TVET CERTIFICATE V in NETWORKING

INSTALLATION, CONFIGURATION AND MANAGEMENT OF WINDOW SERVER

NEWWS501

Install, configure, manage window server

Competence

Credits: 8

Learning hours: 80

Sector: ICT

Sub-sector: NEWORKING

Module Note Issue date: June, 2020

Purpose statement

This module is intended to the learner pursuing TVET certificate V in networking, at the end of this module the learner will be able to Prepare to install a server, Install server Network Operating System, Configure and administer the server, Monitor and test the server and Complete documentation and he or she will be able to work competitively in the ICT world under non directive supervision.

Table of Contents

Elements of competence and performance criteria		**Page No.**
Learning Unit	Performance Criteria	
1. Prepare to install a server	1.1: Proper choice of the most suitable operating system features and network (server) services with reference to required server solution and technical requirements	23
	1.2:Proper revision of required installation options	
	1.3:Appropriate analysis of data migration requirements	
	1.4: Correct backing up of local data in preparation of installation.	
2. Install server NOS	2.1: Proper installation of the network operating system (NOS) and right update of the NOS with all required patches	43
	2.2: Appropriate post-installation and configuration of the server	
3. **Configure and administer the server**	3.1: Right installation and administration of active directory, active directory groups and organizational units (OUs)	74
	3.2: Appropriate deployment and configuration of network services such as IPV4 addressing, DHCP , DNS, PRINT Server service	
	3.3: Adequate configuration of the server roles and features; file and share access services	
4. Monitor and test the server	4.1: Correct test of the services by giving access to customer to match their specification and requirements according to test plan, and record outcomes	21
	4.2: Adequate usage of the troubleshooting tools	

	and techniques to diagnose the correct server issues	
	4.3: Right test of the required changes or additions for customer satisfaction	
	4.4: Proper installation, configuration and maintenance of the antivirus for the proper protection of the systems.	

Total Number of Pages: 165

Learning Unit 1 – Prepare to install a server

LO 1.1 – Choose suitable operating system features and network (server) services

- **Content/Topic 1: Description of Current and common used Windows Servers**

A. Window Server Overview

- ✓ **Windows Server** is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications. Previous versions of Windows Server have focused on stability, security, networking, and various improvements to the file system. Other improvements also have included improvements to deployment technologies, as well as increased hardware support. Microsoft has also created specialized SKUs of Windows Server that focus on the home and small business markets. Windows Server 2012 R2 is the latest release of Windows Server, and focuses on cloud computing.
- ✓ **Server Core** is a minimal server installation option for the Windows Server 2008 R2 operating system. Server Core provides a low-maintenance environment capable of providing core server roles. Server Core is designed to provide an environment that reduces .A **core** is part of a CPU that receives instructions and performs calculations, or actions, based on those instructions.
- ✓ Window server 2019 is the latest version of Microsoft windows server. The current version of window server 2019 improves on the previous window 2016 version in regards with better performance , improved security and excellent optimizations for hybrid integration AppS4Rent compares both the version

B. Window server edition

The Standard edition is designed for small-to-medium-sized organizations. It allows you to run two instances of the server software in a virtual operating system on the licensed server. If you need to run additional virtual instances, you can acquire licenses that are more standard.

The Essentials edition is designed for small organizations with up to 25 users and 50 devices. It allows only one instance of the server software to be run in the physical.

The following table describes the current documented versions of Windows Server.

Window server version	description
Window server2003or 2003R2	Integrates a number of features from Windows XP. Includes improved networking installation and integration, improved web services, and increased capabilities for DTFS
Window server2008 or2008R2	Includes a number of additional security and administrative features shared with Windows Vista: a re-written networking stack, improved Firewall, additional .NET Framework technology, and numerous improvements to the kernel, file, and memory systems
Window server2012 and 2012R2	Emphasizes cloud support with features such as improved IP-addressing, updated Hyper-V, and a new file system (ReFS). Windows Server 2012 R2 includes enhancements to virtualization, management, storage, networking, virtual desktop infrastructure, access protection, information protection, web services, and application platform infrastructure
Window server 2016	It Is the seventh release of window server operating system developed by Microsoft as part of the windows NT family of operating systems. it was developed concurrently with window 10 and is the successor to window server 2012R2.

Window server 2019	It is for the time being the latest version of the server operating system released by Microsoft. Generally available since October 2018, window server 2019 is built on the strong foundation of Microsoft's previous released window server 2016.

Current window server version comparisons (window server2016 Vs 2019)

Features related to hybrid capabilities		
features	**Window server 2016**	**Window server2019**
Hybrid cloud option Both on-premise and cloud solution work together	χ	√
Integrated apps and infrastructure with Azure Backup and fileSyc	√	√
VM protection Replicate workloads running on physical and virtual machine	√	√
Azure network Adapter Connect to Azure virtual networks	√	√
Storage migration service Migrate from legacy system to windows and/ or Azure	χ	√

C. Window Server Roles

These **server roles** are meant to provide services to the clients on the network. Some of these services include Active Directory, File, Print, DNS, DHCP and Web (IIS). The Active Directory can be used to store details about the users on the network, computers, and printers. A few common server roles are listed below:

1. Domain controller.

2. Database server.
3. Backup server.
4. File server.
5. Print server.
6. Infrastructure server.
7. Web server.
8. E-mail server.

D. Window server role services

Active Directory (AD) manages authentication of users and devices on the network, enforces security policies assigned to those users and devices, and allows for management and administration of the network. Many other services and applications are dependent on AD. Because of the critical and foundational nature of AD, organizations tend to set up redundant domain controllers (the name for servers running the AD role) in case one goes down.

- **Active Directory Rights Management Server**: is a Microsoft Windows security tool that provides persistent data protection by enforcing data access policies. The server component is made up of multiple web services that run on a Microsoft server.
- **Remote Desktop Services Connection Broker**: A remote desktop connection broker is software that allows clients to access various types of server-hosted desktops and applications.
- **Windows Server Update Server (WSUS):** is a free add-on application offered by Microsoft that can download and manage updates and patches for Windows Server operating systems. It is the successor of the previous Software Update Services (SUS) program.
- **DHCP server** (Dynamic Host Configuration Protocol) Server is a role in Windows Server that leases IP addresses to devices that want to connect to the network. While many organizations use Windows Server as a DHCP server, some organizations prefer to let their firewall, network switch, or all-in-one router handle DHCP.
- **DNS server** The DNS (Dynamic Name System) role helps translate a human-readable web address that looks like www.microsoft.com into an IP address a machine can

resolve, such as 131.107.0.89. DNS is important because it is one of the industry standards that allow people to browse the internet, and it plays a role in filtering out malicious websites.

- **File and Storage services** The File and Storage services role provides services that allow users to store and share files on a given network. Permissions on shares can be configured to allow only certain groups or individuals to access or modify files.
- **Hyper-V** The Hyper-V role in Windows Server provides a virtualization platform that allows organizations to run many virtual machines on a single physical computer in order to more efficiently utilize resources and isolate workloads.
- **Virtualization:** means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.
- **Print and document services** Print and Document Services is a Windows Server role that provides centralized management of and access to networked printers, so that everyone on the network with the right permissions can connect to these devices.
- **Web Server** Internet Information Server (IIS): is an extensible web server created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP.
- **Windows Server Update Server (WSUS):** is a free add-on application offered by Microsoft that can download and manage updates and patches for Windows Server operating systems. It is the successor of the previous Software Update Services (SUS) program.
- **Streaming Media Services:** is transmitted by a server application and received and displayed in real-time by a client application called a media player.

E. Windows Server Features

A feature is something that helps a server performs its primary duty (Windows Backup, network load balancing).

Microsoft Windows Features on Demand is a feature that allows system to add or remove roles and features in Windows 8 and Windows Server 2012, and later versions of the client and server operating system to alter the file size of those operating systems.

- ✓ **Microsoft .NET Framework 3.5:** NET is a programming framework created by Microsoft that developers can use to create applications more easily. So nobody

besides developers would need a package like .NET, which provides applications with an orderly way to access databases, web services, and other communication tools.

- ✓ **Windows PowerShell:** Windows PowerShell is a Windows command-line shell designed especially for system administrators. Windows PowerShell includes an interactive prompt and a scripting environment that can be used independently or in combination.
- ✓ **Background Intelligent Transfer Service (BITS):** is a component of Microsoft Windows XP and later iterations of the operating systems, which facilitates asynchronous, prioritized, and throttled transfer of files between machines using idle network bandwidth. **Some examples of window server features include:**

1. .NET Framework 3.5 Features
2. .NET Framework 3.5 (includes .NET 2.0 and 3.0)
3. HTTP Activation
4. Non-HTTP Activation
5. .NET Framework 4.6 Features
6. .NET Framework 4.6
7. ASP.NET 4.6
8. WCF Services
9. HTTP Activation
10. Message Queuing (MSMQ) Activation
11. Named Pipe Activation
12. TCP Activation
13. TCP Port Sharing
14. Background Intelligent Transfer Service (BITS)
15. Compact Server

F. RAID configuration

RAID is a technology that is used to increase the performance and/or reliability of data storage. The abbreviation stands for either Redundant Array of Inexpensive Disks or Redundant Array of Independent Drives. A **RAID** system consists of two or more drives working in parallel.

A RAID system consists of two or more drives working in parallel. These can be hard discs, but there is a trend to also use the technology for SSD (Solid State Drives). There are different RAID levels, each optimized for a specific situation. These are not standardized by an industry group or standardization committee. This explains why companies sometimes come up with their own unique numbers and implementations. This article covers the following RAID levels:

RAID 0 Striping

RAID 1 mirroring

RAID 5 Striping with parity

RAID 6 Striping with double parity

RAID 10 combining mirroring and striping

Enable RAID, use one of the following methods, depending on your board model.

Go to Configuration > SATA Drives, set Chipset SATA Mode to RAID.

Go to Advanced > Drive Configuration, set Configure SATA As to RAID.

Go to Advanced > Drive Configuration, set Drive Mode to Enhanced and set the RAID option to Enabled.

G. Features on Demand

Features on Demand (FODs) are Windows **features** that can be added at any time. Common **features** include language resources like handwriting recognition or other **features** like the. NET Framework (When Windows 10 or Windows Server needs a new **feature**, it can request the **feature** package from Windows Update.

H. Definition of server core

Server Core is a minimal installation option introduced in Windows Server 2008 as a way to run Windows Server with a limited set of features and with support for only certain server roles.

The Server Core installation option is available in the Standard, Enterprise and Datacenter editions of Windows Server 2008.

LO 1.2 – Revise required installation options

- **Content/Topic 1: Revising the Current and common used Windows Servers**

A. Window Server Overview

Windows Server is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications. Previous versions of Windows Server have focused on stability, security, networking, and various improvements to the file system. Other improvements also have included improvements to deployment technologies, as well as increased hardware support. Microsoft has also created specialized SKUs of Windows Server that focus on the home and small business markets. Windows Server 2012 R2 is the latest release of Windows Server, and focuses on cloud computing.

B. Definition of server core

Server Core is a minimal installation option introduced in Windows Server 2008 as a way to run Windows Server with a limited set of features and with support for only certain server roles.

The Server Core installation option is available in the Standard, Enterprise and Datacenter editions of Windows Server 2008.

1. Window server edition

- ✓ **The Standard edition** is designed for small-to-medium-sized organizations. It allows you to run two instances of the server software in a virtual operating system on the licensed server. If you need to run additional virtual instances, you can acquire licenses that are more standard.
- ✓ **The Essentials edition** is designed for small organizations with up to 25 users and 50 devices. It allows only one instance of the server software to be run in the physical.
- ✓ **The following table describes the current documented versions of Windows Server.**

Window server version	description
Window server2003or 2003R2	Integrates a number of features from Windows XP. Includes improved networking installation and integration, improved web services, and increased capabilities for DTFS

Window server2008 or2008R2	Includes a number of additional security and administrative features shared with Windows Vista: a re-written networking stack, improved Firewall, additional .NET Framework technology, and numerous improvements to the kernel, file, and memory systems
Window server2012 and 2012R2	Emphasizes cloud support with features such as improved IP-addressing, updated Hyper-V, and a new file system (ReFS). Windows Server 2012 R2 includes enhancements to virtualization, management, storage, networking, virtual desktop infrastructure, access protection, information protection, web services, and application platform infrastructure
Window server 2016	It Is the seventh release of window server operating system developed by Microsoft as part of the windows NT family of operating systems. it was developed concurrently with window 10 and is the successor to window server 2012R2.
Window server 2019	It is for the time being the latest version of the server operating system released by Microsoft. Generally available since October 2018, window server 2019 is built on the strong foundation of Microsoft's previous released window server 2016.

2. Current window server:

- ✓ Window server 2019 is the latest version of Microsoft windows server. The current version of window server 2019 improves on the previous window 2016 version in regards with better performance , improved security and excellent optimizations for hybrid integration AppS4Rent compares both the version.
- ✓ **Current window server version comparisons (window server2016 Vs 2019)**

Features related to hybrid capabilities		
features	**Window server 2016**	**Window server2019**
Hybrid cloud option	**X**	**√**

Both on-premise and cloud solution work together		
Integrated apps and infrastructure with Azure Backup and fileSyc	√	√
VM protection Replicate workloads running on physical and virtual machine	√	√
Azure network Adapter Connect to Azure virtual networks	√	√
Storage migration service Migrate from legacy system to windows and/ or Azure	χ	√

3. Window Server Roles

These **server roles** are meant to provide services to the clients on the network. Some of these services include Active Directory, File, Print, DNS, DHCP and Web (IIS). The Active Directory can be used to store details about the users on the network, computers, and printers. A few common server roles are listed below:

1. Domain controller.
2. Database server.
3. Backup server.
4. File server.
5. Print server.
6. Infrastructure server.
7. Web server.
8. E-mail server.

- Content/Topic 2: Explanation of Window server role services

There are several window server role services, each with a specific purpose. With explanation, the following may be noted:

- ✓ **Active Directory (AD)** manages authentication of users and devices on the network, enforces security policies assigned to those users and devices, and allows for management and administration of the network. Many other services and applications are dependent on AD. Because of the critical and foundational nature of AD, organizations tend to set up redundant domain controllers (the name for servers running the AD role) in case one goes down.
- ✓ **Active Directory Rights Management Server**: is a Microsoft Windows security tool that provides persistent data protection by enforcing data access policies. The server component is made up of multiple web services that run on a Microsoft server.
- ✓ **Remote Desktop Services Connection Broker**: A remote desktop connection broker is software that allows clients to access various types of server-hosted desktops and applications.
- ✓ **Windows Server Update Server (WSUS):** is a free add-on application offered by Microsoft that can download and manage updates and patches for Windows Server operating systems. It is the successor of the previous Software Update Services (SUS) program.
- ✓ **DHCP server** (Dynamic Host Configuration Protocol) Server is a role in Windows Server that leases IP addresses to devices that want to connect to the network. While many organizations use Windows Server as a DHCP server, some organizations prefer to let their firewall, network switch, or all-in-one router handle DHCP.
- ✓ **DNS server** The DNS (Dynamic Name System) role helps translate a human-readable web address that looks like www.microsoft.com into an IP address a machine can resolve, such as 131.107.0.89. DNS is important because it is one of the industry standards that allow people to browse the internet, and it plays a role in filtering out malicious websites.
- ✓ **File and Storage services** The File and Storage services role provides services that allow users to store and share files on a given network. Permissions on shares can be configured to allow only certain groups or individuals to access or modify files.

- ✓ **Hyper-V** The Hyper-V role in Windows Server provides a virtualization platform that allows organizations to run many virtual machines on a single physical computer in order to more efficiently utilize resources and isolate workloads.
- ✓ **Virtualization:** means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.
- ✓ **Print and document services** Print and Document Services is a Windows Server role that provides centralized management of and access to networked printers, so that everyone on the network with the right permissions can connect to these devices.
- ✓ **Web Server** Internet Information Server (IIS): is an extensible web server created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP.
- ✓ **Windows Server Update Server (WSUS):** is a free add-on application offered by Microsoft that can download and manage updates and patches for Windows Server operating systems. It is the successor of the previous Software Update Services (SUS) program.
- ✓ **Streaming Media Services:** is transmitted by a server application and received and displayed in real-time by a client application called a media player.

- Content/Topic 3: Description of Windows Server Features

A. Window server features

A feature is something that helps a server performs its primary duty (Windows Backup, network load balancing).

Microsoft Windows Features on Demand is a feature that allows system to add or remove roles and features in Windows 8 and Windows Server 2012, and later versions of the client and server operating system to alter the file size of those operating systems.

Microsoft .NET Framework 3.5: NET is a programming framework created by Microsoft that developers can use to create applications more easily. So nobody besides developers would need a package like .NET, which provides applications with an orderly way to access databases, web services, and other communication tools.

Windows PowerShell: Windows PowerShell is a Windows command-line shell designed especially for system administrators. Windows PowerShell includes an interactive prompt and a scripting environment that can be used independently or in combination.

Background Intelligent Transfer Service (BITS): is a component of Microsoft Windows XP and later iterations of the operating systems, which facilitates asynchronous, prioritized, and throttled transfer of files between machines using idle network bandwidth.

B. Features on Demand

Features on Demand (FODs) are Windows **features** that can be added at any time. Common **features** include language resources like handwriting recognition or other **features** like the. NET Framework (When Windows 10 or Windows Server needs a new **feature**, it can request the **feature** package from Windows Update.

Examples of window server features include:

1) .NET Framework 3.5 Features
2) .NET Framework 3.5 (includes .NET 2.0 and 3.0)
3) HTTP Activation
4) Non-HTTP Activation
5) .NET Framework 4.6 Features
6) .NET Framework 4.6
7) ASP.NET 4.6
8) WCF Services
9) HTTP Activation
10) Message Queuing (MSMQ) Activation
11) Named Pipe Activation
12) TCP Activation
13) TCP Port Sharing
14) Background Intelligent Transfer Service (BITS)
15) Compact Server

C. Configuration of RAID

❖ **RAID Definition**

RAID is a technology that is used to increase the performance and/or reliability of data storage. The abbreviation stands for either Redundant Array of Inexpensive Disks or Redundant Array of Independent Drives. A **RAID** system consists of two or more drives working in parallel.

A RAID system consists of two or more drives working in parallel. These can be hard discs, but there is a trend to also use the technology for SSD (Solid State Drives). There are different RAID levels, each optimized for a specific situation. These are not standardized by an industry group or standardization committee. This explains why companies sometimes come up with their own unique numbers and implementations. This article covers the following RAID levels:

RAID 0 Striping

RAID 1 mirroring

RAID 5 Striping with parity

RAID 6 Striping with double parity

RAID 10 combining mirroring and striping

- **To enable RAID, use one of the following methods, depending on your board model.**

Go to Configuration > SATA Drives, set Chipset SATA Mode to RAID.

Go to Advanced > Drive Configuration, set Configure SATA As to RAID.

Go to Advanced > Drive Configuration, set Drive Mode to Enhanced and set the RAID option to Enabled.

LO 1.3 Learning Outcome 1.3: Analyze data migration requirements

- Content/Topic 1: Analysis of Data migration requirements

Data migration is the process of transporting data between computers, storage devices or formats. It is a key consideration for any system implementation, upgrade or consolidation.

After you have verified your source server meets the Requirements, verify that your target server meets the requirements below for data migration.

- **Operating system**—Your existing physical or virtual target server can have any of the following Windows operating system editions. Windows Server 2008 or 2008 R2 Datacenter, Enterprise (i3 86, x64), Standard (i3 86, x64), Essential Business Server, Web Server, Foundation Server, Small Business Server, or Storage Server Edition.

Windows Server 2003 or 2003 R2 Datacenter, Enterprise (i386, x64), Standard (i386, x64), Web Server, Small Business Server, or Storage Server Edition. Each of the Windows 2003 operating systems requires Service Pack 1 or later.

- **System memory**—The minimum system memory on each server should be 1 GB. The recommended amount for each server is 2 GB.
- **Disk space for program files**—This is the amount of disk space needed for the Double-Take program files. For Windows 2003, this is approximately 300 MB. For Windows 2008, this is approximately 375 MB.The program files can be installed to any volume while the Microsoft Windows Installer files are automatically installed to the operating system boot volume. Make sure you have additional disk space for Double-Take queuing, logging, and so on.
- **Disk space for data files**—this is the amount of disk space needed for the source data files. This will be dependent on the applications you are running and the amount of data files you have.
- **Server name**—Double-Take includes Unicode file system support, but your server name must still be in ASCII format. If you have the need to use a server's fully-qualified domain name, your server cannot start with a numeric character because that will be interpreted as an IP address.
- **Protocols and networking**—your servers must meet the following protocol and networking requirements.

Your servers must have TCP/IP with static IP addressing. (Some job types allow you to add DHCP addresses for failover monitoring, although only after a job has already been created. Keep in mind that depending on your failover configuration, a source reboot May or may not cause a failover but having a new address assigned by DHCP may also cause a failover.)

By default, Double-Take is configured for IPv6 and IPv4 environments, but the Double-Take service will automatically check the server at service start-up and modify the appropriate setting if the server is only configured for IPv4. If you later add IPv6, you will need to manually modify the Default Protocol server setting. See Server and job settings for details.

- IPv6 is only supported for Windows 2008 servers.
- If you are using IPv6 on your servers, your clients must be run from an IPv6 capable machine.
- In order to properly resolve IPv6 addresses to a hostname, a reverse lookup entry should be made in DNS.

- **Microsoft .NET Framework**—Microsoft .NET Framework version 3.5 Service Pack 1 is required. This version is not included in the .NET version 4.0 release. Therefore, even if you have .NET version 4.0 installed, you will also need version 3.5.1. You can install this version from the Double-Take CD, via a web connection during the Double-Take installation, or from a copy you have obtained manually from the Microsoft web site.
- **Cloud**—Double-Take can be used to migrate data to an existing server in the cloud. Keep in mind that you should enable appropriate security measures, like VPN, to protect your data as it migrates to the cloud.
- **Supported configurations**—the following table identifies the supported configurations for a data migration job.
- **Data migration Job**: data migration is commonly described as the process of moving data from one location to another. That of cause is a wildly simplified summary of the job, and the work of data migration specialist goes well beyond this primary function.
- **Managing and controlling data migration jobs**: to manage or control data migration job flow the following keys steps in a data migration:

1. Explore and assess the solution. Before **migrating** data. You must know(and understand) what you are migrating as well as how it fits within the target system.
2. Define and design the migration
3. Build the migration solution
4. Conduct a live test
5. Flipping the switch
6. Audit

- **Cutting over data migration job:** the cutover process is the final step in completing your data migration. It involves multiple steps and should be a highly orchestrated event also considers how you intend to destroy data on the old storage array before it is removed from the data center.
- **Data migration process steps:** the data migration process steps are:
  - plan the strategy
  - work with your end user
  - audit the data and fixe any Issue
  - backup the source data before you move it
  - final test and shutdown

LO 1.4 Back up local data in preparation for installation

- Content/Topic 1: Description of Windows Server Backup

A. Overview of Window Server Backup

Windows Server Backup **(WSB**) is a feature that provides backup and recovery option for windows server environments. Administrators can use windows server backup to back up a full server, the system state, selected storage volumes or specific files or folders, as long as the data volume is less than 2 terabytes.

The most common backup types are a full backup, incremental backup and differential backup. Other backup types include synthetic full backups and mirroring. In the debate over cloud VS local backup, there are some types of backup that are better in certain locations. If you are performing cloud backup, incremental backups are generally a better fit because they consume fewer resources. You might start out with full backup in the cloud and then shift to incremental backup, though, is typically more of on-premises approach and often involved disk.

B. Checklist Schedule Automatic Backups.

You can use the Backup Schedule Wizard in Windows Server Backup to schedule backups that run automatically once or more per day.

An automatic backup will make backing up your information much easier. It eliminates human error. You can schedule automatic backups of the data on your company's computers. This can be done with both an external hard drive and an offsite server.

You can save scheduled backups to one or more attached disks (either internal or external)—or, new in Windows Server 2008 R2, you can save a scheduled backup to a volume or a remote shared folder. If you use disks, they must be available and online for the schedule to be configured and for you to complete the wizard. However, later when you start running scheduled backups, if you are using multiple disks, we recommend that you only connect one at a time so that backups will keep being saved to the same disk. Then, when you want to move that set of backups offsite, attach another disk in the series.

C. Checklist: Perform a Manual Backup

You can use the Backup Once Wizard in Windows Server Backup to create single backups of your computer. You can also create one-time backups using the **Wbadmin start backup** or **Wbadmin start systemstatebackup** commands or the Windows PowerShell cmdlets for Windows Server Backup.

D. Checklist: Recover Files, Folders, Applications, Volumes, or the Operating System

You can use the following tools to perform recovery tasks:

Recovery Wizard in Windows Server Backup: This wizard helps you recover files and folders, applications, volumes, and the system state.

Catalog Recovery Wizard in Windows Server Backup: This wizard helps you recover the backup catalog, a file that stores details about your backups. This wizard is only available if your backup catalog has become corrupted.

Windows Recovery Environment and a backup created with Windows Server Backup.

Windows Recovery Environment can be accessed from a computer running Windows Server 2008 R2 or a Windows Setup disc. This method helps you recover your operating system or full server.

Backup and recovery describes the process of creating and storing copies of data that can be used to protect organizations against data loss. This is sometimes referred to as *operational recovery*. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data. A proper backup copy is stored in a separate system or medium, such as tape, from the primary data to protect against the possibility of data loss due to primary hardware or software failure.

E. Installation of Windows Server Backup Tools

To access backup and recovery tools, you must install the **Windows Server Backup Features** and subordinate items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

Windows Server Backup Microsoft Management Console (MMC) snap-in

Wbadmin command-line tool

Windows PowerShell cmdlets for Windows Server Backup

❖ **Install the Windows Server Backup feature on Server, perform the following steps:**

1. Log in to Server and open Server Manager.
2. Click Manage → Roles and Features.
3. Click Next when the Add Roles and Features Wizard appears.
4. Click Next on the Select installation type screen.
5. Click Next on the Select destination server screen.
6. Click Next on the Select server roles screen.
7. Select Windows Server Backup and click Next.
8. Select Restart the destination server automatically if required and click Yes to allow automatic restarts.
9. Click Install and then click Close.

After the installation completes, you can launch the Windows Server Backup Microsoft Management Console (MMC) snap-in by selecting Server Manager → Tools → Windows Server Backup.

To view the list of commands supported by the wbadmin command-line tool, open a command prompt while logged on with administrative rights and use the following command:

wbadmin /?

To view the Windows PowerShell cmdlets available for Windows Server Backup module, use the following command from within Windows PowerShell:

PS C:\ Get-Command -Module WindowsServerBackup -CommandType Cmdlet

Install Windows Server Backup Features on a Server Core Using Windows PowerShell.

To install the Windows Server Backup features on a Server Core installation, perform the following steps:

1. Log in to the Server Core installation.

Enter the following command from within the command window that appears and then press enter to start a windows PowerShell session.

PS C:\Import-Module Servermanager

Enter the following command to add the Windows Server Backup feature:

PS C:\Install-WindowsFeature Windows-Server-Backup

Enter the following command to confirm the Windows Server Backup feature is installed:

PS C:\Get-WindowsFeature | where {$_.Name -eq "Windows-Server-Backup"}

2. Type Exit to end the Windows PowerShell session and return to the command window.
3. Type wbadmin /? and confirm wbadmin tools are installed.

F. Backing Up Your Server

You can use Windows Server Backup to protect your operating system, system state, volumes, files, and application data. Backups can be saved to single or multiple disks, single or multiple volumes, DVDs, removable media, or remote shared folders. They can be scheduled to run automatically or manually.

Backing Up the Server Windows Server 2003 includes a great backup tool (ntbackup.exe) to back up and archive user data and also the entire operating system and disk volumes. You can use Windows Server 2003 Backup tool (ntbackup.exe) to back up and restore both Windows Server 2003 and and also Exchange 2003 data. Windows Server 2003 Backup tool (ntbackup.exe) can be used to backup directories, selected files, and System State data, including Windows Server 2003 operating system registry information. Windows Server 2003 Backup is included on all the different versions of Windows 2003 family Operating Systems.

G. Recovering Your Server

you can use the backups you have created with Windows Server Backup to recover your operating system, system state, volumes, applications and application data, backup catalog, and In the **Add Features Wizard**, on the **Select Features** page, expand **Windows Server Backup Features**, and then select the check boxes for **Windows Server Backup** and **Command-line Tools**.

H. Optimizing of Backup and Server Performance

You can use the Optimize Backup Performance dialog box to improve the performance of backups for full volumes, which can improve server performance. It is available from the homepage of the Windows Server Backup snap-in. However, these settings apply only if you are including entire volumes in the backup. The performance settings will not be applied if you specify a file or folder backup (in this case, backups will be created using the file backup engine and these settings will not be applied.)

To adjust performance settings for Windows Server Backup

Click **Start**, click **Administrative Tools**, and then click **Windows Server Backup**.

In the **Actions** pane of the snap-in default page, under **Windows Server Backup**, click **Configure Performance Settings**. This opens the **Optimize Backup Performance** dialog box.

In the **Optimize Backup Performance** dialog box, do one of the following:

Click **Normal backup performance**. Choose this option to specify that the backups you create are full backups. During a backup operation, Windows transfers all the contents of the volume being backed up, but the space used on the backup storage location is only for the changed blocks on the source.

Click **Faster backup performance**. Choose this option to specify that the backups that you create are incremental backups. Windows will leave a shadow copy on the source volume to use to track the changes.

During next backup operation, only the changes since last the backup are transferred (by reading from the “diff area” of the shadow copy)—as compared to the **Normal backup performance** option, where the entire source volume data is transferred. (Because only

I. Testing of backup Using Cmd

You can use the Windows PowerShell cmdlets for Windows Server Backup to automate and manage backups. Before you begin, you must install the cmdlets as part of installing Windows Server Backup. (For instructions, see Install Windows Server Backup Tools.) Then, each time you use the cmdlets, you must add the Windows Server Backup cmdlet snap-in to the instance of Windows PowerShell that you have opened. changed blocks are written, there is a performance increase.) The space used on the backup storage location will still only be for the changed blocks detected on the source. Use this method for servers that are less I/O intensive because shadow copies can degrade the performance of write operations for the volume they are on (read operations are not affected).

J. Resources for Backup and Recovery

The need for a backup software solution cannot be stated enough, because of the risk of losing all your files, photos, music, and other important documents to an accident or computer crash.

✓ **Backing up option**

- There are many different options available for backing up. This might include copying files and folders to a rewritable CD or DVD, USB drive, or external harddrive, or even using a cloud backup solution so you can access and sync your files and folders between different devices.
- While it's great if you're using even one method, it's even more ideal if you're using multiple backup methods to provide a real and practical degree of redundancy. However, doing so might make it more difficult to manage your backups.

✓ **Backup hardware include:**

1. **CD or DVD**
2. **USB Flash Disk**
3. **External hard drive**

✓ **Server Backup software**

This is where backup software really comes into it's own, as it allows you to more easily manage and automate backing up tasks, allowing you to just let everything run and save in the background while you're working.

Server backup software is used to ensure the information stored or processed via server hardware remain intact in case of mechanical failure or errors. These solutions store the information processed by server in a remote location or a remote cloud, or some other on0promises hardware device. Companies use server backup software to prevent data loss in disaster scenarios as well as to ensure their business data or customer business data remains available.

Server backup software includes:

- EaseUS Todo Backup Free
- Veeam
- Acronis cyber backup
- Acronis cyber backup cloud for service provider
- Solarwinds backup

K. User Interface: Windows Server Backup

The Windows Server Backup Microsoft Management Console (MMC) snap-in contains the following wizards to help you schedule and create backups, and perform recoveries:

- Backup Schedule Wizard
- Backup Once Wizard Recovery Wizard
- Catalog Recovery Wizard

Learning Unit 2 Install server Network Operating System

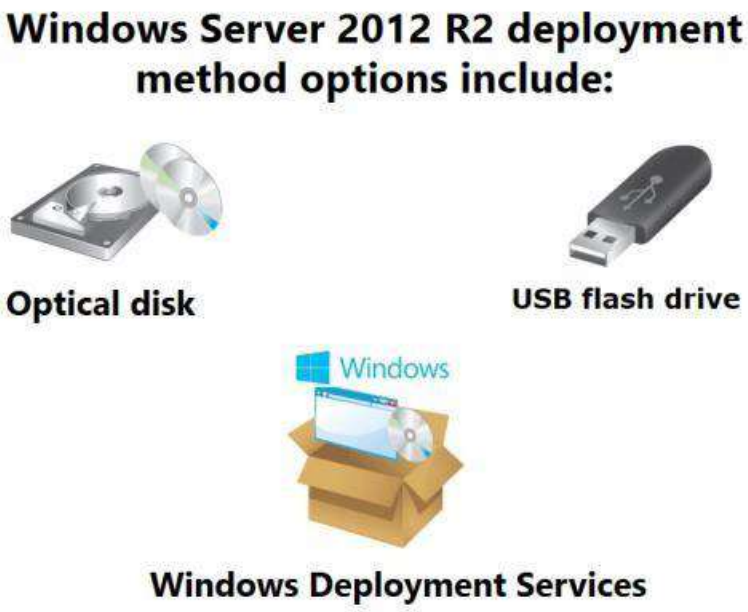
LO 2.1Install the network operating system (NOS) and update the NOS with all required patches

- **Content/Topic 1: Installation of Window Server2012R2**

A. Installation Methods

Microsoft distributes Windows Server 2012R2 on optical media and in an .iso (ISO) image format. ISO format is becoming more common as organizations acquire software over the Internet rather than by obtaining physical removable media. Once you have obtained the Windows Server 2012 operating system from Microsoft, you can use your own method to deploy the operating system. You can install Windows Server 2012 by using a variety of methods, including the following:

1. Optic media Install window server setup from storage media such as CD, DVD.
2. USB flash Disk(boot from)
3. Install window server from internet this method require internet(boot from internet)



B. Installation Types

Three different types of installation can be carried out for Windows XP Professional. The type of installation chosen can affect various stages of the installation process. The three types are as follows:

Clean installation: one where there is no existing operating system on the computer or you do not want to preserve the existing installation. The biggest advantage of a clean installation knows that nothing remains from a previous installation, leading to improved performance and stability. However, you will need to reinstall all of your applications and reconfigure your Windows settings.

Upgrade installation: one in which Windows server is installed over a previous version of Windows. The biggest advantage of an upgrade is that you can retain application installations and user settings. However, this can also be a disadvantage if you would be better off without these applications and settings.

Multiple boot installation: one in which several operating systems are installed on the same computer and the user can choose which operating system to boot during system startup.

Migration: migration means moving from your existing operating system to window server 2012R2 by transfering to different set of hardware.

Choosing Whether to Upgrade or Migrate

A new version of a software or hardware product designed to replace an older version of the same product. Typically, software companies sell upgrades at a discount to prevent

users from switching to other products. In most cases, you must prove you own an older version of the product to qualify for the upgrade price.

System migration is a method of installing a system at a different version that is different from its current version.

Server migration is a technique in which data is positioned from one server to another. The reasons behind server migration are security concerns, equipment is being replaced and many other factors.

C. Hardware Requirements for Windows Server 2012R2

The following are estimated system requirements for the window server 2012R2. If your computer has less than the “minimum” requirements, you will not be able to install this product correctly. Actually requirements will vary based on your system configuration and the application, features your install.

Criteria	2012r2	
	Minimum	Recommended
CPU	1.4 GHz 64bit	2 GHz or faster
RAM	512 MB	2 GB or greater
Available disk space	32GB	40 GB or greater
Optical Driver	DVD-ROM drive	DVD-ROM drive

Other requirements

you also must have the following:

Gigabit(10/100/1000 baseT) Ethernet adapter

DVD Drive(if entend to install the operating system from DVD media).

A. Installation of Windows Server 2012 R2 steps

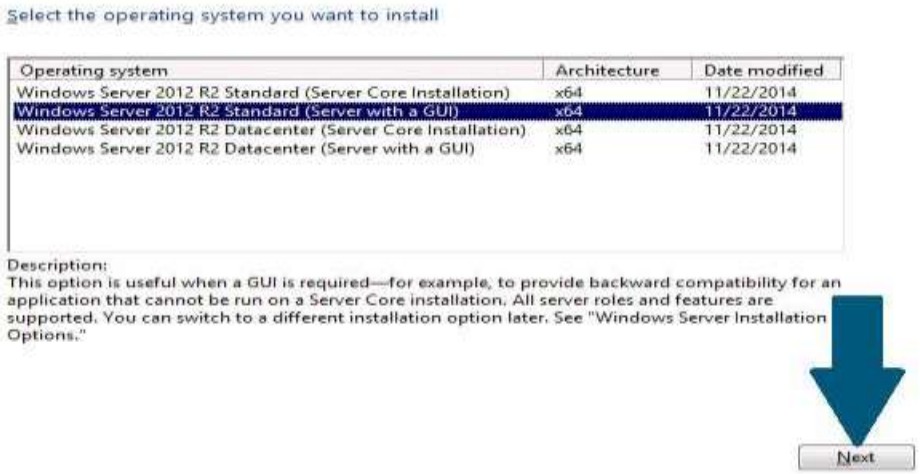
Step 1: Insert a DVD of Windows Server 2012 R2 into your system and start it. Once you get a message

"Press any key to boot from CD or DVD..", press an **Enter** key

Step 2: Choose the language, time and currency format, keyboard or input method and click **next.**

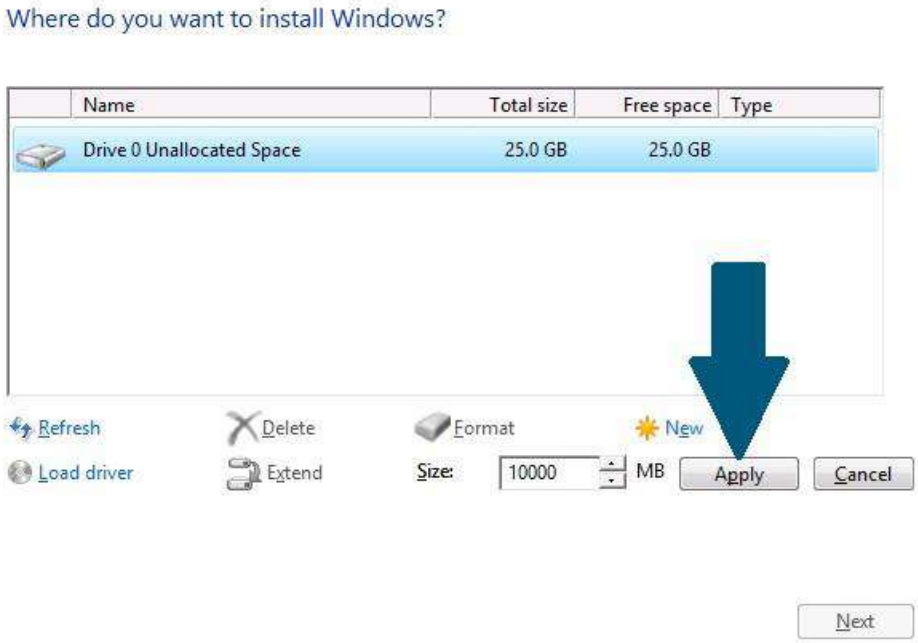
Step 3: Click **Install now**

Step 4: Choose the operating system you want to install and click **Next**



Step 5: Click **Custom: Install Windows only (advanced)**

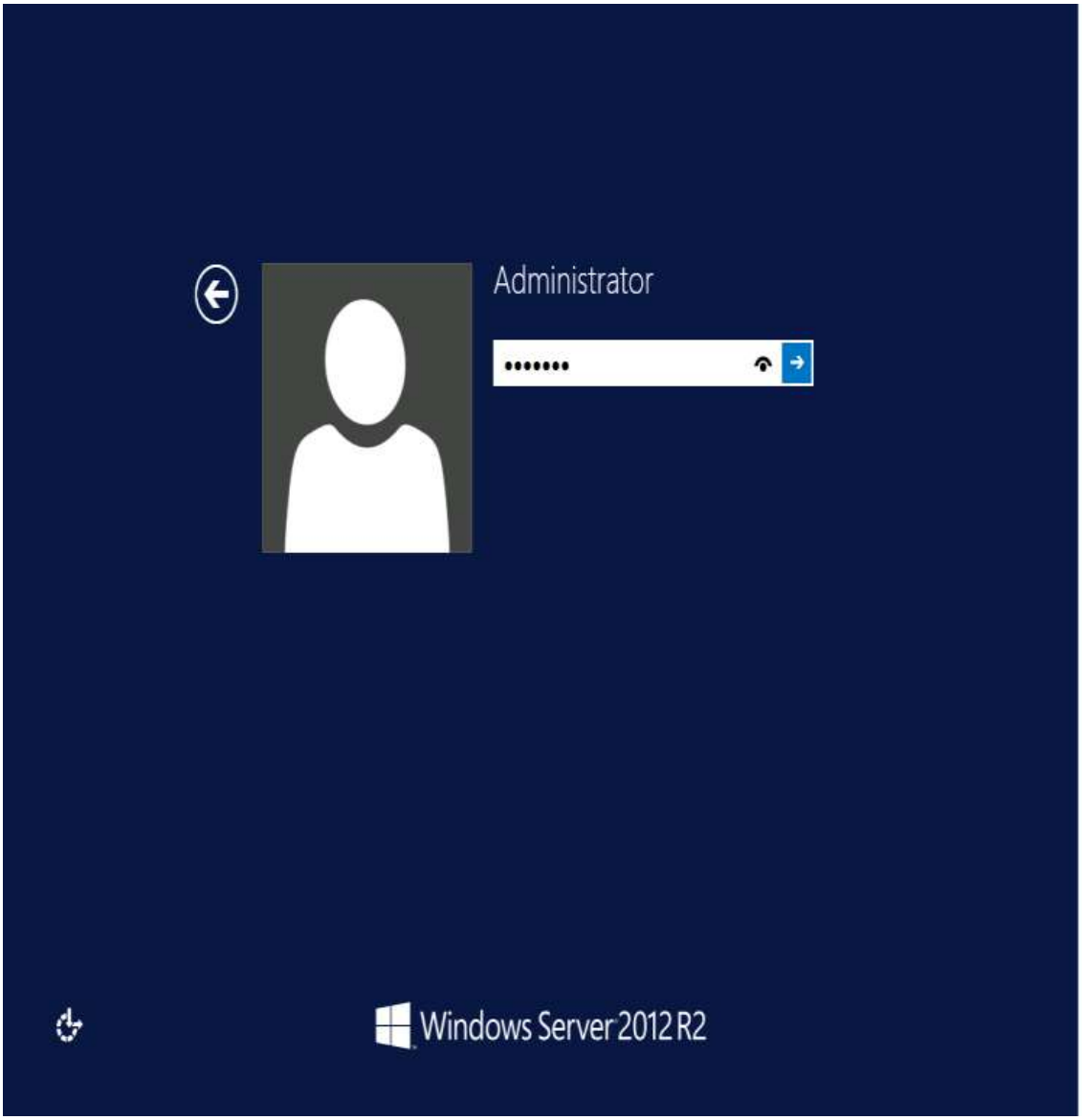
Step 6: Click **new** to partition the hard disk and provide size in MB for this drive, **delete** for delete exiting partition and click **format** to format partition. When done, click Apply



Step 7: Choose the drive other than Primary and click **Next.** Sit back and relax while Installation takes a moment

Step 8: Upon reboot, provide an administrative password and click **Finish**

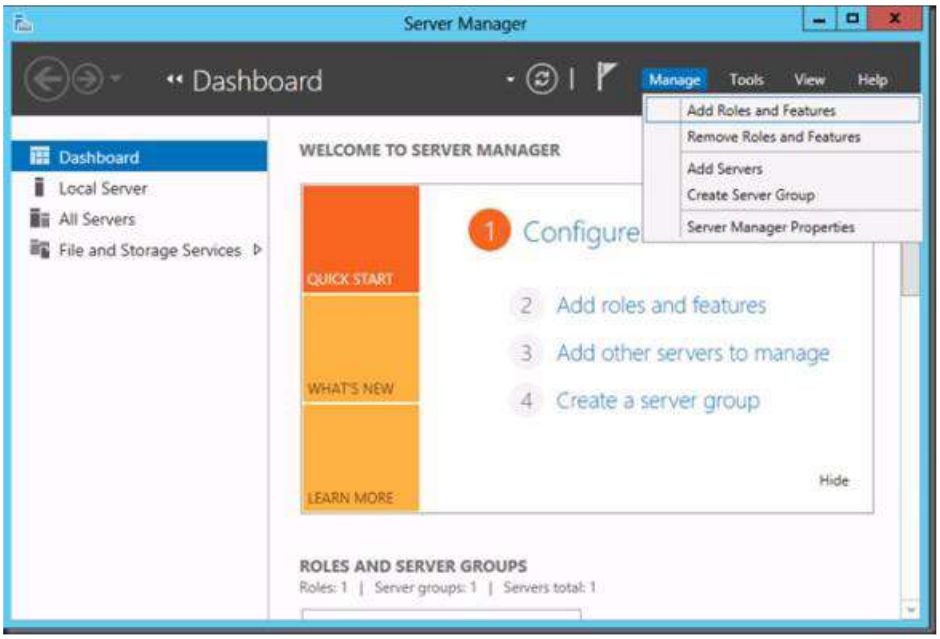
Step 9: Login with your current password and start enjoying Windows Server 2012 R2 by press Alt+Ctr+Del



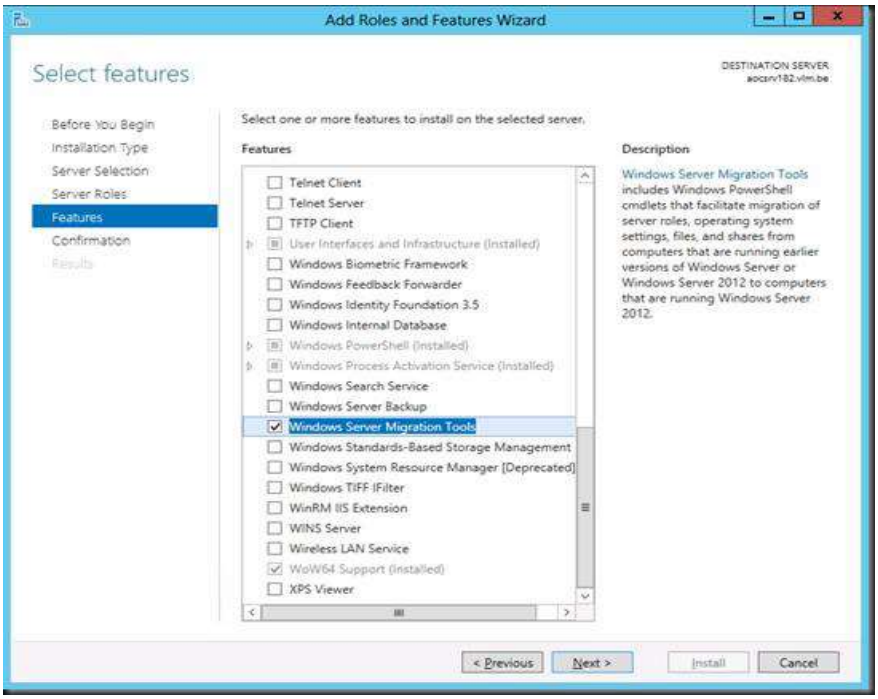
- **Content/Topic 2: Installation of Windows Server2012R2 Migration Tools**

Installing the Windows Server Migration Tools on the DESTINATION Server

First we have to install the on the DESTINATION host (W2K12 in our case, the server to which you are migrating)). For this we launch Server Manager and on the dashboard select Manage and choose Add Roles & Feature.

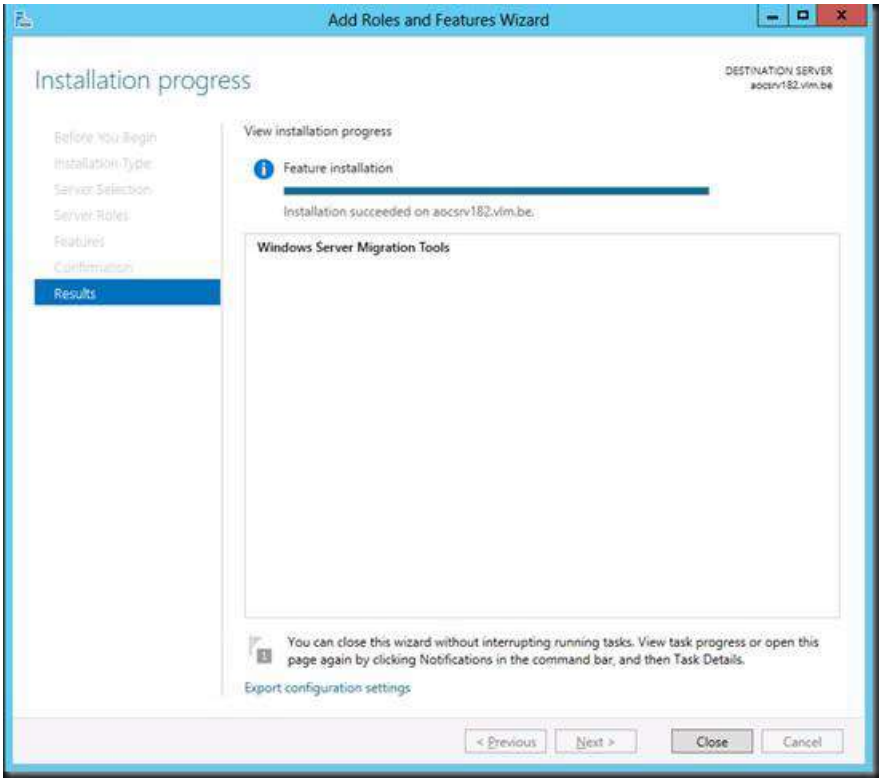


Navigate through the wizard until you get to Features. Find and select Windows Server Migration Tools.



Choose window server migration tools then Click Next.

Click Install to kick of the installation.



Click close

- ✓ **<u>Installation of Windows Server Migration Tools on the SOURCE *Server*</u>**

Data migration is simply the process of moving data from a source system to a target system. Companies have many different reasons for migrating data.

You may want to migrate data when you acquire another company and you need to integrate that company's data.

There are three primary types of data migration tools to consider when migrating your data:

On-premise tools: Designed to migrate data within the network of a large or medium Enterprise installation. **Open Source tools:** Community-supported and developed data migration tools that can be free or very low cost.

Cloud-based tools: Designed to move data to the cloud from various sources and streams, including on- premise and cloud-based data stores, applications, services, etc.

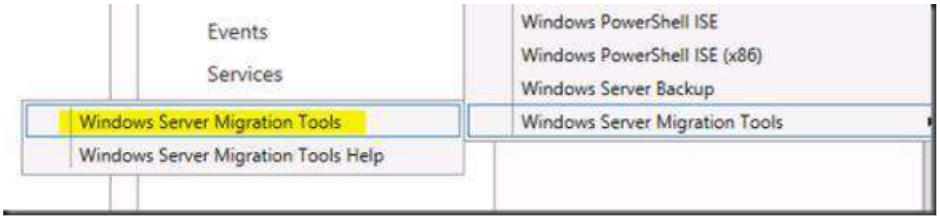
How to select a data migration tool

Selecting the right data migration tool depends largely on your needs. There are many excellent data migration tools, but they won't help if they don't meet your company's particular goals. Here are a few questions to help you choose the right tool for you.

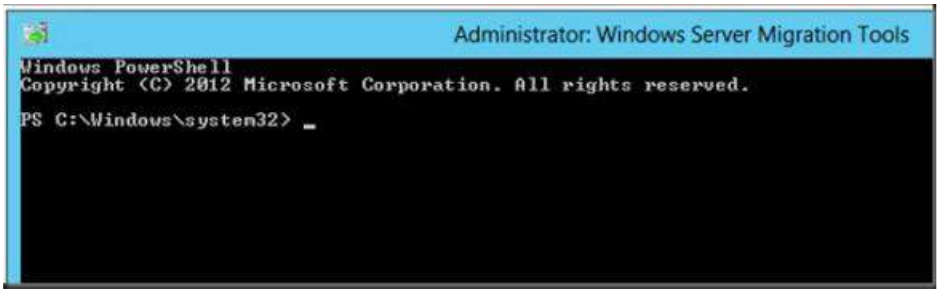
- ✓ **Location**. Do you want to migrate data on-premise (in the same environment)? Or, do you want to move data from on-premise to the cloud? Or from one cloud store to another cloud store? This will help you determine which group of tools to consider.
- ✓ **Cost**. Is cost-effectiveness a priority? Using open source tools can be free or significantly cheaper than commercial solutions, assuming you have the right expertise in place. Using a cloud-based data migration tool can save you significantly on infrastructure and manpower costs, freeing up resources for other projects.
- ✓ **Data model**. Do you need to change your data model? You may be moving from an on-premise data warehouse to a cloud-based data warehouse, or you may move from relational data to a mix of structured and unstructured data. Cloud-based data migration tools tend to support the widest variety of data models, whereas on-premise tools tend to be the least flexible.
- ✓ **Data transformation**. Do you need to transform (enrich, cleanse, merge, etc.) your data or support new source types? Because you will be adding or changing data sources, you will almost certainly need to transform your data as part of the migration process. All migration tools can transform data, but cloud- based systems tend to be the most flexible, supporting the widest range of data types.
- ✓ **Security**. Is any of the data you are migrating sensitive? If you want to migrate sensitive data, it is subject to compliance requirements, which can be hard to support during migration. Cloud-based tools are likely to be extremely secure and compliance certified. On-premise solutions depend on the security of your overall infrastructure. And security may vary widely for open source tools.

To install the Windows Server Migration Tools on the SOURCE server, you need to run the appropriate PowerShell command on the DESTINATION server. This is what trips people up a lot of the time. You deploy the correct version of the tools from the destination server to the source server, where you will than register them for use. Do this with an admin account that has admin privileges on both the DESTINATION & SOURCE Computer.

Start up the Windows Server Migration Tools from Server Manager, Tools.



This launches the Windows Server Migration Tools PowerShell window.

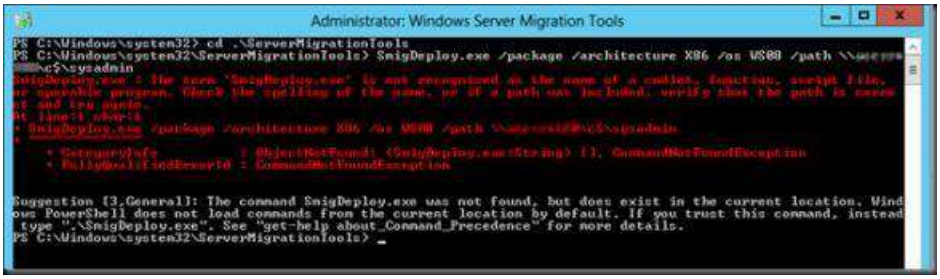


Our SOURCE server here is the32 bit (X86) Windows 2008 TS Gateway Server. The documentation tells us the correct values to use for the parameters /architecture and /OS to use.

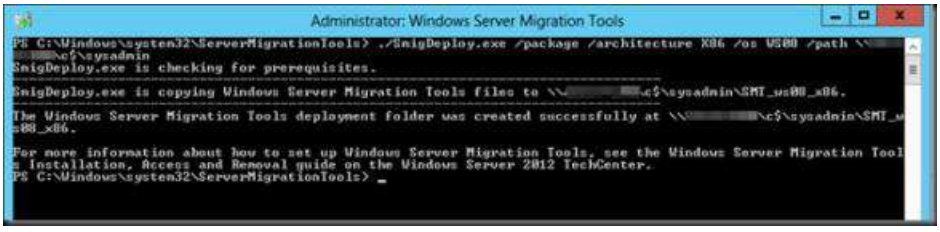
SmigDeploy.exe /package /architecture X86 /os WS08 /path \SourcerServerc$sysadmin

Now before you run this command be sure to go to the ServerMigrationTools folder as the UI fails to do that for you.

Also this is PowerShell so use . in front of the command otherwise you'll get the error below.



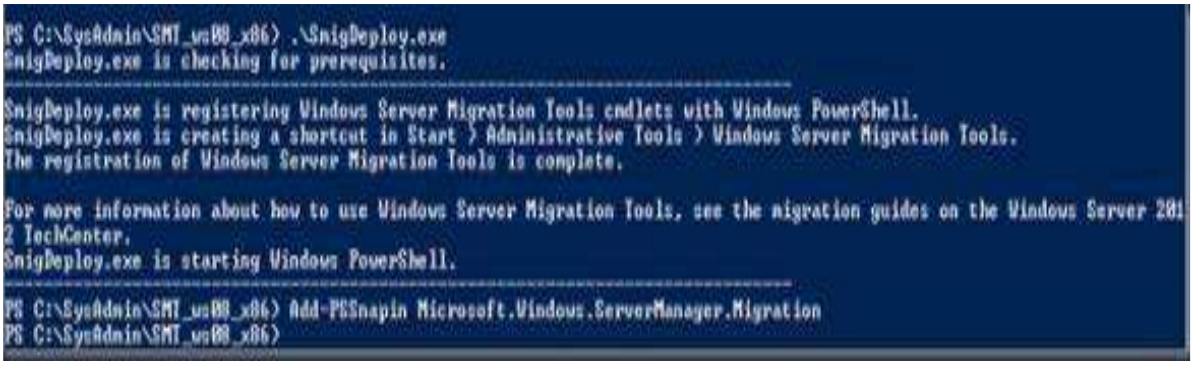
While you want this:



While you want this:

Now you have also deployed the correct tools to the SOURCE server, our old legacy TS Gateway Server. Next we need to register these tools on the SOURCE Server to be able to use them. You might have gotten the message already you need PowerShell deployed on the SOURCE Server as documented.

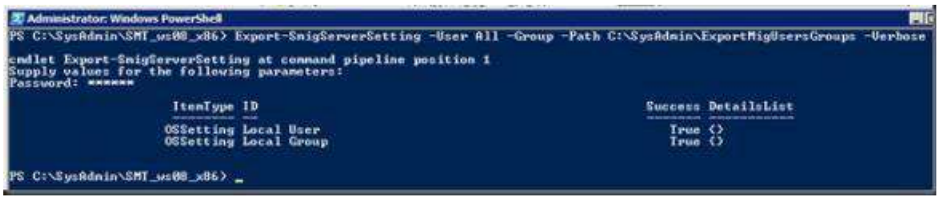
If you have PowerShell, launch the console with elevated permissions (Runs As Administrator) and run the following command: .SmigDeploy.exe



Using the Windows Server Migration Tools To Migrate Local Users & Groups

To export the local users and groups from the source TS/RD Gateway server you start up the Windows Server Migration Tools on the SOURCE server (see the documentation for all ways to achieve this) and run the following PowerShell command:

Export-SmigServerSetting -User All -Group –Path C:SysAdminExportMigUsersGroups –Verbose

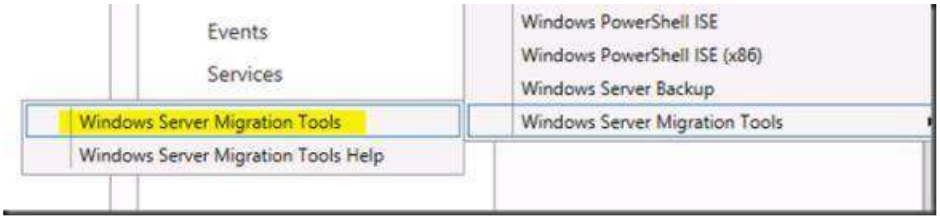


As you can see I elected to migrate all user accounts not just the enabled or disabled ones. We'll sort

those out later. Also note the command will create the folder for you.

To import the local users and groups to the target RD Gateway server you start up the Windows Server

Migration Tools on the Destination server (see the documentation) , i.e. our new Windows Server 2012 RD Gateway VM.



Run the following PowerShell command:

Import-SmigServerSetting -User Enabled -Group -Path C:SysAdminExportMigUsersGroups -Verbose

Do note that the migrated user accounts will be disabled and have their properties set to "Next Logon". This means you will have to deal with this accordingly depending on the scenarios and communicate new passwords & action to take to the users.

LO 2.2 Post-Install and Configure the Server

Content/Topic 1: introduction of window server2012R2 Post-installation and configuration

A. Definition of common networking terms

Networking In the world of computers, **networking** is the practice of linking two or more computing devices together for the purpose of sharing data and resources. Networks are built with a mix of hardware and software.

Protocol In computing, a protocol is a set of rules which is used by computers to communicate with each other across a network.

Internet Protocol (IP)

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet.

Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. There exist two versions of IP, IPv4 and IPv6

Transport Control Protocol (TCP) and User Datagram Protocol (UDP). These are two types of internet protocol (IP) traffic TCP and UDP, and both have very different uses

TCP

Transmission Control Protocol is a connection-oriented protocol, a connection can be made from client to server, and from then on, any data can be sent along that connection.

It is Reliable - when you send a message along a TCP socket, you know it will get there unless the connection fails completely. If it gets lost along the way, the server will re-request the lost part. This means complete integrity, things don't get corrupted**.**

UDP

- ✓ User Datagram Protocol is a simple message- based connectionless protocol. With UDP you send messages (packets) across the network in chunks.
- ✓ **It is Unreliable -** When you send a message, you don't know if it will get there, it could get lost on the way.
- ✓ **It is Not ordered** - If you send two messages out, you don't know what order they will arrive in.

Class full Network

There are five classes of IP addresses. Each class is identified by a letter from A to E.

These classes each have their own specificities in terms of distribution of the number of bytes used to identify the network or computers connected to the network:

- ✓ An IP address class A has a network ID part with only a single byte.
- ✓ An IP address class B has a network ID part with two bytes.
- ✓ A Class C IP address has a network ID part with three bytes.
- ✓ IP addresses of classes D and E correspond to particular IP addresses.

In order to identify which class an IP address, it is necessary to examine the first bits of the address.

Class A

- ✓ An IP address class A has a single byte to identify the network and three bytes to identify the hosts on the network.
- ✓ A Class A network can contain up to more than 16 million hosts.
- ✓ The first octet of a Class A IP address always begins with the bit 0, it is between 0 and 127, some values are reserved for special purposes.
- ✓ An example of IP address class A is 10.50.49.13.

Class B

A Class B IP address has two bytes to identify the network and two bytes to identify the machines on the network.

- ✓ A class B network can contain up to 65534 hosts.

- ✓ The first byte of a Class B IP address always begins with the bit sequence 10, so it is between 128 and 191.
- ✓ An example of IP address class B is 172.16.1.23.

Class C

An IP address of class C has three bytes to identify the network and a single byte to identify the machine on that network.

- ✓ A Class C network can contain up to 254 hosts.
- ✓ The first bytes of a Class C IP address always begins with the bit sequence 110, it is between 192 and 223.
- ✓ An example of a Class C IP address is: 192.168.1.34.

Class D

The Class D addresses are used for multicast communications. The first bytes of a Class D IP address always begins with the bit sequence 1110, so it is between 224 and 239.

An example of a class D IP address is: 224.0.0.1

Class E

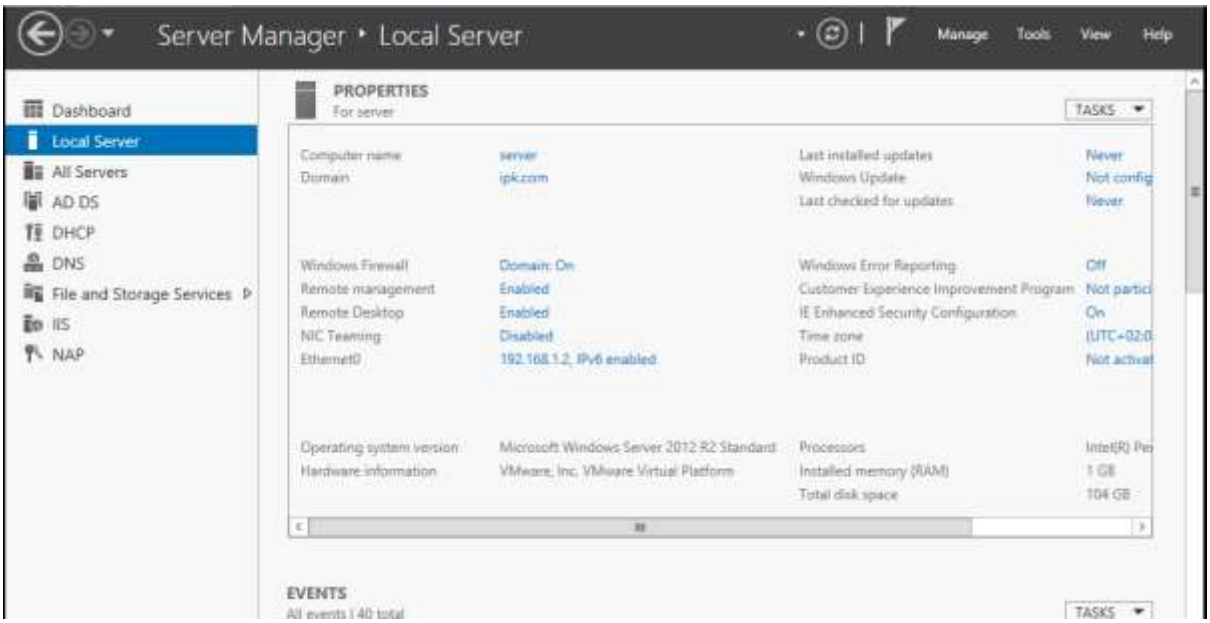
Class E addresses are reserved by IANA for use not determined. Class E addresses begin with 240.0.0.0 and ends in 255.255.255.255

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	1.0.0.0	126.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

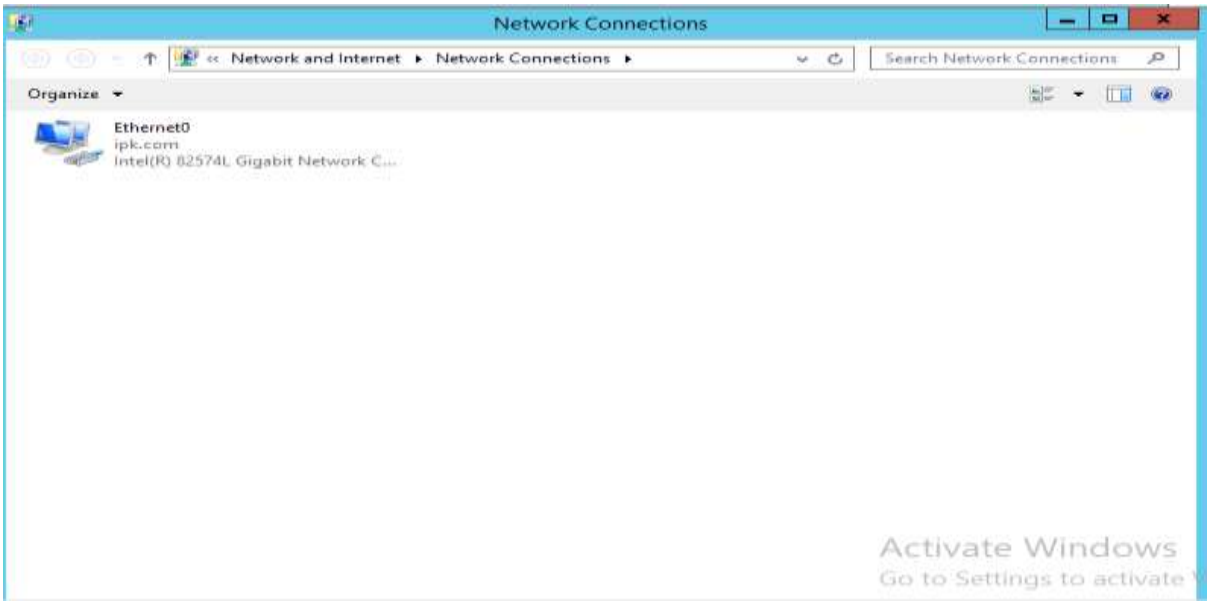
Content/Topic 2: managing window server2012r2 Post-Installation

A. Configuration of server network settings (Configure the IP address) in window server2012R2

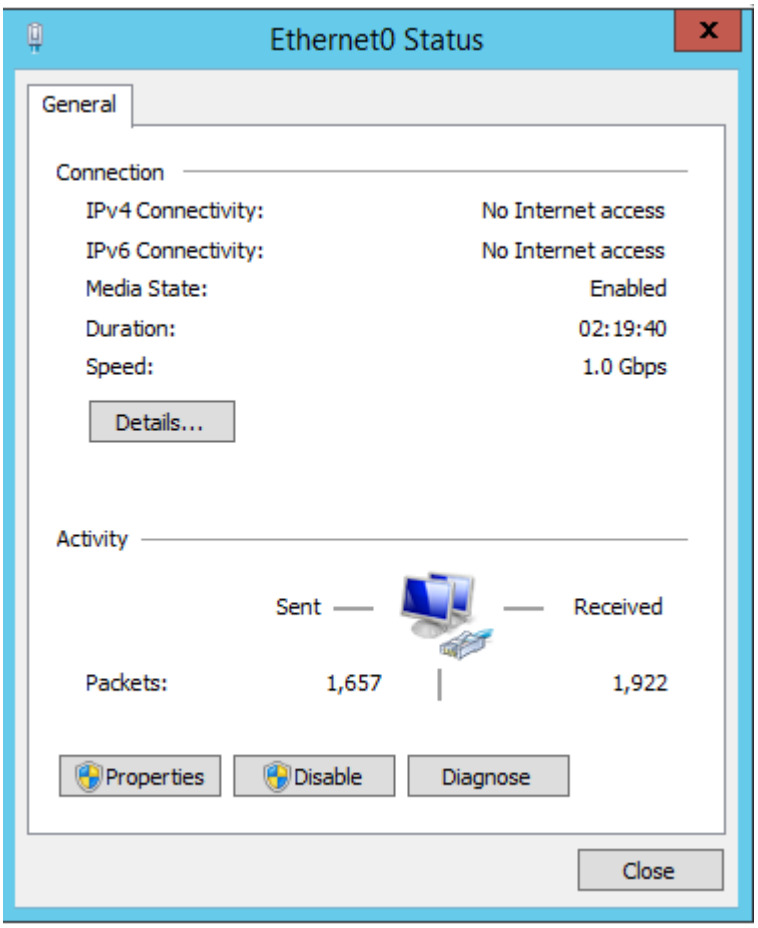
Open local sever



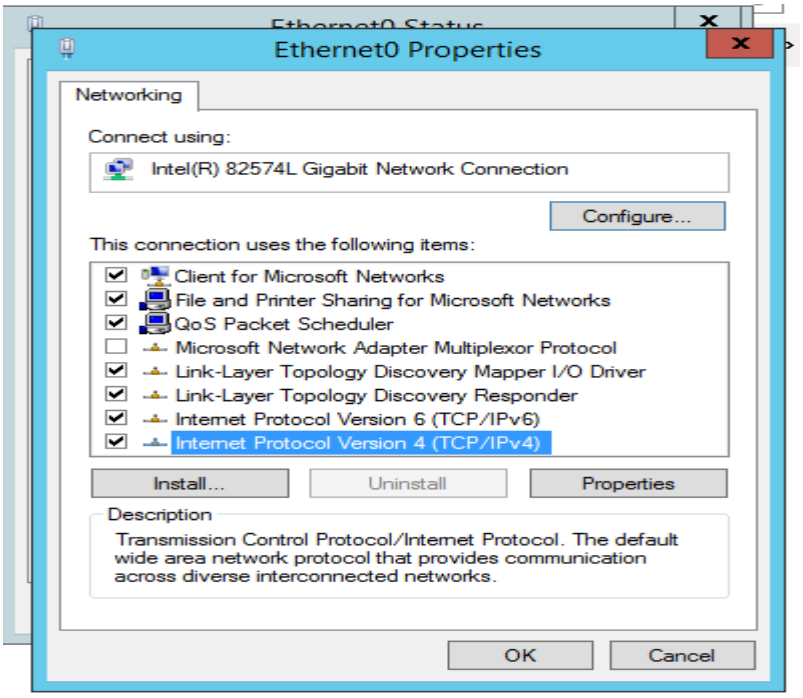
Double click on Ethernet



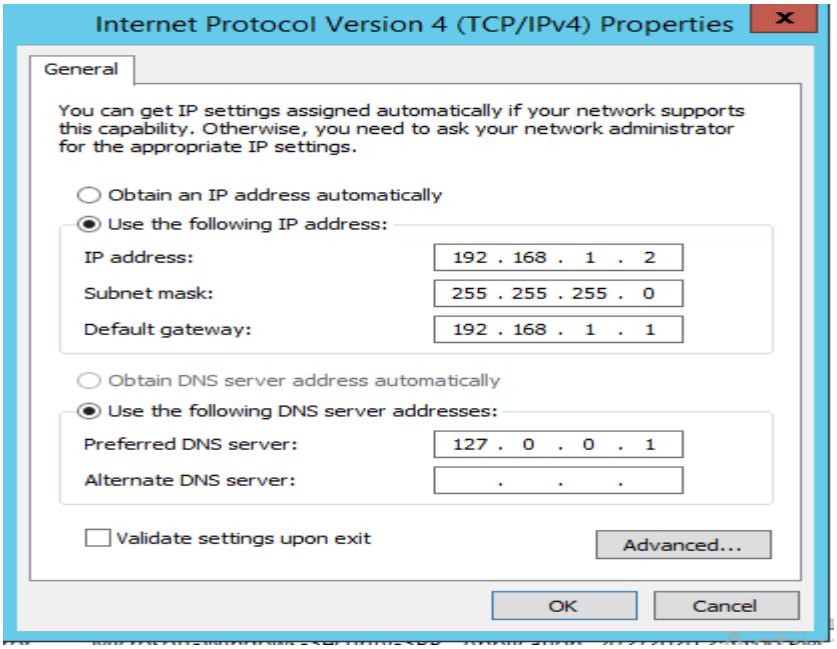
Double click again



Click on property



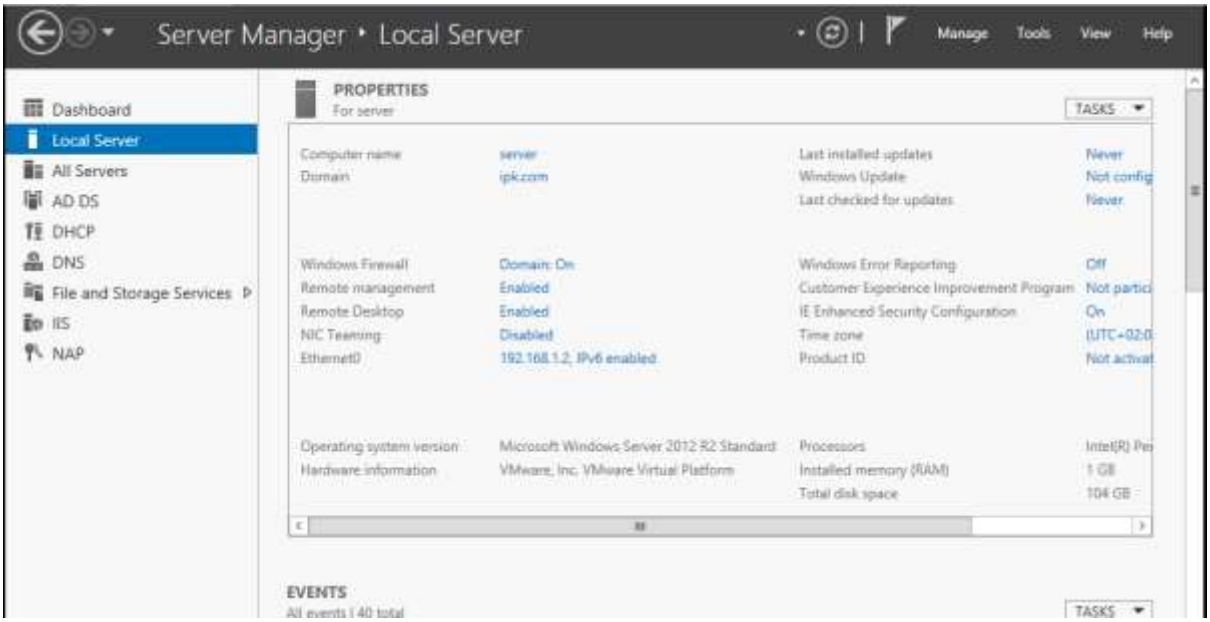
Double click on internet protocol version



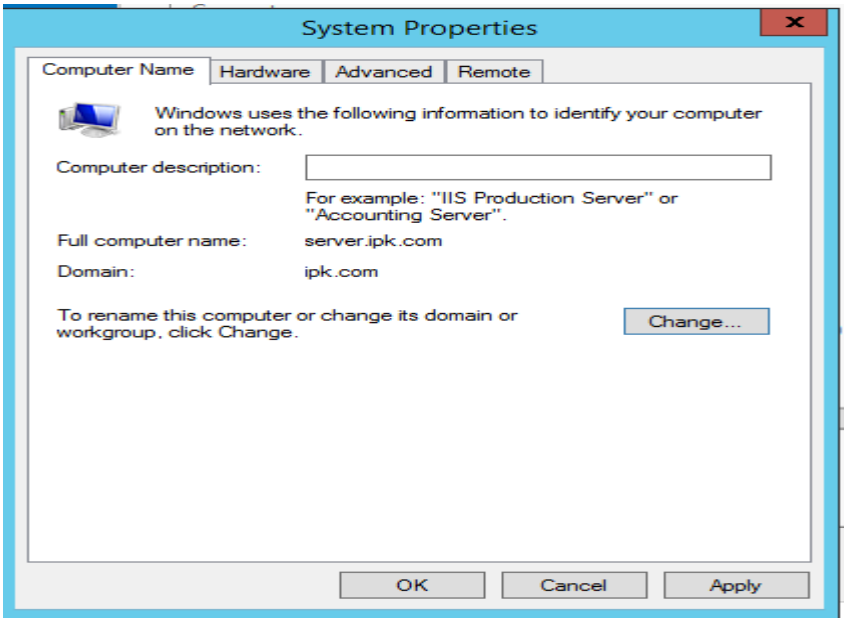
Enter IP address, subnet mask, default gateway and preferred DNS server then click ok

A. Setting the computer name

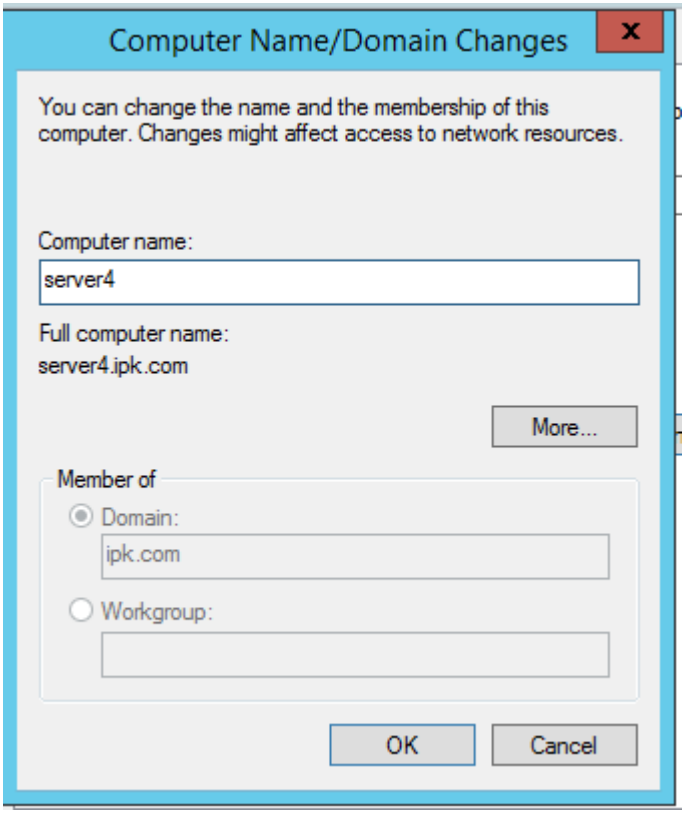
- Double click on computer name

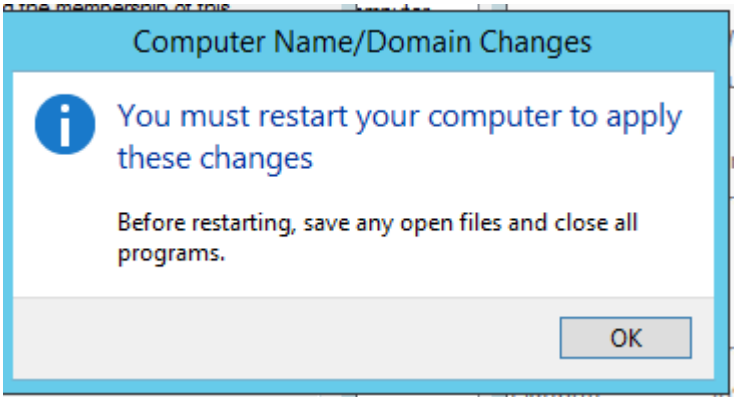


- Click change

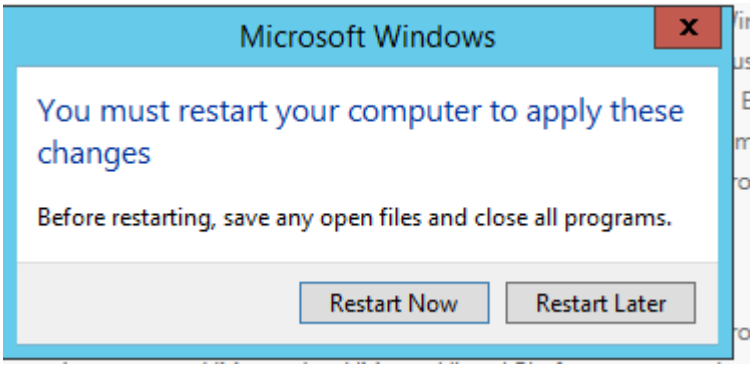


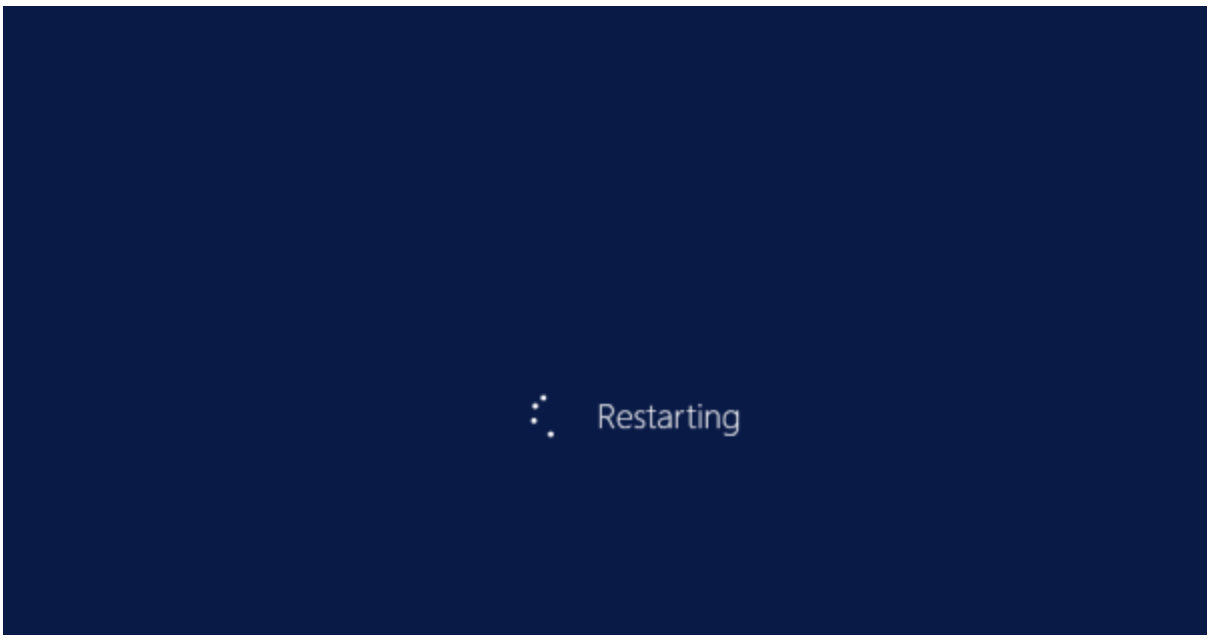
- Type computer name then click ok and ok



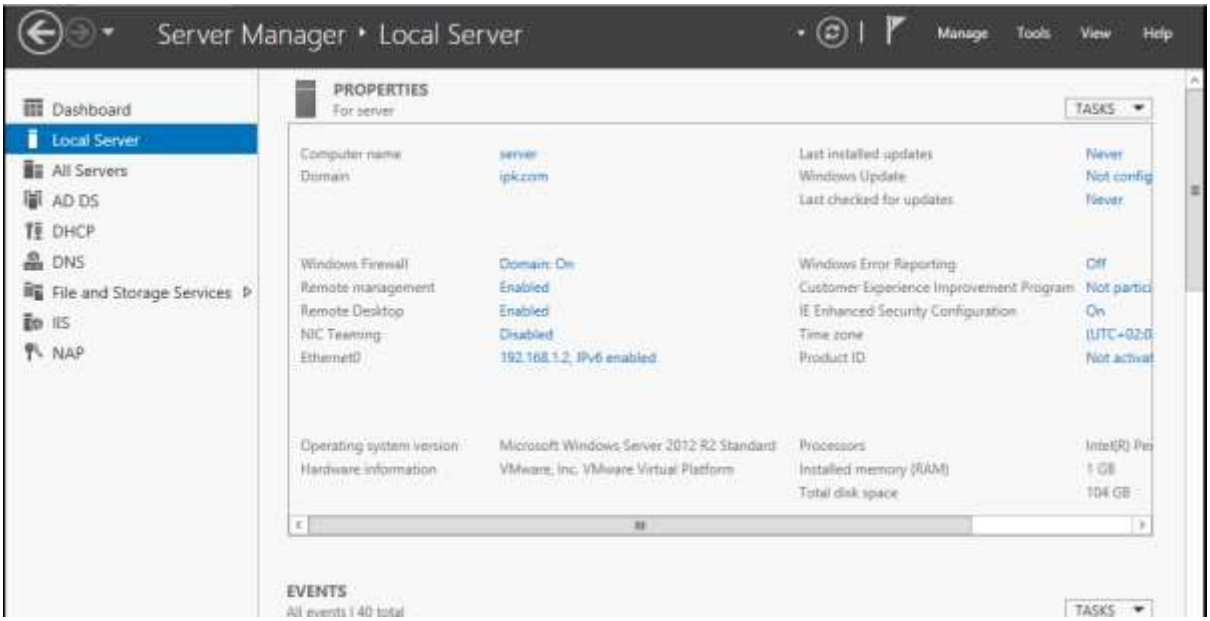


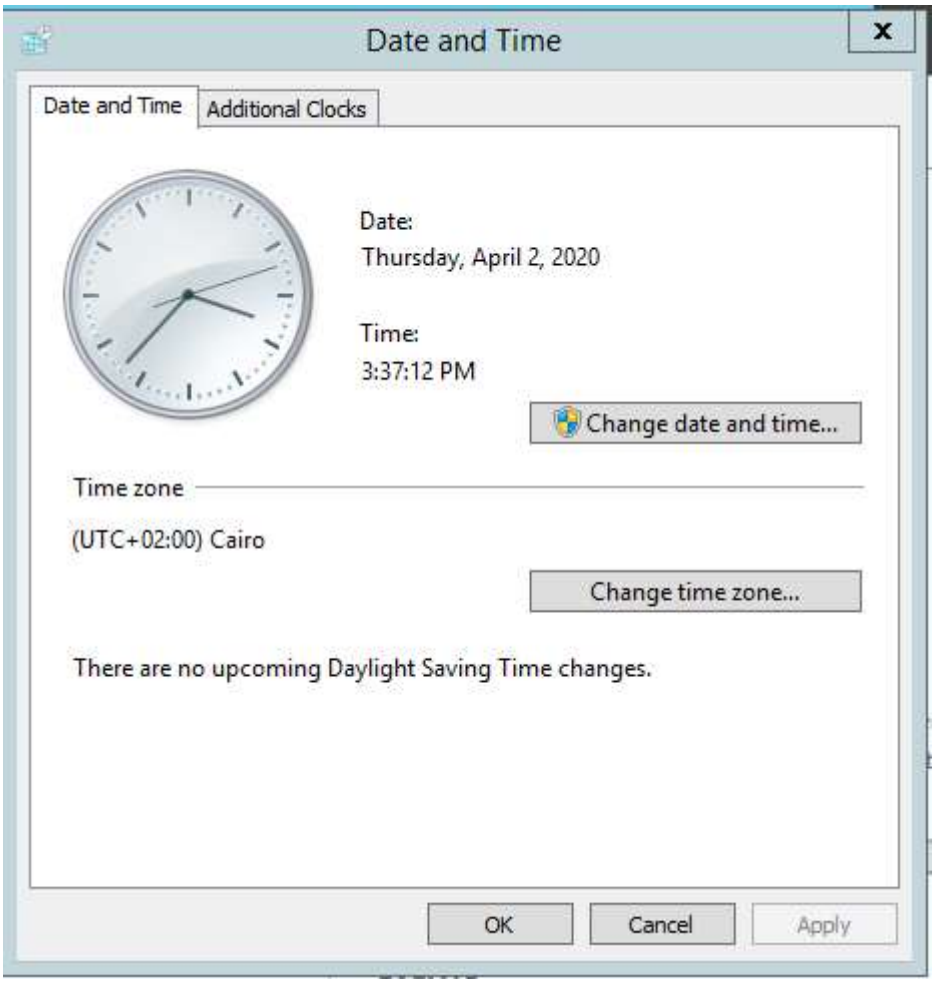
- Click restart now to restart computer



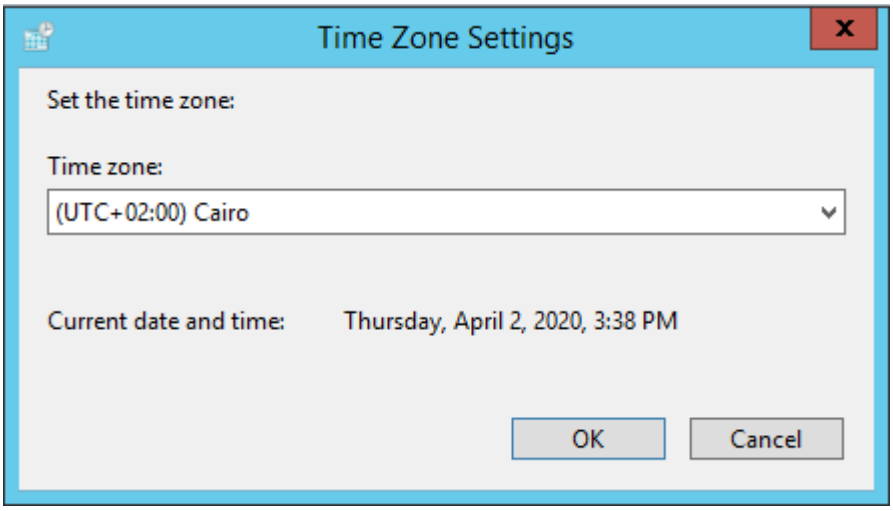


B. <u>Configuring the time zone</u>

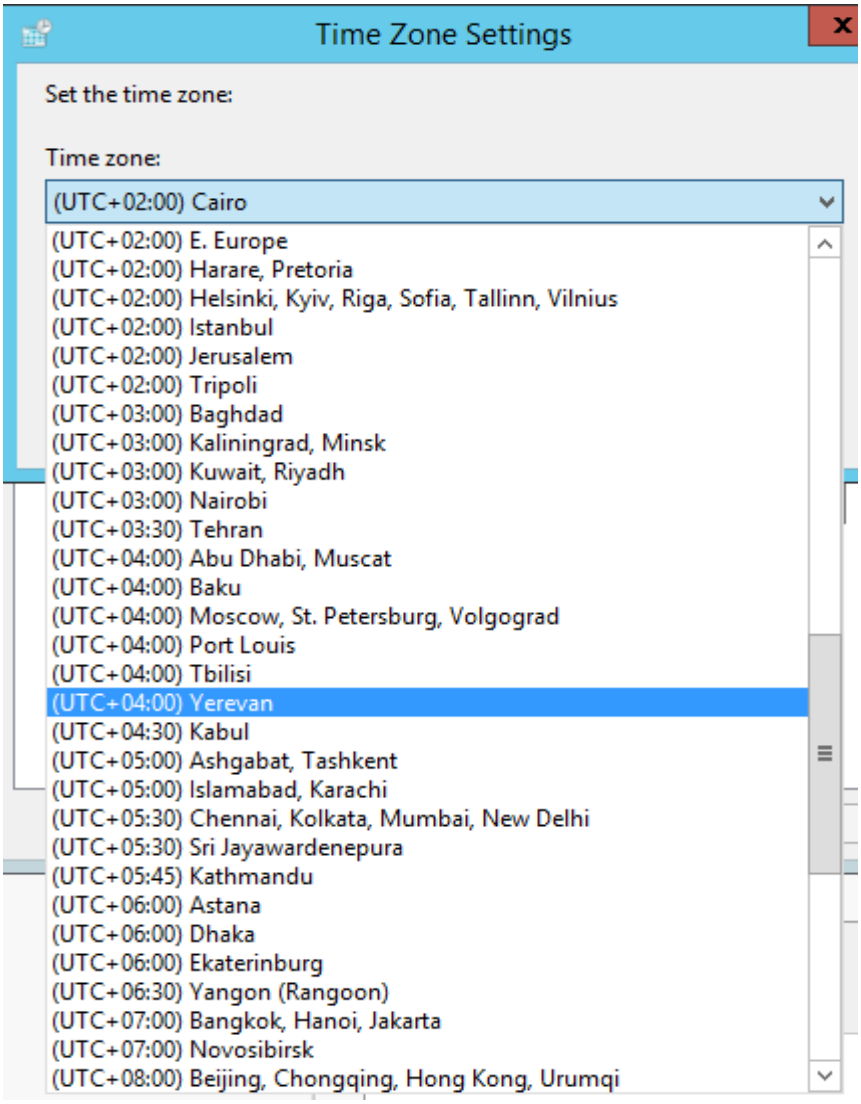




Click on change time zone



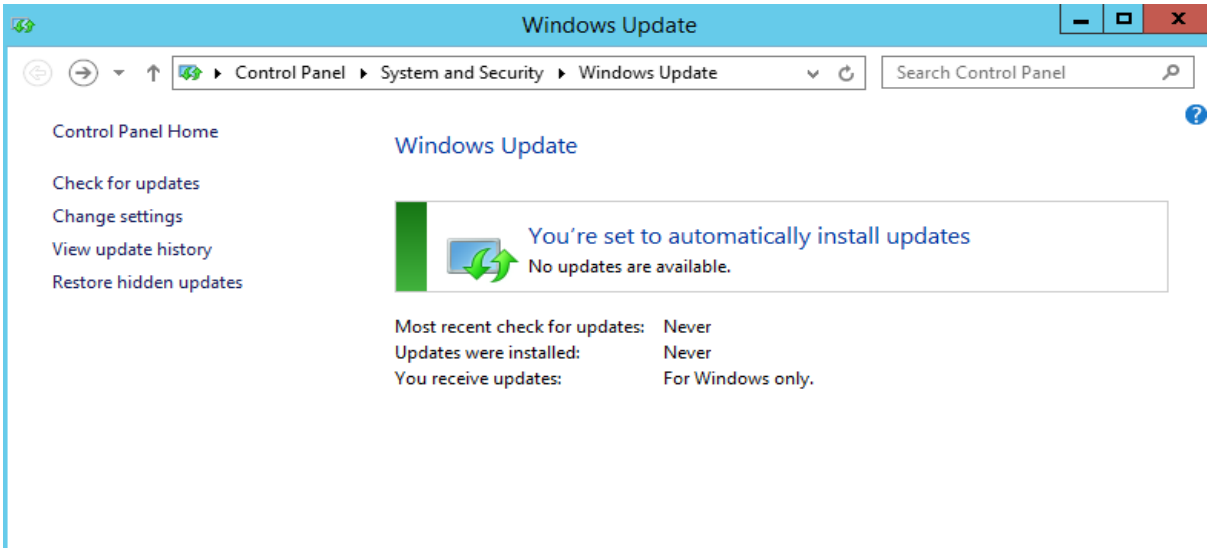
Select time zone from the list



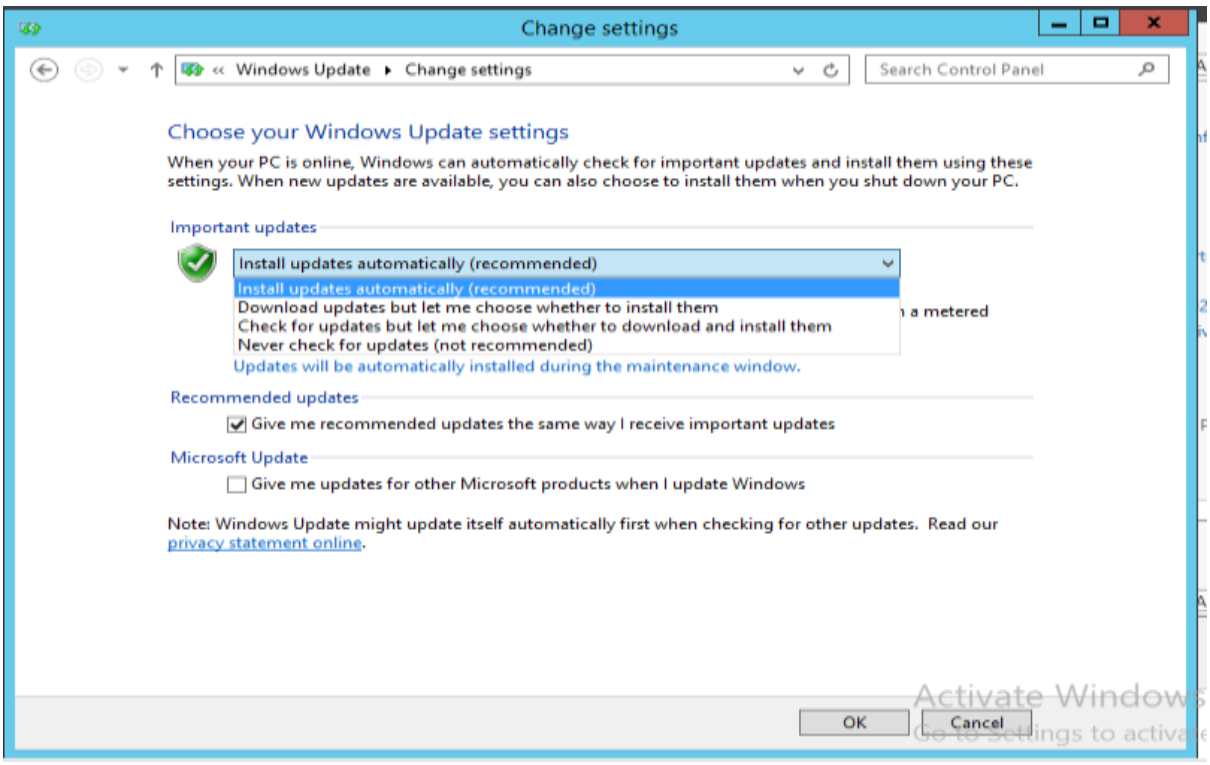
Clicks apply and ok

C. <u>Configuring automatic updates</u>

Double click on windows update to change setting



Select install update automatically from the list to enable automatic windows updates then click ok

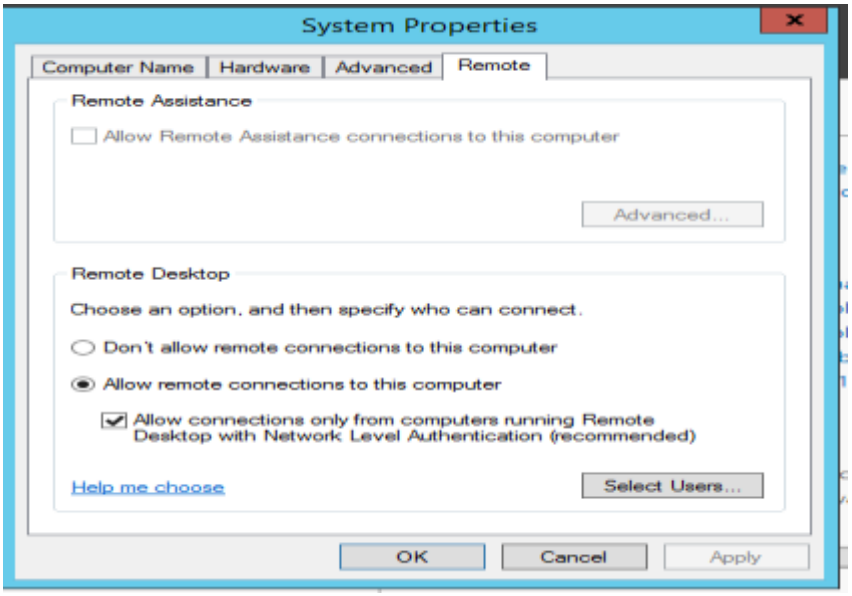


D. Add role and Features window server 2012 has the following roles which can different roles and features which can be used and in the subsequent learning units, will see how to install and configure the most important ones. The following steps shows how to add role and features :

- Select start > server manager
- Add role and features
- In server Manager select manager > Add roles Services and features
- In the Add roles features wizard, click next unit the server roles page appears
- Select the following then click next
- In the features page select the one more feature

E. **Enabling remote desktop**

Click on remote desktop then choose option allows remote connection to this computer



Click Apply and ok

F. **Joining a domain**

We have shown you how to install Active Directory on your network, but it's pointless to have a Domain Controller unless you add your machines to the Domain, so today we're going to cover how to do that.

Adding a Computer to an Active Directory Domain is not hard by any means, but there are 3 things you should always remember:

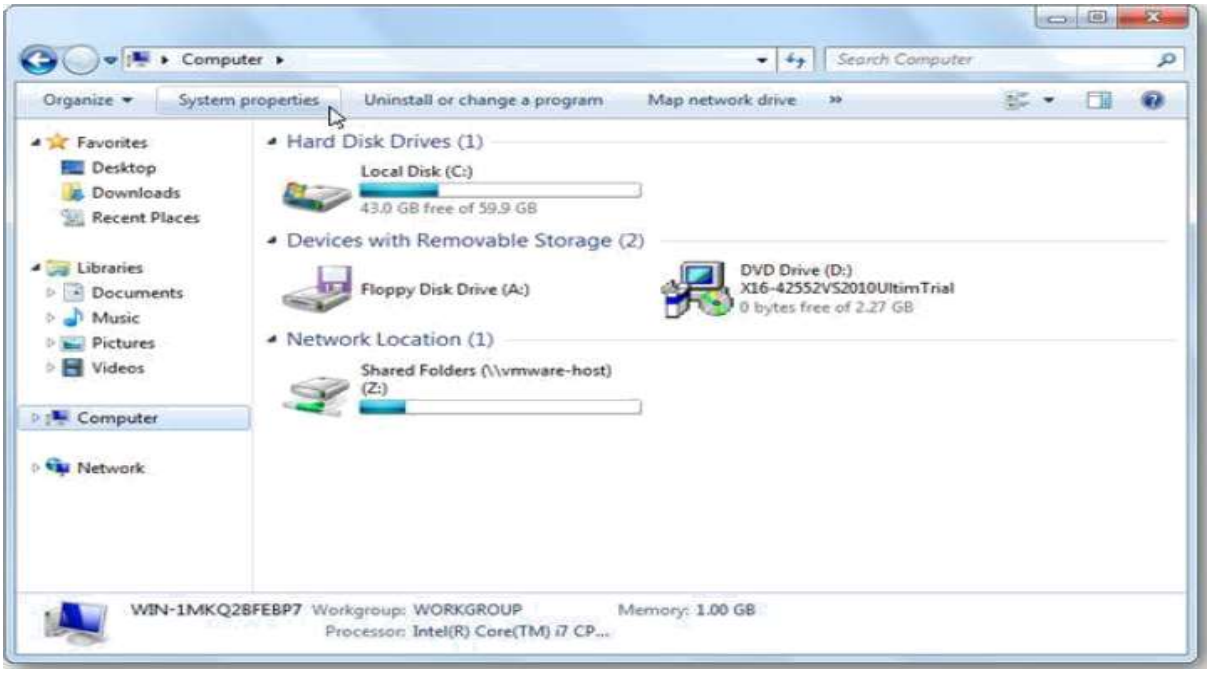
• Rename the machine to a user friendly, recognizable name before adding it to the Domain.

• Make sure your DNS settings are pointing to the correct DNS Server for the domain.

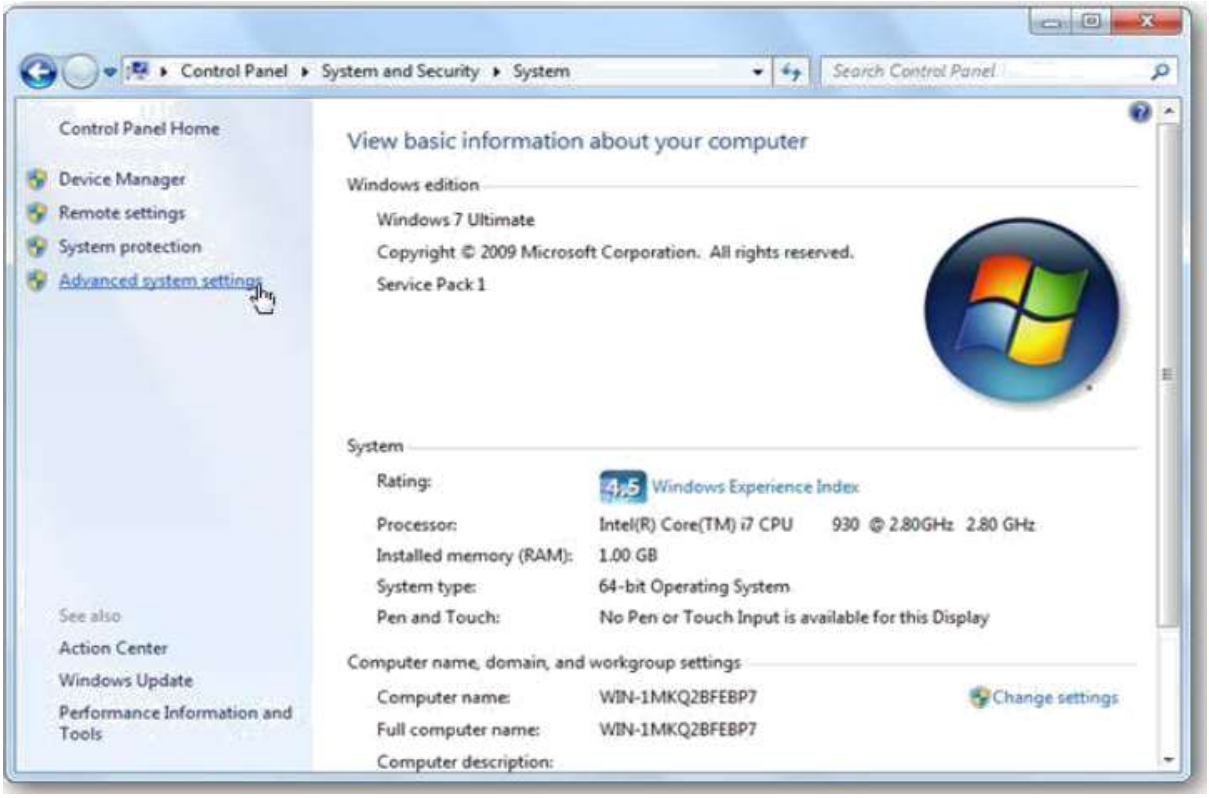
• You have to have access to a Domain account that is part of the Domain Admins security group.

Joining a client to a Domain

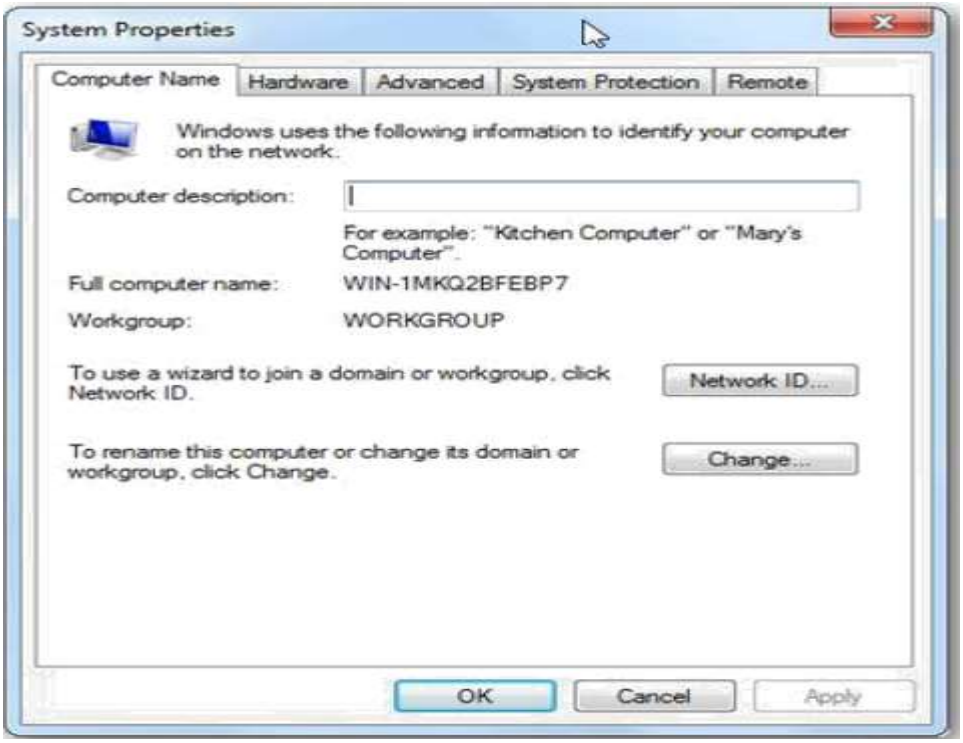
Open Computer and click on the System Properties button.



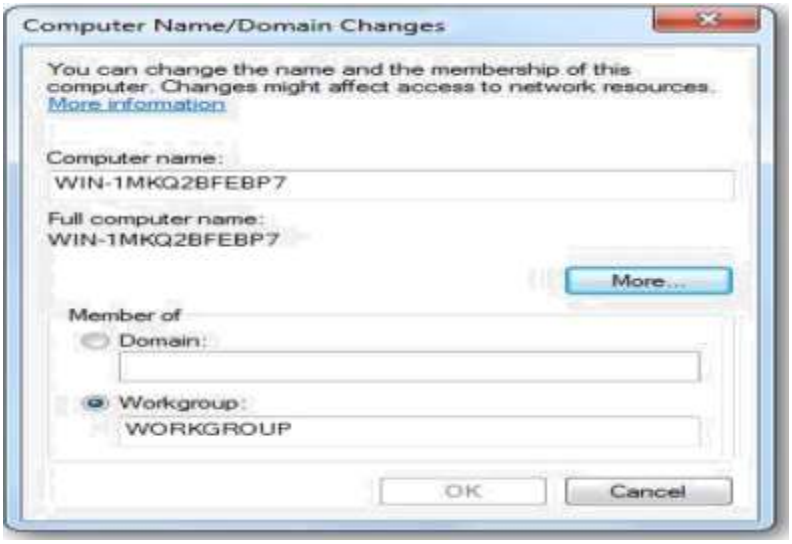
Now click on the advanced system settings link on the left hand side.



When the advanced system settings open, switch to the computer name tab.

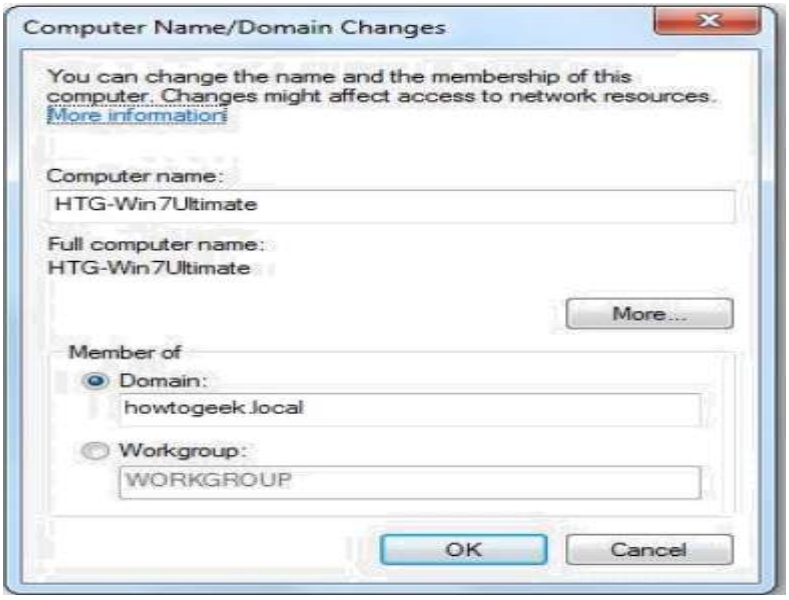


Click on the change button, from here you can change your Computers Name to a more friendly name.



Now switch the radio button, in the bottom section, from Workgroup to Domain. This will make the text box become available.

Now type in the name of your domain, local, but yours will be whatever you made it when you set up Active Directory.



If you specify the correct credentials you will be welcomed to the Domain.

G. **Configuring a Server Core Installation**

The Server Core option is a minimal installation option that is available when you are deploying the Standard or Datacenter edition of Windows Server. Server Core includes most but not all server roles.

✓ **Benefits of a Server Core installation**

The Server Core installation option provides the following benefits:

Reduced maintenance: Because the Server Core installation option installs only what is required to have a manageable server for the AD DS, AD LDS, DHCP Server, DNS Server, File Services, Print Services, and Streaming Media Services roles, less maintenance is required than a full Windows Server installation with a graphical interface.

Reduced attack surface: Because Server Core installations are minimal, there are fewer applications running on the server, which decreases the attack surface.

Reduced management: Because fewer applications and services are installed on a server running the Server Core installation, there is less to manage.

Less disk space required: A Server Core installation requires only about 1 GB of disk space to install and approximately 2 GB for operations after the installation.

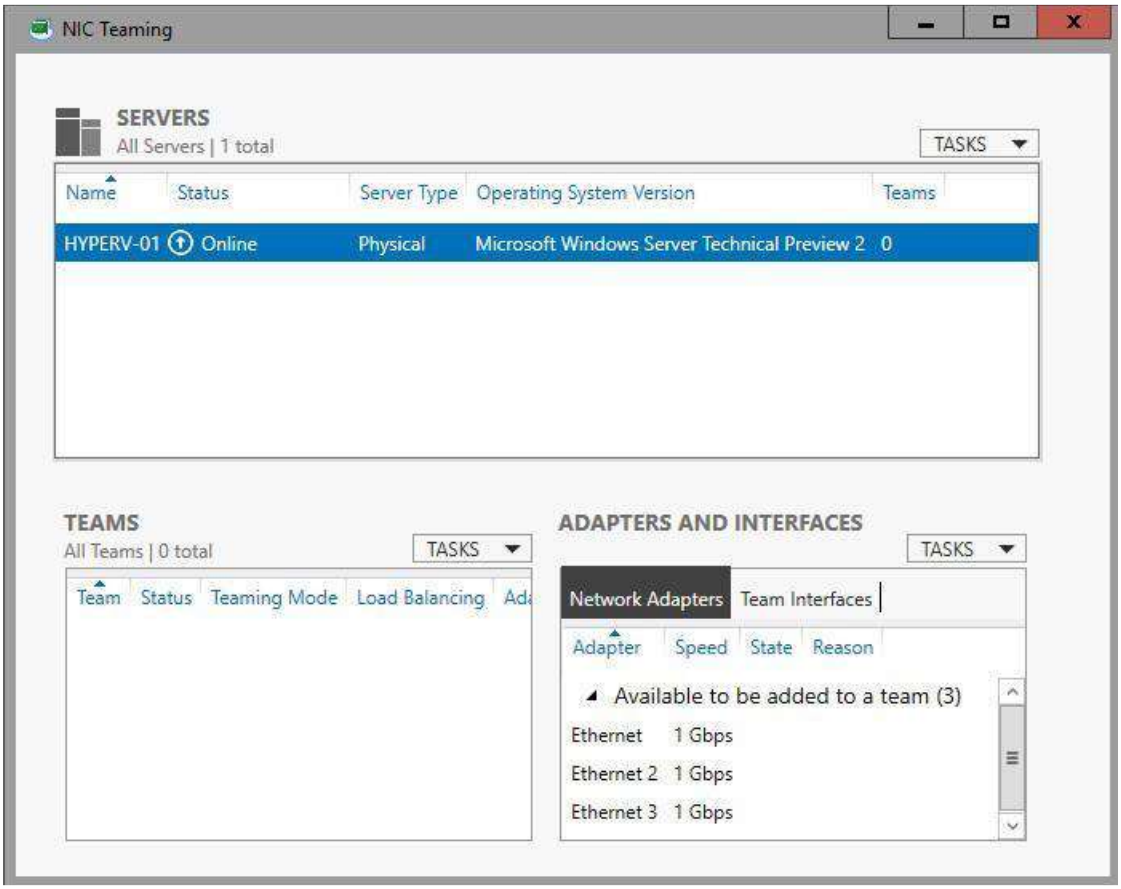
A server running a Server Core installation supports the following server roles:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS) DHCP Server
- DNS Server File Services Print Services
- Streaming Media Services
- Web Server (IIS)

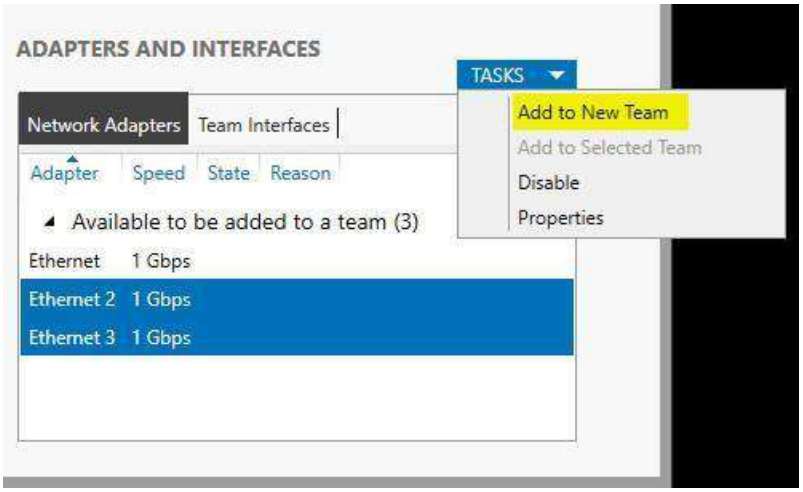
H. Configuring Network Interface Card Teaming

In Server Manager, click **Local Server**.

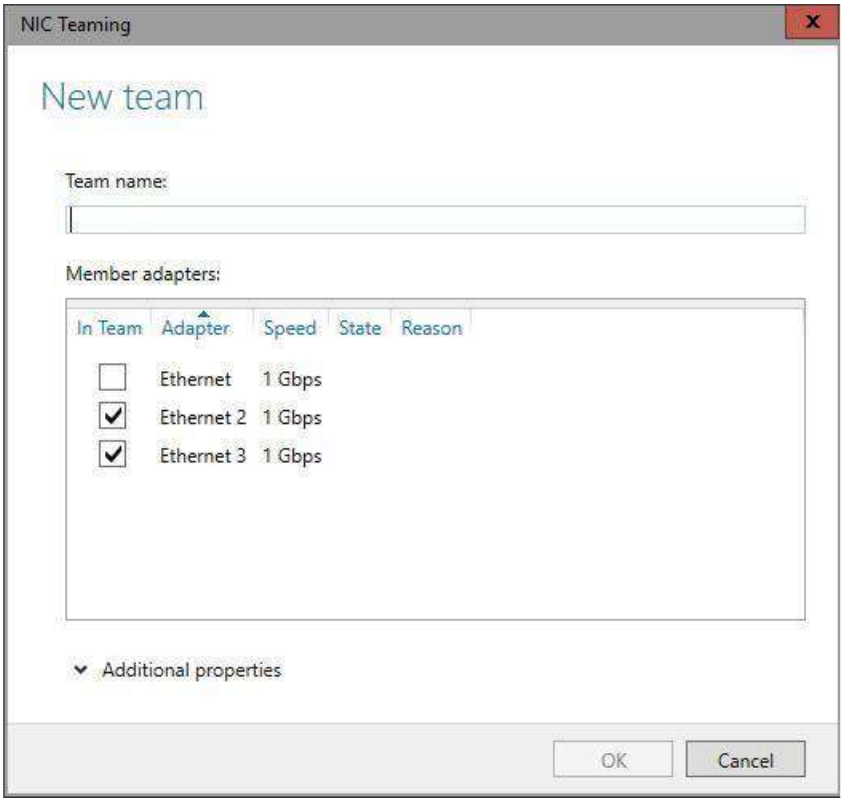
In the Properties pane locate NIC Teaming, and then click the link **Disabled** to the right. The NIC Teaming dialog box opens.



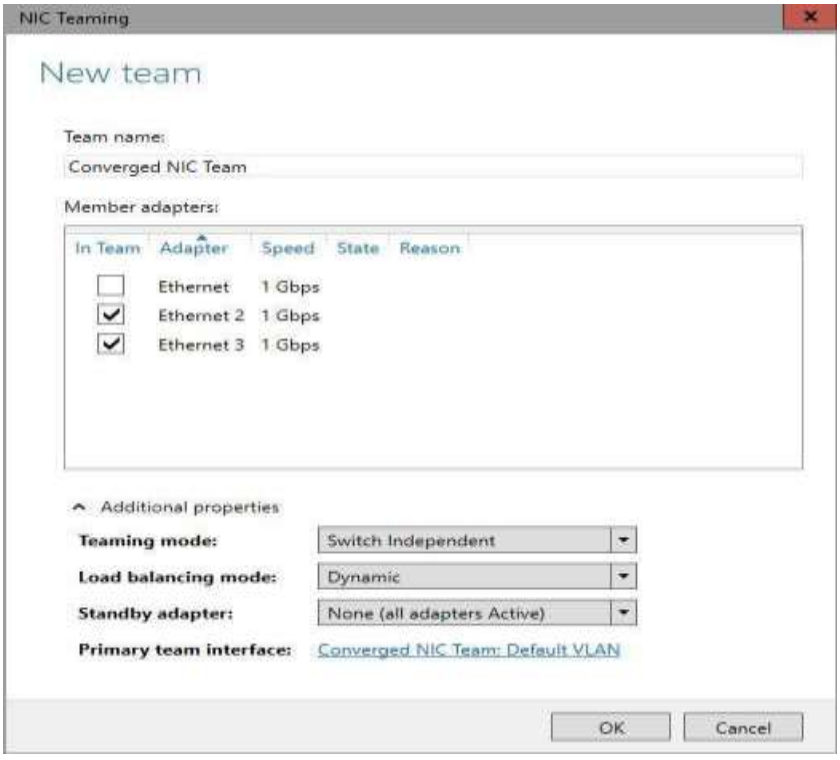
In Adapters and Interfaces, select the network adapters that you want to add to a NIC Team. Click **TASKS**, and then click **Add to New Team**.



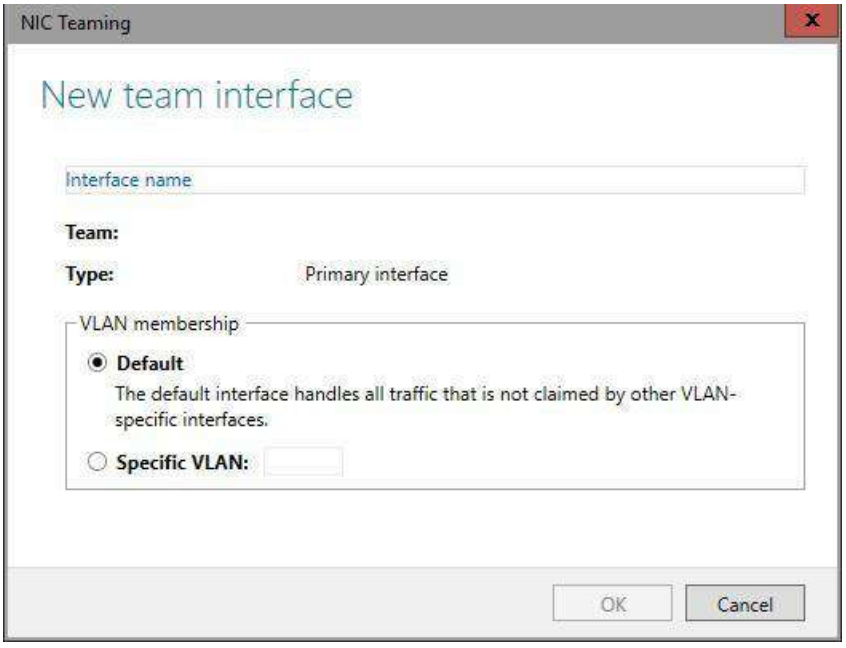
The New team dialog box opens and displays network adapters and team members. In Team name, type a name for the new NIC Team.



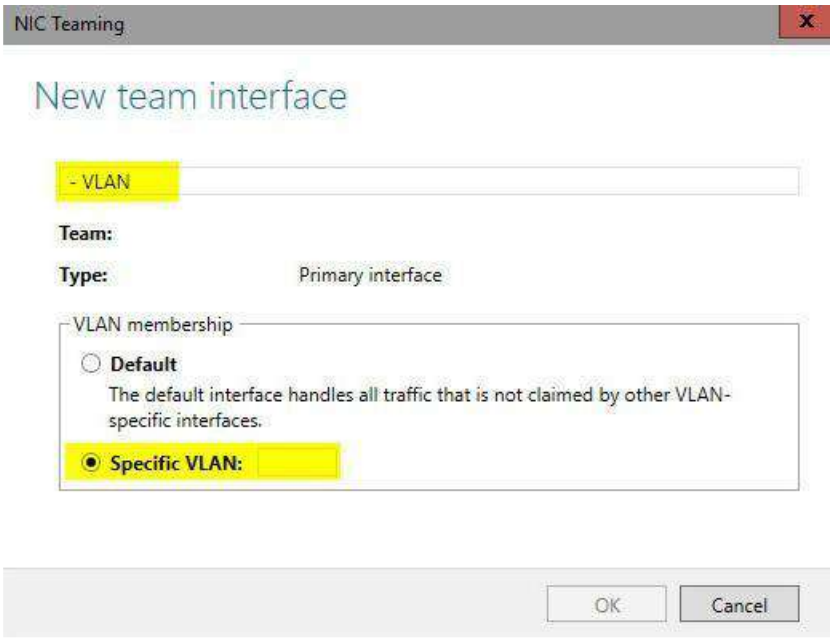
If needed, in **Additional properties**, select values for Teaming mode, Load balancing mode, and Standby adapter. In most cases, the highest-performing load balancing mode is Dynamic.



If you want to configure or assign a VLAN number to the NIC Team, click the link to the right of Primary team interface. The New team interface dialog box opens.



To configure VLAN membership, click **Specific VLAN**. Type the VLAN information in the first section of the dialog box



Click OK

I. Activating Windows Server

To ensure that your organization is correctly licensed and to receive notices for product Updates, you must activate every copy of Windows Server 2012 that you install. Unlike with Previous versions of the Windows Server operating system, there is no longer an activation Grace period. If you do not perform activation, you cannot perform operating system Customization. Also, until activated, the server will shut down every hour.

To activate Windows Server 2012, you can use one of two general strategies:

- Manual activation. Suitable when you are deploying a small number of servers.
- Automatic activation. Suitable when you are deploying larger numbers of servers.

I.1 Manual Activation

With manual activation, you enter the product key, and the server contacts Microsoft. Alternatively, an administrator performs the activation over the phone or through a special clearinghouse website.

You can perform manual activation from the Server Manager console by performing the following procedure:

1. Click the Local Server node.

2. In the Properties window, next to Product ID, click **Not Activated**.

3. In the **Windows Activation** dialog box, enter the product key, and then click **Activate**.

4. If a direct connection cannot be established to the Microsoft activation servers, details will display about performing activation using a website from a device that has an Internet connection, or by using a local telephone number.

Because computers running the Server Core installation option do not have the Server Manager console, you can also perform manual activation using the slmgr.vbs command. Use the slmgr.vbs /ipk command to enter the product key, and slmgr.vbs /ato to perform activation once the product key is installed.

You can perform manual activation by using either the retail product key or the multiple activation key.

You can use a retail product key to activate only a single computer. However, a multiple activation key has a set number of activations that you can use. Using a multiple activation key, you can activate multiple computers up to a set activation limit.

An original equipment manufacturer (OEM) key is a special type of activation key that is provided to a manufacturer and allow automatic activation when a computer is first powered on.

This type of activation key is typically used with computers that are running client operating systems such as Windows 7 and Windows 8.1. OEM keys are rarely used with computers that are running server operating systems. Performing activation manually in large-scale server deployments can be cumbersome. Microsoft provides a method of activating large

numbers of computers automatically without having to enter product key son each system manually.

I.2 Automatic Activation

In previous versions of the Windows Server operating system, you could use the Key Management Service (KMS) to perform centralized activation of multiple clients. The Volume Activation Services server role in Windows Server 2012 allows you to manage a KMS server through a new interface. This simplifies the process of installing a KMS key on the KMS server. When you install Volume Activation Services, you can also configure Active Directory-based activation. Active Directory-based activation allows automatic activation of domain-joined computers. When you use Volume Activation Services, each computer activated must periodically contact the KMS server to renew its activation status.

J. configuration of window firewall

✓ **Definition Windows Firewall**

Windows Firewall is a Microsoft Windows application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the firewall.

Windows Firewall allows you to block or unblock all connection requests, helps block computer worms and viruses and creates a security log of successful and unsuccessful attempts to connect to your computer, according to the Microsoft Corporation.

✓ **Types of Firewalls**

There are many different types of firewall you can implement in order to control various activities in different places and operating systems. The two main types of firewall are host-based and network-based firewall.

- ✓ **Host-based firewall.** This type of firewall runs on individual systems, physical or virtual. It is a piece of software installed on an operating system which stands between the host and other network devices. Same as any other firewall, it controls and filters incoming and outgoing network traffic, but only for a single host. The benefit of this type of firewall is that it can protect from both external and internal attacks. Host-based firewall is highly customizable and every host can have unique firewall rules to match its specific needs. This allows organizations to tightly control how people use the network.

- ✓ **Network-based firewall.** These are network devices built into the IT infrastructure and they stand between public and internal networks. A network-based firewall can be a hardware device or a virtual solution. Most modern routers have this firewall built into them and it can range from basic to a firewall with advanced security settings. The benefit is that every network device behind it is protected, not only a single host.
- ✓ **<u>Configuring window firewall setting</u>**

Step 1

Windows Server 2012: Log into your server using remote desktop and press the Windows key to bring up the start menu.

Windows Server 2016 or 2019: Log into your server using remote desktop and click the *search*

icon located next to the start menu icon.

Step 2

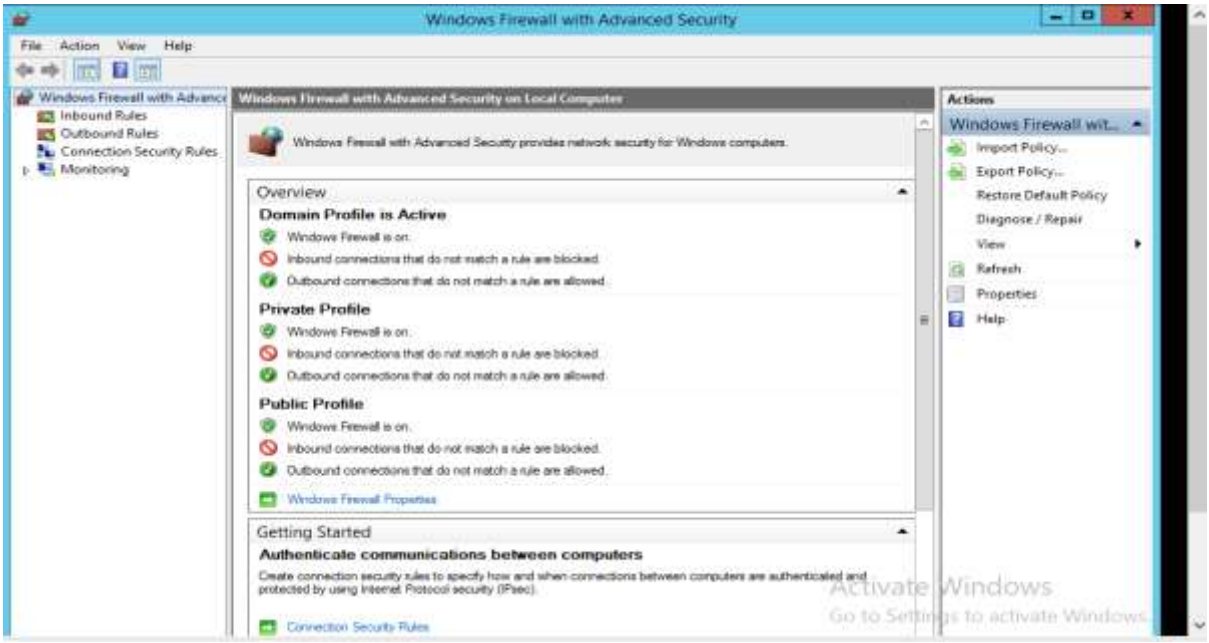
Type firewall and click on the **Windows Firewall with Advanced Security** icon.

Check your current Firewall settings

Step 3

Open your firewall, you will see the firewall overview, this shows what the current settings are for each profile (Domain, Private and Public).

To check your Inbound or Outbound rules select either one from the left hand pane.

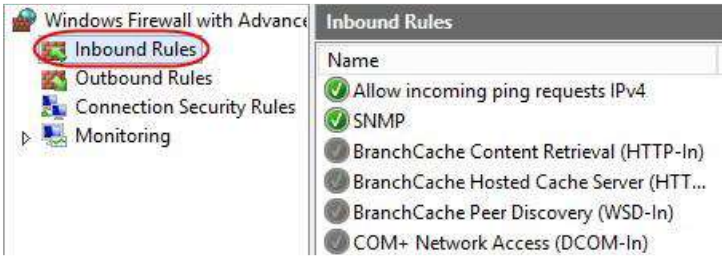


Domain Traffic to and from a network on which it can detect a domain controller of the domain to which the computer is joined.

Private Traffic to and from the local server or the local network to which it is attached.

Public Traffic to and from non-local sources such as the World Wide Web.

Step 4



Rules with a green tick next to them are active, if they are greyed out this means they are inactive rules.

An inactive rule does not mean that a service is blocked. For example to block a service the rule to do this must be active.

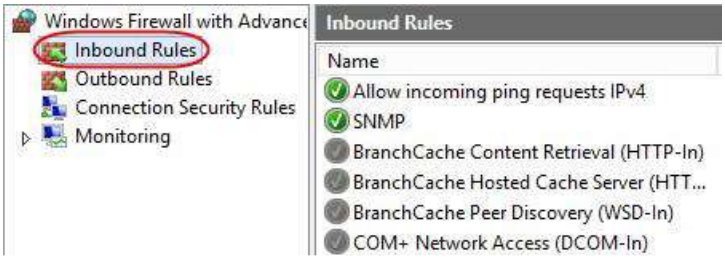
- ✓ **<u>Enabling or Disabling a Firewall rule</u>**

Step 1

Log on to your server and open up your Windows Firewall.

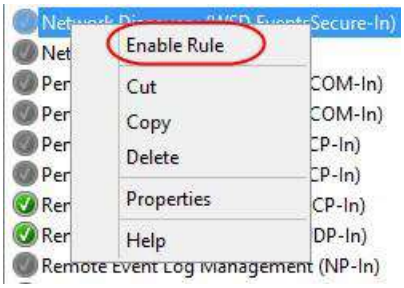
Step 2

Select either *Inbound Rules* or *Outbound Rules* depending on if you want to edit.

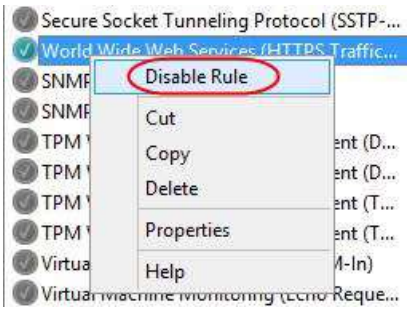


Step 3

To enable the rule right click on the greed out rule and select *Enable Rule.*



To disable a rule right click on a green rule and select *Disable Rule*.



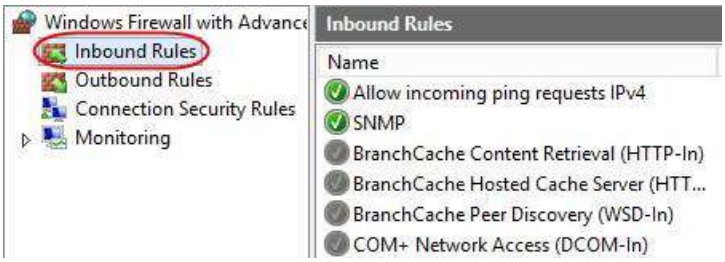
- ✓ **<u>Add a Firewall Rule</u>**

Step 1

Log on to your server and open up your Windows Firewall.

Step 2

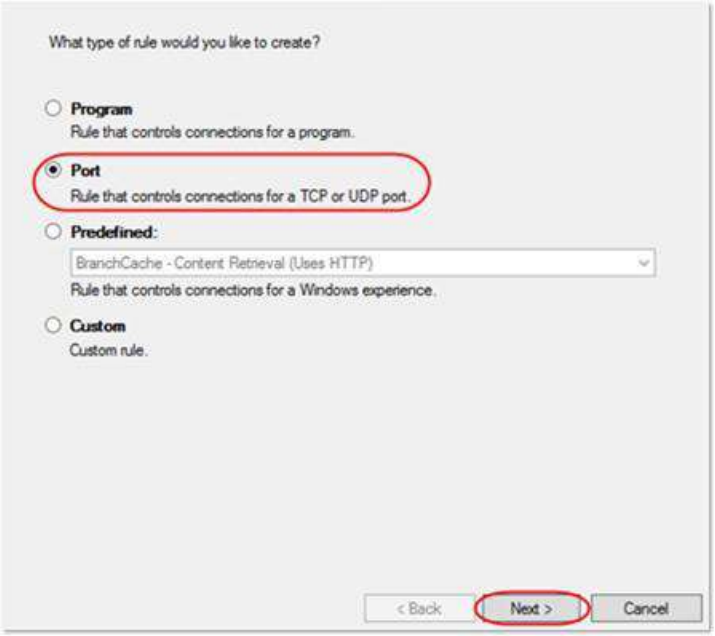
Select either *Inbound Rules* or *Outbound Rules* depending on if you want to add.



Step 3 Select *New Rule* from the right hand side **Actions** menu.

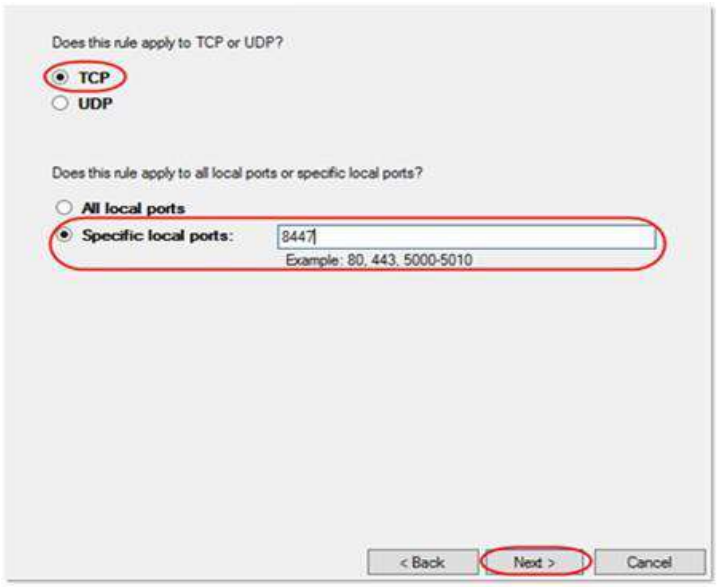
Step 4

Select the *Rule Type* that you want to create and click **Next**. In this example **Port** has been chosen.



Step 5

Select either *TCP* or *UDP* depending on the type of traffic the port you are creating a rule for. Select *Specific local ports* and enter a port, a list of ports or a port range and click **Next**.

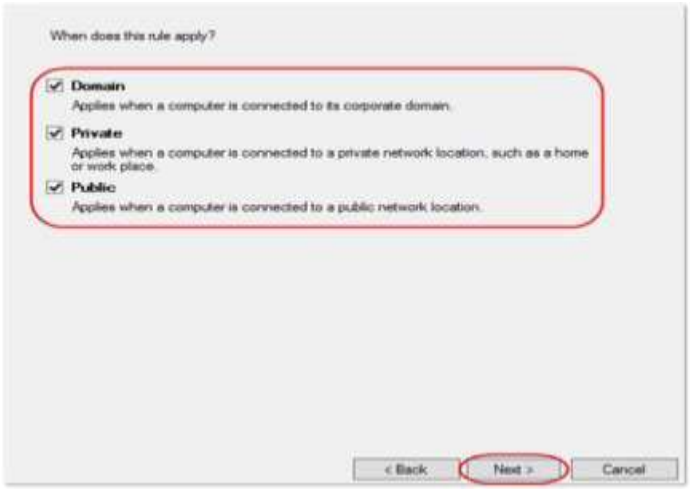


Step 6

Select what action you would like the rule to perform and click **Next**. You can choose to *Allow the connection, Allow the connection if it is secure* or *Block the connection.*

Step 7

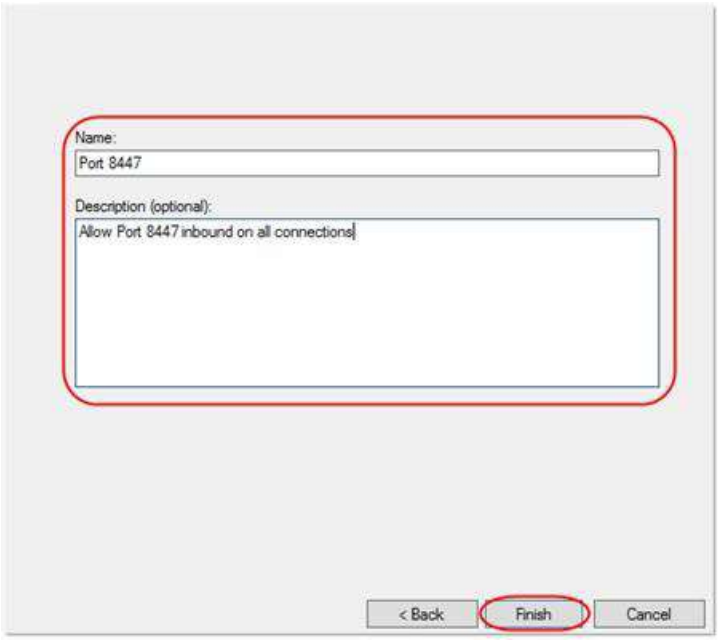
Select the *Profiles* to apply the rule to and click **Next**.



For more information on profiles see the *Check your current Firewall settings* section.

Step 8

Give the rule a meaningful name and description and click **Finish**.



- ✓ **<u>Edit a Firewall Rule</u>**

Step 1

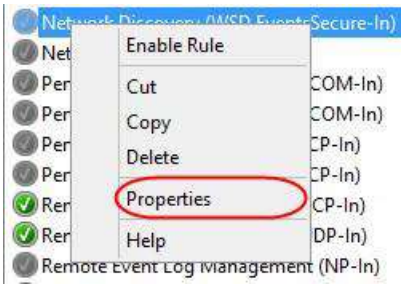
Log on to your server and open up your Windows Firewall.

Step 2

Select either *Inbound Rules* or *Outbound Rules* depending on if you want to edit.

Step 3

Right click on the rule you want to edit and select *Properties.*

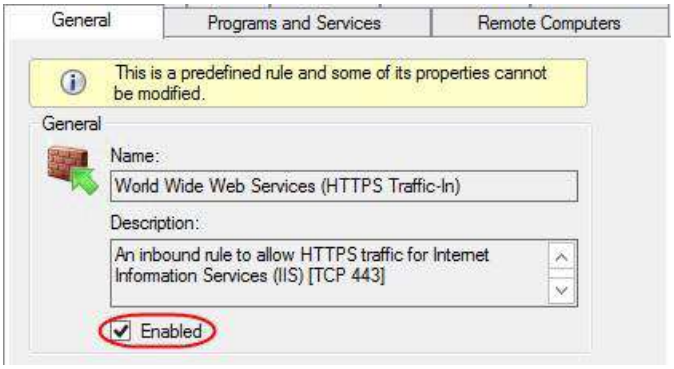


Step 4

There are several tabs within the rule properties, this guide will cover those that are the most commonly used.

General

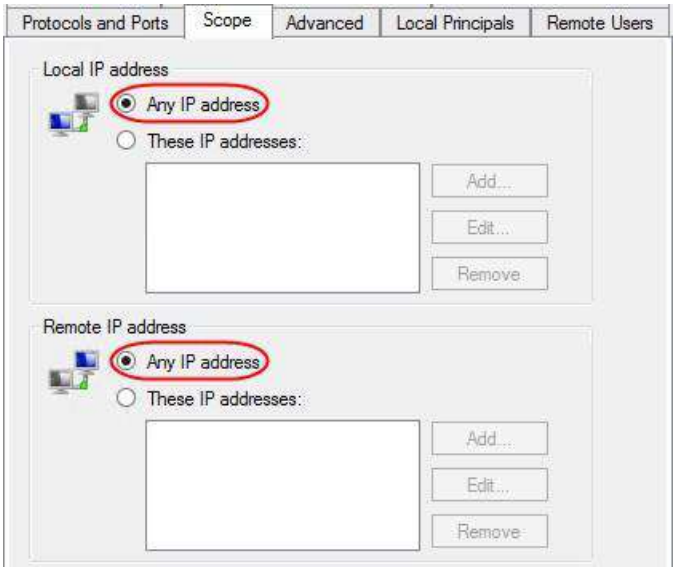
Under the *General* section of the tab you can only enable or disable the rule by ticking or unticking the *Enabled* check box.



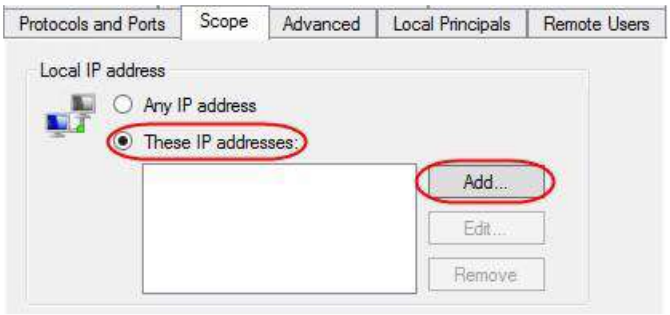
Under the *Action* section of the *General* tab you can choose whether to *Allow the connection, Block the connection* or *Allow the connection if it is secure*.

Scope

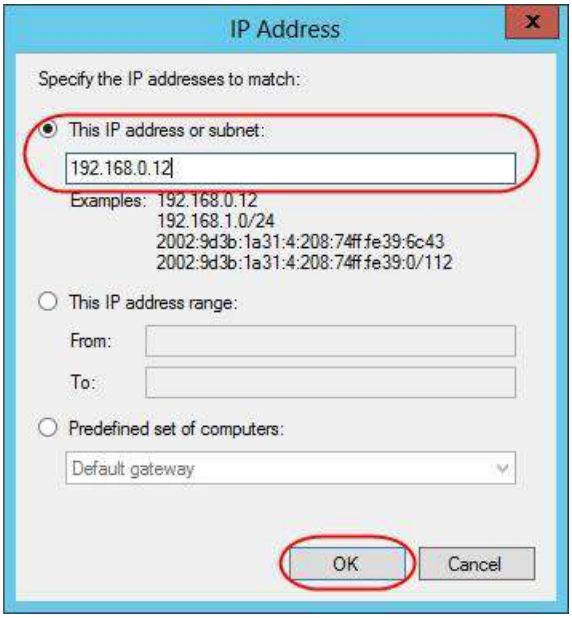
Under the Scope tab you can limit the rule to specific local or remote IP addresses, subnets and IP ranges. You can apply the rule to any IP (local or remote) by leaving the *Any IP address* option selected.



To limit a rule to an IP, subnet or IP range (local or remote) select *These IP addresses* and select the **Add** button.



A new window will open with the options to input an IP, subnet or an IP range. Select which option you want and input the values needed. Click **OK** once finished.



USING DISM to Add window features

Deployment Image Servicing and Management (DISM) tool is a command line tool that is used to modify Window images. You can use DISM to enable windows features directly from the command prompt or by applying an answer file to the image. You can enable or disable windows features on WIM or VHD File, or online on running operating system.

To mount on offline image for servicing

1. Open Command prompt with administrator privileges.
2. To use DISM from an installation of the window assessment and deployment Kit (windows ADKK) locate the window ADK servicing folder and navigate to this directory. By default, DISM is installed at C:/program files(x86)/ windows its/10.0/assessment and deployment it/Deployment tools/in windows 10, C:/program files(x86)/windows Kits/8.1/assessment and deployment Kits/deployment tools/in windows 8.DIMS is available in:

- Windows 10
- Windows 8.1
- Windows 8
- Windows server 2016
- Windows server 2012
- Windows server 2012

You can install DIMS and other deployment and image tools. Such as windows system image manager (windows SIM), on another supported operating system from the windows ADK.

3. Use the /Get –image Info option to retrieve the name or index number for the image you want to modify.

To enable or disable windows features using DISM and an answer files steps:

- In windows SIM open existing catalog by clicking select a window image on the file menu and specifying the catalog file type(.clg) in the drop-down list. Or create a new catalog by clicking create catalog on the tools menu
- Expand the catalog in the windows image pane and then expand packages
- Expand foundation and right click Microsoft-windows-foundation-package.
- Click add to answer file
- Click enabled or Disabled next to the features that you intended to enable or disable. Click the arrow to select the opposite choice.
- Click tools on the main menu and then click validate answer file.
- Correct any errors that appear in the massages pane and save the answer file.
- At the command prompt type the following command to apply the unattended answer file to the image.

To service an offline image, specify the location of the mounted image directory. For example, type:

To commit changes on an offline image

- Commit the changes and unmount the image. For example, type:

Learning Unit 3 Configure and administer the server

LO 3.1 Install and administer active directory, Organizational units (OUs).

- **Content/Topic1: Installation and Administration of an Active Directory and Organization Unit(OUs)**

A. **overview of window server manager**

Windows Server Administration is an advanced computer networking topic that includes server installation and configuration, server roles, storage, Active Directory and Group

Policy, file, print, and web services, remote access, virtualization, application servers, troubleshooting, performance, and reliability.

B. Definition of Server Manager

Server manager is utility tool in Windows Servers for the administrator for managing servers roles (like adding or removing server roles.

Windows PowerShell is Command-Line Shell developed by Microsoft. The main purpose of the PowerShell is to automate administrative tasks which work both local and remote windows machines. PowerShell is built on .NET Framework.

C. Use the server manager console to perform the following tasks on both local servers and remote servers:

- **View role-related events.**

Events, **Services**, and **Performance** tiles are part of role and group home pages. Commands on the **Tasks** menu of these tiles let you specify the data that you want collected from managed servers. The tiles include filters and queries to further limit the log entries that are displayed in the tile, if desired.

- **Run the Best Practice Analyzer for a role.**

This steps show us how to run best practice analyzer using server manager:

1. Open server manager. To open server manager click start, point to administrative tools and then click server manager.
2. In the tree pane, open roles and then select the role for which you want to open BPA.
3. In the details pane open the summary section, and then open the best Practices analyzer area.

- **List the tools available from Server Manager.**

The available tools from server manager are:

1. Basic system configuration task
2. Performance monitoring tool
3. Device manager tools
4. Viewing the role and features that are installed on a server
5. Viewing the windows event logs
6. Powershell based management

- **Restart windows server**

This point show us how to restart windows server using GUI

Click on the **start** menu > power button > **Restart**

How to restart windows server using command prompt

1. Open the command. Press ctrl+Alt+Del. The system should present a menu – Click task manager
2. Reboot the window server Operating system. In the command prompt window, type windows server restart command, then press Enter: shutdown -r

D. <u>Illustrate an administrative Tools and Remote Server Administration Tools</u>

✓ **Remote Server Administration Tools** (RSAT) enables IT administrators to **remotely** manage roles and features in Windows **Server** from a computer that is running Windows 10, Windows 8.1, Windows 8, Windows 7, or Windows Vista. You cannot install RSAT on computers that are running Home or Standard editions of Windows.

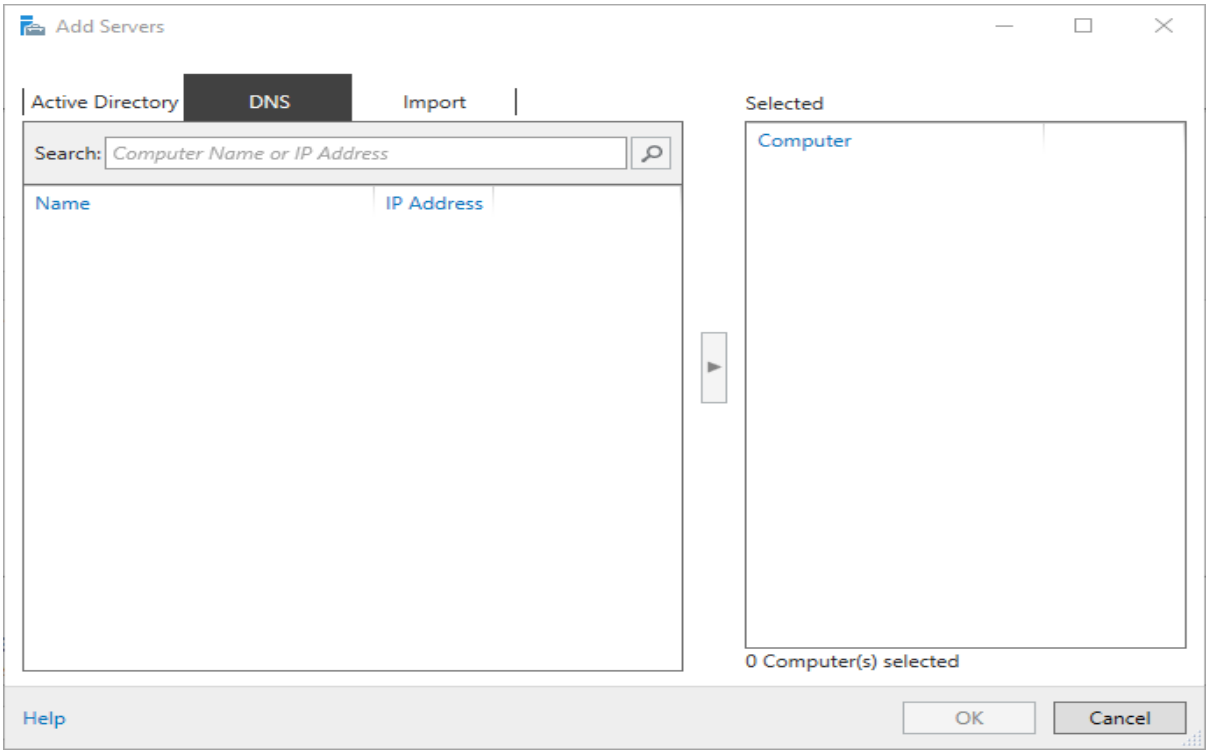
Remote Server Administration Tools in window server 2012 includes the following:

- **Server Manager**,
- Microsoft Management Console (mmc) snap-ins consoles,
- Windows PowerShell cmdlets and providers, and some command-line tools for managing roles and features that run on Windows Server.

E. <u>Managing non-domain joined Windows Server with RSAT and Server Manager</u>

Provide administrative credentials for the server not joined to the domain

To add a non-domain joined server or a Workgroup server to Server Manager, you must use DNS or Import option in the Add Servers Wizard.



Then you must right-click on the selected server and select *"Manage As"* from the context menu. This displays a Windows Security dialog box, in which you must supply the administrative credentials for the remote server.

Add the non-domain joined server to the TrustedHosts list on the computer running Server Manager.

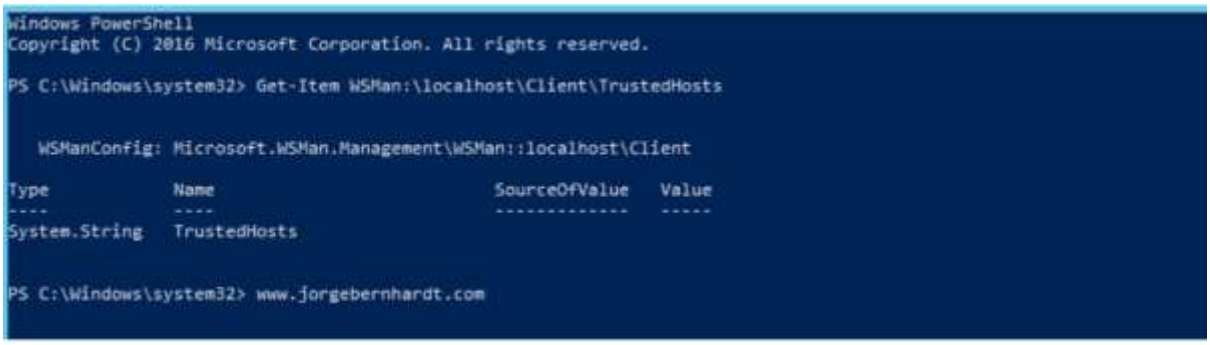
Domain membership automatically establishes a trust relationship between the computers in the domain.

To manage computers that aren't in the same domain or are in a workgroup, you must establish that trust yourself by adding the computers you want to manage to the **TrustedHosts** list on the computer running Server Manager.

The **TrustedHosts** list is located on a logical drive called WSMan:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> cd WSMan:\localhost\Client\
PS WSMan:\localhost\Client> Get-ChildItem


   WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Client

Type            Name                           SourceOfValue   Value
----            ----                           -------------   -----
System.String   NetworkDelayms                                5000
System.String   URLPrefix                                     wsman
System.String   AllowUnencrypted                              false
Container       Auth
Container       DefaultPorts
System.String   TrustedHosts


PS WSMan:\localhost\Client> www.jorgebernhardt.com
```

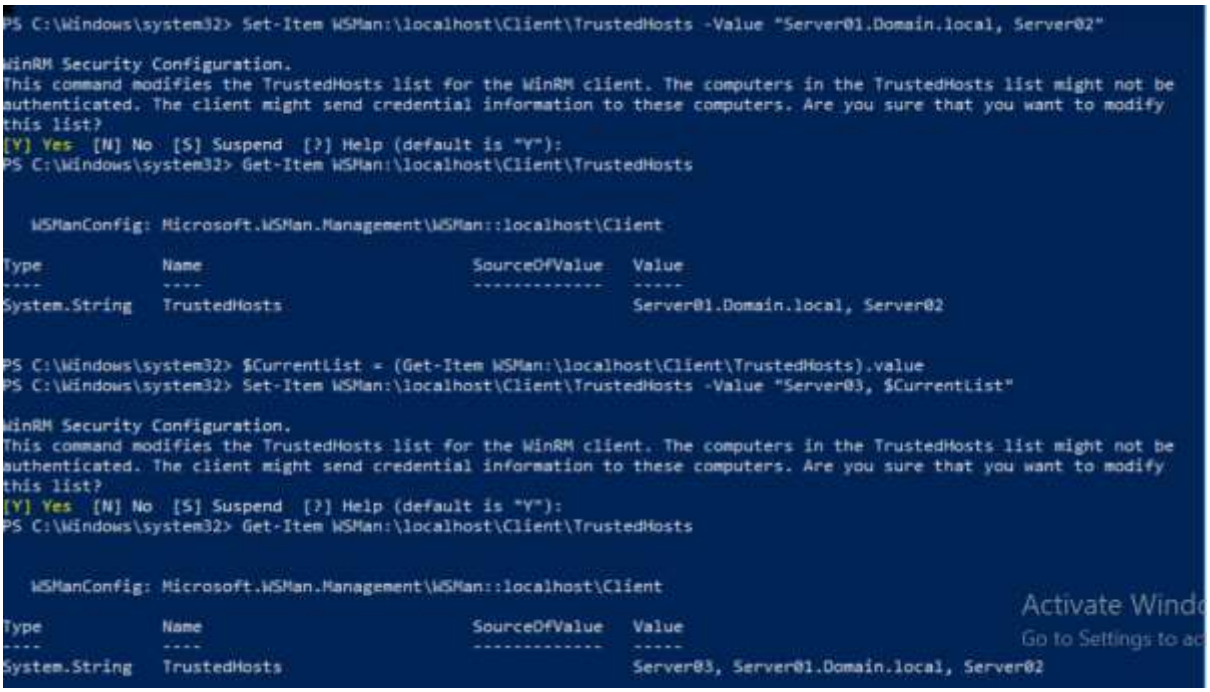
With the following command, you can see the list of machines that are in the **TrustedHosts** list, by default the list is empty.



To add a server to the list you must use the following command:

- Add specific computers to the TrustedHosts list
- Set-Item WSMan:\localhost\Client\TrustedHosts -Value "Server01.Domain.local, Server02"
- Add specific IP address to the TrustedHosts list
- Set-Item WSMan:\localhost\Client\TrustedHosts -Value 192.168.1.200
- Add all domain computers to the TrustedHosts list
- Set-Item WSMan:\localhost\Client\TrustedHosts *.Domain.local

The **TrustedHosts** list only saves the last set value. This is because the **TrustedHosts** list is updated using the **Set-Item** command that you have executed by overwriting the previous entries. if you want to add an additional computer, without deleting the previous entries, you must use the following method.



```
PS C:\Windows\system32> www.jorgebernhardt.com
```

F. Configuring Services

- **Startup Types**

There are several Acceptable startup types include:

- ✓ **Automatic**: The service starts at system logon.
- ✓ **Automatic** (Delayed): The service starts a short while after the system has finished starting up. ...
- ✓ **Manual**: The service starts only when explicitly summoned.
- ✓ **Disabled**: The service is **disabled**.

- **Service Recovery** As you probably know **Windows** has the ability to automatically perform some predefined action in response to the failure of a **Windows Service**. The **Recovery** tab in the **Service** property page let you in fact define the actions that the system has to perform on first failure, second failure, and subsequent failures.

Configure recovery settings for Windows services

1. Start the **Windows** Services manager.
2. Right-click the ArcGIS Monitor **Service** <Name> **service** that needs to be updated and click Properties.
3. Click the **Recovery** tab.
4. Choose Restart the **Service** in the First failure, Second failure, and Subsequent failures drop-down menus.
5. Type 1 in the Restart **service** after text box.

- **Managed Service Accounts** Group **Managed Service Accounts** can only be configured and administered on computers running **Windows Server 2012** but can be deployed as a single **service** identity solution in domains that still have some DCs running operating systems earlier than **Windows Server 2012**.

G. Installation and Managing an Active Directory Domain Services

1. Overview of AD DS

Active Directory Domain Services (**AD DS**) are the core functions in **Active Directory** that manage users and computers and allow system admins to organize the data into logical hierarchies. **AD DS** provides for security certificates, Single Sign-On (SSO), LDAP, and rights management.

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts. For more information about the Active Directory data store, see Directory data store.

Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network. For more information about Active Directory security, see Security overview.

Active Directory also includes:

- A set of rules, **the schema**, that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects,

and the format of their names. For more information about the schema, see Schema.

- A **global catalog** that contains information about every object in the directory. This allows users and administrators to find directory information regardless of which domain in the directory actually contains the data. For more information about the global catalog, see The role of the global catalog.
- A **query and index mechanism**, so that objects and their properties can be published and found by network users or applications. For more information about querying the directory, see Finding directory information.
- A **replication service** that distributes directory data across a network. All domain controllers in a domain participate in replication and contain a complete copy of all directory information for their domain. Any change to directory data is replicated to all domain controllers in the domain. For more information about Active Directory replication, see Replication overview.

2. **Components of Active Directory**

Component	**Description**
Organization unit	Organizational units are container objects. You use these container objects to arrange other objects in a manner that supports your administrative purposes. By arranging objects in organizational units , you make it easier to locate and manage them. You can also delegate the authority to manage an organizational unit. Organizational units can be nested in other Organizational units. You can arrange objects that have similar administrative and security

	requirements into organizational units. Organizational units provide multiple levels of administrative authority, so that you can Apply Group Policy settings and delegate administrative control.
Domains	Domains are container objects. Domains are a collection of administratively defined objects that share a common directory database, security policies, and trust relationships with other domains. In this way, each domain is an administrative boundary for objects. A single domain can span multiple physical locations or sites and can contain millions of objects.
Domain Trees	Domain trees are collections of domains that are grouped together in hierarchical structures. When you add a domain to a tree, it becomes a child of the tree root domain. The domain to which a child domain is attached is called the parent domain. A child domain might in turn have its own child domain. The name of a child domain is combined with the name of its parent domain to form its own unique Domain Name System

	(DNS) name such as Corp.nwtraders.msft. In this manner, a tree has a contiguous namespace.
Forest	A forest is a complete instance of Active Directory. Each forest acts as a top-level container in that it houses all domain containers for that particular Active Directory instance. A forest can contain one or more domain container objects, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. The first domain in the forest is called the forest root domain. The name of that domain refers to the forest, such as Nwtraders.msft. By default, information in Active Directory is shared only within the forest. In this way, the forest is a security boundary for the information that is contained in that instance of Active Directory.

By understanding the purpose and hierarchical structure of these components, you can complete a variety of tasks, including installing, configuring, managing, and troubleshooting Active Directory. Although the logical structure of Active Directory is a hierarchical

organization of all users, computers, and other physical resources, the forest and domain form the basis of the logical structure.

Forests, which are the security boundaries of the logical structure, can be structured to provide data and service autonomy and isolation in an organization in ways that can both reflect site and group identities and remove dependencies on the physical topology. Domains can be structured within a forest to provide data and service autonomy (but not isolation) and to optimize replication with a given region.

This separation of logical and physical structures improves manageability and reduces administrative costs because the logical structure is not impacted by changes in the physical structure, such as the addition, removal, or reorganization of users and groups.

Note

• You can view and manage components of the logical structure by using the Active Directory Users and Computers, Active Directory Domains and Trusts, and Active Directory Schema Microsoft Management Console (MMC) snap-ins, and other tools.

3. Benefits of Active Directory

- Single user name and password - NetID
- Password synced between AD and LDAP Directory Services
- Reduce overhead through standardization
- Improve services through centralized management capabilities
- Provide foundation for the following AD related services:
- Exchange
- SharePoint
- Improve workstation security
- Central storage provided for individuals and departments
- Backup and restoration services for central storage
- Server storage space for user documents
- Backed up data on Home and Departmental drives

4. Overview of Domain Controllers

Domain Controllers Domain Controller is used in windows based operating systems for security authentication of users, computers etc. It is a central database for storing users

account information and security enforcement. For example, DC helps which users to allow or deny the access to a particular folder in a particular domain.

5. Installing a Domain Controller

AD DS can be installed in Windows Server 2012 r2 by using the Add Roles Wizard in Server Manager, followed by the Active Directory Domain Services Configuration Wizard, which is new beginning in Windows Server 2012 r2. The Active Directory Domain Services Installation Wizard (dcpromo.exe) is deprecated beginning in Windows Server 2012 r2.

The following sections explain how to create server pools in order to install and manage AD DS on multiple servers, and how to use the wizards to install AD DS.

To Configure Windows Active Directory and Domain Controller

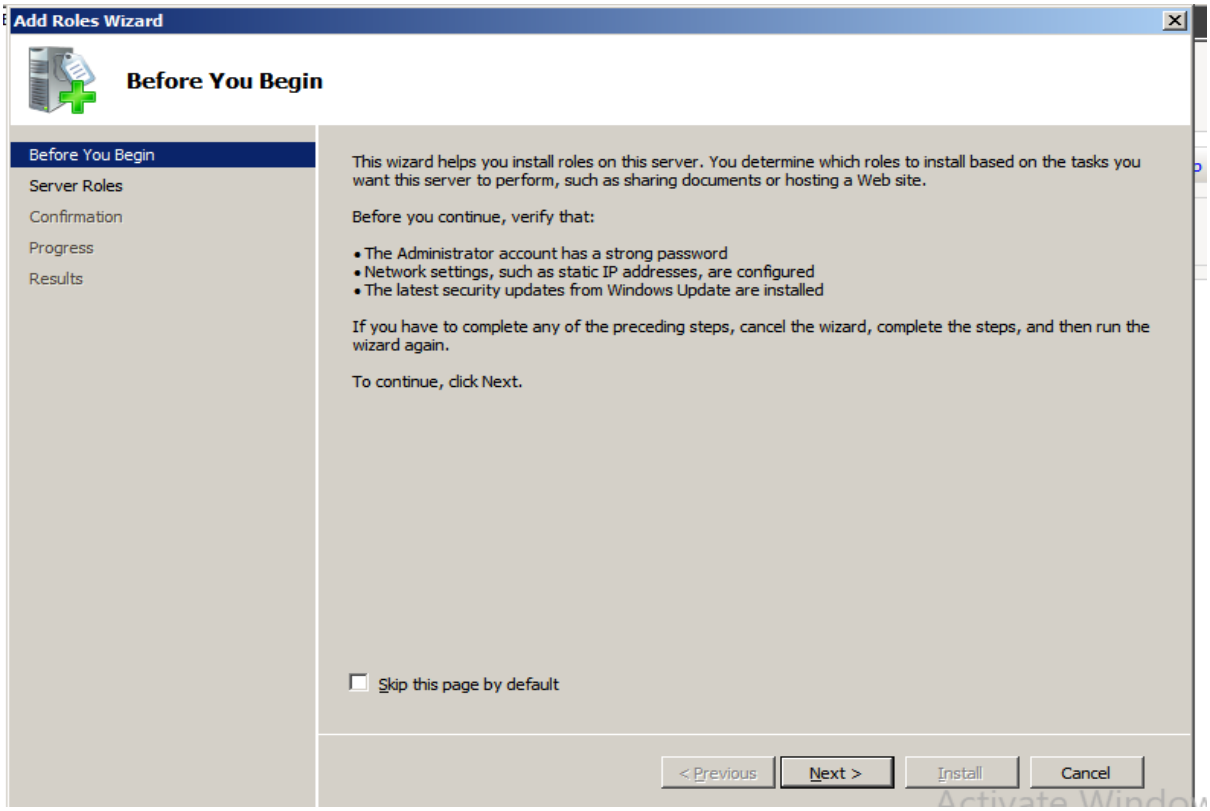
1. Log in as an administrator to the Windows 2000 or 2003 server host.
2. From the Start menu, go to Administrative Tools > Manage Your Server. ...
3. **Install** the Active Directory **Domain Controller**. ...
4. **Install** Windows Support Tools. ...
5. Create a new user account. ...
6. Create a user account to map to the Kerberos service.

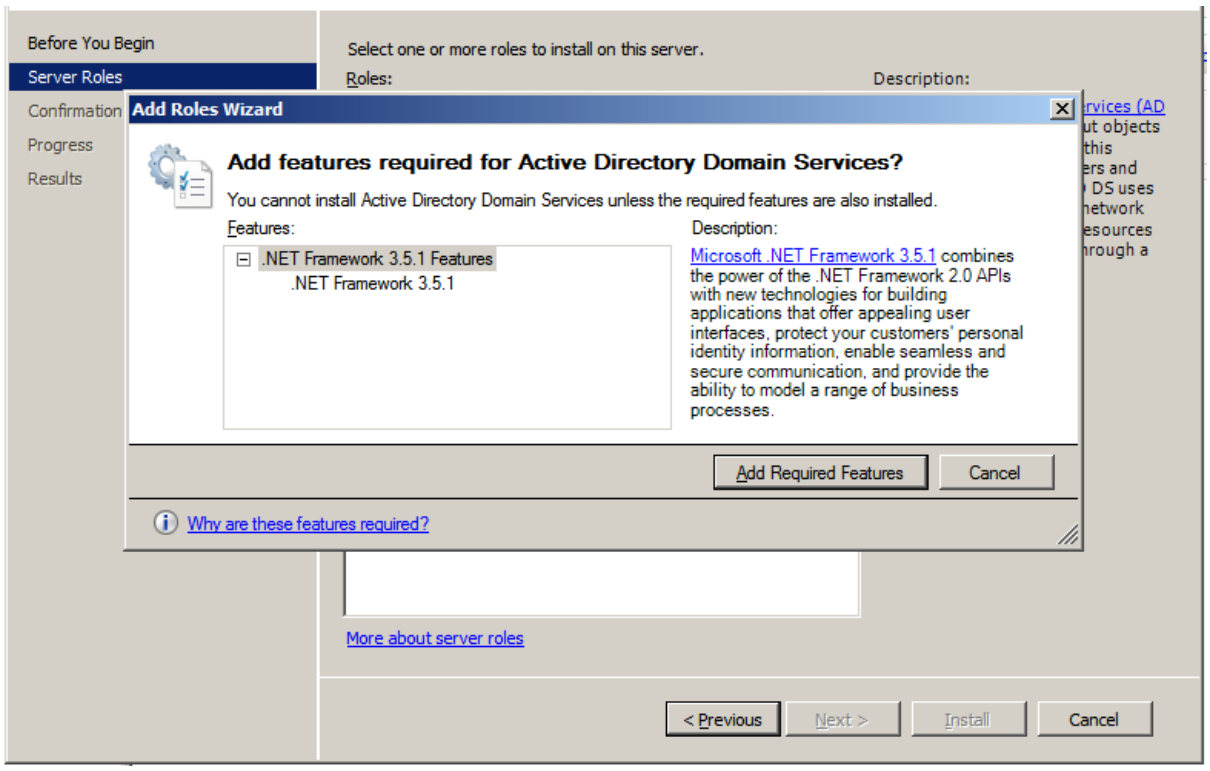
6. The steps of Installing AD DS

To install AD DS by using Server Manager

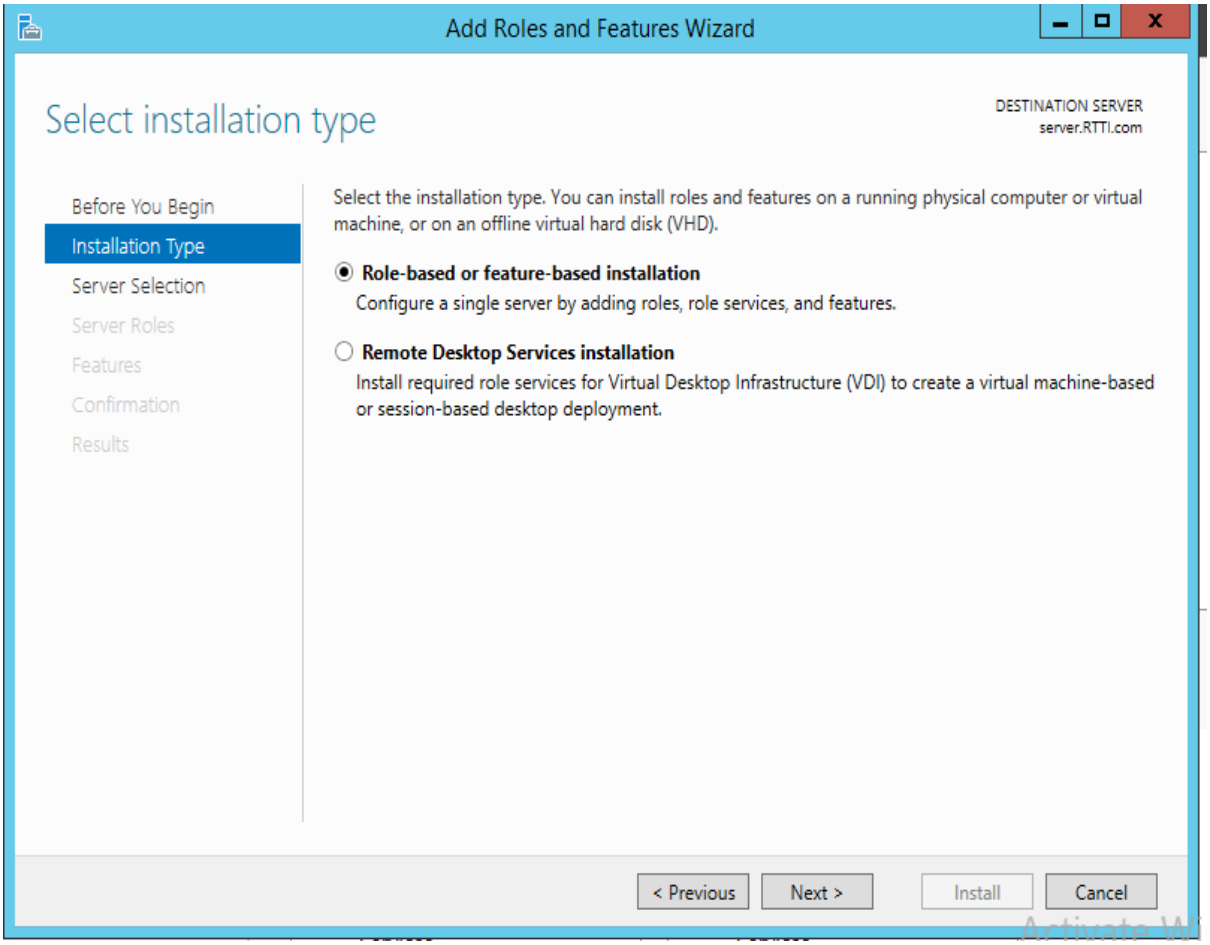
1. In Server Manager, click **Manage** and click **Add Roles and Features** to start the Add Roles Wizard.

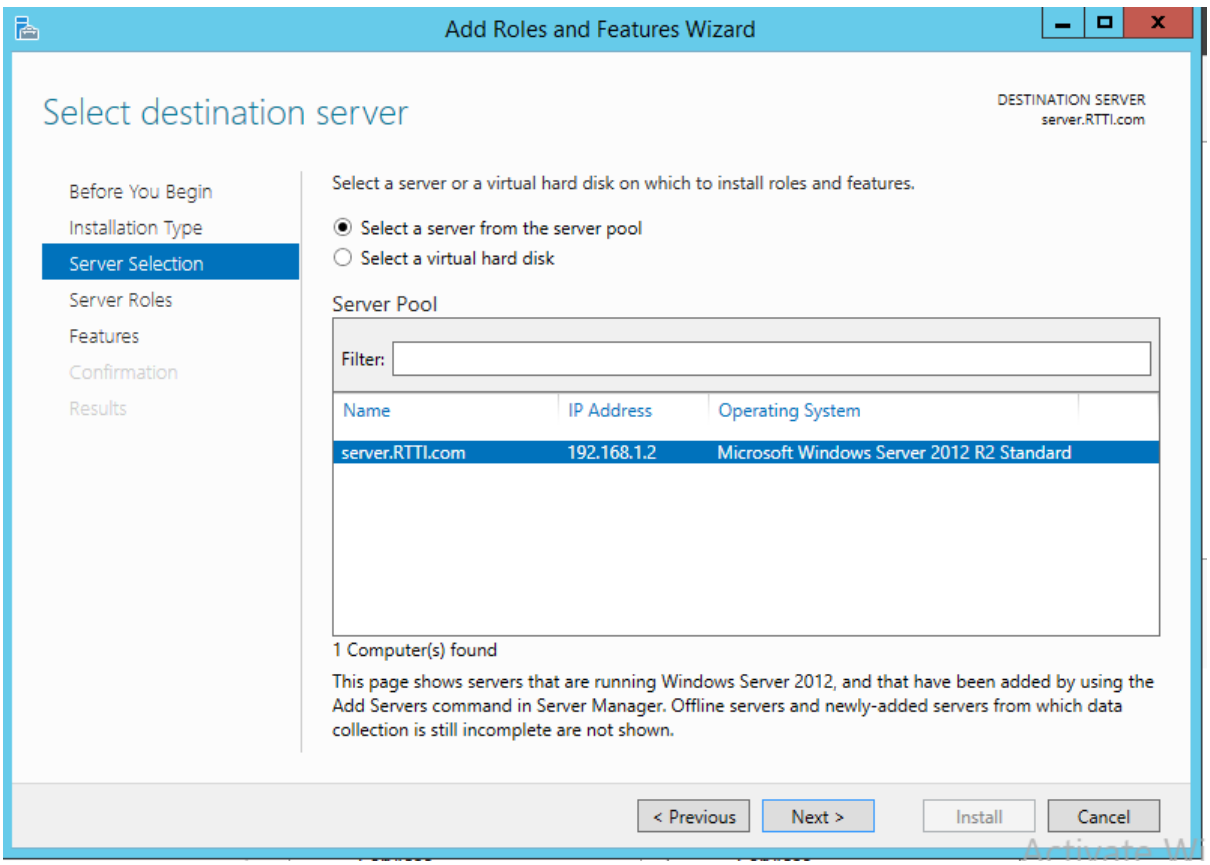
2. On the **before you begin** page, click **Next**.



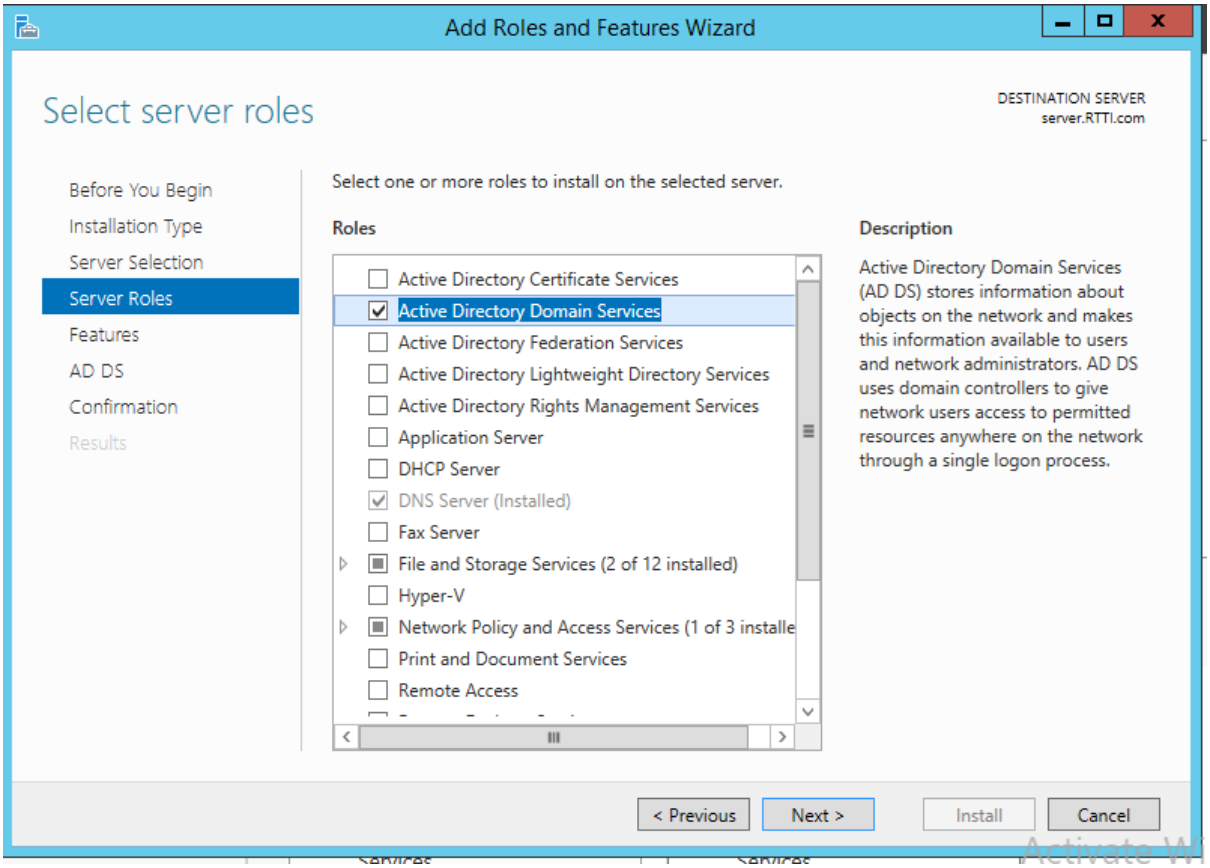


3. On the **Select installation type** page, click **Role-based or feature-based installation** and then click **Next**.

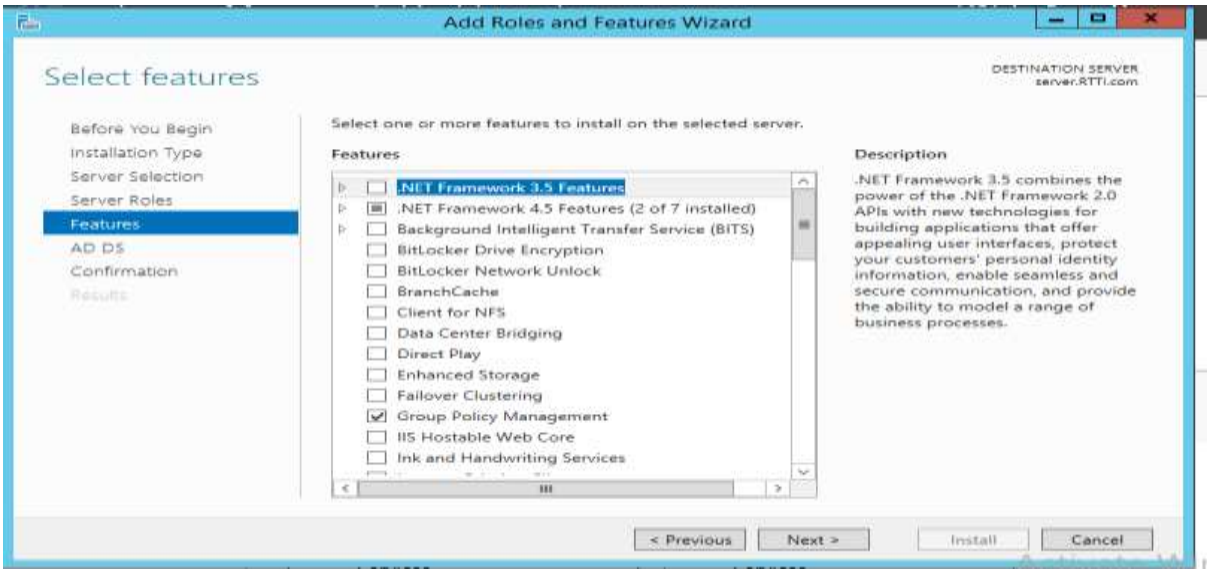

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
server.RTTI.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
server.RTTI.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
server.RTTI.com
192.168.1.2
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

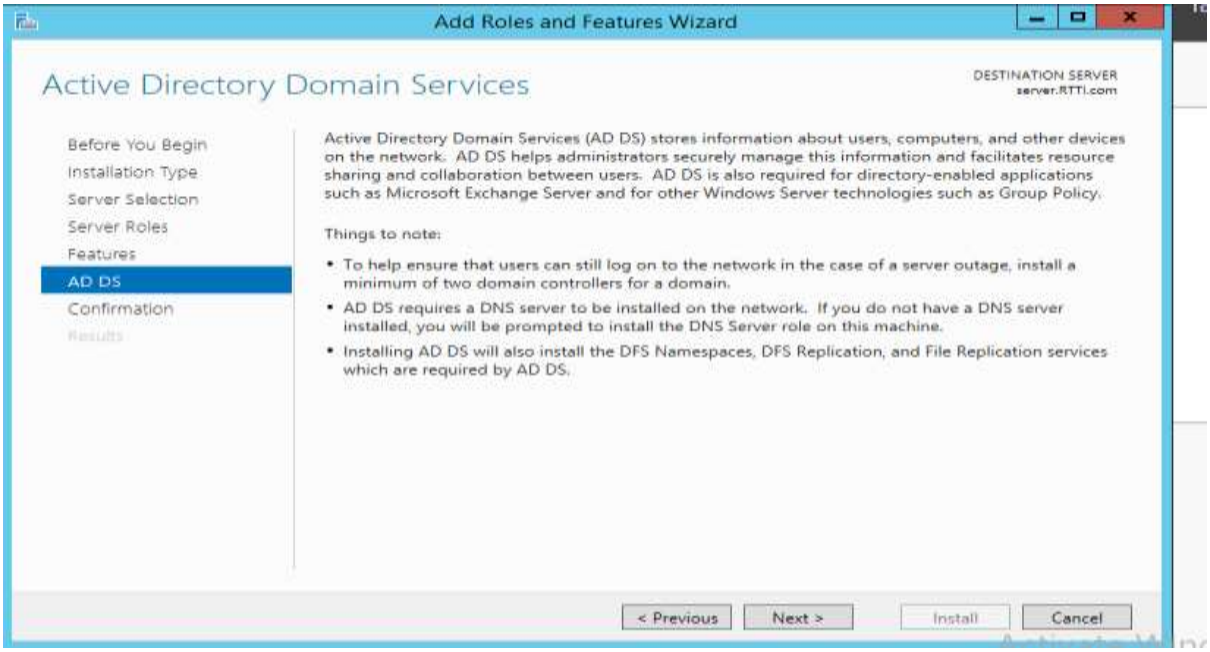
5. On the **Select server roles** page, click **Active Directory Domain Services**, then on the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then click **Next**.



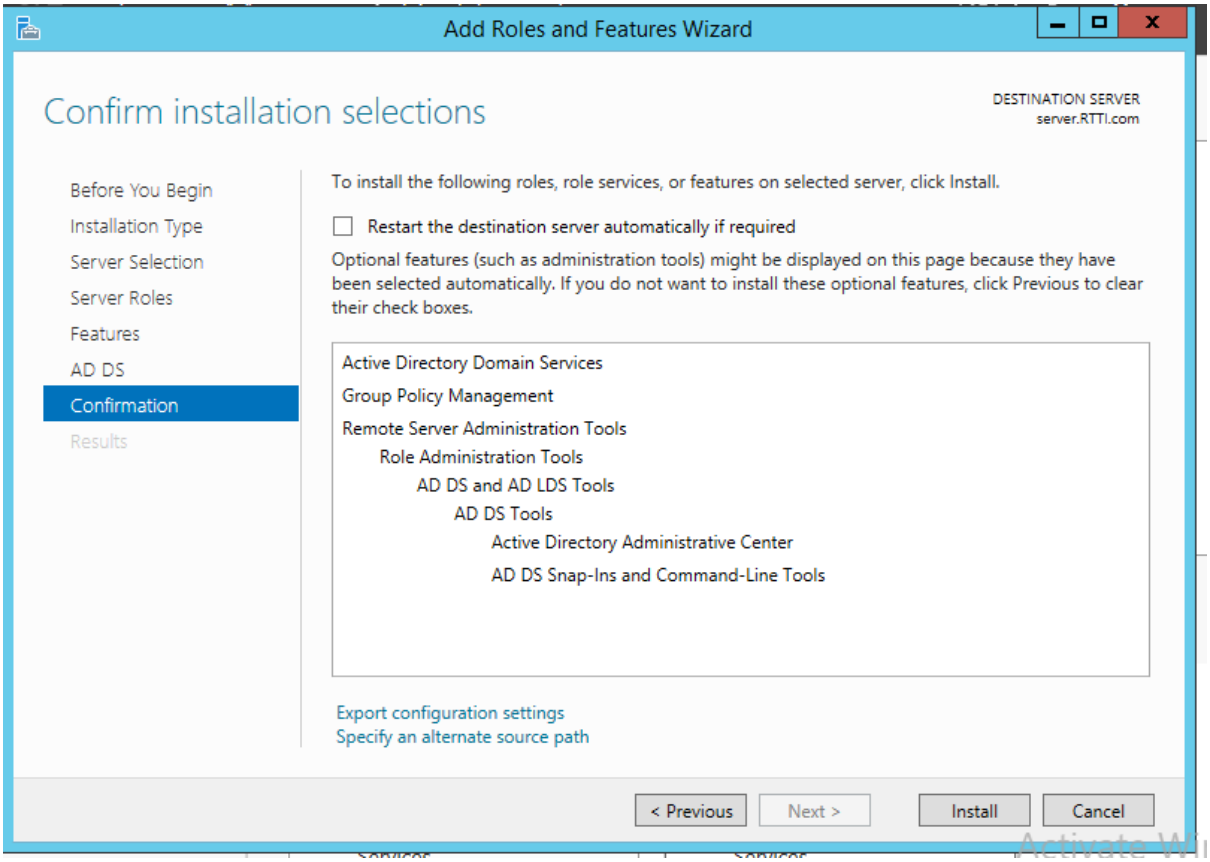
6. On the **Select features** page, select any additional features you want to install and click next



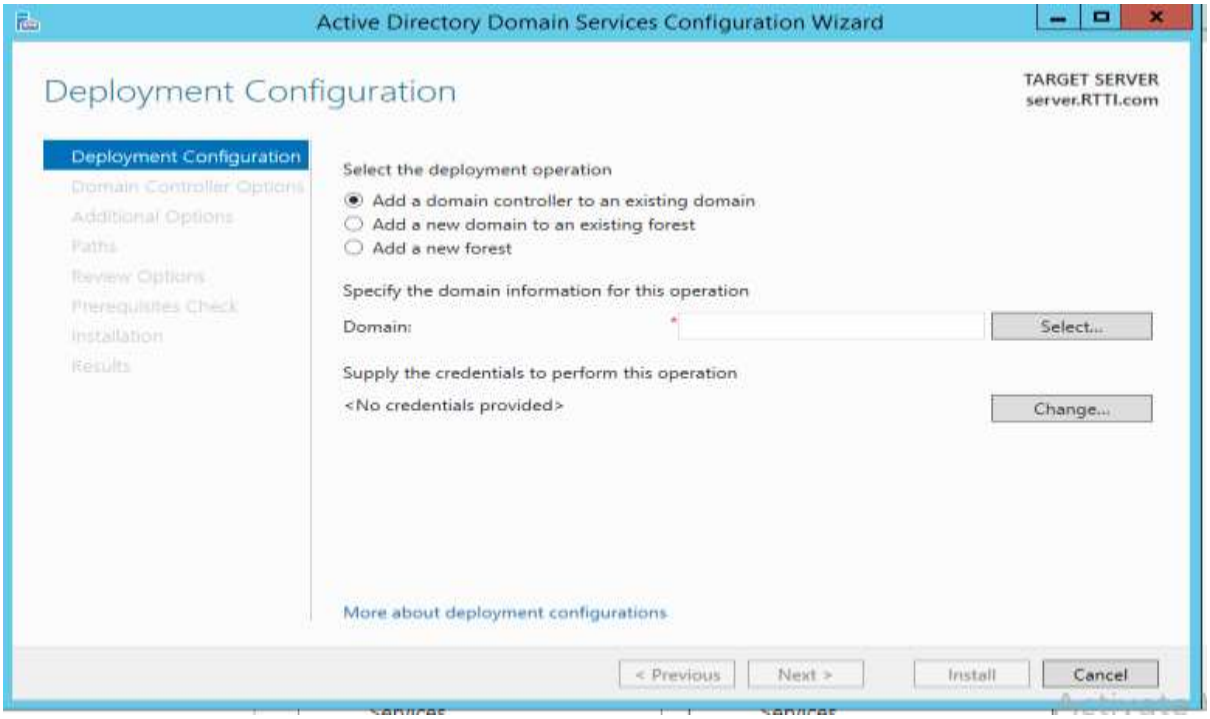
7. On the **Active Directory Domain Services** page, review the information and then click **next**.



8. On the **Confirm installation selections** page, click **Install**.



9. On the **Results** page, verify that the installation succeeded, and click **Promote this server to a domain controller** to start the Active Directory Domain Services Configuration Wizard.



10. On the **Deployment Configuration** page, choose one of the following options:

o If you are installing an additional domain controller in an existing domain, click **Add a domain controller to an existing domain**, and type the name of the domain (for example, emea.corp.contoso.com) or click **Select...** to choose a domain, and credentials (for example, specify an account that is a member of the Domain Admins group) and then click **Next**.

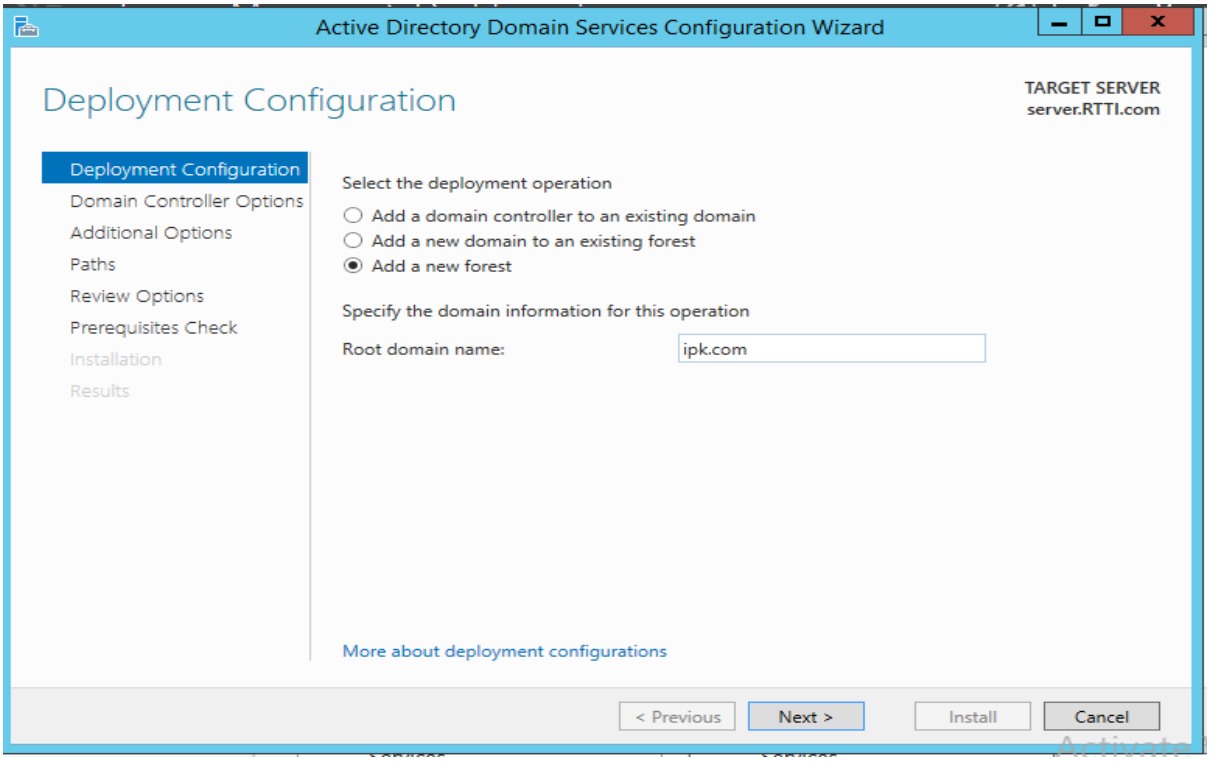
Note

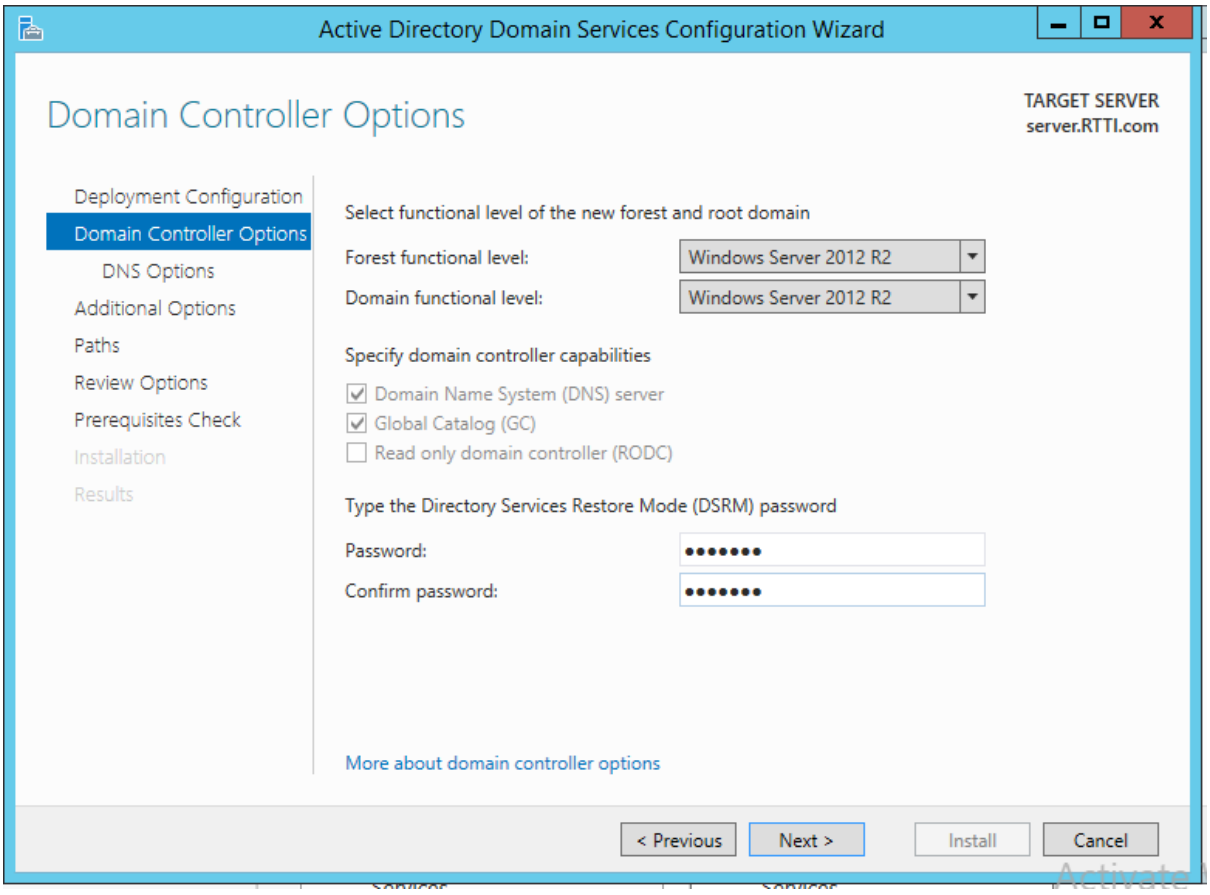
The name of the domain and current user credentials are supplied by default only if the machine is domain-joined and you are performing a local installation. If you are installing AD DS on a remote server, you need to specify the credentials, by design. If current user credentials are not sufficient to perform the installation, click **Change...** in order to specify different credentials.

o If you are installing a new child domain, click **Add a new domain to an existing forest**, for **Select domain type**, select **Child Domain**, type or browse to the name of the parent domain DNS name (for example, corp.contoso.com), type the relative name of the new child domain (for example emea), type credentials to use to create the new domain, and then click **Next**.

o If you are installing a new domain tree, click **Add new domain to an existing forest**, for **Select domain type**, choose **Tree Domain**, type the name of the root domain (for example, corp.contoso.com), type the DNS name of the new domain (for example, fabrikam.com), type credentials to use to create the new domain, and then click **Next**.

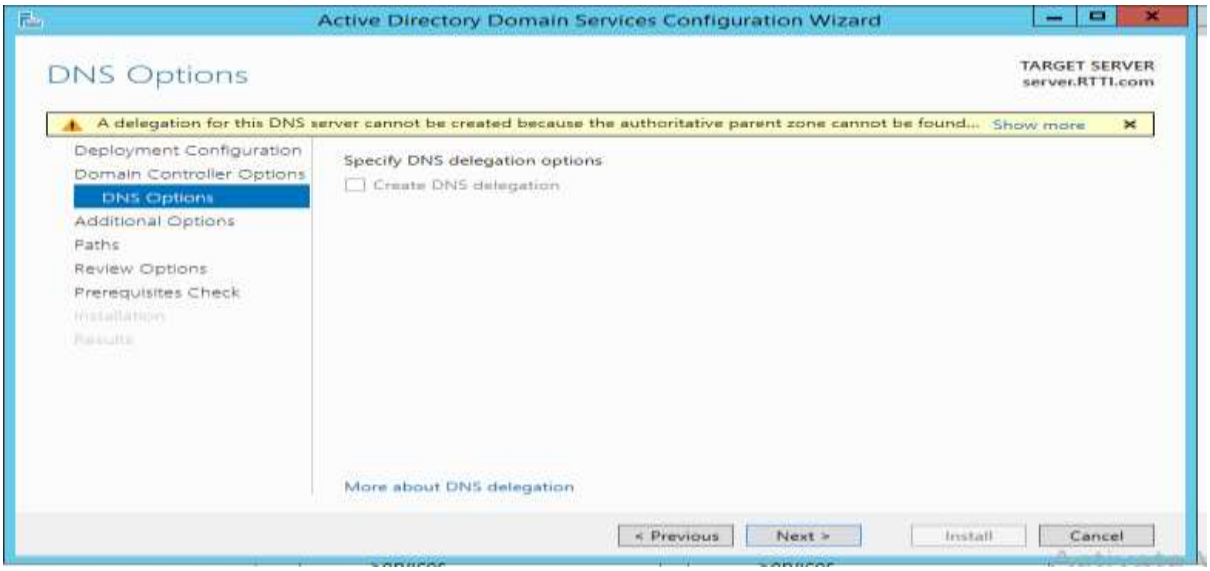
o If you are installing a new forest, click **Add a new forest** and then type the name of the root domain (for example, ipk.com).



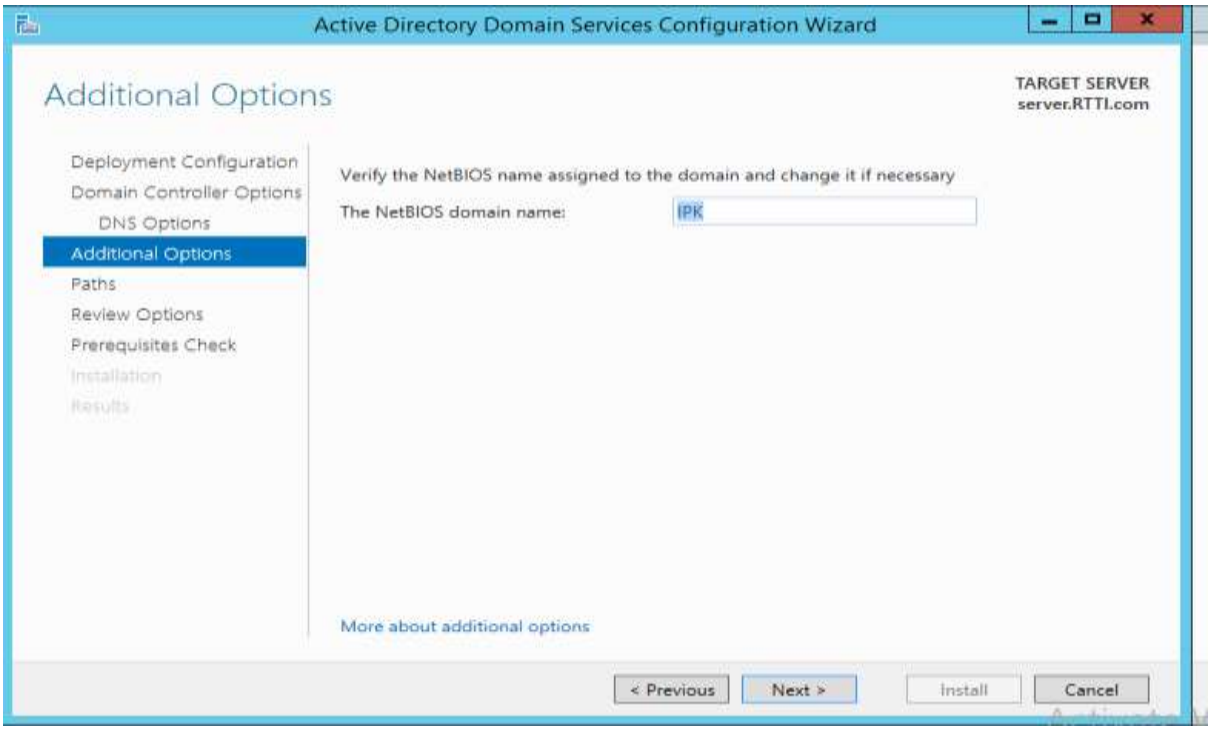


12. On the **DNS Options** page (which appears only if you install a DNS server), click **Update DNS delegation** as needed. If you do, provide credentials that have permission to create DNS delegation records in the parent DNS zone.

If a DNS server that hosts the parent zone cannot be contacted, the **Update DNS Delegation** option is not available. Click next



13. On the **RODC Options** page (which appears only if you install an RODC), specify the name of a group or user who will manage the RODC, add accounts to or remove accounts from the Allowed or Denied password replication groups, and then click **Next**.

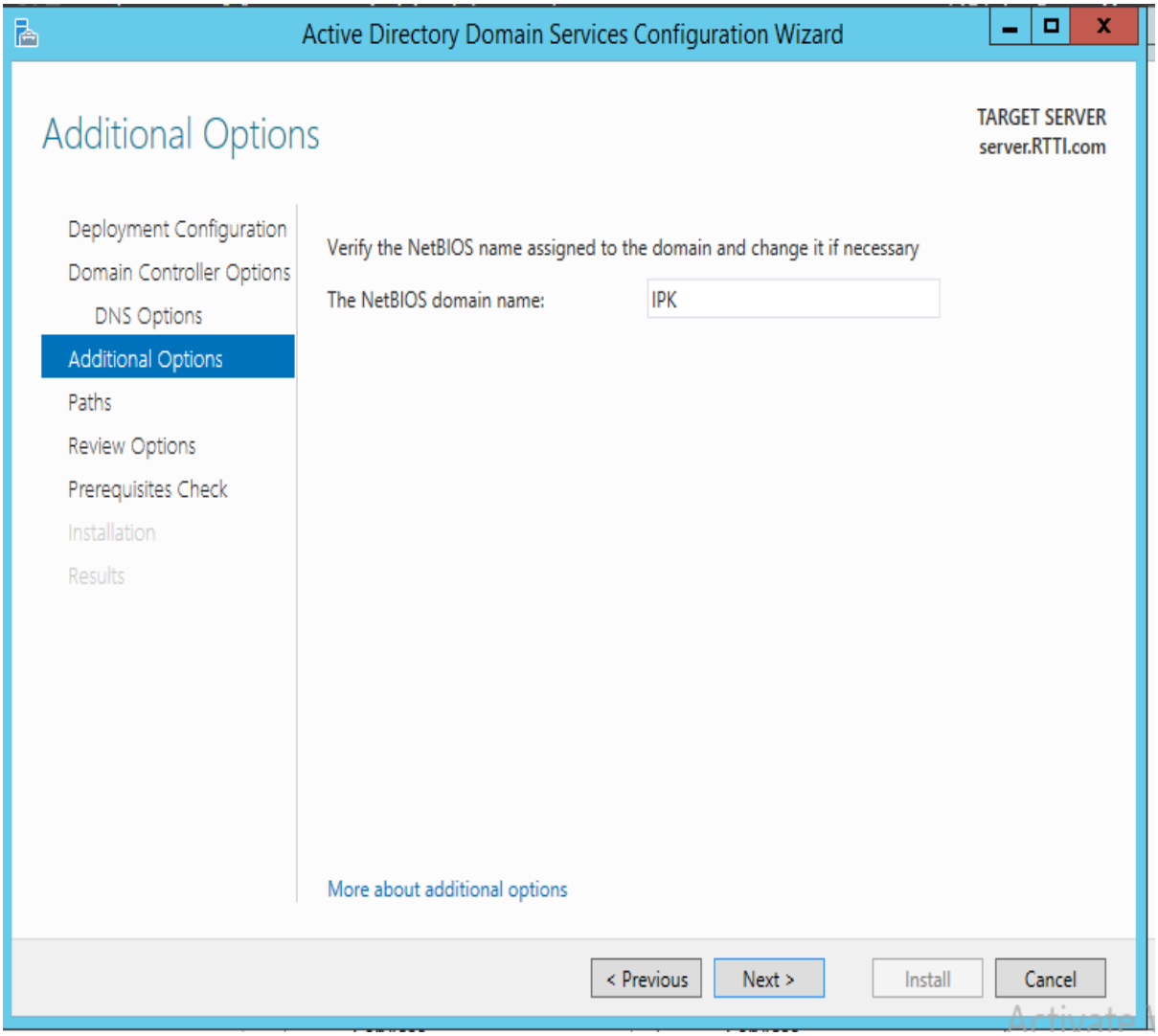


14. On the **Additional Options** page, choose one of the following options:

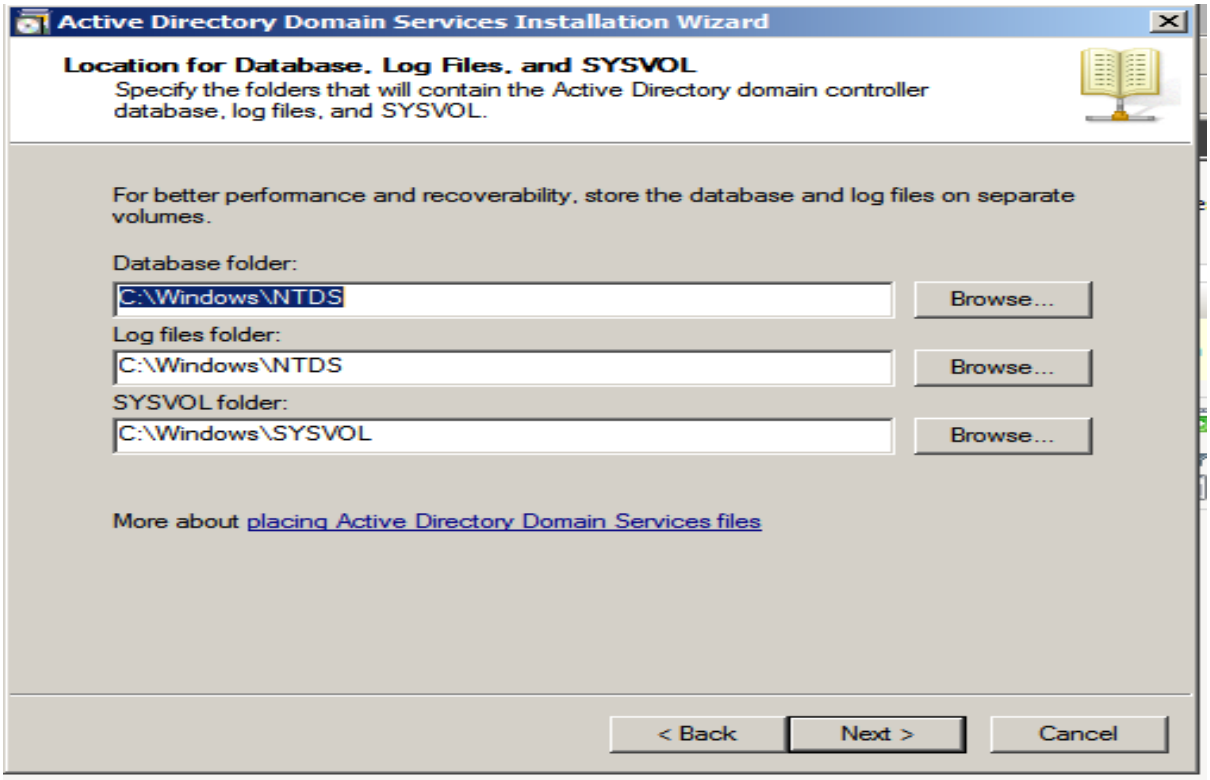
o If you are creating a new domain, type a new NetBIOS name or verify the default NetBIOS name of the domain, and then click **Next**.

o If you are adding a domain controller to an existing domain, select the domain controller that you want to replicate the AD DS installation data from (or allow the wizard to select any domain controller). If you are installing from media, click **Install from media path** type and verify the path to the installation source files, and then click **Next**.

You cannot use install from media (IFM) to install the first domain controller in a domain. IFM does not work across different operating system versions. In other words, in order to install an additional domain controller that runs Windows Server 2012 by using IFM, you must create the backup media on a Windows Server 2012 domain controller.



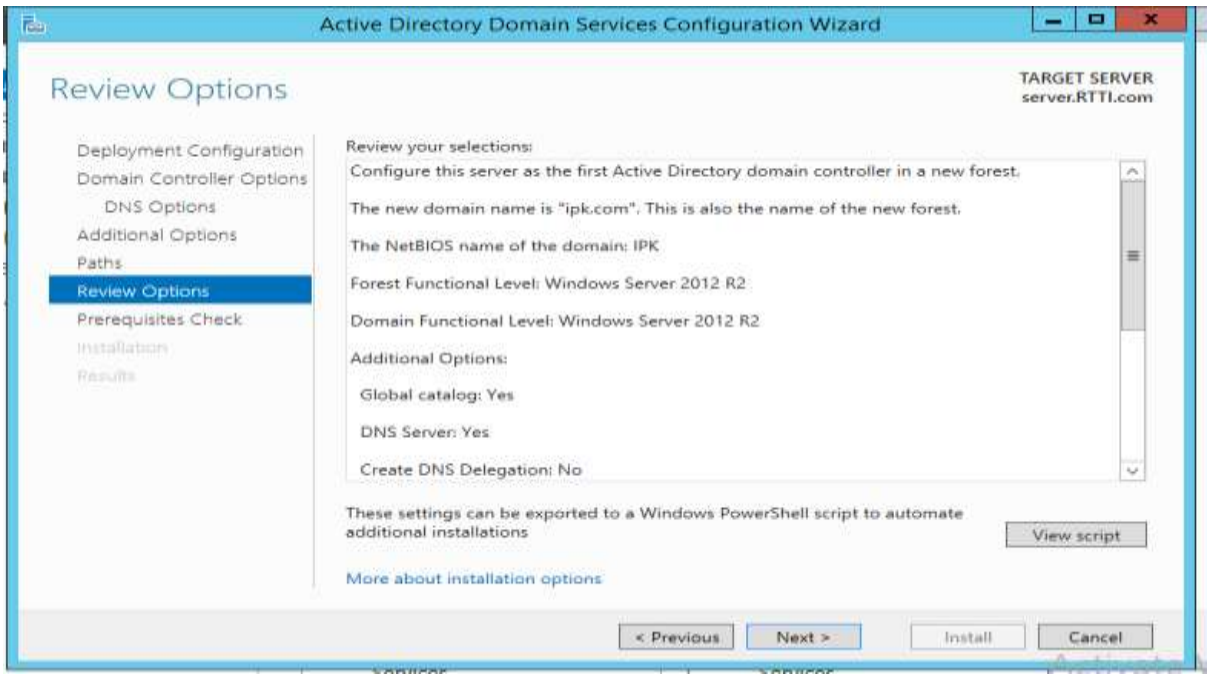
15. On the **Paths** page, type the locations for the Active Directory database, log files, and SYSVOL folder (or accept default locations), and click **Next**.



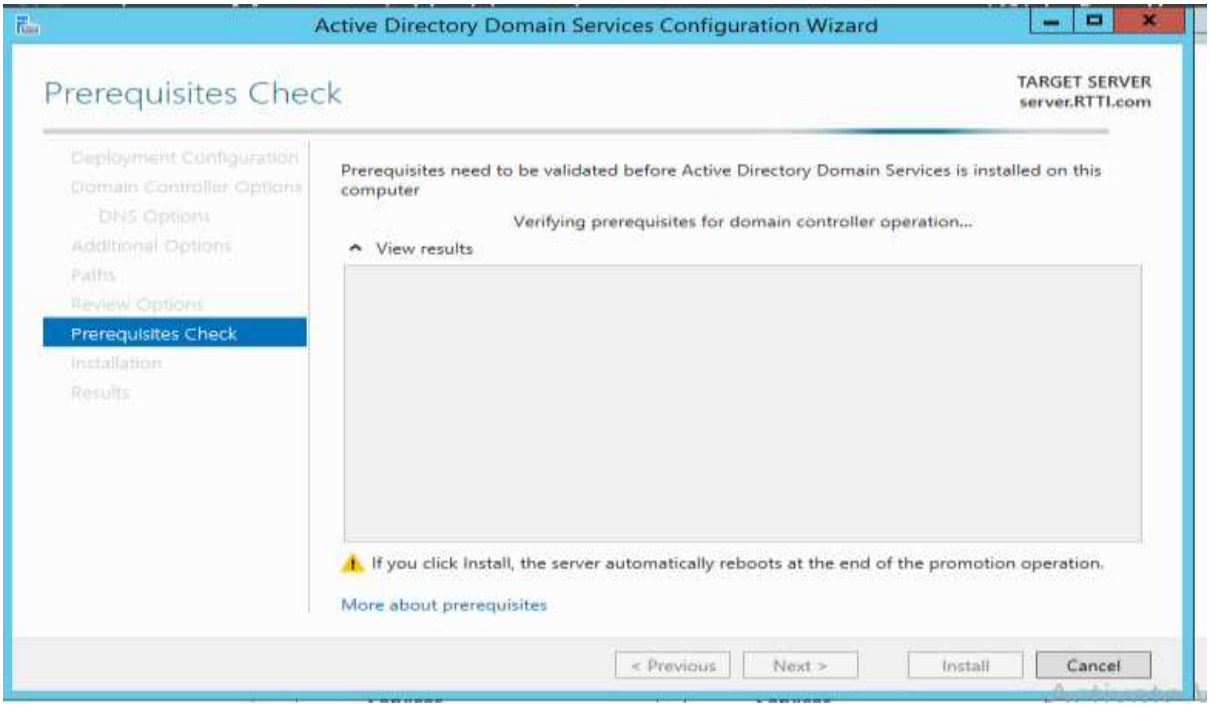
Important

Do not store the Active Directory database, log files, or SYSVOL folder on a data volume formatted with Resilient File System (ReFS).

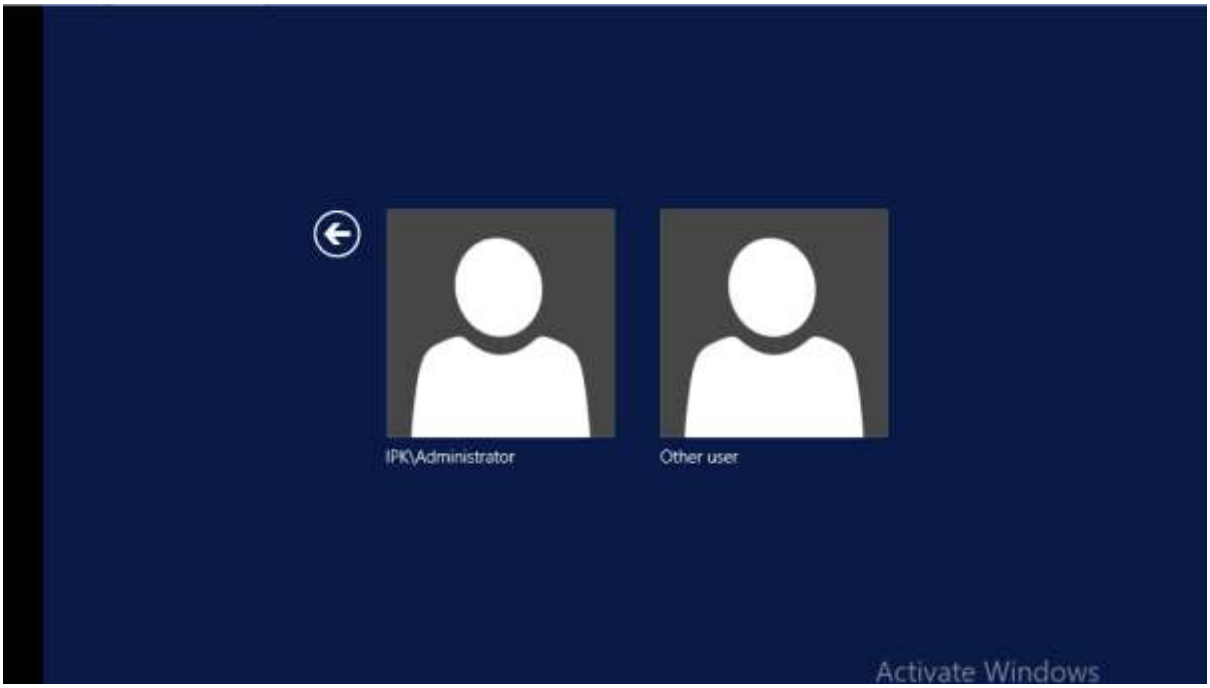
16. On the **Review Options** page, confirm your selections, click **View script** if you want to export the settings to a Windows PowerShell script, and then click **Next**.



17. On the **Prerequisites Check** page, confirm that prerequisite validation completed and then click **Install**.



18. On the **Results** page, verify that the server was successfully configured as a domain controller. The server will be restarted automatically to complete the AD DS installation.



- **Content/Topic 2: Managing Active Directory Domain Services Objects**

1. **Managing User Accounts:**

By using the Active Directory Users and Computers Snap-in

1. To start the Active Directory Users and Computers snap-in, click **Start**, point to **Programs**, point to **Administrative Tools**, and then **click Active Directory Users and Computers**.

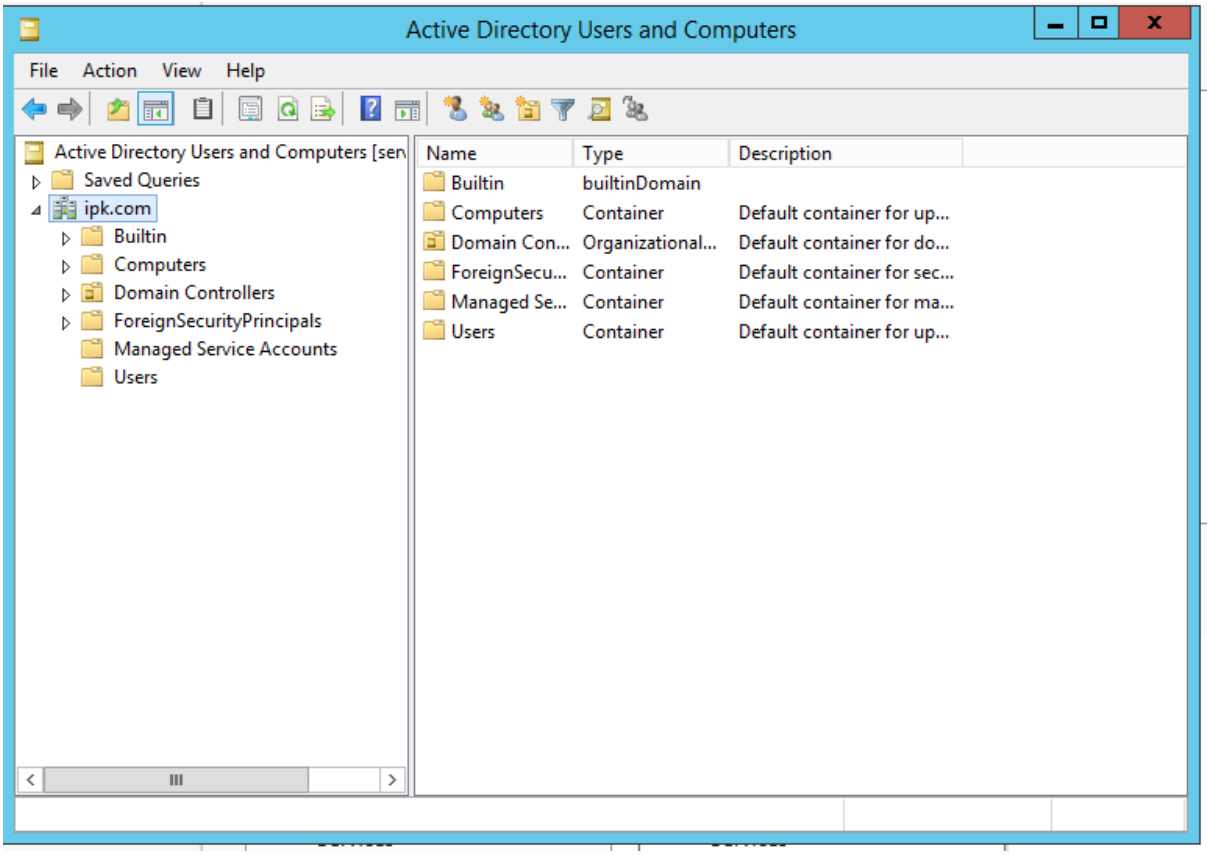
2. Expand **Reskit.com** by clicking **+**.

Figure 2 below displays the key components of the **Active Directory Users and Computers** snap-in. **Using the ActiveDirectory Users and Computers Snap-in**

1. To start the Active Directory Users and Computers snap-in, click **Start**, point to **Programs**, point to **Administrative Tools**, and then **click Active Directory Users and Computers**.

2. Expand **Reskit.com** by clicking **+**.

Figure 2 below displays the key components of the **Active Directory Users and Computers** snap-in.



1.1 Recognizing Active Directory Objects

The objects described in the following table are created during the installation of Active Directory.

Icon	Folder	Description
	Domain	The root node of the snap-in represents the domain being administered.
	System	Contains Active Directory systems and services information.
	user	Contains all the users in the domain. In an upgrade, all users from the previous domain will be migrated. Like computers, the user objects can be moved.

You can use Active Directory to create the following objects.

Icon	Object	Description
	User	A user object is an object that is a security principal in the directory. A user can log on to the network with these credentials and access permissions can be granted to users.
	Contact	A contact object is an account that does not have any security permissions. You cannot log on to the network as a contact. Contacts are typically used to represent external users for the purpose of e-mail.
	Computer	An object that represents a computer on the network. For Windows NT-based workstations and servers, this is the machine account.
	Organizational Unit	Organizational units are used as containers to logically organize directory objects such

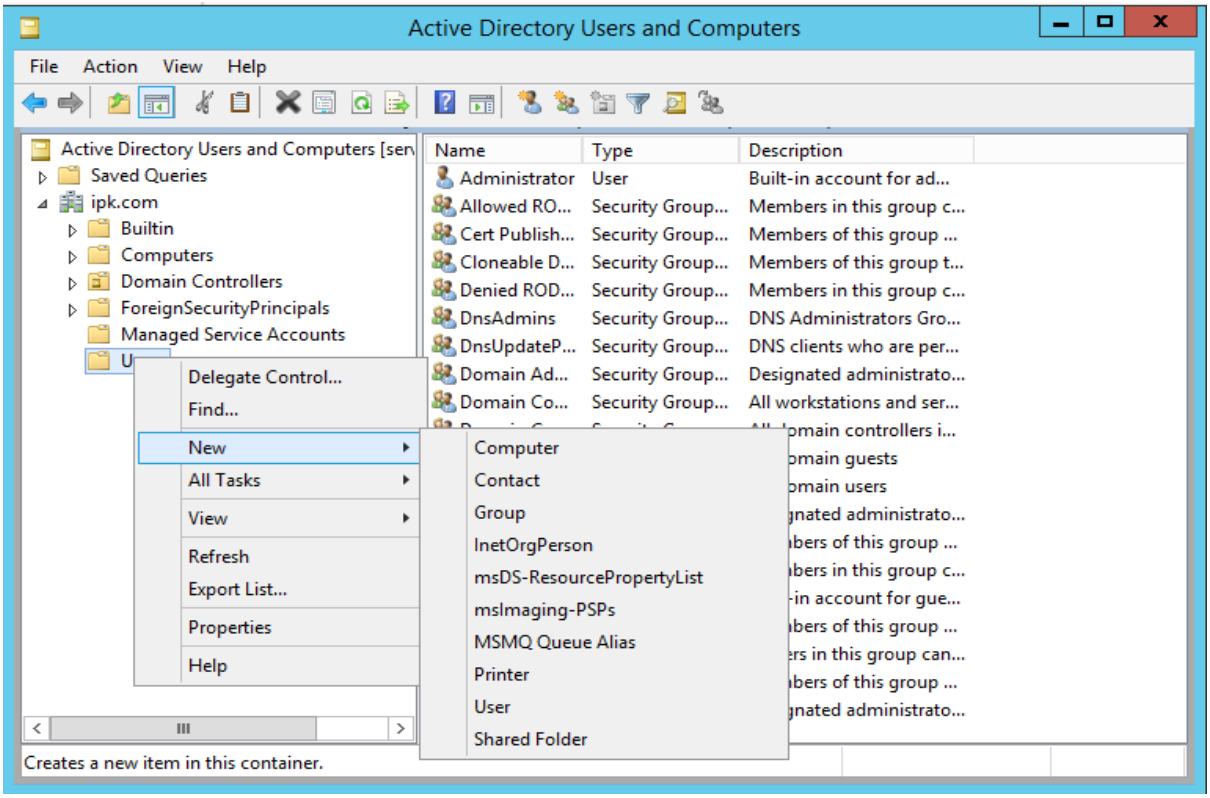
		as users, groups, and computers in much the same way that folders are used to organize files on your hard disk.
	Group	Groups can have users, computers, and other groups. Groups simplify the management of large numbers of objects.
	Shared Folder	A shared Folder is a network share that has been published in the directory.
	Shared printer	A shared printer is a network printer that has been published in the directory

1.2 Creating a User Account

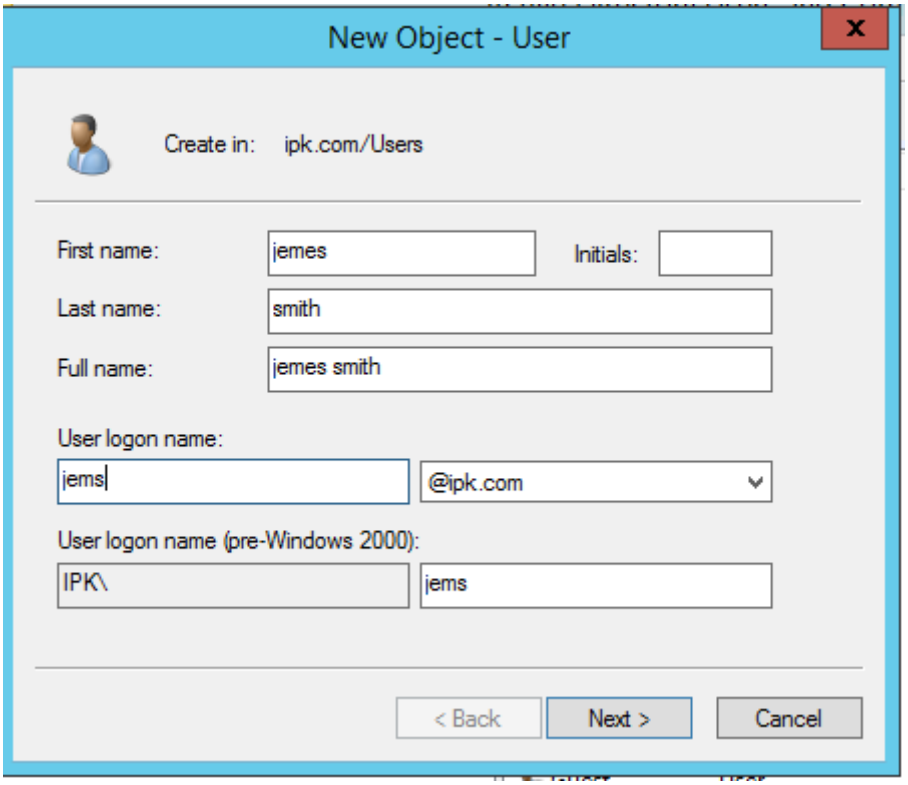
The following procedure creates the user account **James Smith** in the **Construction** OU.

To create a new user account

1. Right-click the **Construction** organizational unit, point to **New**, and then click **User**, or click **New User** on the snap-in toolbar.



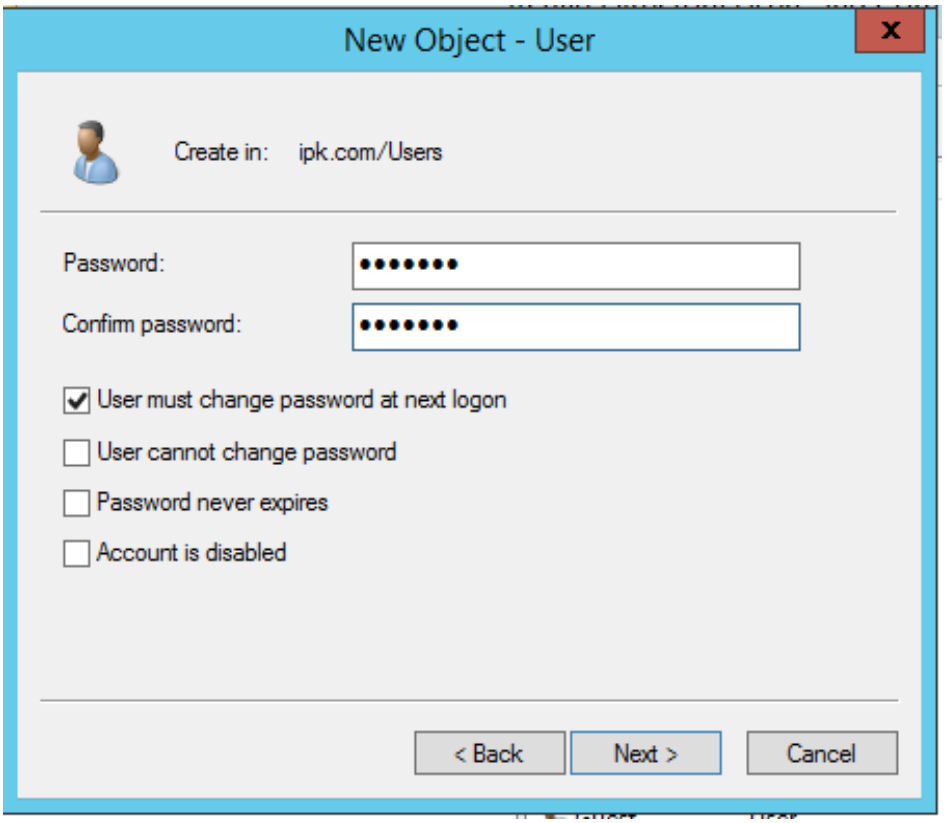
2. Type user information as in Figure 4 below:



Note that the Full name is automatically filled in after you enter the First and Last names.

Click **Next** to proceed.

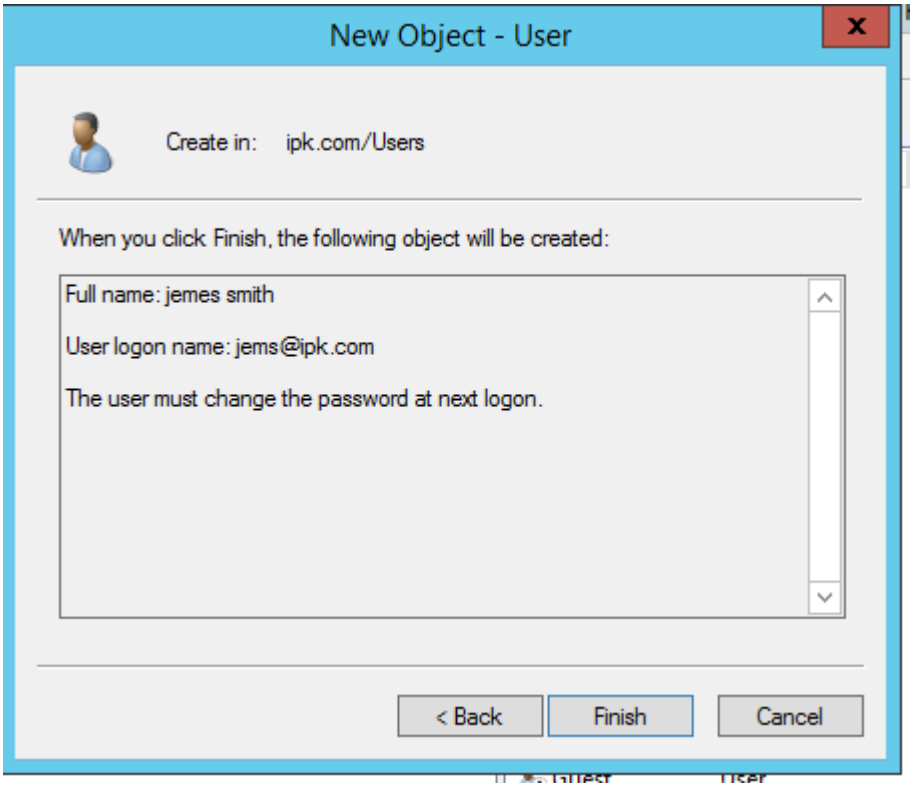
3. Type a password in both the **Password** and **Confirm password** boxes and click **Next**.



4. Accept the confirmation in the next dialog box by clicking **Finish**.

You have now created an account for James Smith in the Construction OU to add

Additional information about this user:



5. Select **Construction** in the left pane, right-click **James Smith** in the right pane, and then Click **Properties**.

6. Add more information about the user in the **Properties** dialog box on the **General** tab as shown in Figure above, and click **OK**. You are provided with this selection of optional entries. Click each tab you want to go to.

1.3 Moving a User Account

Users can be moved from one organizational unit to another in the same domain or a different

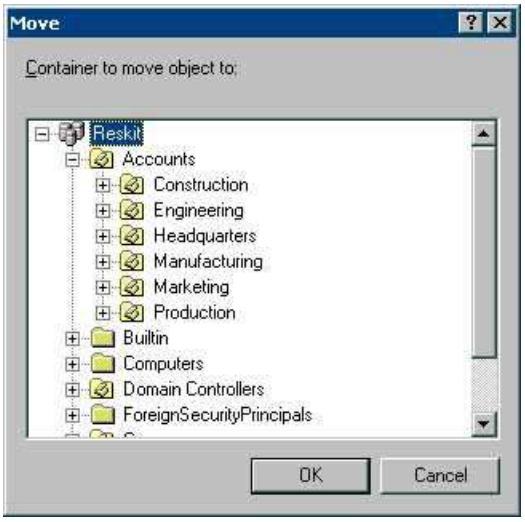
domain. For example, in this procedure, James Smith moves from the Construction division to

the Engineering division.

Step1.Click the **James Smith** user account in the right pane, right-click it, and click **Move**.

step2. Click the **+** next to **Accounts** to expand it as in below.

step3. Click the **Engineering** OU, and click **OK**.



If you upgrade from an earlier version of Windows NT Server, you might want to move existing users from the **Users** folder to some of the OUs that you create.

2. Managing a Groups

2.1 creating group

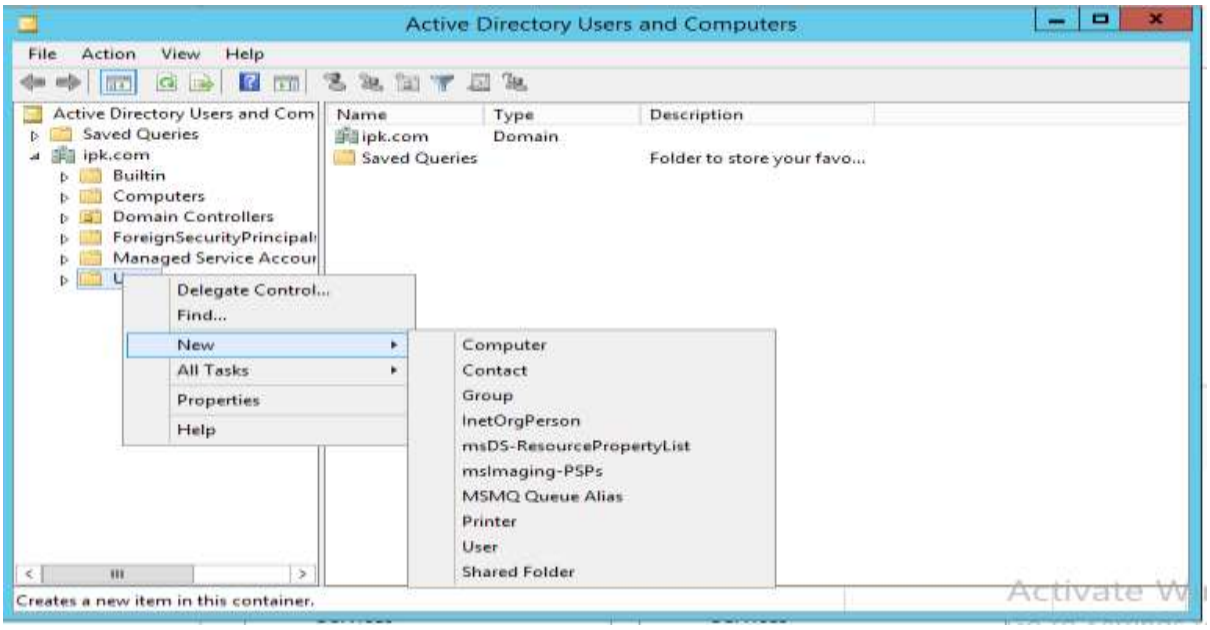
1. Right-click the Engineering OU, Click New, and then click Group.

2. In the Name of New Group text box, type: Tools

Select the appropriate Group type and Group scope and then click OK.

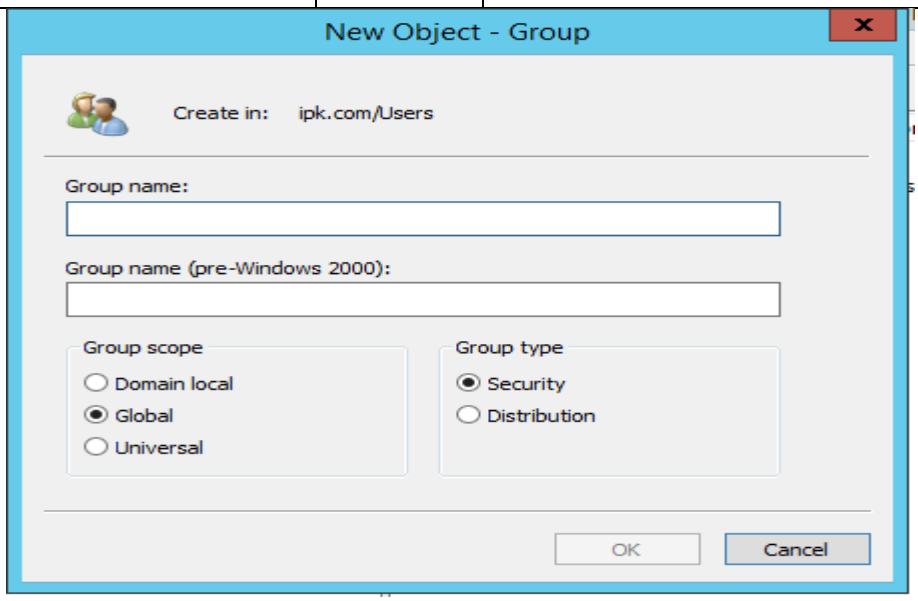
- ✓ The **Group type** indicates whether the group can be used to assign permissions to other network resources, such as files and printers.

Both security and distribution groups can be used for e-mail distribution lists.



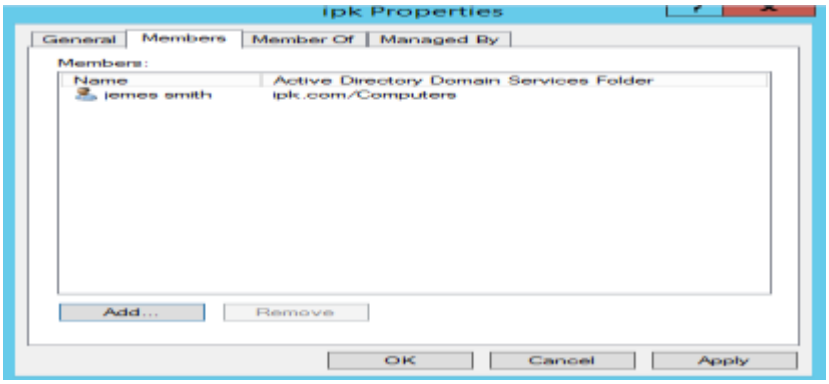
The **Group scope** determines the visibility of the group and what type of objects can be contained within the group.

Scope	Visibility	May contain
Domain Local	Domain	Users, Domain Local, Global, or Universal Groups
Global	Forest	Users or Global groups
Universal	Forest	Users, Global, or Universal Groups



2.2 Adding a User to a Group

1. Click **Engineering** in the left pane.
2. Right-click the **Tools** group in the right pane, and click **Properties**.
3. Click the **Members** Tab and click **Add**.
4. Scroll to **James Smith**, select his name, click **Add**, then click OK as in Figure 7 below



Click Apply then OK

Note: You can select multiple users or groups in this dialog by pressing the **CTRL** key as you Click them. You can also type the name directly. If the name is ambiguous, a further list is displayed to confirm your selection.

Alternatively, you can select the users from the results pane, right click then click **Add members**

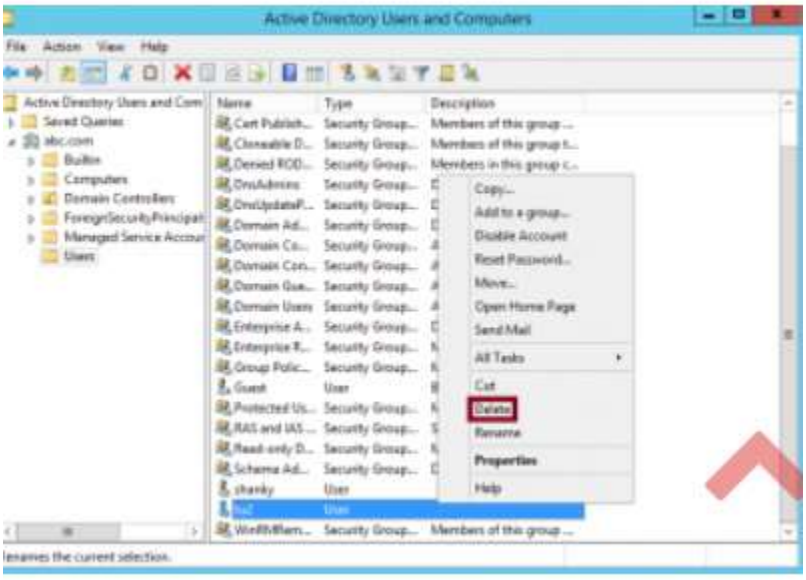
to a Group. Or you can click **Add the selected objects to a group you specify** on the snap-in toolbar. This may be more efficient for adding large numbers of members to a group.

Publishing a Shared Folder Any shared network folder, including a Distributed File System (Dfs) folder, can be published in Active Directory. Creating a Shared folder object in the directory does not automatically share.

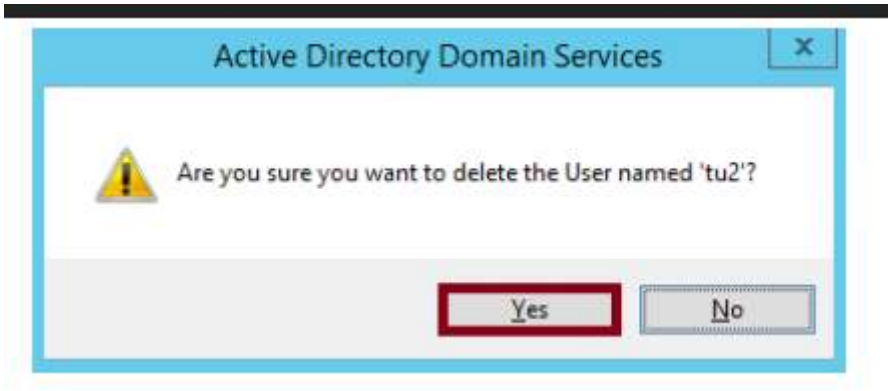
2.3 Deleting User

In this article, we will learn the steps show us how to delete user **account.** User IDs **are like** the logon account that we create, in domain environment logon accounts are created on domain controller and in workgroup accounts are created on local machine. Logon account created on domain controller can be used to logon to any computer that is part of the same domain. However user account created on workgroup machine can be used to logon to same machine on which it is created and cannot be used to logon to any other machine. So follow the bellow steps to delete user account:

1. Select the user that you want to delete.
2. Right click the object and select “delete”



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



3. *Managing Computer Accounts*

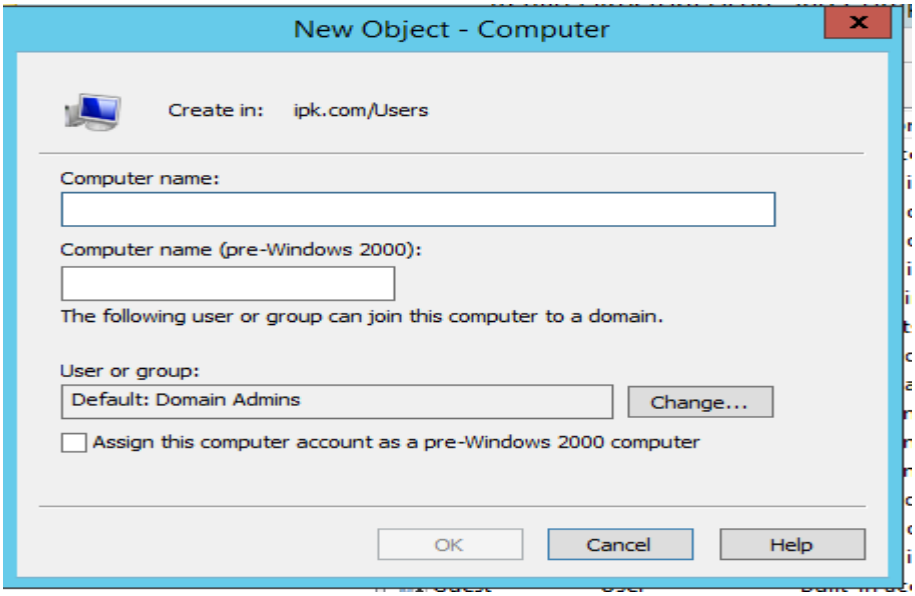
3.1 Creating a computer Accounts

The following procedure creates the user account **James Smith** in the **Construction** OU.

To create a new computer account

1. Right-click the **Construction** organizational unit, point to **New**, and then click **User**, or

Click **New User** on the snap-in toolbar.



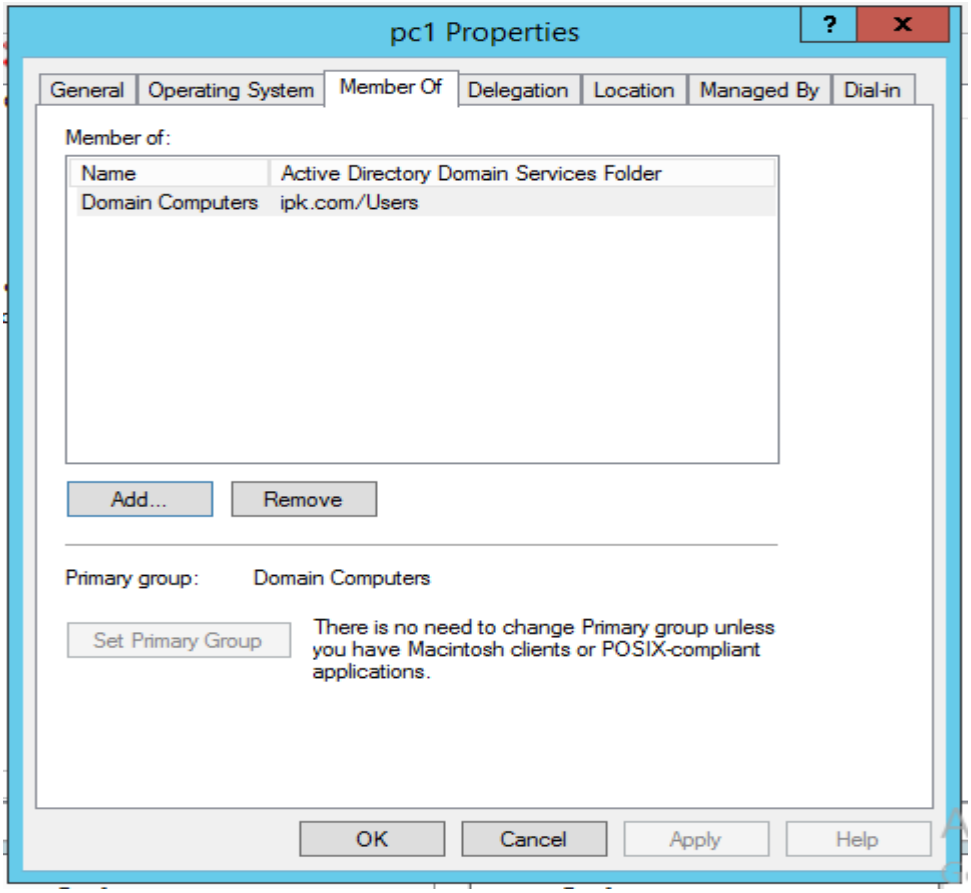
3.2 Adding a User to a Computer

1. Click **Engineering** in the left pane.

2. Right-click the **Tools** group in the right pane, and click **Properties**.

3. Click the **Members** Tab and click **Add**.

4. Scroll to **James Smith**, select his name, click **Add**, then click OK as in Figure 7 below.



4. DELEGATE ADMINISTRATION

4.1 Delegation overview

In this article we'll learn the steps to **delegate control in Active Directory Users and Computers**. In Organizations, delegate control is given to the help-desk representative to perform the tasks of reset password, add computer or server in domain, create new user, etc. In a domain, domain administrator is a user who can perform all operations and tasks related to domain and Active Directory. **Domain Administrator** is a member of **Domain Admins group** and also a user who is not available 24 x 7 x 365. So, the question is when the domain administrator is not available then who will manage the Active Directory.

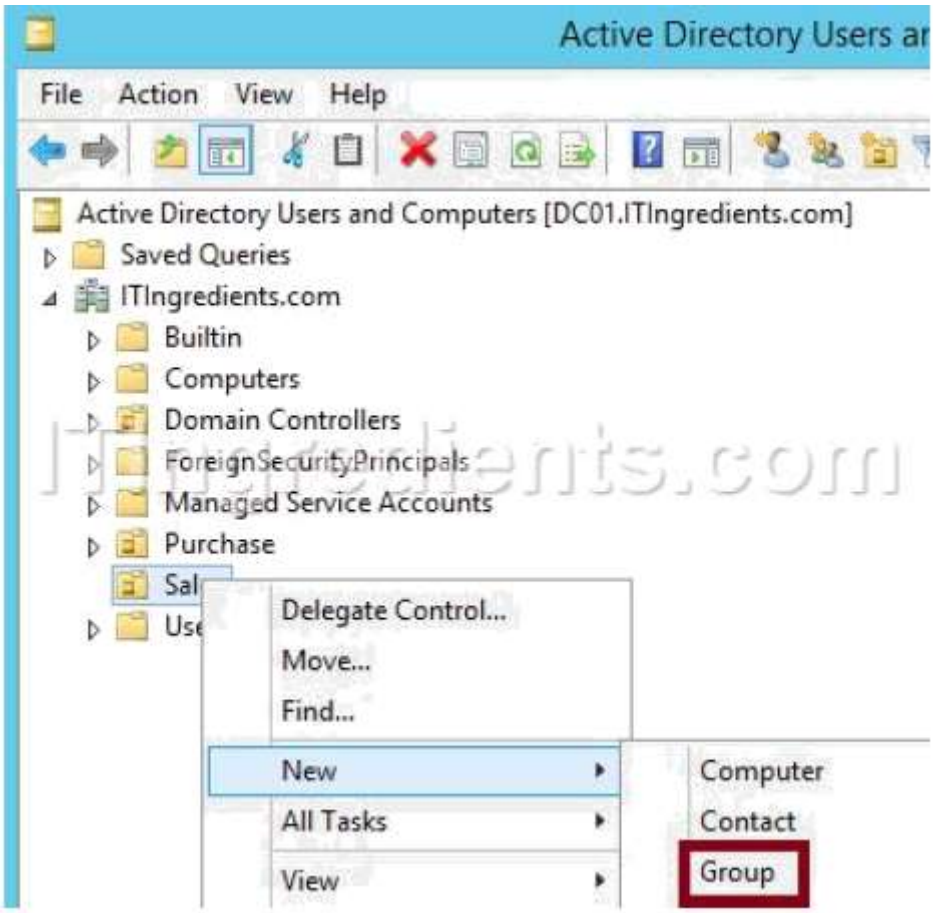
First option is that, we will add any other user into the **Domain Admins group**. This would assign Domain Admin permissions to the newly added user, these rights are sufficient to perform any domain level change in the environment. But do you really want to give **keys of kingdom to anyone**? In my opinion, this is not the right way of delegating control.

There is an another option of **Delegate Control** using Active Directory Users and Computers, through which we can deploy customized access and permissions for the **domain users**. Through this, users can perform the tasks that Administrator is designated to perform.

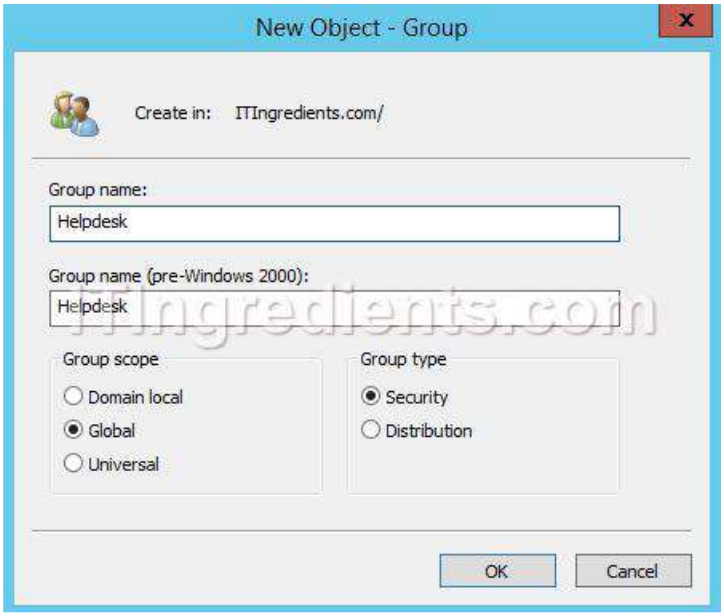
4.2 Steps to Delegate Control to Domain Users

We'll create group of users, to whom we'll delegate rights to manage user accounts. It is recommended to delegate access to groups instead of delegating permissions to individual users.

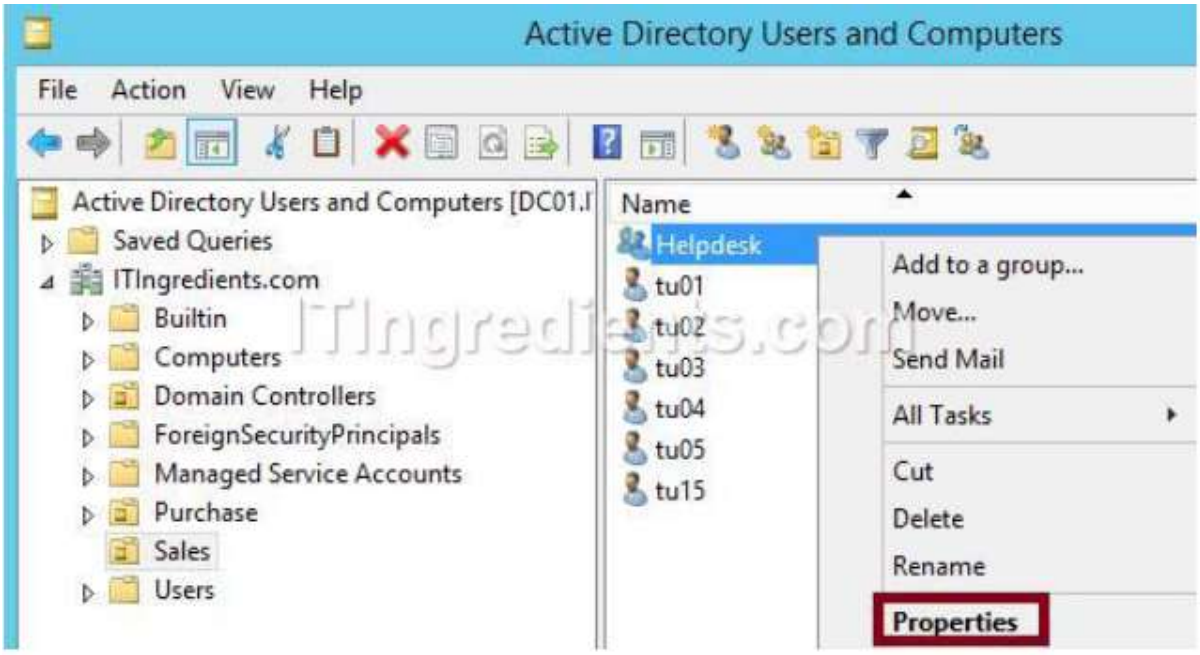
1. Open Active Directory Users and Computers, right click on an Organizational Unit (Sales) on which we have to delegate control and then click on "New" and click on Group to create a new group.



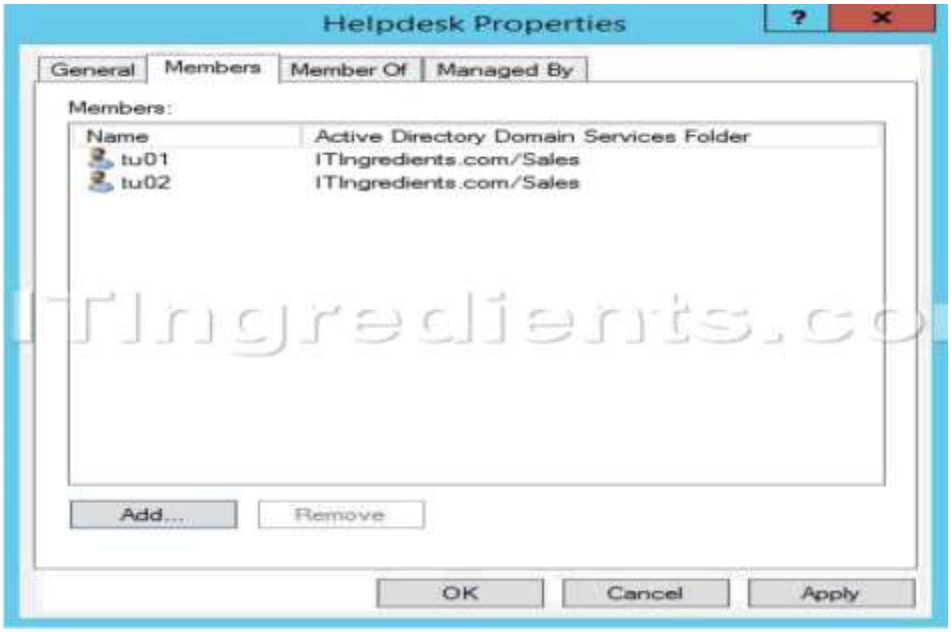
2. On New Object-Group console, enter the group name, select Global and Security options from the given options in group scope and group type respectively. Click on ok. In this example, we will create a group naming **Helpdesk**.



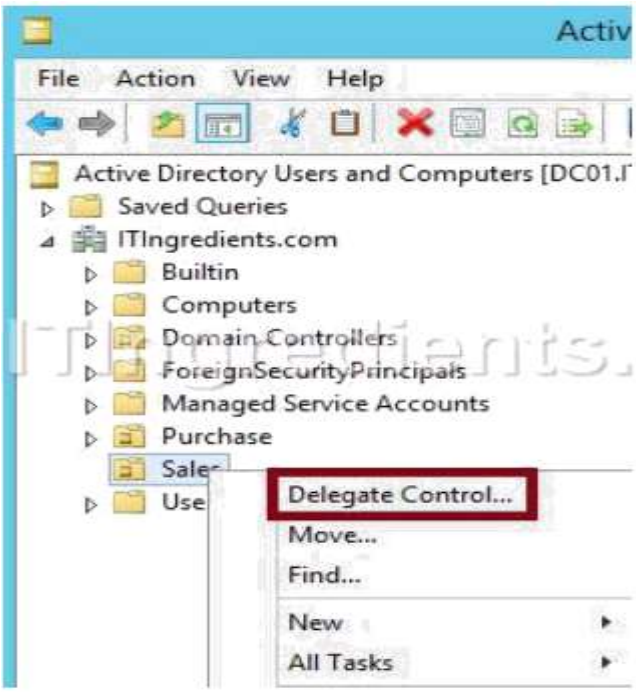
3. Right click on the group (Helpdesk) and click on Properties to open the properties console to modify various group



4. On Group Properties console, under members tab click on **Add** to add users into this group. Verify all the added users. Now, these users are the group members of Helpdesk group.

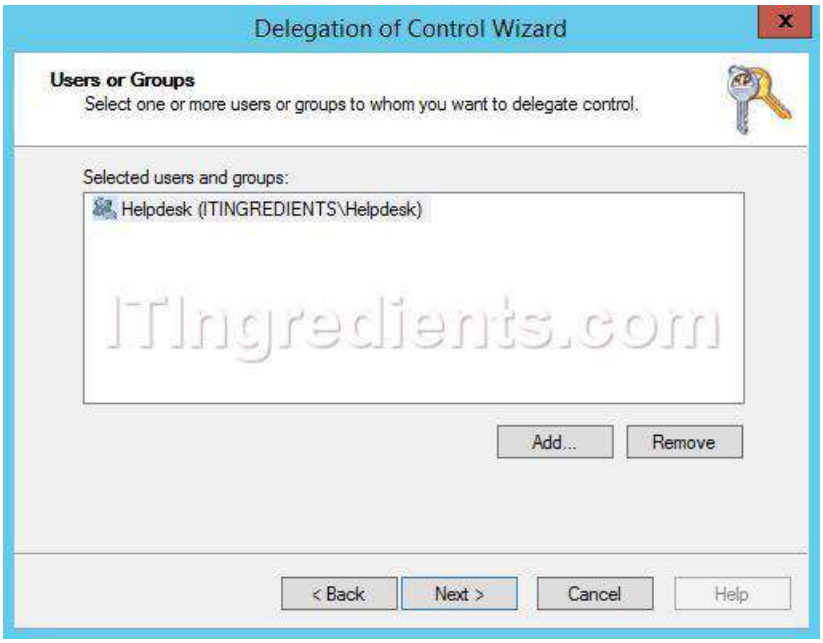


5. Right click on the Organizational Unit (Sales) and click on **Delegate Control** to delegate the customized permissions to the user or a group of users. This wizard will only delegate access for Sales OU and not for other OUs.



6. . On the "**Delegation of Control W**izard" we can see the relevance of delegate control. We can grant users permission to manage users, computers, groups, OU and other objects of AD Users and Computers. Click on Next

7. In users and groups console, click on **Add** to add the group. Here, we have added **Helpdesk group** so that we can assign permissions to the group members. Click on next to continue.



8. In Tasks to Delegate console, select “delegate the following common tasks” and select permissions from the given tasks. Or select the “Create a custom task to delegate” to give custom permissions to the users other than the above permissions. Click on Next to continue. For this example, we’ll delegate control for “create, delete and manage user accounts” and “Reset user passwords and force password change at next logon”.

9. On the “Completing the Delegation of Control Wizard” verify the selected options on previous consoles and Click on Finish to close the console.

Access Delegated Control from Client Computer

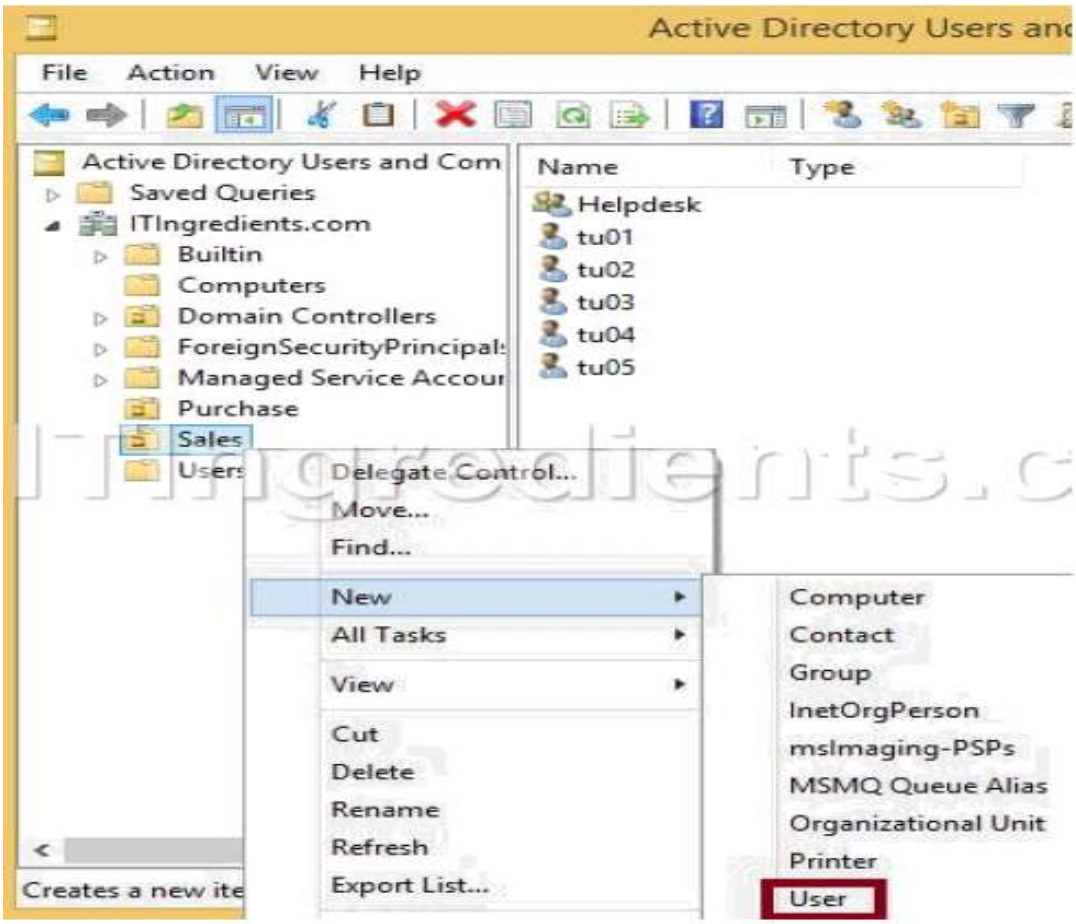
A user (**TU1**) is a member of **Helpdesk** Group and have delegated permissions. But these rights would not enable domain user to login to Domain Controller. This user cannot access **Active Directory Users and Computers** either by login to Domain Controller or using RDP from any client machine e.g. Windows 7 operating system because he is not a member of **Domain Admins** group.

To enable user to access Active Directory users and computers from client machine, we need to install the **Active Directory Domain Services** role on Windows 7 client, to install the role, install the windows update package (Windows8.1-KB2693643-x64). You can download this update package from the given link

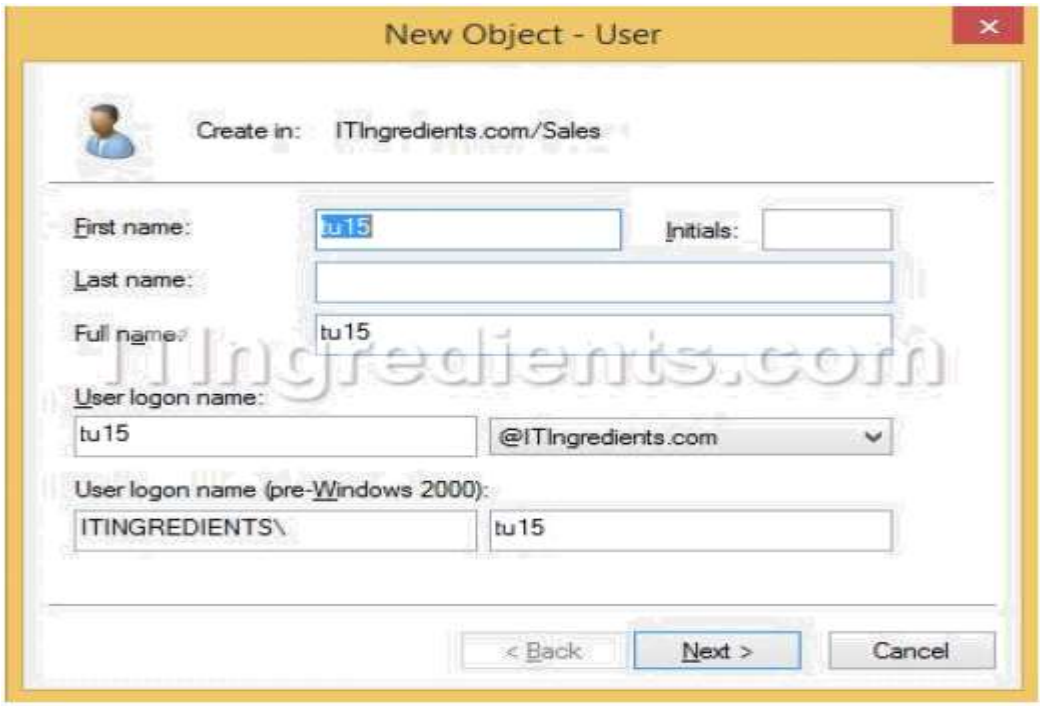
(https://www.microsoft.com/en-us/download/details.aspx?id=7887).

1. After installing this package, we can see the icon of **Active Directory Users and Computers** in the start menu under Administrative Tools on Windows 7 Operating System, or use (MMC) command in run. Click on the icon of AD Users and Computers to open the console.

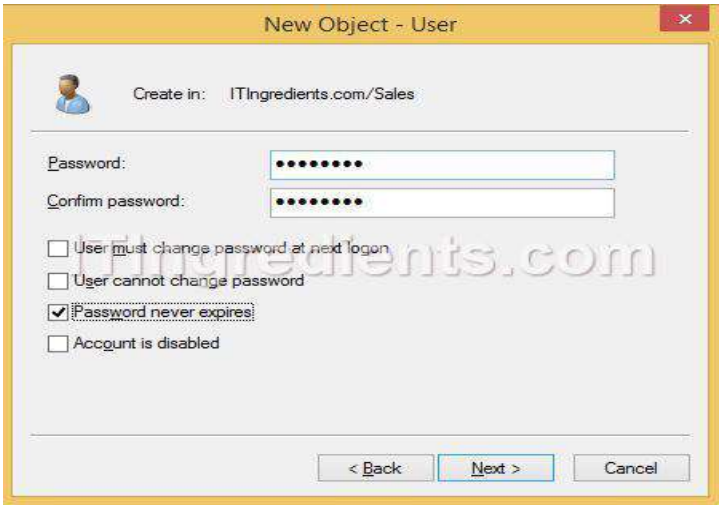
2. Through this console, this user (TU01) can only perform the operations that we have delegated to “Helpdesk Group”. Learn how to create user. We will try to create a new user in the Organizational Unit (Sales) to the check that given permissions are delegated successfully or not. Right click on the OU (Sales) and then click on New and then User to create a new user.



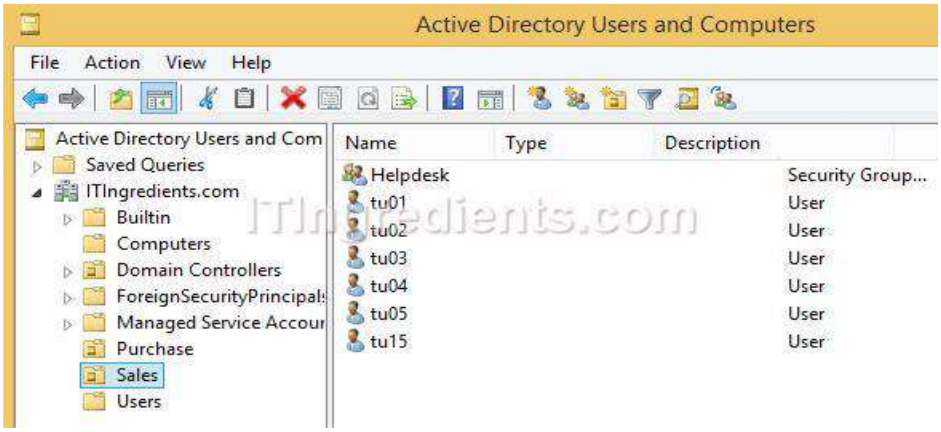
3. On New Object – User console, enter the details like First name, Last Name, User logon name of the new user which you want to create. Click on Next to continue.



4. Enter the password in the Password and Confirm Password field of the user which we are creating and select the option according to your requirement from the given options. Click on Next to continue. On the next console verify all the settings and then click on Finish.



5. On Active Directory Users and Computers, in Sales OU we can verify that user tu15 is successfully created. It clearly shows that rights are successfully delegated to the user **tu01** through the security group **helpdesk.**



This user **(TU01)** can perform other delegated rights e.g. resetting user account password, deleting user account and other similar operations.

Conclusion:

Delegate access would enable set of users to perform the tasks that are normally performed by Domain Admins. It would only restrict the user to the OU on which rights are delegated.

LO 3.2 Deploy and configure server roles

- Content/Topic 1: Deployment and configuration of Dynamic Host configuration Protocol(DHCP)

A. Overview of the DHCP Server Role

A.1 what is a DHCP?

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

A.2 Why DHCP?

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed.

With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database that includes:

• Valid TCP/IP configuration parameters for all clients on the network.

Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.

• Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.

• The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

• A valid IP address for the subnet to which it is connecting.

• Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients. Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name.

A.3 Benefits of DHCP

In Windows Server, the DHCP Server service provides the following benefits:

• **Reliable IP address configuration**. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

• **Reduced network administration**. DHCP includes the following features to reduce network administration:

- Centralized and automated TCP/IP configuration.
- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet

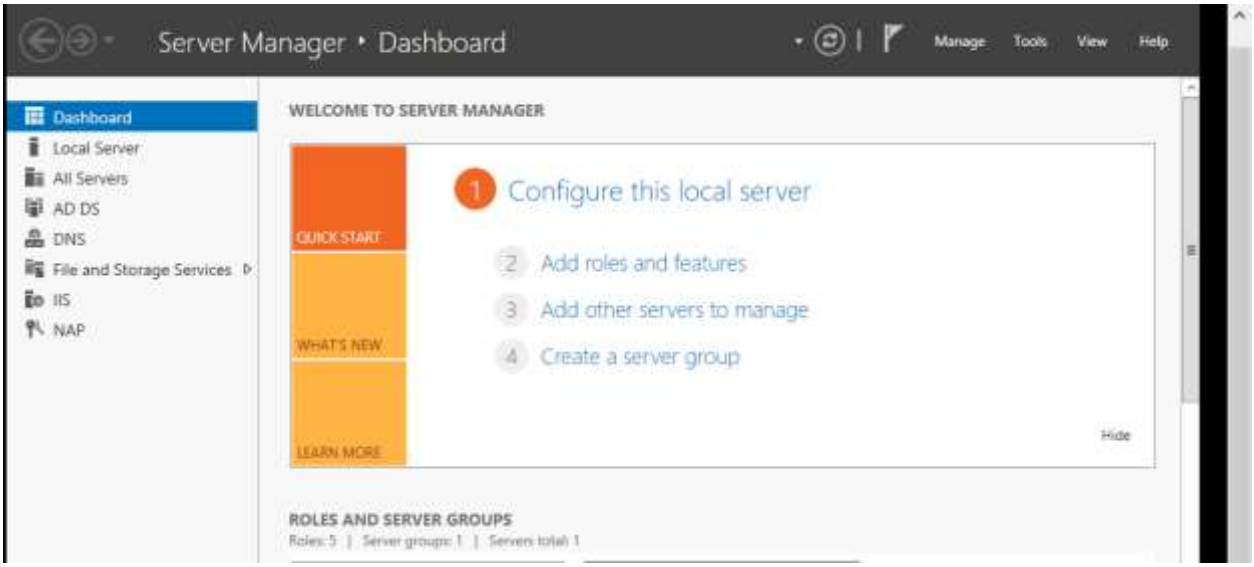
A.4 Installation of DHCP role steps

✓ Ensure the computer has at least one static IP address assigned before starting the role installation.

✓ Launch the Add Role Wizard from Server Manager.

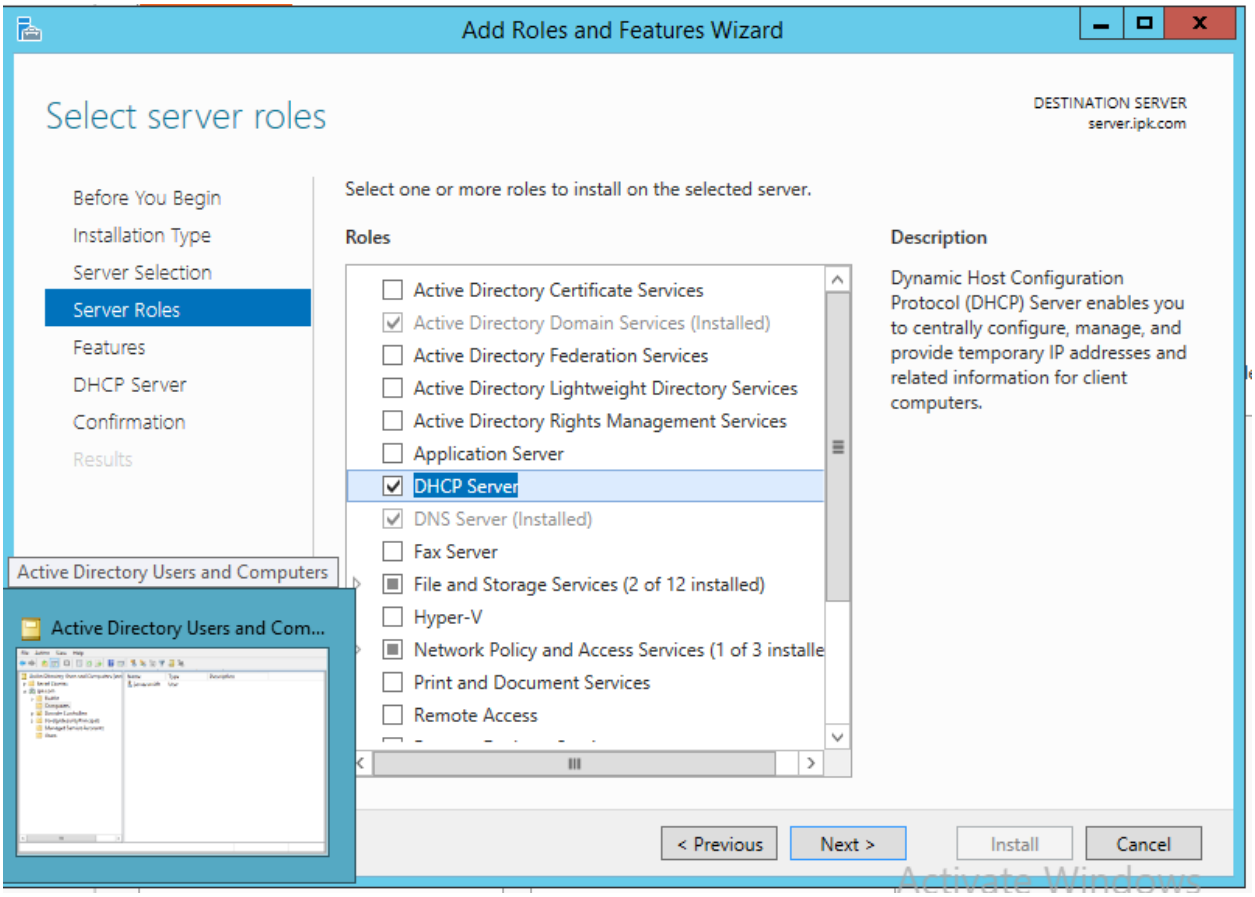
✓ Select DHCP server role and go through the steps needed for installation.

✓ The last page of the wizard (which comes up after the role has been installed), provides a link – **"Complete DHCP configuration"**. This provides some tasks that need to be performed to enable the DHCP server role to work properly after role installation.



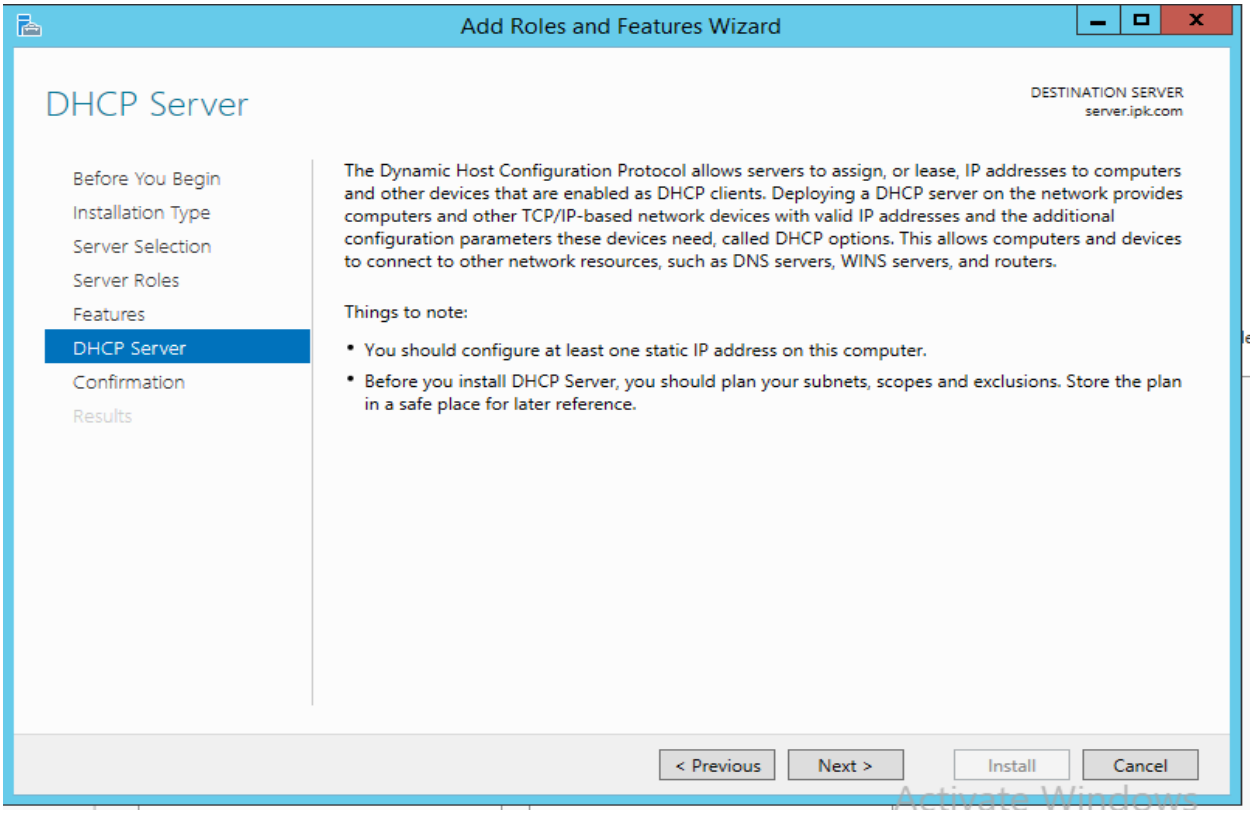
Then click on “Add Roles” option to open Add roles Wizard.

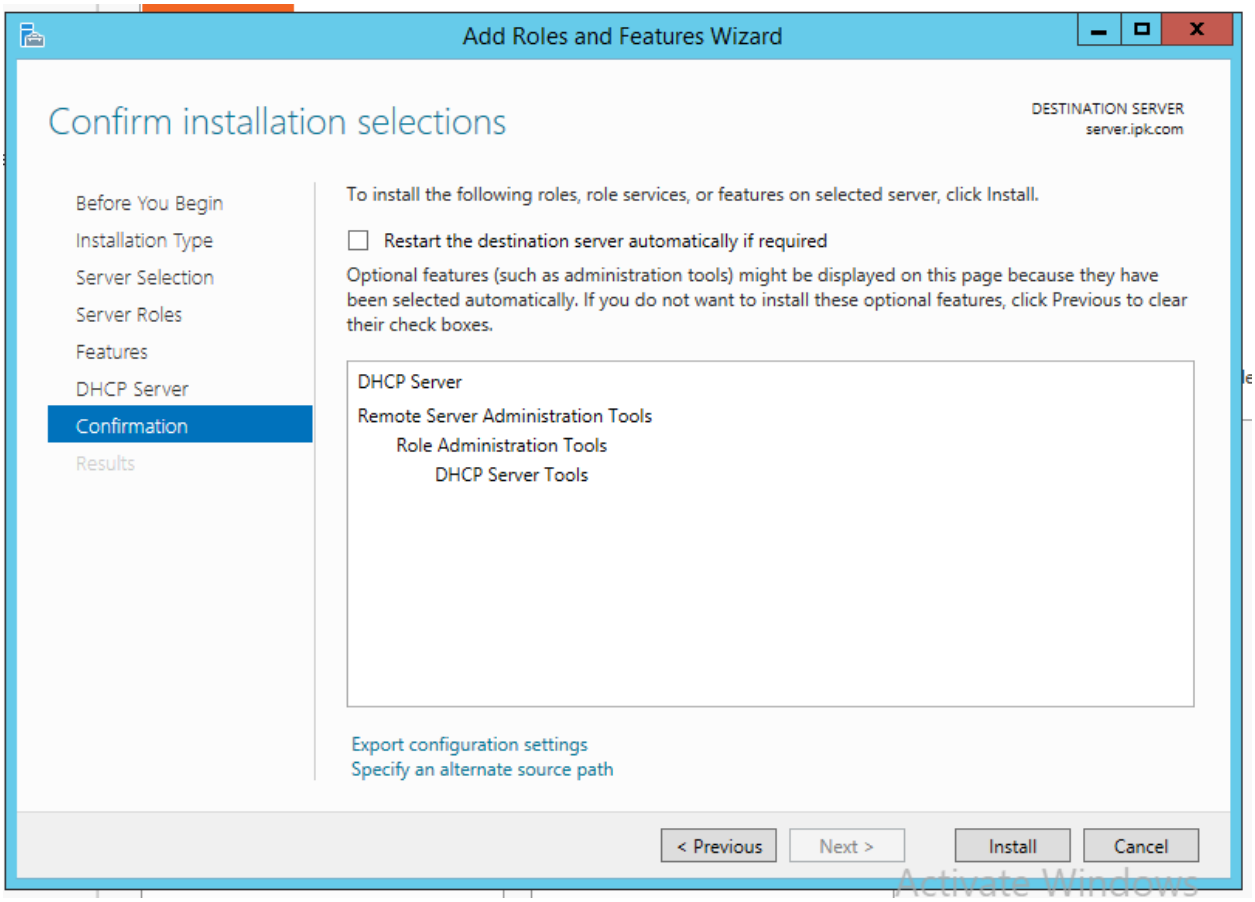
Then it will load the Roles Wizard and select the “DHCP Server” From the list and click next to continue.



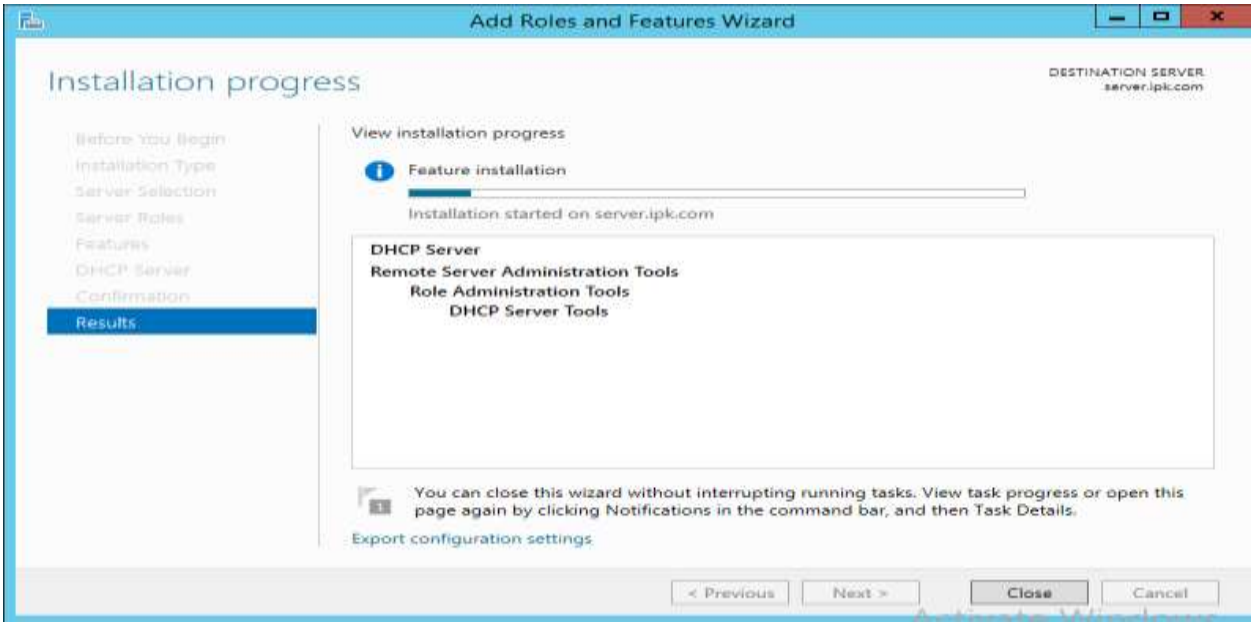
Then it will give description about the role. Click Next to continue. Next

.

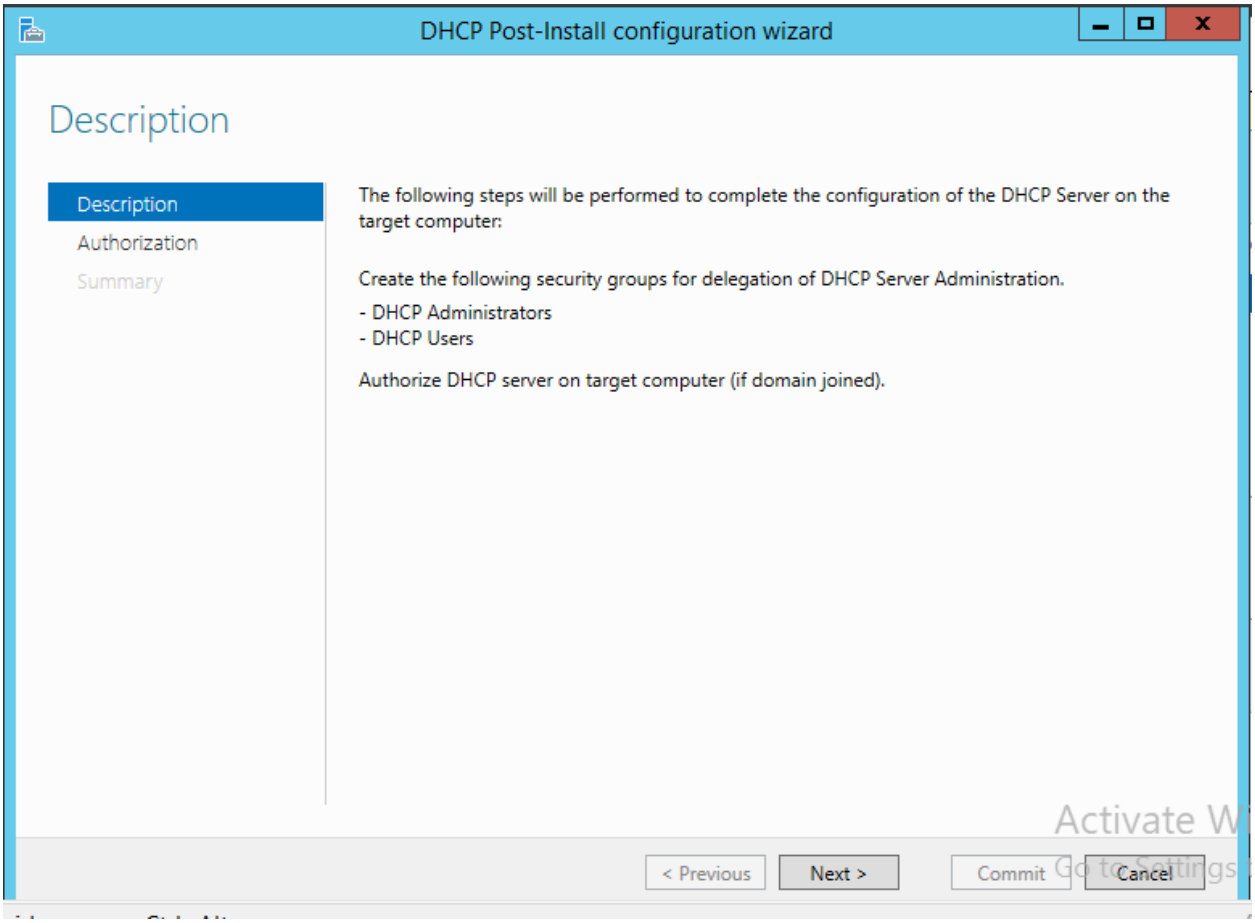




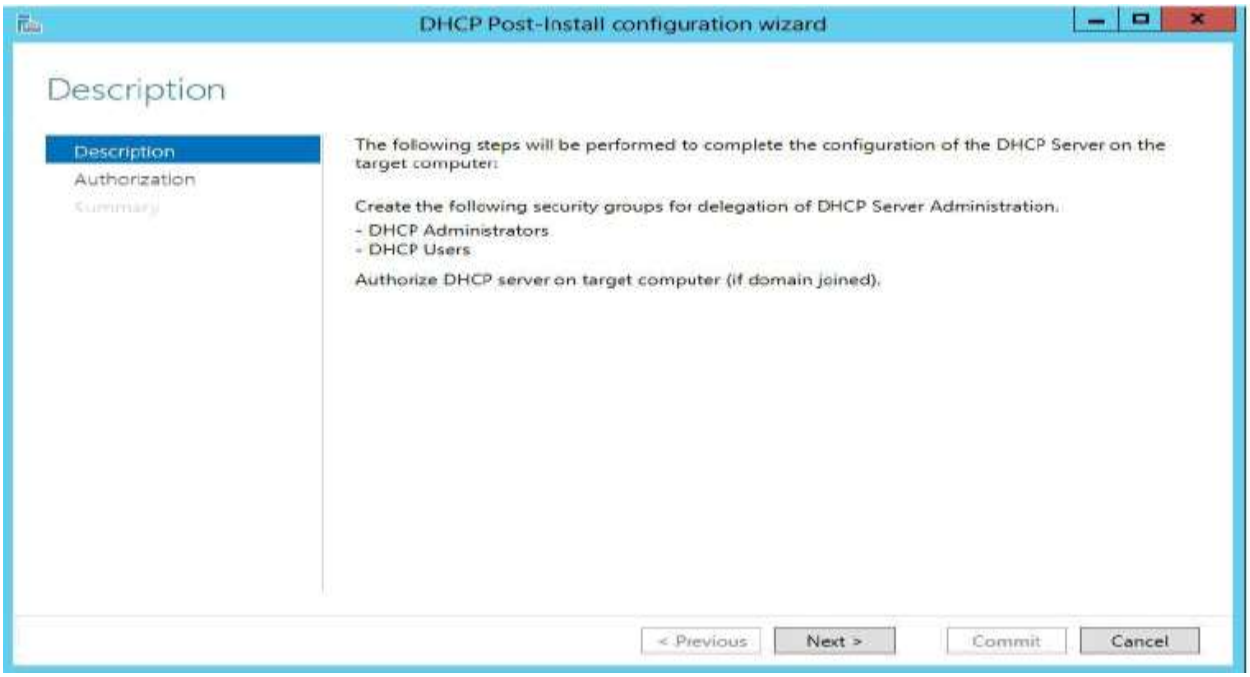
Click install



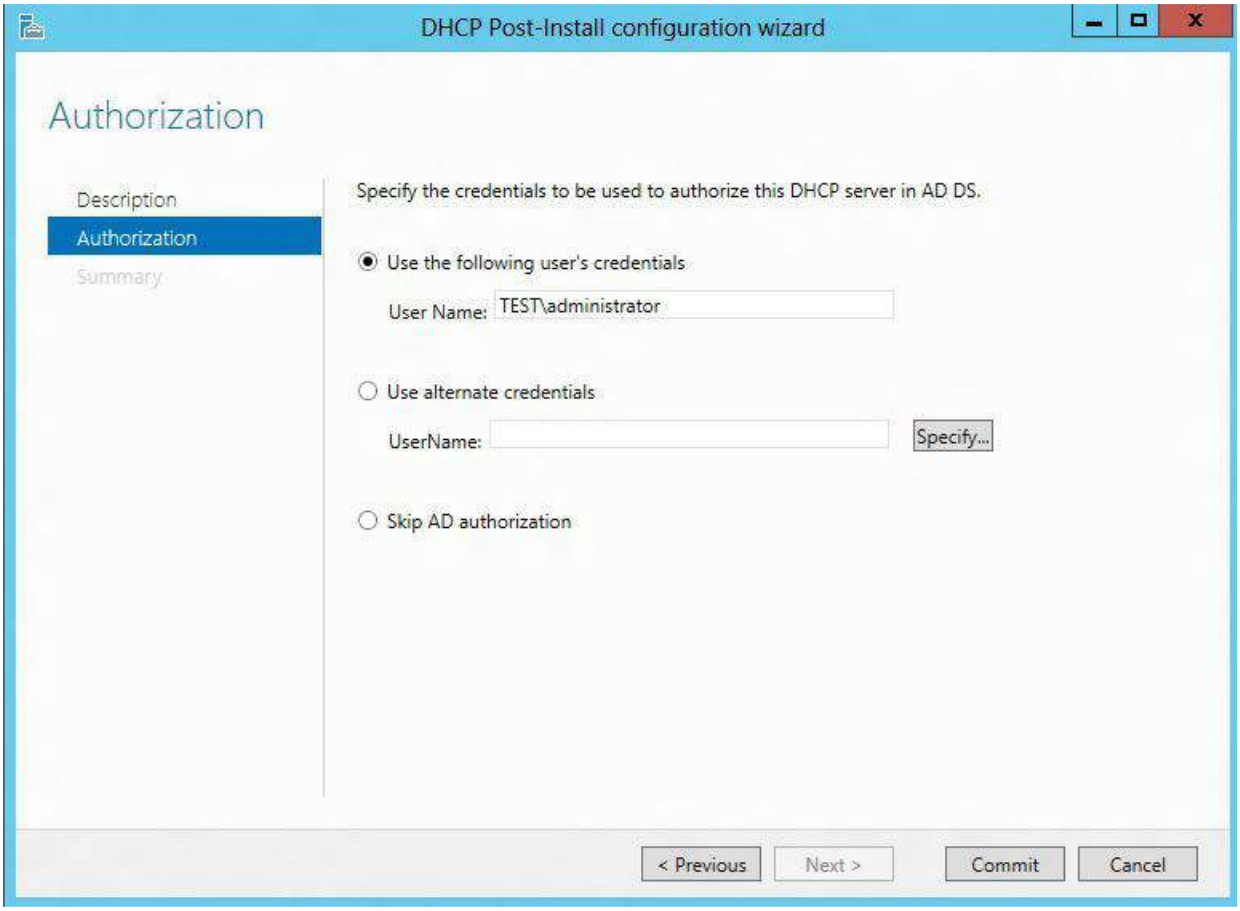
Click close

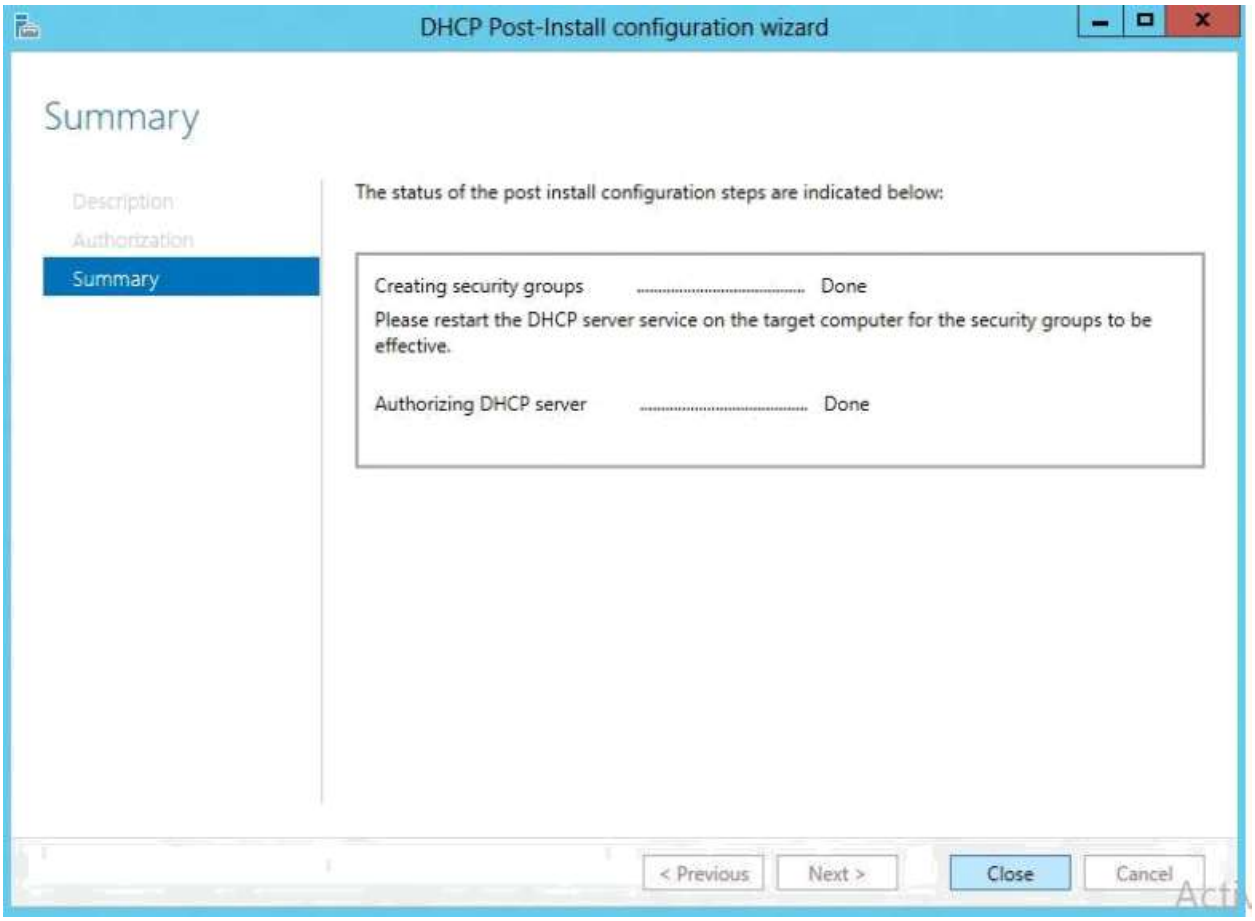


- Launch the DHCP post-install wizard and complete the steps required.
- Creation of DHCP security groups (DHCP Administrators and DHCP Users). For these security groups to be effective, the DHCP server service needs to be restarted. This will need to be performed separately by the administrator.

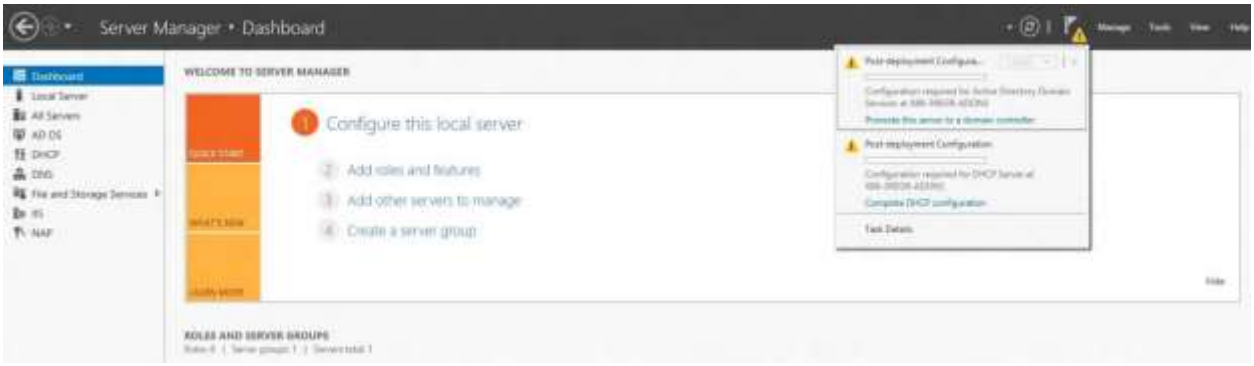


- Authorization of DHCP server in Active Directory (only in case of a domain-joint setup). In a domain joined environment, only after the DHCP server is authorized, it will start serving the DHCP client requests. Authorization of DHCP server can only be performed by a domain user that has permissions to create objects in the Net services container in Active Directory.

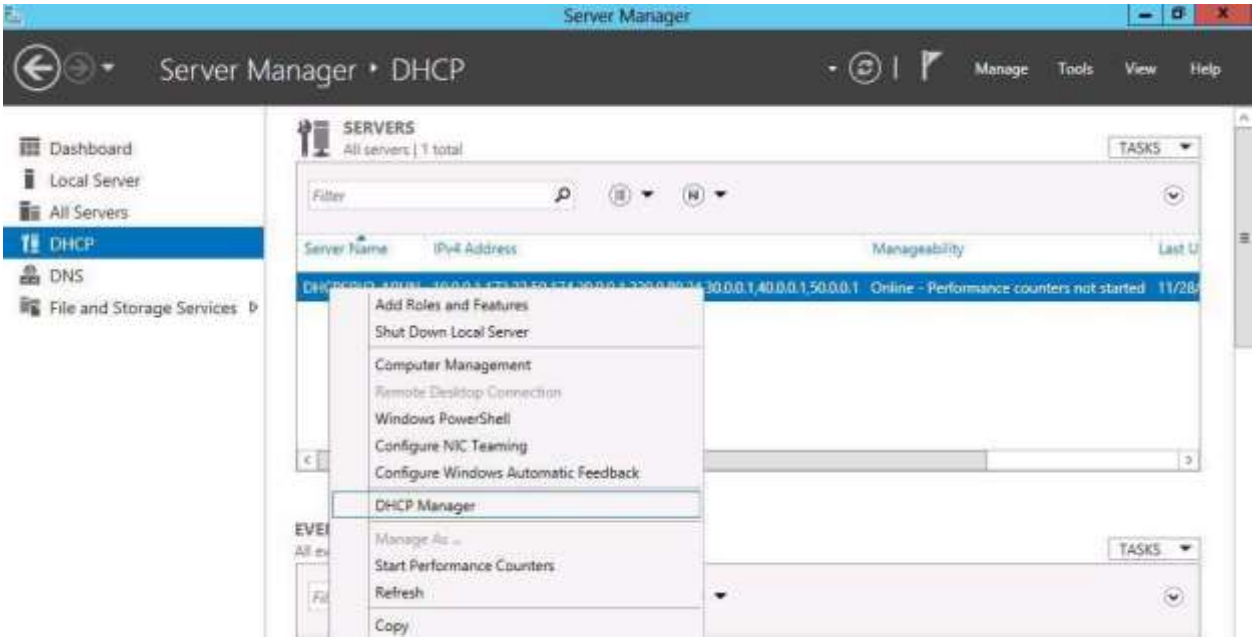

DHCP Post-Install configuration wizard
Authorization
Description
Authorization
Summary
Specify the credentials to be used to authorize this DHCP server in AD DS.
Use the following user's credentials
User Name: TEST\administrator
Use alternate credentials
UserName:
Specify...
Skip AD authorization
< Previous
Next >
Commit
Cancel


DHCP Post-Install configuration wizard
Summary
Description
Authorization
Summary
The status of the post install configuration steps are indicated below:
Creating security groups ..... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.
Authorizing DHCP server ..... Done
< Previous
Next >
Close
Cancel

• In case completing of the post-install step is missed after role installation, the administrator will continue to see a notification on the action pane and also a link on the DHCP role tile on the main Server Manager page suggesting that some configuration is required. That link would go away only after completion of the post-install task.



The configuration of DHCP server parameters such as scope, options etc. are no longer available in the new Server Manager. The administrator can now launch DHCP MMC either via Server manager (as shown below), or via the DHCP MMC application in the Start Menu, or writing *dhcpmgmt.msc* on the command prompt. The administrator can now create scopes, set option values so as to be able to lease out IP addresses and provide option values to clients.



Content/Topic 3: Configuration of DHCP Scopes

- ✓ **DHCP scope**

1. On the Server Manager Menu bar, click **Tools** and then click **DHCP**. The DHCP console opens.

2. In the DHCP console tree, navigate to **IPv4**. Right-click **IPv4** and then click **New Scope**. The **New Scope Wizard** opens.

3. Click **Next** and then type a name for the new scope next to **Name** (ex: Contoso-scope1).

4. Click **Next** and then in **IP Address Range**, type **192.168.100.1** next to **Start IP address**, type **10.0.0.254** next to **End IP address**, and type **24**next to **Length**. The value of Subnet mask will change automatically to **255.255.255.0**.

5. Click **Next**, and then in **Add Exclusions and Delay** type **192.168.100.1** under **Start IP address**, type **192.168.100.10** under **End IP address**, and then click **Add**. This allows the first ten IP addresses in the 10.0.0.0/24 subnet to be used for static addressing of servers on the network.

6. Click **Next** and then in **Lease Duration** under **Limited to** enter **0 Days**, **0 Hours**, and **2 Minutes**. This very short lease duration will simplify the DHCP demonstration.

7. Click **Next** three times, and then in **Domain Name and DNS Servers**, verify that the **Parent domain** is **tctita.local** and **192.168.100.1** is listed as the only DNS server.

8. Click **Next** twice, and then in **Activate Scope** select **Yes, I want to activate this scope now**.

9. Click **Next**, and then click **Finish**.

10. In the DHCP console tree, right-click **itadc1.tctita.local**, and then click **Authorize**.

11. Refresh the view in the DHCP console and verify that DHCP1 is authorized and that the Contoso-scope1 is active.

- ✓ **Managing a DHCP Database**

The DHCP database is a dynamic database that is updated when DHCP clients are assigned or as they release their TCP/IP address leasesThe DHCP database contains DHCP configuration data, such as information about scopes, reservations, options, and leases.

Windows Server 2003 stores the DHCP database in the directory %Systemroot%\System32\DhcpThe DHCP database files include:

- DHCP.mdb
- Tmp.edb
- J50.log and J50*.Log
- Res*.log
- J50.chk

- ✓ **Securing and Monitoring DHCP**

Monitor and Manage Windows **DHCP** Server Scopes When managing your IP Address space, it is often required to relate your available and used IP Addresses to your **DHCP** Servers. ... OpUtils lets you combine managing your IP Addresses and **DHCP** Servers so that you get a clear view of your IP space at one place.

- Content/Topic 4: installation of Domain Name System

1. Overview

The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, Services or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
Most importantly, it translates domain names meaningful to humans into the numerical Identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. The table below describe Domain Name System elements.

DNS Element	Description
Nameserve	Nameservers "point" your domain name to the company that controls its DNS settings. Usually, this will be the company where you domain name registered the domain name. However, if your website is hosted by another company, sometimes they will provide nameservers you need to point to instead.
Zone File	Zone Files are simply the files that store all of your domain's DNS settings. Your domain name's Zone File is stored on the company's nameserver.
A Record	A Records point your domain name to an individual server using an IP address. An example IP address is 123.4.67.5. Every domain name has a primary A Record called "@," which controls what your domain name does when some visits it directly. You can also use A Records to point subdomains (for example *subdomain.coolexample.com*) to a server's IP address.
CNAME	CNAMEs point your subdomains to another server using a server name, like *server1.godaddy.com*. Most domain names have many CNAMEs.

	Unlike A Records, CNAMEs cannot use IP addresses.
MX Records	MX Records point your domain name's email to its email provider.

- ✓ **How does DNS work?**

When you visit a domain such as *dyn.com,* your computer follows a series of steps to turn the human-readable web address into a machine-readable IP address. This happens every time you use a domain name, whether you are viewing websites, sending email or listening to Internet radio stations.

Step 1: Request information

The process begins when you ask your computer to resolve a hostname, such as visiting *http://dyn.com*. The first place your computer looks is its local DNS cache, which stores information that your computer has recently retrieved. If your computer doesn't already know the answer, it needs to perform a **DNS query** to find out.

Step 2: Ask the recursive DNS servers

If the information is not stored locally, your computer queries (contacts) your ISP's **recursive DNS servers**. These specialized computers perform the legwork of a DNS query on your behalf. Recursive servers have their own caches, so the process usually ends here and the information is returned to the user.

Step 3: Ask the root nameservers

If the recursive servers don't have the answer, they query the **root nameservers**. A **nameserver** is a computer that answers questions about domain names, such as IP addresses. The thirteen root nameservers act as a kind of telephone switchboard for DNS. They don't know the answer, but they can direct our query to someone that knows where to find it.

Step 4: Ask the TLD nameservers

The root nameservers will look at the first part of our request, reading from right to left — *www.dyn.**com*** — and direct our query to the **Top-Level Domain (TLD) nameservers** for *.com*. Each TLD, such as *.com*, *.org*, and *.us*, have their own set of nameservers, which act like a receptionist for each TLD. These servers don't have the information we need, but they can refer us directly to the servers that *do* have the information.

Step 5: Ask the authoritative DNS servers

The TLD nameservers review the next part of our request — *www.**dyn.com*** — and direct our query to the nameservers responsible for this *specific* domain. These **authoritative nameservers** are responsible for knowing all the information about a specific domain, which are stored in **DNS records**. There are many types of records, which each contain a different kind of information. In this example, we want to know the IP address for *www.dyndns.com*, so we ask the authoritative nameserver for the **Address Record (A)**.

Step 6: Retrieve the record

The recursive server retrieves the A record for *dyn.com* from the authoritative nameservers and stores the record in its local cache. If anyone else requests the host record for *dyn.com*, the recursive servers will already have the answer and will not need to go through the lookup process again. All records have a **time-to-live** value, which is like an expiration date. After a while, the recursive server will need to ask for a new copy of the record to make sure the information doesn't become out-of-date.

Step 7: Receive the answer

Armed with the answer, recursive server returns the A record back to your computer. Your computer stores the record in its cache, reads the IP address from the record, then passes this information to your browser. The browser then opens a connection to the webserver and receives the website.

- ✓ **Steps to Setup & Configure DNS Server on Windows 2012 R2 Server**

However, most Windows administrators still rely on the Windows Internet Name Service (WINS) for name resolution on local area networks and some have little or no experience with DNS. We'll explain how to install, configure, and troubleshoot a Windows Server 20012 DNS server.

2. **Name Resolution for Windows Clients and Servers**

Clients connecting to resources on Microsoft **servers**, typically through **Windows** File Manager or Network Neighborhood, most often use NetBIOS **name resolution**. Host **name resolution** resolves the **names** of TCP/IP resources that do not connect through the NetBIOS interface

3. **Identify step by steps DNS Installation:**

Step 1: Install a DNS server from the Control Panel, follow these steps:

- Go to **Start—> Control Panel —> Administrative Tools —> Server Manager**.
- Expand and click Roles
- Click on Add Roles

4. Installing and Configuring DNS in Windows Server 2012R2

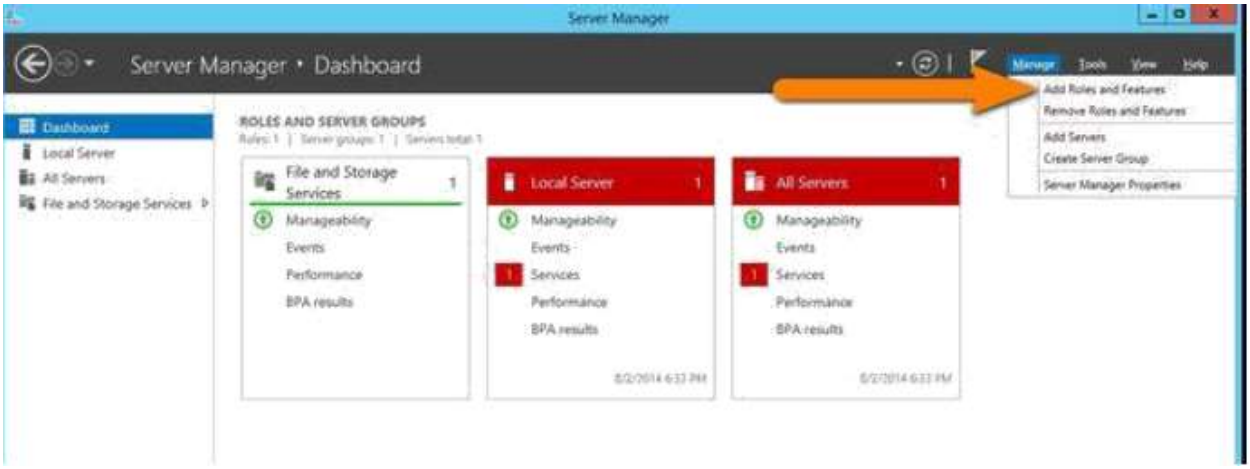
Setting up a Domain Name System (DNS) on Windows Server involves installing the DNS Server Role.

This tutorial will walk you through the DNS installation and configuration process in Windows Server 2012.

Microsoft Windows Server 2012 is a powerful server operating system capable of many different roles and functions. However, to prevent overloading production servers with features and options that are never used, Windows Server provides a modular approach in which the administrator manually installs the services needed. To setup and configure DNS, one must install the DNS Server Role on Windows Server 2012.

Install DNS Server Role in Server 2012

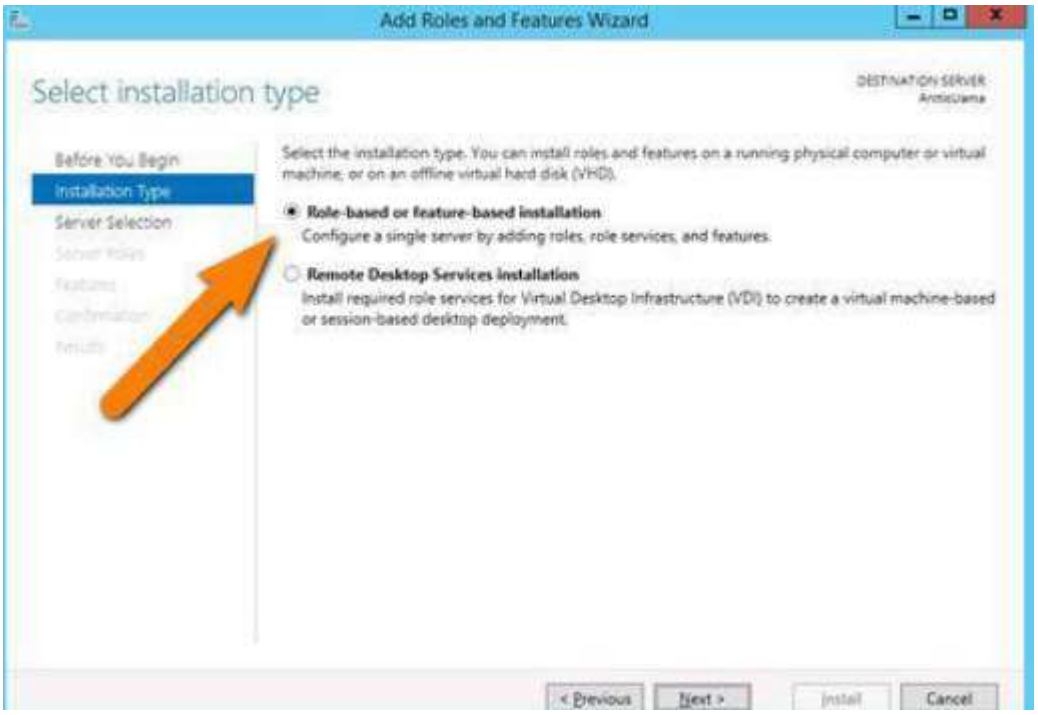
To add a new role to Windows Server 2012, you use Server Manager. Start Server Manager, click the Manage menu, and then select **Add Roles and Features**.



Click Next on the

Add Roles and Features Wizard Before you begin window that pops up. (If you checked **Skip this page by default** sometime in the past, that page will, of course, not appear.)

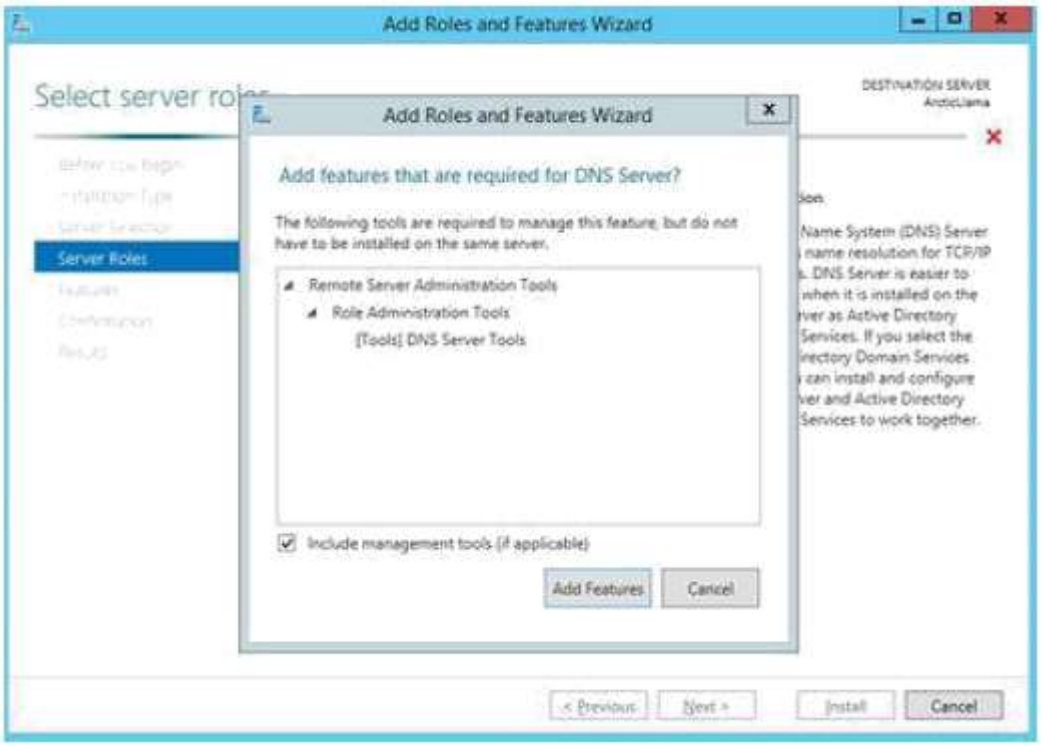
Now, it's time to select the installation type. For DNS servers, you will be selecting the **Role-based or feature-Based installation**.



Next, you will choose which server you want to install the DNS server role on from the server pool. Select the server you want, and click next.

At this point, you will see a pop-up window informing you that some additional tools are required to manage the DNS Server. These tools do not necessarily have to be installed on the same server you are installing the DNS role on. If your organization only does remote administration, you do not have to install the DNS Server Tools.

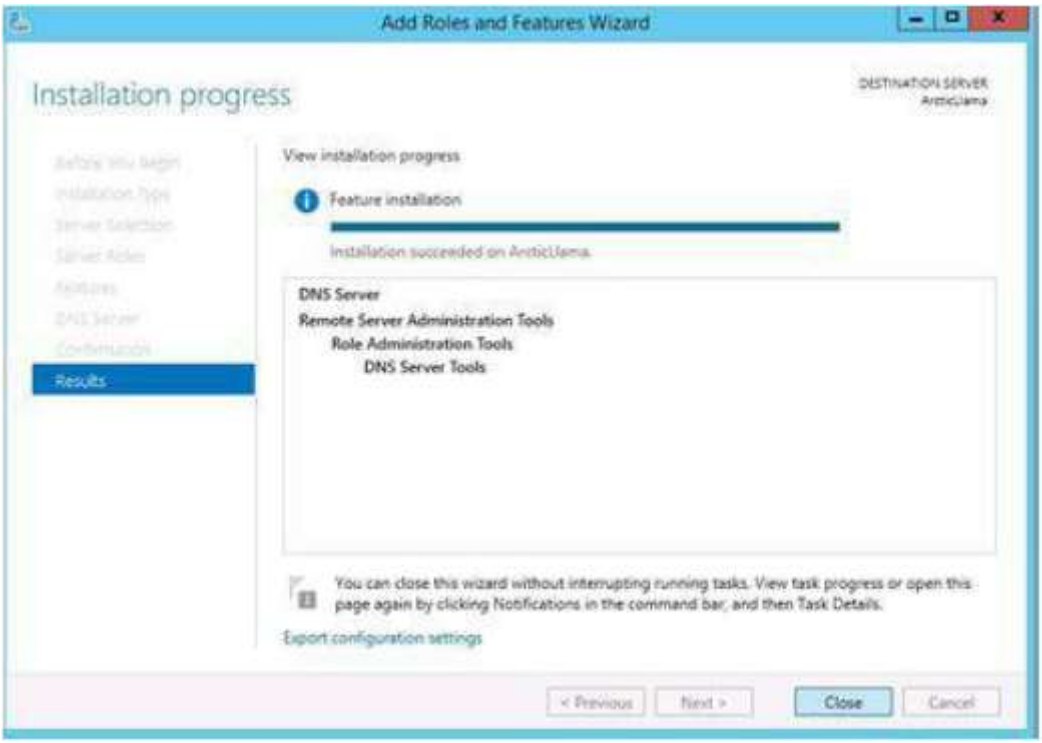
However, in a crunch you may find yourself sitting at the server console or remotely using the console and needing to manage the DNS Server directly. In this case, you will wish you had the tools installed locally. Unless your company policy forbids it, it is typically prudent to install the management tools on the server where the DNS will be housed.



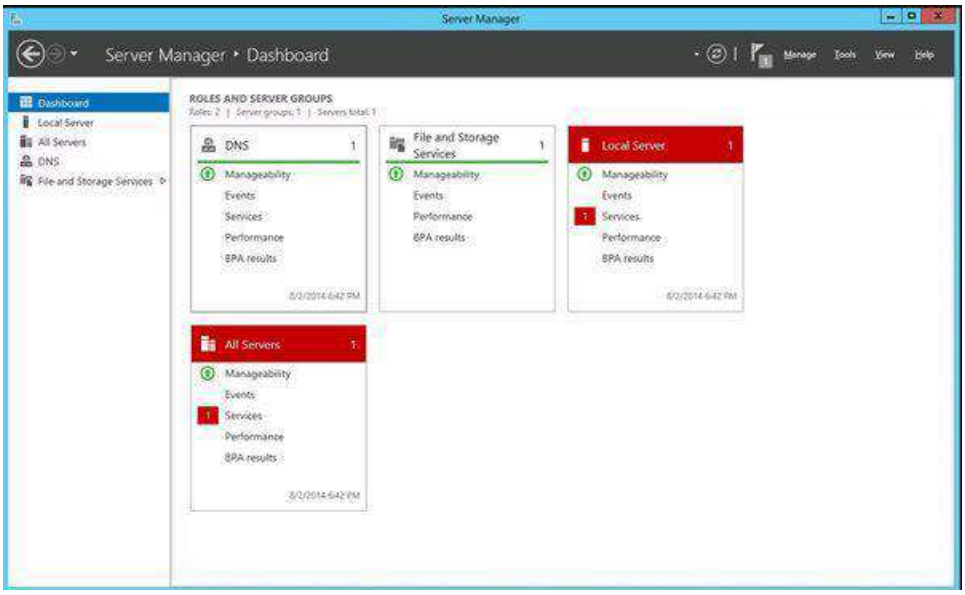
Now you should see the Features window. No need to make any changes here; just click Next.

Next is an informational window about DNS Server and what it does, although one would assume that if you've gotten this far, you are already aware of what it is. Click Next to move on.

This is the final confirmation screen before installation completes. You can check the box to **restart the destination server automatically**, if you like. Installing the DNS Server does not require a restart, but unless you've planned for the downtime, keep that box unchecked, just in case.



The DNS Server role should now be installed on your server. There should be a new NS Role tile in your Server Manager

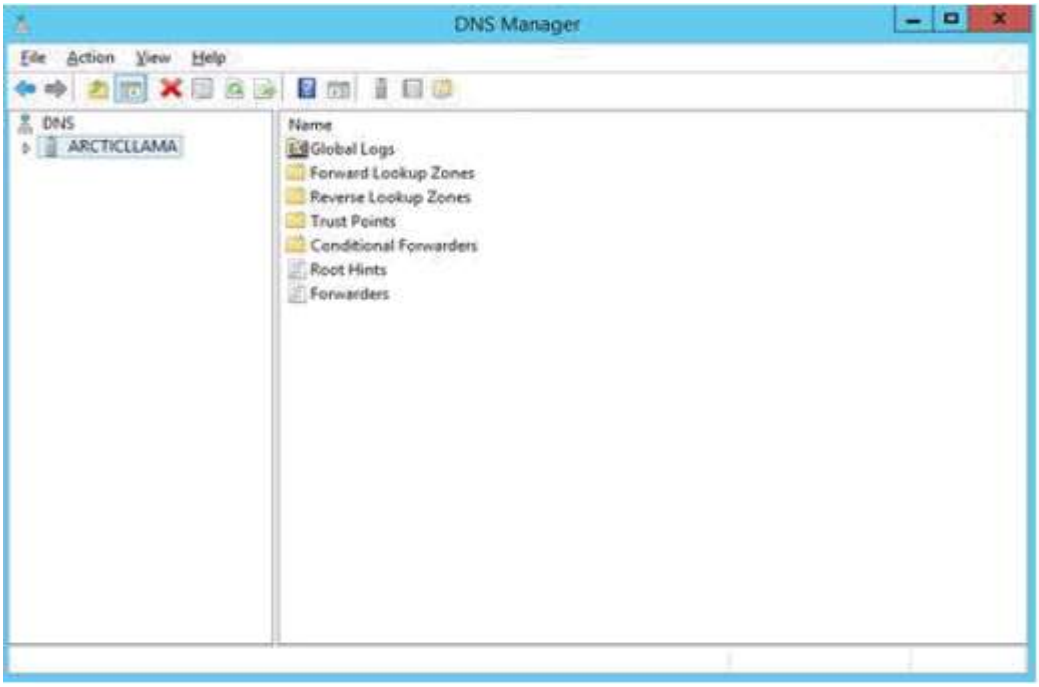


5. Managing DNS Zones

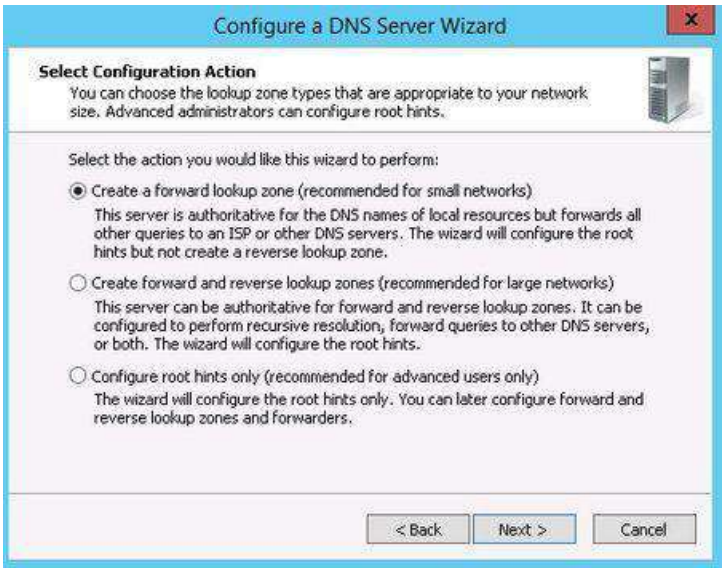
If you are an old pro with DNS server files, Windows Server 2012 does let you edit the files directly. However, Microsoft recommends that you use the interface tools to avoid errors, especially if you are integrating DNS with Active Directory.

If you want to use the command line to configure your DNS, use the **dnscmd** command. For those of us who don't memorize TechNet for fun, a few clicks is all it takes.

Within Server Manager, to configure the DNS Server, click the Tools menu and select **DNS**.



This brings up the wizard. There are three options here. You can either: configure a forward lookup zone only, create forward and reverse lookup zone, or configure root hints only.



A forward lookup zone allows you to do the standard DNS function of taking a name and resolving it into an IP address.

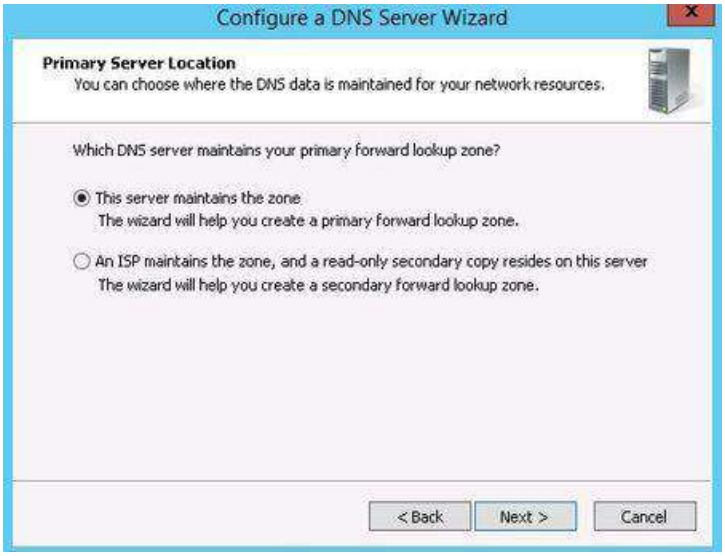
A reverse lookup zone allows you to do the opposite, taking an IP address and finding its name. For example, if a user is set up to print to a printer with an IP address of 10.20.12.114, but you need to know what name that

printer goes by so you can find it, a reverse lookup can help. ("Ah, hah! It's you Third Floor Vending Room Printer #1. Why you give me so much trouble?)

Root hints only will not create a database of name records for lookups, but rather will just have the IP addresses of other DNS servers where records can be found. If you already have DNS setup on your network, you'll probably want to continue using the same configuration you already have. If not, use forward and backward for most situations. (Backup zones typically don't hurt anything, and they are nice to have when the need arises.)

After you've made your section, click Next.

Now, you choose whether this server will maintain the zone, or if this server will have a read-only copy of the DNS records from another server.



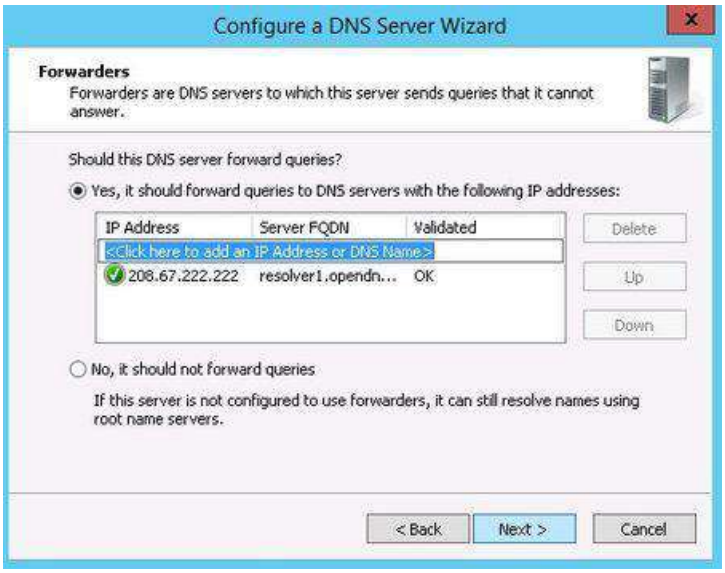
Next enter your zone name. If this is your first DNS server, then this needs to be the root zone name for your entire organization. For example, my zone name might be arcticllama.com. If however, this server will be authoritative only for a subset, and other DNS servers will be responsible for other zones, then the name will need to reflect that. For example, us.arcticllama.com would be the zone name for just the American part of my vast corporate empire : Click next when you have entered the name.

Now, you need to choose the file name where the DNS records will be stored. The default filename is to add a **.dns** extension to the name of the zone you chose in the previous window. Unless you have a corporate policy stating otherwise, stick with the convention to make things easier on yourself down the line.

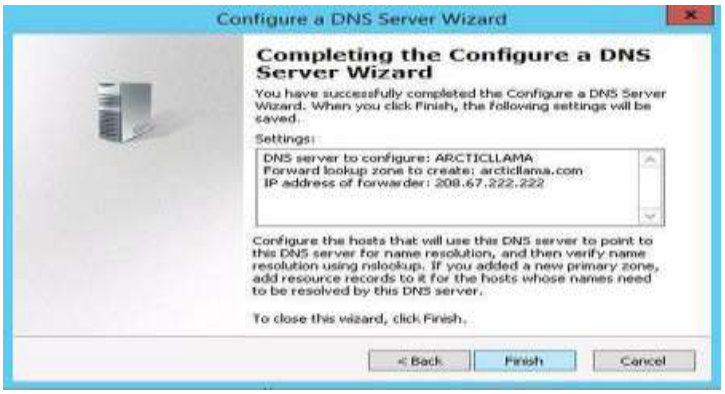
Next you select how this server will respond to Dynamic Updates. Although there are three choices here, only two should actually be used in production. Select the first option to **allow only secure dynamic updates** if you are integrating your DNS with Active Directory. Select **do not allow dynamic updates** if your DNS is not integrated with Active Directory and you

don't want to allow dynamic updates. Do not allow unsecured dynamic updates unless you really know what you are doing and have a very good reason for doing so.

Up next is the option to configure forwarders. If your DNS server ever gets a query for which it has no record, it can forward that request on to another DNS server to see if it has the answer.



For example, in order to provide name resolution for internet connectivity, you can input your ISP name servers here, or use a DNS provider such as OpenDNS. You can (and should) have more than one server listed in case a DNS server is unreachable for some reason. The order forwarders are listed in is the order they are tried, so place your faster and most reliable forwarder at the top of the list. Click Next and your DNS server is now configured and ready for use.



LO 3.3 configure the server roles and features: file and share access services

- Content/Topic 1: configuration of File and Printer Services

A. Securing Files and Folders

- Select the **file** or **folder** you want to encrypt.
- Right-click the **file** or **folder** and select Properties.
- On the General tab, click the advanced button.
- Check the box for the "Encrypt contents to **secure** data" option, and then click OK on both windows.

B. Protecting Shared Files and Folders

This is a two-step process: you must first share the folder, and then publish it in Active Directory.

1. Use **Windows Explorer** to create a new folder called **Engineering Specs** on one of your Disk volumes.

2. In **Windows Explorer**, right-click the folder name, and then click **Properties**.

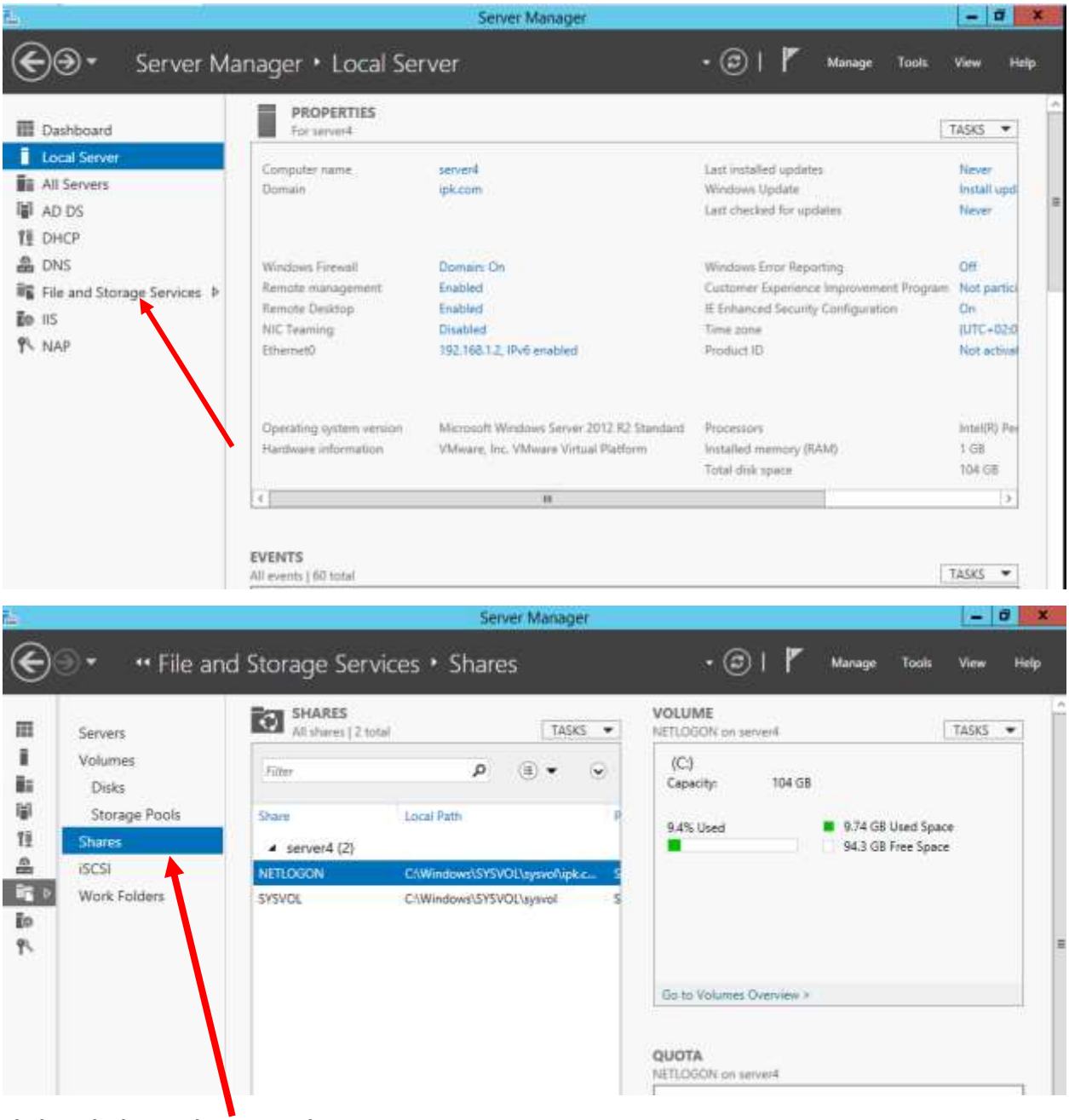
Click **Sharing**, and then click **Share this folder**.

3. In the **New Object–Shared Folder** dialog box, type **ES** in the **Share name** box and click **OK**. By default, Everyone has permissions to this shared folder. If you want, you can change the default by clicking the **Permissions** button.

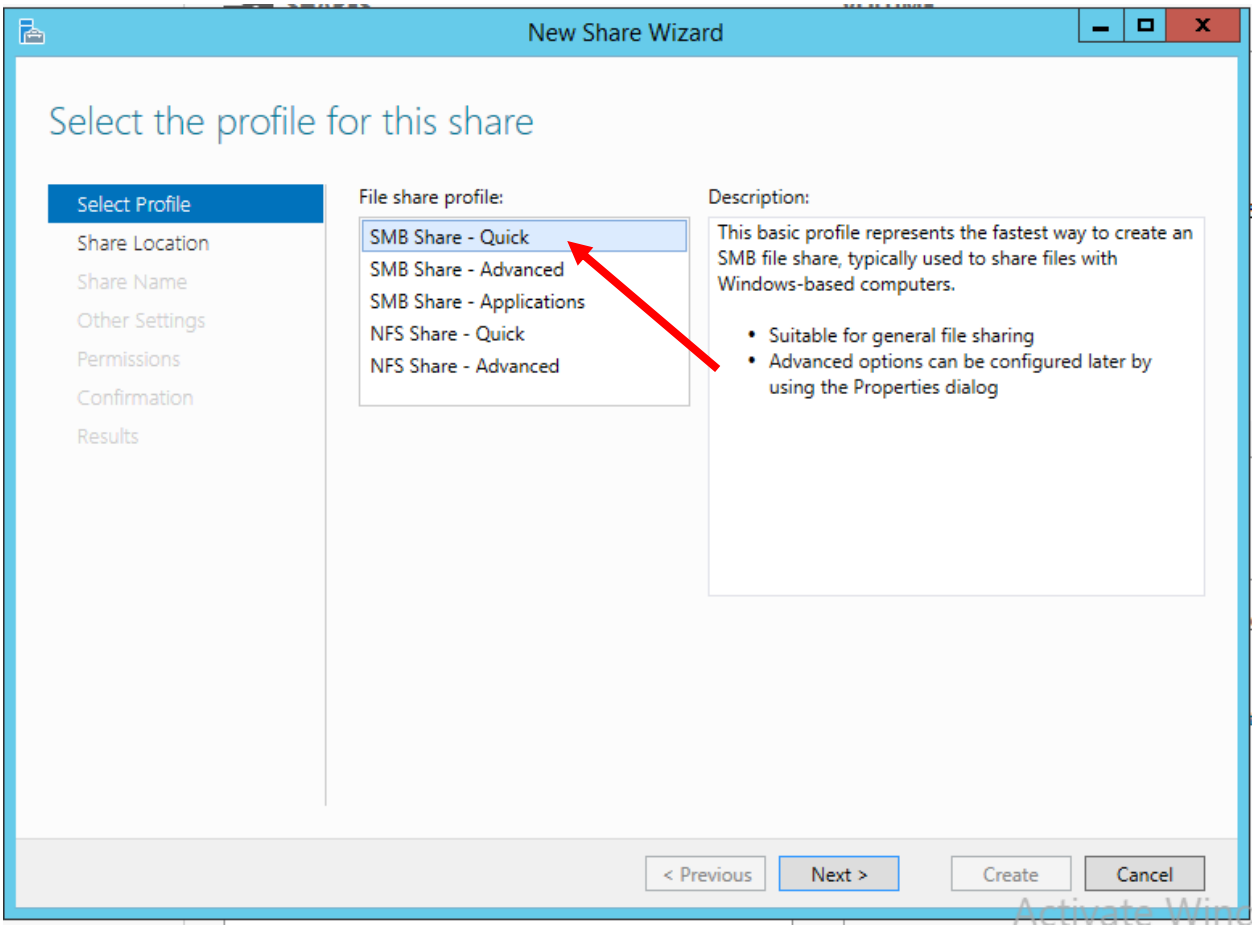
4. Populate the folder with files, such as documents, spreadsheets, or presentations.

To publish the shared folder in the directory in window server 2012 R2 steps

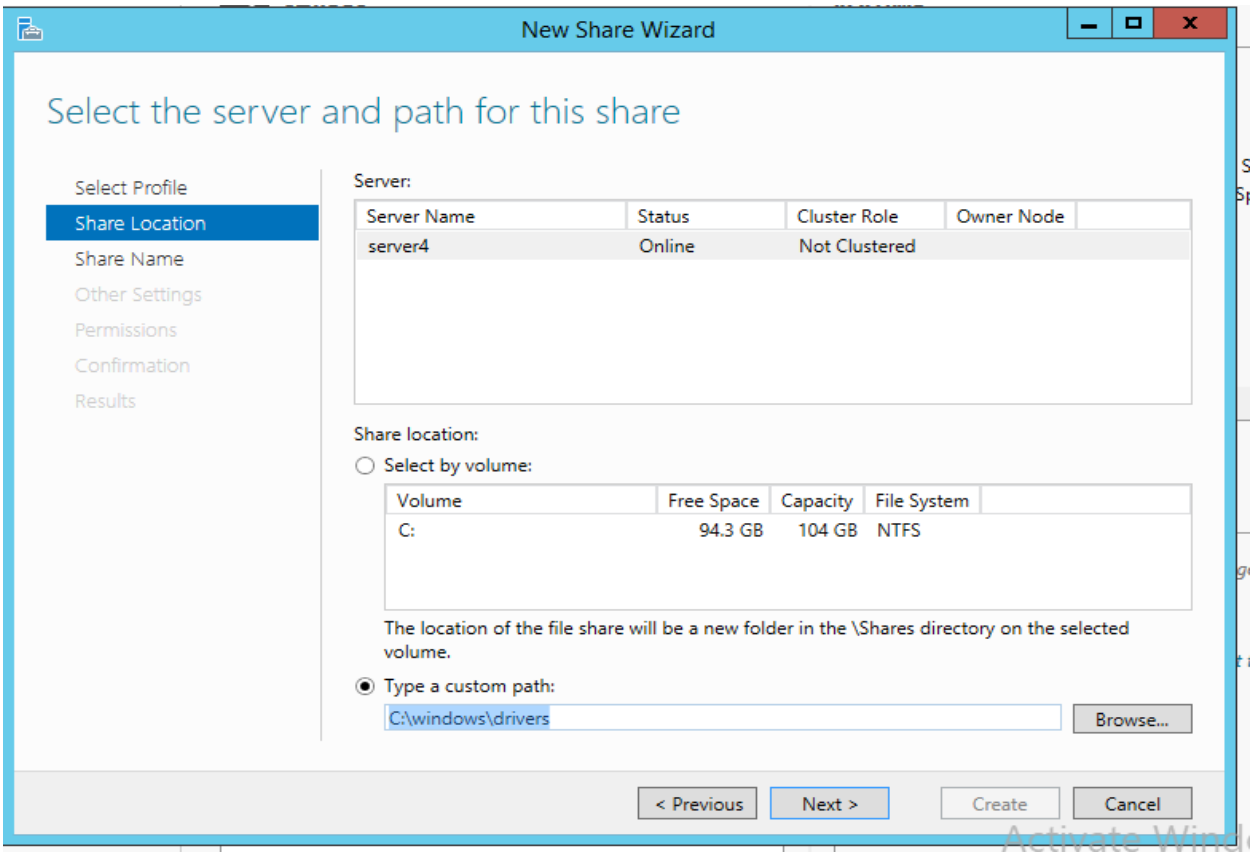
Step 1 Open server manager then click file and storage services



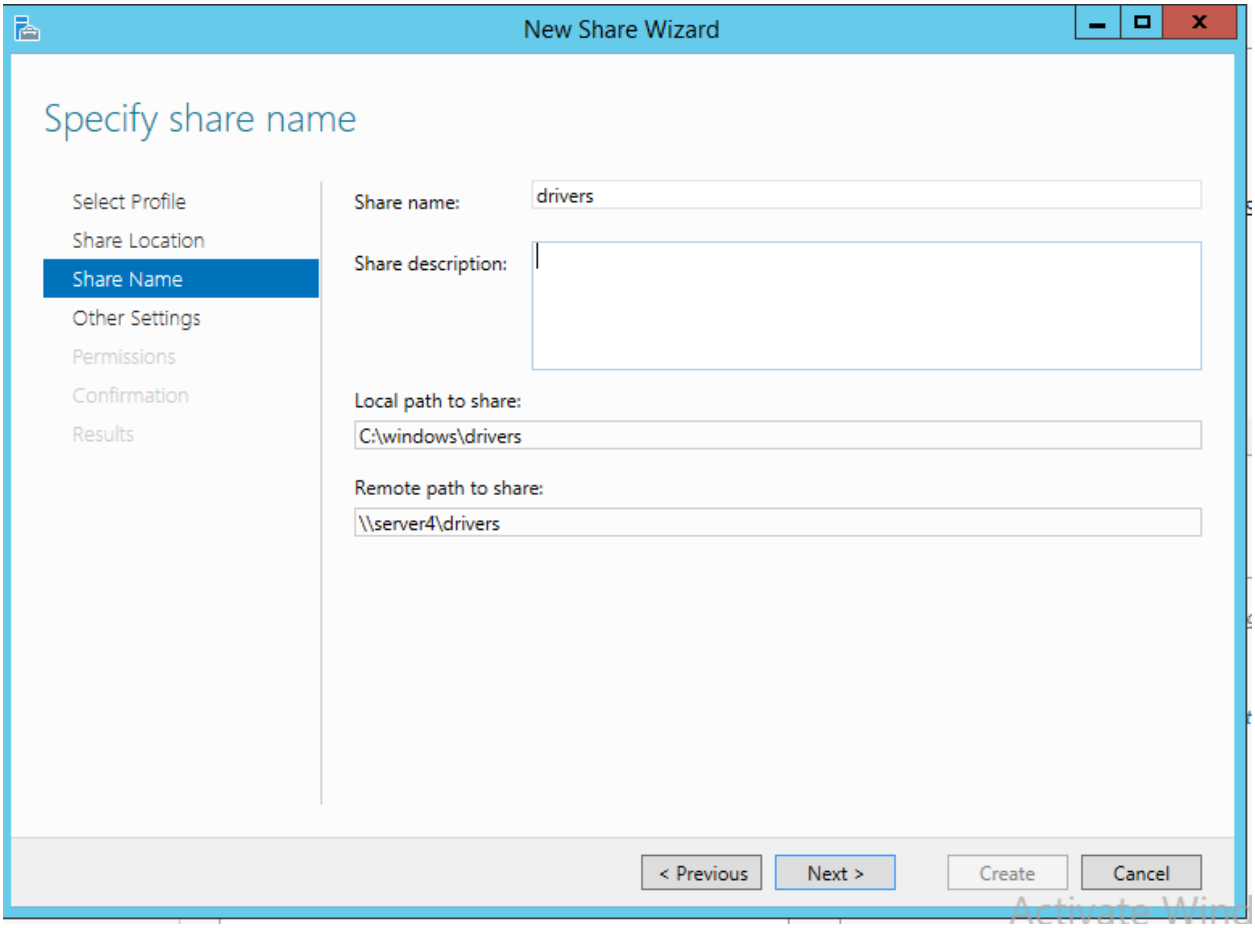
Click task then select new share



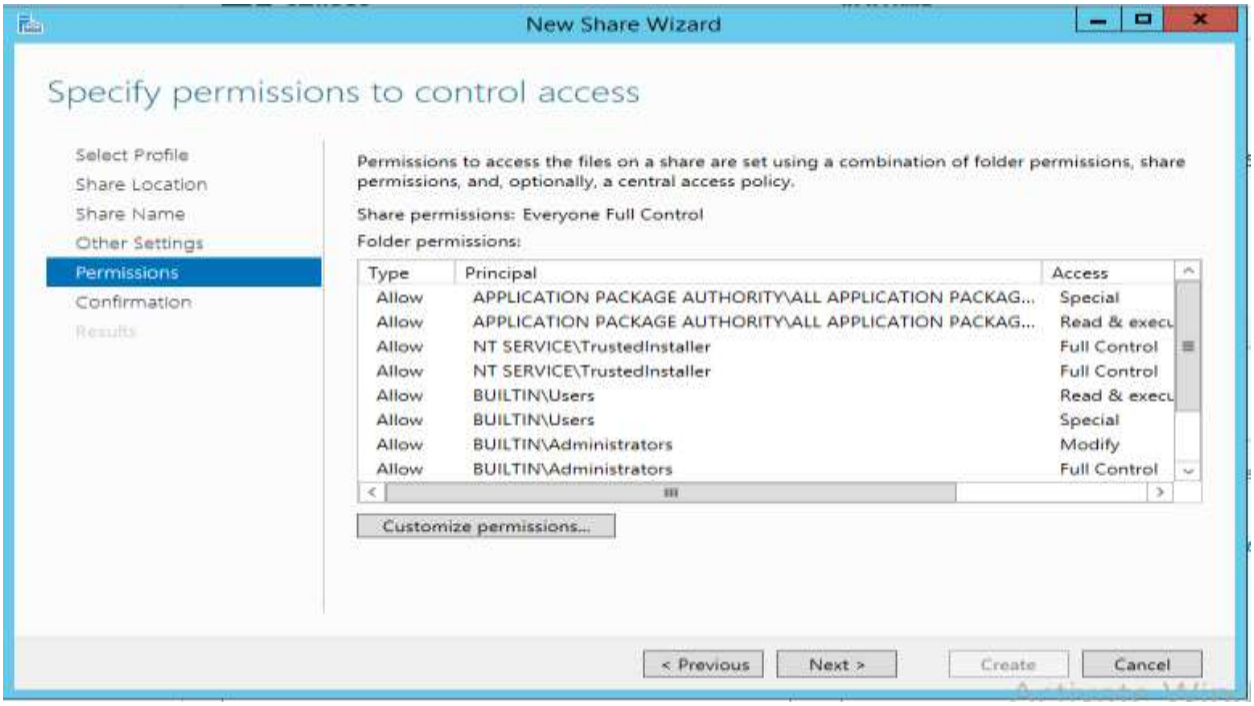
Select SMB share quick from different type of file shares then Click next



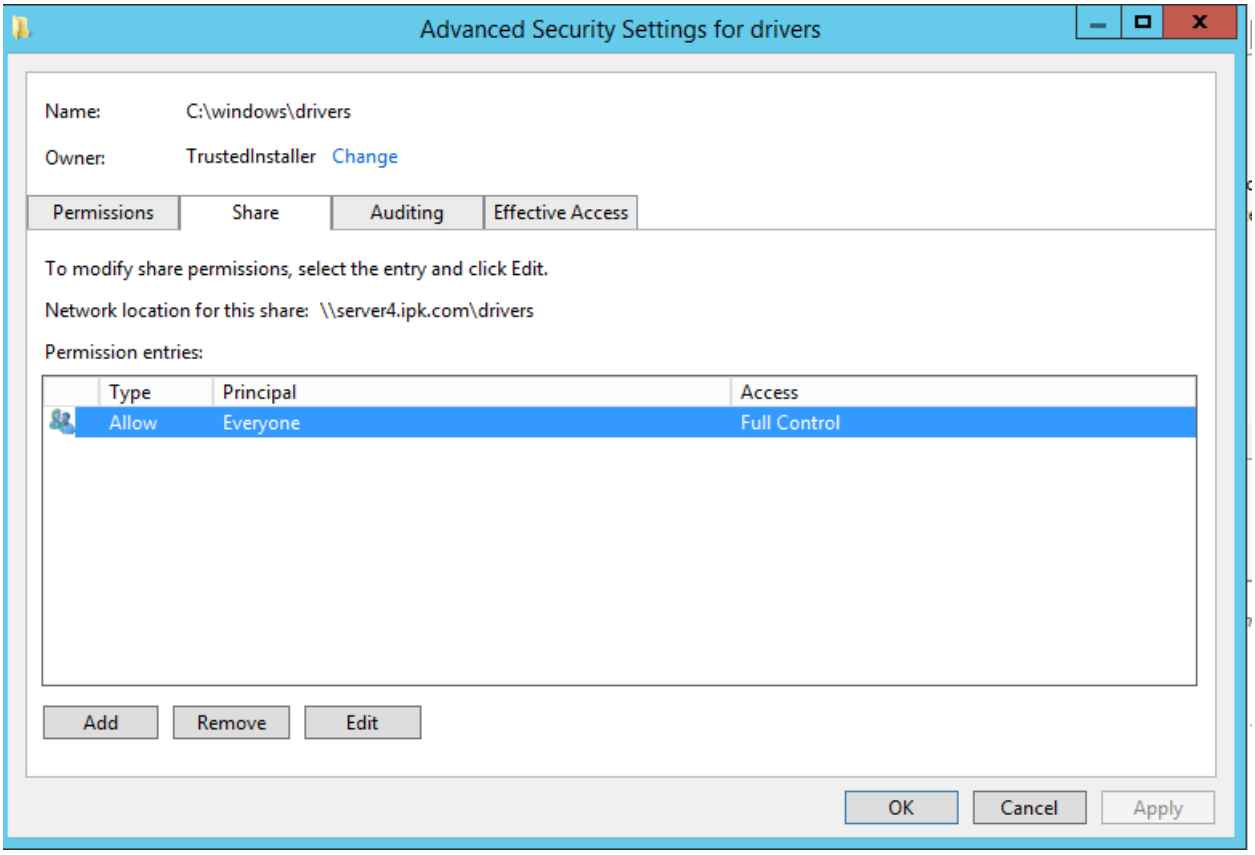
Select the volume of the file share from the location by click the option type a custom path then click next.



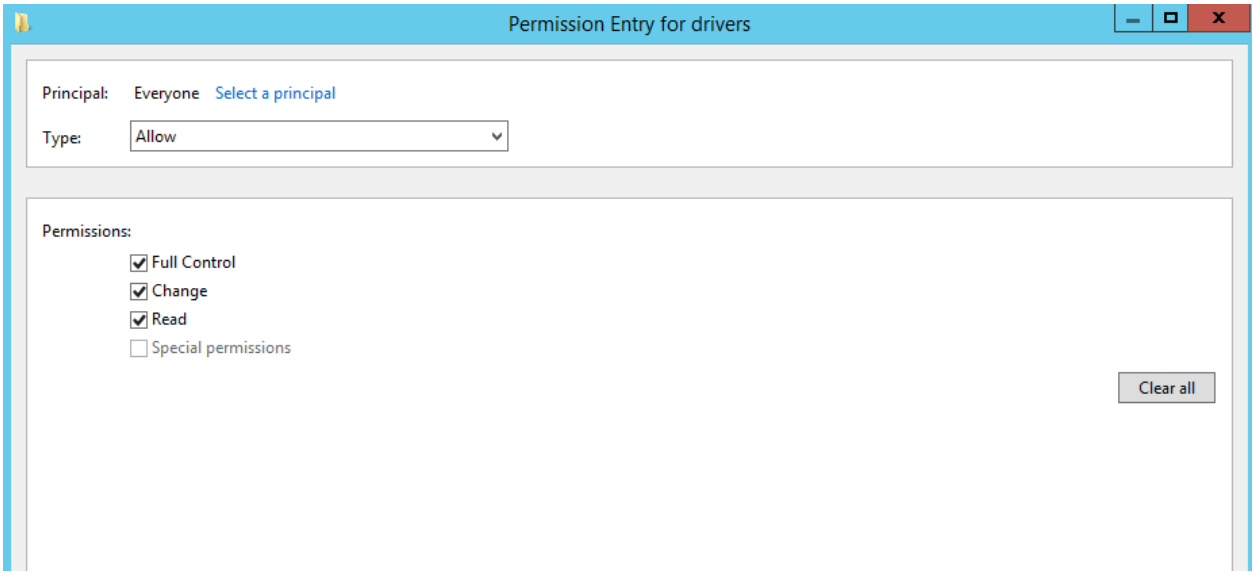
Type the name of share folder and share description then click next. NEXT



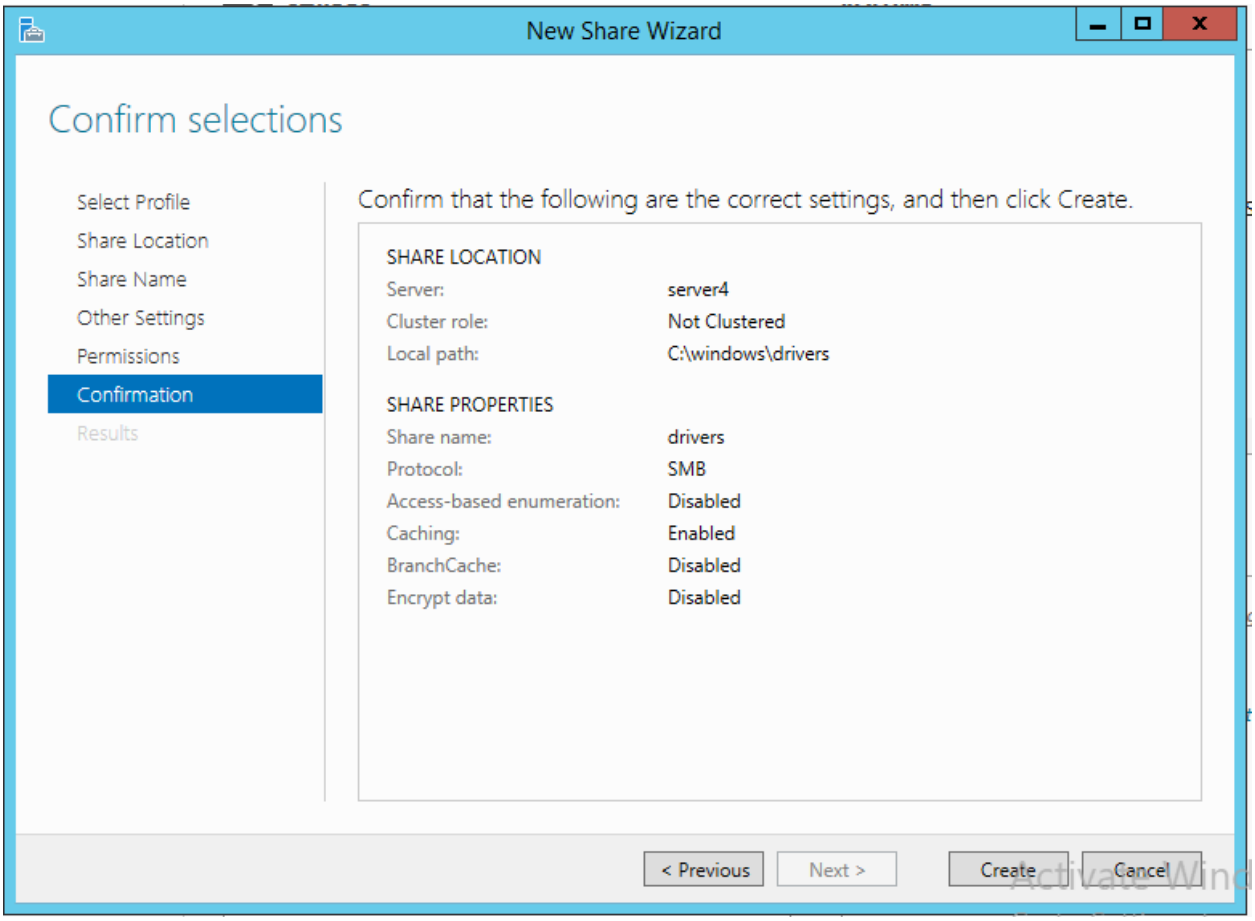
Click customize permission to specify permission to control access



Share this folder to everyone then click edit to modify permission



Give permission either full control or one of them, then clicks ok, ok and next.



Click create to confirm the task

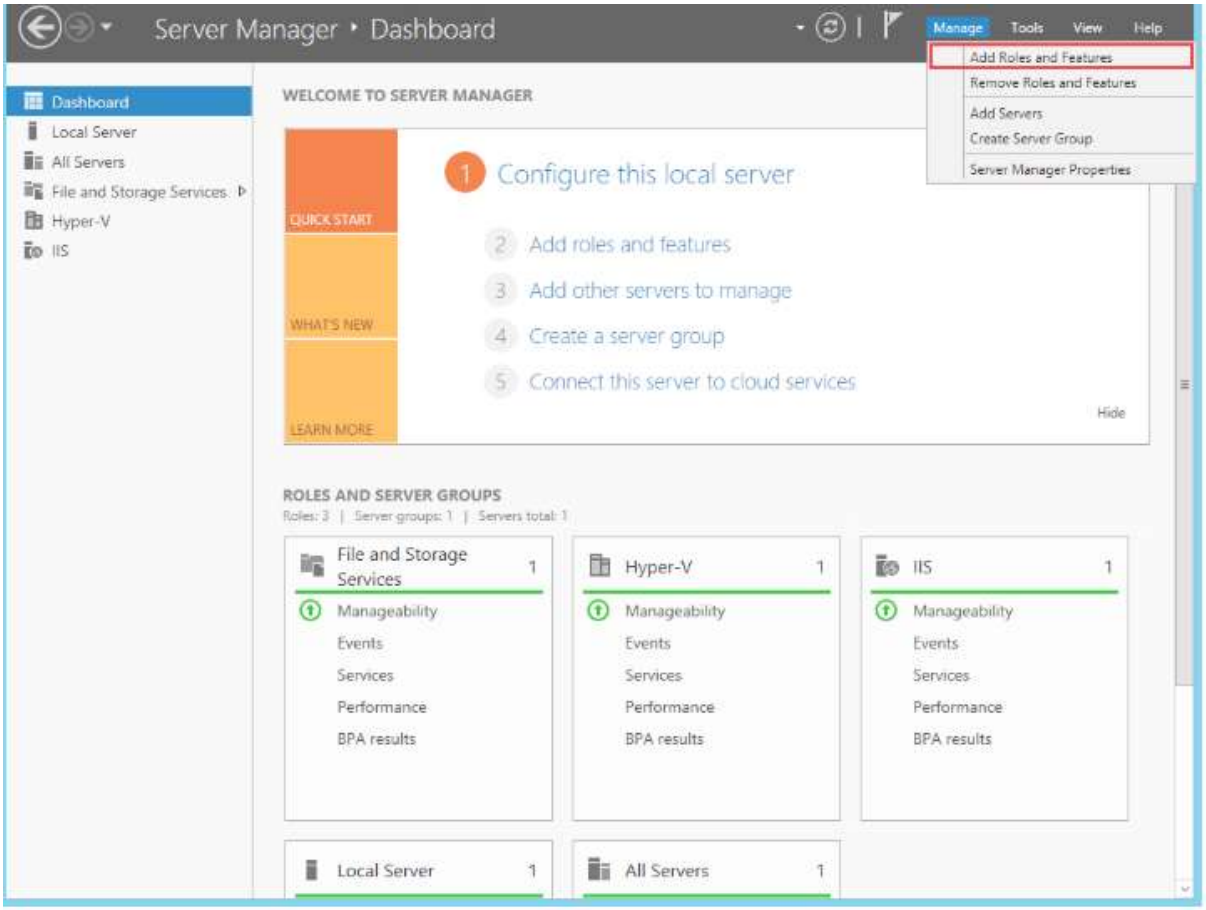
C. Configuring Work Folders

Work Folders is a quite interesting feature introduced by **Microsoft** with **Windows Server 2012 R2**. In a nutshell, Work Folders is a *synchronization service* for folders that works in a similar fashion of **Dropbox**, but in your own network/servers. You can access the synced data from Windows PCs or from mobile devices, an interesting opportunity for your company.

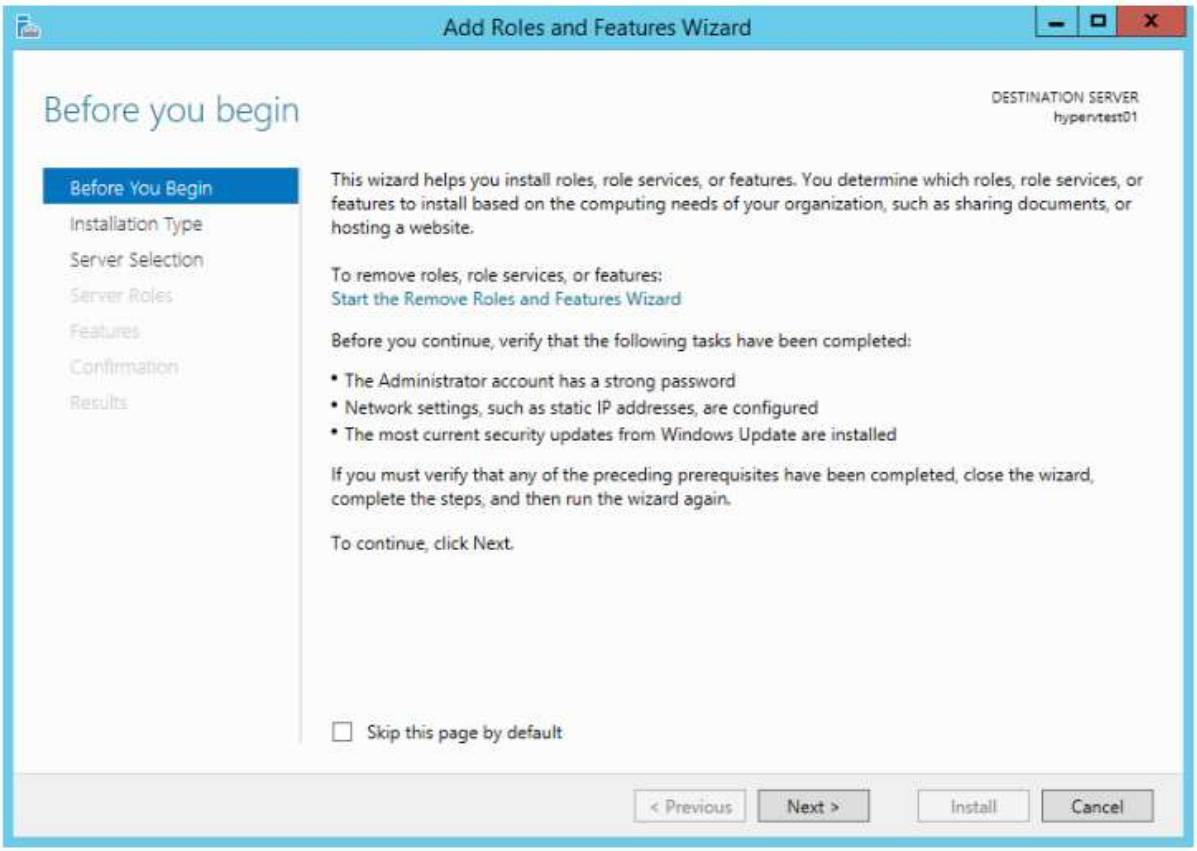
In an organization, every user wants to have one centralized file location where they can work on their files anytime and anywhere. Microsoft® introduces Work Folders in Windows® 2012 R2 to give users the flexibility to work on files offline or online. This allows data to auto sync with the centralized file server once it is connected to the Internet.

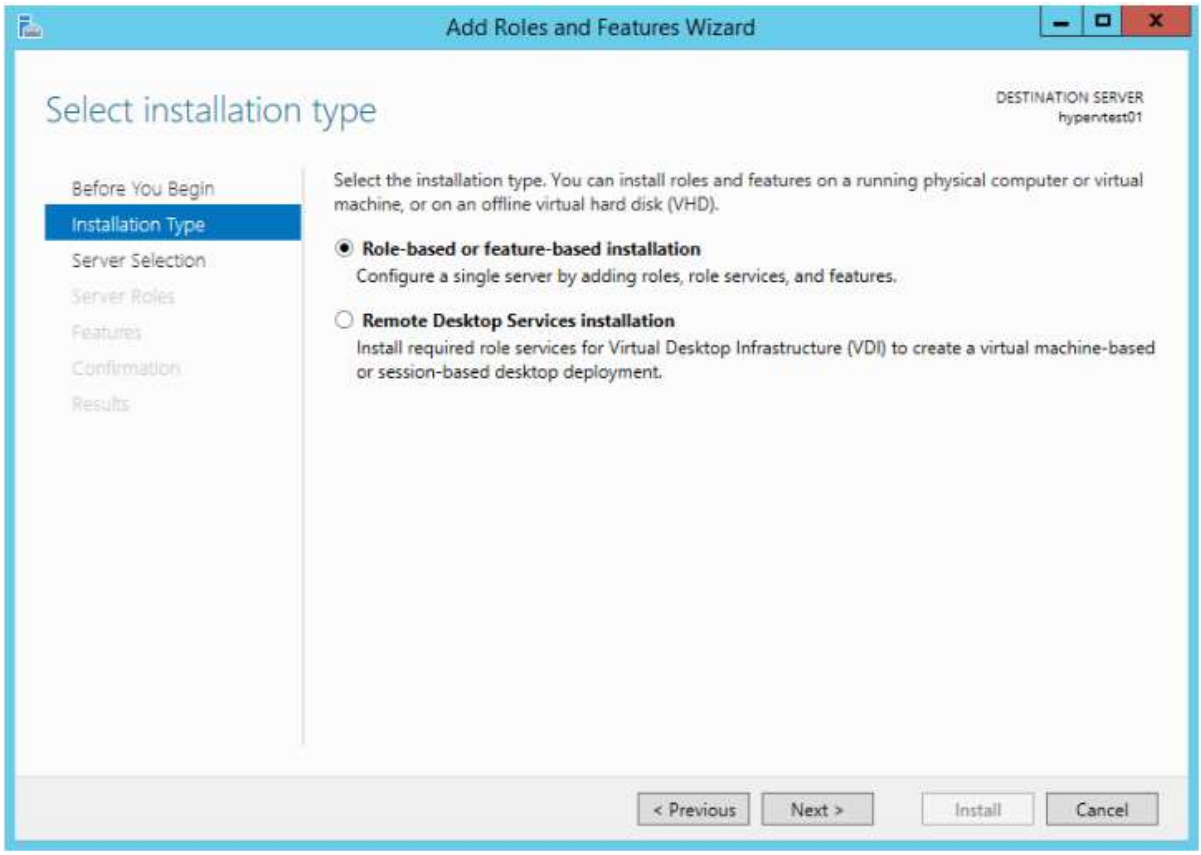
Step one: Install the Work Folders role

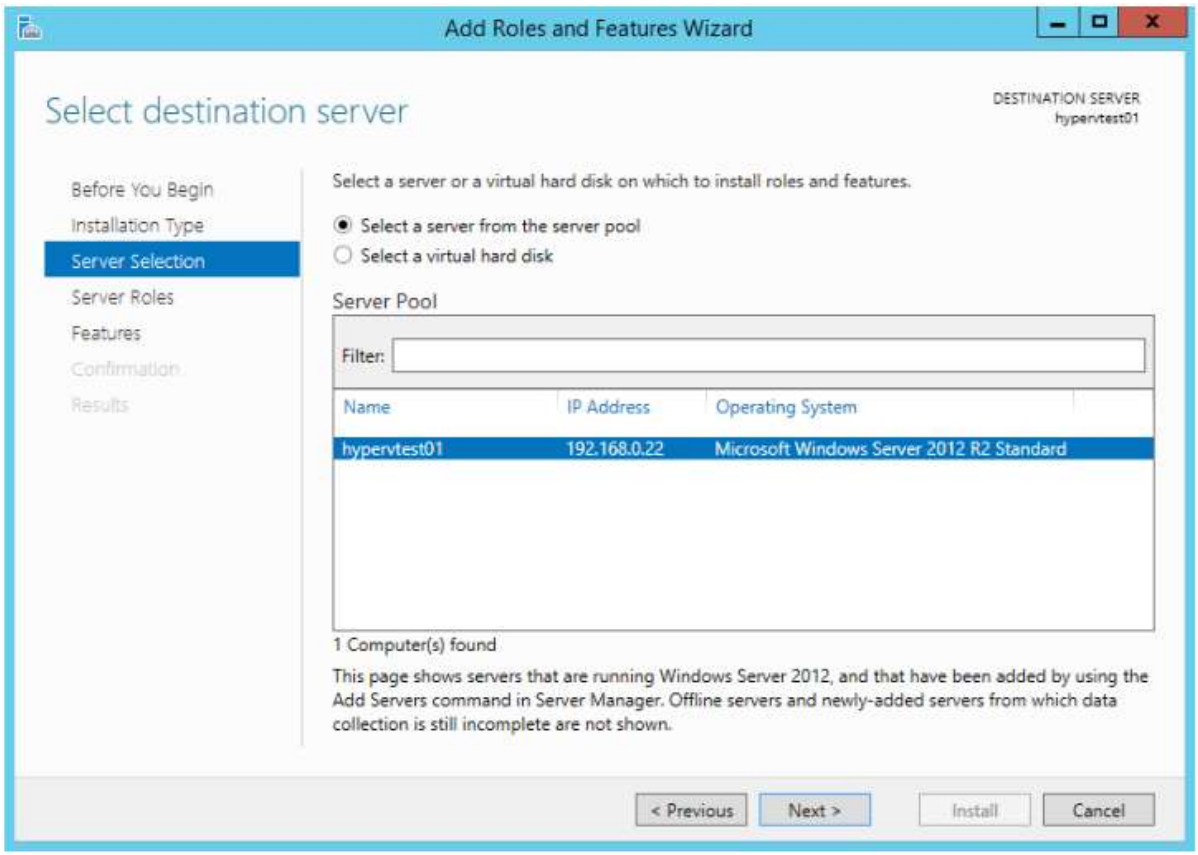
Launch the *Server Manager* and click on *Add Roles and Features* under the *Manage* menu:

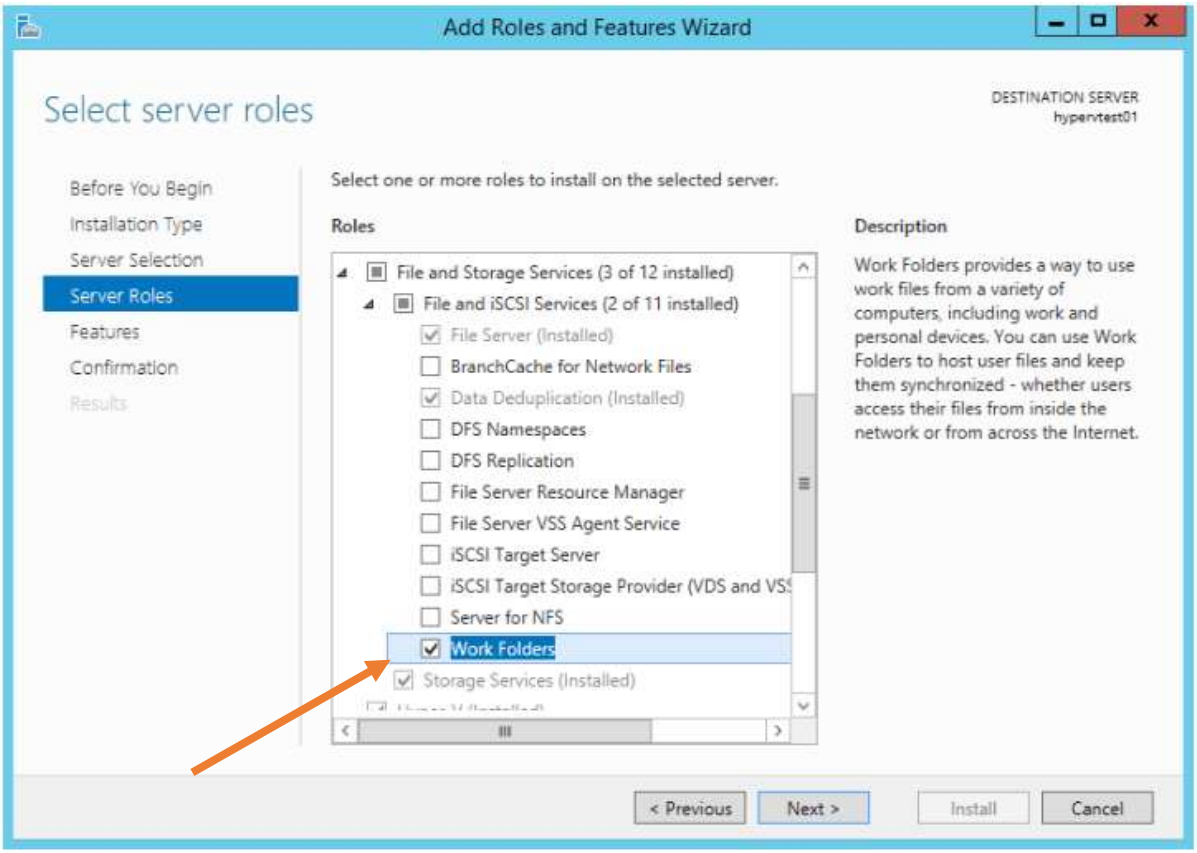


Follow the indications of the Wizard and go on:

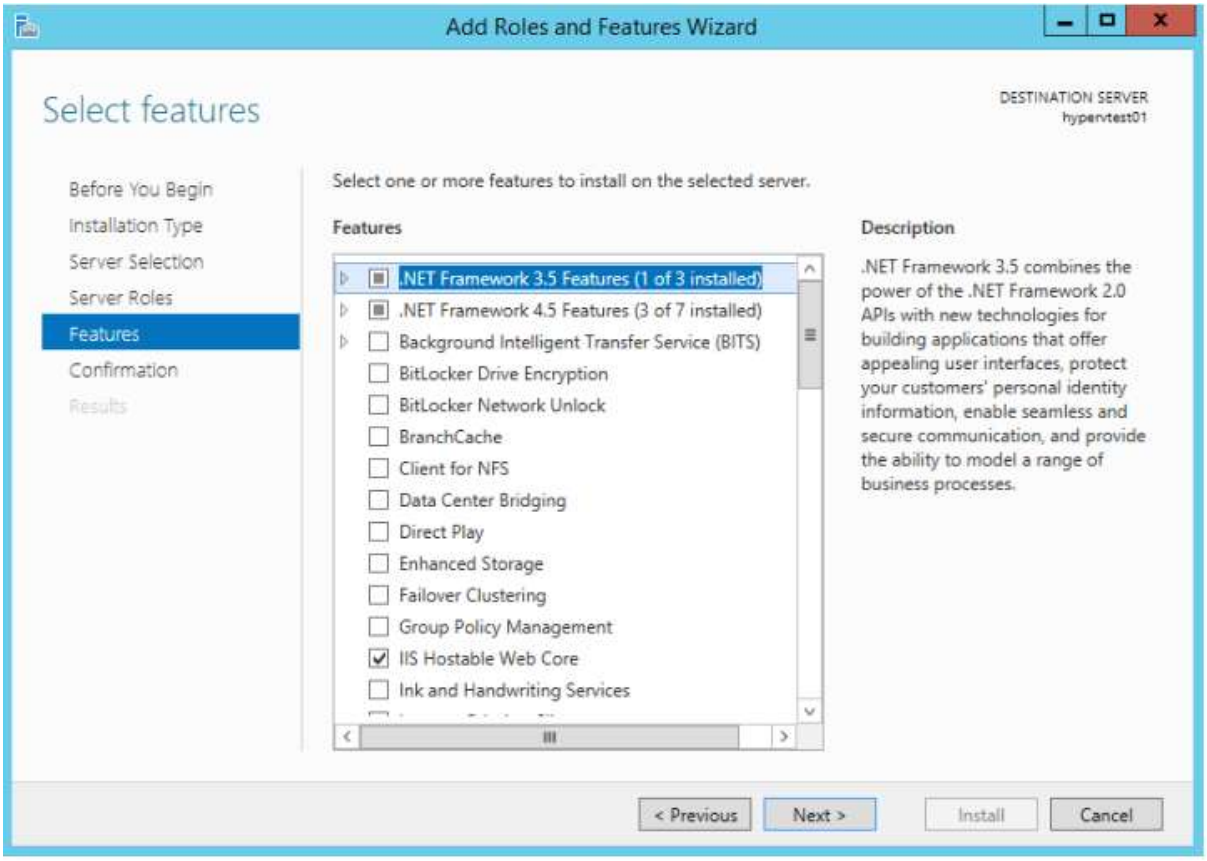



Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
hypervtest01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

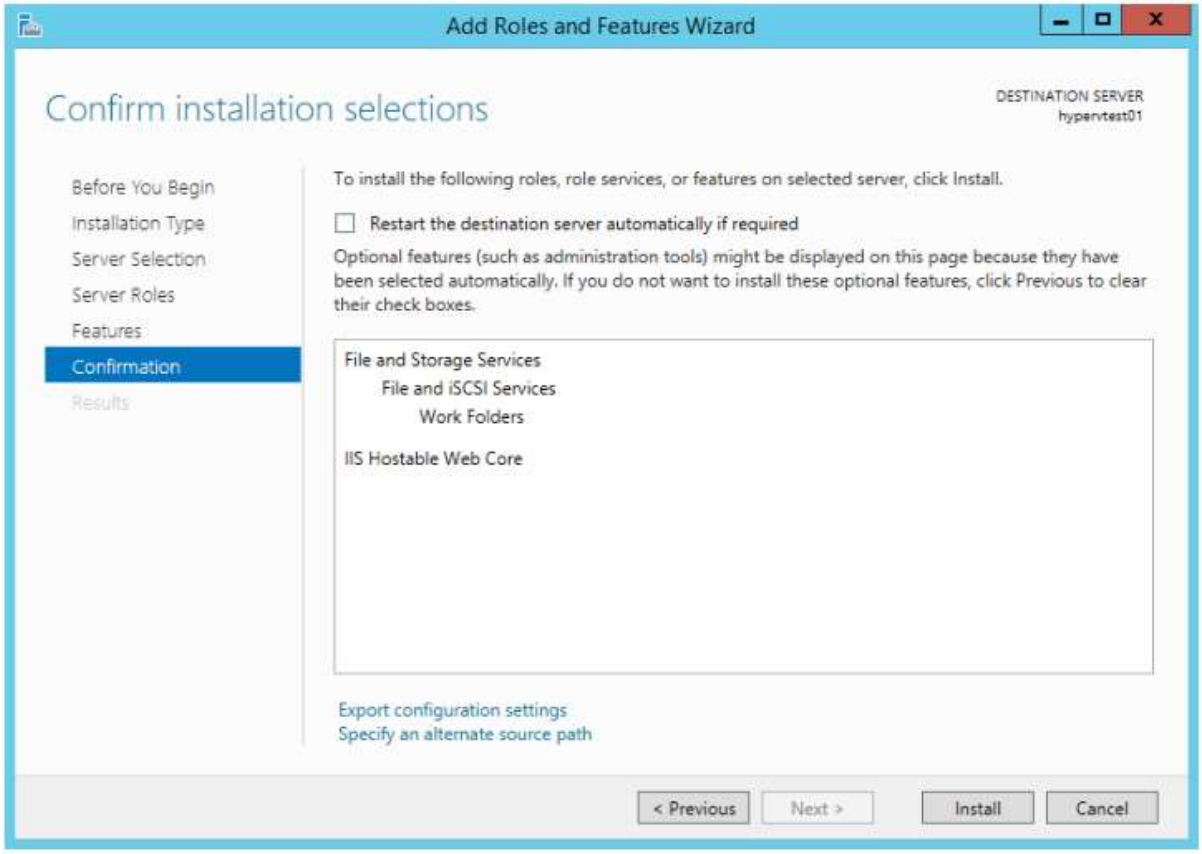

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
hypervtest01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
hypervtest01
192.168.0.22
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

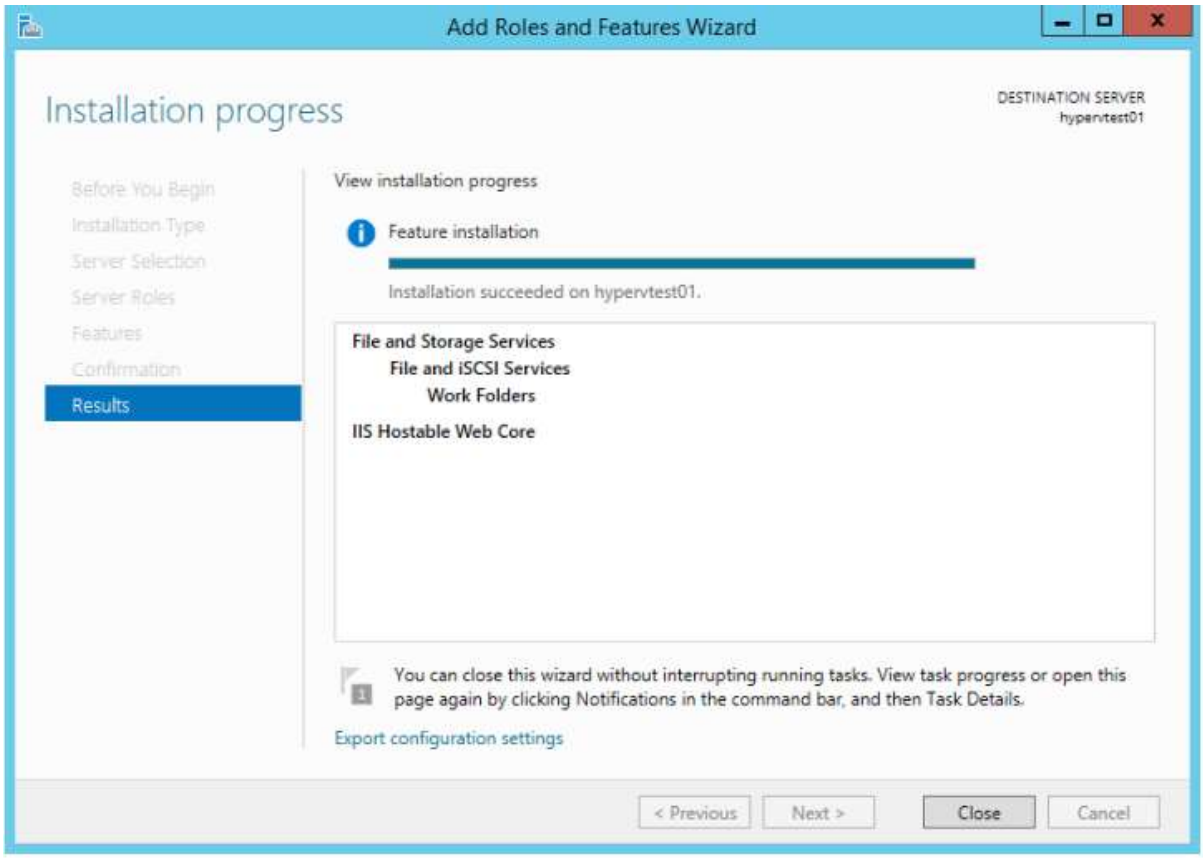


Ignore the **Features** step and go on:



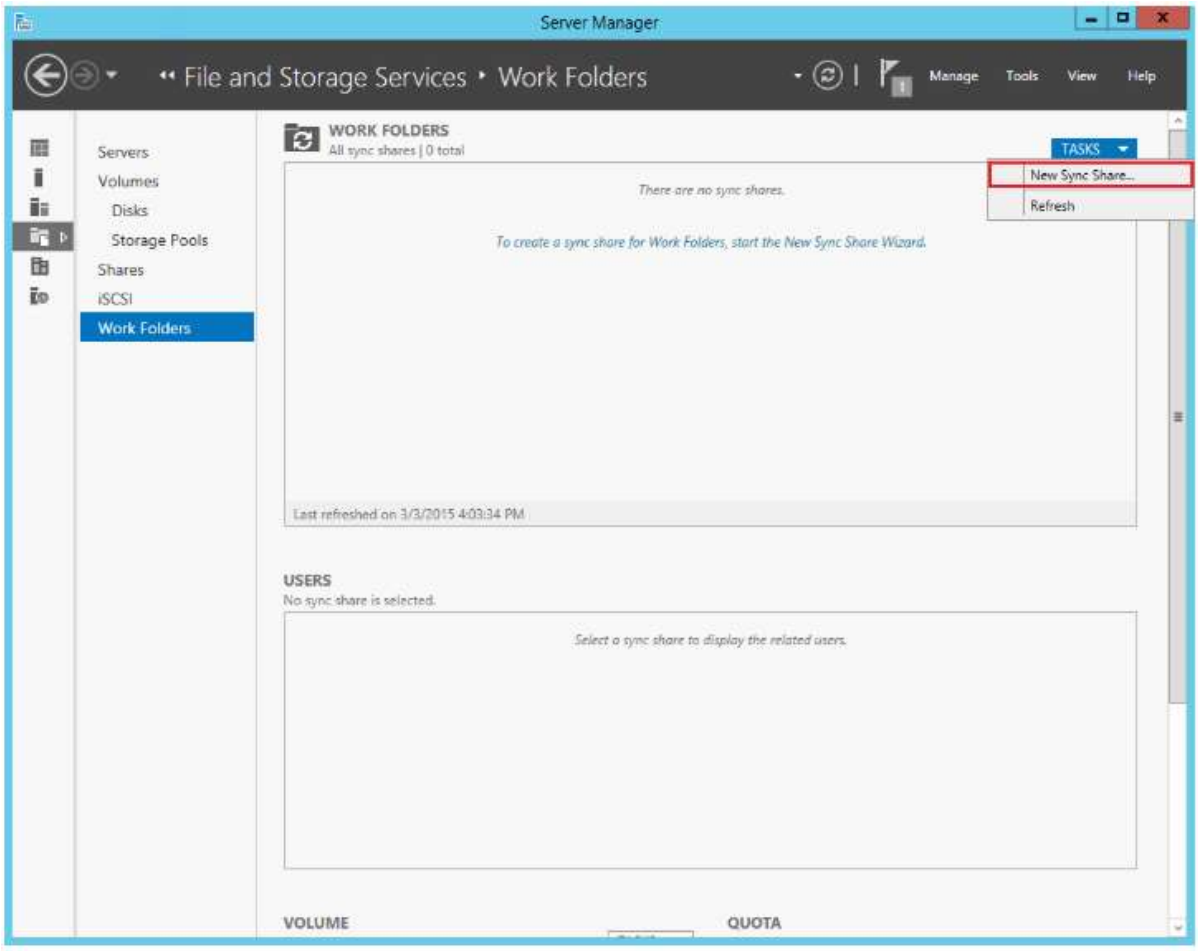
Confirm and the installation will begin:



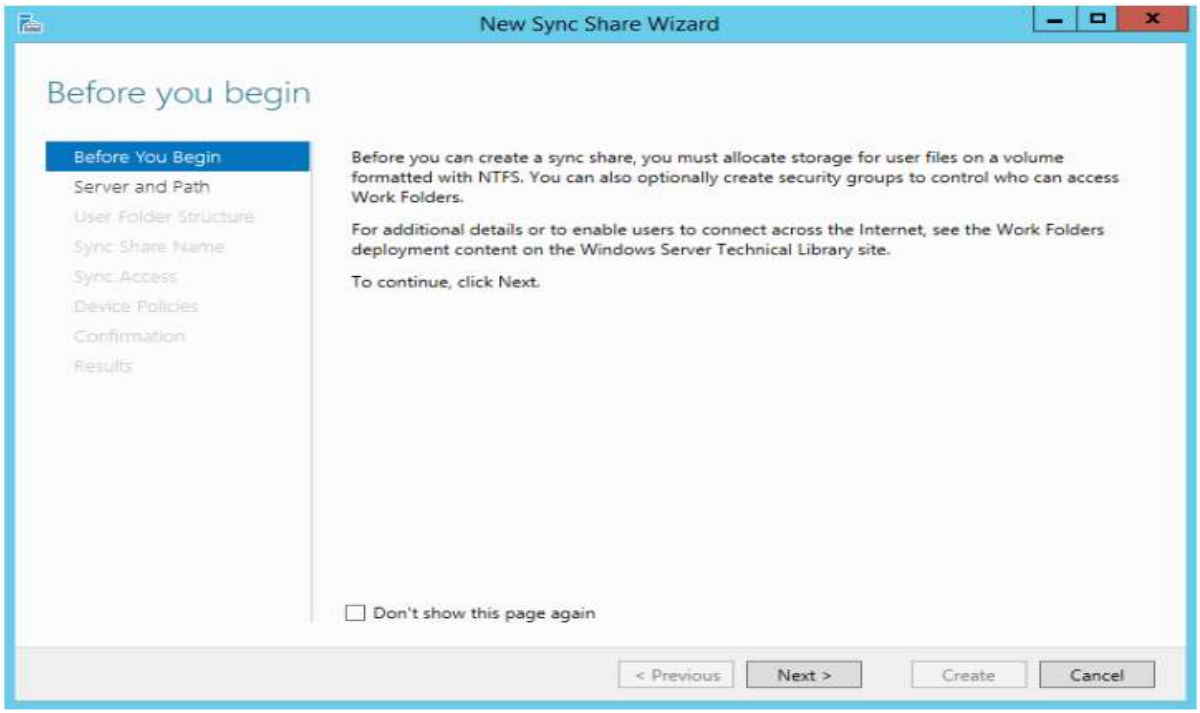


Step two: Create the Sync Share

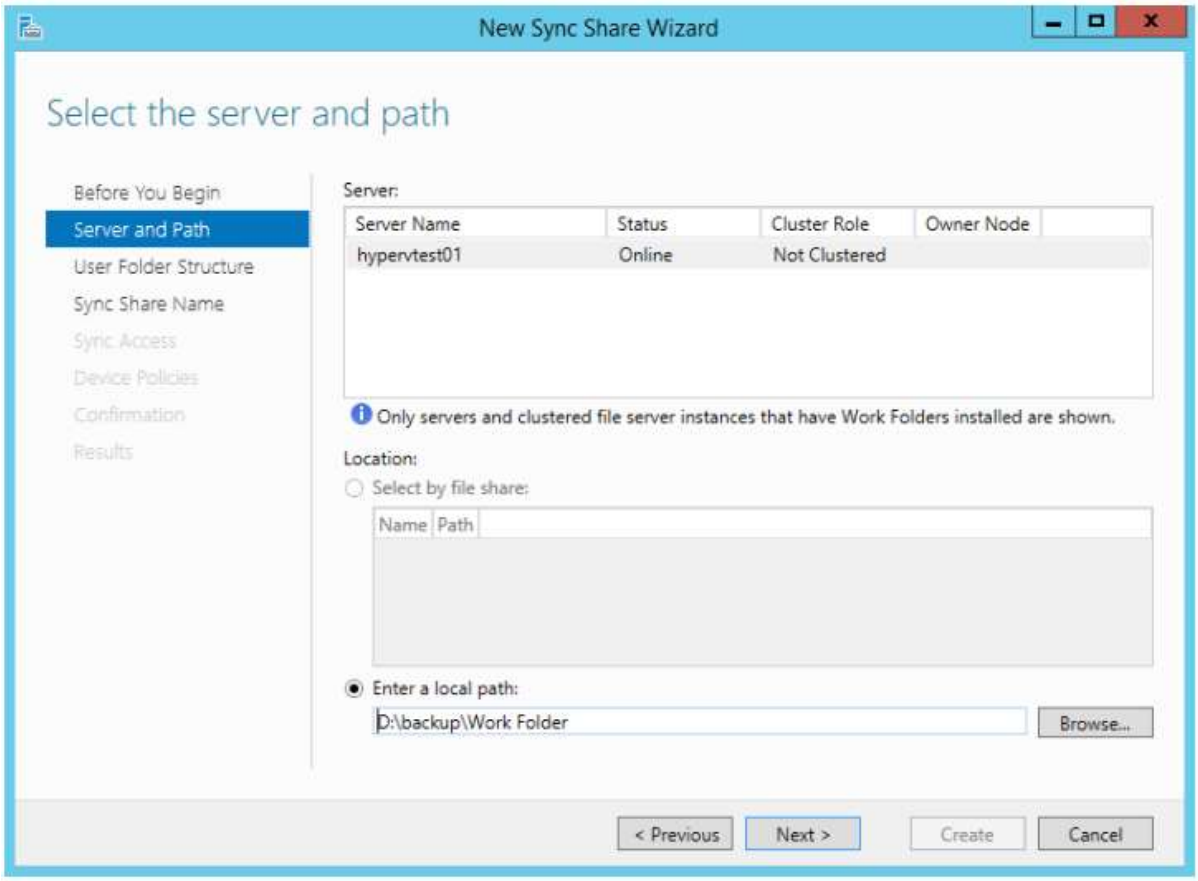
It's time to create the **Sync Share**. Go to the *File and Storage Services* area of the *Server Manager* and click on *TASKS*. Select *New Sync Share:*



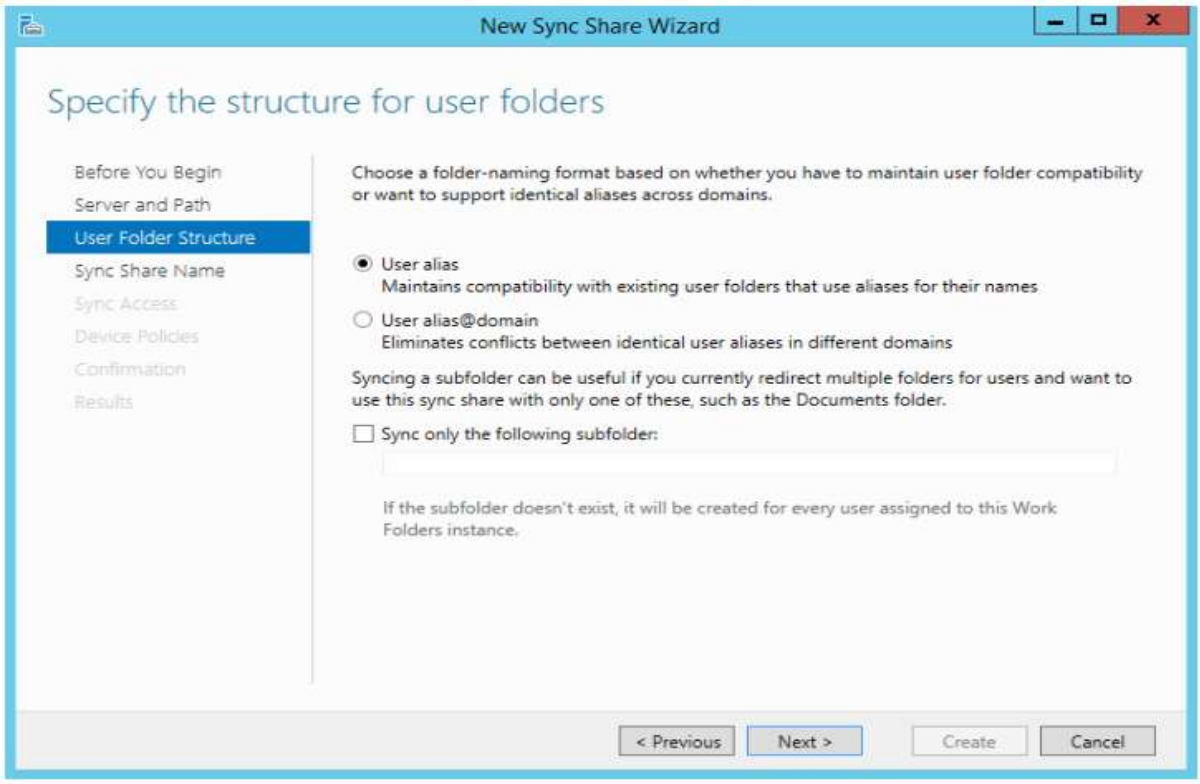
Click on *Next:*

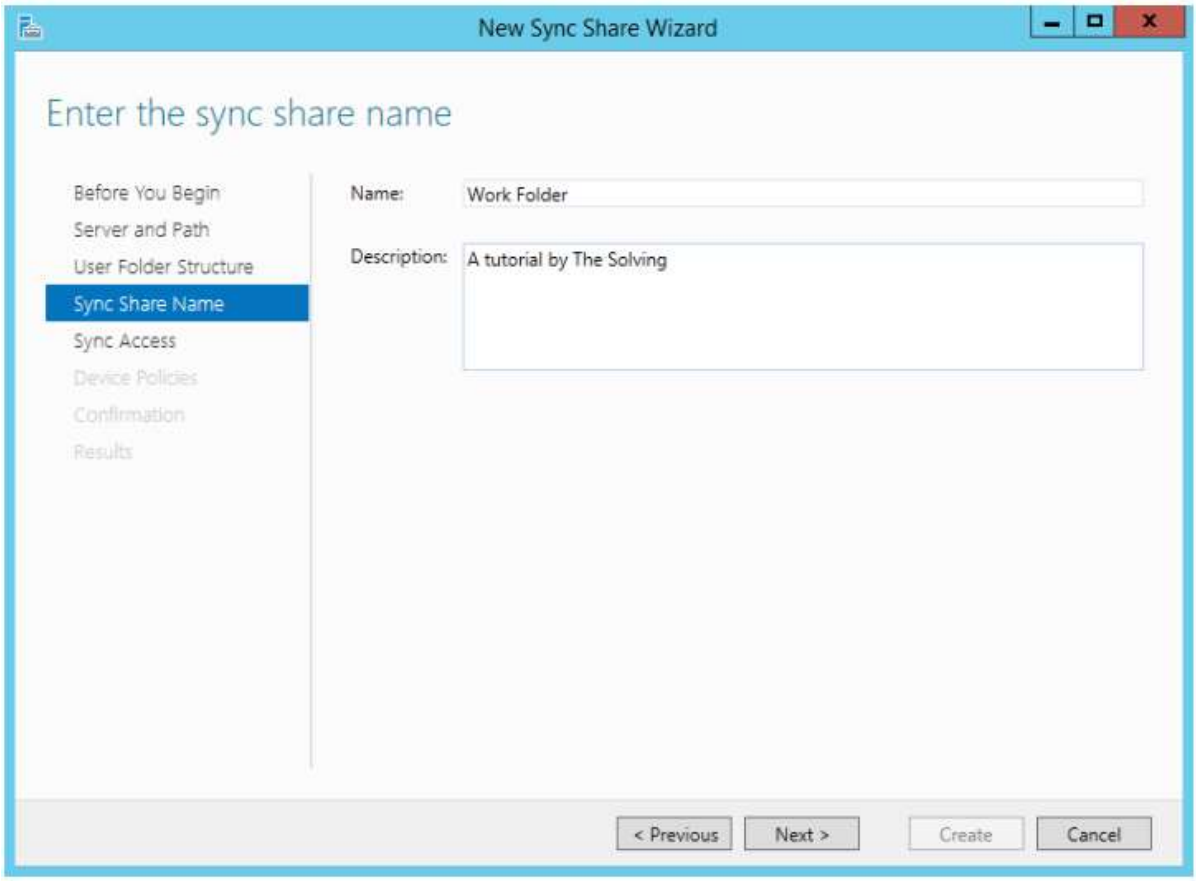


Specify the local path – must be *NTFS* – where the data will be synced:

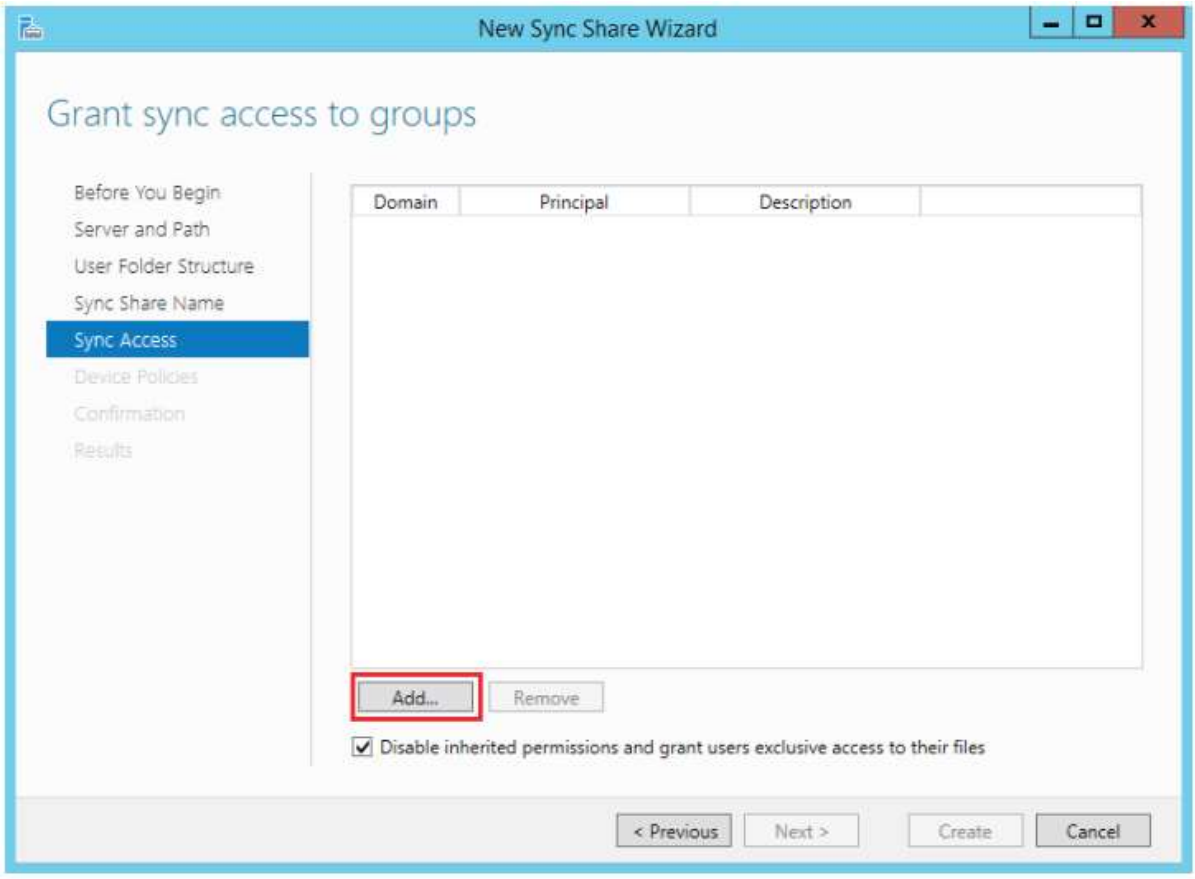


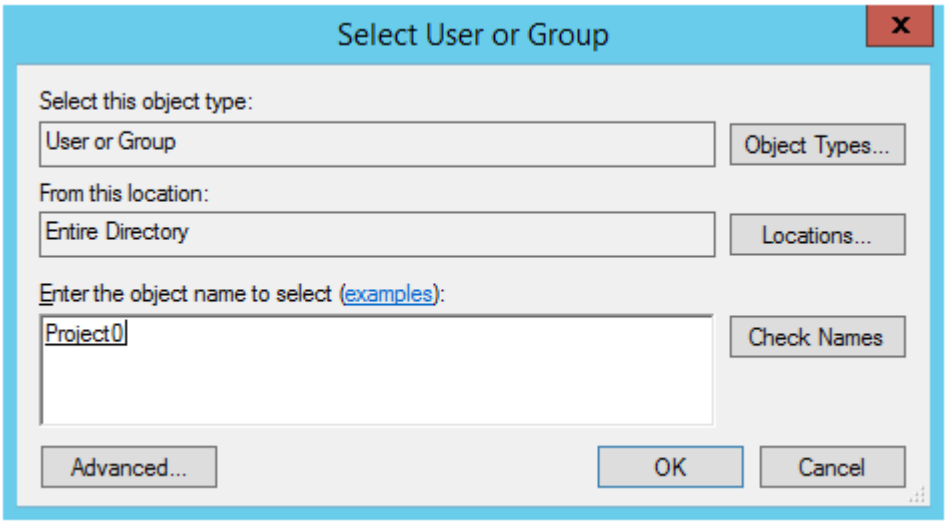
Define folder structure and name of the *Sync Share:*

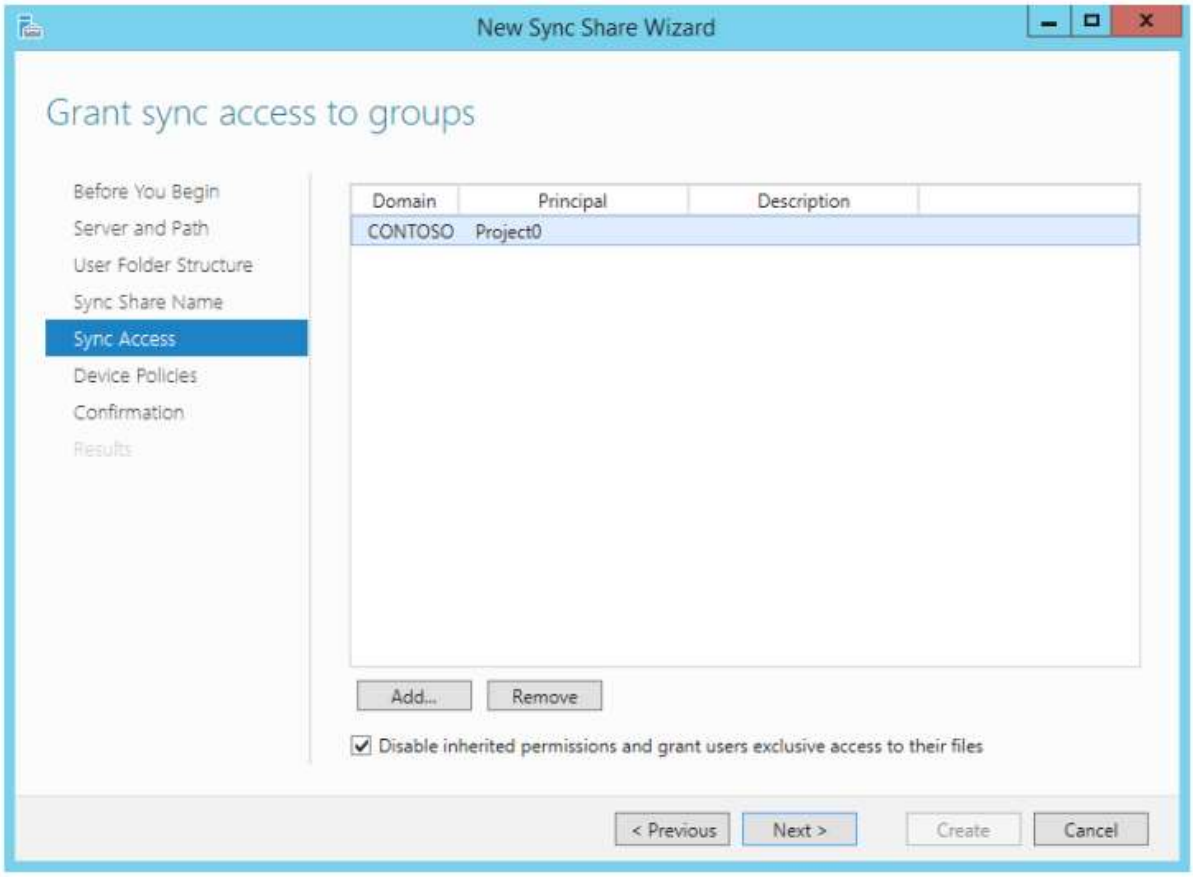




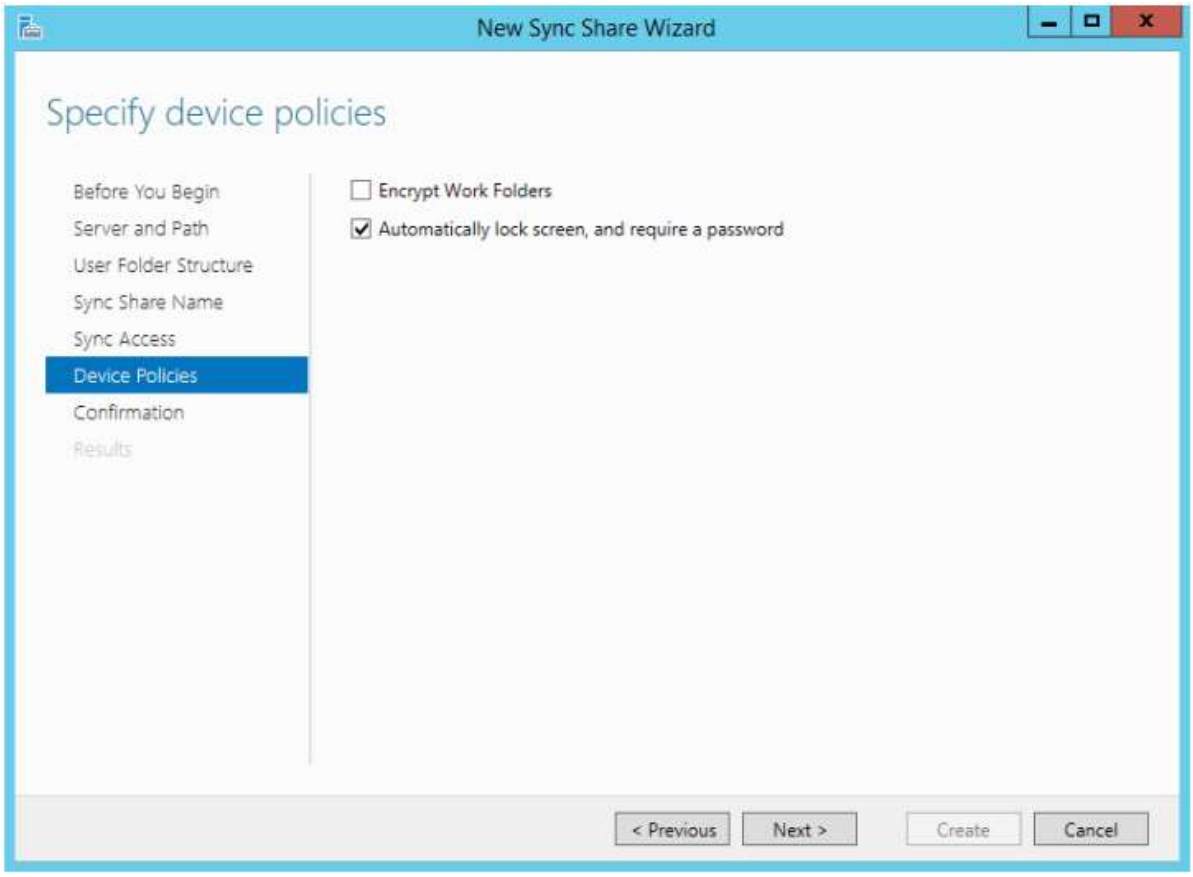
It’s time to select the users or the groups who will be able to access the *Sync Share:*



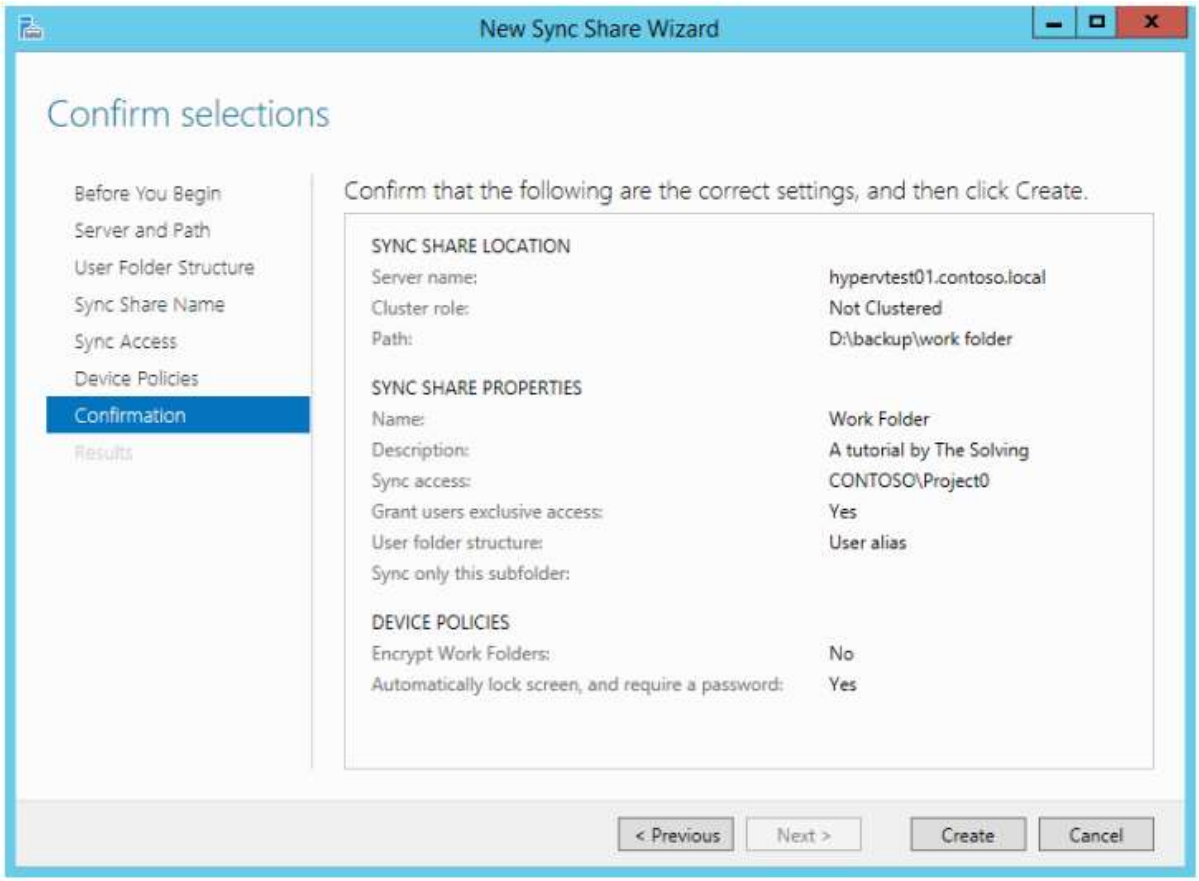


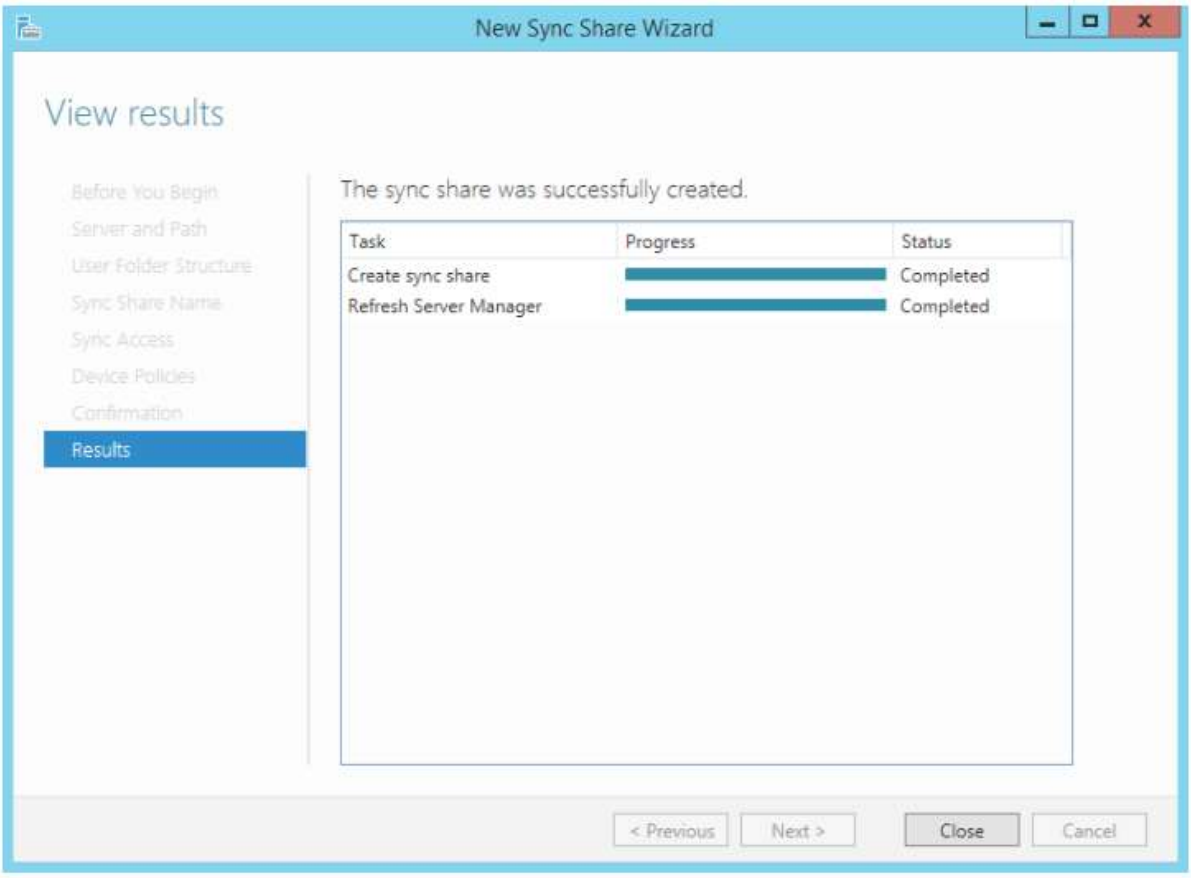


You can also encrypt the data if you desire:



Click on *Create* and your first *Sync Share* will be ready for use:





Content/Topic 2: Configuration of Network Printer

- **Publishing a Printer**

This section describes the processes for publishing printers in a Windows 2012R2 Active Directory based network.

- **Windows 2012R2 Printers**

You can publish a printer shared by a computer running Windows 2012r2 by using the **Sharing** tab of the printer Properties dialog box. By default, **Listed in the directory** is enabled.

The director is the Active Directory data store. (This means that Windows 2000 Server publishes the shared printer by default.) The print subsystem will automatically propagate changes made to the printer attributes (location, description, loaded paper, and so forth) to the directory.

Note: For this section of this guide, you must have a printer available and know its IP address. If you do not have an IP printer, you can still run through these procedures, substituting the correct port for Standard TCP/IP Port.

- **To add a new printer**

1. Click **Start**, point to **Settings**, click **Printers**, and then double-click **Add Printer**.

The **Add Printer Wizard** appears. Click **Next**.

2. Click **Local Printer**, clear the **automatically detect and install my Plug and Play printer** checkbox, and click **Next**.

3. Click the **Create a new port** option, then scroll to **Standard TCP/IP Port**, and click **Next**.

4. The **Add Standard TCP/IP Printer Port Wizard** appears. Click **Next**.

5. On the **Add Port** page, type the IP address of the printer in the **Printer Name or IP Address** box, type the port name in the **Port name** box, and click **Next**. Click **Finish**.

6. Select your printer's manufacturer and model in the Printers list box, and then click **Next**.

7. In the **Printer name** text box, type the name of your printer.

8. On the **Printer Sharing** page, type a name for the shared printer. Choose a name no more than eight characters long so computers running earlier versions of the operating system display it correctly.

9. Type in the **Location** and **Comment** in those text boxes.

10. Print a test page. Click **Finish**.

After you create the printer, the printer is automatically published in Active Directory and the **Listed in the Directory** check box is selected.

You might also need to find the server from which a printer is shared out before adding it to the machine you're working on.

- **To locate a printer**

1. Click **Start**, point to **Settings**, and then click on **Printers**.

2. Double-click the **Add Printer** icon.

3. In the **Add Printer Wizard** dialog box, click the **Next** button.

4. Select the **Network printer** button, and then click **Next**.

5. Select the **Find a printer in the Directory** button, and then click **Next**.

6. The **Find Printers** dialog box displays. If you know which domain your printer resides in, click the **Browse** button and choose that domain to narrow your search. Then, on the **Printer** tab, add the printer **Name**, **Location**, or **Model** to those text boxes, and click the **Find Now** button.

Note: If you don't know the name, location, or model of the printer, you can simply click the Find Now button, and all the printers in the domain you selected will be listed in the list box.

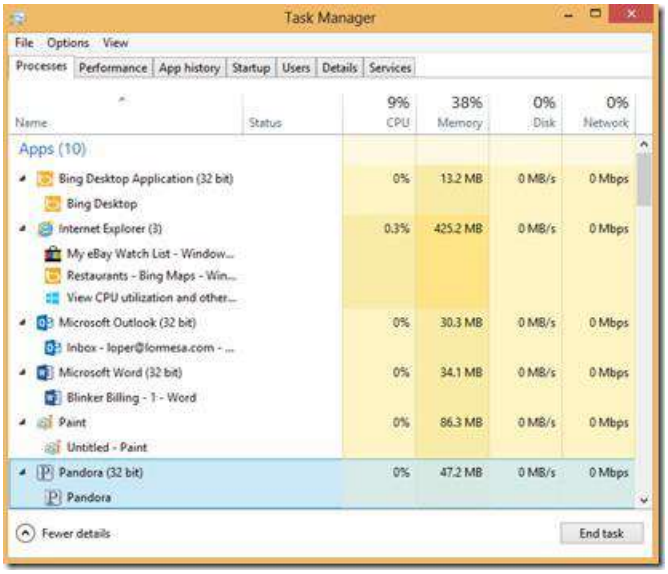
LO 4.1 Test the server performance

- Content/Topic 1: Testing and Monitoring Server performance

1. CPU Usage

Resource Monitor is a tool built into Windows and Windows Server that provides more detail about processor usage than Task Manager. ... This tab provides details about processor usage such as Name, PID, Description, Status, Threads, CPU, and Average CPU. The rows of data can be sorted in ascending or descending order.

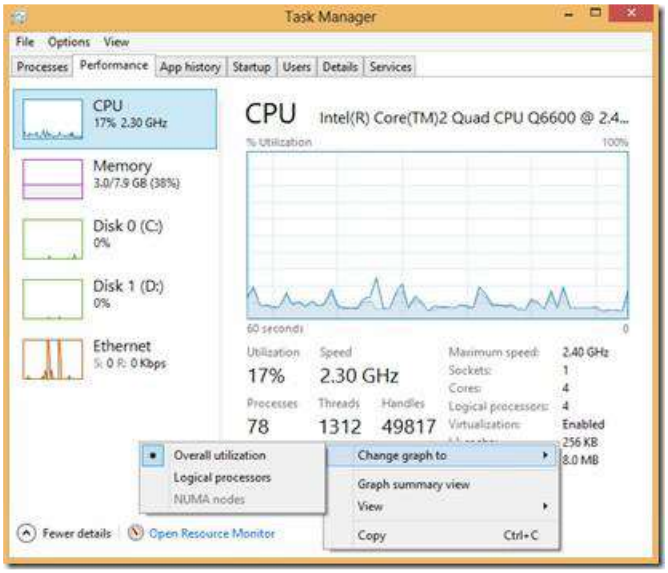
The most basic form of monitoring comes from the Task Manager. The Task Manager has seen many improvements over the years. In Windows Server 2012 and Windows 8, we now have a very detailed and robust, built-in means of monitoring many performance aspects in real time. As you can see from the screen shot below, the new Task Manager has a significantly different look to it. We now list all Applications, Windows Processes, and Background Processes and allow each item to be expanded out for more detail. In the screen shot below, you can see that we have expanded out the Internet Explorer process so that it shows each window or tab that is open. This allows us to see what CPU resources are being utilized be each open windows or tab. This is very useful for troubleshooting an web page or app that may be frozen or causing a performance on a machine.



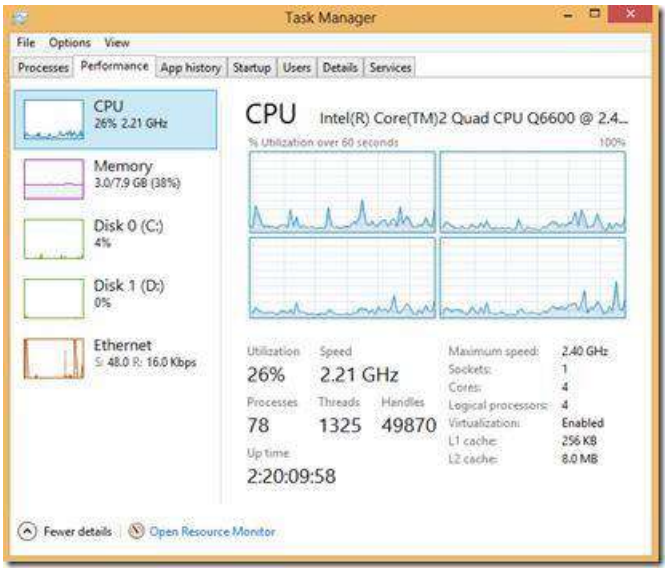
When we select the Performance tab in Task manager, we also have a new view into the big 4 items. For CPU monitoring, the default view consolidates all physical and logical CPU's into a single CPU view. in the sample from my machine, the default view shows the cumulative

performance across all CPU's. Even though it only shows a single CPU in this view, my machine is actually a quad-processor machine. To change the view to chow all logical CPU's, right click in the main window, and select **Change graph to –> Logical Processors**

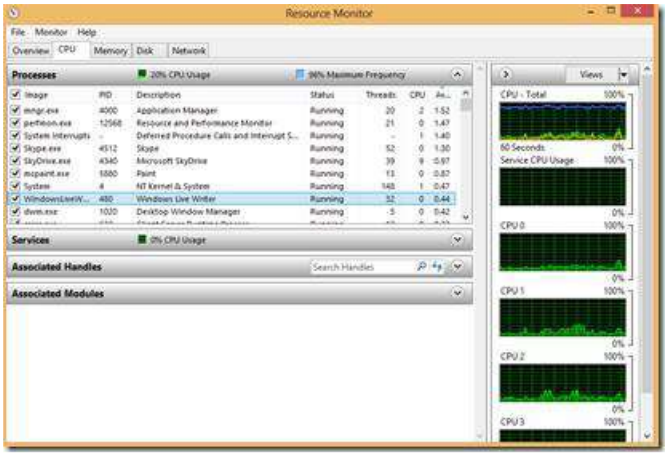
Default View



Showing all Logical Processors



Another feature we have in the Task Manager is access to the **Resource Monitor**. It is the link at the bottom of the previous screen shot. When you open the Resource Monitor we can get a detailed real time view of CPU usage across any process. You can check the box to the left of a process to add/remove it from the graphed processes on the far right hand side.



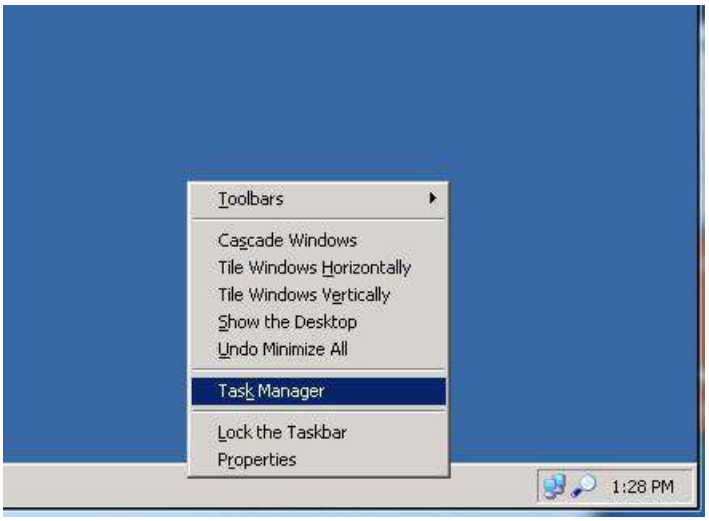
2. Memory Consumption

In the first section we run through using the Task Manager to view RAM utilisation on a Windows Server 2003 VPS. The second section covers Windows Server 2008 and using the Performance Monitor to view VPS RAM utilization.

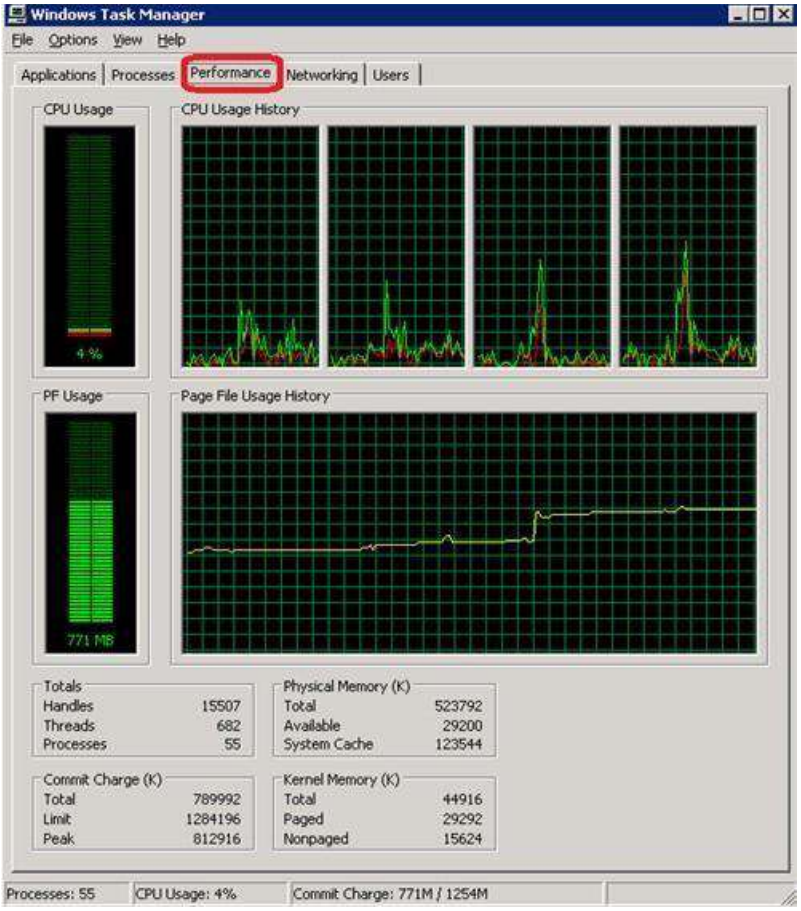
Windows 2003

Start by logging into your VPS with Remote Desktop.

Click on the Task Bar located at the bottom of the VPS screen with the right mouse button. Select Task Manager from the pop-up dialogue.



Once the Task Manager window has opened, click the Performance tab.



In the bottom section of the window, you will see Physical Memory (K), which displays your current RAM usage in kilobytes (KB). One MB is 1024KB. Dividing the values shown in this section by 1024(or roughly 1000) will give you the RAM usage in MB. e.g. 523792 KB is approximately 511 MB.

A value of 32768KB (32MB) Available or less would indicate the VPS is close to, or at it's physical memory limit.

3. **I/O Network**

Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive.

So why is it important to monitor networks? The network is the life line of the IT infrastructure. When networks fail, the flow of information required by applications and business operations stop.

Networks are dynamic environments. Network Admins are continually asked to add new users, technologies and applications to their networks. These changes can impact their ability to deliver consistent, predictable network performance.

Disk I/O monitoring allows you to monitor Read and Write operations of logical disks on your machine and set thresholds so that you get alerted if any of the below metrics reaches some critical level preset by you:

Reads/sec – the rate of read operations on the disk. Writes/sec – the rate of write operations on the disk.

Queue length – the number of requests outstanding on the disk at the time the performance data is collected.

Busy time – the percentage of elapsed time that the selected disk drive was busy servicing read or writes requests.

4. **Disk Usage:** when we speak on "disk usage" (DU) we are talking about the percentage of your computer storage that is in use at a given moment, meaning that your computer disk is occupied by some or the other task. Note that we are not talking about disk capacity, (what your computer hard drive is capable of storing)
5. **Process:** the window process activation service **(WAS)** manages application pool configuration and the creation of lifetime of worker processes for HTTP and other protocols. The world wide web publishing service and other services depend on WAS. This test monitors the windows process activation service and reports useful statistics revealing how well the services manages the worker processes and how healthy these worker processes are. This test is disable by default. To enable the test, go to the ENABLE / DISABLE Tests page using the menu sequence: Agents->tests-?Enable/Disable, pick the desired component type, set performance as the Test type, choose the test from the Disabled tests list, and click on the button to move the test to the Enabled Tests List. Finally click update button.
6. **Port scanning:** is used to determine what ports a system may be listening on. This will help an attacker to determine what services may be running on the system. Some port scanners scan through ports in numeric order; some use a random order. There are many different methods used for port scanning including SYN scanning, AC scanning and FIN scanning.
7. **Response Time**

If your server response time is slow, then your whole site will be slow, no matter how optimized your other resources are. According to Google and other speed test tools such as GTmetrix, you should aim for a server response time of less than 200ms.

Why Monitor Response Time?

1) If a webpage is slow the experience for the visitor is usually bad. Many users simply leave a site if it doesn't respond within a few seconds.

2) When a site has a high response time it is usually an indication that the server is struggling. Slow response times are really common when servers are overloaded, and the information can be used to identify server problems or to explain that there is a problem when contacting a web host.

3) Slow response times and high levels of downtime are linked. A site that has a high response time is more likely to suffer from downtime than a site that is running quickly.

8. **Window Server built-in monitoring tools include the following:**

- ✓ **Event Viewer:** The Event Viewer is a Microsoft Management Console (MMC) snap-in that enables you to browse and manage event logs. It is included in the Computer Management and Server Manager MMC and is included in Administrative Tools as a stand-alone console.You can also execute the eventvwr.msc command.Event Viewer enables you to perform the following tasks:

- View events from multiple event logs
- Save useful event filters as custom views that can be reused
- Schedule a task to run in response to an event
- Create and manage event subscriptions.

- ✓ **Device Manager**: The Device Manager will list all of the **hardware** devices installed on a PC. Any device with a problem will have a **warning symbol** next to it, and double clicking on that device would give details and suggested remedies for the problem.
- ✓ **Task Manager** is one of the handiest programs you can use to take a quick glance at performance to see which programs are using the most system resources on your computer. You can see the status of running programs and programs that have stopped responding, and you can stop a program running in memory using Task Manager.
- ✓ **Resource Monitor:** Windows Resource Monitor is a powerful tool for understanding how your system resources are used by processes and services.In addition to monitoring resource usage in real time, Resource Monitor can help you analyze unresponsive processes, identify which applications are using files, and control processes and services. To start Resource Monitor, execute the resmon.exe command.
- ✓ **Performance Monitor**: Configuration Windows Performance Monitor is a Microsoft Management Console (MMC) snap-in that provides tools for analyzing system

performance. From a single console, you can monitor application and hardware performance in real time, specify which data you want to collect in logs, define thresholds for alerts and automatic actions, generate reports, and view past performance data in a variety of ways.

- ✓ **System Memory:** If your computer lacks the RAM needed to run a program or perform an operation, Windows uses virtual memory to compensate.Virtual memory combines your computer's RAM with temporary space on your hard disk. When RAM runs low, virtual memory moves data from RAM to a space called a paging file. Unfortunately, when something needs to be accessed from the virtual memory on disk, it is much slower than accessing it directly from RAM.
- ✓ **Windows Repair:** You need to have processes in place to plan, design, implement, monitor, and retire servers, services, and applications.
- ✓ Reliability Monitor: is the feature, found in window server 2012 and windows 8.1 that can help troubleshoot issues by providing a history of the OS. **Windows reliability monitoring** is also a windows application that assists you in the identification of software issues in the windows operating system that may affect the system performance and reliability.
- ✓ Data collector sets: a data collector set organizes data collection points, such as performance counters and event trace data. Data that is collected for performance counters by data collector set is stored in log files, which you can open and view in windows performance monitor.

LO 4.2 Use troubleshooting tools and techniques to diagnose and correct server issues

- Content/Topic 1: Troubleshooting Window Server

A. Resources for Top Areas of Support for Windows Server

What to do if the Performance Monitoring Service does not start?

The System Monitor Performance Service on server Computer started and then stopped. Some services stop automatically if they are not in use by other services or programs.

B. The Event Log and errors

System Monitor - Performance Monitoring Services records errors and operation event information in the event log on the management server under the event log name "System Monitor - Performance Monitoring Services".

Type	category	Description
information	Service	Started Performance Monitoring Service. Stopped Performance Monitoring Service. Paused Performance Monitoring Service.

		Restarted Performance Monitoring Service
Error	Service	Error when Started Performance Monitoring Service. Error when Stopped Performance Monitoring Service. Error when Paused Performance Monitoring Service. Error when Restarted Performance Monitoring Service. Stopped Performance Monitoring Service because an irrecoverable error was detected.
information	Management console	The user (account: domain\account) from the machine ‘machine’ logged out.
error	Data collecting	The specified performance data (title: 'title', category name: ’category’, instance name: ’instance’, counter name: ’counter’) cannot be collected on the monitored machine ‘Machine’. This type of performance data is not available for machine ‘Machine’.
Error	Data collecting	Failed to collect performance data (title: 'title', category name: ’category’, instance name: ’instance’, counter name: ’counter’) on the monitored machine ‘Machine’.
Error	Other	Failed to connect to the database (Server: Server\Instance, DataBase: DataBase).
		Failed to update the database.
		Failed to initialize the data.
		Failed to reference the database.
		Failed to initialize the logging facility. Failed to delete performance data after the storage period.

		Failed to stop the logging facility.
error	Management console	Cannot access the monitored machine 'Machine'. An unknown user account attempted to connect.
Warning	Service	Failed to save the Performance Monitoring Service settings. Will read the previous settings at the next activation. Failed to read the Performance Monitoring Service settings. Will read the initial settings.
error	Performance information	No performance indicator (title: 'Title') specified for the OS of the object machine (machine name: 'Machine').

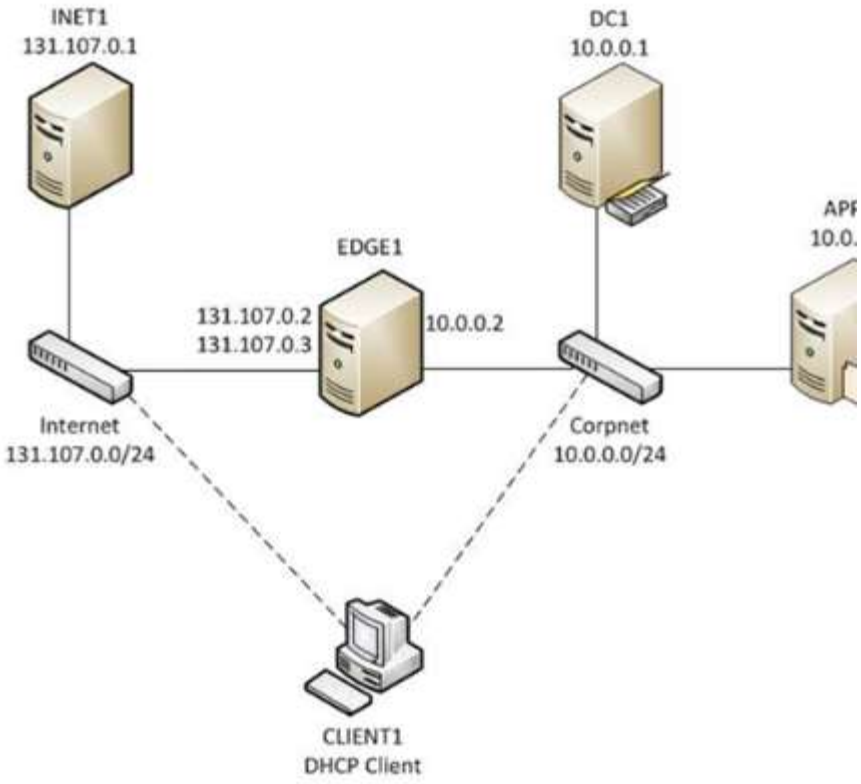
Note: When collecting performance data of the monitored machines which are registered in System Monitor - Performance Monitoring Services by SystemProvisioning Configuration Application is interrupted, the access errors are not output to the event logs. Only when the conditions of the machine meet the all following terms in the SystemProvisioning, data collection will be started. In any other cases, data collection will be interrupted.

- Power Status: "On"
- OS Status: "On"
- Executing Status: "Not Executing"

LO 4.3 Test the required changes or additions for customer satisfaction

- **Content/Topic 1: Testing windows Server Troubleshooting tools**

The test lab guides describe how to configure and demonstrate the new features and functionality in window server 2012 and window 8 in a simplified and standardized test lab environment. The test lab start with the window server 2012 base configuration test lab, which can consist of two subnet representing a simplified intranet and simulate internet. The following figure show the initial setup of the windows server 2012 test lab base on the test lab guide:



Some key differences between the window server2012 base configuration test lab and window server 2008 base configuration test lab are the following:

- The configuration of a simplified public key infrastructure (PKI) has been removed. You can add this to your base configuration with the window server 2012 in-module.
- Window POWESHELL commands equivalents are now available in addition to the UI-based procedure.

✓ Resources for Top Areas of Support for Windows Server

- Upgrade a domain controllers
- Restore and repair your server
- Make disk cleanup of window server

Upgrade a domain controller applied to window server 2012, 2012R2 and window server 2016

Steps to upgrade

The recommend way to upgrade a domain is to promote domain controllers that run newer version of window server and demote older domain controllers as needed.

That method is preferable to upgrade the operating system of an existing domain controller. This list covers general steps to follow before you promote a domain controller that runs a newer version of windows server.

1. Verify the target server meets system requirement
2. Verify application compatibility

3. Verify security settings.
4. Check connectivity of necessary operation master roles
5. Be sure to apply the necessary credential to run the AD DS

Restore or repair server

The following procedure describes how to restore your server system driver from a backup by using the window server essentials installation media (to find out how to use the installation media to restore to factory default settings, see the documentation from the server manufacture.

Notice

If the server uses storage spaces, and you are restoring the data to a new server, you should recover the system drive first, and then log on to the windows server essentials Dashboard, configure storage space in a similar way as on the old server, and then recover the data volumes.

To restore the server system drive from a backup using installation media

1. Insert the window server essential installation DVD in the server DVD drive, restart the server and then press any key to start from DVD.

Note!

If the restore process does not start automatically, check the bios settings for your server to ensure that the DVD driver appears first boot menu. Or if the manufacture preloaded the installation media on the server, press F8 at startup to start from the installation media.

2. After the windows server files load, choose your language and other preferences, and then click Next
3. On the next page of the wizard click repair your computer

Caution

Do not choose the installation now option. That option will guide you through a full system installation that deletes all configuration settings and all data on the system drive.

4. On the choose option page, click troubleshoot.
5. On the system Image recovery page, select the current system? Either window server essentials.
6. On the select a system Image backup page you can choose to use the latest backup or you can select an earlier backup. The system will be restored to the state that it was in at the time of the backup that you choose for storing or repairing your server/ data that was added or changes to settings that were made after the backup was saved must be recreated. Select one of the following options and then click next.

- ❖ Use the latest available system image (recommended)
- ❖ Select system image

7. Follow the instructions in the wizard to complete the system restore.
8. After the server is successfully restored, remove the instruction DVD if you used one and then restart the server.

Using Disk cleanup: the disk cleanup tool clears unnecessary files in windows server environment. This tool is available by default on windows server 2019 and window server 2016, but you might have to take a few manual steps to enable it earlier version of window server.to start the disk cleanup tool, either run the cleanmgr.exe command, or select xtart, select windows administrative tools, and then select Disk cleanup.

You can also run Disk cleanup by using the **cleanmgr window command** and use command-line options to specify that Disk cleanup cleans up certains files.

Enable Disk Cleanup on an earlier version of windows server by installing the Desktop experience

- ❖ Follow these steps to use the add role and features wizard to install desktop experience on a server running windows server 2012R2 or earlier, which also install Disk cleanup.

If server manager is already open go on the next step. If server manager is not already open, open it by doing the following:

1. On the windows desktop start server manager by clicking server manager in the windows taskbar.
2. On the manager menu, select add roles and features.
3. On the before you begin page , verify that your destination server and network environment are prepared for the feature that you want to install. Select next.
4. On the select installation type page, sect role-based or features-based installation to install all parts on a single server. Select next.
5. On the sect destination server page select a server from the server pool or select an offline VHD. Select Next.
6. On the select server roles page, select next.
7. On the sect features page, select user interface and infrastructure, and then select desktop experience.
8. In add features that are required for desktop experience, select add features.
9. Proceed with the installation, and then reboot the system
10. Verify that the disk cleanup option button appears in the properties dialog box.

- ✓ **Best Practices Analyzer:**

Best pratice analyzer (BPA) is a server management tool that is available in windows server 2012R2, windows server 2012, and windows server 2008 R2. Best practice analyzer can help administrators to reduce best practice violations by scanning roles that are installed on managed server that are running windows server 2012 or windows server 2008R2, and reporting best practice violations to the administrator.

You can run best pratice analyzer (BPA) to scan either from server manager, by using the PA GUI or by Using CMDlets in windows Poweshell. Starting with windows server 2012, you can scan one role or multiple roles at one time, on multiple servers,whether you use the best practices analyzer tile in the server manager console or windows PowerShell cmdlets to run scans.

You can also instuct BPA to exclude or ignore scan results that you do not want to see.

How BPA works

BPA works by measuring a role's compliance with best practice rules in eight different categories of effectiveness, trustworthiness and reliability. Results of measurements can be any of the three severity levels described in the following table:

Severity level	Description
error	Error results are returned when a role does not satisfy the conditions of a best practice rules and functionality problems can be

	expected.
information	Information results are returned when a role satisfies the conditions of a best practice rules
warning	Warning results are returned if the results of noncompliance can cause the problems if changes are not made. The application might be compliant as operating currently, but may not satisfy the conditions of a rule if changes are not made to its configuration or policy settings. For example a scan of remote desktop services might show a warning result if a licence server is unavailable to the role because even if no remote connections are active at the time of the scan not having the license server prevent new remote connections from obtaining valid client access licenses.

Rule categories

The following table describes the best practice rules categories against which roles are measured during a best practices analyzer scan.

Category Name	description
Security	Secure rules applied to measure a role's risk for exposure to threats such as unauthorized or malicious users, or loss or theft of condition or proprietary data
Performance	Performance rules are applied to measure role's ability to process request and perform its prescribed in the enterprise within expected periods of gevin the role's

	workload
Configuration	Configuration rules are applied to identify role settings that might require modification for the role to perform optimally. Configuration rules can help to prevent conflicts in settings that can result in error messages or prevent the role from performing its prescribed duties in an enterprise.
Policy	Policy rules are applied to identify possible failures of a role to perform prescribed task in the enterprise.
Pre-deployment	Pre-deployment results are applied before an installed role is deployed in the enterprise.
Post-deployment	Post-deployment rules are applied after all required services has started for a role and after the role is running in the enterprise.
Prerequisites	Prerequisite rules explain configuration settings policy settings and features that are required for a role before BPA can apply specific rules from other categories. A prerequisite scan results indicates that incorrect setting, a missing program, an incorrectly enabled or disabled policy, a registry key settings or other configuration has prevented BPA from applying one or more rules during a scan

Scanning roles by using the best practice GUI

Follow these steps to scan one or more roles in the BPA GUI

1. Do one of the following to open server manager if it is not already open.

- On the windows taskbar click the server manager button.
- On the start screen click the server manager tile.

2. In the navigation pane open a role or group page. Running BPA scans from a role or group page scans all roles that are installed on server in the group.
3. On the tasks menu of the best practice analyzer tile, click start BPA scan.
4. Depending on the number of rules that are evaluated for the role or group you selected the BPA scan can require a few munities to finish.

- **Events and Errors** you

The event viewer: is a tool in windows that display detailed information about significant on your computer. Examples of these are program that does not start as expected or automatically downloaded update.

Event viewer displays these types of events:

- **Error:** a significant problem such as loss of data or loss of functionality. For example if service fails to load during startup, an error will be logged.
- **Warning:** is an event that is not necessarily significant but may indicate possible future problem. For examples when disk space is low a warning will be logged.
- **Information**: is an event that describes the successful operation of an application driver or service. For example when a network driver loads successfully an information event will be logged.
- **Success audit:** is an audited security access attempt that succeeds. For example a user's attempt to log on to the system will be logged as success audit event.
- **Failure audit:** an audited security access attempt that fails. For example if a user tries to access a network drive and fails, the attempt will be logged as a failure audit event.

The event logs service start automatically when you start windows. Application and system logs can be viewed by all users but security logs are accessible only to administrators. Using the event logs in event viewer you can gather information about hardware software and system problems and monitor windows security event.

To access the event view in windows server 2012R2 follow the below steps

1. Right click on the start button and select control panel > system and security and double click administrative tools
2. Double click on event viewer
3. Select the type of logs that you wish to review(ex: application, system)

Note: to access the application logs once in event viewer go to windows logs > application, for shutdown errors refer to application and system logs

LO 4.4 Install, configure and maintain the antivirus for the proper protection of the systems

- Content/Topic 1: Installation, configuration and maintaining Antivirus in a server

1. **System protected**

- The process of security maintenance includes the following steps:
- Monitoring and analyzing logging information
- Performing regular backups
- Recovering from security compromises
- Regularly testing system security using appropriate software maintenance processes to patch and update all critical software and to monitor and revise configuration as needed.
- Scanning virus by using antivirus software

2. Installation of Anti-viruses software on windows server

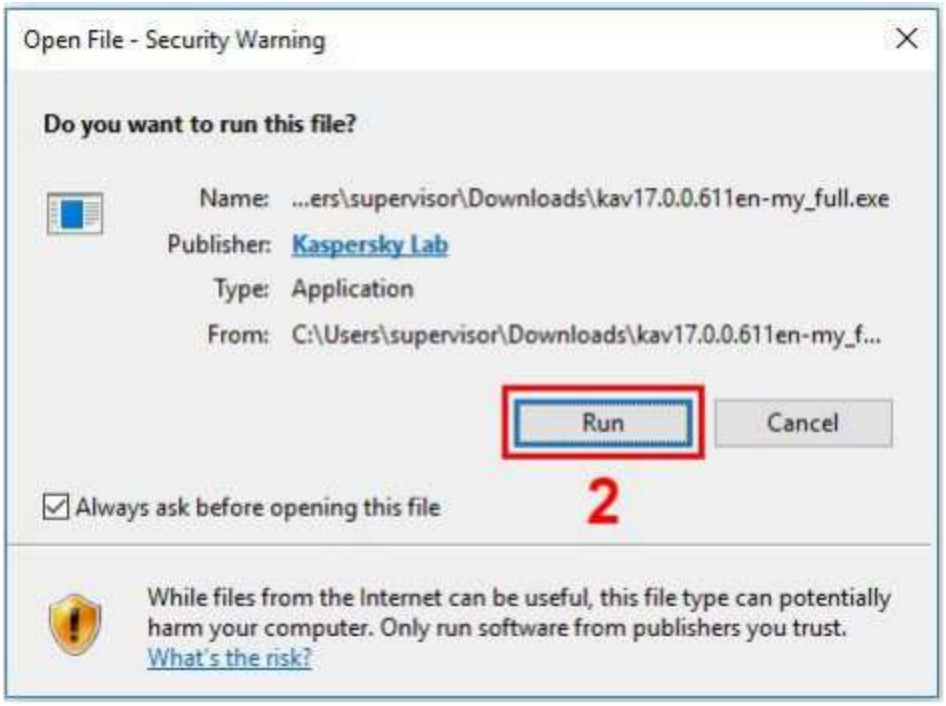
Antivirus - A proactive antivirus engine that automatically detects and eliminates different types of malware including viruses, worms and trojans. Defence a unique collection of prevention- based security technologies that help preserve the integrity, security and privacy of the server operating system and data.

Antivirus software, or anti-virus software (abbreviated to AV software), also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Antivirus software was originally developed to detect and remove computer viruses, hence the name.

How to install Kaspersky Anti-Virus 2018

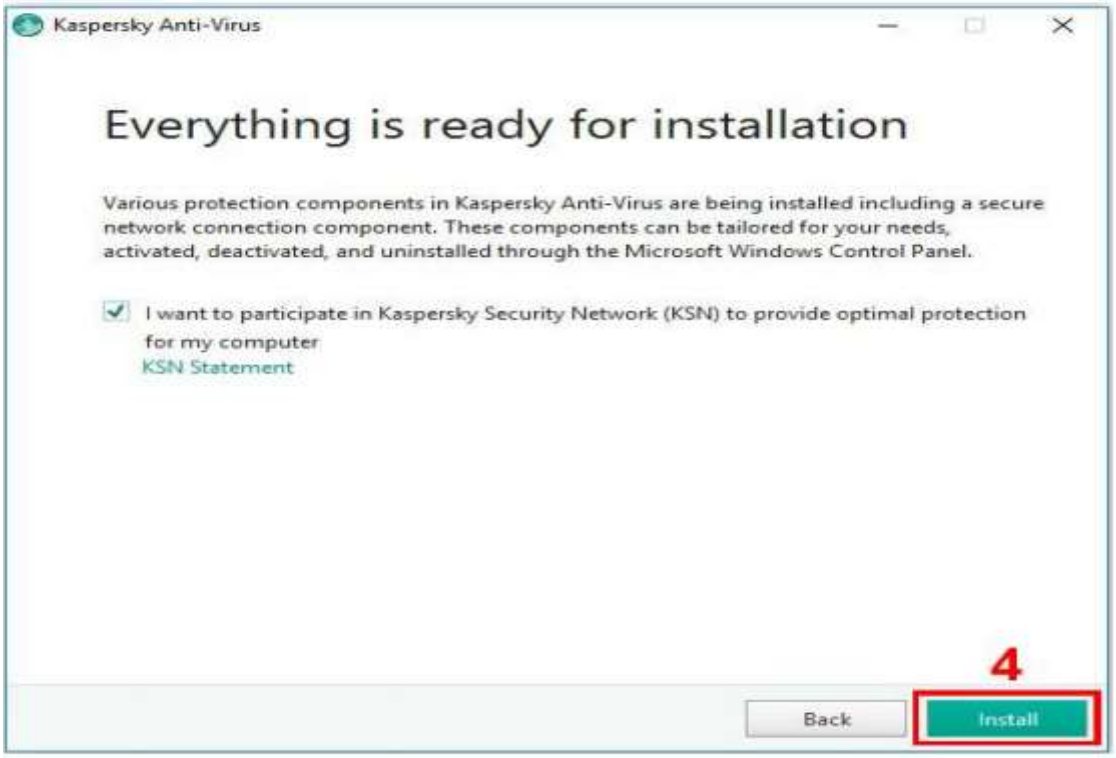
Double-click the downloaded file. You can download Program latest version as link http://www.icom.co.th/kaspersky_thai/Download/kav18.0.0.405en-my_full.exe

1. Click Run



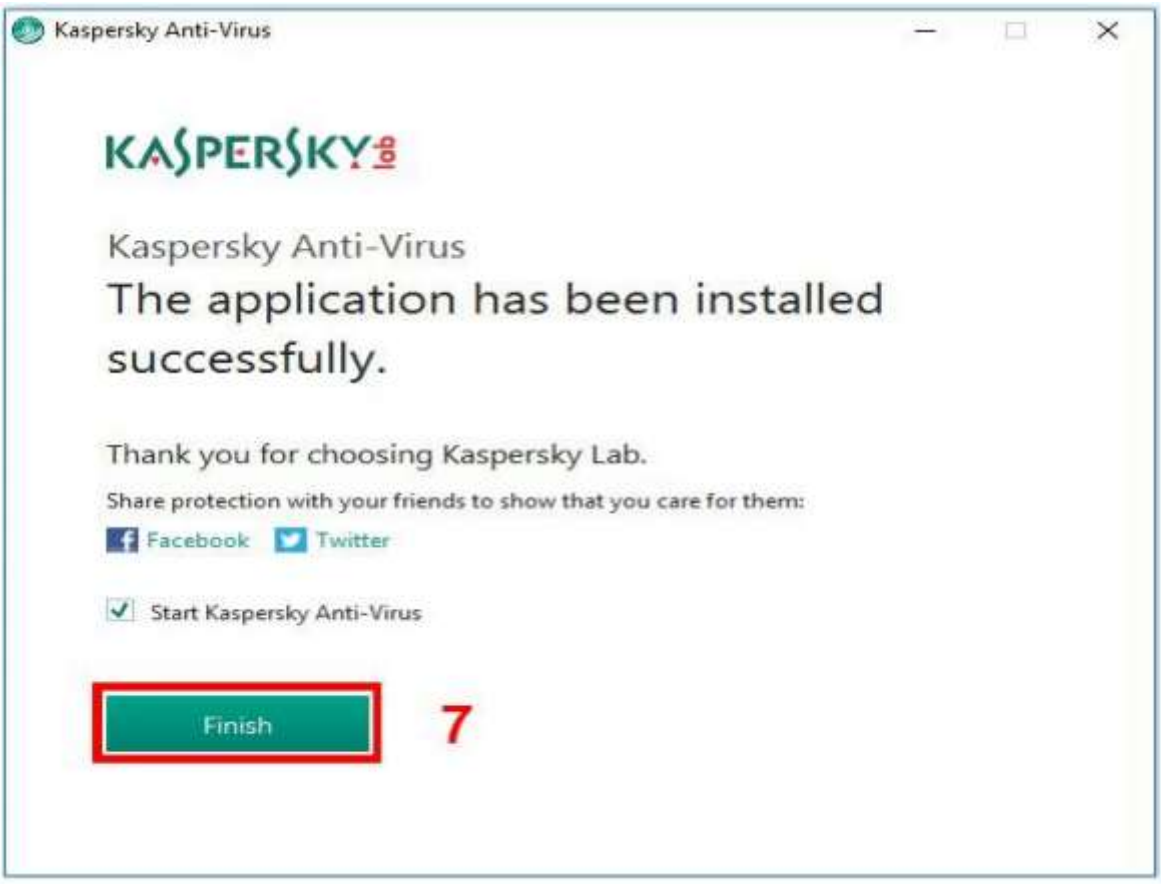
2. Click continue

3. Click Install

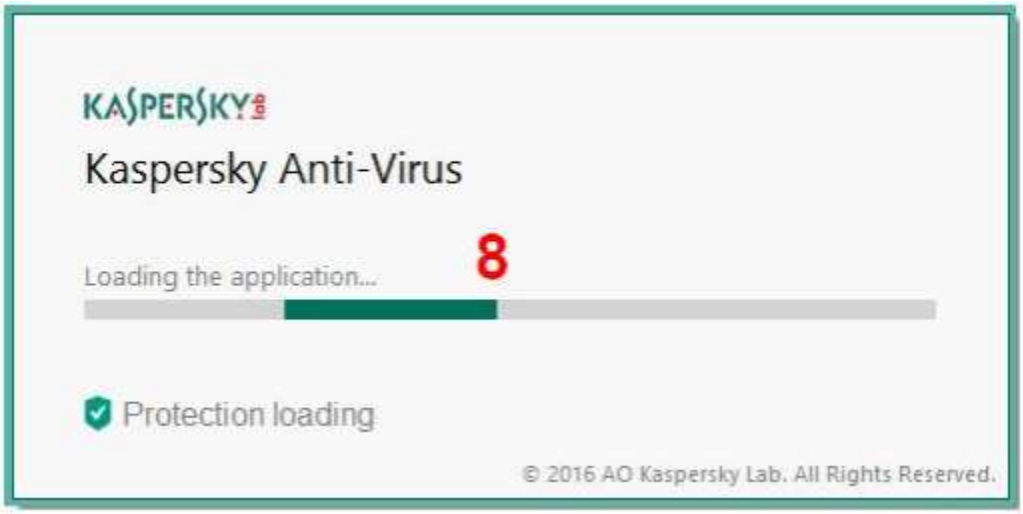


4. If you are installing the application under Windows server 2008, or Windows server 2012, you may see a notification from the User Account Control (UAC) service after you click the Install button. To proceed with the installation, enter your administrative password and click Yes.in the User account control window.
5. Wait for the installation to complete

6. Make sure that the check box Run Kaspersky Anti-Virus is selected and click the Finish button to complete the installation.



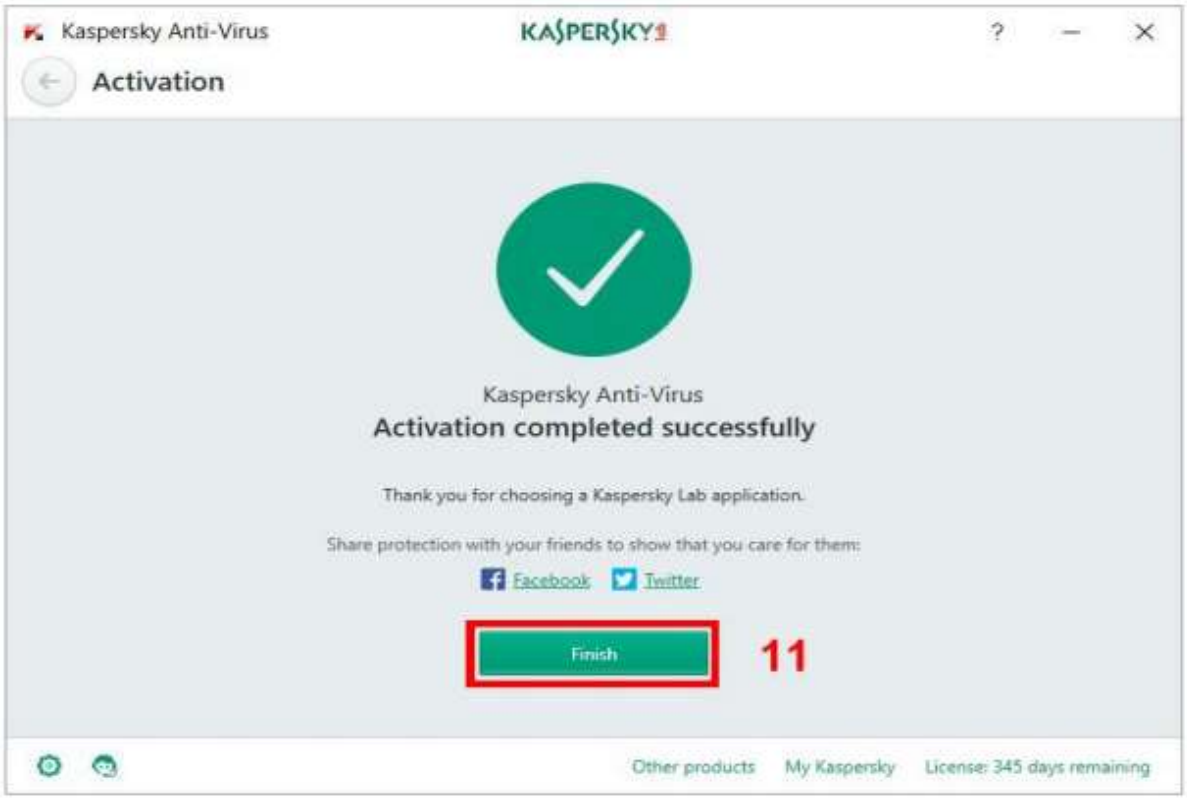
7. Wait for loading the application



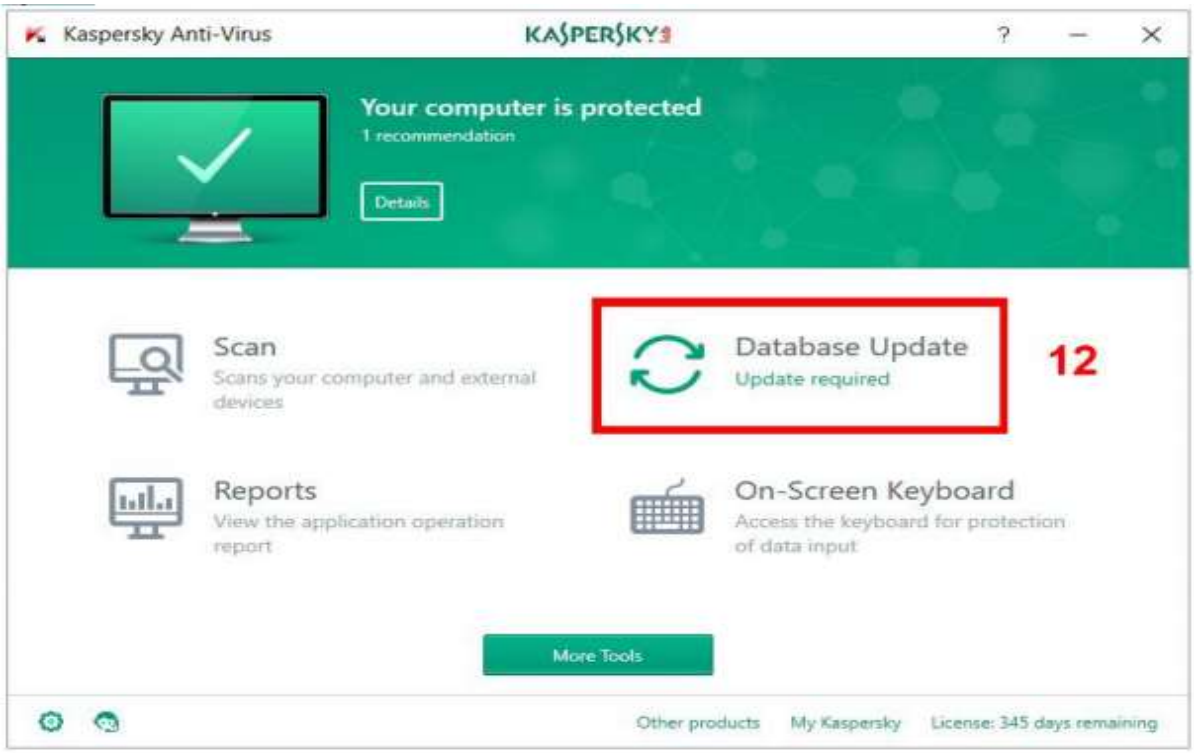
8. You can take a tour through the app features by clicking continue. Or Skip it.

9. Enter the activation code into the field in the Activation window.Click Activate.

10. Wait until the Activation completed successfully window appears and click Finish.



11. Once the installation is complete, the main Kaspersky window will appear then Click Database Update



Updating Antivirus in an Industrial Control System

When properly deployed and up-to-date, antivirus software is an important part of a defense in-depth strategy to guard against malicious software (malware) in industrial control systems (ICS)1. Antivirus is widely used in both ICS and information technology (IT) systems since it is an effective defensive measure against malware. The term “antivirus” covers anti-malware applications, which are not limited to defending only against viruses, but also other forms of malicious software.

This method of transferring antivirus updates uses the following steps:

- Verify the source of the update.
- Download the update file(s) to a dedicated host (server or workstation).
- Scan the downloaded file(s) for malware.
- Verify the cryptographic hash of each downloaded file(s).
- Scan the removable media for malware or other unexpected data before use to verify its integrity. The safest options are to securely erase the removable media and reformat the drive with the appropriate file system (for flash or magnetic media) or to use a new CD or DVD (for optical media) for each update.
- Write the file(s) to the removable media. Dedicate this media exclusively for updates.
- Lock the media so others cannot write to it.
- Load the media into the test environment and verify that it has no adverse impact to the test system.
- Re-scan the media for malware or other unexpected data to verify that nothing transferred to the removable media from the test environment host.
- Install the update on a non-critical endpoint or segment of the system and verify that it has no adverse impact to the production system.
- Install the update on the remaining hosts.
- Monitor the system for any unusual behavior and verify proper operation of the ICS

Reference(s):

- Wiley India PVT.LTD 1st Edition(January 1,2013),Microsoft window server 2012
- Independently published(September 25,2019) Window Server 2019 &Essentials Installation Guide For Small Businesses
- CreateSpace Independent publishing platform(October21,2015)Active Directory Infrastructure
- https://docs.microsoft.com/en-us/windows/win32/srvnodes/windows-server
- https://download.doubletake.com/_download/dt60/docs/Move/User%27s%20GuWWW.petri.com
- https://searchitchannel.techtarget.com/feature/Windows-server-backup-in-Windows-Server-2008-r2
- https://www.petri.com/windows-server-2008-r2-backup