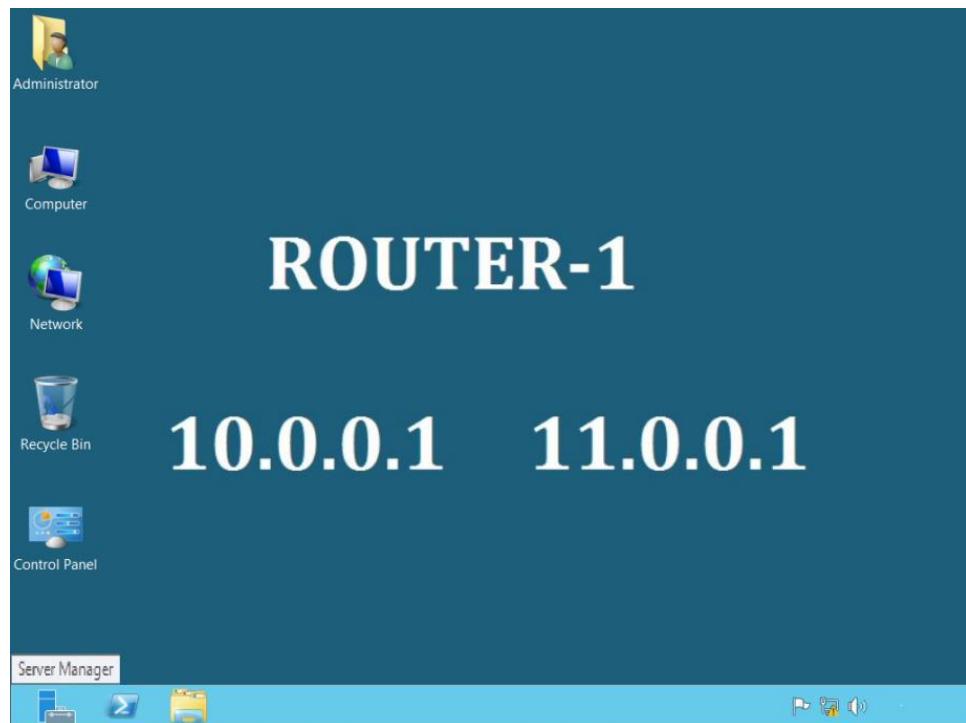
→ **Properties** → Define the IP address as mentioned below.



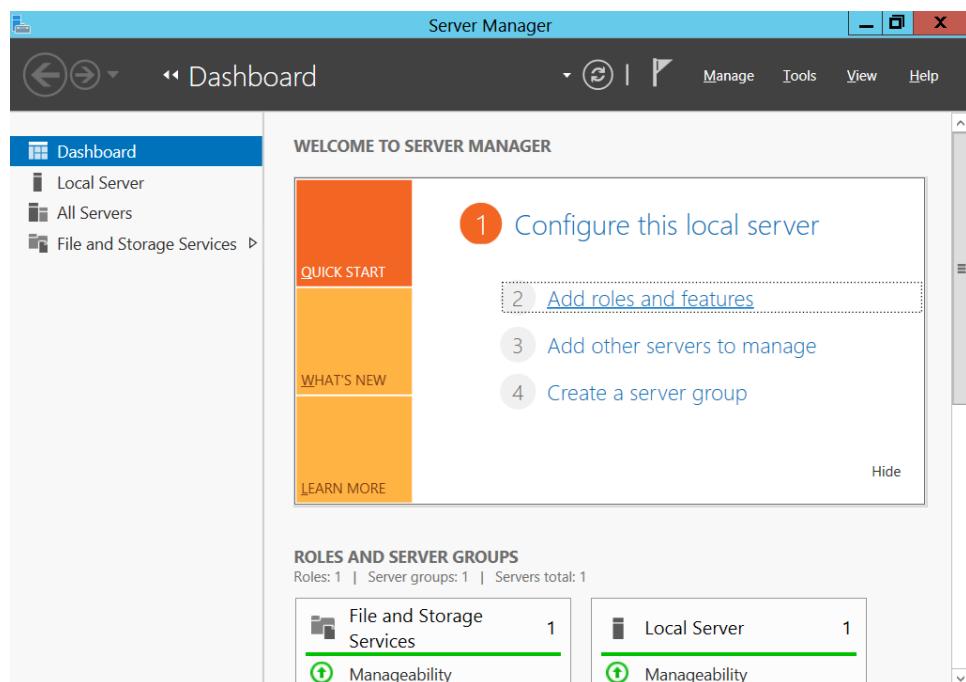
Lab – 2: Installing Routing Service on Router1 & Router2

SYS2– CONFIGURATION

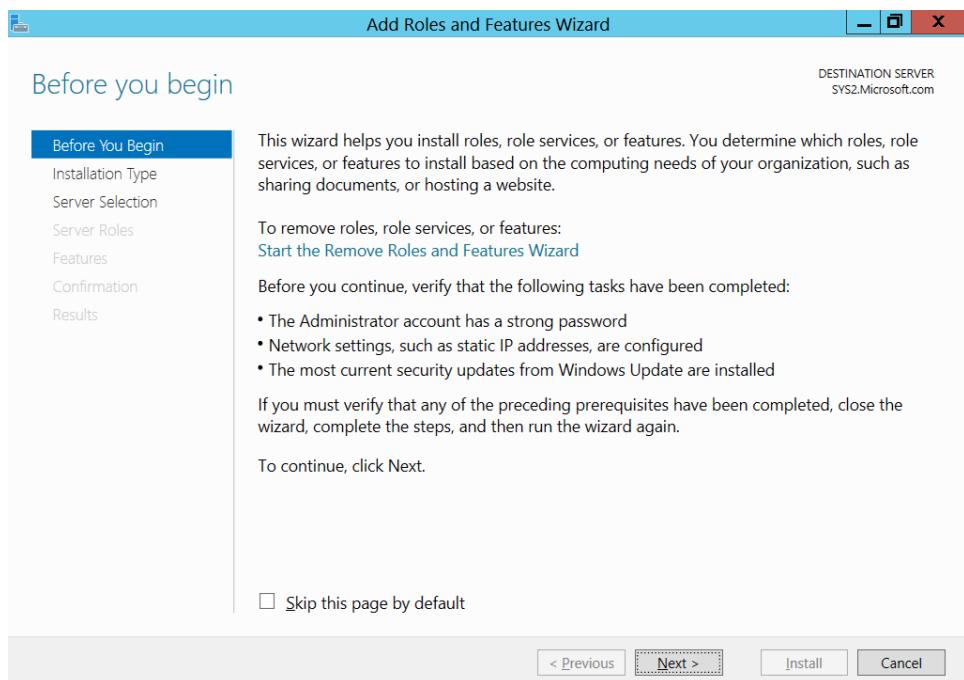
1. Click **Server Manager**



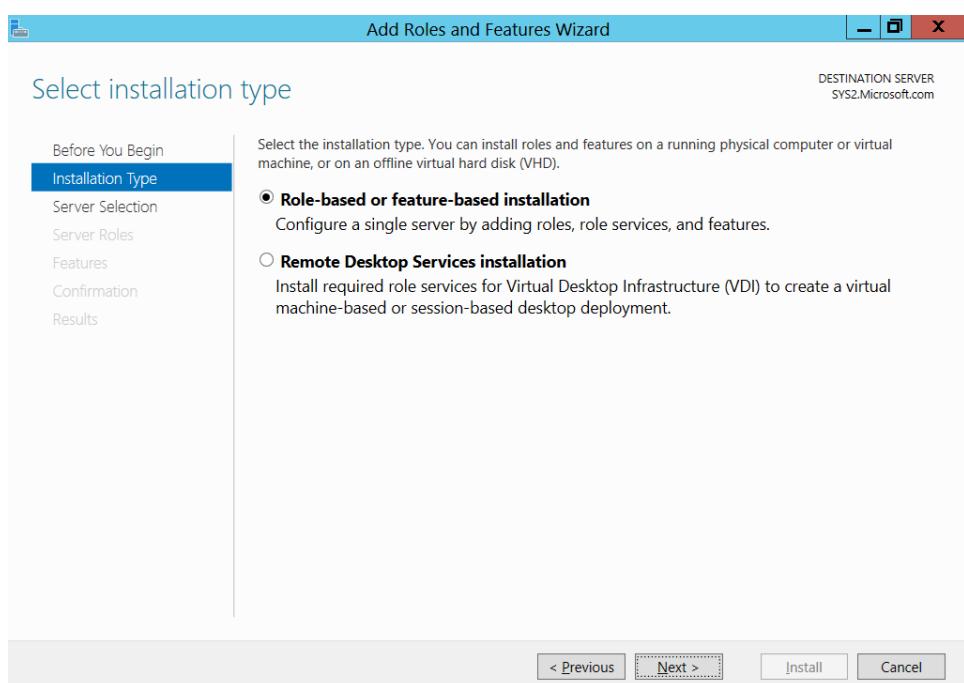
2. Select **Add roles and features**.



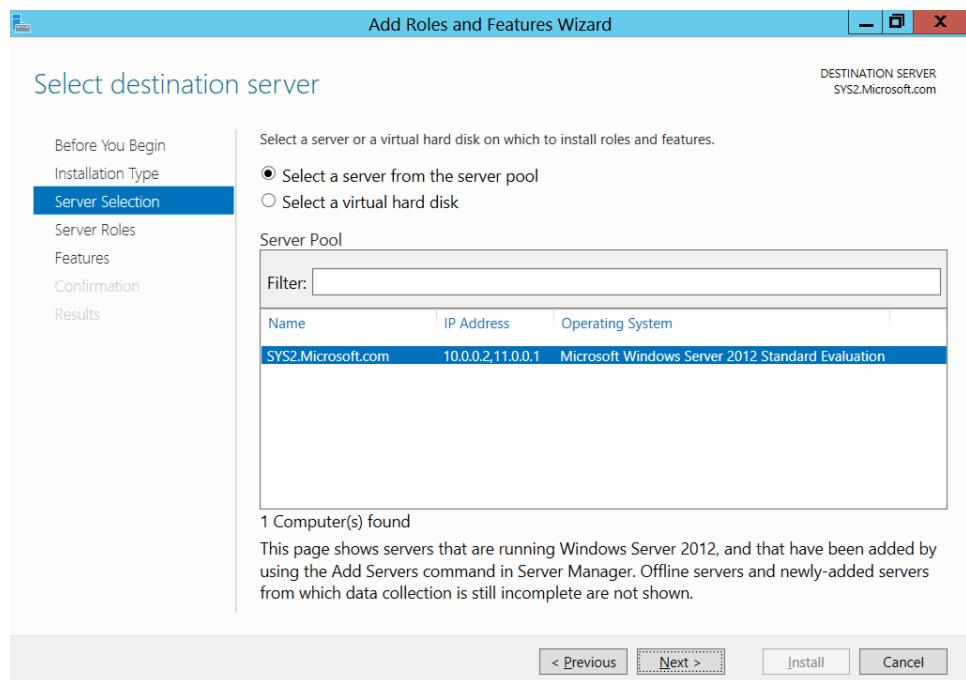
3. In Before you begin page, click **Next**.



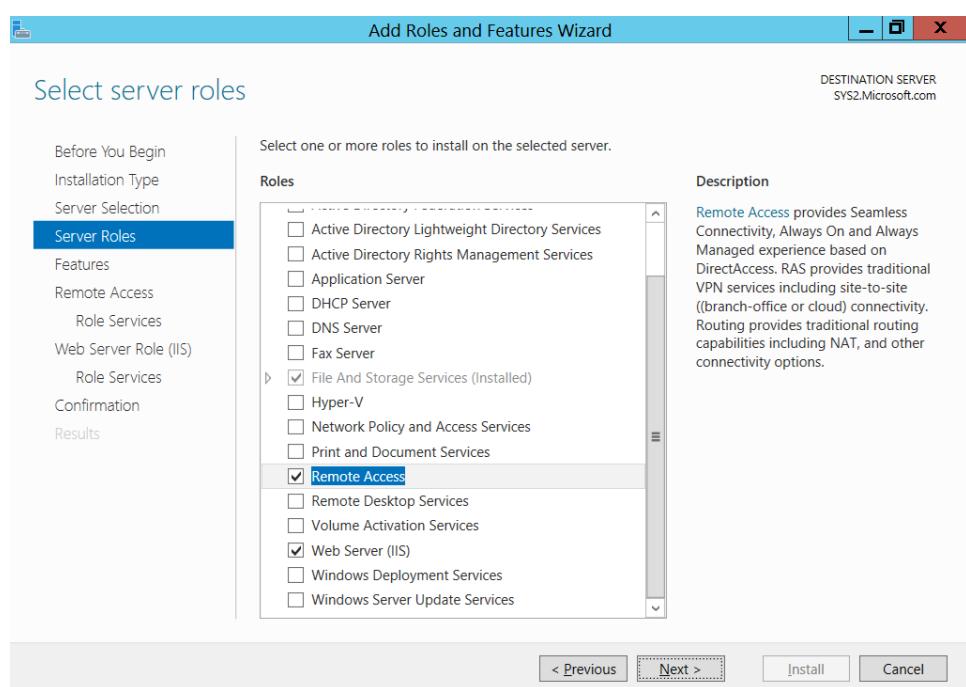
4. Select **Role-based or feature-based installation** → click **Next**



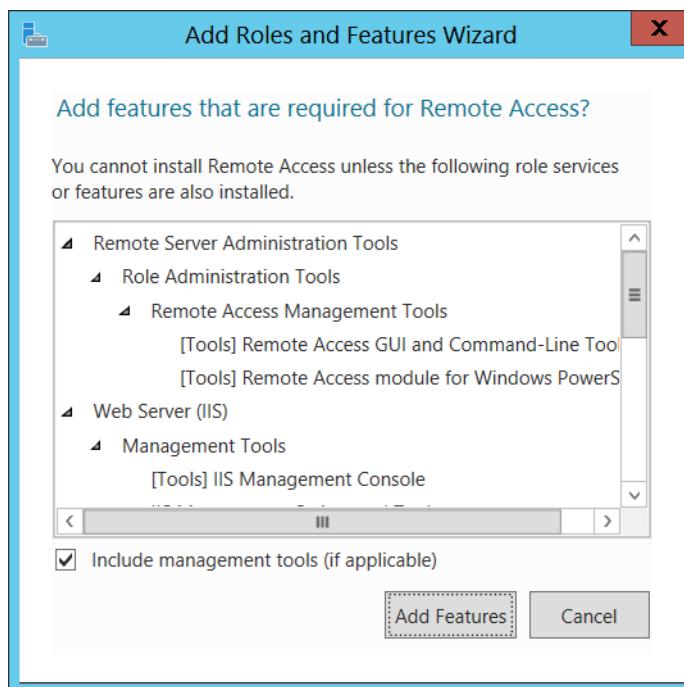
- 5. Select a server (**SYS2.Microsoft.com**) from the server pool and click **Next**.**



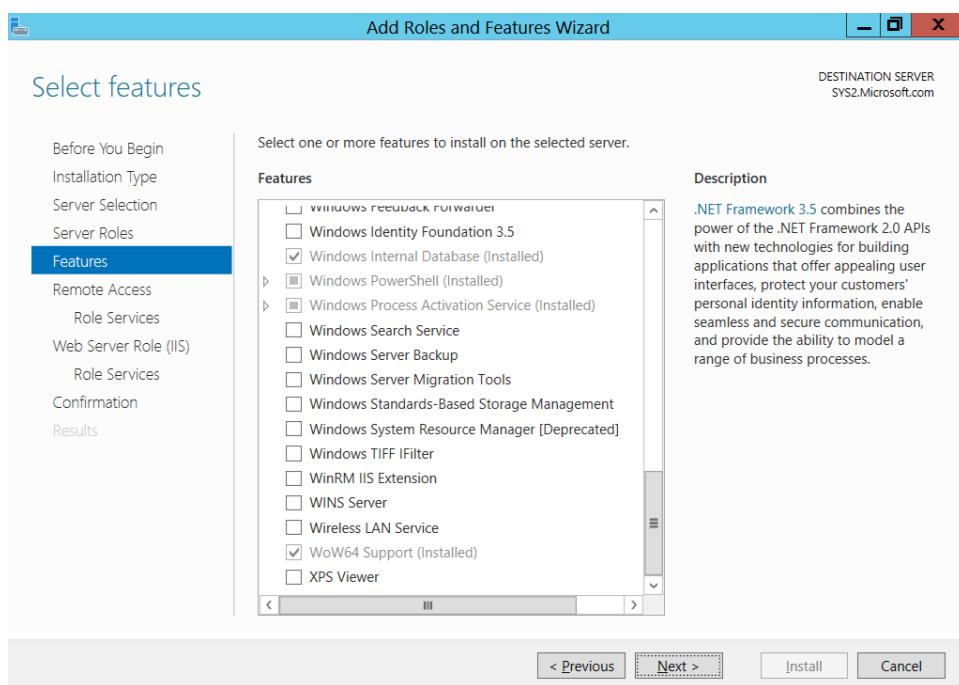
- 6. In select server roles, check the box **Remote Access**.**

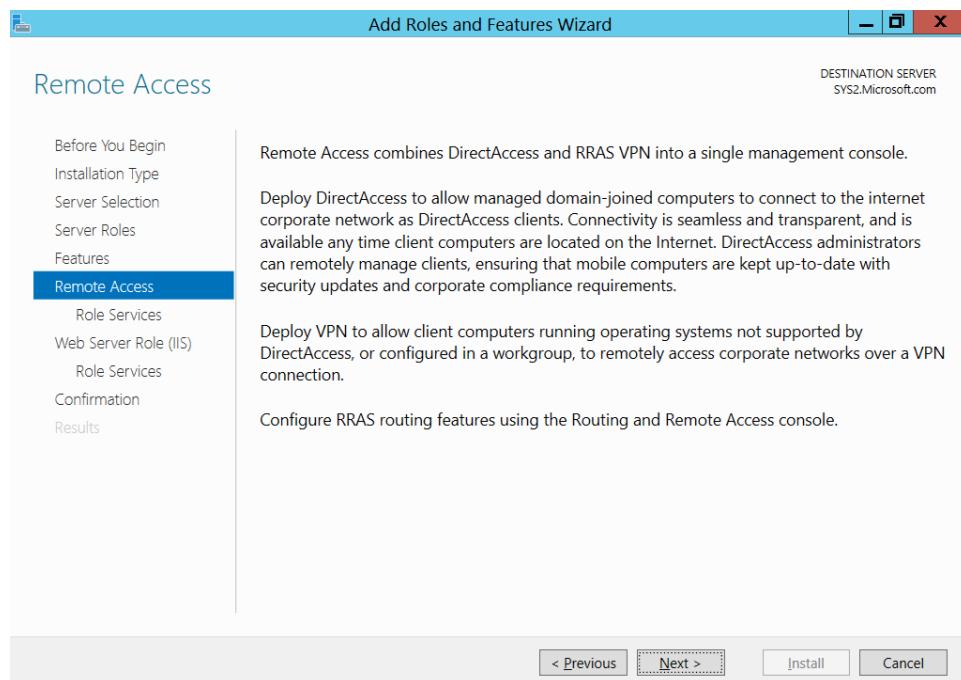
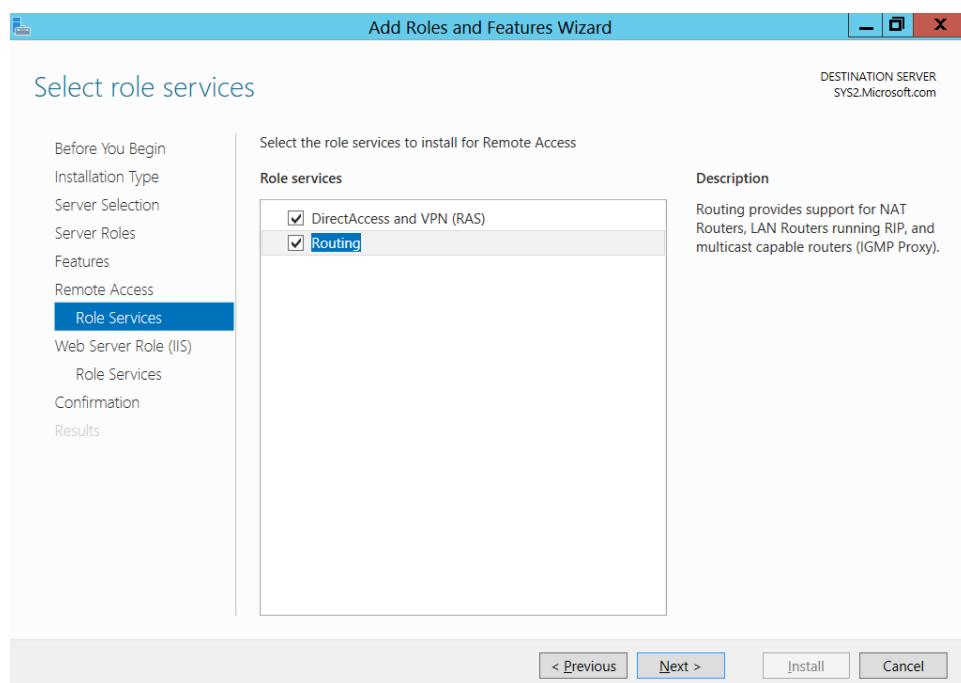


7. Click **Add Features**, to install the required features for Remote Access. Click **Next**.

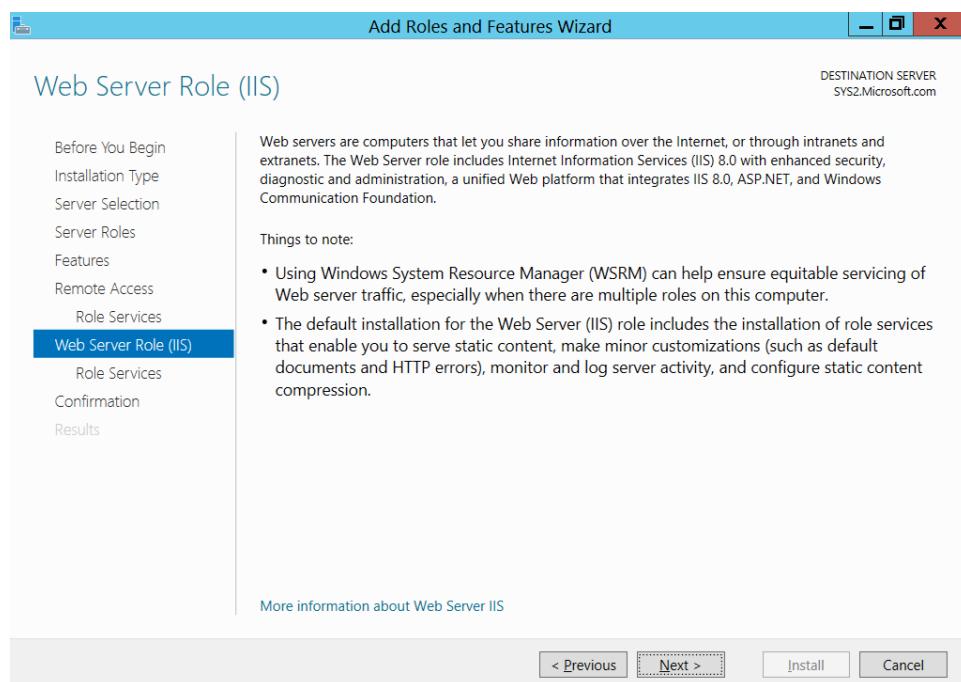


8. In Select features wizard, click **Next**.

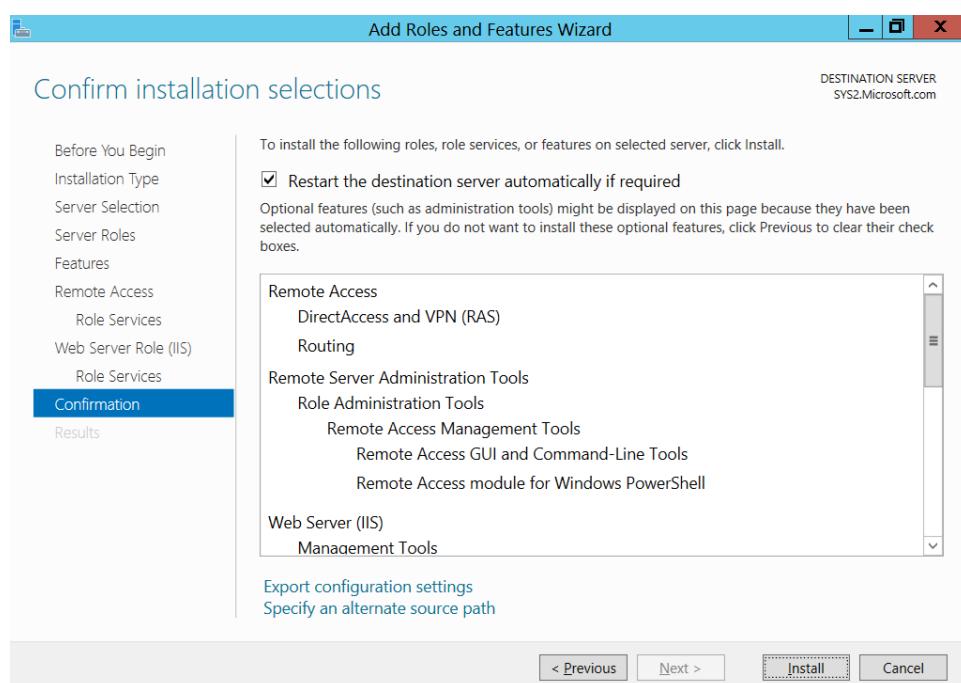


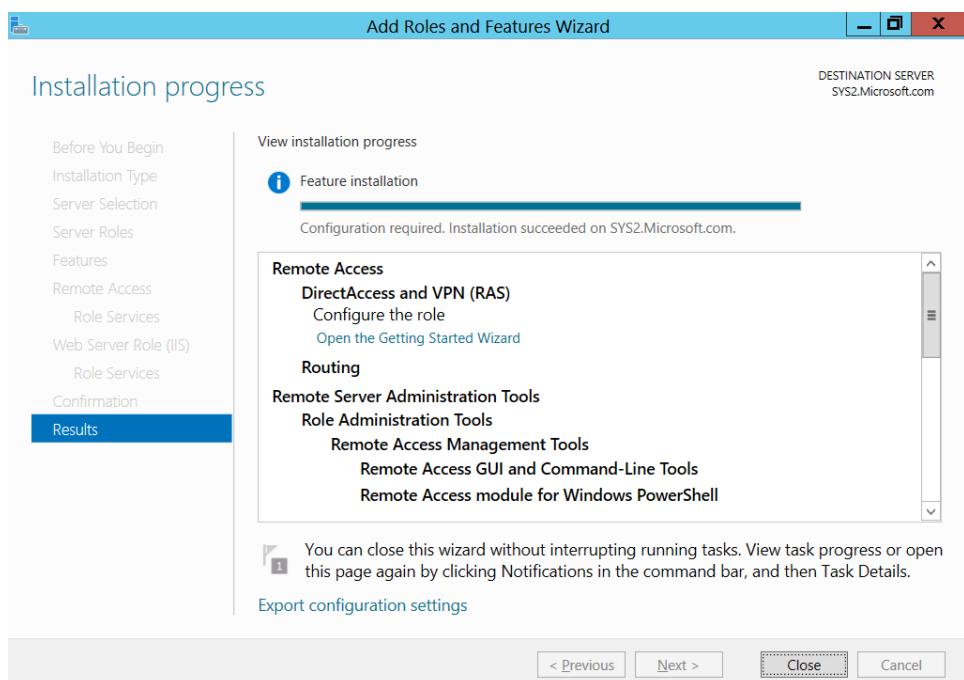
9. In Remote Access Page, click **Next**.10. Check the box **Routing**, click **Next**.

11. In Web Server Role (IIS) Page, click **Next.**



12. Check the box **Restart the destination server automatically if required. Click **Install**.**



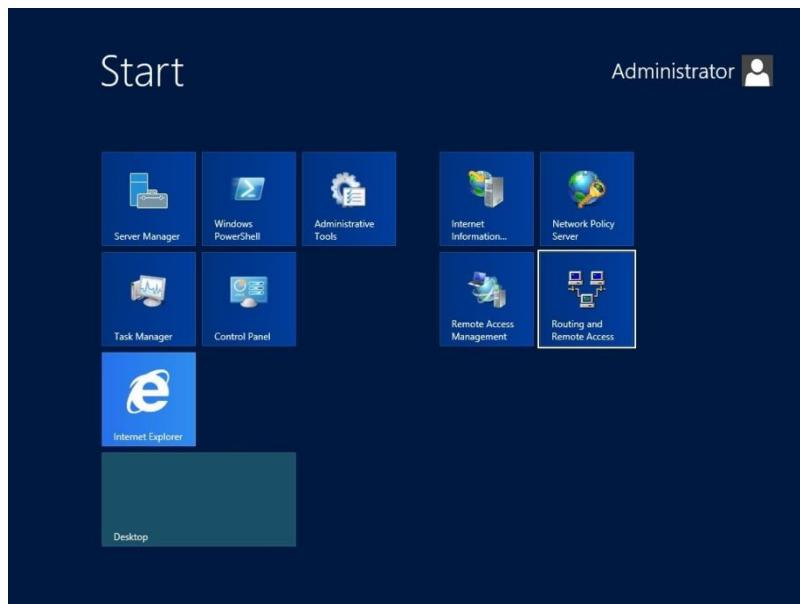
13. Click Close.

Note: - Repeat the process of LAB2 on Router-2 (SYS3) also.

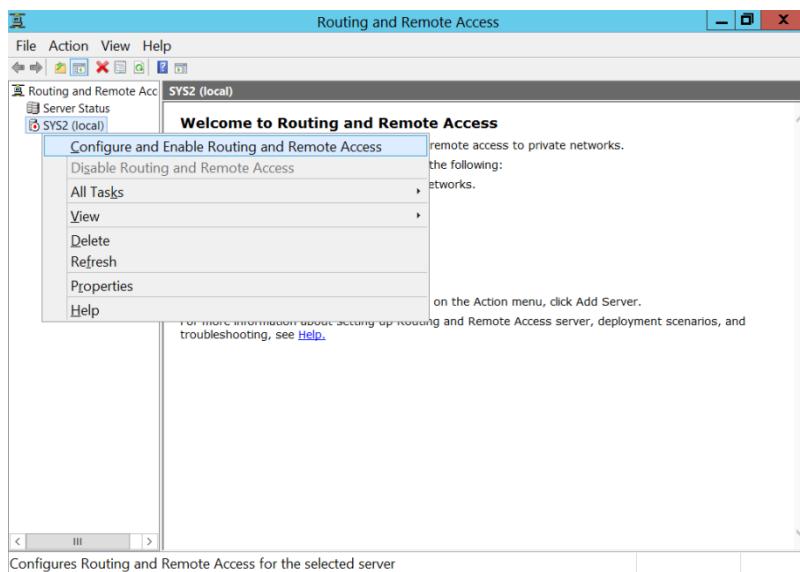
Lab – 3: Enabling Routing on Router1 & Router2

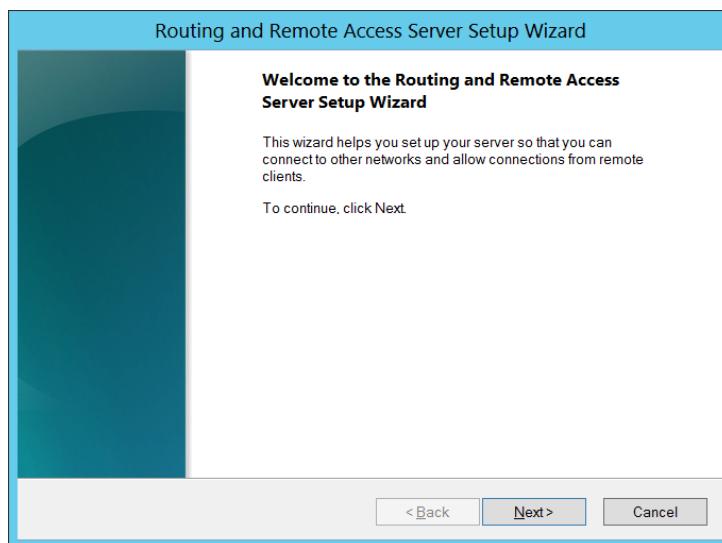
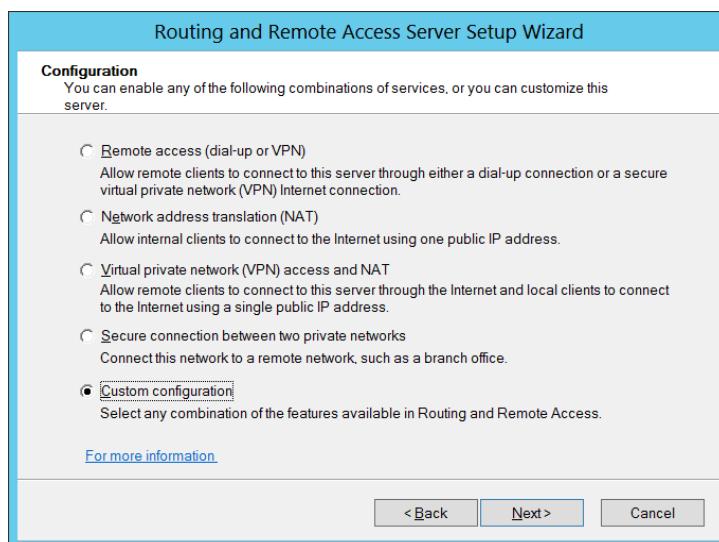
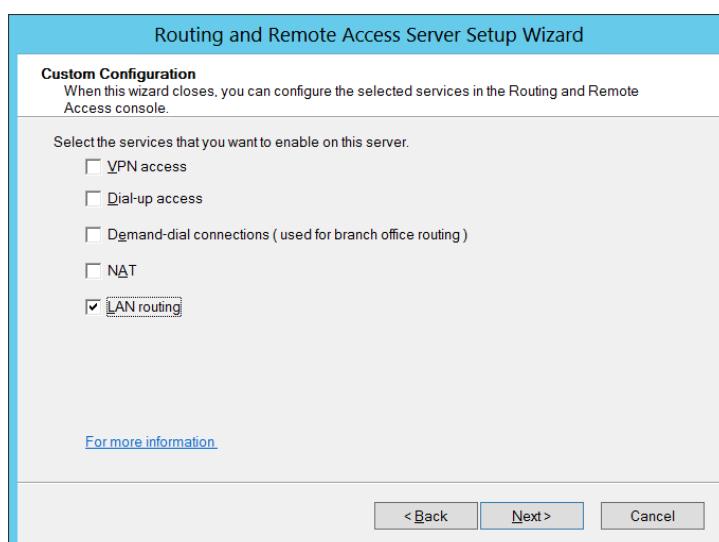
SYS2 – CONFIGURATION

1. Go to Start, select **Routing and Remote Access**.

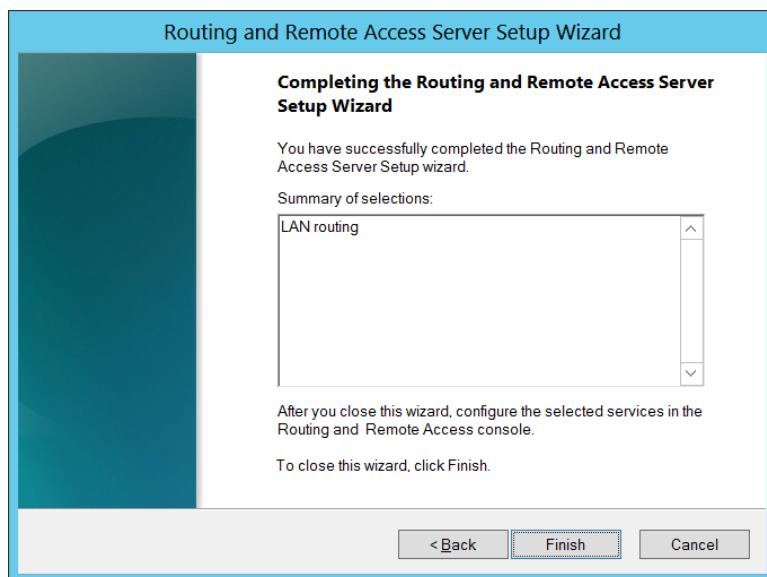


2. Right click on system name **Configure and Enable Routing and Remote Access**.

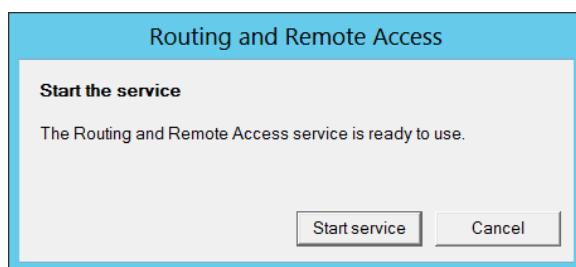


3. Click **Next**4. Select **Custom configuration** → click **Next**.5. Select **LAN routing** → **Next**

6. Click **Finish**



7. Click **Start service**



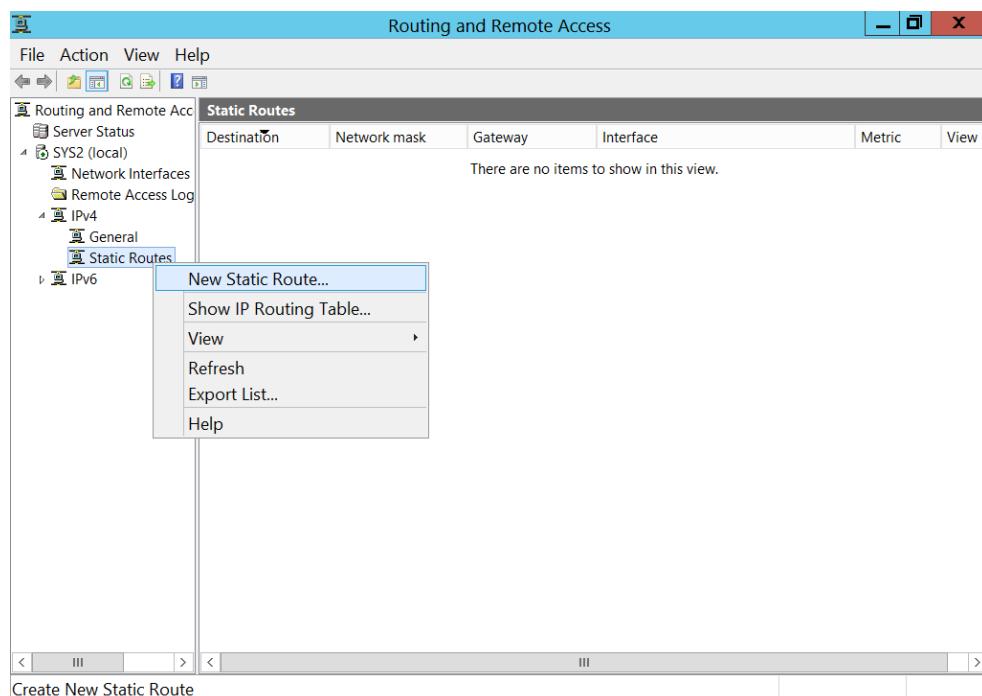
Note: - Repeat the process of LAB3 on Router-2 (SYS3) also.

Lab – 4: Configuring Static Routes

SYS2 – CONFIGURATION

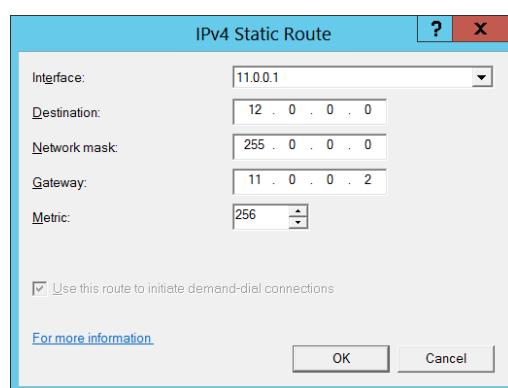
ON ROUTER 1:

1. Go to Routing and Remote access → Expand System name → Expand IPv4 → Select Static Routes → Right click and select New Static Route



2. Define the static route as mentioned below → click OK.

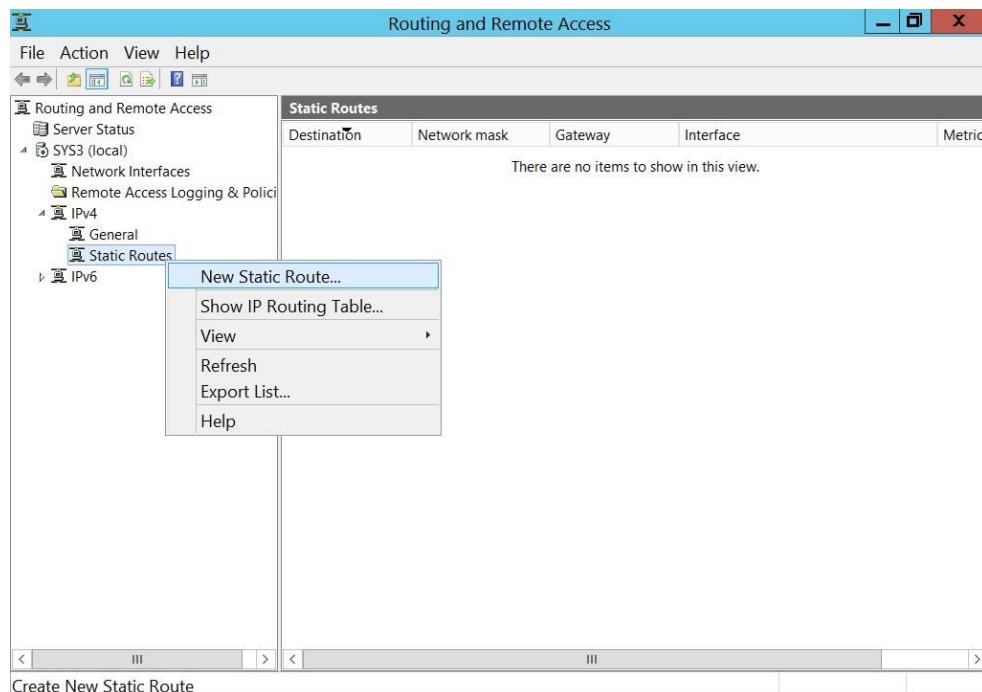
Interface 11.0.0.1
 Destination 12.0.0.0
 Network Mask 255.0.0.0
 Gateway 11.0.0.2
 Metric 256



SYS3 – CONFIGURATION

ON ROUTER 2:

1. Go to Routing and Remote access → Expand System name → Expand IPv4
→ Select Static Routes → Right click and select New Static Route



2. Define the static route as mentioned below → click OK.

Interface 11.0.0.2

Destination 10.0.0.0

Network Mask 255.0.0.0

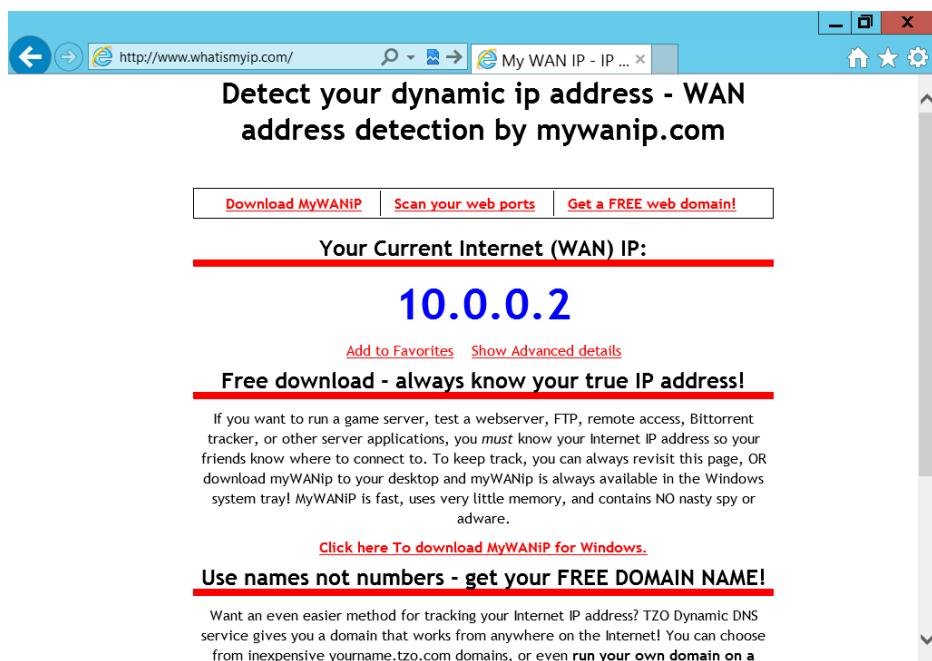
Gateway 11.0.0.1

Metric 256



Verification:

1. Check the connectivity between 10.0.0.0 and 12.0.0.0 Networks.
2. Log on to **SYS4**(12.0.0.2)→open command prompt, **Ping 10.0.0.2 -t** and verify for reply
3. Log on to **SYS1** (10.0.0.2)→Open the Internet Explorer and access the website <http://www.whatismyip.com>(Website is present on 12.0.0.2), to verify the communication between both networks.

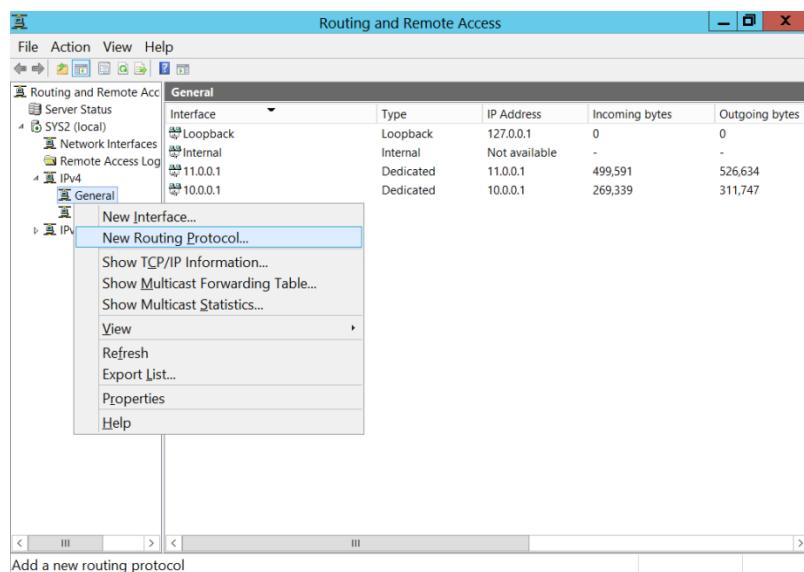


Lab – 5: Configuring Network Address Translation

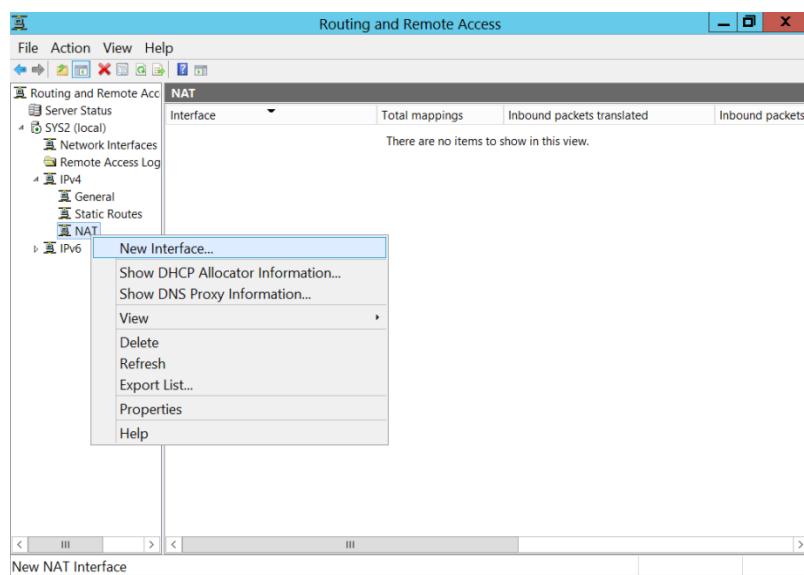
SYS2 – CONFIGURATION

On ROUTER1:

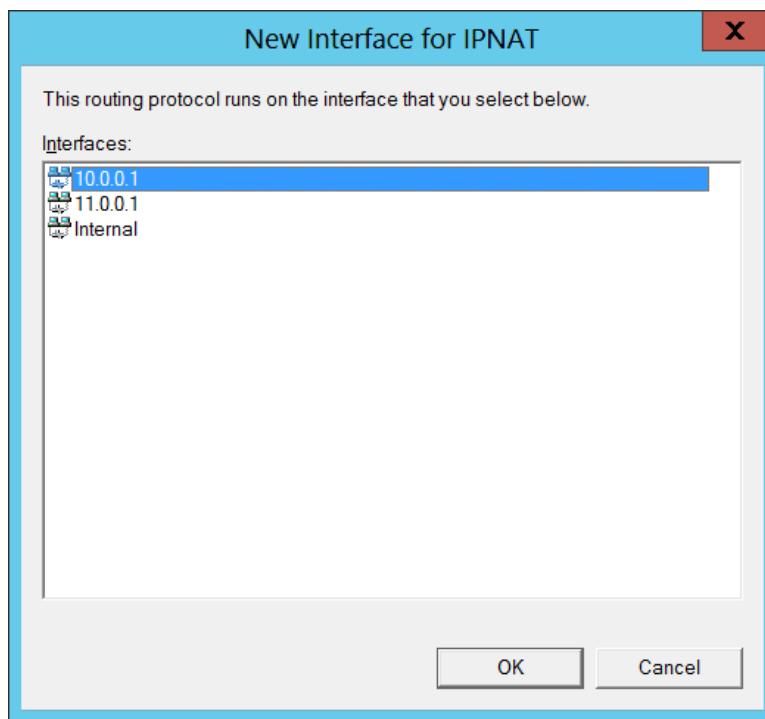
1. Go to Routing and Remote access → Expand System name → Expand IPv4
2. Right click on General → Select New Routing Protocol



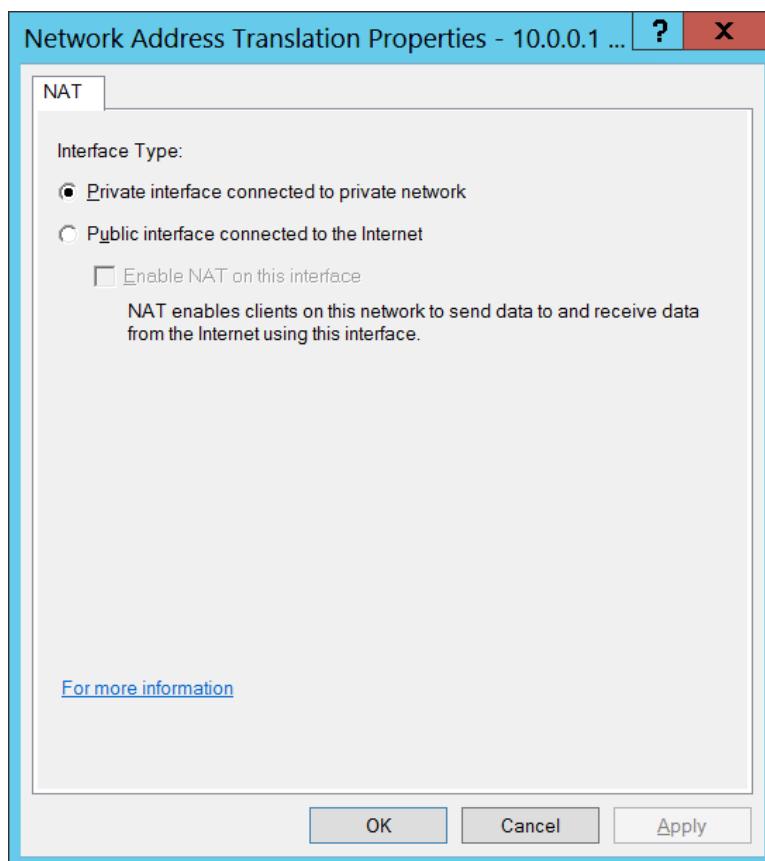
3. Select NAT → click OK
4. Right click on NAT → Select New interface



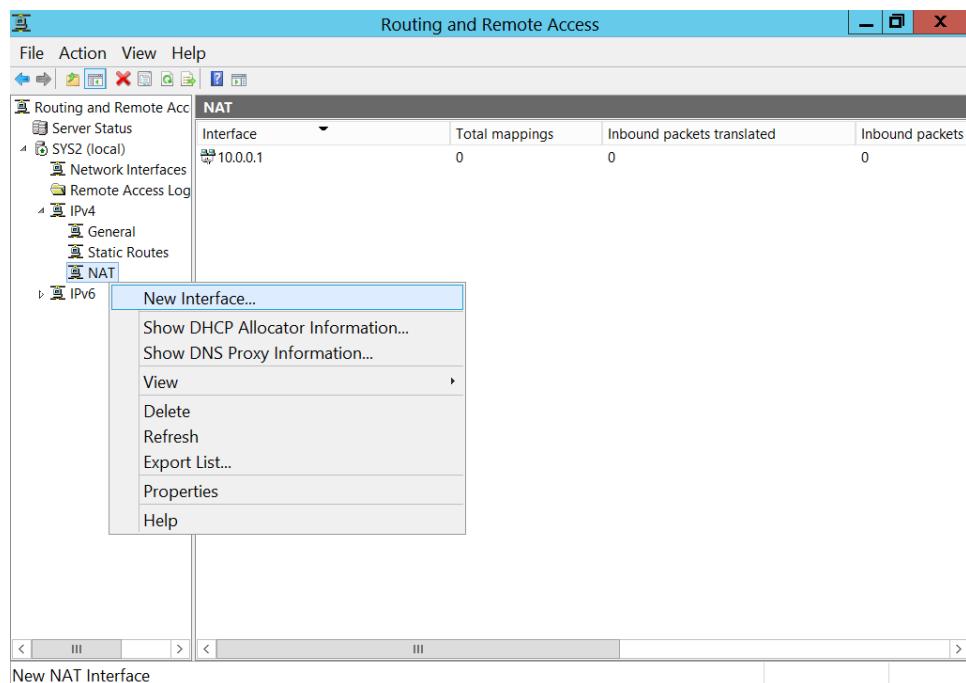
5. Select **LAN** interface → click **OK**



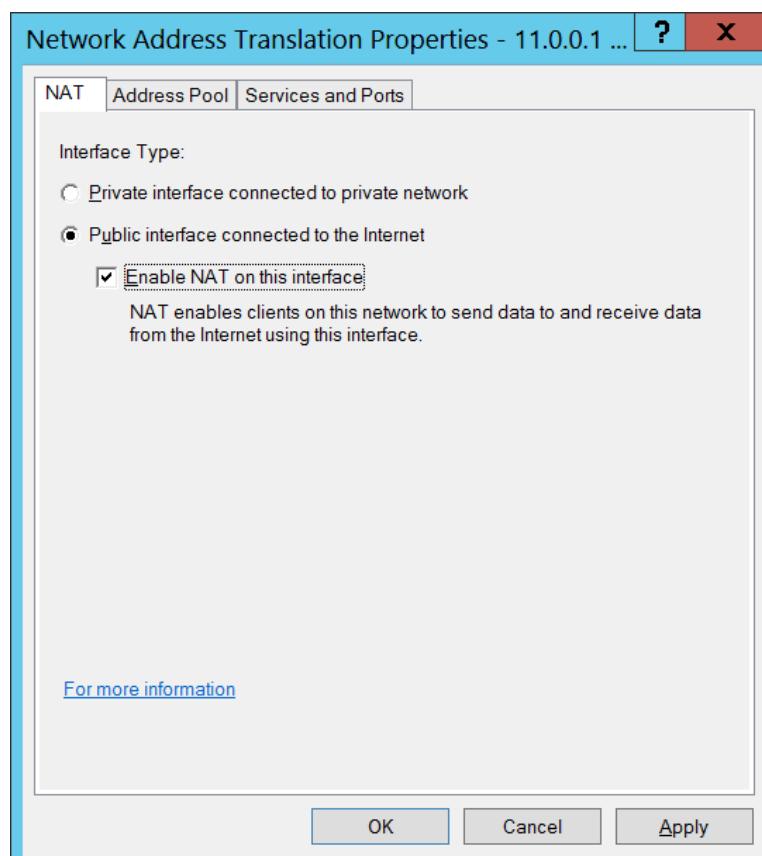
6. Select **Private interface** → click **OK**.



- 7. Again Right click on NAT →Select New interface**



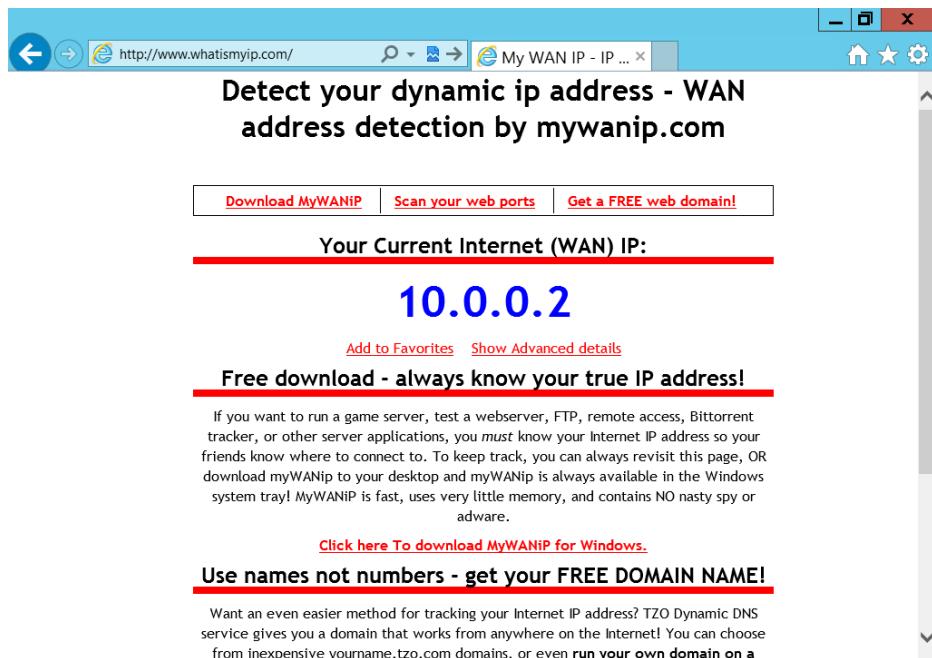
- 8. Select WAN Interface (11.0.0.1)→click OK**
9. Select Public interface, Select Enable NAT →click OK.



Verification:

Before NAT:

On Private → Open Internet Explorer & access <http://www.whatismyip.com> the IP address is shown as 10.0.0.2 Private IP.



Detect your dynamic ip address - WAN address detection by mywanip.com

Your Current Internet (WAN) IP:
10.0.0.2

Add to Favorites Show Advanced details

Free download - always know your true IP address!

If you want to run a game server, test a webserver, FTP, remote access, BitTorrent tracker, or other server applications, you *must* know your Internet IP address so your friends know where to connect to. To keep track, you can always revisit this page, OR download myWANIP to your desktop and myWANIP is always available in the Windows system tray! MyWANIP is fast, uses very little memory, and contains NO nasty spy or adware.

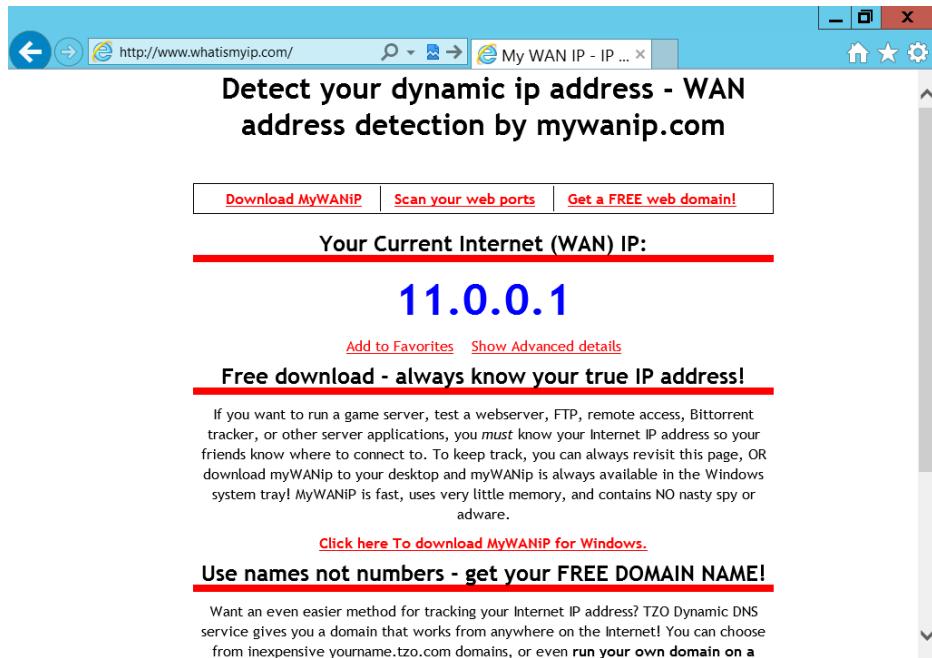
[Click here To download MyWANIP for Windows.](#)

Use names not numbers - get your FREE DOMAIN NAME!

Want an even easier method for tracking your Internet IP address? TZO Dynamic DNS service gives you a domain that works from anywhere on the Internet! You can choose from inexpensive [yourname.tzo.com](#) domains, or even [run your own domain on a](#)

After NAT

On Private → Open Internet Explorer & access <http://www.whatismyip.com> the IP address is shown as 11.0.0.1 Public IP.



Detect your dynamic ip address - WAN address detection by mywanip.com

Your Current Internet (WAN) IP:
11.0.0.1

Add to Favorites Show Advanced details

Free download - always know your true IP address!

If you want to run a game server, test a webserver, FTP, remote access, BitTorrent tracker, or other server applications, you *must* know your Internet IP address so your friends know where to connect to. To keep track, you can always revisit this page, OR download myWANIP to your desktop and myWANIP is always available in the Windows system tray! MyWANIP is fast, uses very little memory, and contains NO nasty spy or adware.

[Click here To download MyWANIP for Windows.](#)

Use names not numbers - get your FREE DOMAIN NAME!

Want an even easier method for tracking your Internet IP address? TZO Dynamic DNS service gives you a domain that works from anywhere on the Internet! You can choose from inexpensive [yourname.tzo.com](#) domains, or even [run your own domain on a](#)

Lab – 6: Configuring DHCP Relay Agent

SYS1-CONFIGURATION

Note: Install DHCP service and create a scope with 12.0.0.10 to 12.0.0.100 with the router IP as 12.0.0.1.

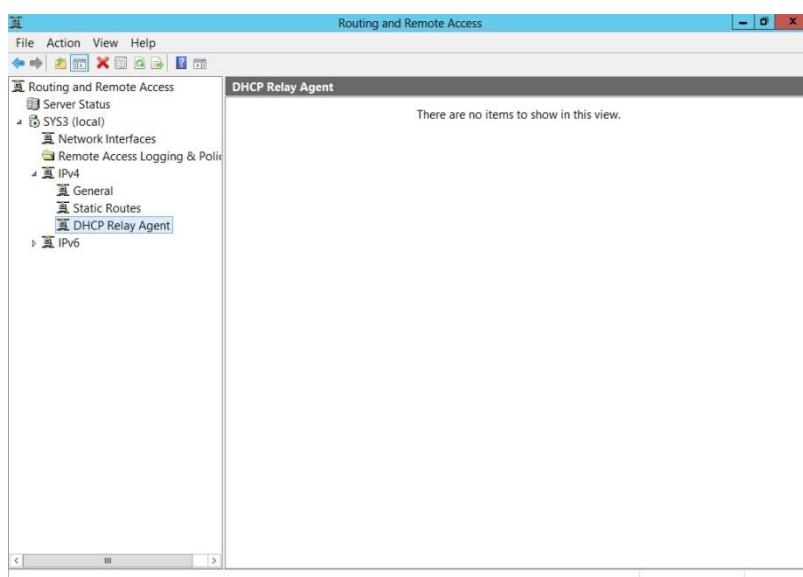
On Router2

SYS3-CONFIGURATION

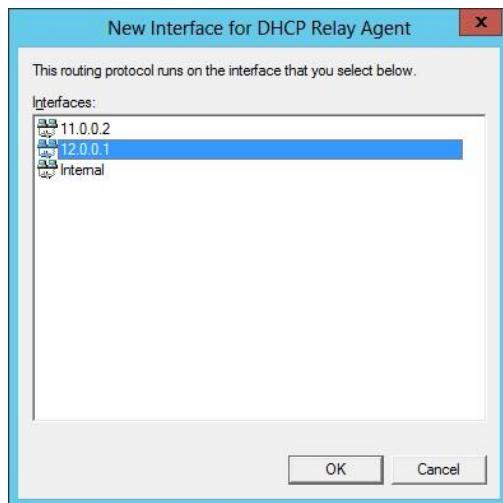
1. Go to **Routing and Remote Access** → Expand **System name** → Expand **IPv4**
2. Right click **General** → Select **New Routing Protocol**
3. Select **DHCP Relay Agent** → click **OK**.



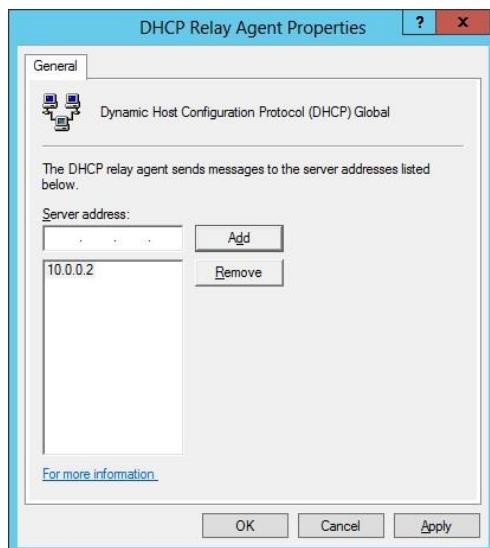
4. Right click on **DHCP Relay Agent**, Select **New Interface**.



5. Select **12.0.0.1 Interface** → click **OK** → and click **OK**.



6. Right click on **DHCP Relay Agent** → **Properties** → Enter the IP Address of **DHCP Server (10.0.0.2)** → click **Add** → **Apply** and **OK**



Verification:

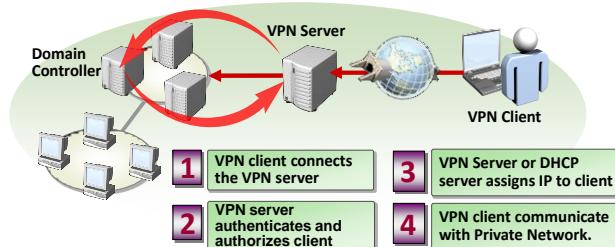
SYS4-CONFIGURATION

1. Log on as **Administrator** to **DHCP Client (SYS4)** and set the IP address to **obtain the IP address automatically**.
2. Start → Run → Cmd → **Ipconfig /release**.
3. Type **Ipconfig /renew**.
4. An IP address will be assigned by **DHCP server**.
5. Check the IP Address by typing **Ipconfig /all**.

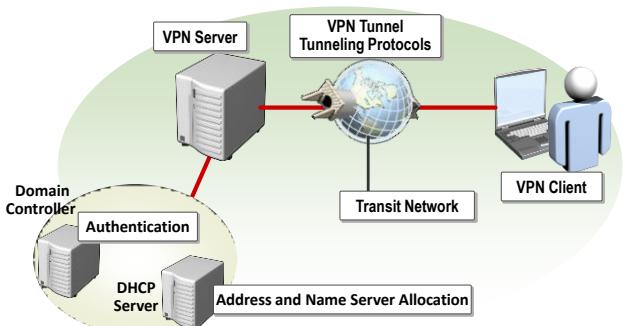
REMOTE ACCESS SERVICES (RAS)

How a VPN Connection Works

- A VPN extends a private network across shared or public networks such as the Internet.

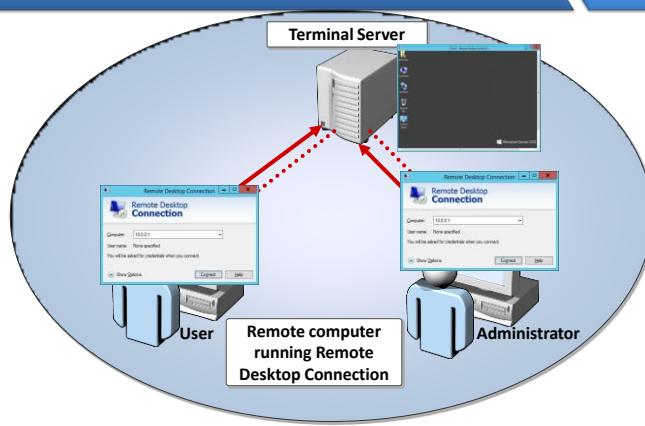


Components of a VPN Connection



REMOTE DESKTOP SERVICES

What is Remote Desktop Service?



Modes of Remote Desktop Services

- **Remote Administration Mode**
 - Specially designed for remote management of server.
 - Only two connections are Supported.
 - License is not required.

Remote Desktop Services Sessions

- Disconnect Session
 - If the Session is disconnected all the programs will continue to run in the background & the user can reconnect to same session
- Logoff Session
 - If the Session is logged off then all programs will be closed and next time new session will be established.

HYPER TEXT TRANSFER PROTOCOL Over SECURE SOCKET LAYER

HTTPs

- Hypertext Transfer Protocol over Secure Socket Layer (SSL)
- HTTPS encrypts and decrypts the information between the client browser and the web server using a secure Socket Layer (SSL).
- SSL transactions are encrypted between the client and the server, this is usually 40 or 128 bit encryption (the higher the number of bits the more secure the transaction).

HTTPS

- SSL Certificate is issued by a trusted source, known as the Certification Authority (CA).
- CAs verifies the existence of your business, the ownership of your domain name, and your authority to apply for the certificate.

How Secure Sockets Layer Works

- An SSL Certificate enables encryption of sensitive information during online transactions.
- Each SSL Certificate contains unique, authenticated information about the certificate owner.
- A Certification Authority verifies the identity of the Certification owner when it is issued.

You need SSL if...

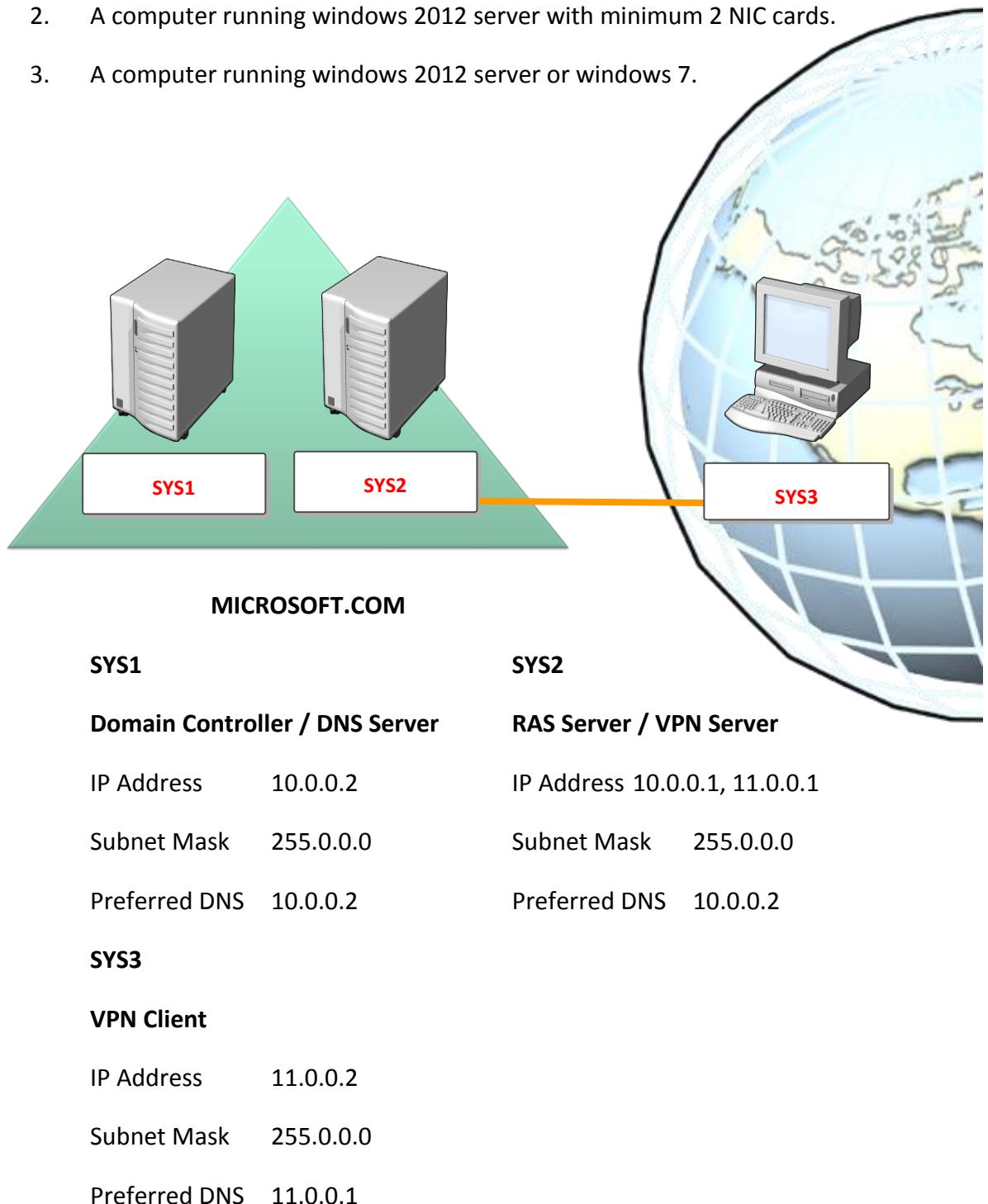
- You have an online store or accept online orders and credit cards
- You offer a login or sign-in on your site
- You process sensitive data such as address, date of birth, license etc
- You value privacy and expect others to trust you

REMOTE ACCESS SERVICES (RAS)

Prerequisites:

Before working on this lab, you must have

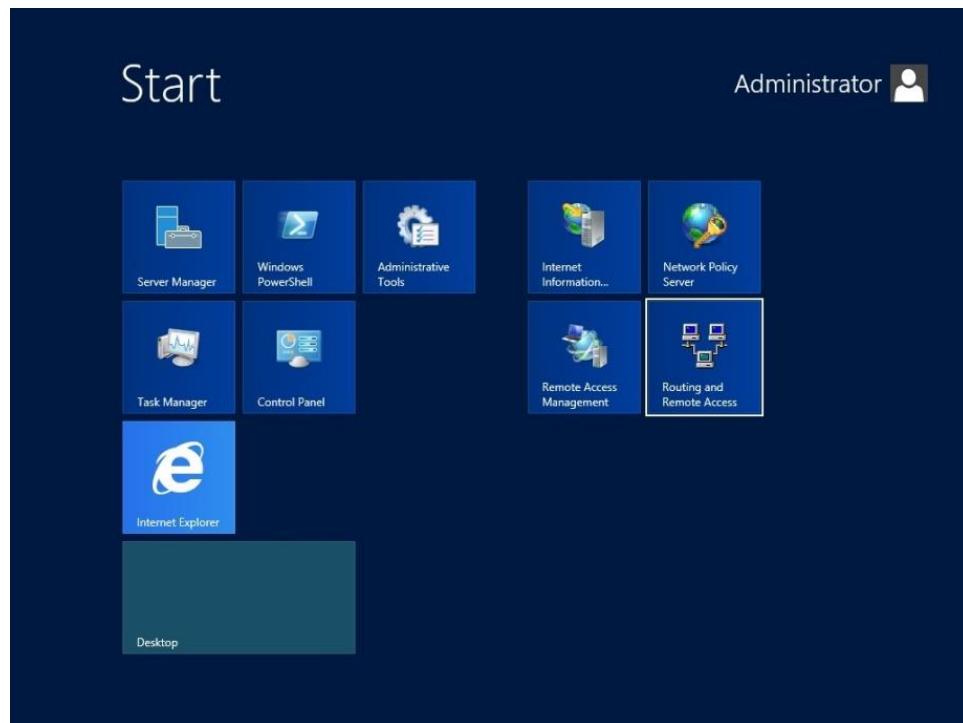
1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server with minimum 2 NIC cards.
3. A computer running windows 2012 server or windows 7.



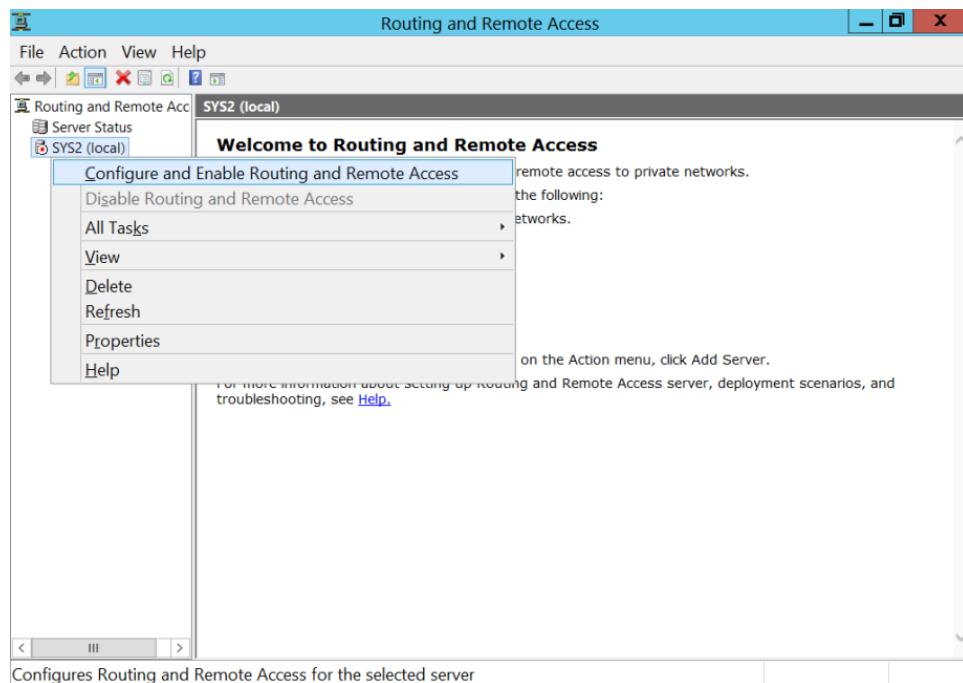
Lab – 1: Configuring VPN Server

SYS2 – CONFIGURATION

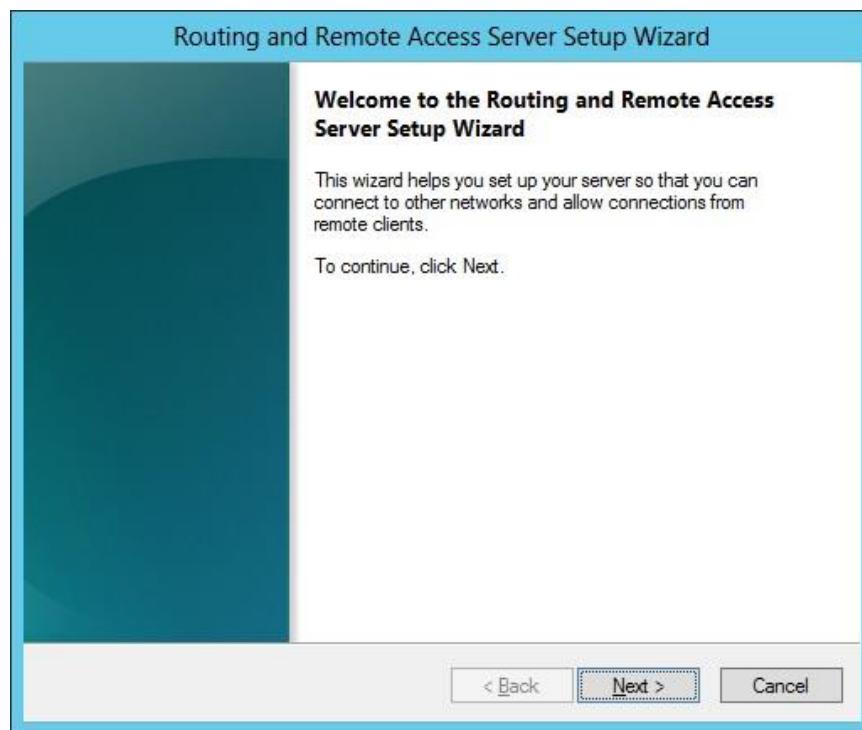
1. Go to Start, select Routing and Remote Access.



2. Right click on system name **Configure and Enable Routing and Remote Access**.



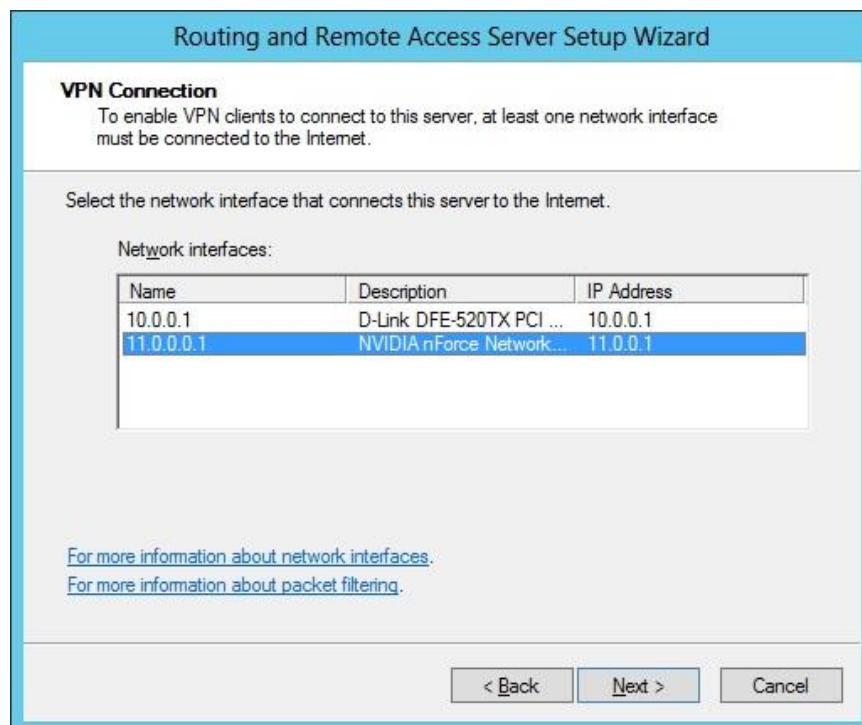
3. In Welcome wizard, click **Next**



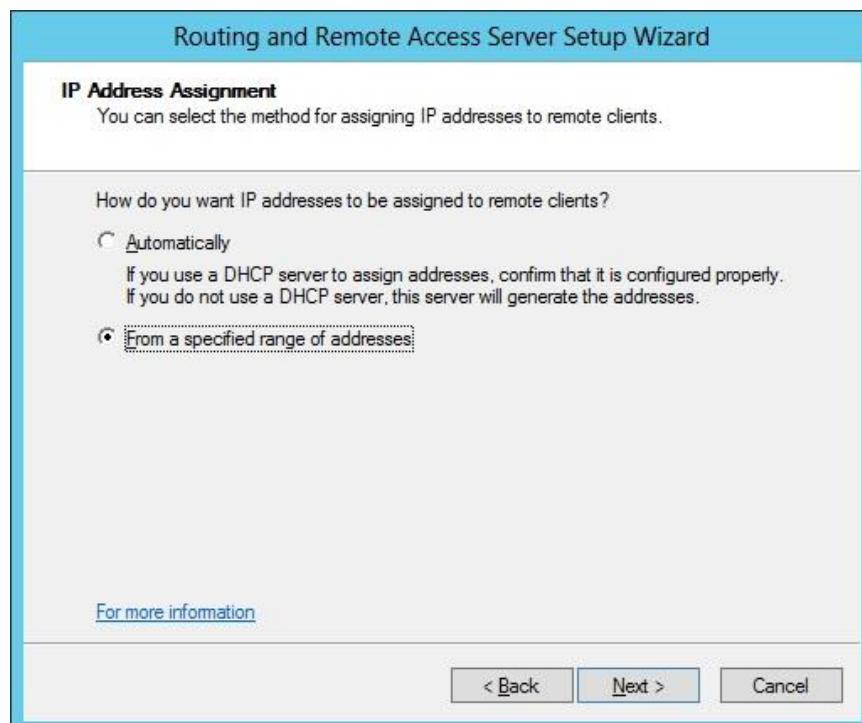
4. Select Virtual private network (VPN) access and NAT → click **Next**.



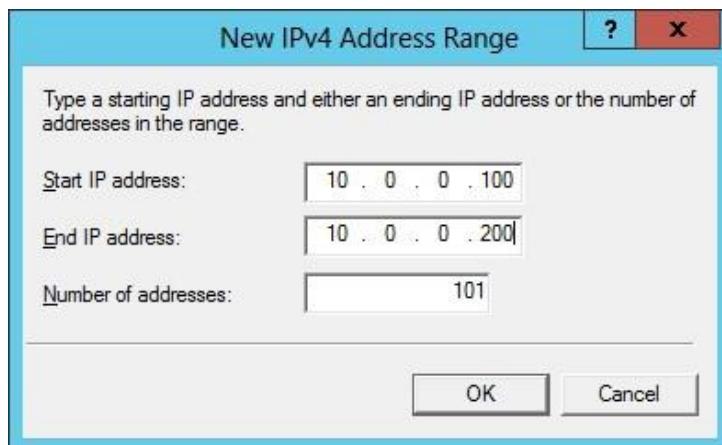
5. Select Public interface (Ex: 11.0.0.1) → click **Next**.



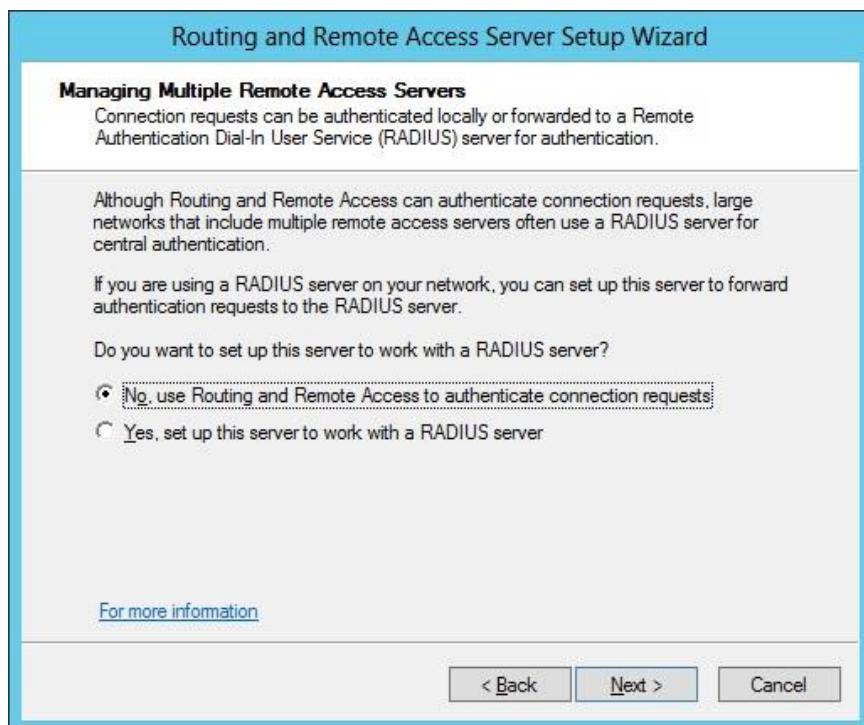
6. Select From a specified range of address (if DHCP is not configured in the private network, select automatically if DHCP is configured), click **Next**.

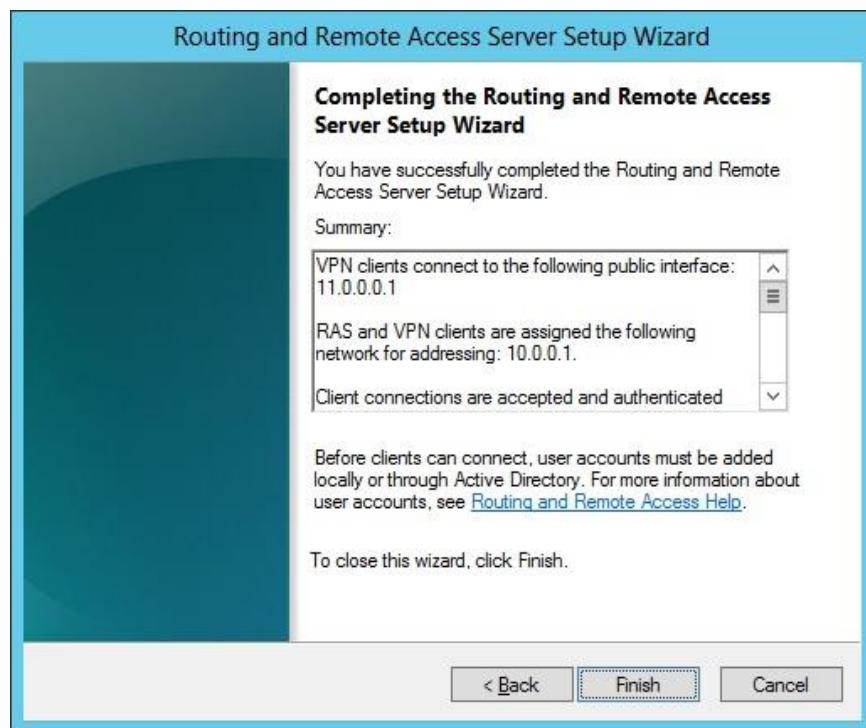
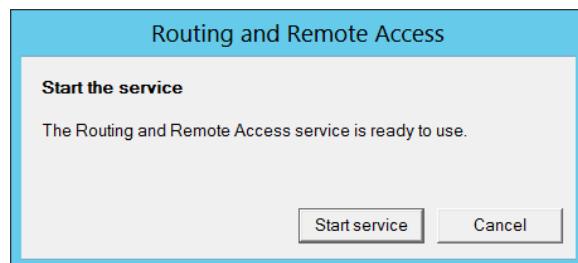


7. Enter the IP Address range to be leased to VPN Clients (Ex: 10.0.0.100 to 10.0.0.200), click **OK**.



8. Select No, use Routing and Remote Access to authenticate connection requests (if VPN Server is Member Server), click **Next**.

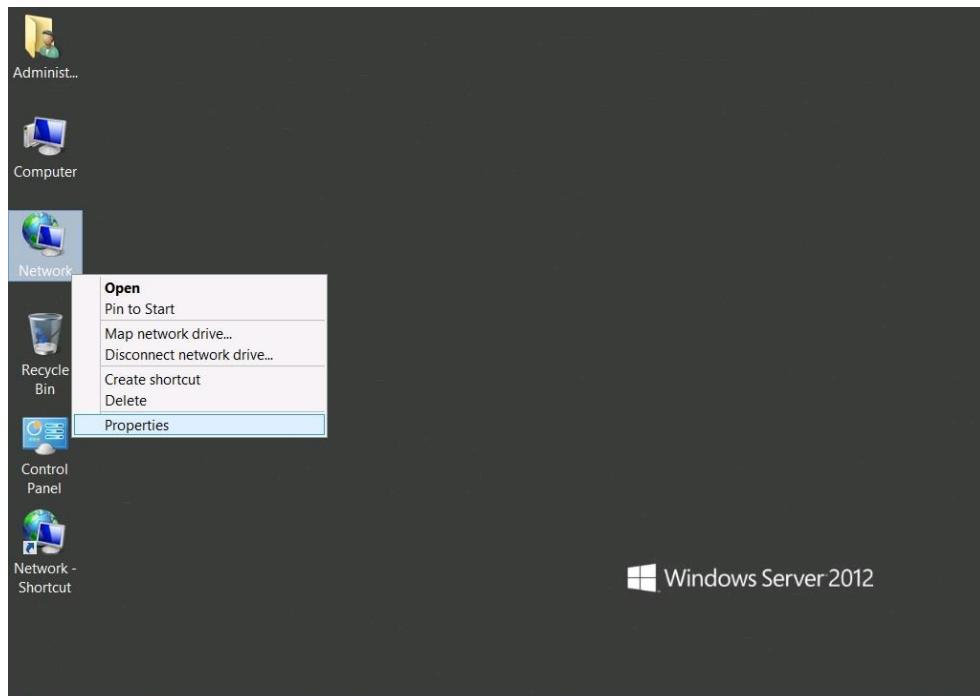


9. Click **Finish**10. Click **Start service**

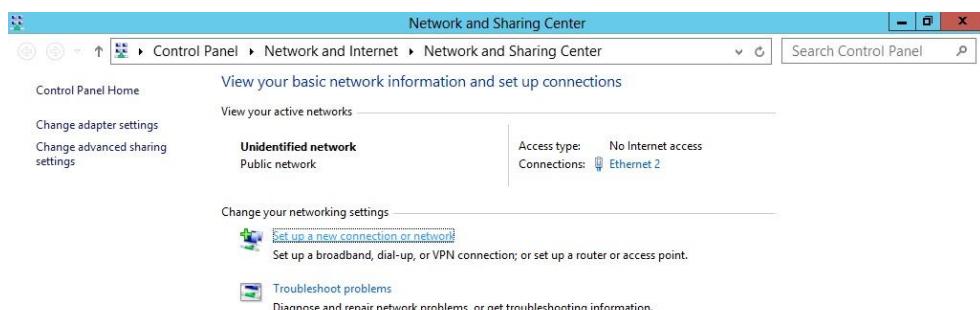
Lab – 2: Establishing VPN Connections

SYS3 – CONFIGURATION

1. Log on to RAS Client (SYS3), Right click on Network icon → Properties.

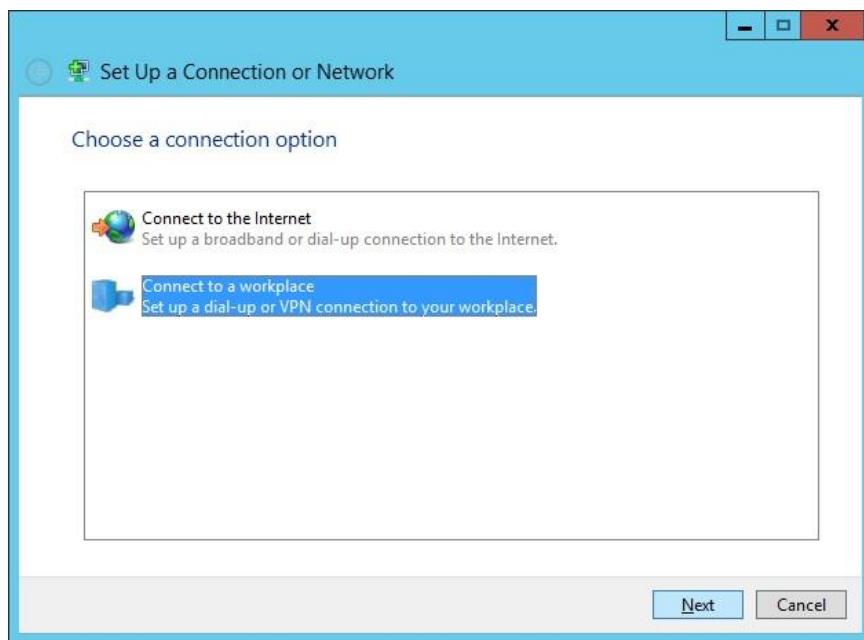


2. Select Set up a Connection or network

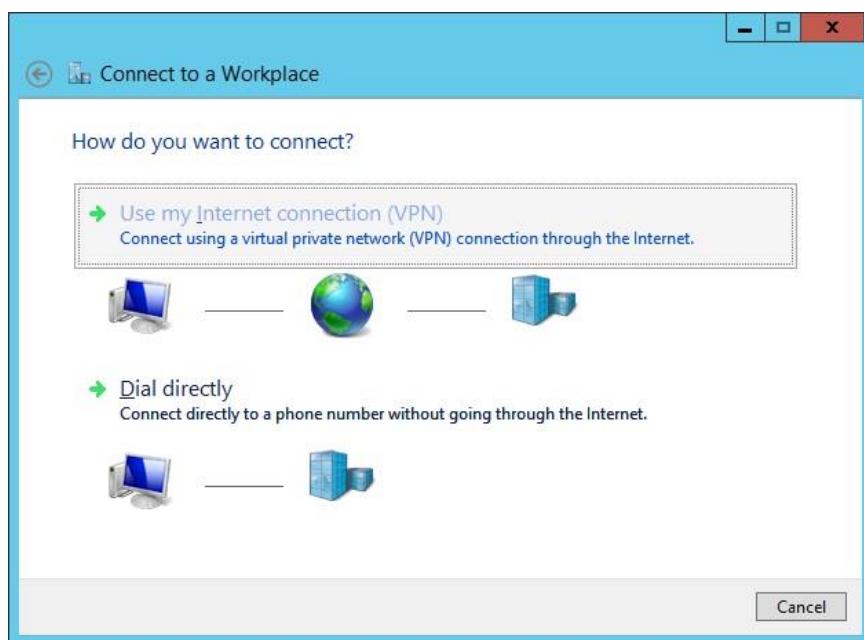


See also
[Internet Options](#)
[Windows Firewall](#)

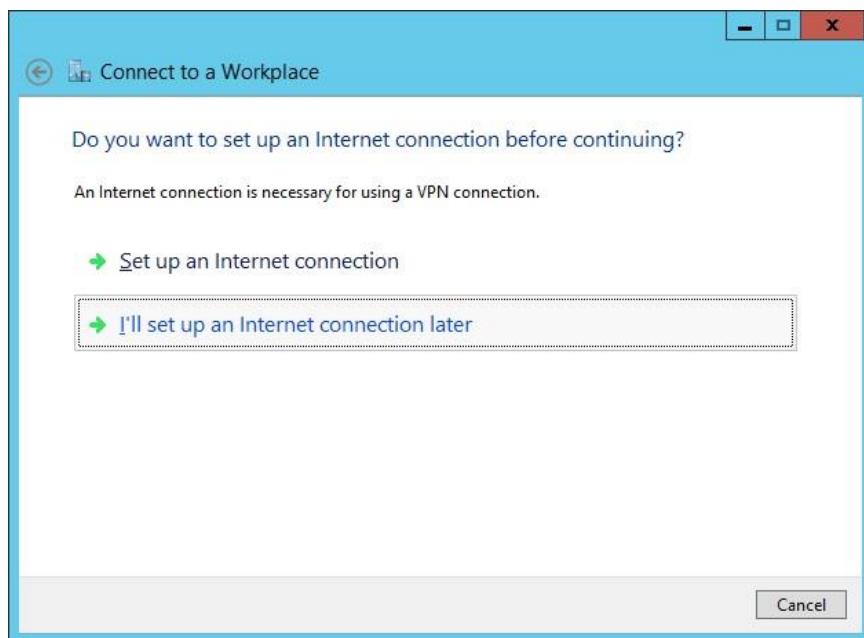
3. Connect to a workplace → click **Next**.



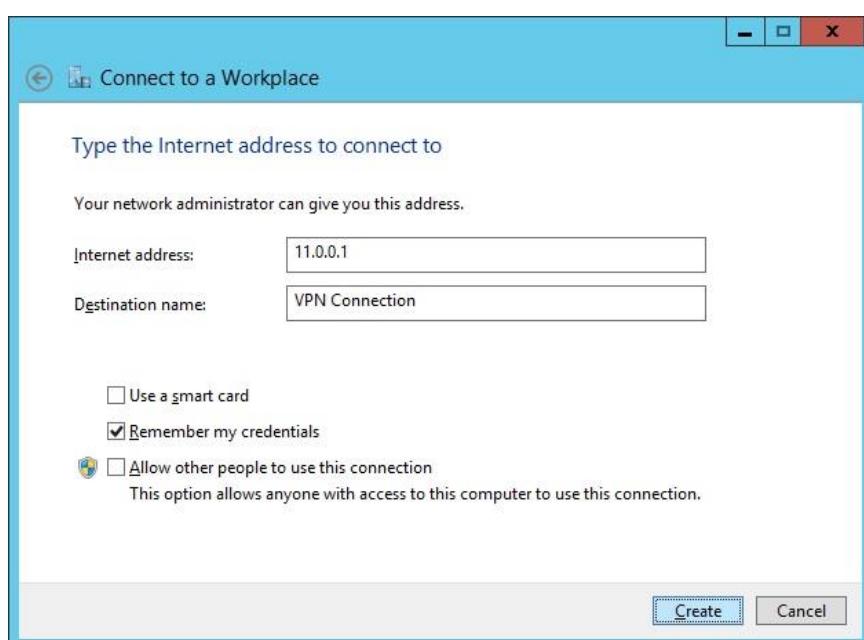
4. Select **Use my Internet connection (VPN)** → click **Next**.



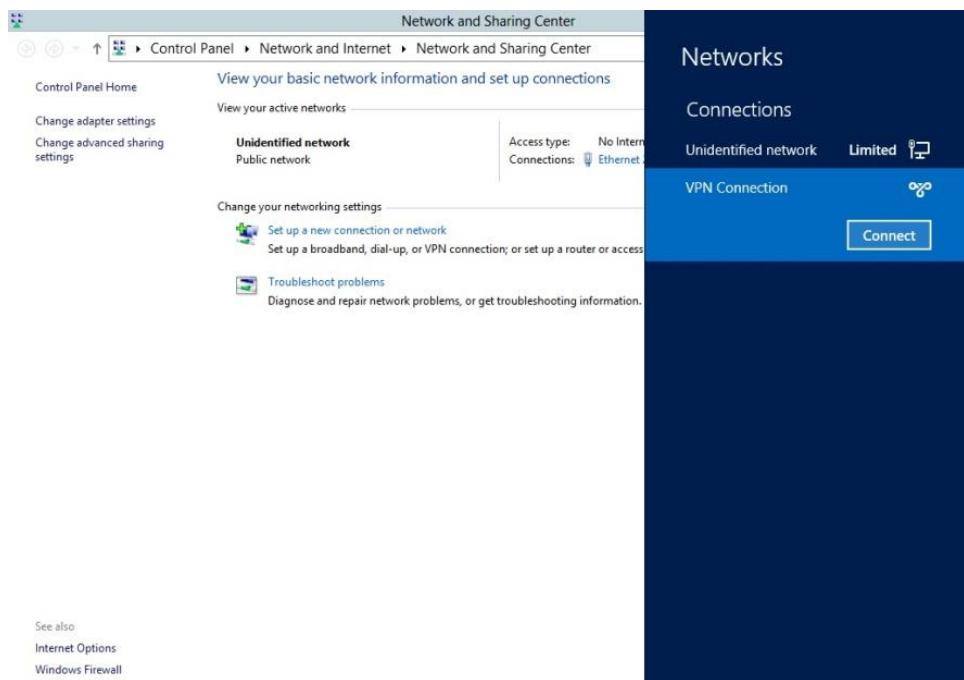
5. Select **Use this Connection** → click **Next**.



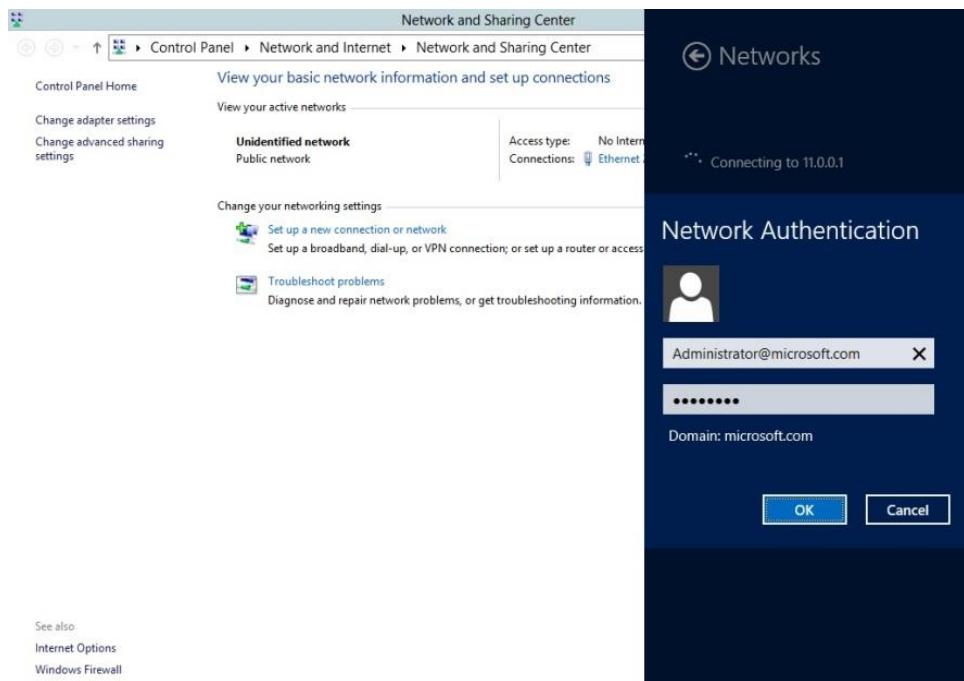
6. Mention the **IP Address of VPN Server** → click **Next**



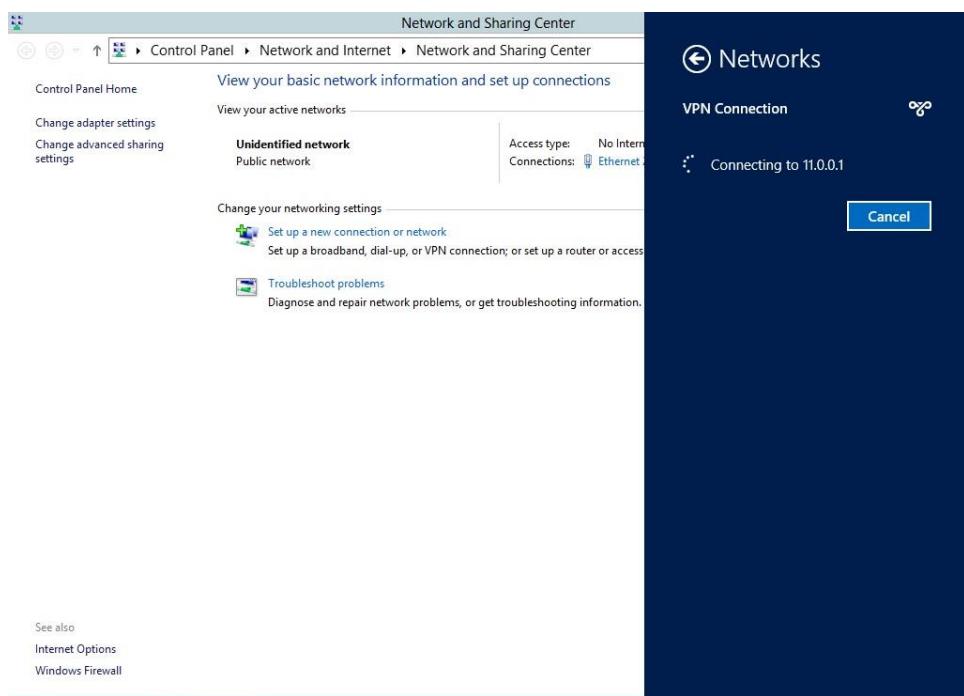
7. Click VPN Connection → click Connect.



8. Enter Network Authentication, (Ex: Administrator@microsoft.com) and Password click OK.



9. Connection is created successfully.



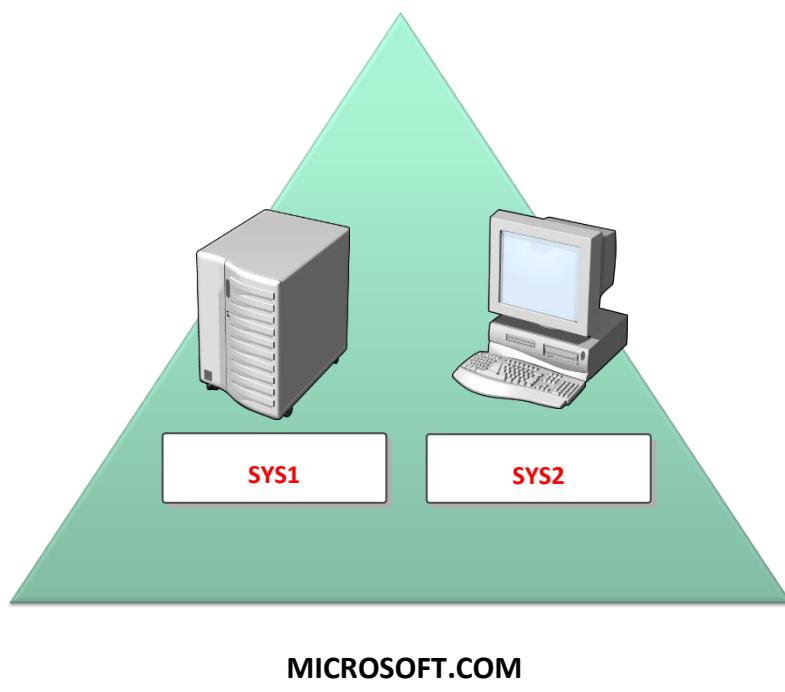
10. Go to **Command prompt & type Ipconfig /all** to view the IP Address of the Client computer.
11. Now try to access the LAN Network.
12. Go to Start → Run → type **\LAN computer IP address\Drive\$ or Share folder name**
Ex:**\10.0.0.2\c\$**

REMOTE DESKTOP SERVICES

Prerequisites:

Before working on this lab, you must have

1. A computer running windows 2012 server or Domain Controller.
2. A computer running windows 2012 server or windows 7.



SYS1

D.C. / Remote Desktop Server

IP Address 10.0.0.1

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

SYS2

Member Server / Client

IP Address 10.0.0.2

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

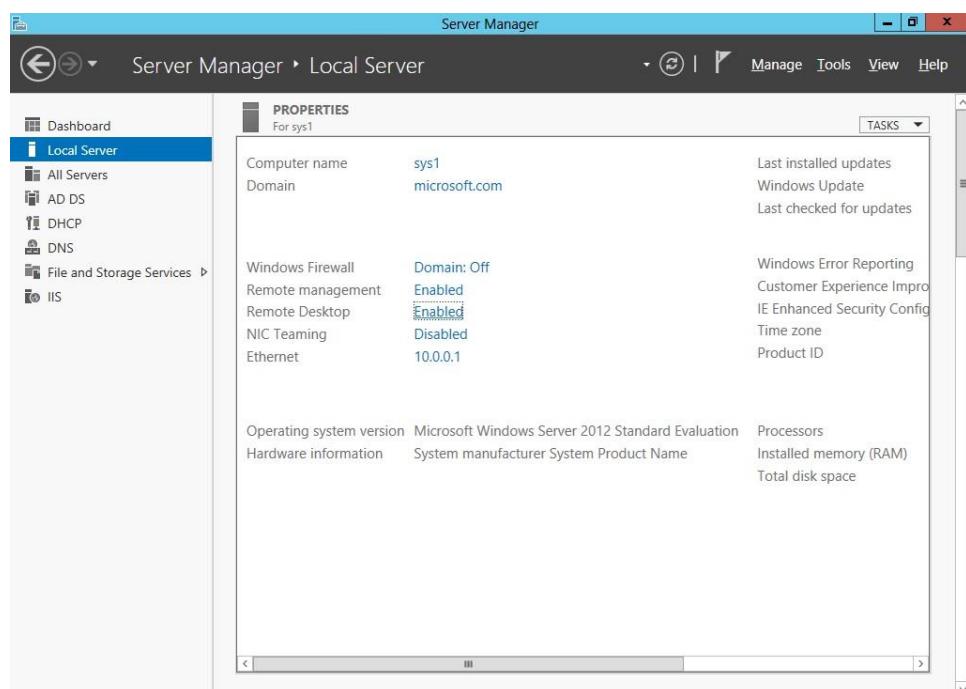
Lab – 3: Configuring Remote Desktop Server in Remote Admin Mode

SYS1 – CONFIGURATION

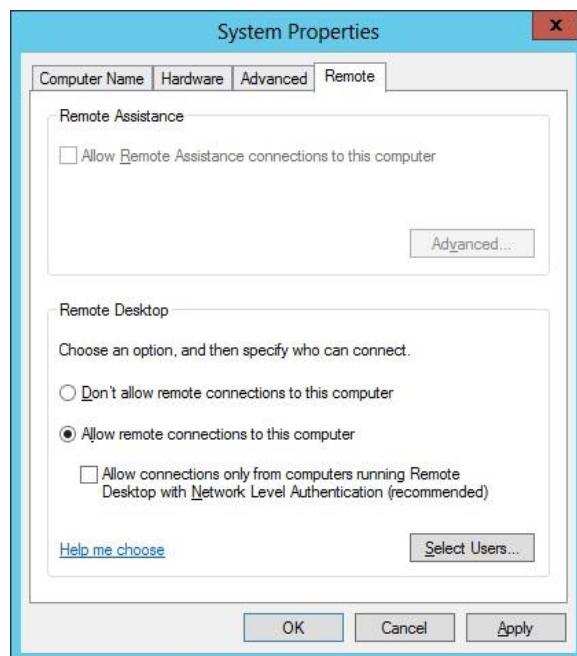
1. Select Server Manager



2. Select Remote Settings.

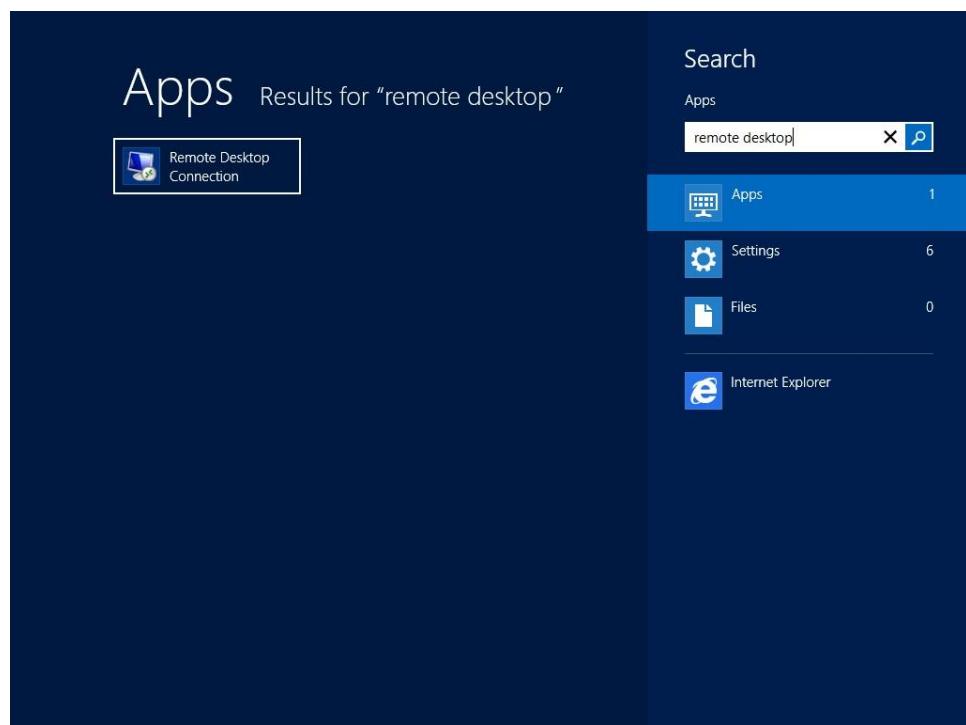


4. Check the box “Allow Connections from computers running any version”.



Go to Terminal Client (SYS2)

1. Go to Start, Type Remote Desktop Connection in search in Apps, select **Remote Desktop Connection**.



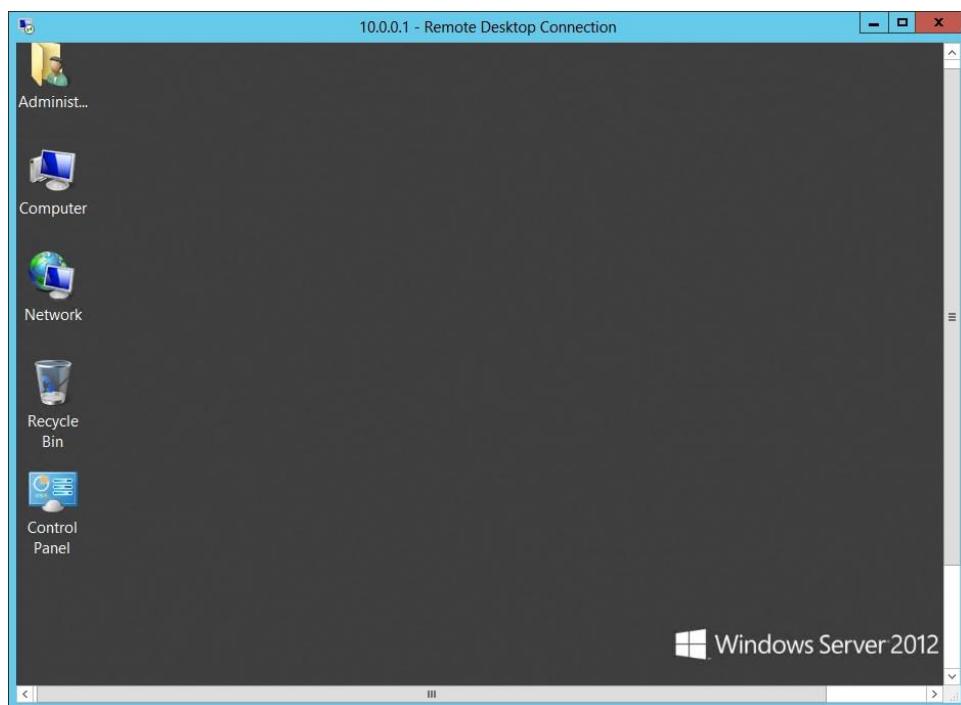
2. Specify the IP Address 10.0.0.1 or computer name of terminal server → click **Connect**.



3. Specify username as **Administrator** and type the password. → click **OK**

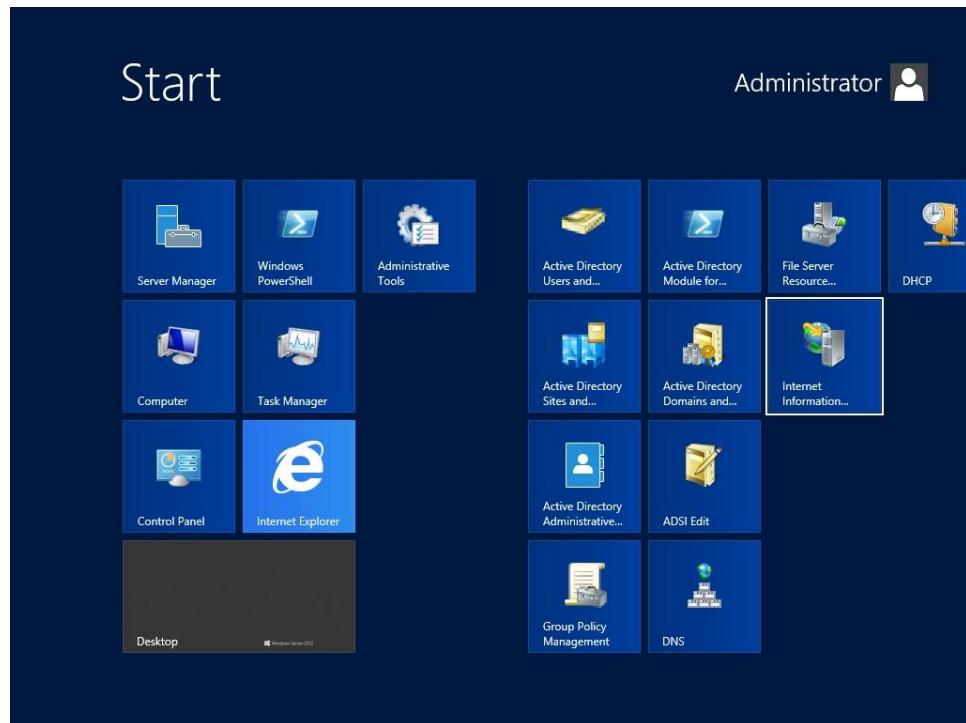


4. The **Administrator** will connect to the Terminal Server Remotely.

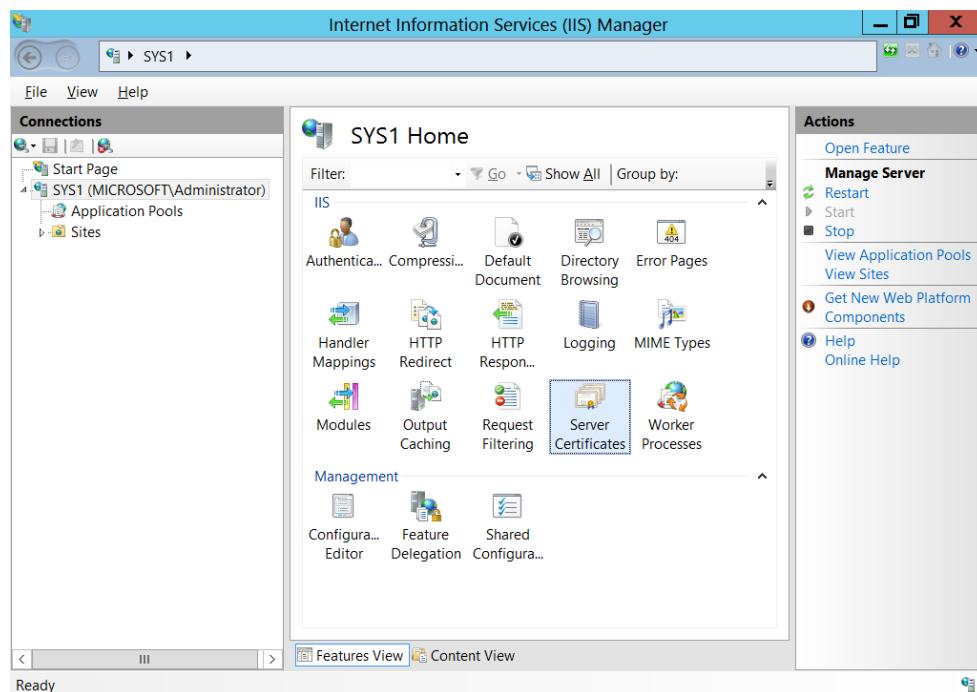


Lab – 3: Creating Self-Signed Certificate for HTTPS Website

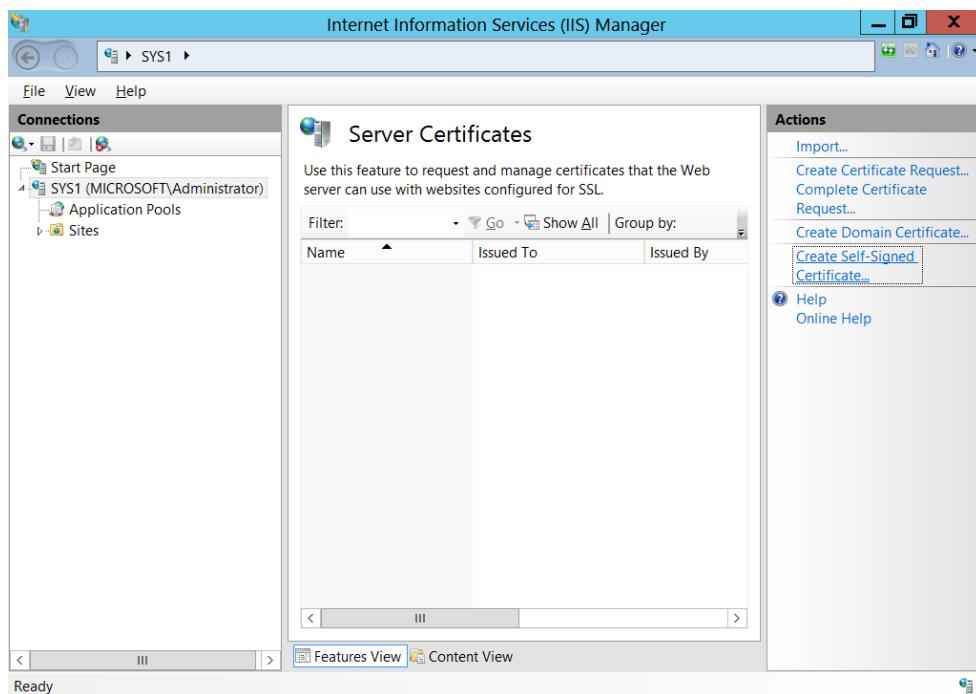
1. Go to Start, select **Internet Information Services Manager**.



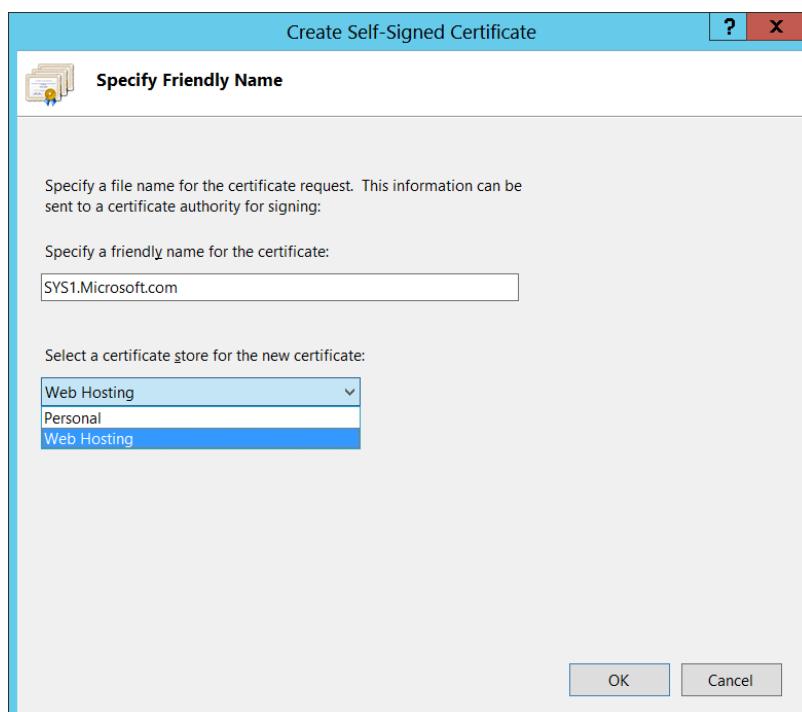
2. Select the system name (Ex: SYS1), and select **ServerCertificates**.



3. In Server Certificates, click **Create Self-Signed Certificate**, from Actions pane.

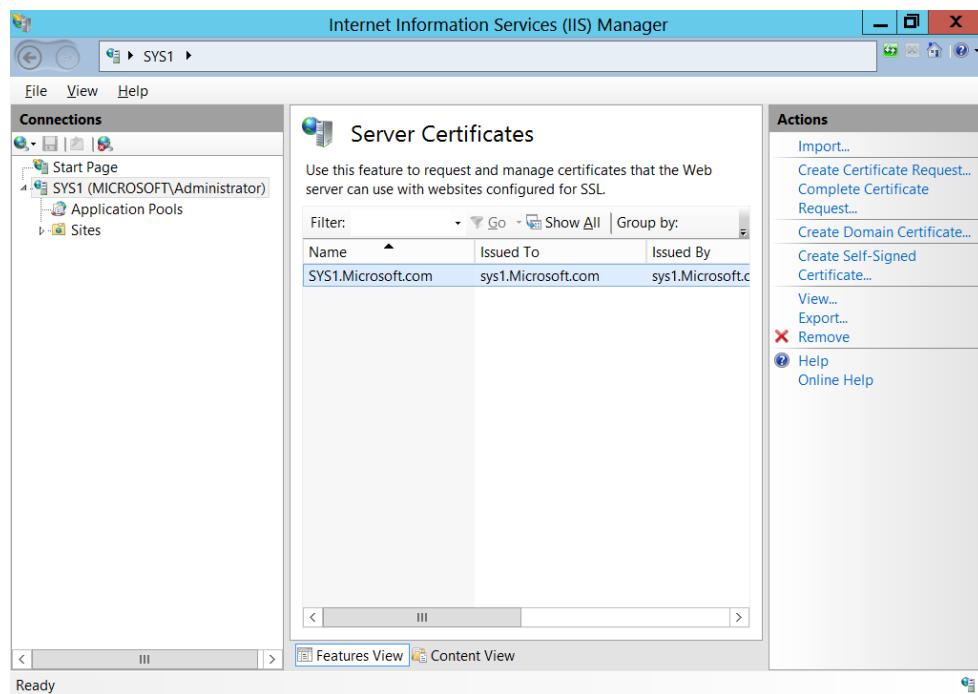


4. Mention the Certificate name (Ex: SYS1.Microsoft.com), select **Web Hosting**.



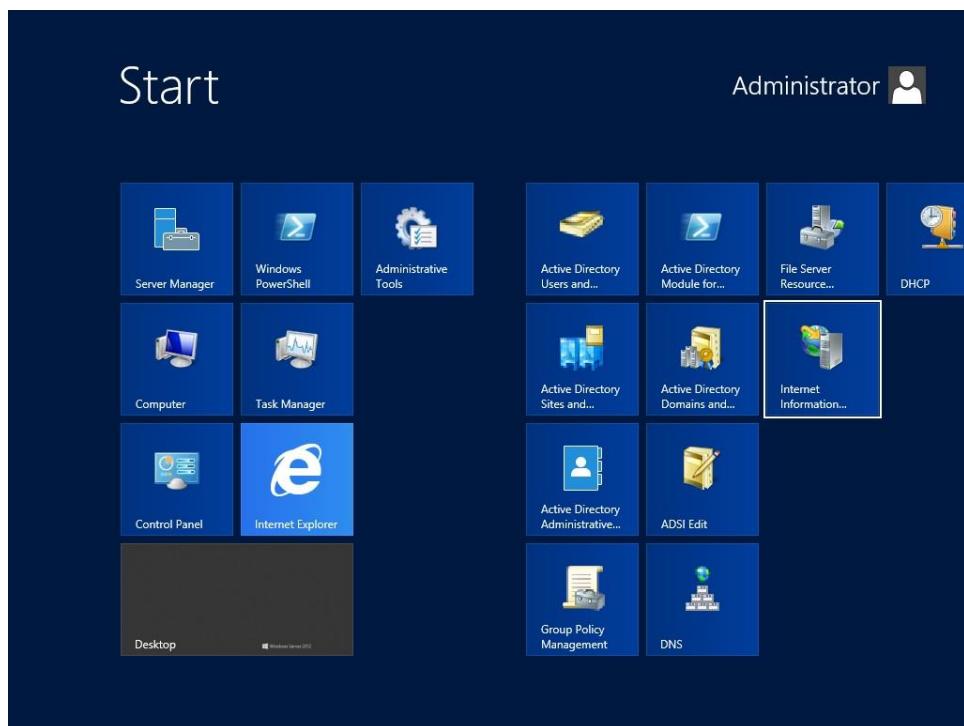
5. Click **OK**.

6. Certificate is created

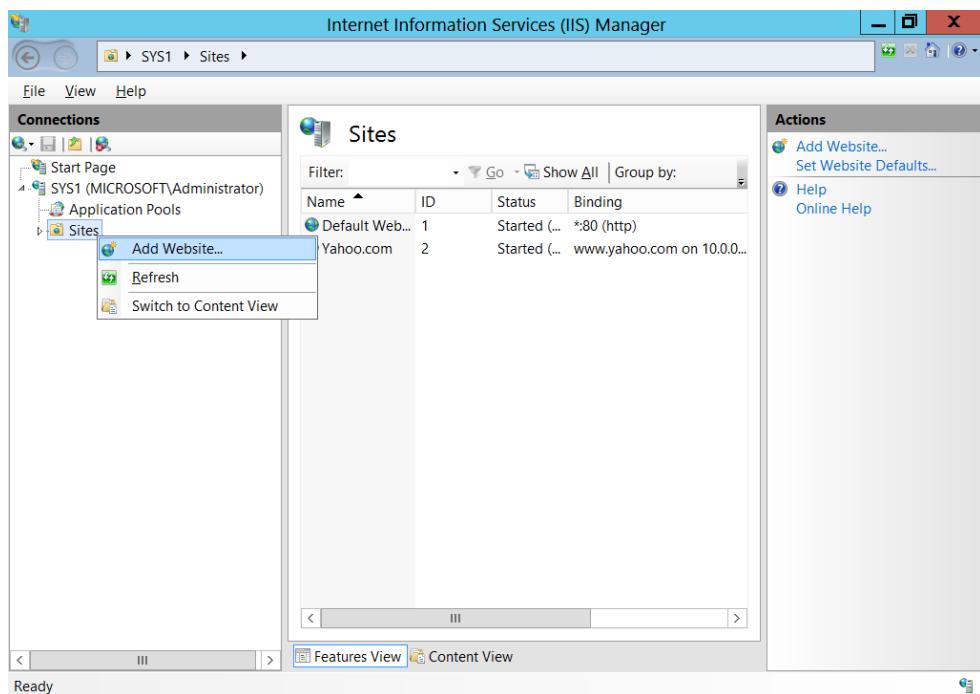


Lab – 7: Creating a HTTPS Web Site

1. Go to Start, select **Internet Information Services Manager**.

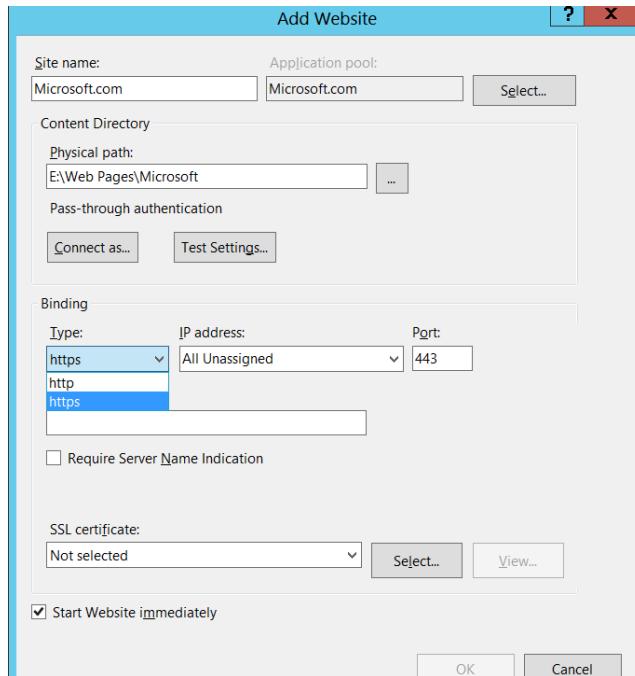


2. In the left pane of the **Internet Information Services**, Expand the server → Right click on sites and select **Add Web Site**.

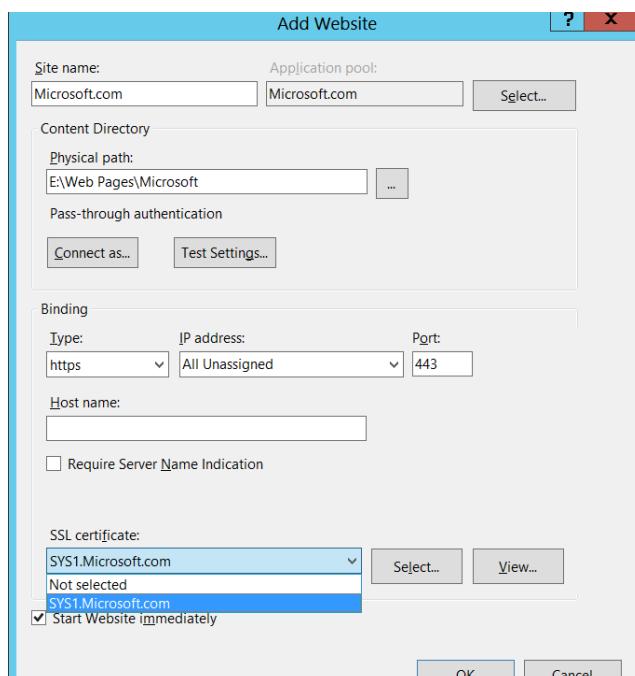


3. **Add Web Site** wizard opens → In the Site name type a **Name** (Ex: **Microsoft.com**)
In Physical path, browse and select the location of **Home Directory (Webpage's Folder)**

4. Select the protocol as **HTTPS**



5. Select the SSL Certificate (Ex:[SYS1.MICROSOFT.COM](#)).



6. Click **OK**, Web Site will be successfully added.
7. Enable **Directory Browsing**. (Repeat the process of Directory Browsing)
8. Apply **Default Document**. (Repeat the process of Default Document)

Accessing the HTTPS site from the Web Server

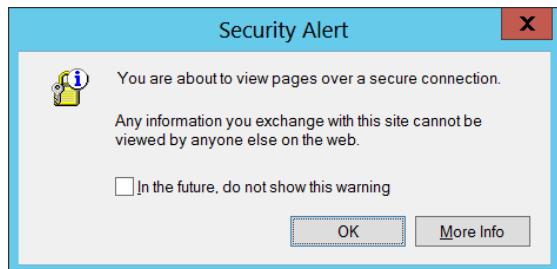
SYS1 – CONFIGURATION

1. Open the browser and type <https://certificate-name>

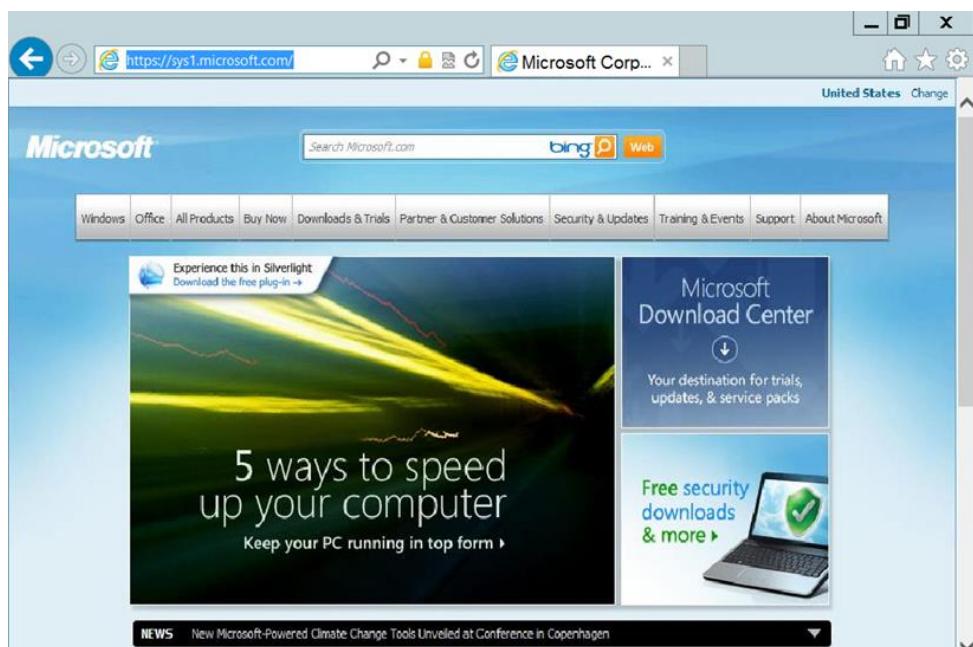
Ex: [Https://sys1.microsoft.com](https://sys1.microsoft.com)



2. A warning will be given, click OK to proceed



3. Web site is displayed, verify for Yellow Lock beside Address bar.



Accessing the HTTPS site from the Client Computer

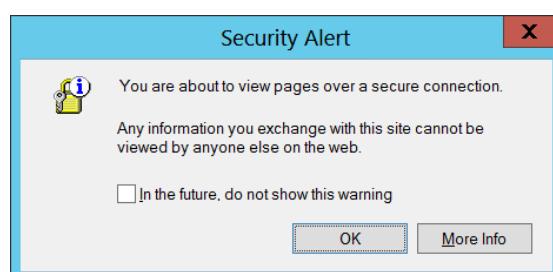
SYS2 – CONFIGURATION

1. Open the browser and type <https://certificate-name>

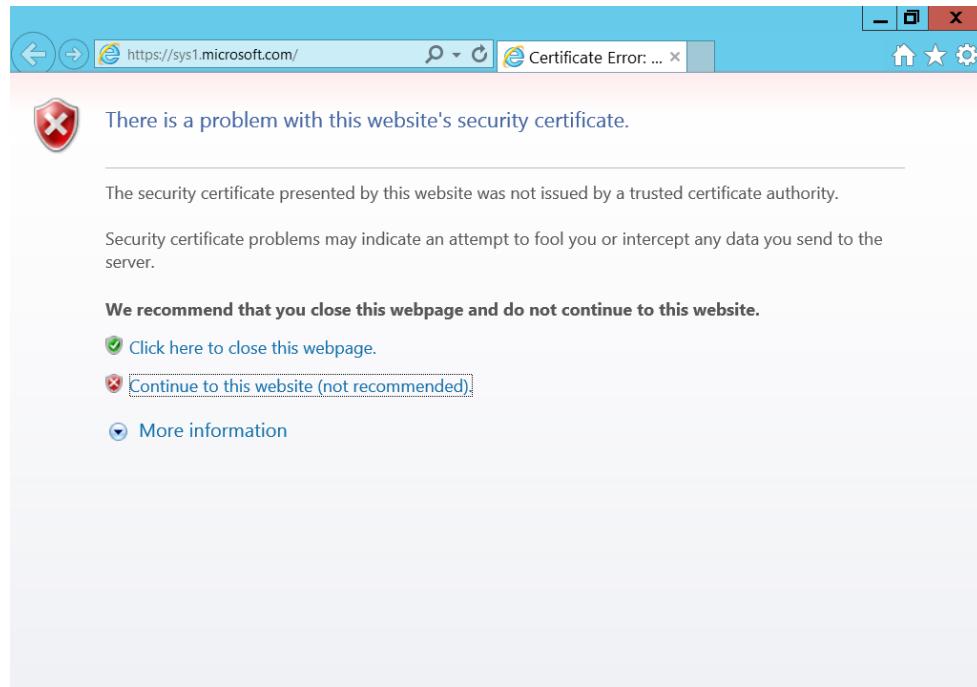
Ex: [Https://sys1.microsoft.com](https://sys1.microsoft.com)



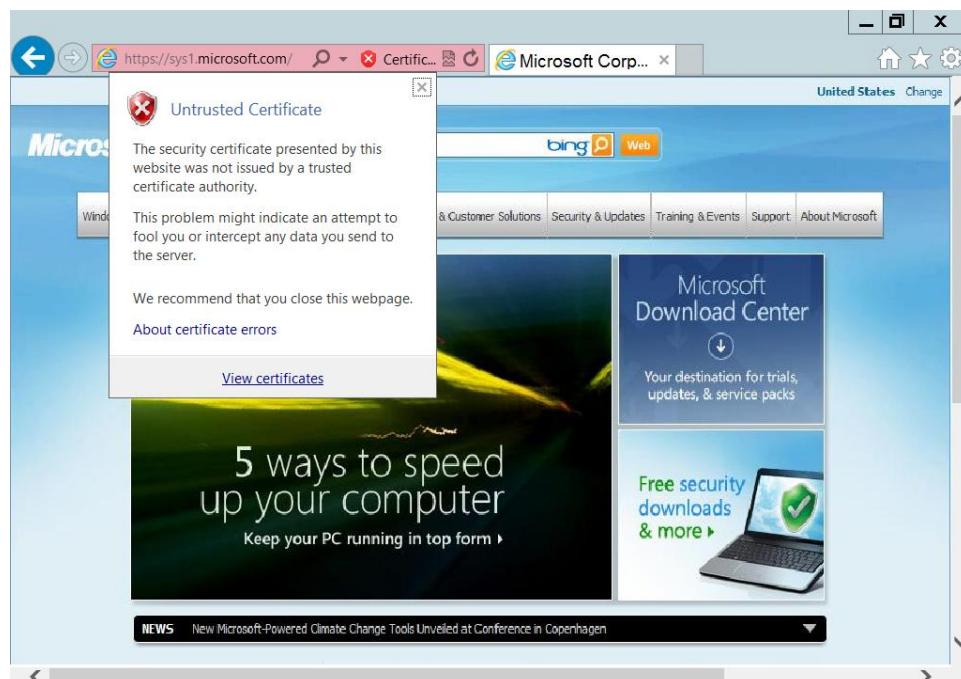
2. A warning will be given, click OK to proceed



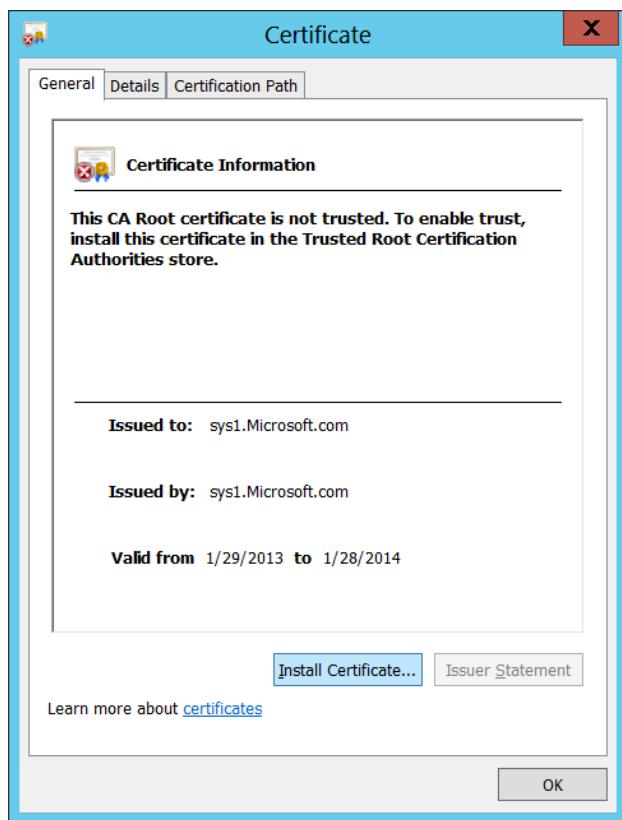
3. There is a problem with Website's Security Certificate (The Security Certificate presented by website was not issued by a Trusted Certification Authority), Click on **Continue to this Web site (Not Recommended)**



4. Web site is displayed but there is a **Certificate Error**
5. Click on **Certificate Error** and Click on **View Certificates**

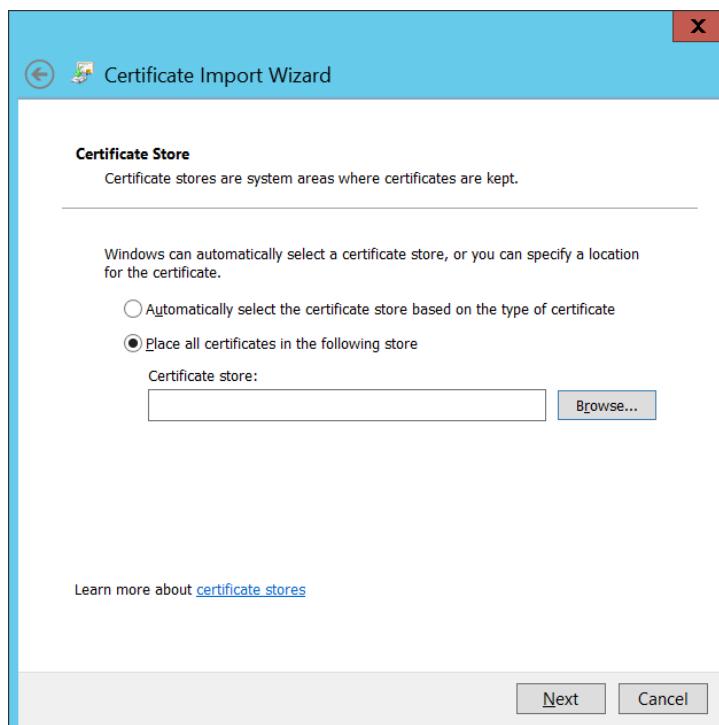


6. Click on **Install Certificate**

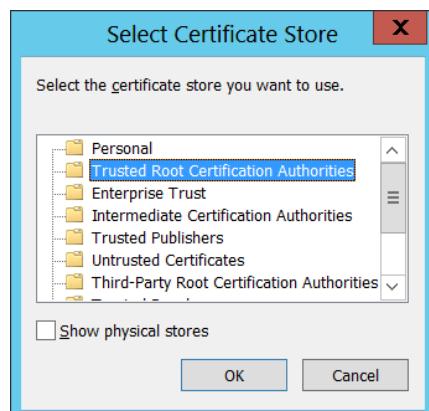


7. Click Next

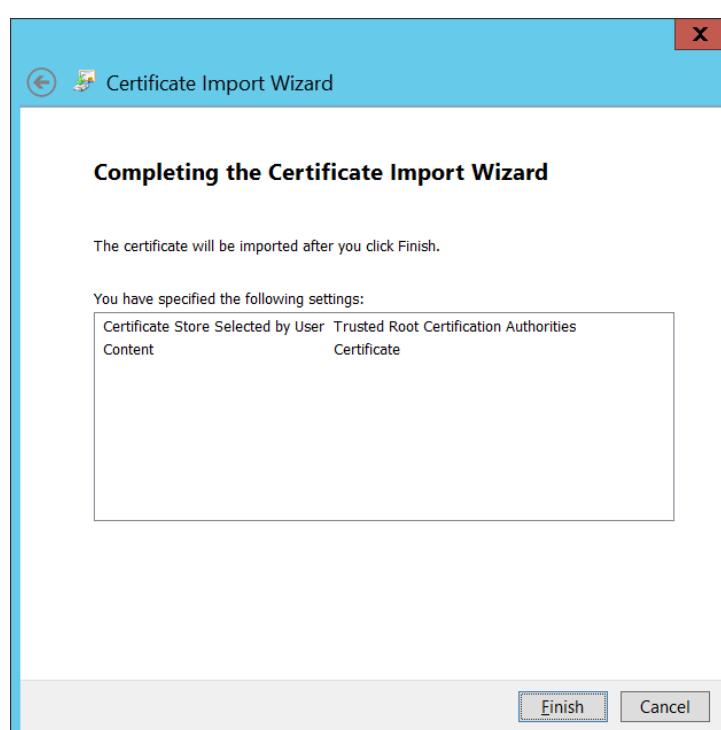
8. Select **Place all certificates in the following store** → Click **Browse**.



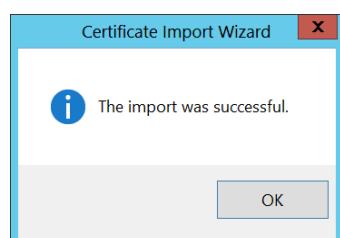
9. Select Trusted Root Certification Authority → Click OK → Click Next



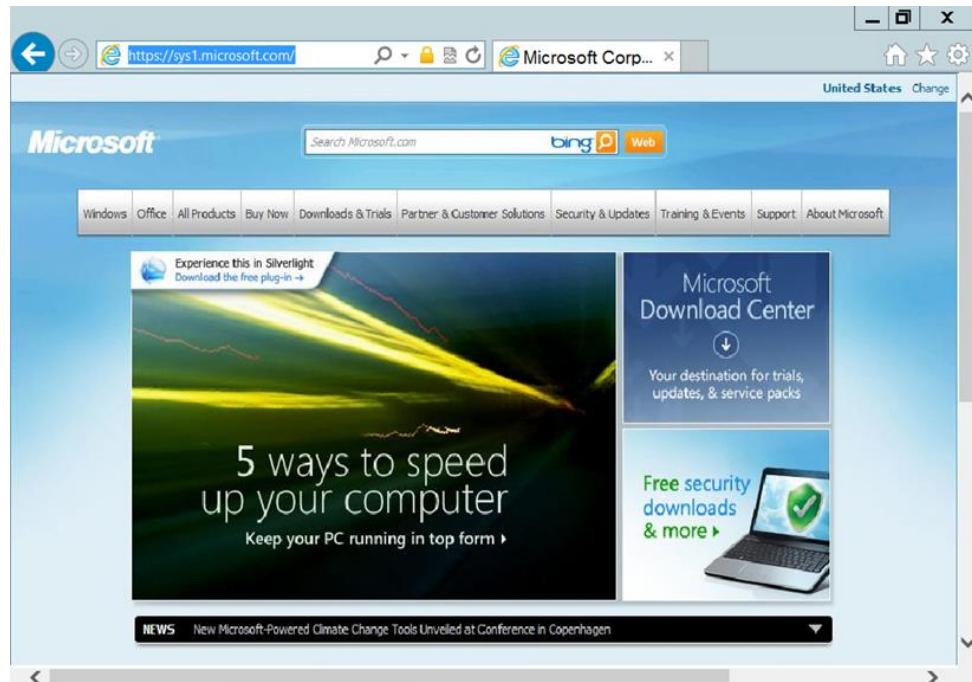
10. Click Finish



11. Click Yes → Click OK → Click OK.



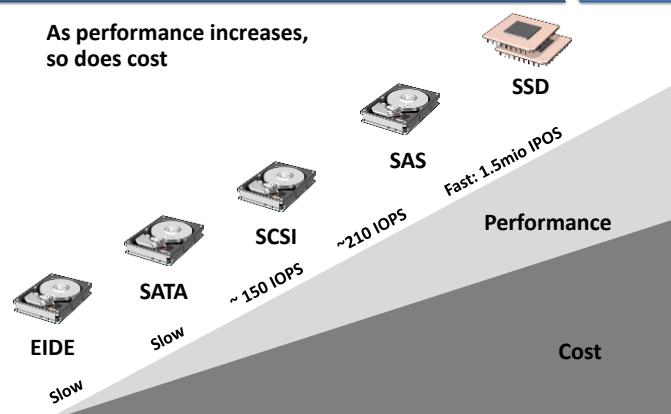
12. Web site is displayed, Click on the Yellow Lock beside Address bar, to see the website security status



Storage Management

Disk Types and Performance

As performance increases,
so does cost



Built-in Disk Management Tools

- **Built-in Disk Management Tools in Windows**

Windows Server 2012

- Storage pools.
- Disk Management.

Selecting a Partition Table Format

MBR

- Standard Partition table format since early 1980s
- Supports a maximum of 4 primary partitions per drive
- Can partition a disk up to 2 TB

GPT

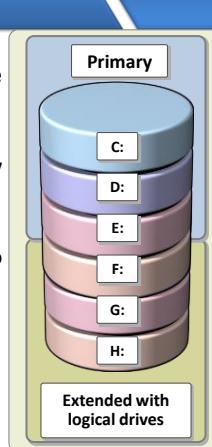
- GPT is the successor of MBR partition table format
- Supports a maximum of 128 partitions per drive
- Can partition a disk up to 18 EB

✓ Use MBR for disks smaller than 2 TB

✓ Use GPT for disks larger than 2 TB

What is a Partition?

- A physical disk is sectioned into separate partitions
- A physical disk can have up to three primary partitions and one extended partition
- Extended partitions are subdivided into logical drives



Selecting a File System

When selecting a file system, consider the differences between FAT, NTFS, and ReFS

FAT provides:

- Basic file system
- Partition size limitations
- FAT32 to enable larger disks
- exFAT developed for flash drives

NTFS provides:

- Metadata
- Auditing and journaling
- Security (ACLs and encryption)

ReFS provides:

- Backward compatibility support for NTFS
- Enhanced data verification and error correction
- Support for larger files, directories, volumes, etc.

What Is Direct Attached Storage?

DAS disks are physically attached to the server

Advantages:

- Easy to configure
- Inexpensive solution

Disadvantages:

- Isolated because it attaches only to a single server
- Slower



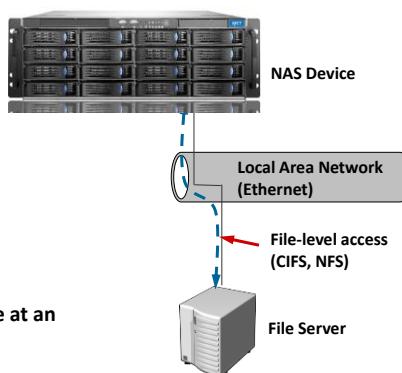
Server with attached disks

What Is Network Attached Storage?

NAS is storage that is attached to a dedicated storage device and accessed through network shares

Advantages:

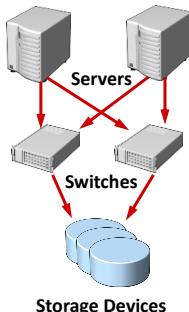
- Relatively inexpensive
- Easy to configure



NAS offers centralized storage at an affordable price

What Is a SAN?

SANs offers higher availability with the most flexibility



Advantages:

- Fastest access times
- Easily expandable
- Centralized storage
- High level of redundancy

Disadvantages:

- More expensive
- Requires specialized skills

SANs can be implemented using Fibre Channel or iSCSI

iSCSI Storage

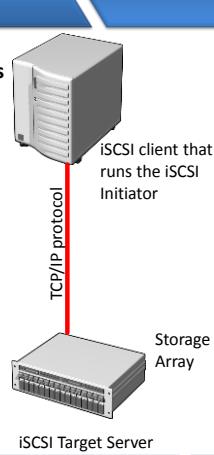
What is iSCSI storage ?

- iSCSI storage is an inexpensive and simple way to configure a connection to remote disks. Many application requirements dictate that remote storage connections must be redundant in nature for fault tolerance or high availability.

What is iSCSI storage ?

- iSCSI transmits SCSI commands over IP networks

Component	Description
IP network	Provides high performance and redundancy
iSCSI targets	Run on the storage device and enable access to the disks
iSCSI initiators	A software component or host adapter on the server that provides access to iSCSI targets
IQN	A globally unique identifier used to address initiators and targets on an iSCSI network



iSCSI Target Server and iSCSI Initiator

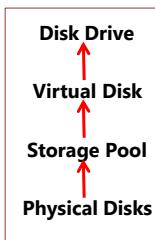
The iSCSI target server	The iSCSI initiator
<p>Is available as a role service in Windows Server 2012</p> <p>Provides the following features:</p> <ul style="list-style-type: none">- Network/diskless boot- Server application storage- Heterogeneous storage- Lab environments	<p>Runs as a service in the operating system</p> <p>Is installed by default on Windows 8 and Windows Server 2012</p>

What Is the Storage Spaces Feature?

Use storage spaces to add physical disks of any type and size to a storage pool, and then create highly-available virtual disks from the storage pool

To create a virtual disk, you need the following:

- One or more physical disks
- Storage pool that includes the disks
- Virtual drives that are created with disks from the storage pool
- Disk drives that are based on virtual drives



Virtual drives are not virtual hard disks (VHDs); they should be considered a drive in Disk Manager

What Is RAID?

- RAID combines multiple disks into a single logical unit to provide fault tolerance and performance
- RAID provides fault tolerance by using:
 - Disk mirroring
 - Parity information
- RAID can provide performance benefits by spreading disk I/O across multiple disks
- RAID can be configured using several different levels
- RAID should not replace server backups

What Is Fault Tolerance?

- The ability to survive hardware failure
- Fault-tolerant volumes provide data redundancy
- Fault-tolerant volumes are not a replacement for backup

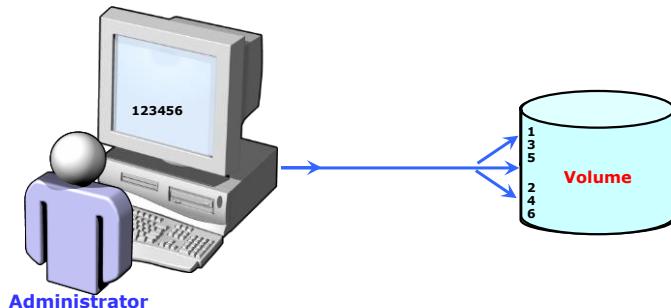
Types of RAID Volumes in Windows 2012

- Simple Volume (RAID-0)
- Mirrored Volume (RAID-1)
- RAID-5 Volume (Striped With Parity)

What Is a Simple Volume (RAID-0)?

- Minimum - 2 Hard Disks
- Data is written alternately and evenly to two or more disks
- Spanning is available
- Fault Tolerance is not available
- Read & Write Speed is Fast

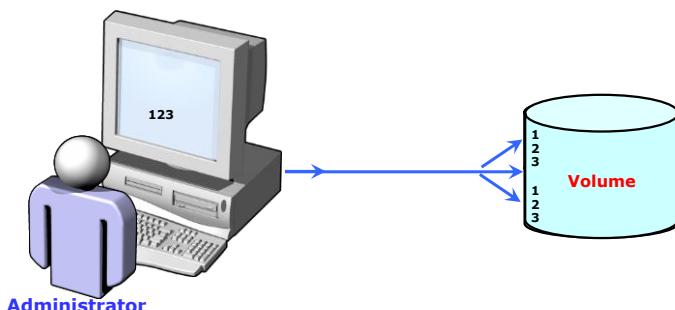
How RAID-0 works?



What Is a Mirrored Volume (RAID-1)?

- Minimum - 2 Hard Disks
- Simultaneously data will be written to two volumes on two different disks
- Any volume can be mirrored including the system and boot volumes
- Fault Tolerance is available
- Read Speed is Fast & Write Speed is Slow
- 50% overhead

How RAID-1 works?



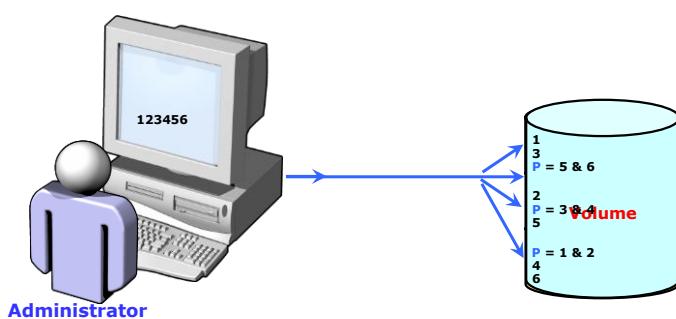
What Is a Parity (RAID-5) Volume?

- Minimum - 3 Hard Disks
- Data is written alternately and evenly to two or more disks and a parity is written on one disk
- Fault Tolerance is available
- Read & Write Speed is Fast,

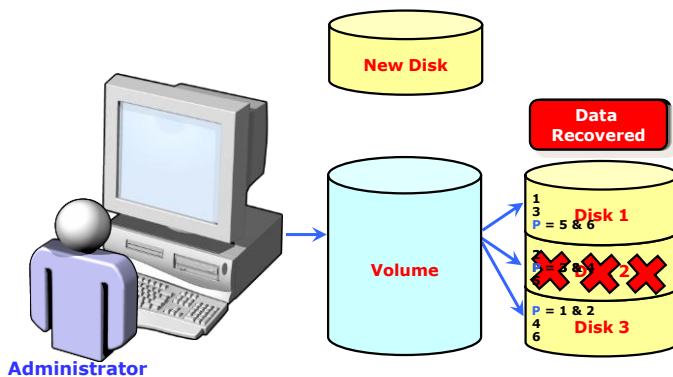
What Is a Parity (RAID-5) Volume?

- Minimum - 3 Hard Disks
- Data is written alternately and evenly to two or more disks and a parity is written on one disk
- Fault Tolerance is available
- Read & Write Speed is Fast,

How RAID-5 works?



What will happen ?



What Are Mount Points and Links?

A mount point is a reference to a location on a disk that enables Windows operating system access to disk resources

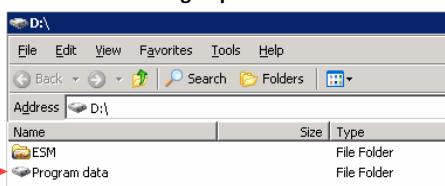
- **Use volume mount points:**
 - To mount volumes or disks as folders instead of using drive letters
 - When you do not have drive letters available for creating new volumes
 - To add disk space without changing the folder structure

A link file contains a reference to another file or directory

- **Link options:**
 - Symbolic file link (or, soft link)
 - Symbolic directory link (or, directory junctions)

What Is a Mounted Drive?

- Is assigned a path rather than a drive letter
- Allows you to add more drives without using up drive letters
- Adds volumes to systems without adding separate drive letters for each new volume

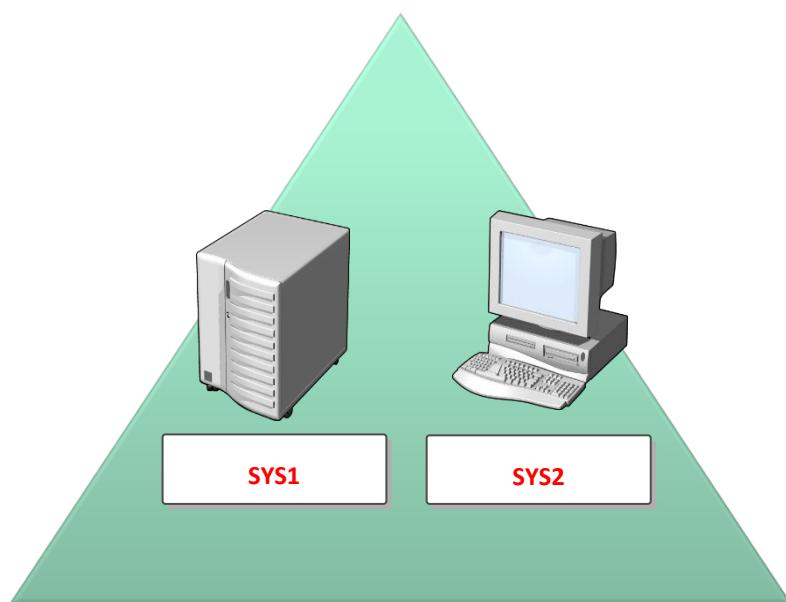


STORAGE MANAGEMENT

Prerequisites:

Before working on this lab, you must have

3. A computer running windows 2012 server or Domain Controller.
4. A computer running windows 2012 server or windows 7.



SYS1

Domain Controller / Terminal Server

IP Address 10.0.0.1

Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

SYS2

Member Server / Client

IP Address 10.0.0.2

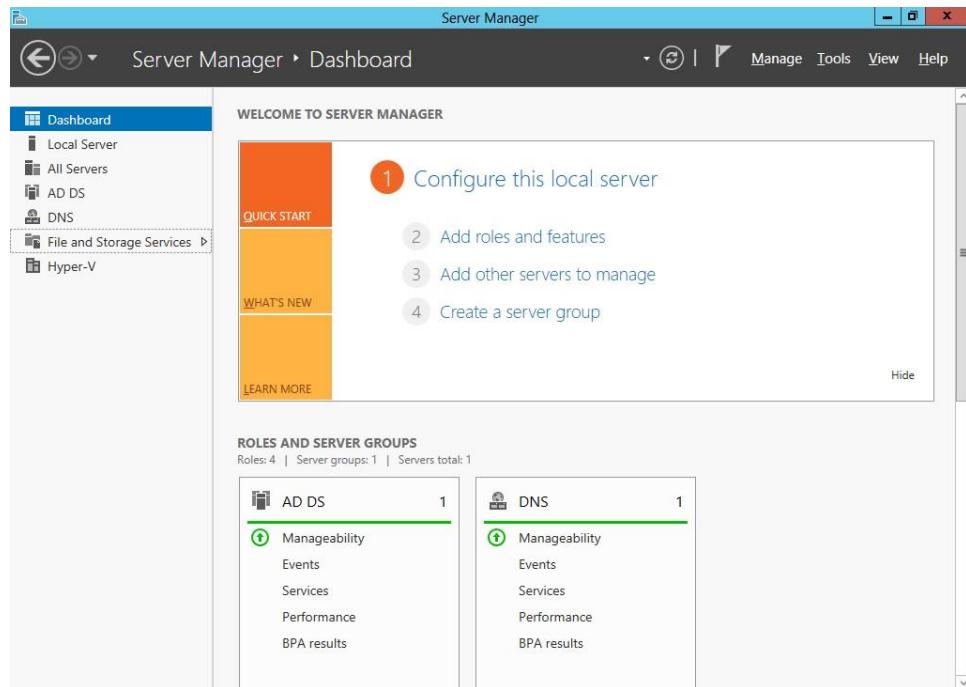
Subnet Mask 255.0.0.0

Preferred DNS 10.0.0.1

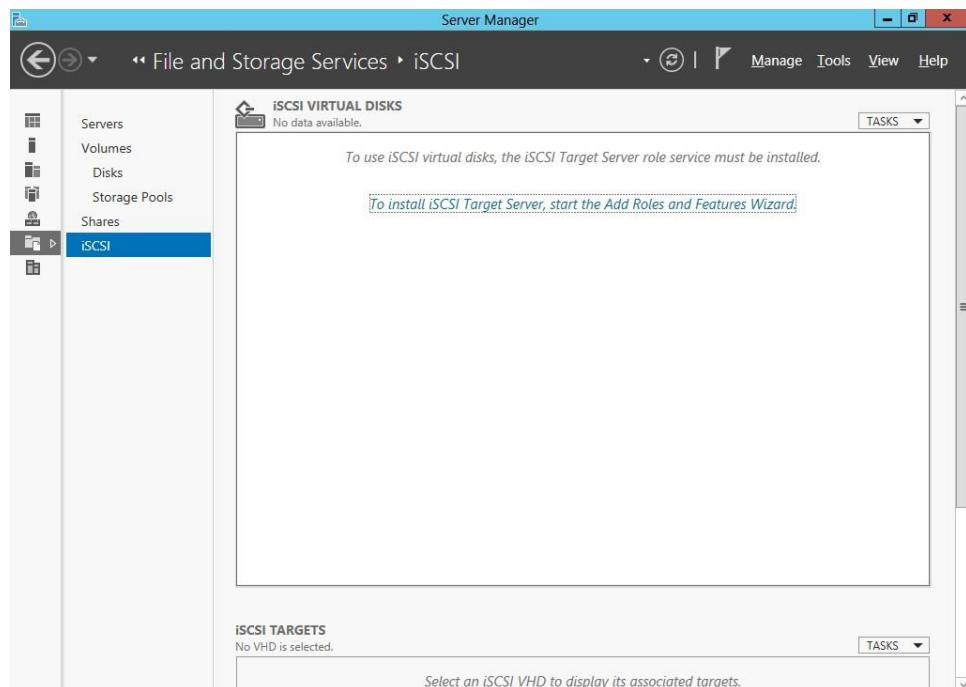
Lab – 1: Configuring iSCSI Target Server

SYS1 – CONFIGURATION

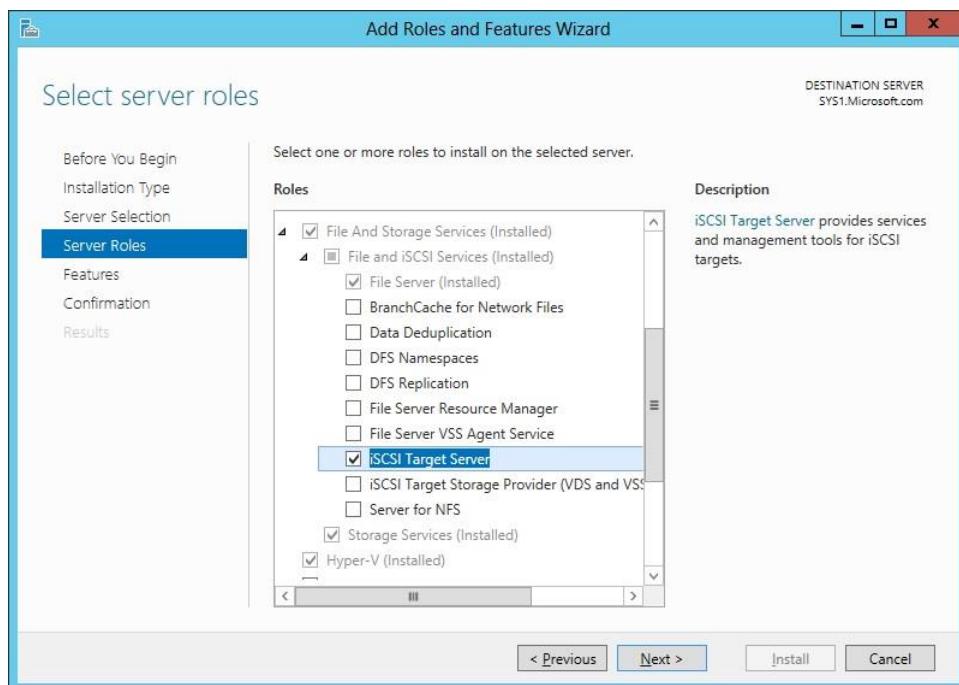
1. Go to Server Manager, click **File and Storage Services**.



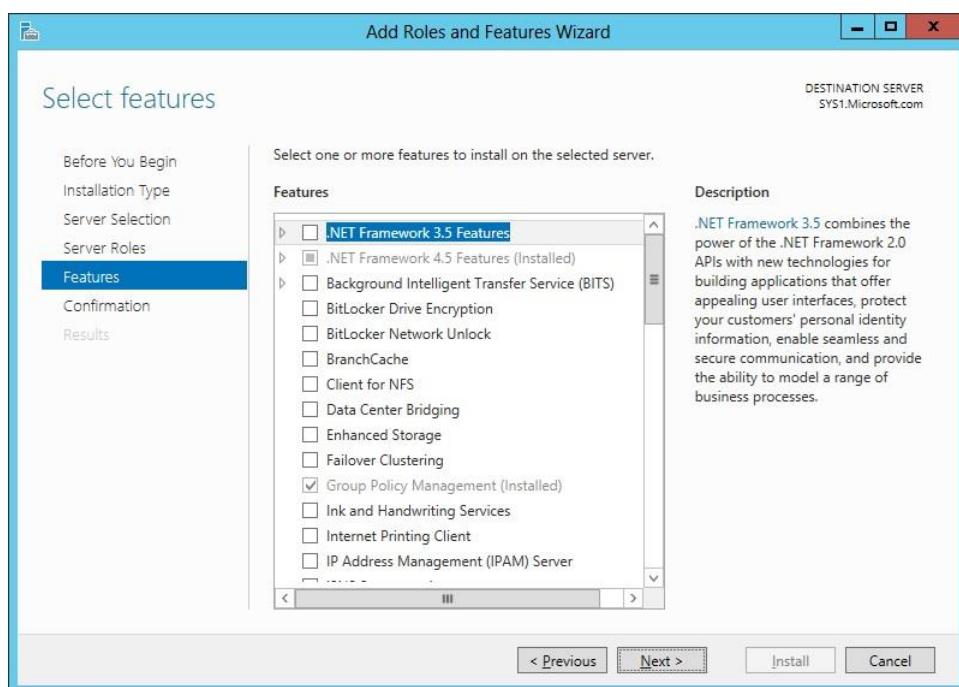
2. Click **To install iSCSI Target Server, start the Add roles and Features Wizard.**



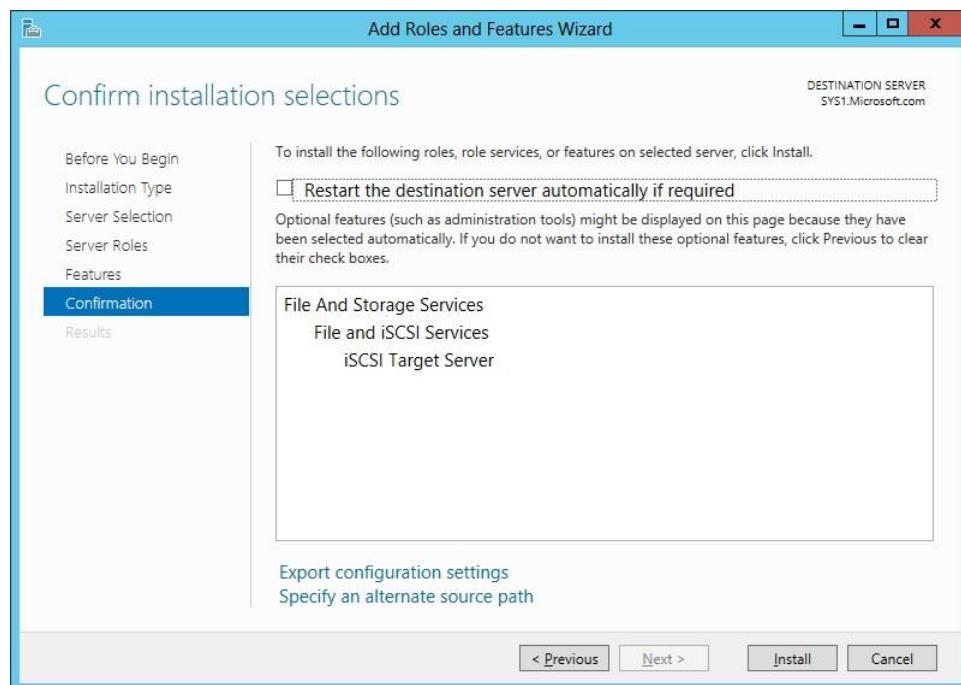
3. In Select server roles page, check the box iSCSI Target Server, click **Next**.



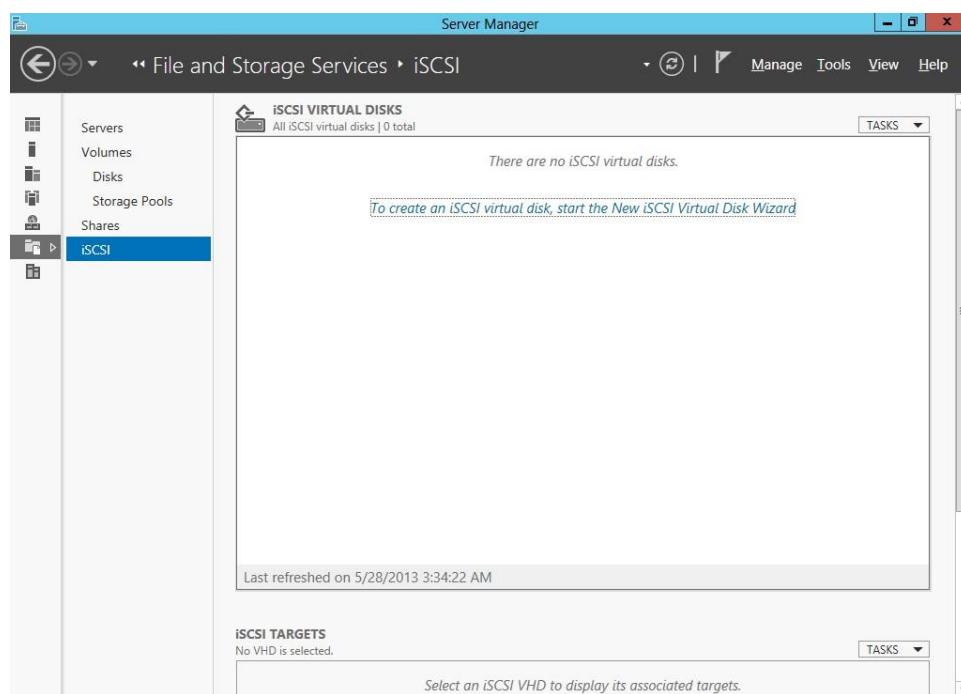
4. In Select features page, click **Next**.



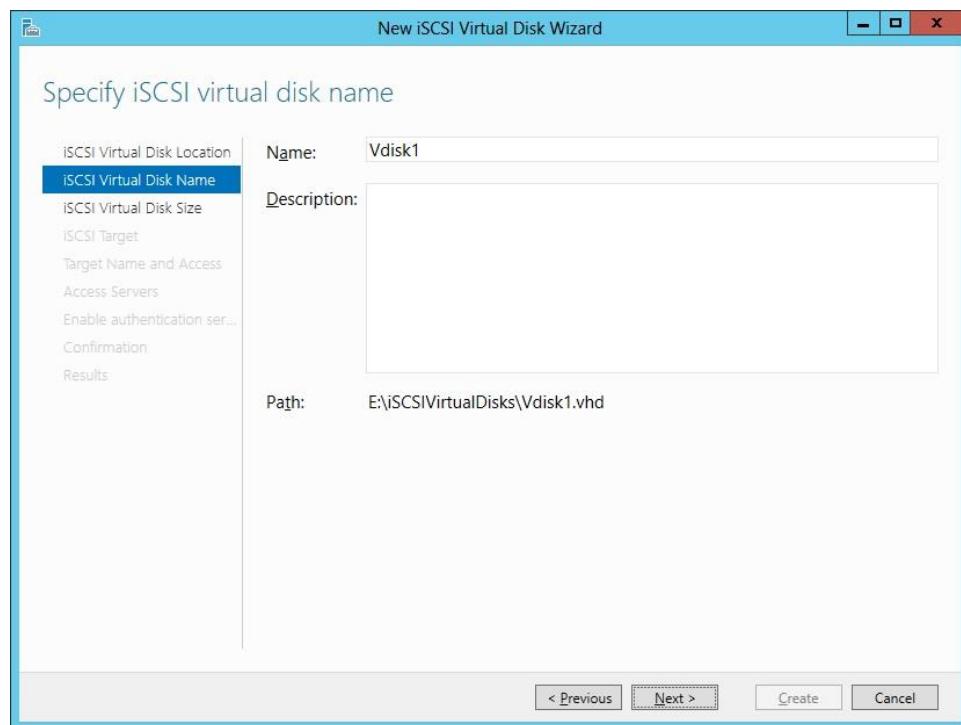
5. Check box Restart the destination server automatically if required, click **Install**.



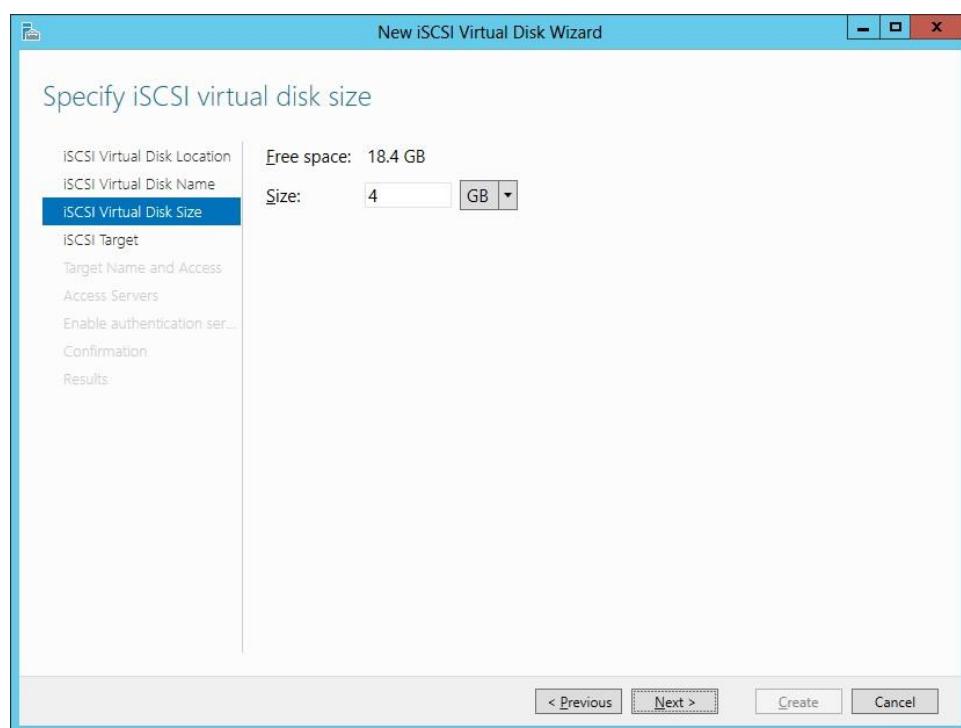
6. Go to Server Manager, select File and Storage Services, and select iSCSI, click **To create an iSCSI virtual disk, start the New iSCSI Virtual Disk Wizard**.



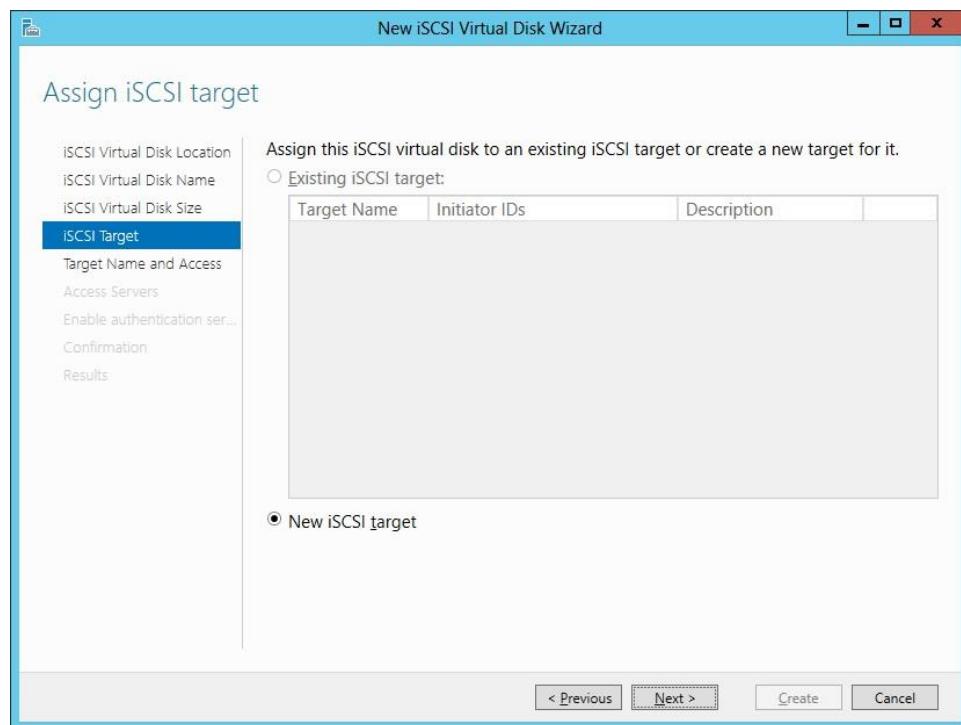
7. Enter **Name** (Ex: Vdisk1), click **Next**.



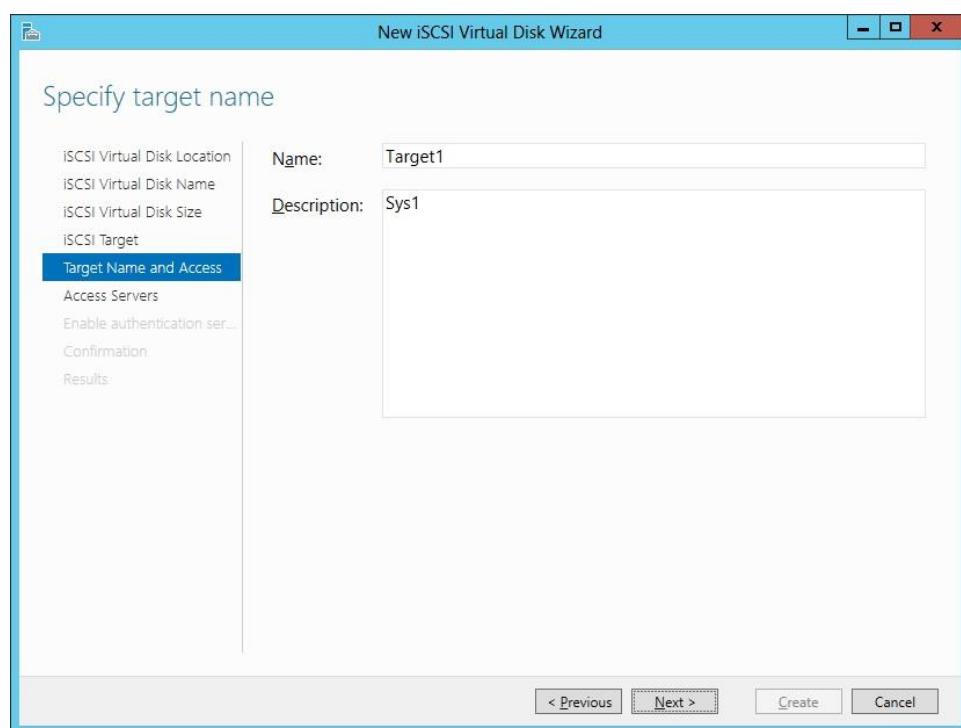
8. Enter the iSCSI virtual disk size (Ex: 4 GB), click **Next**.



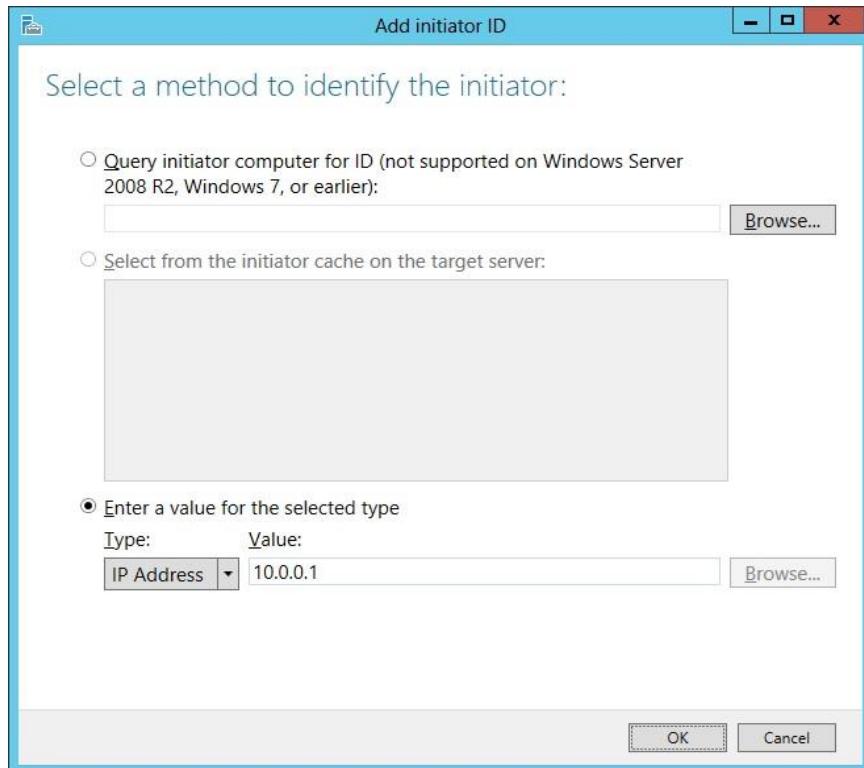
9. Select New iSCSI target, click **Next**.



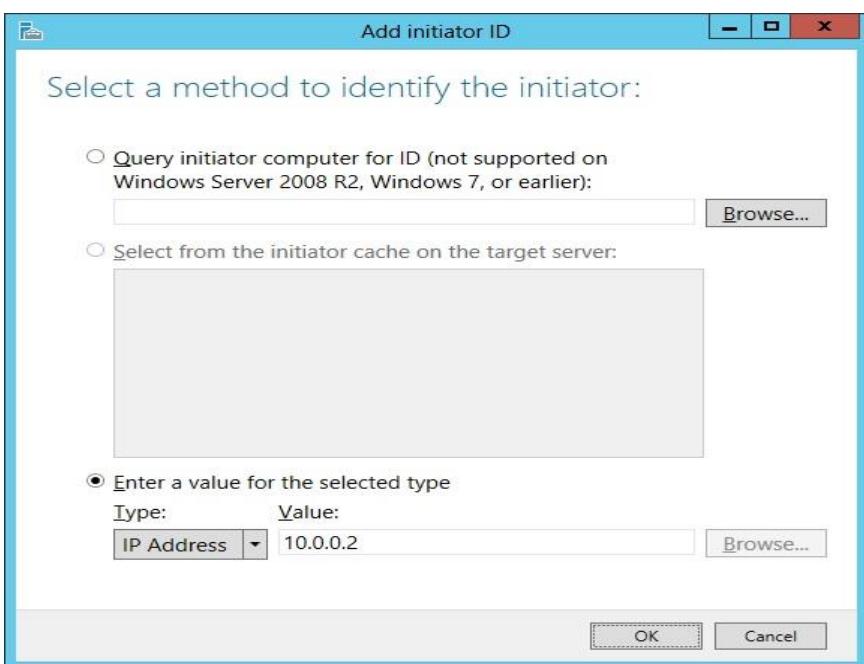
10. Enter the **Name** (Ex: Target1), click **Next**.



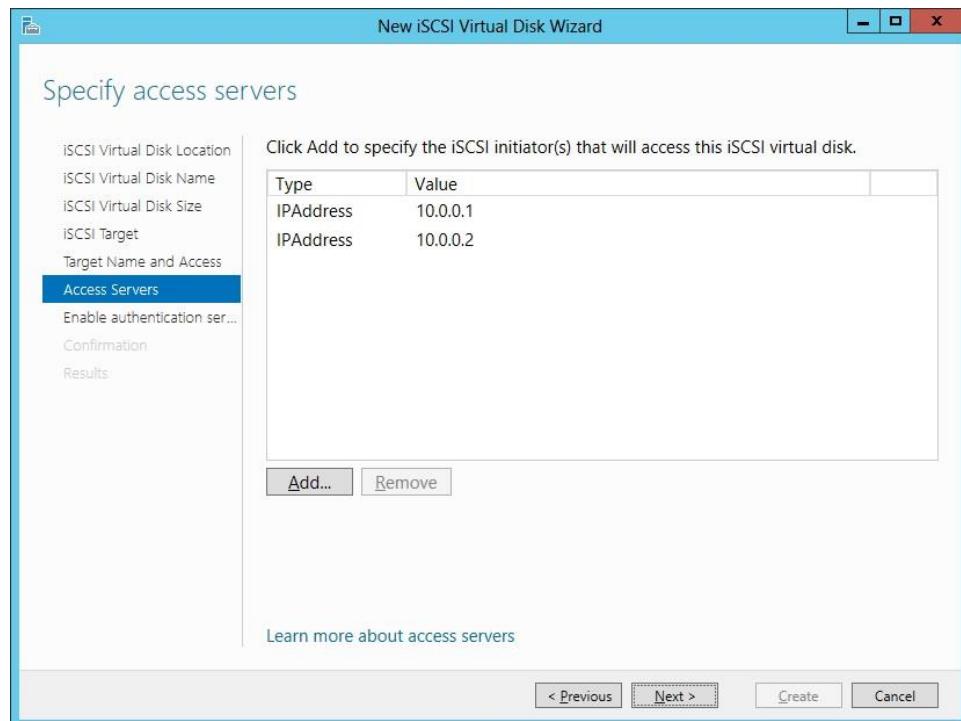
11. Select Enter a value for the selected type, select **IP Address** in Type, enter the Value (Ex: 10.0.0.1), click **OK**.



12. To allow other computers to access the iSCSI Target Server, Select Enter a value for the selected type, select **IP Address** in Type, enter the Value (Ex: 10.0.0.1), click **OK**.

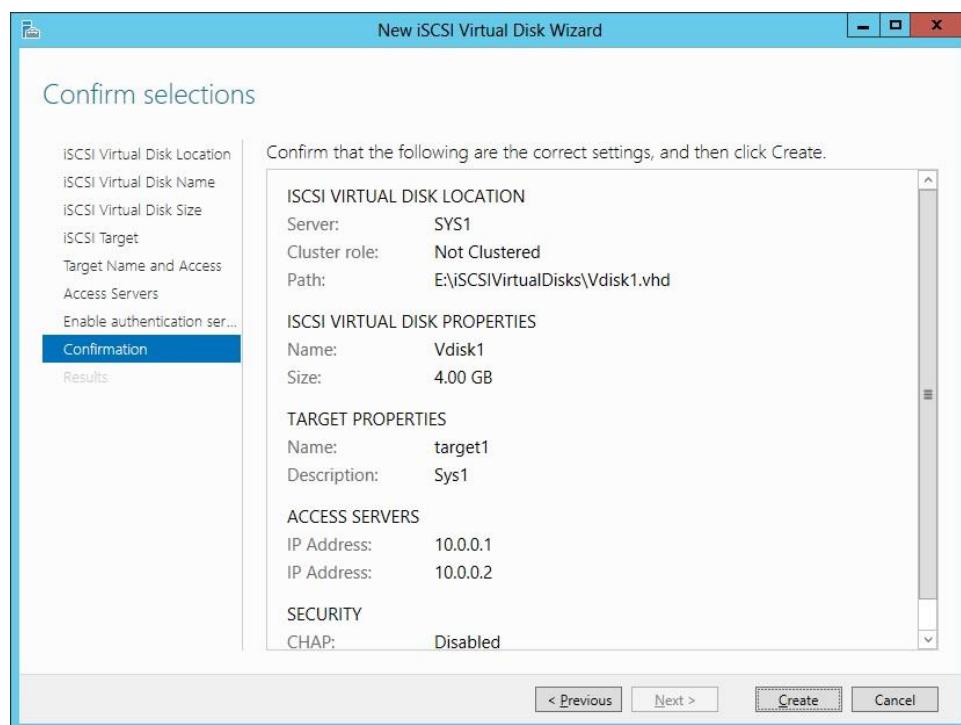
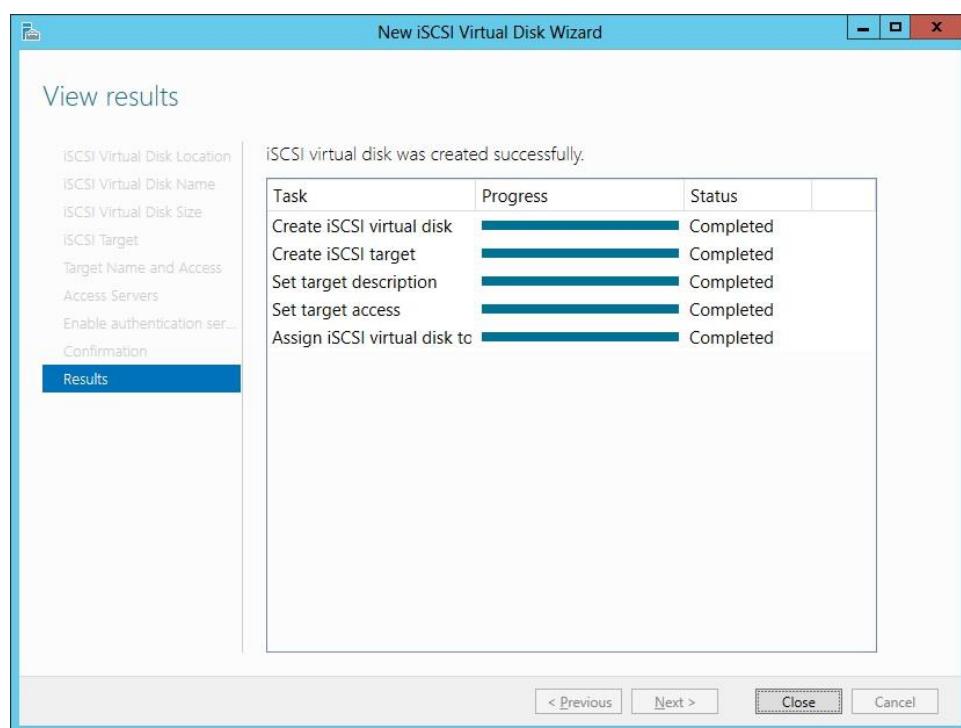


13. Only the specified servers can access the iSCSI Target Server, click **Next**.

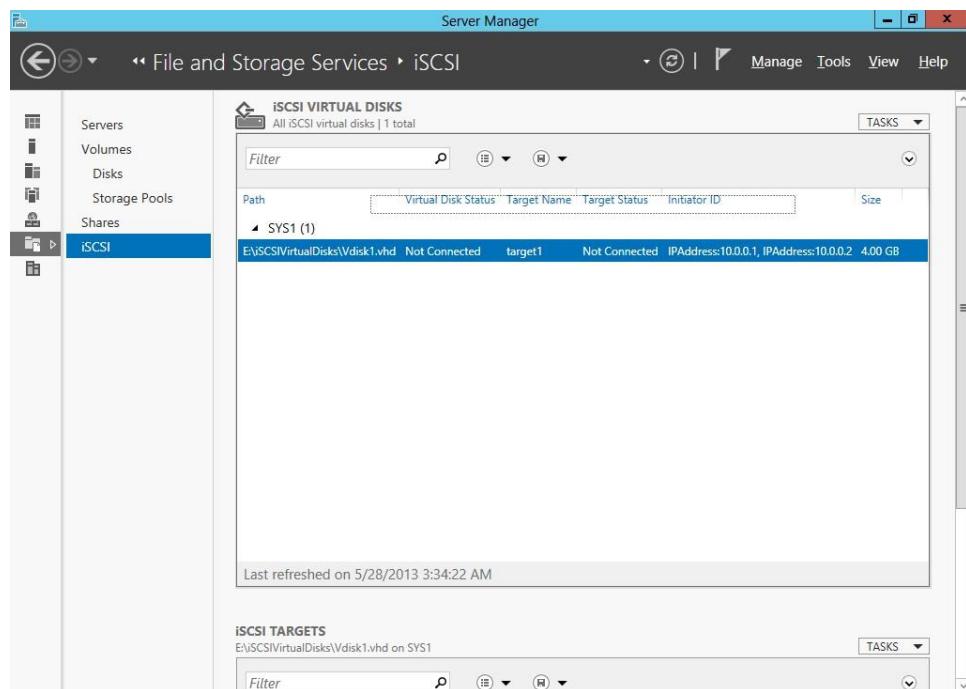


14. In Enable Authentication page, click **Next**.



15. Click **Create**.16. Verify the message Completed, click **Close**.

17. iSCSI Virtual Disk Vdisk1.vhd has been created.

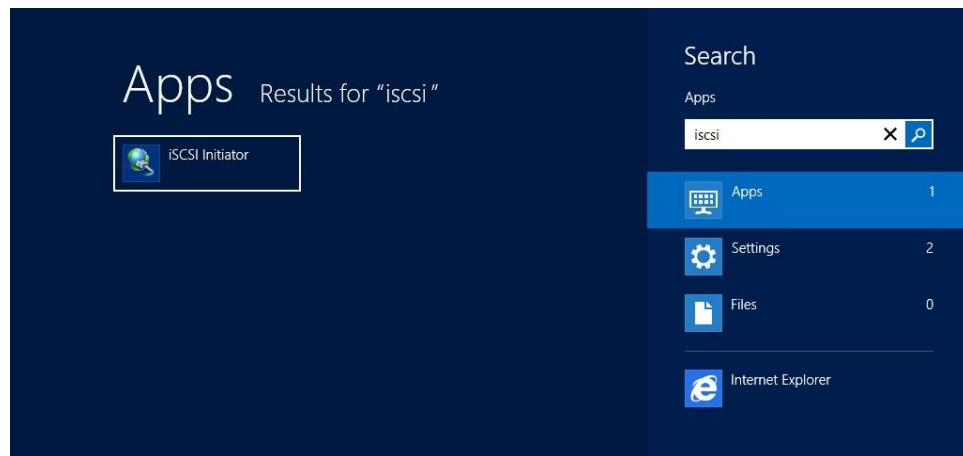


18. Similarly create multiple iSCSI Virtual Disk that can be accessed from **SYS2**.

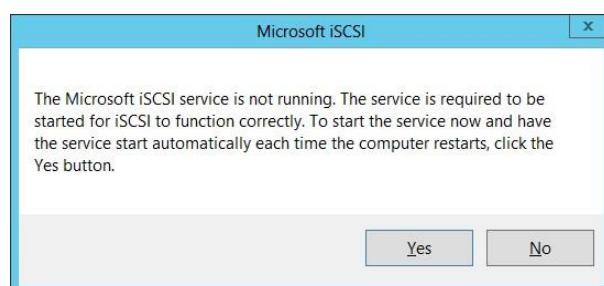
Lab – 2: Configuring iSCSI Initiator

SYS2 – CONFIGURATION

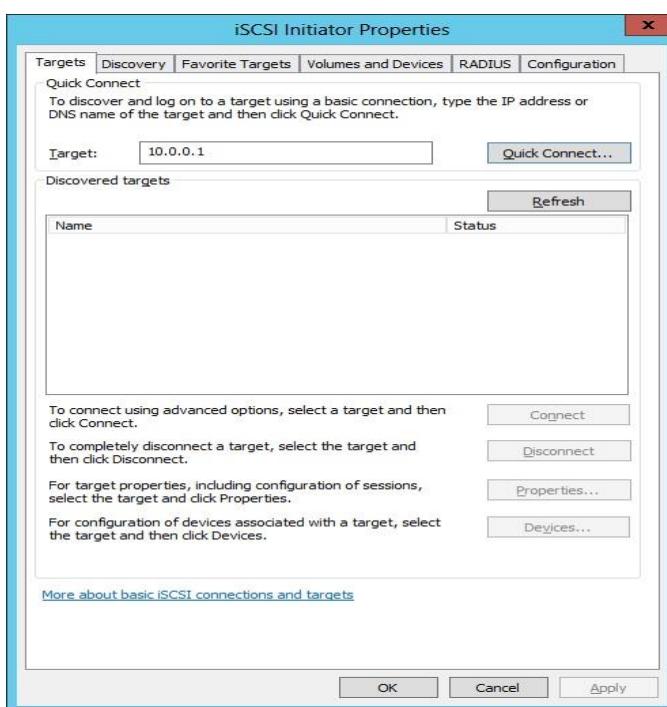
1. Go to Start, type iSCSI in Search Apps, select **iSCSI Initiator**.



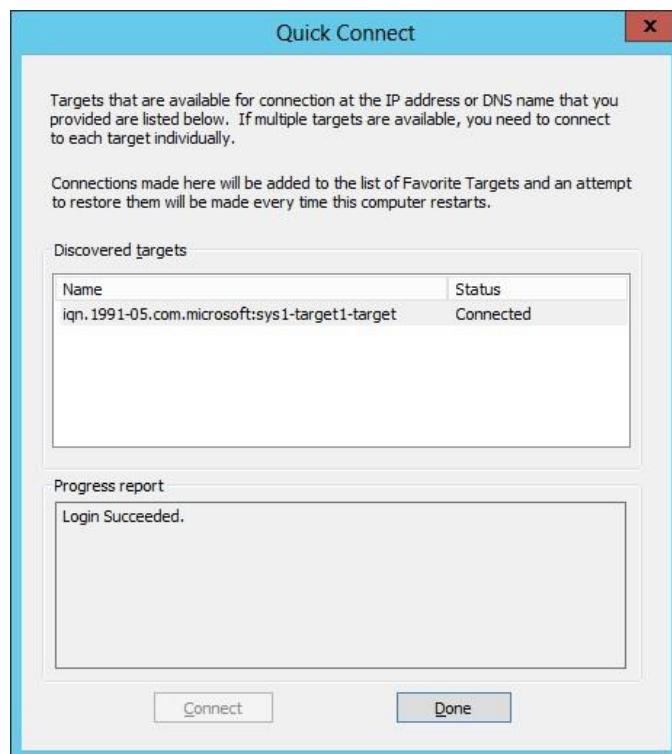
2. Click **Yes** to Microsoft iSCSI service.



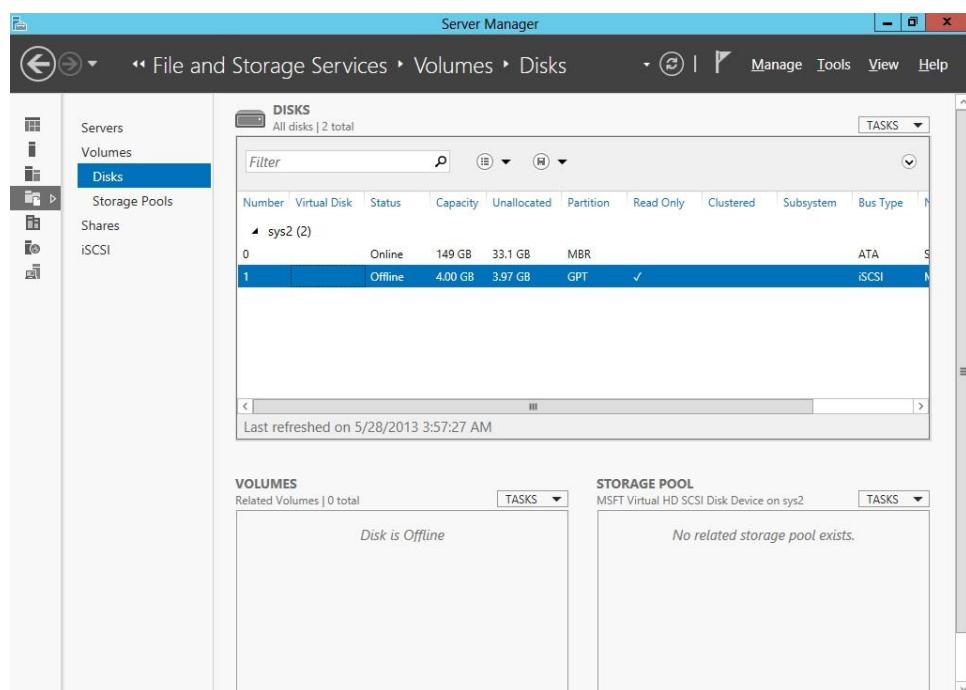
3. Enter the IP Address of Target Server (Ex: 10.0.0.1), click **Quick Connect**.



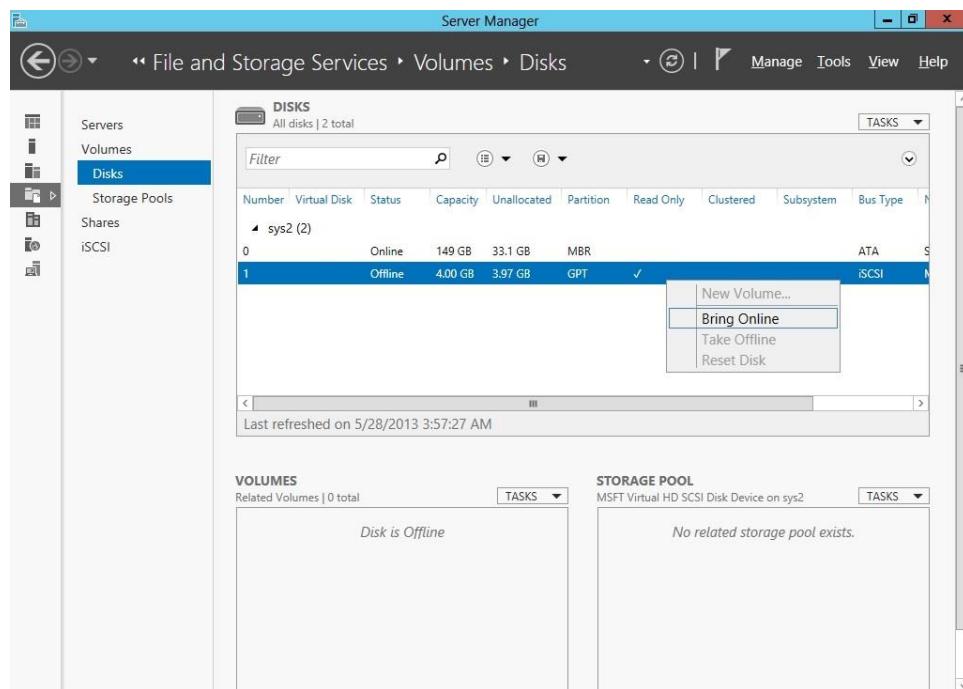
4. Verify for the message Connected, Login Succeeded, click Done.



5. Go to Server Manager → File and Storage Services → Disks.



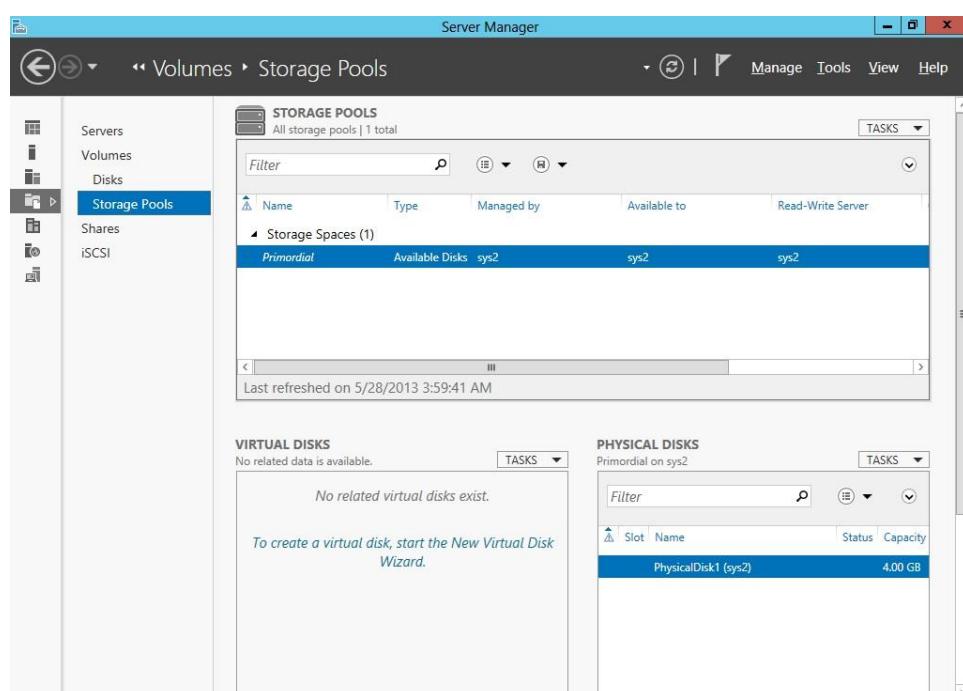
6. Right click on offline disk iSCSI, select Bring Online.



7. Click Yes



8. Select Storage Pools, and Verify for Physical Disk1



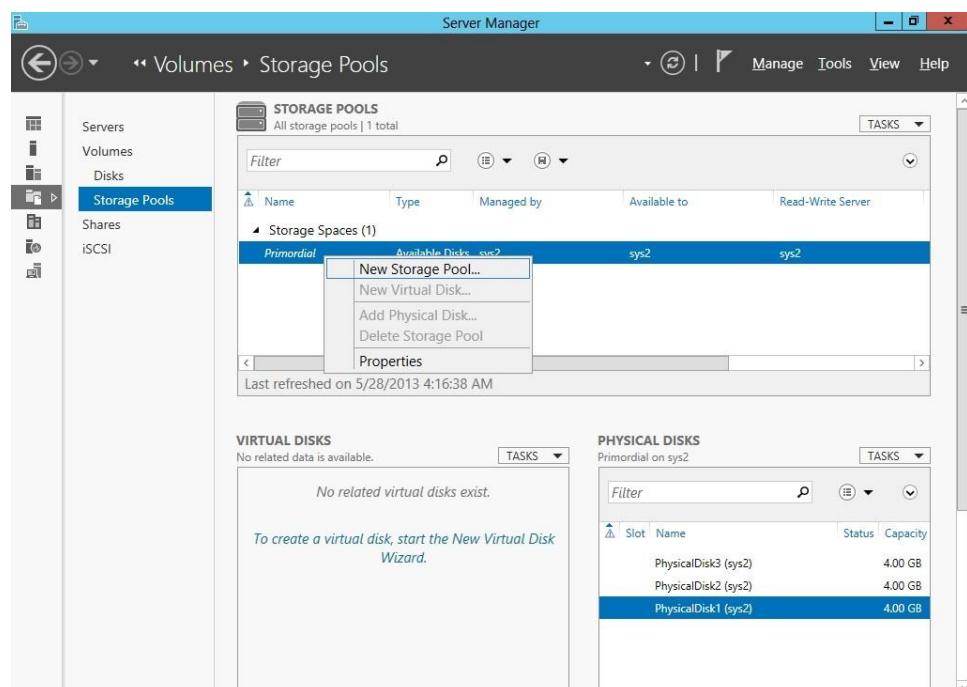
Lab – 3: Creating Storage Pool and Simple Volume

SYS1 – CONFIGURATION

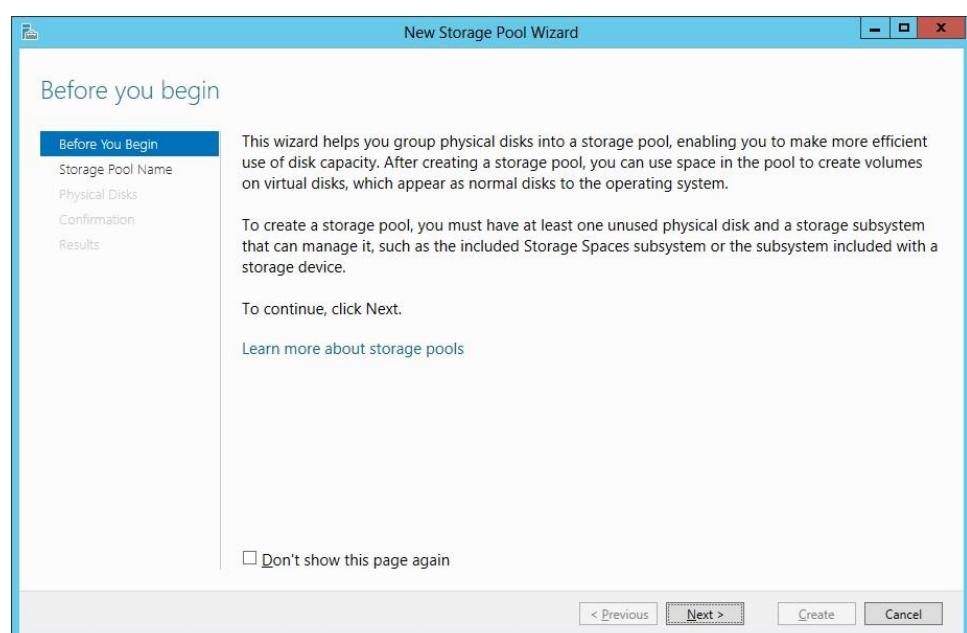
1. Create multiple iSCSI Virtual Disk (Ex: Vdisk1, Vdisk2, Vdisk3...)

SYS2 – CONFIGURATION

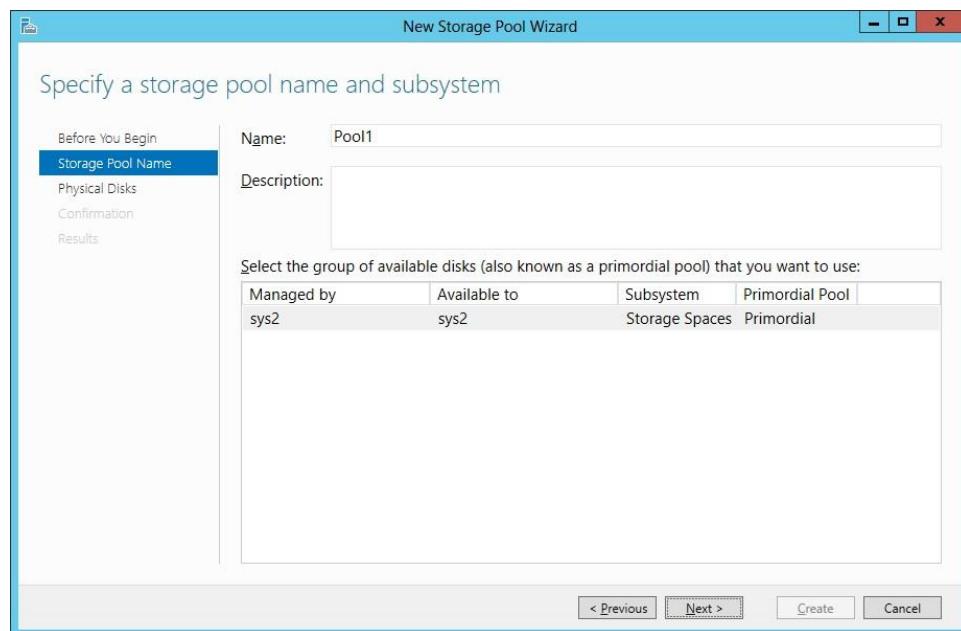
1. Go to Server Manager → File and Storage Services → Storage Pools → select New Storage Pool.



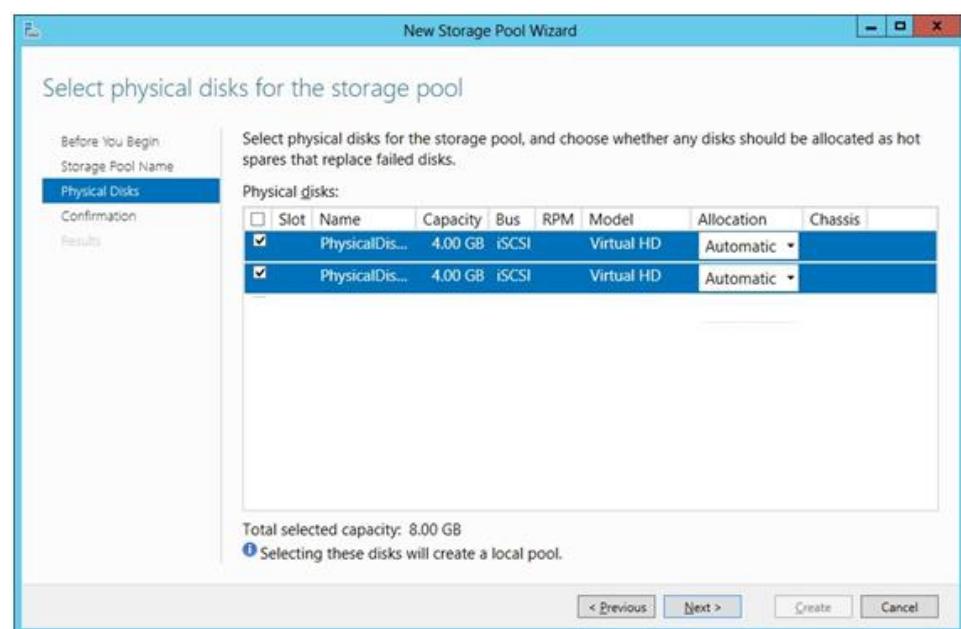
2. In Before you begin page, click Next.

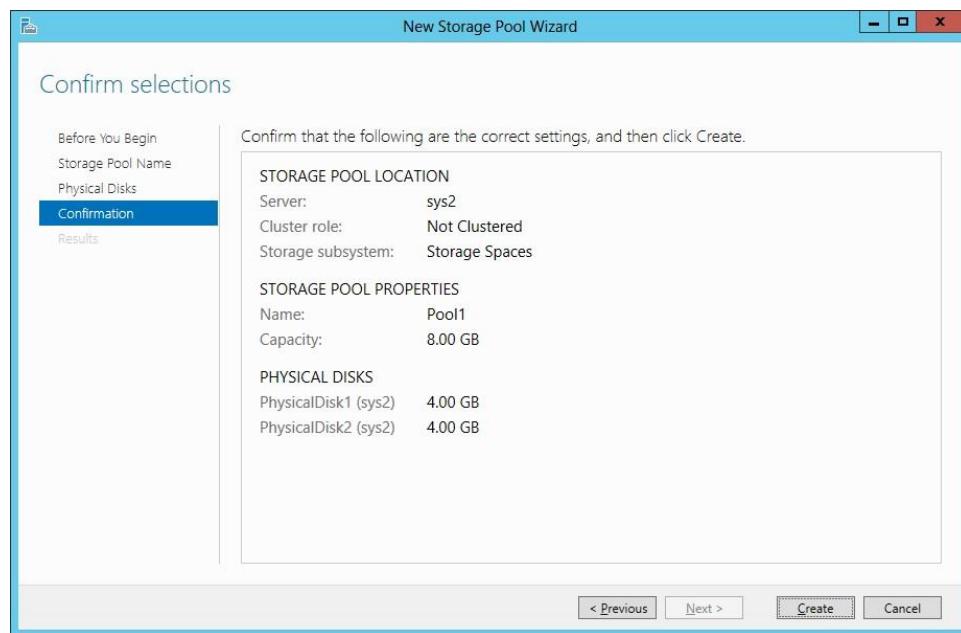
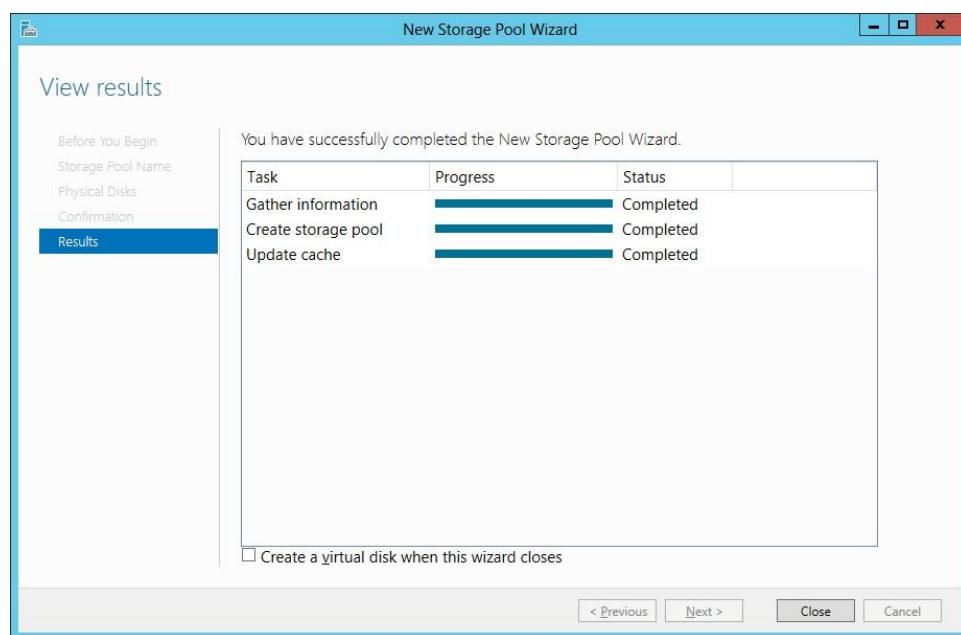


3. Enter Name (Ex: Pool1), click Next.

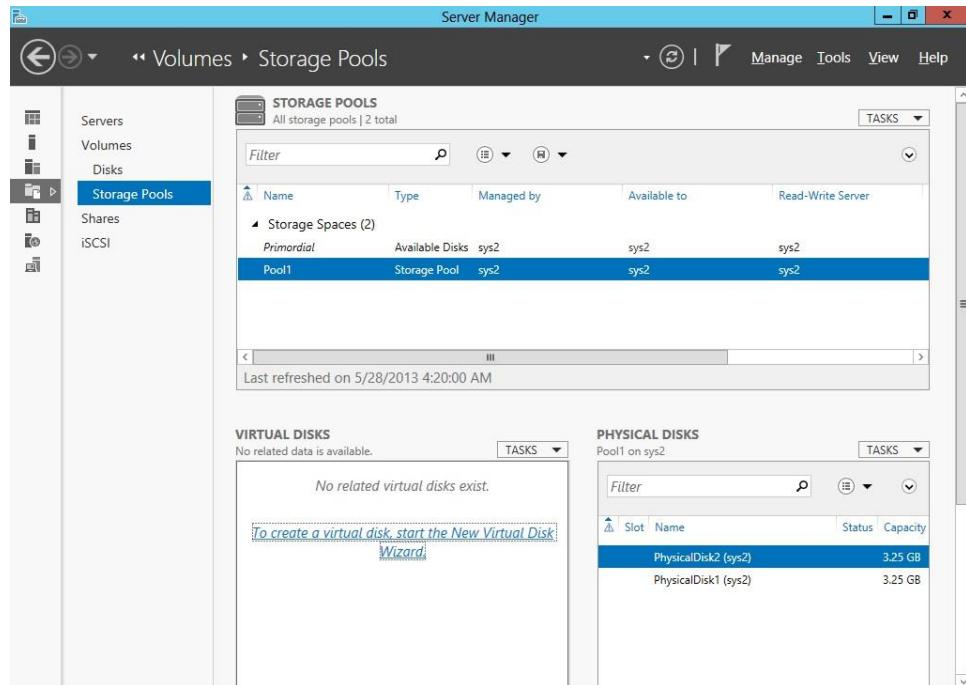


4. Check the boxes to select the physical disk for storage pool, click Next.

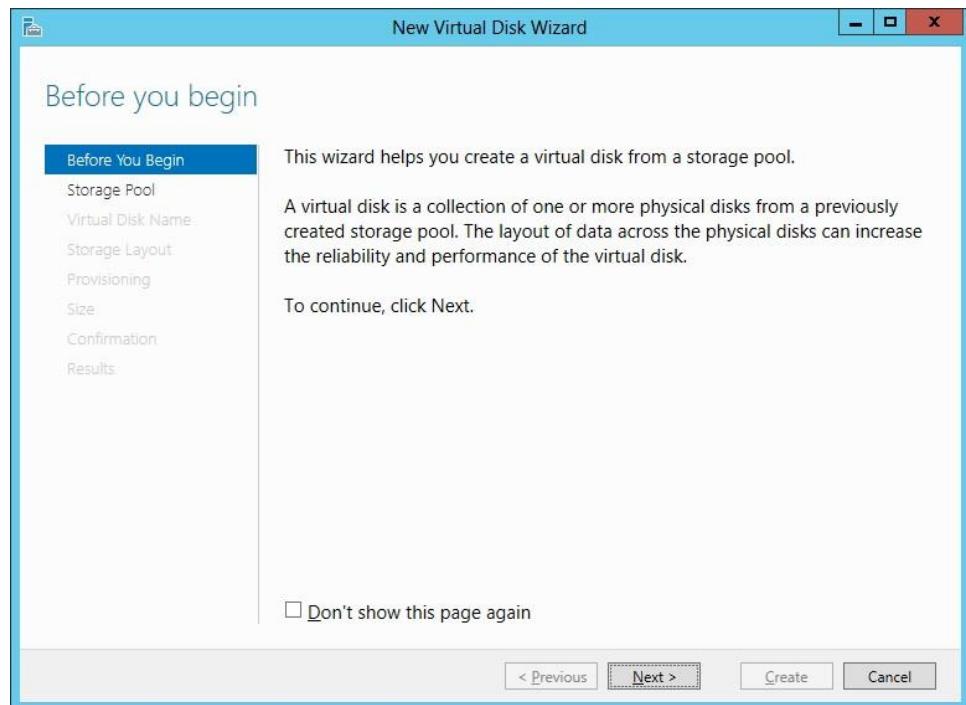


5. Click **Create**.6. Click **Close**.

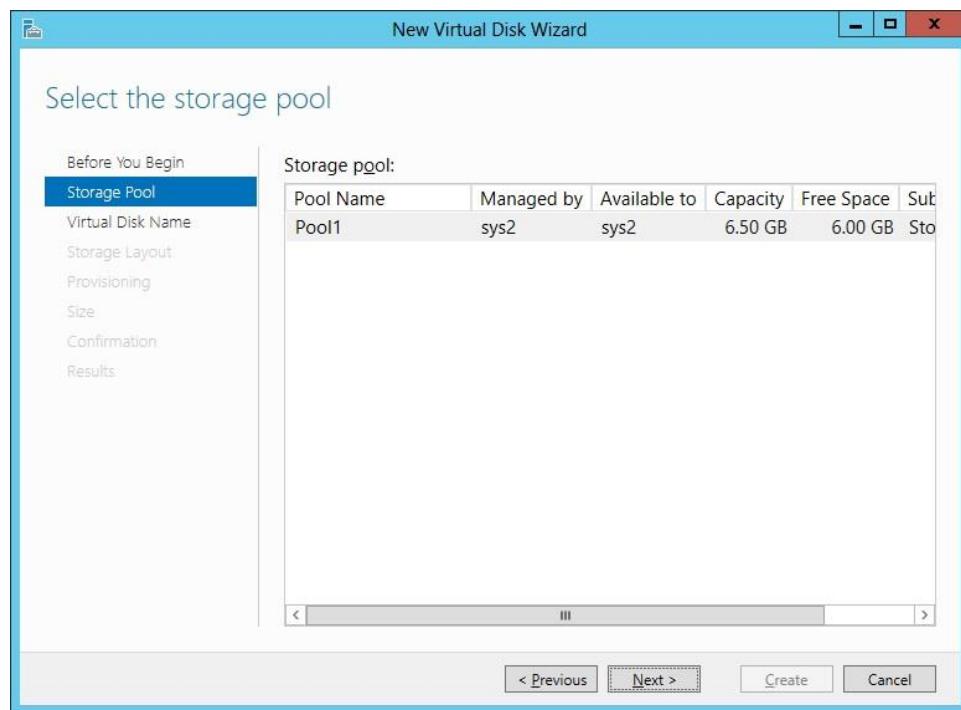
7. In Storage Pools, select Pool1, and click **To create a virtual disk, start the New Virtual Disk Wizard.**



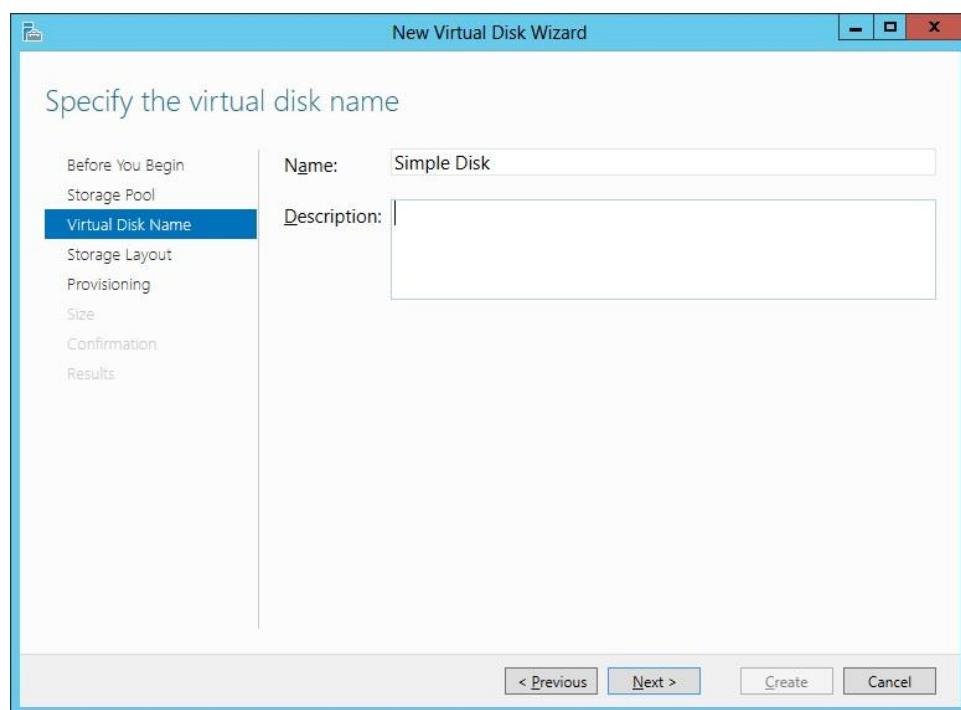
8. In Before you begin page, click **Next**.



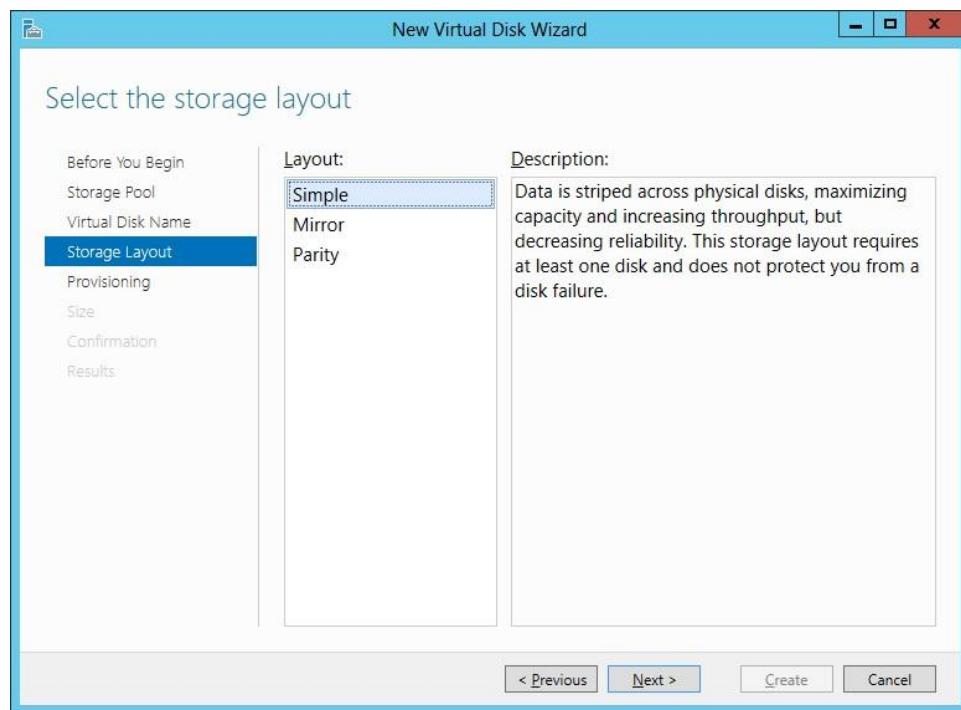
9. Select the storage pool (Ex:Pool1), click **Next**.



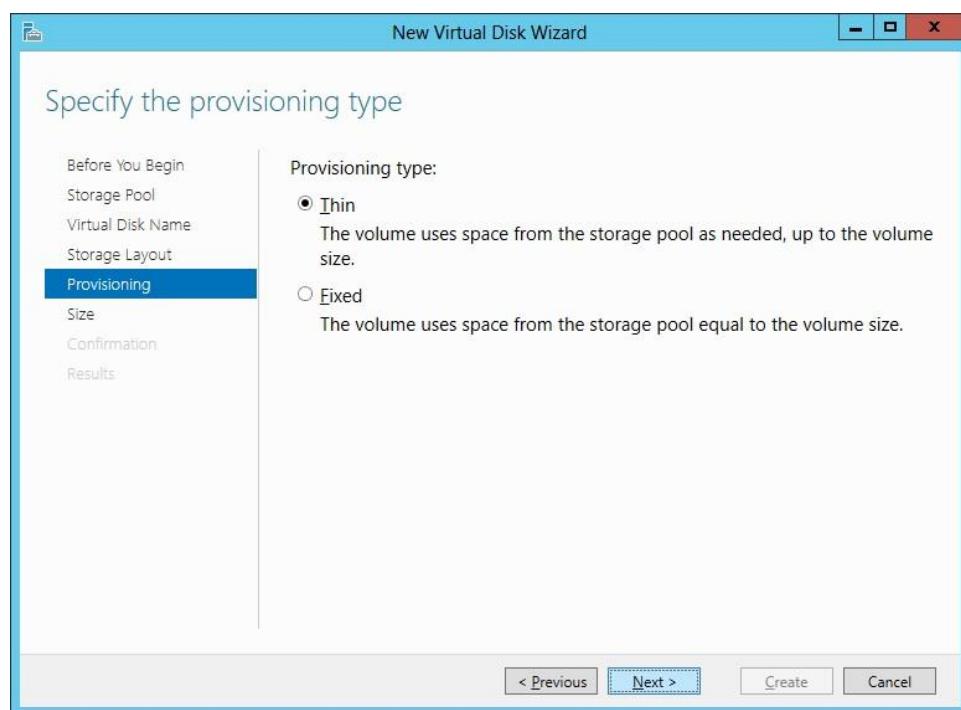
10. Enter **Name** (Ex: Simple Disk), click **Next**.



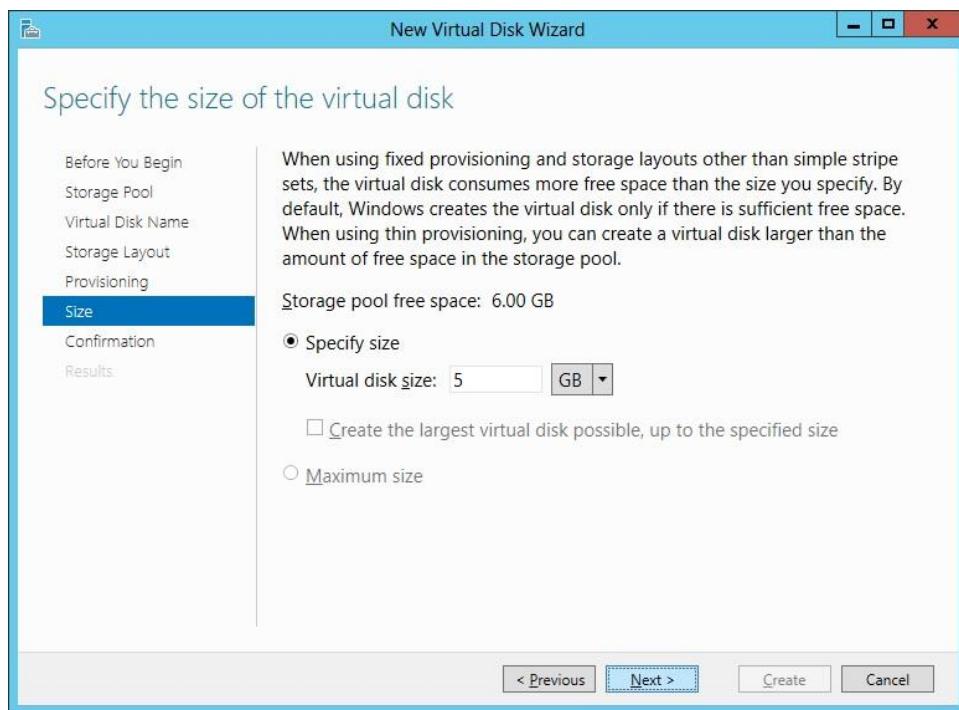
11. Select the Layout **Simple**, click **Next**.



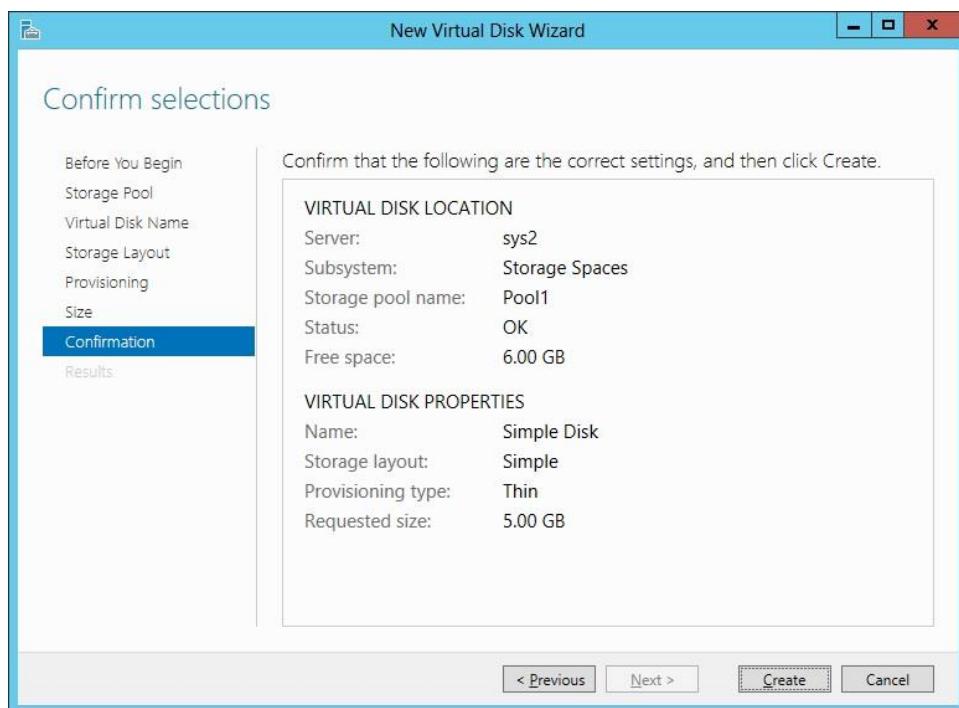
12. Select **Thin** or **Fixed**, click **Next**.



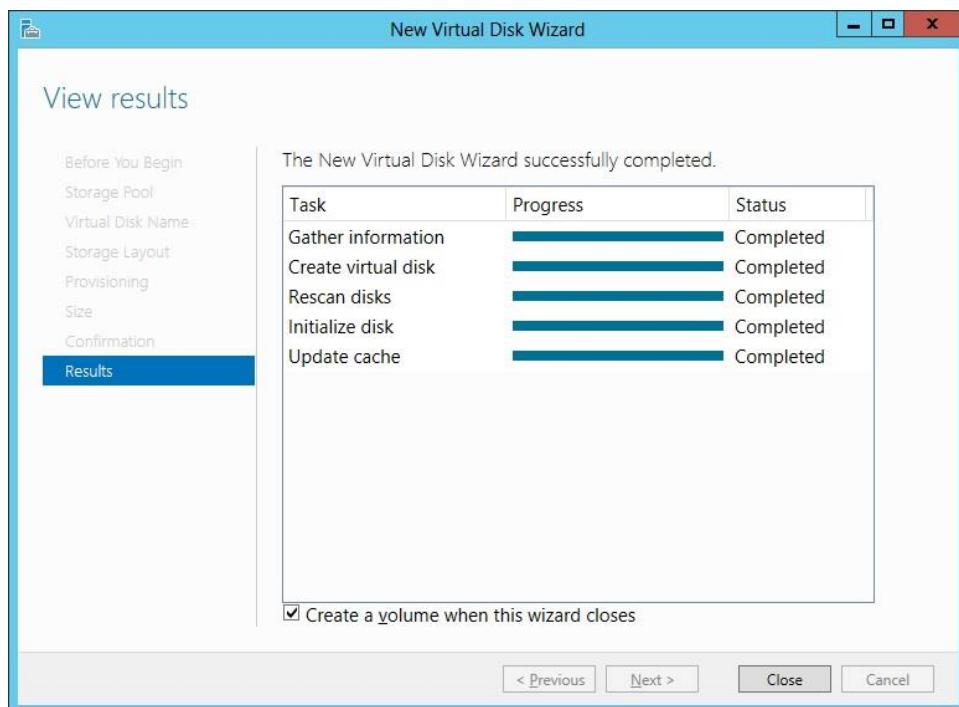
13. Enter the size of the virtual disk, click **Next**.



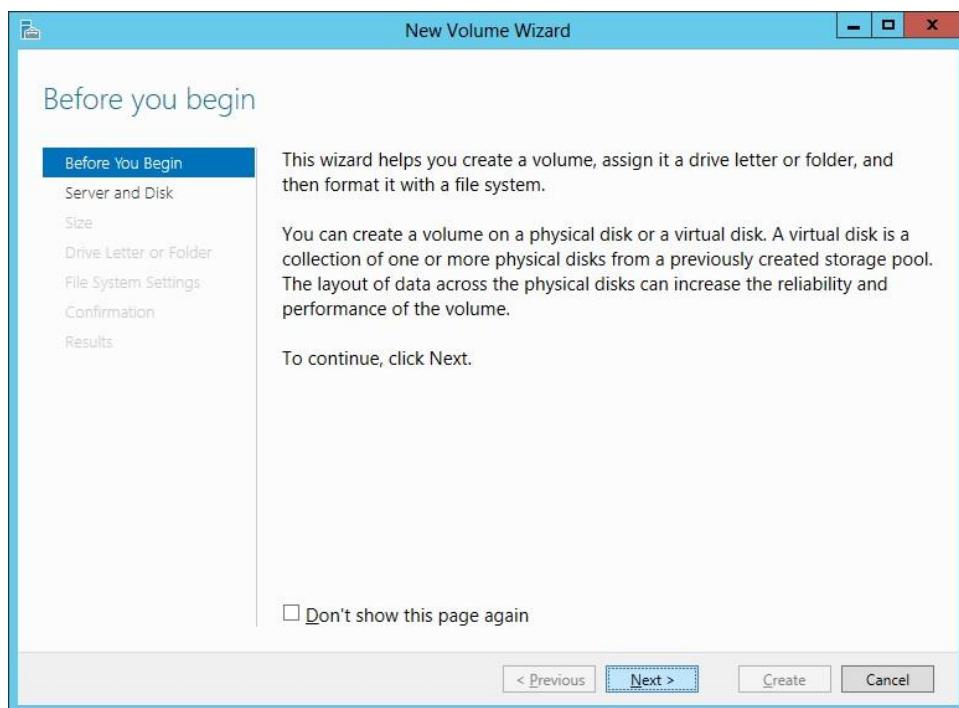
14. Click **Create**.



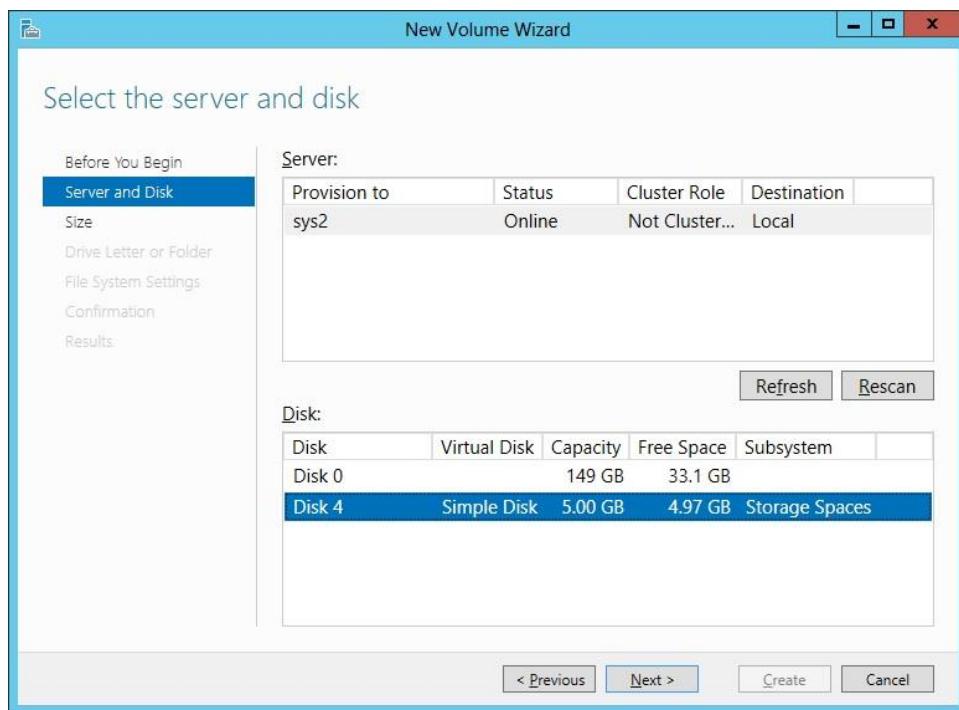
15. Click **Close**, verify the check box Create a volume when wizard closes.



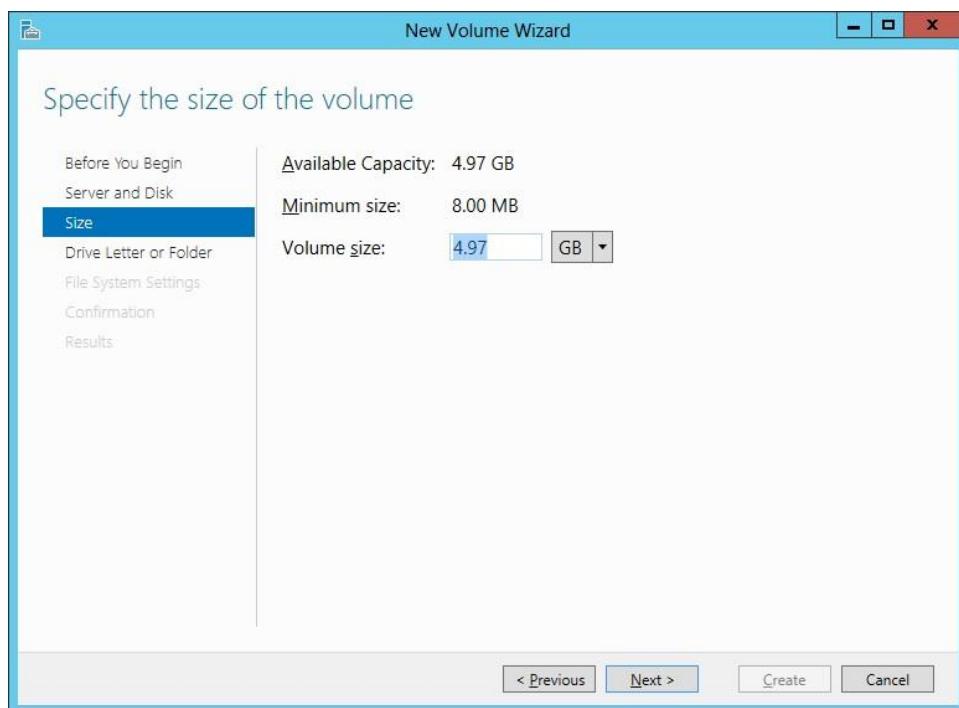
16. In Before you begin page, click **Next**.



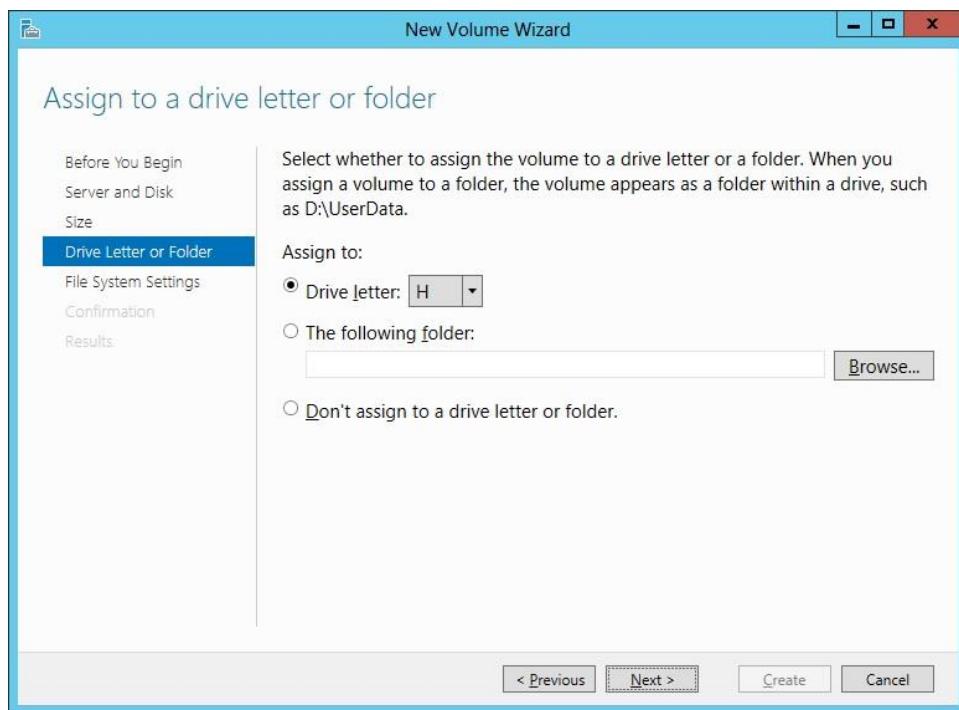
17. Select the disk (Simple Disk), click **Next**.



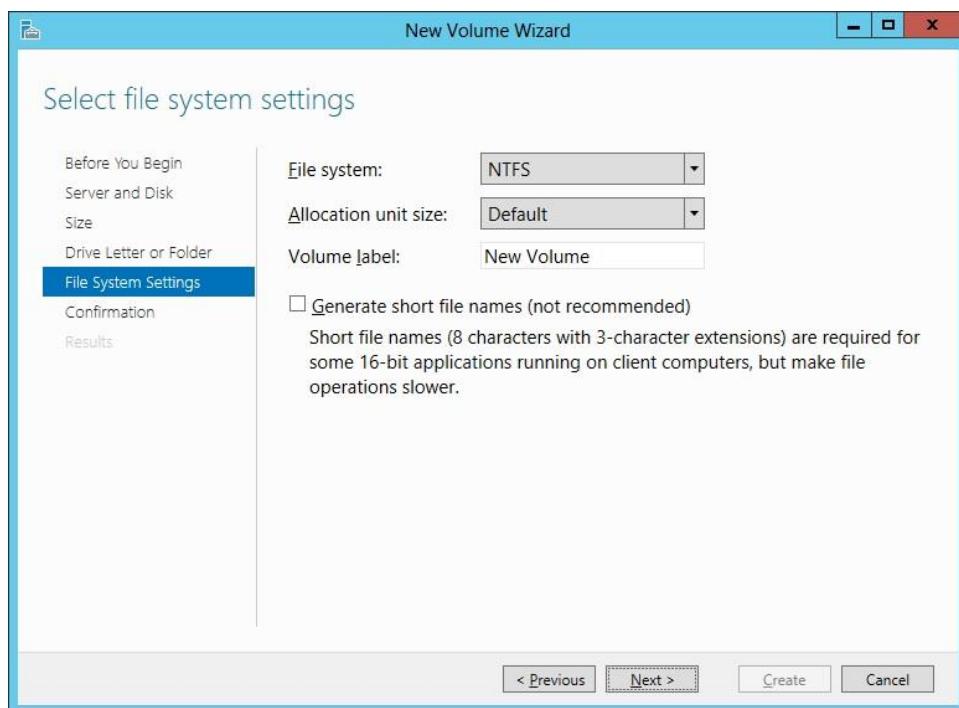
18. Enter the size of the volume, click **Next**.

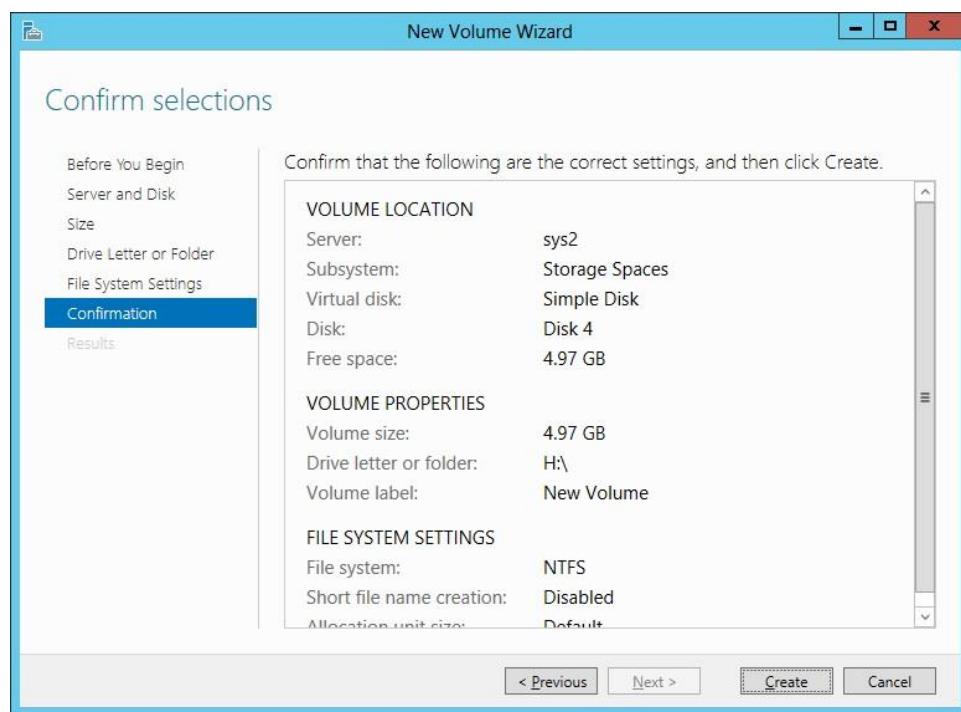
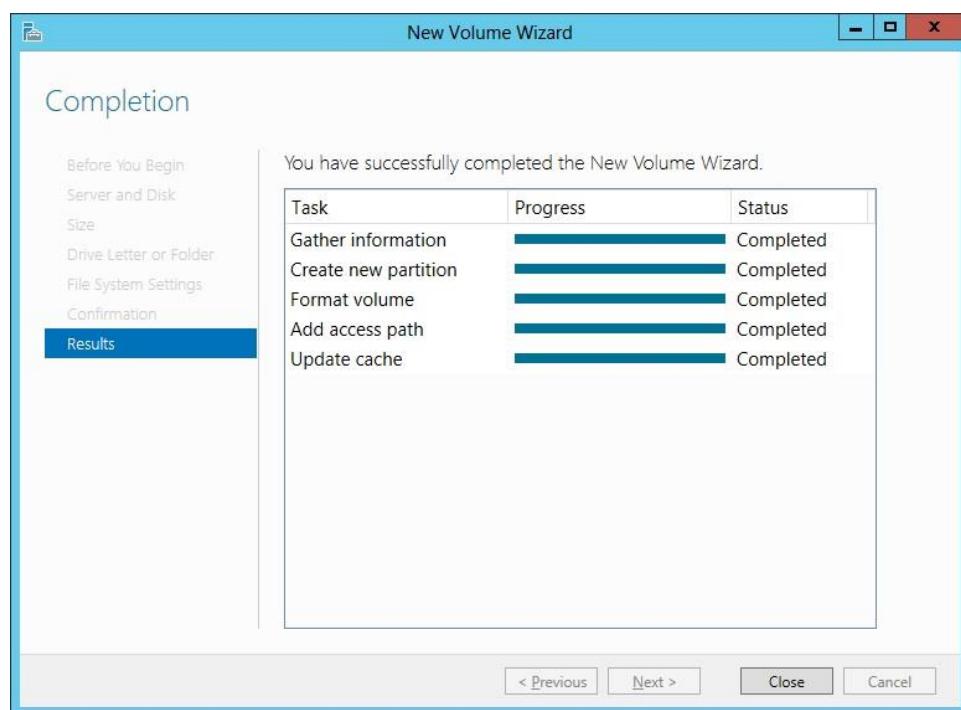


19. Select the Drive letter, click **Next**.



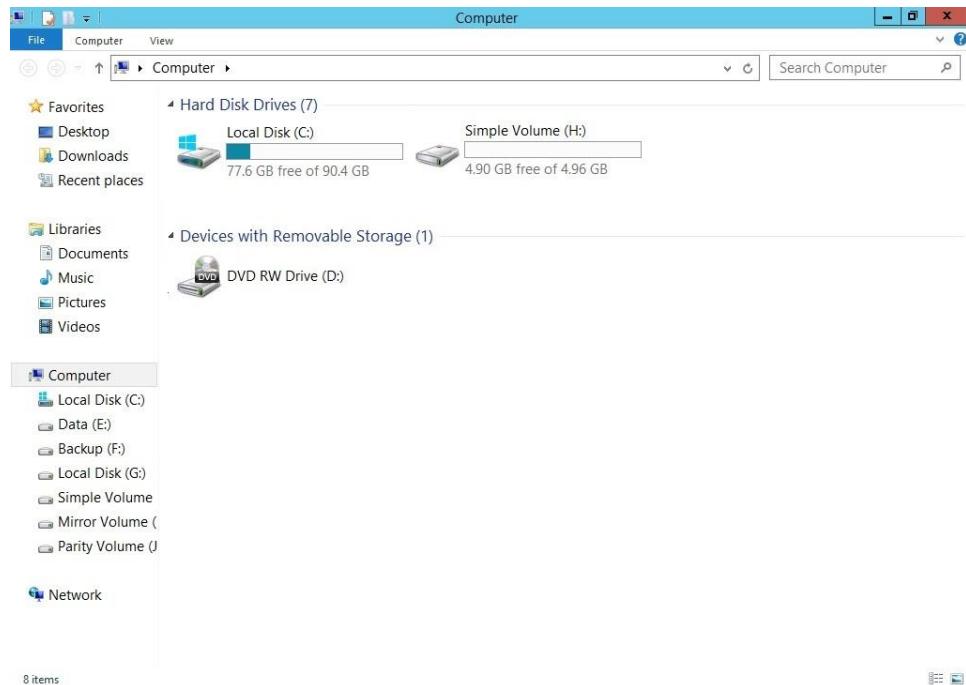
20. Select the File system, click **Next**.



21. Click **Create**.22. Click **Close**.

Verification

1. Go to Start, select Computer Icon and verify for the Simple volume.



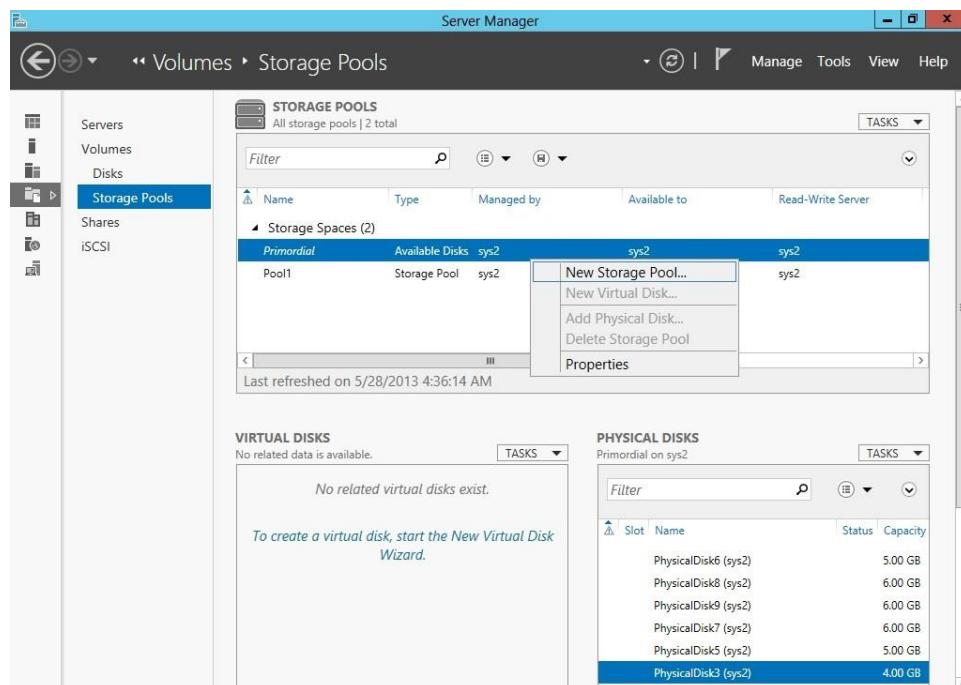
Lab – 4: Creating Mirror Volume (RAID-1)

SYS1 – CONFIGURATION

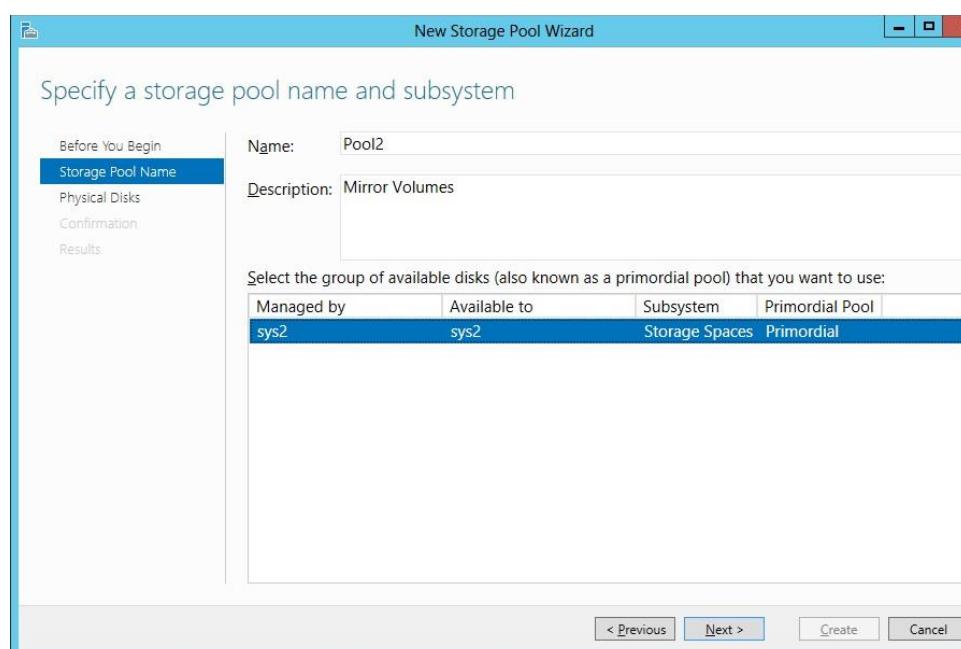
1. Create multiple iSCSI Virtual Disk (Ex: Vdisk4, Vdisk5, Vdisk6...)

SYS2 – CONFIGURATION

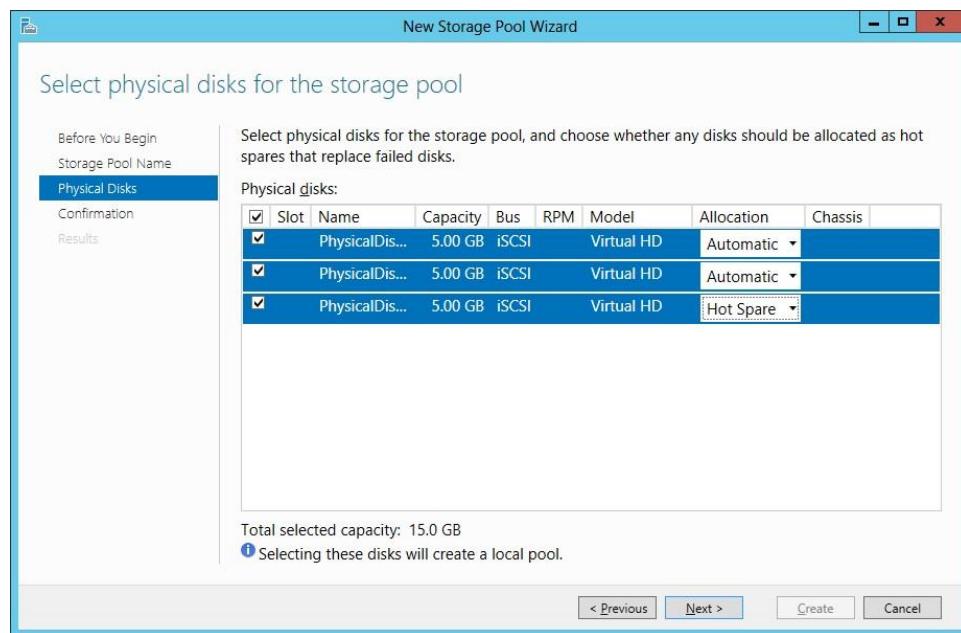
1. Go to Server Manager → File and Storage Services → Storage Pools → right click Primordial storage pool → select **NewStoragePool**.



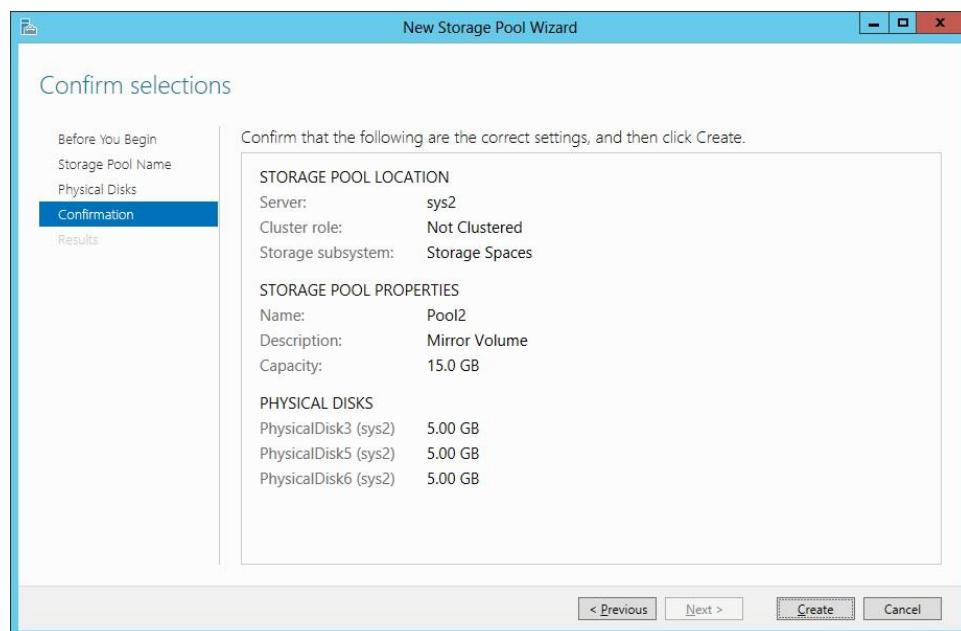
2. Enter Name (Ex: Pool2), click **Next**.



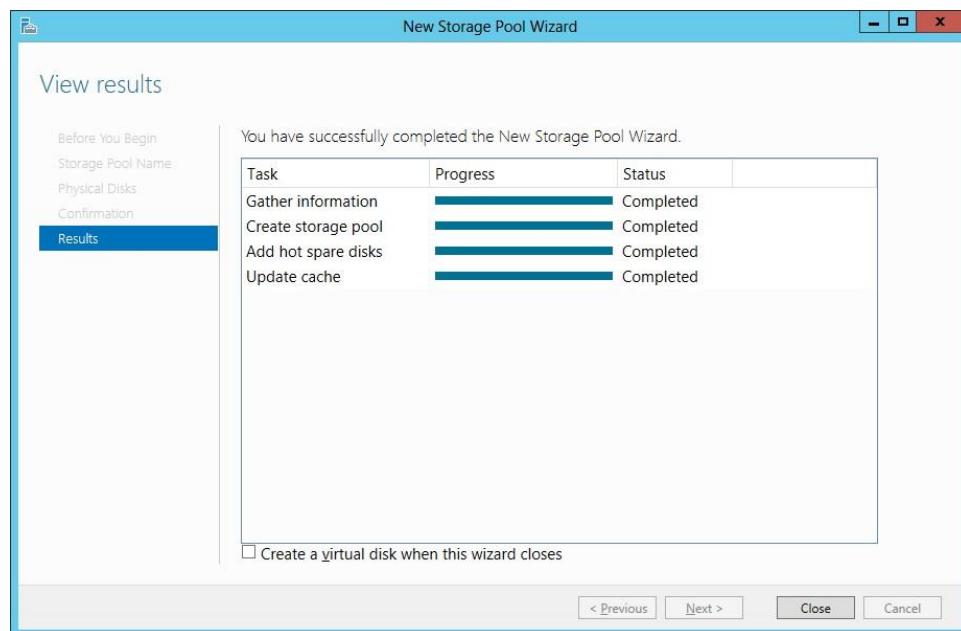
3. Check the boxes and select the physical disks for the Storage pool, click **Next**.



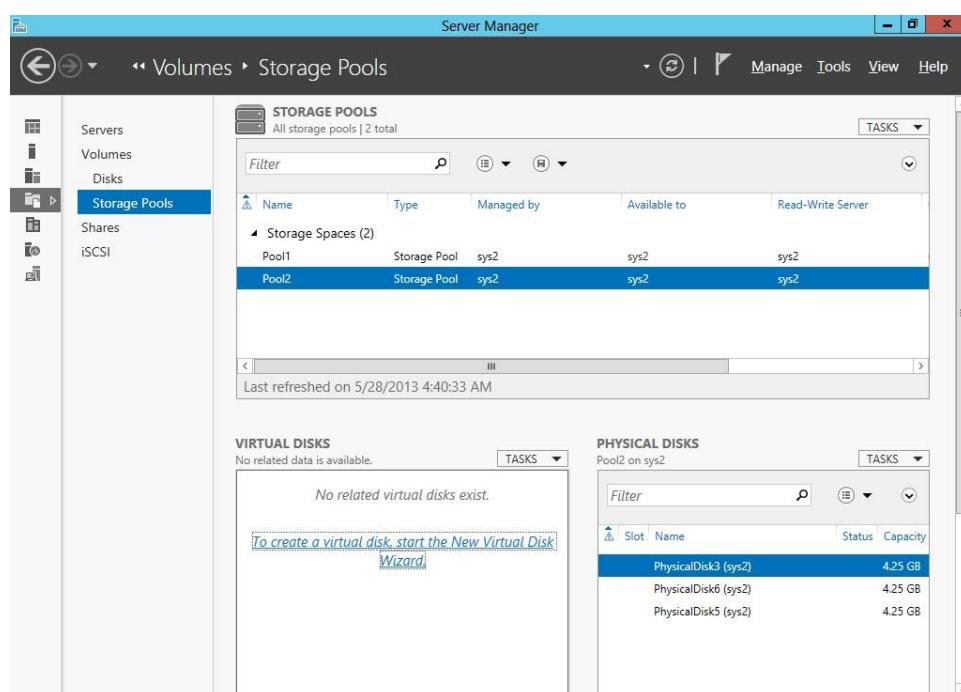
4. Click **Create**.



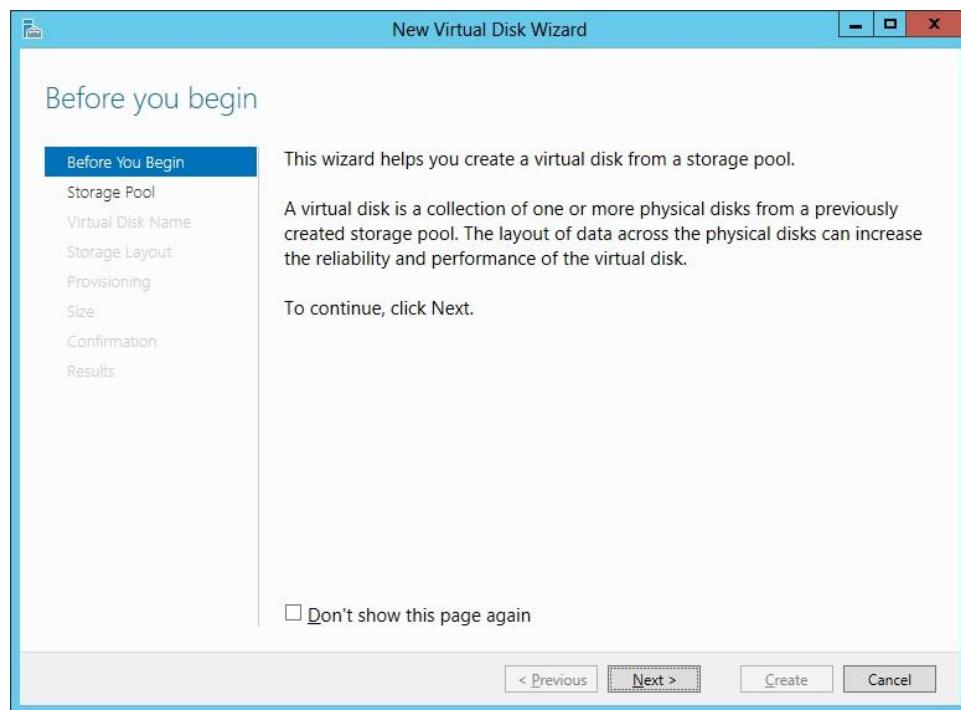
5. Click Close.



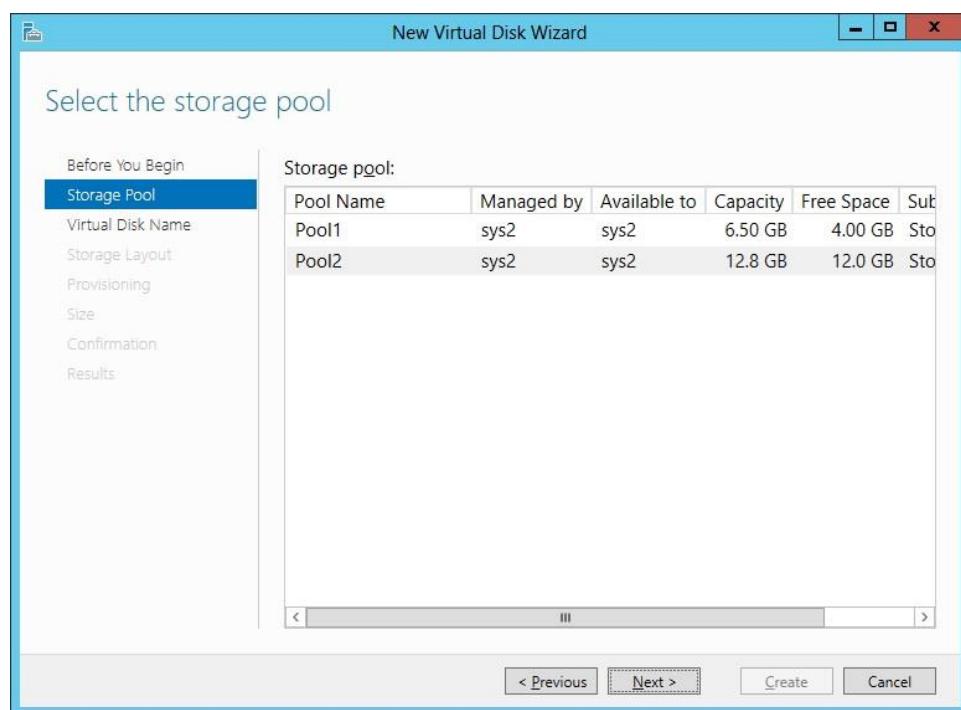
6. In Server Manager, Storage Pools, select Pool2, and click *To create a virtual disk, start the New Virtual Disk Wizard.*



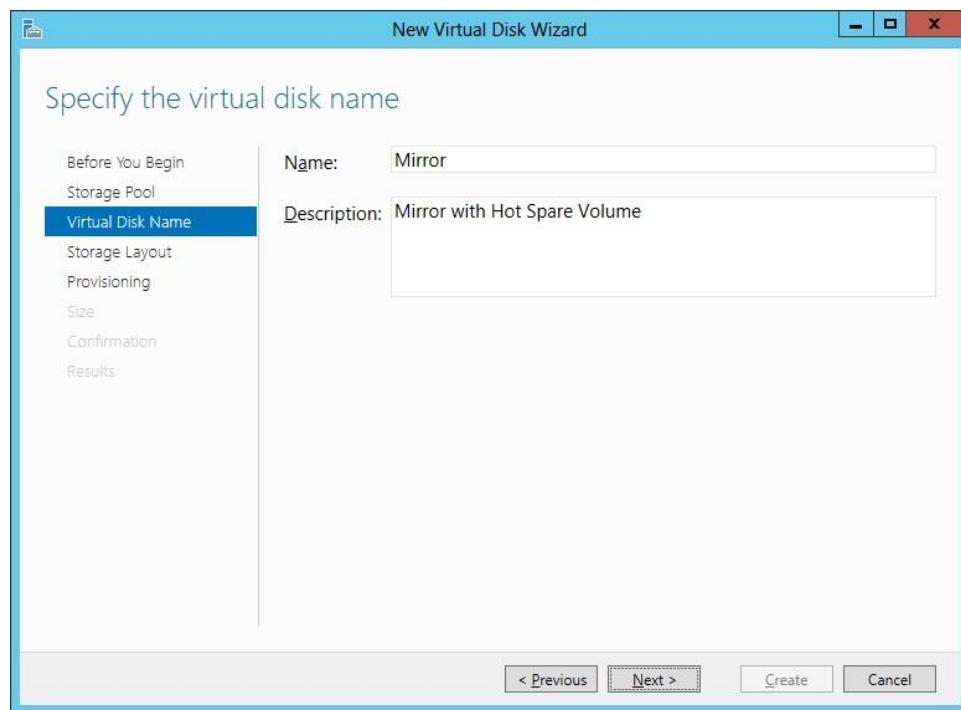
7. In Before you begin page, click **Next**.



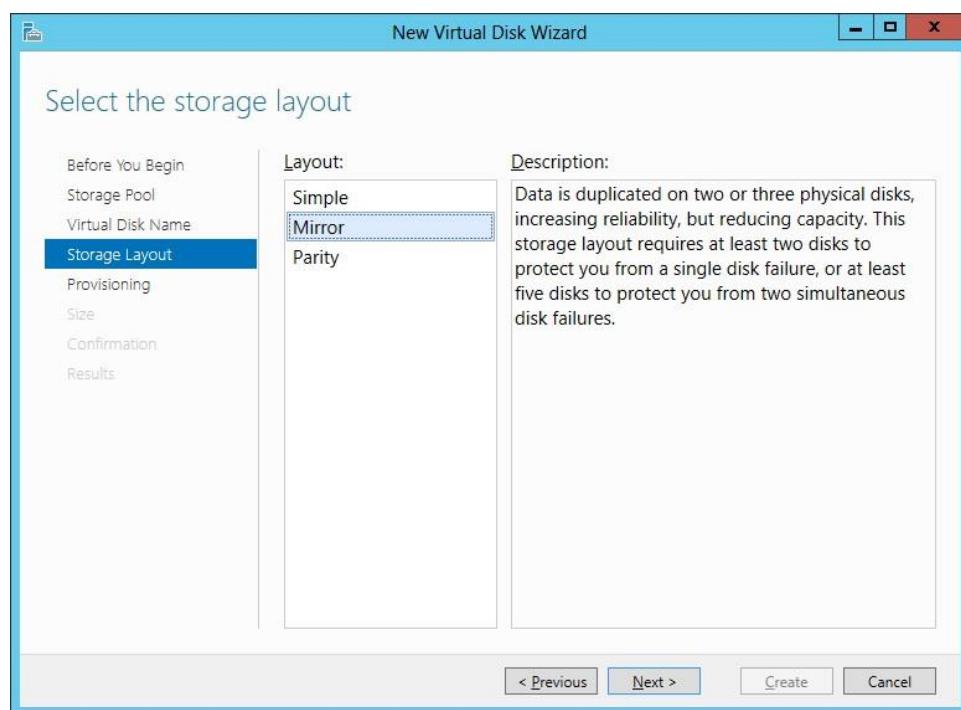
8. Select the storage pool (Ex: Pool2), click **Next**.



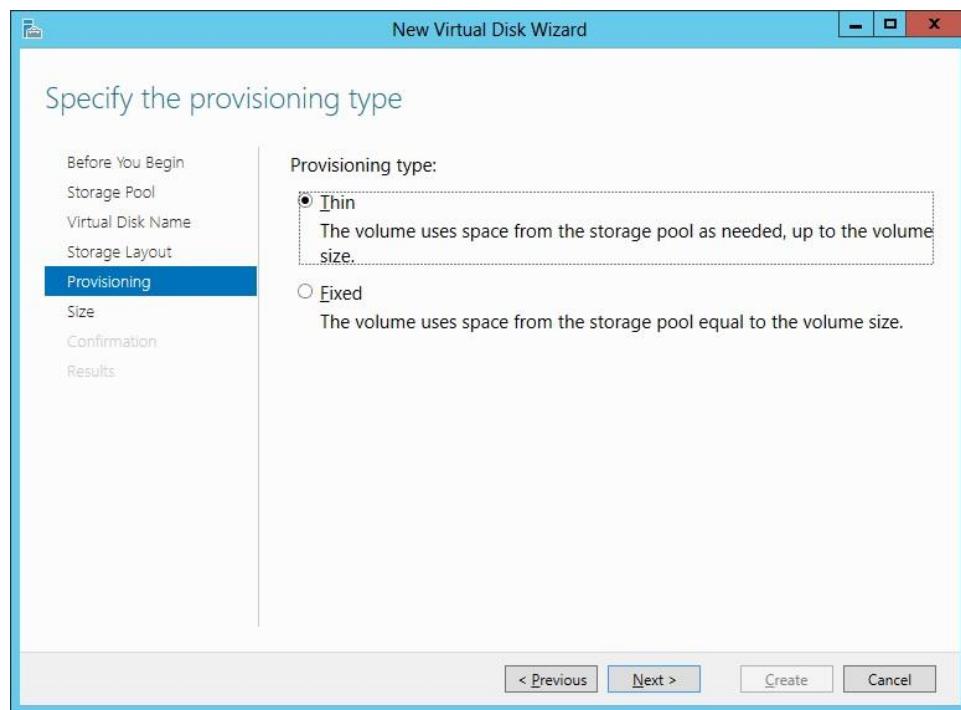
9. Enter Name (Ex: Mirror), click **Next**.



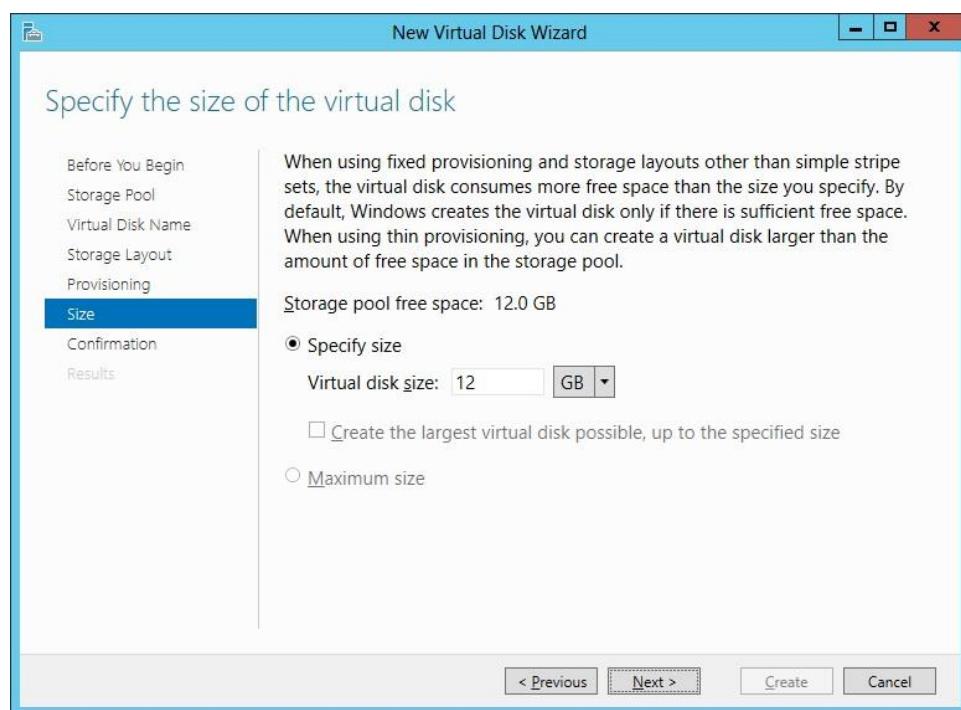
10. In Layout, select Mirror, click **Next**.

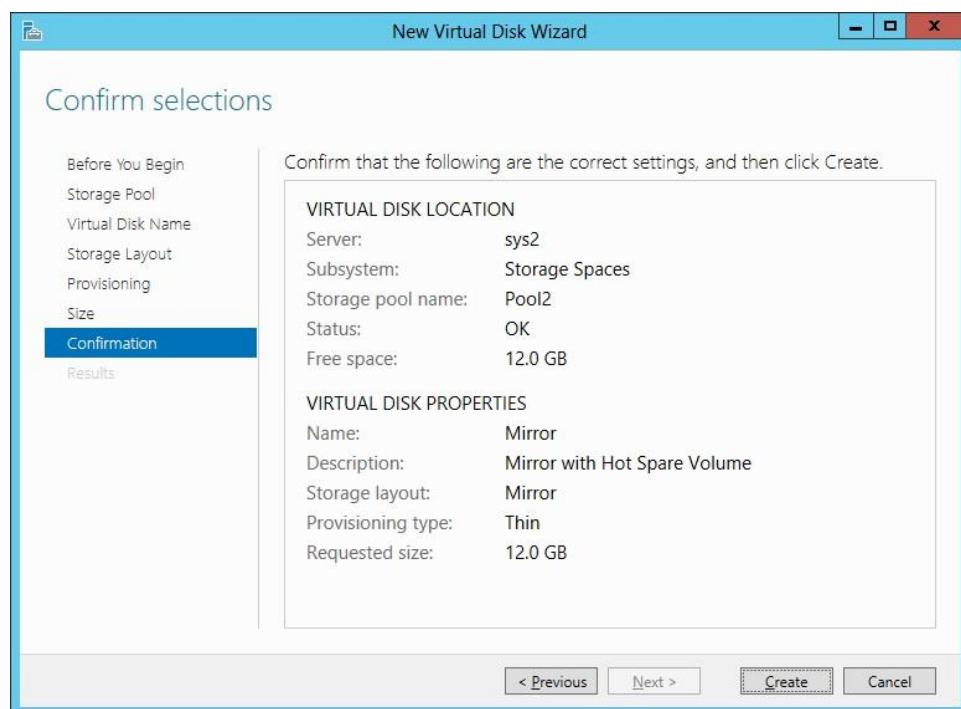
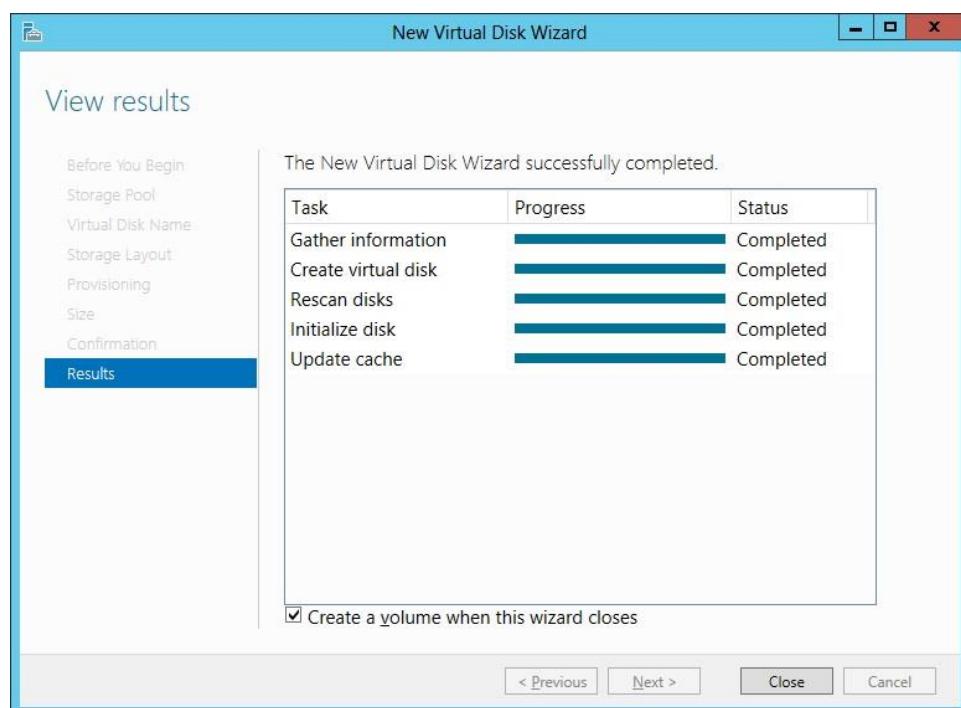


11. Select Thin or Fixed, click **Next**.

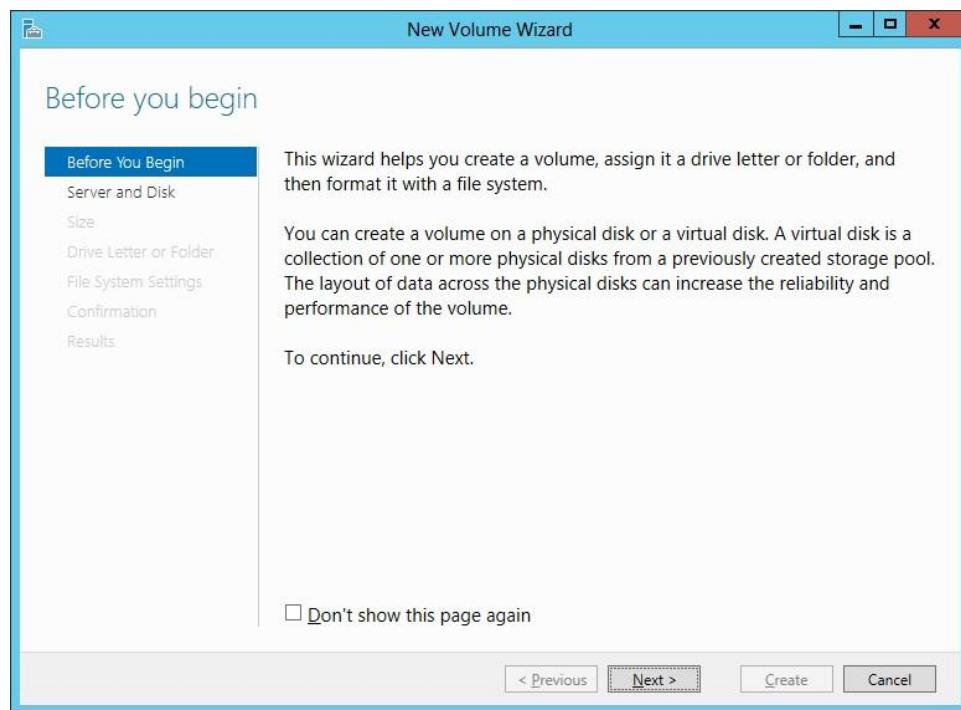


12. Enter the size of the virtual disk, click **Next**.

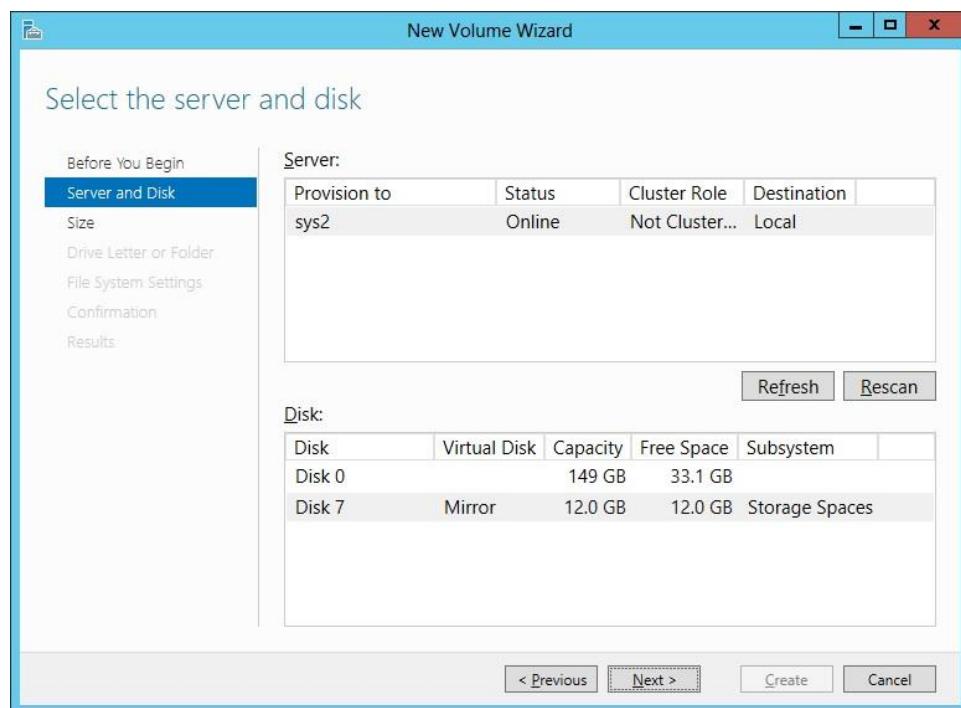


13. Click **Create**.14. Click **Close**.

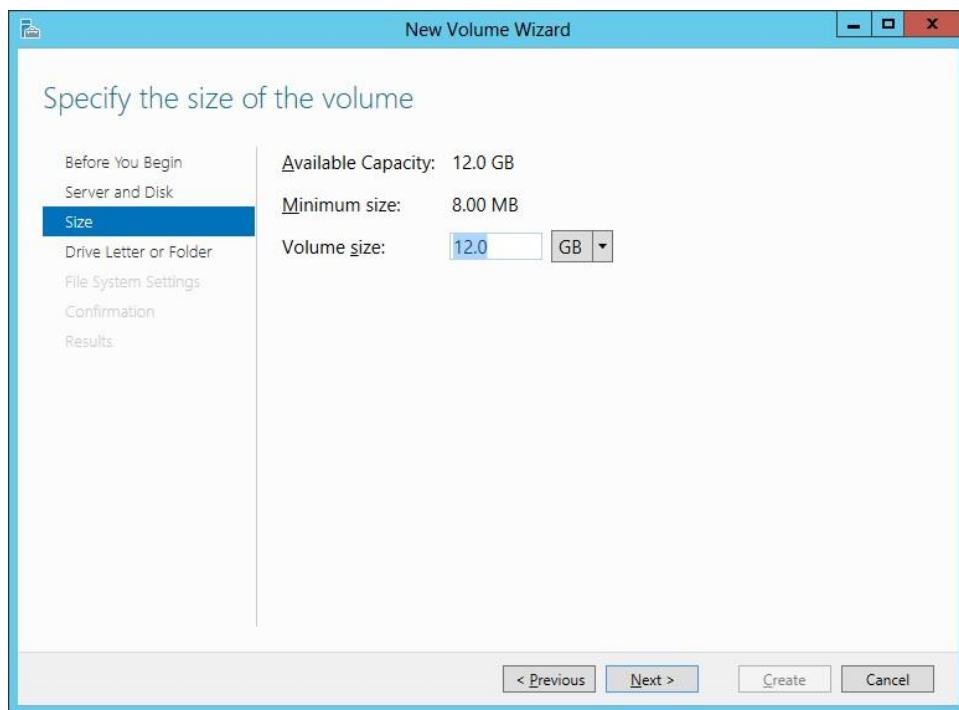
15. In Before you begin page, click **Next**.



16. Select the Disk (Ex: Mirror), click **Next**.



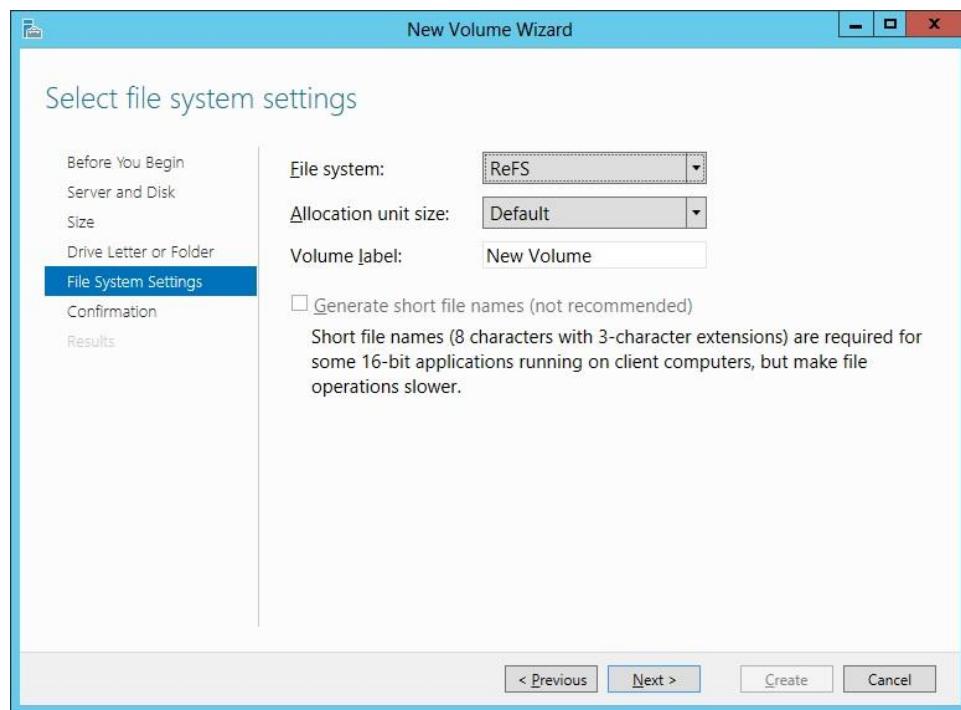
17. Enter the size of the volume, click **Next**.



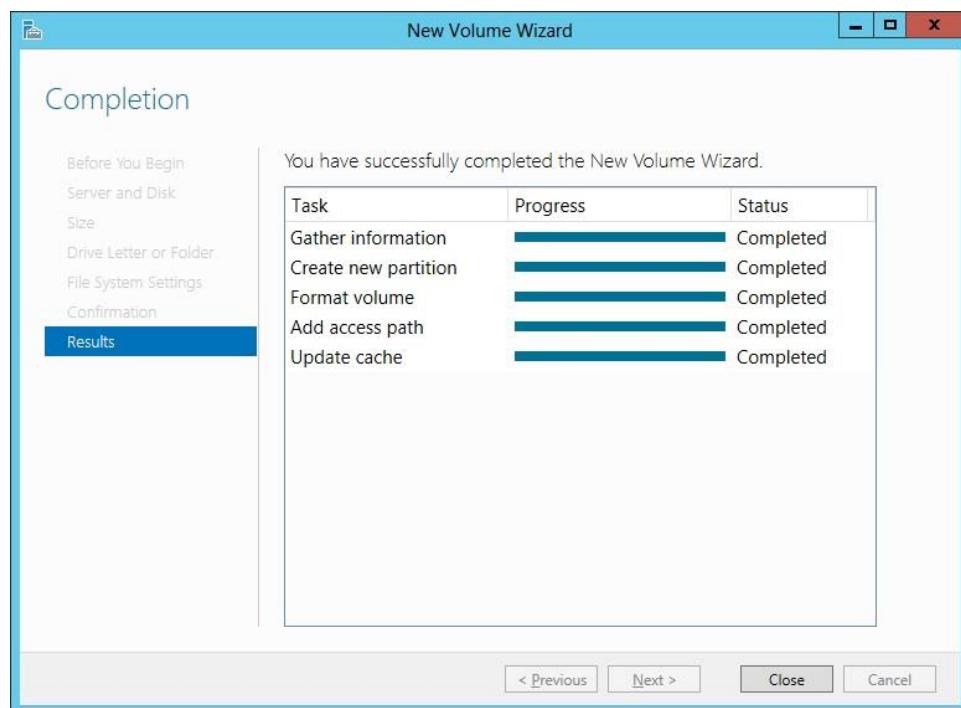
18. Select the Drive letter, click **Next**.



19. Select the File system, click **Next**.

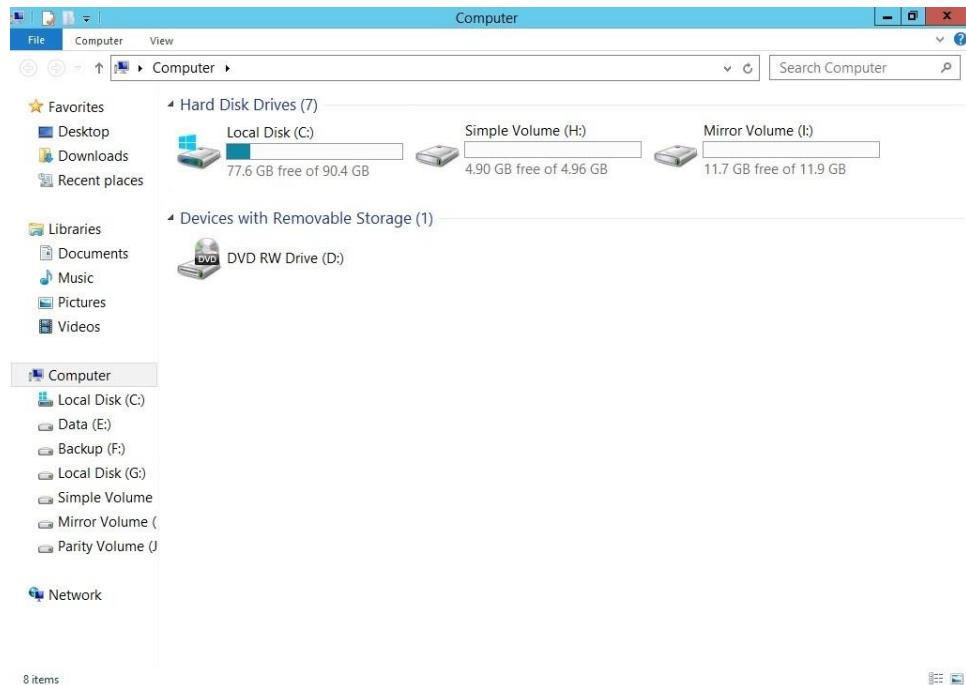


20. Click Create, click **Close**.



Verification

1. Go to Start, select Computer Icon and verify for the Mirror volume.



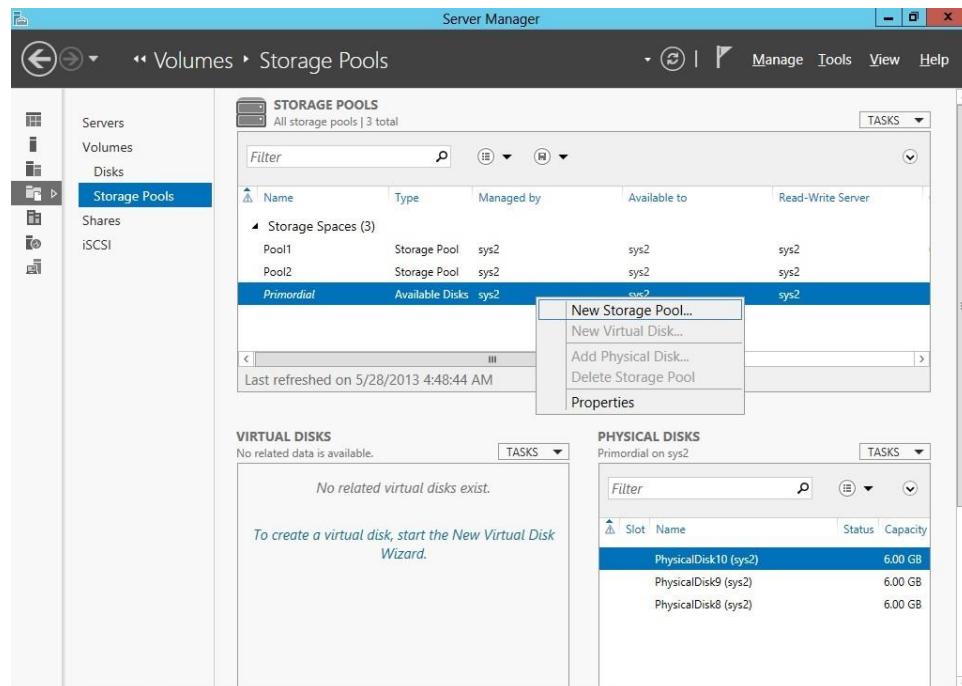
Lab – 4: Creating Mirror Volume

SYS1 – CONFIGURATION

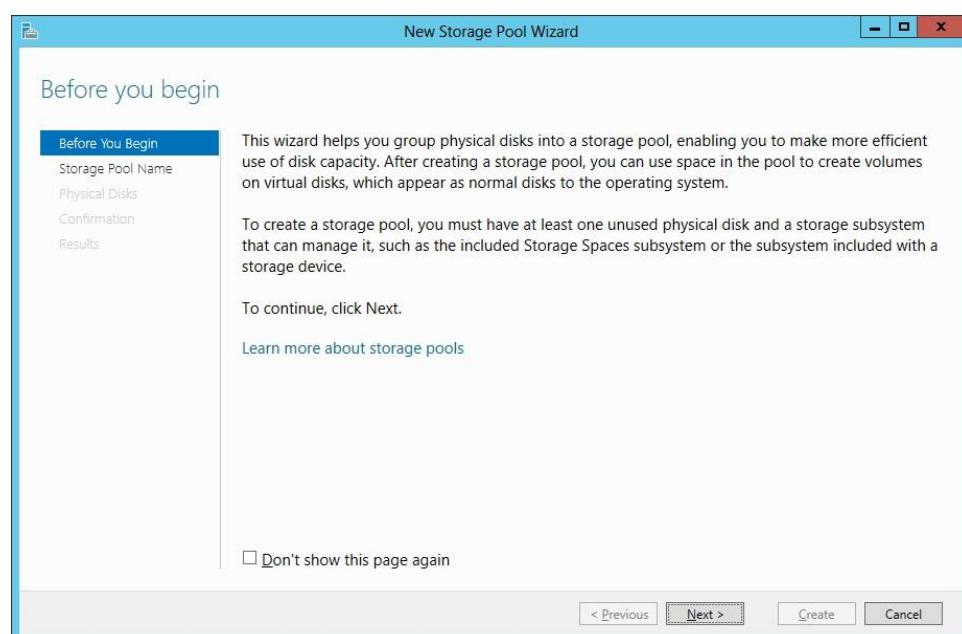
1. Create multiple iSCSI Virtual Disk (Ex: Vdisk7, Vdisk8, Vdisk9...)

SYS2 – CONFIGURATION

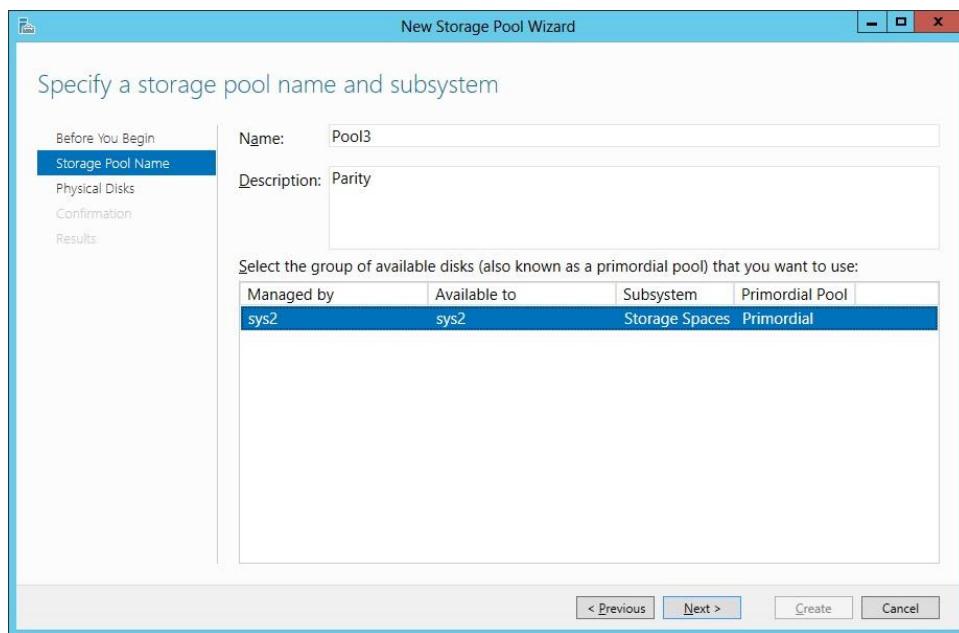
1. Go to Server Manager → File and Storage Services → Storage Pools → right click Primordial storage pool → select **New Storage Pool**



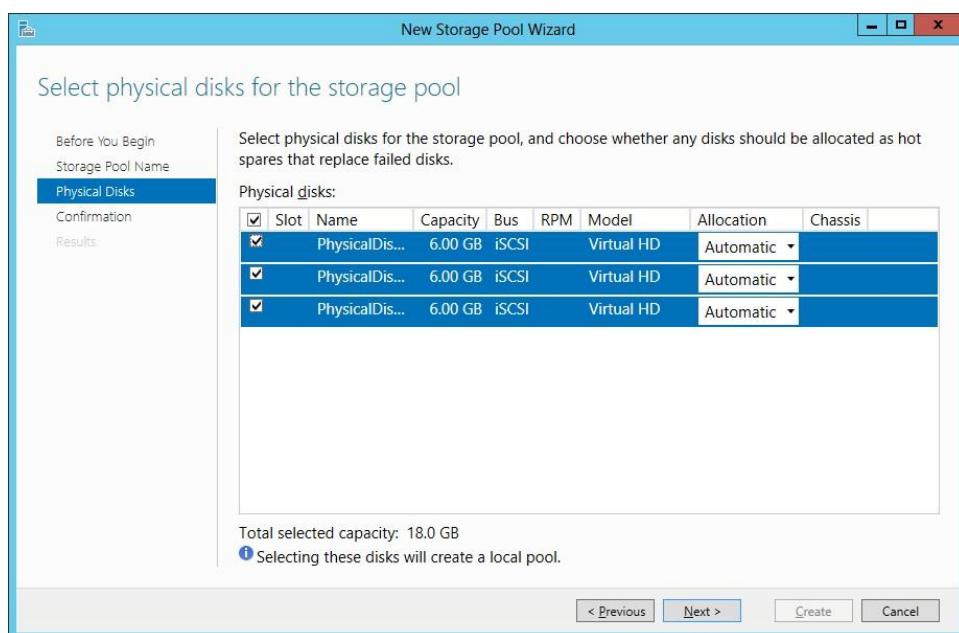
2. In Before you begin page, click **Next**.

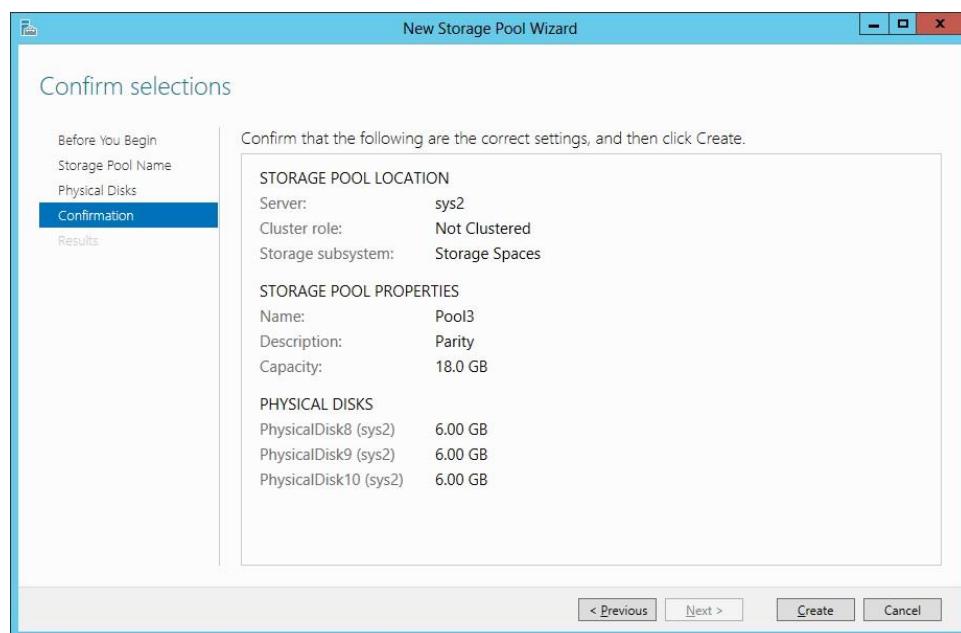
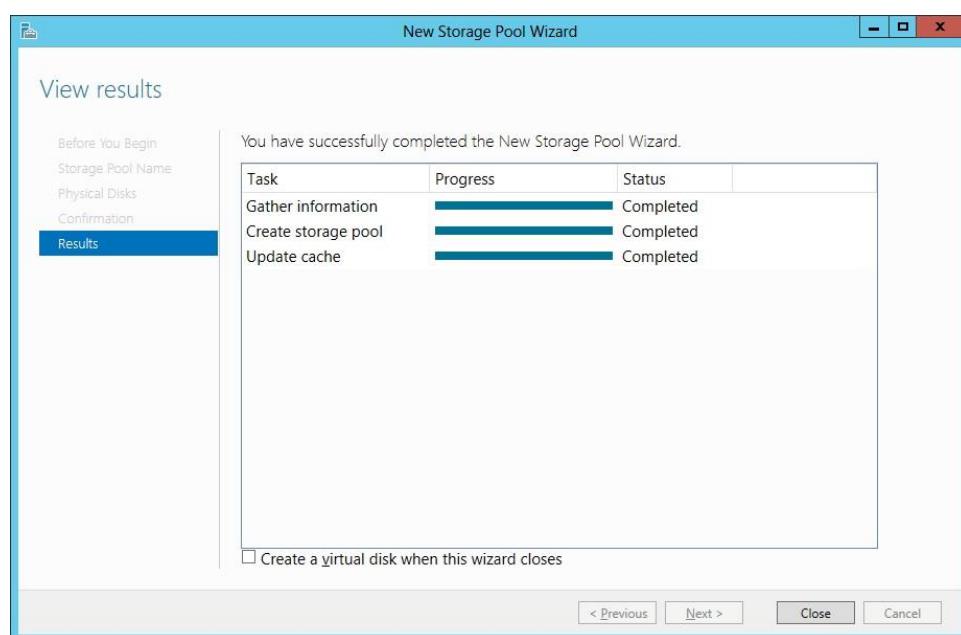


3. Enter Name (Ex: Pool3), click **Next**.

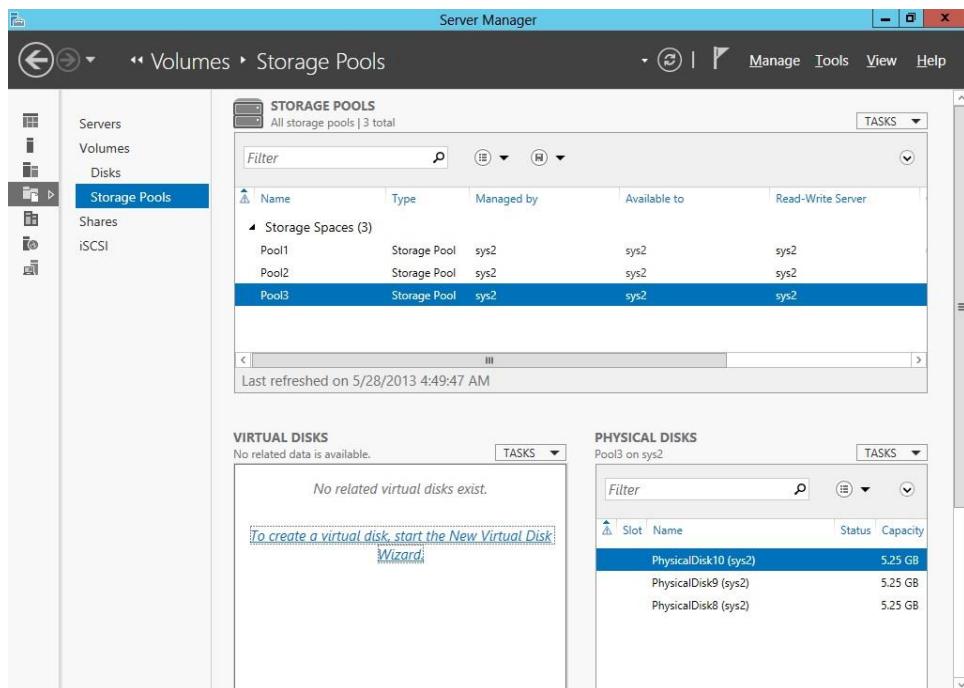


4. Check the boxes, to select the physical disks for the storage pool, click **Next**.

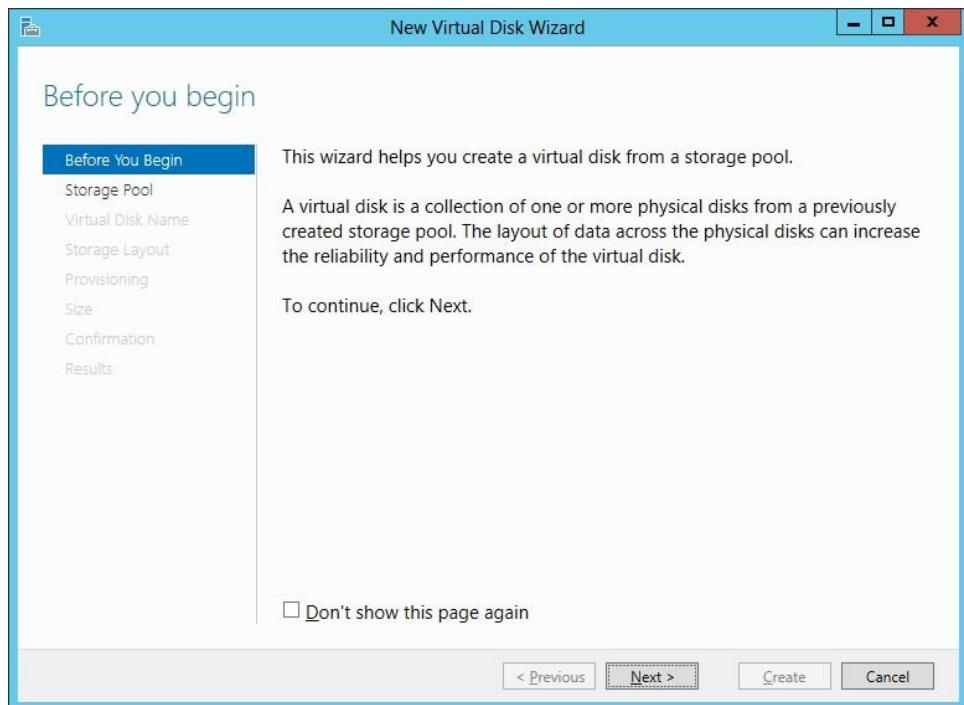


5. Click **Create**.6. Click **Close**.

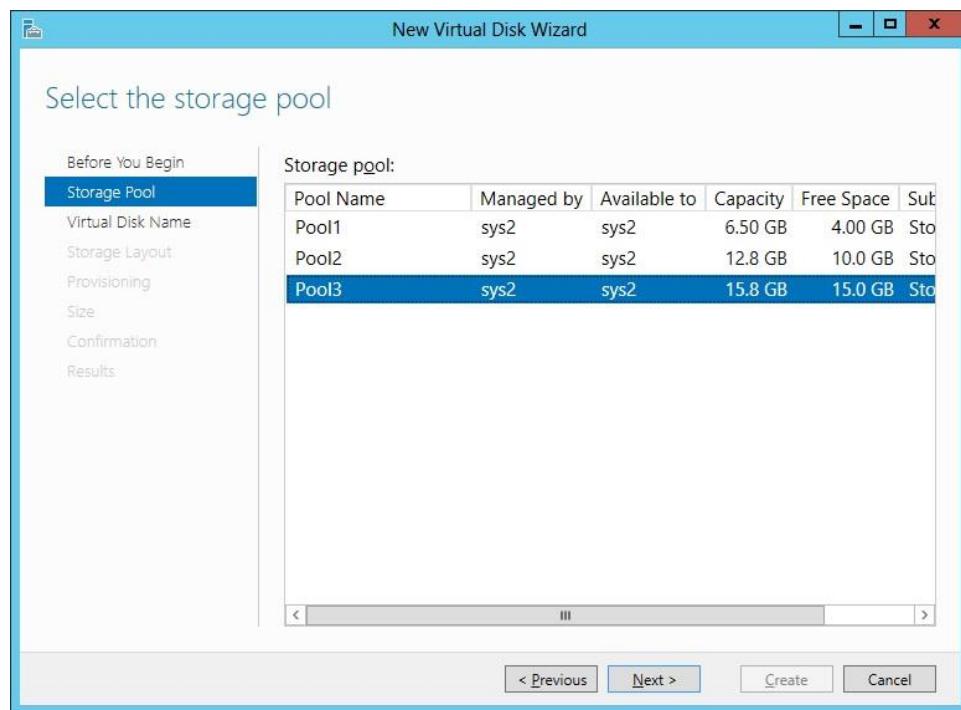
7. In Server Manager, Storage Pools, select Pool3, and click **To create a virtual disk, start the New Virtual Disk Wizard.**



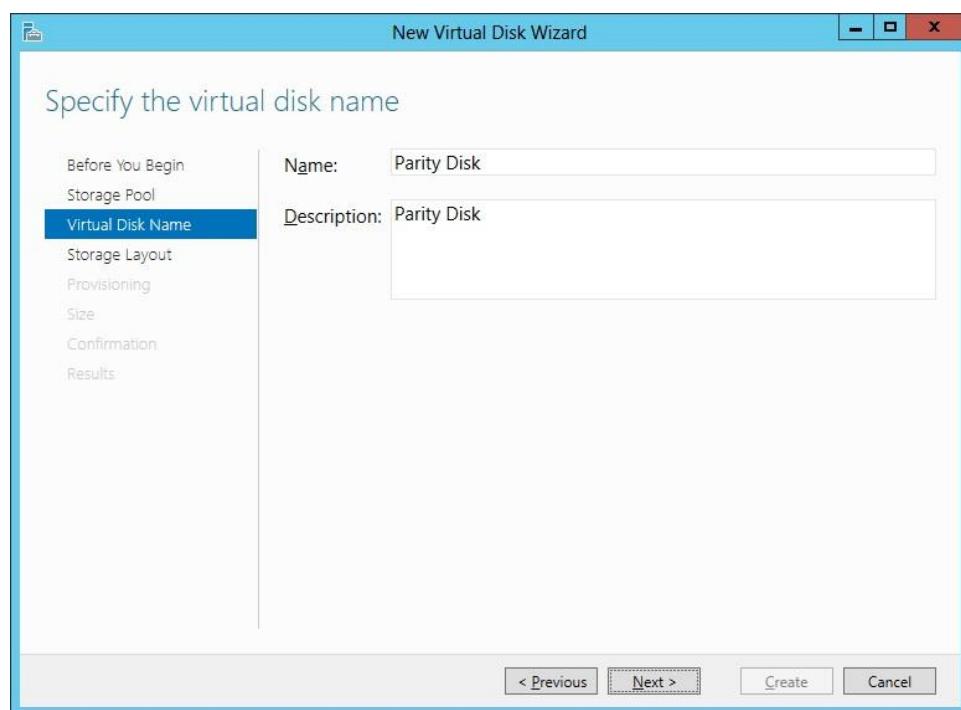
8. In Before you begin page, click **Next**.



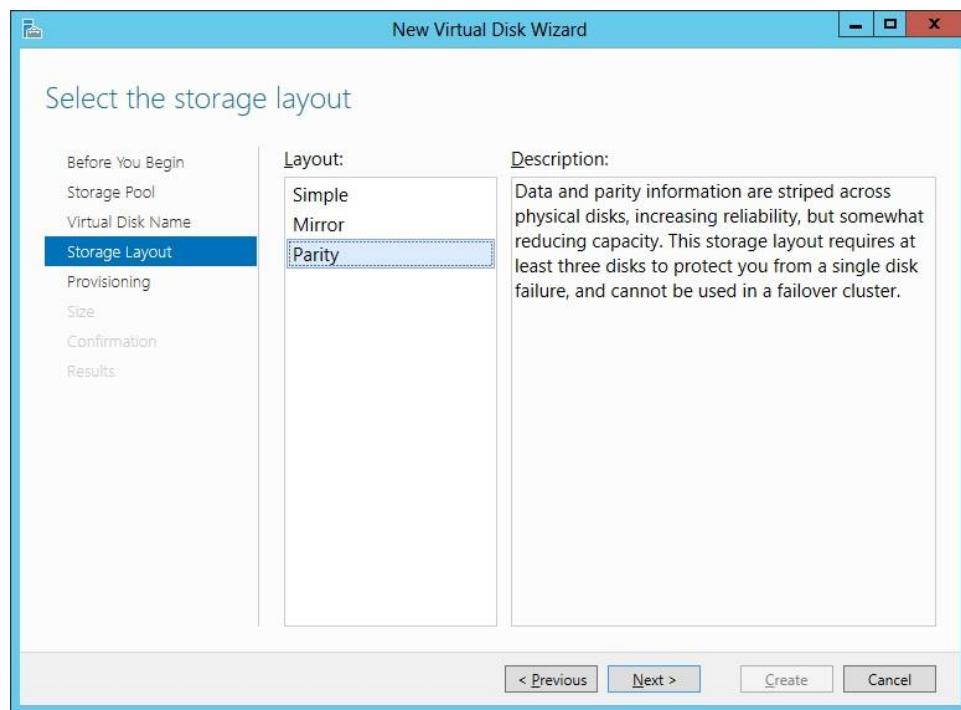
9. Select storage pool (Ex: Pool3), click **Next**.



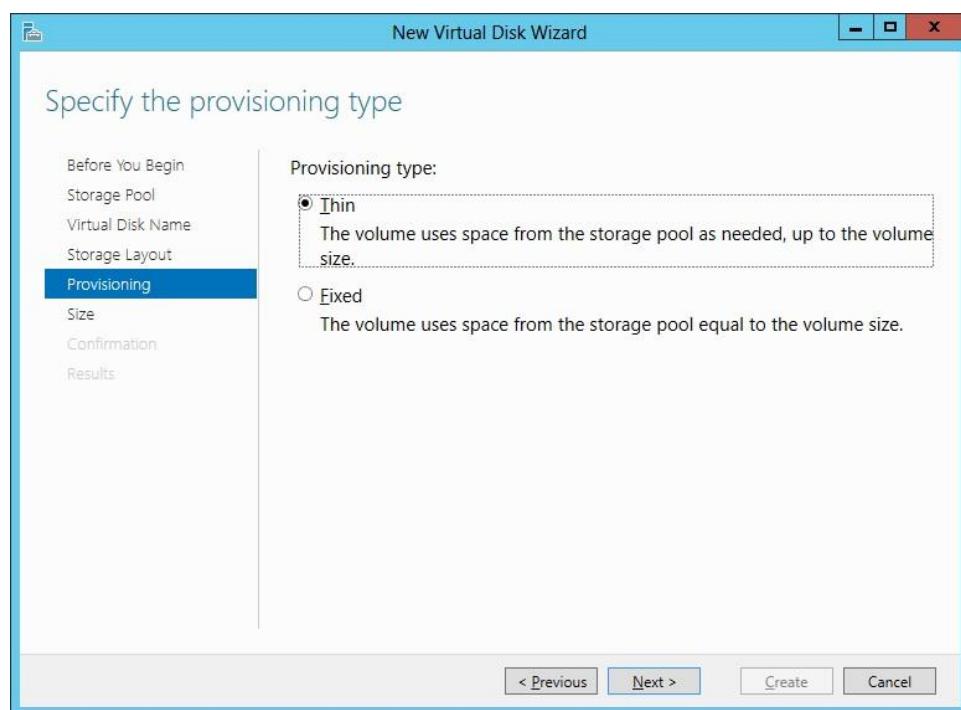
10. Enter Name (Ex: Parity Disk), click **Next**.



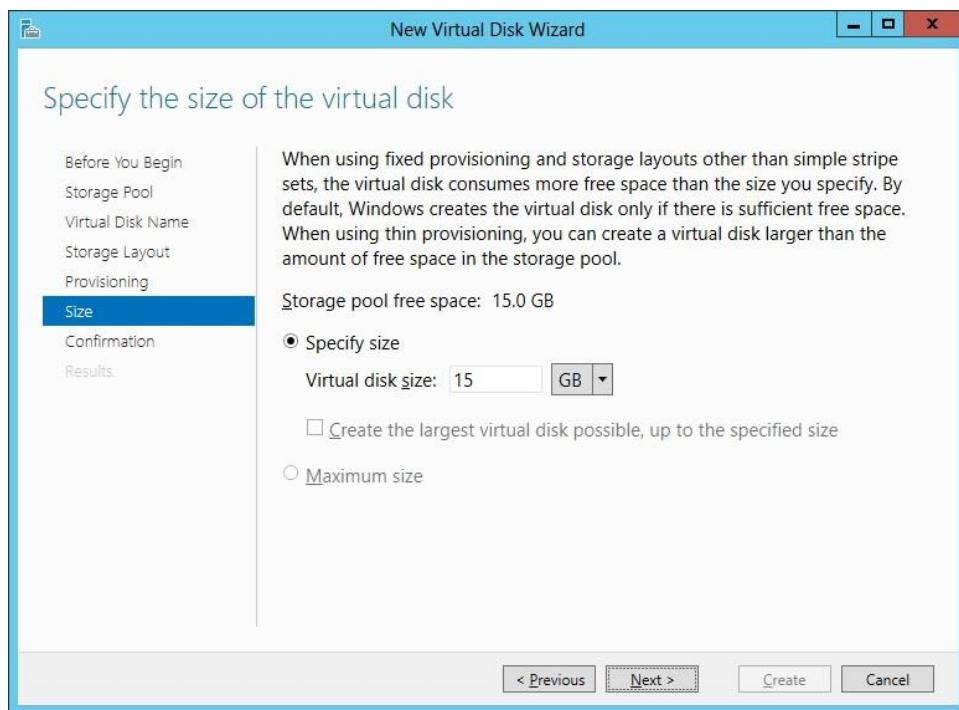
11. In Layout, select Parity, click **Next**.



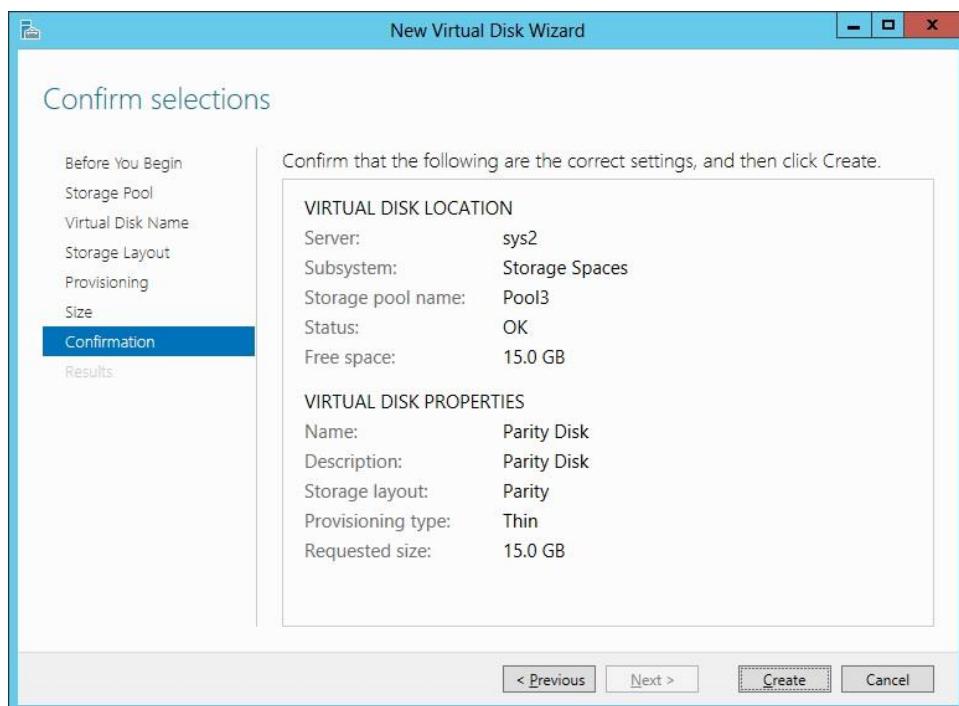
12. Select Thin or Fixed, click **Next**.



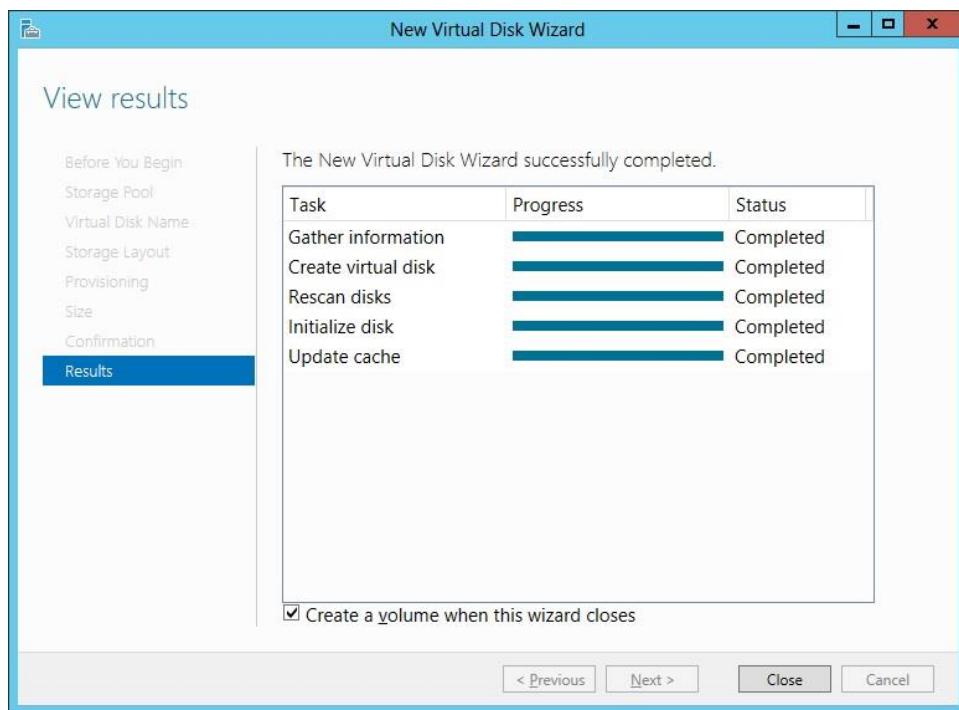
13. Enter the size of the virtual disk, click **Next**.



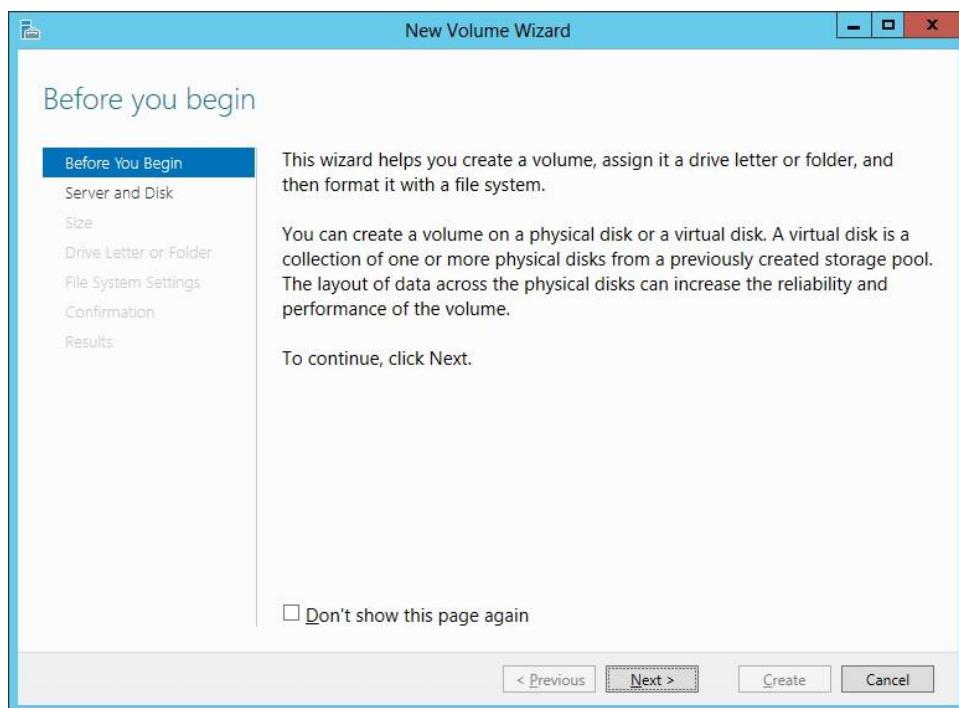
14. Click **Create**.



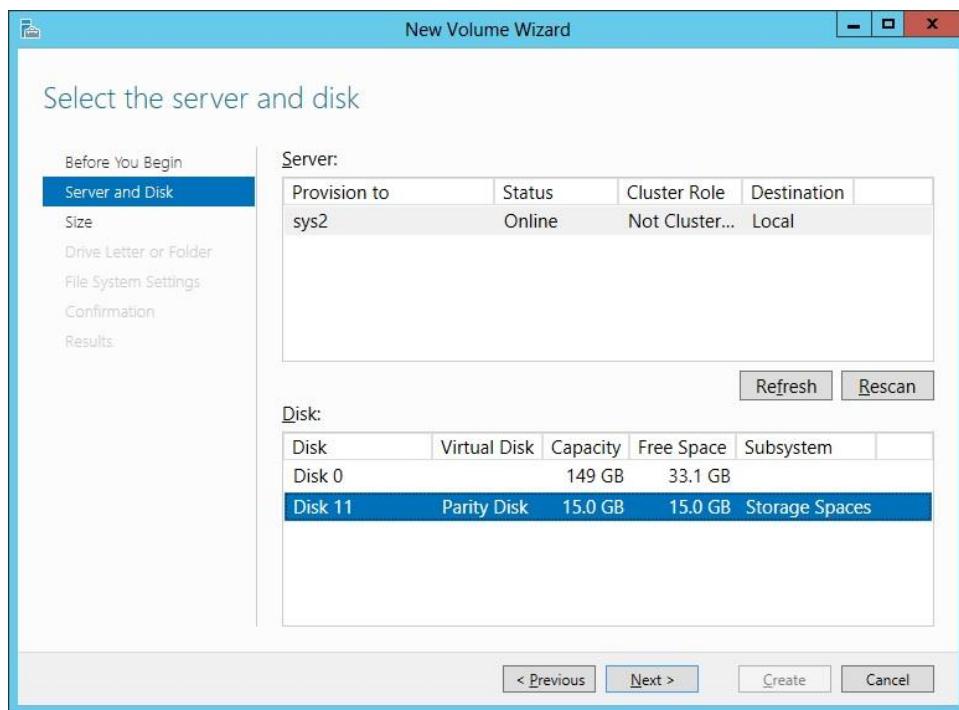
15. Click **Close**, verify for the check box Create a volume when this wizard closes.



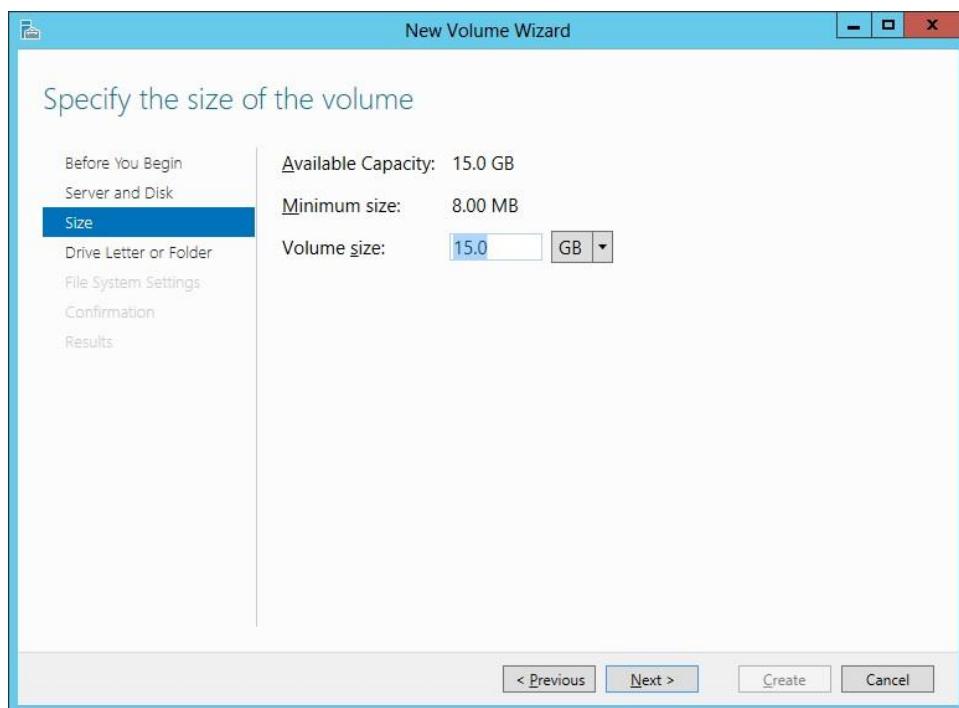
16. In Before you begin page, click **Next**.



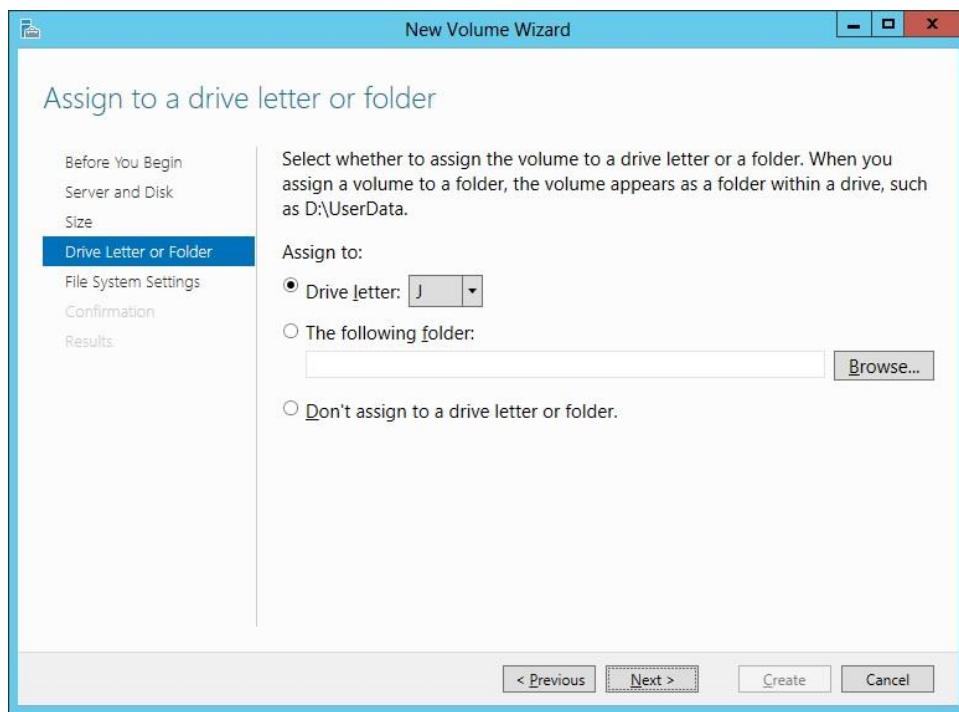
17. Select the Disk (Ex: Parity Disk), click **Next**.



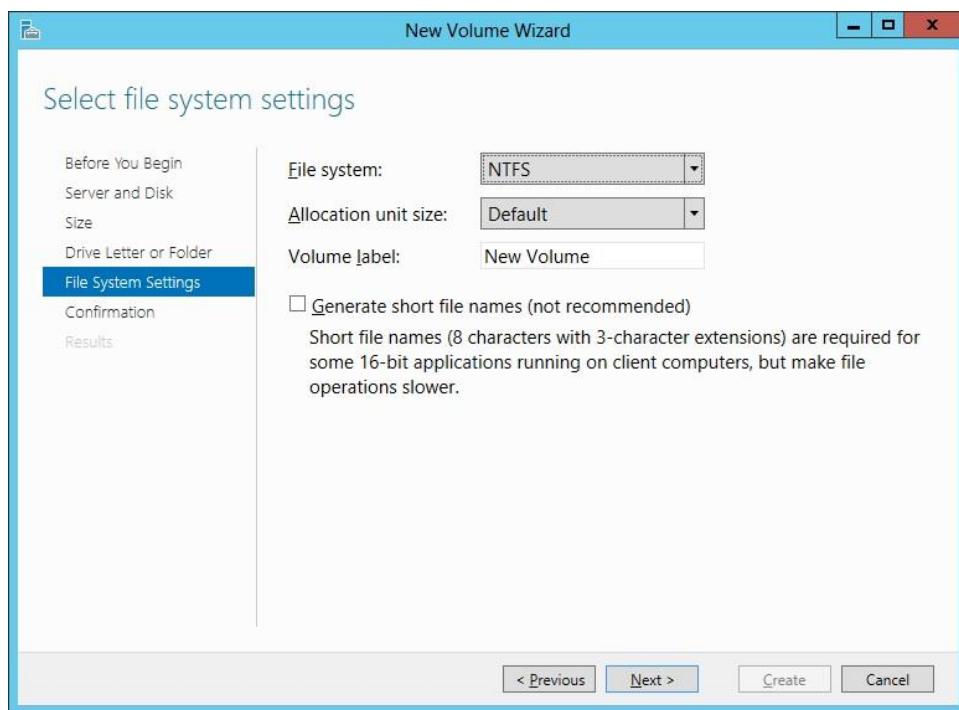
18. Enter the size of the volume, click **Next**.



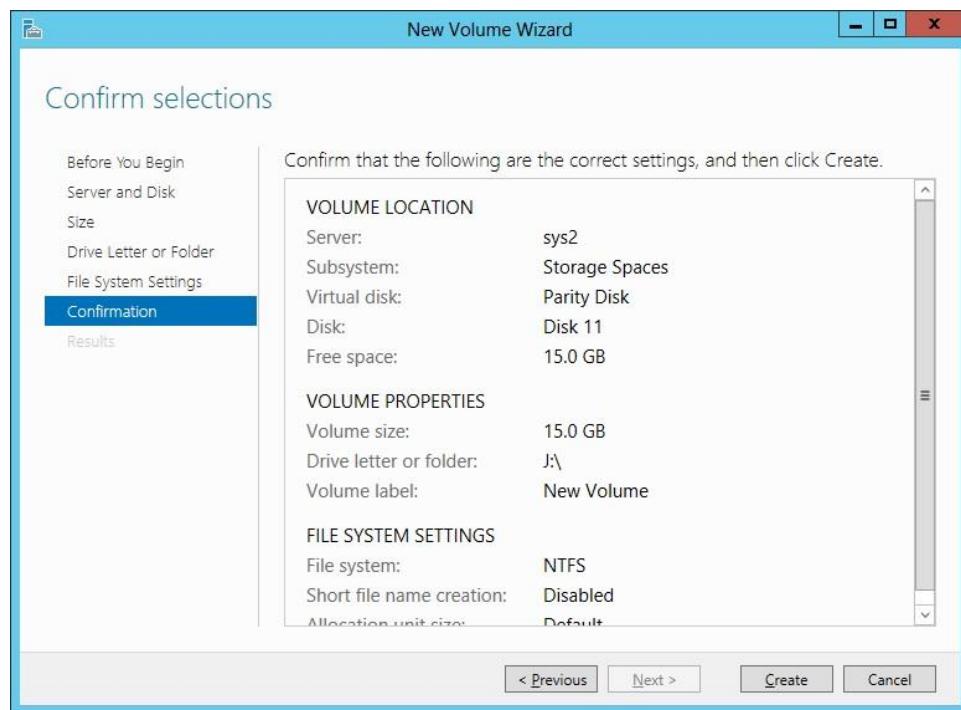
19. Select the Drive letter, click **Next**.



20. Select the file system, click **Next**.



21. Click Create.



22. Verify for the Volumes (Simple, Mirror, Parity).

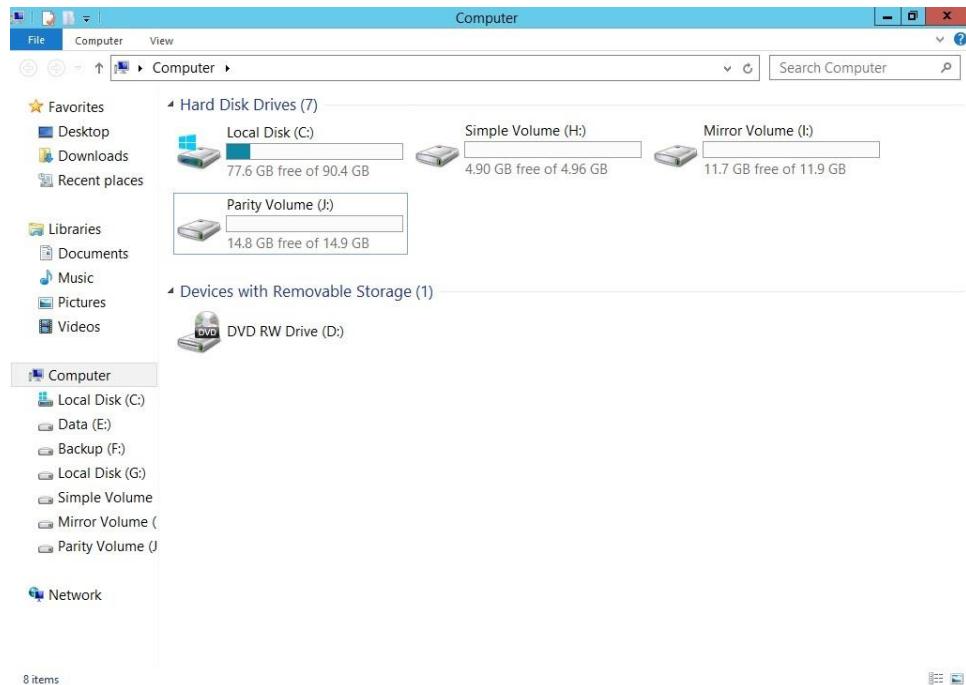
DISKS	Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only	Clustered	Subsystem	Bus Type
sys2 (4)	0	Simple Disk	Online	149 GB	33.1 GB	MBR			ATA	S
	4	Simple Disk	Online	5.00 GB	0.00 B	GPT			Storage Sp...	Storage S...
	7	Mirror	Online	12.0 GB	0.00 B	GPT			Storage Sp...	Storage S...
	11	Parity Disk	Online	15.0 GB	0.00 B	GPT			Storage Sp...	Storage S...

VOLUMES	Volume	Status	Provisioning	Capacity	Free Space
sys2 (1)	J:	Thin		15.0 GB	14.9 GB

STORAGE POOL	Microsoft Storage Space Device on sys2	
Pool3	Capacity:	15.8 GB
27% Used	4.25 GB Used Space	11.5 GB Free Space
Subsystem:	Storage Spaces	
Servers:	sys2	
Volumes:	J:	

Verification

1. Go to Start, select Computer Icon and verify for the Parity volume.



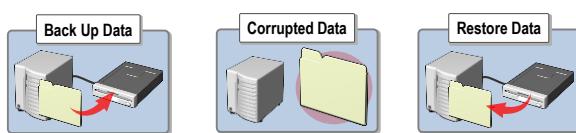
Backup and Recovery

What is Backup?

- Copy data to alternate media
- Prevent data loss
- Only Administrators can backup the data



Backup

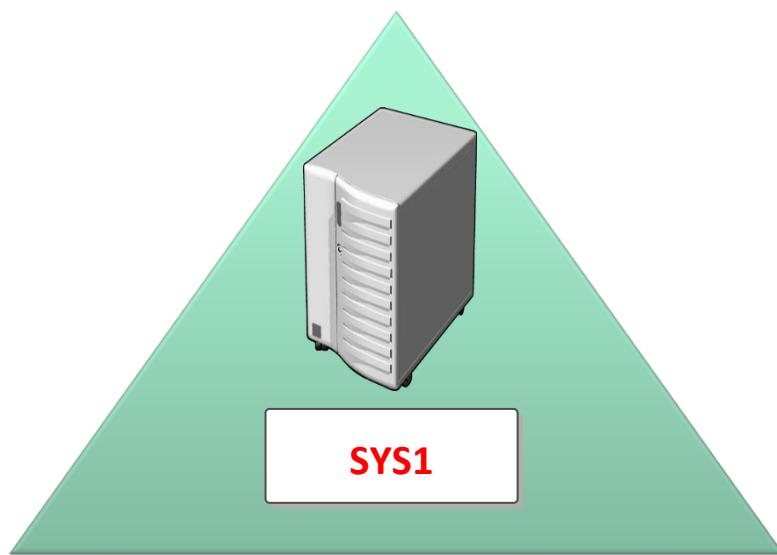


WINDOWS SERVER BACKUP & RECOVERY

Prerequisites:

Before working on this lab, you must have

1. A Computer with Windows Server 2012 Domain Controller



MICROSOFT.COM

SYS1

Domain Controller

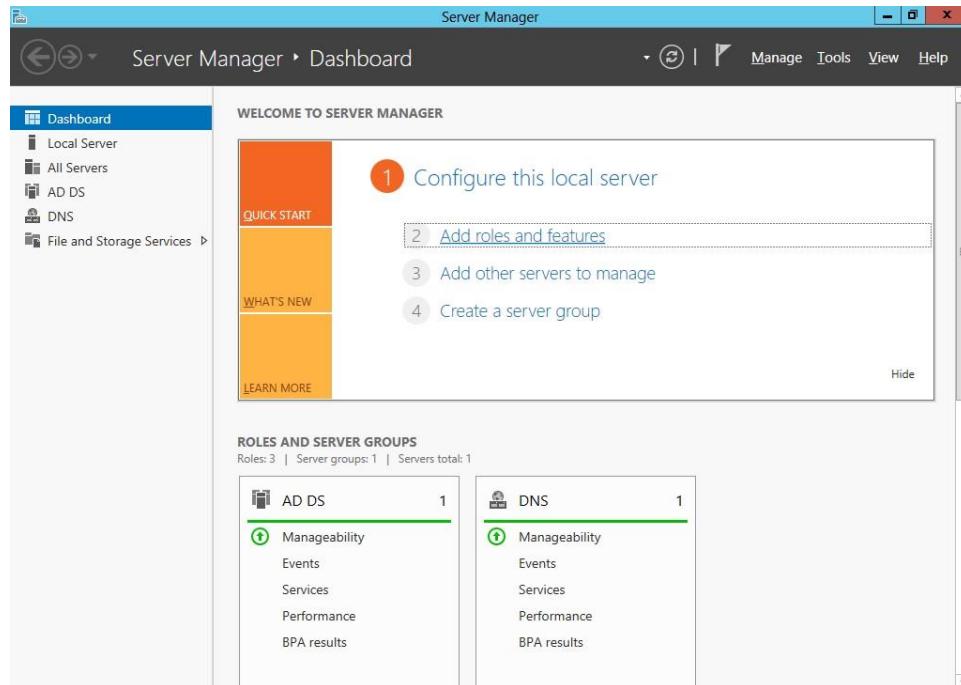
IP Address 10.0.0.1

Subnet Mask 255.0.0.0

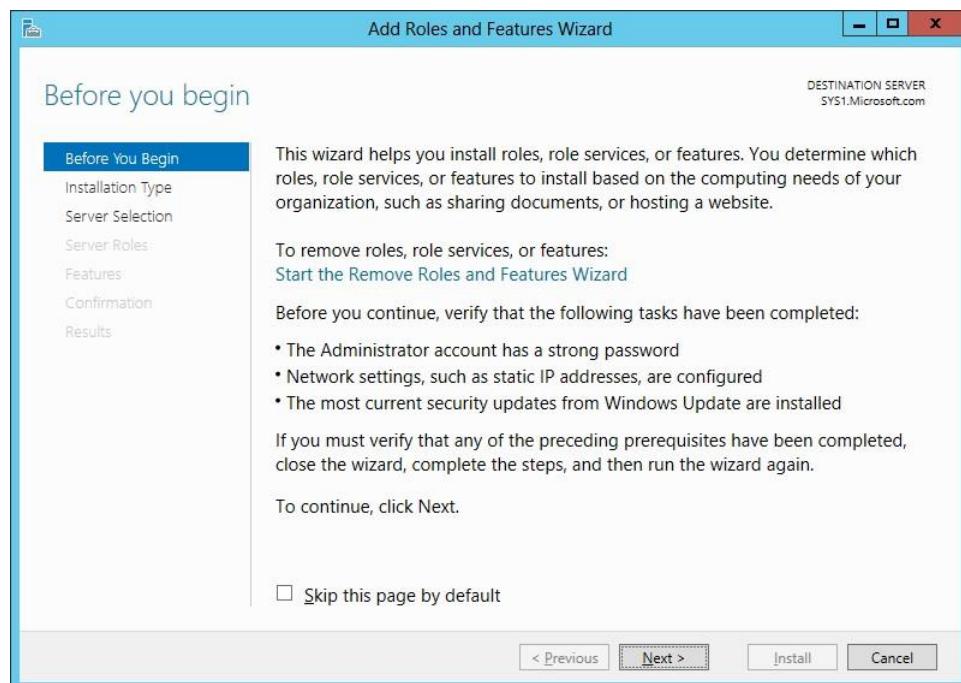
Preferred DNS 10.0.0.1

Lab – 1: Configuring Windows Server Backup and Recovery

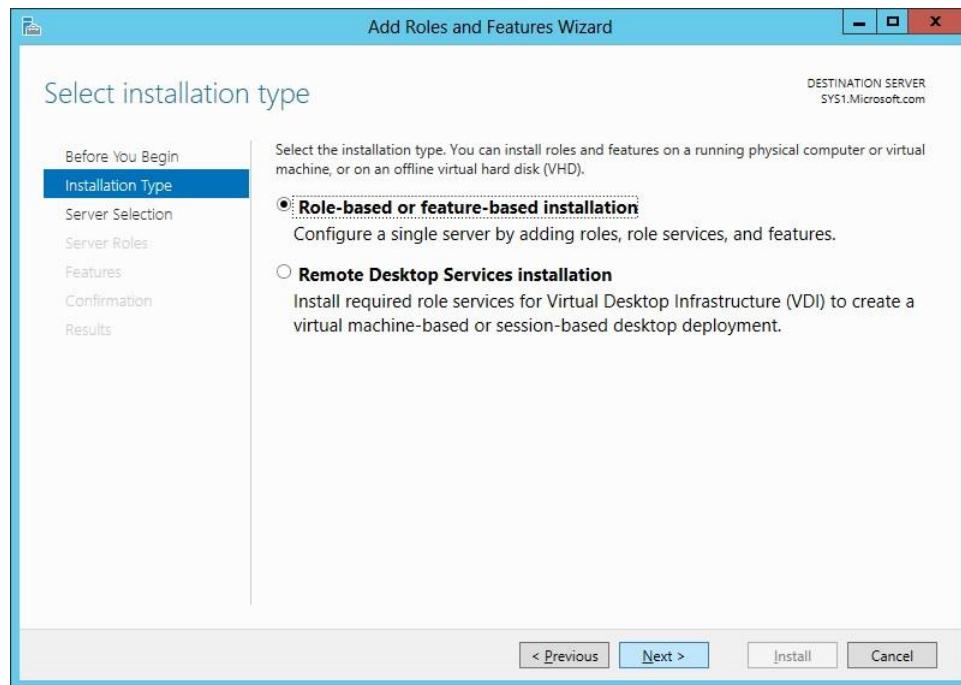
1. Login as **Administrator**, go to ServerManager Dashboard and click **Add roles and features**.



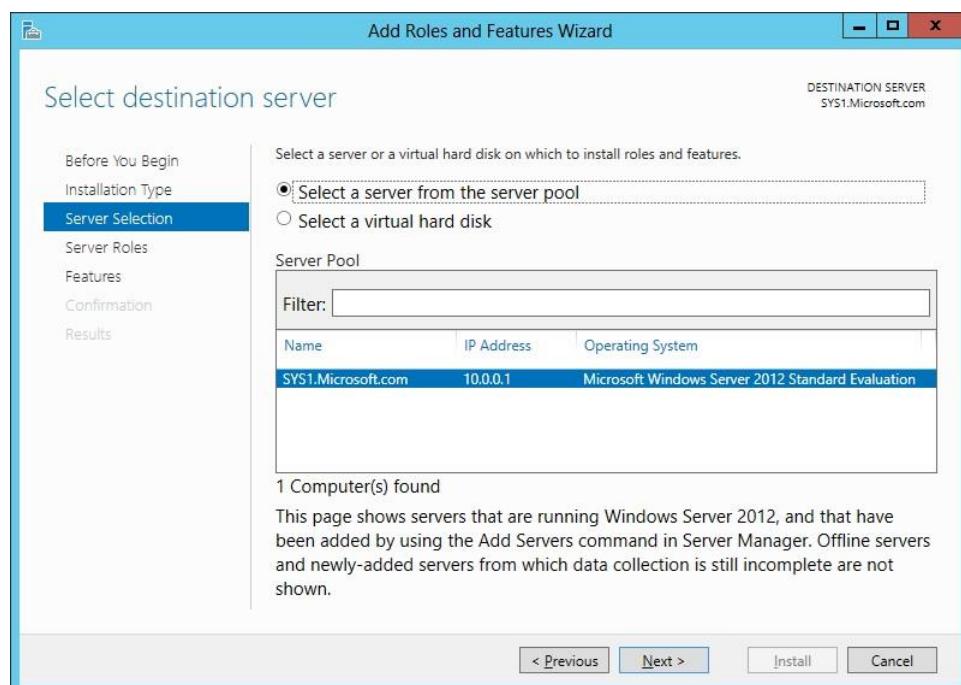
2. In Before you begin page, click **Next**.



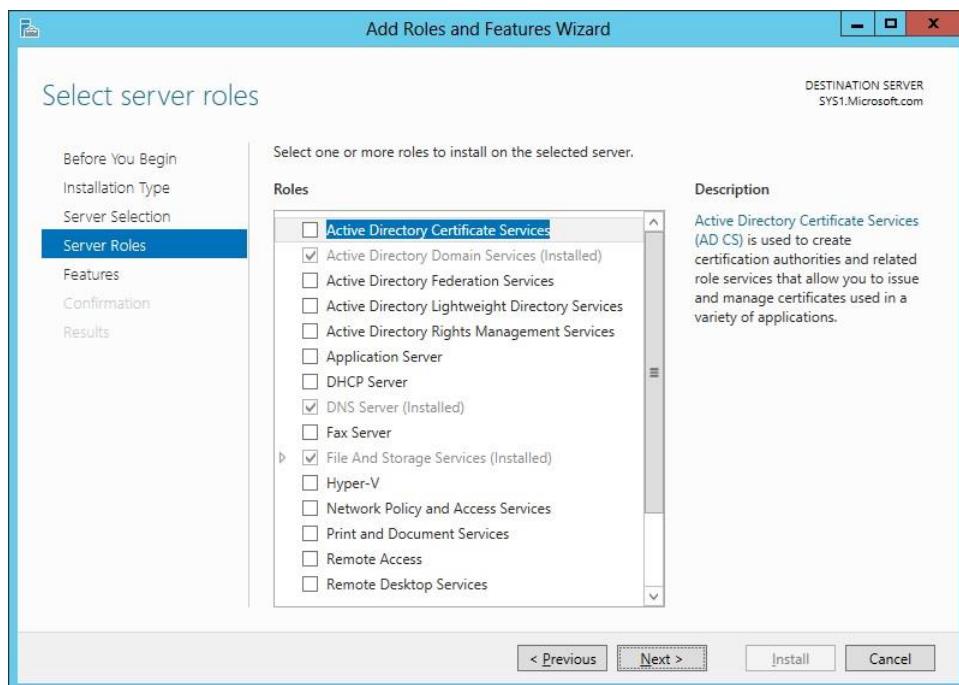
3. Select **Role-based or feature-based installation**, click **Next**.



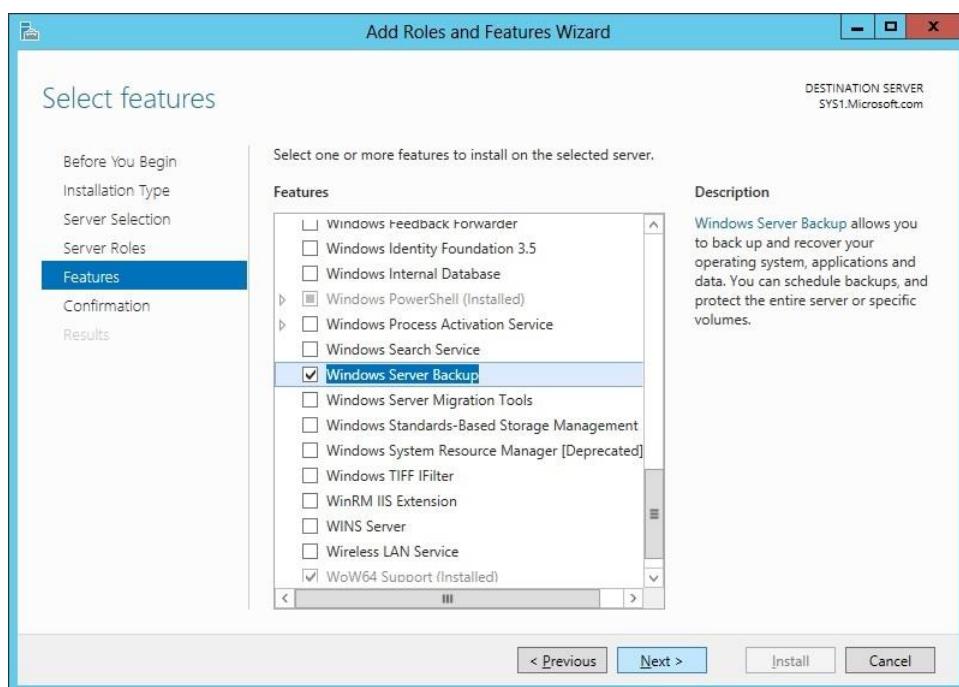
4. In Select destination server page, select a server (**SYS1.Microsoft.com**) from the server pool and click **Next**.



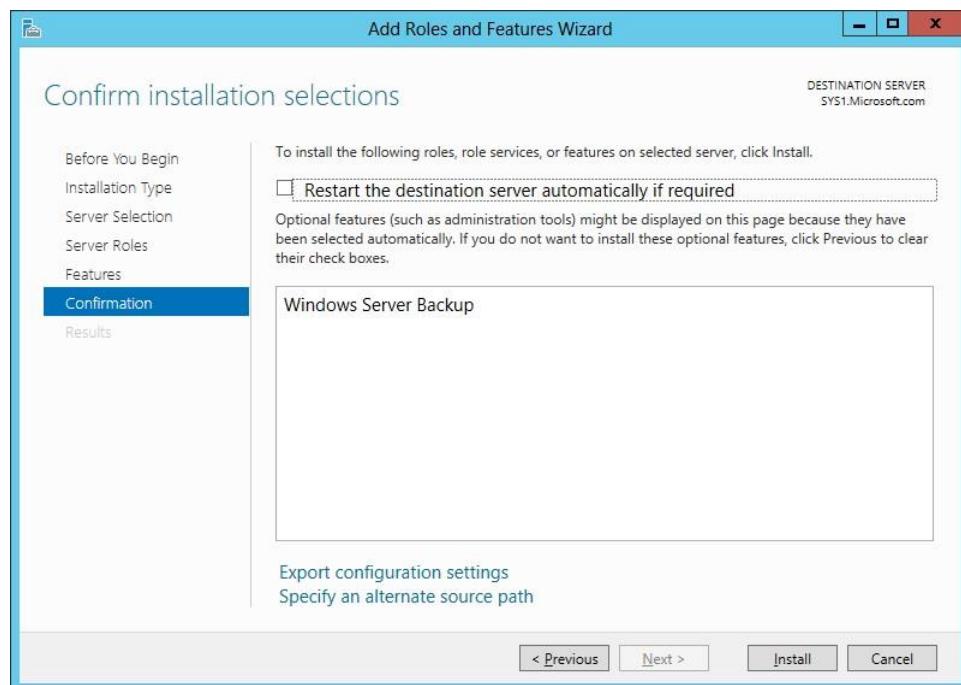
5. In Select server roles page, click **Next**.



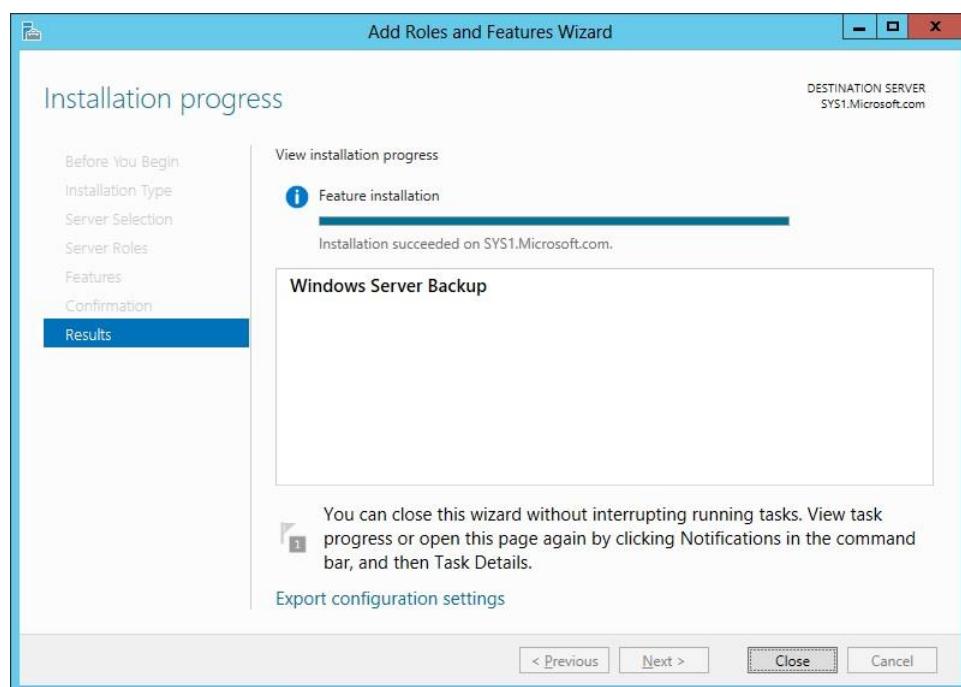
6. In Select features page, check the box **Windows Server Backup** and click **Next**.



7. Check box **Restart the destination server automatically if required**, click **Install**.

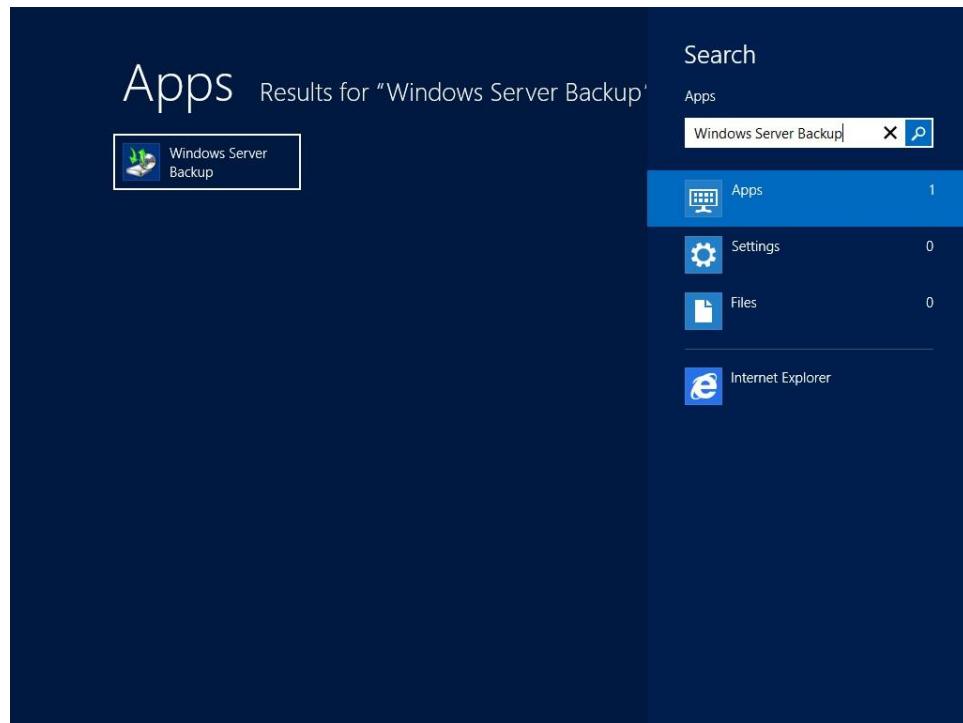


8. Click **Close** to complete the feature installation.

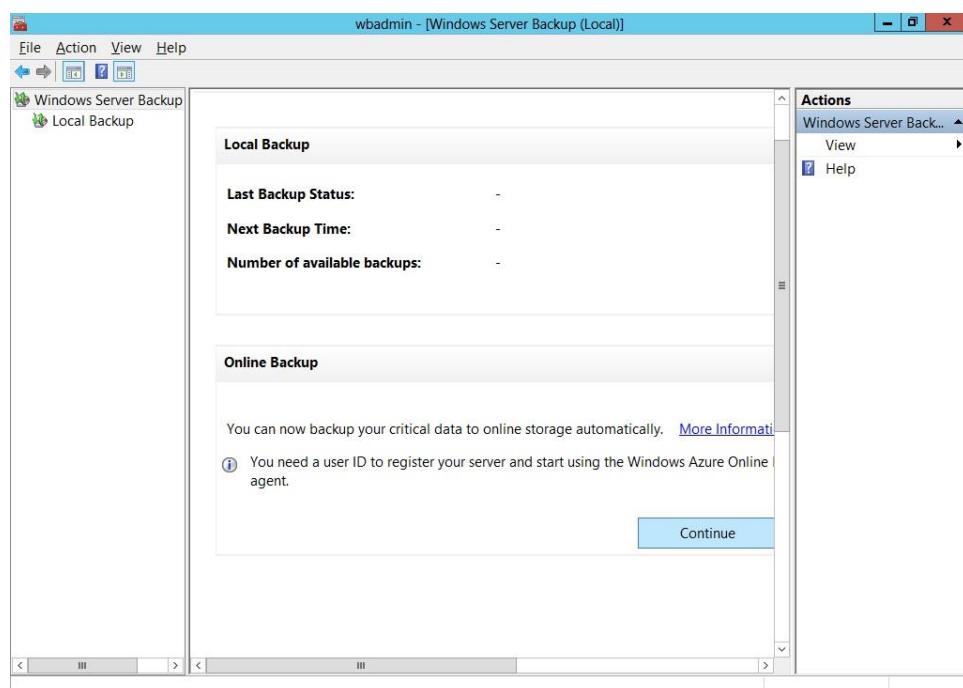


How to Backup Data using Windows Server Backup

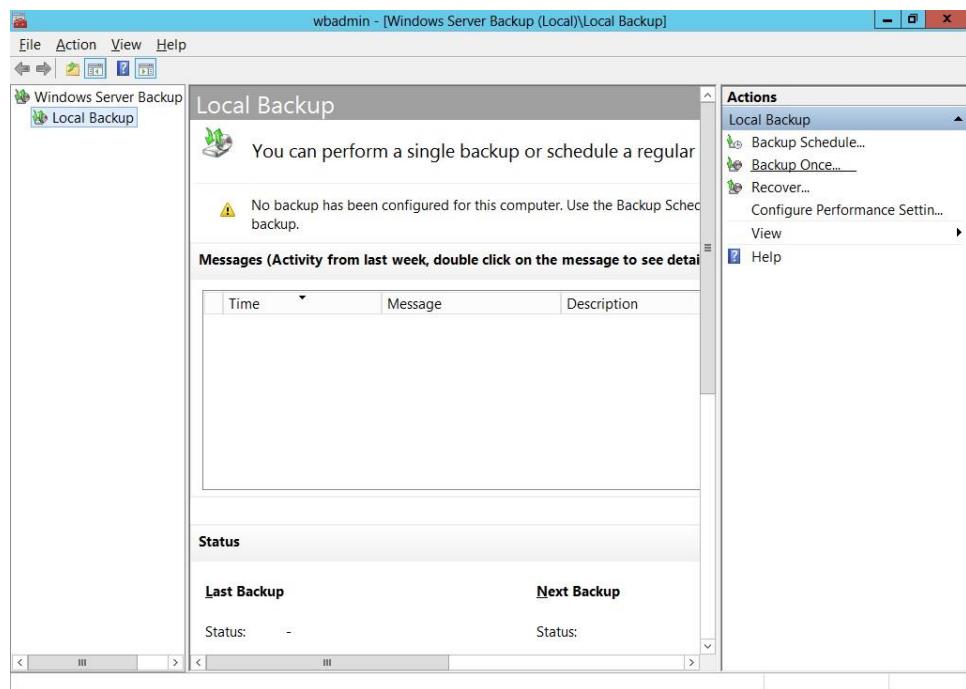
1. Go to Start, type Windows Server Backup in Search Apps, select **Windows Server Backup**.



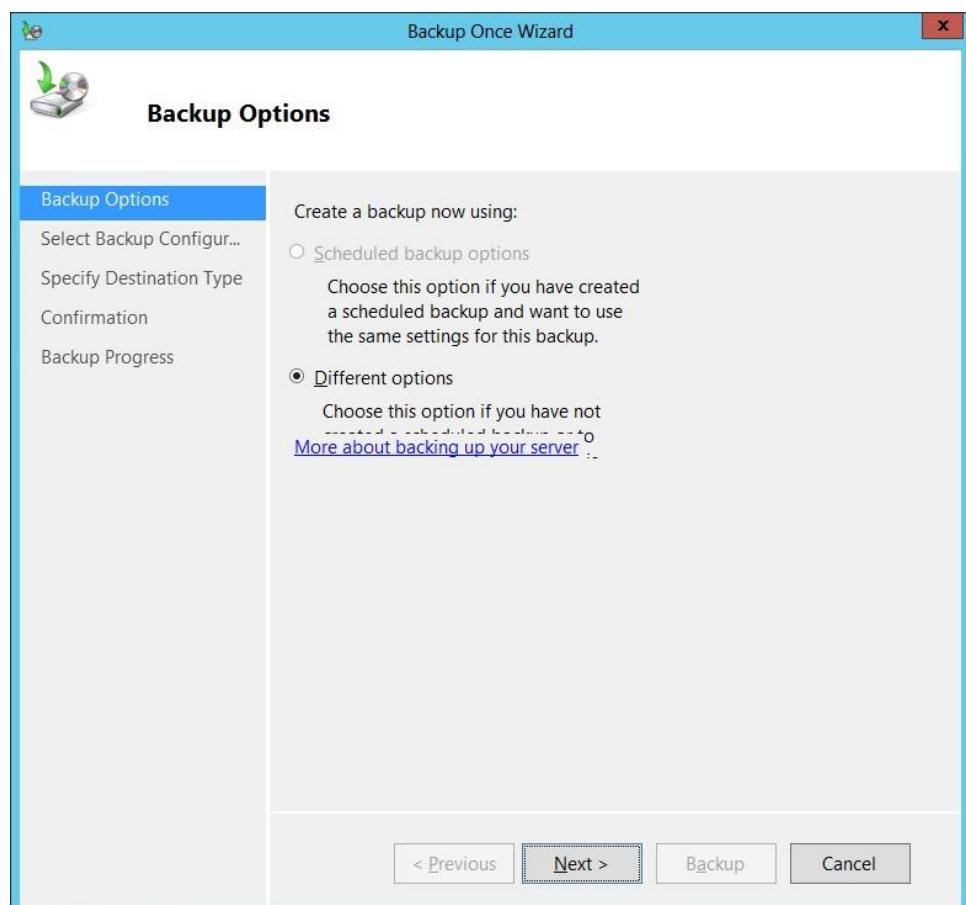
2. Select **Windows Server Backup**, (or) to use online backup click Continue under Online backup.

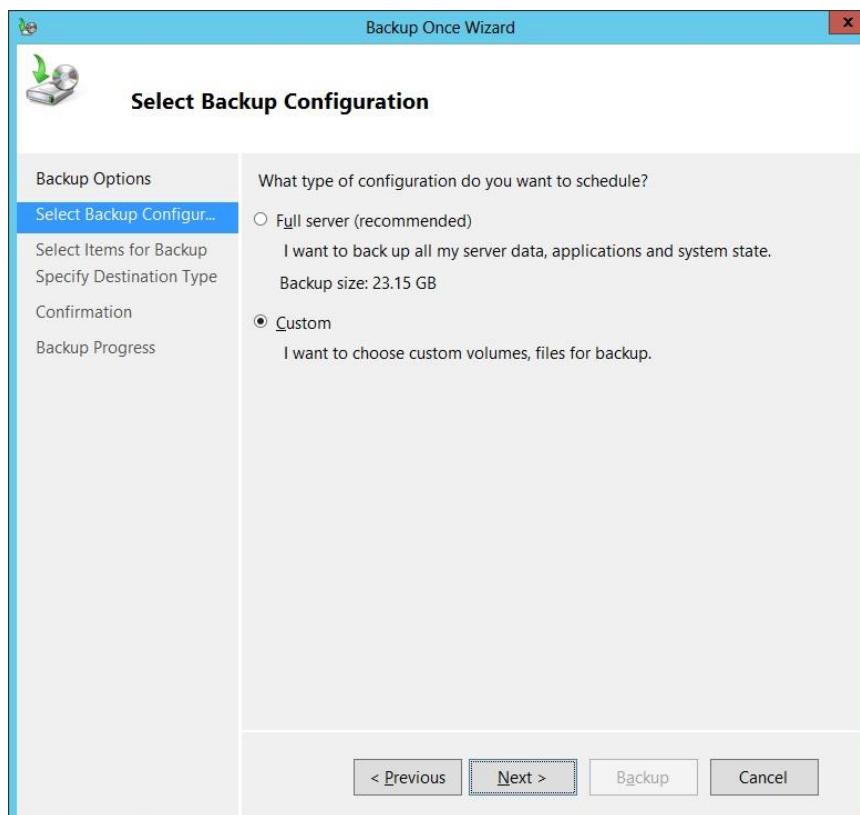
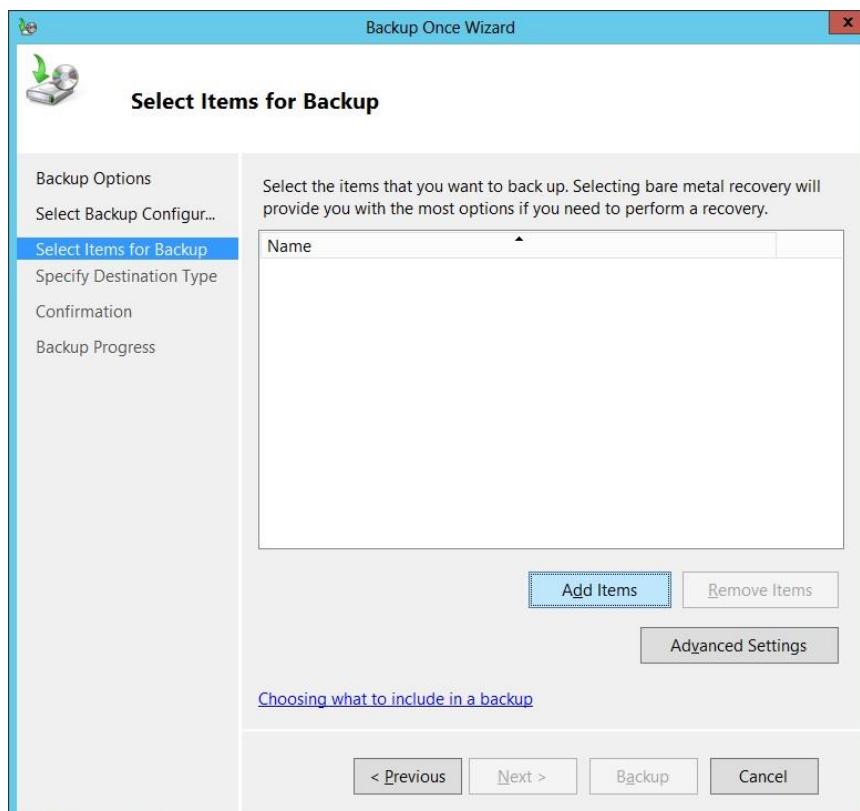


3. Select Local Backup, and click **Backup Once**.

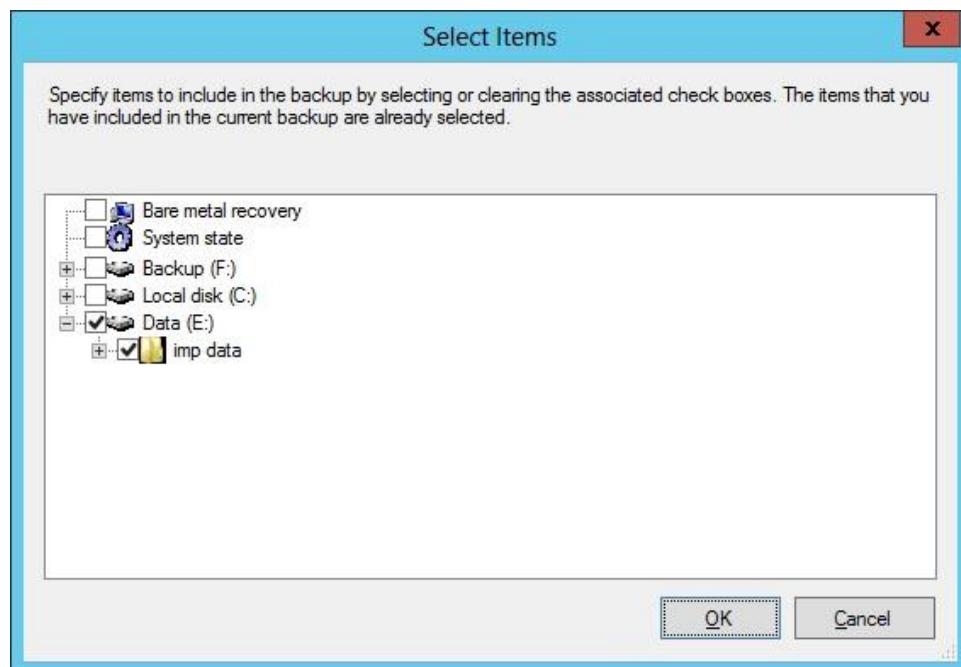


4. Select Different Options, click Next.

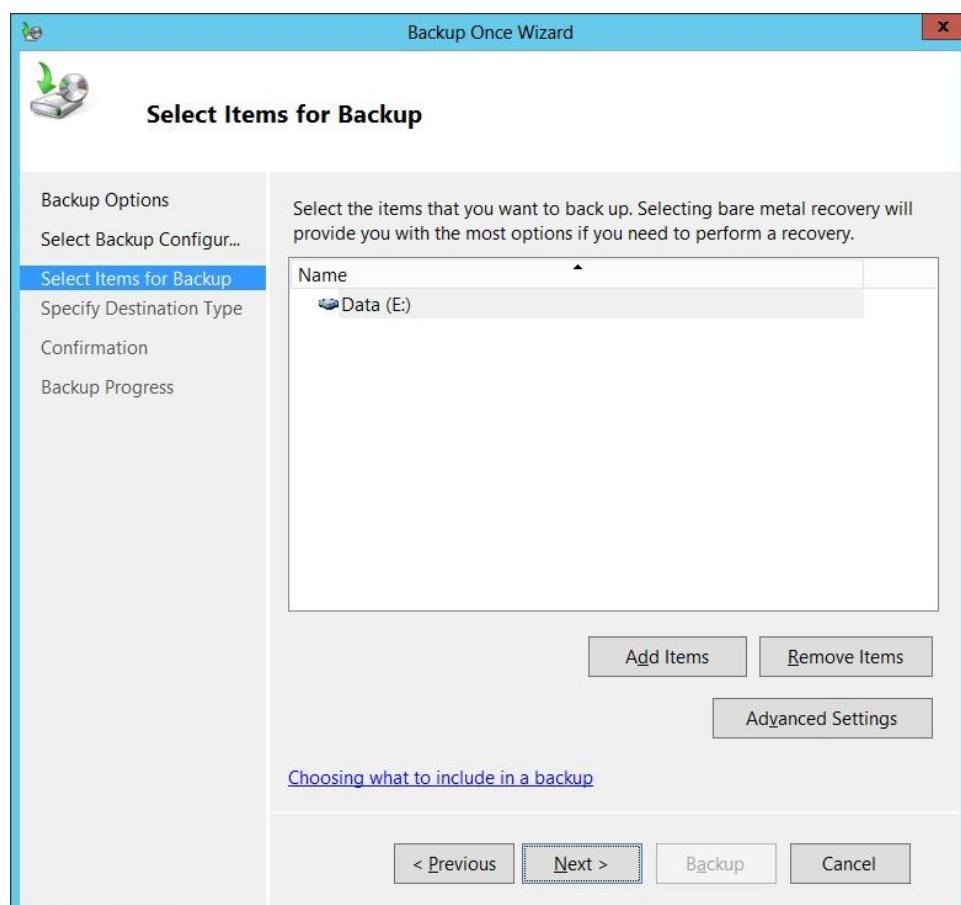


5. Select **Custom**, click **Next**.6. In Selects items for Backup, click **Add Items**.

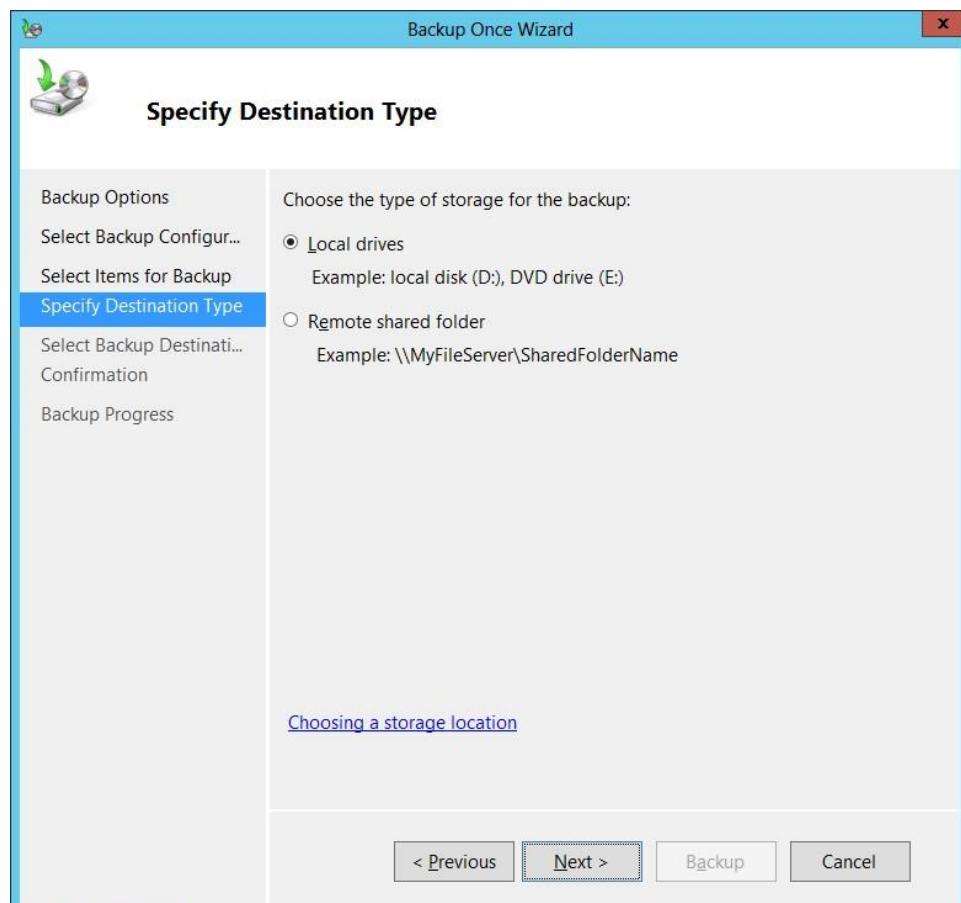
7. In Select Items window, check the box **imp data folder**, click **OK**.



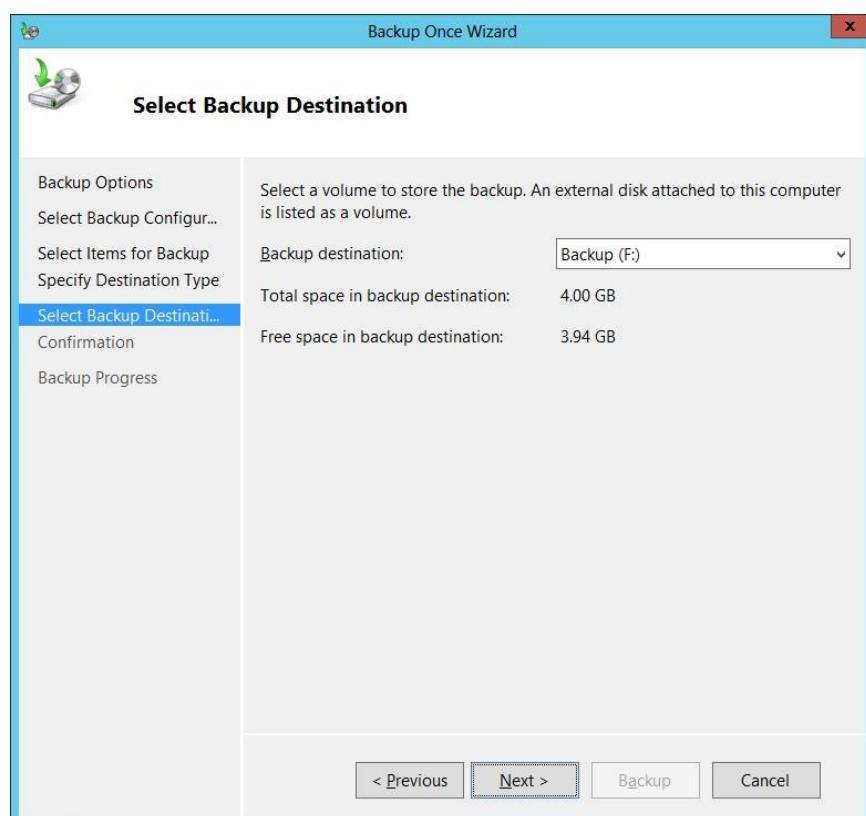
8. In Select Items for Backup page, click **Next**.



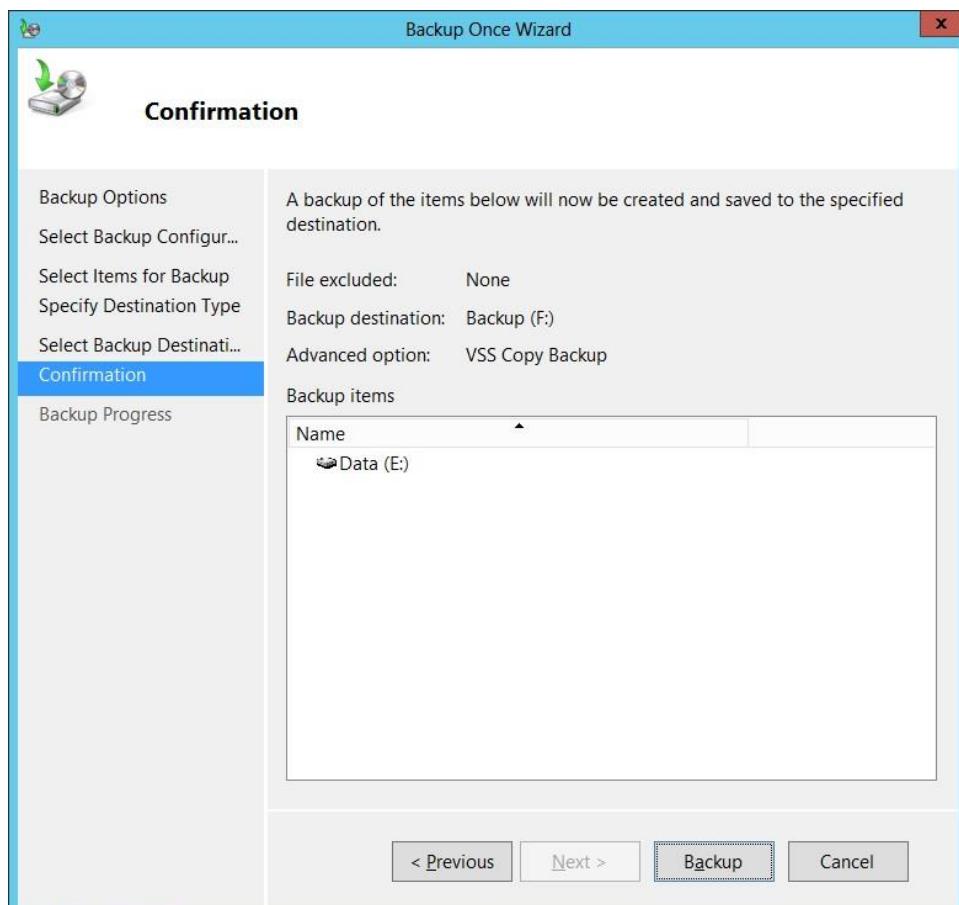
9. In Specify Destination Type page, select **Local drives**, click **Next**.



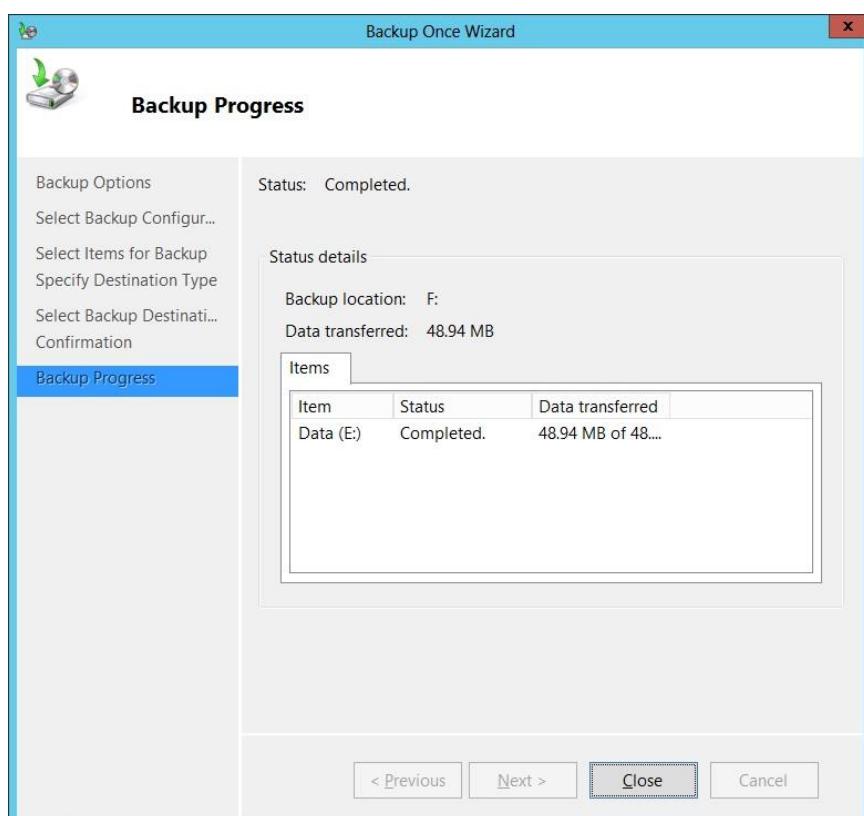
10. In Select Backup Destination, select Backup destination **Backup Drive**, click **Next**.



11. In Confirmation page, click **Backup**.

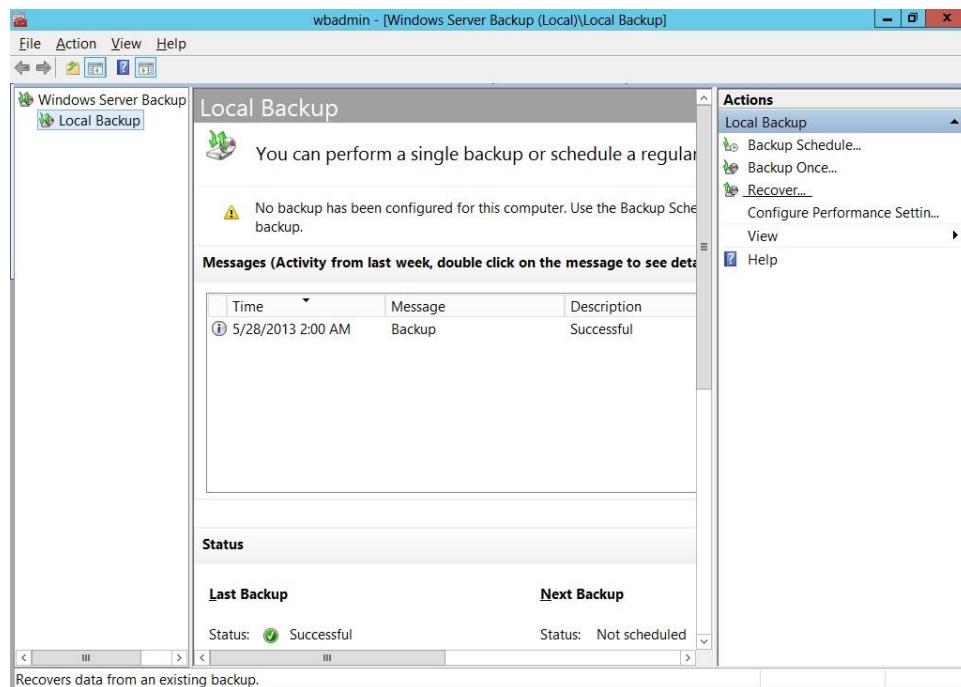


12. Finally click **Close**.

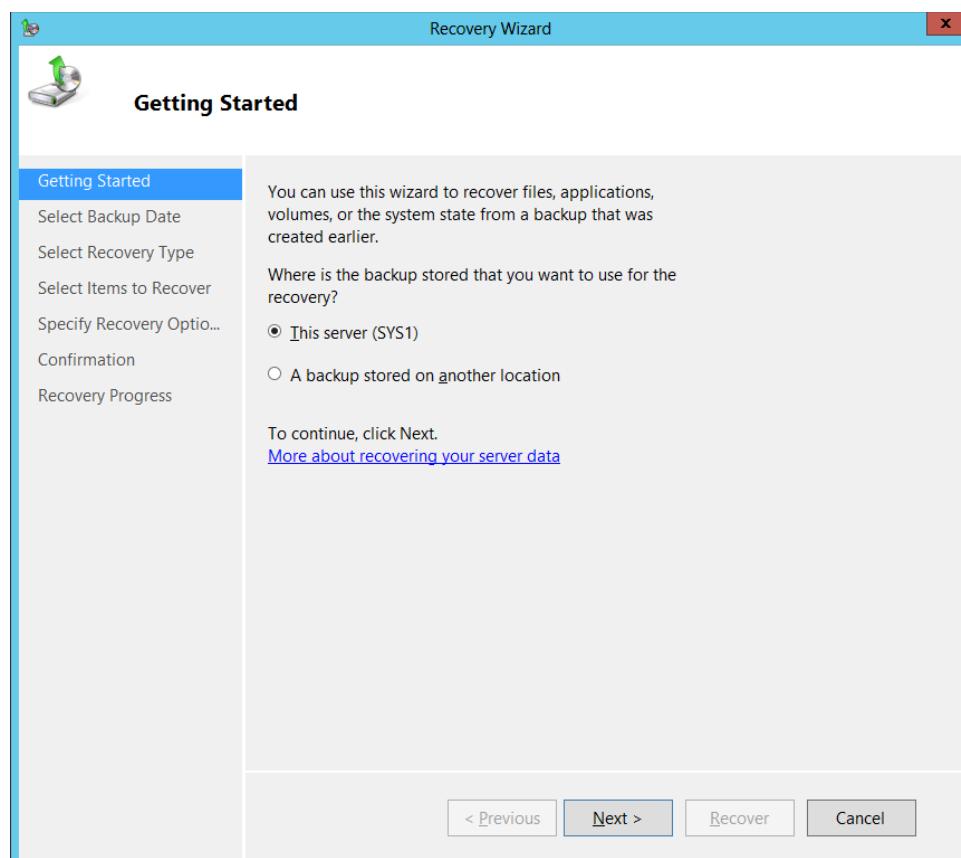


How to Recover the Data from Backup File.

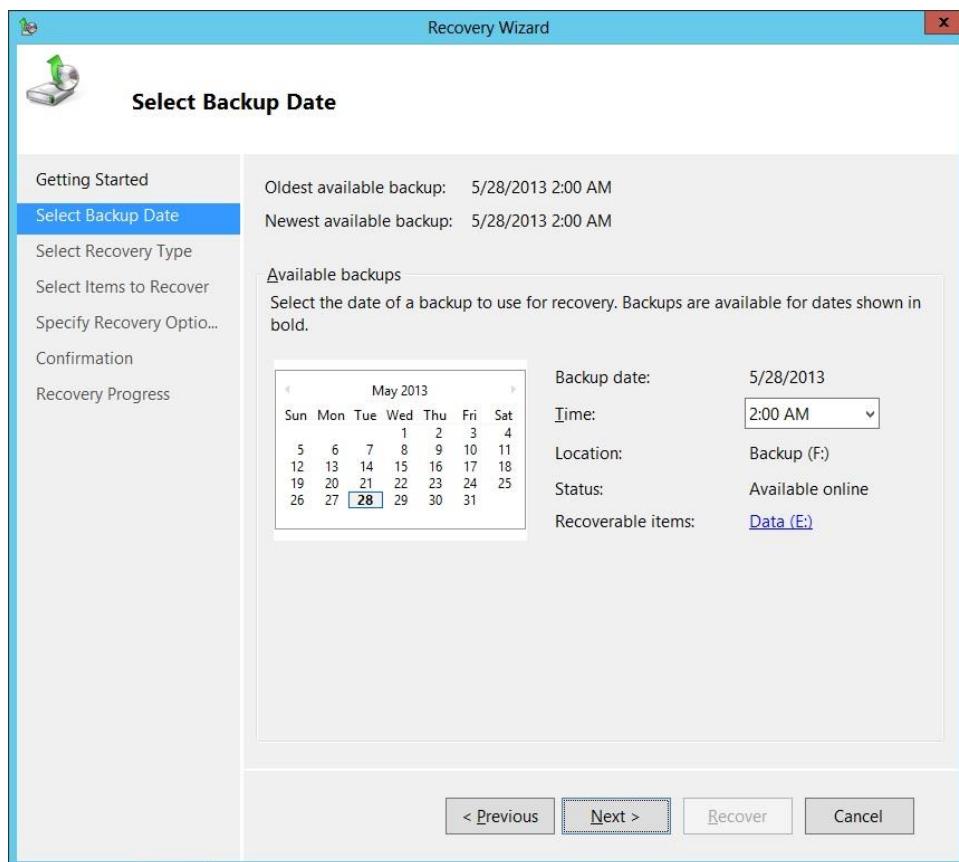
1. Before Restoration, go to the drive and delete the data. (only for Lab purpose)
2. Go to Windows Server Backup, select Local Backup, and click Recover.



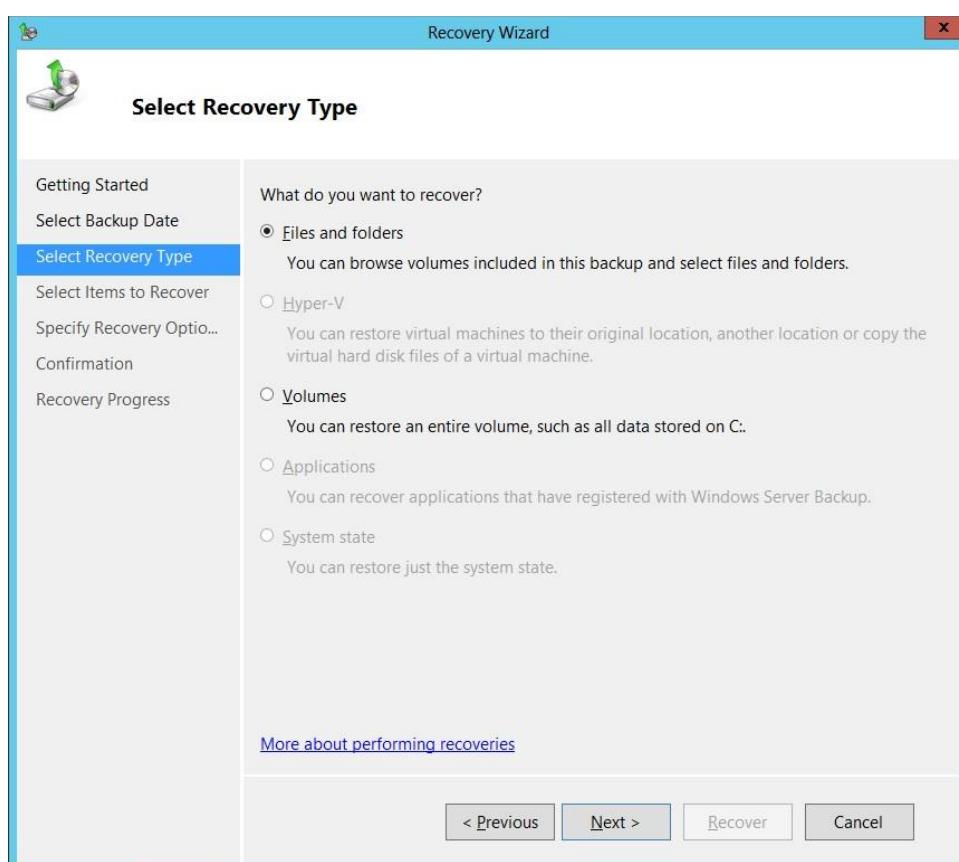
3. In Getting Started page, select This server, click Next.



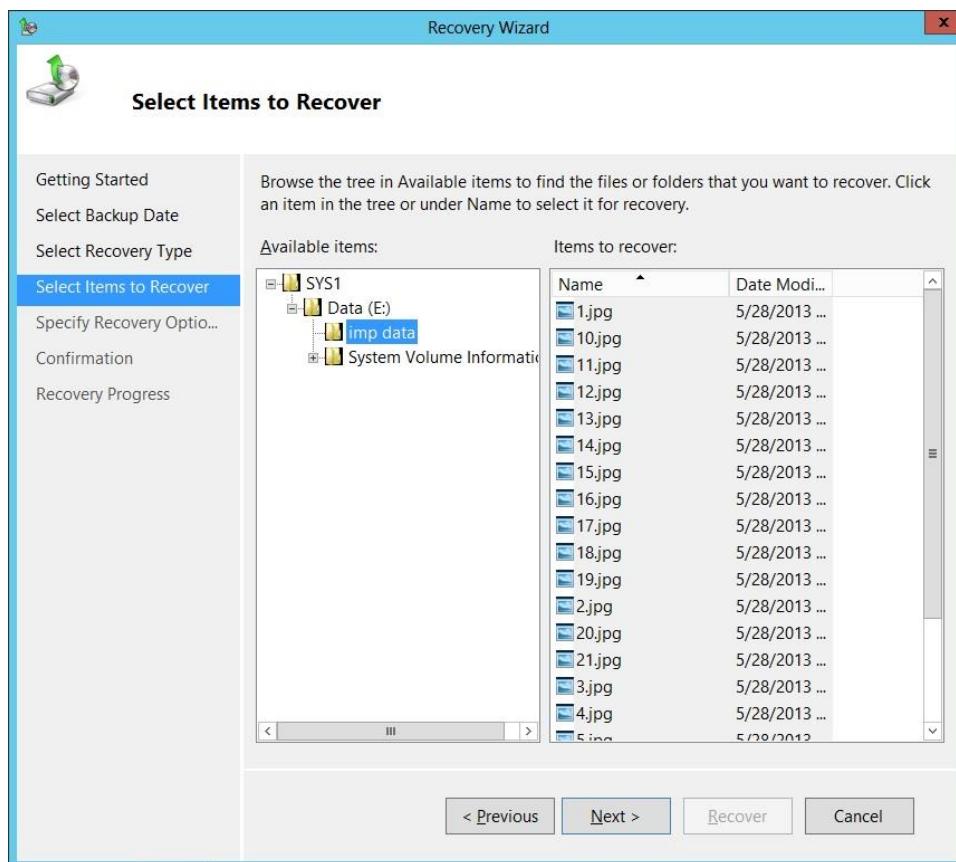
4. Select Date and Time of the Backup file to be restored, click **Next**.



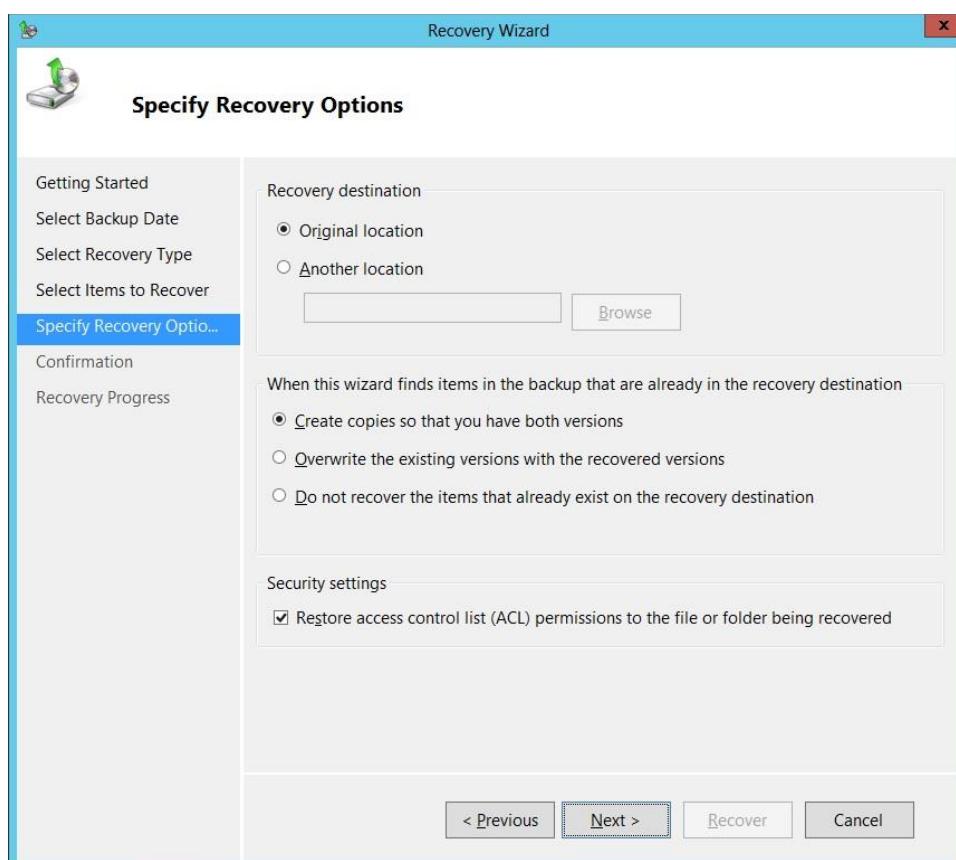
5. In select Recovery Type, select **Files and folders**, click **Next**.



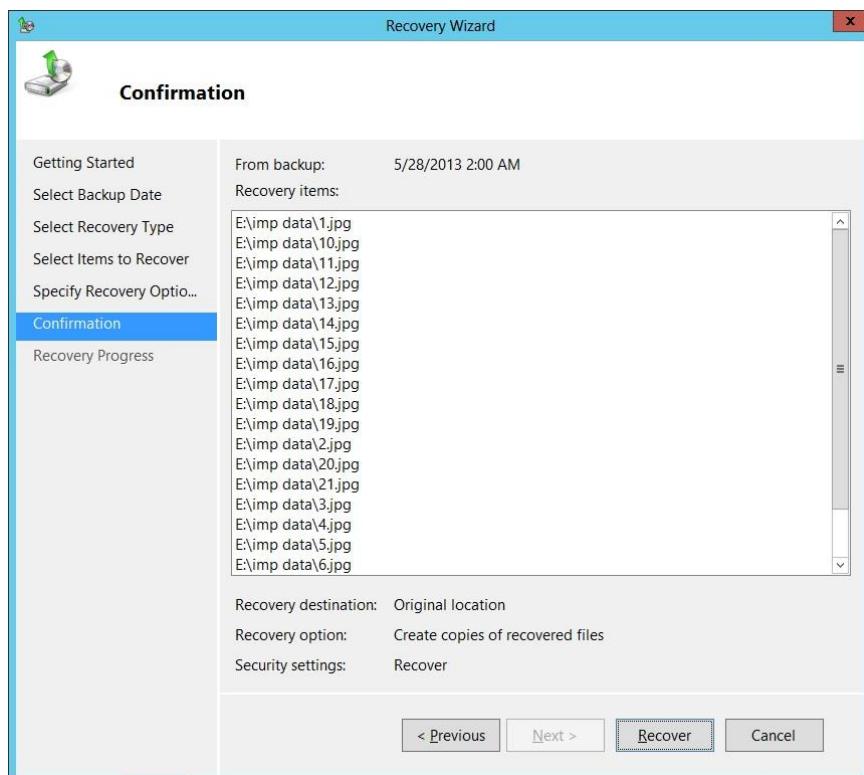
6. Select the folder or files to be recovered and click **Next**.



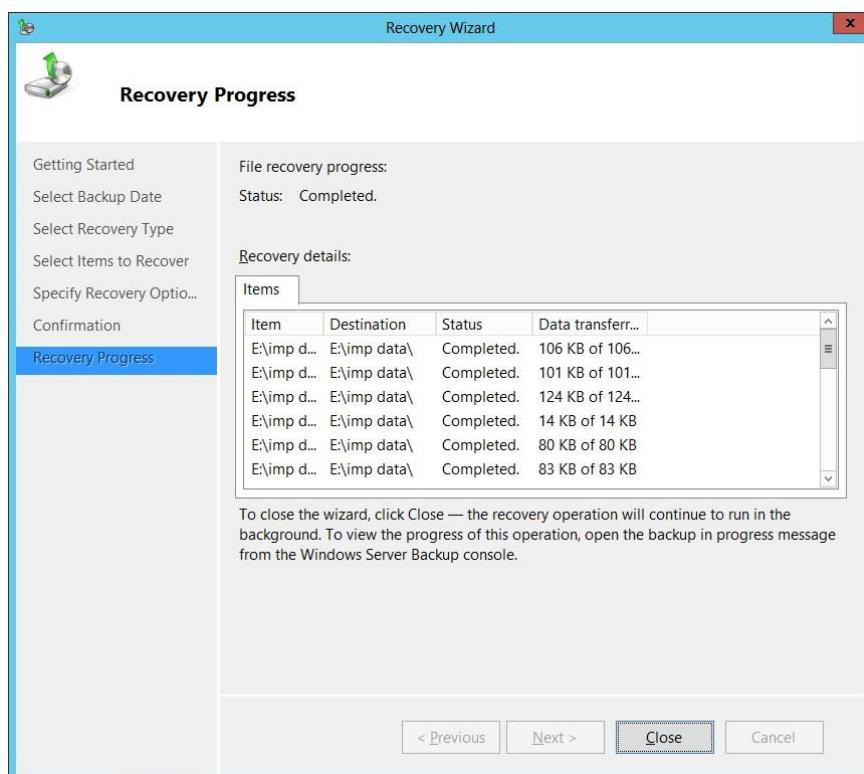
7. Select **Original location**, click **Next**.



8. In Confirmation page, click Recover.



9. Click Close.



Verification:

1. Go to the **drive** and verify for the **folder** and **files**.

ADVANCED TOPICS

ACTIVE DIRECTORY

- Domain Services (AD-DS)
- Lightweight Directory Services (AD-LDS)
- Rights Management Services (AD-RMS)
- Federation Services (AD-FS)
- Certificate Services (AD-CS)

Lightweight Directory Services (AD-LDS)

- AD LDS Provides an LDAP accessible directory service that supports identity management scenarios
- Removes all other AD DS features
 - No Kerberos authentication
 - No forests, domains, DC, GC, sites, group policies
 - No dependency on DNS
- Each AD LDS server can host multiple directory stores (i.e. instances)

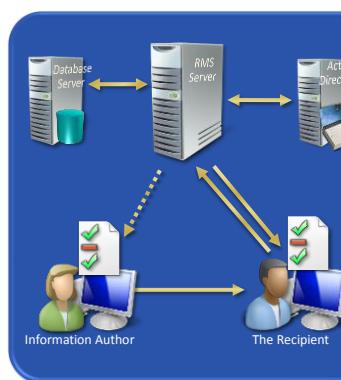
Lightweight Directory Services (AD-LDS)

- Within each instance
 - Schema partition
 - Configuration partition
 - Zero or more application partitions

Rights Management Services (AD-RMS)

- RMS enables customers to keep internal information internal
 - Confidential files protection
 - E-mail forwarding
 - Web applications
- Benefits:
 - Safeguards sensitive internal information
 - Digitally enforces organization policies
 - Persistently protects information

Rights Management Services Work flow

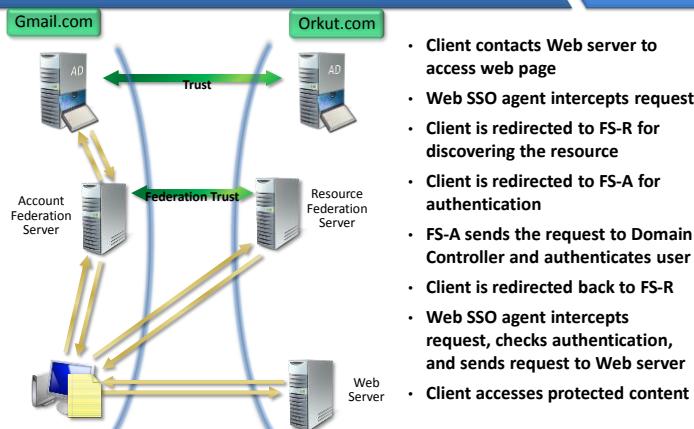


- Author receives a client license certificate the “first time” they right-protect the information.
- Author defines a set of usage rights and rules for their file & creates a “publishing license” to encrypt file.
- Author distributes file.
- Recipient opens the file, the application calls the RMS server which validates the user and issues a “use license.”
- Application opens the file and enforces rights.

Federation Services (AD-FS)

- AD FS provides an identity access solution
- AD FS is a service that allows for the creation of federated relationships between organizations for web application authentication
- Deploy federation servers in multiple organizations to facilitate business-to-business (B2B) transactions
- AD FS provides a Web-based Single Sign-On (SSO) solution

Federation Services (AD-FS)



Certificate Services (AD-CS)

- AD CS Provides PKI certificate issuance and management services
- Not significantly different than CS in 2003
- Provides a certificate issuance and Certification Authority (CA) service
- Issues Digital certificates to web server for Secure data transfer (HTTPS)

NETWORK ACCESS PROTECTION (NAP)

Network Access Protection

What is Network Access Protection?

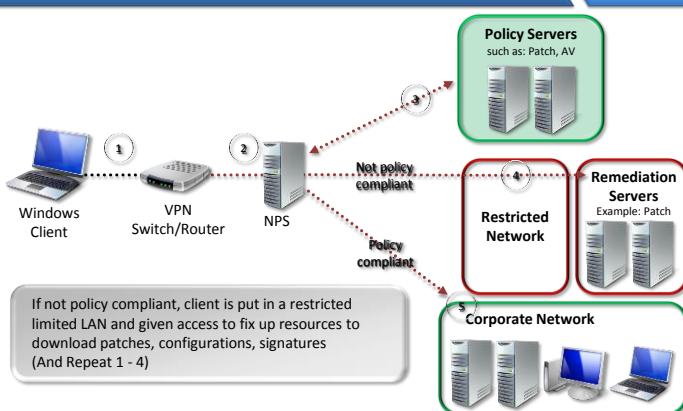
Health Policy Validation

Health Policy Compliance

Ability to Provide Limited Access

Enhanced Security

How Network Access Protection works?

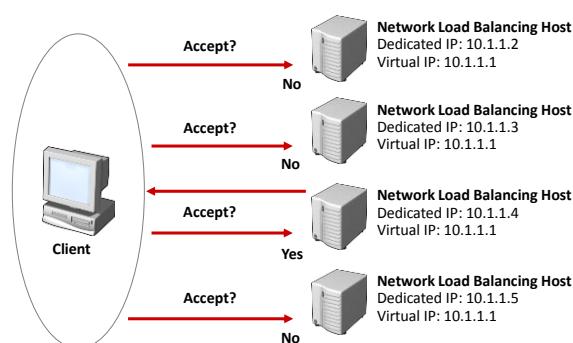


Network Load Balancing

Network Load Balancing

- Network Load Balancing (NLB) uses a distributed algorithm to balance IP traffic load across multiple hosts. It helps to improve the scalability and availability of business-critical, IP-based services.
- NLB also provides high availability, because it detects host failures and automatically redistributes traffic to surviving hosts.
- Windows Server 2012 NLB clusters can have between 2 and 32 nodes.
- Balances traffic based on node utilization
 - New traffic will be directed to the node that is being utilized the least
 - You can configure NLB to preference some nodes over others

How NLB Works



Server Failures and Recovery

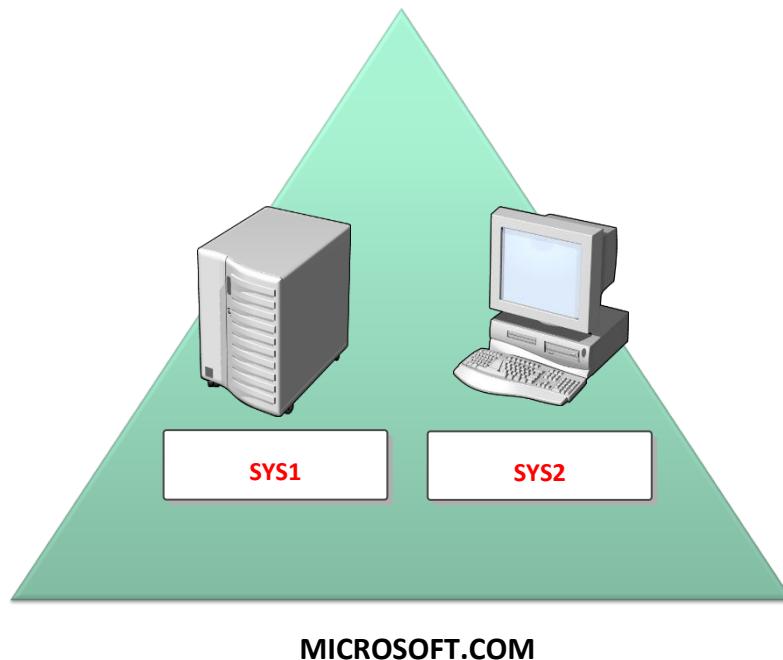
- NLB cluster heartbeats are transmitted every second between nodes in a cluster
- Convergence occurs when:
 - A node misses five consecutive heartbeats, at which time it is automatically removed from an NLB cluster
 - A node that was member of a cluster returns to functionality
 - An administrator adds or removes a node manually

ADVANCED TOPICS

Prerequisites:

Before working on this lab, you must have

1. A computer running windows 2012 server Domain Controller.
2. A computer running windows 2012 server or Member Server.

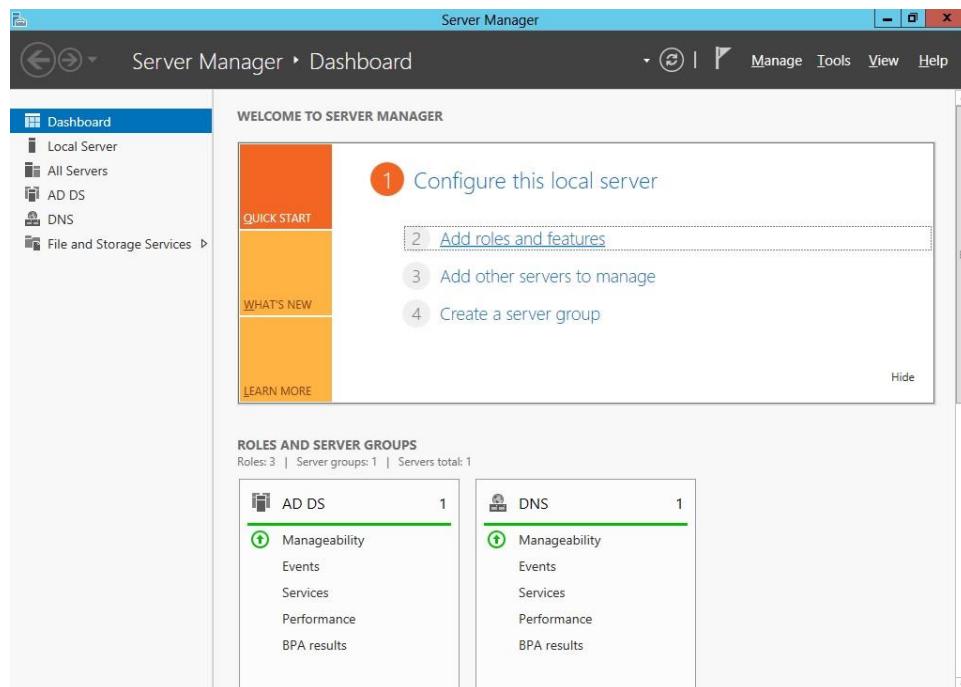


SYS1	SYS2
Domain Controller	
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1
Member Server	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0
Preferred DNS	10.0.0.1

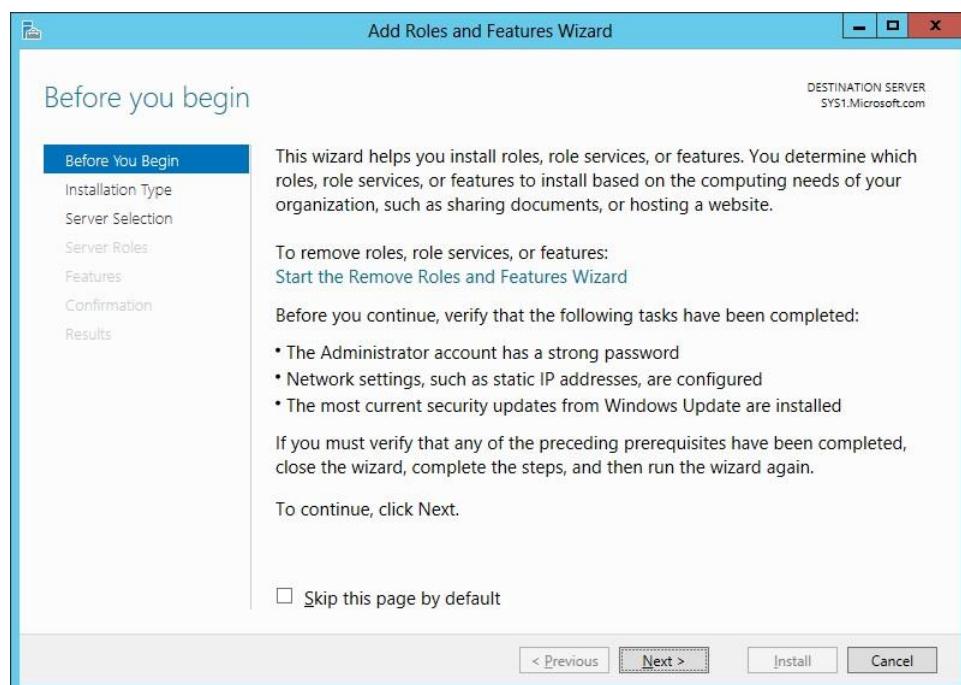
Lab – 1: Configuring Network Load Balancing

Step-1: Install Network Load Balancing Feature on SYS1 and SYS2.

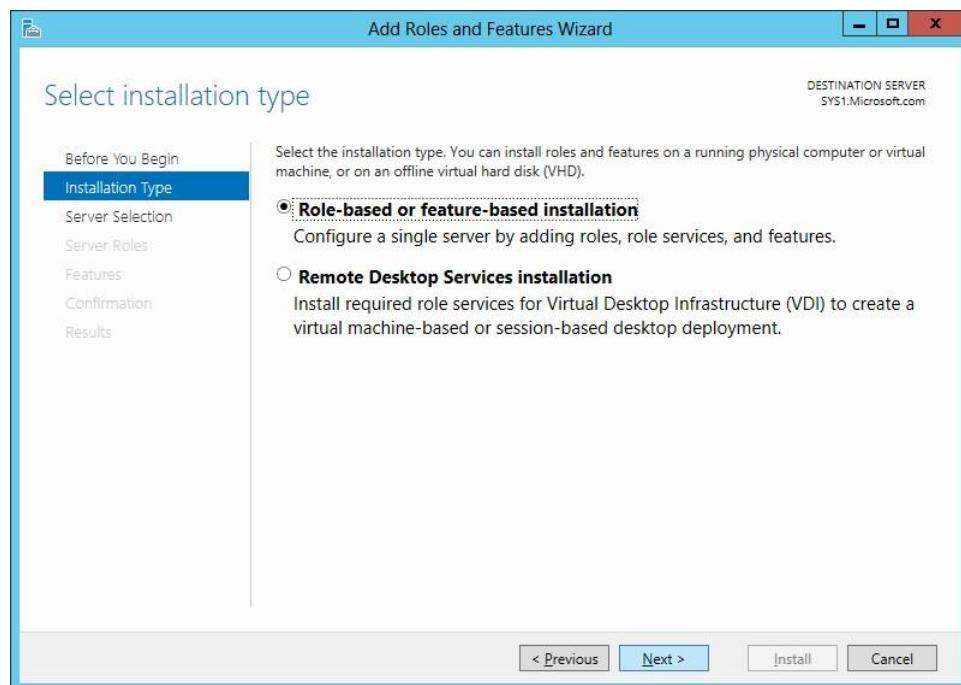
1. Login as **Administrator**, go to ServerManager Dashboard and click **Addrolesandfeatures**.



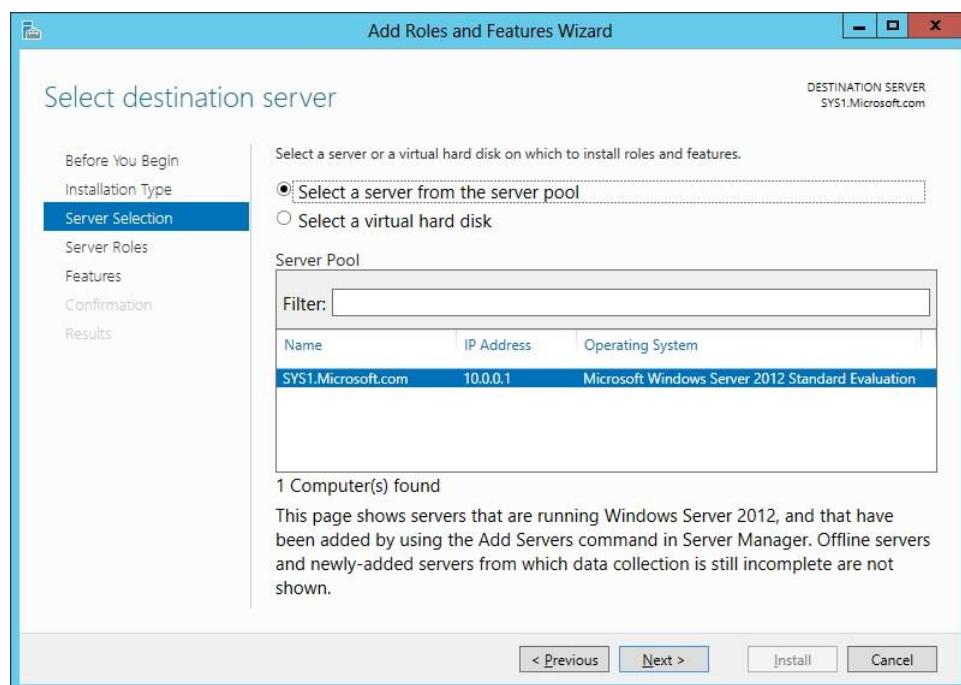
2. In Before you begin page, click **Next**.



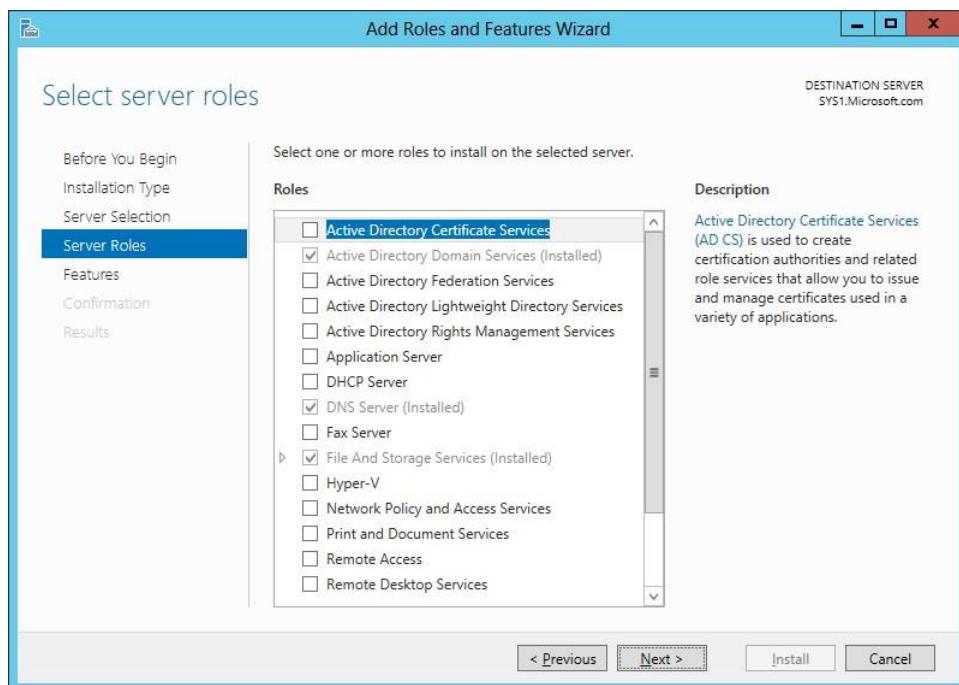
3. Select Role-based or feature-based installation, click **Next**.



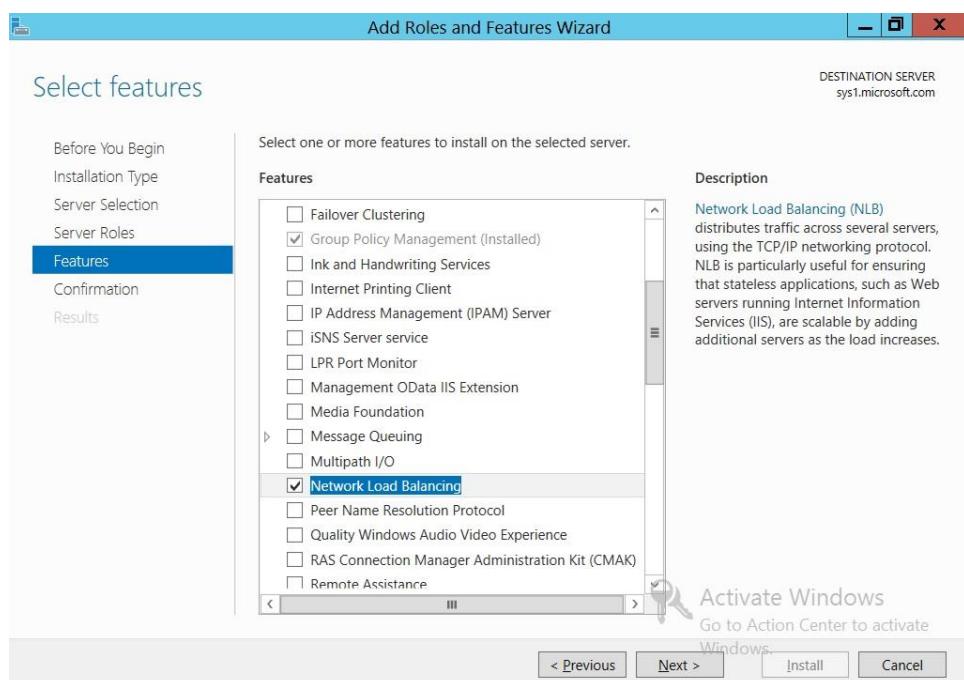
4. In Select destination server page, select a server (**SYS1.Microsoft.com**) from the server pool and click **Next**.



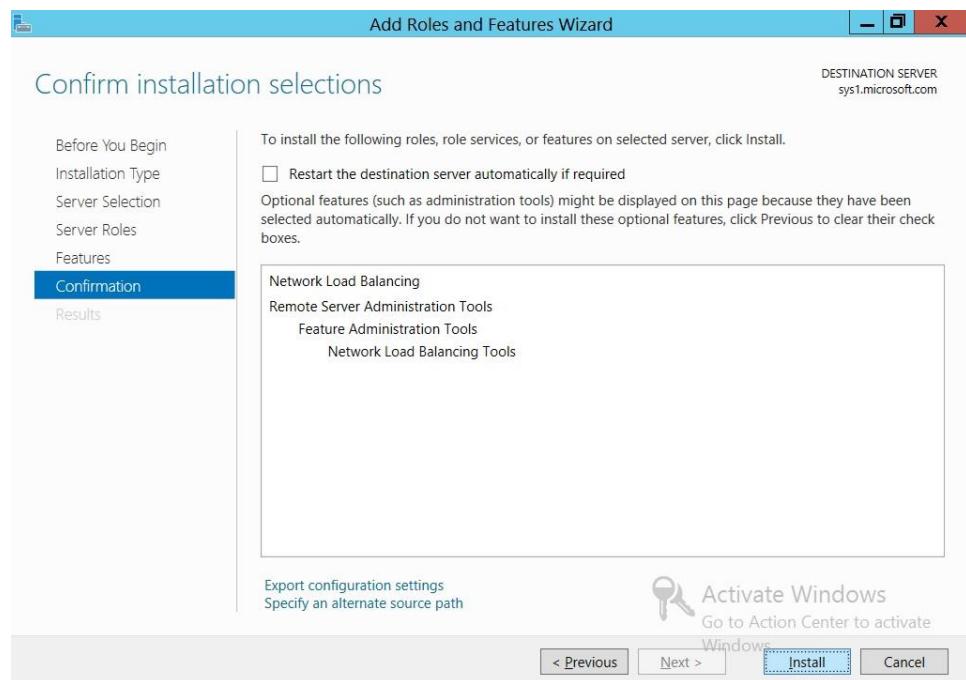
5. In Select server roles page, click **Next**.



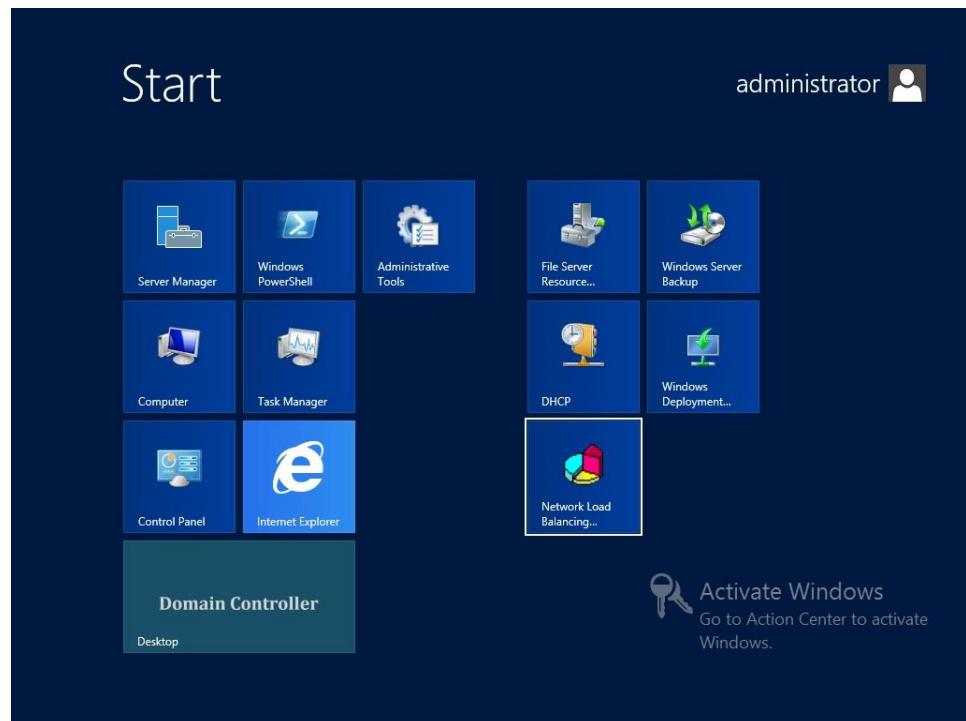
6. In Select features page, check the box **Network Load Balancing** and click **Next**.

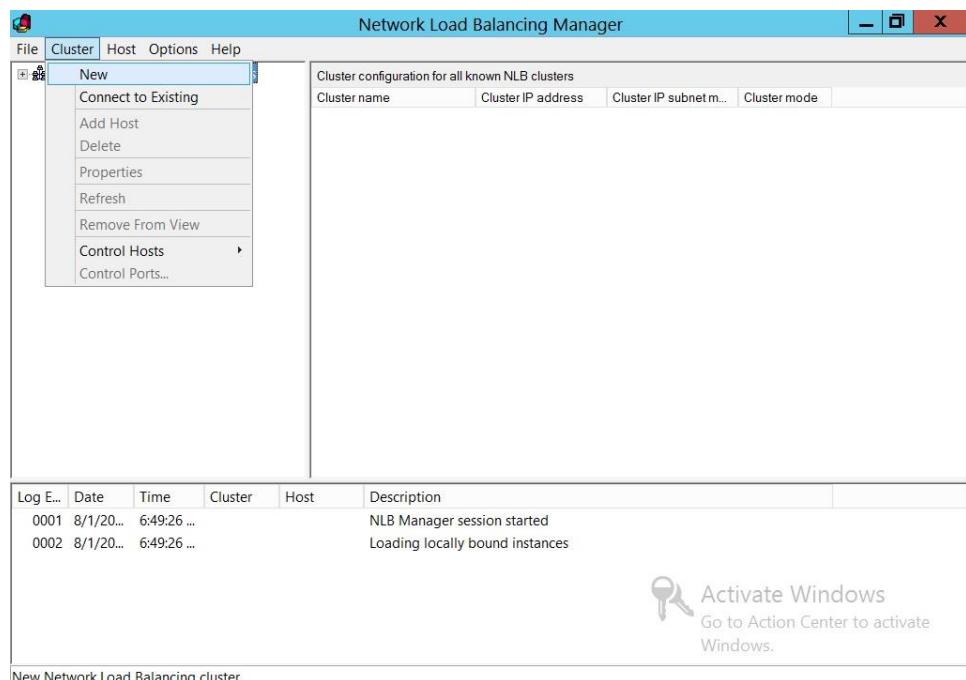


7. Check box **Restart the destination server automatically if required**, click **Install**.



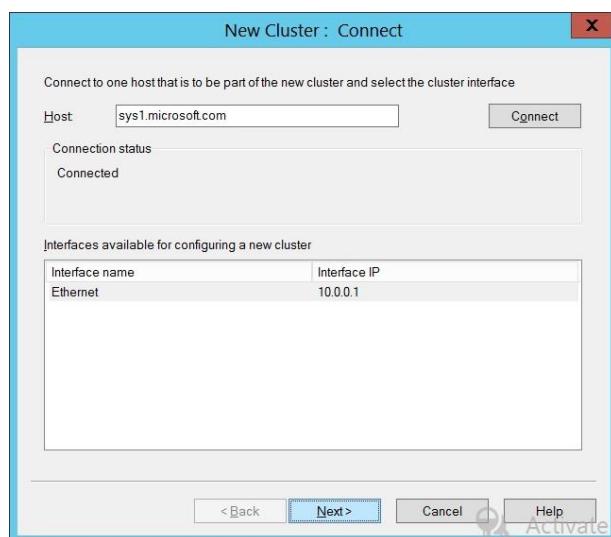
8. Go to Start, click **Network Load Balancing Manager**.



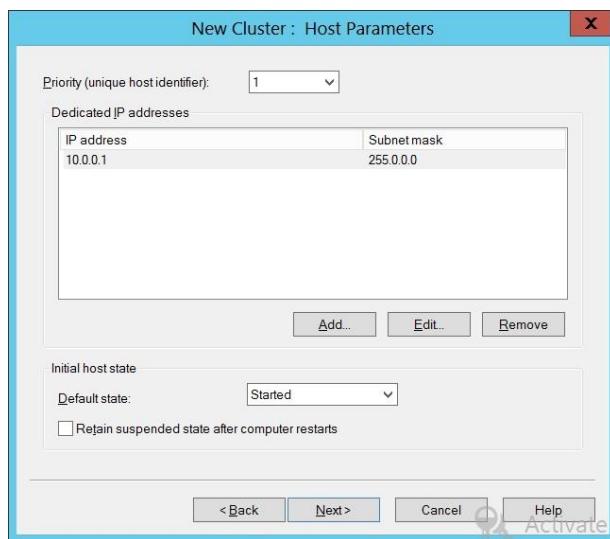
9. Click **Cluster**, select **New**.

Activate Windows
Go to Action Center to activate Windows.

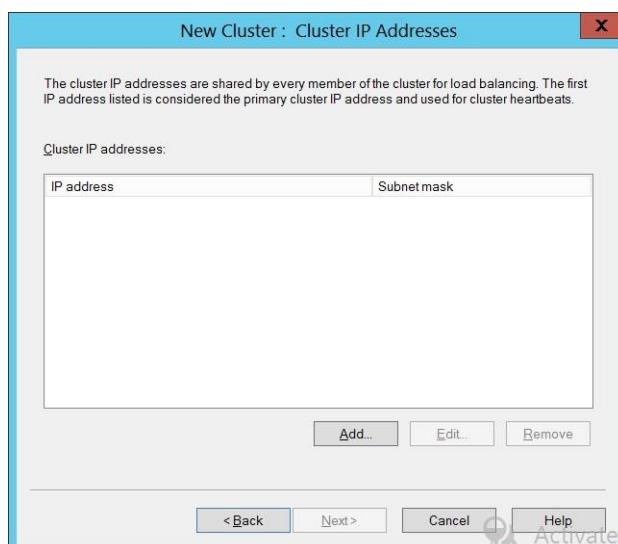
New Network Load Balancing cluster.

10. Enter the host name **Sys1.microsoft.com** and click **Connect** and **Next**.

11. Verify the Priority and click **Next**.

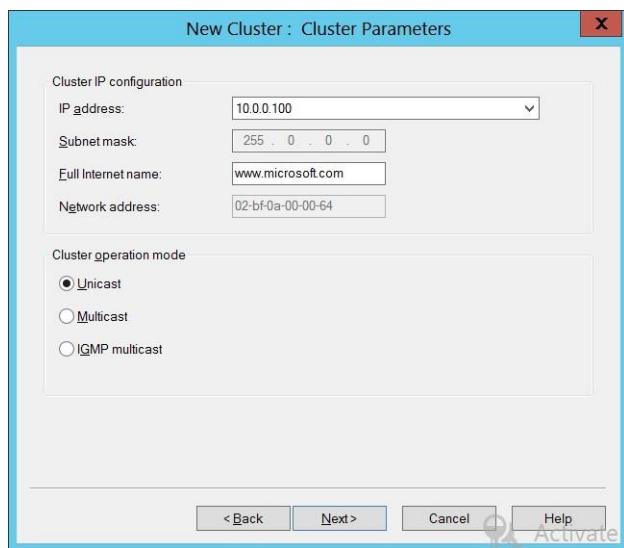
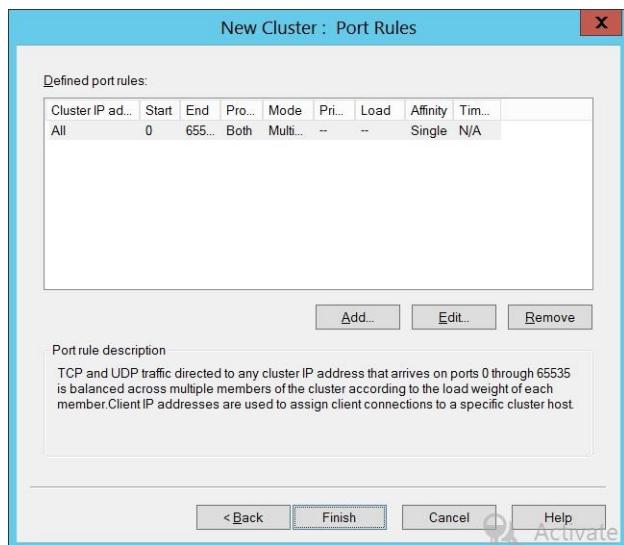


12. Click **Add**

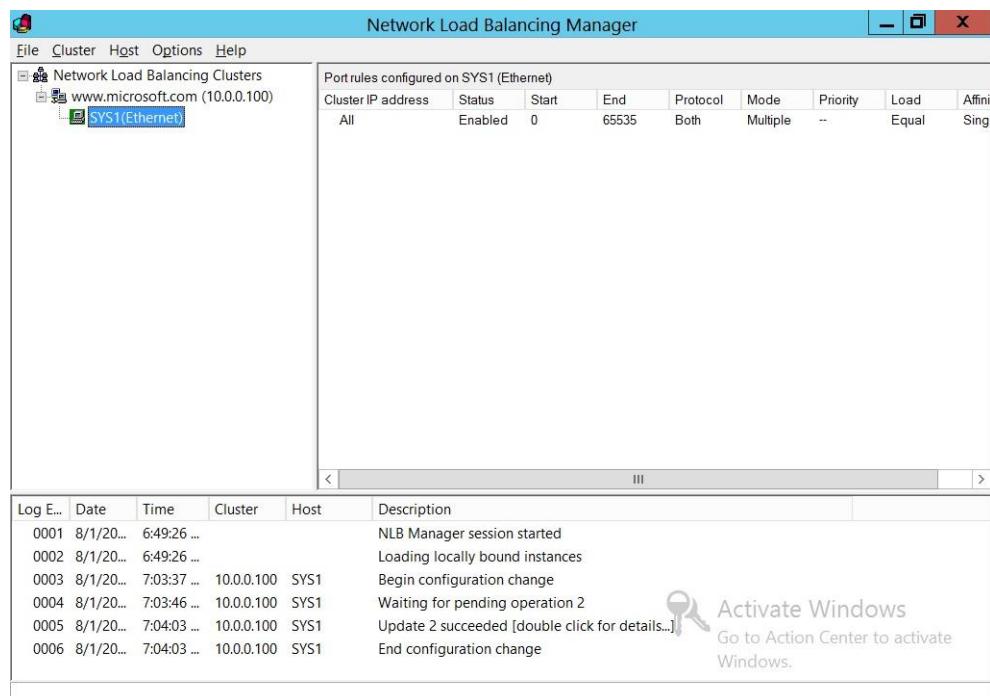


13. Enter **Cluster IP Address** (Ex: 10.0.0.100) and **Subnet** (Ex: 255.0.0.0)

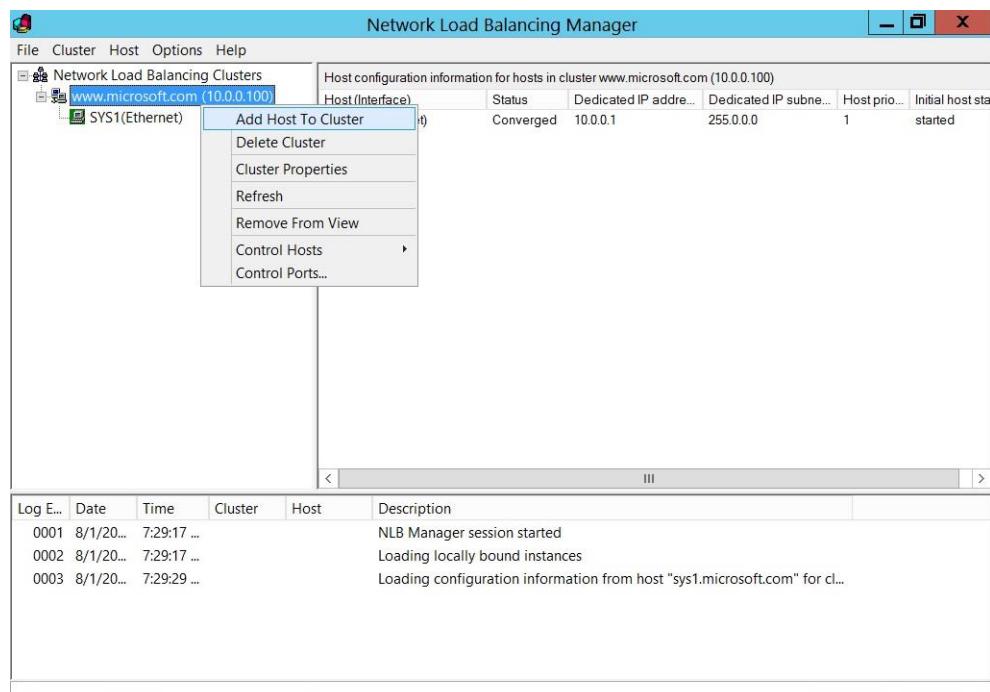


14. Enter the Full Internet Name (Ex: **www.microsoft.com**)15. Click **Finish**.

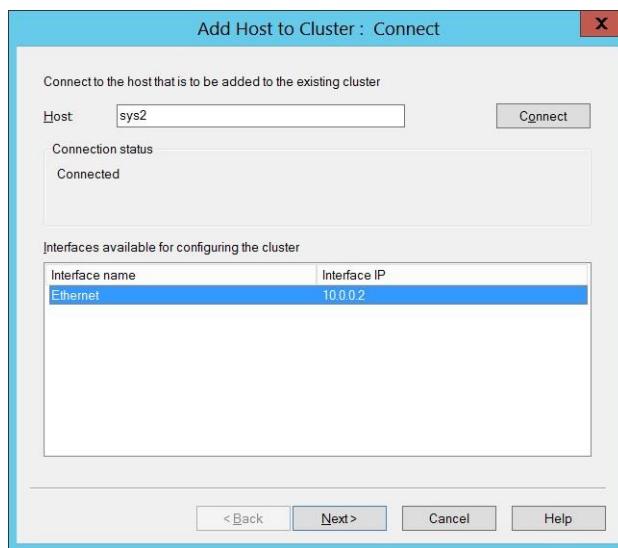
16. Verify for **Sys1 added as host in Cluster.**



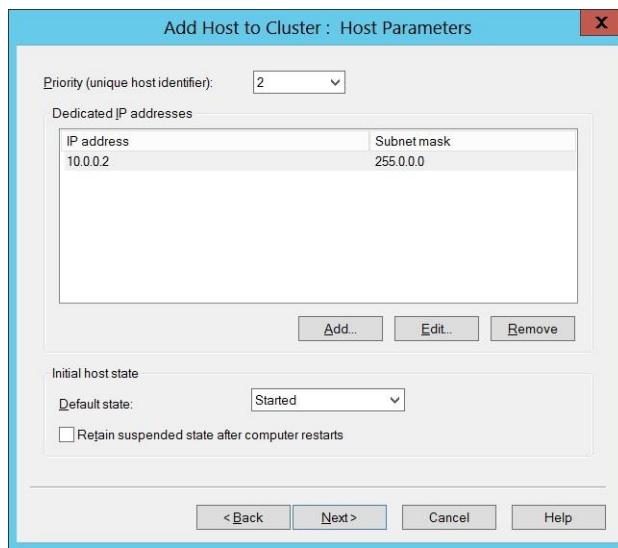
17. Right click on the Cluster (Ex: **www.microsoft.com), select **Add Host to Cluster**.**



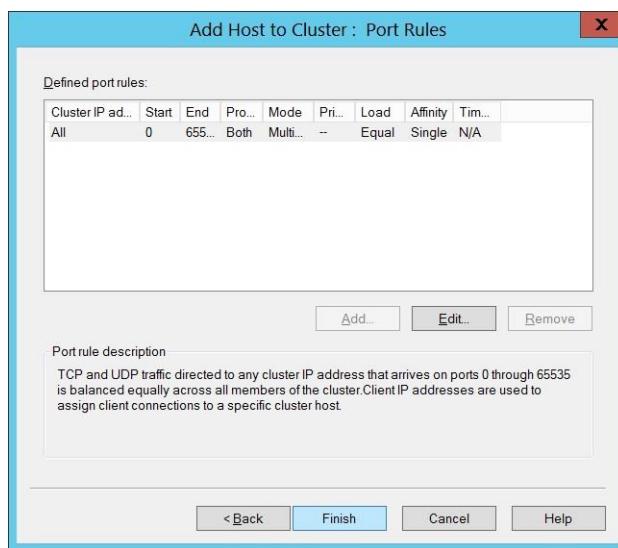
18. Enter Host name **SYS2, click **Connect** and **Next**.**



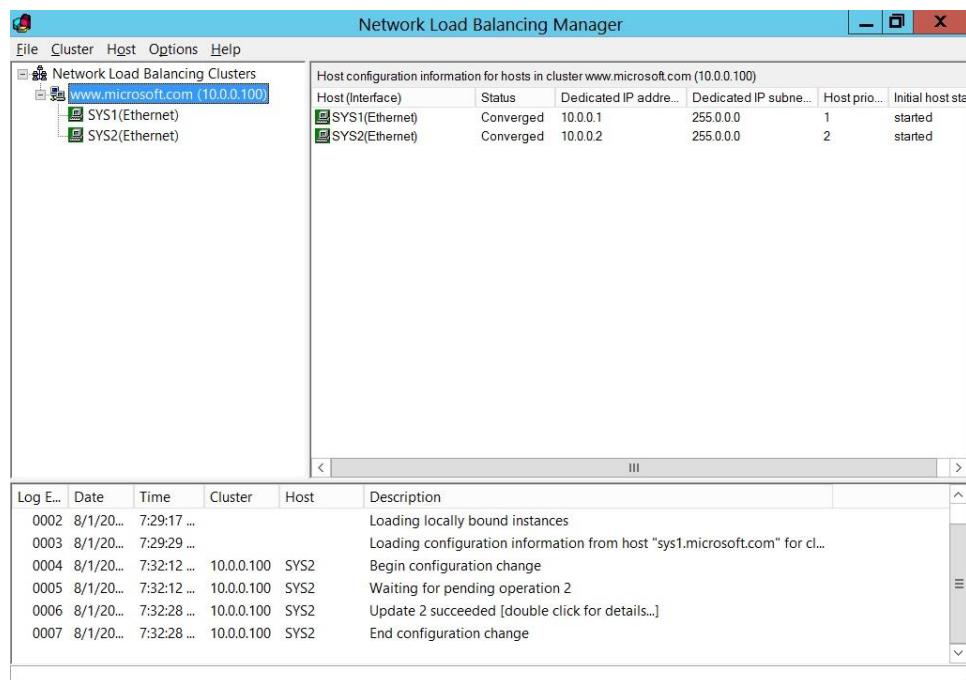
19. Verify the Priority and click **Next.**



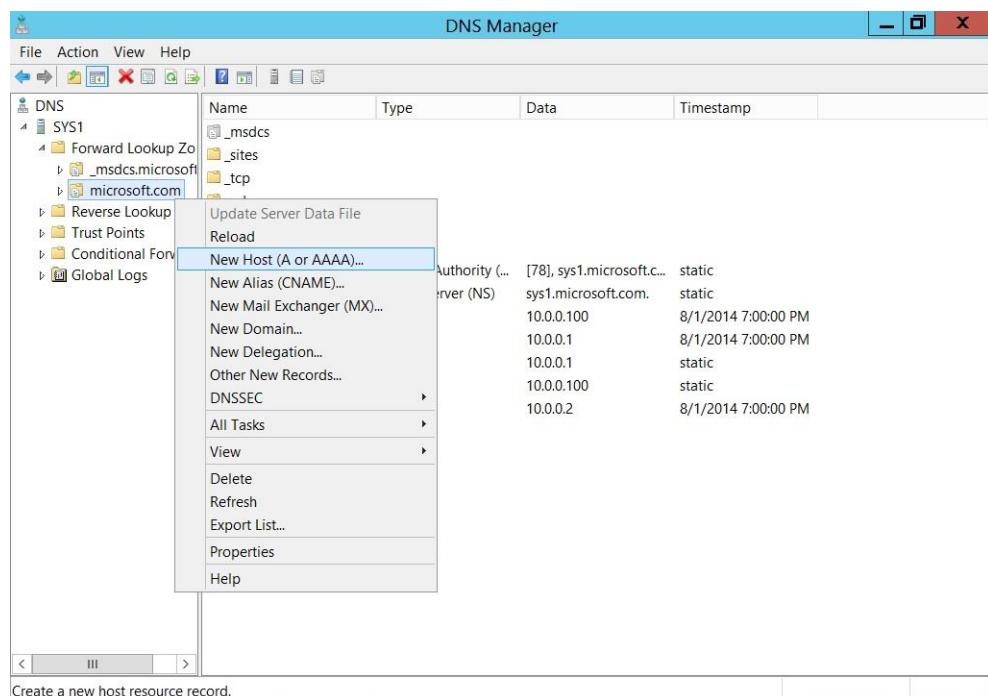
20. Click **Finish.**



21. Verify the hosts in status of Converged.

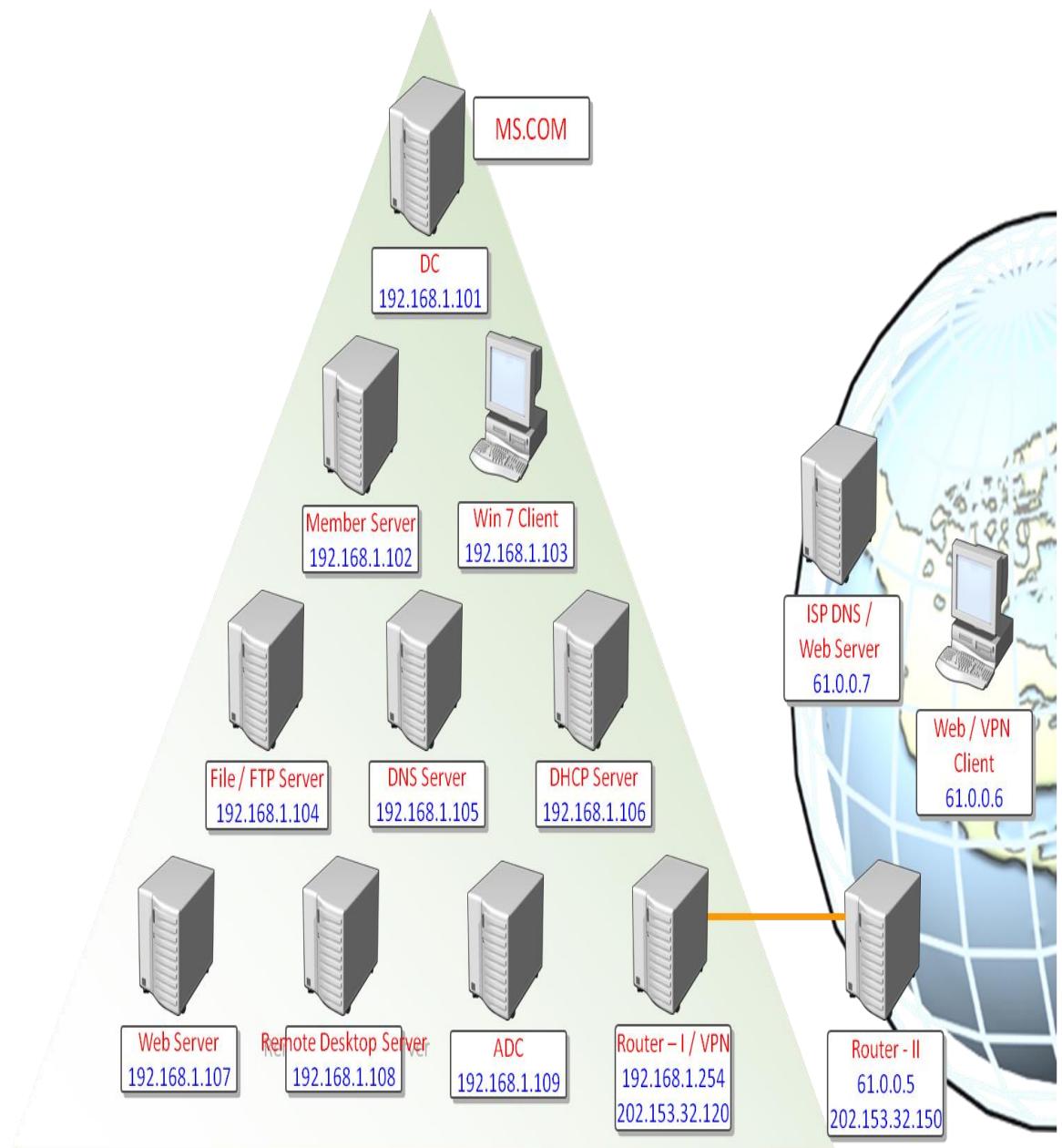


22. Configure DNS Host record for Cluster IP Address.



23. Verify for the Host record www.microsoft.com mapped to 10.0.0.100.

LIVE SETUP



DOCUMENTATION OF LIVE SETUP

Prerequisite:

Internal Network

Servers:

Domain Controller	– 192.168.1.101
File server	– 192.168.1.104
DNS server	– 192.168.1.105
DHCP server	– 192.168.1.106
Local Web server	– 192.168.1.107
FTP server	– 192.168.1.104
Remote Desktop {RDP} server	– 192.168.1.108
Additional Domain controller	– 192.168.1.109
VPN server	– 192.168.1.254

Clients:

Member Server	– 192.168.1.102
Windows 7 Client	– 192.168.1.103

Router I

LAN Interface	– 192.168.1.254
WAN Interface	– 202.153.32.120

External Network:

Router II

WAN Interface	– 202.153.32.150
WAN2 Interface	– 61.0.0.5

Clients:

Client	– 61.0.0.6
Web server	– 61.0.0.7

Configure 61.0.0.7 as Internet Web Server and DNS Server for www.Whatismyip.com

CONFIGURATION STEPS

- Configure **192.168.1.101 as Domain Controller** along with DNS with the name **Microsoft.com**
- **Join** all the systems to the domain (Windows 2012 / Windows 7)
- **Create Users on DC&** login using the same user from Client (Windows 2012 / Windows 7)
- Configure **192.168.1.104 as File Server**
 - User profiles - Roaming
- Configure the Separate **DNS server** for Domain {obtain SRV Records} **on 192.168.1.105**
- Configure **192.168.1.106 as DHCP Server**
 - Scope
 - Reservation for File server etc,
 - Assign Dynamic IP's to all systems
- Configure **192.168.1.107 as Web Server** for www.Microsoft.com
 - Create DNS zone for this site on DNS server only {192.168.1.105}.
 - Access this web site from Internal network
- Configure **192.168.1.104 as FTP Server**
 - Access this FTP site from Internal network
- Configure **192.168.1.108 as Terminal {RDP} Server**
 - Access this Terminal server from Internal network

- Configure **192.168.1.109** as ADC for **Microsoft.com**
 - Turn off the DC & login as user from **Client or Member Server**.
- Configure **192.168.1.254** as **Private Router I** and **WAN IP is 202.153.32.120**
 - Add Static Route for 61.0.0.0 network
- Configure **202.153.32.150** as the **Public Router II** and **WAN IP is 61.0.0.5**
 - Add Static Route for 192.168.1.0 network
 - Access www.Microsoft.com from External network
 - Access the Local FTP site from External network
- Configure **Router I** as **NAT server**
 - Configure Local DNS Server to forward the request to ISP DNS server{61.0.0.7}
 - Access www.whatismyip.com from Internal network
- Configure **ROUTER1** as **VPN Server**
 - Access the VPN server from External network
- Maintain **61.0.0.6** as **public client** to access Remote Desktop Server, VPN Server & Web sites.
 - Create a VPN Tunnel from **61.0.0.6** to **202.153.32.120**
 - Access www.Microsoft.com from External network through VPN
 - Access the Remote Desktop server from External network through VPN