# Dar es Salaam Institute of Technology

# Network Administration Laboratory Manual

# For User Course Training

**Prepared by**: Hamza Mohamed bakari

**September 2019**

# Table of Contents

# Acronyms

| | |
|---|---|
| ADAC | Active Directory Administrative Center |
| ADDS | Active Directory Administrative Service |
| ASCII | American Standard Code for Information Interchange |
| ASP | AppleTalk Session Provider |
| DVD | Digital Versatile Disk |
| DC | Domain Controller |
| DNS | Domain Name System |
| DHCP | Dynamic Host Configuration Protocol |
| EBCDIC | Extended Binary Coded Decimal Interchange Code |
| FDDI | Fiber Distributed Data Interface |
| FSRM | File Server Resource Manager |
| FTP | File Transfer Protocol |
| FGGP | Fine Grained Password Policy |
| GPO | Group Policy Object |
| HP | Hewlett Packard |
| HTML | HyperText Markup Language |
| HTTP | HyperText Transfer Protocol |
| I/O | Input Output |
| IEEE | Institute of Electrical and Electronic Engineers |
| ICMP | Internet Control Message Protocol |
| IIS | Internet Information Services |
| IP | Internet Protocol |
| IPV4 | Internet Protocol Version 4 |
| IPV6 | Internet Protocol Version 6 |
| ISP | Internet Service Provider |
| ISCSI | Internet Small Computer Systems Interface |
| IPX | Internetwork Package Exchange |
| JPEG | Joint Photographic Experts Group |
| LDAP | Lightweight Directory Access Protocol |

| | |
|---|---|
| LAN | Local Area Network |
| MAC | Media Access Control |
| MAN | Metropolitan Area Network |
| MPEG | Moving Picture Experts Group |
| MAU | Multi-station Access Unit |
| NIC | Network Interface Card |
| NTFS | New Technology File System |
| OSI | Open System Interconnection |
| OS | Operating System |
| OUI | Organizationally Unique Identifier |
| OU | Organizational Unit |
| P2P | Peer-to-Peer |
| PAN | Personal Area Network |
| PC | Personal Computer |
| STP | Shielded Twisted Pair |
| SQL | Structured Query Language |
| SACL | System Access Control List |
| TCP | Transmission Control Protocol |
| UNC | Universal Naming Convention |
| UTP | Unshielded Twisted pair |
| VGA | Video Graphics Array |
| WAN | Wide Area Network |
| WINS | Windows Internet Name Service |

# Objective of the Manual

This laboratory manual is prepared to help and guide Network Administration trainees to understand the general concepts of Computer Network and its practical application using Windows Server 2012 R2 operating system. This manual has been classified in to five (5) parts and seventeen (17) chapters. After successfully completing the training session using this manual, trainees are expected to understand and be able to implement the following topics:

- Computer Network
- Network Topologies
- Networking devices
- Making Straight-Through, Crossover and Rollover cables
- Network protocols
- OSI reference model and layers
- IP addressing and Subnetting
- Windows Server 2016 installation and administration
- Adding Roles and Features
- Domain Name System (DNS)
- Active Directory and Active Directory Domain Name Service
- Fine-Grained password policies in Active Directory Domain Name Service
- Shared folder setup
- File server and Disk quota management
- Group Policy Management
- Audit policy
- Dynamic Host Configuration Protocol (DHCP)
- Configuration of File transfer protocol (FTP)
- Install and configure a print server
- Backup and Restore
- Removing roles and features from Windows Server 2016

## Required Hardware, Software and Network tools

Hardware, Software and Network tools required for the practical session are listed in the following tables:

| *No.* | *Required Hardware* | *Description* |
|---|---|---|
| 1. | Computer | Used to as a main working area by running the virtual machine workstation |
| 2. | Switch/Hub | Used to interconnect the different network devices that we have |
| 3. | Printer (if available) | Used to work on the installed print server. |

| *No.* | *Required Software* | *Version* | *Description* |
|---|---|---|---|
| 1. | Virtual Machine Workstation (or Virtualbox | latest | Used to run Windows server 2012 and Windows seven operating systems simultaneously. |
| 2. | Windows Server 2012-R12 or above | Data center | Used to working on it as a Network Administrator |
| 3. | Windows Operating System | Any versions of Windows 7pro or above | Serves us as a client machine |

| *No.* | *Required Network tool* | *Description* |
|---|---|---|
| 1. | Cable (UTP Cat 5 and above) | Used to make a Straight-through, Crossover and Rollover cable arrangements. |
| 2. | Crimper | Used to affix a connector to the end of a cable. |
| 3. | RJ 45 | Used to connect to the network through cables |
| 4. | Tester | Used to test the strength and connectivity of our crimped cables. |

# Part I: Introduction to Computer Networks

# Chapter One: Computer Network

## 1.1 Introduction

A computer network is a system in which multiple computers are connected to each other to share information and resources.

A Computer Network

## 1.2 Characteristics of a Computer Network

- Share Resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over network.

## 1.3 Categories of Computer Networks

**1. Based on size, ownership, the distance it covers:**

### 1.3.1 Personal Area Network (PAN)

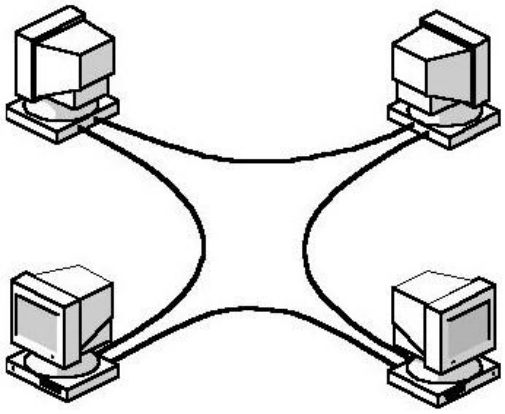
Personal area network is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants. PANs can be used for communication amongst the personal devices themselves (interpersonal communication), or for connecting to a higher level network and the Internet (an uplink) where one "master" device takes up the role as internet router.

- **Wired Personal Area Network**: The data cable is an example of the above PAN. This is also a Personal Area Network because that connection is for the user's personal use. PAN is used for personal use only.

- **Wireless Personal Area Network**: - is a low-powered PAN carried over a short-distance wireless network technology such as: INSTEON, IrDA, Wireless USB, Bluetooth, Z-Wave, ZigBee, and Body Area Network.

## 1.3.2 Local Area Network (LAN)

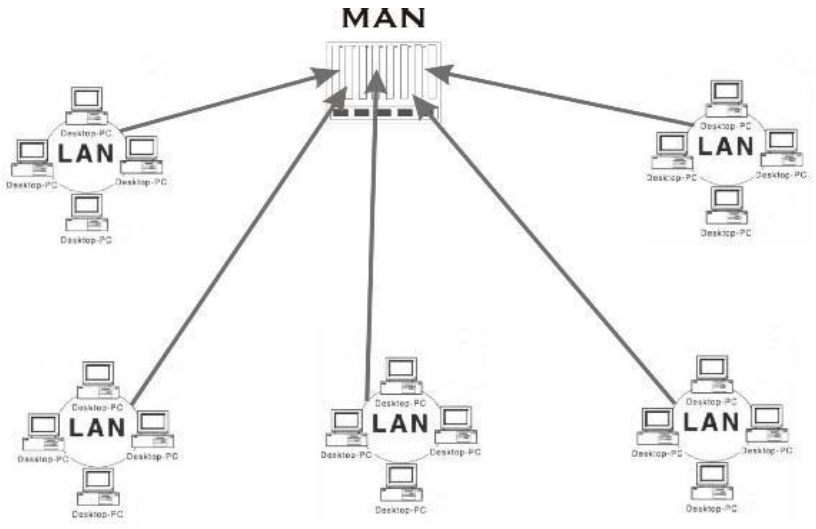
LAN is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment. Computers and other mobile devices use a LAN connection to share resources such as a printer or network storage. Ethernet and Wi-Fi are the two primary ways to enable LAN connections. Ethernet is a specification that enables computers to communicate with each other. Wi-Fi uses radio waves to connect computers to the LAN. Other LAN technologies, including **Token Ring**, **Fiber Distributed Data Interface** and **ARCNET**, have lost favor as Ethernet and Wi-Fi speeds have increased. The rise of virtualization has fueled the development of virtual LANs, which allows network administrators to logically group network nodes and partition their networks without the need for major infrastructure changes.



Local Area Network

## 1.3.3 Metropolitan Area Network (MAN)

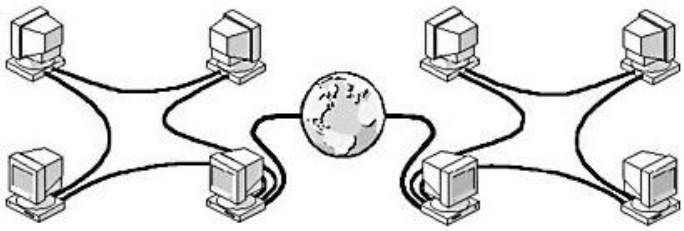
Metropolitan area network is designed to extend over an entire city; it may be a single network or interconnected Local Area Networks.




Metropolitan Area Network

### 1.3.4 Wide Area Network (WAN)

Slightly more complex than a Local Area Network (LAN), a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they are miles apart. The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.



Wide Area Network

| Interprocessor distance | Processors located in same | Example |
|---|---|---|
| 1 m | Square meter | Personal area network |
| 10 m | Room | Local area network |
| 100 m | Building | |
| 1 km | Campus | |
| 10 km | City | Metropolitan area network |
| 100 km | Country | Wide area network |
| 1000 km | Continent | |
| 10,000 km | Planet | The Internet |

Distance coverage areas of Network categories summary

**Based on Functional Relationship:**

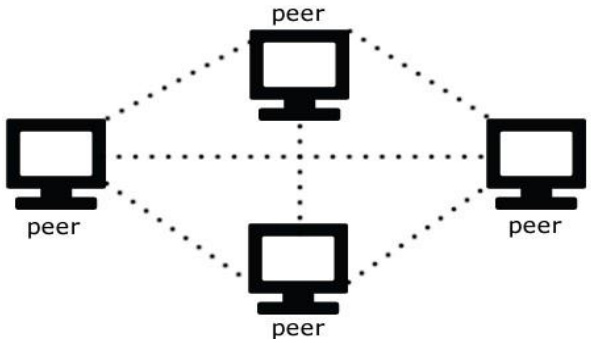
The functional relationship category of a computer network is also referred to as architecture of the network; this includes the type of computers on the network and determines how network resources are handled.

The two common types are:

- Peer-to-peer
- Client-Server

## 1.3.5 Peer to Peer Network (P2P)

It is a type of decentralized and distributed network architecture in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources. In other words, Networks in which all computers have equal status are called peer-to-peer or P2P networks. In a peer-to-peer network, tasks (such as searching for files or streaming audio/video) are shared amongst multiple interconnected peers who each make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for centralized coordination by servers.




Peer-to-Peer Network Model

Advantages:

- Easy to set up
- Less expensive
- Demands moderate level of skill to administer
- User is able to control their own resources

Disadvantages:

- Only works with less than ten  nodes
- Very low level of security
- Performance suffers when a computer is accessed

Peer-to-peer networks are good choices for environments where:

- There are 10 users or fewer
- Users share resources, such as printers, but no specialised servers exist
- Security is not an issue
- The organization and the network will experience only limited growth within the foreseeable future

### 1.3.6 Client-Server Model

The client–server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. A server host runs one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests. Examples of computer applications that use the client–server model are Email, network printing, and the World Wide Web.

**Server**: - is a computer designed to process requests and deliver data to other (client) computers over a local network or the internet with more RAM, larger hard disk and more processing capability.

Some examples of servers in Networking Environment:

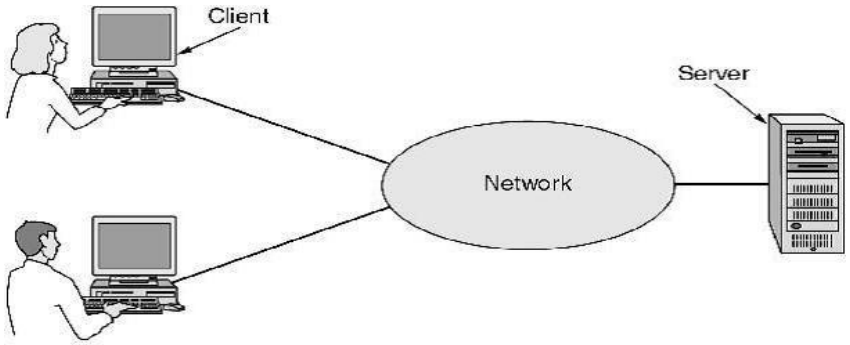
- **File and Print Servers**: manage user access and use of file and printer resources.
- **Application Servers**: make the server side of client/server applications, as well as the data, available to clients. An application server differs from a file and print server. With a file and print server, the data or file is downloaded to the computer making the request. With an application server, the database stays on the server and only the results of a request are downloaded to the computer making the request.
- **Web servers** deliver (serves up) **Web** pages.
- **Mail Servers:** operates like application servers in that there are separate server and client applications, with data selectively downloaded from the server to the client.
- **Fax Servers**: manage fax traffic into and out of the network by sharing one or more fax modem boards.
- **Directory Services Server**: enable users to locate, store, and secure information on the network.

Advantages of client/server architecture

- All files are stored in central location
- Network peripherals are controlled centrally
- Backups and network security is controlled centrally
- Users can access shared data which is centrally controlled
- A server-based network can support thousands of users

Disadvantages of client/server architecture

- A special network operating system is needed
- More complex to install, configure, and manage
- Specialist staff such as Network Administrator is needed
- The server is expensive to purchase
- If any part of the network fails a lot of disruption can occur




Client-Server Relationship

## 1.4 Network Topology

The topology of a network defines how the nodes of a network are connected through communication links. A network can be defined by a physical topology and a logical topology.

**1.4.1 Physical Topology**: defines how the nodes of the network are physically connected; it is the arrangement or physical layout of computers, cables, and other components on the network and can be referred as Physical layout, Design, Diagram or Map of the network. Bus Topology, Star Topology, Ring Topology, Mesh Topology, Tree Topology, Daisy chain Topology and Hybrid Topology are the main types of physical topology.

### 1.4.1.1 Bus Topology

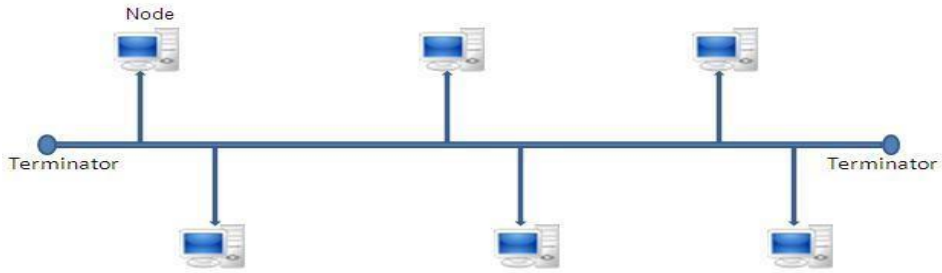
All devices share a single communication line or backbone cable. A network that uses a bus topology is referred to as a "bus network" which was the original form of Ethernet networks. Ethernet 10Base2 (also known as thinnet) is used for bus topology. This network can still work if one of the computers malfunctions. Terminators are required at both ends of the backbone cable.

Advantages:

- Easy to wire and less expensive
- It is easy to extend a network by adding cable with a repeater that boosts the signal and allows it to travel a longer distance

Disadvantages:

- Becomes slow by heavy network traffic with a lot of computer because networks do not coordinate with each other to reserve times to transmit
- It is difficult to troubleshoot a bus because a cable break or loose connector will cause reflections and bring down the whole network




Bus Topology

### 1.4.1.2 Star Topology

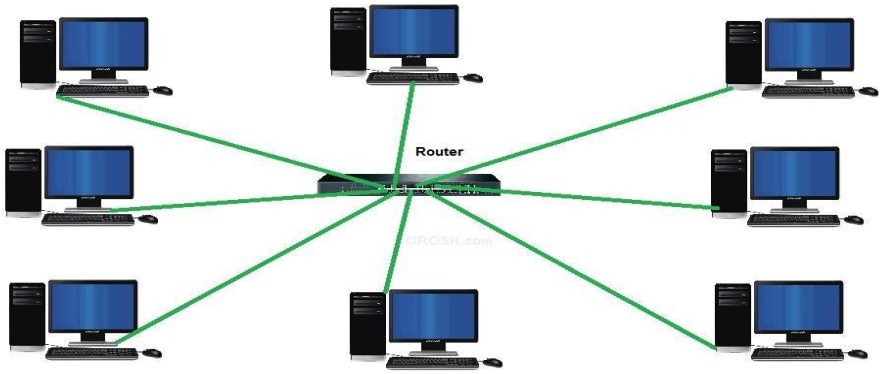
Links the computers by individual cables to a central unit called hub, multiport repeater or concentrator. The central point may be “passive”, “active”, or “intelligent”. A passive hub simply connects the arms of a star, no signal regeneration is performed. An active hub is like a passive hub, except that it regenerates signals. Intelligent hubs are not only regenerate signals but also perform activities such as intelligent path selection and network management. When a computer or other networking component transmits a signal to the network, the signal travels to the hub. Then, the hub forwards the signal simultaneously to all other components connected to the hub. Ethernet 10BaseT is a network based on the star topology. Star topology is the most popular way to connect computers in a workgroup network.

Advantages:

- The failure of a single computer or cable doesn't bring down the entire network.
- fault identification and isolation are easy
- less expensive than mesh topology (but more expensive than others)

Disadvantages:

- Failure of the central unit causes the whole network failure
- Requires more cable length than a linear topology
- More expensive than linear bus topologies because of the cost of the concentrators




Star Topology

### 1.4.1.3 Ring Topology

The nodes are joined by point-to-point connection to form a closed loop or ring. The signal is passed along the ring in one direction, from device to device, until it reaches its destination; each device incorporates a repeater to regenerate received signal before passing it. Some form of access control is needed to determine which node and when will transmit the signal. The ring topology is commonly used in token ring networks that the ring of a token ring network is concentrated inside a device called a Multi-station Access Unit (MAU) and fiber Distributed Data Interface (FDDI) networks that the ring in this case is both a physical and logical ring and usually runs around a campus or collection of buildings to form a high-speed backbone network.

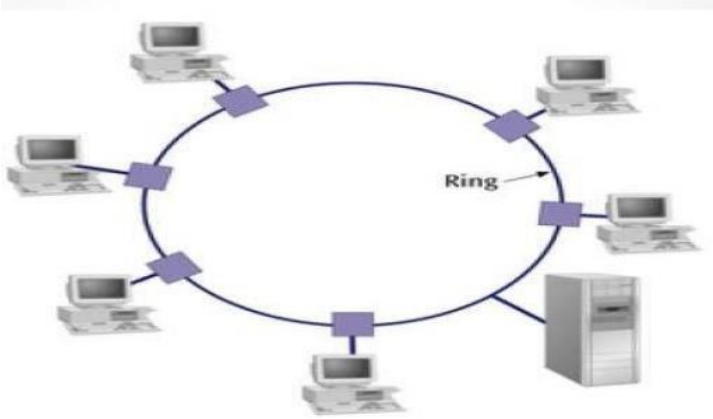
Advantages:

- Equal access for all users
- Each workstation has full access speed to the ring
- As workstation numbers increase performance diminishes slightly
- One computer cannot monopolize the network

- Easy to insert and remove a node

Disadvantages:

- Costly wiring
- The number of edges involved in each communication will be very high resulting in high signal attenuation and network blocking probability
- Failure of one computer can affect the whole network.
- It is difficult to troubleshoot
- Adding and removing computers disrupts the network




Ring Topology

### 1.4.1.4 Mesh Topology

Every node in the network has a connection to each of the other nodes in that network. Every connected device must have n-1 I/O ports. A mesh topology can be **a full mesh topology** or a **partially** connected mesh topology.

**Full Mesh Topology**

Every computer in the network has a connection to each of the other computers in that network. The number of connections in this network can be calculated using the following formula (***n*** is the number of computers in the network): **n(n-1)/2.**

**Partially connected Mesh Topology**

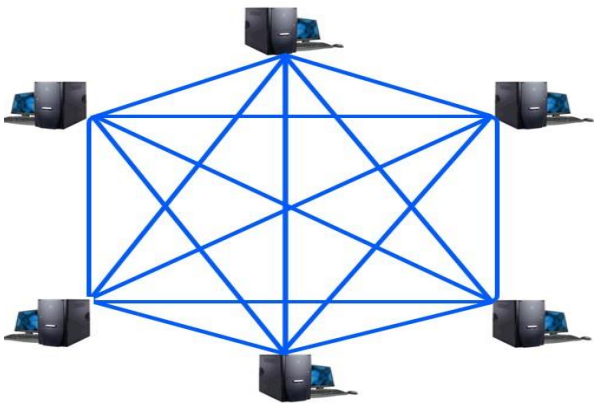
At least two of the nodes in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that one of the primary nodes or connections in the network fails, the rest of the network continues to operate normally.

Advantages：

- Can handle high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.
- fault identification and isolation are easy
- privacy or security guaranteed
- provides fault tolerance-if a wire or other components fails, data can travel along an alternate path

Disadvantages:

- The cost to implement is higher than other network topologies, making it a less desirable option (The amount of cabling and I/O ports needed is very expensive)
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

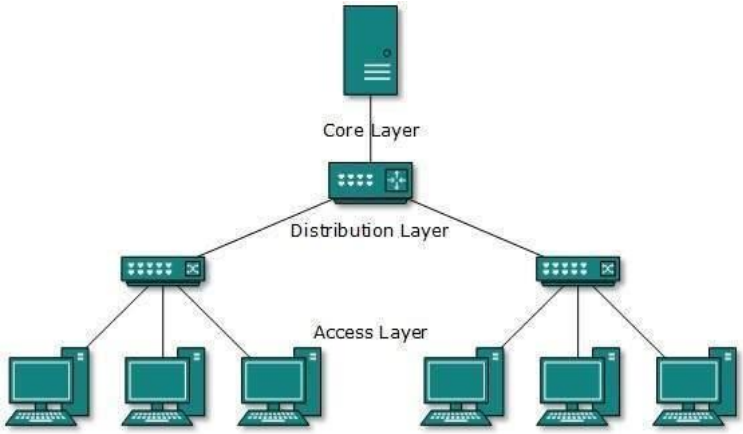


Mesh Topology

### 1.4.1.5 Tree Topology

Tree topology is the most common form of network topology in use presently; imitates as extended Star topology and inherits properties of Bus topology.

Tree topology divides the network in to multiple levels of network. Mainly in LANs, a network is divided into three types of network devices. The lowermost is **access-layer** where computers are attached. The middle layer is known as **distribution layer**, which works as mediator between upper layer and lower layer. The highest layer is known as **core layer**, and is central point of the network, i.e. root of the tree from which all nodes divide.




Tree Topology

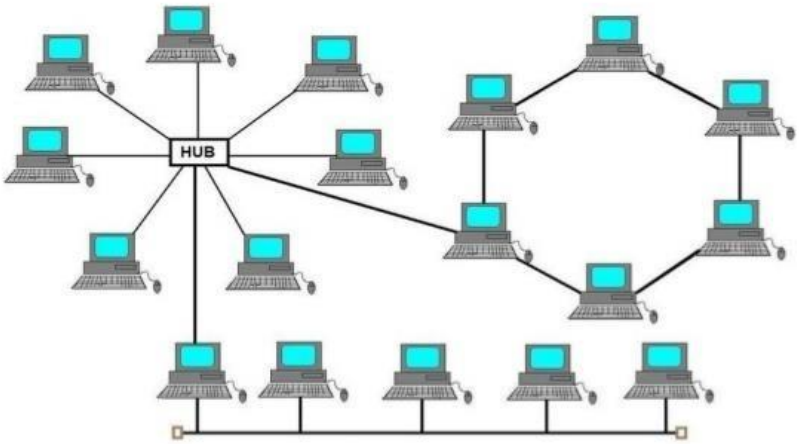
### 1.4.1.6 Daisy Chain Topology

Connects all the hosts in a linear fashion; Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts, Means, if the end hosts in daisy chain are connected then it represents Ring topology. Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

Daisy Chain Topology

### 1.4.1.7 Hybrid Topology

Contains more than one topology, inherits merits and demerits of all the incorporating topologies.




Hybrid Topology

**1.4.2 Logical Topology**: is bound to network protocols and describe how data is moved across the network. In order to have an efficient system, the logical topology should be chosen. It is also an important issue to select the logical topology for the simplicity of the routing.

# Chapter Two: Networking Devices

## 2.1 Introduction

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers etc. These devices also need cables to connect them.so; we are going to discuss these important devices.

## 2.2 Network Cables

Network Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network

The following are the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable

### 2.2.1 Unshielded Twisted Pair Vs Shielded Twisted Pair

Twisted pair cables are widely used in transmitting information, especially across great distances. The twist in the wire cancels out any magnetic interference that may develop in the wiring. There are two common types of twisted pair cabling, STP and UTP. The S stands for Shielded, the U stands for Unshielded, and the TP stands for twisted pair for both. STP simply has additional shielding material that is used to cancel any external interference that may be introduced at any point in the path of the cable. UTP cables have no protection against such interference and its performance is often degraded in its presence. Using STP cables ensure that you get the maximum bandwidth from your cabling even if the external condition is less than ideal.

The biggest drawback to using STP cables is the higher cost. The shielding is an additional material that goes into every meter of the cable, thereby raising its total cost. The shielding also makes the cable heavier and a bit more difficult to bend or manipulate in any way. This is not a big issue but something that users should know when choosing between STP and UTP.

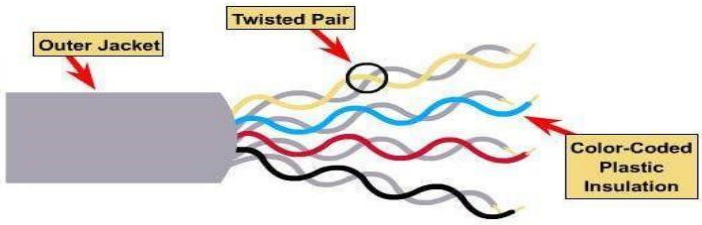
In terms of usage, UTP is the more prevalent and popular cabling that is used in most homes, offices, and even in large scale businesses due to its lower cost. STP is commonly used by large scale companies in high-end applications that require the maximum bandwidth. STP cables are also used in outdoor

environments where the cables are exposed to the elements and manmade structures and equipment that may introduce additional interference. Good examples of this would be the telephone/internet cables that run from your home, to the junction box, down to the establishments of your provider or ISP.

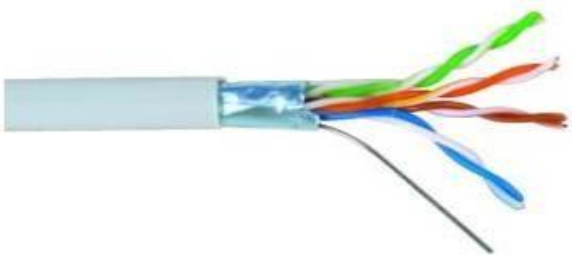
For most common uses, it does not really matter whether you use STP or UTP as both would probably perform well. UTP is the more logical choice as it is cheaper and much easier to find in the majority of computer equipment retailers.

Summary:

1. STP cables are shielded while UTP cables are unshielded
2. STP cables are more immune to interference and noise than UTP cables
3. STP cables are better at maximizing bandwidth compared to UTP cables
4. STP cables cost more per meter compared to UTP cables
5. STP cables are heavier per meter compared to UTP cables
6. UTP cables are more prevalent in SOHO networks while STP is used in more high-end applications




Unshielded Twisted Pair



Shielded Twisted Pair (STP) Cable

**Table 1: UTP cable Categories**

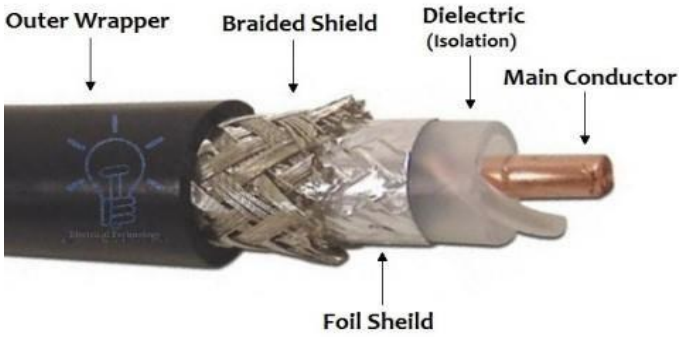
| UTP Category | Data Rate | MAX-Length | Cable Type | Application |
|---|---|---|---|---|
| **CAT 1** | Up to 1Mbps | --- | Twisted pair | Old telephone cable |
| **CAT 2** | Up to 4 Mbps | --- | Twisted pair | Token ring Networks |
| **CAT 3** | Up to 10Mbps | 100m | Twisted pair | Token ring & 10BASE-T Ethernet |
| **CAT 4** | Up to 16Mbps | 100m | Twisted pair | Token ring Networks |
| **CAT 5** | Up to 100Mbps | 100m | Twisted pair | Ethernet, Fast Ethernet and Token ring |
| **CAT 5e** | Up to 1Gbps | 100m | Twisted pair | Ethernet, Fast Ethernet and Gigabit Ethernet |
| **CAT 6** | Up to 10Gbps | 100m | Twisted pair | Gigabit Ethernet, 10G Ethernet (55 meters) |
| **CAT 6a** | Up to 10Gbps | 100m | Twisted pair | Gigabit Ethernet, 10G Ethernet (55 meters) |
| **CAT 7** | Up to 10Gbps | 100m | Twisted pair | Gigabit Ethernet, 10G Ethernet (100 meters) |

✓ The most commonly used Ethernet cable is Category 5 cable with a connector RJ-45.

UTP Category 5 cable with a connector RJ-45

### 2.2.2 Coaxial Cable

A Coaxial cable is a cable used in the transmission of video, communications, and audio. This cable has high bandwidths and greater transmission capacity. Most users relate to a coaxial or coax cable as a cable used to connect their TVs to a cable TV service. However, these cables are also used in networks and what allow a broadband cable Internet connection using a cable modem.

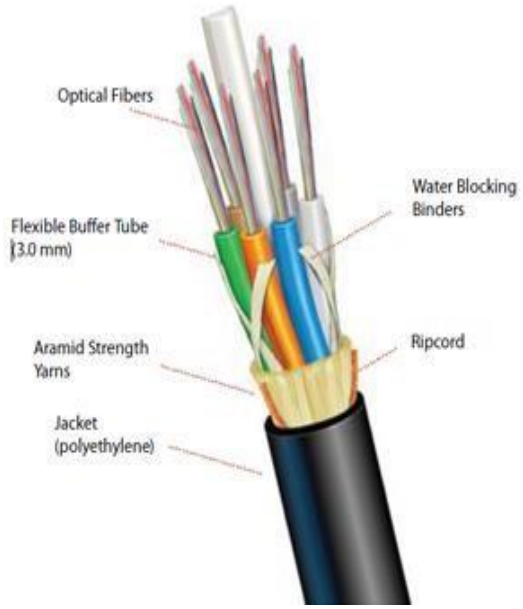



Coaxial cable

### 2.2.3 Fiber optic cable

A **fiber optic cable** defined in **IEEE 802.8** is cable that contains optical fibers (usually glass) coated in plastic that are used to send data by pulses of light. The coating helps protect the fibers from heat, cold, electromagnetic interference from other types of wiring, as well as some protection from ultraviolet rays from the sun. Fiber optics allow for a much faster data transmission than standard copper wires, because they have a much higher bandwidth. They are common amongst corporate networks or world-wide networks, such as Internet backbones, because of the capabilities of the cable. In TV and stereo systems, an **optical cable** can be used to transmit sound from a DVD player or TV to

a sound system, such as a stereo receiver or sound bar. The optical cable can transmits high quality of sound, ensuring little or no sound degradation.




Fiber optic cable

## 2.3 Network interface card (NIC)

A network interface card is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly. The NIC provides the transfer of data in megabytes.

Network Interface Card (NIC)

Every device on a network that needs to transmit and receive data must have a network interface card (NIC) installed. They are sometimes called network adapters, and are usually installed into one of the computer's expansion slots in the same way as a sound or graphics card. The NIC includes a transceiver, (a transmitter and receiver combined). The transceiver allows a network device to transmit and receive data through the transmission medium. Each NIC has a unique 48-bit Media Access Control (MAC) address burned in to its ROM during manufacture. The first 24 bits make up a block code known as the Organizationally Unique Identifier (OUI) that is issued to manufacturers of NICs, and identify the manufacturer. The issue of OUIs to organizations is administered by the Institute of Electrical and Electronics Engineers (IEEE). The last 24 bits constitute a sequential number issued by the manufacturer.

The **Media Access Control (MAC)** address is sometimes called a hardware address or physical address, and uniquely identifies the network adapter. It is used by many data link layer communications protocols, including Ethernet, the 802.11 wireless protocol and Bluetooth. The use of a 48-bit address allows for $2^{48}$(281,474,976,710,656) unique addresses. A MAC address is usually shown in hexadecimal format, with each octet separated by a dash or colon, For example: 00-60-55-93-R2-N7

## 2.4 Repeater

A Repeater is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable runs longer than 100 meters away from the computer. As signals travel along a transmission medium there will be a loss of signal strength i.e. attenuation. A repeater is a non-intelligent network device that receives a signal on one of its ports, regenerates the signal, and then retransmits the signal on all of its remaining ports. Repeaters can extend the length of a network (but not the capacity) by connecting two network segments. Repeaters cannot be used to extend a network beyond the limitations of its underlying architecture, or to connect network segments that use different network access methods. They can, however, connect different media types, and may be able to link bridge segments with different data rates.


Repeater

Repeaters are used to boost signals in coaxial and twisted pair cable and in optical fibre lines. An electrical signal in a cable gets weaker the further it travels, due to energy dissipated in conductor

resistance and dielectric losses. Similarly a light signal traveling through an optical fiber suffers attenuation due to scattering and absorption. In long cable runs, repeaters are used to periodically regenerate and strengthen the signal.

## 2.5 Hub

A Hub contains multiple ports. When a packet arrives at one port, it is copied to all the ports of the hub for transmission. In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times. Additionally, a 10/100Mbps hub must share its bandwidth with each and every one of its ports. So when only one PC is broadcasting, it will have access to the maximum available bandwidth. If, however, multiple PCs are broadcasting, then that bandwidth will need to be divided among all of those systems, which will degrade performance.

Network Hub

## 2.6 Bridge

A network Bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges don't know anything about protocols, but just forward data depending on the destination address in the data packet. This address is not the IP address, but the MAC (Media Access Control) address that is unique to each network adapter card. The bridge is basically just to connect two localarea networks (LANs), or two segments of the same LAN that use the same protocol. Bridges can extend the length of a network, but unlike repeaters they can also extend the capacity of a network, since each port on a bridge has its own MAC address. When bridges are powered on in an Ethernet network, they start to learn the network's topology by analyzing the source addresses of incoming frames from all attached network segments (a process called backward learning). Over a period of time, they build up a routing table.

The bridge monitors all traffic on the segments it connects, and checks the source and destination address of each frame against its routing table. When the bridge first becomes operational, the routing table is blank, but as data is transmitted back and forth, the bridge adds the source MAC address of any incoming frame to the routing table and associates the address with the port on which the frame arrives. In this way, the bridge quickly builds up a complete picture of the network topology. If the bridge does not know the destination segment for an incoming frame, it will forward the frame to all attached segments except the segment on which the frame was transmitted. Bridges reduce the amount of traffic on individual segments by acting as a filter, isolating intra-segment traffic. This can greatly improve response times.

## 2.7 Switch

The switch is a relatively new network device that has replaced both hubs and bridges in Local Area Networks. A switch uses an internal address table to route incoming data frames via the port associated with their destination MAC address. Switches can be used to connect together a number of end-user devices such as workstations, or to interconnect multiple network segments. A switch that interconnects end-user devices is often called a **Workgroup Switch**. Switches provide dedicated fullduplex links for every possible pairing of ports; effectively giving each attached device its own network segment, this significantly reduces the number of intra-segment and inter-segment collisions. A switch normally has numerous ports, with the intention being that most or the entire network is connected directly to the switch, or another switch that is in turn connected to a switch.

24 and 48 port Network Switches

## 2.8 Router

Router is a networking device that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. A network environment that consists of several interconnected networks employing different network protocols and architectures requires a sophisticated device to manage the flow of traffic between these diverse networks. Such a device, sometimes referred to as an intermediate system, but more commonly called a Router, must be able to determine how to get incoming packets (or datagrams) to the destination network by the most efficient route. Routers gather information about the networks to which they are connected, and can share this information with routers on other networks. The information gathered is stored in the router's internal routing table, and includes both the routing information itself and the current status of various network links. Routers exchange this routing information using special routing protocols.

A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its Internet Service Provider's network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keeps the networks connected to the Internet. When data is sent between locations on one network or from one network to a second network the data is always seen and directed to the correct location by the router. The router accomplishes this by using headers and forwarding tables to determine the best path for forwarding the data packets, and they also use protocols such as The **Internet control message protocol** (**ICMP)** to communicate with each other and configure the best route between any two hosts.

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite; it is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached

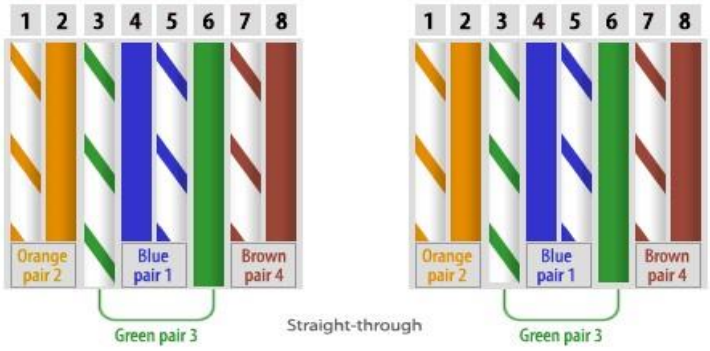
Router

# Chapter Three: Networking Cables Arrangement

# 3.1 Making Straight-Through, Crossover and Rollover Cables

## 3.1.1 Straight-Through cables

A straight through (Straight over) network cable acts as an extension enabling a device with a network interface card to be attached to a network. A common form of network media is the UTP Cat5 (Unshielded Twisted Pair Category 5) cable.




The cables should have trimmed back at each end by approximately 13mm in order to expose the wires for sorting. The wires should then be flattened out and sorted into the following order from left to right; **White/Orange, Orange, White/Green, Blue, White/Blue, Green, White/Brown, Brown.**

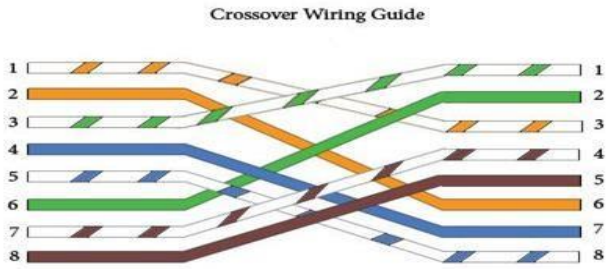
At this point it is best to make sure that the wires are the same length and trim them as necessary. It's a good idea to check the order of the wires before moving onto the next stage to make sure that orange and brown have not been mixed up as some white wires don't have their markings colored clearly. Once the wires are confirmed to be in the correct order then it is time to attach the RJ-45 connectors. This is a simple case of pushing the wires in as far as they will go and then using a crimping tool to secure them into place.

Once one end is done simply repeat the process for the second end, after that be sure to test the cable with an appropriate device before using it in your network. RJ-45 connectors are the most common form of connectors used on UTP Cat5 cables. The RJ simply means Registered Jack and the 45 designation specifies the pin numbering scheme. The cable itself contains four twisted pairs of wires making a total of eight wires.

## 3.1.2 Crossover cables

Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at opposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A

goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B etc. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.




### 3.1.3 Rollover cables

Rollover cables have opposite Pin assignments on each end of the cable or in other words it is "rolled over". Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as **Yost cables** are most commonly used to connect to a devices console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.

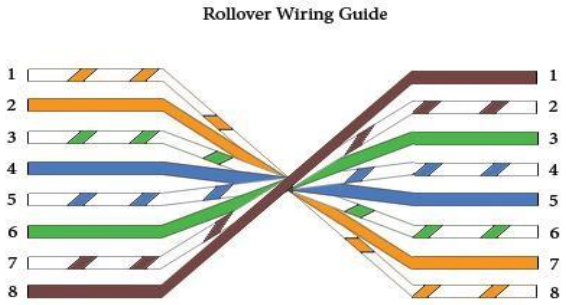



**Table 2: The relationship among Network devices with cable arrangement**

| | **Hub** | **Switch** | **Router** | **Workstation** |
|---|---|---|---|---|
| **Hub** | Crossover | Crossover | Straight | Straight |
| **Switch** | Crossover | Crossover | Straight | Straight |
| **Router** | Straight | Straight | Crossover | Crossover |
| **Workstation** | Straight | Straight | Crossover | Crossover |

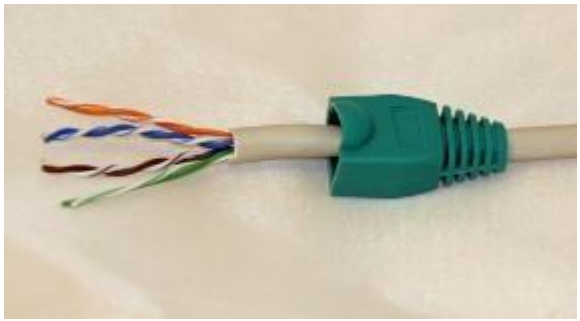
**Table 3: Cable Arrangement and RJ-45 Installation**

| PIN | Color | Pair | Name |
|---|---|---|---|
| 1 | Orange-White | 2 | Transmit Data + |
| 2 | Orange | 2 | Transmit Data - |
| 3 | White-Green | 3 | Receive Data + |
| 4 | Blue | 1 | Not Used-POE |
| 5 | White-Blue | 1 | Not Used-POE |
| 6 | Green | 3 | Receive Data - |
| 7 | White-Brown | 4 | Not Used-POE |
| 8 | Brown | 4 | Not Used-POE |

## 3.2 Installation of Network cables practical steps:

1. Fit Boot - Expose 40mm Wires

2. Straighten Wires Put in Order

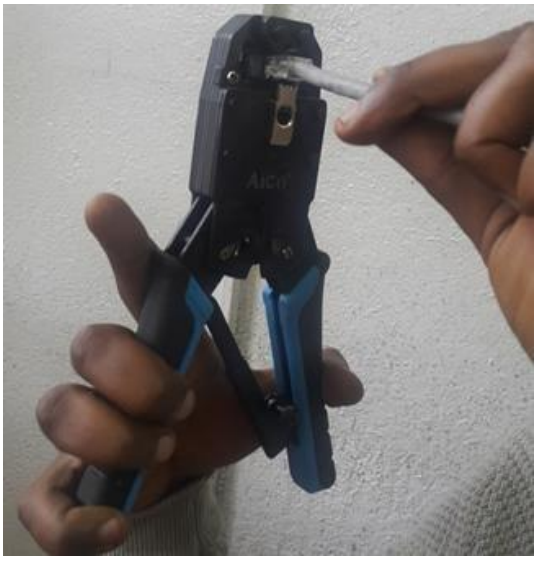


3. Use Crimper to fit Wires

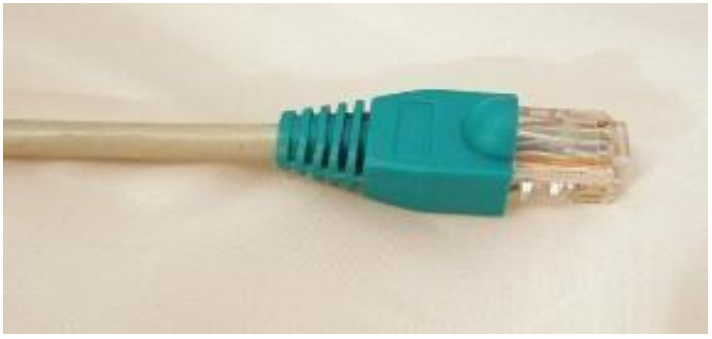
**N.B**. Fit to 13mm

5. Insert into RJ45 Connector

7. Crimp Cable to RJ45 Connector



8. Completed Connection



# Chapter Four: Network Protocols

## 4.1 Introduction

A protocol is the special set of rules that end points in a Network connection use when they communicate. Protocols specify interactions between the communicating entities; in other word it is a set of rules that governs data communications.

A protocol defines what is communicated, how it is communicated, and when it is communicated

The **TCP/IP** Internet protocol is a common example protocol.

- **Transmission Control Protocol** (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level
- **Internet Protocol** (IP), which uses a set of rules to send and receive messages at the Internet address level
- Additional protocols that include the **Hypertext Transfer Protocol** (HTTP) and **File Transfer Protocol** (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet

The key elements of a protocol are:-

- **Syntax**: refers to the structure or format of the data.
- **Semantics**: refers to the meaning of each section of bits.
- **Timing**: refers to when data should be sent and how fast they can be sent.

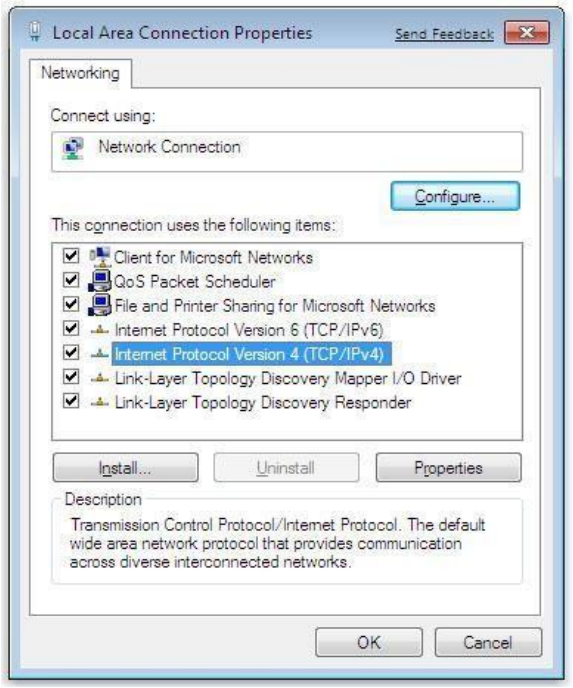
- In a network environment each device must perform the same steps in the same way, so that the data will arrive and reassemble properly; if one device uses a protocol with different steps, the two devices will not be able to communicate with each other

- Whether communication is one way or in both directions simultaneously.
  - Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

## 4.2 Change TCP/IP settings

TCP/IP defines how a computer communicates with other computers, to make it easier to manage TCP/IP settings; the recommend one is using automated Dynamic Host Configuration Protocol (DHCP). DHCP automatically assigns Internet Protocol (IP) addresses to the computers on your network, if your network supports it. If you use DHCP, then you don't have to change your TCP/IP settings if you move your computer to another location, and DHCP doesn't require you to manually configure TCP/IP Settings, such as Domain Name System (DNS) and Windows Internet Name Service (WINS). To enable DHCP or change other TCP/IP settings, follow these steps:

1. Open Network Connections by clicking the **Start button**, and then clicking **Control Panel**. In the search box, type adapter, and then, under Network and Sharing Center, click View network connections.
2. Right-click the connection that you want to change, and then click **Properties**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Click the **Networking** tab. Under This connection uses the following items, click either **Internet Protocol Version 4** (**TCP/IPv4**) or **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.




4. To specify IPv4 IP address settings, do one of the following:

4.1 To get IP settings automatically using DHCP, click Obtain an IP address automatically, and then click OK.

4.2 To specify an IP address, click Use the following IP address, and then, in the IP address, Subnet mask, and Default gateway boxes, type the IP address settings.

4.3 To specify IPv6 IP address settings, do one of the following:

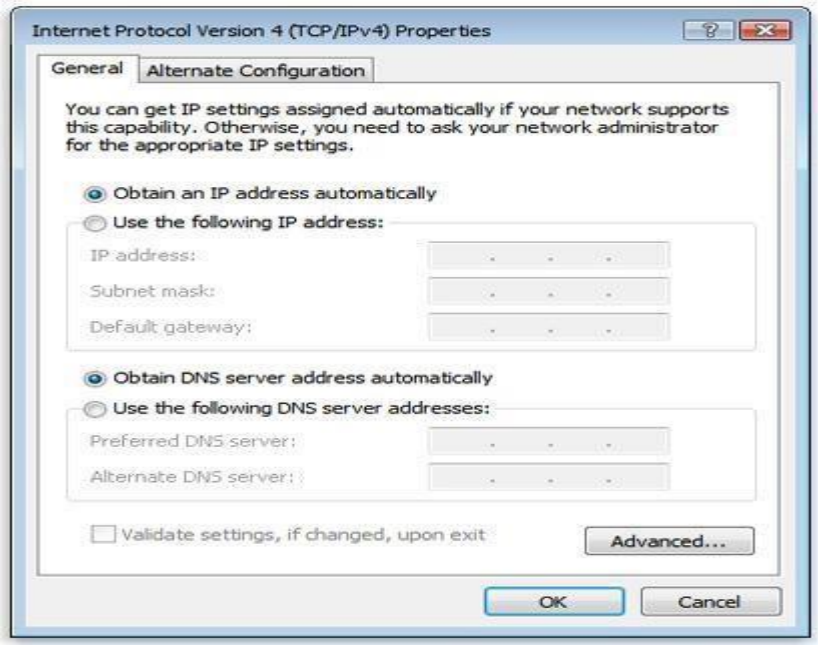
4.5 To get IP settings automatically using DHCP, click Obtain an IPv6 address automatically and then click OK.

4.4 To specify an IP address, click Use the following IPv6 address, and then, in the IPv6 address, Subnet prefix length, and Default gateway boxes, type the IP address settings.

5. To specify DNS server address settings, do one of the following:

5.1 To get a DNS server address automatically using DHCP, click Obtain DNS server address automatically, and then click OK.

5.2 To specify a DNS server address, click Use the following DNS server addresses, and then, in the Preferred DNS server and Alternate DNS server boxes, type the addresses of the primary and secondary DNS servers.




6. To change advanced DNS, WINS, and IP settings, click **Advanced**.

## 4.3 Open Systems Interconnection (OSI) Reference Model

Open System Interconnection (OSI) is the reference model for how applications can communicate over a network. It was developed by the International Organisation for Standardisation (ISO) in 1984 and now days considered the primary Architectural model for inter-computer communications. A reference model is a conceptual framework for understanding relationships.

Purposes of OSI reference model:

- To ensure greater compatibility and interoperability between various types of network technologies.
- To describe how information or data makes its way from application programmes (such as word processor) through a network medium (such as cable) to another application programme located on another network.
- To divide the problem of moving information between computers over a network medium into ***SEVEN*** smaller and more manageable problems.
- To define how each layer communicates and works with the layers immediately above and below it.

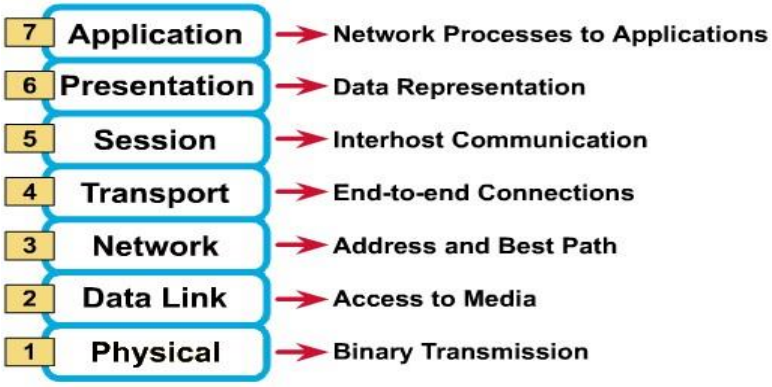
### 4.3.1 OSI Reference Model Layers

The main concept of OSI is that the process of communication between two endpoints in a network can be divided into seven distinct groups of related functions, or layers. Each communicating user or program is at a computer that can provide those seven layers of function. So in a given message between users, there will be a flow of data down through the layers in the source computer, across the network and then up through the layers in the receiving computer. The seven layers of function are provided by a combination of Applications, Operating systems, Network card device drivers and Networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol).

The Seven OSI Reference Model Layers:

- ✓ Each layer provides a service to the layer above it in the protocol specification.
- ✓ Each layer communicates with the same layer's software or hardware on other computers.
- ✓ The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- ✓ The upper three layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.

- ✓ Data is encapsulated with the necessary protocol information as it moves down the layers before network transit.




The seven OSI Reference Model Layers

## Layer 7: Application

- The application layer is the OSI layer that is closest to the user.
- It provides network services to the user's applications.
- Contains all the higher level protocols that are commonly needed by users

## Layer 6: Presentation

- The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system.
- If necessary, the presentation layer translates between multiple data formats by using a common format.
- Provides encryption and compression of data.

Examples: - JPEG, MPEG, ASCII, EBCDIC, HTML.

## Layer 5: Session

- The session layer defines how to start, control and end conversations (called sessions) between applications.
- This includes the control and management of multiple bi-directional messages using dialogue control.
- keeping track of whose turn it is to transmit

- It also synchronizes dialogue between two hosts' presentation layers and manages their data exchange.
- Preventing two parties from attempting the same critical operation at the same time.
- The session layer offers provisions for efficient data transfer.
- check pointing long transmissions to allow them to continue from where they were after a crash

Examples: - SQL, ASP (AppleTalk Session Protocol).

## Layer 4: Transport

- Accepts data from above, splits it up into smaller units if need be, passes them to the network layer, and ensure that the pieces all arrive correctly at the other end
- The transport layer segments data from the sending host's system and reassembles the data into a data stream on the receiving host's system.  End-to-end error free delivery of entire message  Services include:

✓ Service port addressing ○ Port number

✓ Segmentation /reassembly

✓ Connection control ○ Connectionless or connection oriented

✓ Flow and error control

## Layer 3: Network

- Defines end-to-end delivery of packets.
- Defines logical addressing so that any endpoint can be identified.
- Defines how routing works and how routes are learned so that the packets can be delivered.
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

Examples: - IP, IPX, AppleTalk.

## Layer 2: Data Link

- Provides access to the networking media and physical transmission across the media and this enables the data to locate its intended destination on a network.

- Provides reliable transit of data across a physical link by using the Media Access Control (MAC) addresses.
- Uses the MAC address to define hardware or data link address in order for multiple stations to share the same medium and still uniquely identify each other.
- Concerned with network topology, network access, error notification, ordered delivery of frames, and flow control.

  Examples: - Ethernet, Frame Relay, FDDI.

## Layer 1: Physical

- The layer that actually interacts with the transmission media
- The physical part of the network that connects network components together
- Involved in physically carrying information from one node in the network to the next
- The physical layer deals with the physical characteristics of the transmission medium.

Physical layer defines:

- **Mechanical**: the size and shape of the network connector, how many pins does the network connector has and what each pin is used for.
- **Electrical**: how many volts represent a one (1) and how many a zero (0).
- **Timing**: how many nanoseconds a bit lasts.

# Part II: Internet Protocol (IP) Addressing & Sub-netting Concepts

# Chapter Five: Internet protocol (IP) Address

An Internet protocol address is an address used in order to uniquely identifies a device on an IP network; in another word An IP address is the unique numerical address of a device in a computer network that uses Internet Protocol for communication. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Here is how binary octets convert to decimal: The right most bit, or least significant bit, of an octet holds a value of $2^0$. The bit just to the left of that holds a value of $2^1$. This continues until the leftmost bit, or most significant bit, which holds a value of $2^7$. So if all binary bits are a one, the decimal equivalent would be 255 as shown here:

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)

Here is a sample octet conversion when not all of the bits are set to 1.

0 1 0 0 0 0 0 1

0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)

And this sample shows an IP address represented in both binary and decimal.

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

## 5.1 Types, Features and Classes of IP Address

### 5.1.1 Types of IP addresses

The IP addresses can be classified into two. They are listed below.

1) Static IP addresses

2) Dynamic IP addresses

#### 5.1.1.1 Static IP Addresses

As the name indicates, the static IP addresses usually never change but they may be changed as a result of network administration. They serve as a permanent Internet address and provide a simple and reliable

way for the communication. From the static IP address of a system, we can get many details such as the continent, country, region and city in which a computer is located, The Internet Service Provider (ISP) that serves that particular computer and non-technical information such as precise latitude and longitude of the country, and the locale of the computer.

### 5.1.1.2 Dynamic IP Addresses

Dynamic IP addresses are the second category. These are temporary IP addresses. These IP addresses are assigned to a computer when they get connected to the Internet each time. They are actually borrowed from a pool of IP addresses, shared over various computers. Since limited numbers of static IP addresses are available, ISPs usually reserve the portion of their assigned addresses for sharing among their subscribers in this way.

- Static IP addresses are considered as less secure than dynamic IP addresses because they are easier to track.

## 5.1.2 IP Version 4 and IP Version 6

The two versions of IP addresses currently running are IP versions 4 (IPv4) and IP versions 6 (IPv6). There are many features with these two versions.

### 5.1.2.1 IP Version 6

The IPv6 is the most recent version of Internet Protocol. As the Internet is growing rapidly, there is a global shortage for IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF). IPv6 is intended to replace the IPv4. IPv6 uses a 128-bit address and it allows 2128 i.e. approximately 3.4×1038 addresses. The actual number is slightly smaller as some ranges are reserved for special use or not used. The IPv6 addresses are represented by 8 groups of four hexadecimal digits with the groups being supported by colons. An example is given below:

Eg: 2001:0db8:0000:0042:0000:8a2e:0370:7334

**The features of IPv6**

The main features of the IPv6 are :

- ✓ IPv6 provides better end-to-end connectivity than IPv4.
- ✓ Comparatively faster routing.
- ✓ IPv6 offers ease of administration than IPv4.
- ✓ More security for applications and networks.
- ✓ It provides better Multicast and Anycast abilities.
- ✓ Better mobility features than IPv4.

- ✓ IPv6 follows the key design principles of IPv4 and so that the transition from IPv4 to IPv6 is smoother.

These are the key features of the IPv6 when compared to the IPv4. However, IPv6 has not become popular as IPv4.

### 5.1.2.2 IP Version 4

IP Version 4 (IPv4) was defined in 1981. It has not undergone many changes from that time. Unfortunately, there is a need of IP addresses more than IPv4 could supply.

IPv4 uses 32-bit IP address. So the maximum number of IP address is $2^{32}$—or 4,294,967,296.

This is a little more than four billion IP addresses. An IPv4 address is typically formatted as four 8-bit fields. Each 8-bit field represents a byte of the IPv4 address. As we have seen earlier, each field will be separated with dots. This method of representing the byte of an IPv4 address is referred to as the dotted-decimal format. The bytes of the IPv4 are further classified into two parts, the **Network** part and the **Host** part.

**Network Part**

This part specifies the unique number assigned to your network. It also identifies the class of network assigned. The network part takes two bytes of the IPv4 address.

**Host Part**

This is the part of the IPv4 address that you can assign to each host. It uniquely identifies this machine on your network. For all hosts on your network, the network part of the IP address will be the same and host part will be changing.

## 5.1.3 IP Address and Classes

The IP hierarchy contains many classes of the IP addresses. Broadly, the IPv4 addressing system is divided into five classes of IP address. All the five classes are identified by the first octet of the IP address.

The different classes of the IPv4 address are the following:

1. Class A address
2. Class B address
3. Class C address
4. Class D address
5. Class E address

### 5.1.3.1 Class A Address

The first bit of the first octet is always set to zero, so that the first octet ranges from 1 –> 127. The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses. The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks (27-2) and 16777214 hosts (224-2). Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH.

### 5.1.3.2 Class B Address

Here the first two bits in the first two bits are set to zero. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 ($2^{14}$) Network addresses and 65534 ($2^{16}$-2) Host addresses. Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH.

### 5.1.3.3 Class C Address

The first octet of this class has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 ($2^{21}$) Network addresses and 254 ($2^{8}$-2) Host addresses. Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

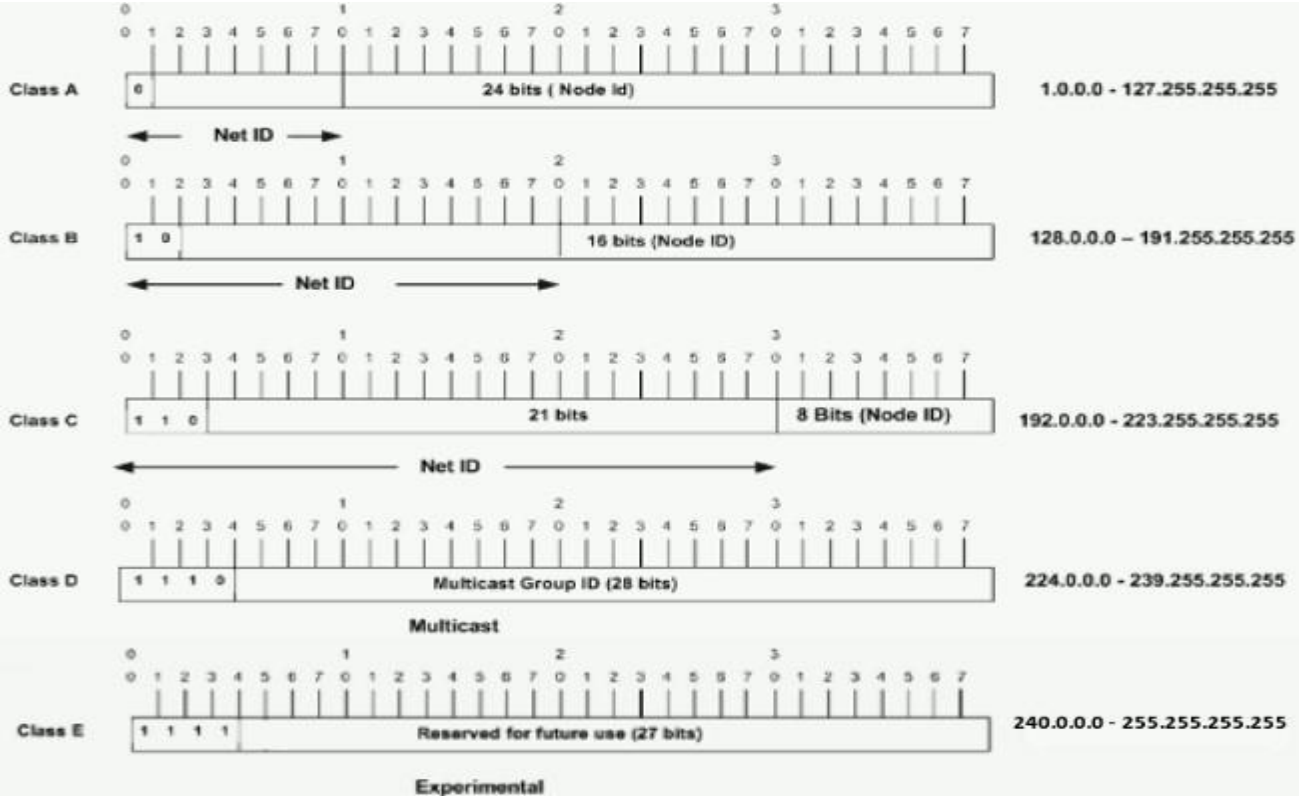
### 5.1.3.4 Class D Address

The first four bits of the first octet in class D IP address are set to 1110. Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not intended for a particular host, but multiple ones. That is why there is no need to extract host address from the class D IP addresses. The Class D does not have any subnet mask.

### 5.1.3.5 Class E Address

The class E IP addresses are reserved for experimental purpose only for R&D or study. IP addresses in the class E ranges from 240.0.0.0 to 255.255.255.254. This class too is not equipped with any subnet mask.

Given an IP address, its class can be determined from the three high-order bits (the three left-most bits in the first octet), the below figure shows the significance in the three high order bits and the range of addresses that fall into each class.




IPv4 addresses

## 5.2 Network Masks

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

1. Class A: 255.0.0.0
2. Class B: 255.255.0.0
3. Class C: 255.255.255.0
4. We can’t have mix of 1s and 0s in subnet mask. Only consecutive 1s is followed by consecutive 0s
5.

**Table 4: Default subnet masks for each Available TCP/IP network classes**

| *Address Class* | *Bits for Subnet Mask* | *Subnet Mask* |
|---|---|---|
| ***Class A*** | *11111111 00000000 00000000 00000000* | *255.0.0.0* |
| ***Class B*** | *11111111 11111111 00000000 00000000* | *255.255.0.0* |
| ***Class C*** | *11111111 11111111 11111111 00000000* | *255.255.255.0* |

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0. In order to see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

Once you have the address and the mask represented in binary, then identification of the network and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

---

**netid | host id**

**netid** = 00001000 = 8 **hostid** =

00010100.00001111.00000001 = 20.15.1

# Chapter Six: IPv4 – Subnetting

## 6.1 Introduction

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Subnetting an IP network is to separate a big network into smaller multiple networks for reorganization and security purposes. All nodes (hosts) in a subnetwork see all packets transmitted by any node in a network. Performance of a network is adversely affected under heavy traffic load due to collisions and retransmissions.

## 6.2 Subnet Mask

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts.

In a Class A address, the first octet is the network portion, so the Class A has a major network address of 1.0.0.0 - 127.255.255.255. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as anyone sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a Class B address, the first two octets are the network portion, so the Class B has a major network address of 128.0.0.0 - 191.255.255.255. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses is used for networks that have between 256 and 65534 hosts.

In a Class C address, the first three octets are the network portion. The Class C has a major network address of 192.0.0.0 - 223.255.255.255. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

**Table 5: Summary of IPV4 classes**

| | | |
|---|---|---|
| **Class A Networks** | 1.0.0.1 to 126.255.255.254 | Supports 16 million hosts on each of 127 |

| | | |
|---|---|---|
| **Class B Networks** | 128.1.0.1 to 191.255.255.254 | Supports 65,000 hosts on each of 16,000 networks |
| **Class C Networks** | 192.0.1.1 to 223.255.254.254 | Supports 254 hosts on each of 2 million |
| **Class D Networks** | 224.0.0.0 to 239.255.255.255 | Reserved for multicast groups. |
| **Class E Networks** | 240.0.0.0 to 254.255.255.254 | Reserved. |

## 6.3 Understanding a Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects *n* networks/subnetworks has *n* distinct IP addresses, one for each network / subnetwork that it interconnects.

In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

204.17.5.0 - 11001100.00010001.00000101.00000000

255.255.255.224 - 11111111.11111111.11111111.11100000

----------|sub|----

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device *since host ids of all zeros or all ones are*

*not allowed* (it is very important to remember this). So, with this in mind, these subnets have been created.

204.17.5.0 255.255.255.224 host address range 1 to 30

204.17.5.32 255.255.255.224 host address range 33 to 62

204.17.5.64 255.255.255.224 host address range 65 to 94

204.17.5.96 255.255.255.224 host address range 97 to 126

204.17.5.128 255.255.255.224 host address range 129 to 158

204.17.5.160 255.255.255.224 host address range 161 to 190

204.17.5.192 255.255.255.224 host address range 193 to 222 204.17.5.224

255.255.255.224 host address range 225 to 254

**Example 1**

Now that you have an understanding of subnetting, put this knowledge to use. In this example, you are given two addresses / mask combinations, written with the prefix/length notation, which have been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can use the address and mask of each device in order to determine to which subnet each address belongs. **DeviceA**: 172.16.17.30/20

**DeviceB**: 172.16.28.15/20

Determine the Subnet for DeviceA:

172.16.17.30 - 10101100.00010000.00010001.00011110

255.255.240.0 - 11111111.11111111.11110000.00000000

----------| sub|----------

**Subnet** = 10101100.00010000.00010000.00000000 = 172.16.16.0

Looking at the address bits that have a corresponding mask bit set to one, and setting all the other address bits to zero (this is equivalent to performing a logical "AND" between the mask and address), shows you to which subnet this address belongs. In this case, DeviceA belongs to subnet 172.16.16.0.

Determine the Subnet for DeviceB:

172.16.28.15 - 10101100.00010000.00011100.00001111

255.255.240.0 - 11111111.11111111.11110000.00000000

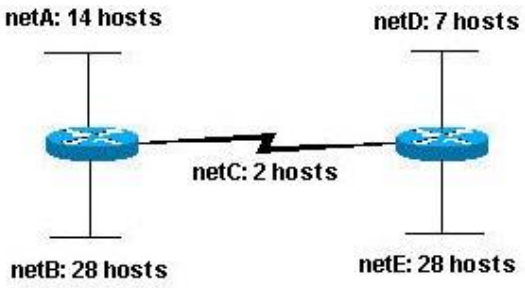
----------| sub|----------

**Subnet** = 10101100.00010000.00010000.00000000 = 172.16.16.0

From these determinations, DeviceA and DeviceB have addresses that are part of the same subnet.

**Example 2**

Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network in the below figure with the host requirements shown.




Looking at the network shown in the above figure, you can see that you are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? If so, then how?

You can start by looking at the subnet requirement. In order to create the five needed subnets you would need to use three bits from the Class C host bits. Two bits would only allow you four subnets ($2^2$).

Since you need three subnet bits that leaves you with five bits for the host portion of the address, how many hosts do this support? $2^5 = 32$ (30 usable). This meets the requirement.

Therefore you have determined that it is possible to create this network with a Class C network. An example of how you might assign the subnetworks is: netA: 204.15.5.0/27 host address range 1 to 30 netB: 204.15.5.32/27 host address range 33 to 62 netC: 204.15.5.64/27 host address range 65 to 94 netD: 204.15.5.96/27 host address range 97 to 126 netE: 204.15.5.128/27 host address range 129 to 158

**Example 3**

Here is a scenario where subnetting is needed. Pretend that a web host with a Class C network needs to divide the network so that parts of the network can be leased to its customers. Let's assume that a host has a network address of 216.3.128.0. Let's say that we're going to divide the network into 2 and

dedicate the first half to itself, and the other half to its customers. 216. 3. 128. (0000 0000) (1st half assigned to the web host)

216. 3. 128. (1000 0000) (2nd half assigned to the customers)

The web host will have the subnet mask of 216.3.128.128 (/25). Now, we'll further divide the 2nd half into eight blocks of 16 IP addresses.

216. 3. 128. (1000 0000) Customer 1 -- Gets 16 IPs (14 usable)

216. 3. 128. (1001 0000) Customer 2 -- Gets 16 IPs (14 usable)

216. 3. 128. (1010 0000) Customer 3 -- Gets 16 IPs (14 usable)

216. 3. 128. (1011 0000) Customer 4 -- Gets 16 IPs (14 usable)

216. 3. 128. (1100 0000) Customer 5 -- Gets 16 IPs (14 usable)

216. 3. 128. (1101 0000) Customer 6 -- Gets 16 IPs (14 usable)

216. 3. 128. (1110 0000) Customer 7 -- Gets 16 IPs (14 usable)

216. 3. 128. (1111 0000) Customer 8 -- Gets 16 IPs (14 usable) ----------
--

255. 255. 255. (1111 0000) (Subnet mask of 255.255.255.240)

# Part III: Administering Windows Server

# Chapter Seven: Introduction to Windows Server

Windows Server is the network operating that is used to manage users and network resources available in the network.

## 7.1 Installation of Windows server

In this easy step by step guide, we will learn how to install and activate Windows Server.

Before you start make sure you have the minimum requirements to install Windows Server on the machine. The basic requirements are:-

**Processor**: minimum 1.4 GHZ

**RAM**: minimum 512 MB

**Disk Space**: 32 GB as a minimum disk space requirement Other

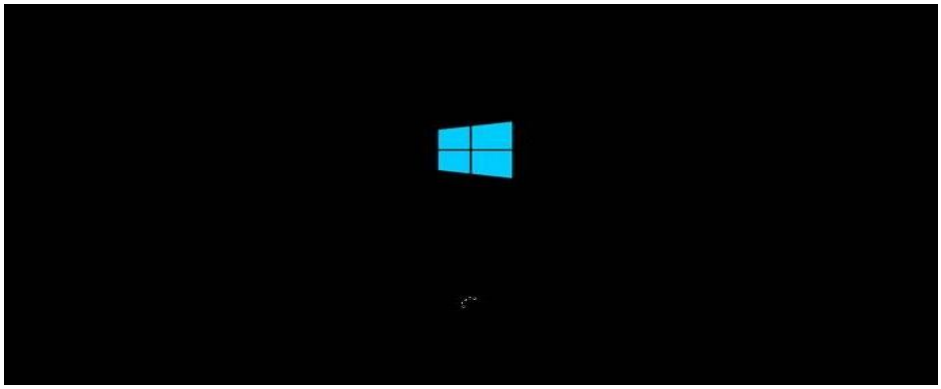
requirements:

- DVD drive
- Super VGA (800 x 600) or higher-resolution monitor.

✓ Now that we have everything we need, we can start:

- Insert the Windows Server DVD or bootable USB and once you get the following message press **Enter** or any key from your keyboard to boot from the setup.

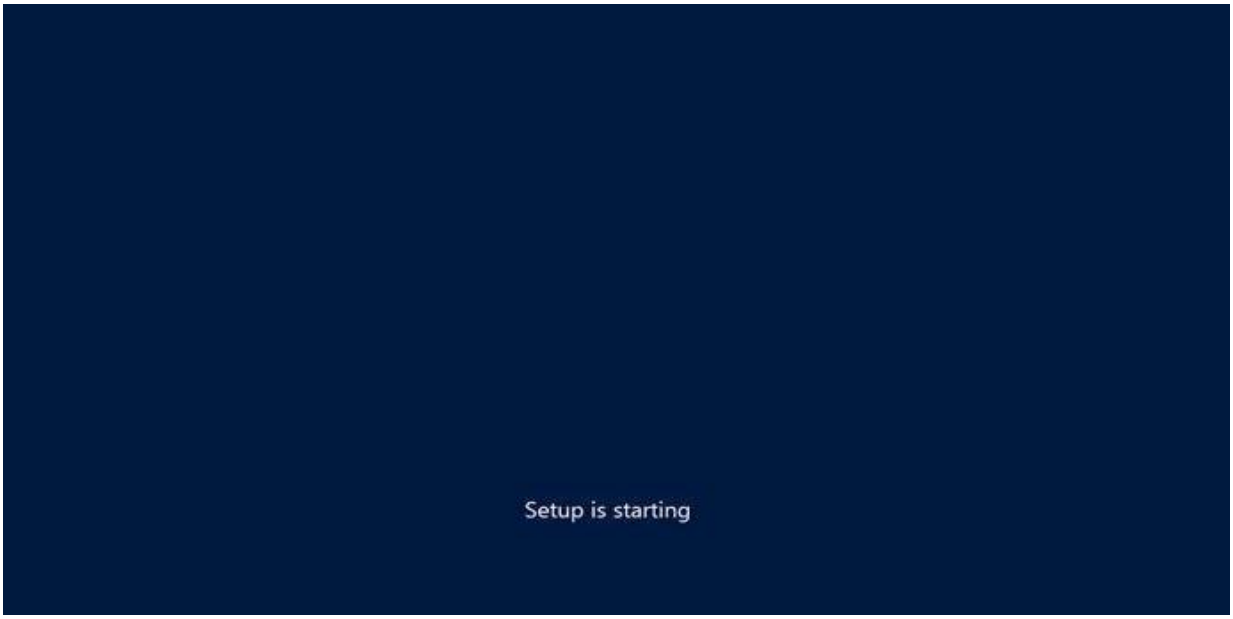

1. Wait for a while till the setup loads all necessary files (Depending on your machine, it will take couple of minutes)



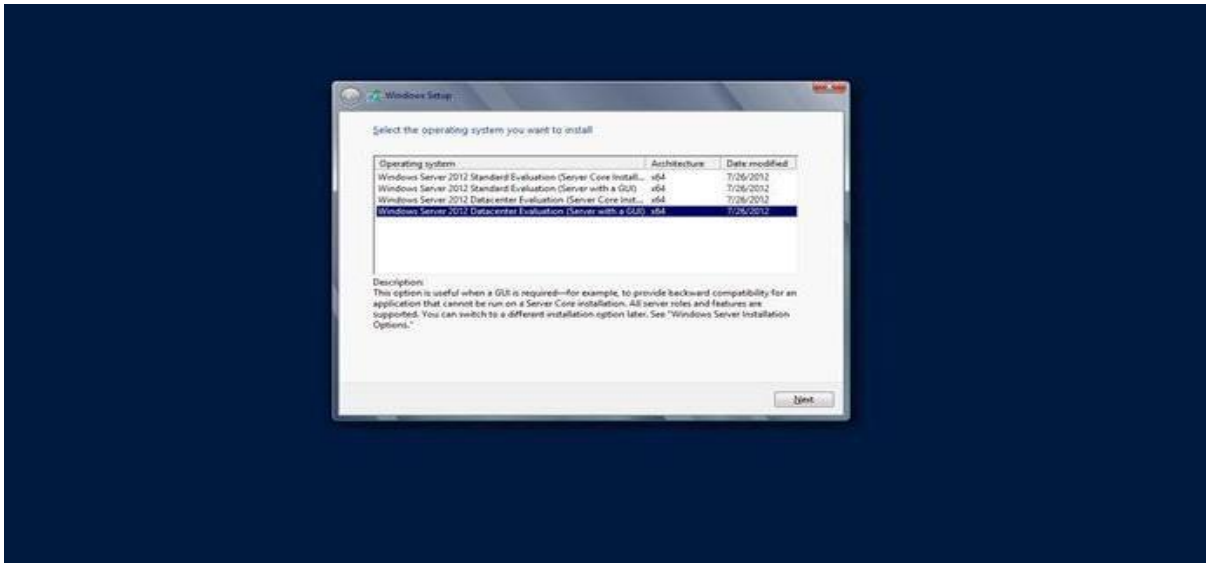
2. Once the setup files are loaded, the setup will start with the following screen. You can change these to meet your needs (the default values should be fine for now)


3. Once you click **Next**, you can start the installation, click "**Install now**"

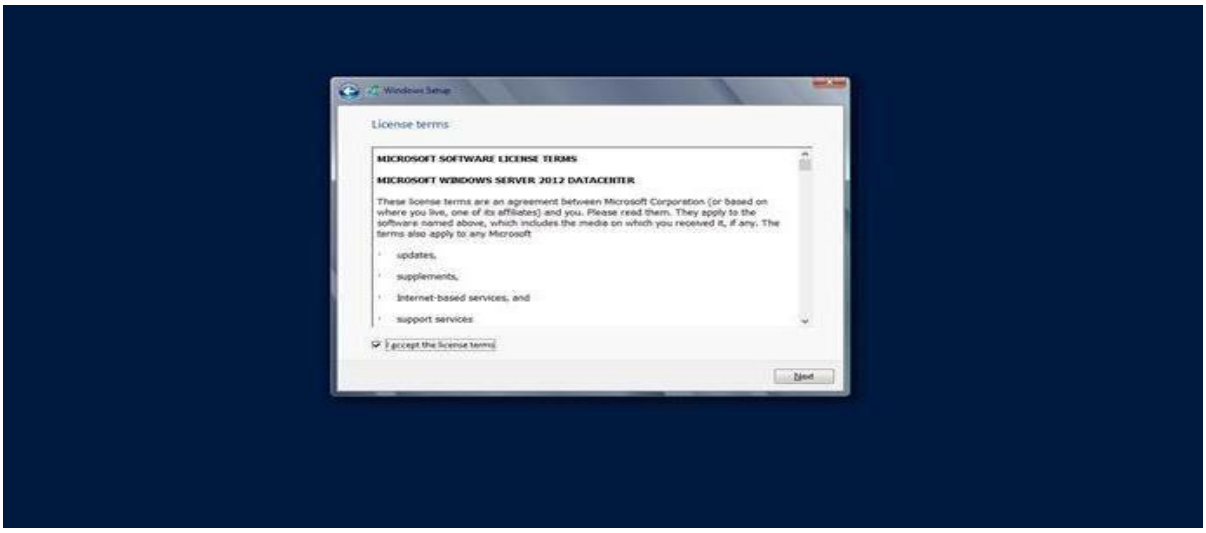
4. You will see the following screen, wait until it finishes loading



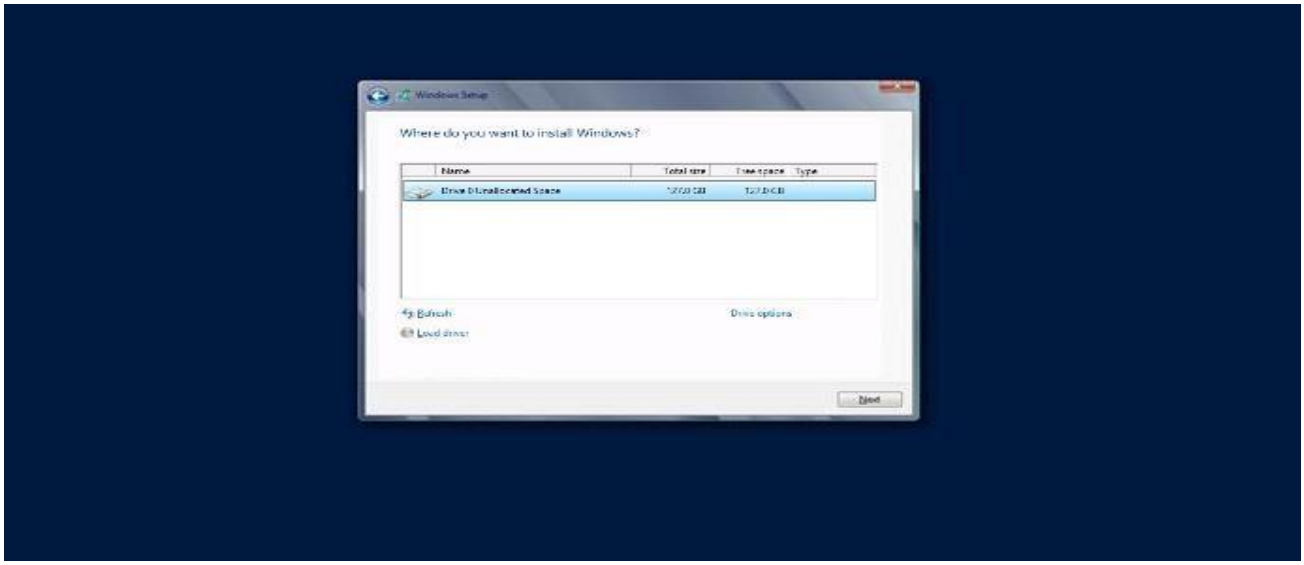

5. In the following setup screen, you will see four options. Select Windows Server 2012 **Datacenter** Evaluation (**Server With GUI**) and click **Next**.



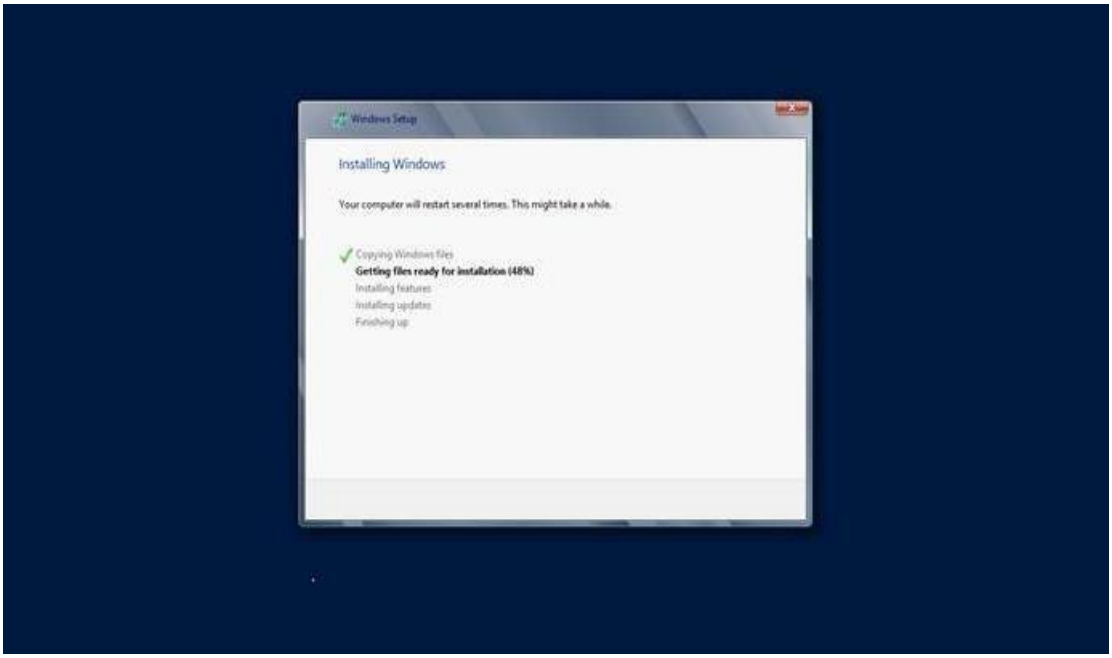

6. After you click Next from previous screen, Read the License terms, tick the **"I accept the license terms"** and click **Next**.



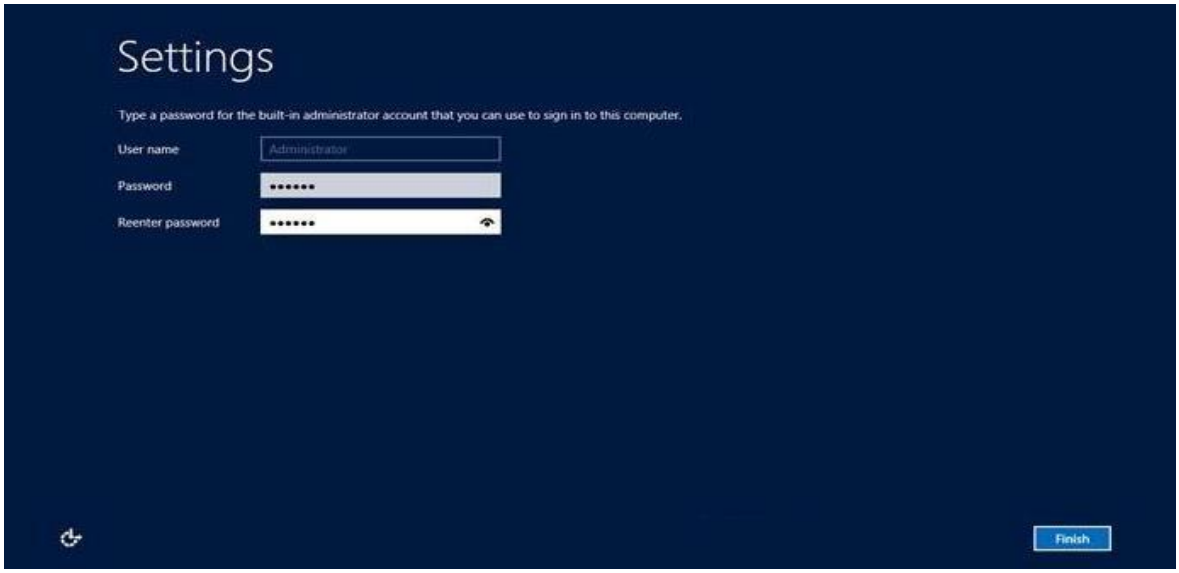

7. Now it will ask you for the drive (or partition) you want to install Windows on. Here the installation is on the one partition. **NOTE**: This will remove the content of the partition. Either you create a partition to install windows on, or you can test this on a testing machine.



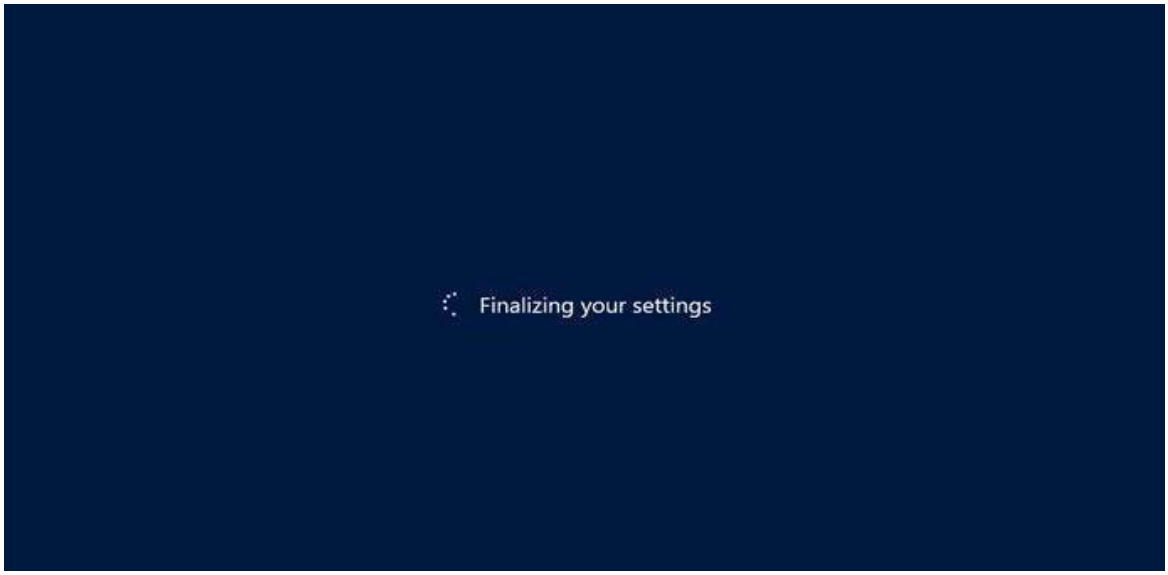

8. Now once we picked our partition, clicking on next from previous screen will start the setup. This process might take a while.



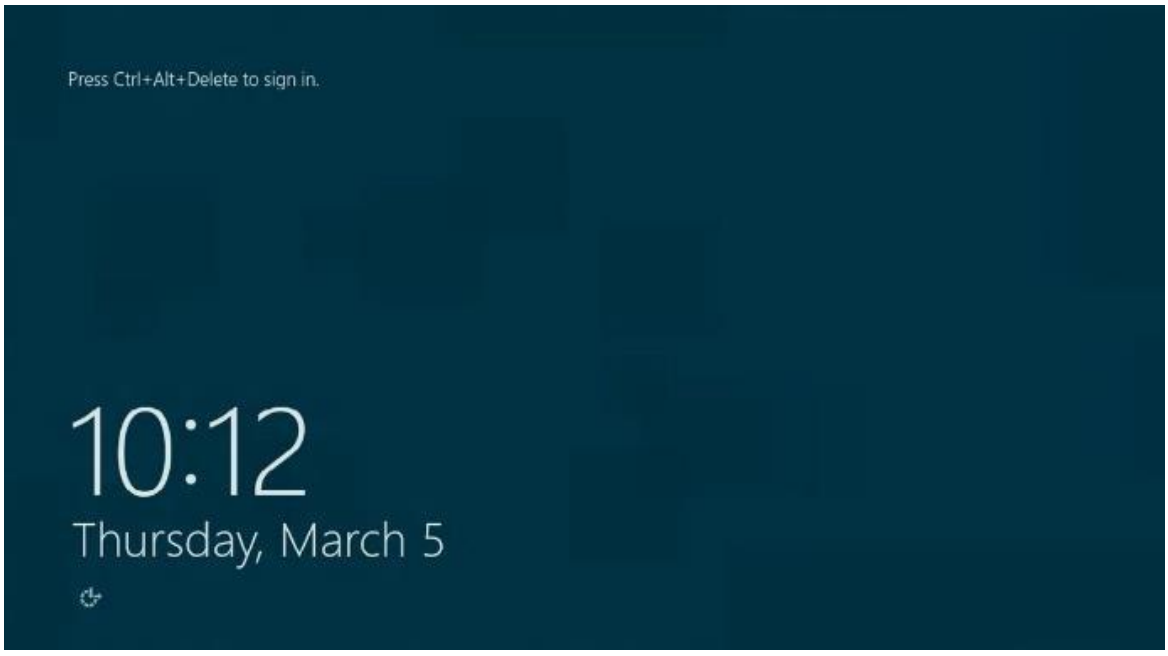

9. Once the setup is done, it will restart and start your Windows Server 2012 for the first time. It will ask you then to set up a **password** for the **Administrator** user.



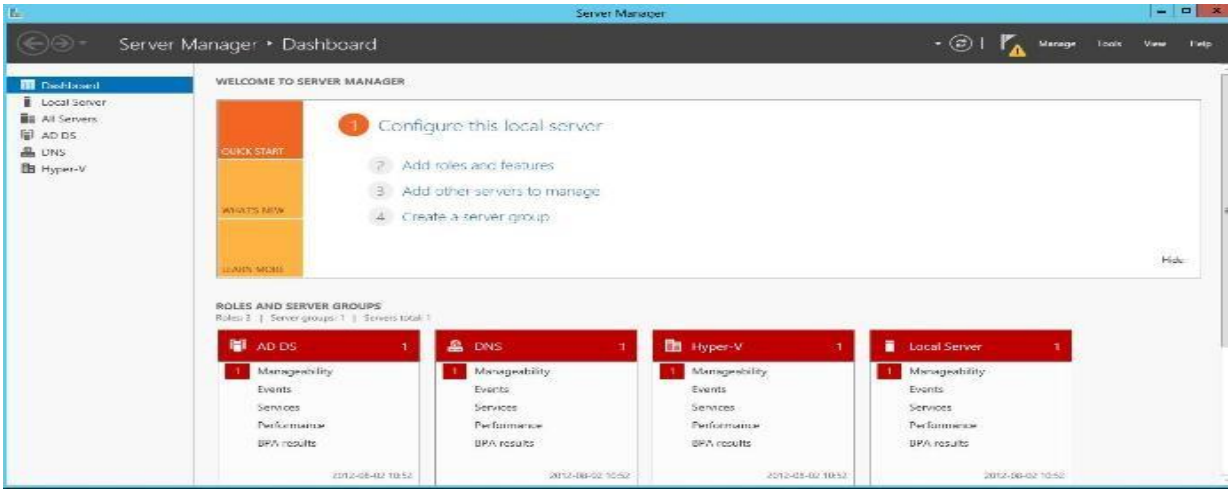

10. The setup will finalize your settings, might take a couple of minutes




11. Once the setup is done, you can log in for the first time to your Windows Server, as the screen says, press **Ctrl+Alt+Delete** to sign in, and use the password you set in the setup process.




12. Once you Log in, Windows Server 2012 will show the Server Manager

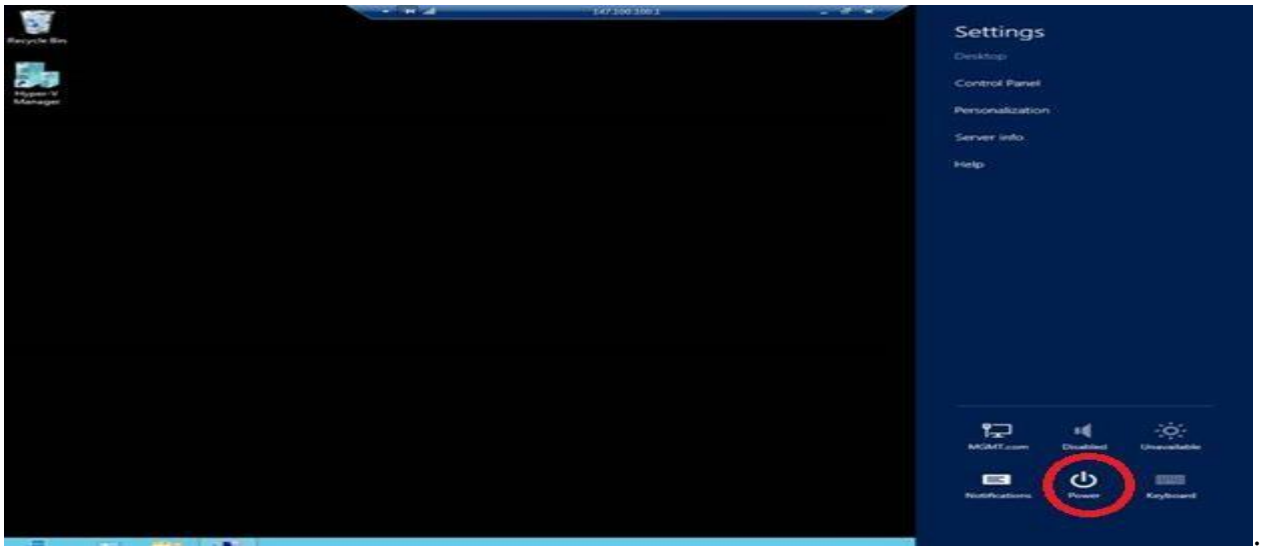



Congratulations! You have now Windows server 2012 Installed with Datacenter.

## 7.2 Working as an Administrator on Windows server

### 7.2.1 Rebooting the Server

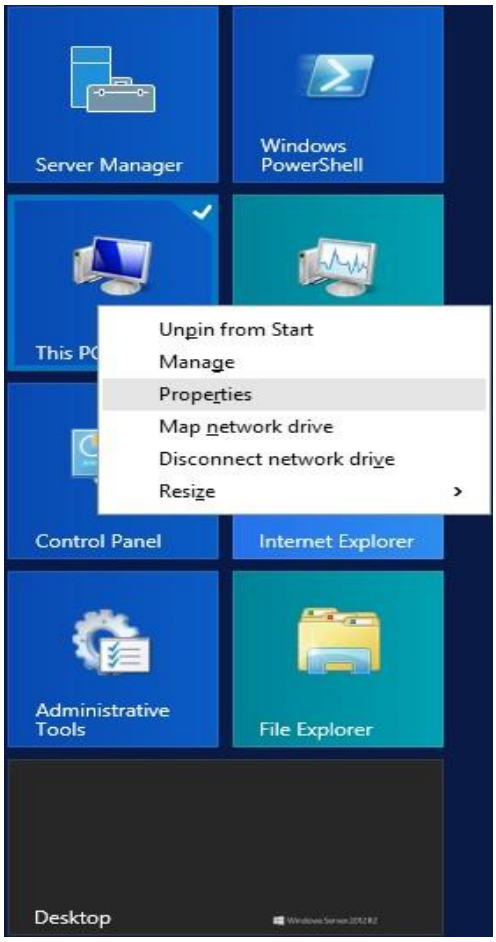
To power down (or reboot) your server, move your mouse to the upper, right corner of the screen. When you do, Windows will display a series of icons along the right side of the screen. Click the Settings icon and you will be taken to the Settings page, which you can see in the below Figure. As you can see in the figure, the bottom row of icons includes a **Power** button. You can use this icon to shut down or to reboot the server.



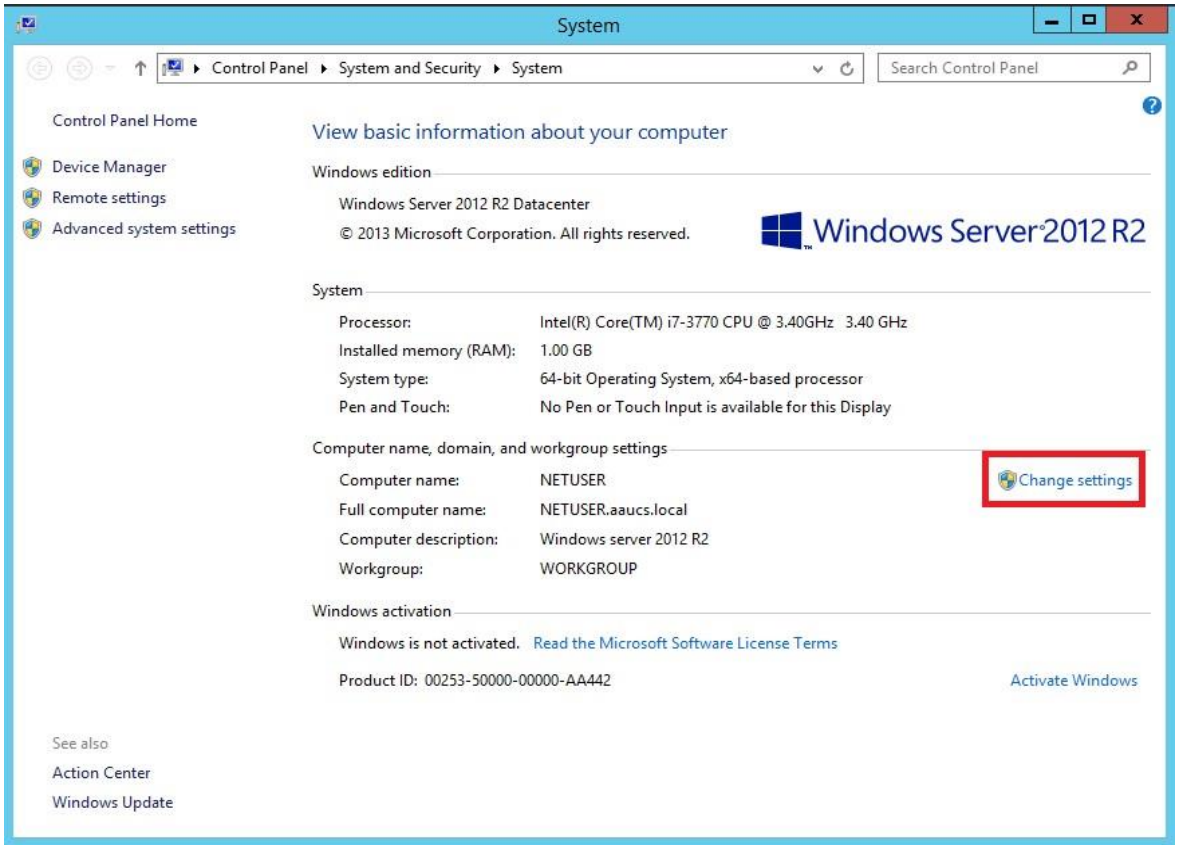
### 7.2.2 Changing the name of the server

1. Click the **Windows** icon on the task bar.

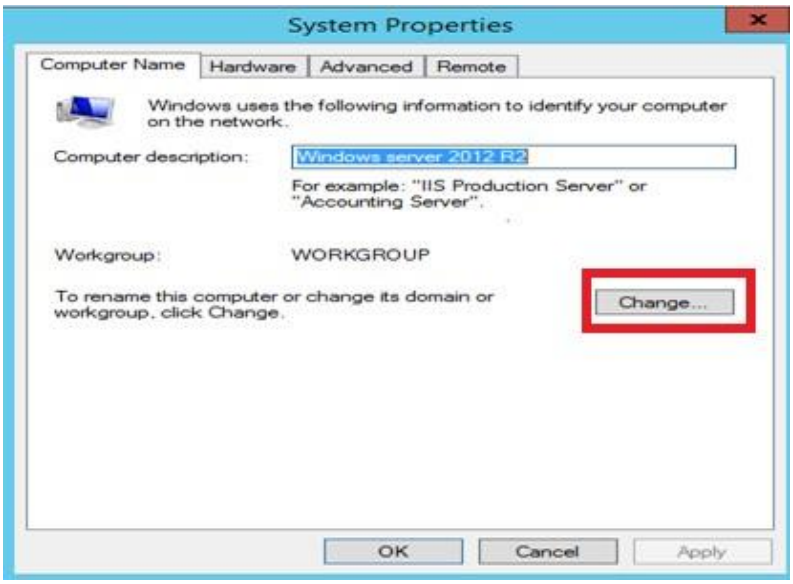
2. Right click on **This PC** and select **Properties** from the drop down options.



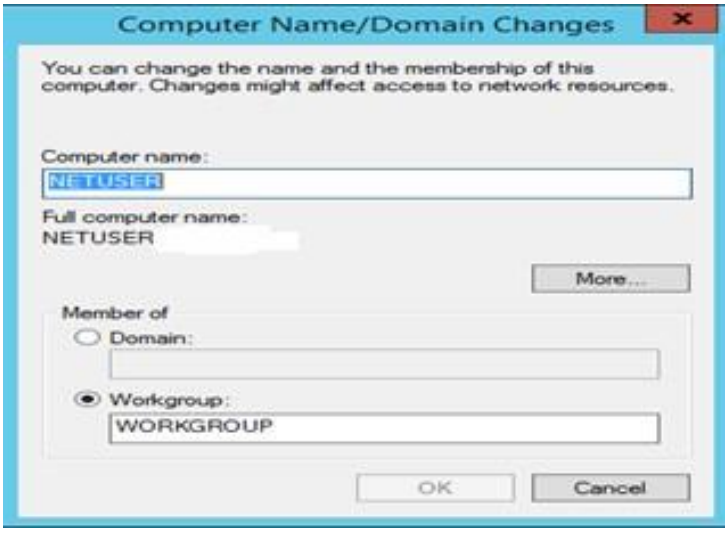

3. On the right hand side of the System pop up window click Change settings.

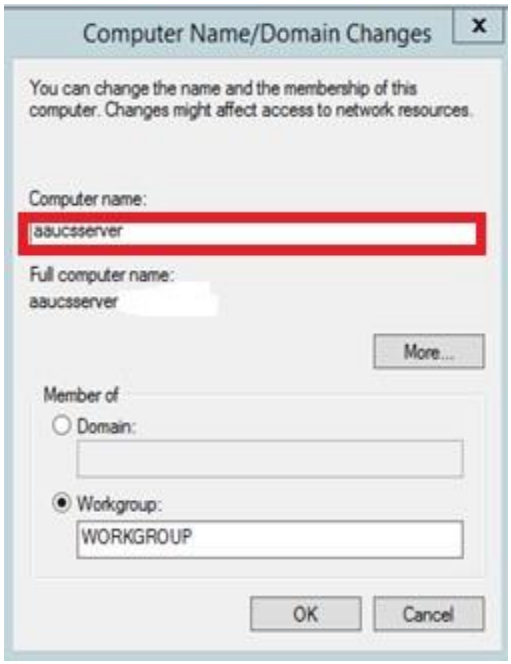



4. Next, to change the name of the server machine click **Change**.

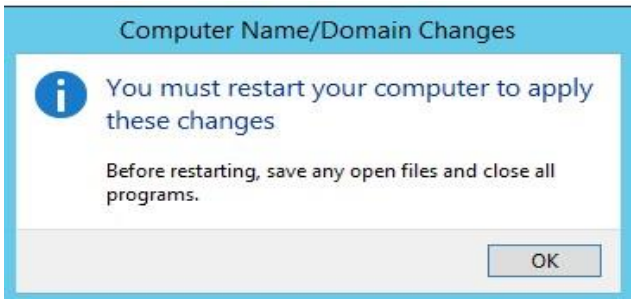


5. To change the name of the server machine by our own need, delete the given name in the Computer name field and write ours new name which we wants to give to the server, In this case, The new name is "**aaucsserver**".




6. The **restart** operation is required to apply this change.



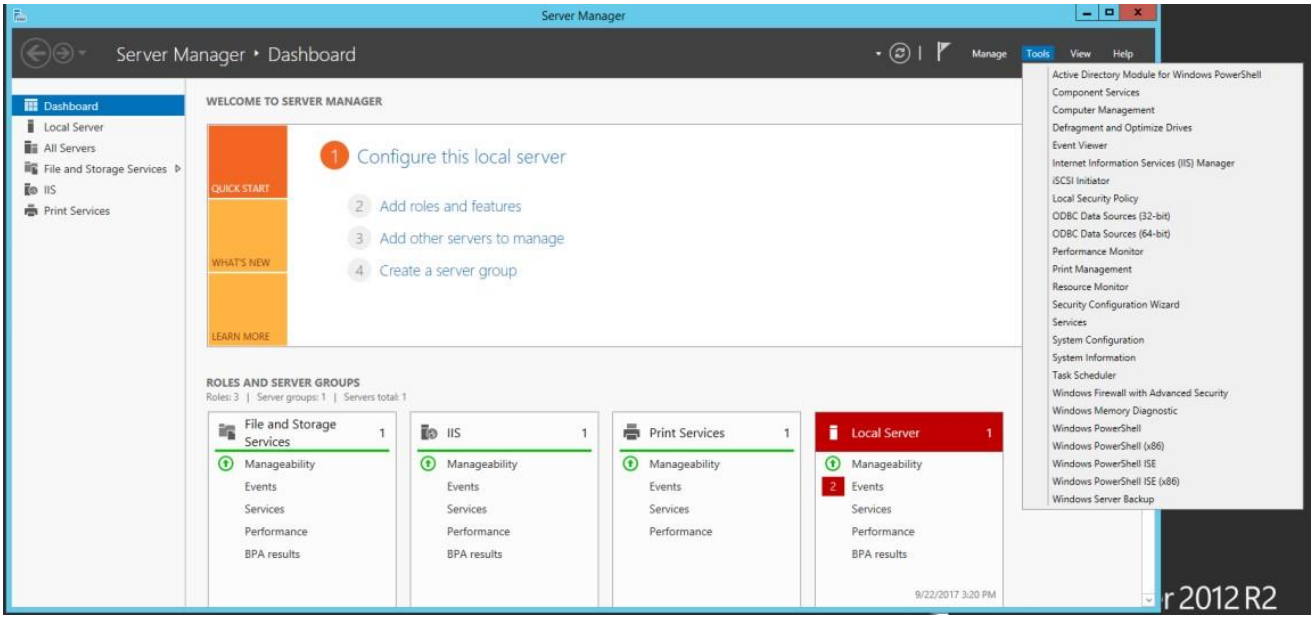

### 7.2.3 Accessing the Control Panel

The first way, Move your mouse to the upper, right corner of the screen and then click on **Settings**. When the **Settings** page appears, click the **Control Panel** link.

Another way to access the Control Panel is to go into **Desktop** mode and then move your mouse pointer to the lower left corner of the screen. When you do, the Start tile will appear. Right click on this tile and a menu will appear. This menu contains an option to access the **Control** *Panel*.


### 7.2.4 Accessing the Administrative Tools

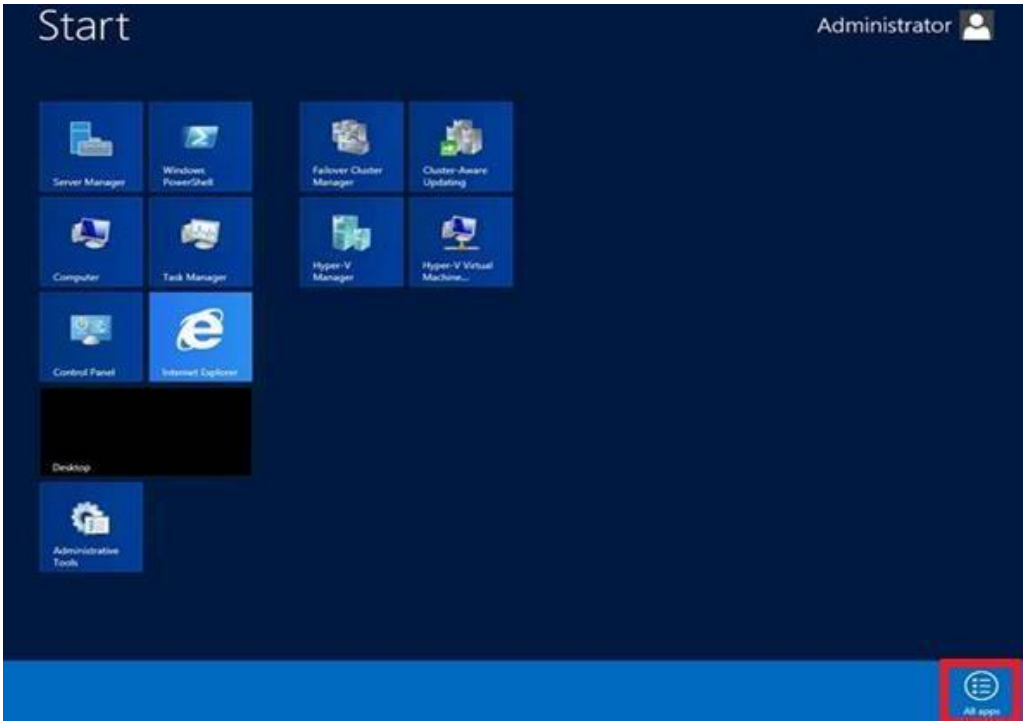
There are a couple of different ways to access the administrative tools in Windows Server 2012. One way involves using the **Server Manager**. As you can see in the below figure, the **Server Manager's Tools** menu contains all of the administrative tools that you are probably familiar with the other previous versions of Windows Servers.

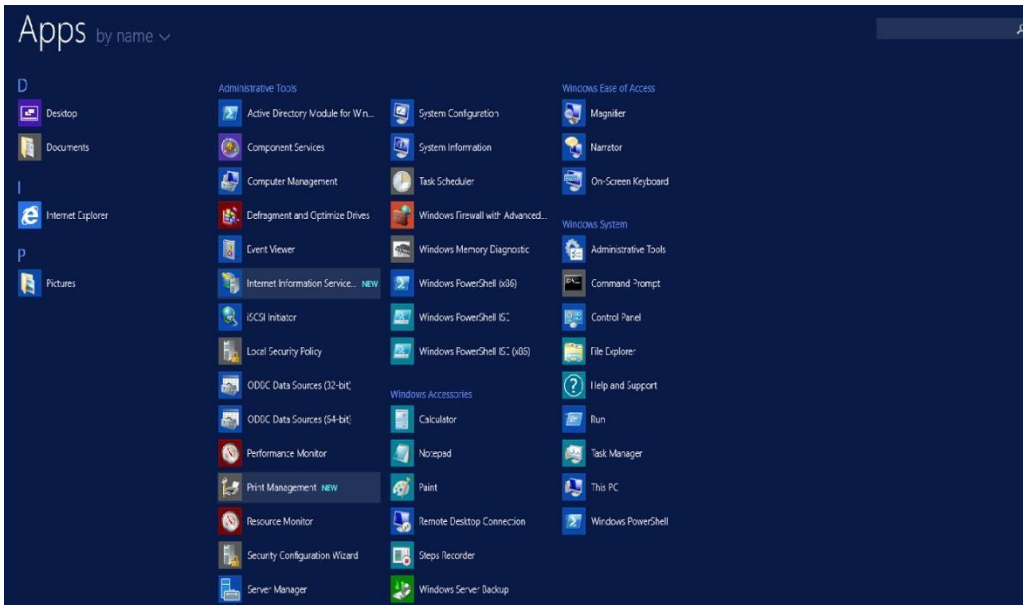



The second way, make sure that you are looking at the Windows Start screen. This technique won't work if you are in Desktop mode. Now, move your mouse to the **upper right corner** of the **screen** and then click on the **Settings** icon. When the Settings page appears, click on the **Tiles** link. As you can see in the below Figure, there is a slide bar that you can use to control whether or not the **Administrative Tools** are shown on the **Start screen**. You can see the **Administrative Tools** icon in the lower left corner of the screen capture.


## 7.2.5 Accessing Applications

To access all of the tiles that the Start screen is hiding, right click on an empty area of the **Start** screen. When you do, a blue bar will appear at the bottom of the screen, as shown in the below Figure, Click on the **All Apps** icon that appears on this bar.



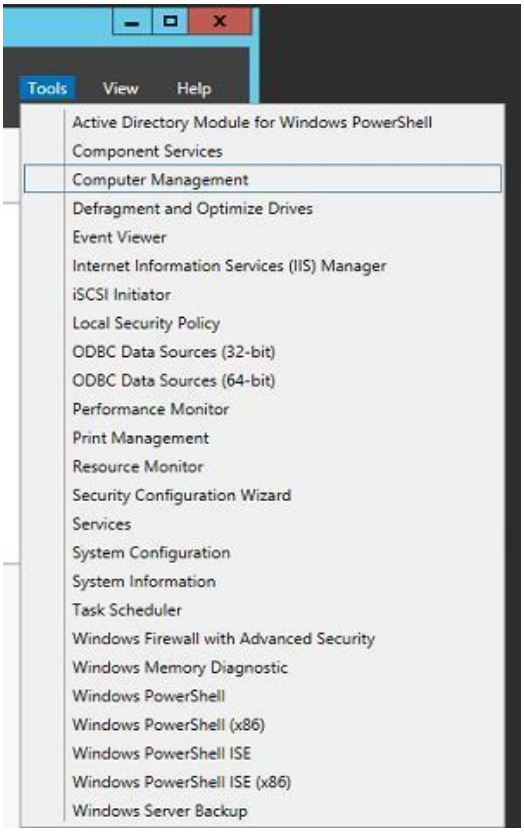

## 7.2.6 Creating a local user account in Windows server 2012

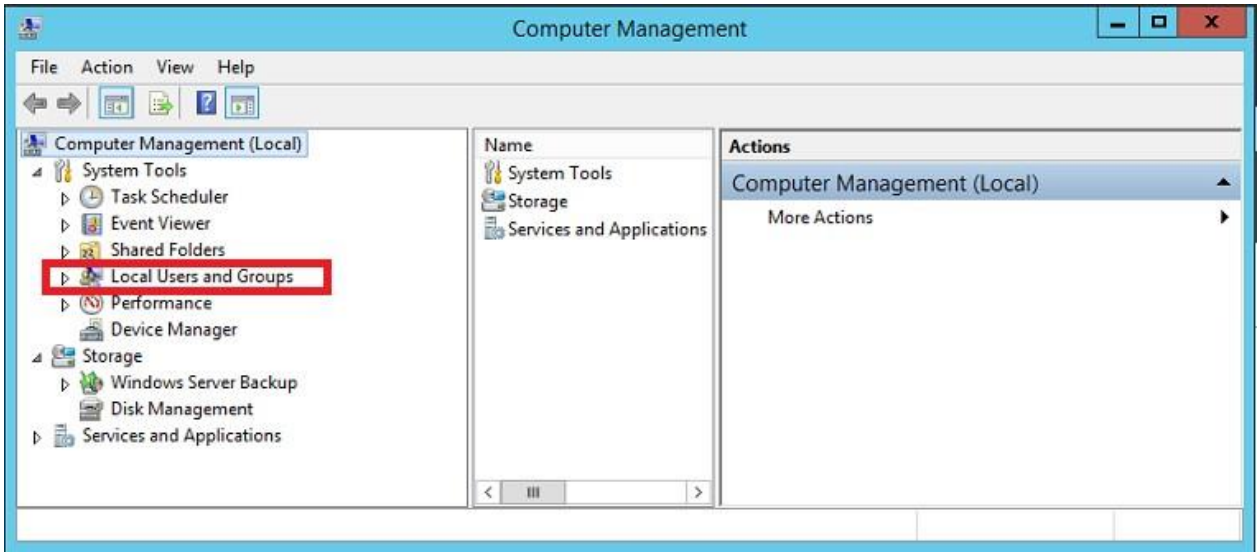
To create a local user account

- Open Computer Management.
- In the console tree, click Users.

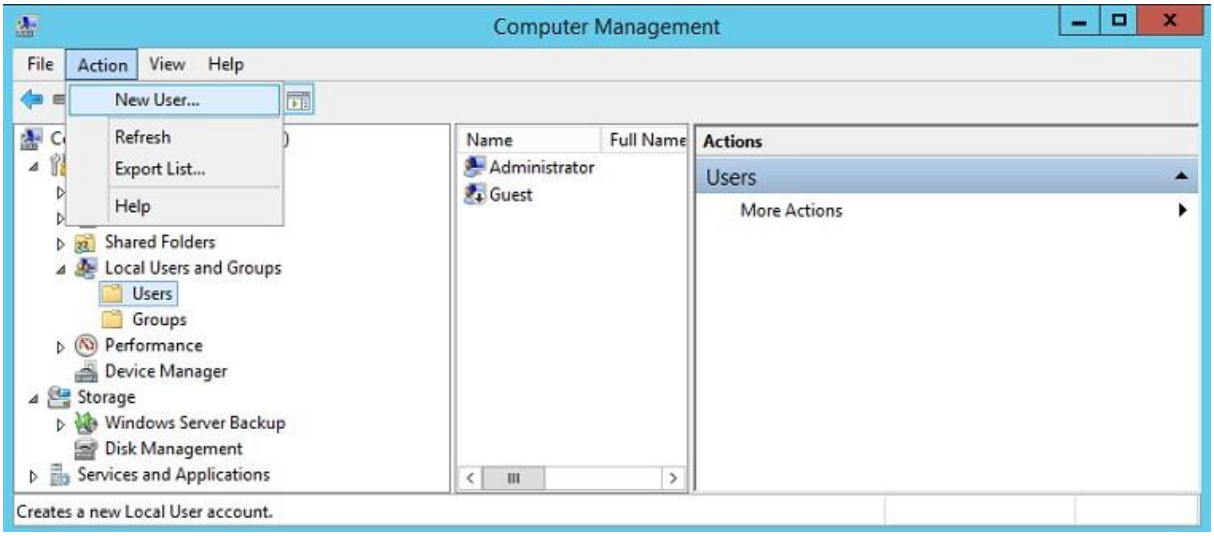
Where?

- Server Manager\ Tools\ Computer Management\ Local Users and Groups

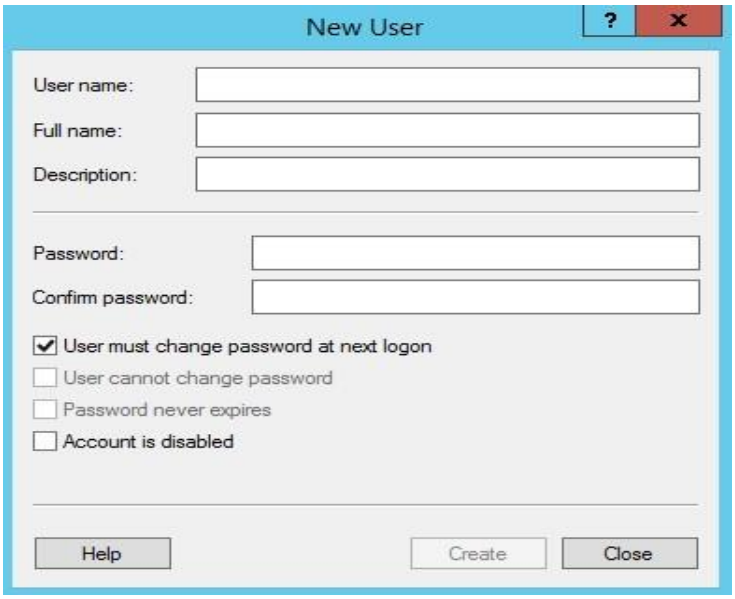



- Under **Local Users and Groups** select **Users** folder and on the **Action** menu, click **New User**.




- Type the appropriate information in the dialog box.




Select or clear the check boxes for:

- User must change password at next logon
- User cannot change password
- Password never expires

- Account is disabled
- Click **Create**, and then click **Close**.

Additional considerations:

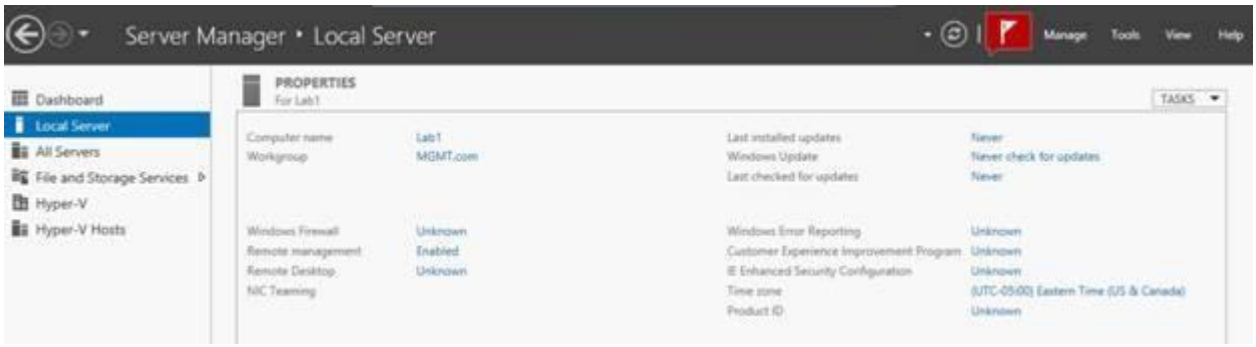
- To perform this procedure, you must provide credentials for the Administrator account on the local computer (if you are prompted), or you must be a member of the Administrators group on the local computer.
- A user name cannot be identical to any other user name or group name on the computer that is being administered. The user name can contain up to 20 uppercase characters or lowercase characters, except for the following: **" " / \ { } [ ] : ; | = + , * ? < > @**.

- A user name cannot consist only of periods (.) Or spaces.

- In **Password** and **Confirm password**, you can type a password containing up to 127 characters.
- The use of strong passwords and appropriate password policies can help protect your computer from attack.

## 7.2.7 The Run Prompt and the Command Line

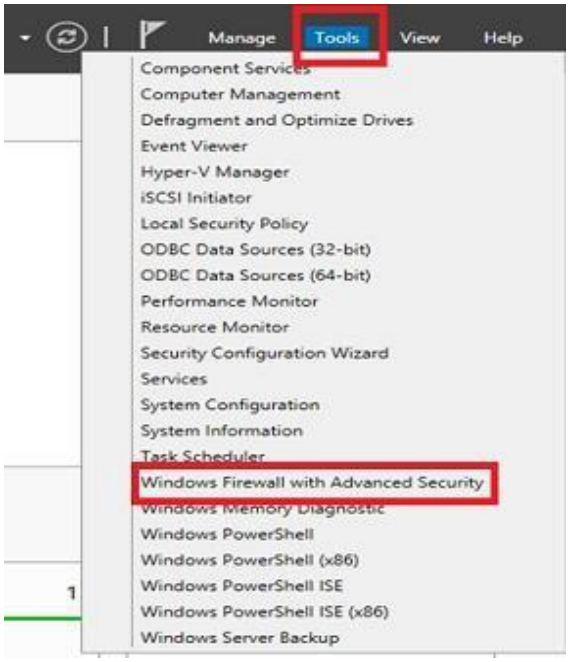
The Run prompt and the Command Prompt are both easily accessible. To reach these items, navigate into Desktop mode. Upon doing so, move your mouse pointer to the lower, left corner of the screen. When the **Start tile** appears, **right click** on it and you will see a menu listing options for Run, Command Prompt and Command Prompt (Admin).




## 7.2.8 Configuring the Windows Firewall

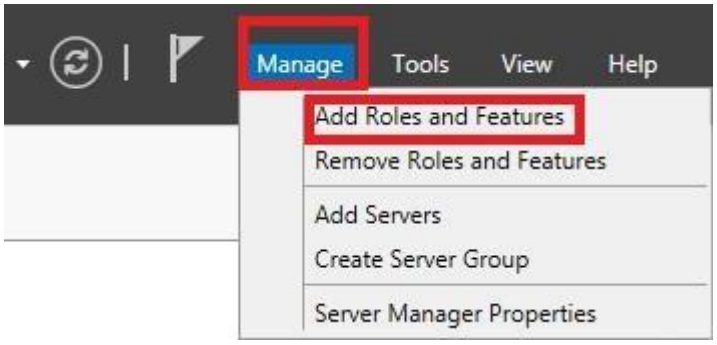
It's possible to control the Windows Firewall through group policy settings or manually. If you need to access the Windows Firewall you can do so by opening the **Server Manager** and then choosing the

**Windows Firewall with Advanced Security** command from the **Tools** menu, as shown in the below Figure.



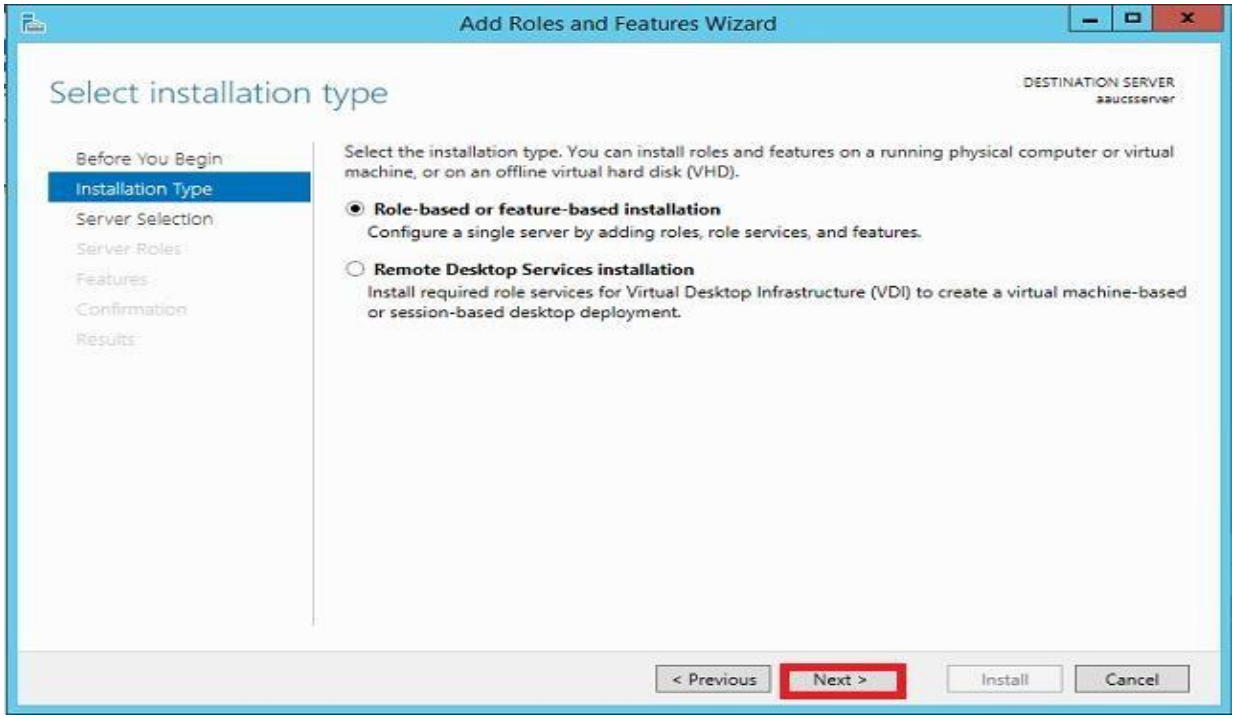

## 7.2.9 Adding Roles and Features

The easiest way to access the **Add roles and features** is to open the **Server Manager** and choose the **Add Roles and Features** command from the **Manage** menu, as shown in the below Figure. This causes Windows to launch the Add Roles and Features wizard. In many ways this wizard is similar to what you might be used to in some of the previous versions of Windows Server, but there are a few differences.

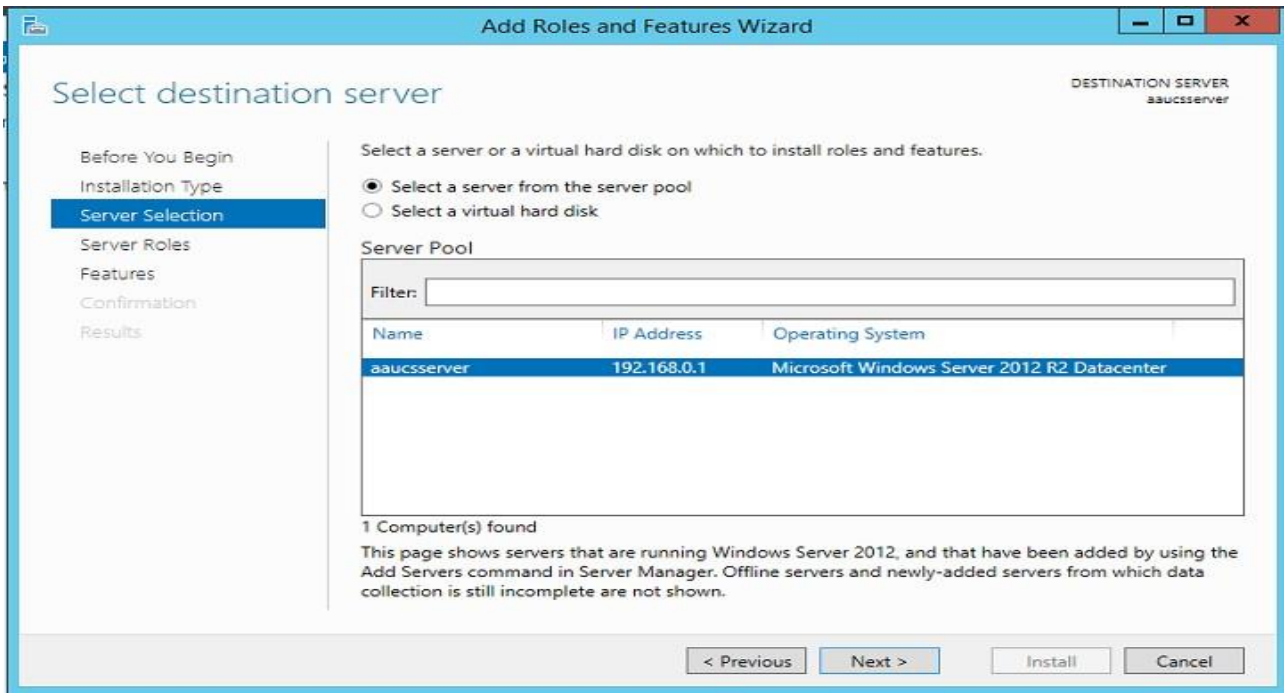



When the wizard begins, click **Next** to bypass the Welcome screen. The next screen that you will see asks you if you want to perform a **Role based or a feature-based installation** or if you would prefer to perform a **Remote Desktop Services installation**. Unless you are configuring the server to run the

Remote Desktop Services, you should choose the Role Based or Feature Based Installation option. Click **Next** to continue.




The next screen that you will see is very different from anything that existed in previous versions of Windows Server. This screen asks you where you would like to install the role or feature. Although this is a seemingly simple question, the wizard gives you a few different options, as shown in the below Figure.

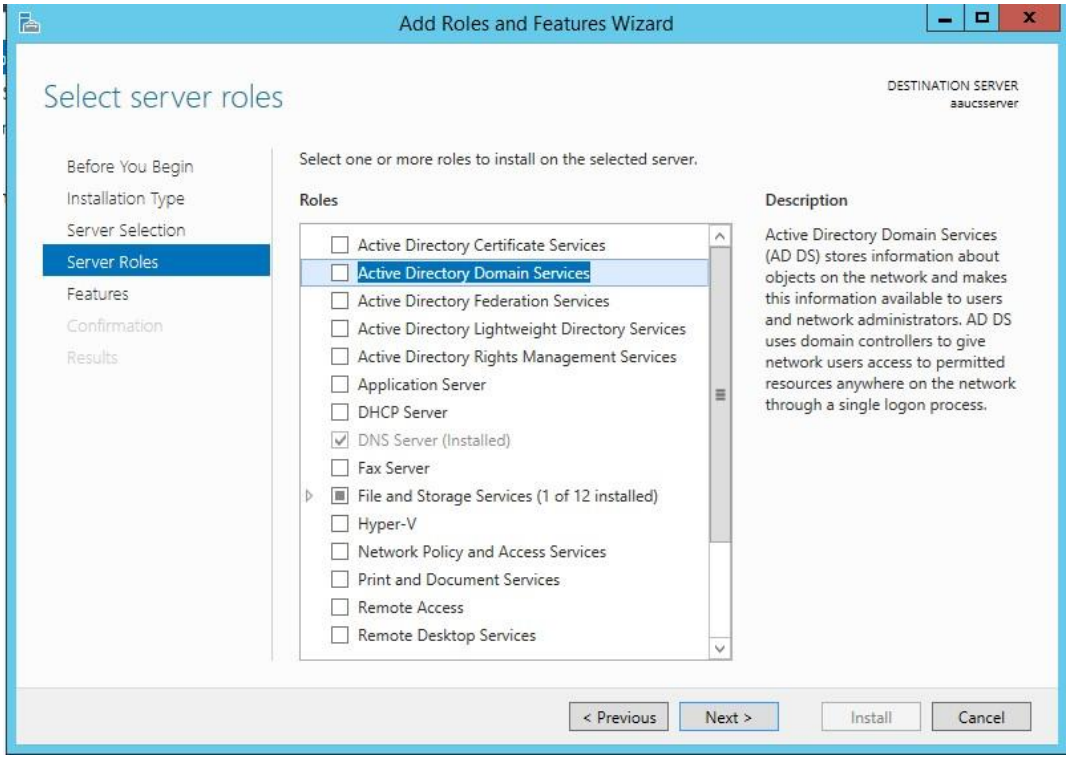


In previous versions of Windows Server it was assumed that if you were installing a role or a feature then you were performing the installation on the local server. Windows Server 2012 still allows you to perform local installations of roles and features. As a matter of fact, this is the default behavior. If you were to simply click Next on the screen above then the wizard would assume that the roles or features that you choose later on will be installed on the local server. Although this is the default behavior, it is not your only option.

If you look closely at the screen capture shown above, you will notice that the option that is selected allows you to select a server from a server pool. In Windows Server 2012, a **server pool** is simply a collection of servers that can be managed through Server Manager. As it stands right now, no additional servers have been added to the server pool for the **aaucsserver** that was used to create the figure above. If additional servers had been added to the server pool however, those servers would appear directly beneath the server that is selected. We will show how to add a server to the server pool on the next title.

The other option that appears on the screen capture is the option to select a virtual hard disk. Previous versions of Windows Server required you to install roles and features on a running copy of Windows. This is not the case in Windows Server 2012. It is actually possible to install a role or a feature on to a virtual hard disk that contains a Windows Server installation that is not currently running.

When you click **Next**, you will see a screen displaying all of the various server roles that you can install. The list of server roles really isn't all that different from those found in Windows Server 2008. When you make your selection you can click **Next** and you will be taken to the Features screen. Here you can choose the features that you want to install.

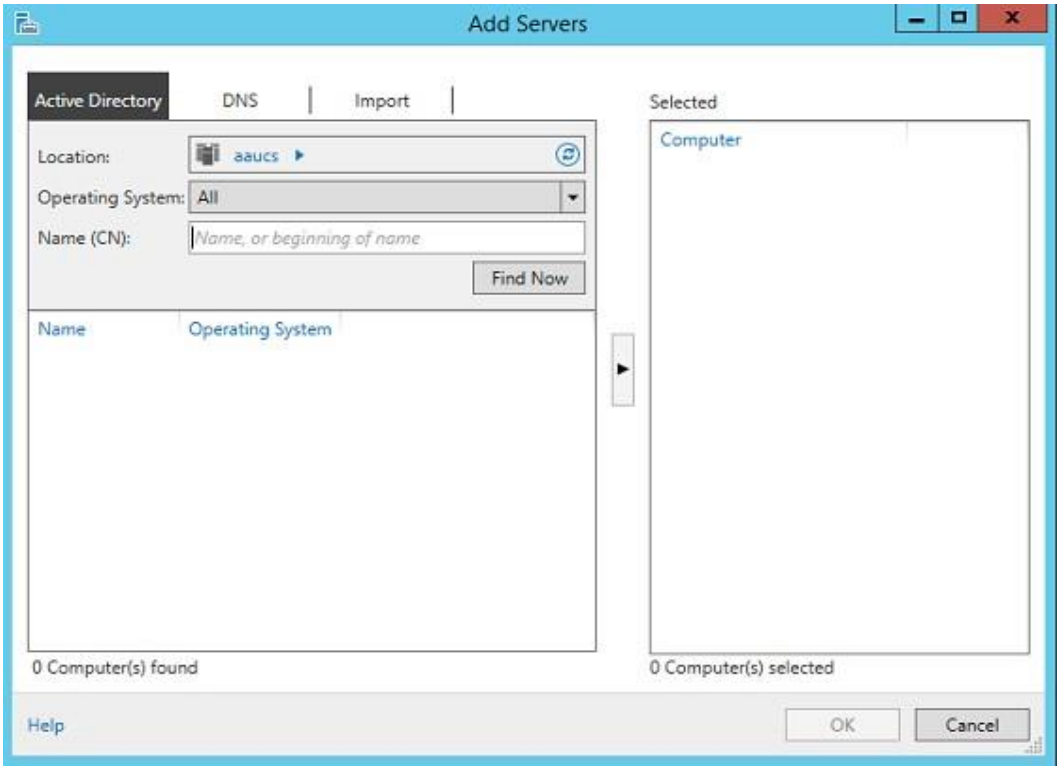


When you click Next once again, you will see a confirmation screen that provides information about the roles were features that are about to be installed. It is a good idea to take just a moment to read this screen and verify that the roles or features that are about to be installed are the ones that you intended. Assuming that all is well, you can click the **Install** button to perform the installation.

### 7.2.10 Adding Servers to the Server Pool

The advantage to populating the server pool is that doing so allows you to manage multiple Windows servers through a single pane of glass.

If you want to add additional servers to the server pool, open **Server Manager** and choose the **Add Servers** command from the **Manage** menu as shown in below figures.


As you can see in the above figure, Windows provides three different methods for adding servers to the server pool. In most cases, you will probably want to use the **Active Directory** tab. This tab allows you to specify the **names** of **computers** that are registered in the Active Directory database.

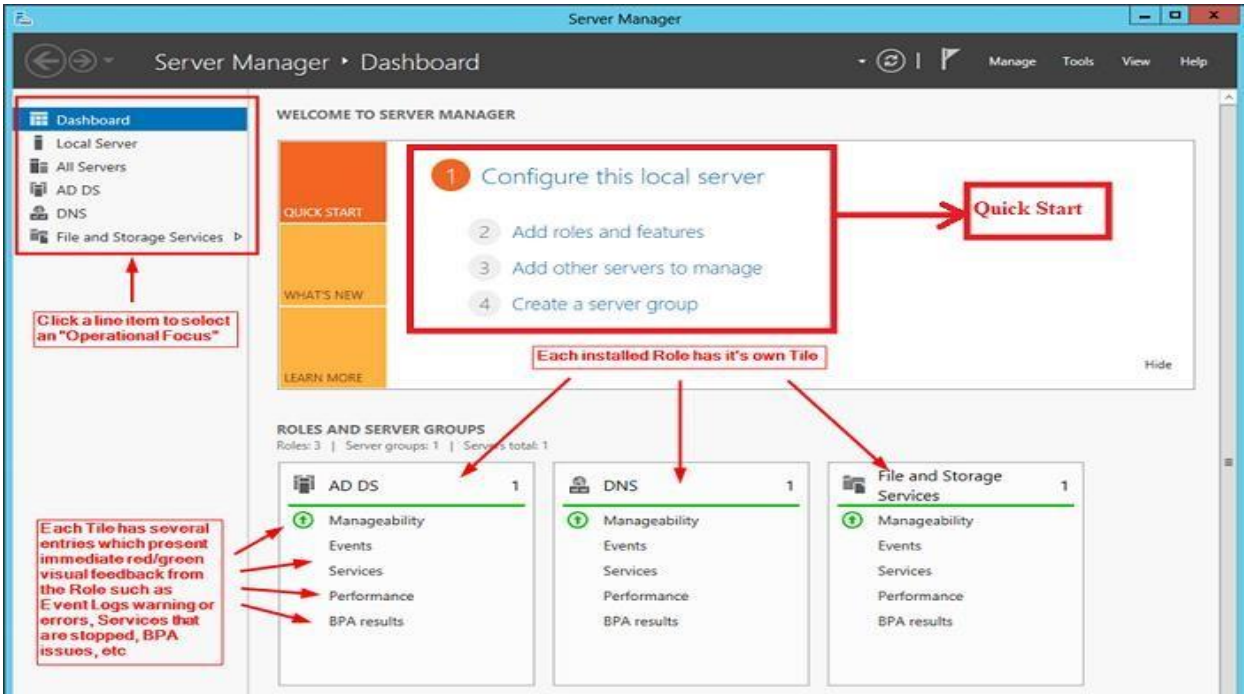
You will notice in the figure above that Windows gives you the option of specifying the computer's location, and you can even filter the search results by operating system.

Another option is to specify computers by their fully qualified domain names or by IP address. This can be accomplished through the **DNS** tab. The **DNS** tab is useful for adding computers that exist on your network, but that are not members of an Active Directory domain. For example, edge servers are almost never domain members.

Finally, the **Import** tab is used for importing large numbers of computers. This method allows you to add all of the computers to a file, and then import that file rather than having to import each computer individually. Once added, the servers in the pool will be accessible through the **Server Manager.**

## 7.2.11 Working with Roles and Features

In the previous article I walked you through the process of installing roles and features onto Windows Server 2012. I want to wrap up this series by showing you what to do after the roles and features have been installed. If you look the figure in below, you will see the **Server Manager dashboard**. There are several items on this screen that are worth paying attention to.




The first thing that you will probably notice is the big, orange section near the center of the screen. This section is designed to help you to quickly get the server configured. As you can see in the figure, this section contains links that you can **click** to **add roles and features**, add other **servers to manage**, or to create server groups. As you have seen throughout this series, all of these tasks can be performed manually, but if you forget how to do so then you can simply click on one of these links to get the ball rolling.

The next most important thing is the column on the left. This column lists a number of different Server Manager Views. At the moment the Dashboard view is selected, but you can switch to a different view by clicking on the view.

Some of the views that are listed are standard for Windows Server 2012. The Dashboard, Local Server, All Servers, and File and Storage Services views are created by default. There are also views that may exist as a result of the way that you have configured your server. For example, in the figure above the AD DS and DNS exist as a direct result of installing the corresponding roles and features.

# Part IV: Installation and configuration of several server roles in Windows Server

# Chapter Eight: Installation and Configuration of Domain Name System (DNS)

## 8.1 What is DNS?

Domain Name System (DNS) is a hierarchical naming system for computer systems, services or for that matter any resource participating in the internet. Much information with domain name is assigned to each of the participants. DNS translates the names of domain into meaningful to humans into binary identifiers that are associated with the equipment of network to locate and address these devices.

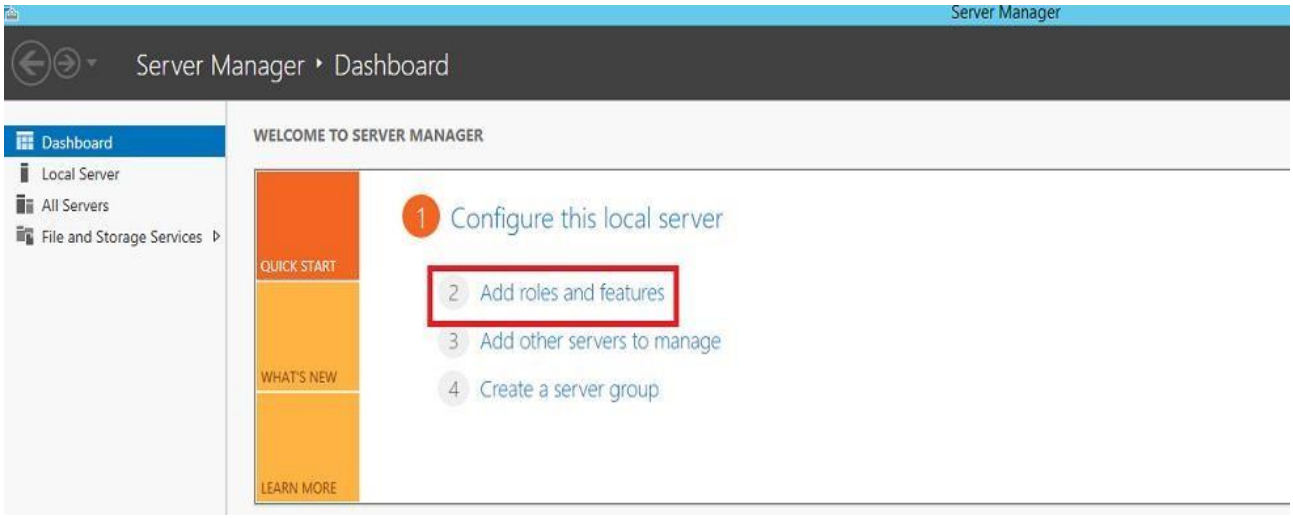
⇨ Setting up a Domain Name System (DNS) on Windows Server involves installing the DNS Server **Role.**

## 8.2 Installation of Domain Name System (DNS) Role

### Steps:

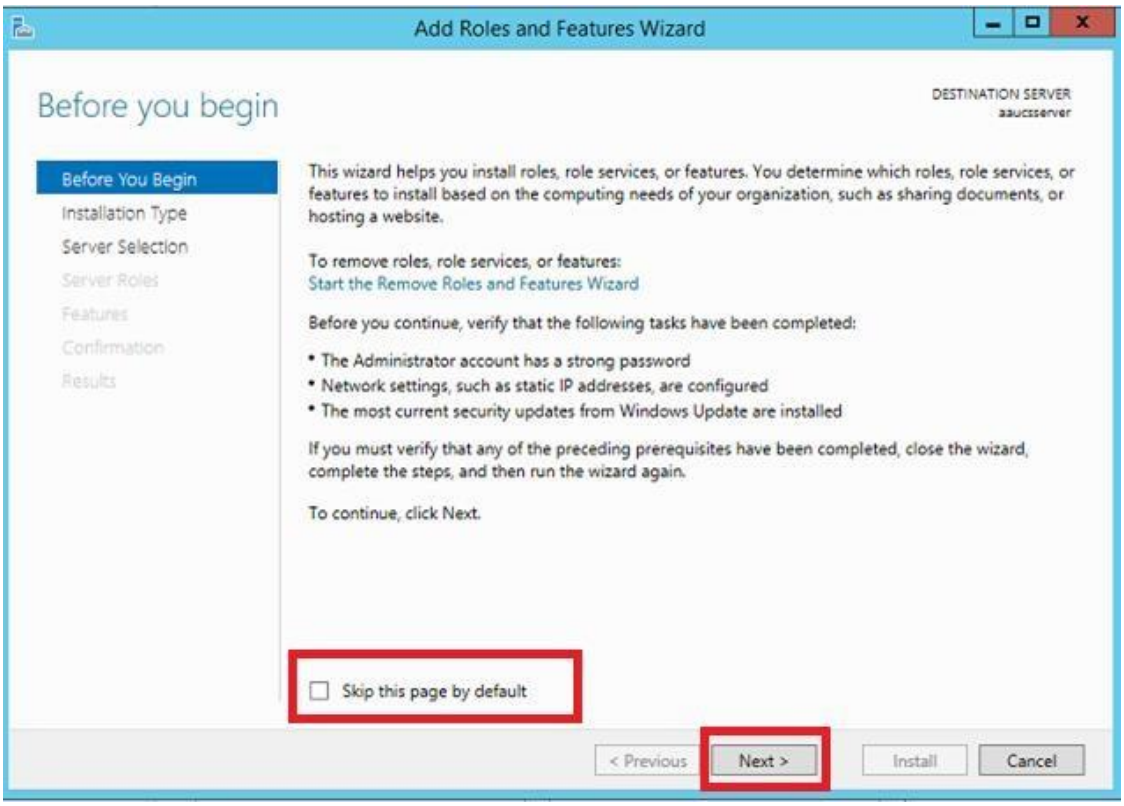
To add a new role to Windows Server 2012, you use Server Manager.

- Start Server Manager, click the Manage menu, and then select Add Roles and Features.

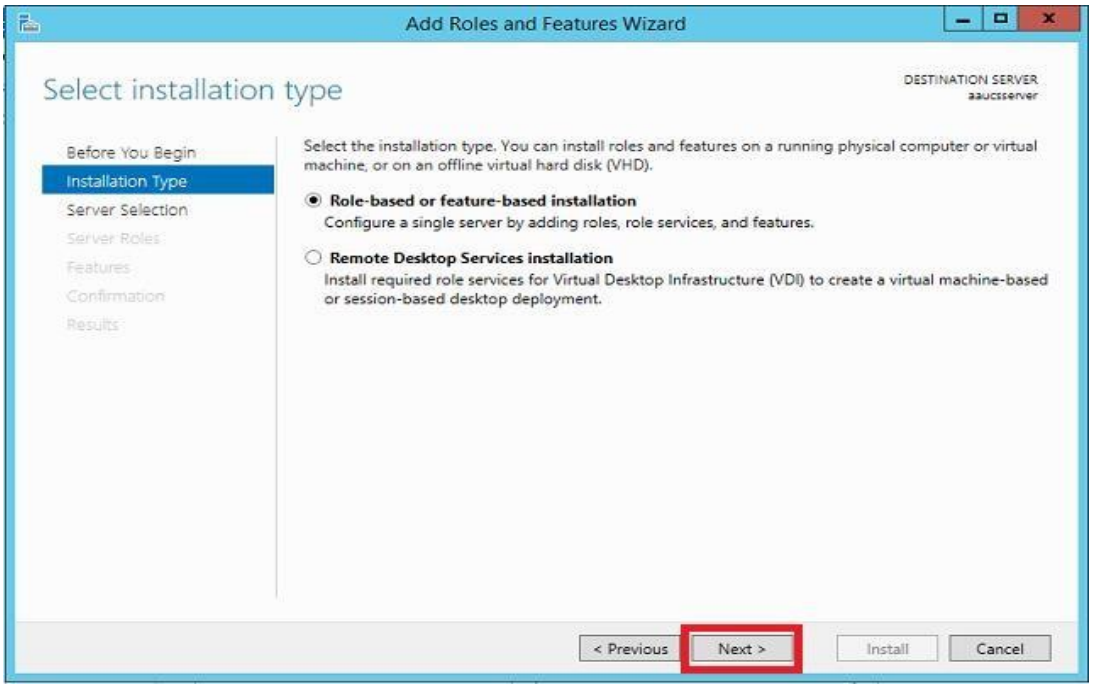



- Click **Next** on the Add Roles and Features Wizard Before you begin window that pops up. If you checked **Skip this page by default** sometime in the past, that page will, of course, not appear.

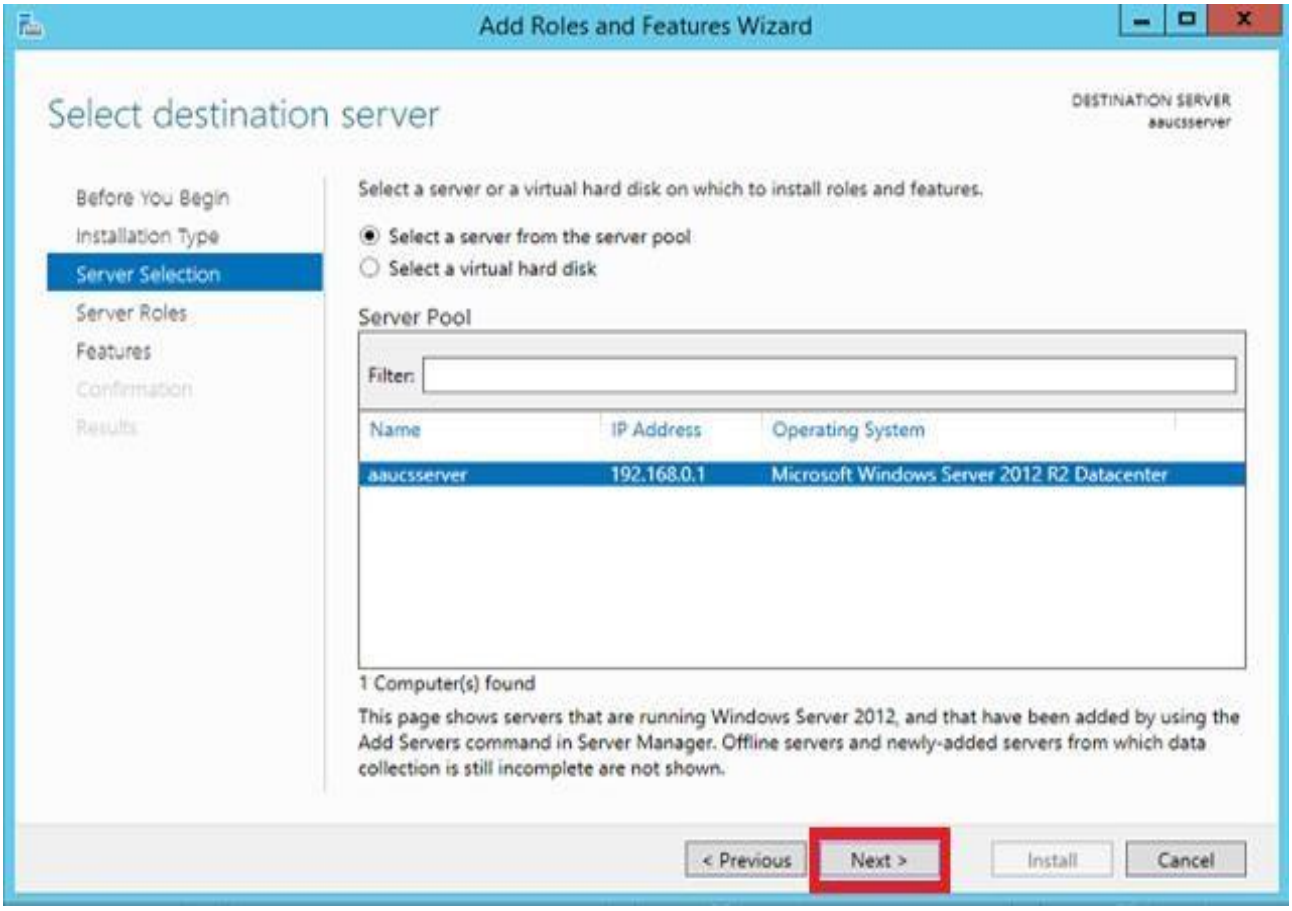
➢



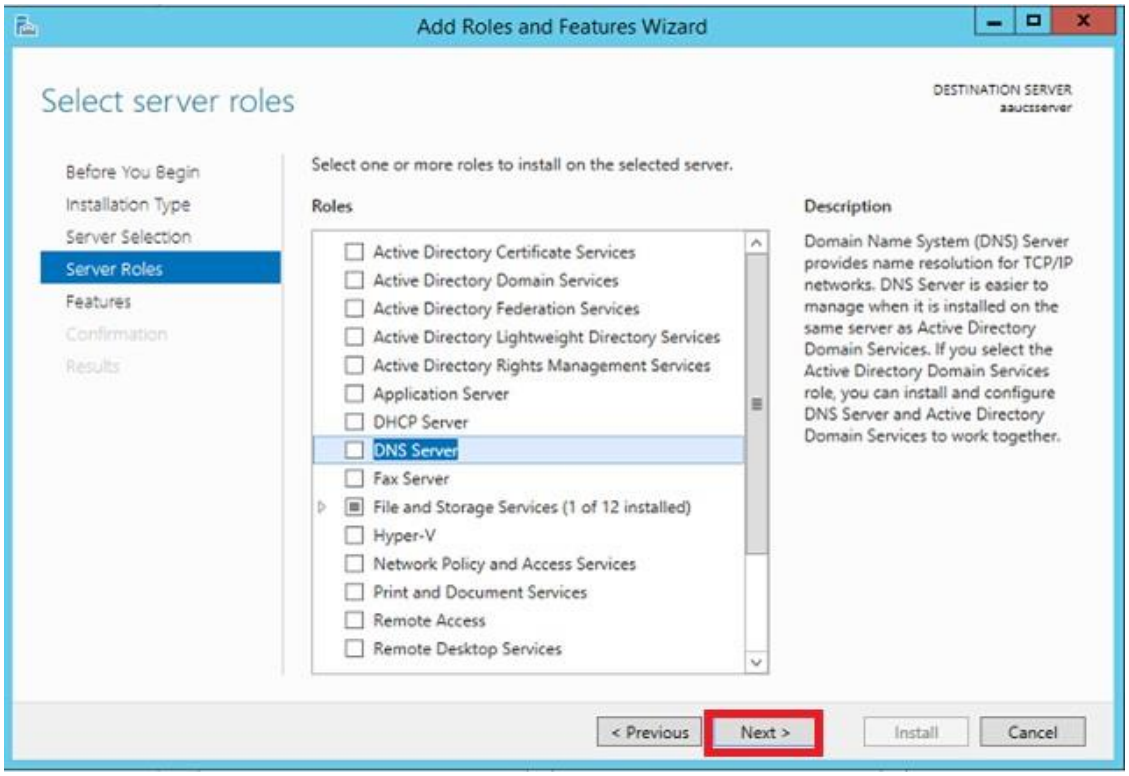

➢ Now, it's time to select the installation type. For DNS servers, you will be selecting the **Role based or feature-based installation**.



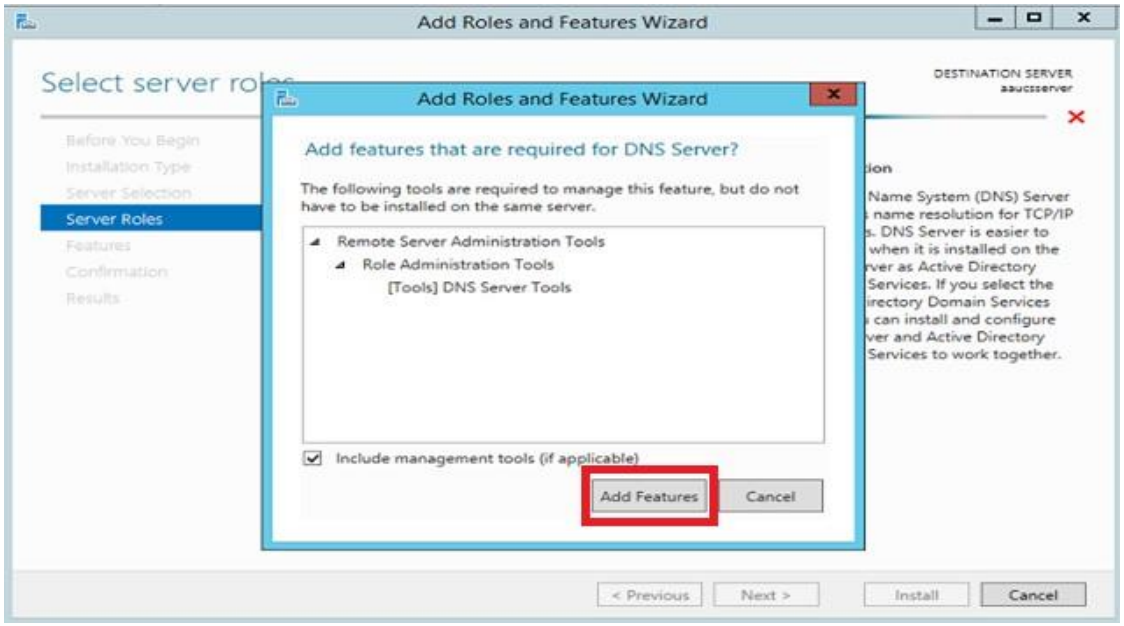
- Next, you will choose which server you want to install the DNS server role on from the server pool. Select the server you want, in our case there is one server named "**aaucsserver**" with IP address 192.168.0.1 and the operating System is Microsoft Windows Server 2012 R2 Datacenter and click **Next**.



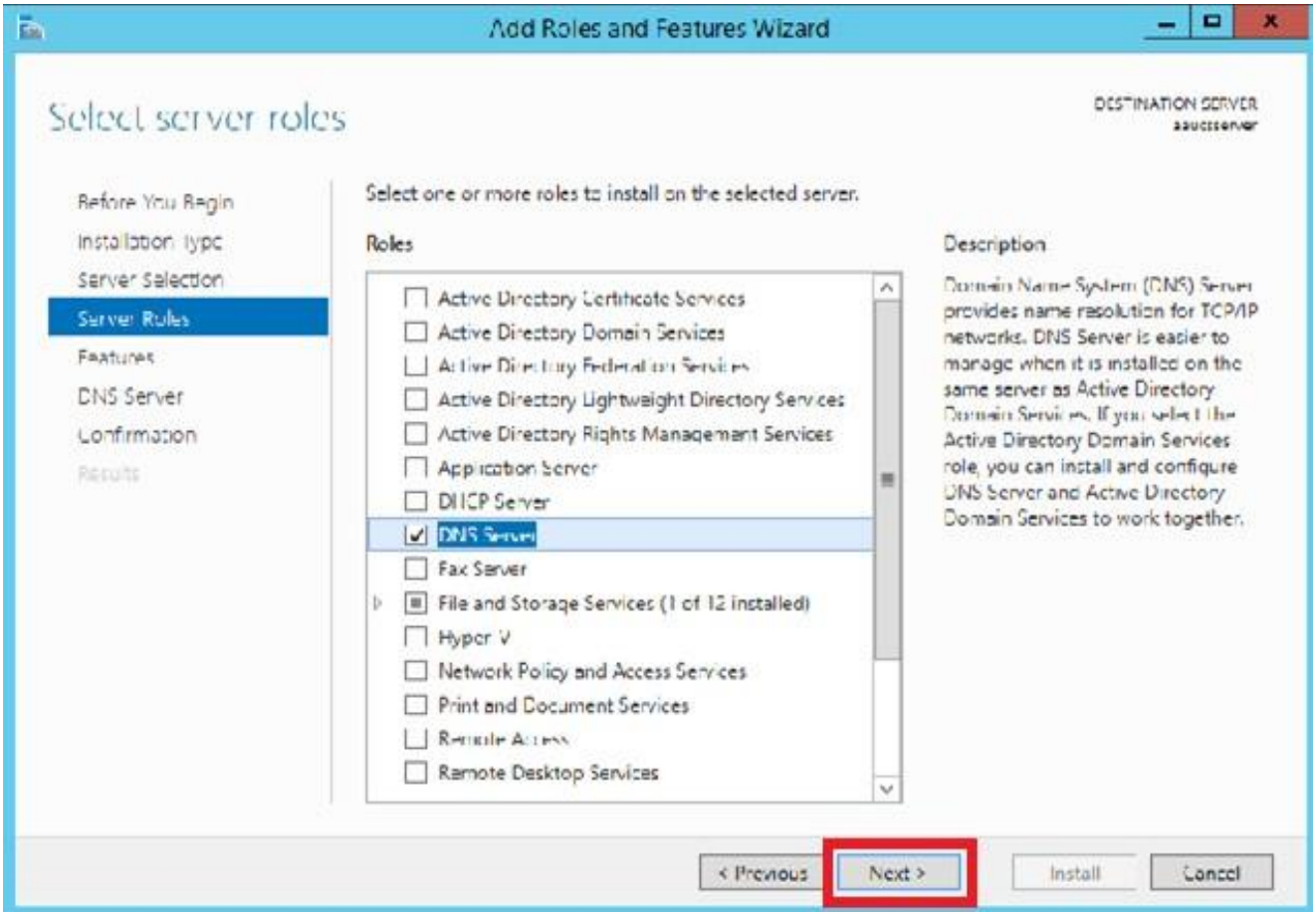

- Next, Select "**DNS Server**" from "**Add Roles and features Wizard**" popup window



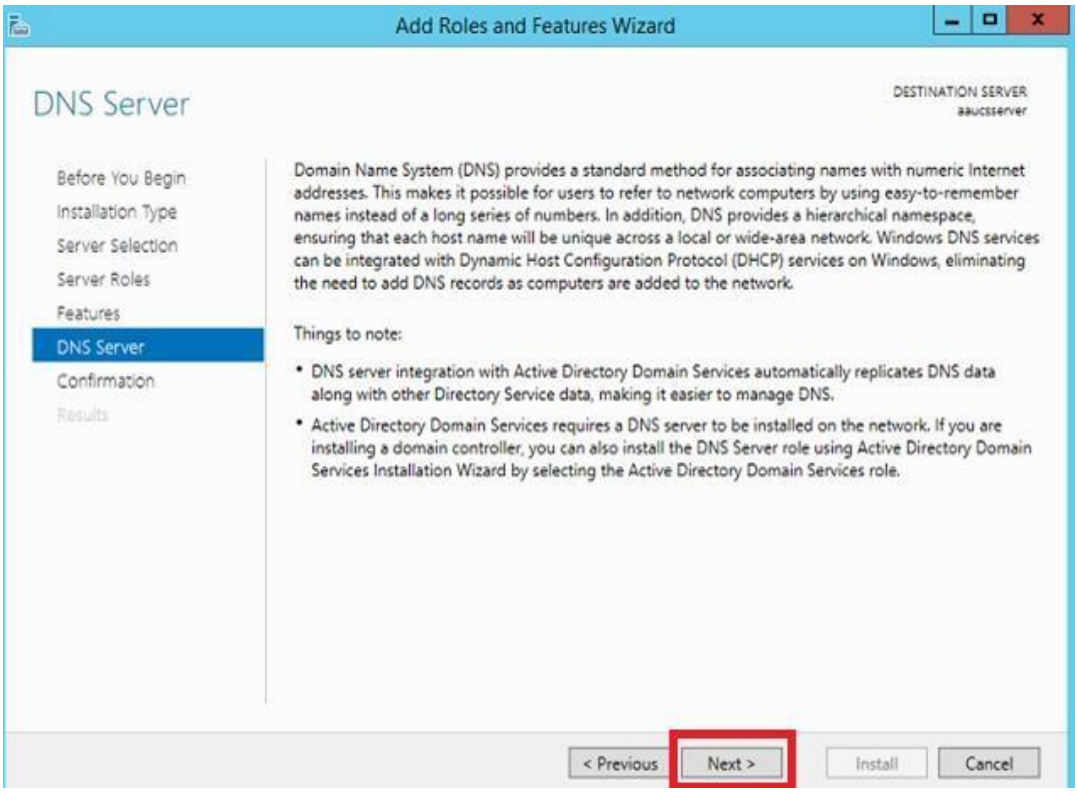

- `At this point, you will see a pop-up window informing you that some additional tools are required to manage the DNS Server. These tools do not necessarily have to be installed on the same server you are installing the DNS role on.



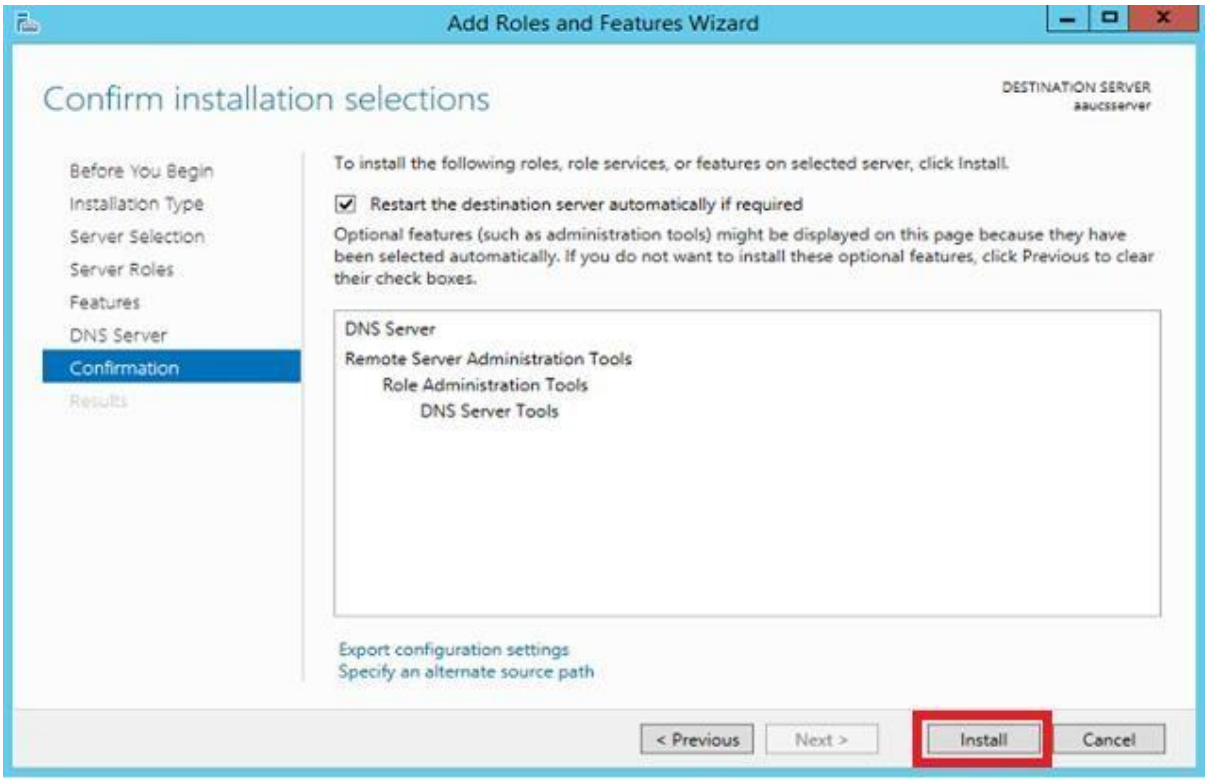
**N.B** If your working environment only does remote administration; you do not have to install the DNS Server Tools.



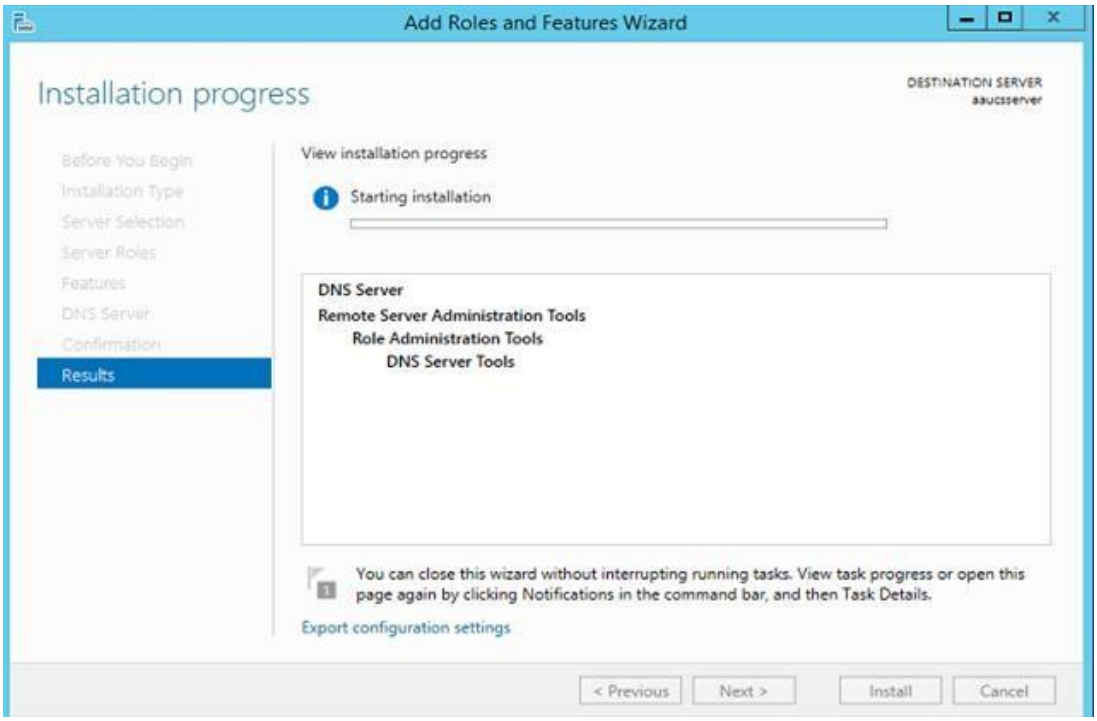

- Next you should see the Features window. No need to make any changes here; just click **Next**, and now there is an informational window about DNS Server and what it does, although one would assume that if you've gotten this far, you are already aware of what it is. Click **Next** to move on.

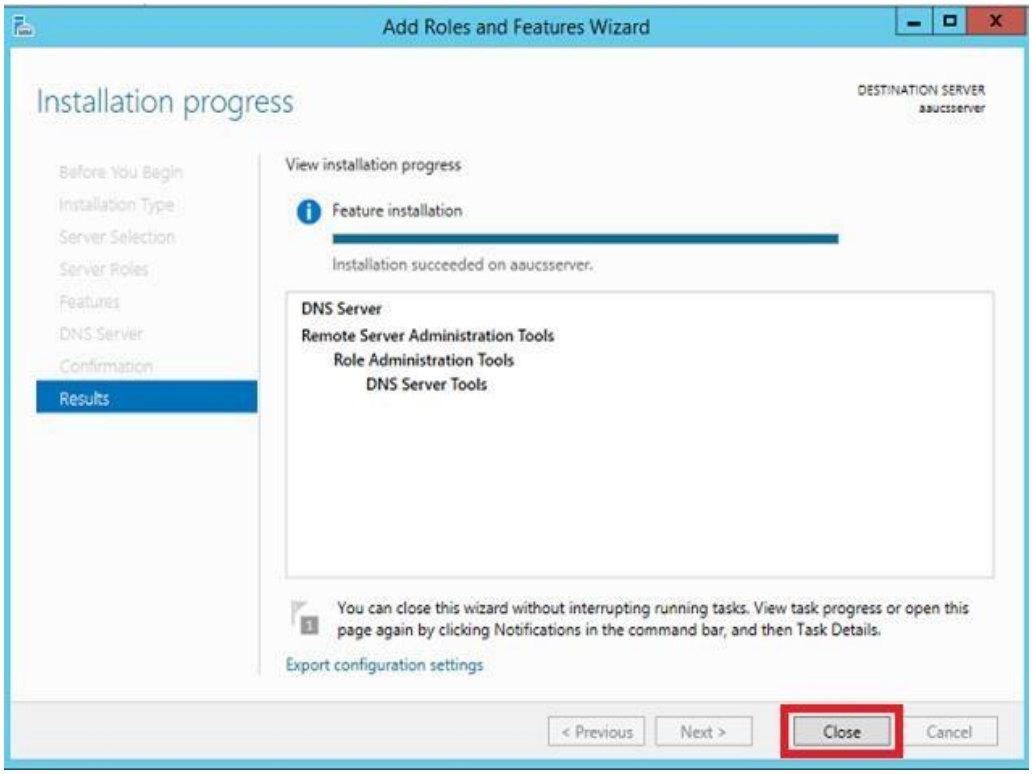



- This is the final confirmation screen before installation completes. You can check the box to “Restart the destination server automatically”, if you like. Installing the DNS Server does not require a restart, but unless you've planned for the downtime, keep that box unchecked, just in case.

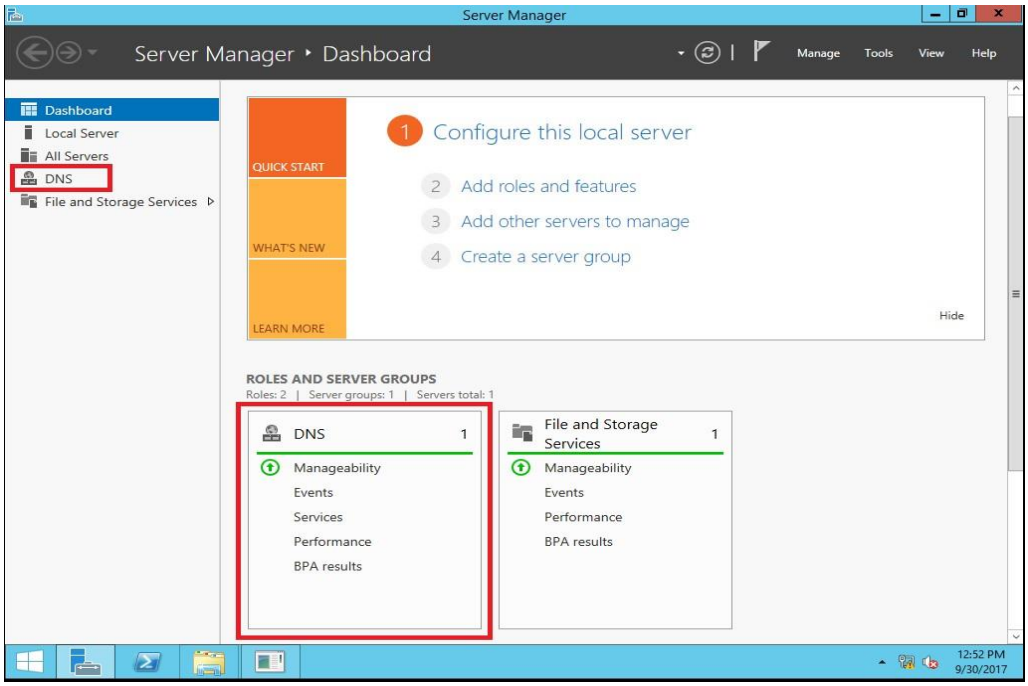



- After you clicked "**Install**" button from the previous step; the installation process is staring and click **Close** button when it finishes the installation process.



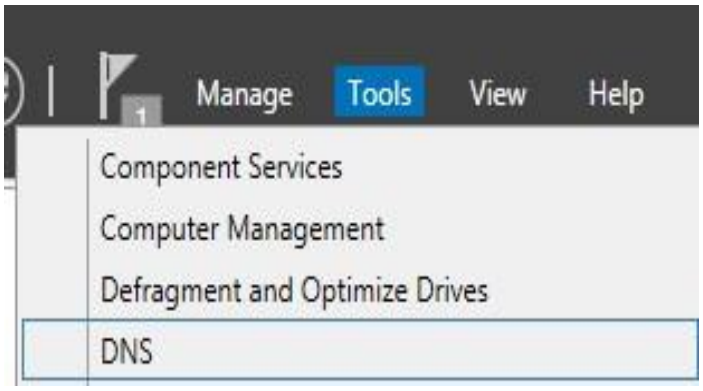



- Finally, The DNS Server role should be installed on your server. There should be a new DNS Role tile in your Server Manager.

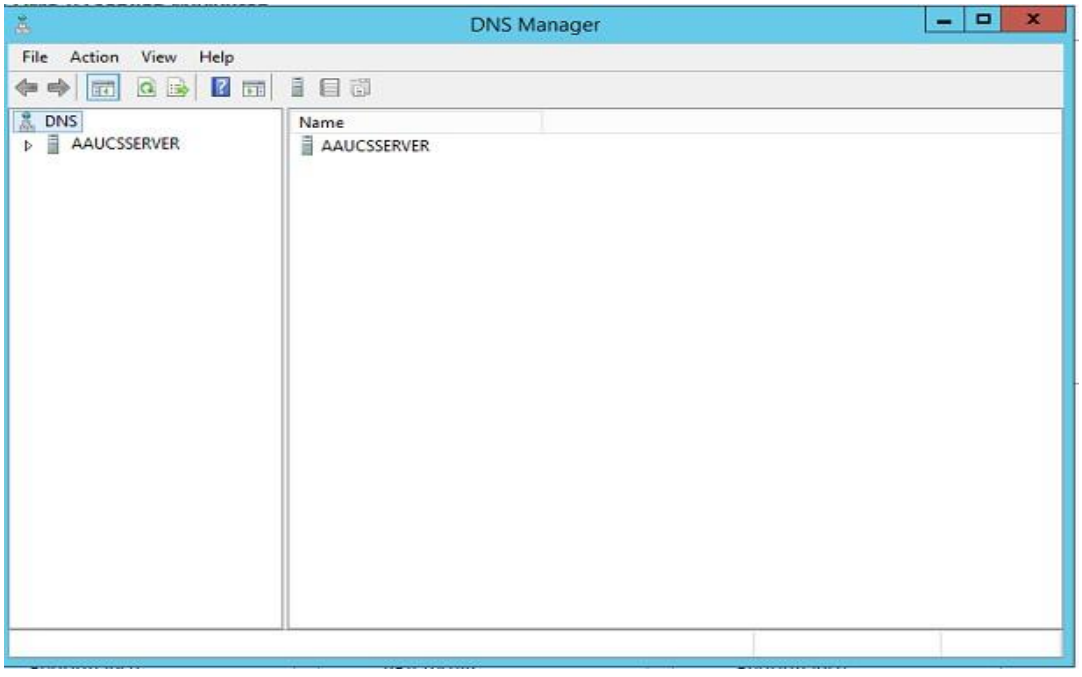


## 8.3 Configuration of a DNS Server

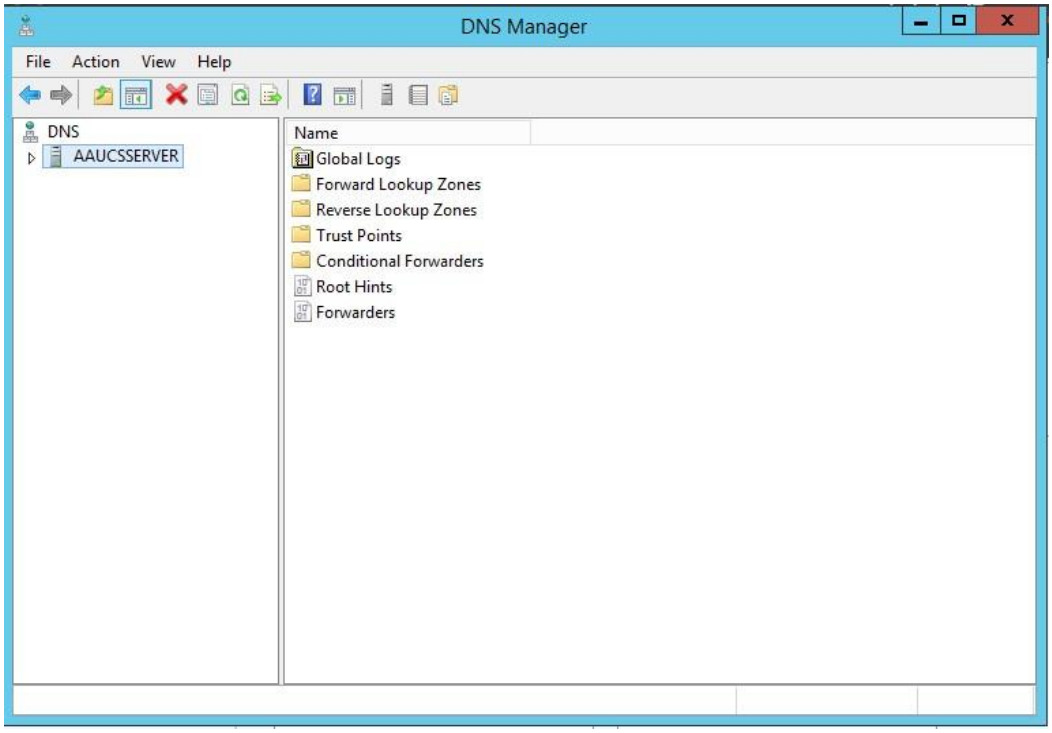
- Within **Server Manager**, to configure the DNS Server,
- click the **Tools** menu and select **DNS**. This brings up the DNS Manager window.



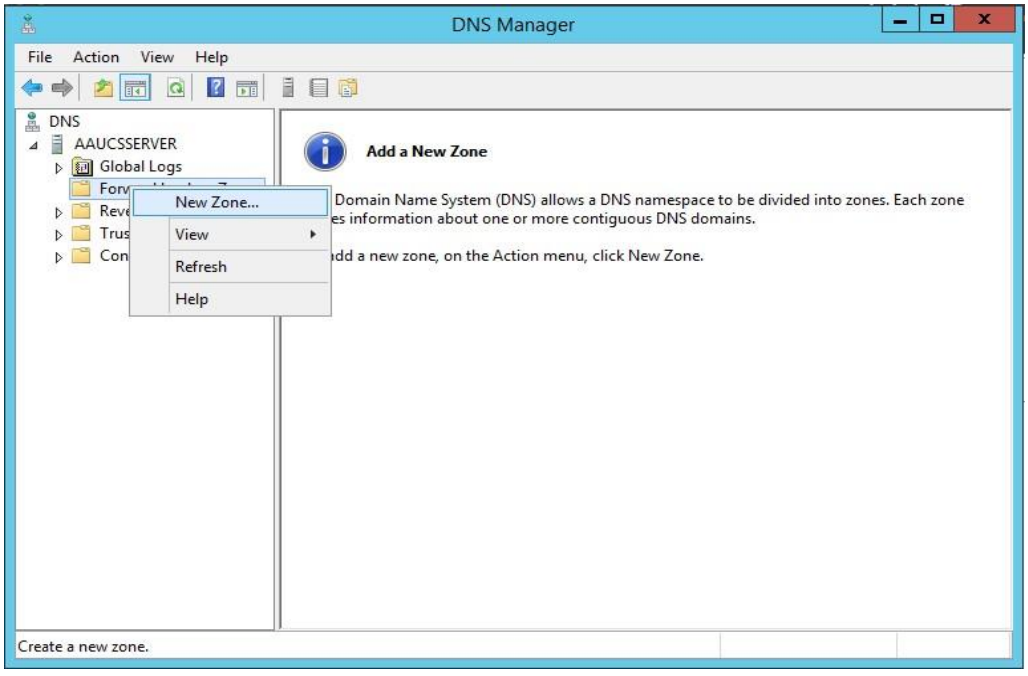

The "**DNS Manager**" window looks like as shown below




- Select your server on the left side of DNS Manager Window to open zone list.



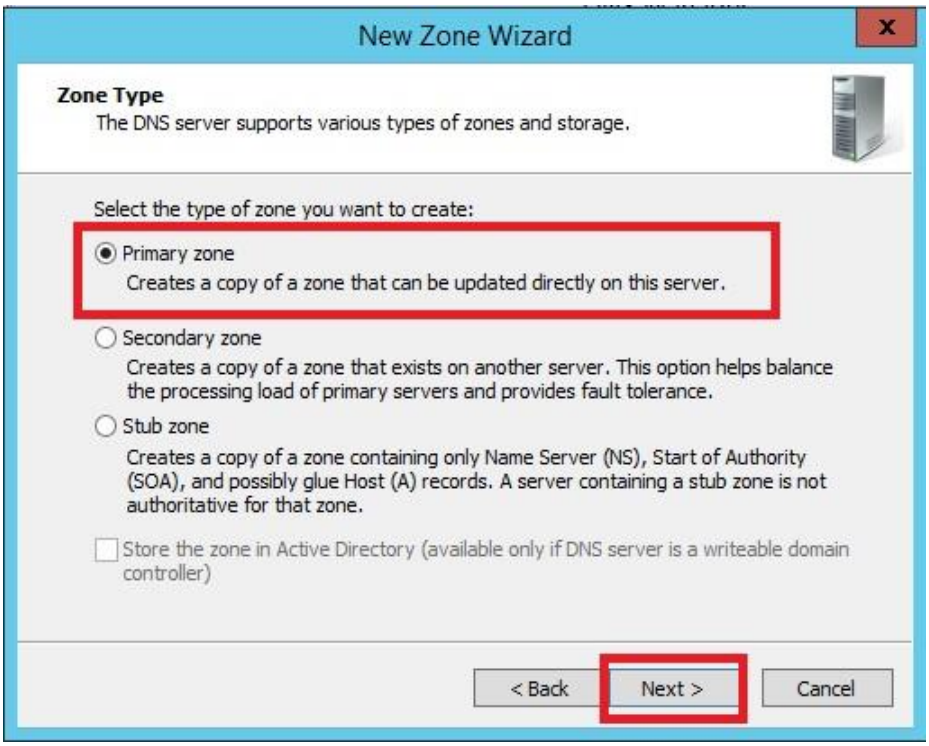

- Right click on **Forward Lookup Zones** and click on **New Zone** from context menu to bring up the **New Zone Wizard**.



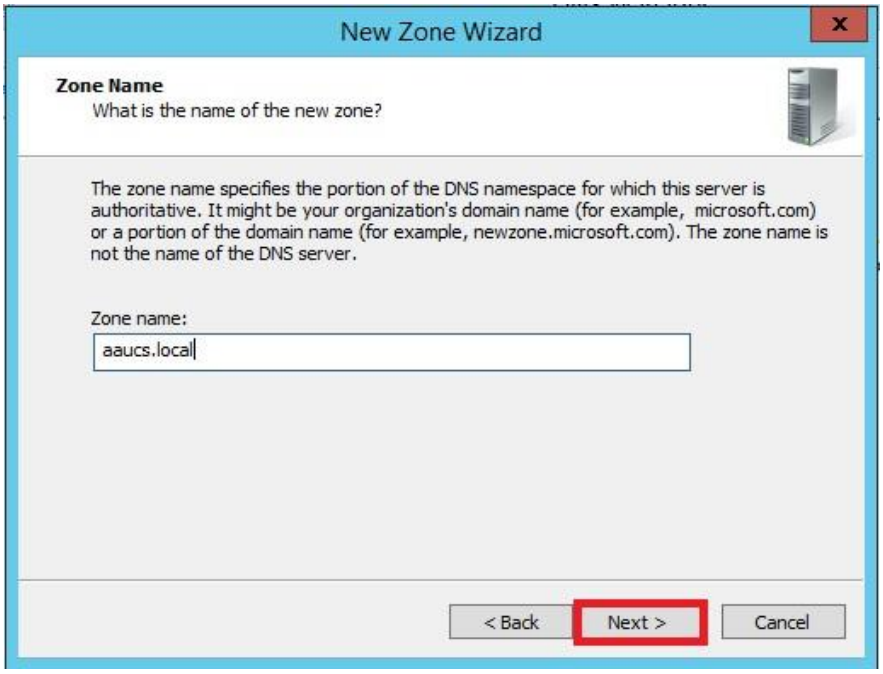
A **forward lookup zone** is used for DNS clients to obtain such information as Internet Protocol (IP) addresses that correspond to DNS domain names or services that is stored in the zone.

- In the next window click **Next**.


- In the next step you can select the type of DNS you want to use. The primary zone will be located on your server; the secondary zone will be located on another server. The secondary zone is used in large networks for load balancing. Choose **Primary zone** and click on **Next** to continue.



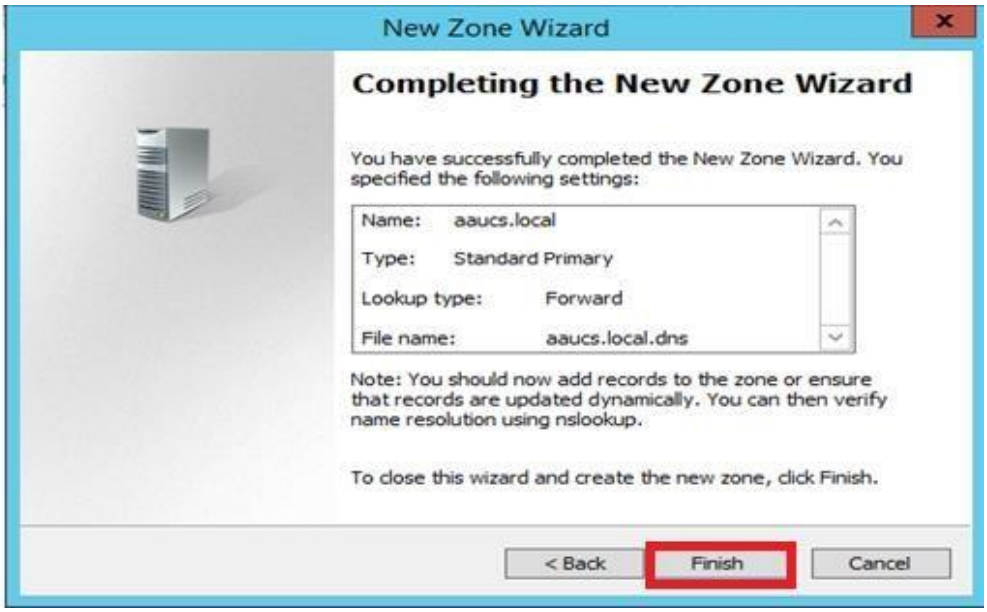

- Enter a name for the new zone and click on **Next** button.



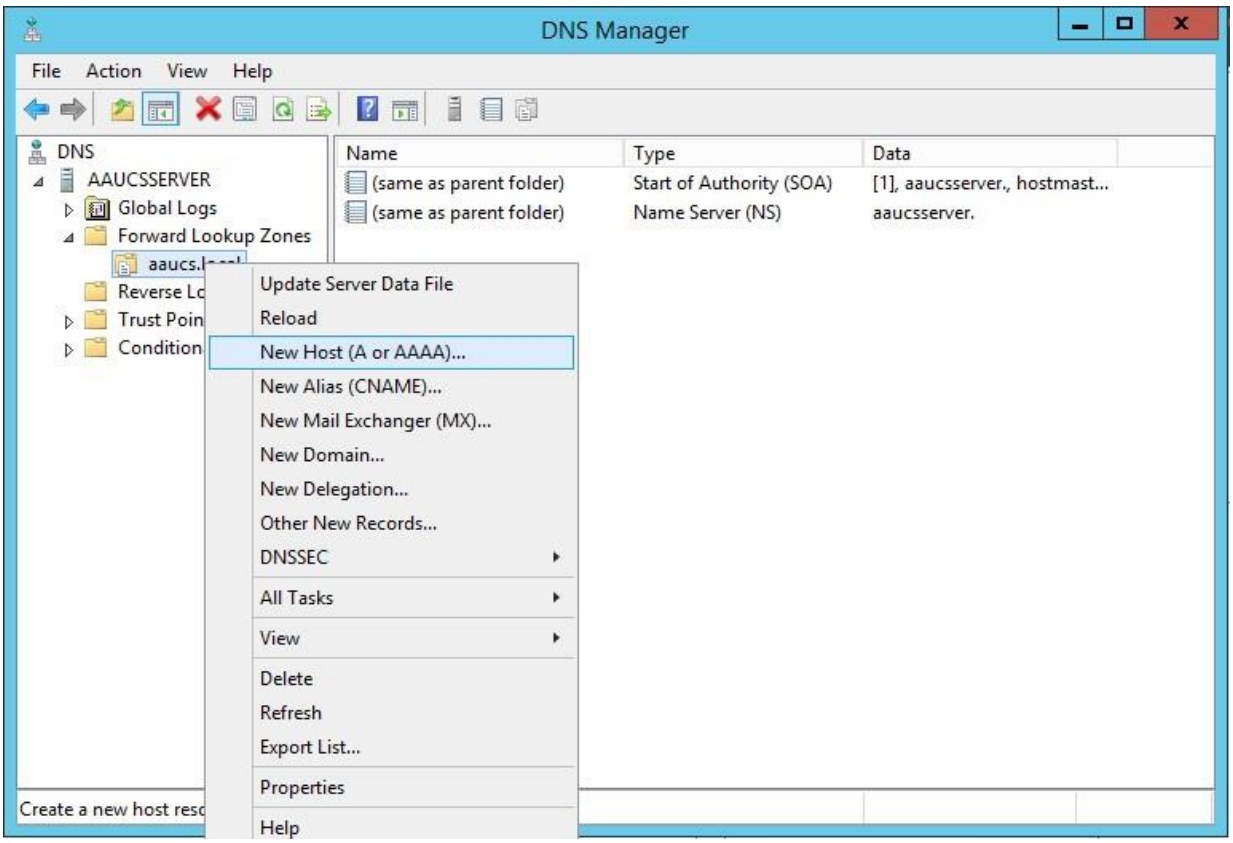

- Enter the new zone file name and click **Next**.


- Select "**don't allow dynamic updates**", Dynamic updates allows to DNS clients to register their resource records in DNS database automatically, but if the network is small we can make updates of DNS database manually.

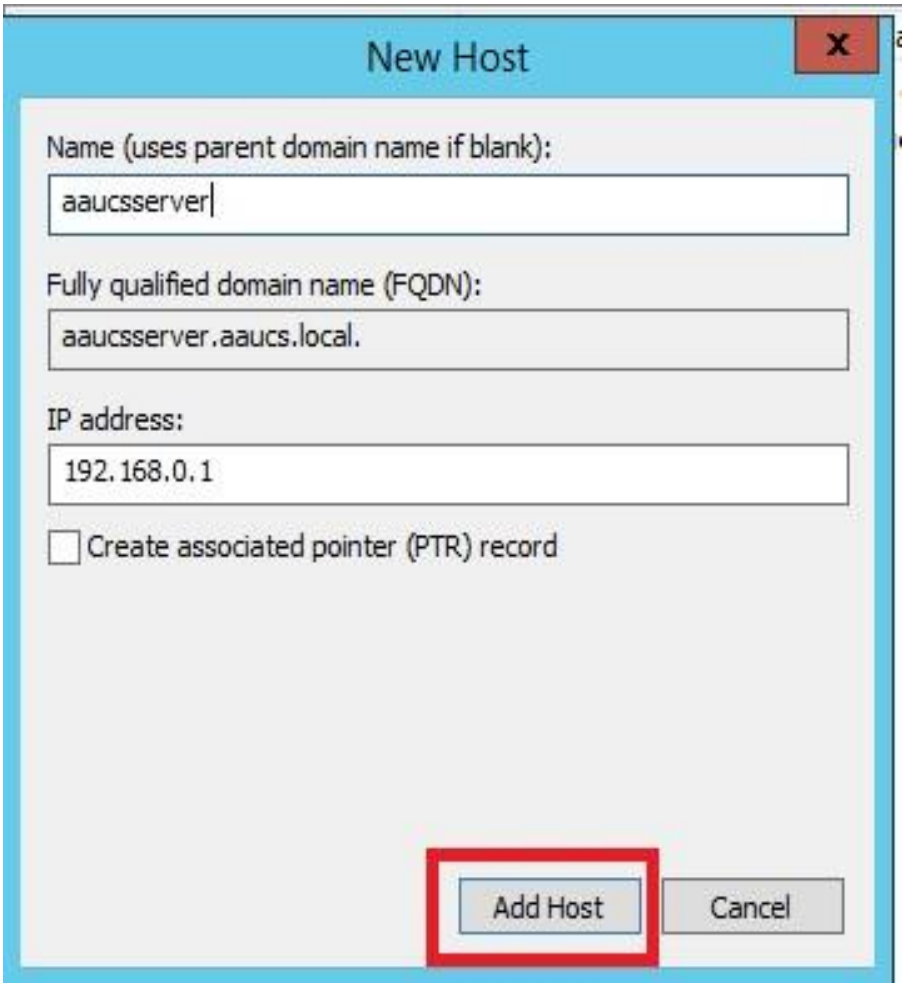

- Next click on **Finish**

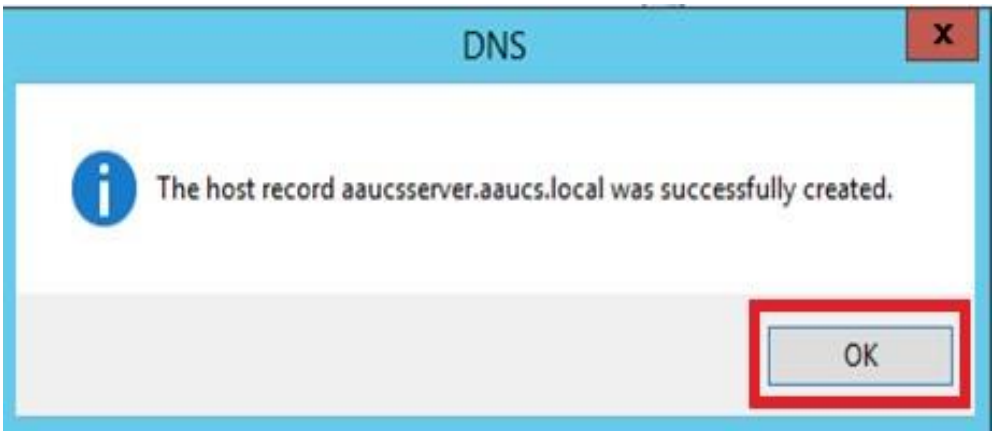



- In earlier step we have chosen "**Do not to allow dynamic updates**"; so we should add records to zone manually. First, add record of the server itself. To do this right click on zone name and click on **New Host (A or AAAA)**.

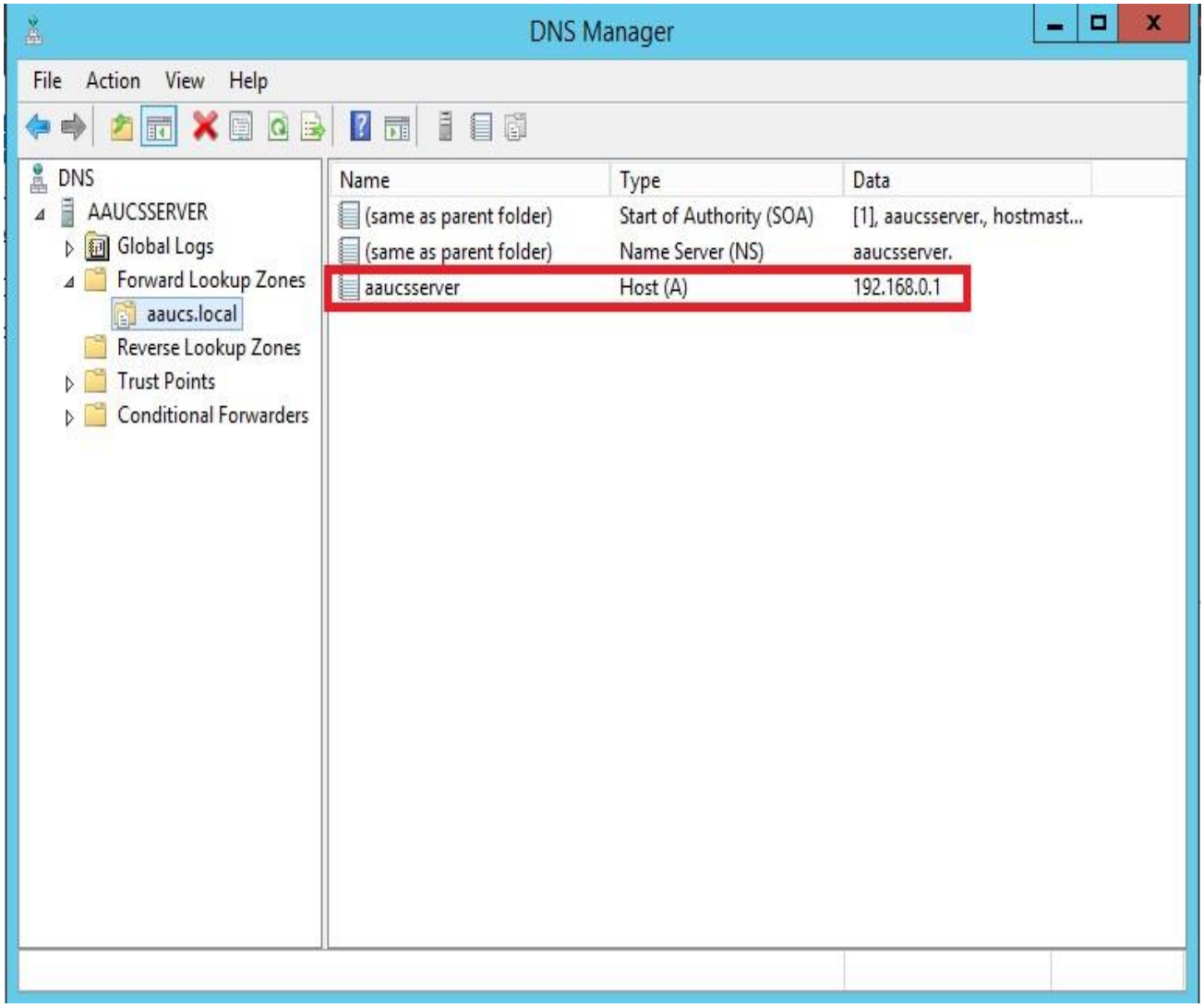


- Then the enter name and IP-address of the DNS Server in appropriate fields and then click **Add Host**.

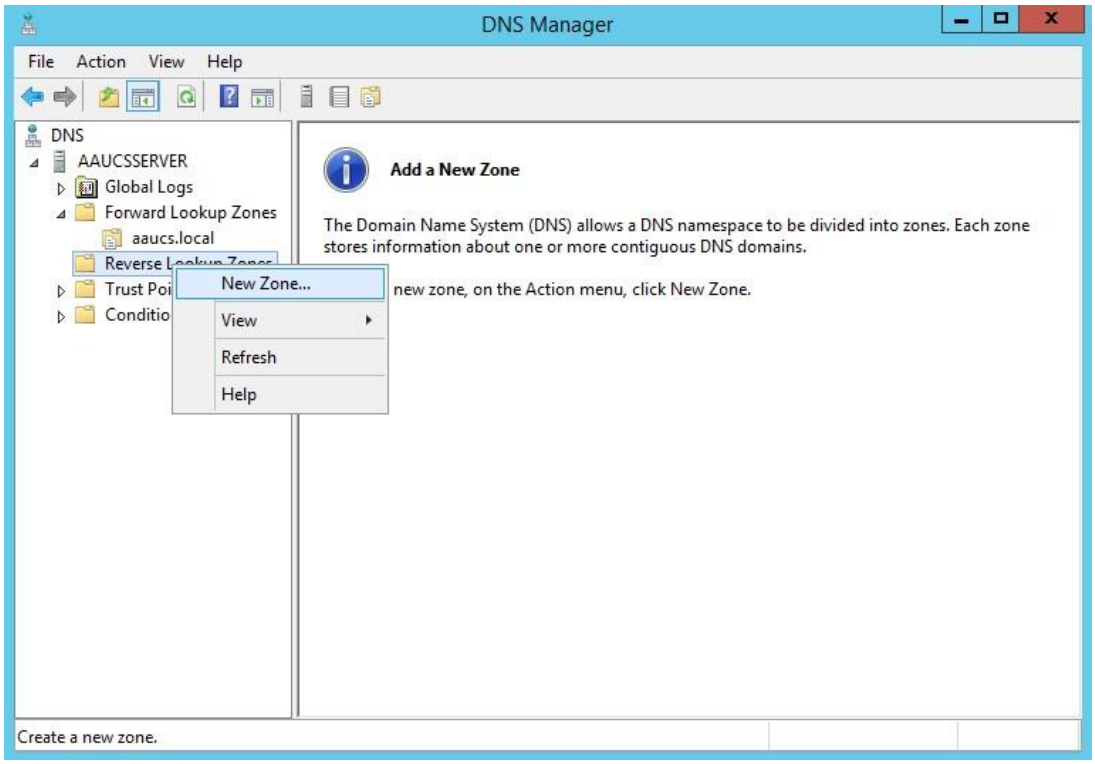


- As you can see on the right side of the DNS Manager window, the new host is now created and it's possible to create records for client computers in exactly the same way.



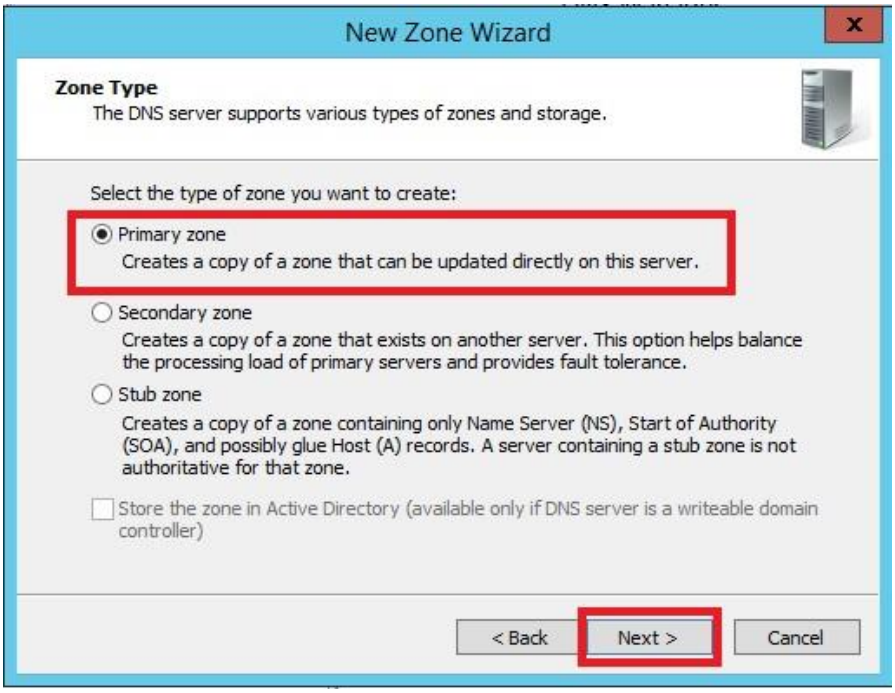

- Next we have to add **Reverse Lookup Zone**. To do this right click on **Reverse Lookup Zone** and click on **New Zone** to bring up the New Zone Wizard.


DNS Manager
File Action View Help
DNS
AAUCSSERVER
Global Logs
Forward Lookup Zones
aaucs.local
Reverse Lookup Zones
Trust Poi
Conditio
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
new zone, on the Action menu, click New Zone.
Create a new zone.

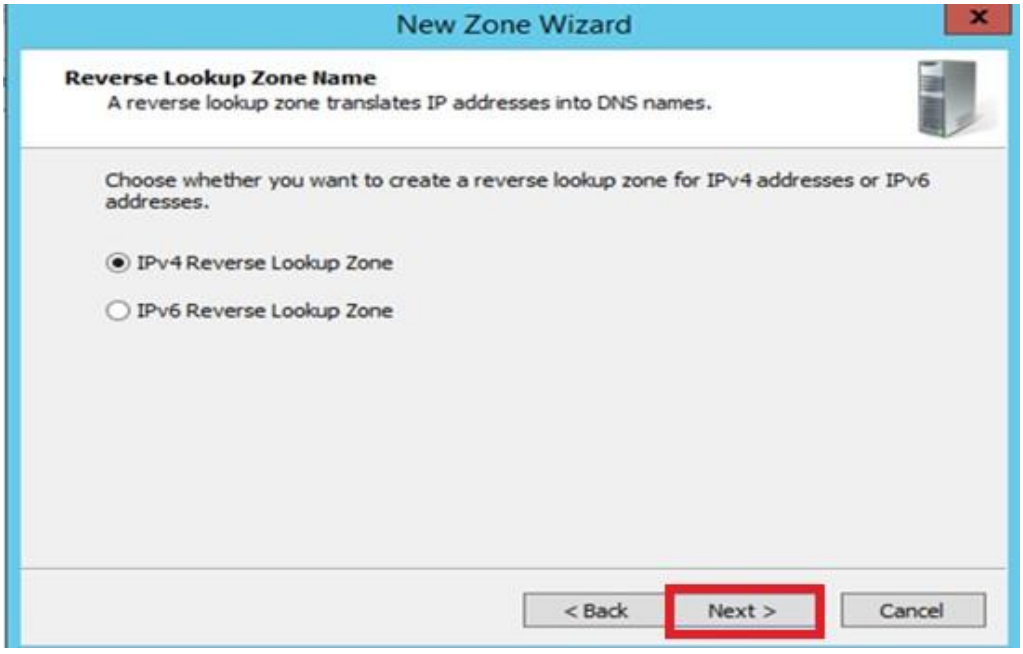

New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel

✓ **Reverse lookup zone** provides mapping from Internet Protocol (IP) addresses back to DNS domain names.

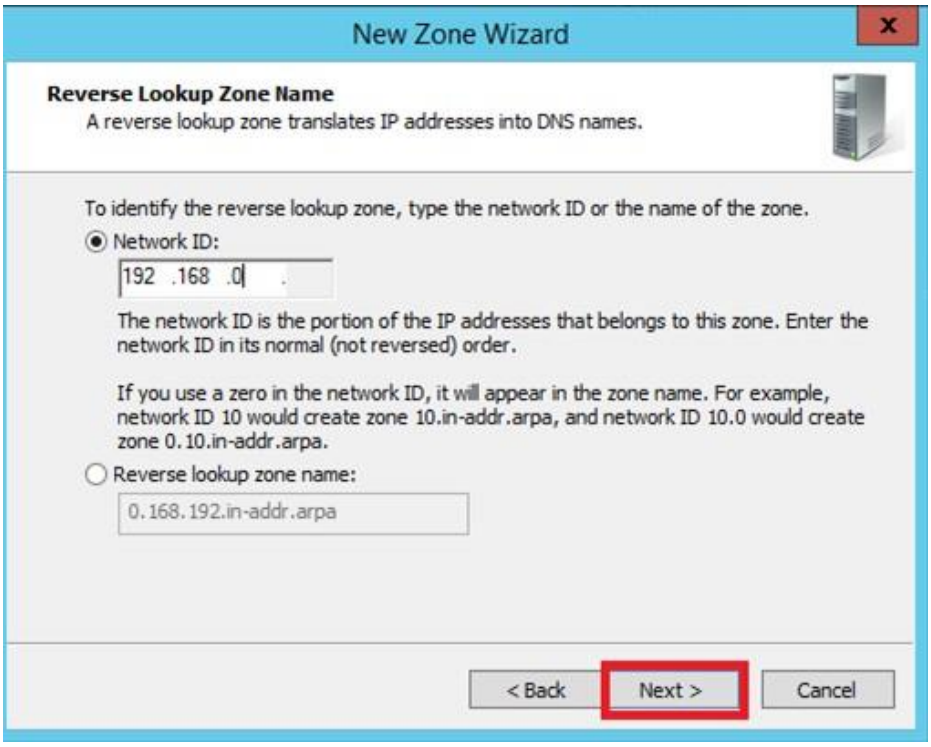
➢ Choose **Primary zone** and click on **Next** to continue.




➢ Select the type of IP-address, check on **IPv4** and click on **Next** to continue.




➢ In **Network ID** field enter the first three octets of your DNS Server IP address.

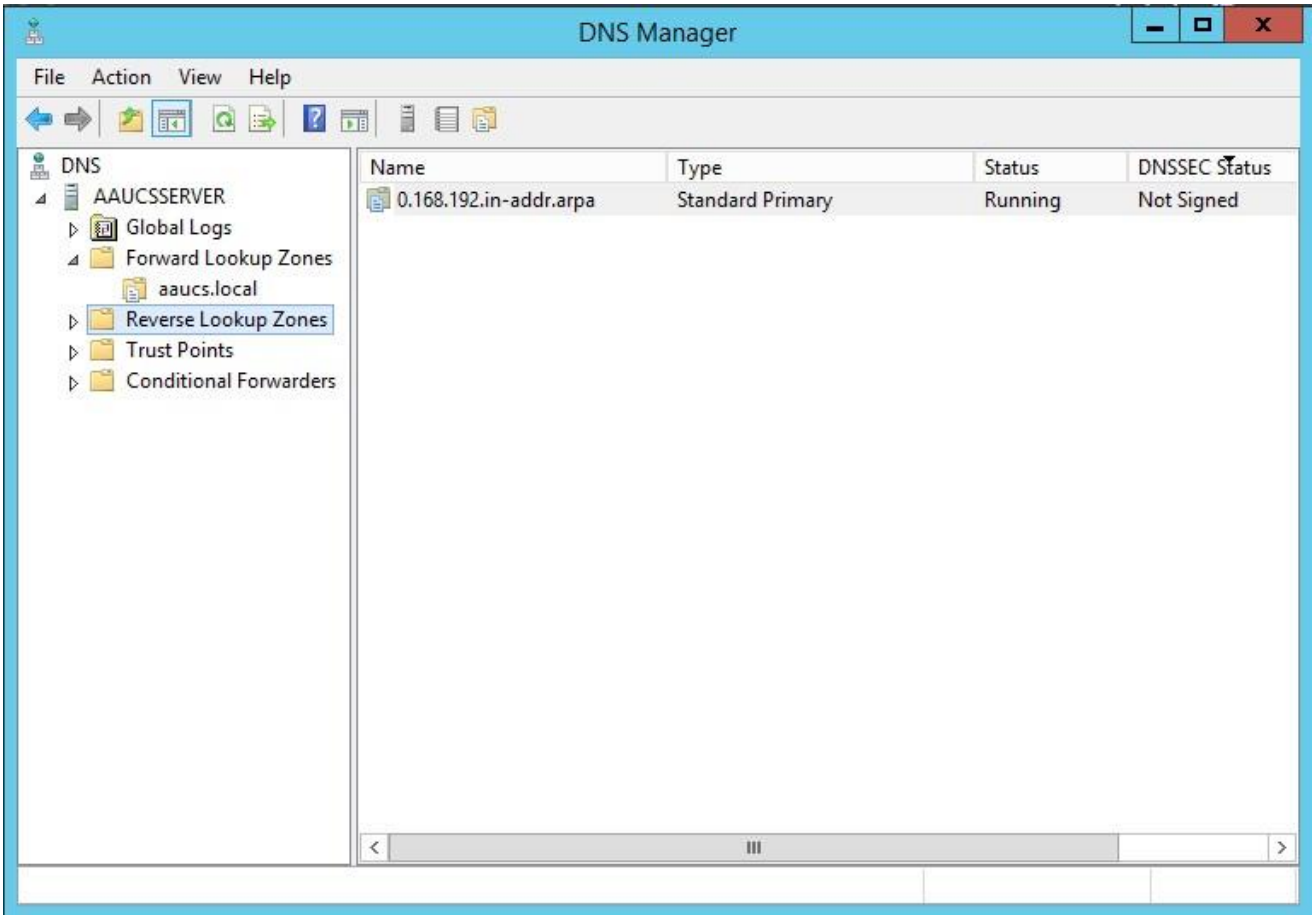



- Just click on **Next**.

- Check "**Do not allow dynamic updates"** and press **Next**.


- Click on **Finish** button and the DNS server is now configured and ready for use.


As you can see on the right side of DNS Manager Window, **Reverse Lookup Zone** is now created.




### 8.3.1 Nslookup

Nslookup is a command line driven utility supplied as part of most Windows operating systems that can reveal information related to domain names and the Internet Protocol (IP) addresses associated with them.

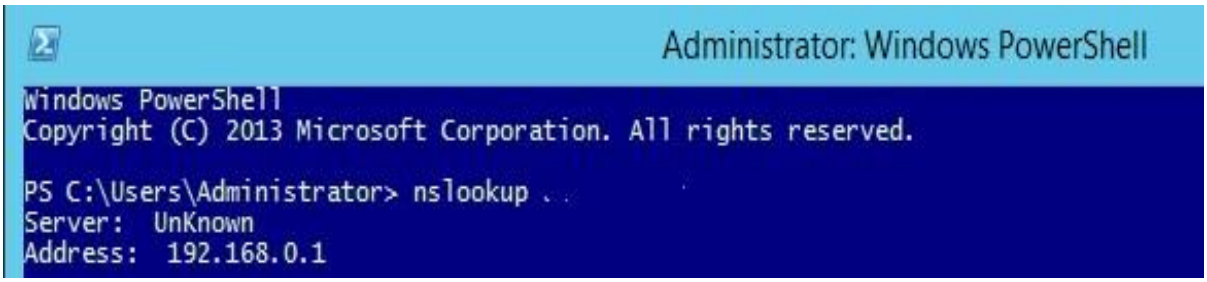
Open your **Administrator: windows PowerShell** on your server or **CMD** on your windows client machine and type Nslookup command.

**c:\nslookup (Press enter)**

**Default Server: aaucsserver.aaucs.local (The default DNS Server)**

**Address: 192.168.0.1 (IP address of the default DNS Server)**

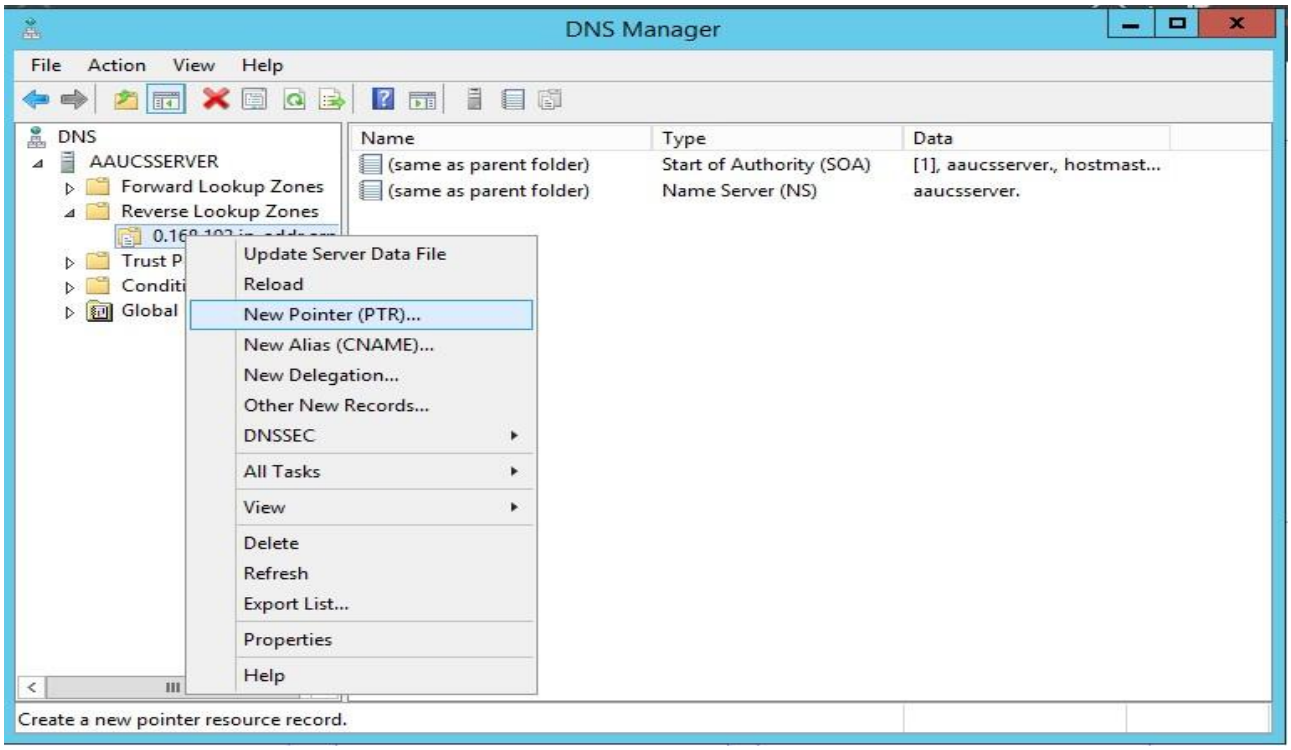
Here for the first time when we are trying to run **Nslookup** command on **powershell** our server name will be definitely expressed as an unknown.




The reason for this is the DNS server does not possess a record for the server itself. Or simply it does not know what its own name is. By creating a New Pointer (PTR) static entry we can fix this and let DNS server know its own name.

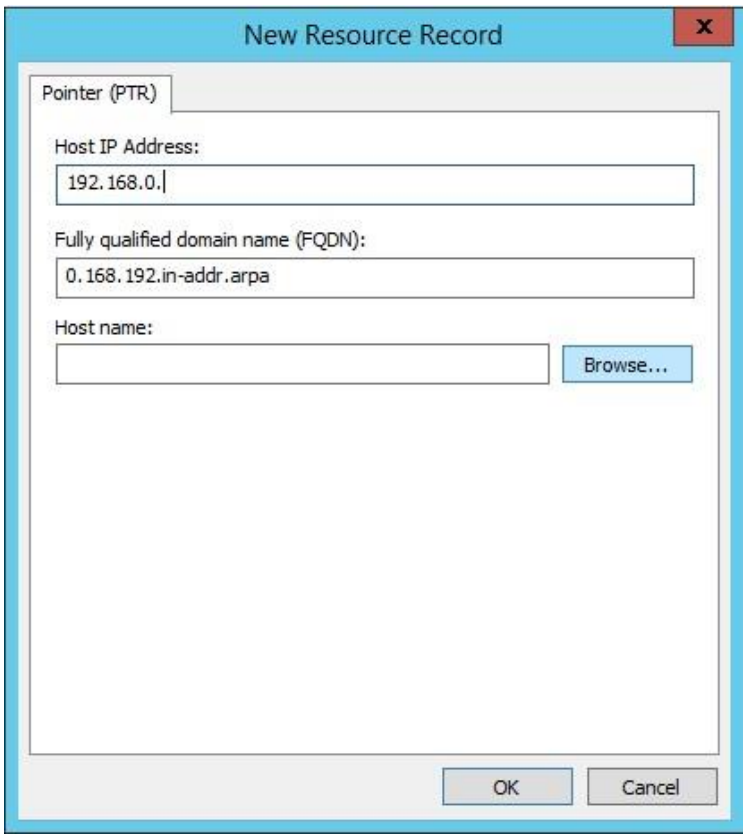
Follow the following Steps:

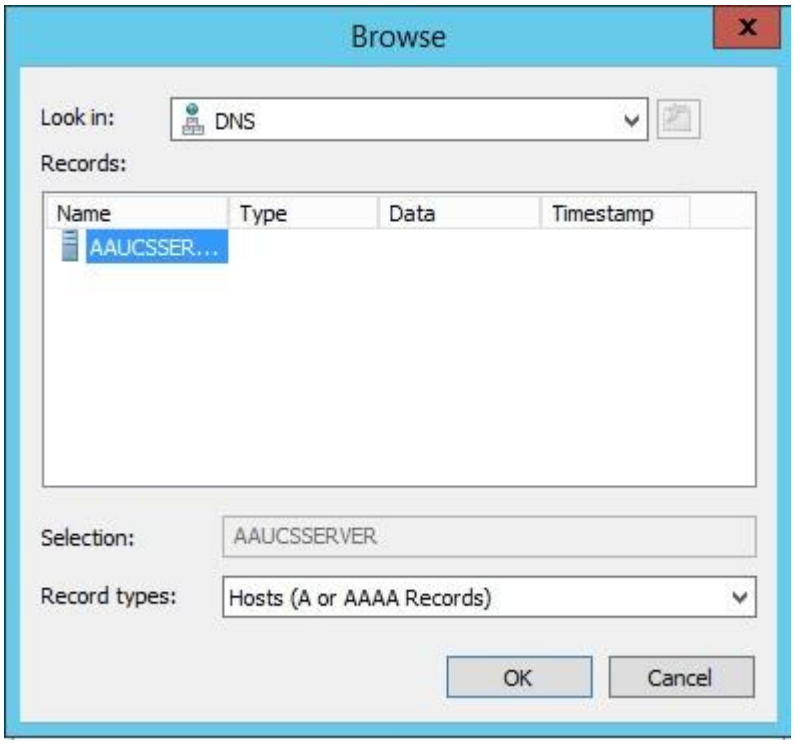
1. Open the DNS management console, go to your reverse lookup zone and right click on it and select "**New Pointer (PTR)**".

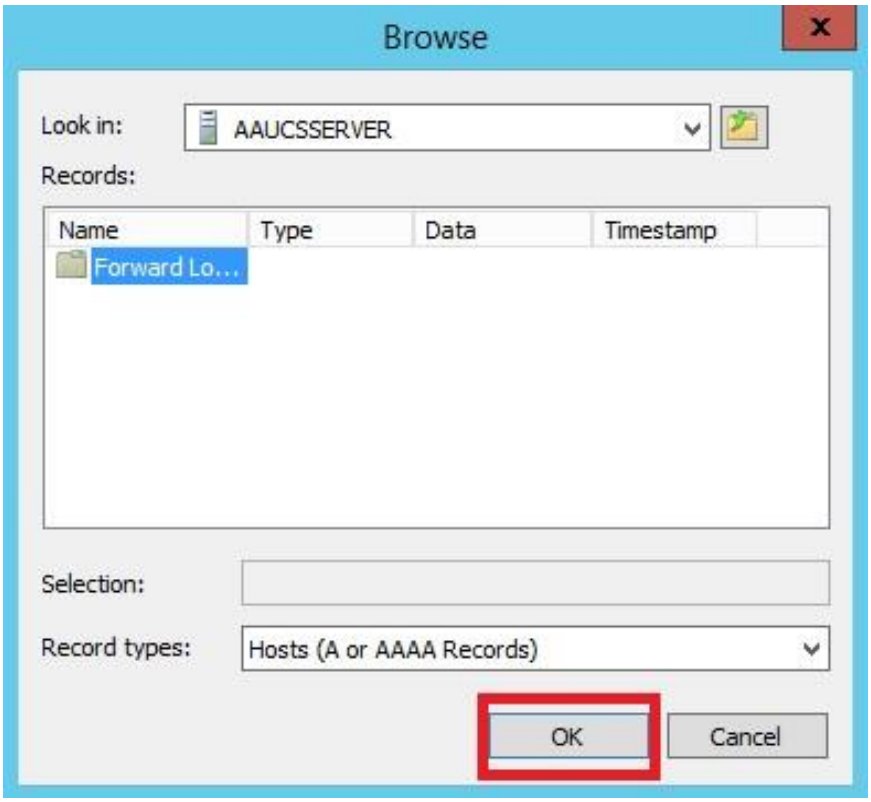


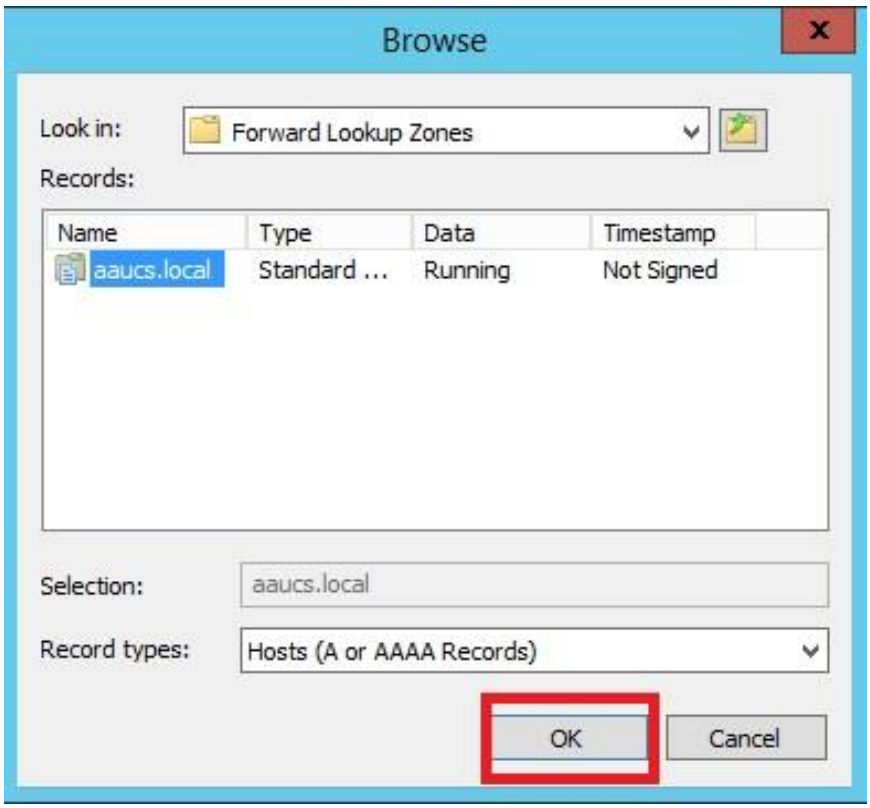

.

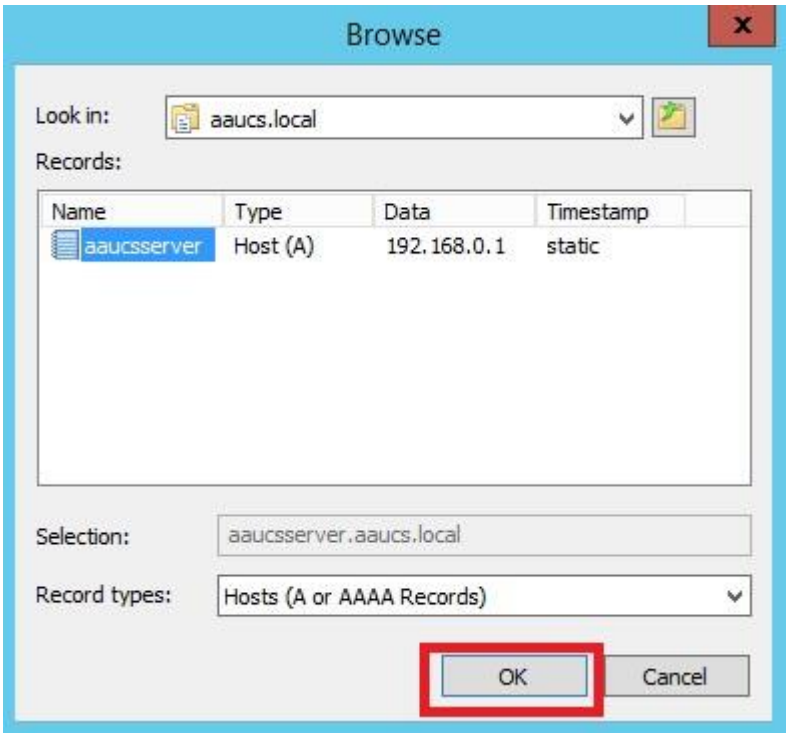
2. In the New Pointer (PTR) window enter the **IP address** of DNS server and click **Browse** button to select the **host name** of the server

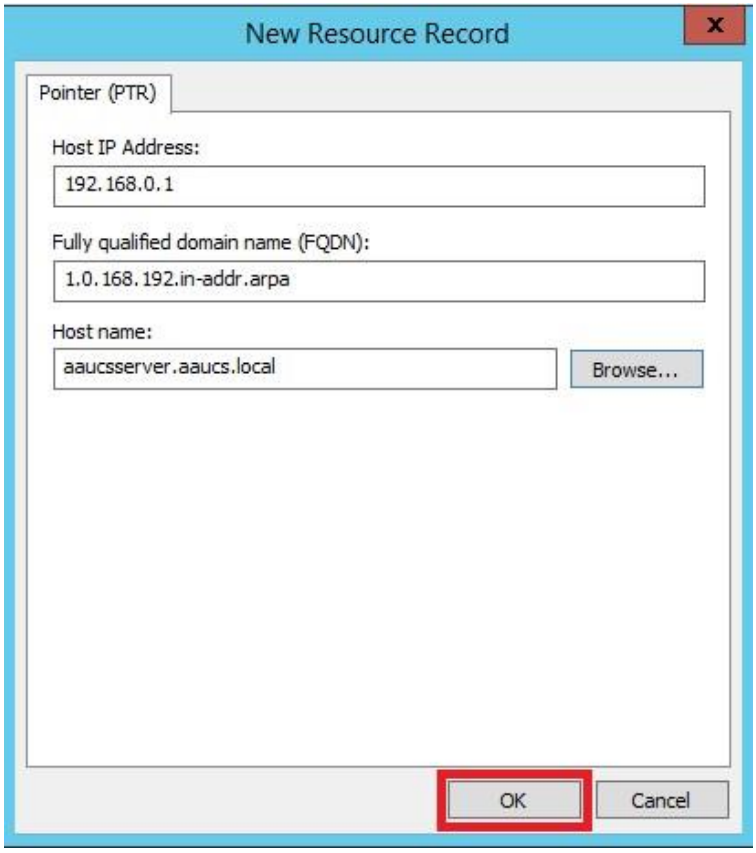

New Resource Record
Pointer (PTR)
Host IP Address:
192.168.0.
Fully qualified domain name (FQDN):
0.168.192.in-addr.arpa
Host name:
Browse...
OK
Cancel


Browse
Look in:
DNS
Records:
Name
Type
Data
Timestamp
AAUCSSER...
Selection:
AAUCSSERVER
Record types:
Hosts (A or AAAA Records)
OK
Cancel

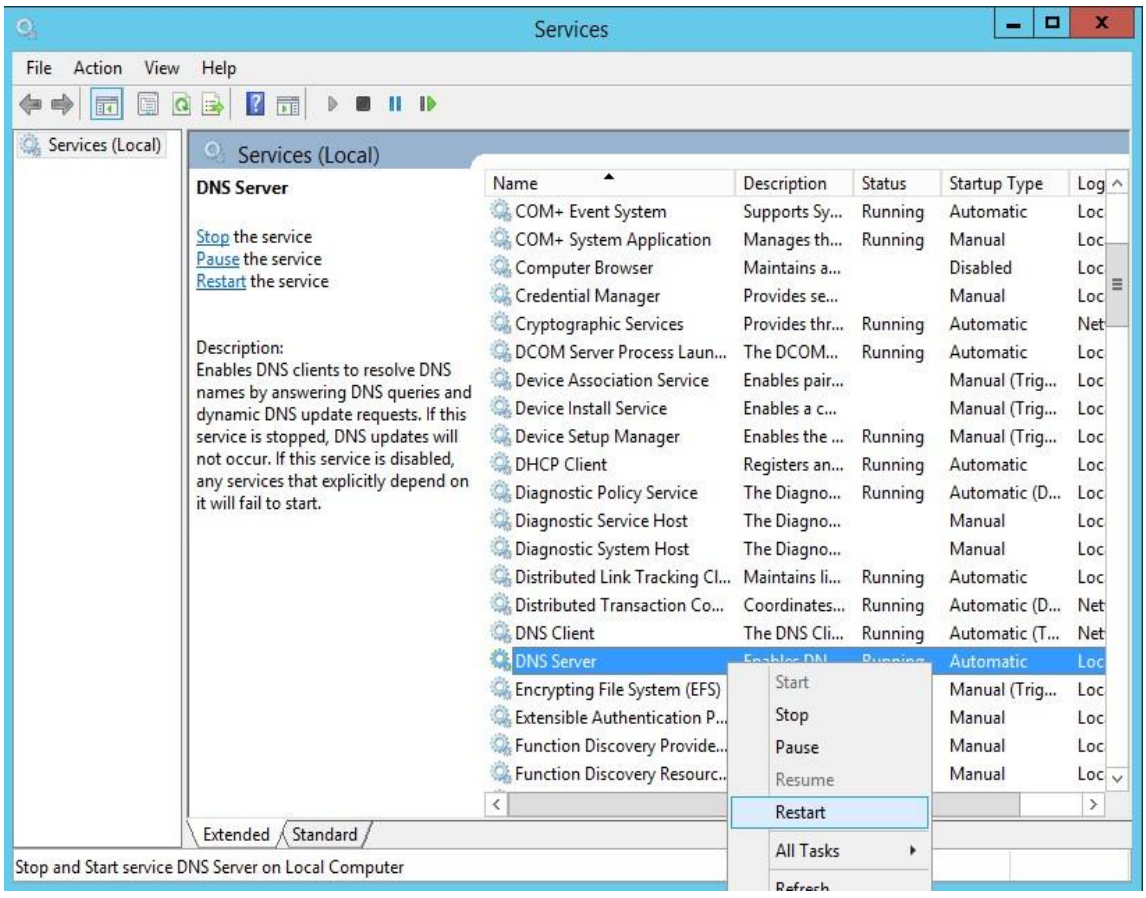

Browse
Look in:
AAUCSSERVER
Records:
Name
Type
Data
Timestamp
Forward Lo...
Selection:
Record types:
Hosts (A or AAAA Records)
OK
Cancel


Browse
Look in:
Forward Lookup Zones
Records:
Name
Type
Data
Timestamp
aaucs.local
Standard ...
Running
Not Signed
Selection:
aaucs.local
Record types:
Hosts (A or AAAA Records)
OK
Cancel


Browse
Look in:
aaucs.local
Records:
Name
Type
Data
Timestamp
aaucsserver
Host (A)
192.168.0.1
static
Selection:
aaucsserver.aaucs.local
Record types:
Hosts (A or AAAA Records)
OK
Cancel


New Resource Record
Pointer (PTR)
Host IP Address:
192.168.0.1
Fully qualified domain name (FQDN):
1.0.168.192.in-addr.arpa
Host name:
aaucsserver.aaucs.local
Browse...
OK
Cancel

3. Finally, go to Server Manager **Tools** menu and select **Services** option and find the **DNS Server** service and right click on it and select **Restart**.

➢ Now let's run the **Nslookup** command on our server machine **Administrator: Windows PowerShell** to check our DNS server able to know its own server name.


As you can see in the above figure our **Default Server** is recognized by the DNS server as **aaucsserver.aaucs.local** (which is the name of the DNS server), so that we have successfully installed The DNS Server on our windows server 2012 R2.

# Chapter Nine: Active Directory

## 9.1 Introduction

Active directory is a centralized and standardized system that automates network management of user data, security, and distributed resources; Enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

Active Directory features:

- Support for the **X.500** standard for global directories.
- The capability for secure extension of network operations to the Web.
- A hierarchical organization that provides a single point of access for system administration. (Management of user accounts, clients, servers, and applications, for example) to reduce redundancy and errors.
- An object-oriented storage organization, which allows easier access to information.
- Support for the Lightweight Directory Access Protocol (**LDAP**) to enable inter-directory operability.

➢ **X.500** Directory Service is a standard way to develop an electronic directory of people in an organization so that it can be part of a global directory available to anyone in the world with Internet access. Such a directory is sometimes called a global White Pages directory. The idea is to be able to look up people in a user-friendly way by name, department, or organization.

➢ **LDAP** (**Lightweight Directory Access Protocol**) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

## 9.2 Active Directory Domain (AD Domain)

An Active Directory domain is a collection of objects within a Microsoft Active Directory network. An object can be a single user or a group or it can be a hardware component, such as a computer or printer. Each domain holds a database containing object identity information.

Active Directory domains are grouped in a tree structure; a group of Active Directory trees is known as a **forest**, which is the highest level of organization within Active Directory. Active Directory

domains can have multiple child domains, which in turn can have their own child domains. Authentication within Active Directory works through a transitive trust relationship.

Active Directory domains can be identified using a DNS name, which can be the same as an organization's public domain name, a sub-domain or an alternate version (which may end in **.local**). While Group Policy can be applied to an entire domain, it is typical to apply policies to subgroups of objects known as organizational units (OUs). All object attributes, such as usernames, must be unique within a single domain and, by extension, an OU.

### 9.2.1 Microsoft Active Directory Domain Services (AD DS)

Active Directory Domain Services (AD DS) is a server role in Active Directory that allows administrators to manage and store information about resources from a network, as well as application data, in a distributed database. AD DS can also help Administrators manage a network's elements (computers and end users) and reorder them into a custom hierarchy.

The structure of the hierarchy includes an Active Directory forest, the forest's domains and organizational units in those domains. AD DS integrates security by authenticating logons and controlling who has access to directory resources.

- An **Active Directory forest** is the highest level of organization within Active Directory. Each forest shares a single database, a single global address list and a security boundary. By default, a user or administrator in one forest cannot access another forest.
- An **organizational unit** (OU) is a container within a Microsoft Active Directory domain which can hold users, groups and computers. It is the smallest unit to which an administrator can assign Group Policy settings or account permissions. An organizational unit can have multiple OUs within it, but all attributes within the containing OU must be unique. Active Directory organizational units cannot contain objects from other domains.

### 9.2.2 Installation of Active Directory Domain Services role

**Requirements**:

Minimum: 1.4 GHz 64-bit processor

Minimum: 512 MB RAM

Minimum: 32 GB or greater

Active directory Domain Name service installation in Windows Server 2012 is divided into the following two parts:

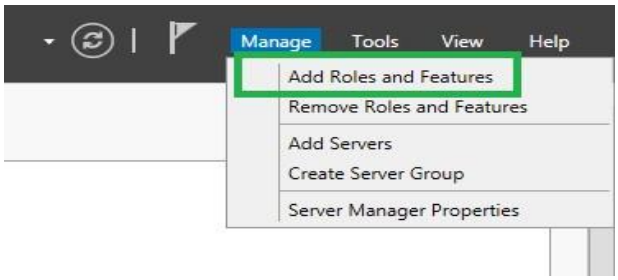
1. Install Active directory Domain Services

2. Promote server as Domain controller

➢ Install Active Directory Domain Service

1. Add Roles and Features

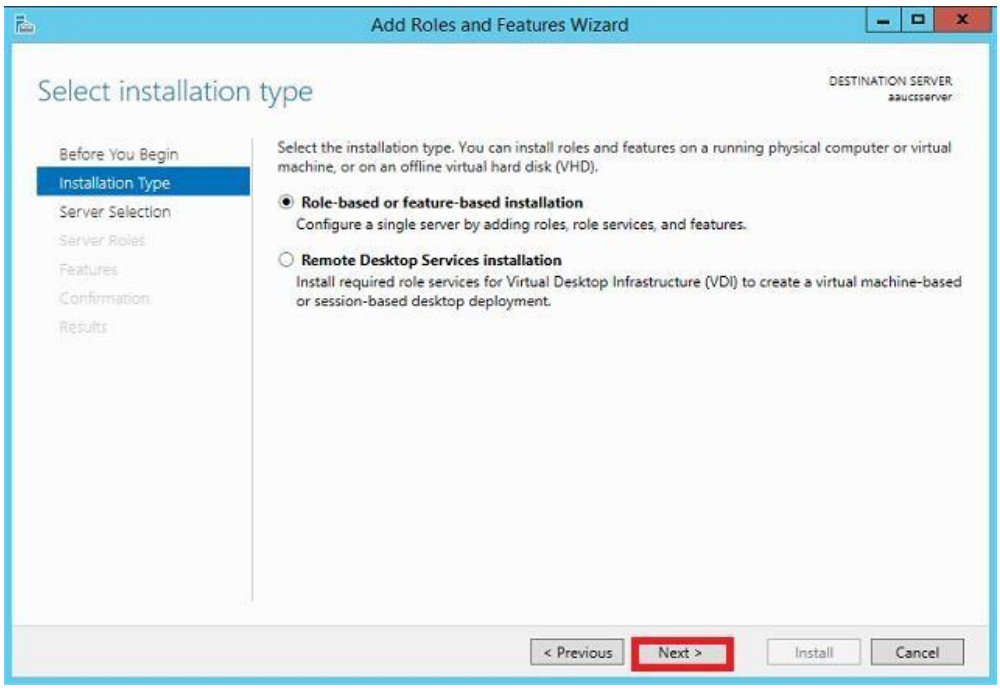
➢ First, Open **server manager**-> Select Add roles and features from Dashboard/Mange options.




➢ Select **Next** on Add Roles and Features Wizard page.

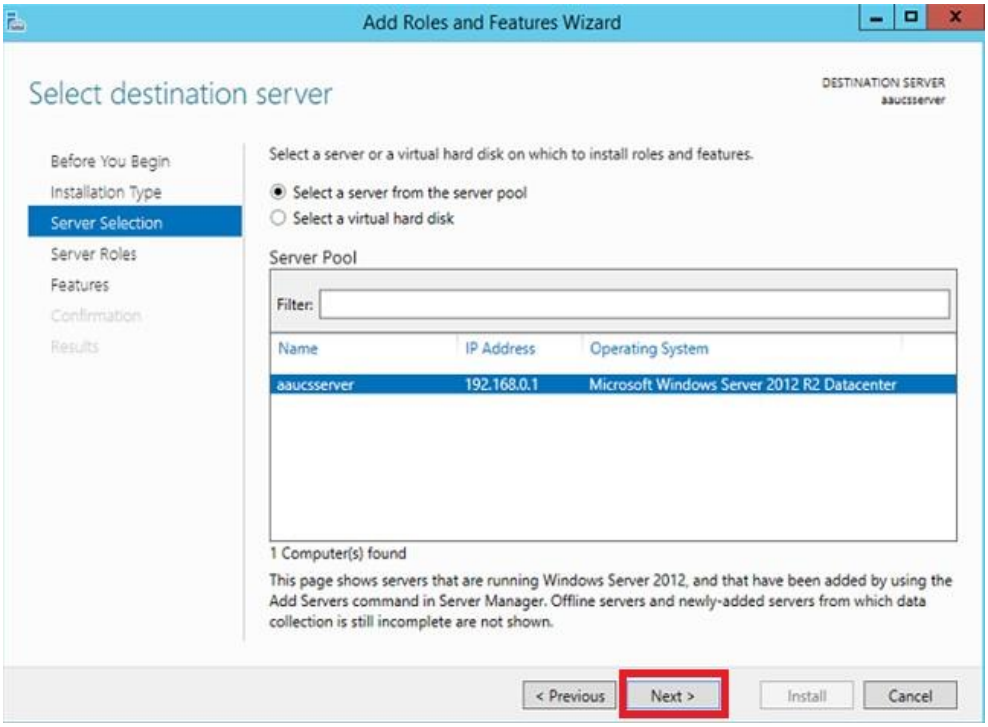
2. Installation Type

Select **Role-based or feature-based installation** option in Add Roles and Features Wizard page.

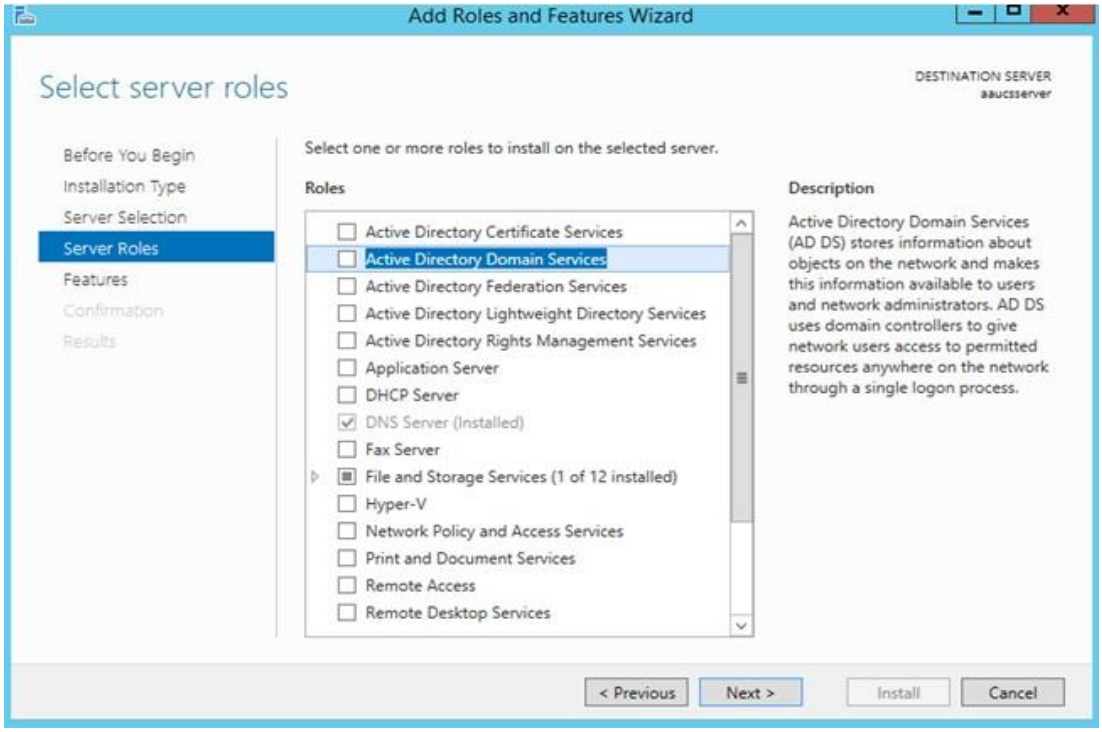



3. Select Server and Server Role

Select the server from the server pool. It will automatically show the server in the list. Typically, you'll see only your server in this list.

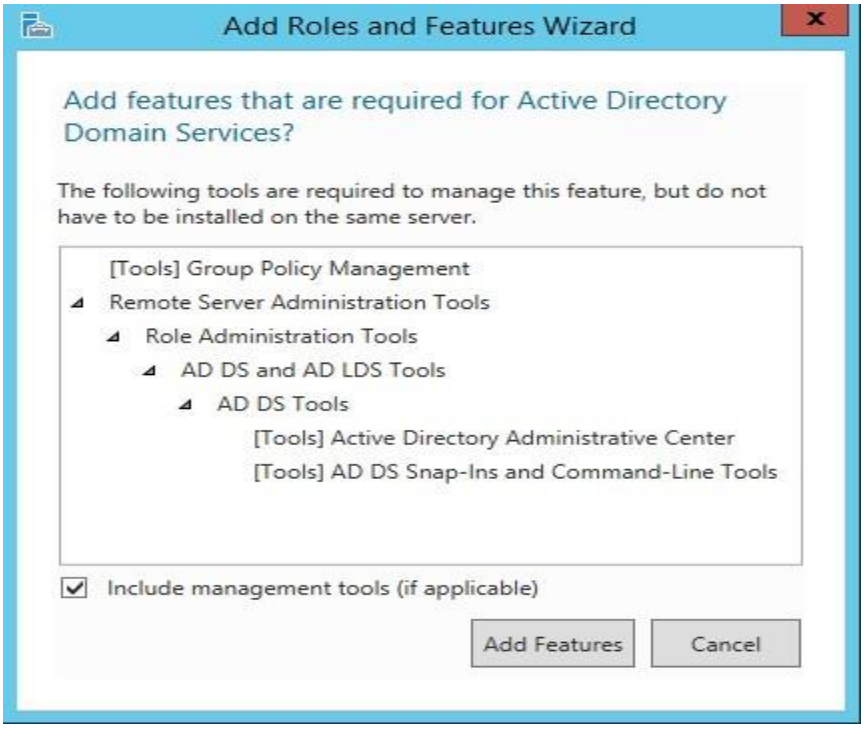


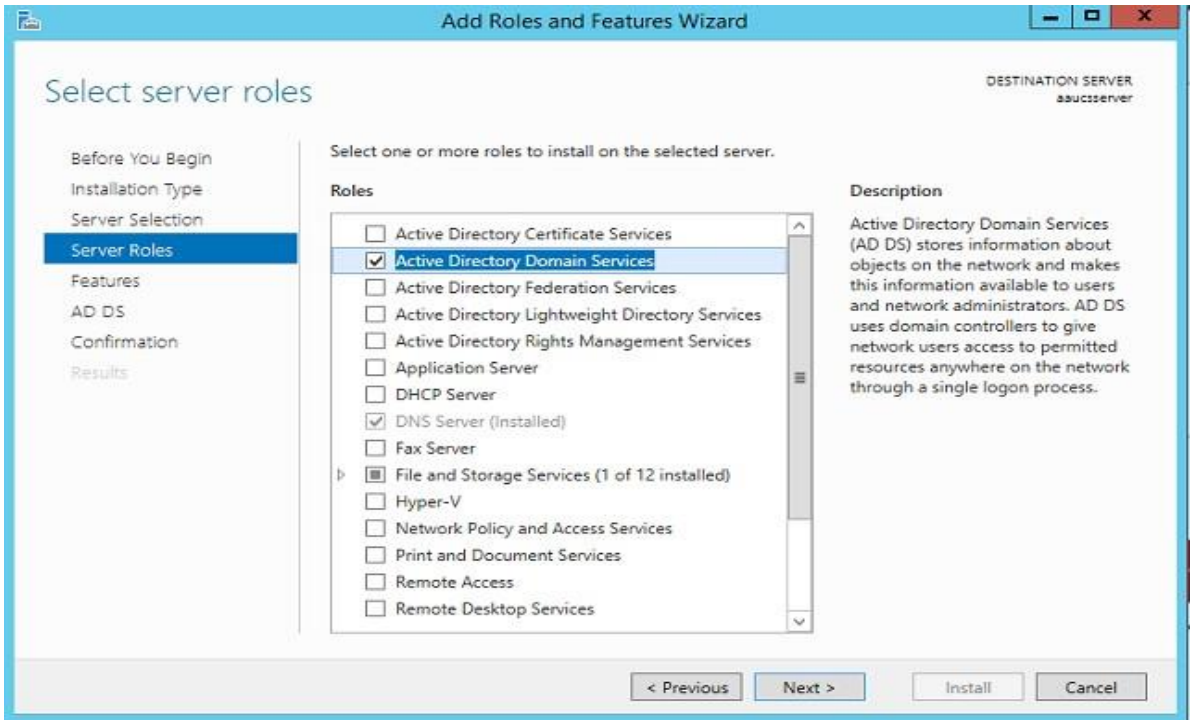

⇨ Select **Active Directory Domain services** in Role lists as shown below.



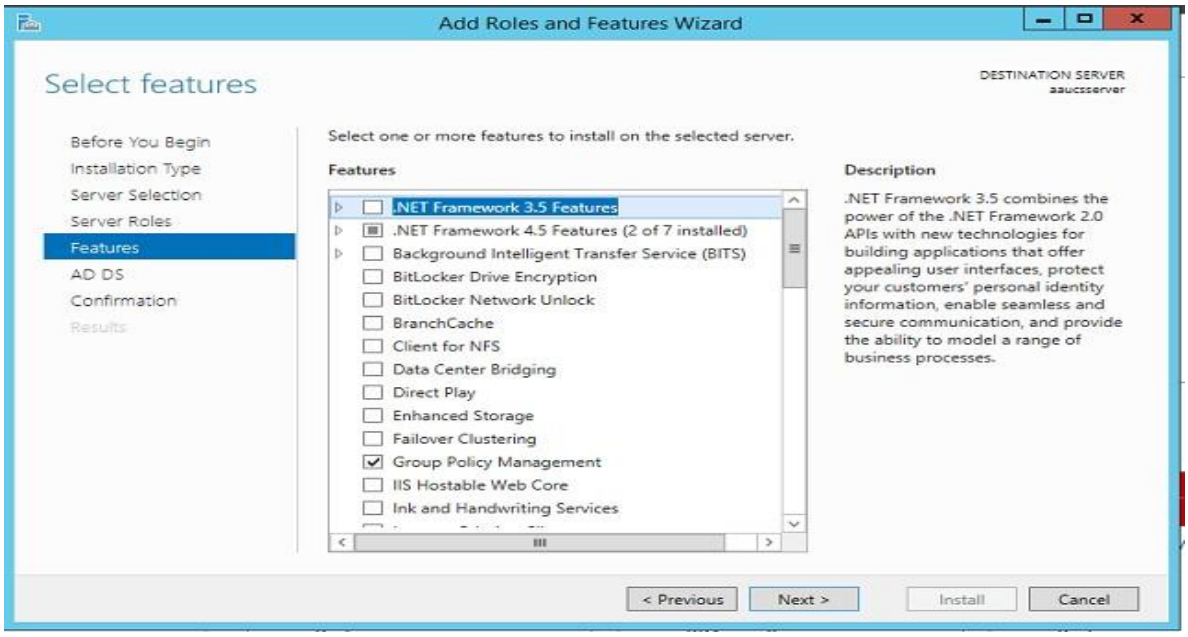
4. Add Features

After selecting Role it will pop up a window to install additional services, Choose add features from popup window.

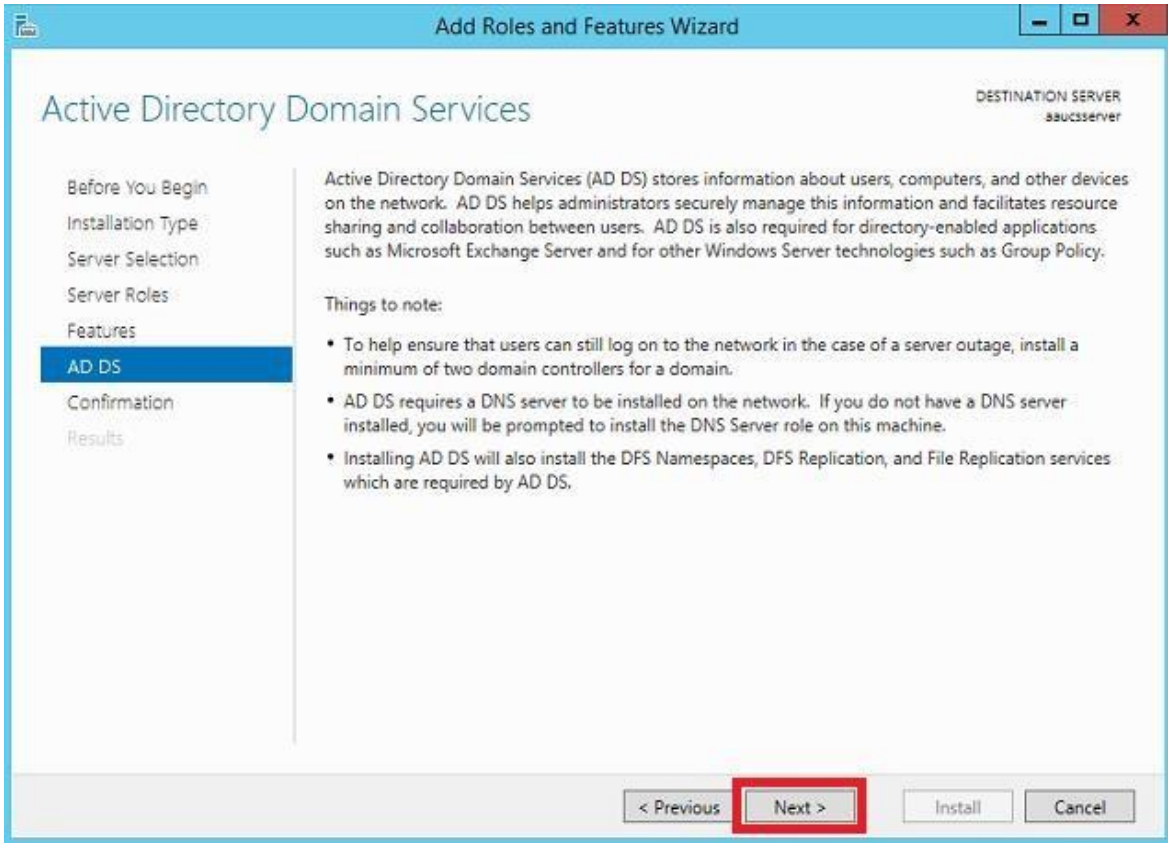


➢ If you want to install any other additional features you can select from this page.

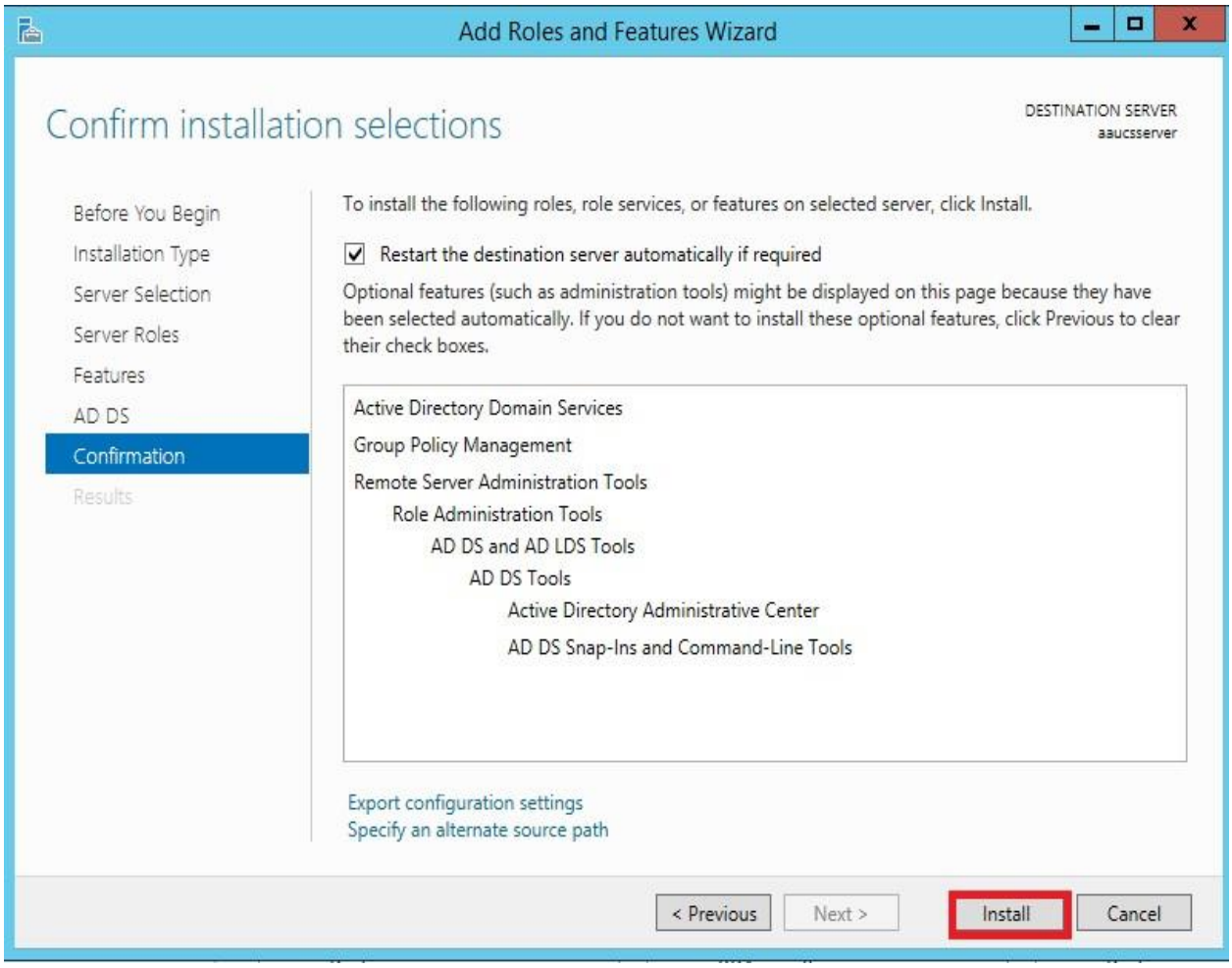



The next window is "**AD DS**" which describes about the AD DS and its functions.

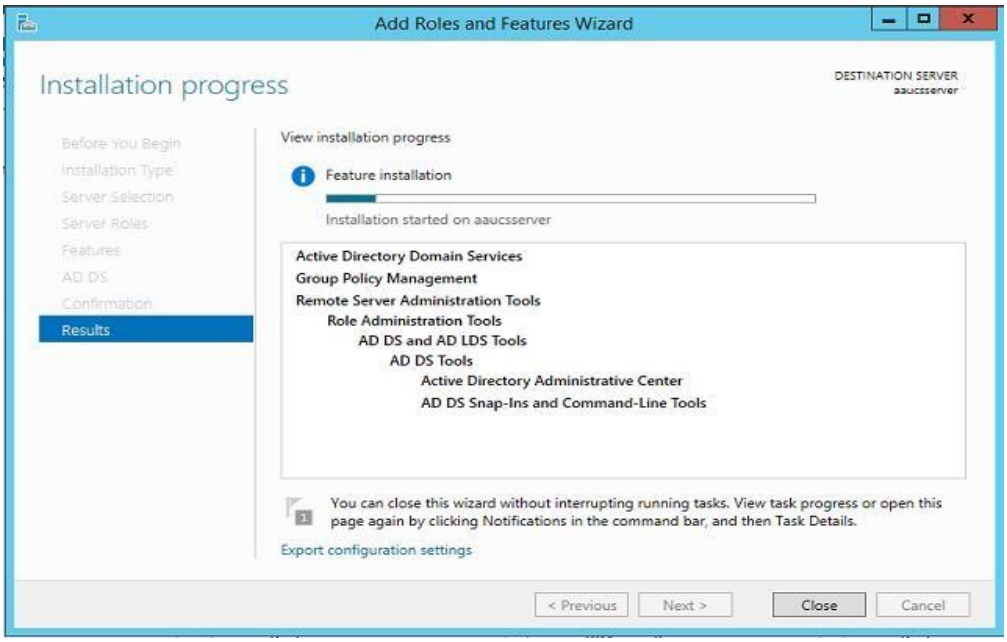


5. Installation of Active Directory Domain Name Service

- Select **Next** in Add Roles and Features Wizard page.
- Confirm the installation selections. Check the Restart check box to restart server automatically after installation and click "**Install**"



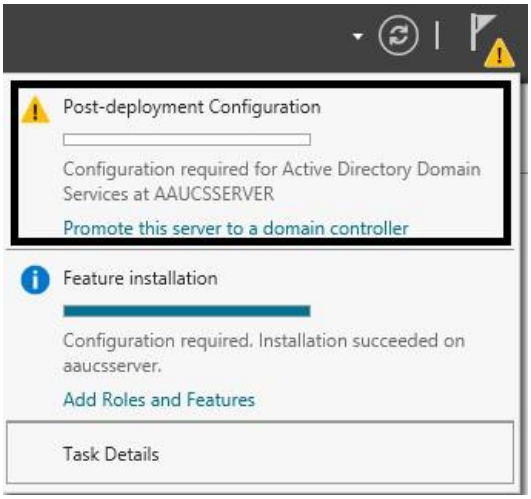

The installation starts and it takes some minutes to finish; after the installation is finished click **Close** button.




## 9.2.3 Promote the Server as a Domain Controller

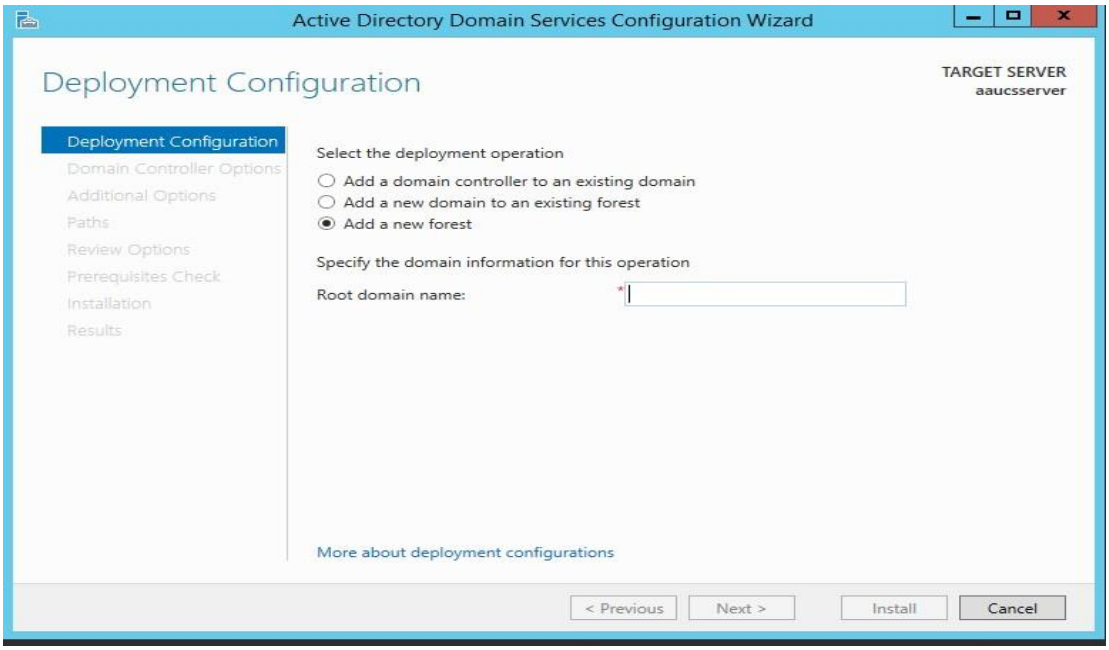
### 9.2.3.1 Server Notification to Promote

After installing Active directory services, select Promote server to a domain controller from the server manager notification page.

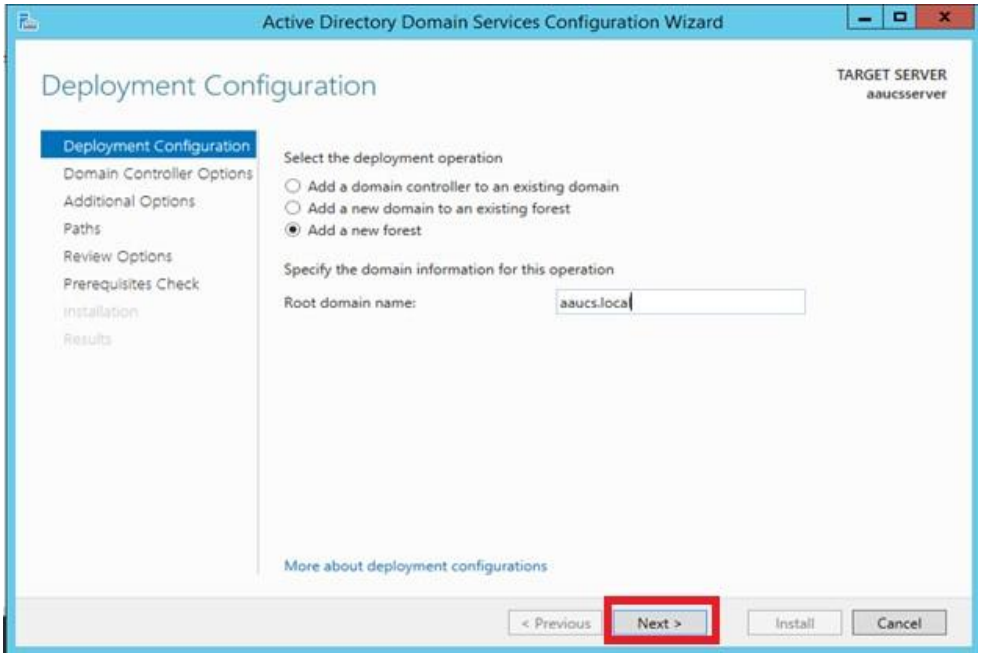



### 9.2.3.2 Deployment Configuration

Select Deployment option as per your requirement. Here we are installing our first Active directory in our server, so we have to select "**Add a New Forest**".




Next, Give the root domain name, in our case as you can see in the below figure the root domain is "**aaucs.local**".

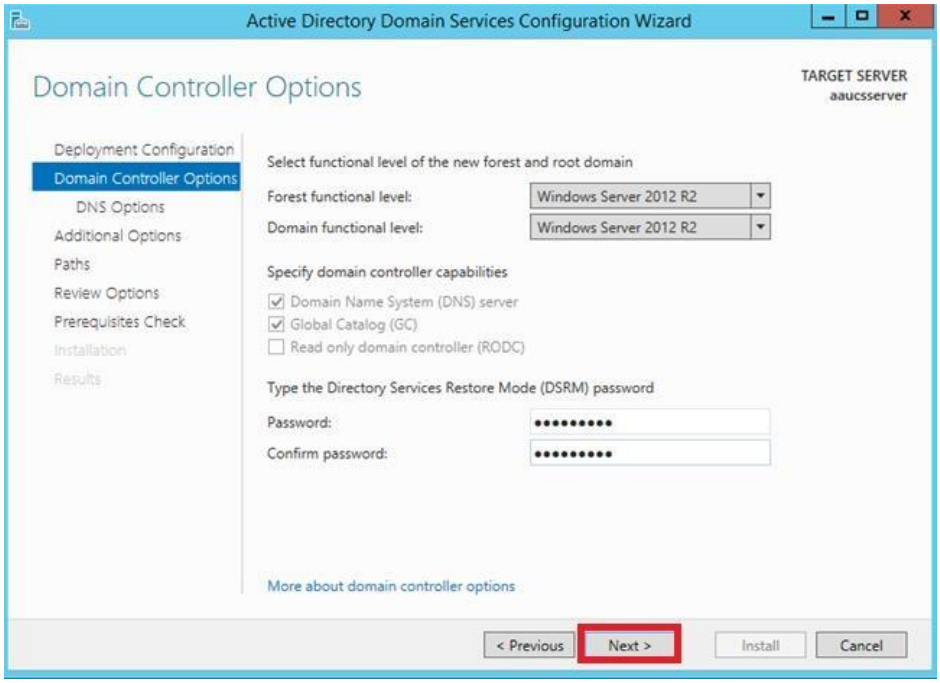



### 9.2.3.3 Domain Controller Options

Select **forest** and **domain functional level**. You have to also set your DSRM password here.

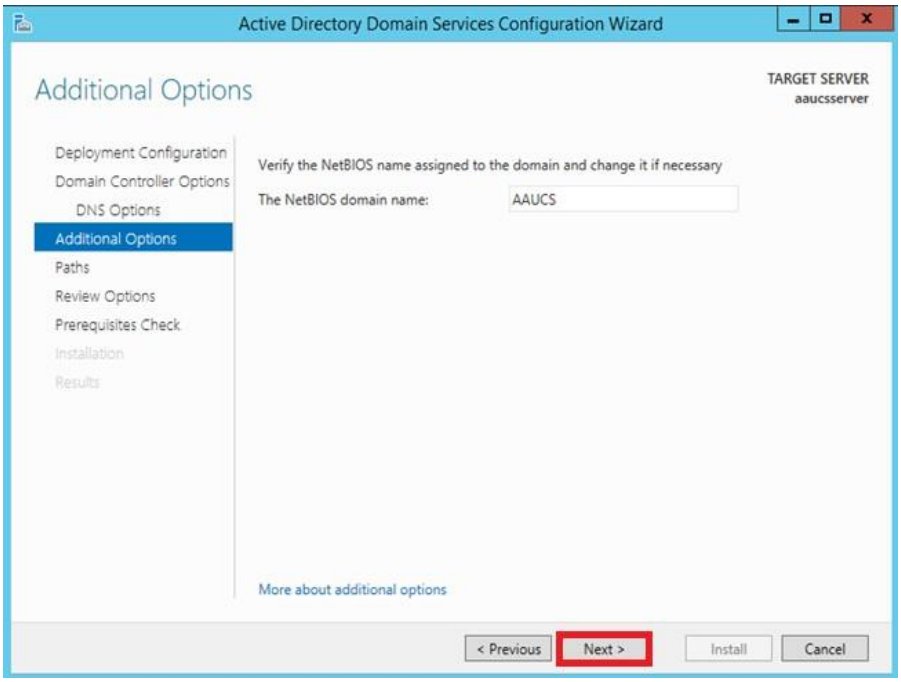
Next screen is DNS delegation; if you have any other DNS in your network you can delegate the

DNS options. This screen might display this message: “A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found”.

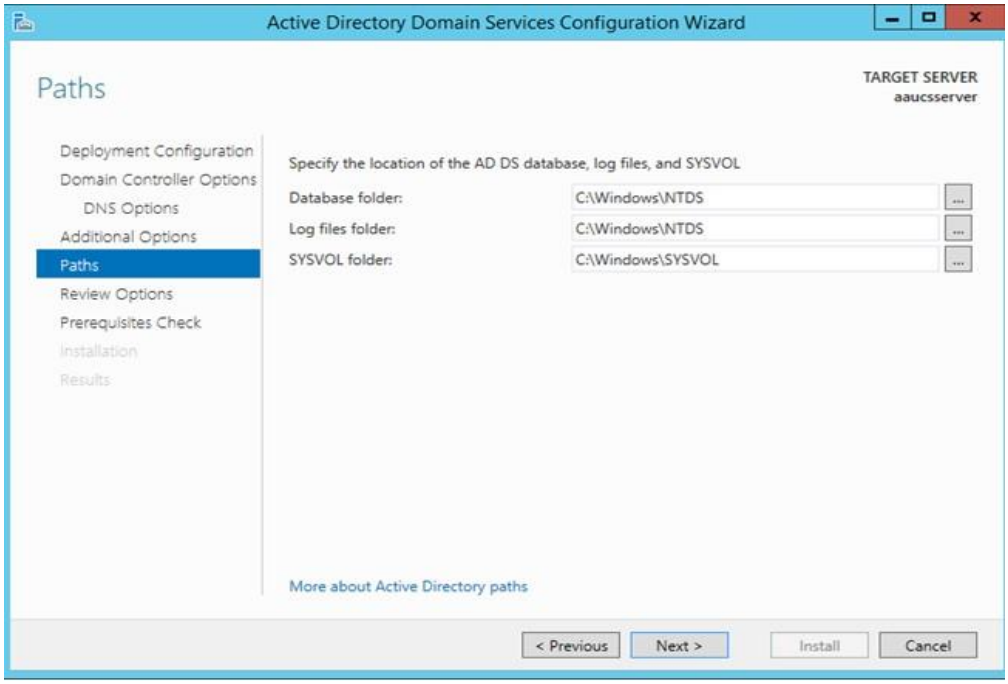



## 9.2.3.4 NetBIOS and Directory Path

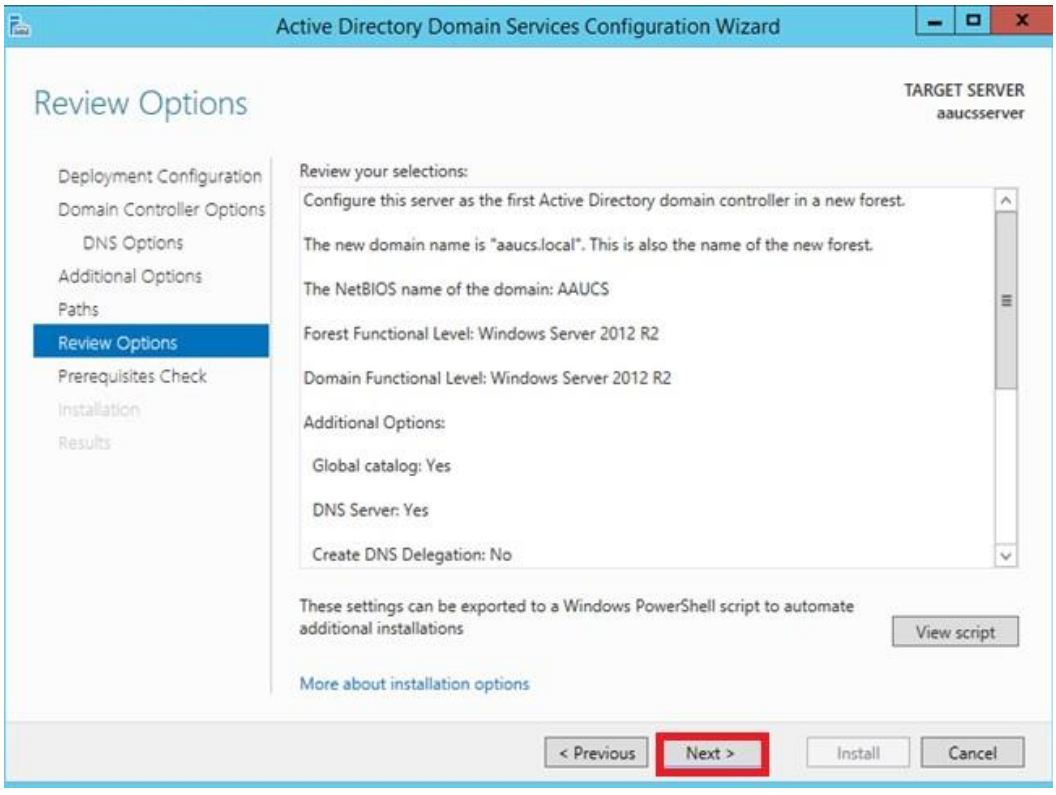
➢ Enter NetBIOS name in the next screen.



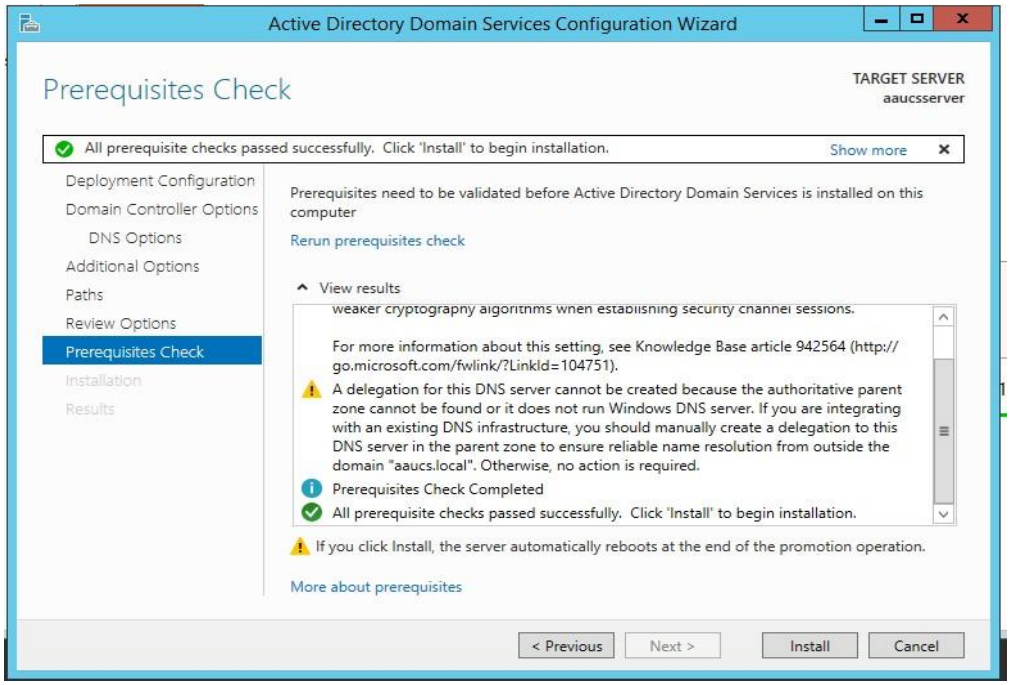
- Next, select the folder path for Active directory database files; by default it will be stored in "**C:\Windows\NTDS**" folder.




- Next, review all your options and click on **Next** button.



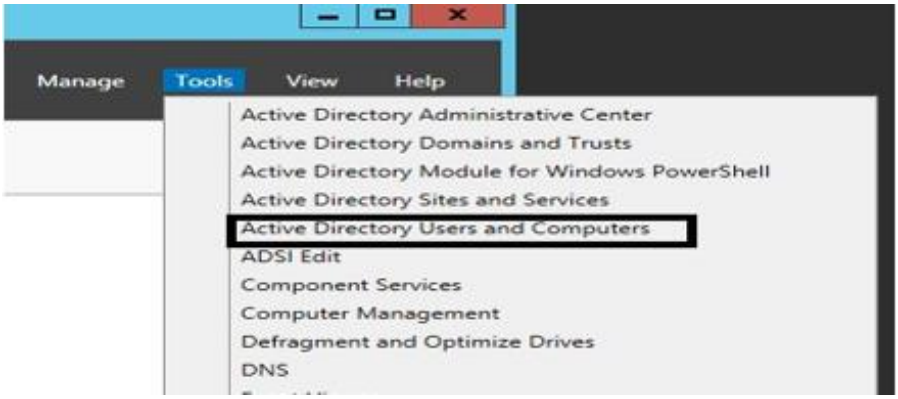
- Finally Prerequisties check window will appear and if the prerequisite check passed successfully click **Install** buuton to start the installation process.

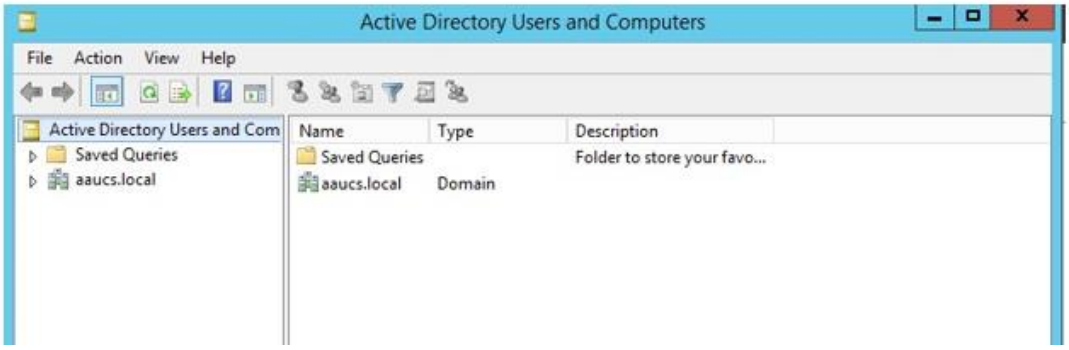



## 9.3 Active Directory Console

Before prompting server as Domain controller it will check the entire prerequisite, if any prerequisite is not installed means it will not start the installation until to complete the prerequisite installation. After completing installation reboot the server, if you checked the reboot automatically option means it will get restart automatically,

- Finally, after the installation, you can launch the **Active directory console** as shown below.





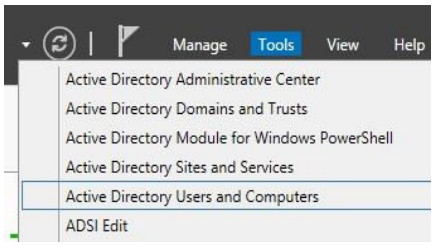

❖ After installing an Active directory Domain Name service on your server and restarting it, the Windows startup log on as shown below.

# Chapter Ten: Creating of Users, Computers and Groups Account in Active Directory Domain Services

## 10.1 User Account creation in a Domain controller

### Step 1: Open Active Directory Users and Computers

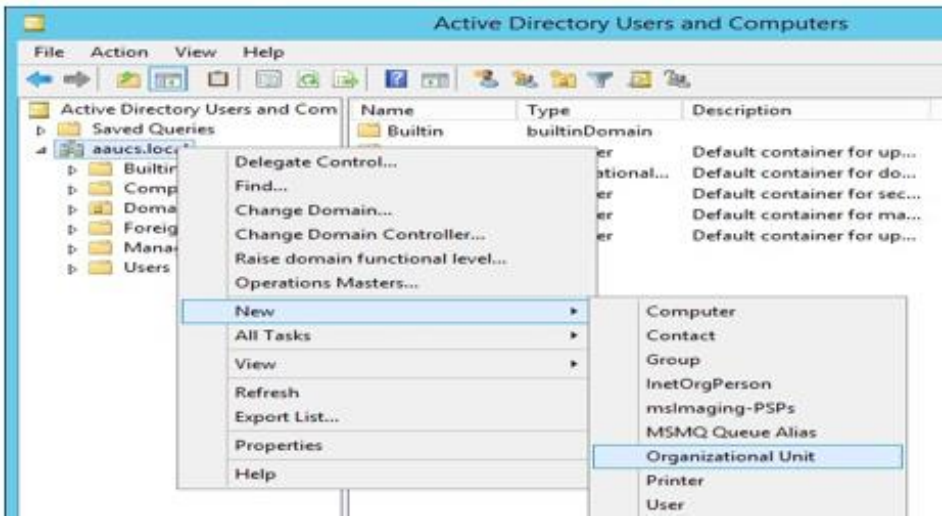
Open AD Users and Computers snap-in from Server Manager. You can also open AD Users and Computers snap-ins by typing dsa.msc on RUN program. You can open RUN application pressing Windows Key + 'R' on your keyboard.



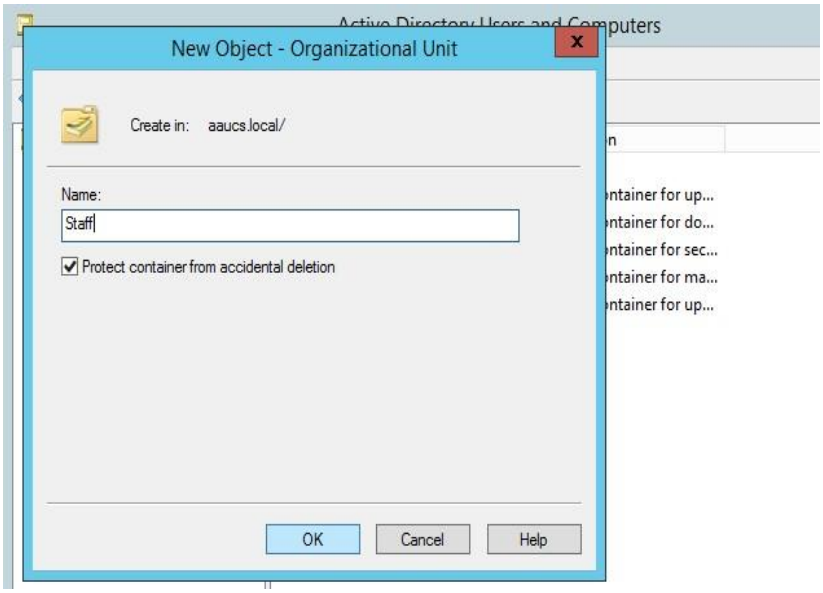

### Step 2: Create an Organizational Unit

Organizational Unit or simply OU is a container object of Active Directory Domain which can hold users, computers, and other objects. Basically, you create user accounts and computers inside an OU. We will create an OU named "**Staff**".

- Right-click on the domain in AD (aaucs.local) chooses New and click Organizational Unit.

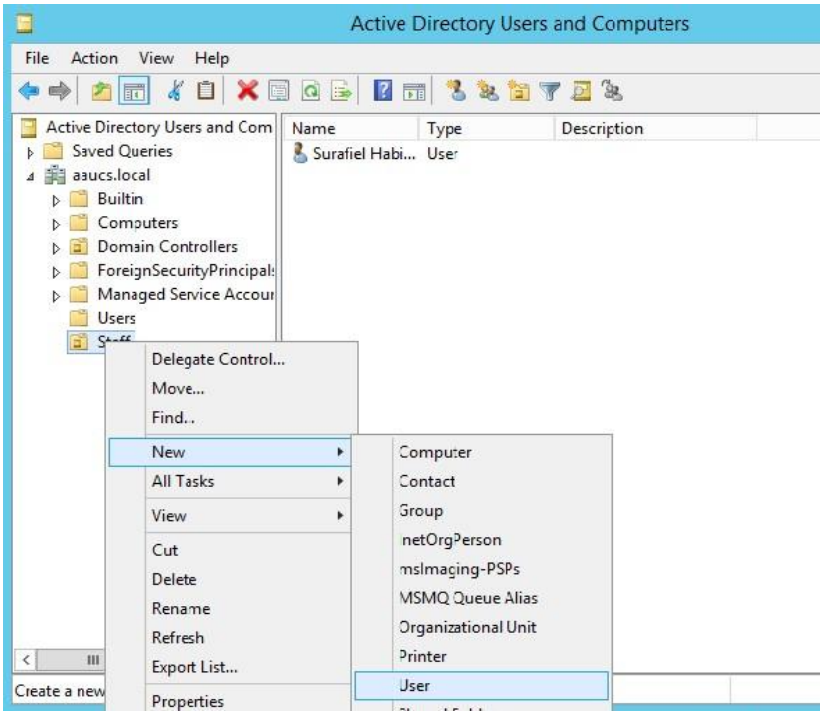


- Type the name **Staff** on the name field of the Organizational Unit. Check the **Protect container from accidental deletion** option. This option will protect this object from accidental deletion.

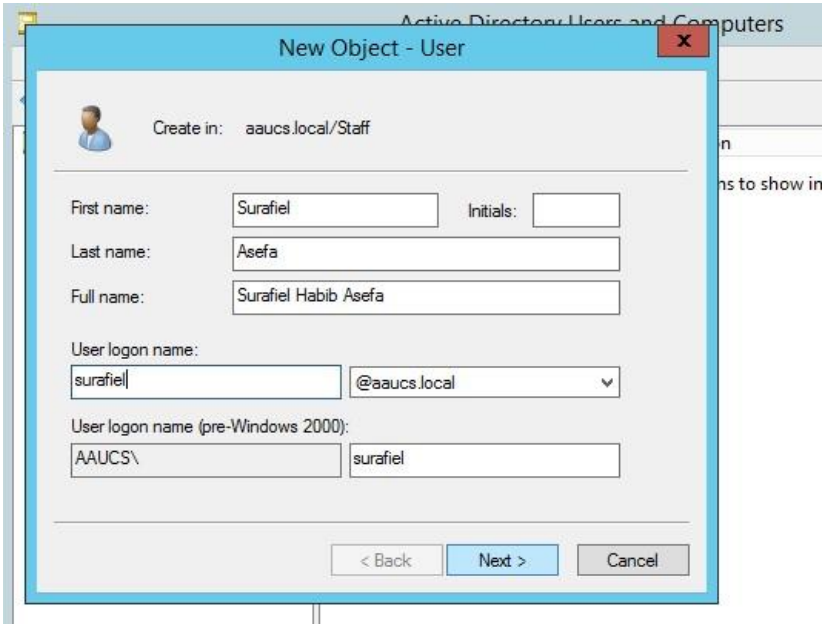



**Step 3: Create a New domain user account under the organizational unit**

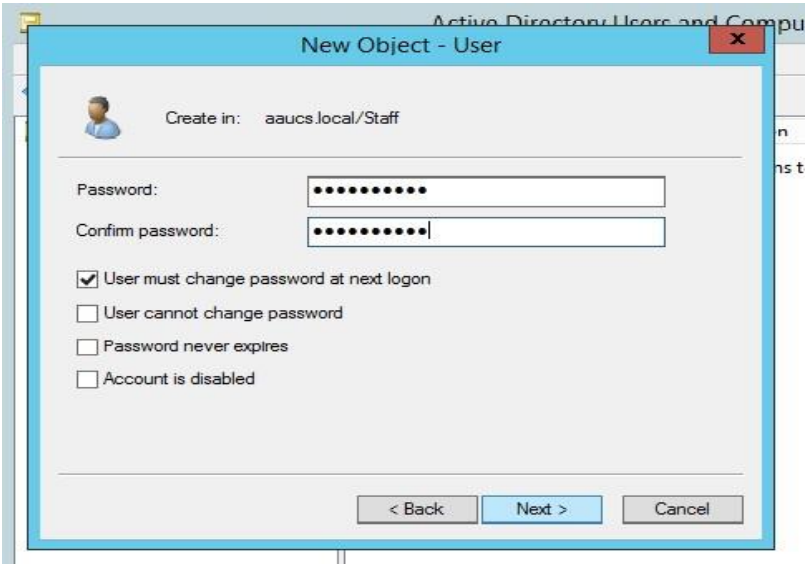
Right-click the Staff Organizational Unit (OU), click New and click User.



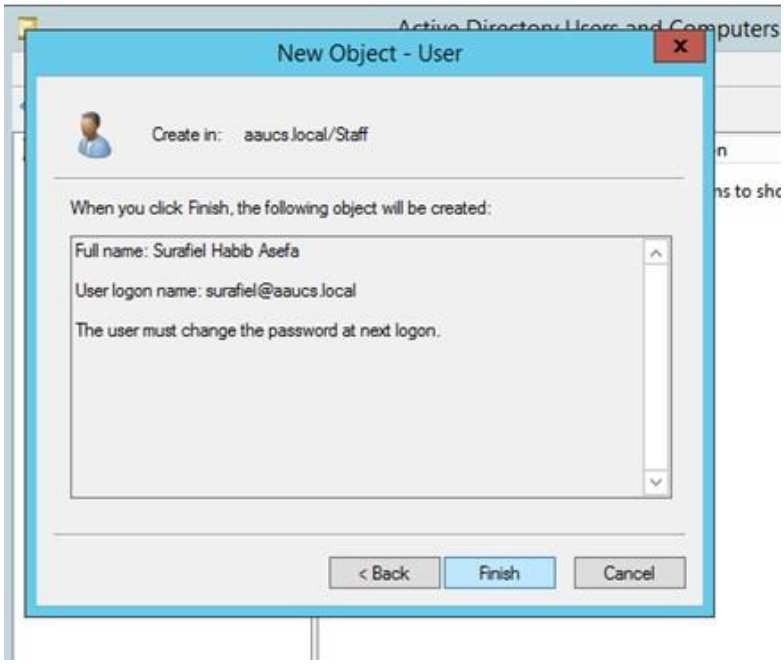
Now type the user information. Type the first name and last name. Here user logon name is the name that the user will use to actually log in the computer in the network. So when user tries to log in, he will type **surafiel@aaucs.local** or **surafiel\aaucs** on username field. Then, click **Next**.



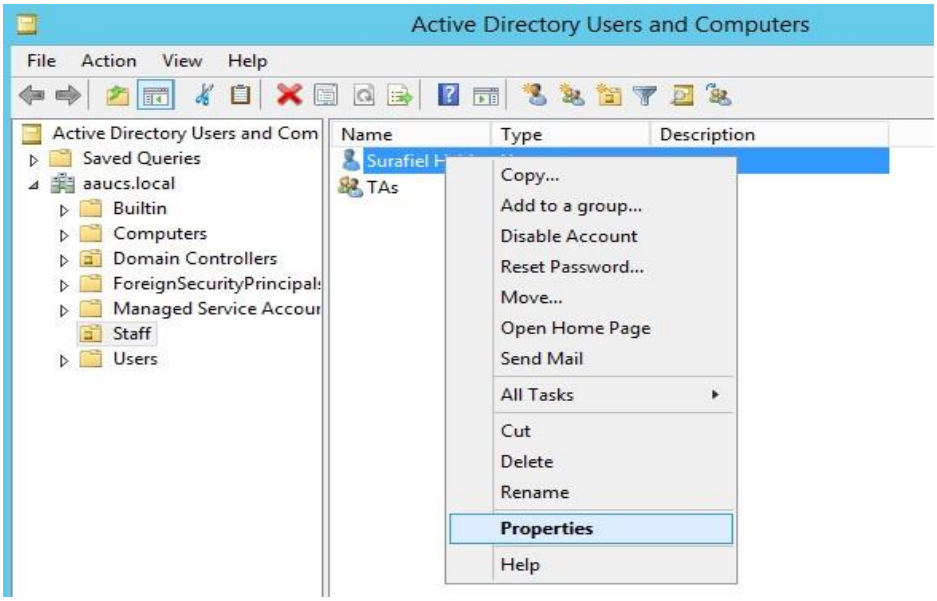

Now type the password. Check **user must change password at next logon**. The user will be forced to change the password when user logs in. Click **Next**.




➢ Finally, Review the user configuration and click Finish.




You have successfully created a user account. You can open the properties of the user account to configure settings.




✓ Summary of creating a Domain user account in Active Directory Domain name service:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the Active Directory Users and Computers window, expand <*domain name*>**.com**.
3. Right-click **Users**, point to **New**, and then click **User**.
4. In the **New Object - User** dialog box, do the following:

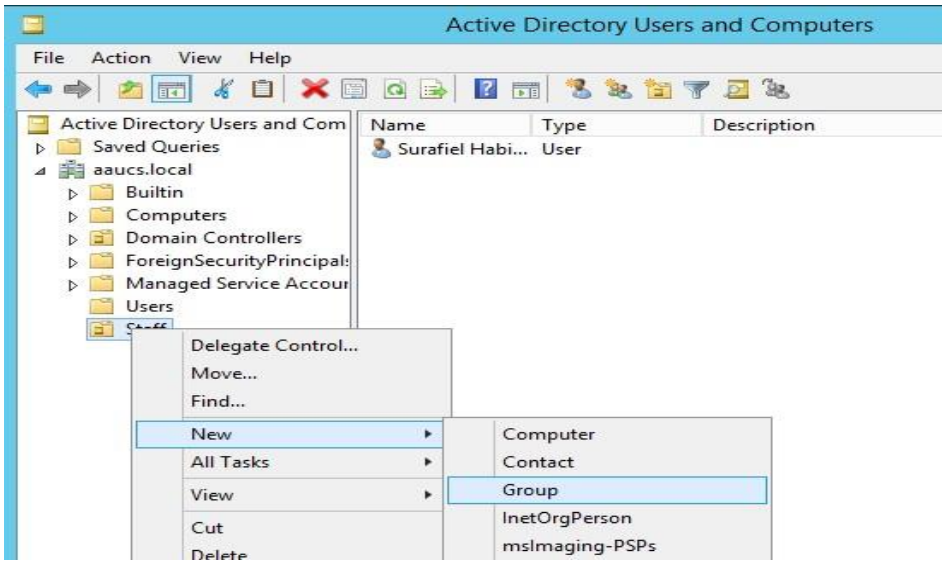
| Use this | To do this |
|---|---|
| First name | Type a first name for the account. |
| User logon name | Type the appropriate account name from the previous list. |

5. Click **Next**.
6. In the **Password** box, type a password for the account, and then in the **Confirm password** box, type the password again.
7. Select **User must change password at next logon** then click **Next**.
8. Click **Finish**.
9. Repeat steps 3 through 8 for all your remaining accounts.

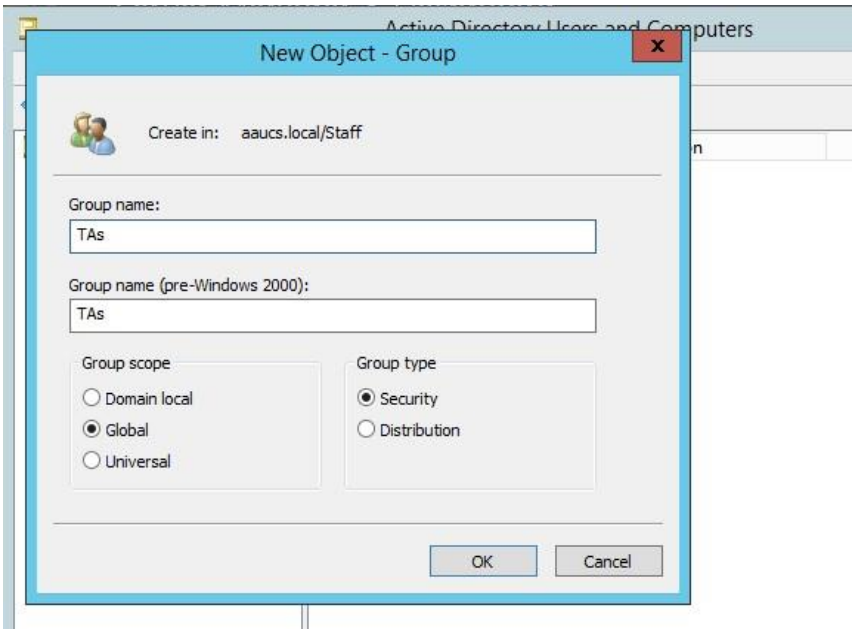
## 10.2 Creating steps of users group account

To create a group of users account in Active Directory on the Domain Controller you have to follow the following steps

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In Active Directory Users and Computers window, expand <*domain name*>**.com** 3. In the console tree, right-click the folder in which you want to add a new group.
4. Click **New**, and then click **Group**.

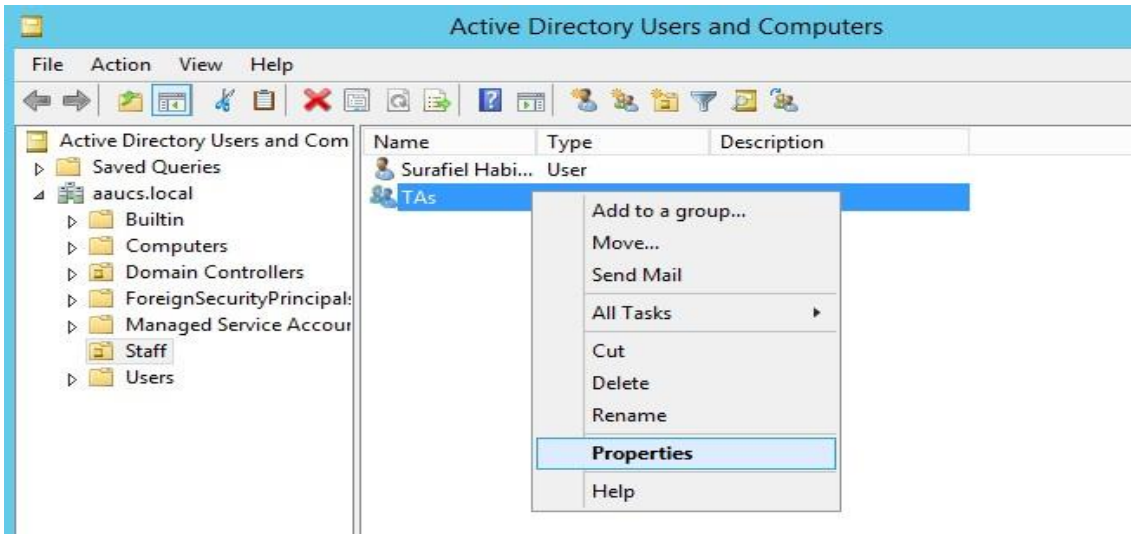


5. Type the name of the new group. Use a name that you can easily associate with the role or service for which you are creating.
6. In the **New Object - Group** dialog box, do the following:
    a. In **Group scope**, click **Global scope**.
    b. In **Group type**, click **Security**.
7. Click **Ok**.




Repeat steps 3 through 7 for all your remaining groups.

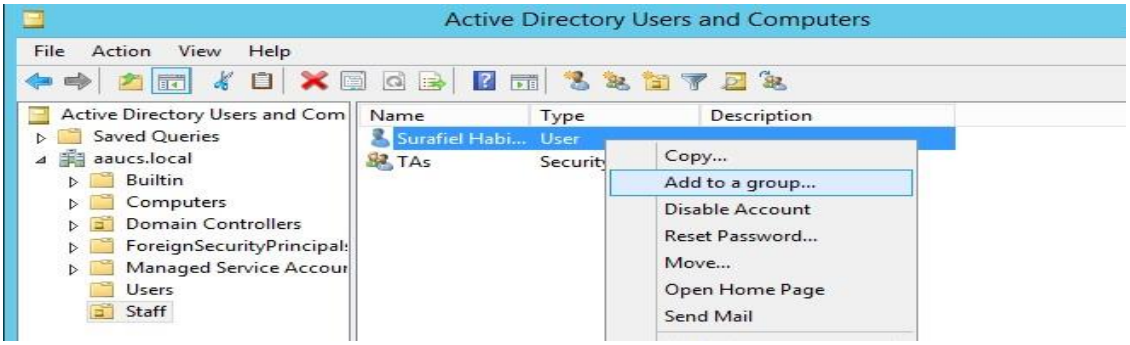
➢ Here we are created “TAs” Group which is associated to Technical Assistants of our **aaucs**.**local** domain.



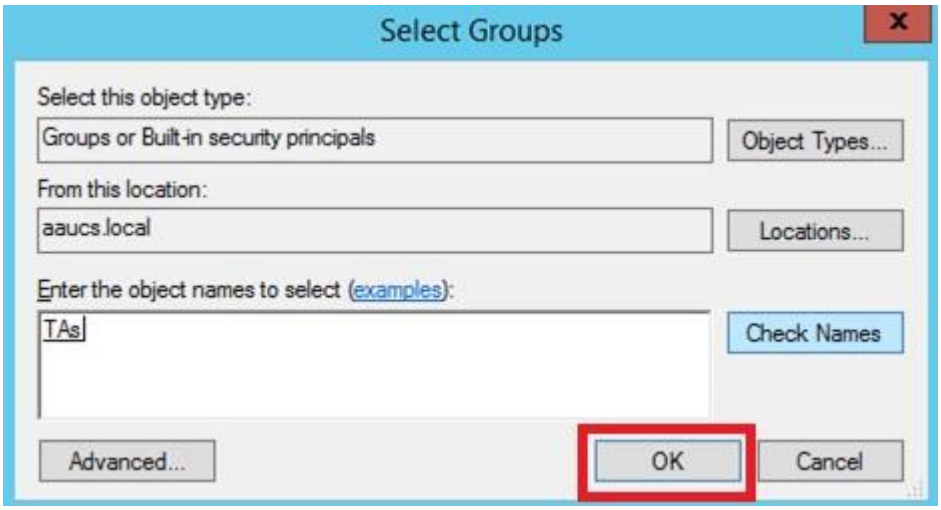


## 10.3 Adding a Domain user account in to a Domain group account

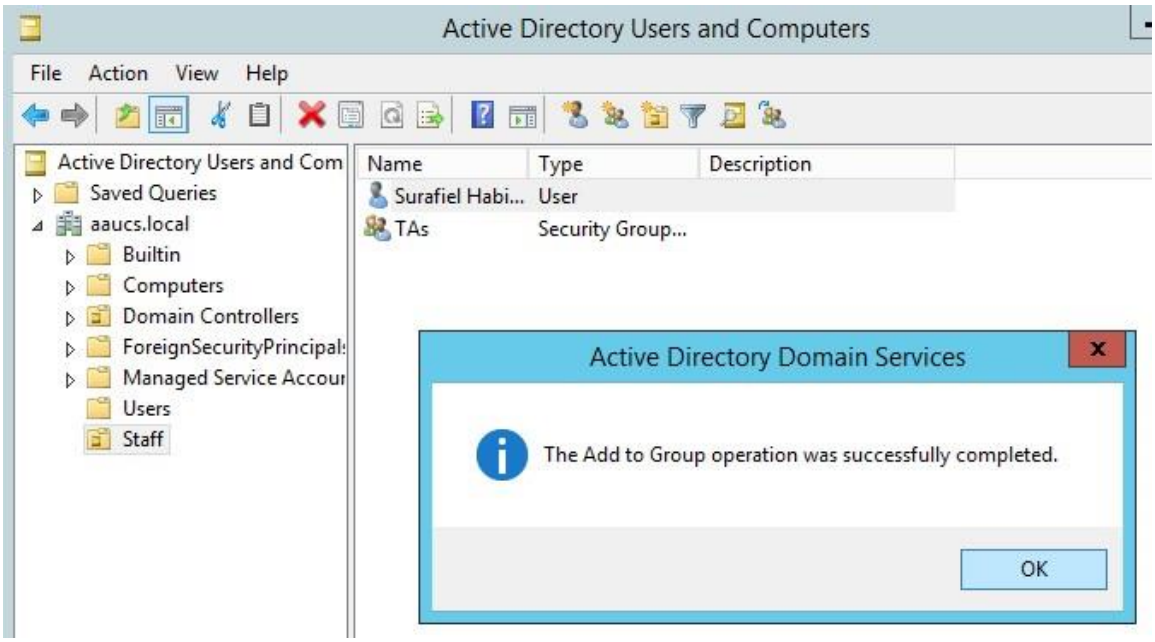
- Right click on your user account which you want to add in a group account.



- Enter your group name which you want to adding a user in it in the place of text area and click **ok**.

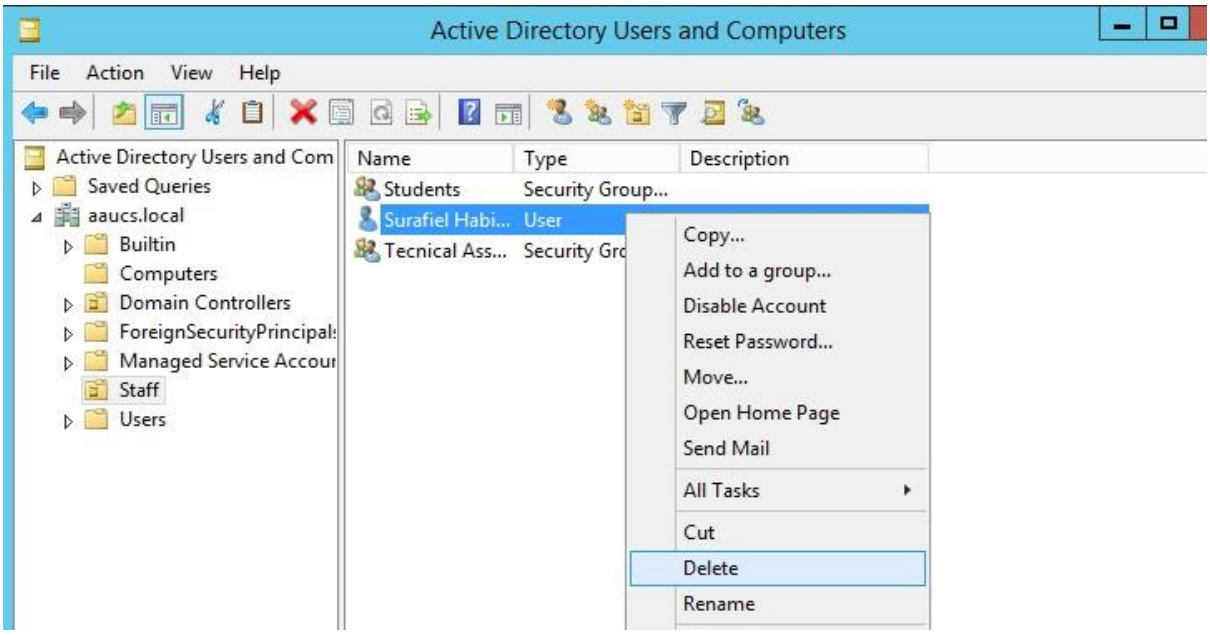



- Finally, you have to get a message for the operation successfulness.



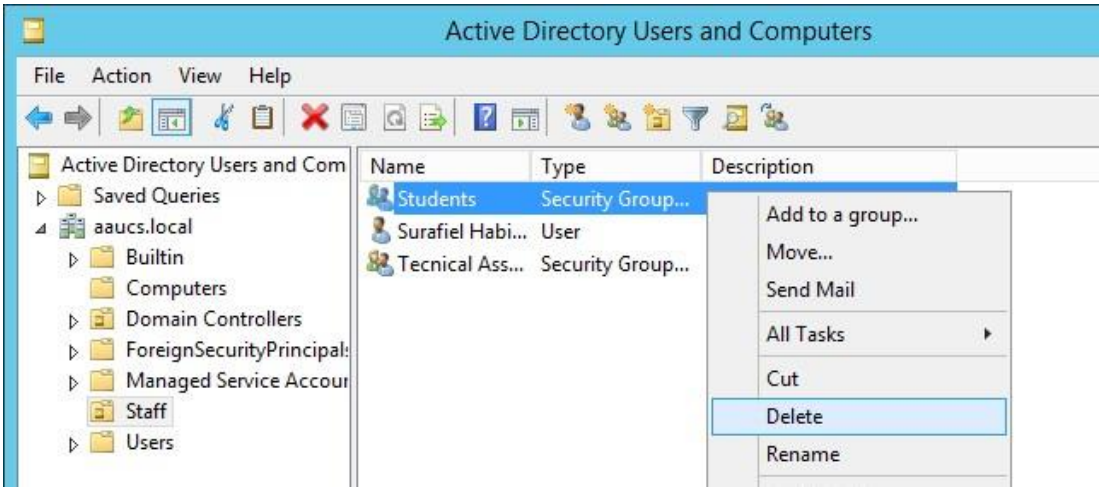

## 10.4 Deleting a Domain User Account

Go to your domain user account through **Server manager** -> **Tools** -> **Active Directory Users and Computers** -> **domain** (In our case the domain is aaucs.local) -> **Organizational unit** (Staff) and then from the given list of user accounts right click on a single user account which you want to remove and click **Delete**.



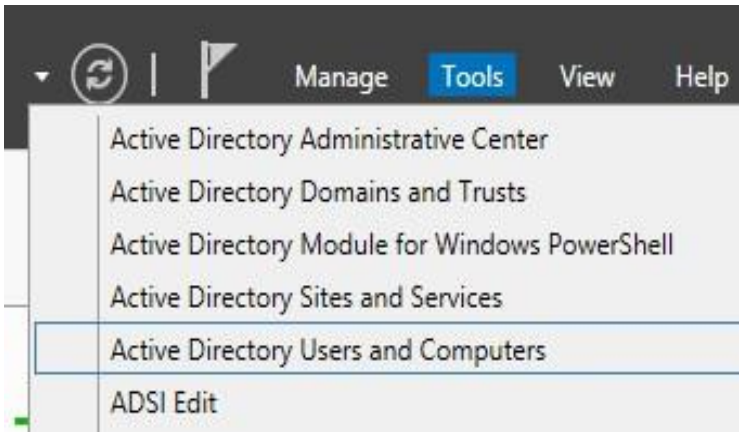

## 10.5 Deleting a Domain Group Account

Go to your domain user account through **Server manager** -> **Tools** -> **Active Directory Users and Computers** -> **domain** (In our case the domain is **aaucs.local**) -> **Organizational unit** (Staff) and then from the given list of group accounts right click on a group account which you want to remove and click **Delete**.

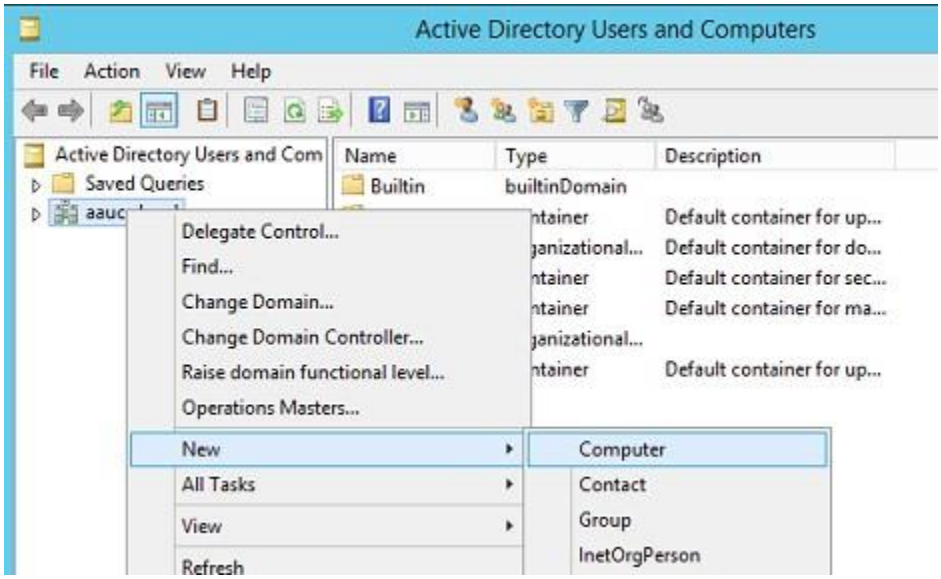



## 10.6 Creating a Client machine (Computer) Account in a domain controller

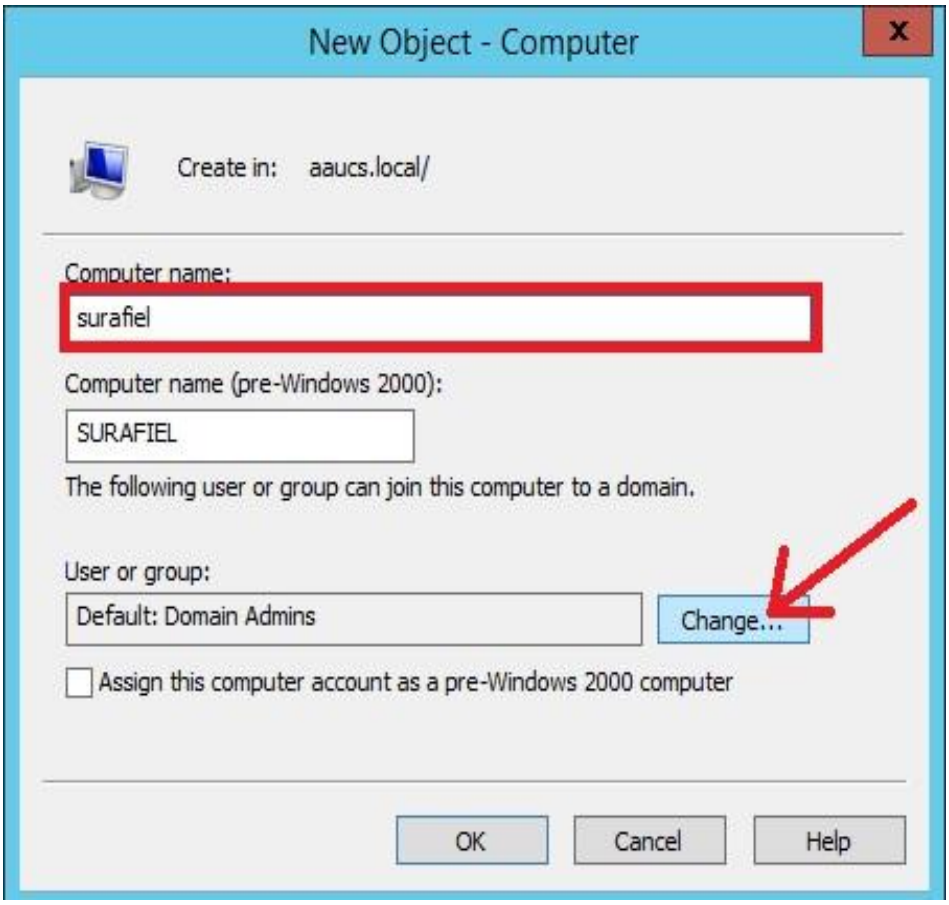
- Go to the server manager on the Tools menu click Active Directory Users and Computers



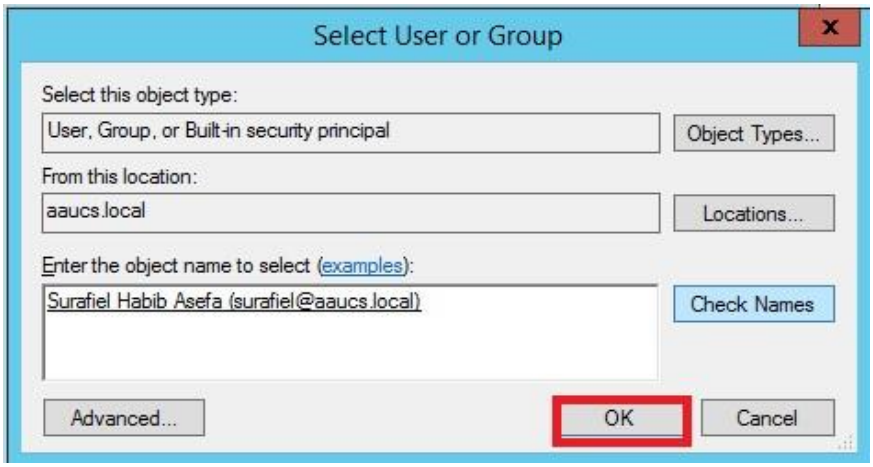

- Right click on your **domain** and from the drop down options select **New** -> **Computer**

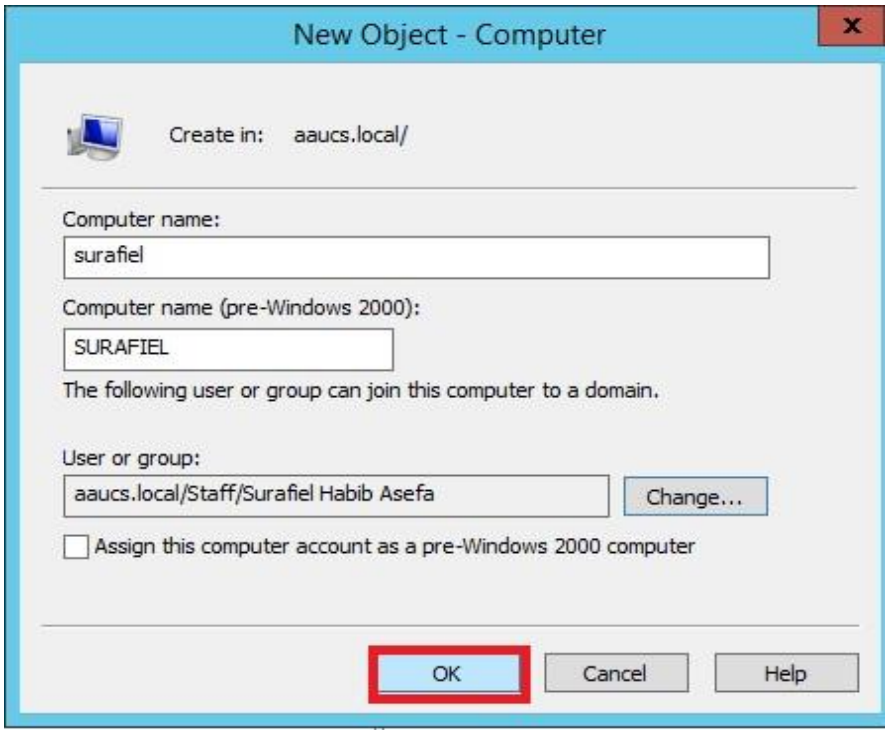



- The "**New Object-Computer**" window will pop up and write the name of the client machine on the **Computer name**: field, if you want to assign the client machine to a specific user or group other than to a Domain Administrator click the **Change** button in the right side of **User or group**: field.



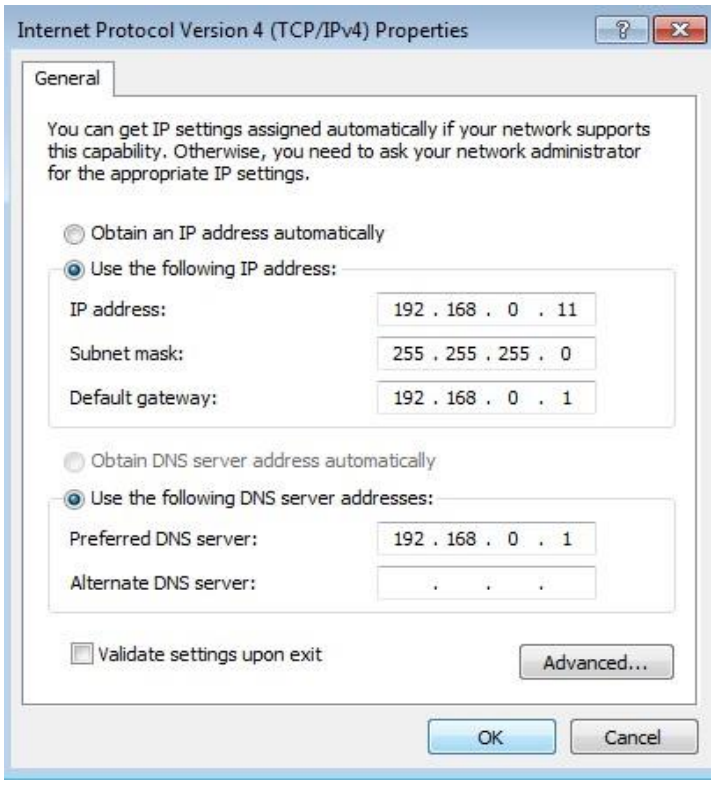

- In our case we are assigned the surafiel pc to the user Surafiel Habib Asefa in a aaucs.local domain.





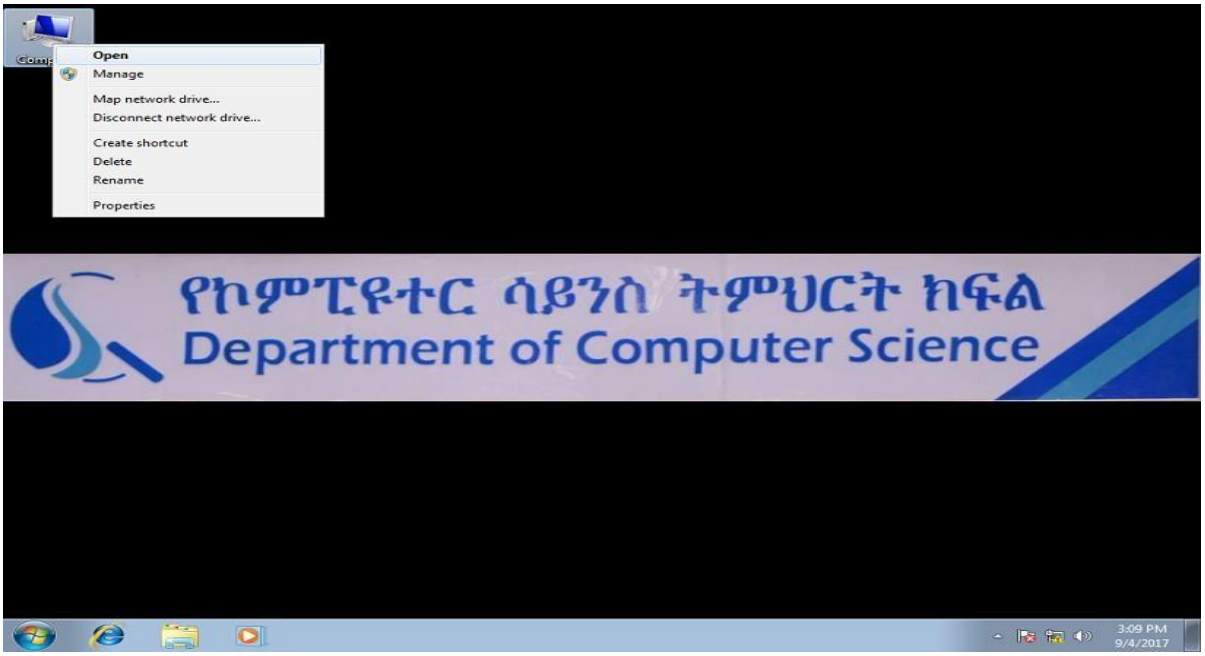

## 10.7 Joining a Client Machine to a Domain controller server from the client side

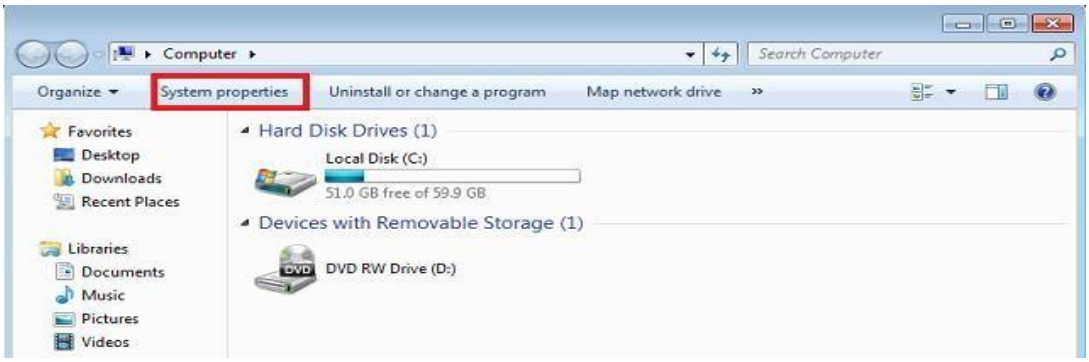
- First you have to set up a static IP address for the client.




## Steps:

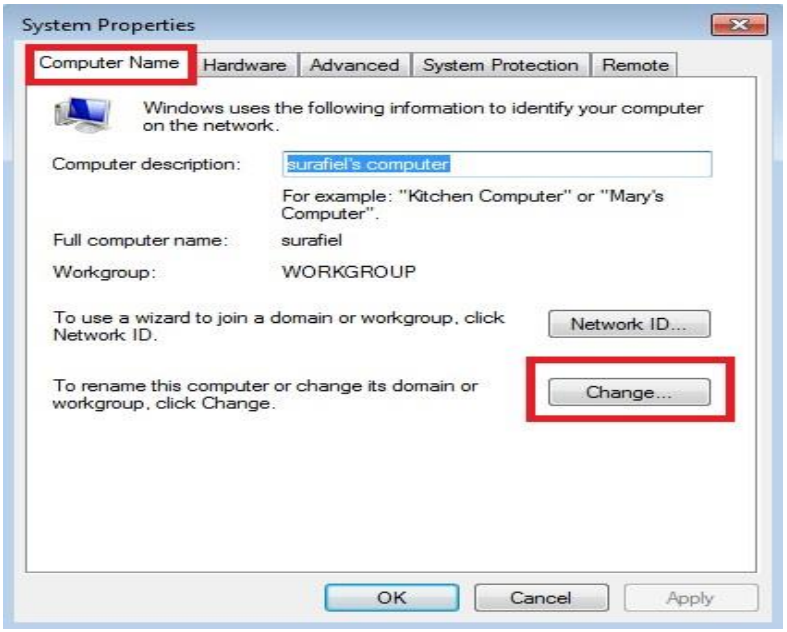
1. Open your client machine "**Computer**" and click on the **System Properties** button. In our case the client machine is Windows 7.



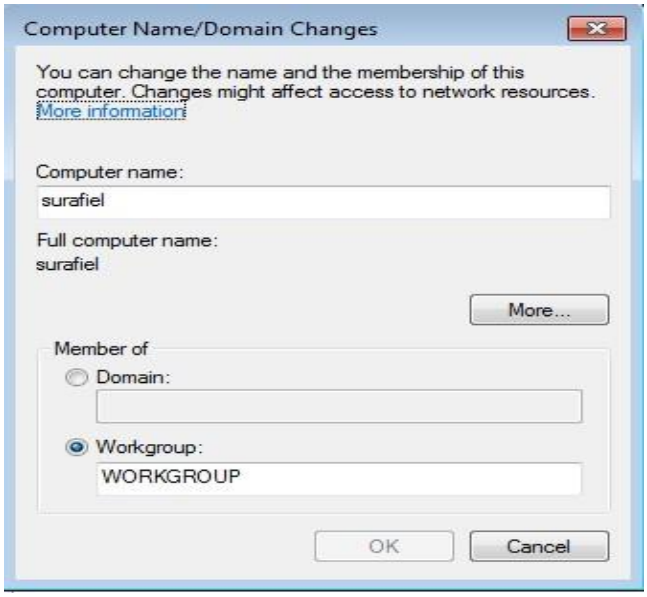



2. Now click on the **advanced system** settings link on the left hand side.

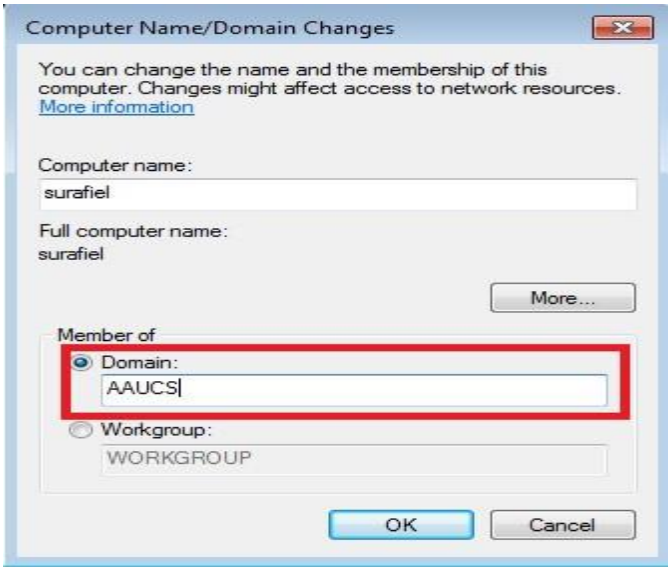

3. When the advanced system settings open, switch to the computer name tab.



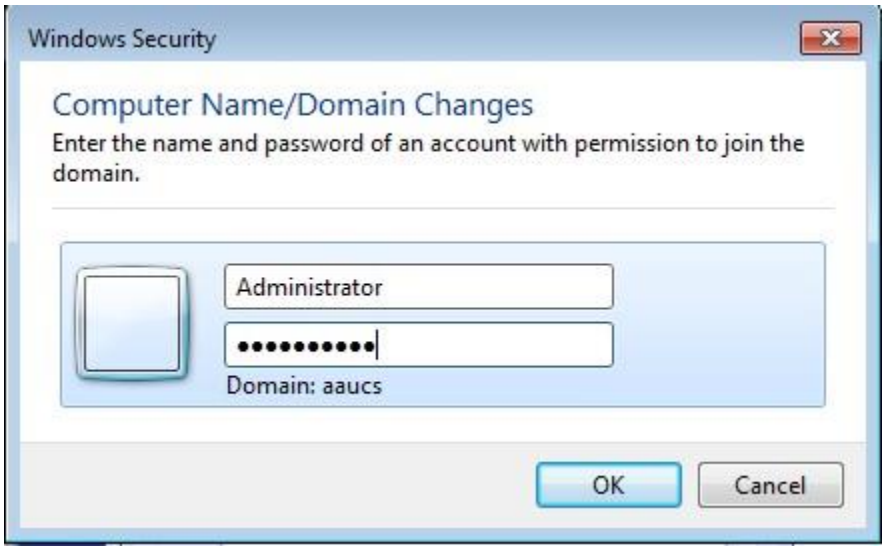
4. Click on the change button, from here you can change your Computers Name to a more friendly name.




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

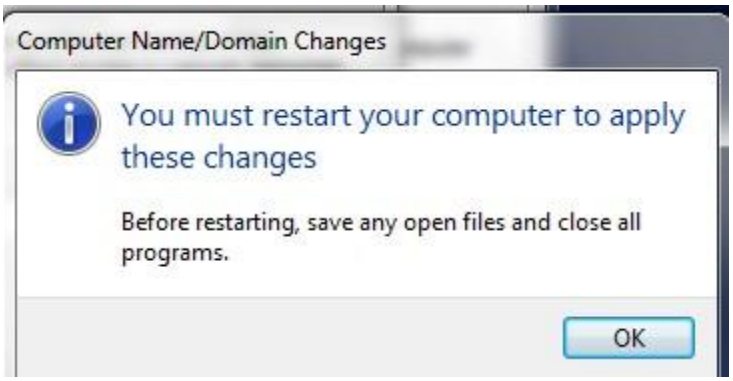



6. When you hit enter, or click **OK**, you will be asked for the user name and password of a Domain Administrator user account.


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

8. Finally, you must restart the client machine to apply these changes.




❖ After restarting the client machine the window log on status changed like as shown below


⇨ By clicking **Switch User** tab you can log on to the domain


⇨ By clicking other user you can log on to **AAUCS** domain using an already domain member user account

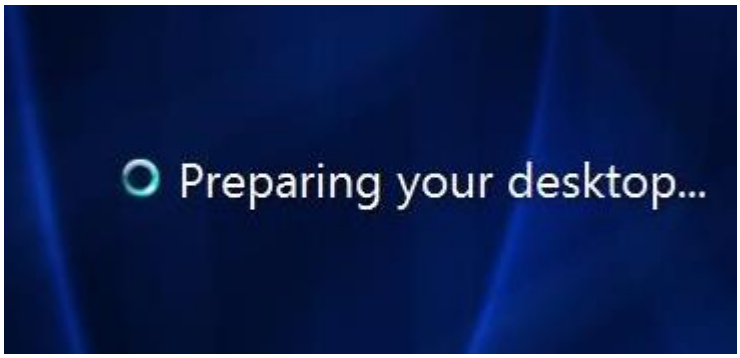

➢ Next, you have to change the already given password for your domain member account by yours own new one, and be able to log on, Click "**OK**"

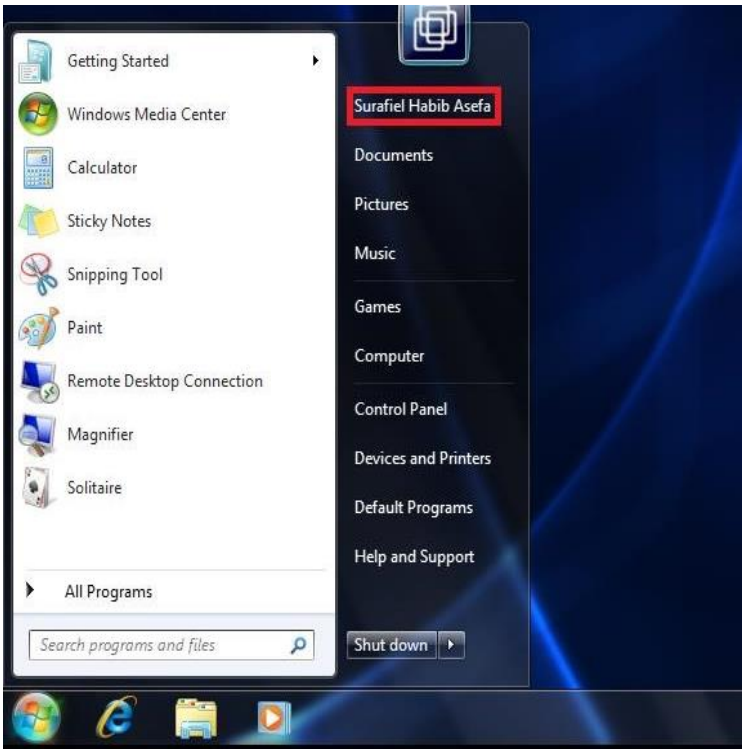
Next, enter your old password and the new one with confirmation and go on.



- If your new password meets the password policy of the domain password policy, you have to get a message that says "**Your password has been changed**" and click "**OK**" then "**Welcome**" and "**Preparing your desktop**" screens will appear successively.


Welcome


Preparing your desktop...


Getting Started
Windows Media Center
Calculator
Sticky Notes
Snipping Tool
Paint
Remote Desktop Connection
Magnifier
Solitaire
All Programs
Search programs and files
Surafiel Habib Asefa
Documents
Pictures
Music
Games
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down

## 10.3 Enabling and Using Fine-Grained Password Policies in Active Directory Domain Services

Fine-grained password policies are used to specify multiple password policies in a single domain and apply different restrictions for password and account lockout policies to different sets of users in a domain. Fine-grained password policies apply only to global security groups and user objects and also they cannot be applied to an organizational unit directly.

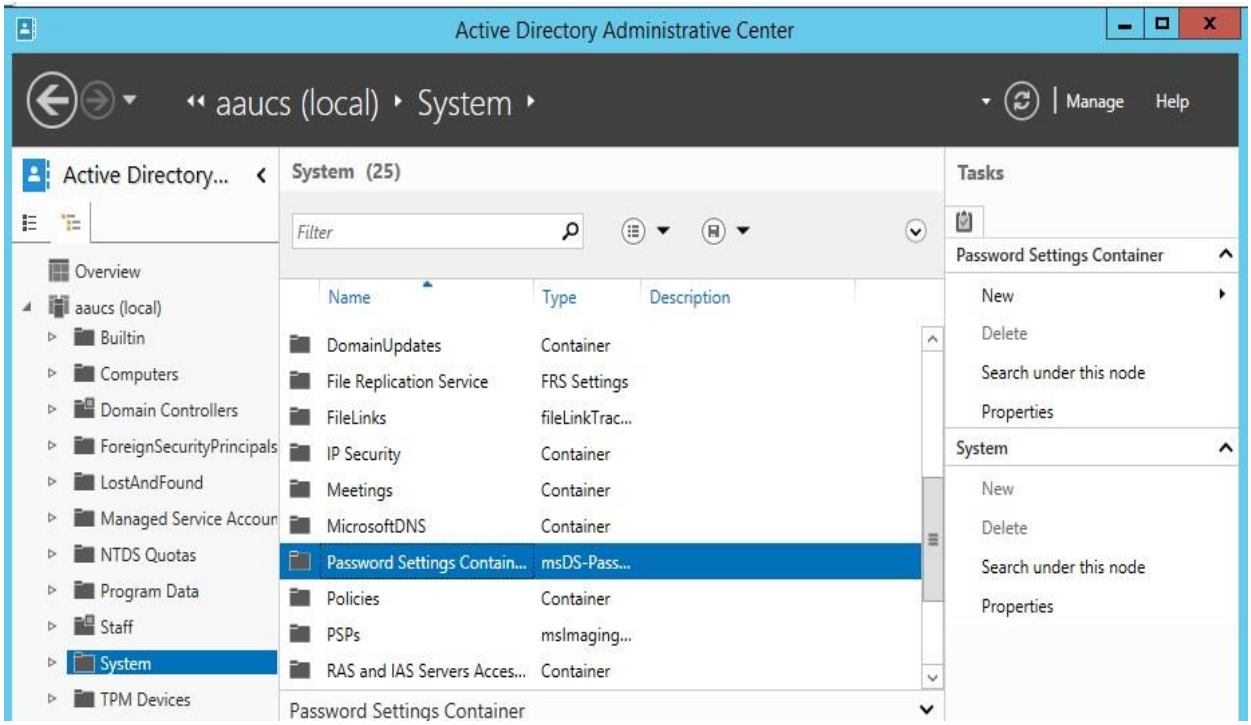
Other considerations are:

- Only members of the Domain Admins group can set fine-grained password policies, but this can be delegated.
- Managing the policies is done through Active Directory Administrative Center and/or Windows PowerShell.

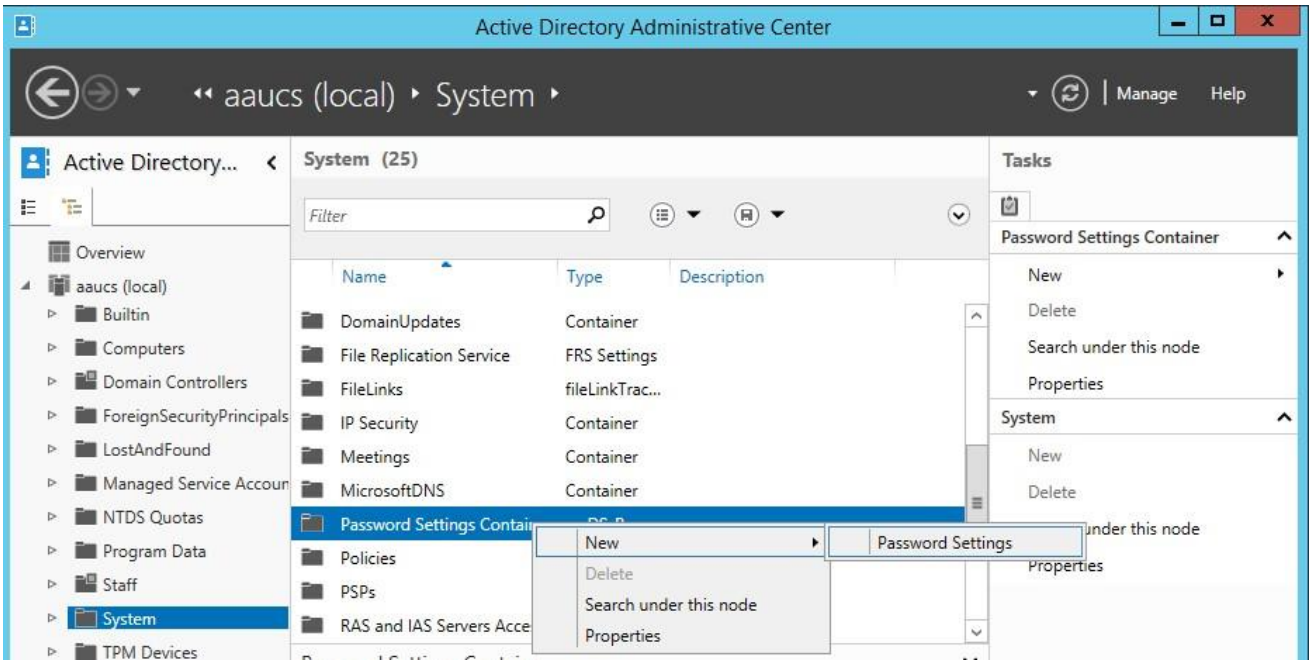
To enable the Fine-grained password policies (FGPP) the following steps will be satisfied:-

1. Open the **Active Directory Administrative Center** (ADAC) from the **Server Manger Tools** menu,

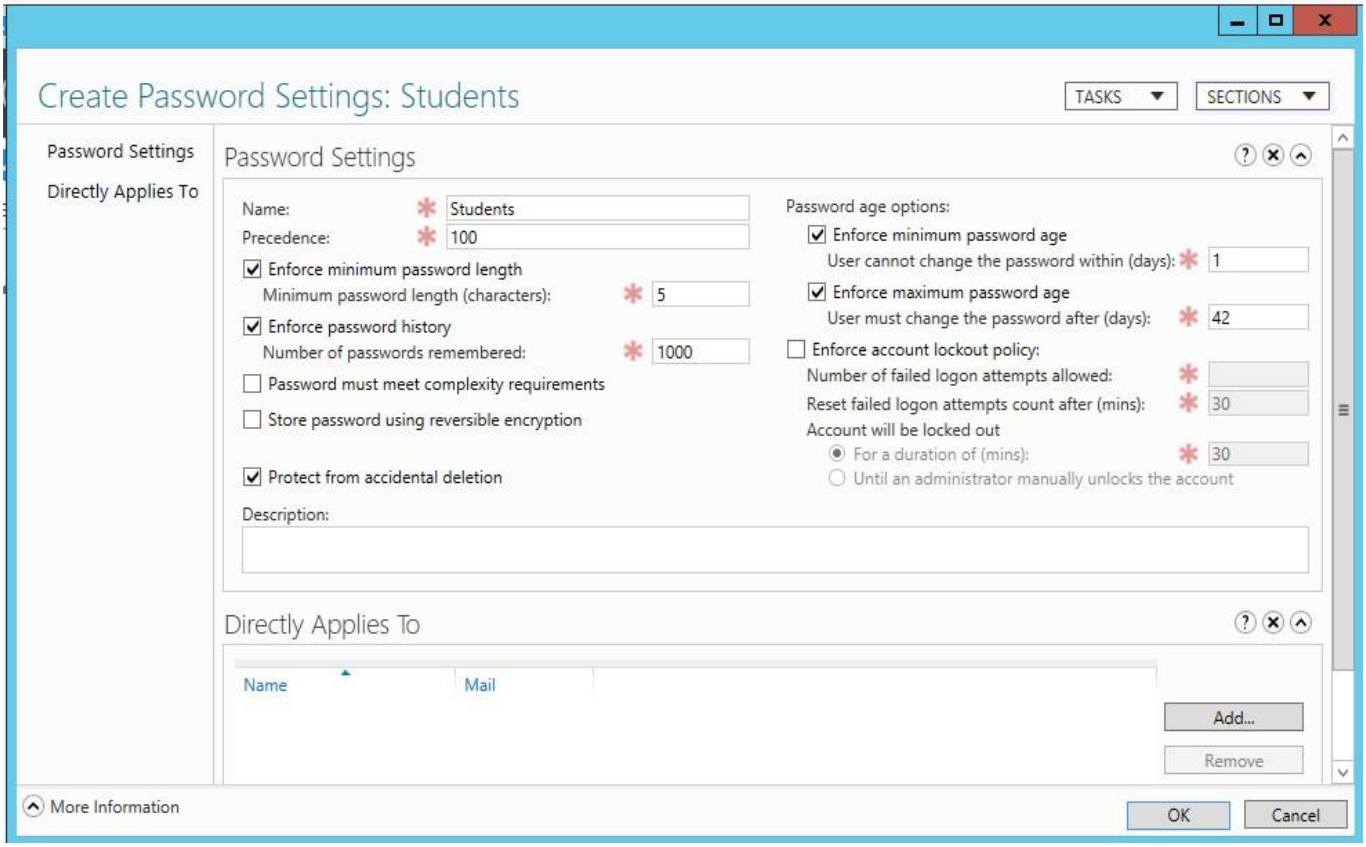

2. Switch to the Tree View and navigate to the **System**, **Password Settings Container**.




3. Right-click the **Password Settings Container object** and select "**New**", "**Password Settings**"




4. In the "**Create Password Policy**" UI, fill all the fields that are appropriate.




- It's suggested a descriptive name and description of why you create a new policy, how this policy differ from the default Password policy. And what group it will apply to.

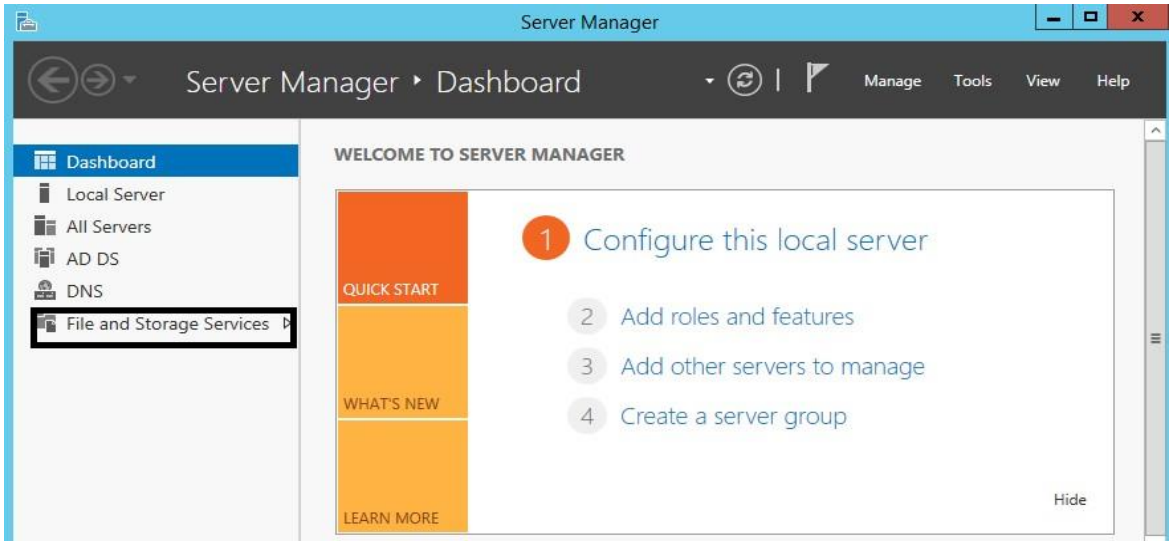
# Chapter Eleven: File and Storage Services

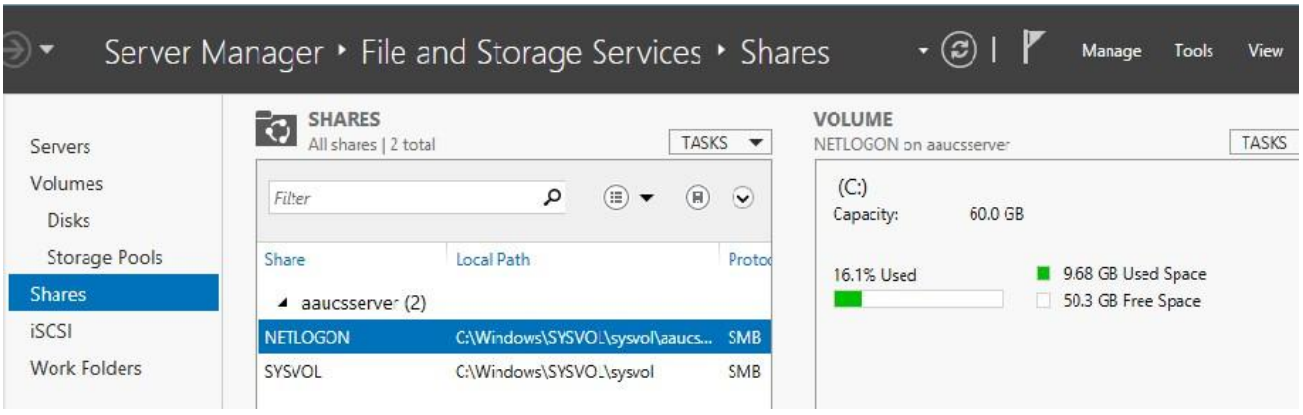
## 11.1 Shared folder setup

There are different ways to share a folder in Server 2012. Most efficient way is to use the Server Manager. Here, we will configure some shared folder from domain controller named aaucs.local. So, let's setup some shared folders.

To do so, open Server Manager.

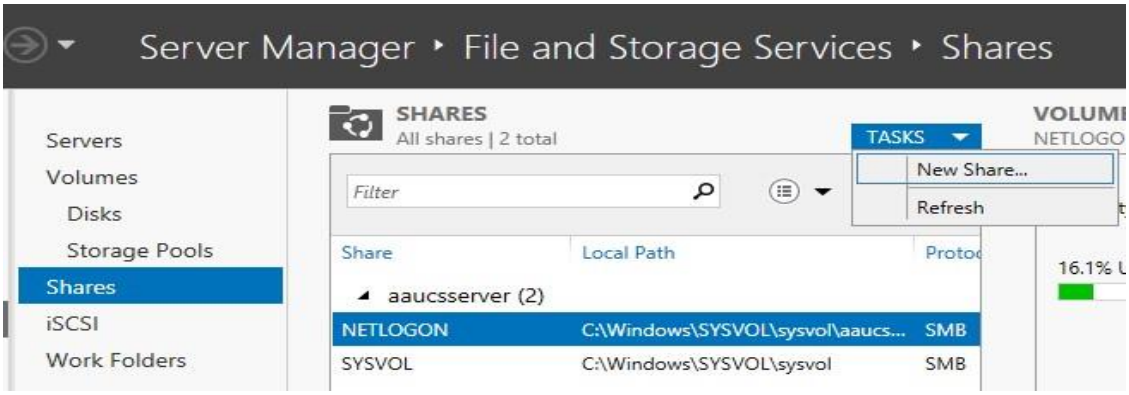
- Click **File and Storage Services** on the left pane.
- Then click **Shares** from the list. You will see the list of shared folders on this server. As you can see below there are two folders, **netlogon** and **sysvol** shared by default. This is because the server is **Active Directory Domain Control**.



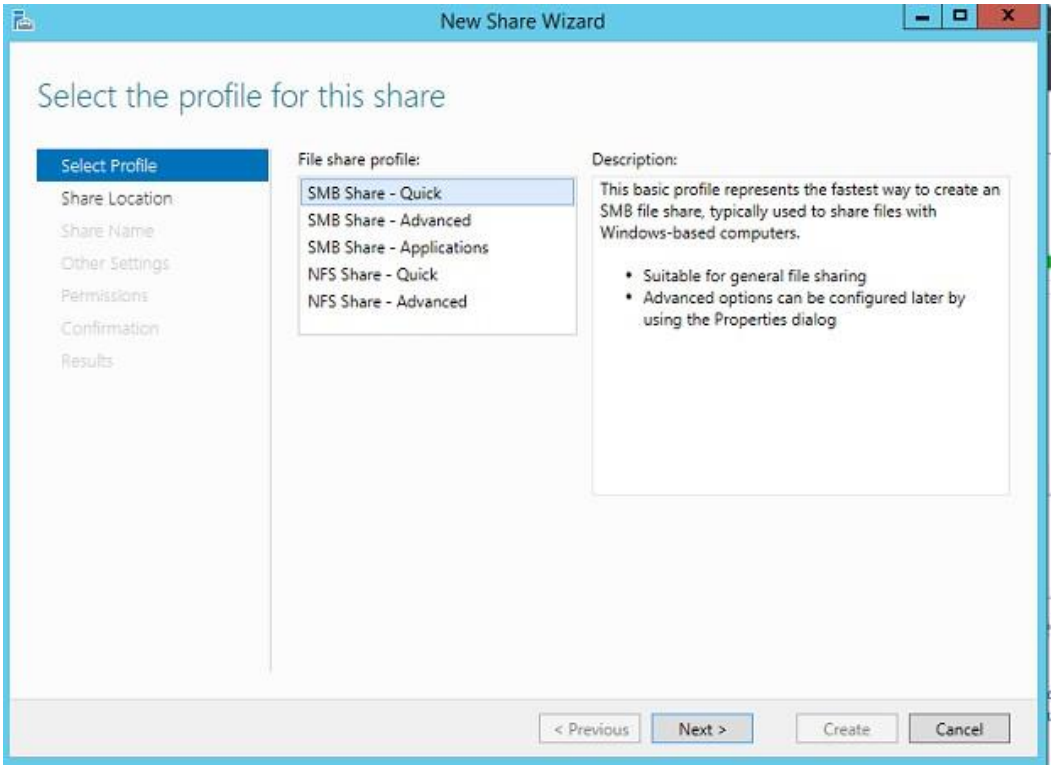



Now let's have a scenario, we want to share a folder named **Academic Materials** to **Students** users **group**. We want only the **Students** group of users to **view** and **execute** the contents of the folder. We already have **Students** users group set up and assigned users into the group. So, let's create the shared folder.

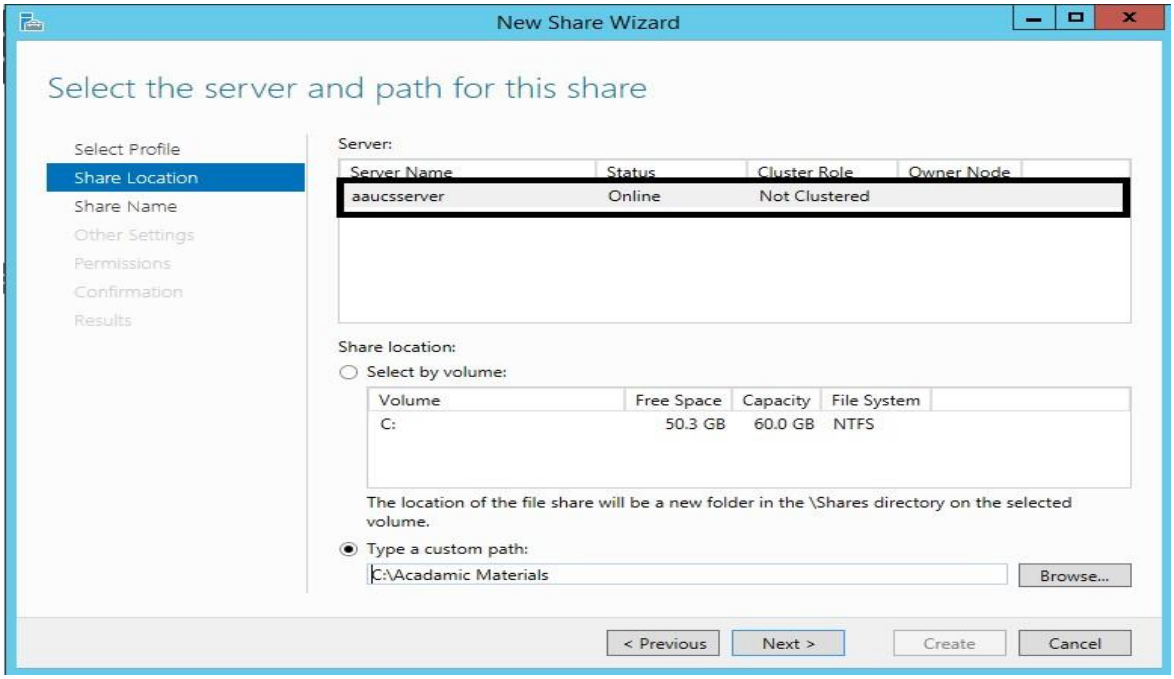
To create a new shared folder, click **Tasks** and click **New Share** in **Server Manager** Console.



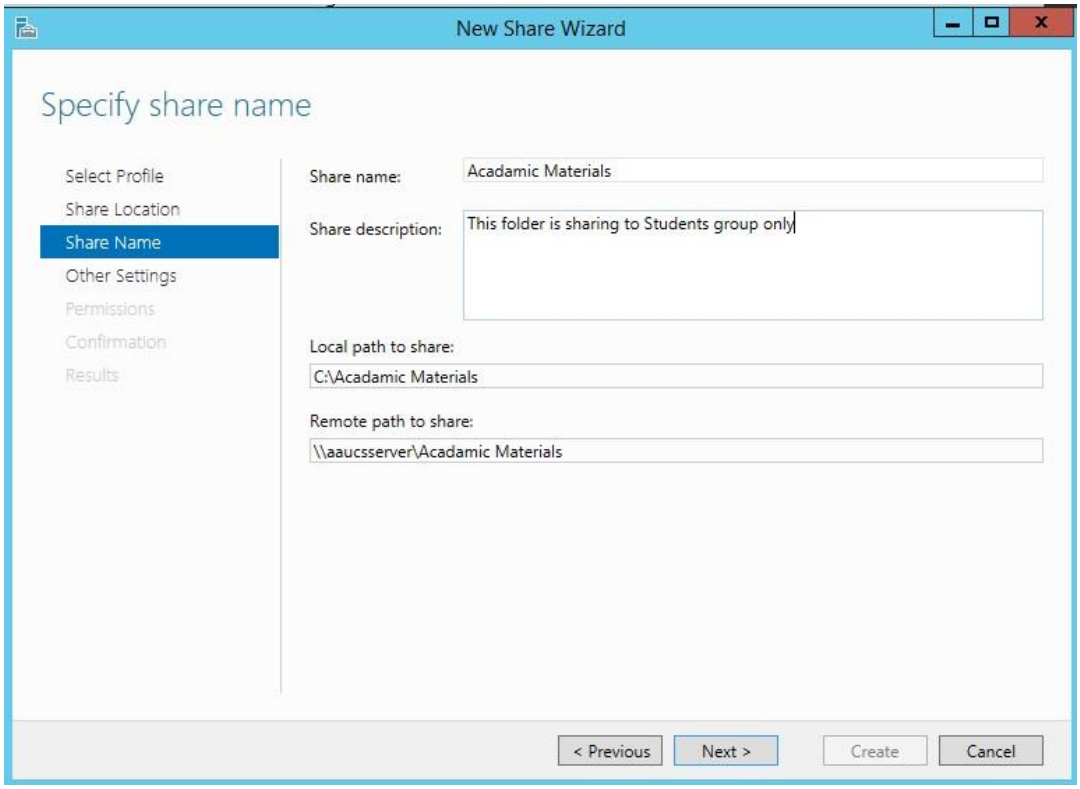

**New Share** wizard pops up. There are number of share profiles by default. You can choose any of these share profiles as you can see below. In our case we will choose **SMB Share** – **Quick** and click **Next**.



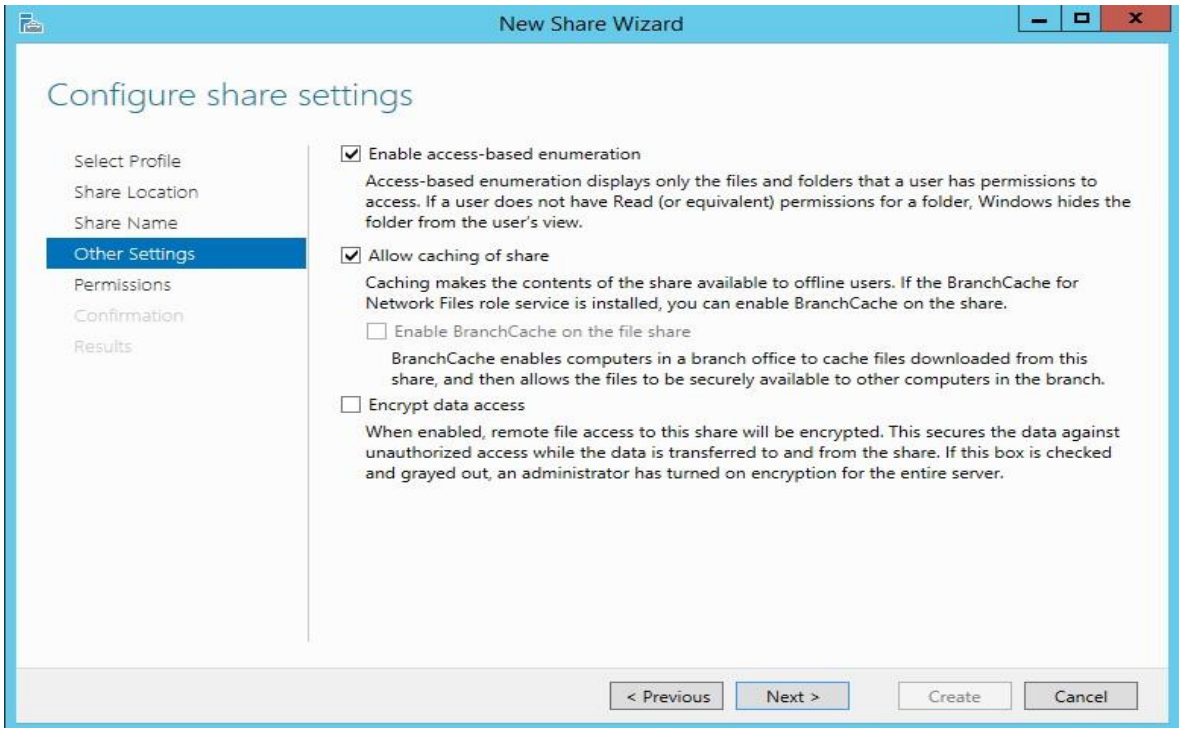
Now you are asked to provide the share location of the folder that you want to share. Here the chosen custom location is as **C:\Acadamic Materials**. Then click **Next**.



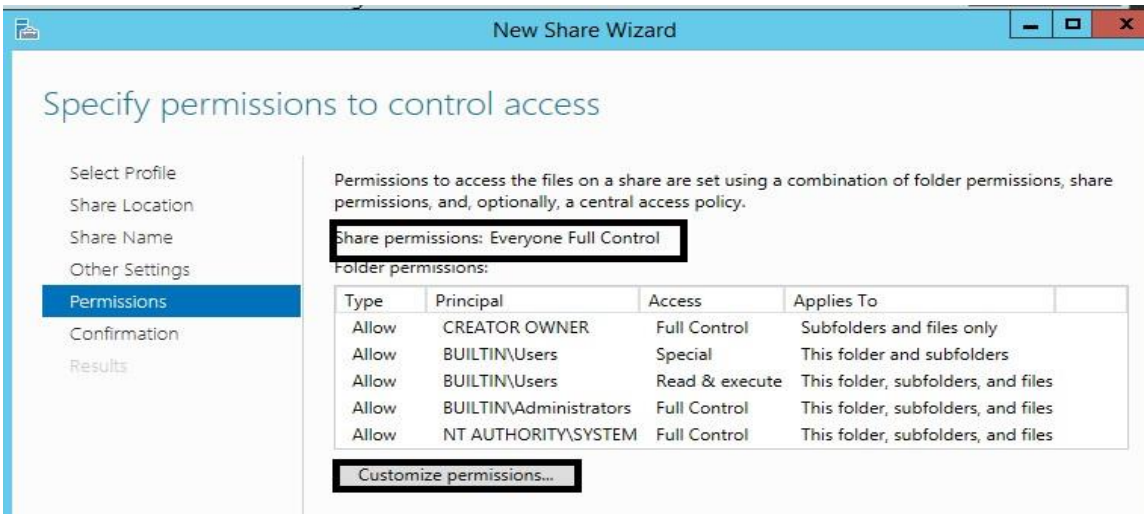

Type the **Share name** and description of the shared folder. Then click **Next**. Click **OK** to create the new directory on path doesn't exist warning will pop up.



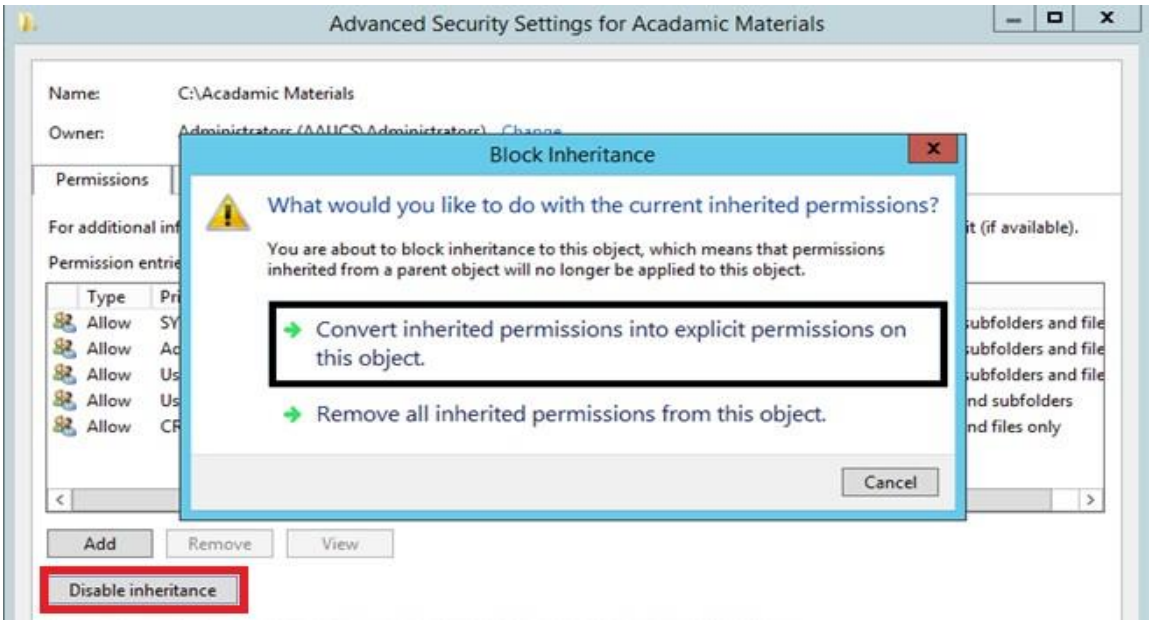
Now configure other settings. Here, you will check to **Enable access-based enumeration**. This option makes the folder visible for users that have permission to access the folder otherwise the folder will be hidden. Allow caching of share option makes the folder to be accessed even when the user is offline. Click **Next**.



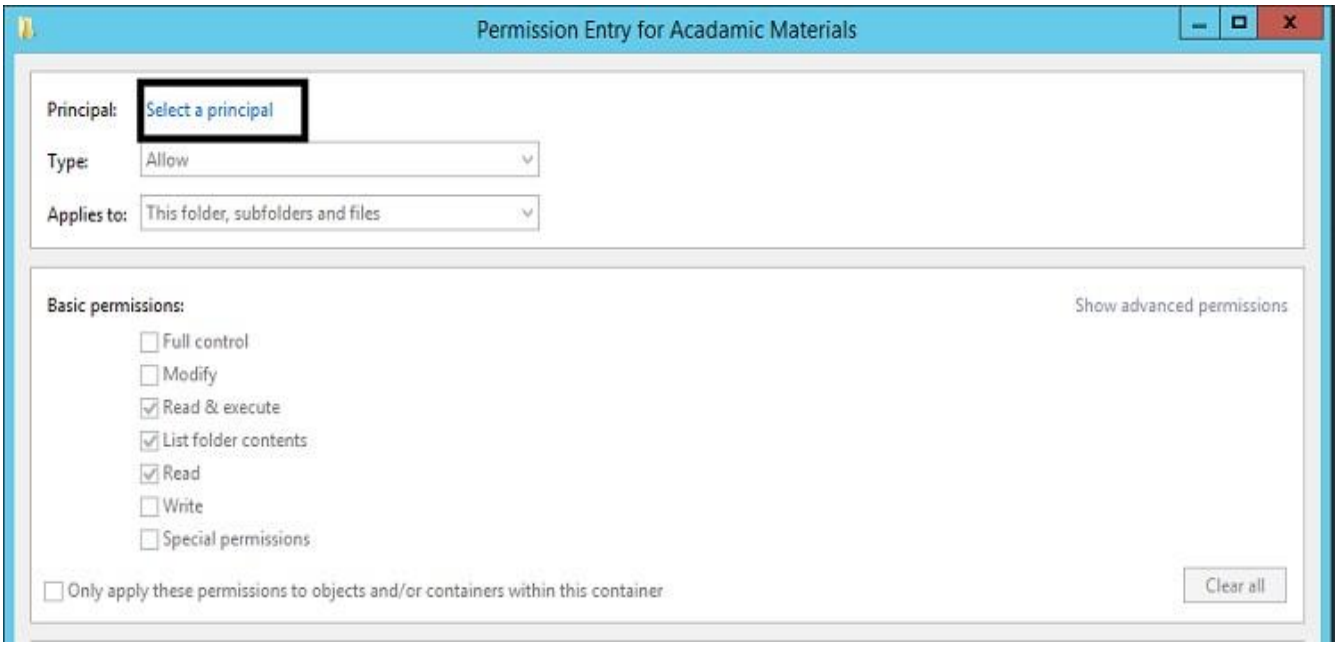

Then, configure the folder permission. The shared folder has shared folder permission and NTFS permission. These both permission works together to allow/deny users to access the shared folder. Microsoft recommends allowing full control for share permission and using **NTFS permission** to restrict and configure folder access. As you can see below, Share permissions: Everyone Full Control. The permission shown here is the **inherited NTFS** permission from drive **NTFS permission**. To change the permission, click Customize permission.

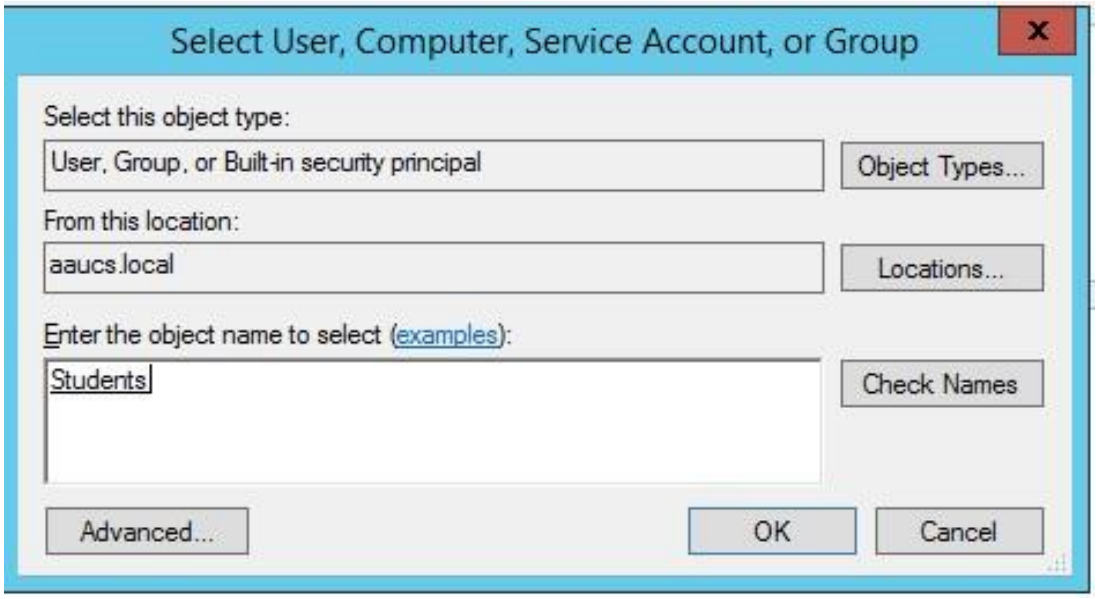


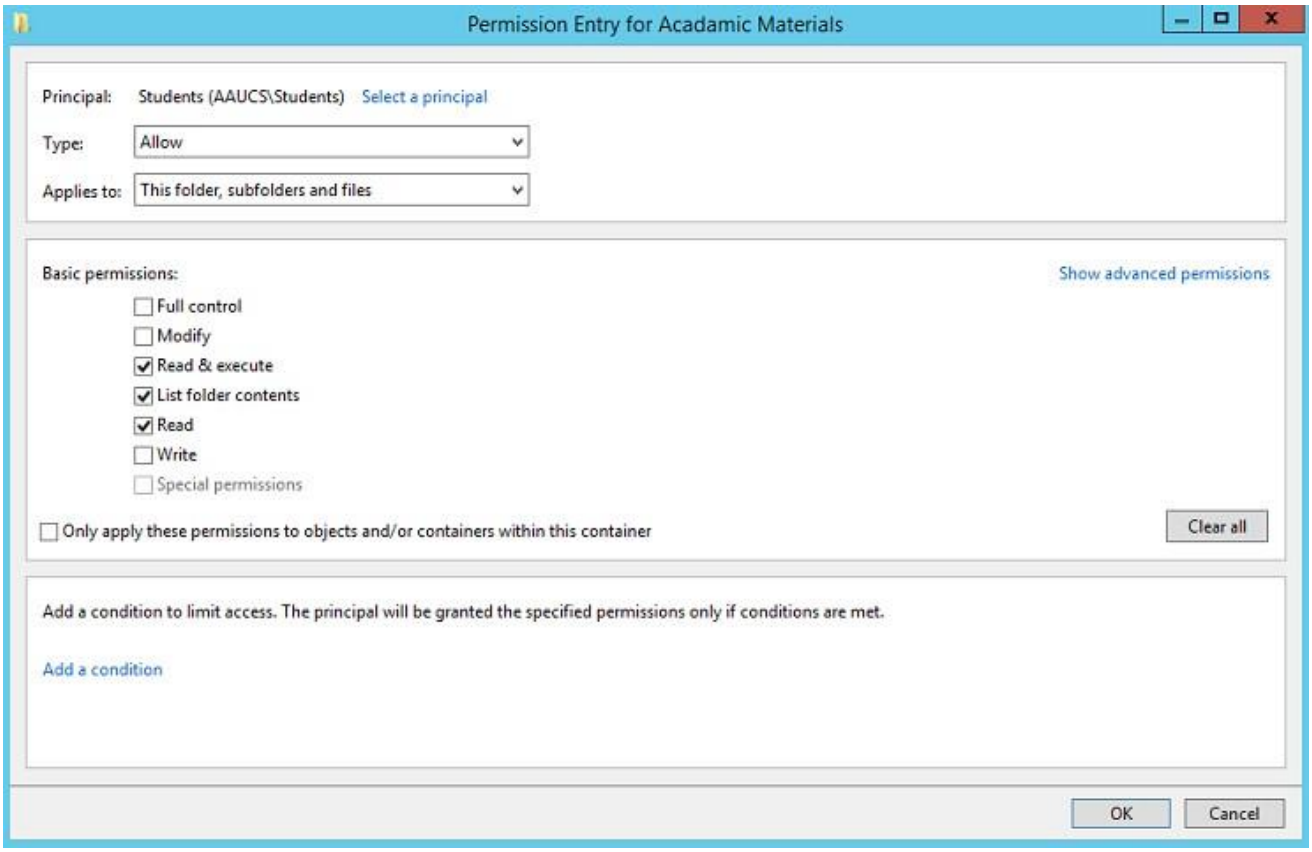

Click Disable **inheritance**. Then select **Convert inherited permission into explicit permissions on this object**.



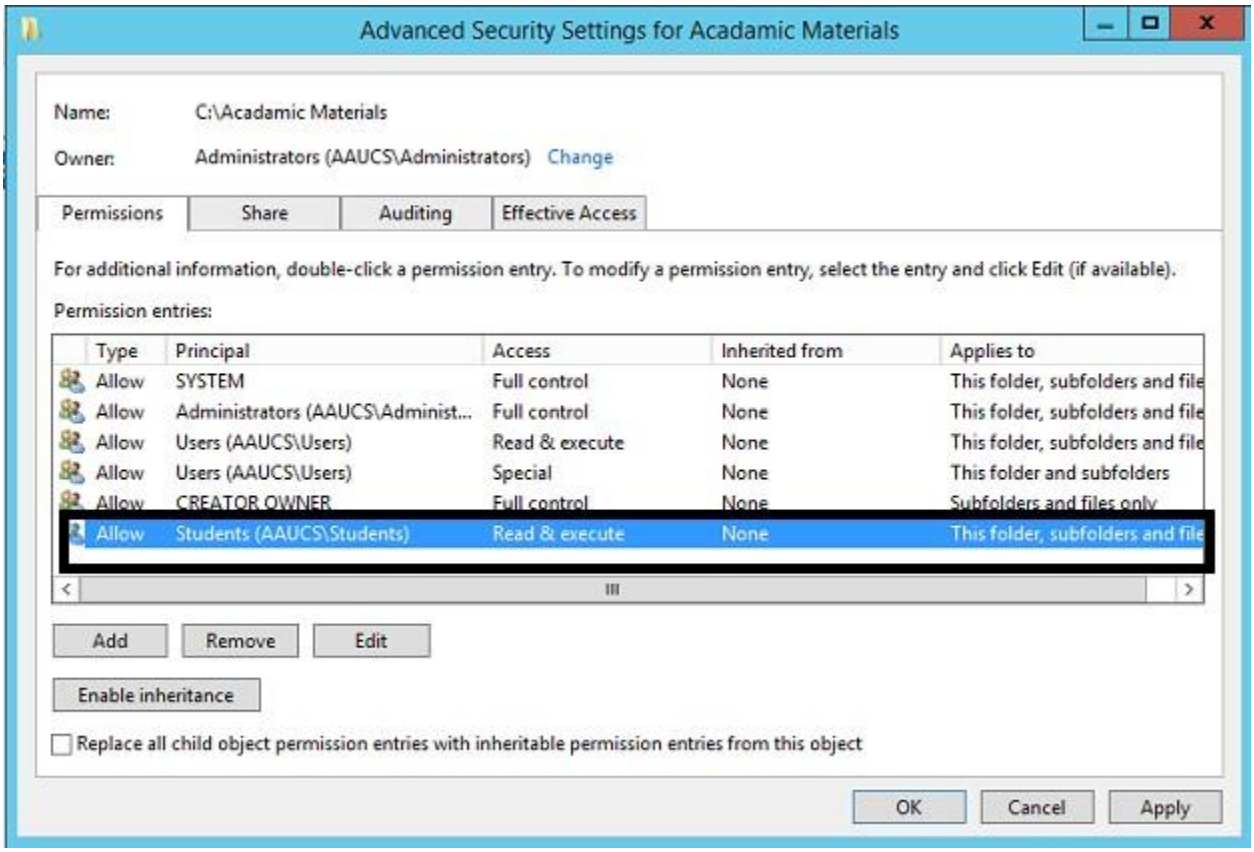

You can see the changes below. Remove both User groups from the permission. This Users group contains all the users of the domain. We don't want all the users of the domain to access this shared folder so remove it. Click **Add** to add the **Students** group. Click **Select a principal** and add **Students** group. Select the basic permissions and click **OK**.


Permission Entry for Acadamic Materials
Principal:
Select a principal
Type:
Allow
Applies to:
This folder, subfolders and files
Basic permissions:
Show advanced permissions
Full control
Modify
Read & execute
List folder contents
Read
Write
Special permissions
Only apply these permissions to objects and/or containers within this container
Clear all

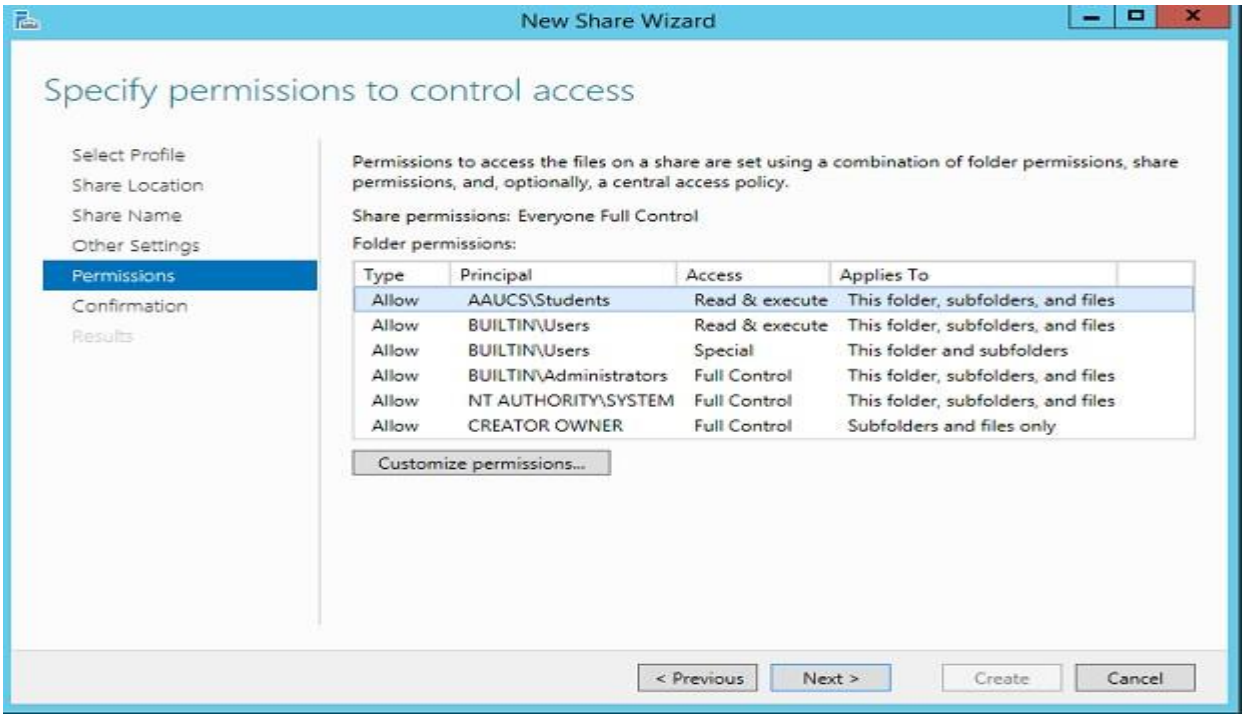

Select User, Computer, Service Account, or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
aaucs.local
Locations...
Enter the object name to select (examples):
Students
Check Names
Advanced...
OK
Cancel



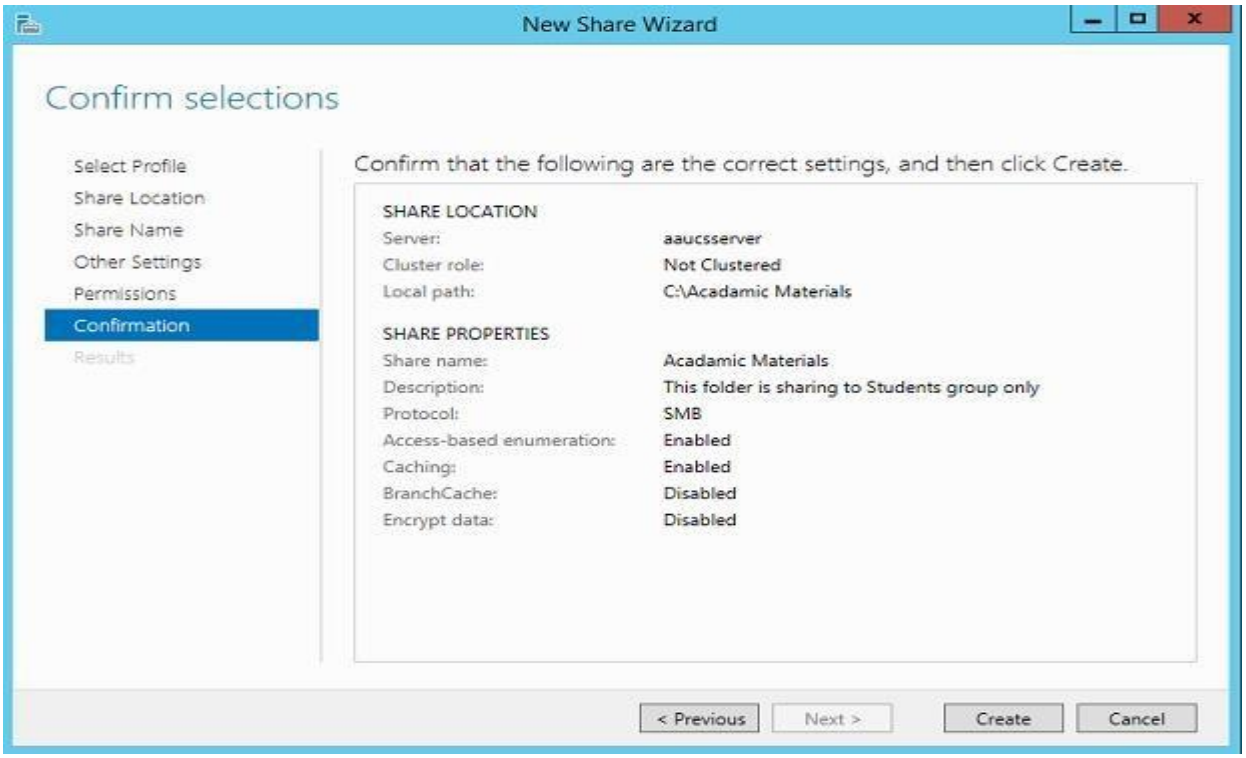

Now the overall permission for the **Academic Materials** folder looks like this. Users of **Students** group can only read the files of **Academic Materials** folder.

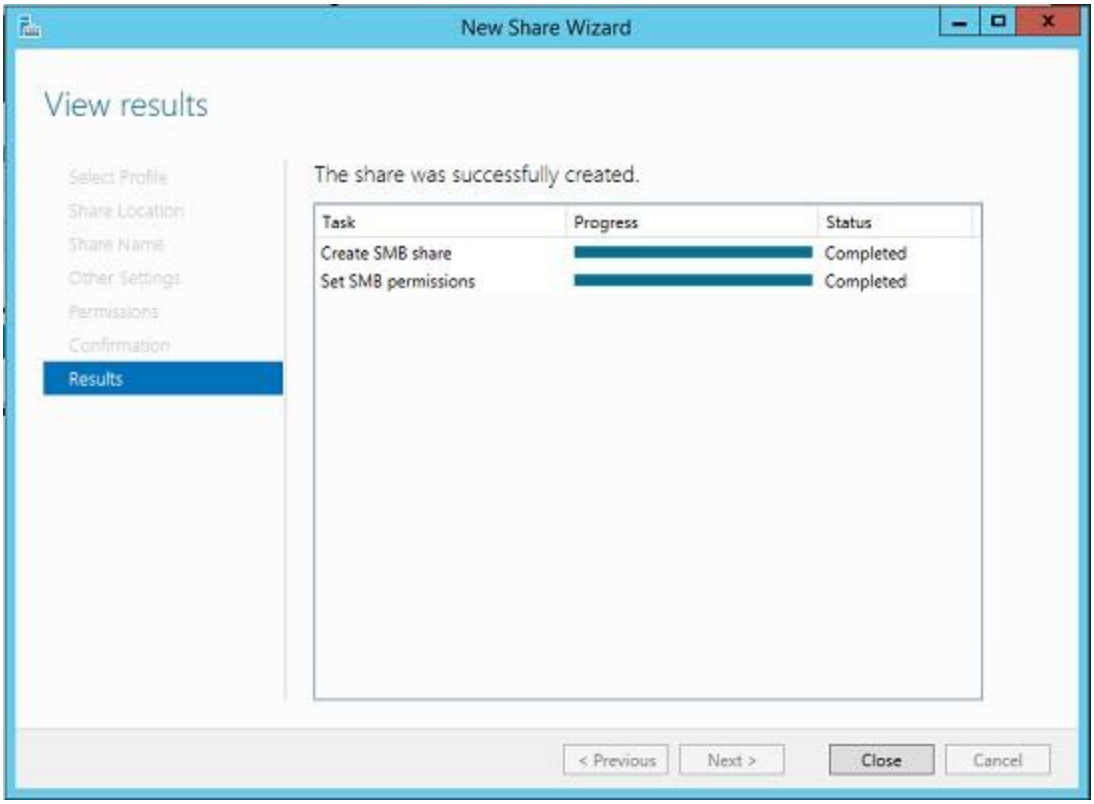



Now let's come back to the wizard and Click **Next**.

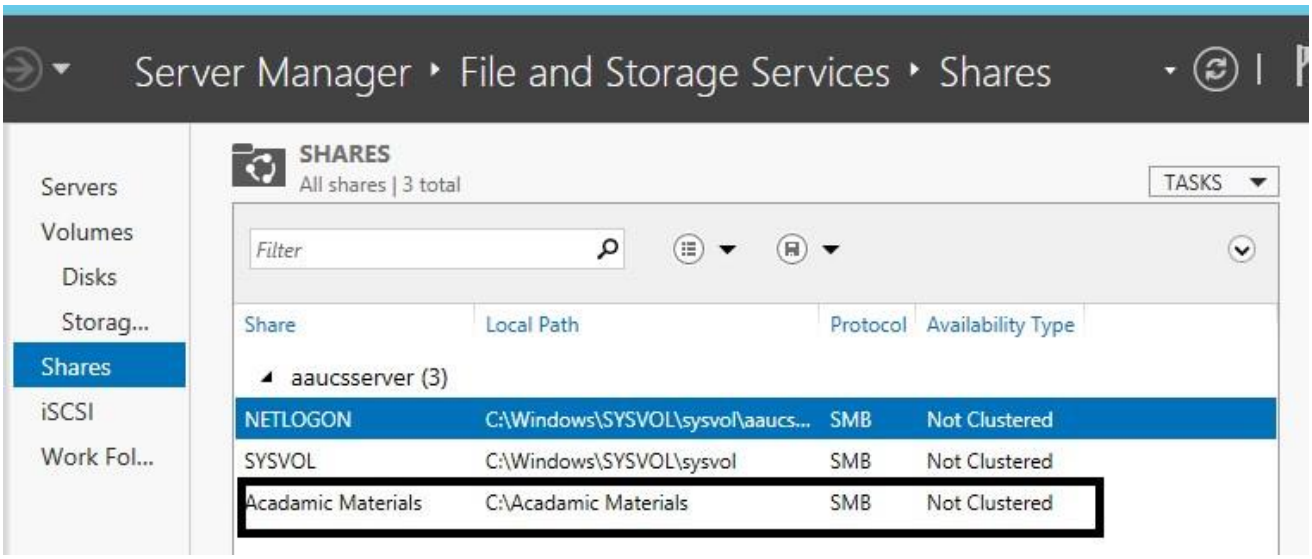



Review the settings and click **Create**.



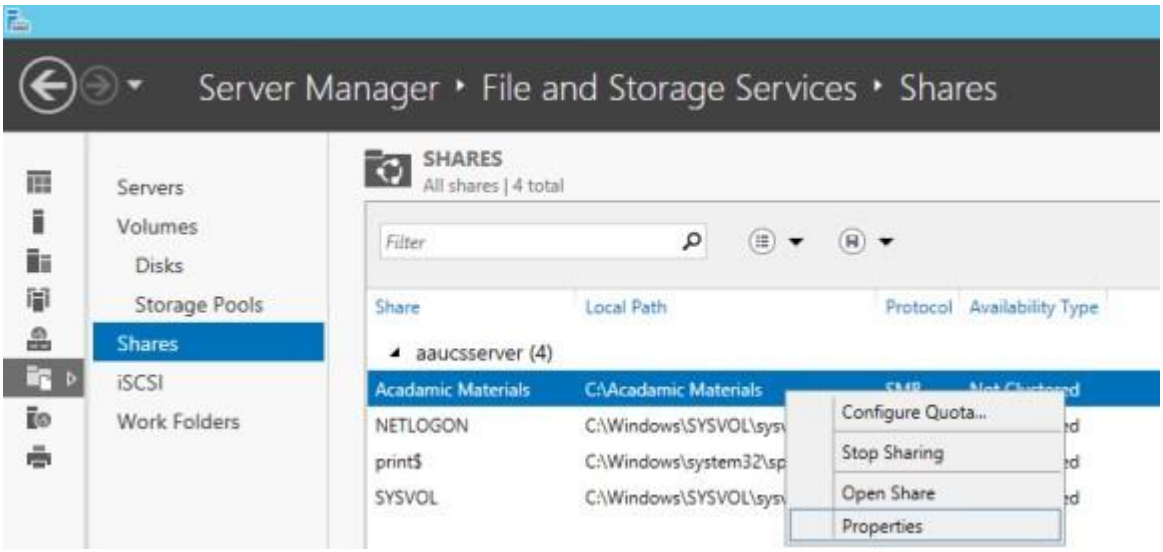




The shared folder is now created. You can view the shared folder in Server Manager Console.

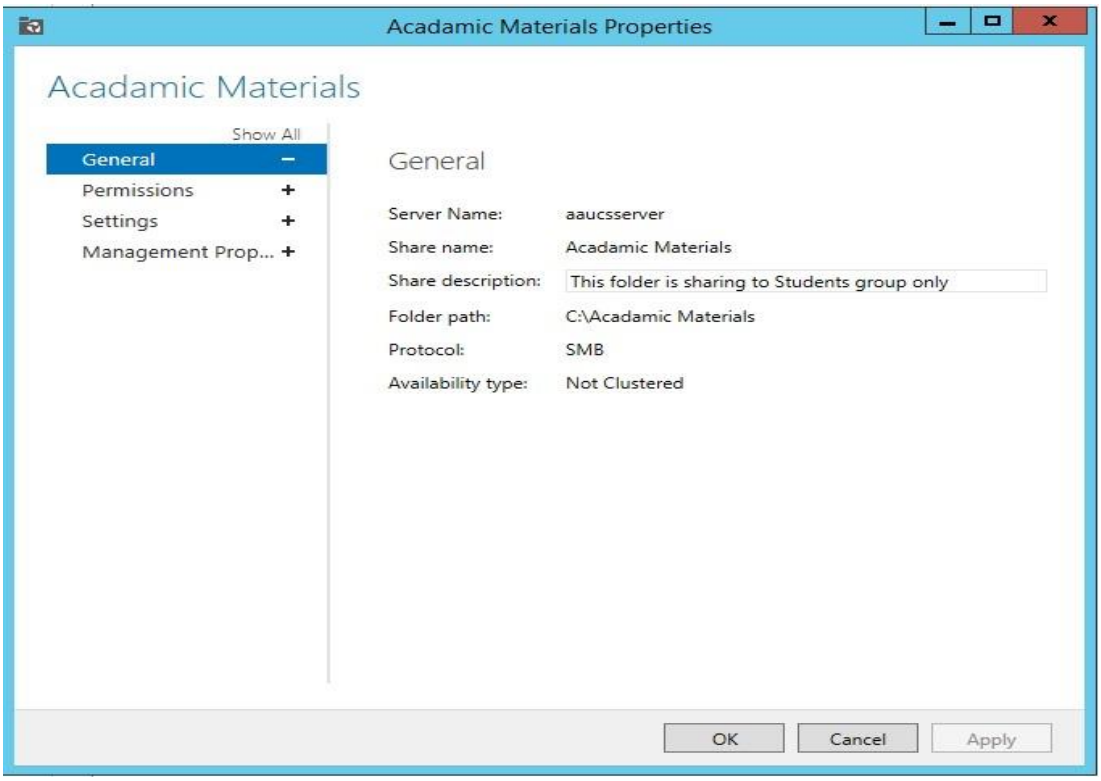



In this way you can configure shared folder using Server Manager. Remember, NTFS permissions and shared folder permissions are different. If NTFS permission and shared folder permission are conflicting, then the most restrictive permission is applied. For example, if you configure NTFS permission to Full Control and shared permission to Read on a folder then the permission applied will be Read only. Best practice to manage permissions for shared folder is, configure full control permission for everyone and restrict the folder access using NTFS permission.

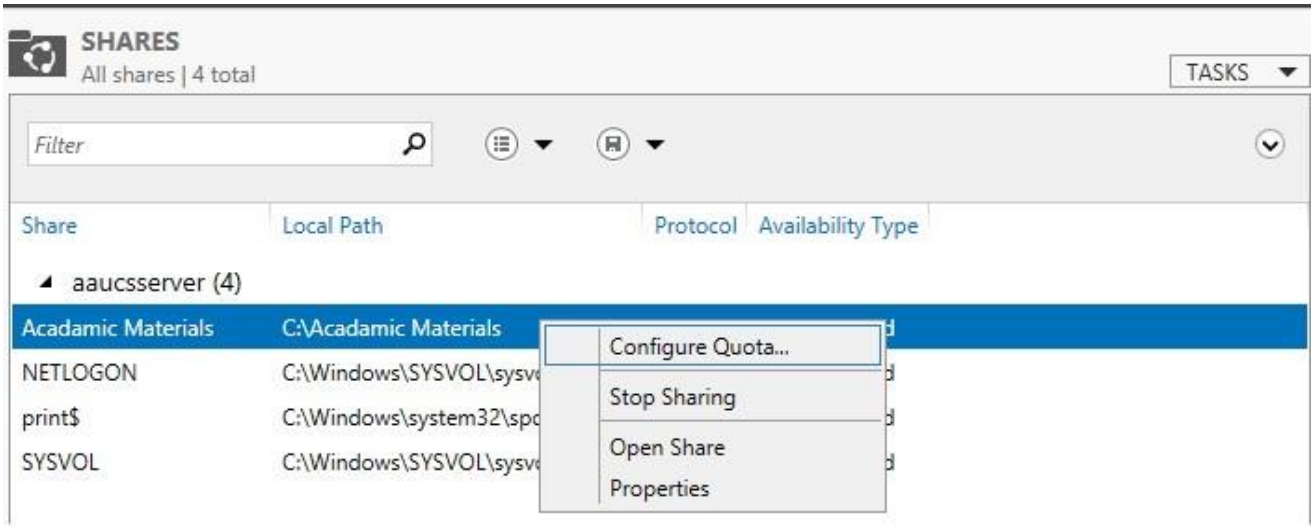
You can see the details of the shared folder by right clicking on it and select **properties** from the given options.



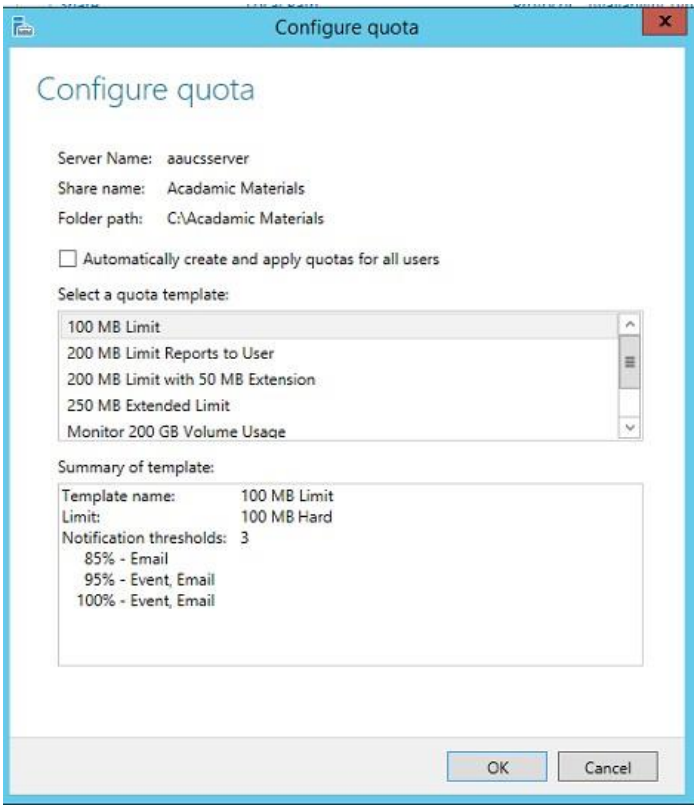
In the **properties** of a shared folder window there are four options that you are going to see and configure, these are **permissions**, **settings** and **management properties**.




To configure the disk quota for a shared folder first select your shared folder, right click on it and select the **configure quota** option.

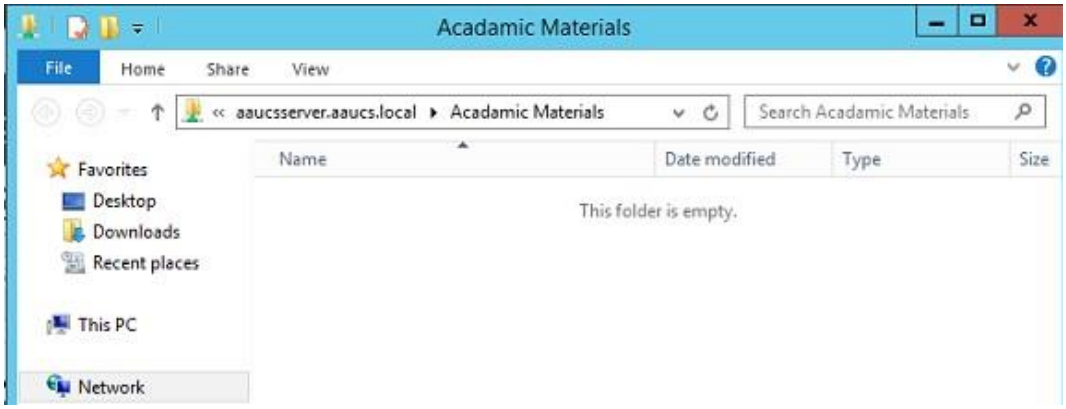


In the pop up disk quota configuration window you can assign any of quotas that you want from the given list of **quota template**. (We will see in detail about disk quota in the next topic)




Clients can now access the shared folder by typing the Universal Naming Convention (UNC) path of the shared folder in windows explorer.

In our case the **UNC** path is **\\aaucsserver.aaucs.local\AcadamicMaterials**. In this way we can access the shared folder contents.

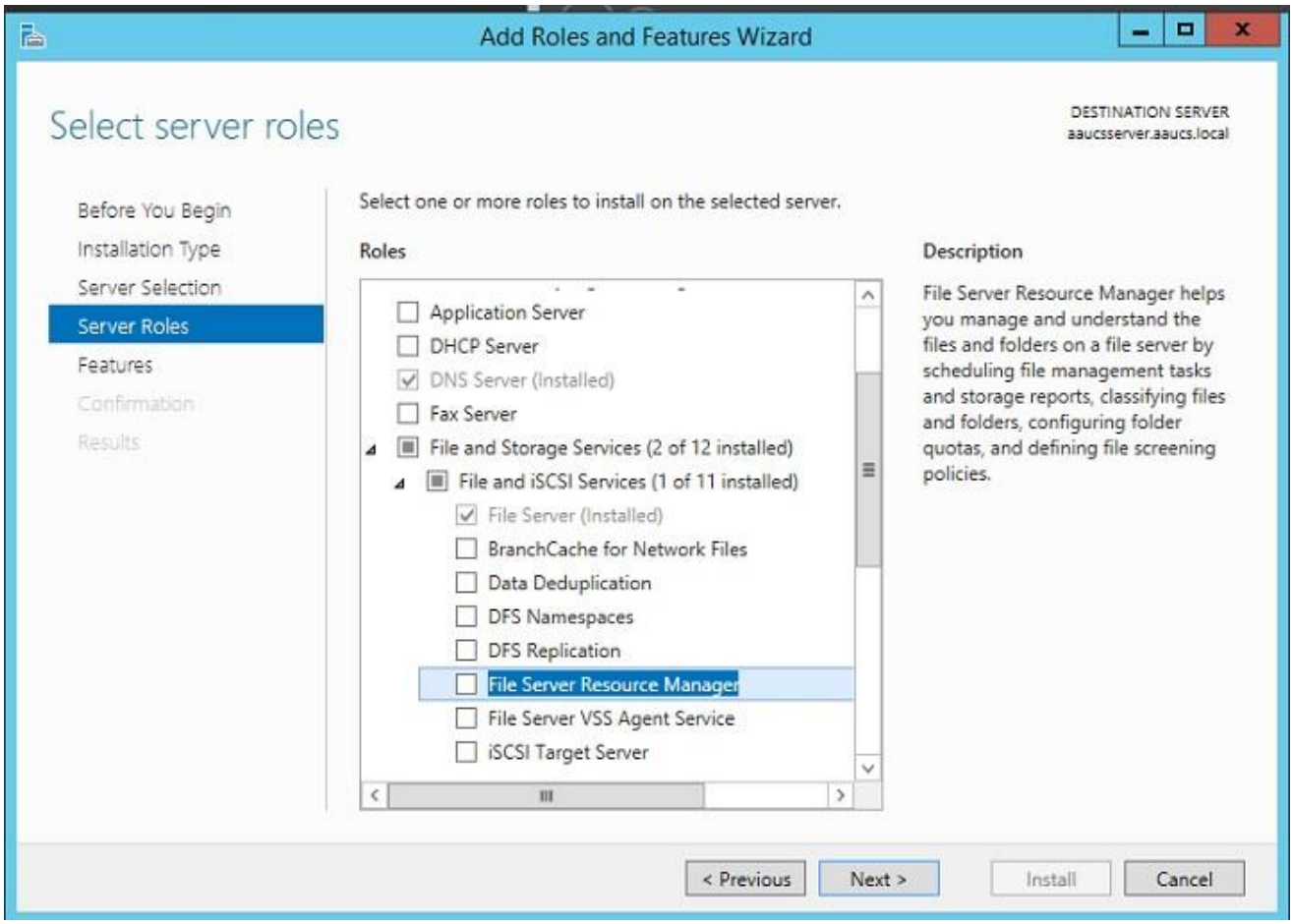


## 11.2 Disk quota management

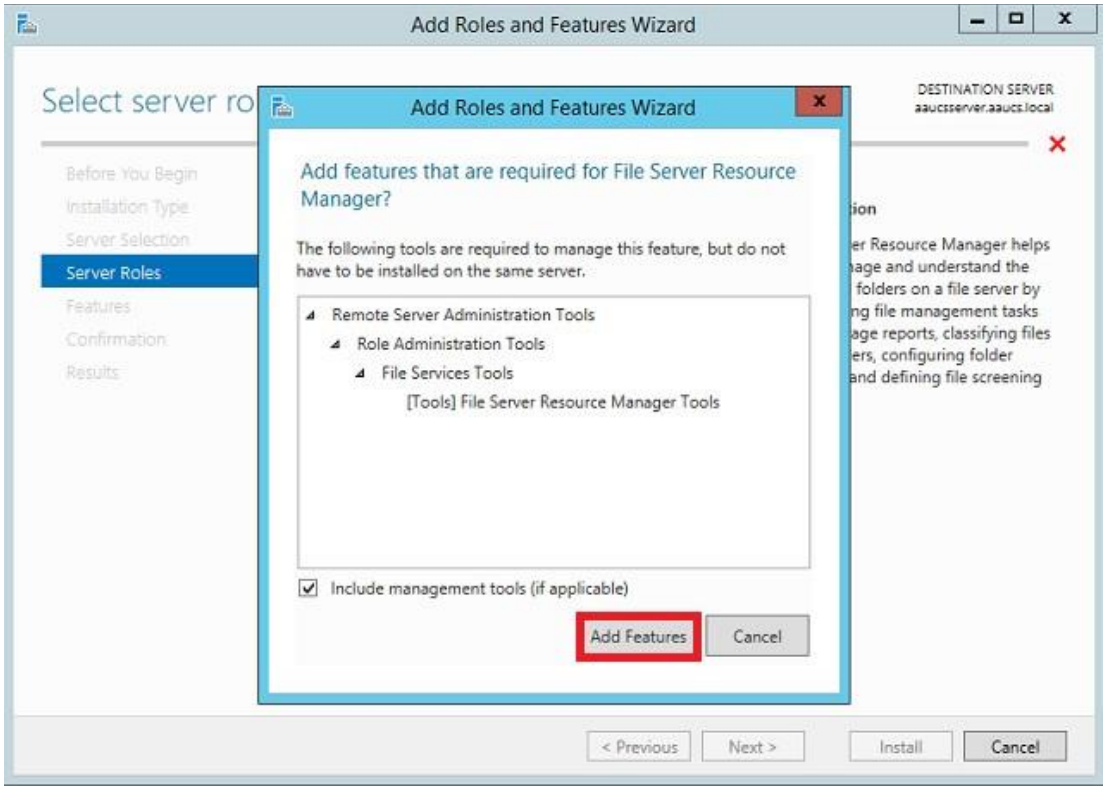
Disk quota management is a permission specified by administrators that set limits on the user, workgroups, or other groups of storage space. By setting a quota, this helps prevents a server or share from becoming full of data, but still allows users to save files.

Before to set or enable a disk quota the **File Server Resource Manager** (**FSRM**) role must be installed in your server, to install it follow the next steps:

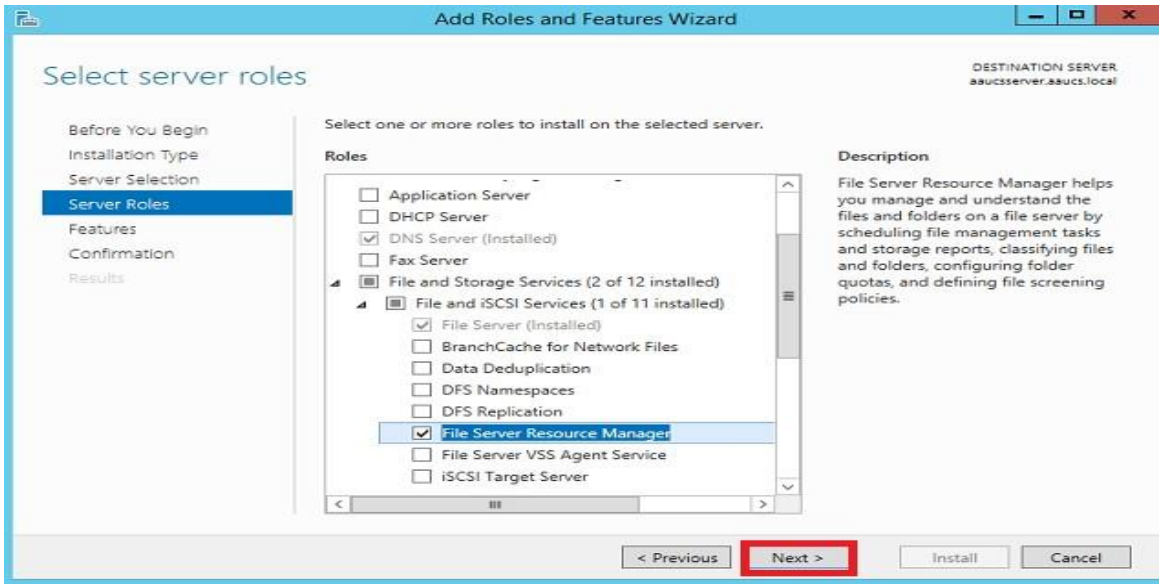
4. Go to the **Server manager** and click on **Add Roles and features** from the **Manage** menu.
5. Select role- based or feature based installation and click **Next** in the next pop up window.
6. Select your destination server from the server selection window and click **Next.**
7. Select **file and storage services -> File and ISCSI services -> File server resource manager** roles from **server roles** window



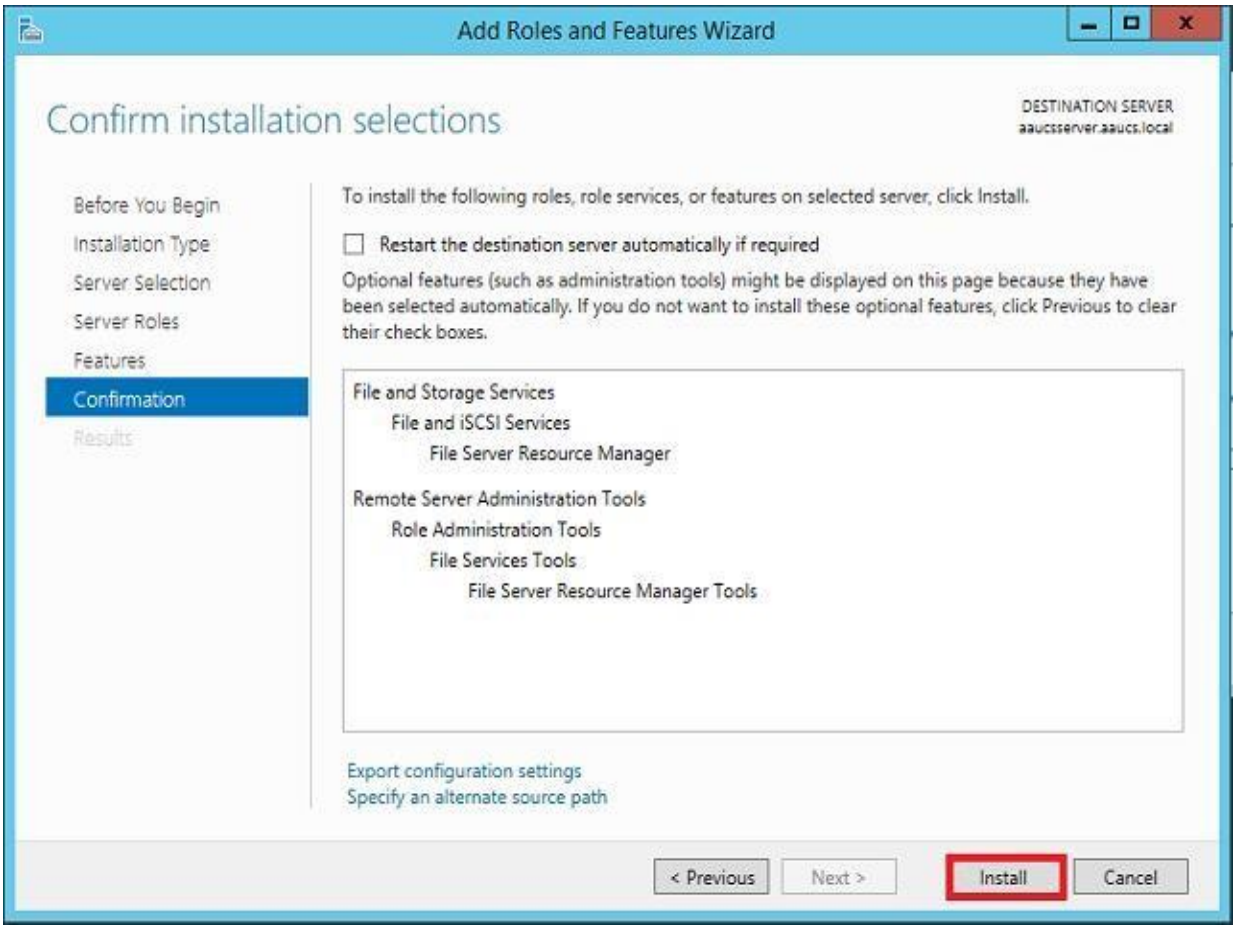
- Click on **Add Features**.

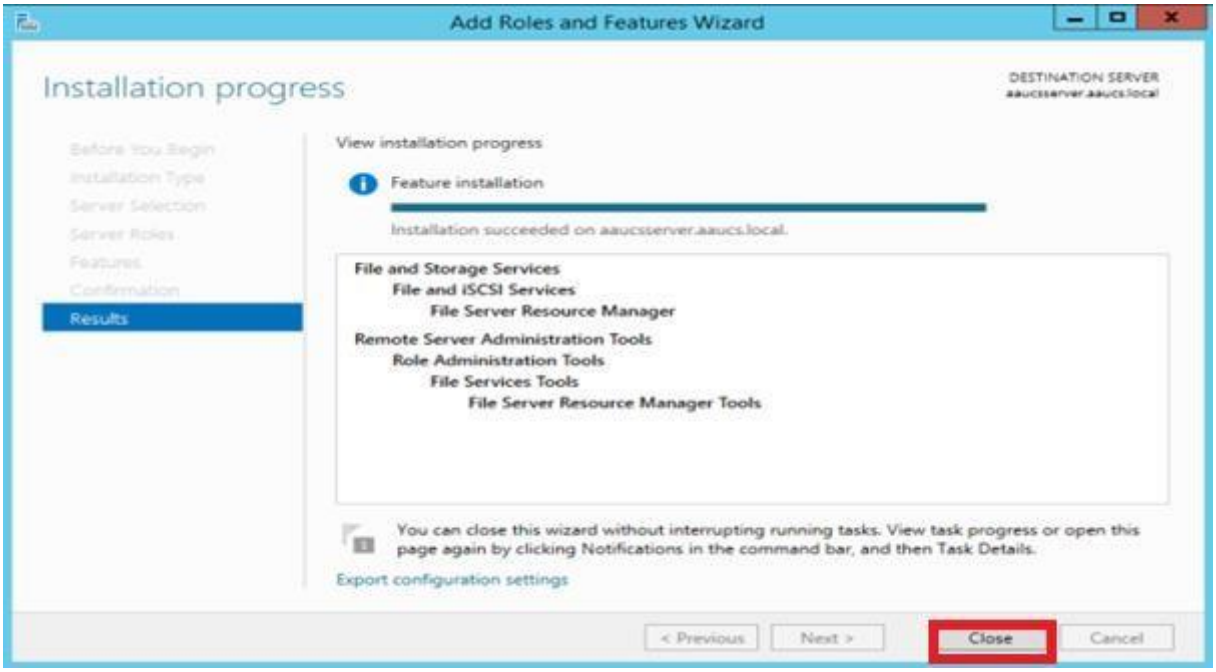



- Click **Next**.



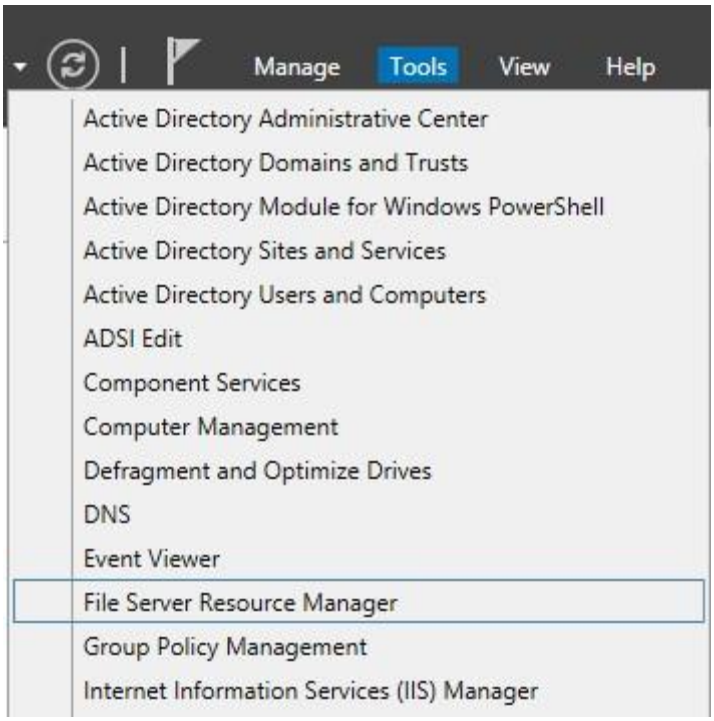

8. In the confirmation window click **Install** button and the installation takes few minutes to complete.


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
aaucsserver.aaucs.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
File and Storage Services
File and iSCSI Services
File Server Resource Manager
Remote Server Administration Tools
Role Administration Tools
File Services Tools
File Server Resource Manager Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

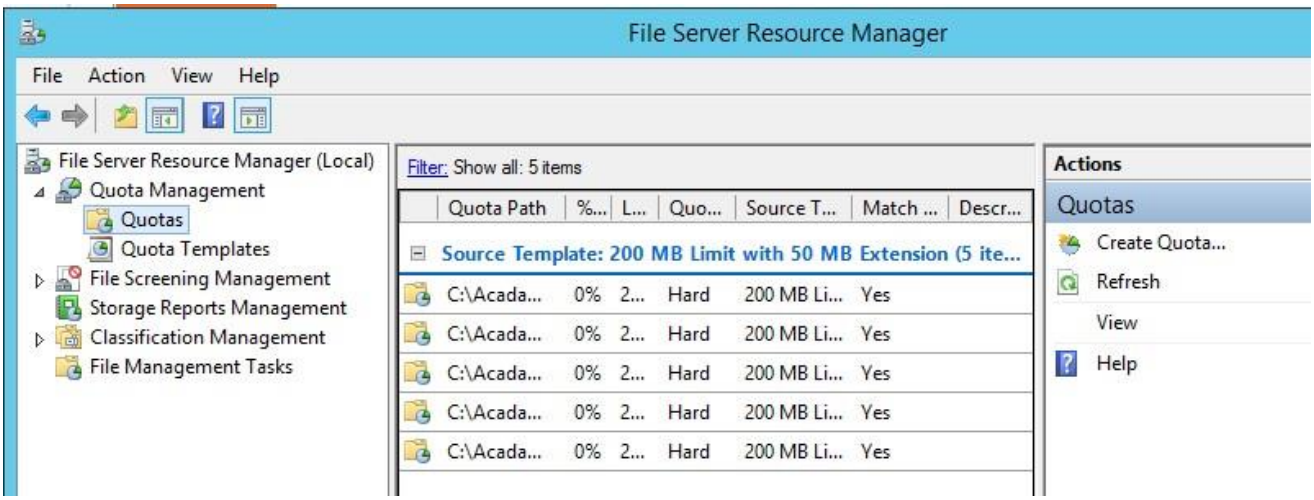

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
aaucsserver.aaucs.local
Results
View installation progress
Feature installation
Installation succeeded on aaucsserver.aaucs.local.
File and Storage Services
File and iSCSI Services
File Server Resource Manager
Remote Server Administration Tools
Role Administration Tools
File Services Tools
File Server Resource Manager Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

### 11.2.1 Creating a quota

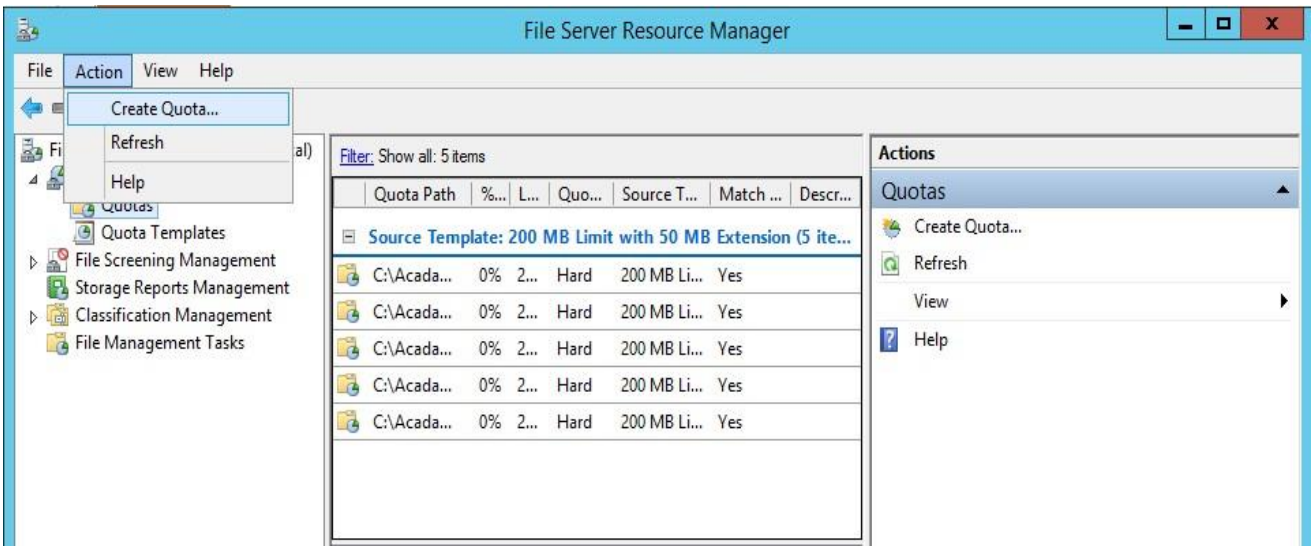
1. Open **Server Manager** using the icon on the desktop Taskbar or from the Start screen as usual.
2. Select **File Server Resource Manager** from the **Tools** menu in Server Manager.



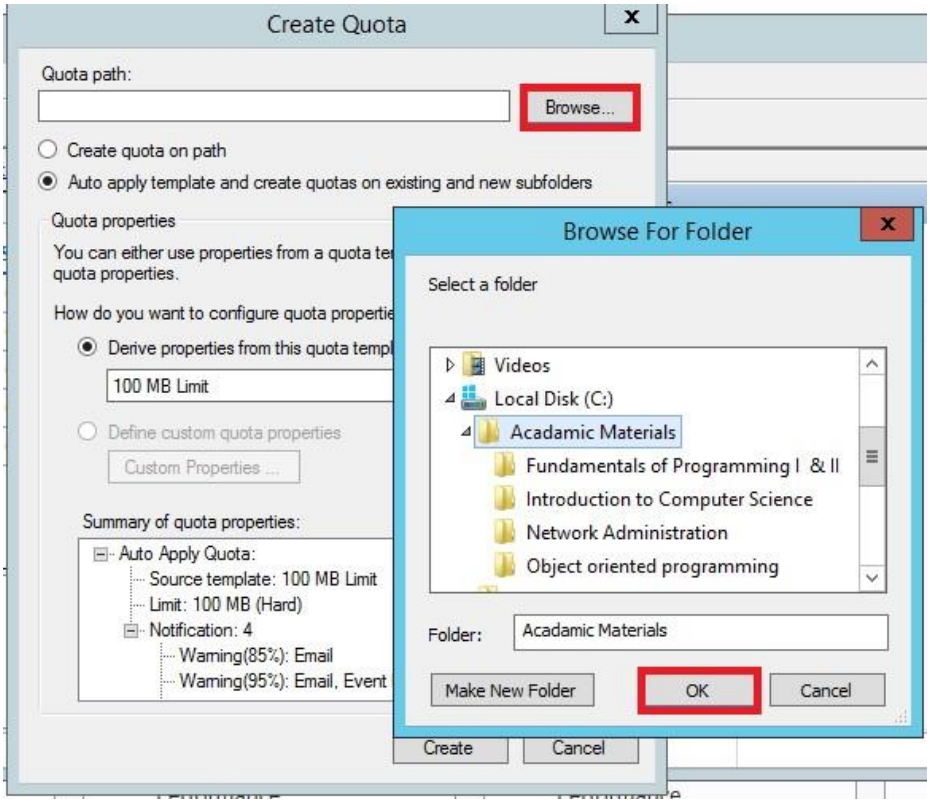

3. In the left pane of **File Server Resource Manager**, expand **Quota Management** and click **Quotas**



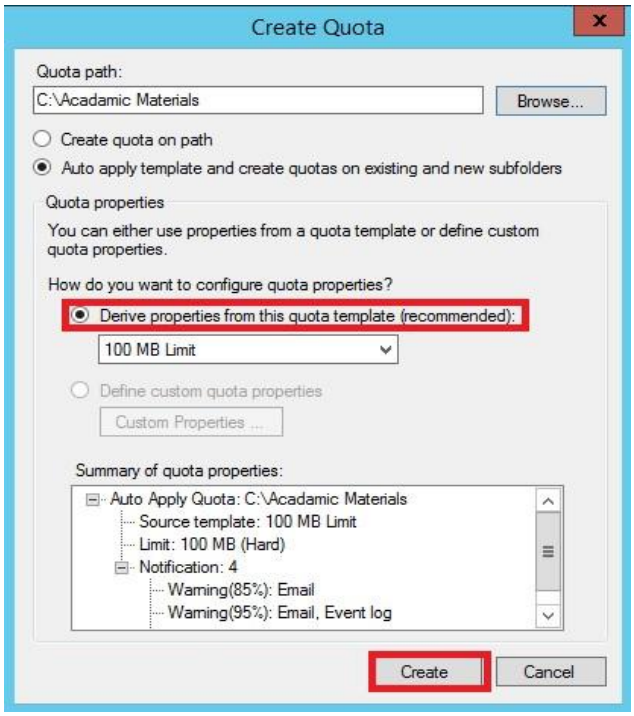

4. In the **Actions** menu click **Create Quota**.



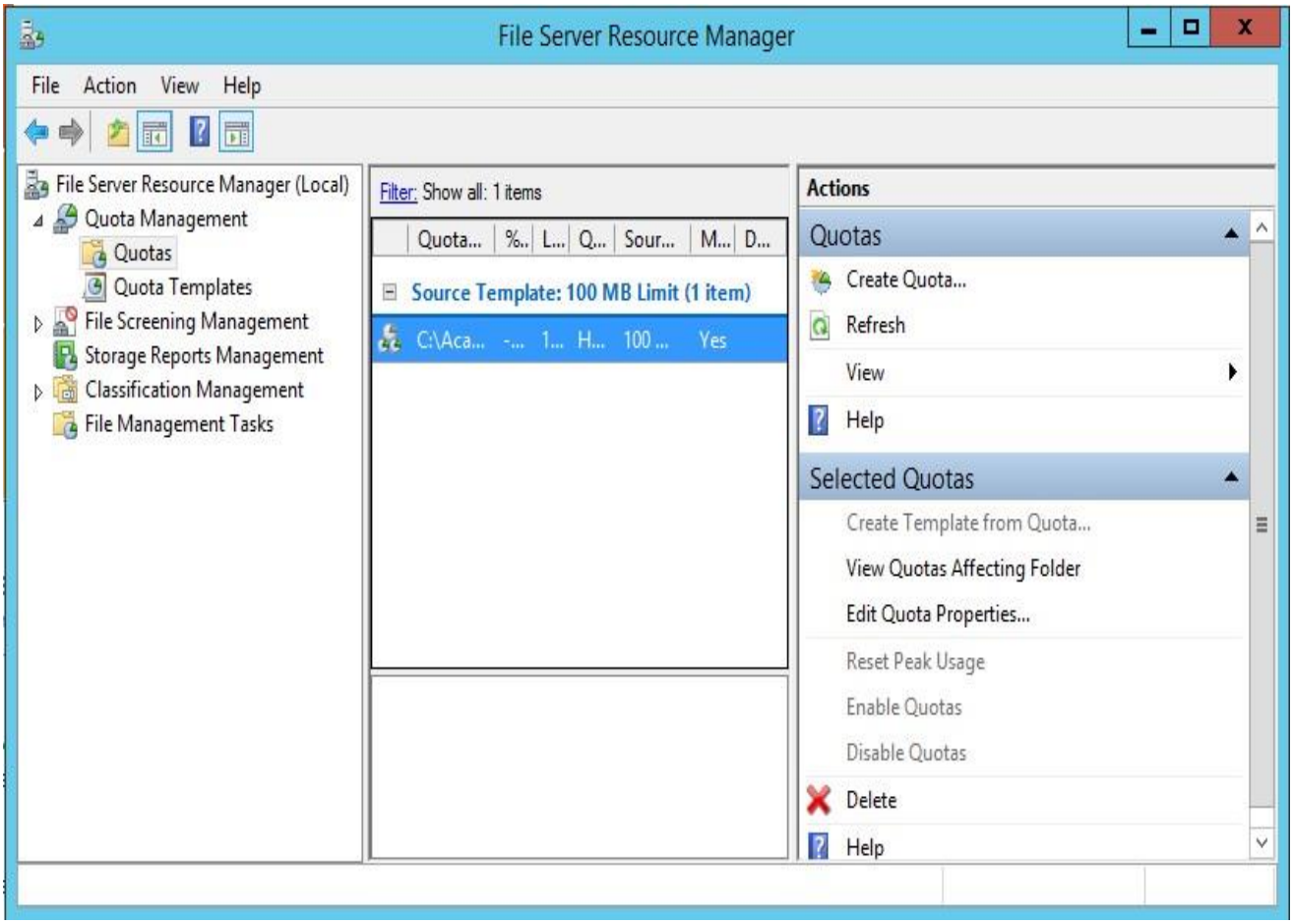

5. In the **Create Quota** dialog, click **Browse** to select the folder to which you want to apply the quota. In this example, c:\Acadamic Materials and then selected **Auto apply template and create quotas on existing and new subfolders** to make certain that any folders added for new users are also included in the quota policy.




6. *Derive properties from this quota template (recommended),* Select the quota template you'd like to apply and click **Create**.




✓ Your quota has been created successfully.



## 11.3 File Screening Management

On the **File Screening Management** node of the File Server Resource Manager, you can perform the following tasks:

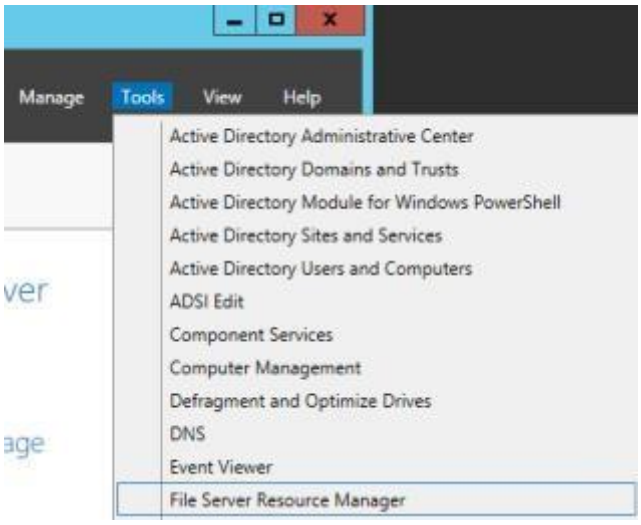
- Create file screens to control the types of files that users can save, and generate notifications when users attempt to save unauthorized files.
- Define file screening templates that can be applied to new volumes or folders and that can be used across an organization.
- Create file screening exceptions that extend the flexibility of the file screening rules.

For example, you can:

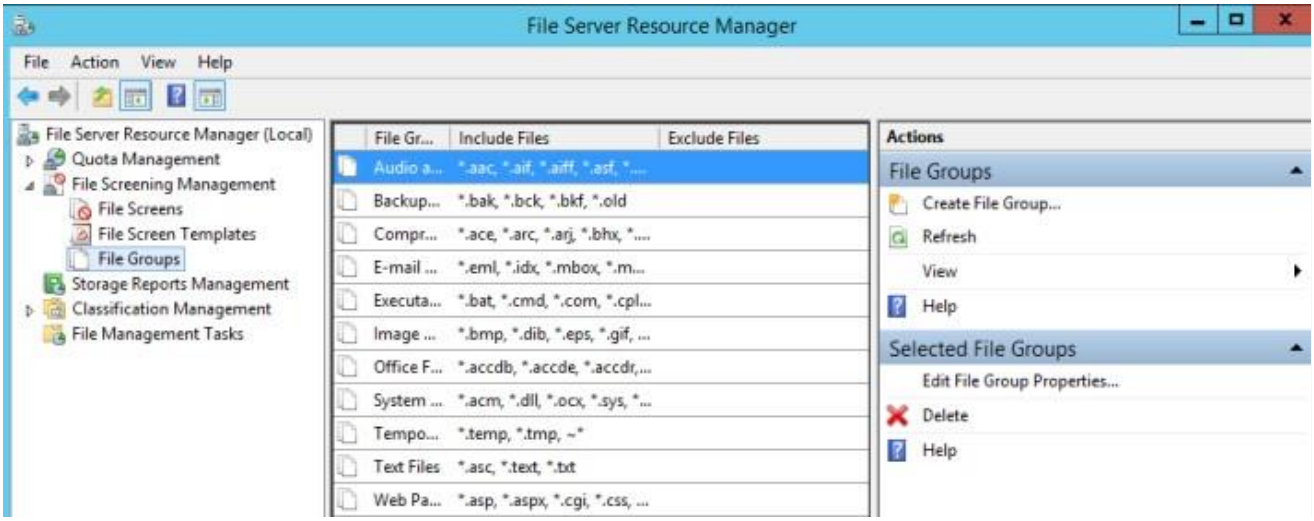
- Ensure that no music files are stored on personal folders on a server—yet you could allow storage of specific types of media files that support legal rights management or comply with company policies. In the same scenario, you might want to give a boss in the company special privileges to store any type of files in his personal folder.
- Implement a screening process to notify you by e-mail when an executable file is stored on a shared folder, including information about the user who stored the file and the exact location of the file, so that you can take the appropriate precautionary steps.

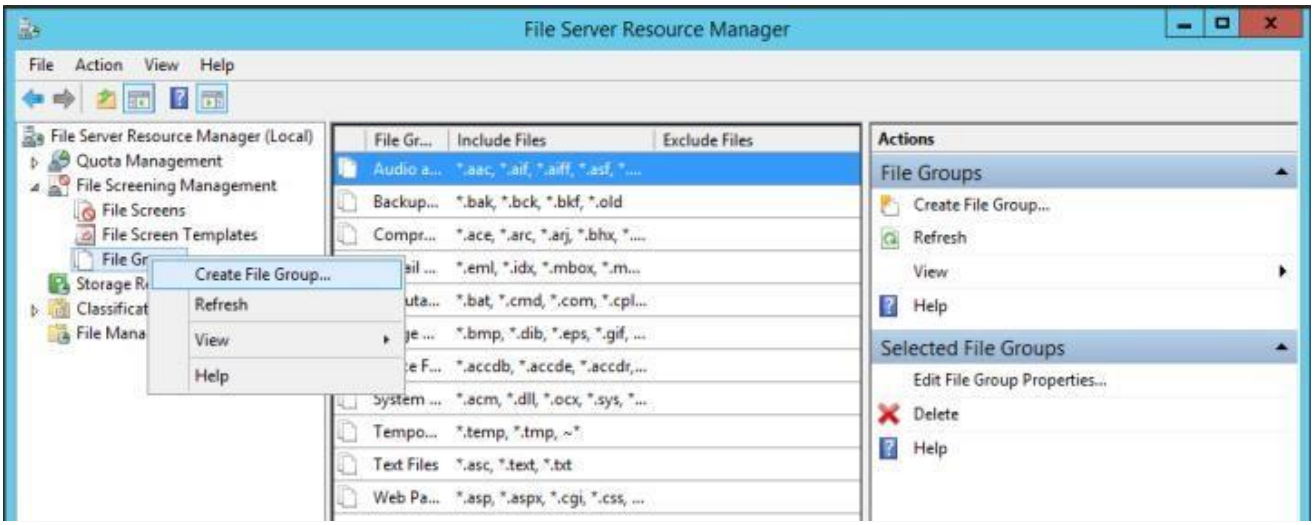
Steps of file screening management

1. Go to **Tools** select **File Server resource manager**.

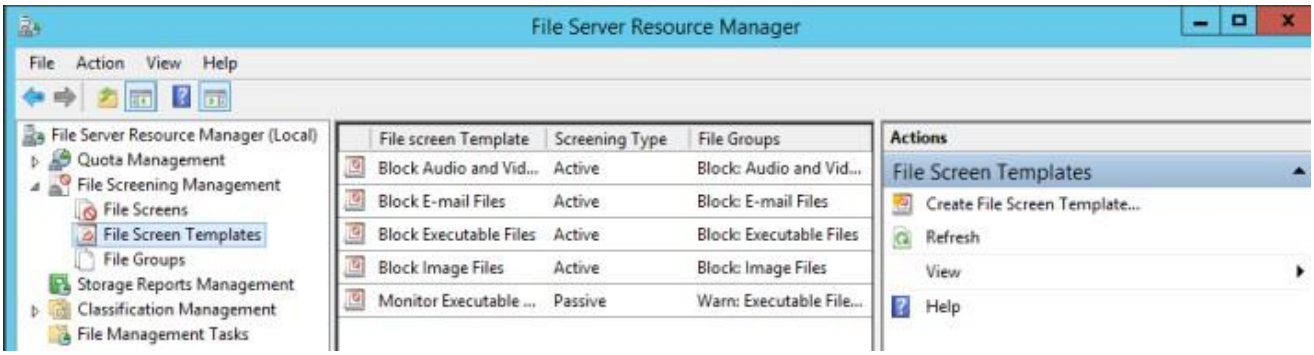


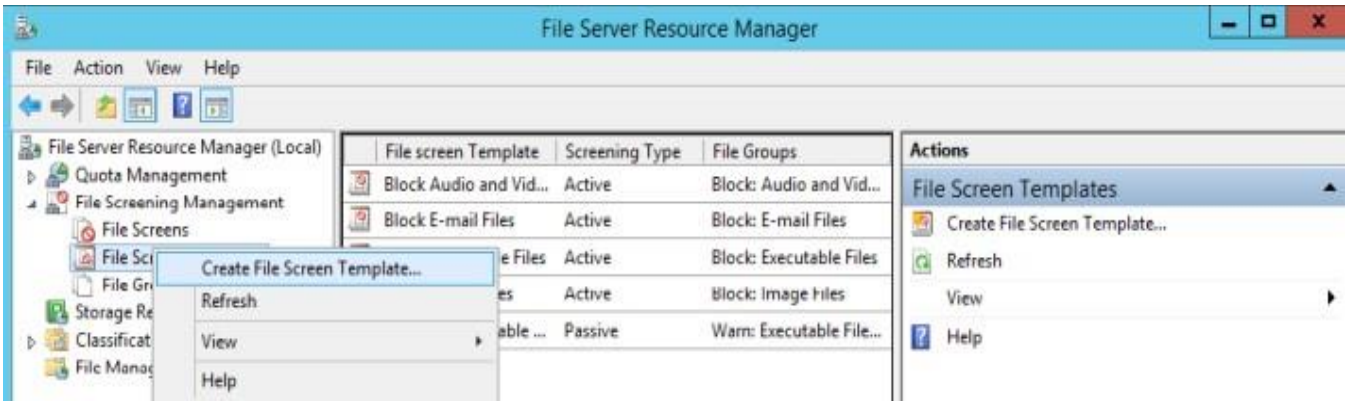
2. In the **Create File Group Properties** window, in the **File group** name box, you can see the available included and excluded file groups and create your own file group by right click on **File group.**



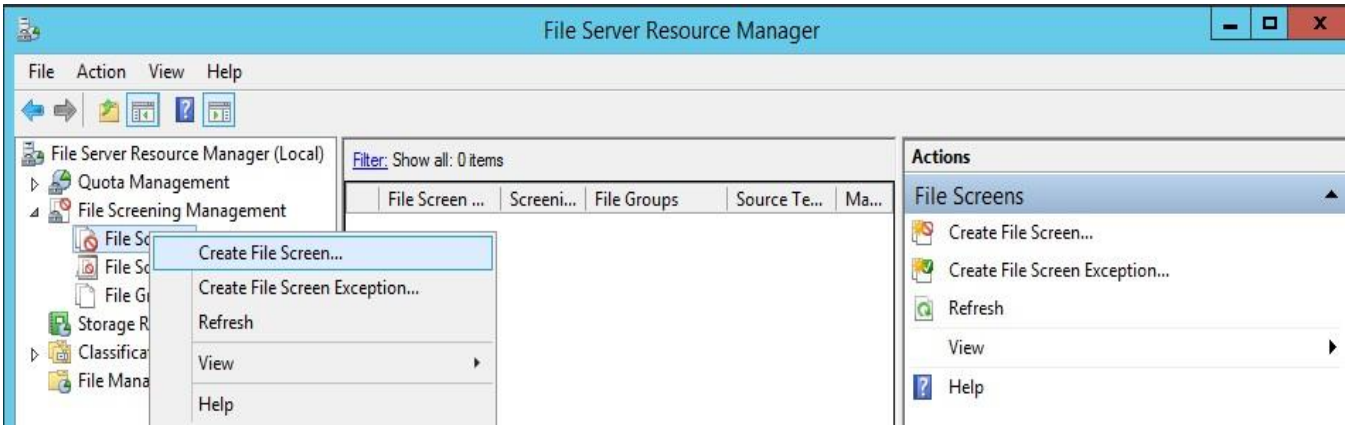




3. In the **Create File Group Properties** window, in the **File screen template** name box, you can see the available file templates with screening type and file group groups and also you can create your own file templates by right clicking on **File screen template** and **select Create file template.**

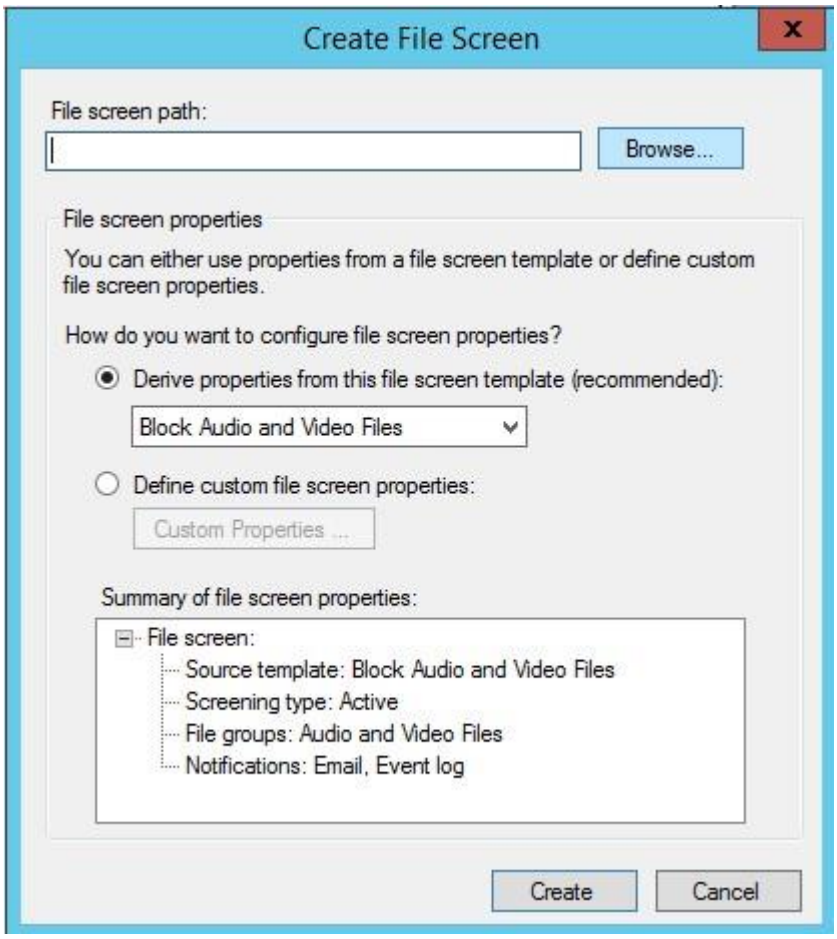


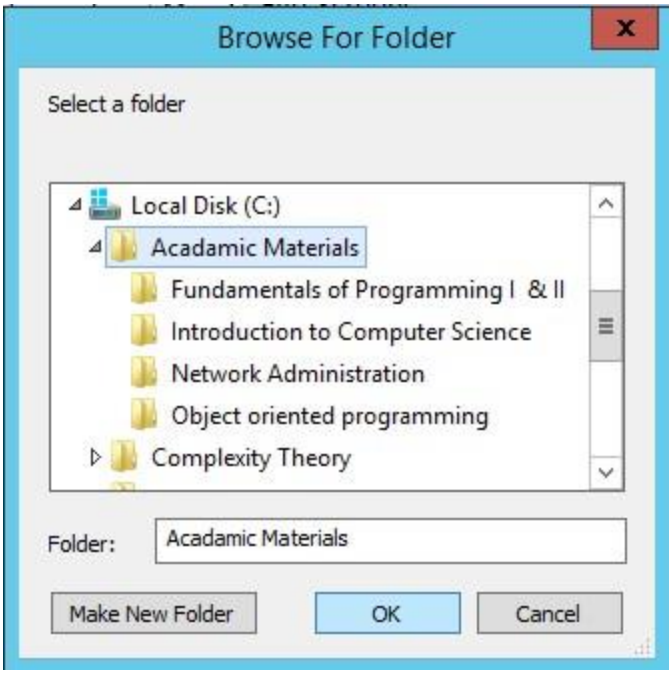



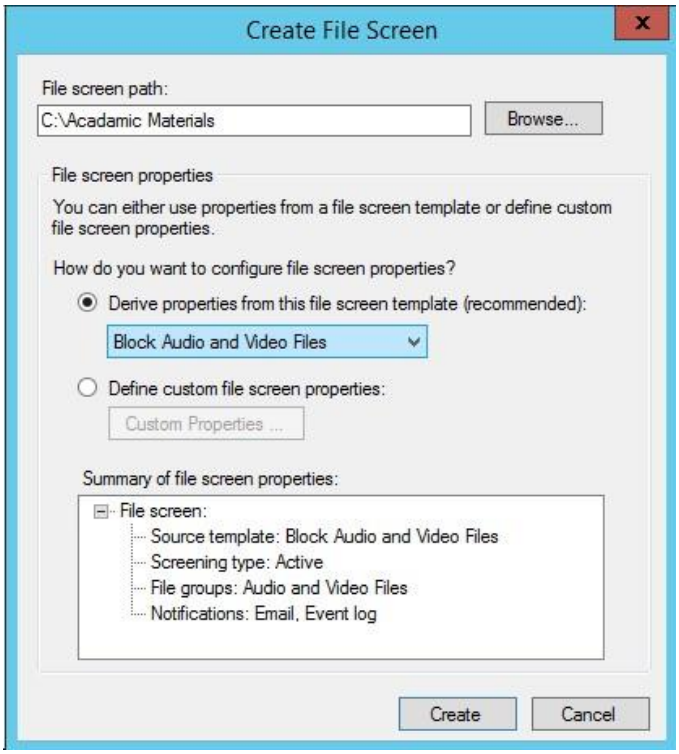

4. You can create a **file screen** option for your shared folder on file screens name box by right clicking and selecting **Create File Screen option**.



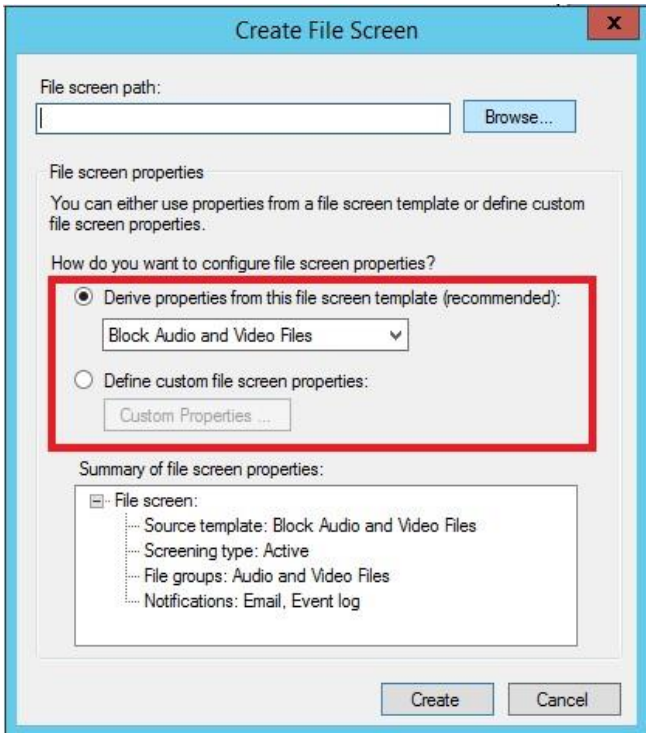

5. On the **File screen window** the first step is click the **Browse** button under file screen path option and select your shared folder directory or the file screen path.


Create File Screen
File screen path:
Browse...
File screen properties
You can either use properties from a file screen template or define custom file screen properties.
How do you want to configure file screen properties?
Derive properties from this file screen template (recommended):
Block Audio and Video Files
Define custom file screen properties:
Custom Properties ...
Summary of file screen properties:
File screen:
Source template: Block Audio and Video Files
Screening type: Active
File groups: Audio and Video Files
Notifications: Email, Event log
Create
Cancel

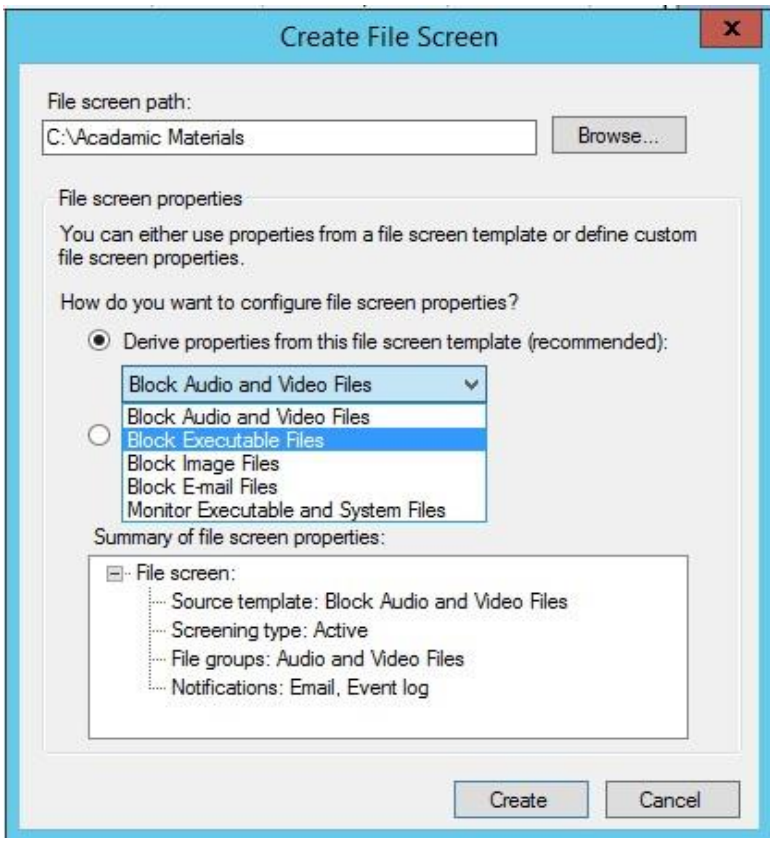

Browse For Folder
Select a folder
Local Disk (C:)
Acadamic Materials
Fundamentals of Programming I & II
Introduction to Computer Science
Network Administration
Object oriented programming
Complexity Theory
Folder:
Acadamic Materials
Make New Folder
OK
Cancel



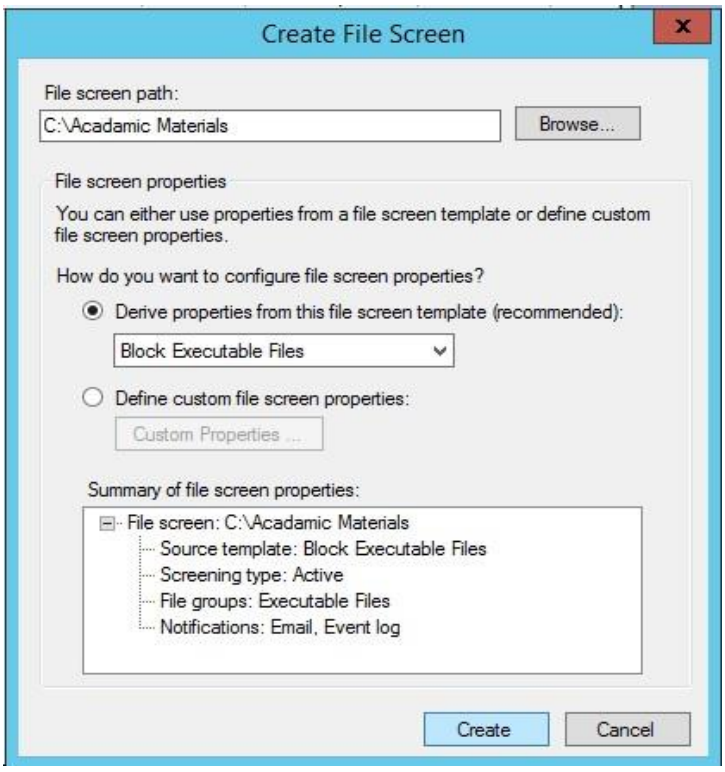

6. For file screen properties you can either use properties from a file screen template (recommended) or define your custom file screen properties.



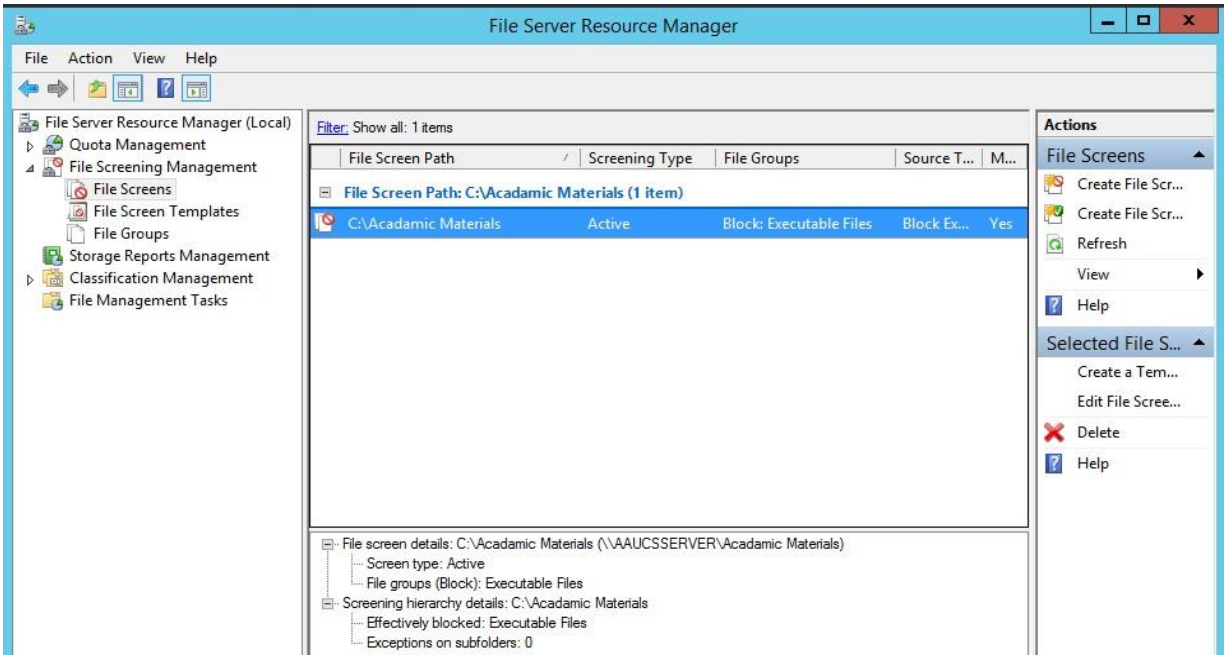

- In this example the selected file screen property is "**Block Executable Files**" under derive property of the file screen template




7. Finally, after you select the file screen path and the file screen property you can create your file screen by clicking the button **Create**.



➢ You have successfully created a file screen for the folder **Acadamic Materials** as shown as below.

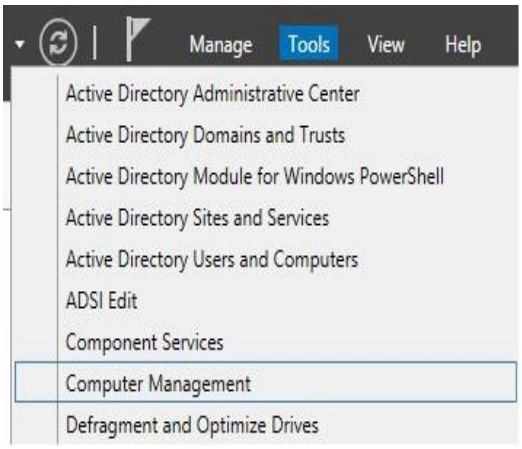



# 11.4 Disk partition

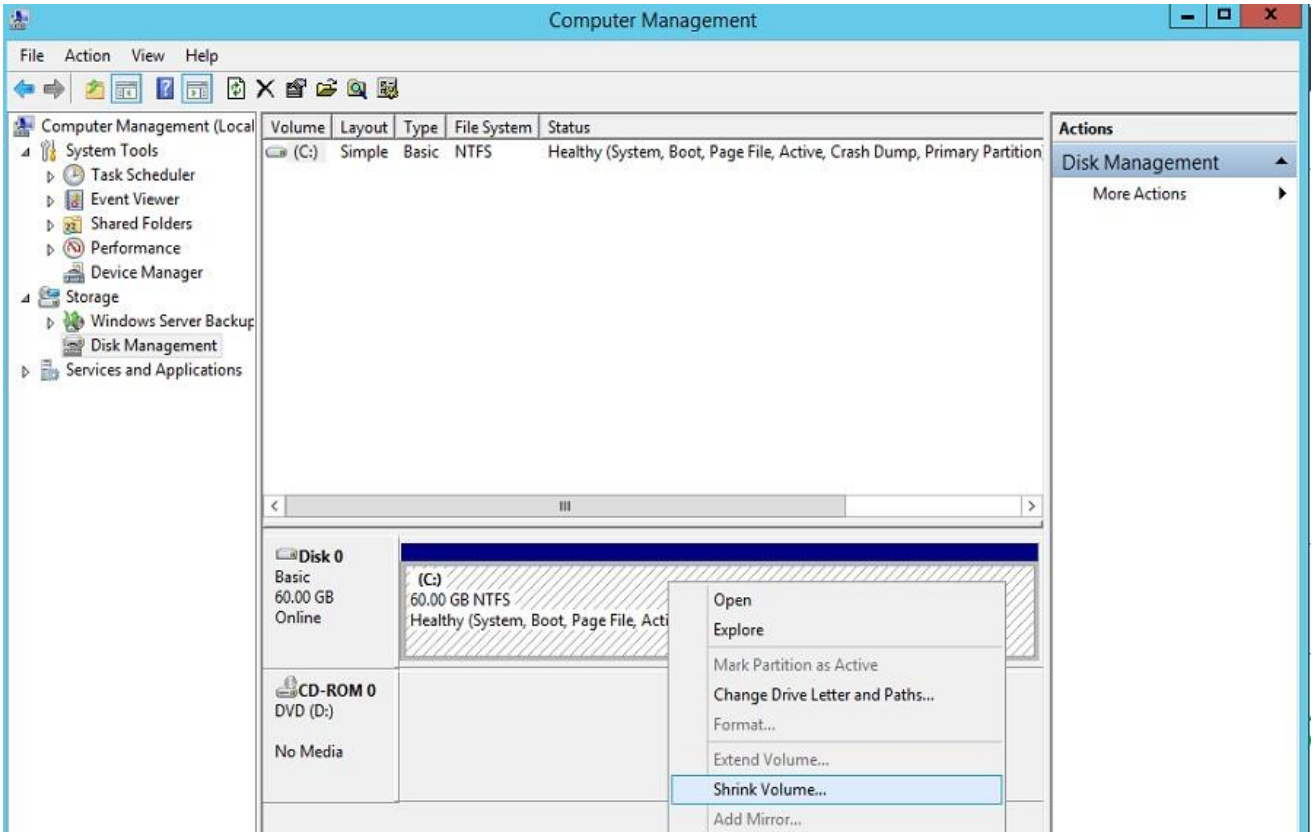
A partition is a logical division of a hard disk that is treated as a separate unit by operating systems and file systems. The operating systems and file systems can manage information on each partition as if it were a distinct hard drive. This allows the drive to operate as several smaller sections to improve efficiency, although it reduces usable space on the hard disk.

➢ To make a hard disk partition on your Windows server 2012 with your installed file and storage services role you have to track the following steps**:**

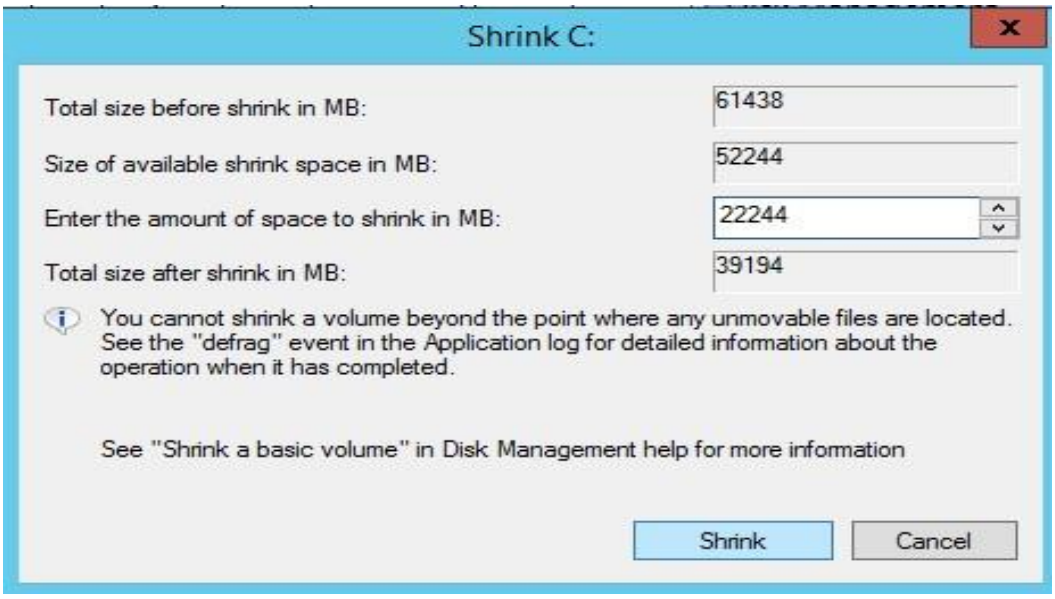
1.Go to **Tools** menu on the **Server manager**.



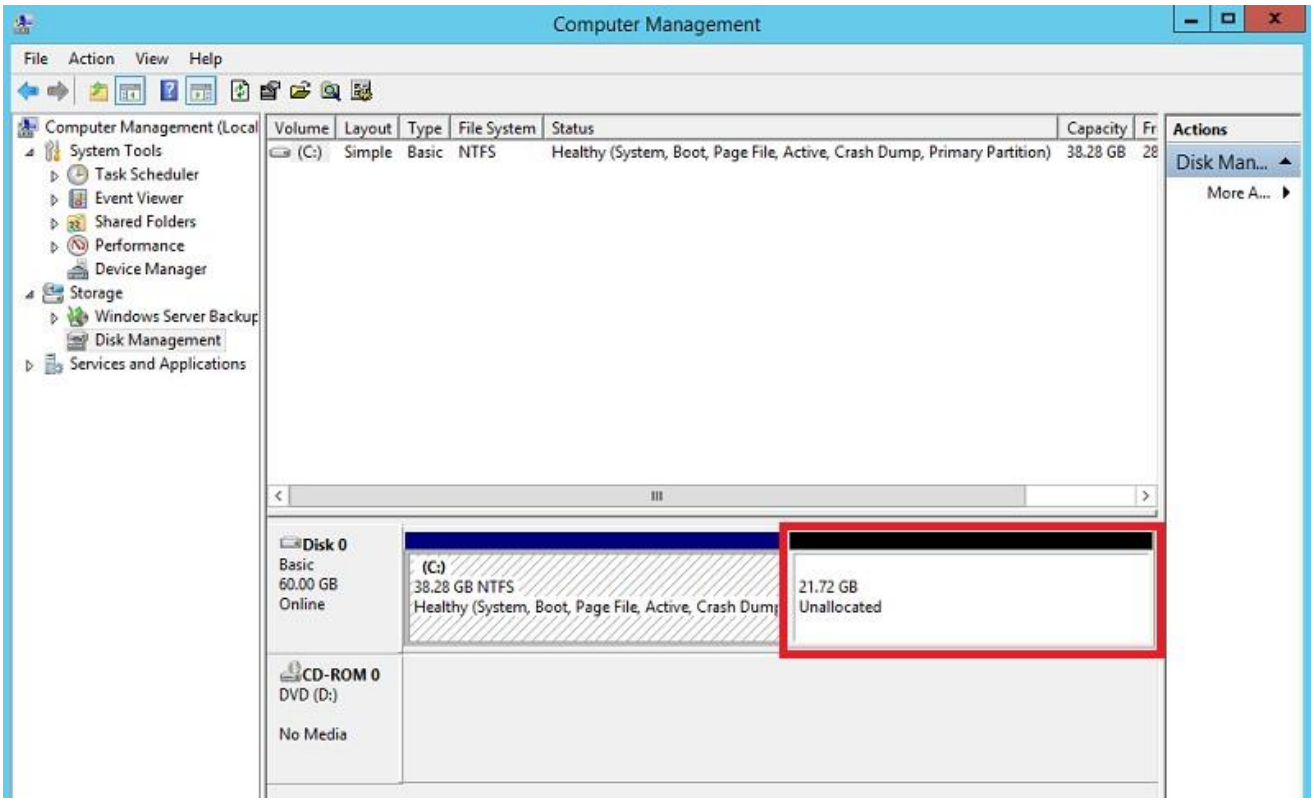

2. In the left side of Computer Management window select Disk Management option, then right click on your **(C:)** drive and select **Shrink volume** option from the drop down lists.



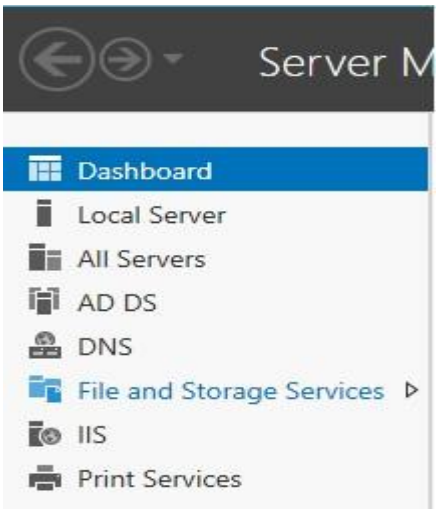

3. Set up the amount of the new disk size in Megabyte, here the new disk size is set as 22244 MB and click Shrink.



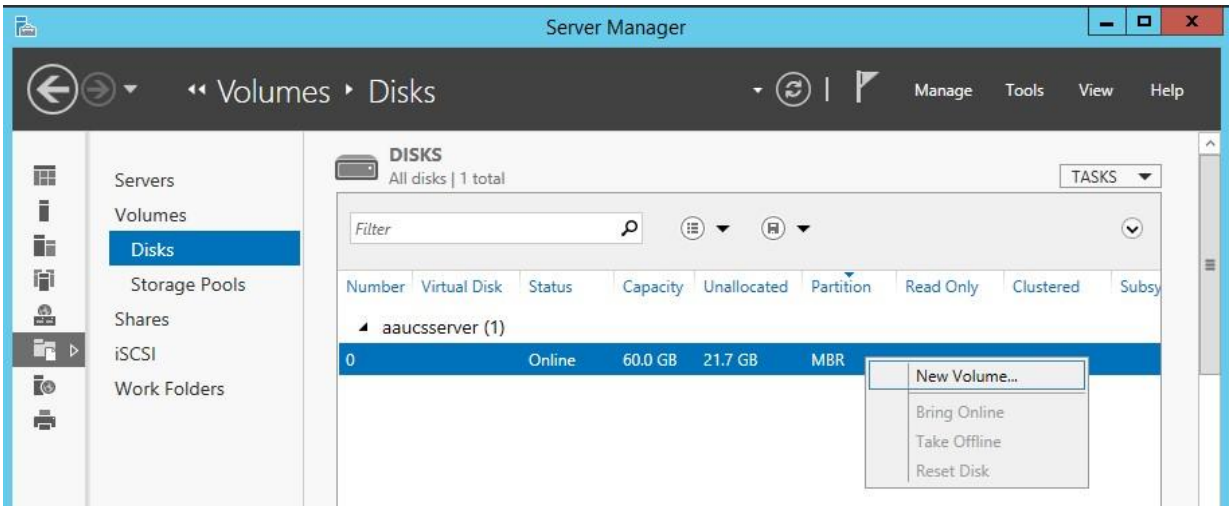

4. The new disk partition will be appeared in Disk management window as an **Unallocated** disk as shown below.




5. To get a new allocated disk go to the server manager dashboard and click **File and Storage Services**.

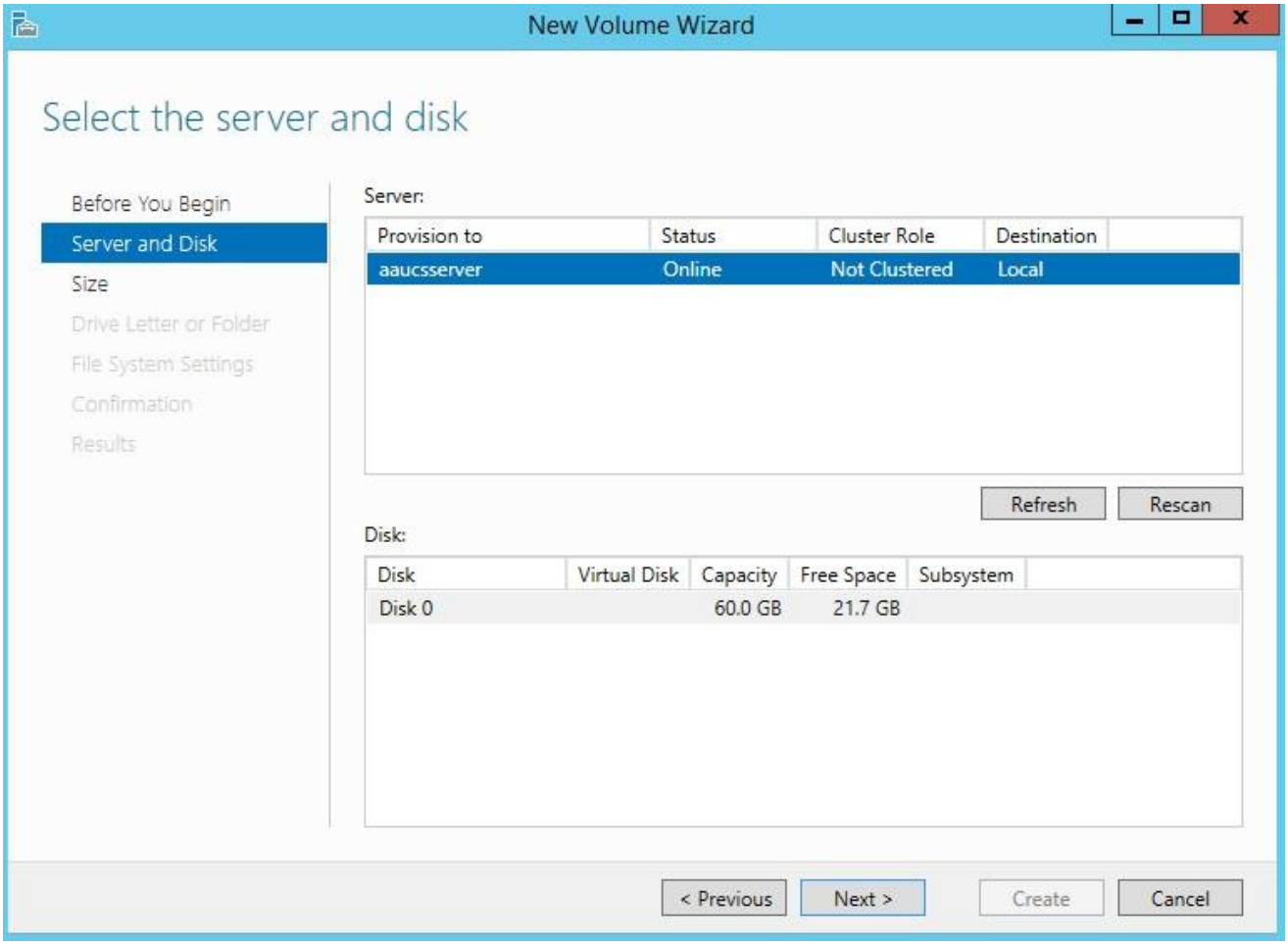



5.1 In the **Disk** list right click on the disk 0 and select **New volume**.

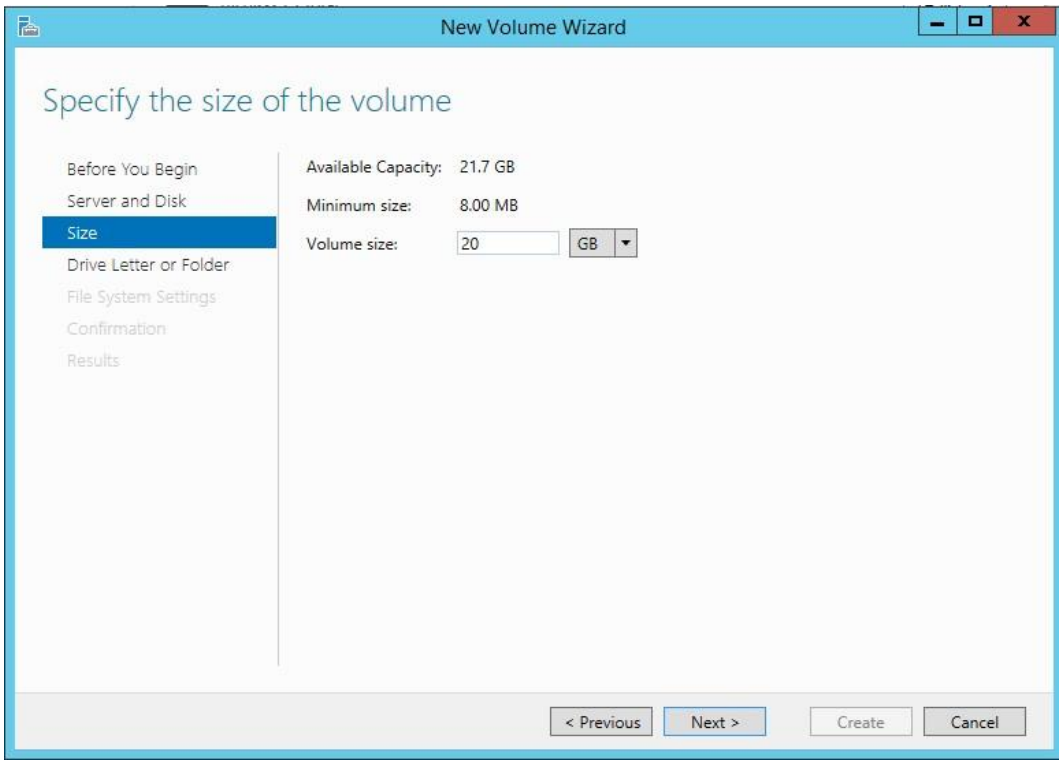



5.2 Pass the "**Before you begin"** window by clicking **Next**.

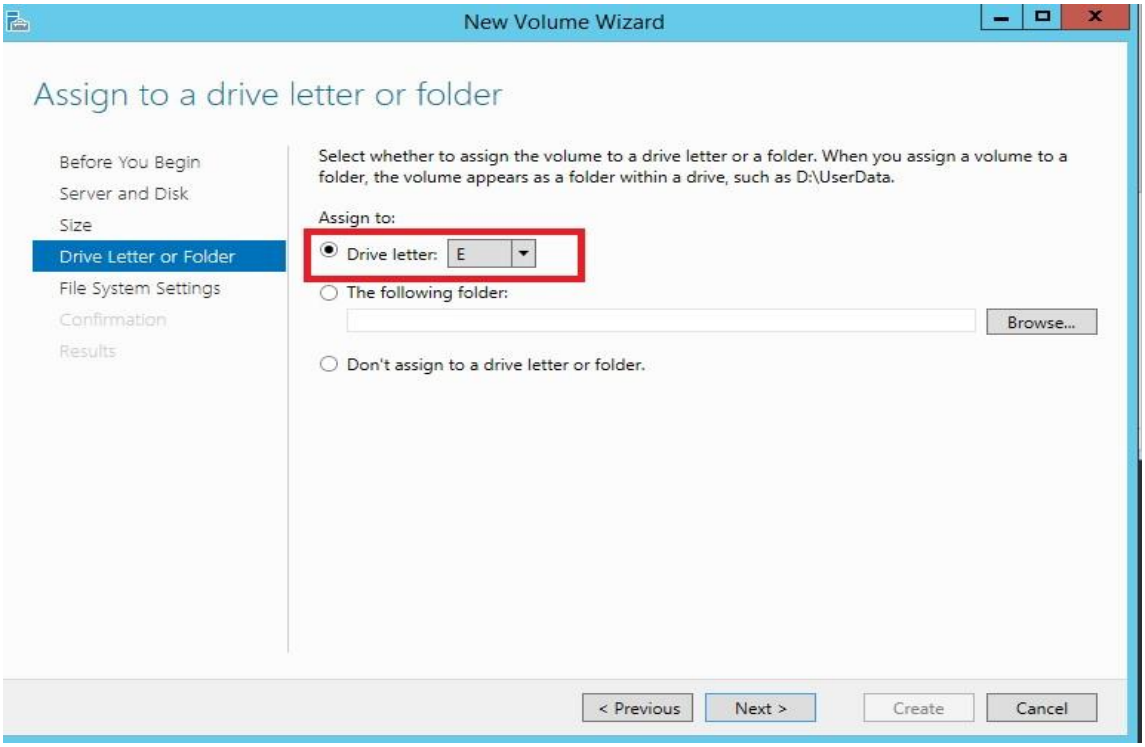
5.3 Select your **Server** and **Disk** from the next window and click **Next**.



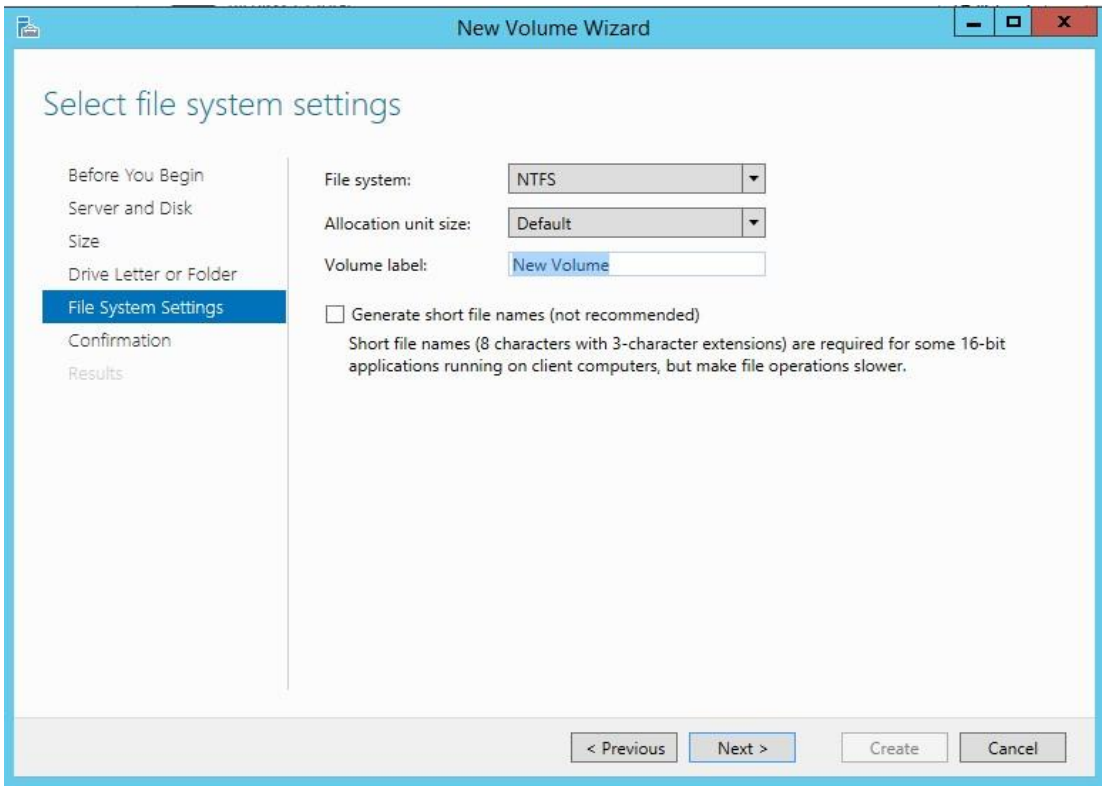

5.4 Specify the size of your new volume and click **Next**.



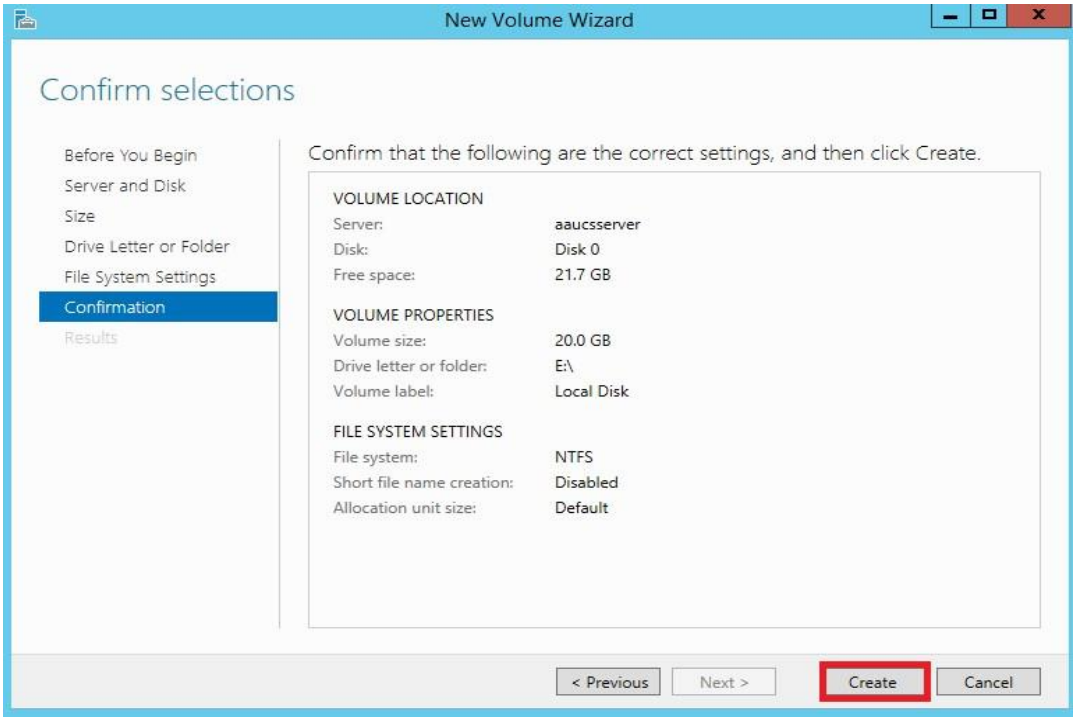

5.5 Assign a derive letter or folder to your new disk volume and click Next. In this example the letter **E** is assigned for the new disk volume.



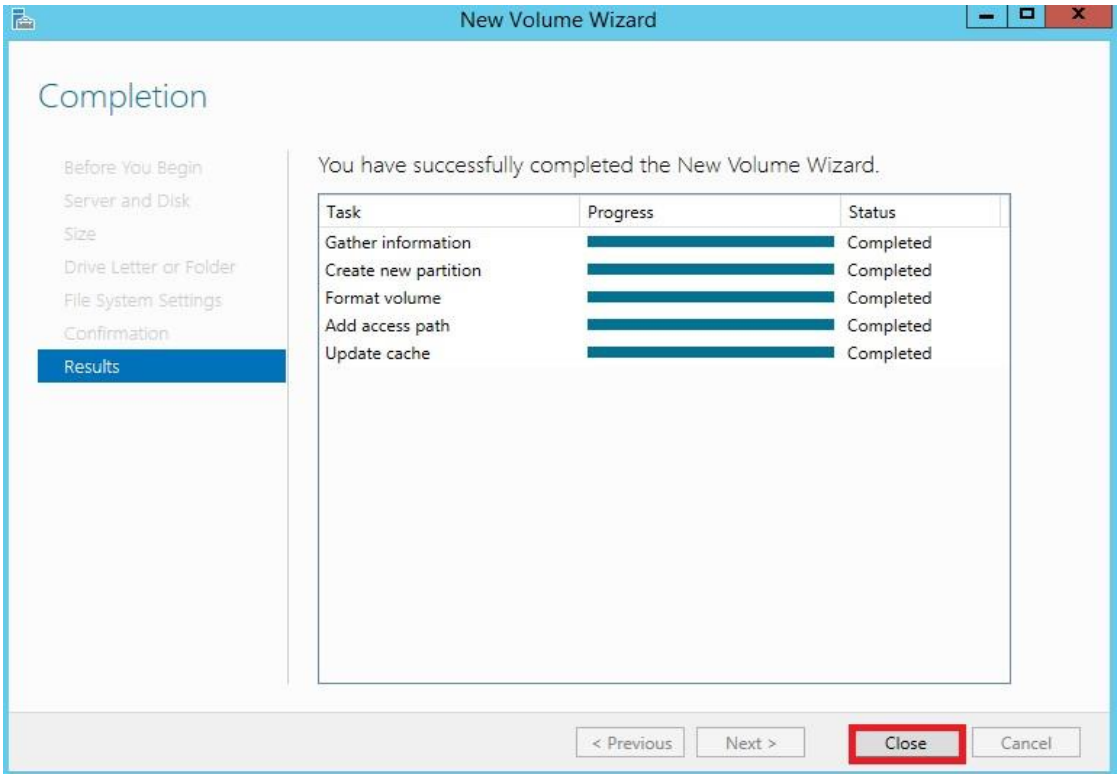

5.6 Select file system settings depends on your need and click **Next**.



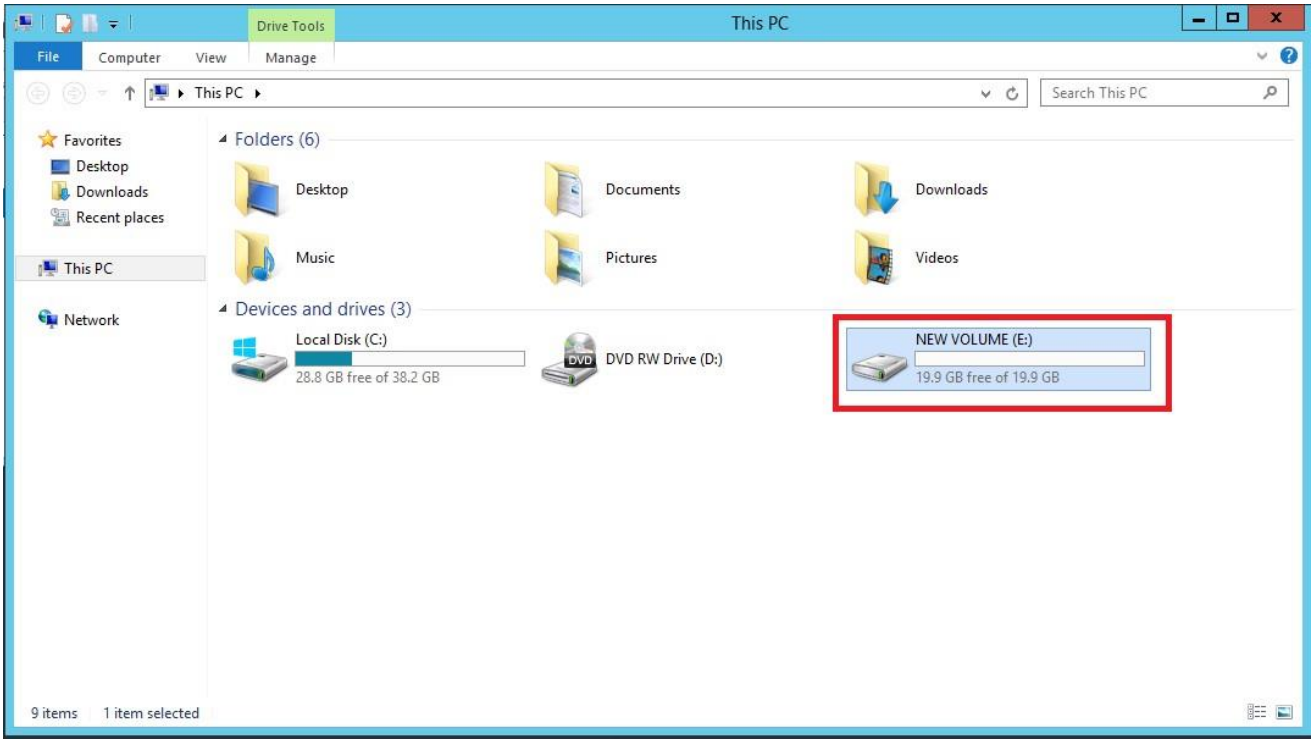

5.7 Confirm your selections and click **Create**.




5.8 You have success fully got the new disk volume and click **Close**.




✓ Finally your New Volume (E:) appears in your file explorer as shown below.



# Chapter Twelve: Group policy Management

## 12.1 Introduction

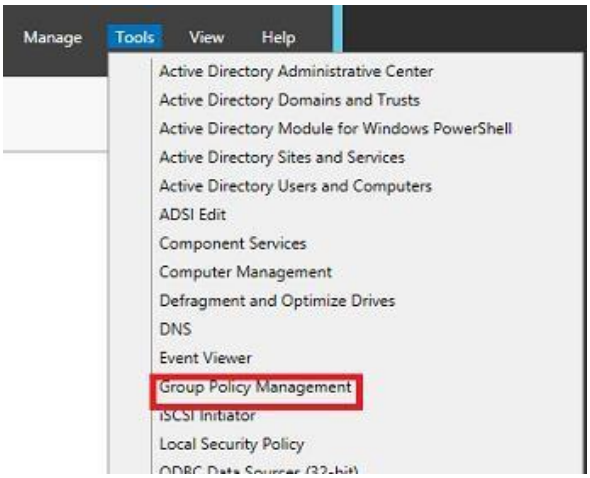
Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers. Group Policy can also be used to define user, security and networking policies at the machine level.

## 12.2 Configuration of a Group policy

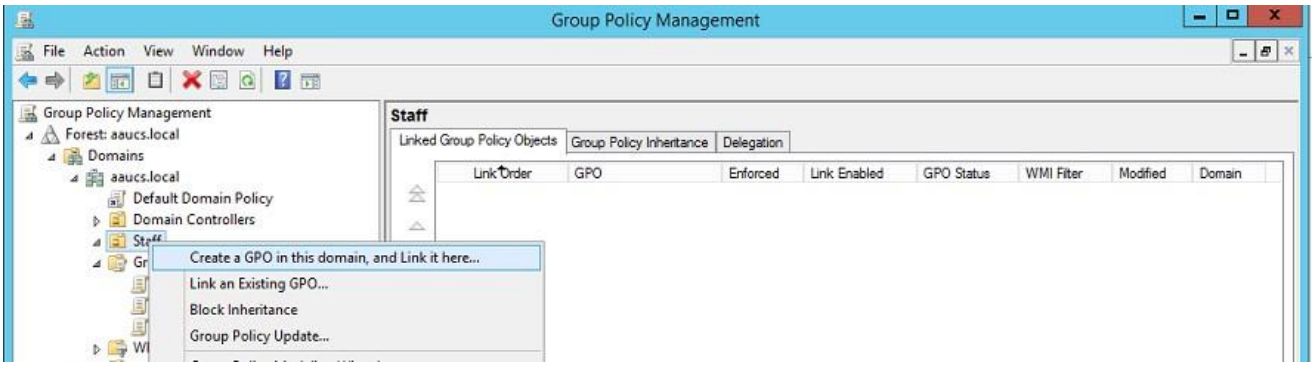
As usual we used our **aaucs.local** domain and our windows seven client, in this group policy our aim will be restrict few applications such as Notepad.exe, calculator.exe and paint.exe for the group called **students** that we already created earlier.

### Steps:

1. on the server manager go to **Tools**, find and click **Group policy Management**

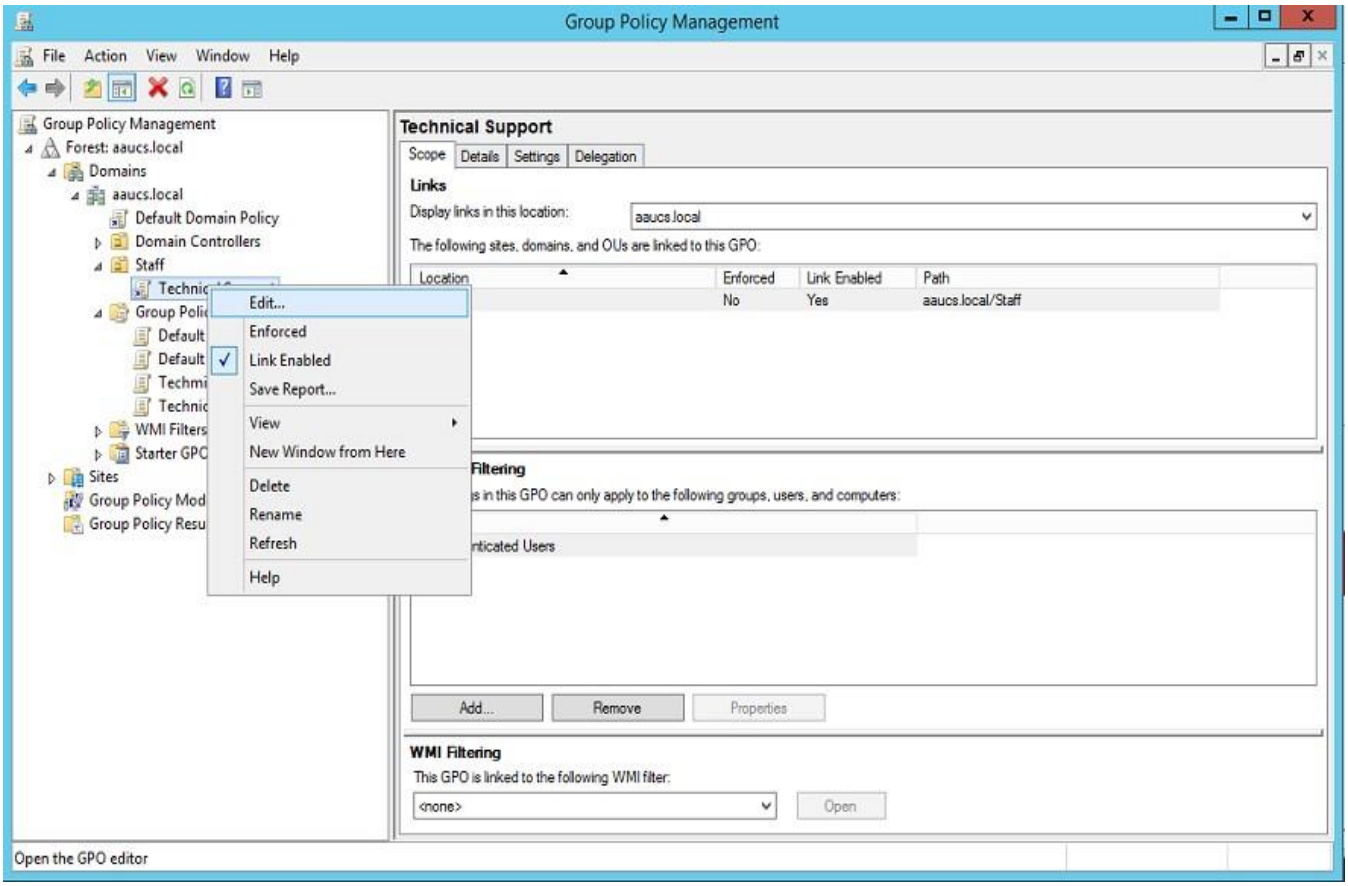



2. As usual on the domain server, **create a new GPO**, in our case the new GPO will be **Technical Support.**

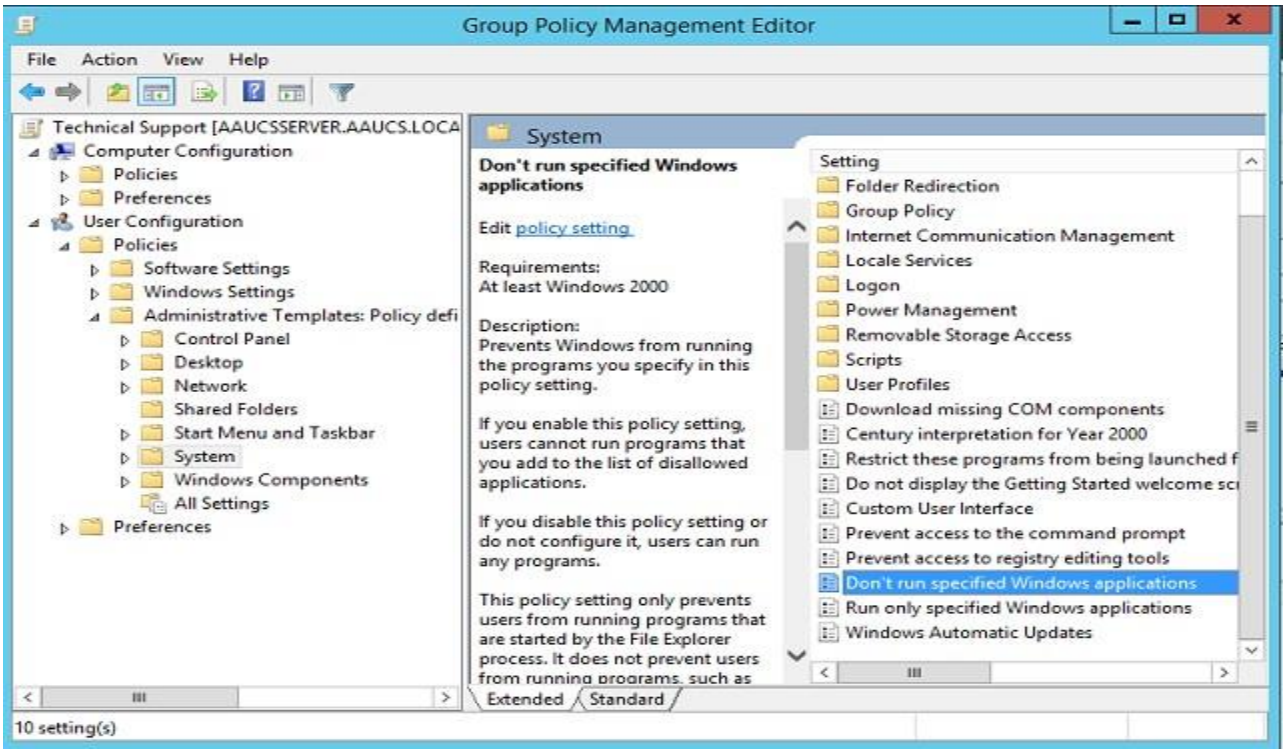




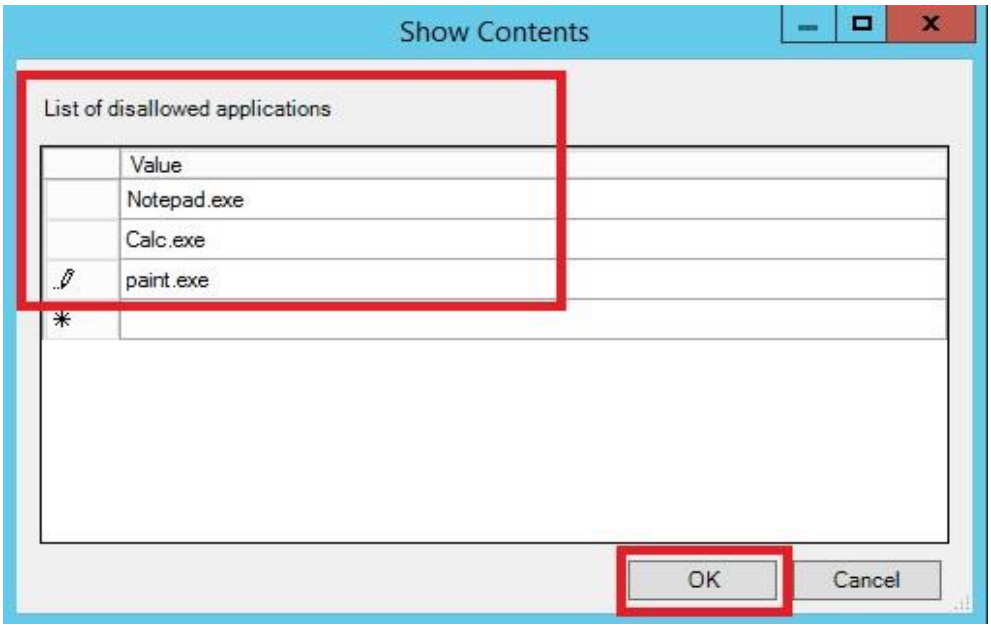
Next, right click on **Technical Support GPO** and click **Edit**



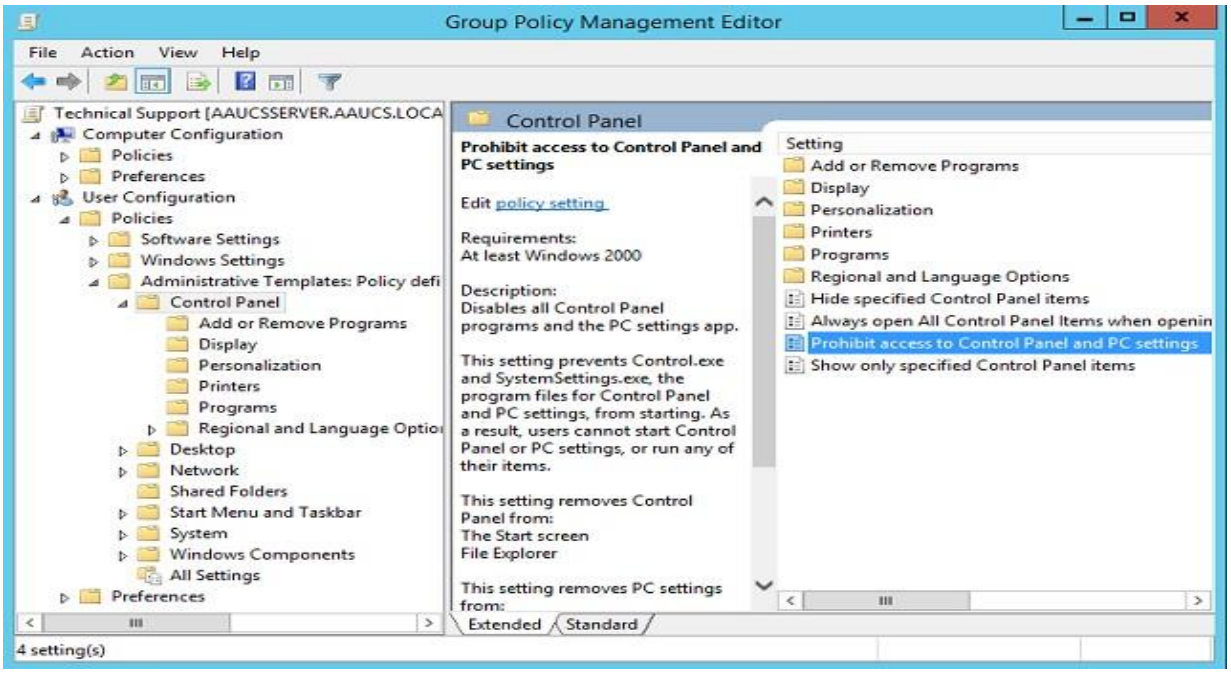

3. Next, on the Group Policy Management Editor, expand **User Configuration**, **Policies**, and **Administrative Templates**, and then click **System**, next double click **Don't run specified Windows applications,** click Enabled and click **Show**

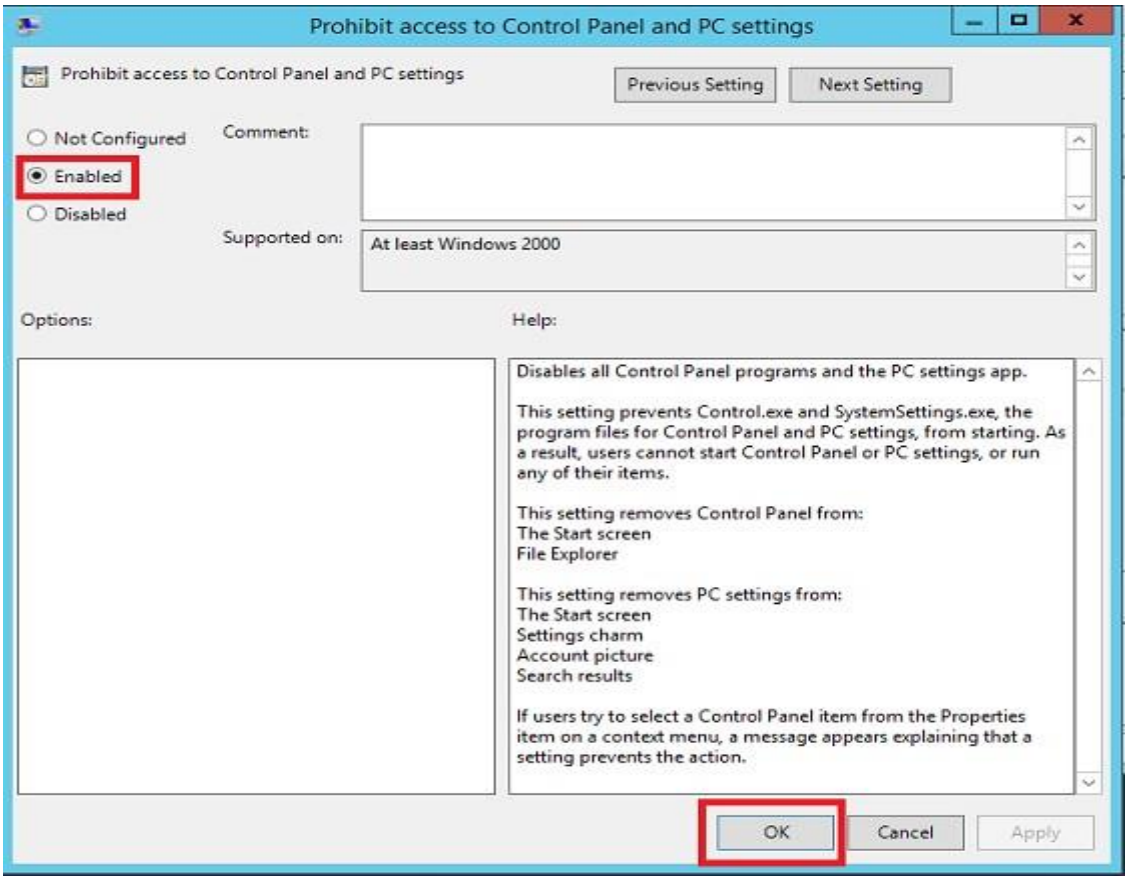



4. In the **Show** Contents box, in the **Value** list, type **notepad**.exe, **Calc**.exe, and **Paint**.exe then click **OK**

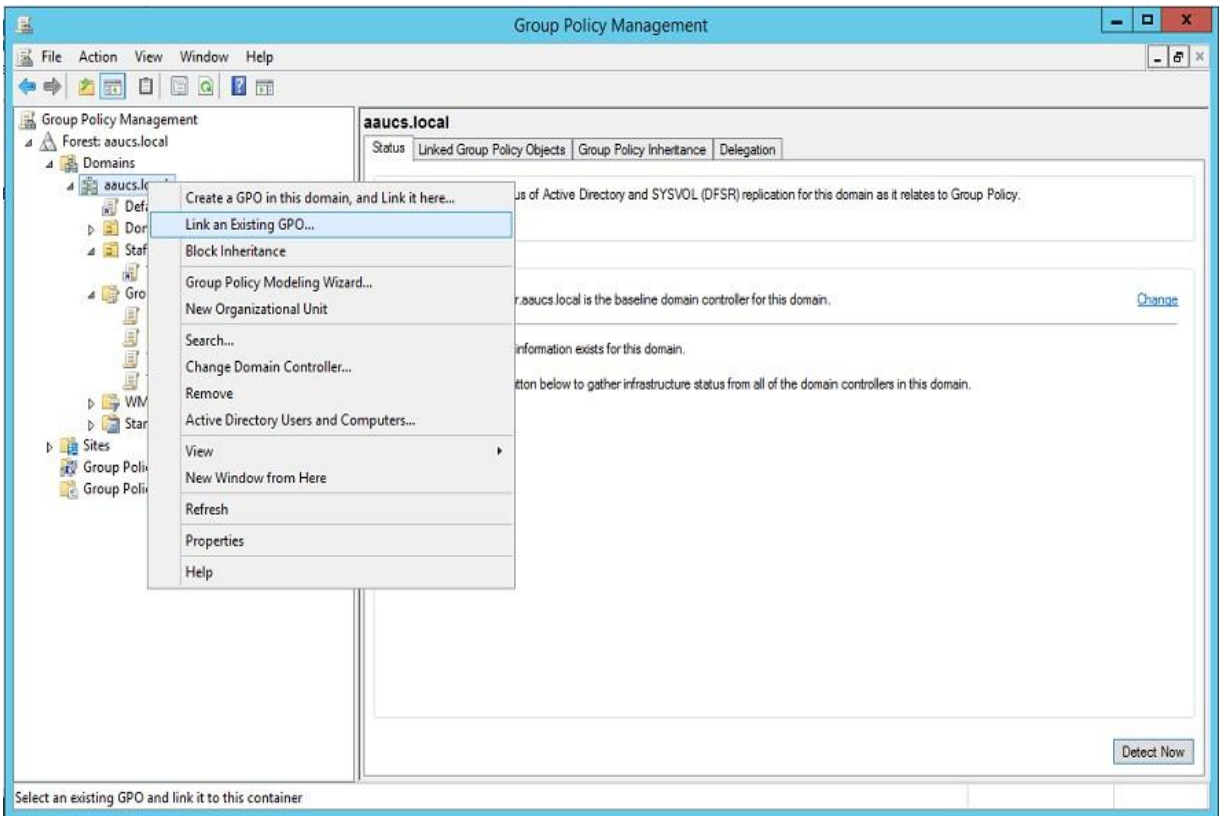



5. Next, click **Control Panel**, on the right pane, double click **Prohibit access to Control Panel and PC Settings**, then click **Enabled** and click **OK**…

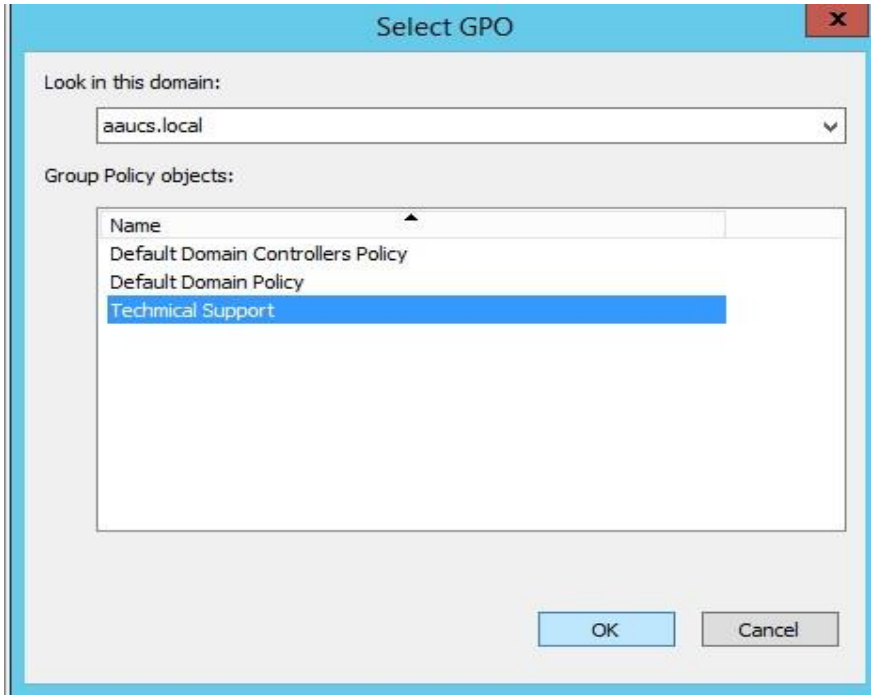


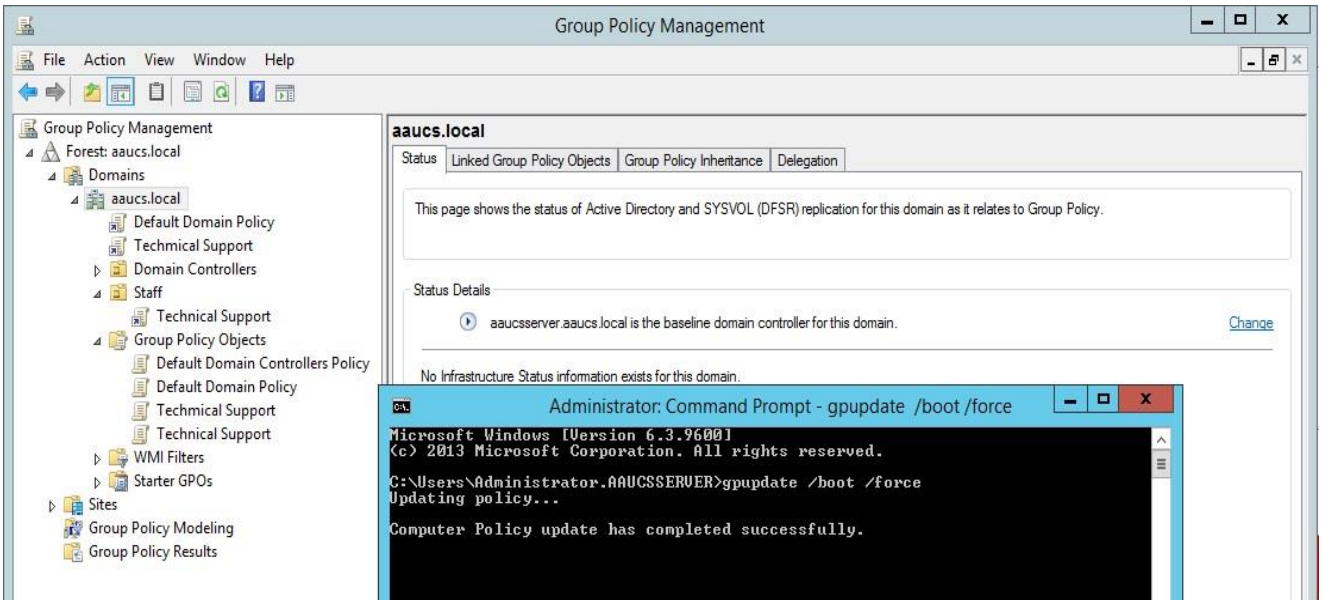

6. Next, let's Link the **Technical support GPO** to our domain, right click **aaucs.local** and click **Link an Existing GPO**…




7. On the Select GPO box, under Group Policy Object, click **Technical Support** and then click **OK** to proceed…




8. Next, you can open Command prompt (CMD) and type **gpupdate /boot /force**




9. Next, log in to your Windows client PC, in our case the clent machine operating system is Windows 7 ultimate and log in as a **surafiel AAUCS** domain user account.

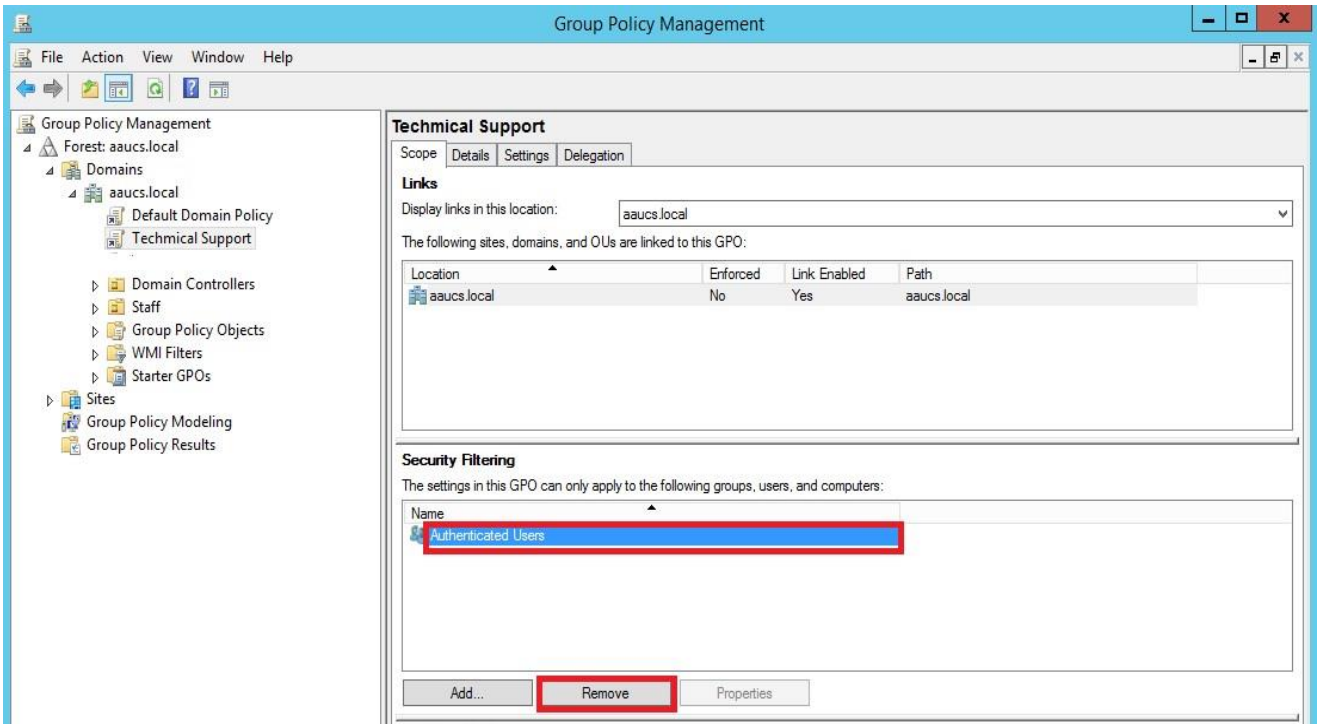

10. Once you successfully log on, try open **notepad** and **Control Panel** and you will be presented with Restrictions warning box

11. Next, back to your Domain Server and open **Control Panel** (remember that our Domain Server is longed in as Domain Administrator)

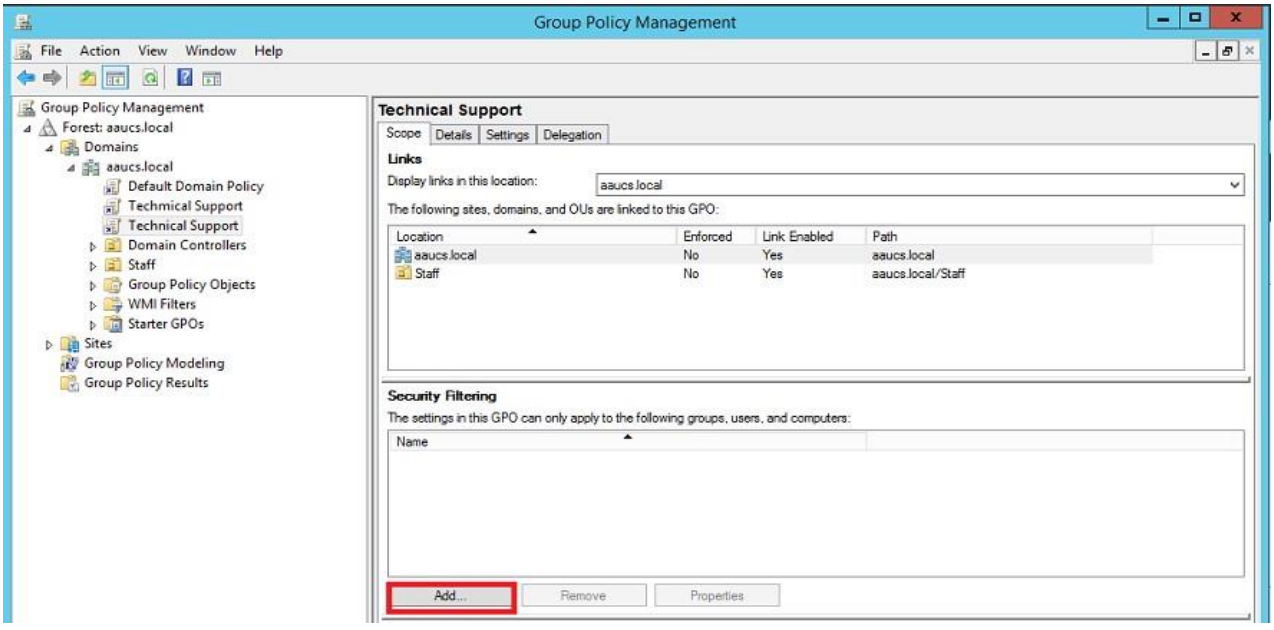

12. Once you click **Control Panel**, you will be presented with **Restrictions warning box**, but you are a **Domain Administrator**, why you had this Restriction??

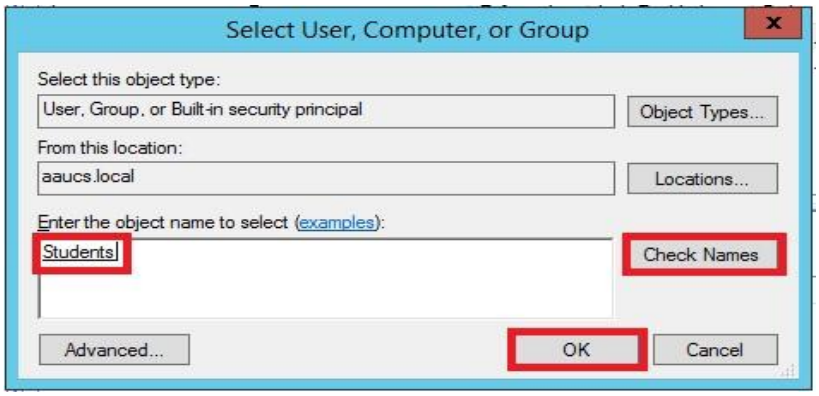

13. What you need to do to solve the above small issue just a simple step where as in the **Group Policy Management**, click **Technical Support** GPO, on the right pane, under **Security Filtering**, click **Authenticated Users** and then click **Remove** and click **OK** to **confirm** remove the Authenticated Users group.

.




14. Next, still in the Security Filtering, we can "**Add**" **Students** group so that only this group will effected with this GPO.






# 12.3 Audit policy

Audit policy is an important side of security. Monitoring the creation or modification of objects gives an administrator a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security crack.

There are nine different kinds of events the administrator can audit. If you audit any of these kinds of events, Windows records the events in the Security log, which you can find in Event Viewer.

- **Account logon events**. Audit this to see each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. Account logon events are generated in the domain controller's Security log when a domain user account is authenticated on a domain controller. These events are separate from Logon events, which are generated in the local Security log when a local user is authenticated on a local computer. Account logoff events are not tracked on the domain controller.
- **Account management**. Audit this to see when someone has changed an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group.
- **Directory service access**. Audit this to see when someone accesses an Active Directory Service object that has its own system access control list (SACL).
- **Logon events**. Audit this to see when someone has logged on or off your computer (either while physically at your computer or by trying to log on over a network).
- **Object access**. Audit this to see when someone has used a file, folder, printer, or other object. While you can also audit registry keys, we don't recommend that unless you have advanced computer knowledge and know how to use the registry.
- **Policy change**. Audit this to see attempts to change local security policies and to see if someone has changed user rights assignments, auditing policies, or trust policies.
- **Privilege use**. Audit this to see when someone performs a user right.
- **Process tracking**. Audit this to see when events such as program activation or a process exiting occur.
- **System events**. Audit this to see when someone has shut down or restarted the computer, or when a process or program tries to do something that it does not have permission to do. For

example, if malicious software tried to change a setting on your computer without your permission, system event auditing would record it.

When an administrator implement audit policy:

- Specify the categories of events that you want to audit. The event categories that you select constitute your audit policy.
- Set the size and behavior of the Security log. You can view the Security log with Event Viewer.
- If you want to audit directory service access or object access, determine which objects you want to audit access of and what type of access you want to audit. For example, if you want to audit any attempts by users to open a particular file, you can configure auditing policy settings in the object access event category so that both successful and failed attempts to read a file are recorded.

The Security log records an audit event whenever users perform certain specified actions. For example, the modification of a file or a policy can trigger an event that shows the action that was performed, the associated user account, and the date and time of the action. These events can be both successful and failed attempts to perform actions.

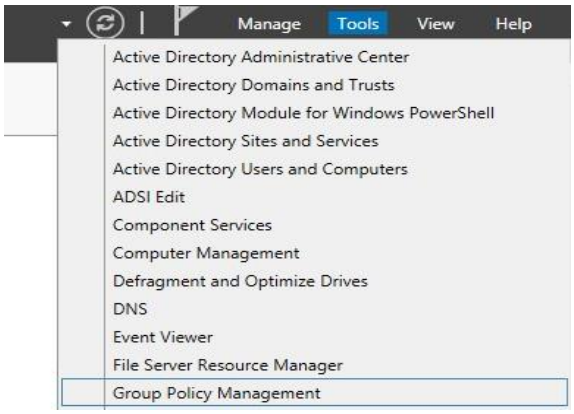
## 12.3.1 Audit policy settings

The vulnerabilities, countermeasures, and potential impacts of all the audit settings are identical. The options for each of the audit settings are also identical:

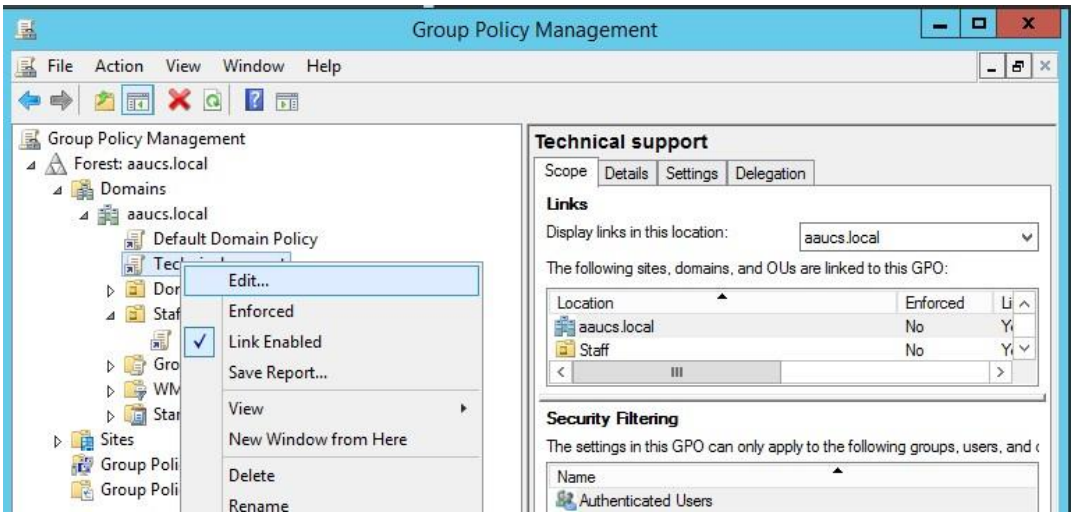
- **Success**: An audit event is generated when the requested action succeeds.
- **Failure**: An audit event is generated when the requested action fails.
- **No Auditing**: No audit event is generated for the associated action.

## 12.3.2 Implementation of an Audit policy

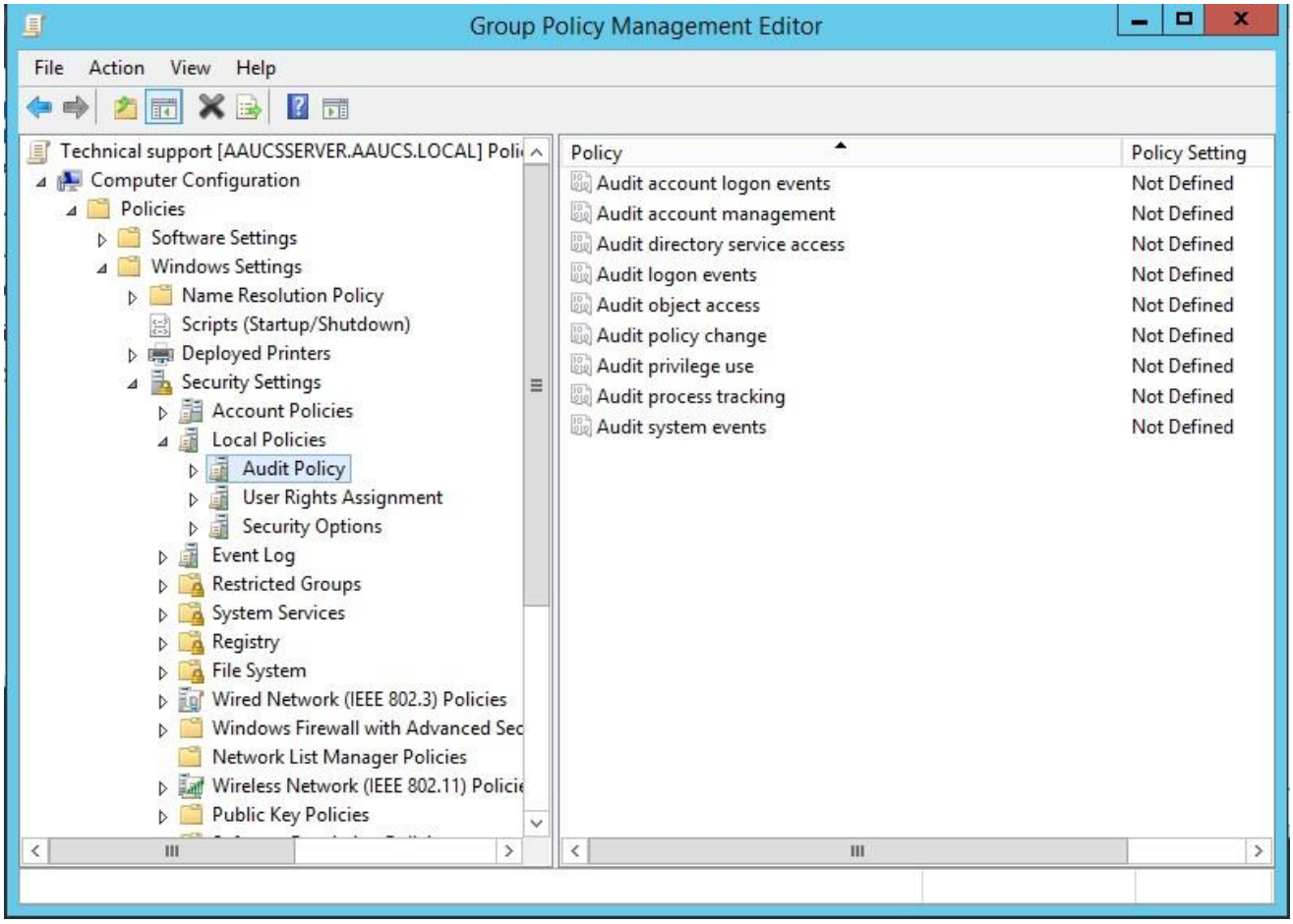
1. Go to Server Manager-> Tools-> Group policy Management.



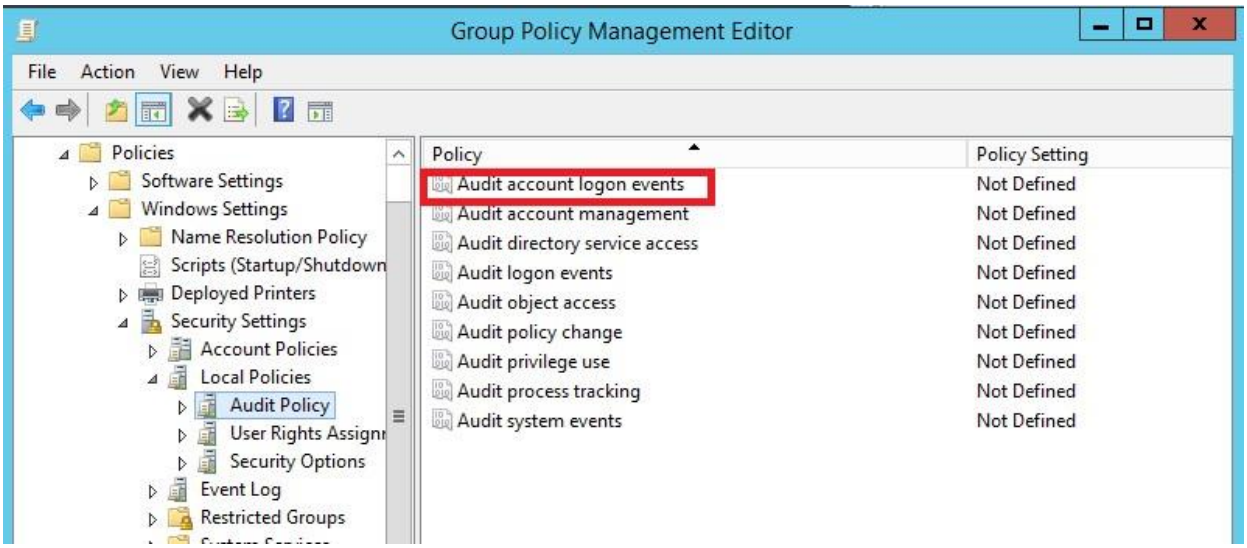

2. Right click on your created GPO (**Technical Support**) under the domain ad select **Edit**.

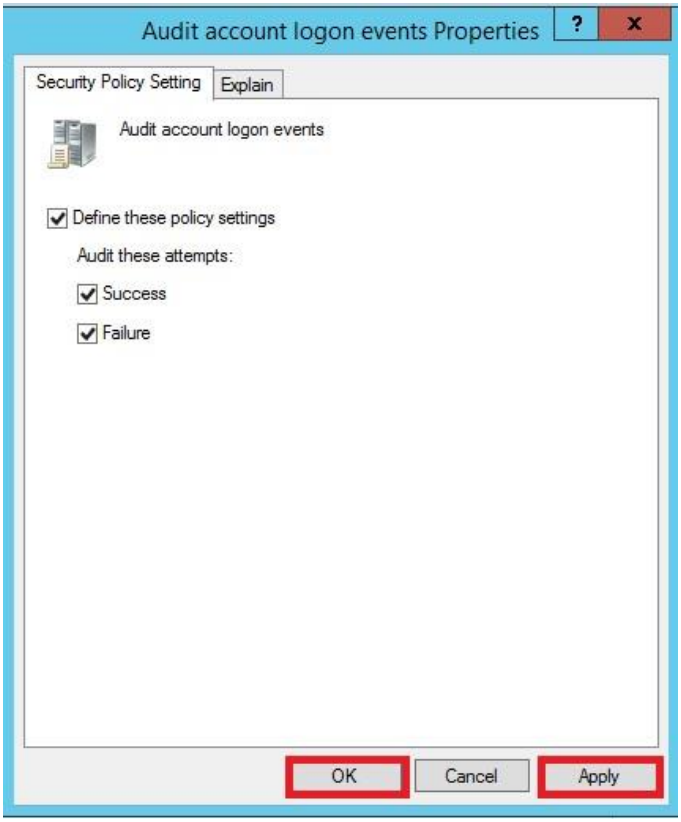


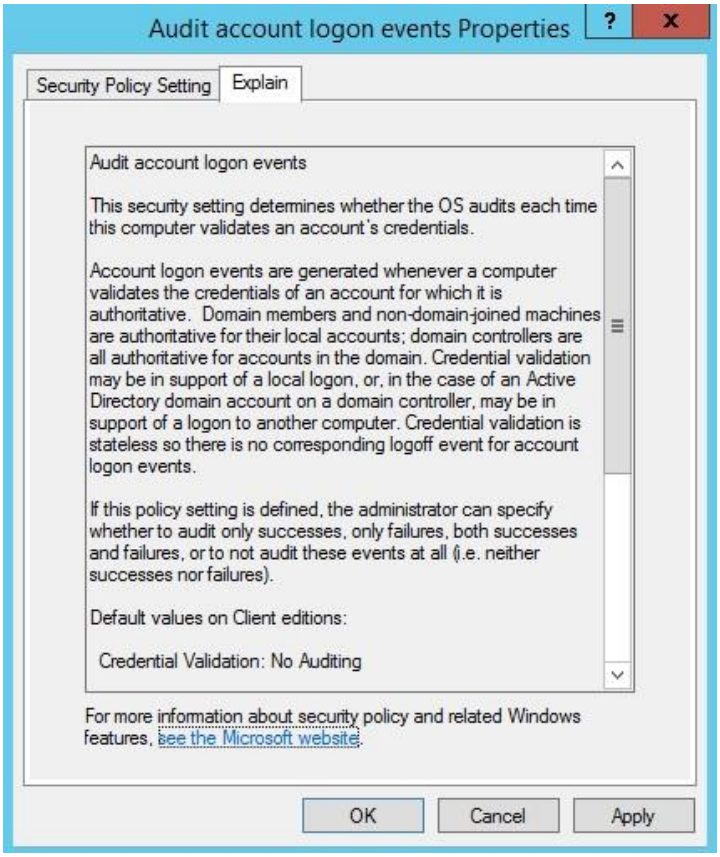

3. Expand the **computer configuration** -> **policies** -> **Windows settings** -> **Security Settings** -> **Local policies** then select **Audit policy**.

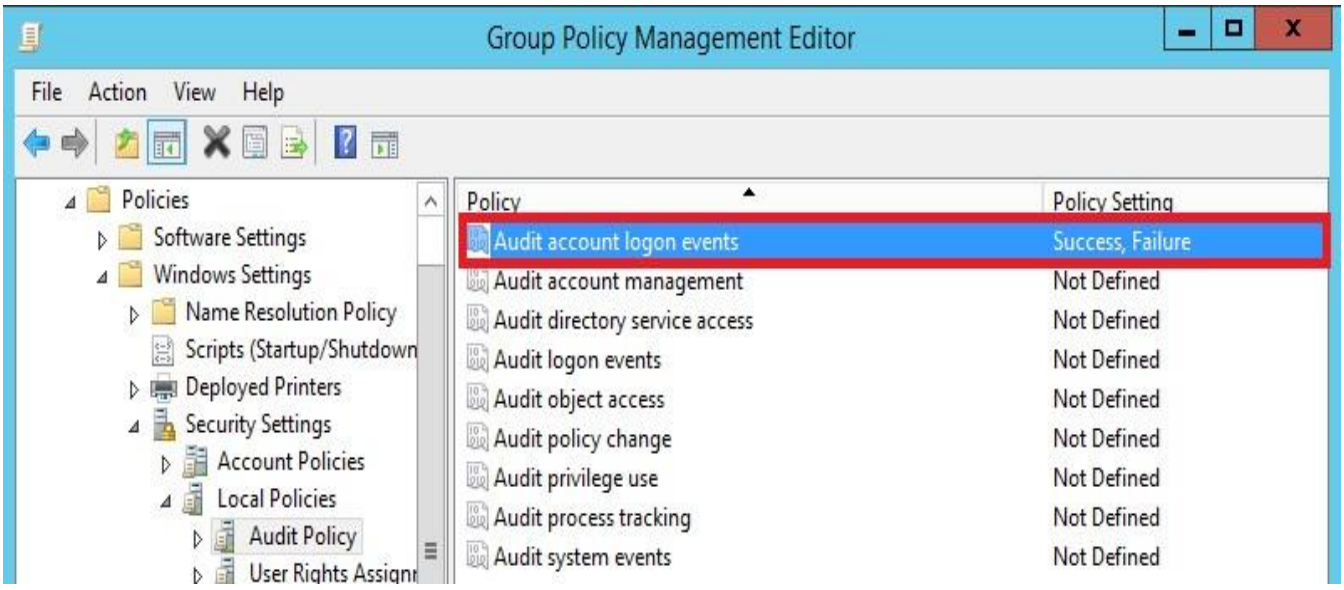



4. Now you can implement the audit policy for what you want in the given lists of audit policies. For example here the "**Audit account logon events**" **is** implemented from the given list of Audit policy.

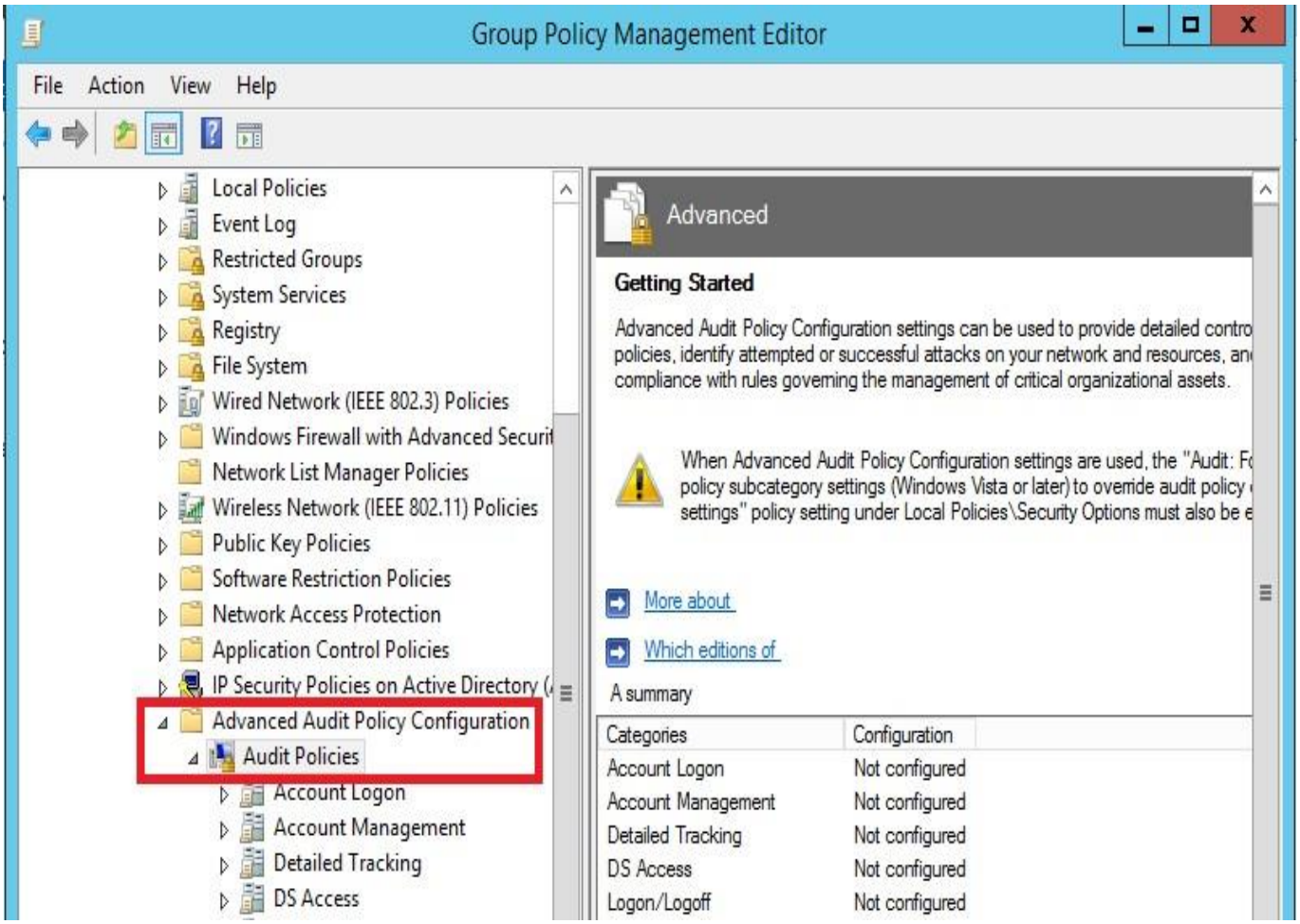

Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assign
Security Options
Event Log
Restricted Groups
Policy
Policy Setting
Audit account logon events
Not Defined
Audit account management
Not Defined
Audit directory service access
Not Defined
Audit logon events
Not Defined
Audit object access
Not Defined
Audit policy change
Not Defined
Audit privilege use
Not Defined
Audit process tracking
Not Defined
Audit system events
Not Defined


Audit account logon events Properties
Security Policy Setting
Explain
Audit account logon events
Define these policy settings
Audit these attempts:
Success
Failure
OK
Cancel
Apply

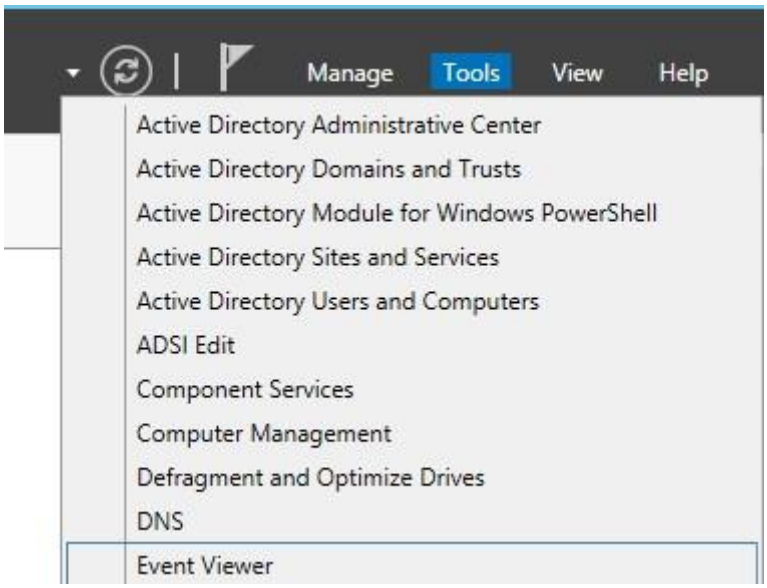


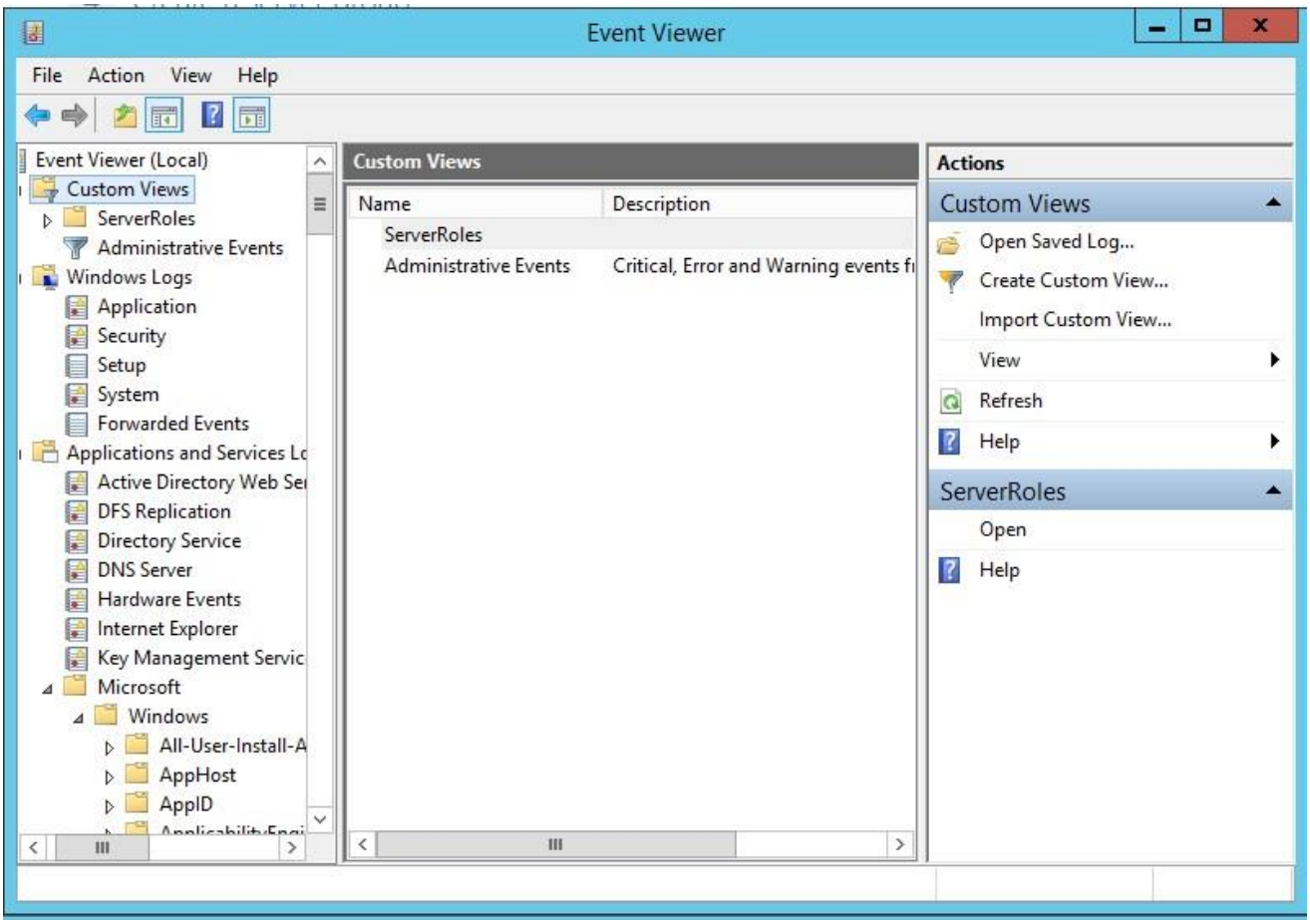




- You can also configure the advanced audit policies under **computer configuration** -> **policies** -> **Windows settings** -> **Security Settings** -> **Advanced Audit Policy Configuration** -> **Audit Policy**.

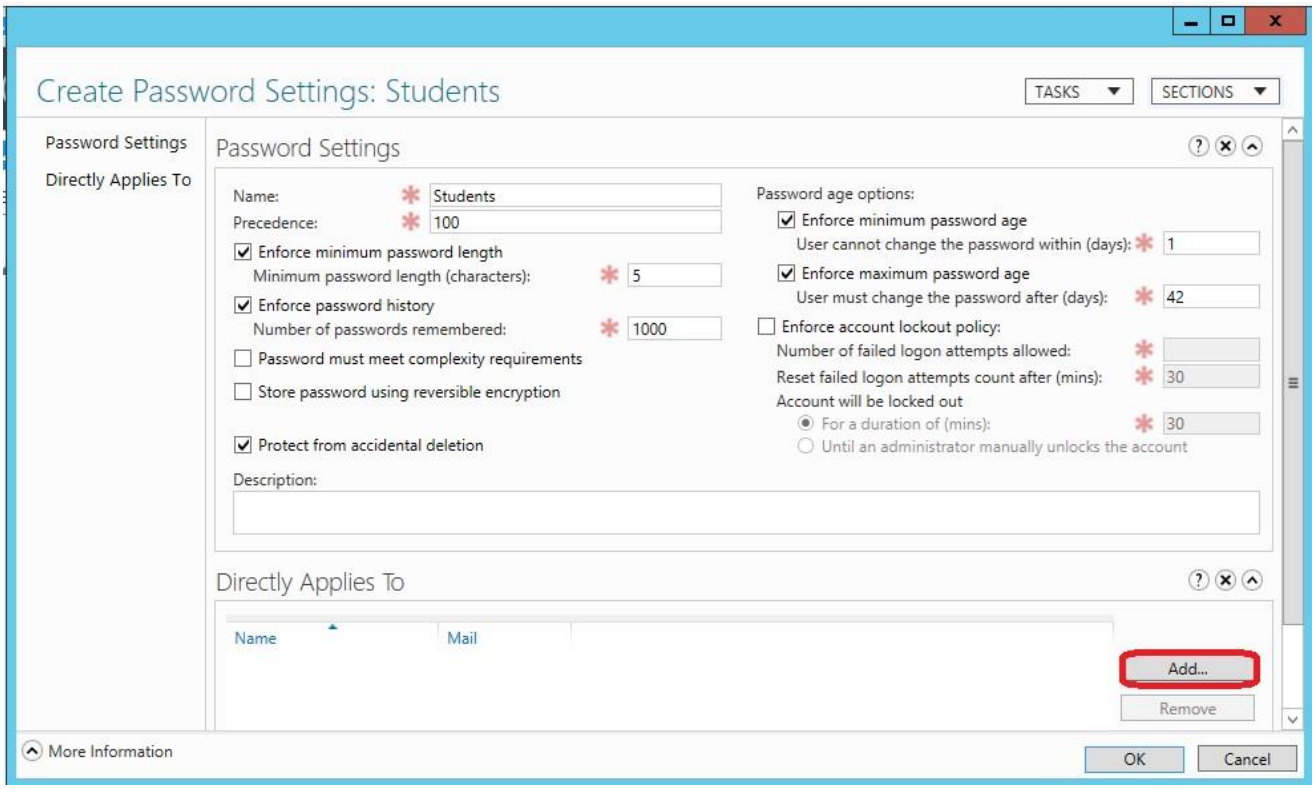



- To see the audit log you can go to through **Server Manager** -> **Tools** -> **Event Viewer**.

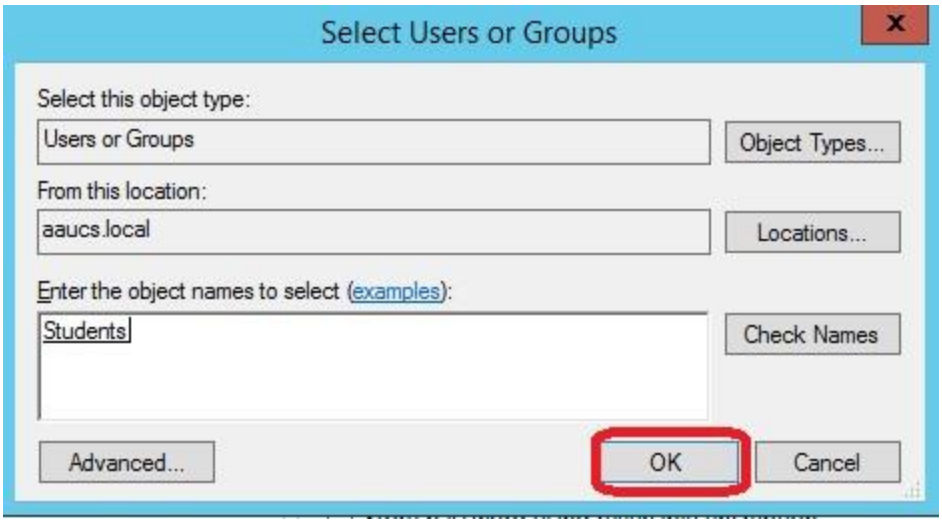


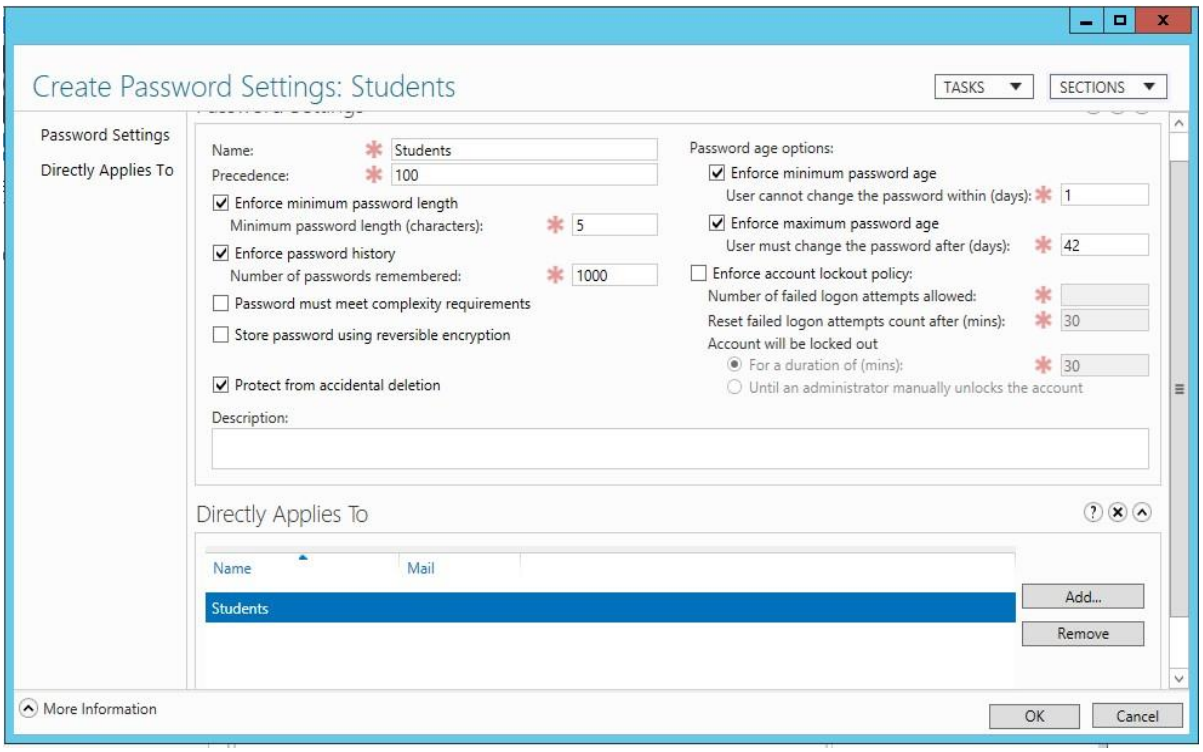

5. Click the **Add** button in the "**Directly Applies To**" section and select the Global Group you want to target.

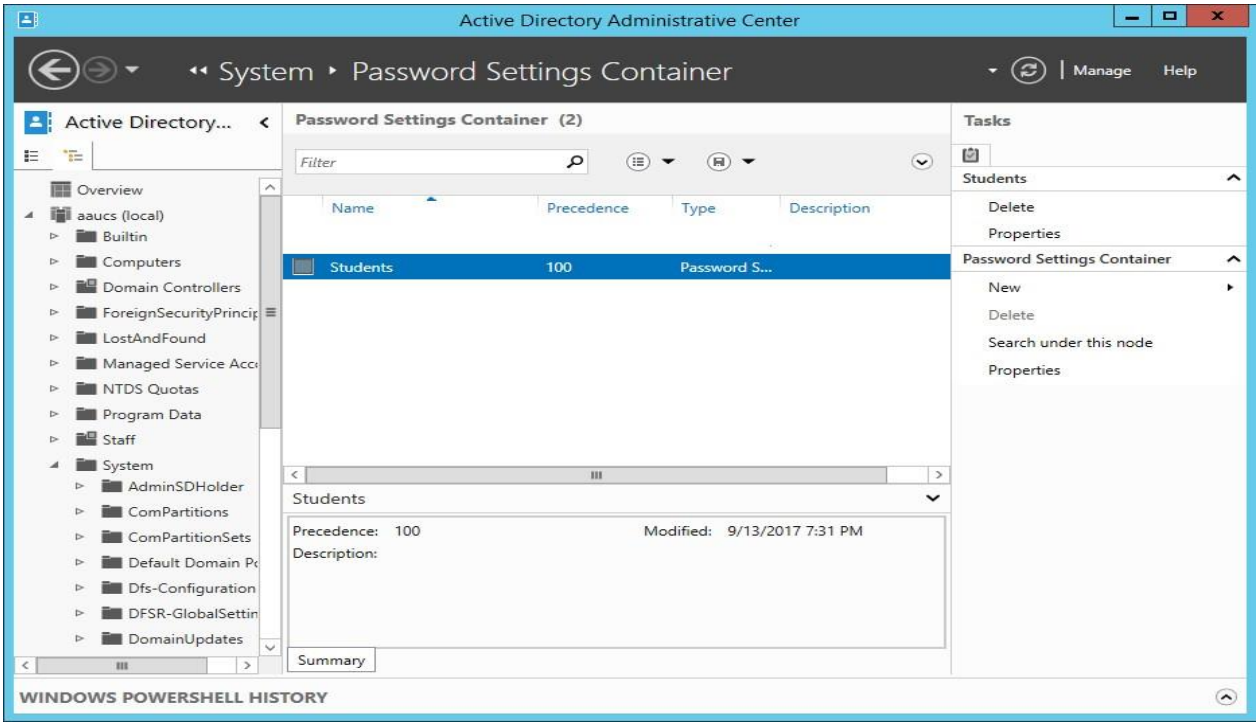



✓ In our case "Students" Group and click OK




6. We have successfully configured a password policy for the "**Students**" domain group of users.


Create Password Settings: Students
TASKS
SECTIONS
Password Settings
Directly Applies To
Name:
Students
Precedence:
100
Enforce minimum password length
Minimum password length (characters):
5
Enforce password history
Number of passwords remembered:
1000
Password must meet complexity requirements
Store password using reversible encryption
Protect from accidental deletion
Password age options:
Enforce minimum password age
User cannot change the password within (days):
1
Enforce maximum password age
User must change the password after (days):
42
Enforce account lockout policy:
Number of failed logon attempts allowed:
Reset failed logon attempts count after (mins):
30
Account will be locked out
For a duration of (mins):
30
Until an administrator manually unlocks the account
Description:
Directly Applies To
Name
Mail
Students
Add...
Remove
More Information
OK
Cancel


Active Directory Administrative Center
System ▸ Password Settings Container
Manage
Help
Active Directory...
Overview
aaucs (local)
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
LostAndFound
Managed Service Acc
NTDS Quotas
Program Data
Staff
System
AdminSDHolder
ComPartitions
ComPartitionSets
Default Domain Pc
Dfs-Configuration
DFSR-GlobalSettin
DomainUpdates
Password Settings Container (2)
Filter
Name
Precedence
Type
Description
Students
100
Password S...
Students
Precedence: 100
Modified: 9/13/2017 7:31 PM
Description:
Summary
Tasks
Students
Delete
Properties
Password Settings Container
New
Delete
Search under this node
Properties
WINDOWS POWERSHELL HISTORY

# Chapter Thirteen: Installation and Configuration of DHCP role

## 13.1 Introduction

**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.

**Benefits of DHCP**

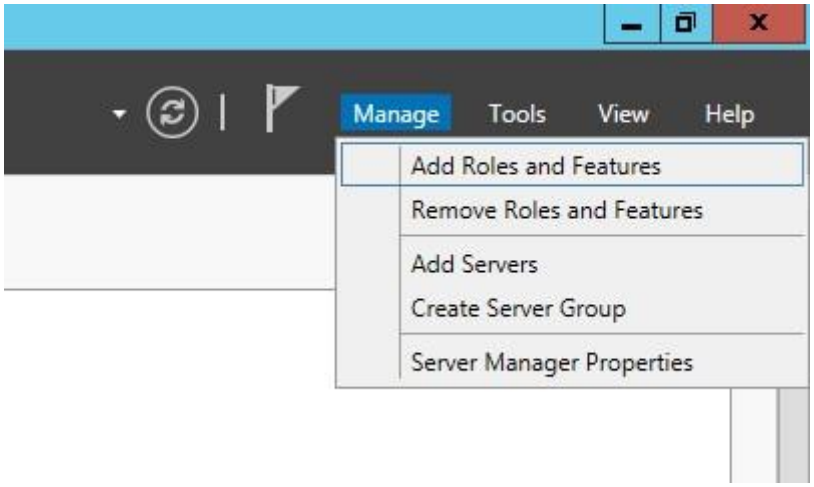
- Safe and reliable configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, as well as address conflicts caused by a currently assigned IP address accidentally being reissued to another computer.
- Reduced network administration.
    - ✓ TCP/IP configuration is centralized and automated.
    - ✓ Network administrators can centrally define global and subnet-specific TCP/IP configurations.
    - ✓ Clients can be automatically assigned a full range of additional TCP/IP configuration values by using DHCP options.
    - ✓ Address changes for client configurations that must be updated frequently, such as remote access clients that move around constantly, can be made efficiently and automatically when the client restarts in its new location.
    - ✓ Most routers can forward DHCP configuration requests, eliminating the requirement of setting up a DHCP server on every subnet, unless there is another reason to do so.

## 13.2 Steps of the installation of DHCP role

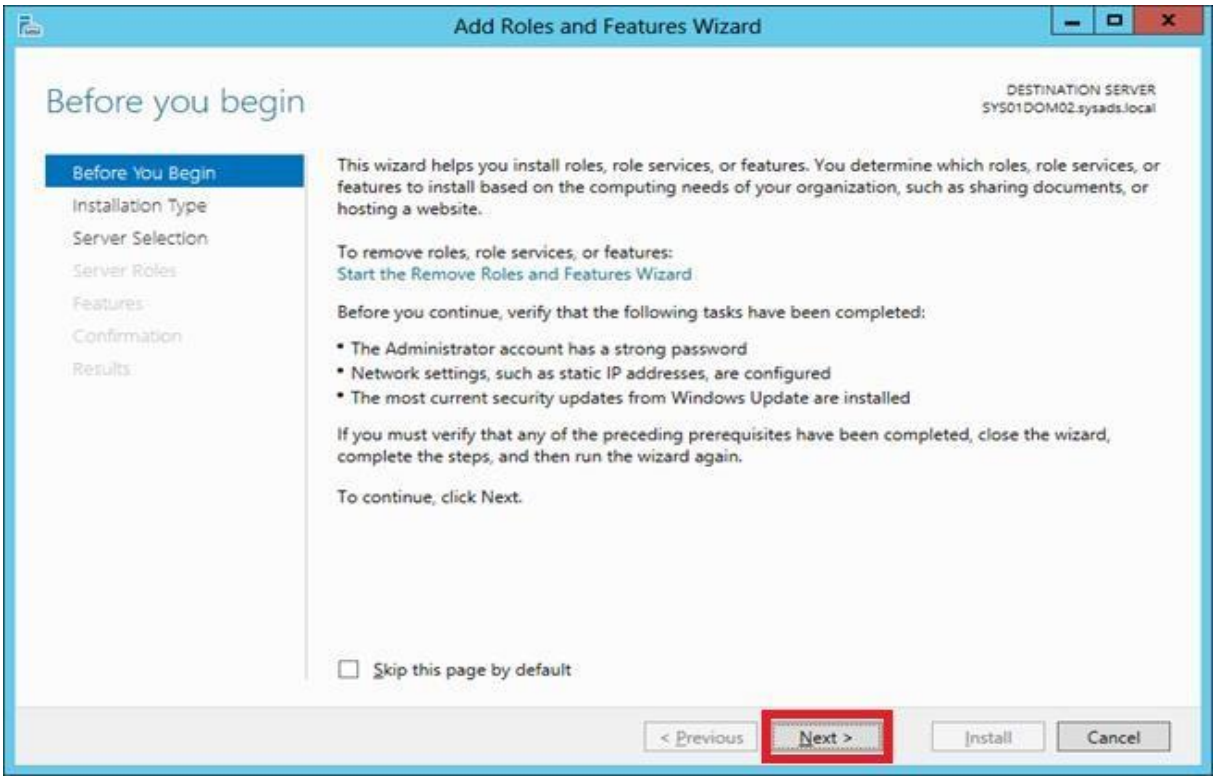
 Be Ensure the computer has at least one static IP address assigned before starting the role installation.

1. Start the Server Manager

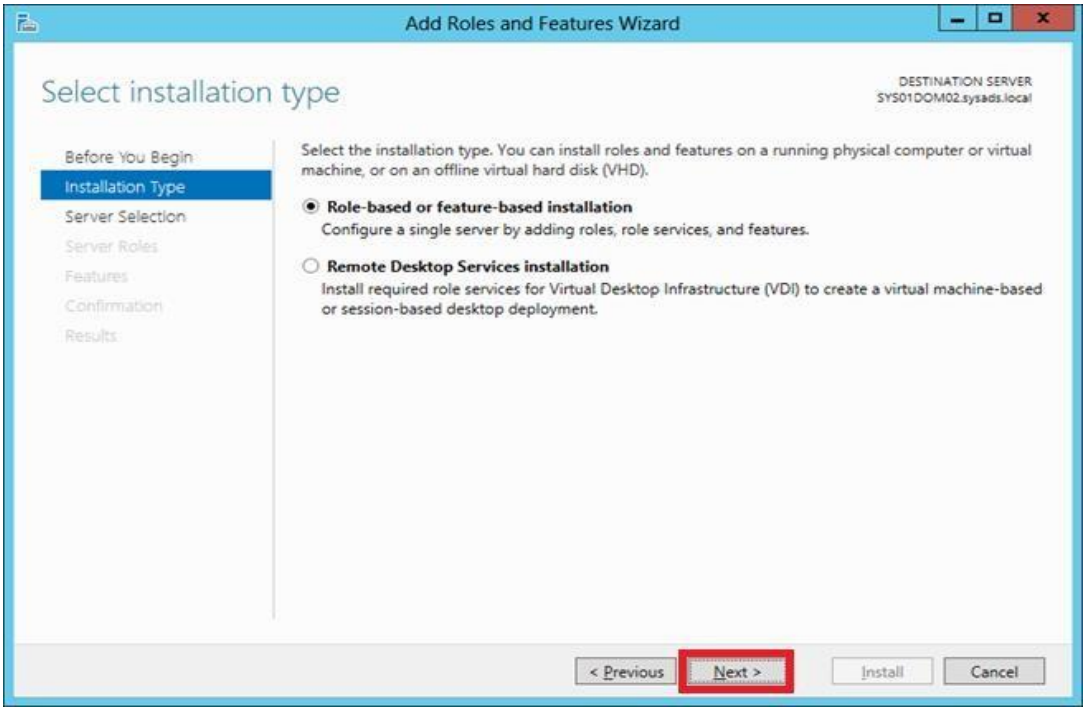

2. Click Add Roles and Features from the Manage Menu



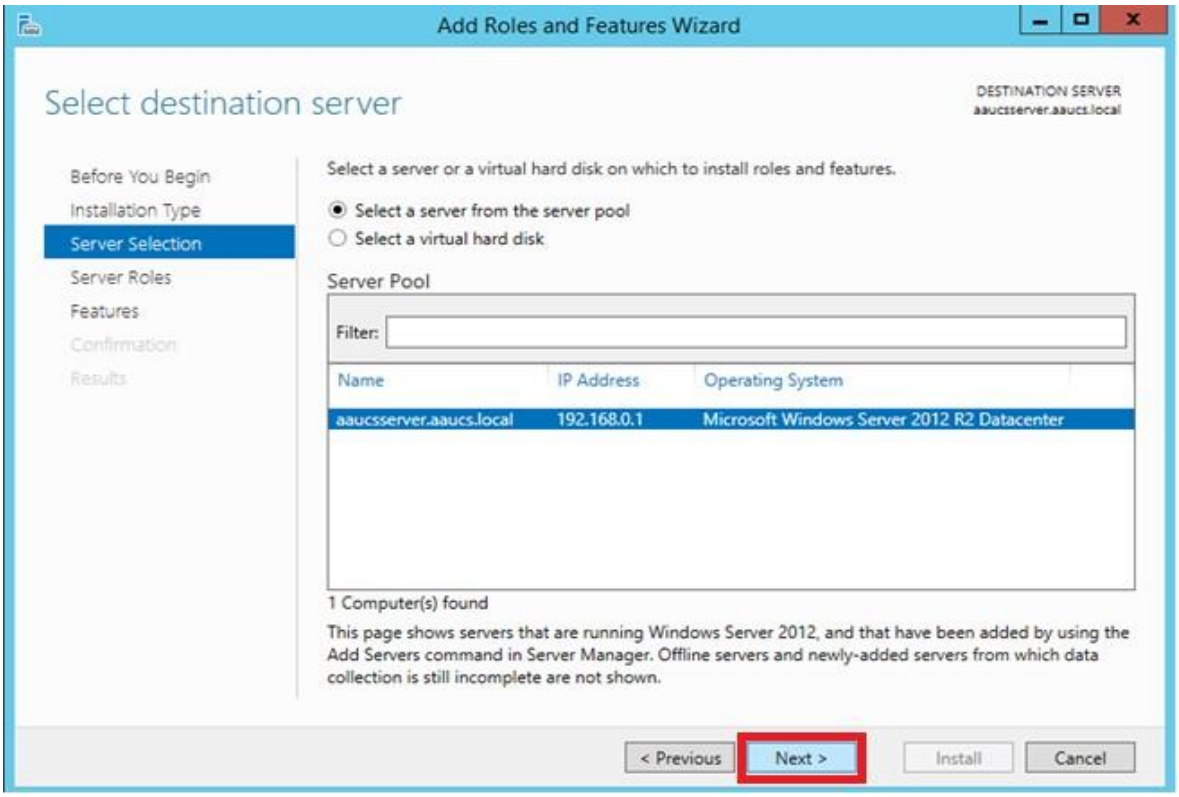

3. On Add Roles and Features wizard begins and click **Next**.



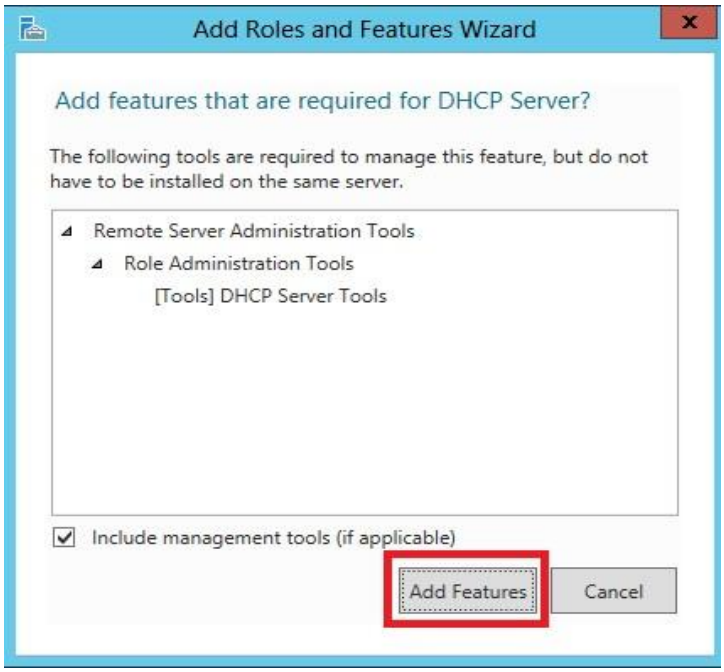

4. Select the Role-based or feature-based installation option and click **Next**.



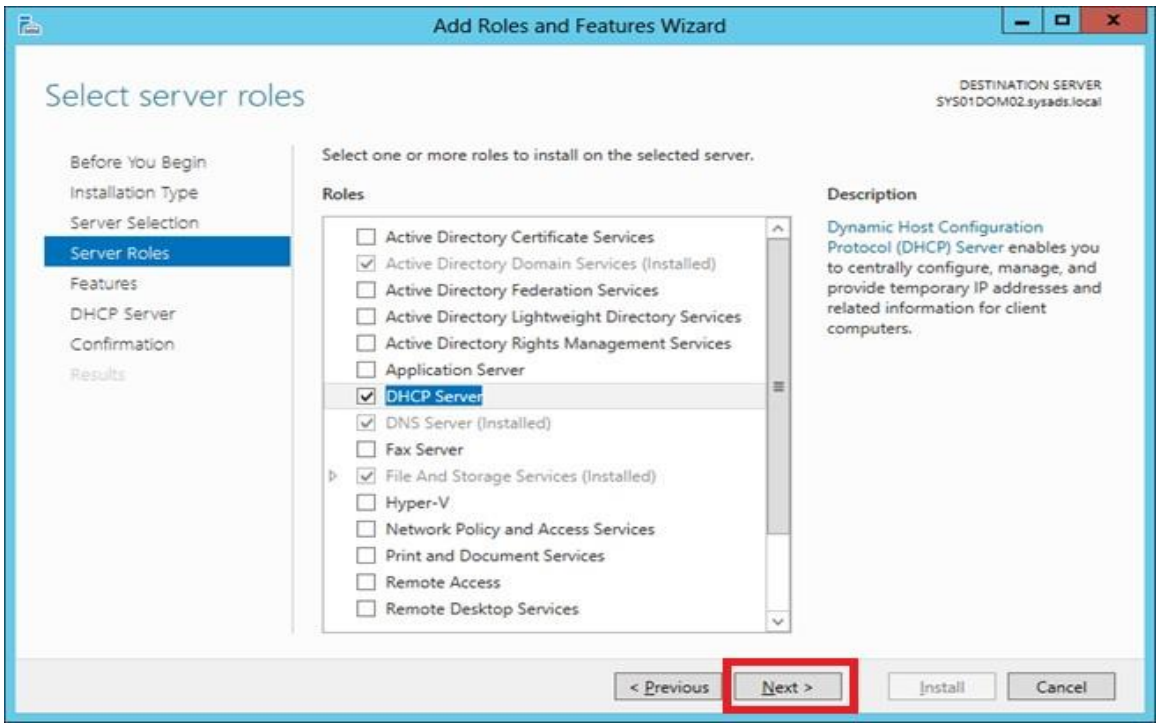

5. If you have more than one server managed through the server manager console, select the desired server you'd like to install DHCP on.



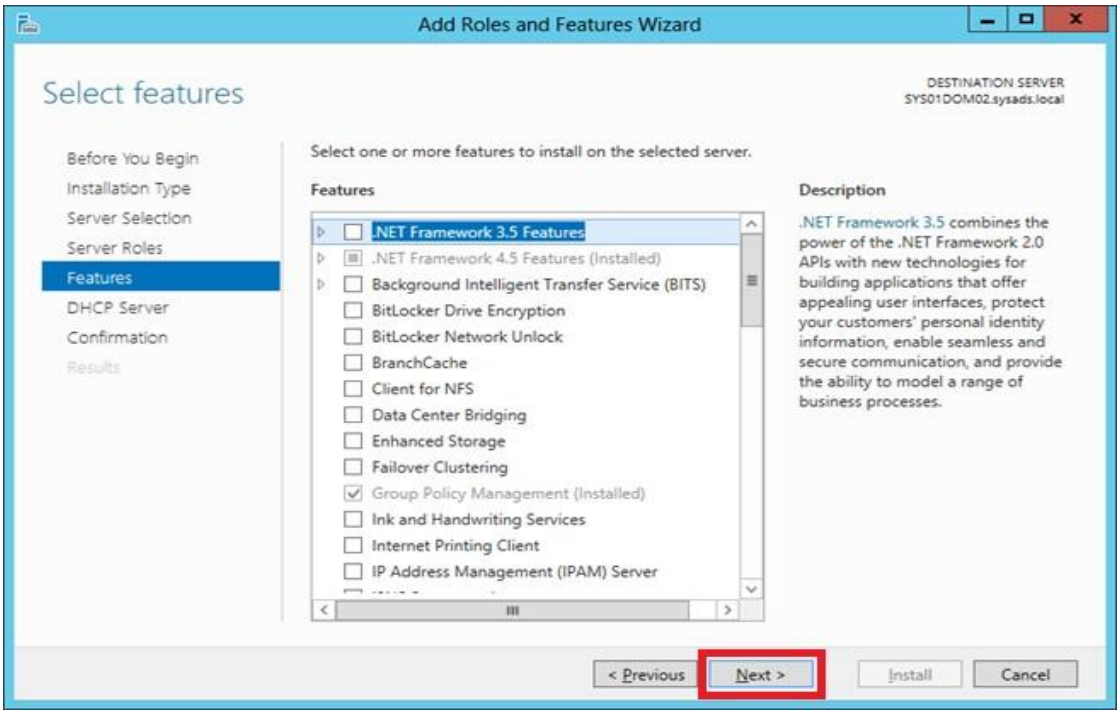

6. From the Roles lists, check the DHCP Server role, click **Add Features** on the popup window.



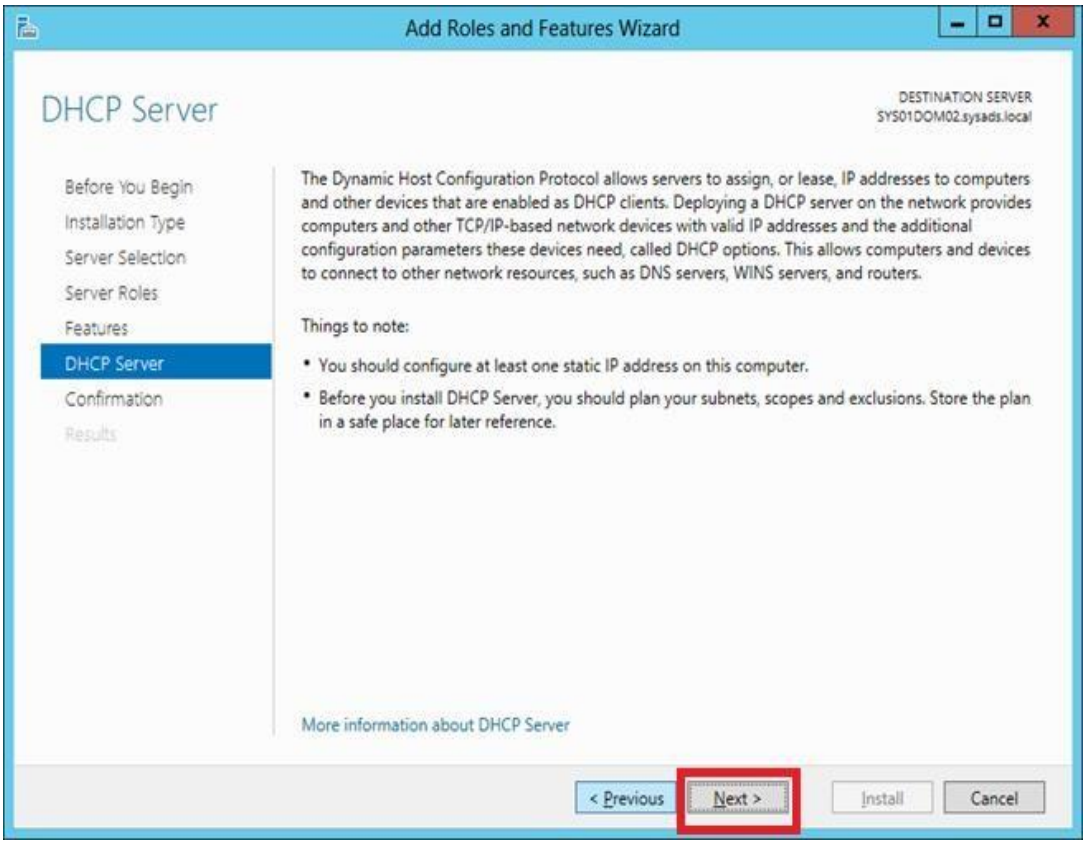
7. Just Click **Next.**



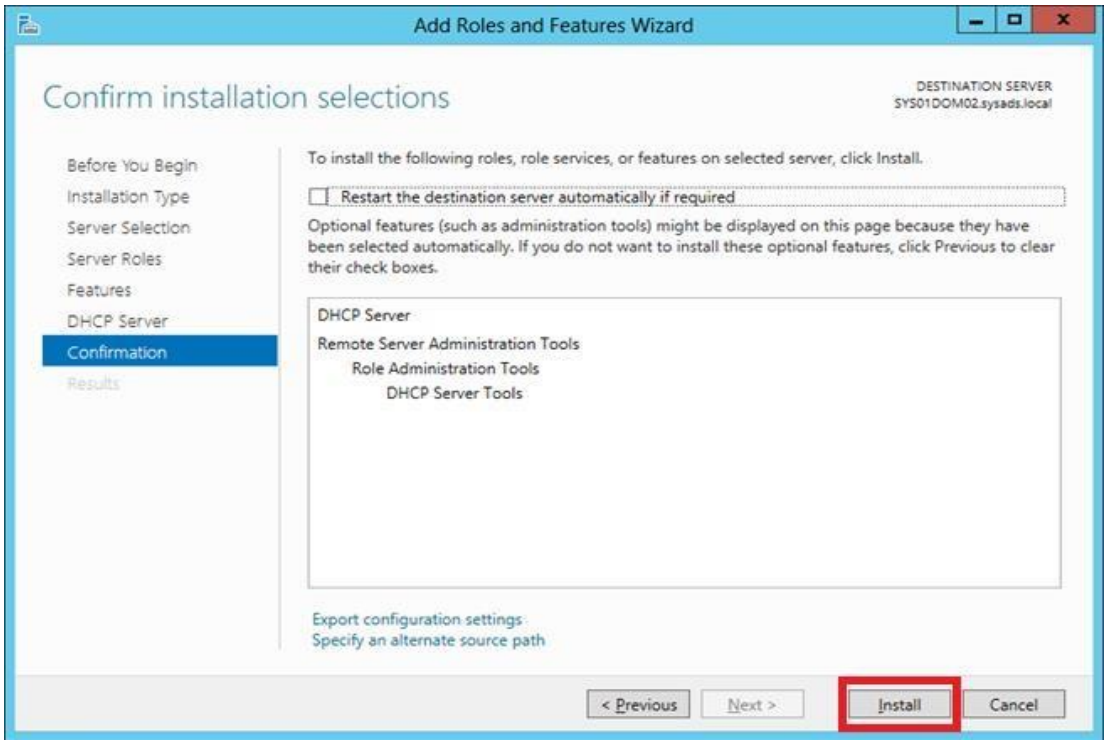

8. Select additional features you desire or leave as default and click **Next**.



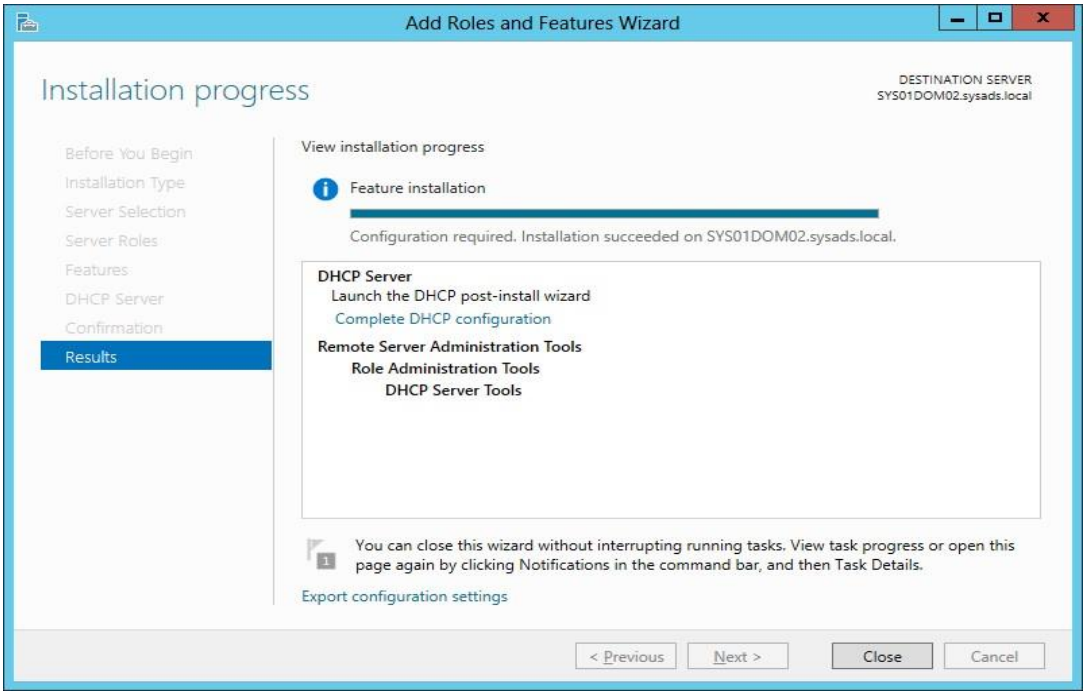
9. Keep in mind ‘Things to note’ and click **Next**.




10. Confirm information on summary page and click **Install**.

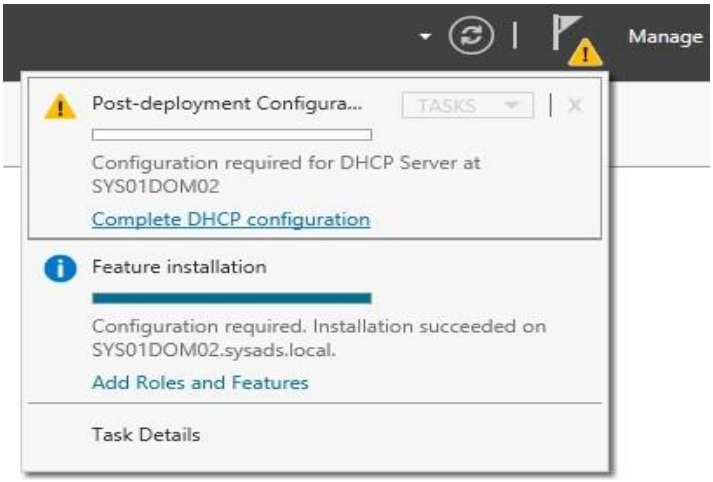



11. After installation process is completed, click **Close.**

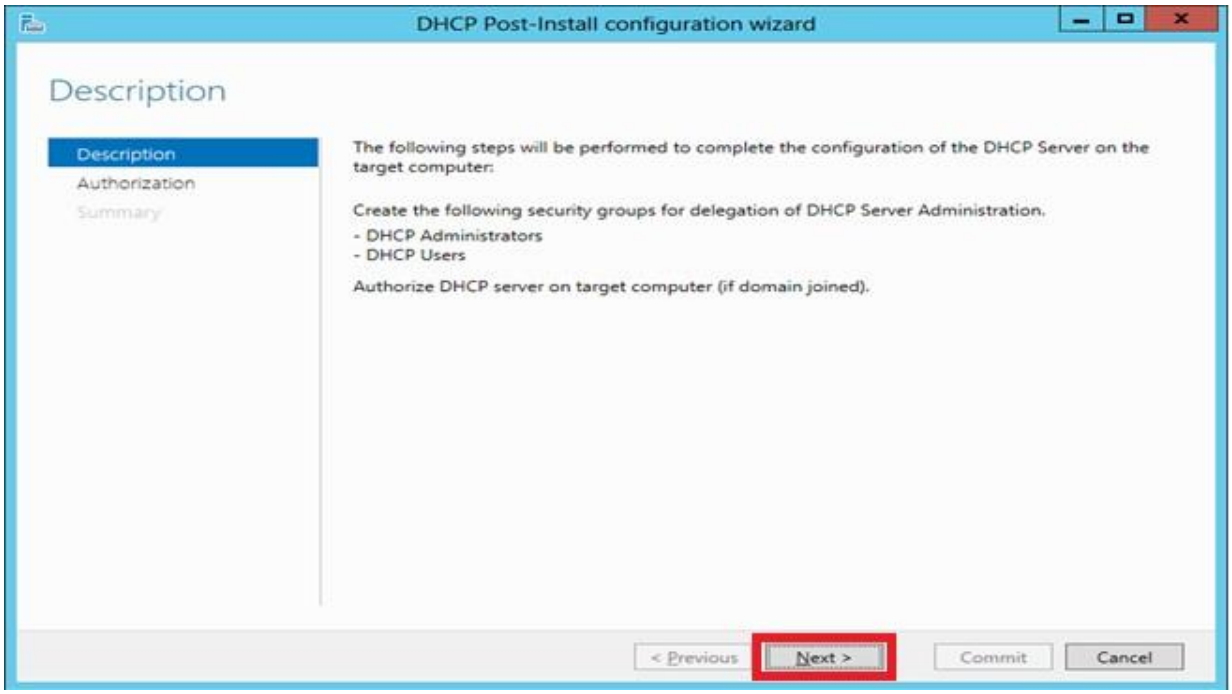


## 13.3 Configuration of DHCP role after installation

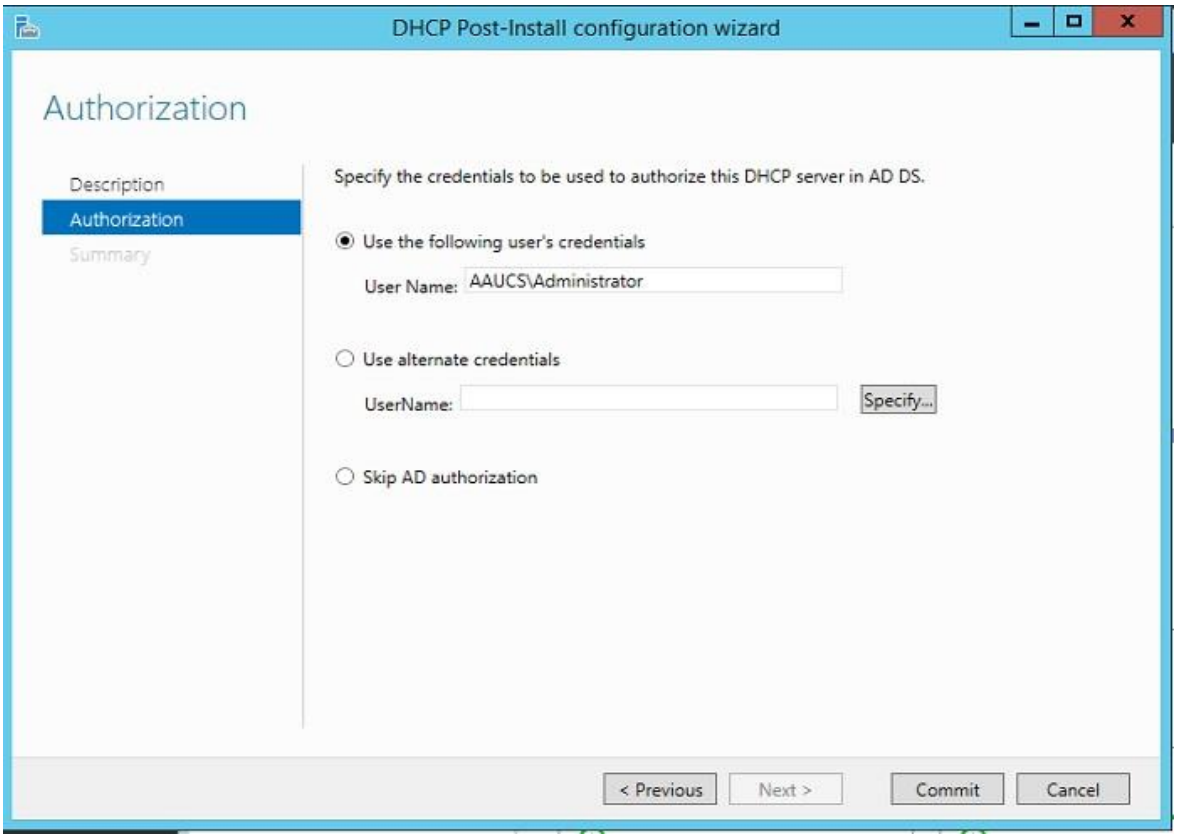
1. **Post Deployment:** open **the Server Manager** Click on the warning (Notification) icon and then click on '**Complete DHCP Configuration**'



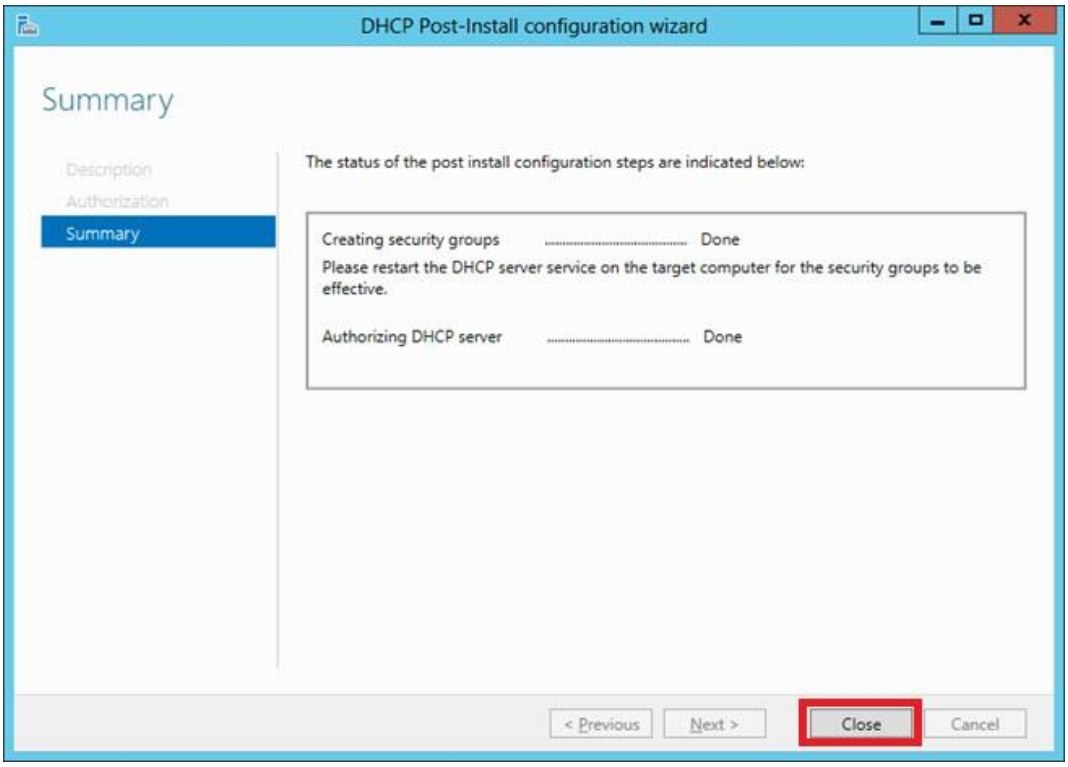

2. On DHCP Post-Install wizard, click **Next**.




3. On Authorization, select a domain user account that has permissions to create objects in the Net Services container in Active directory (For security lock-down) or simply use a domain admin account and click **Next**.



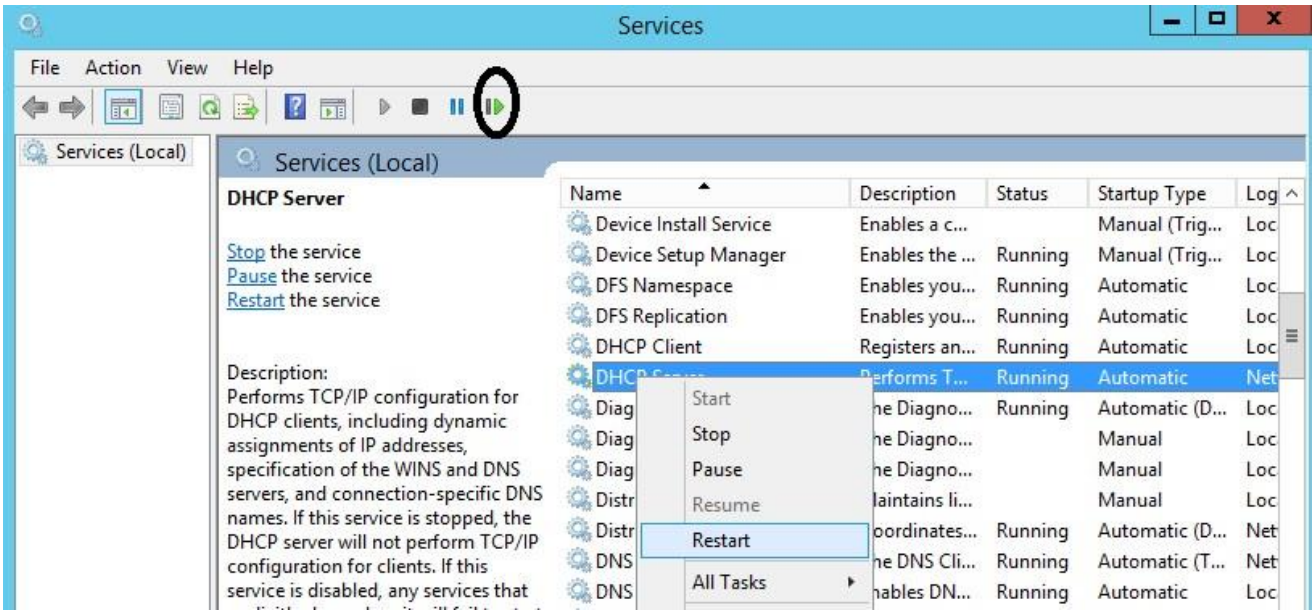

4. Confirm on summary page that the security groups had been created and Authorizing DHCP server role done. **Close** the screen



❖ For the security groups to come into effect, we need to restart the DHCP Server service

5. Click on **Tools** on **Server Manager** menu and click on **Services**


6. Finally Locate "**DHCP Server**" service, click on the **Restart** Service icon to restart the service.

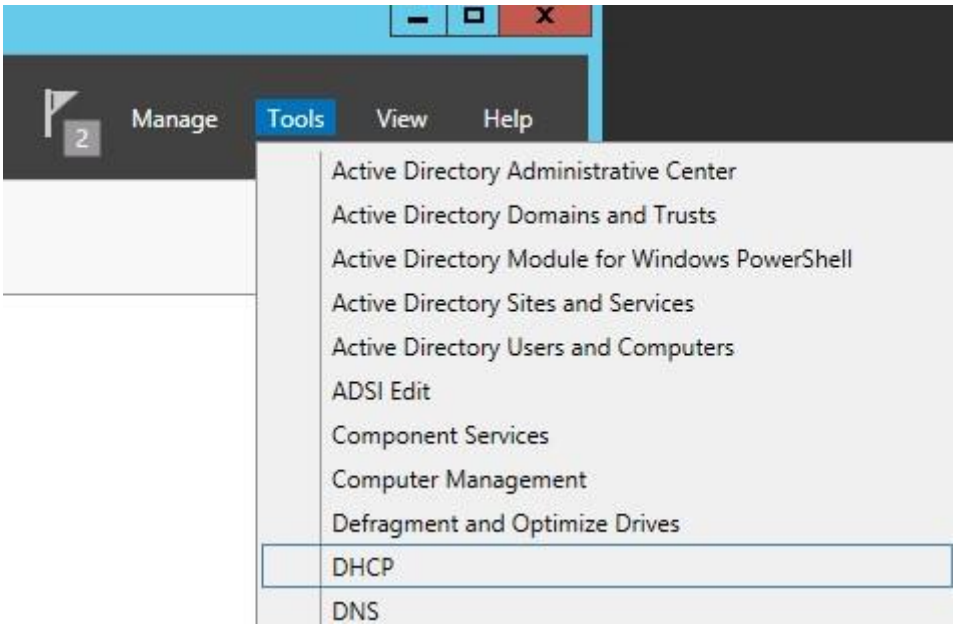



### 10.3.1 Creating a new IPv4 DHCP scope

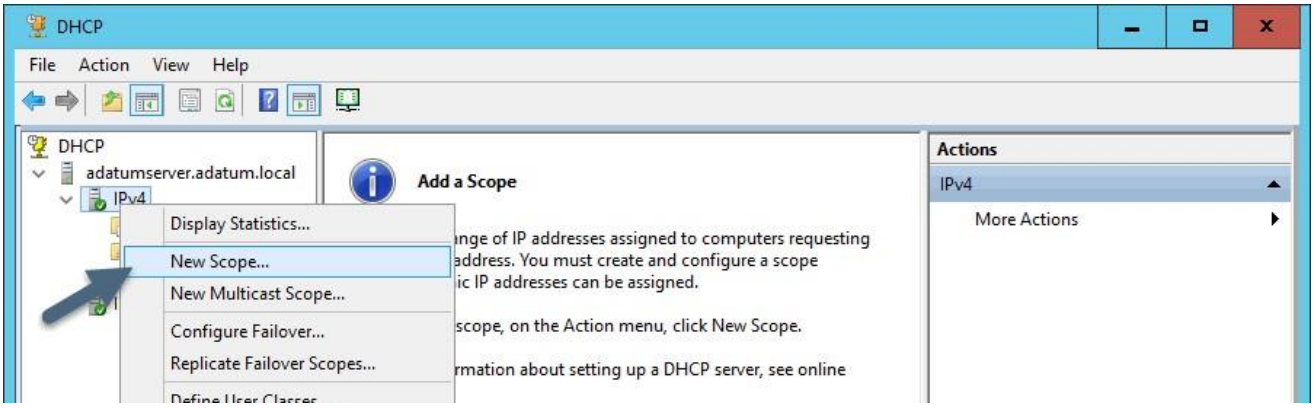
A scope is needed so we can define a range of IP addresses that can be handed out to clients.

Steps:-

1. From Server Manager Tools menu chooses **DHCP**.

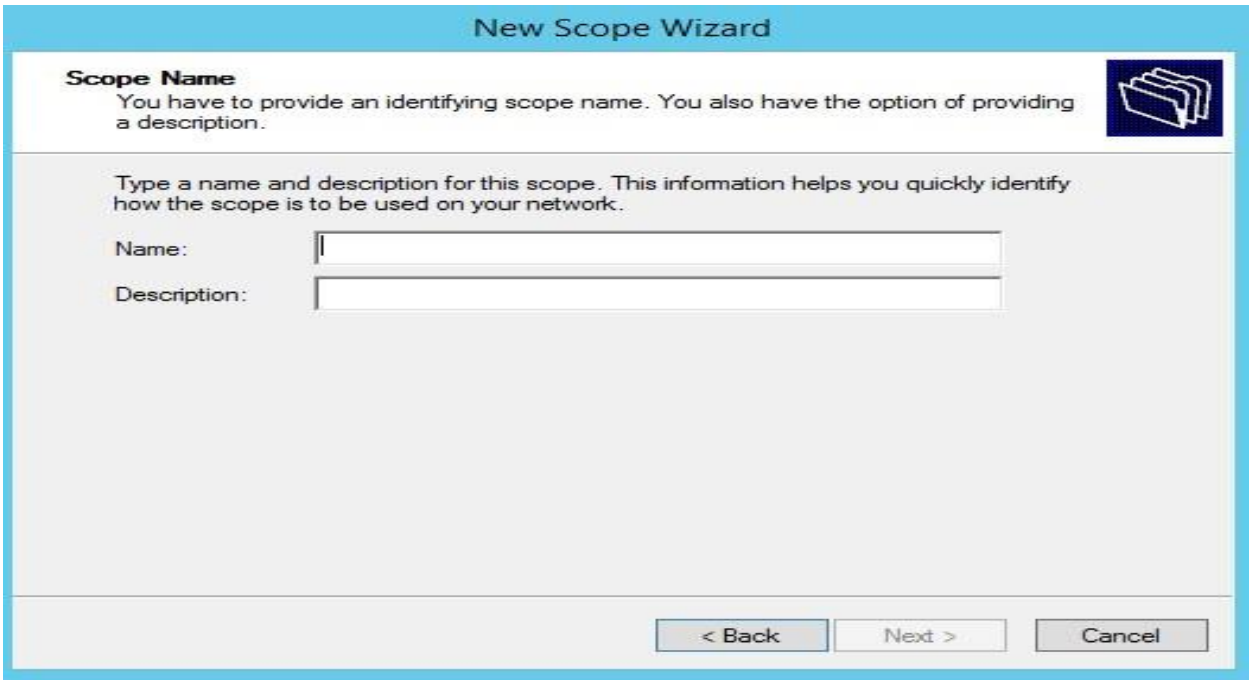


2. Right click **IPv4** and choose new Scope.

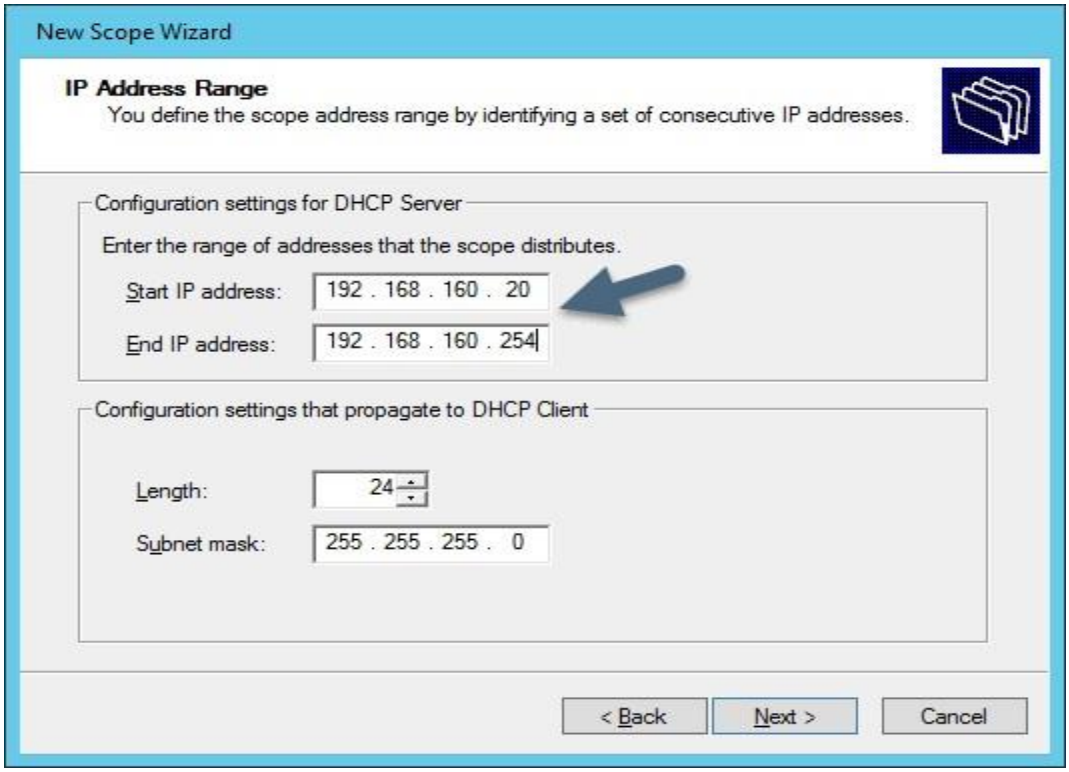



3. Click **Next**

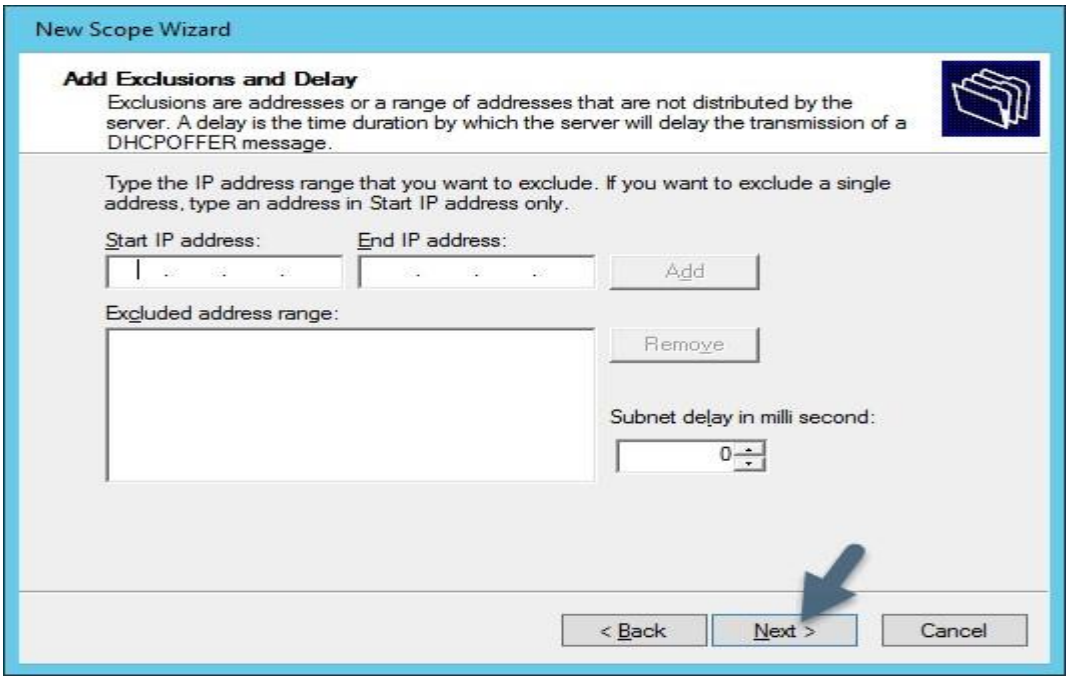

4. Give the scope a meaningful name that you want in addition to the description about it and click **Next**.



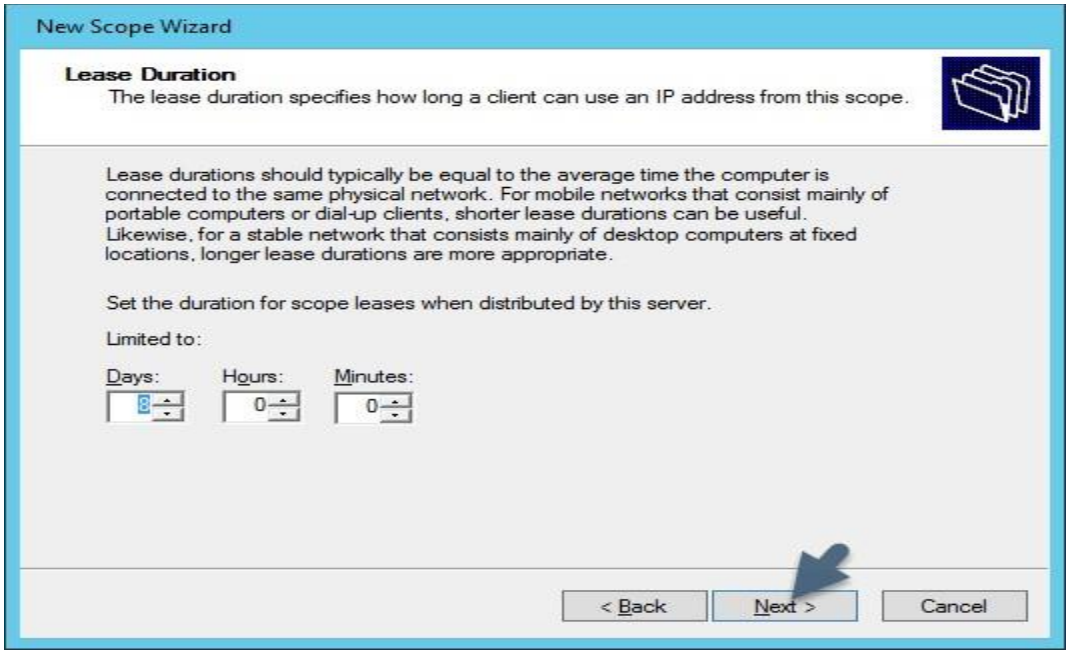

5. In this case the scope starts at .20 and let it end at .254. You may wish to change this to your needs.



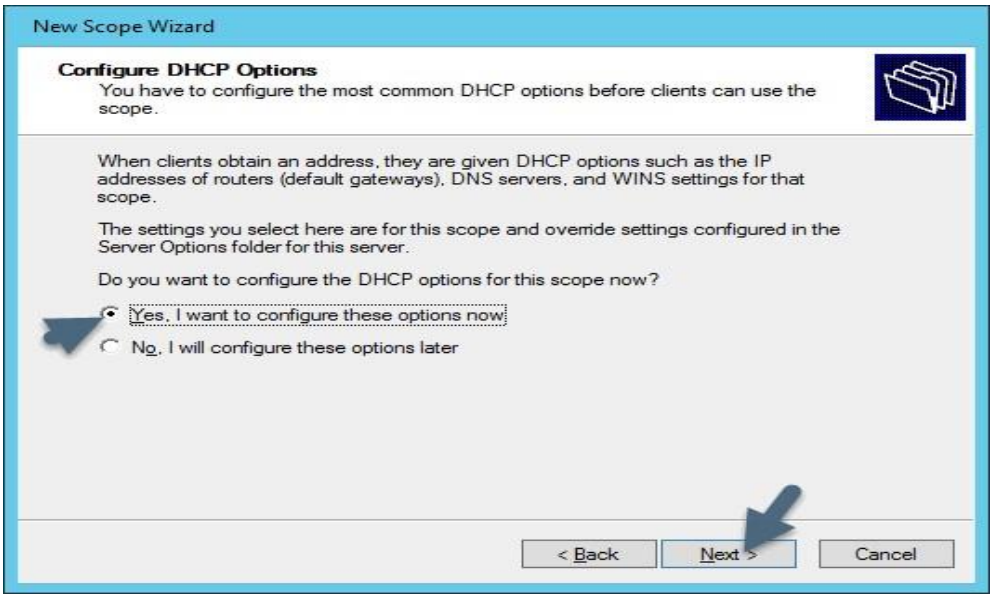

6. In this our IPV4 scope we do not set exclusions or delays but you may need them and can exclude some range of IP address here.



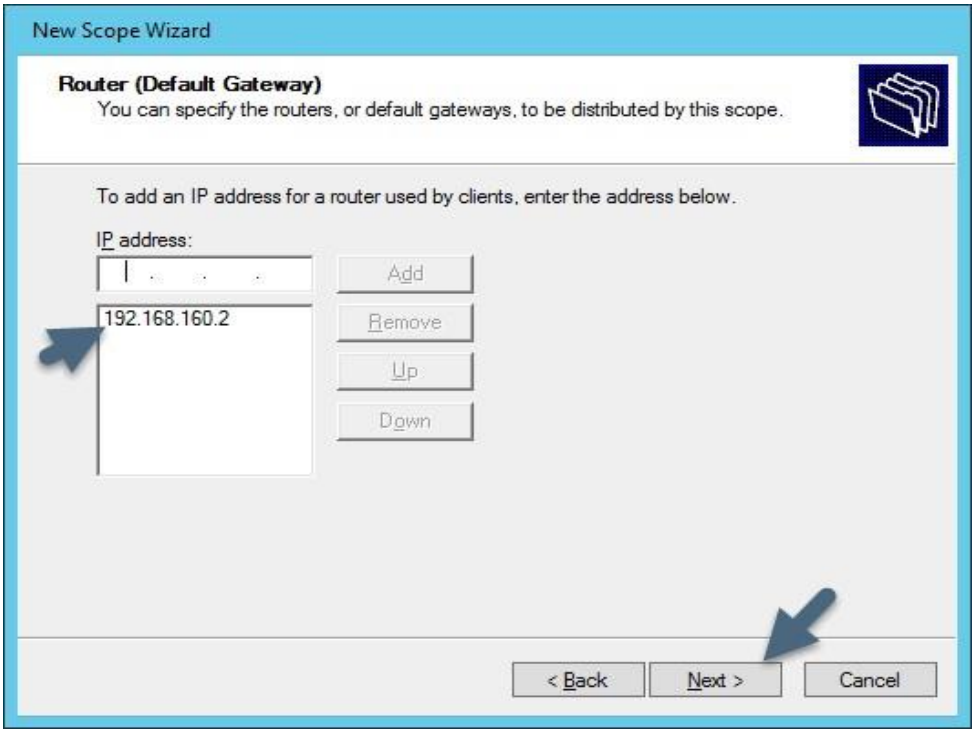

7. Accept the defaults and click Next



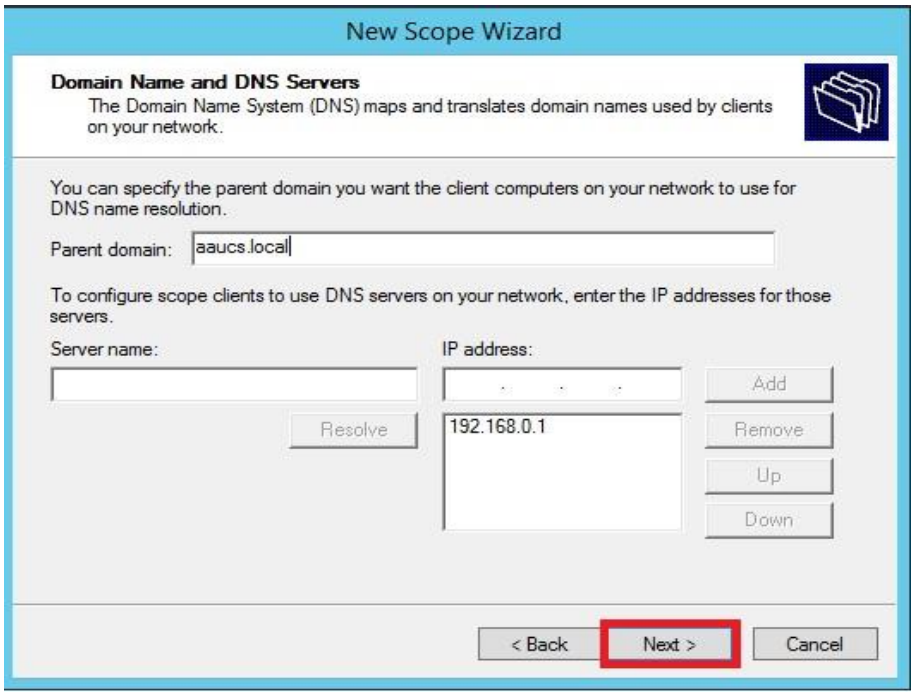

8. Yes, we will configure DHCP options. Click **Next**.



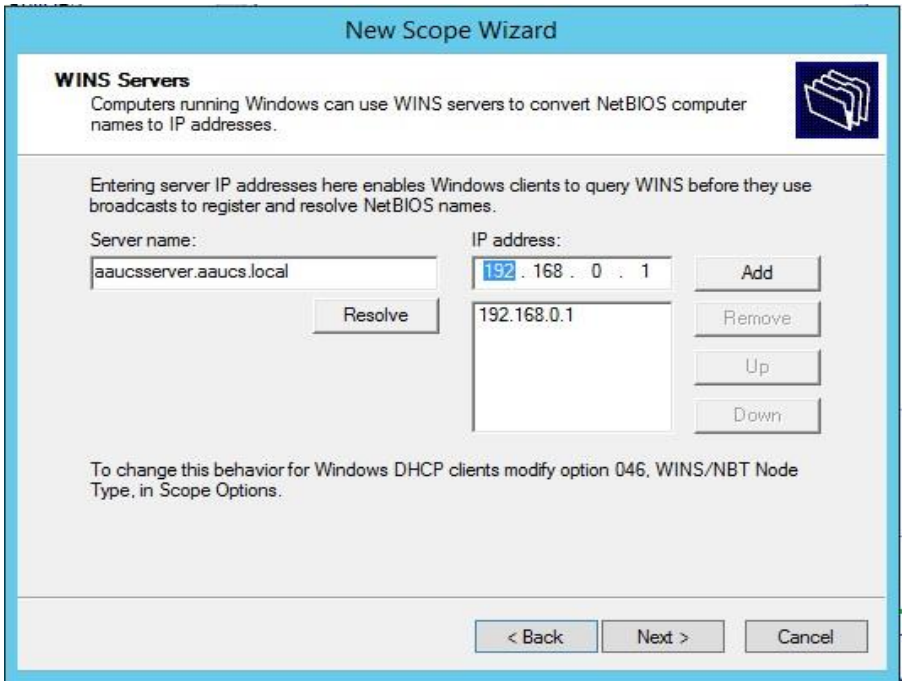

9. In our case the router is at 192.168.160.2 and Click **Next**.




10. Under normal circumstances the wizard will detect the **DNS** server that is installed during the installation of the **DNS** server role or a domain. Click **Next**.



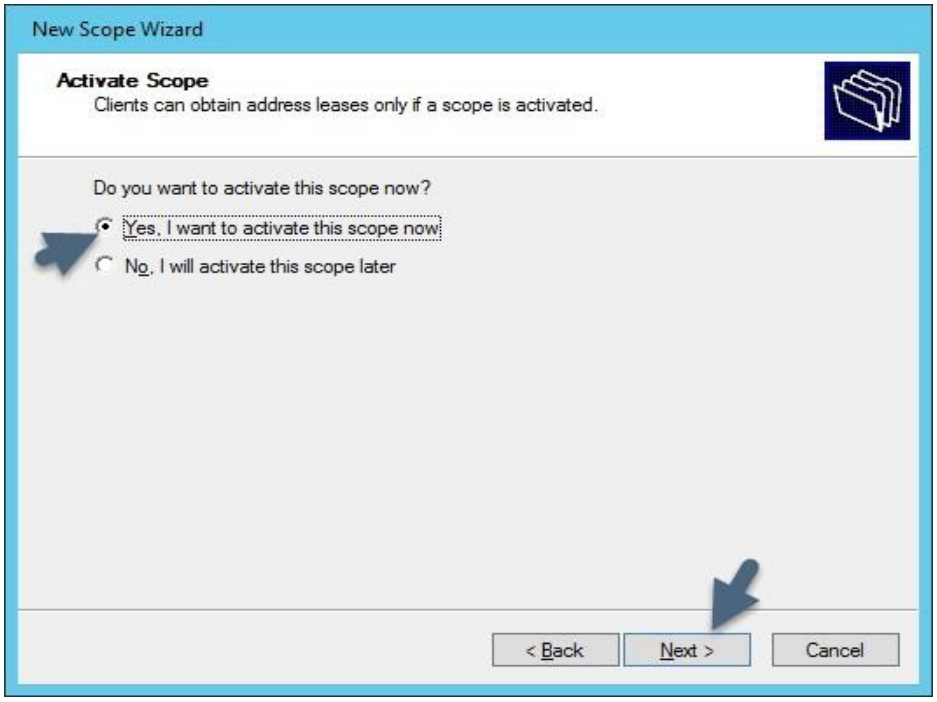

11. Here we do not support any **WINS** servers so just Click **Next**.




- **Windows Internet Name Service** (**WINS**) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name **server** and service for NetBIOS computer names.

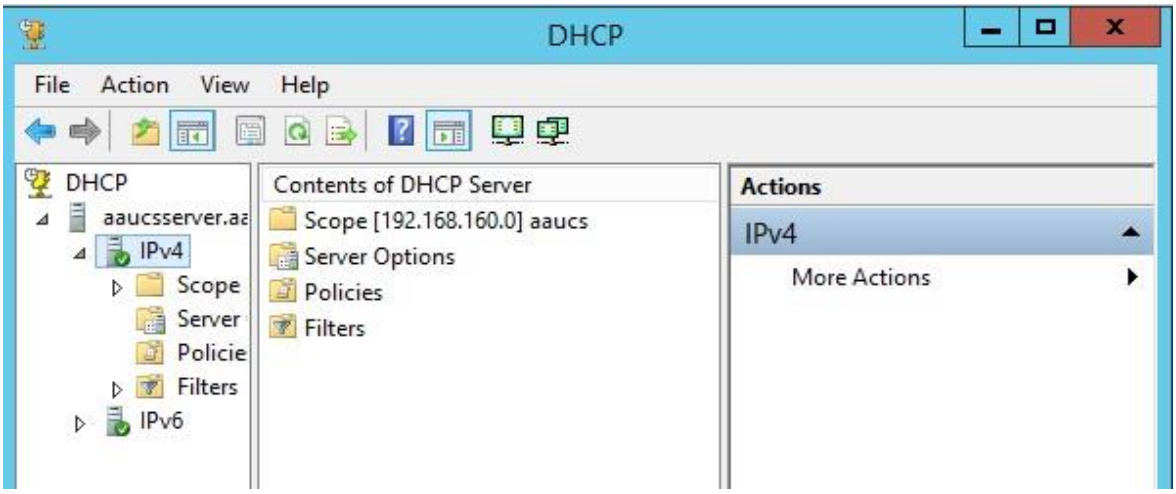
Effectively, **WINS** is to NetBIOS names what DNS is to domain names — a central mapping of host names to network addresses.

12. Click **Next**




13. Just Click **Finish**


14. Here is our **IPv4 DHCP scope**.



# Chapter Fourteen: Installation and configuration of FTP server

## 14.1 Enable Web Server (IIS) role and FTP Server role service:

1. Log in to the server by using an administrative account
2. Open Server Manager
3. Go to **Manage > Add Roles and Features**
4. Click **Next**
5. Select **Role-based or feature-based installation**
6. Click **Next**
7. Select  a server from the **server pool**, and select your server
8. Click **Next**.
9. Scroll down and put a check mark in **Web Server (IIS)**
10. An Add features window pops up. Put a check mark in the **Include management tools (if applicable)** option
11. Click **Add Features** button
12. Click **Next**
13. Click **Next**
14. Click **Next**
15. Scroll down and put a check mark in: **FTP server**, **FTP Service** and **FTP Extensibility**.
16. Click **Next**
17. Click **Install**
18. When installation is finished, click **Close**

## 14.2 Create FTP users:

You need to create users in Windows in order to be able to use FTP services. You can use either local or domain users. In this case, you will create some local users. The only thing that changes if you use domain users is, when you log in to FTP, you must use the domain/account format.

1. In Server Manager go to **Tools**
2. Click **Computer Management**

3. Click **Local Users and Groups**
4. Click **Users**
5. In the center pane, right-click a blank area and then select **New User…**
6. Enter the username information and click the **Create** button
7. Create as many usernames you need here.

➢ Optionally, you can create a group that contains all the FTP users in the **Groups** folder and add the users you created above.

## 14.3 Configuring FTP global IIS settings:

You need to configure some global settings for your IIS server before creating your FTP site. It is very easy, follow the steps below:

1. In Server Manager go to **Tools**
2. Click **Internet Information Services (IIS) manager**.
3. In the left pane, double-click the server icon (in the tree below the option **Start Page**)
4. If a window pops up asking about Microsoft Web Platform, select **Do not show this message**, and click the **No** button
5. In the center pane, double-click the **FTP Authentication** icon
6. If you want to allow anonymous users, right-click **Anonymous Authentication** and set it to **Enable**.
7. To allow access to the windows users you created in Part Two above, right-click **Basic Authentication** and set it to **Enable**.
8. In the left pane, double-click the server icon.
9. Double click the **FTP Authorization Rules** option
10. Delete all rules in the center pane.
11. After all rules have been deleted, right-click a blank area in the center pane and select the option **Add Allow Rule…**
12. Click the option **Specified users.**
13. In the text box type the usernames (separated by commas) you created in Part Two above.
14. Check either the boxes **Read** or **Write** depending the access you want to grant to the user or group of users you are adding.

15. Click the **OK** button
16. Repeat steps 8 to 15 if you want to add more users with different Read / Write permissions.

## 14.4 Creating FTP site:

1. Open Windows Explorer
2. Navigate to **C:\inetpub\ftproot**
3. This is the default local folder where the FTP directory tree will be saved 4. You can create your own folder in another directory or hard drive if you want.
5. Create your own folder at this point if it is desired.
6. Open **Server Manager**
7. Go to **Tools**
8. Click on **Internet Information Services (IIS) Manager**
9. In the left pane, right-click the server icon (in the tree below the option Start Page)
10. Click **Add FTP Site**
11. In FTP site name type a friendly name for your site. (**My FTP Site** for example)
12. In **Physical path** browse to the folder you creates in steps 2 to 5
13. Click **Next**
14. In IP Address, click the drop down menu, and select the server's IP address you want to assign to the site
15. Port remains as **21** by default. You can change it if you want.
16. Ensure the option **Start FTP site automatically** is checked
17. Select the **No SSL** option if you are not required to use certificates. Otherwise, select one of the other options.
18. Click **Next**
19. In the Authentication section, put a check mark in **Anonymous** If you want to allow anonymous users.
20. Put a check mark also in **Basic** to allow access to users created in Part Two.
21. In the Allow access to: drop down menu, select: **Specified Users** 22. In the text box type the usernames of the users you created in Part Two.
23. Check the box **Read** to grant read access to users.
24. Check the box **Write** to grant write access to users.

25. Click **Finish**

## 14.5 IIS Firewall setup:

1. In Server Manager go to **Tools**
2. Click **Internet Information Services (IIS) manager.**
3. In the left pane, double-click the server icon (in the tree below the option **Start Page**)
4. In the center pane, double-click the **FTP Firewall Support** icon
5. In the **Data Channel Port Range** box, make sure the value is **0-0** to use the default port range.
6. Or, you can change it if you want by your own set of ports.
7. Click **Apply**
8. Close Internet Information Services (IIS) Manager

## 14.6 Windows Firewall setup:

By default, all exceptions needed for FTP are added to the Windows Firewall at the time you enable the FTP Server role. Anyway, for troubleshooting purposes, the next steps show the configuration that needs to be in place in order to allow FTP traffic in your server.

1. Open Server Manager
2. In the left pane, click **Local Server**
3. In the right pane, click the hyperlink beside the **Windows Firewall** option. It should say **Public: On** (or off).
4. The Windows firewall window opens. In the left pane click **Advanced Settings**
5. The Windows Firewall with Advanced Security window opens. In the left pane click **Inbound Rules**.
6. In the right pane, verify there's a rule called **FTP Server (FTP Traffic-In)**
7. Double click this rule.
8. In the **General** tab, verify the option **Enabled** is checked.
9. Go to the **Protocols and Ports** tab.
10. Verify the Protocol type is **TCP** and the **Local port** value is **21**.
11. Go to the **Advanced** tab

12. Make sure the profiles: **Domain**, **Private** and **Public** are checked.
13. Click **OK** button
14. Execute the same validation in steps **7-13** for the **FTP Server Passive (FTP Passive TrafficIn)** rule. Except that the local port value in this rule should be **1024-65535**
15. Execute the same validation in steps **7-13** for the **FTP Server Secure (FTP SSL TrafficIn)** rule. Except that the local port value in this rule should be **990**
16. In the left pane, click **Outbound Rules**
17. Execute the same validation in steps **7-13** for the **FTP Server (FTP Traffic-Out)** rule. Except that the local port value in this rule should be **20**
18. Execute the same validation in steps **7-13** for the **FTP Server Secure (FTP SSL TrafficOut)** rule. Except that the local port value in this rule should be **989**
19. Close all windows.

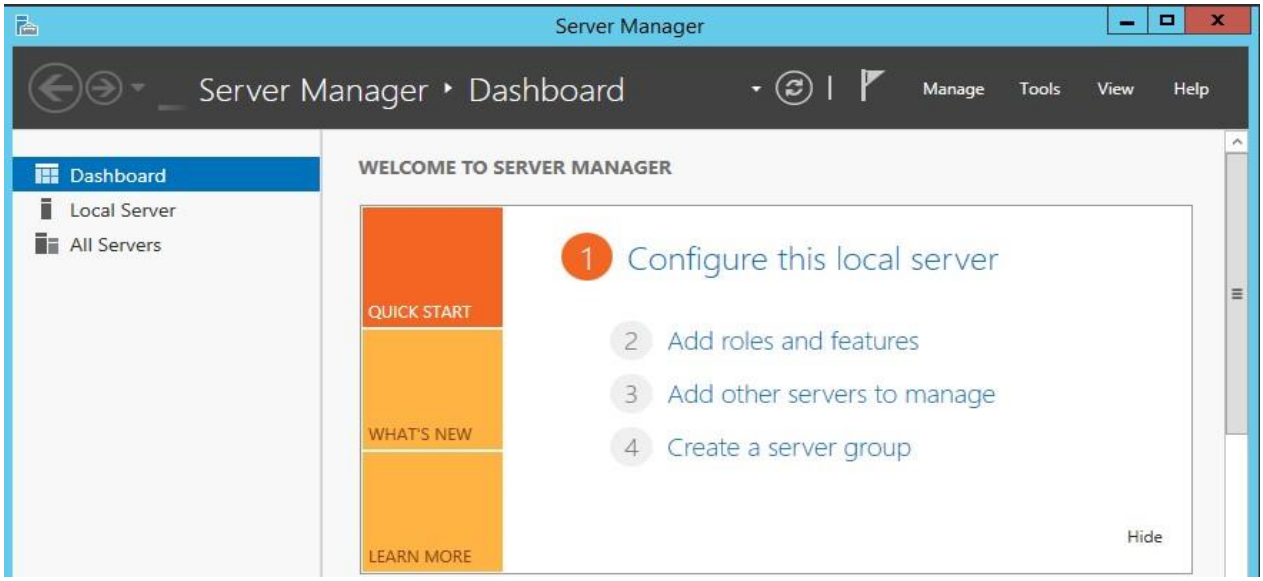
## 14.7 Testing:

- The last part is to test your work.
- Make sure you can connect to the FTP service, first from the local machine and then form a remote computer.
- Try to log in, put files, get files, show folder contents, etc.

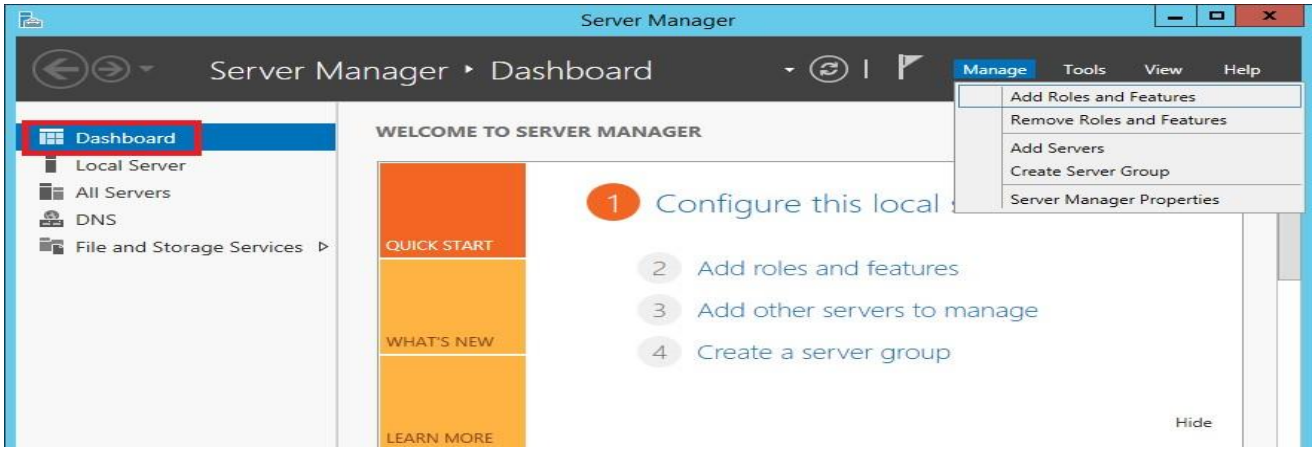
# Chapter Fifteen: Installation and Configuration of a Print Server

## 15.1 Print and Document Services role installation

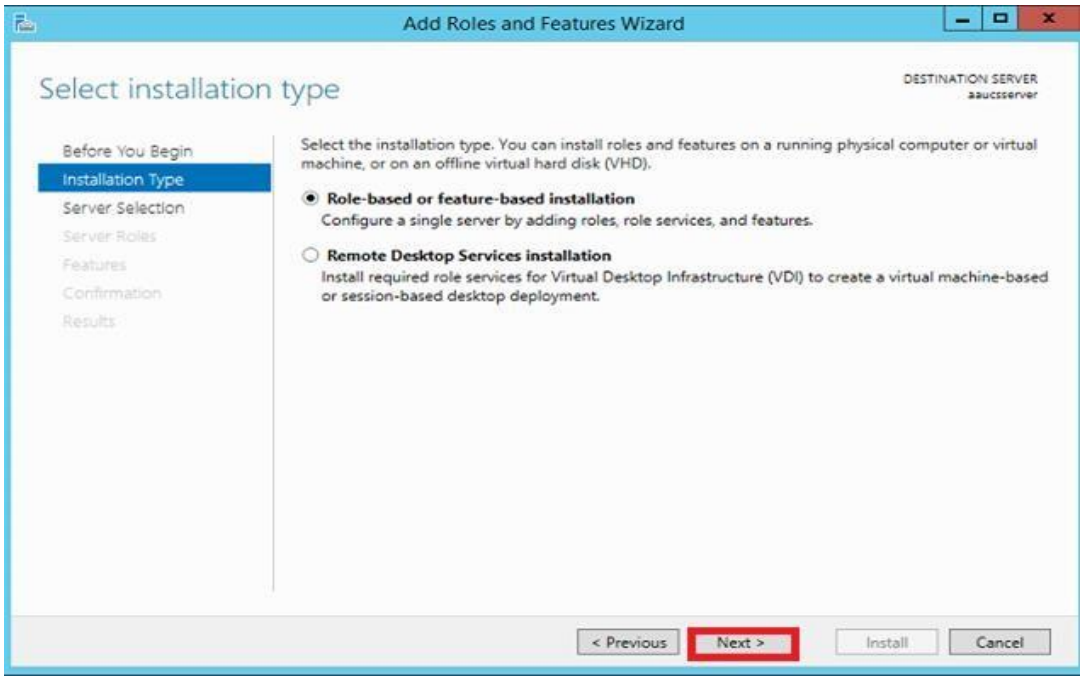
1. Open the **Server Manager** console.



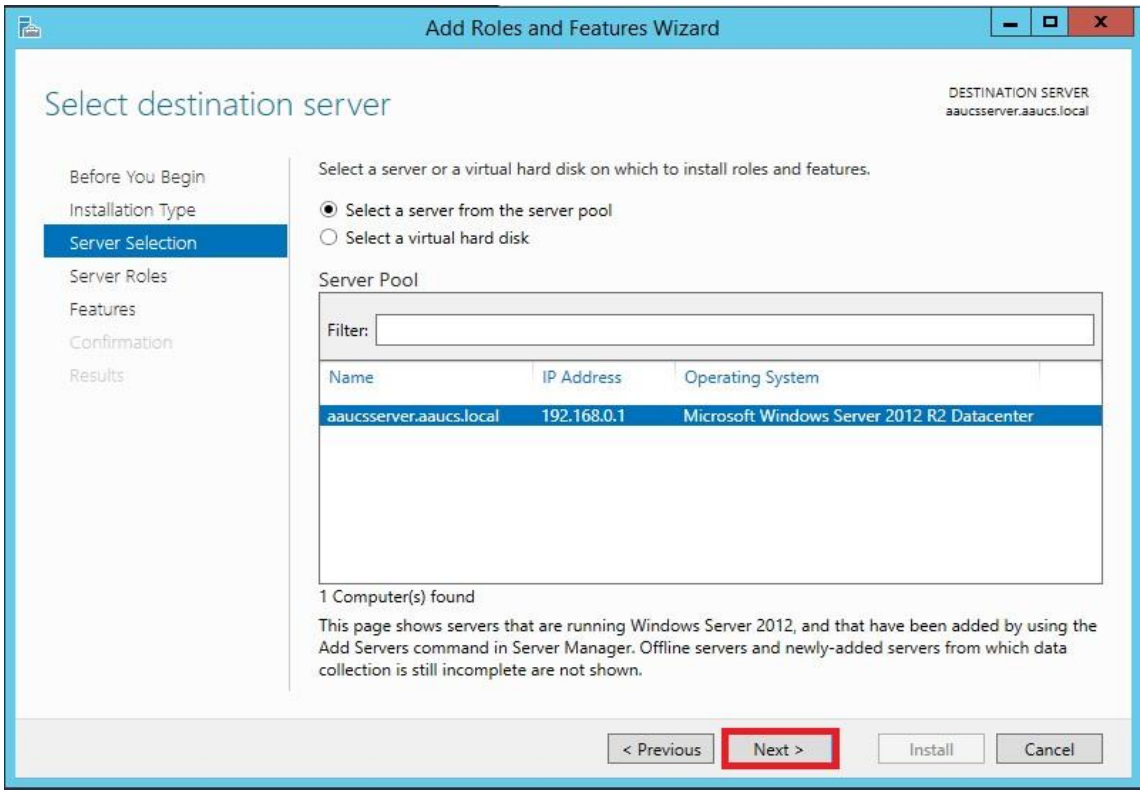

2. To install and configure the print server in Windows Server, you must install Print and Documents Services role. Go to Server Manager **Dashboard** click Manage tab then click **Add roles** and **features**.



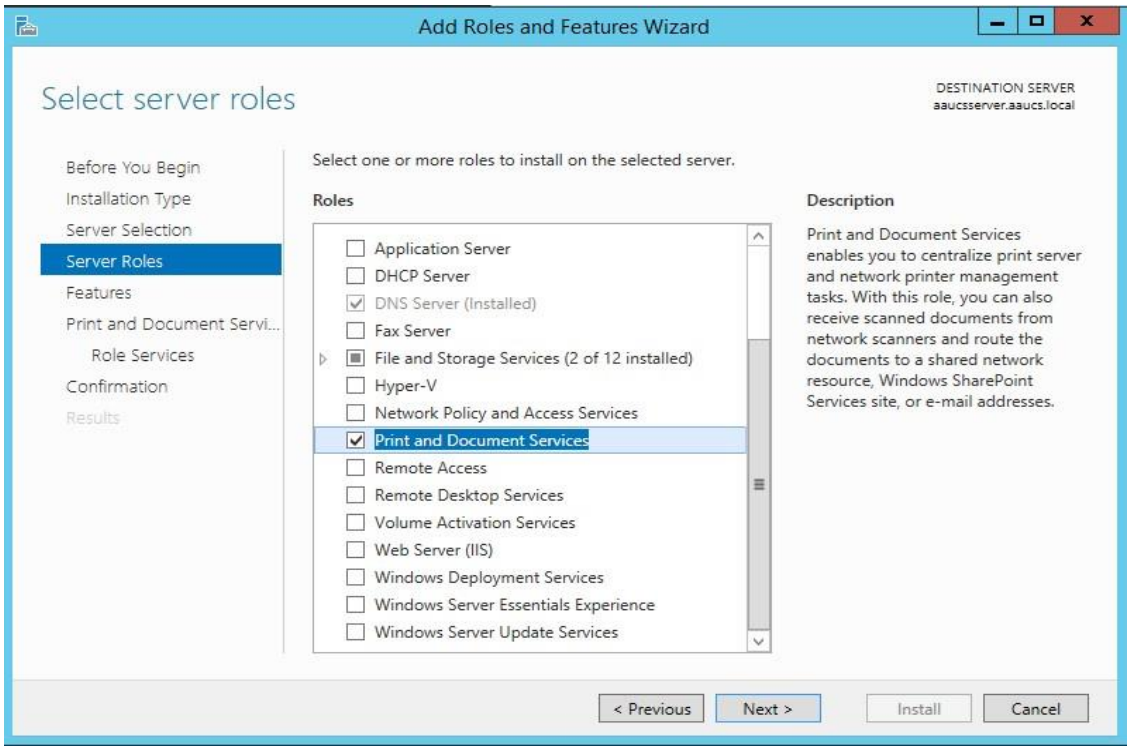

3. On the Before You Begin page click **Next** and select Role-based or feature based installation then click Next.



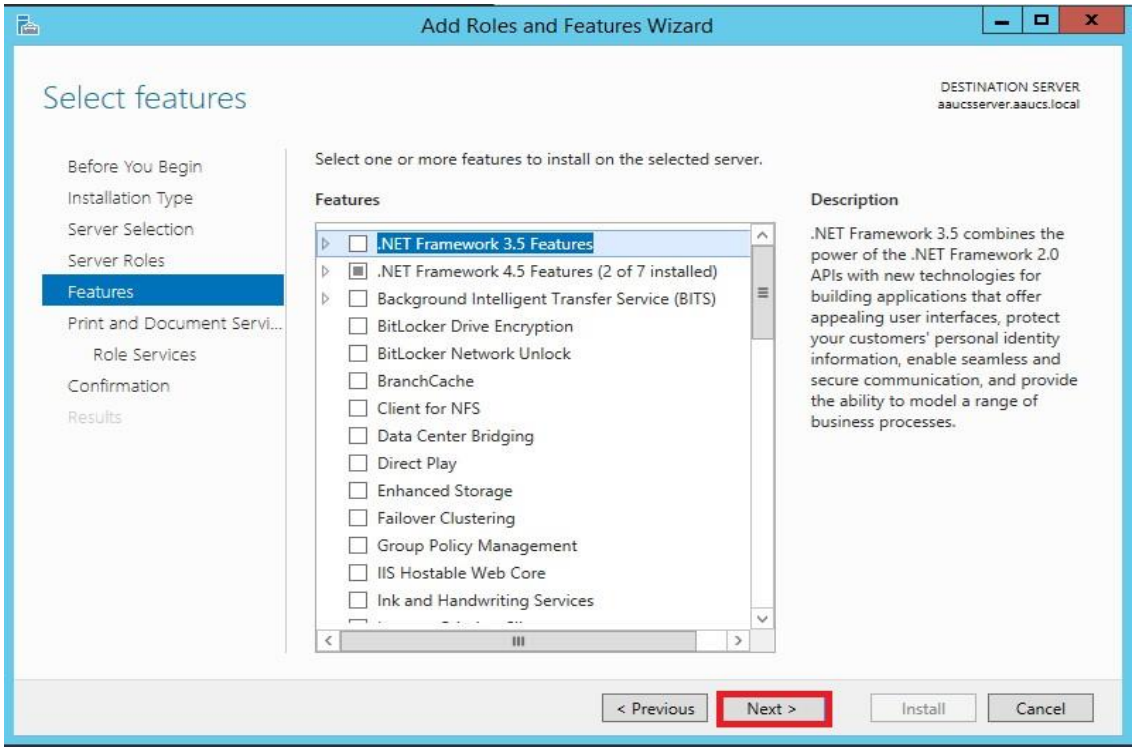

4. On the Server Selection page, choose the server you want then click **Next**.



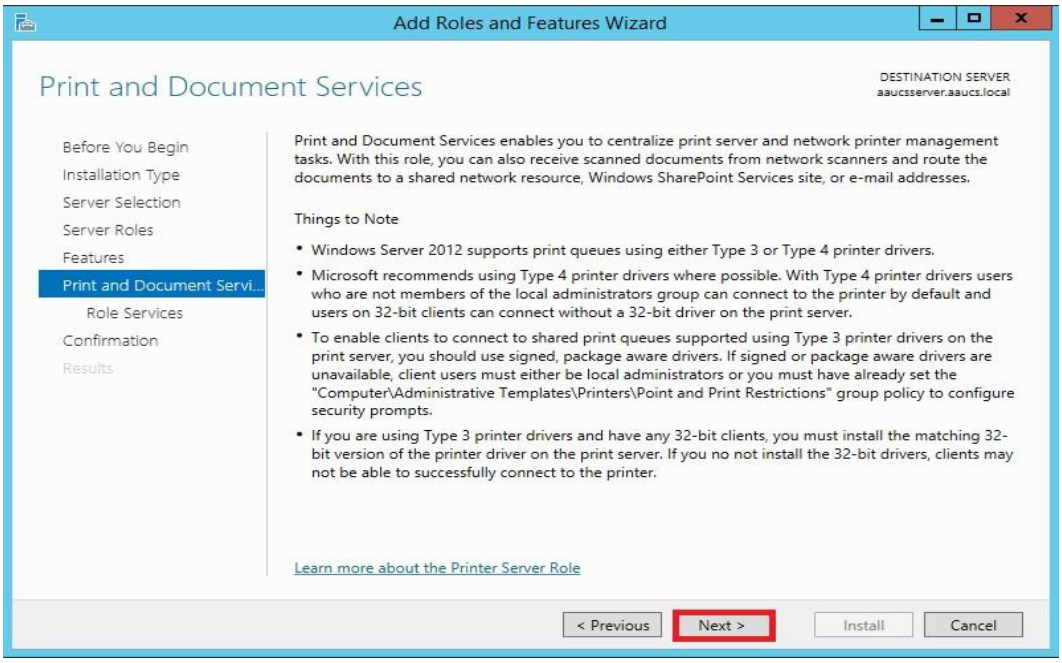

5. Select and tick the check box of "**Print and Document Services"** on the Server Roles page.



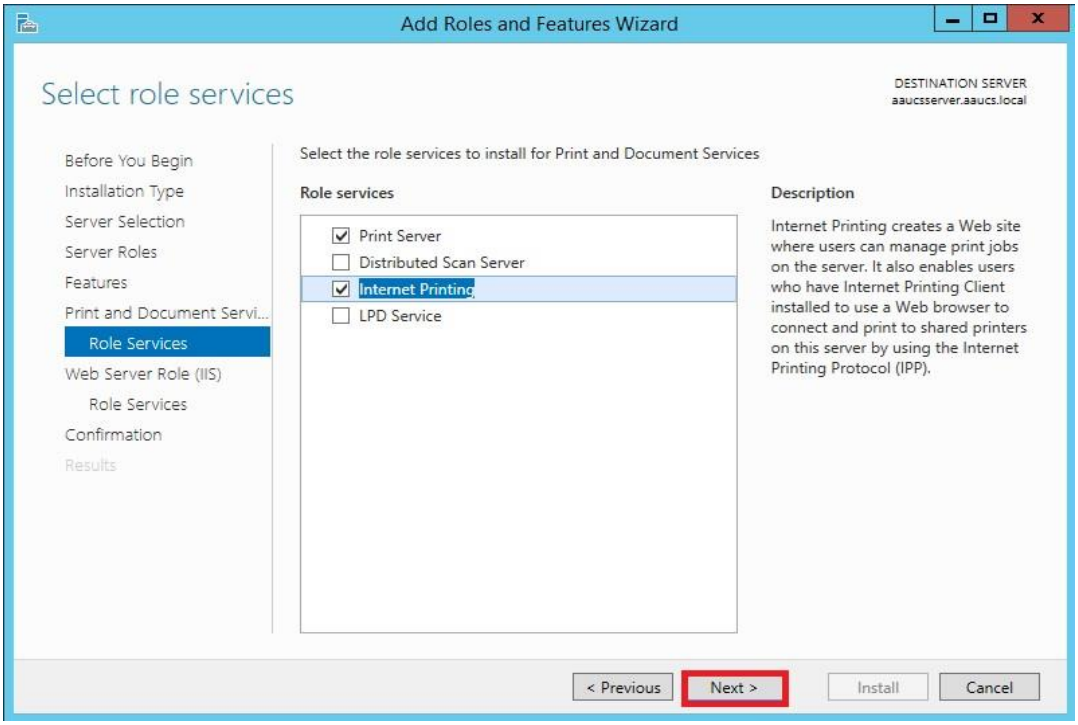

- Now the component and features want to be installed; just click **Add Features** and then click **Next**. Leave the Features page by default and click **Next**. You don't need to install any features for print and document services, so do nothing on this page.



- On the Print and Document Services page read all notification and click **Next**. It is necessary once to read this page carefully.




6. Select the Print Server and Internet Printing options from Role Services.

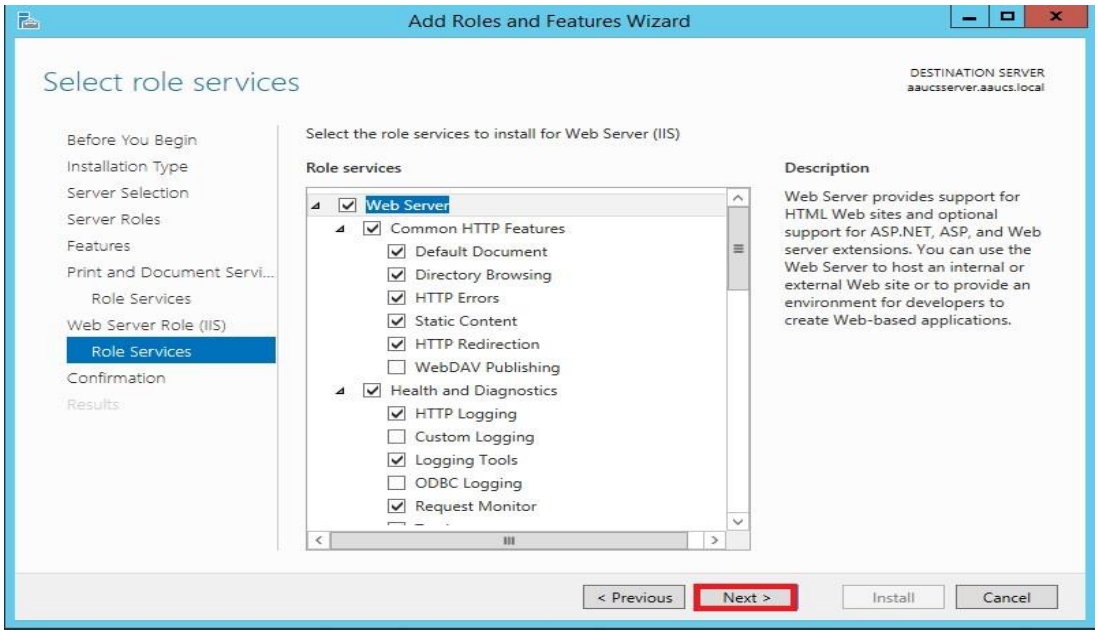


➢ Click Add Feature to install IIS web server with components and features.

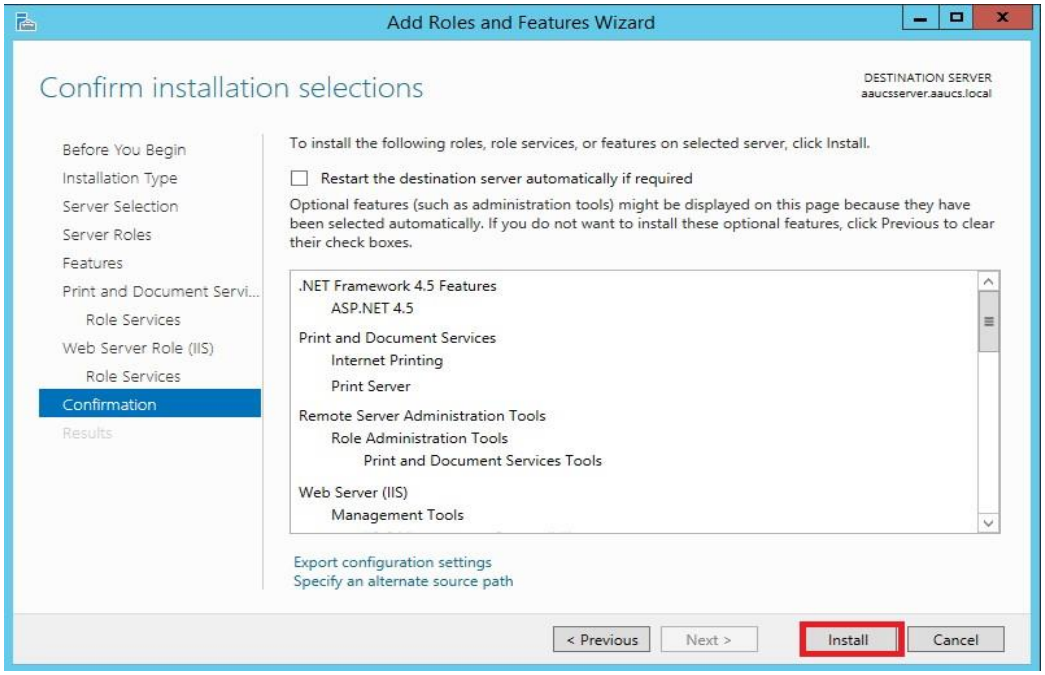

Print and Document Role Services:

- **Print Server:** is the core print management and services.
- **Distributed Scan:** Server is for Document Scanner if you have it.
- **Internet Printing:** will let you manage your printers through the browser.
- **LDP Services:** will share printers between Linux and UNIX base OS.

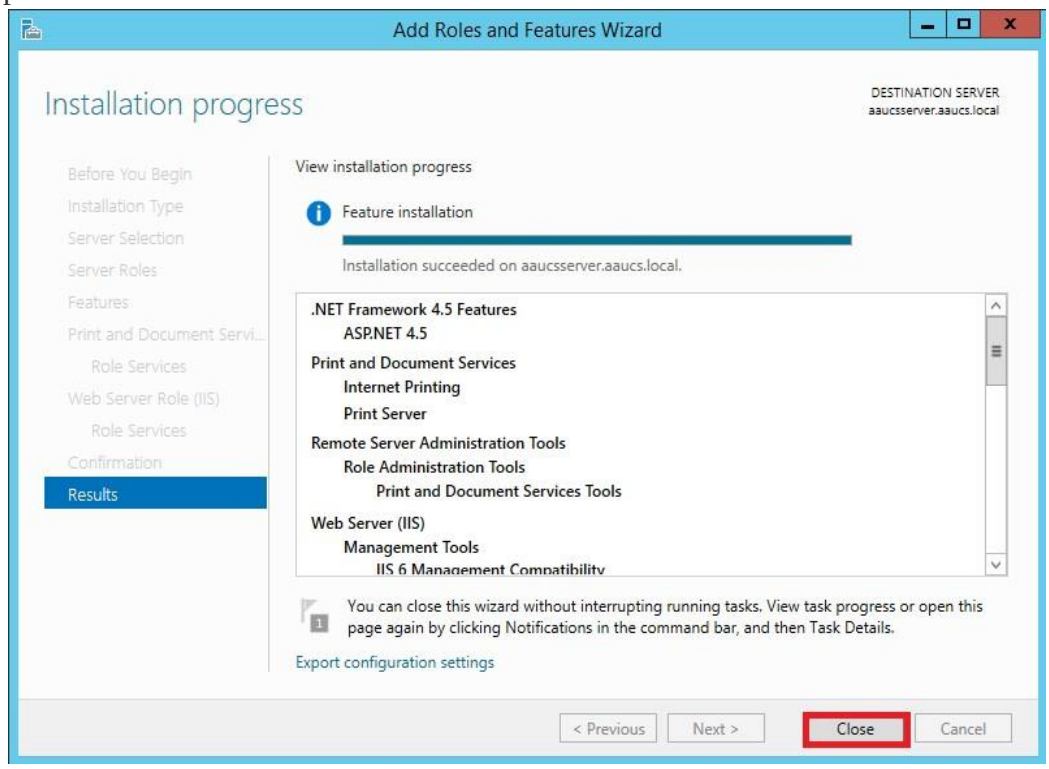
➢ Don't change anything Web Server, just click **Next** on Web Server Roles (IIS), Role Services and Confirmation page to finish the IIS Web Server options.



7. Click **Install** on the **Confirmation** page to finish the IIS Web Server options.

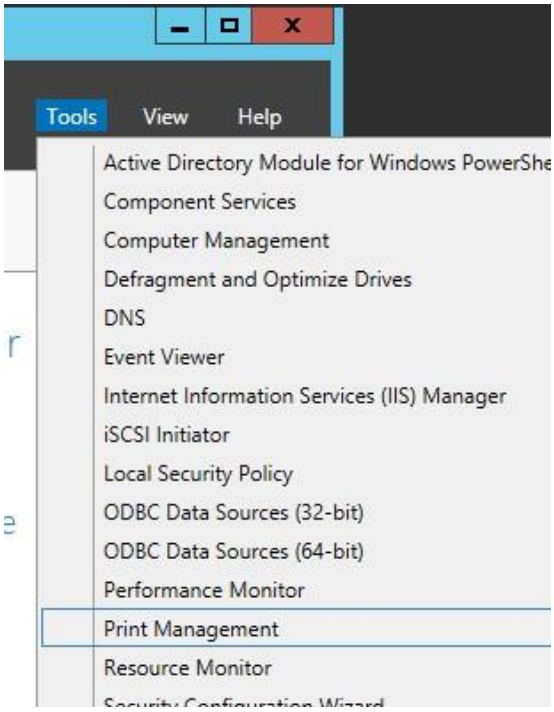



➢ Finally click **Close** due to the installation of Print and document services successful completion.

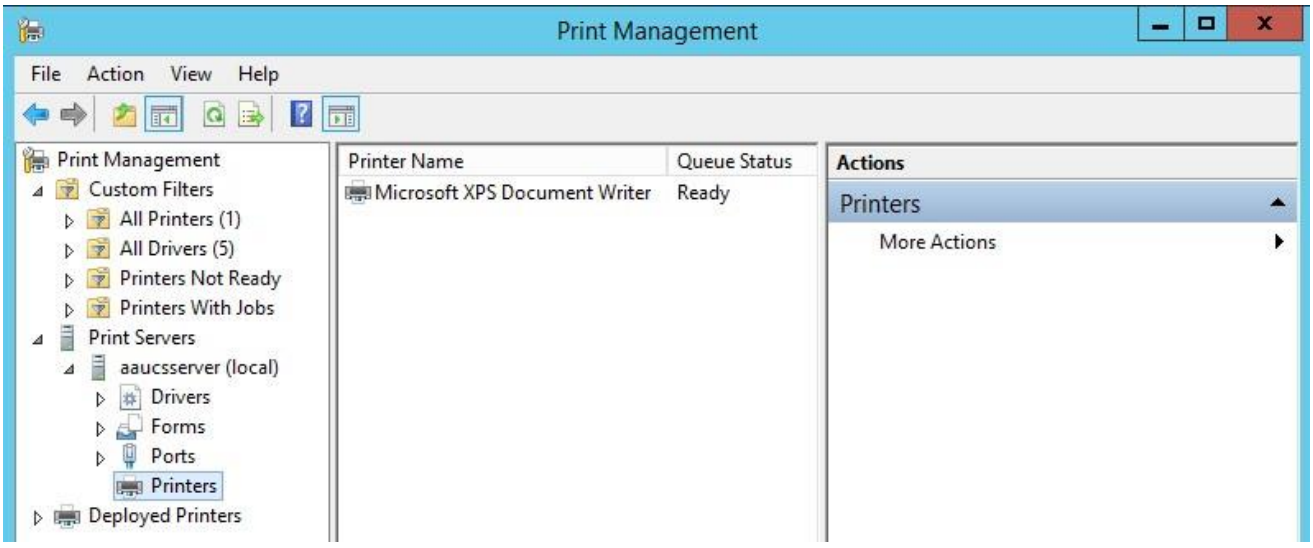


## 15.2 Installation of a Printer

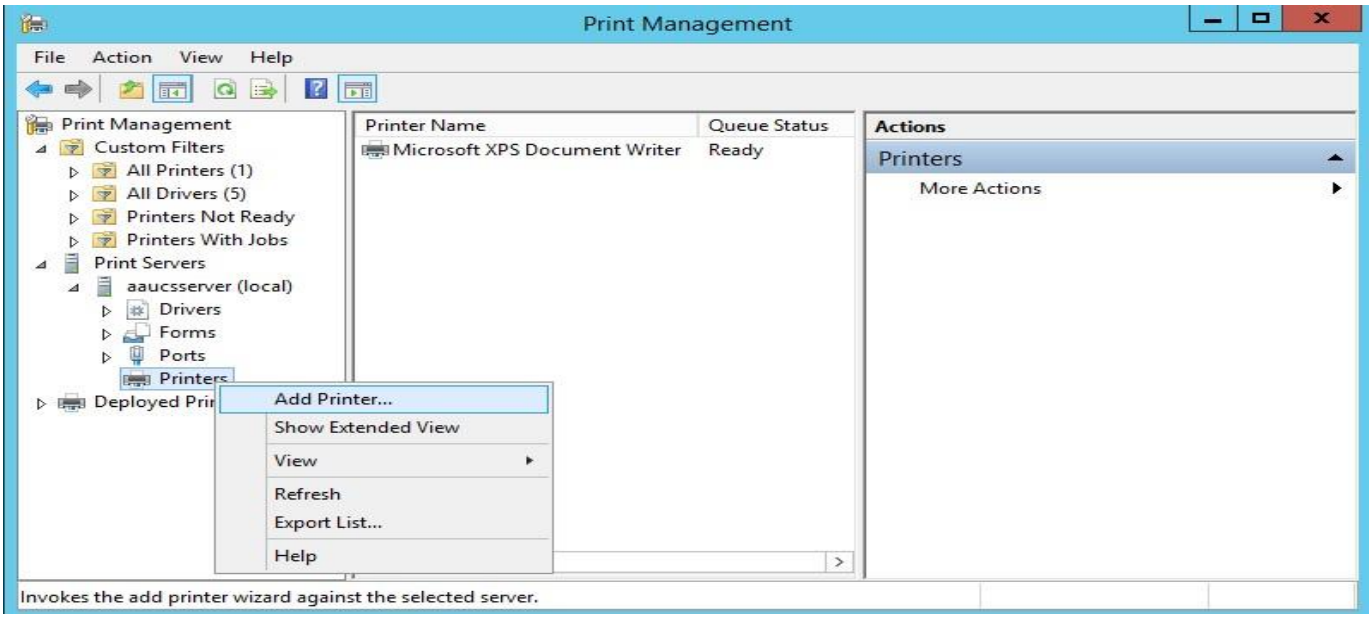
1. Open the **print management** console from **Tools** tab on **Server Manager**.



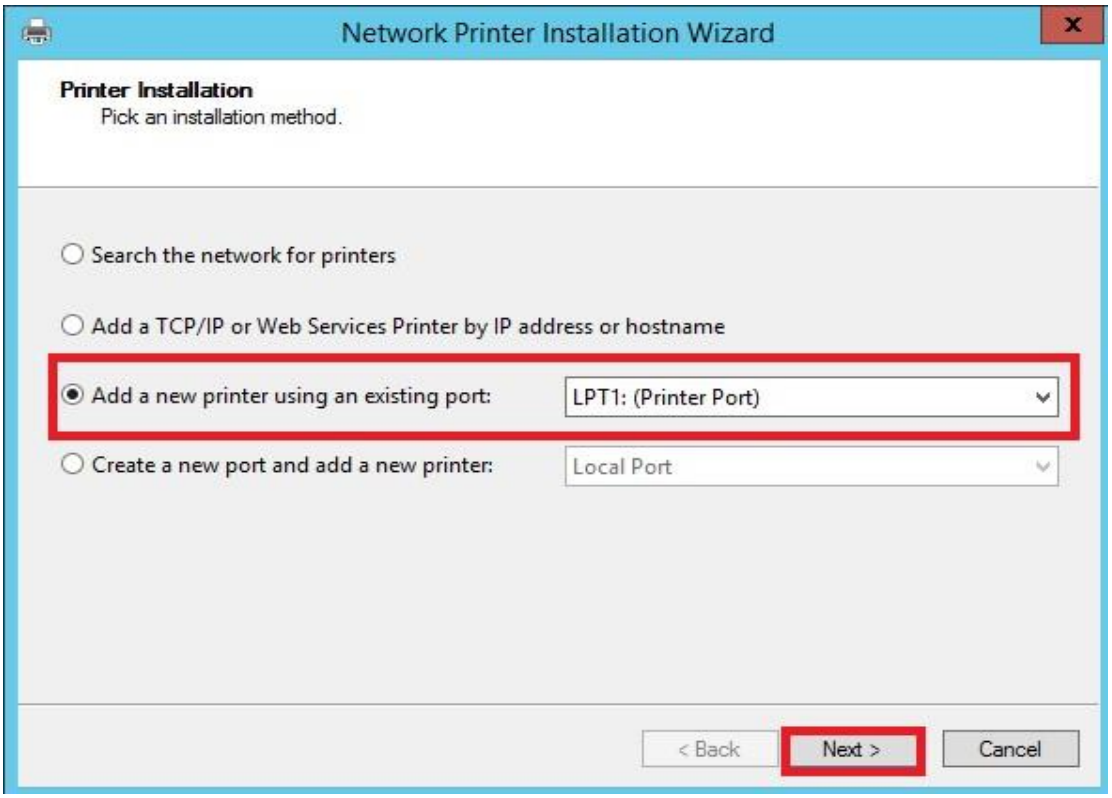

2. There is no installed printer on a print management without the default one.



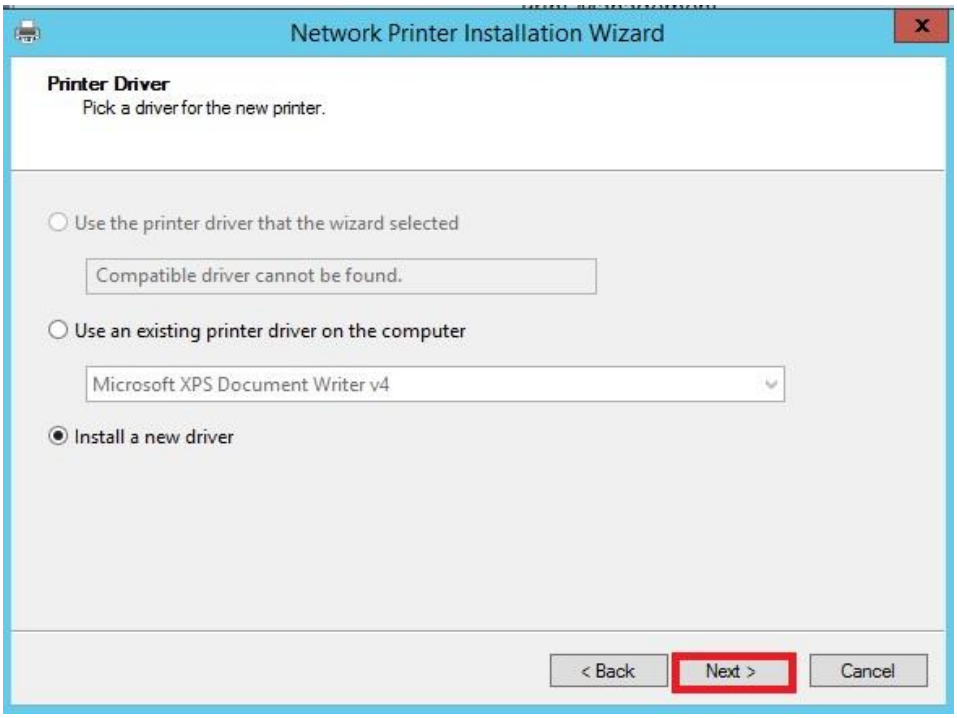
3. Let's add a printer; expand the Print Servers to Printers then right click Printers and click Add printer.



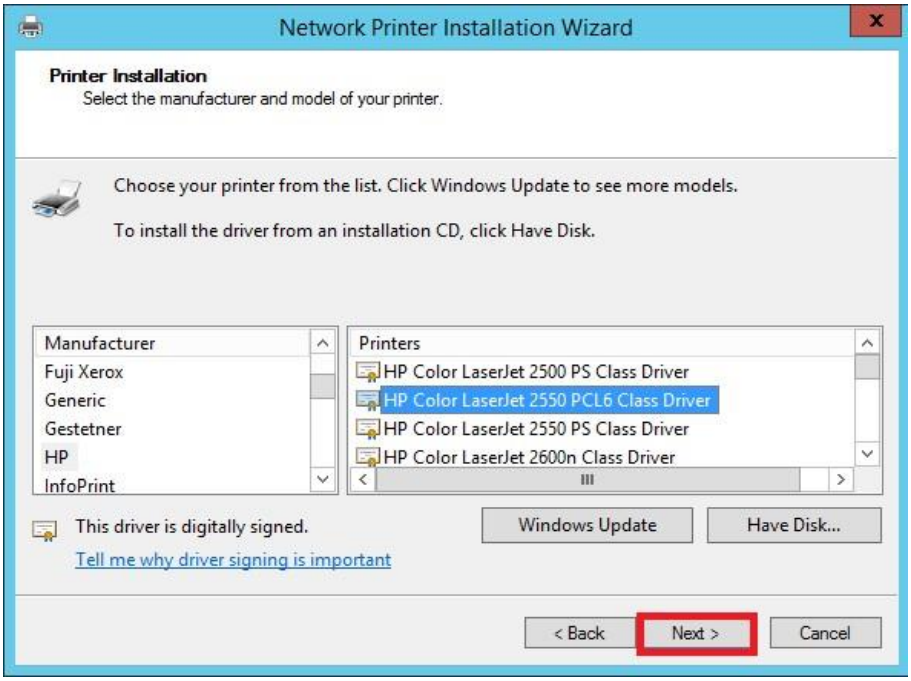

4. On Printer installation page select "Add a new printer using and existing port" and click Next.



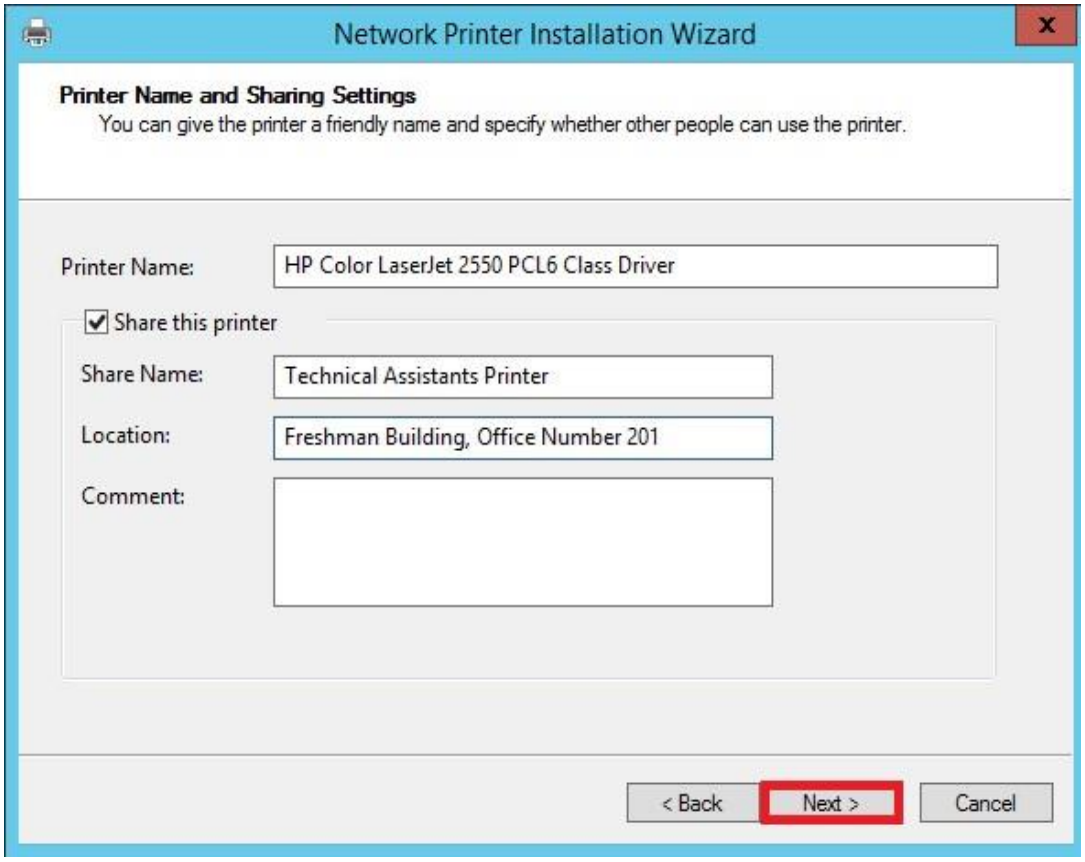

5. Select “Install a new driver” on Printer Driver page and click Next.

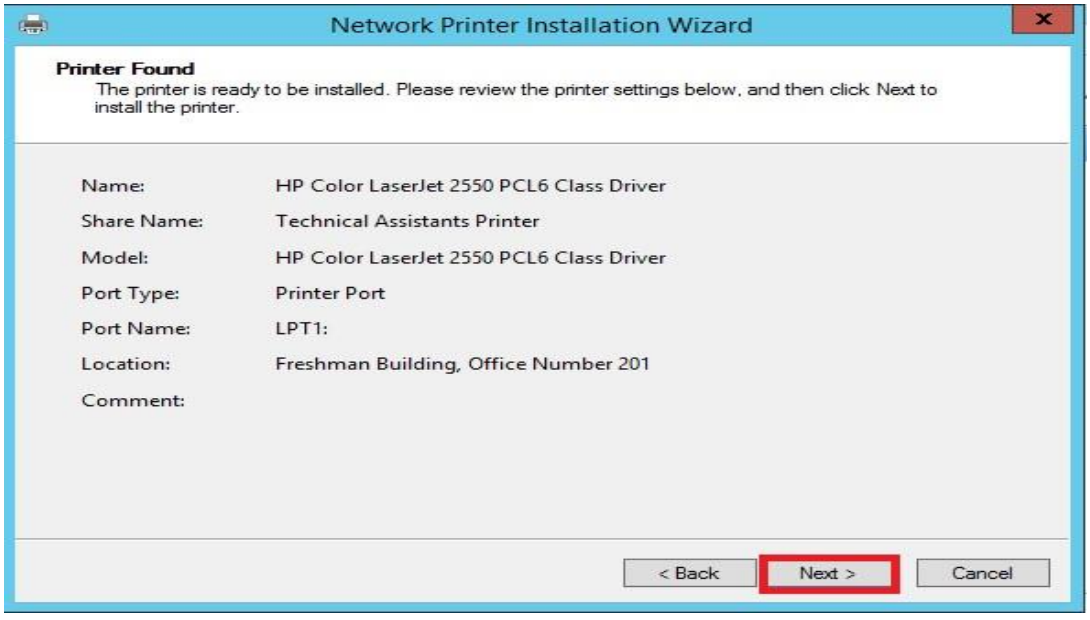



6. Select a proper printer then click **Next**. In this case, the selected printer is HP Color LaserJet 2550 PCL6.

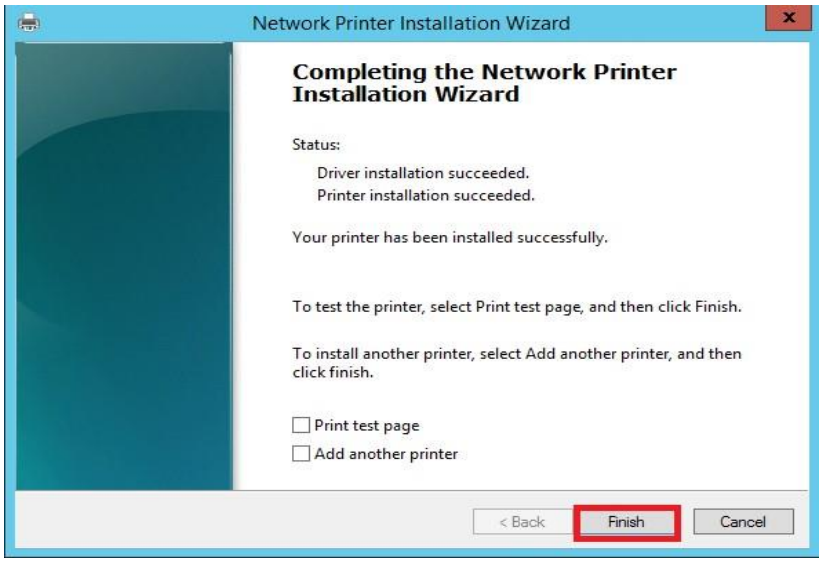



7. Fill the information and tick the check box of **Share this printer** and click **Next** twice.

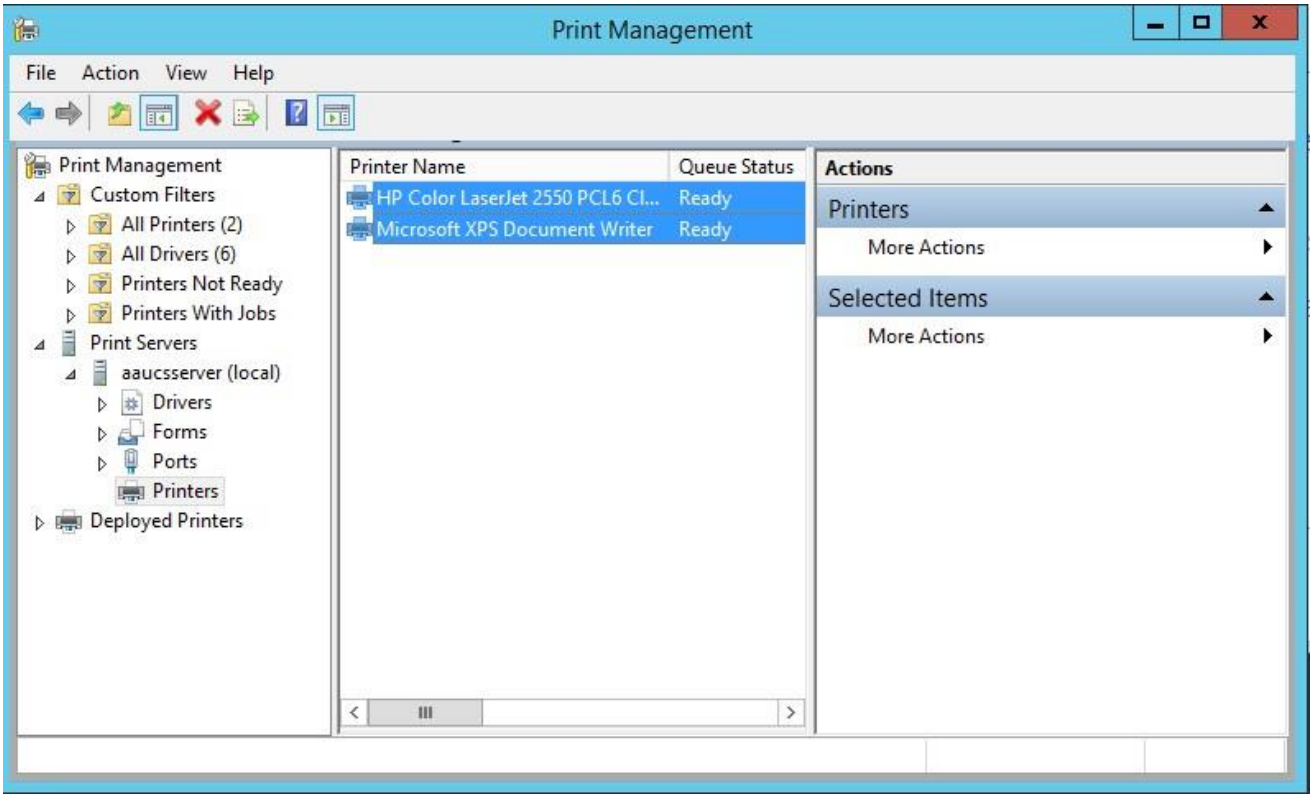



8. Finally, click **Finish** to accomplish the installation task.

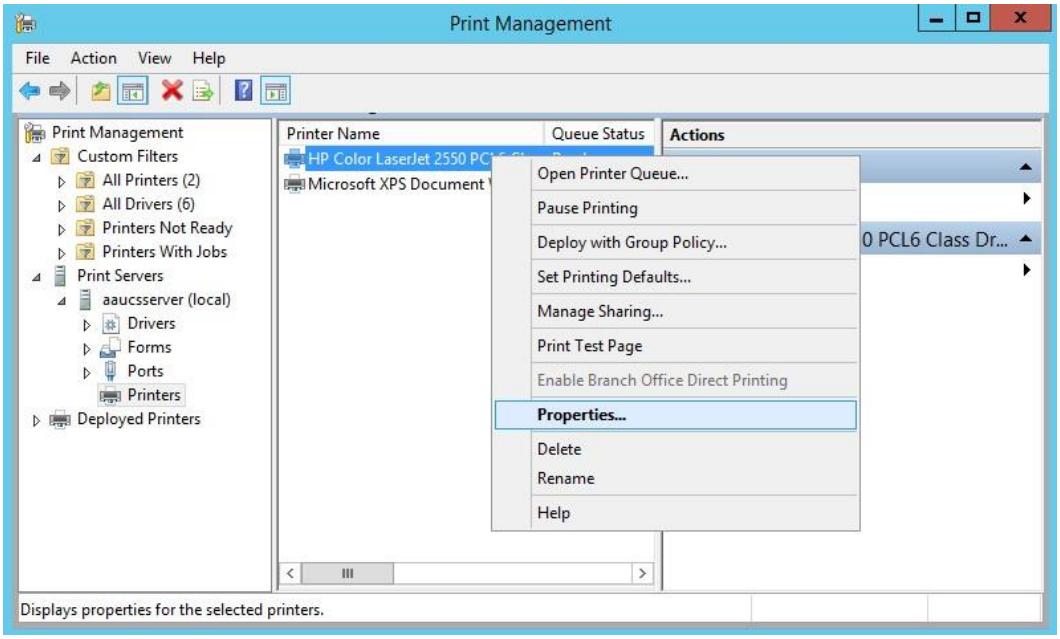


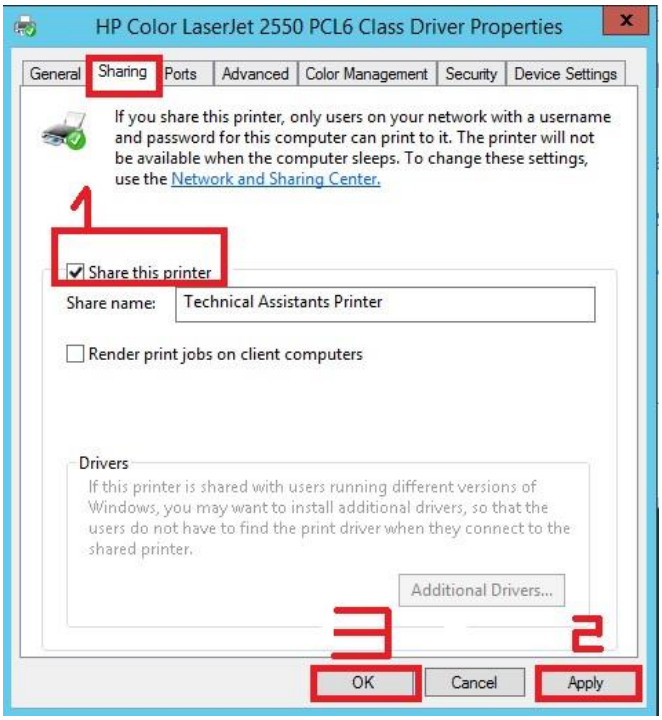

- Go to the **print management** console and see the new printer (HP Color LaserJet 2550 PCL6). We have installed another printer, and now we have two printers.



## 15.3 Sharing a printer to clients

When we are installing a printer, we select the sharing checkbox of first print to share the printer in the network. The sharing occurs, but it is not accessible to network directory for client PCs while you have not ticked the check box of "**share this printer**" of the installed printer going through **properties** -> **sharing** Tab.



# Chapter Sixteen: Backup

## 16.1 Introduction

A backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.

**Backup causes:**

- Software bugs routinely corrupt documents.
- Users accidentally delete data files.
- Hackers and disgruntled employees erase disks.
- Hardware problems and natural disasters take out entire machine rooms

If executed correctly, backups allow an administrator to restore a filesystem to the condition it was in at the time of the last backup.

Backups must be done carefully and on a strict schedule.

The backup system and backup media must also be tested regularly to verify that they are working correctly.

**Backups Recommendations**:

- Perform all backups from a central location
- Label your media
- Pick a reasonable backup interval
- Choose filesystems carefully
- Make daily dumps fit on one piece of media
- Keep media off-site
- Protect your backups
- Limit activity during backups – use snapshots
- Verify your media
- Develop a media life cycle
- Design your data for backups
- Prepare for the worst

## 16.1.2 Types of Backups

### 16.1.2.1 Full Backup

A full backup is exactly what the name implies. It is a full copy of your entire data set. Although full backups arguably provide the best protection, most organizations only use them on a periodic basis because they are time consuming, and often require a large number of tapes or disk.

### 16.1.2.2 Incremental Backup

Because full backups are so time consuming, incremental backups were introduced as a way of decreasing the amount of time that it takes to do a backup. Incremental backups only backup the data that has changed since the previous backup. For example, suppose that you created a full backup on Monday, and used incremental backups for the rest of the week. Tuesday's backup would only contain the data that has changed since Monday. Wednesday's backup would only contain the data that has changed since Tuesday.

The primary disadvantage to incremental backups is that they can be time-consuming to restore. Going back to the above example, suppose that you wanted to restore the backup from Wednesday. To do so, you would have to first restore Monday's full backup. After that, you would have to restore
Tuesday's backup disk, followed by Wednesday's. If any of the disks happen to be missing or damaged, then you will not be able to perform the full restoration.

### 16.1.2.3 Differential Backup

A differential backup is similar to an incremental backup in that it starts with a full backup, and subsequent backups only contain data that has changed. The difference is that while an incremental backup only includes the data that has changed since the previous backup, a differential backup contains all of the data that has changed since the last full backup.

Suppose for example that you wanted to create a full backup on Monday and differential backups for the rest of the week. Tuesday's backup would contain all of the data that has changed since Monday. It would therefore be identical to an incremental backup at this point. On Wednesday, however, the differential backup would backup any data that had changed since Monday.

The advantage that differential backups have over incremental is shorter restore times. Restoring a differential backup never requires more than two disk sets. Incremental backups on the other hand, may require a great number of disk sets. Of course the tradeoff is that as time progresses, a differential backup disk can grow to contain much more data than an incremental backup tape.

### 16.1.2.4 Synthetic Full Backup

A synthetic full backup is a variation of an incremental backup. Like any other incremental backup, the actual backup process involves taking a full backup, followed by a series of incremental backups. But synthetic backups take things one step further.

What makes a synthetic backup different from an incremental backup is that the backup server actually produces full backups. It does this by combining the existing full backup with the data from the incremental backups. The end result is a full backup that is indistinguishable from a full backup that has been created in the traditional way.

As you can imagine, the primary advantage to synthetic full backups is greatly reduced restore times. Restoring a synthetic full backup doesn't require the backup operator to restore multiple tape sets as an incremental backup does. Synthetic full backups provide all of the advantages of a true full backup, but offer the decreased backup times and decrease bandwidth usage of an incremental backup.

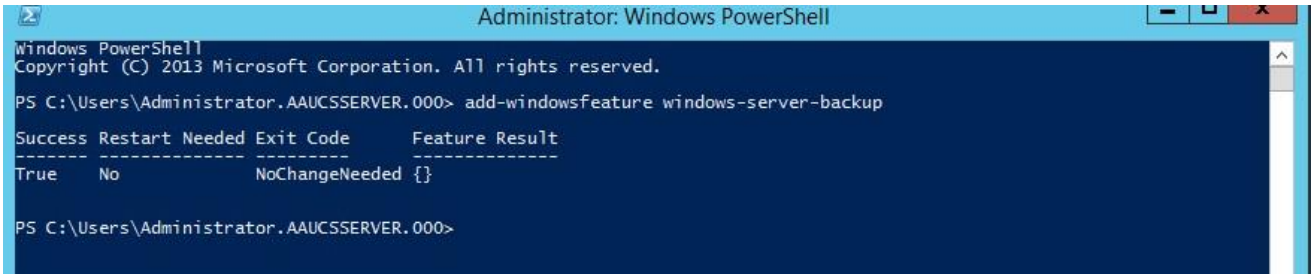
### 16.1.2.5 Incremental-Forever Backup

Incremental-forever backups are often used by disk-to-disk-to-tape backup systems. The basic idea is that like an incremental backup, and incremental-forever backup begins by taking a full backup of the data set. After that point, only incremental backups are taken.

What makes an incremental-forever backup different from a normal incremental backup is the availability of data. As you will recall, restoring an incremental backup requires the tape containing the full backup, and every subsequent backup up to the backup that you want to restore. While this is also true for an incremental-forever backup, the backup server typically stores all of the backup sets on either a large disk array or in a tape library. It automates the restoration process so that you don't have to figure out which tape sets need to be restored. In essence, the process of restoring the incremental data becomes completely transparent and mimics the process of restoring a full backup.

## 16.2 Installation of Windows server 2012 Backup components

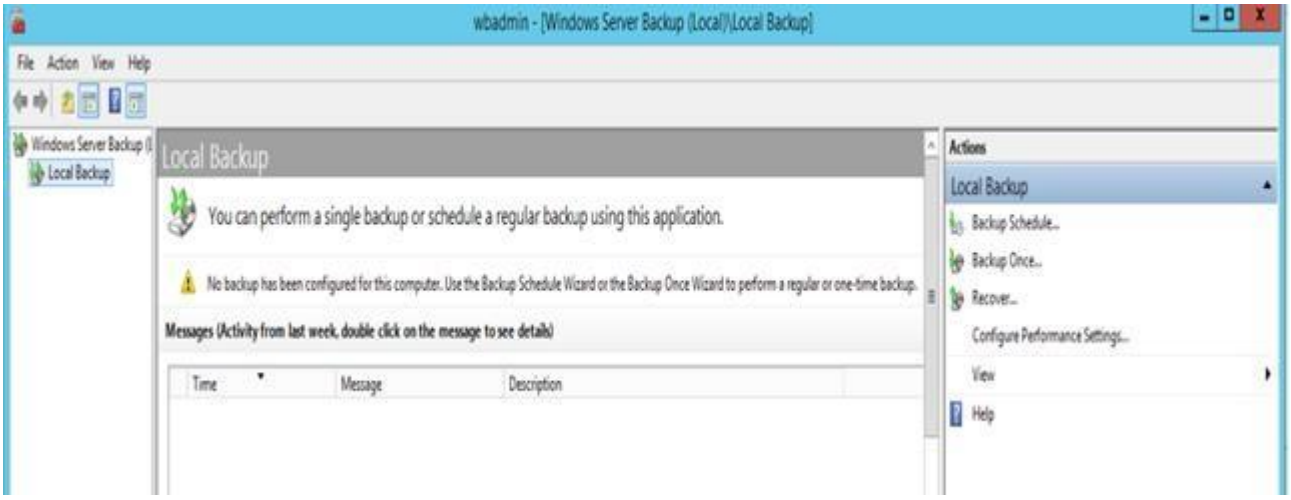
- ✓ Log on to the domain controller (DC) with a domain admin account and open a PowerShell prompt using the blue icon on the desktop taskbar or from the Start screen.
- ✓ In the **PowerShell** console, type **add-windowsfeature windows-server-backup** and press **Enter**.



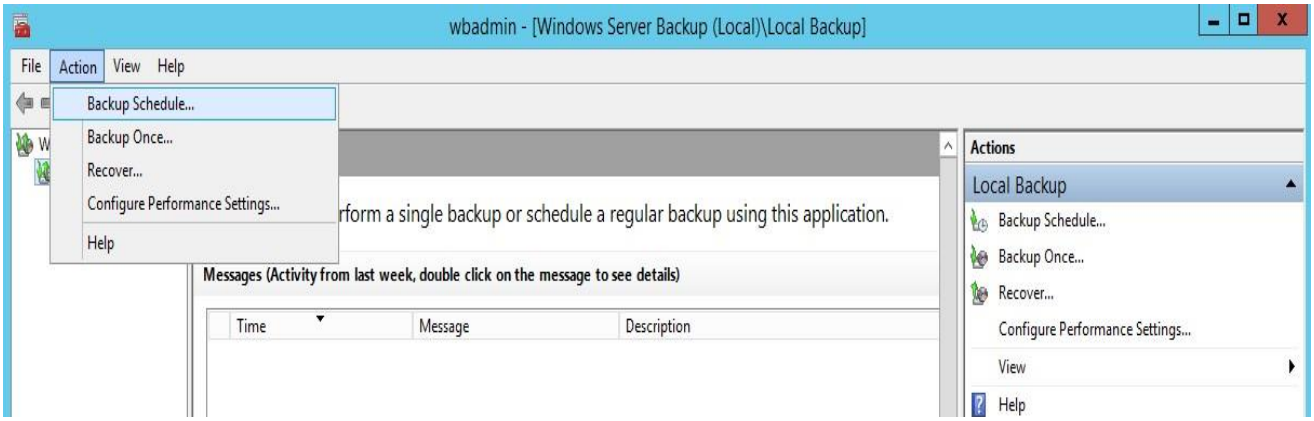

- Or you can follow the GUI procedure to install the Windows Server Backup feature from the Server manager window Add roles and Features option.

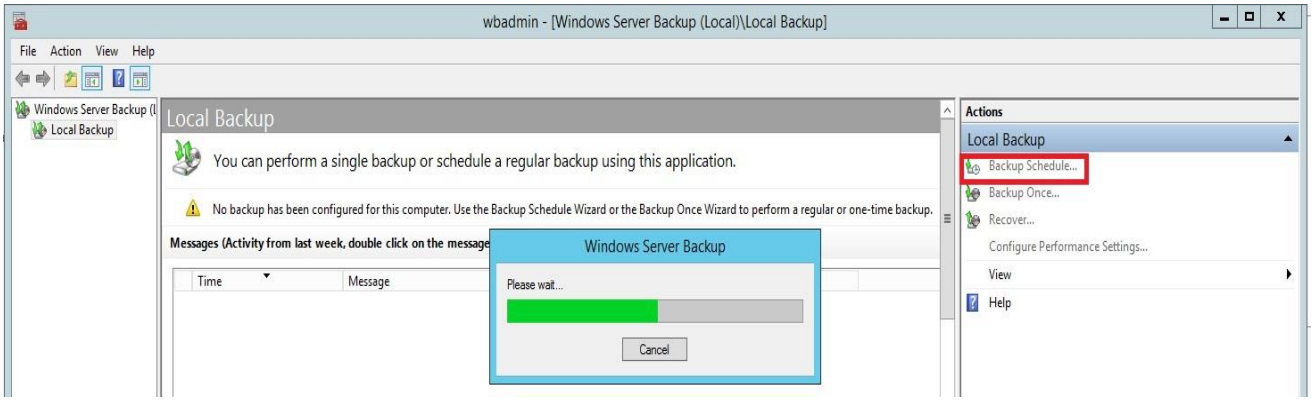
1. Open Server Manager from the desktop taskbar (or from the Start screen if it's not already open) and select **Windows Server Backup** from the Tools menu.

2. In the **webadmin** console, click **Local Backup** in the left pane.

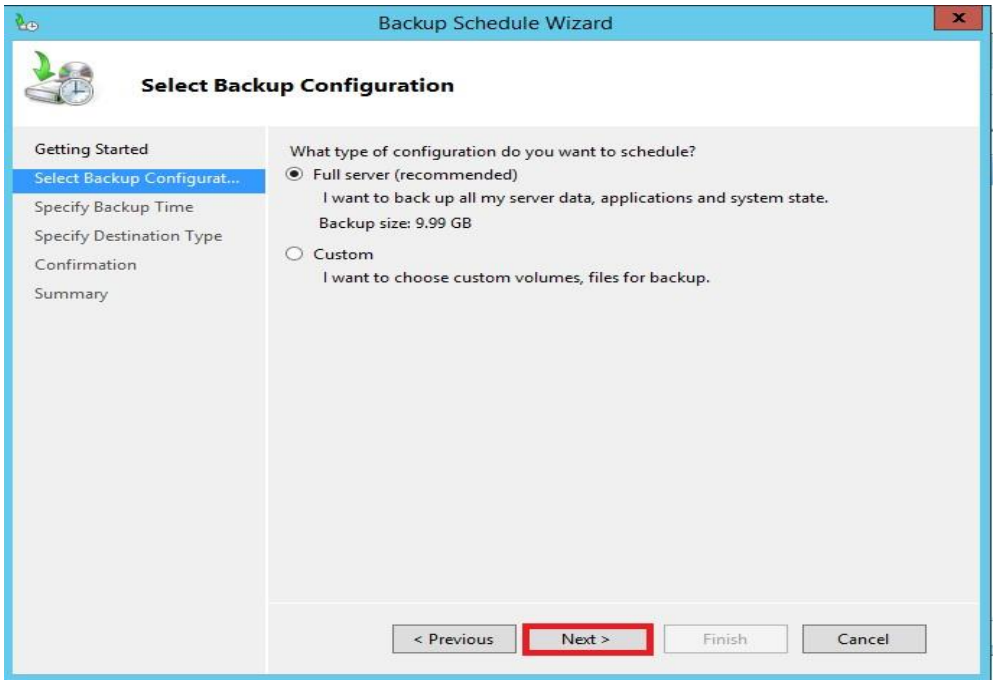



3. Now select **Backup Schedule** under *Actions* in the far right pane.

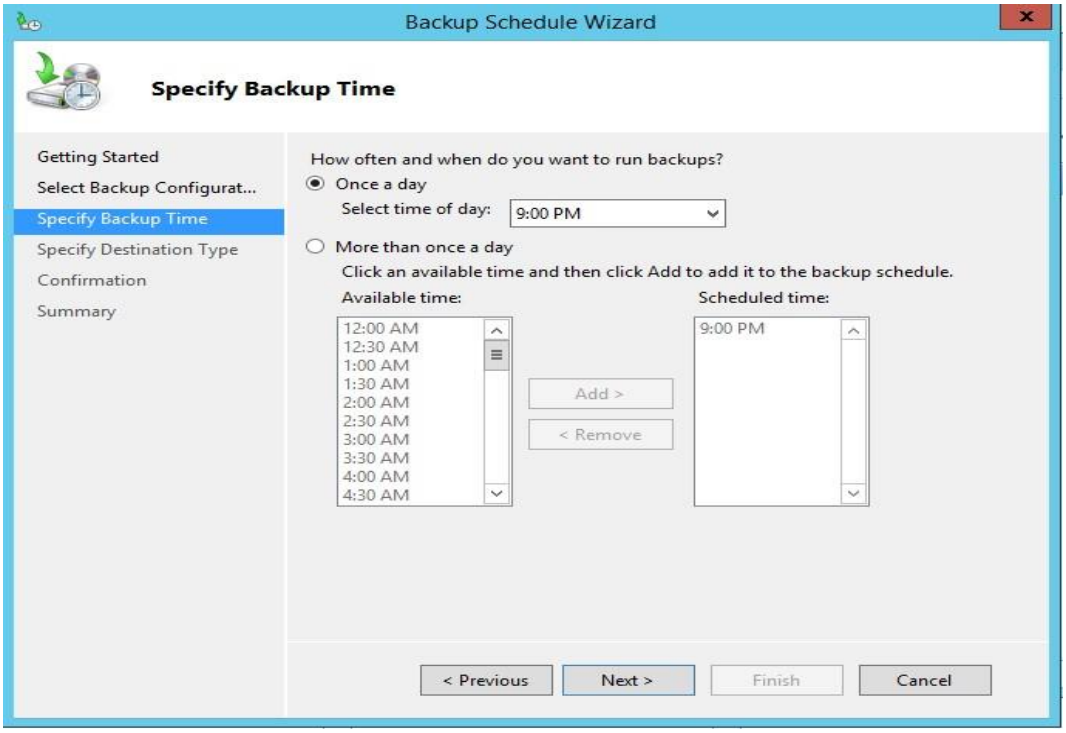


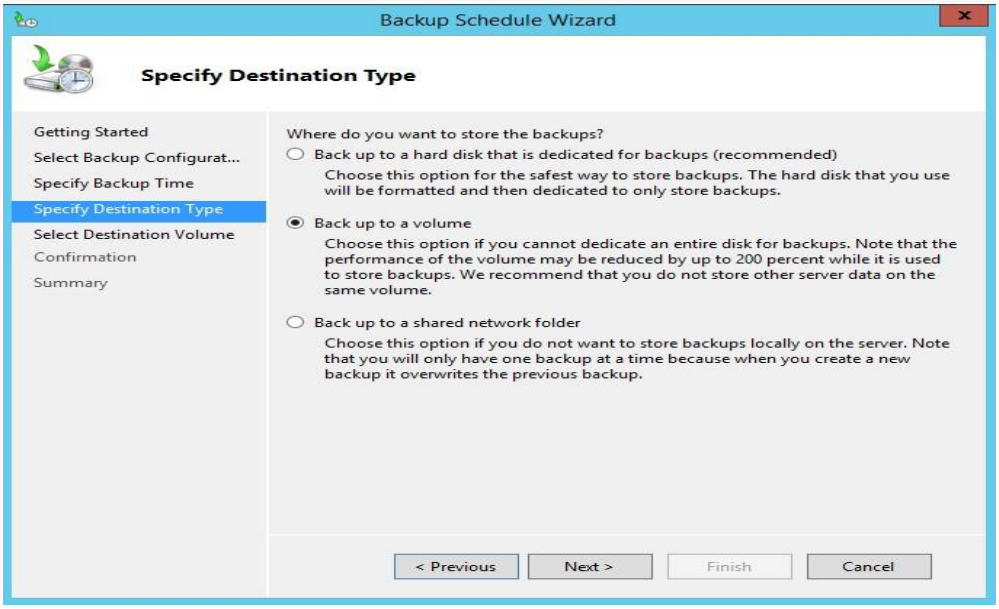
4. On the Select Backup Configuration screen, select **Full server (recommended)** and click **Next**.



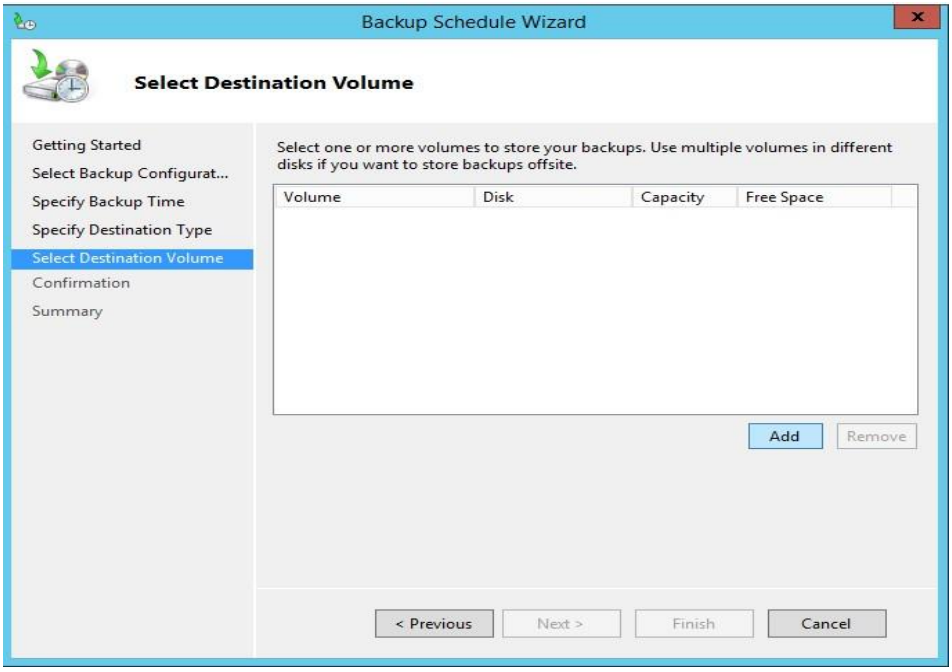

5. On the specify Backup time select the time when do you want to run a backup in this example once in a day at 9:00 is selected because usually most of the backup in the organizations was done in the night due to the server goes very slow when making the backup.



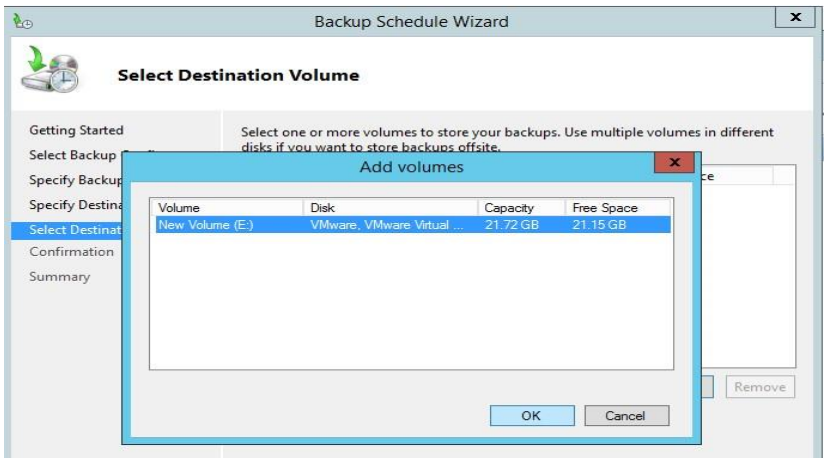
6. On the Specify Backup Destination Type screen, select your dedicated backup destination type in this case Backup to a volume is selected.

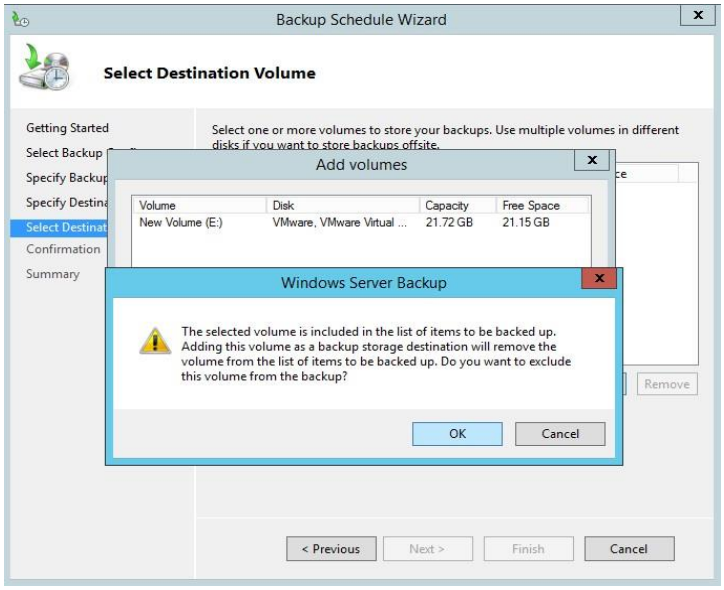


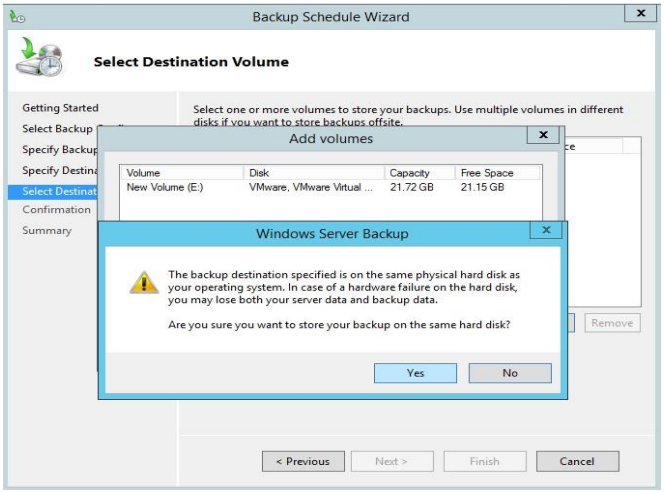

7. On the Select Destination volume screen click **Add** button and add your dedicated backup volume in the Backup destination menu.



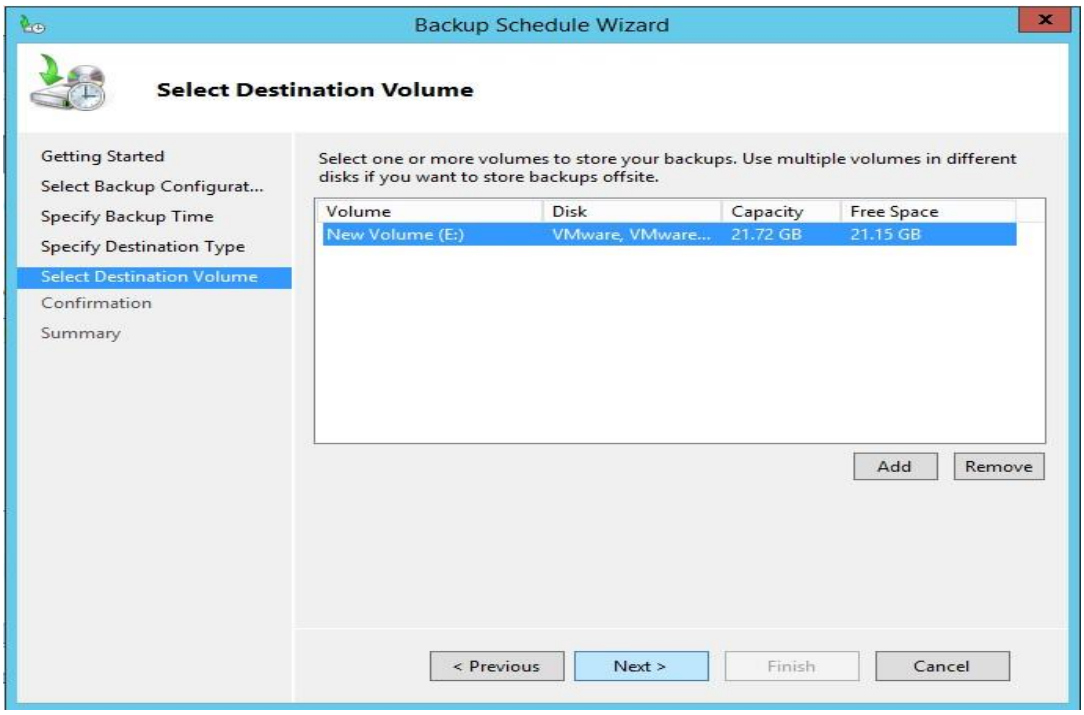

8. Select your backup destination volume and click **OK**.



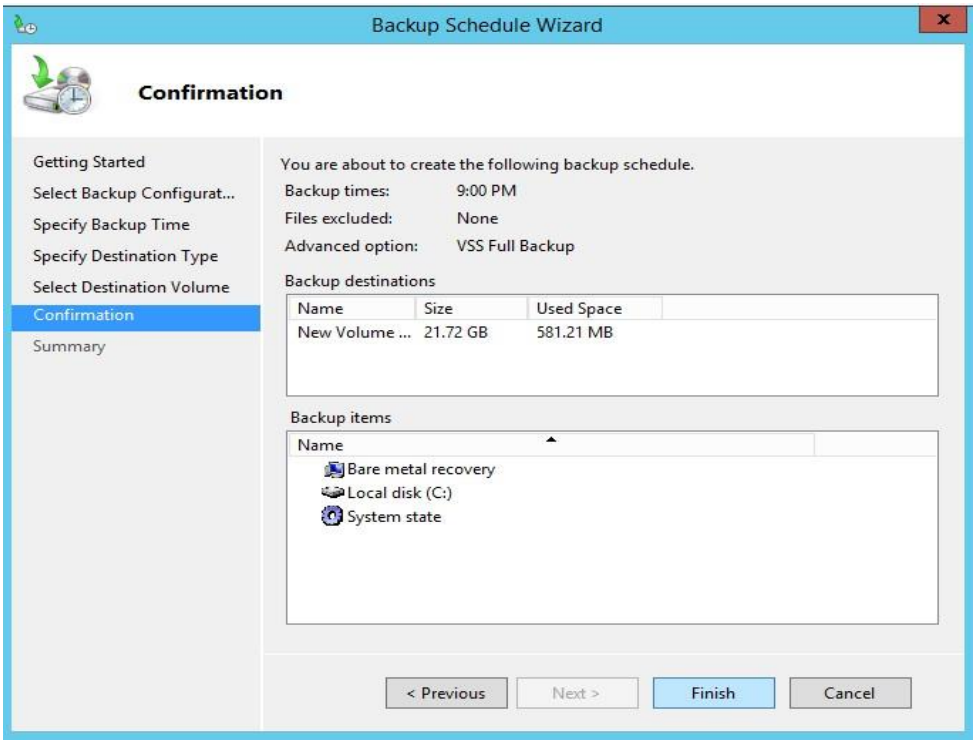



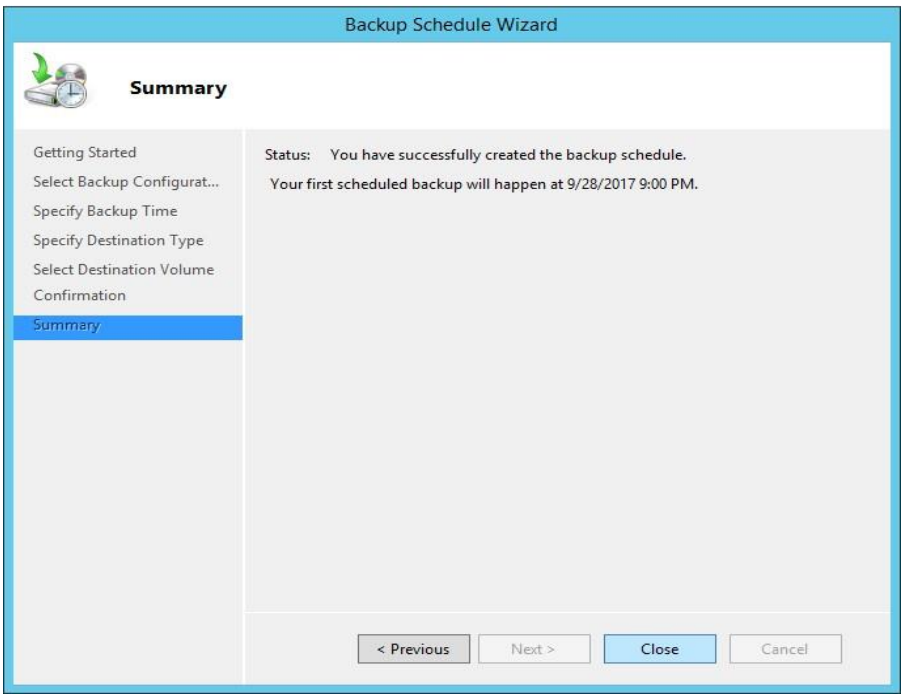

9. Just Click **Next**.



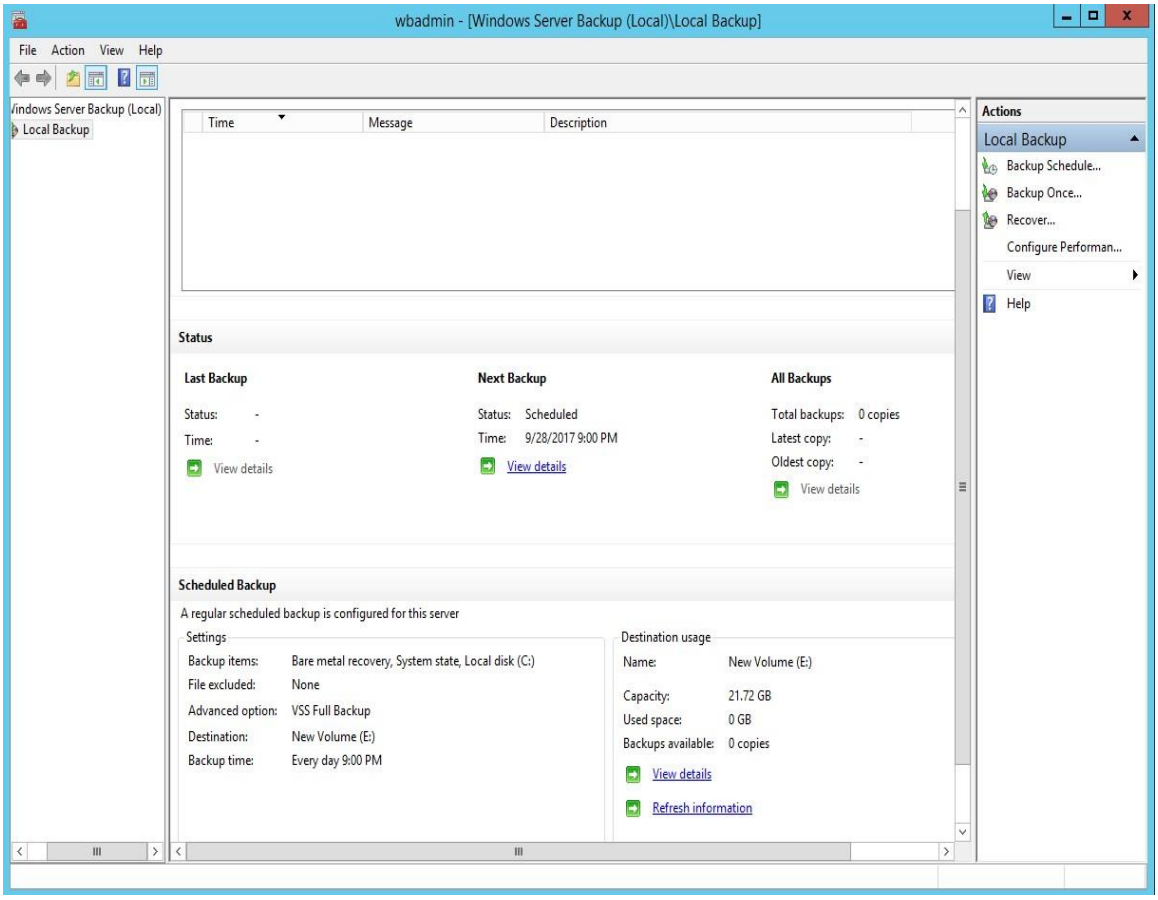

10. Click **Finish** on the confirmation screen.




11. After successfully created the backup schedule close the backup schedule wizard.




12. Finally, the **webadmin** window looks like as shown as below.



## 16.3 How to Restore a Windows Server 2012 Domain Controller from a Backup

To restore a Domain Controller running Windows Server 2012 from a backup, perform the following steps:

- Boot the server with the OS media in the DVD drive or bootable USB flash or a hard disk and press any key when prompted.
- Choose the appropriate language options, time and currency format, and keyboard layout, and click **Next**.


- Click **Repair your computer**

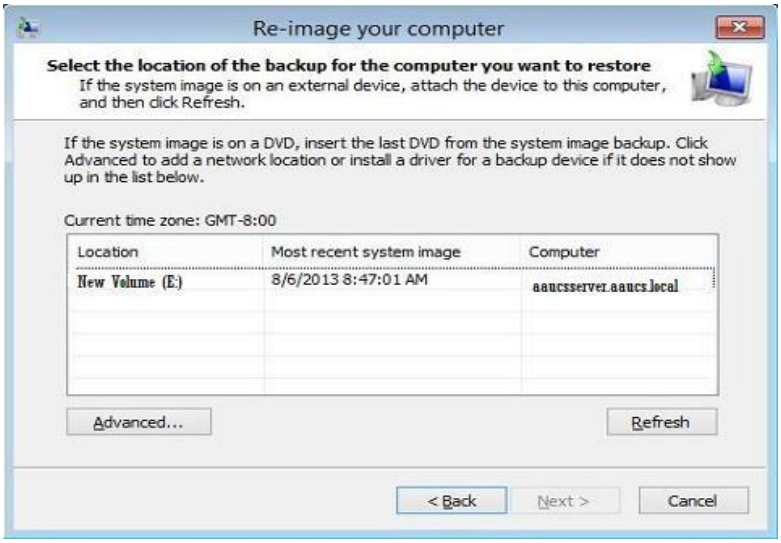

- Click **Troubleshoot**.


- Click **System Image Recovery**.


Select the operating system you wish to recover.

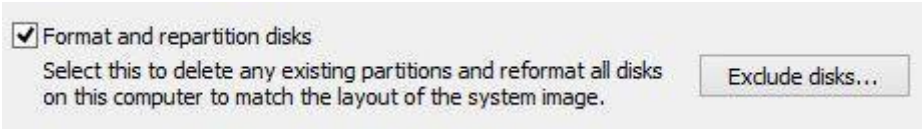

- Locate the backup image you wish to restore and click **Next.**


The most recent image is selected by default, but you may choose an older one if you wish.

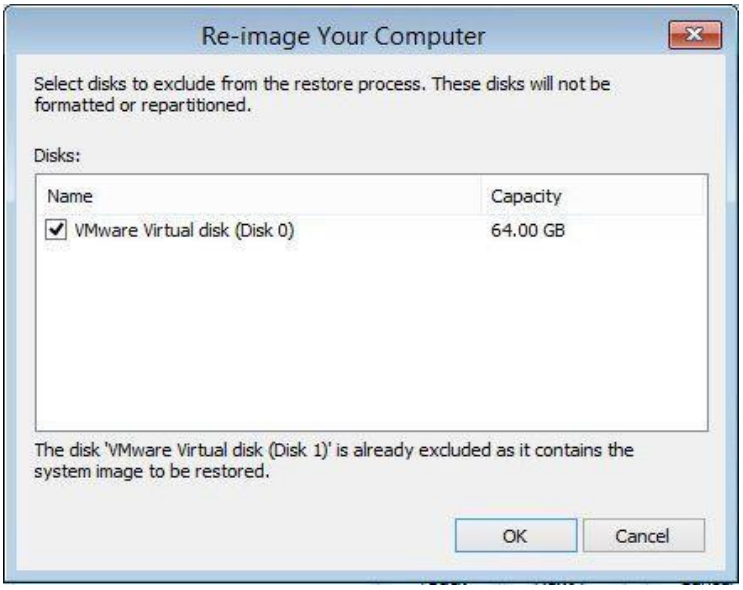



- If necessary, click the **Advanced** button to install a driver or search for an image on the network.

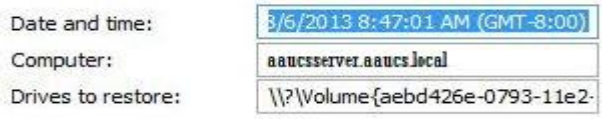

If you wish to recreate the disk partition scheme and reformat disks that Windows can access, select the **Format and repartition disks** checkbox.



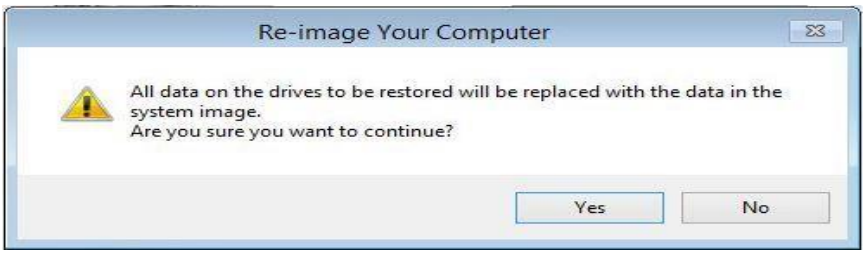

- If you wish to prevent certain disks from being reformatted, click **Exclude Disks** and select the disks that you don't wish to reformat. Click **OK**.




- Click **Next**, review the summary, and then click **Finish**.



. Confirm that you wish to start the restore by clicking **Yes**.



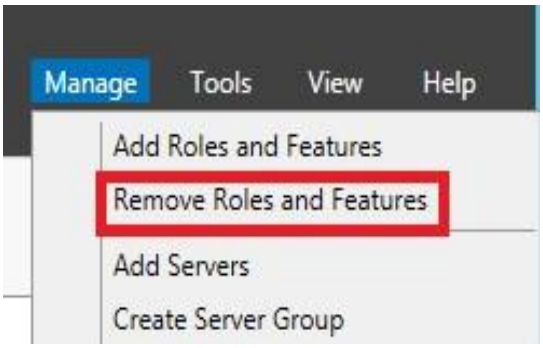

- The restore will begin.


- After the server boots, it is a good idea to review its event logs to verify that everything is functioning properly. Note that some errors can be ignored if they only occur during or shortly after the boot process.

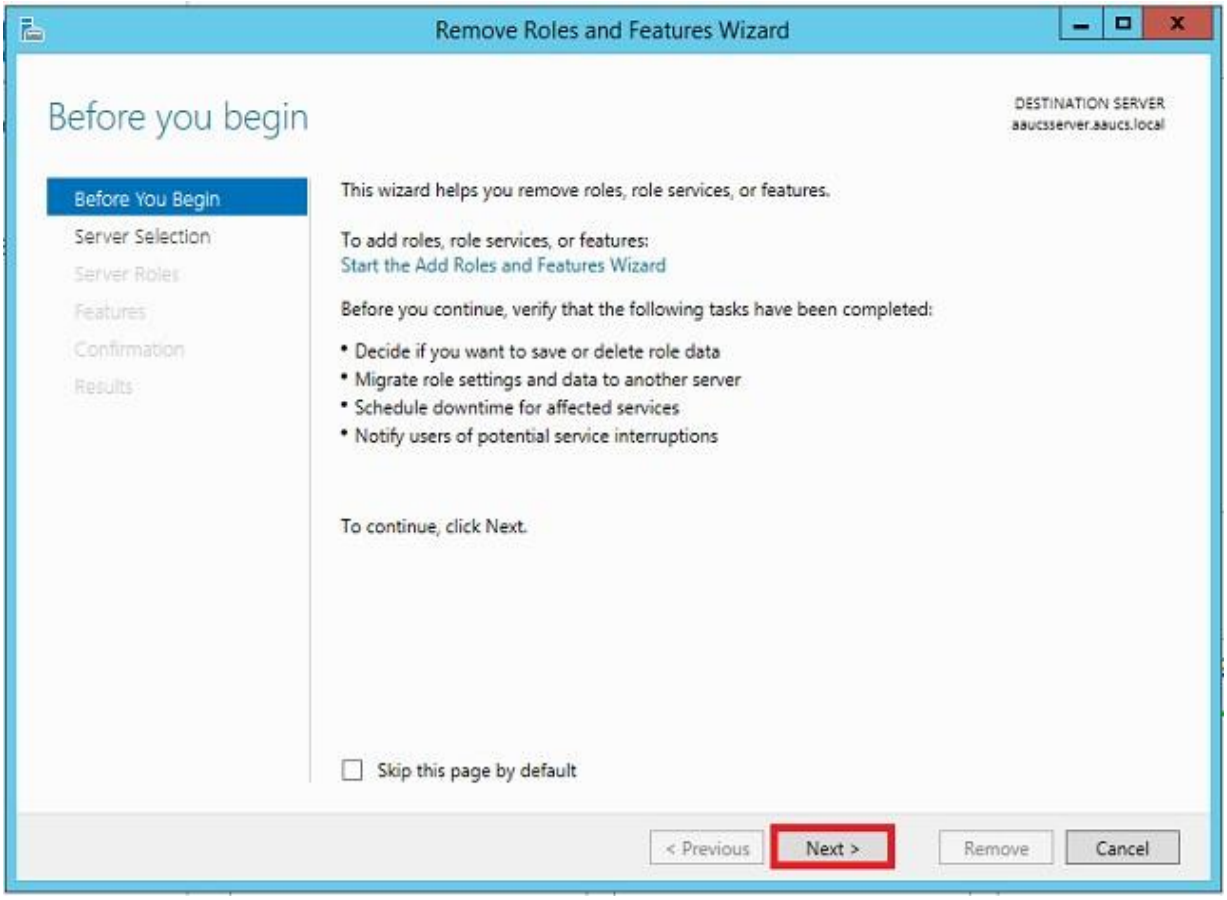
# Part V: Removing Roles and Features in Windows Server 2012

# Chapter Seventeen: Removal process of Roles

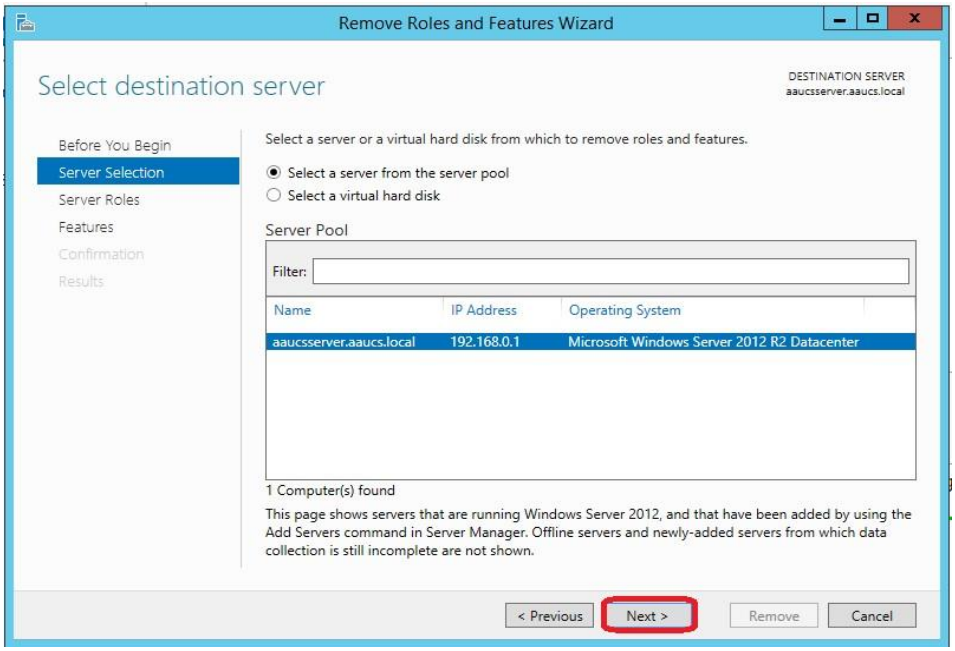
If for any reasons you will need to remove or uninstall server Roles and Features, it is a simple process, From the **Server Manager's Dashboard** click on **Manage** then select **Remove Roles and Features**.



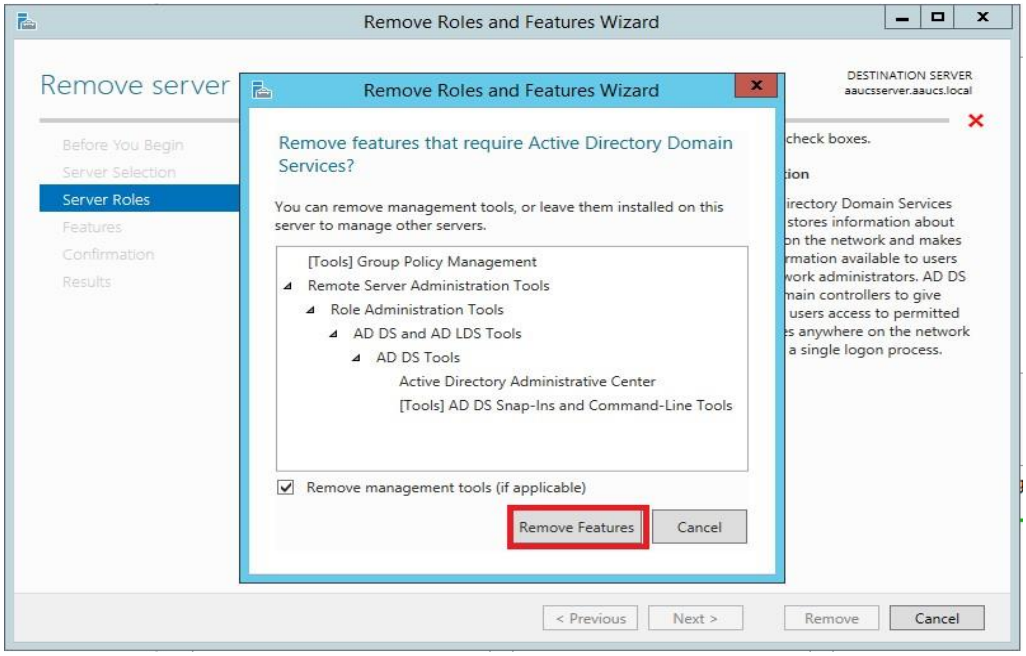

- In the **Before you begin** page in Remove Roles and Features Wizard page click on **Next** to Continue




In the **Select destination server** page select a server from the server pool, click on **Next** to continue.

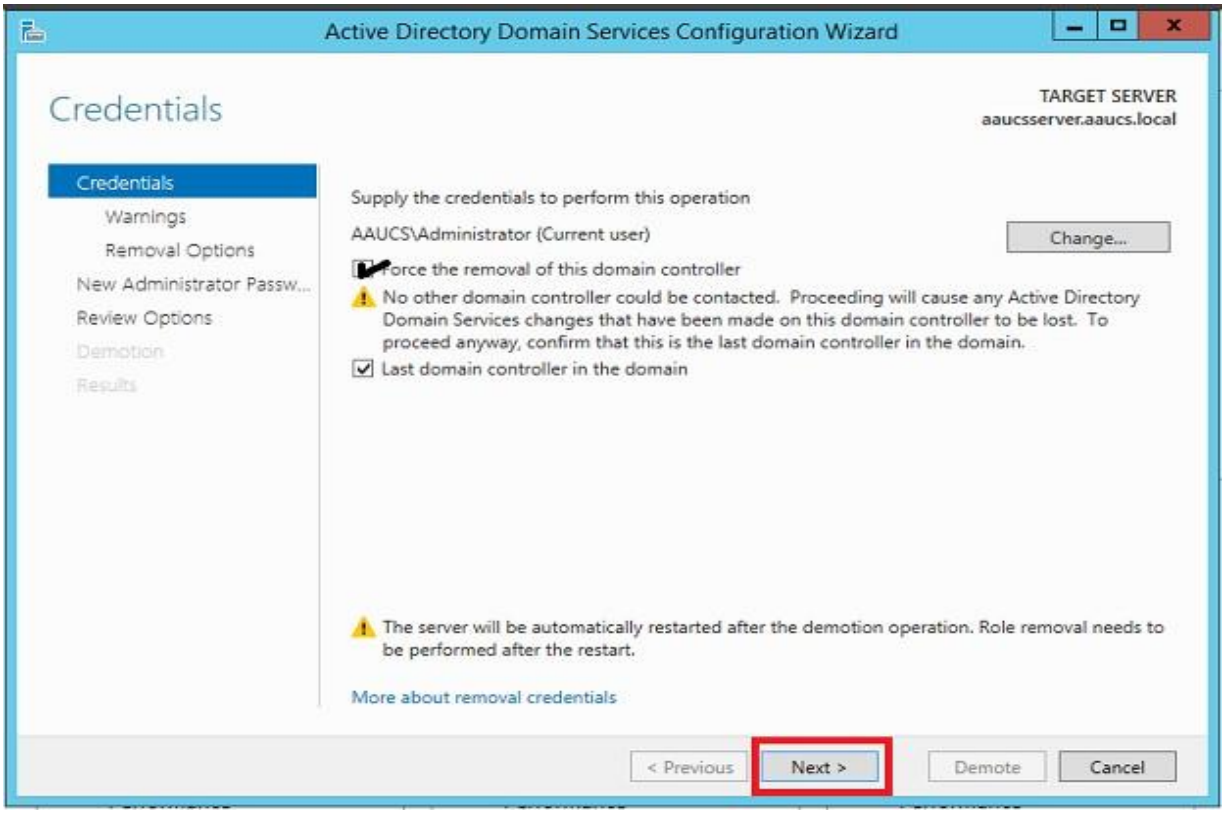



Let's remove the Active Directory Domain Services (AD DS) role including Domain Name Systems (DNS), so that in the **Remove server roles** page click on **Active Directory Domain Services** to uncheck and click on **Remove Features button,** In the **Confirm removal selections** page click on **Remove**.

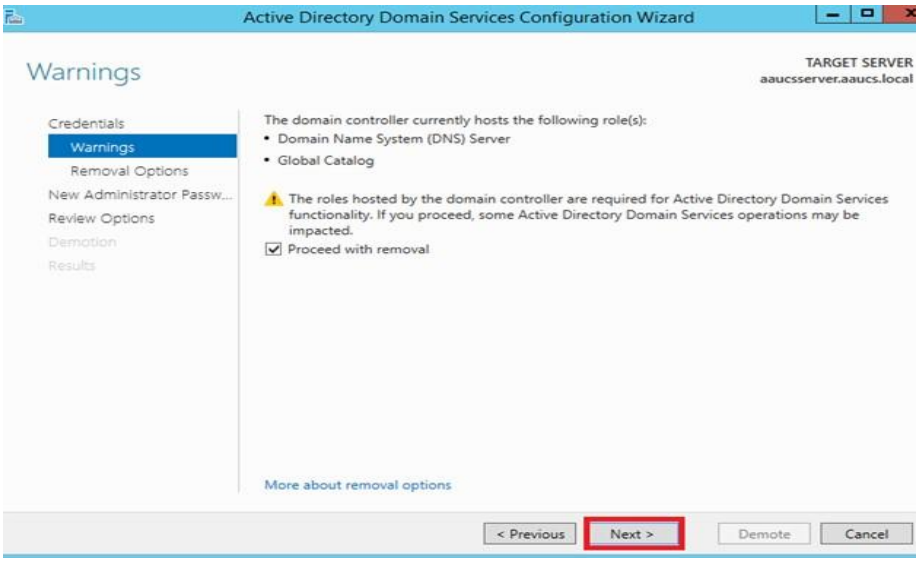


Before the AD DS role can be removed the Domain controller needs to be **demoted,** so, to do that you have to click "**demote this domain controller**" on the "**validated results**" window as shown as in the next figure.

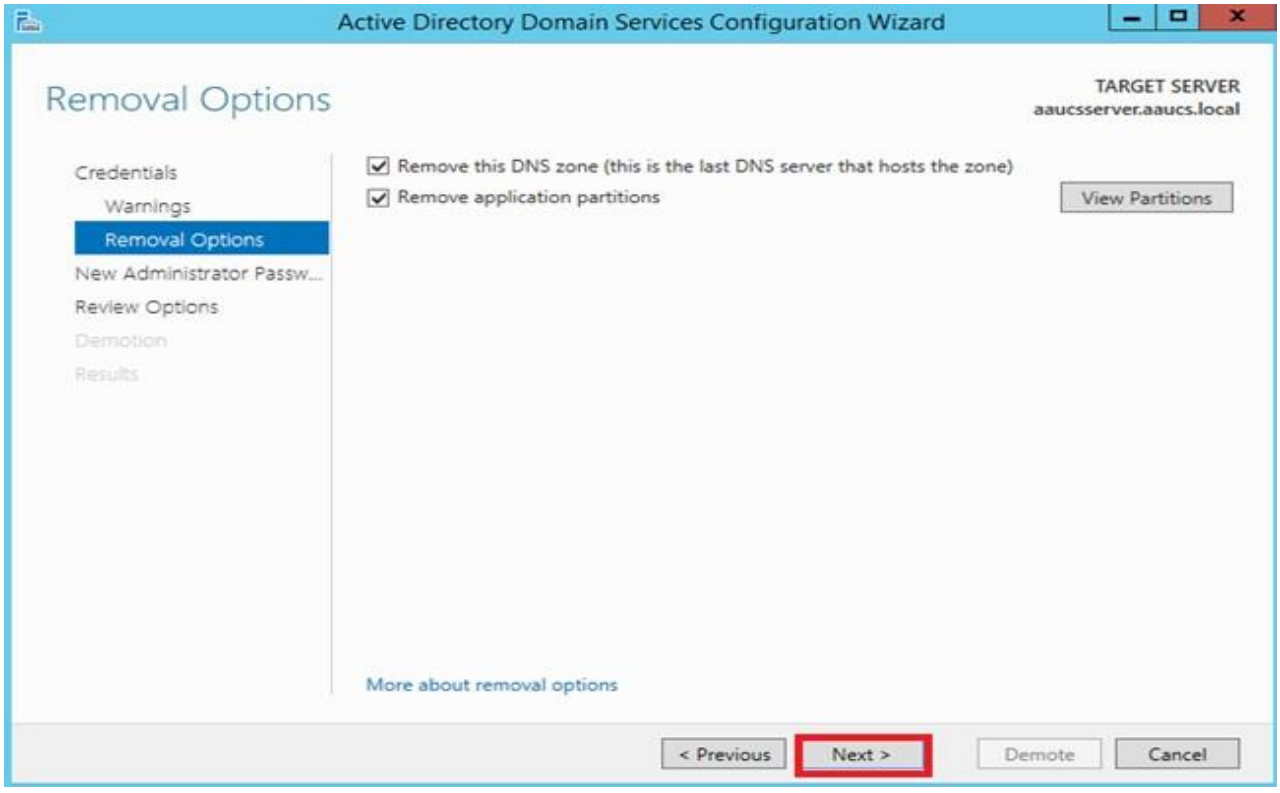

Next select both check boxes and click **Next.**



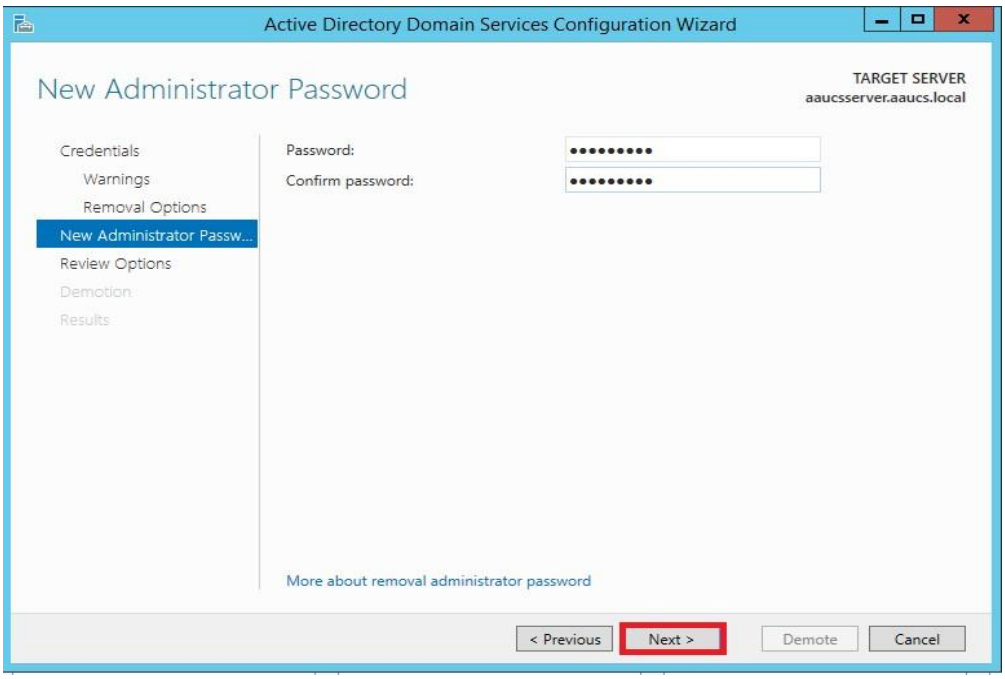

Make sure that you checked "**Proceed with removal**" check box and click **Next.**



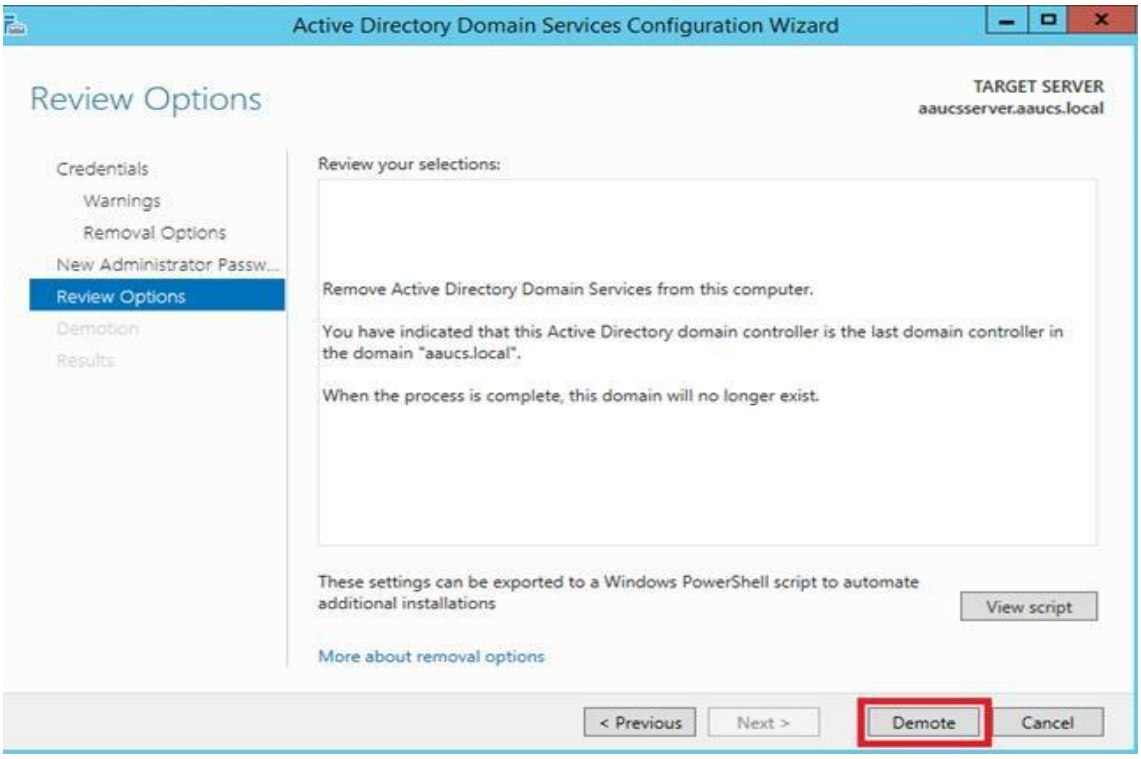

Make sure that you checked both check boxes and click **Next** to proceed**.**



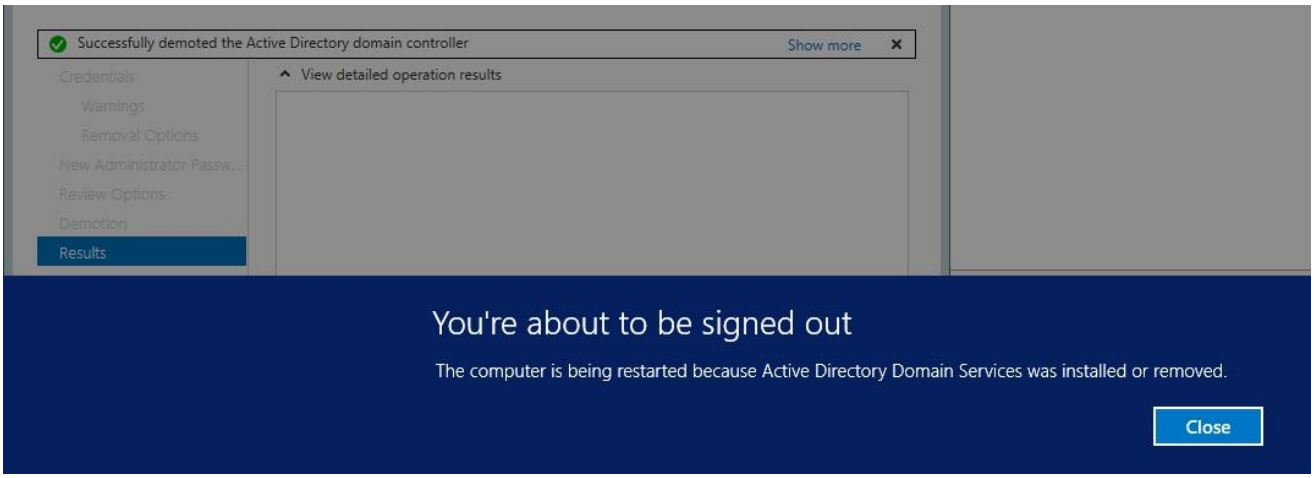

- Enter the new Administrator password and click **Next**.




- On the Review options page click **Demote**.

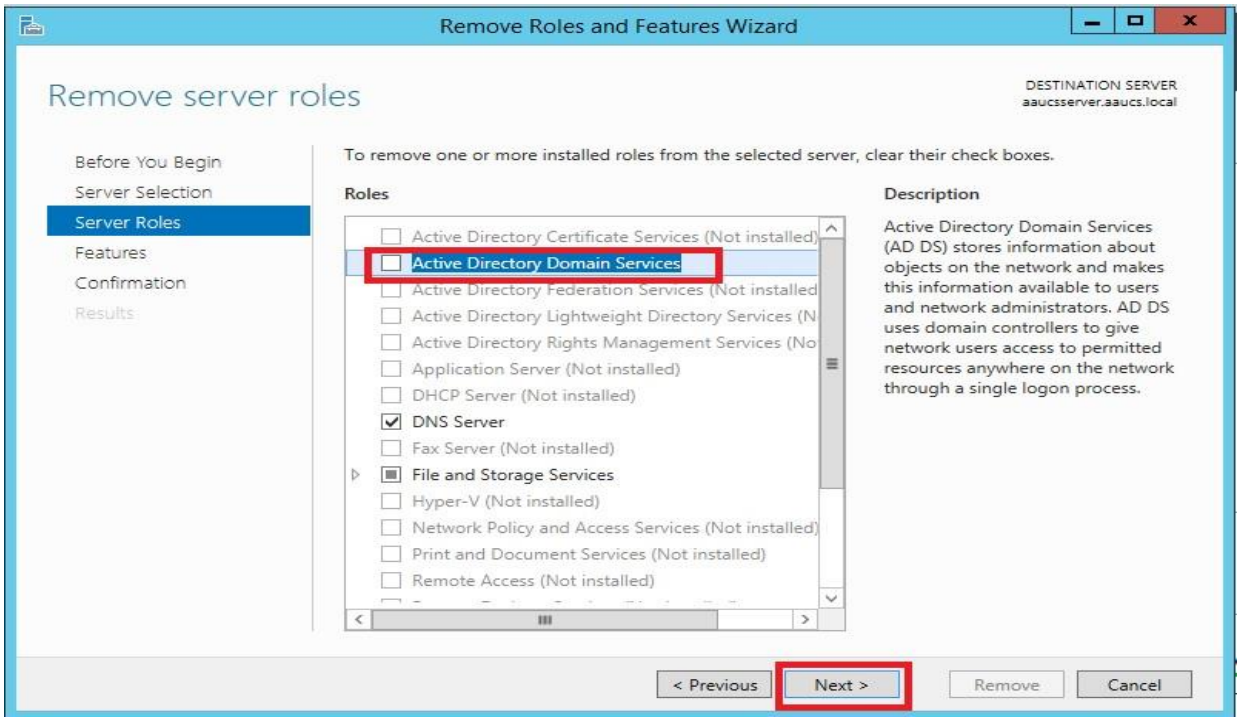



After the demoted process successfully finished your screen will be looks like the figure in below

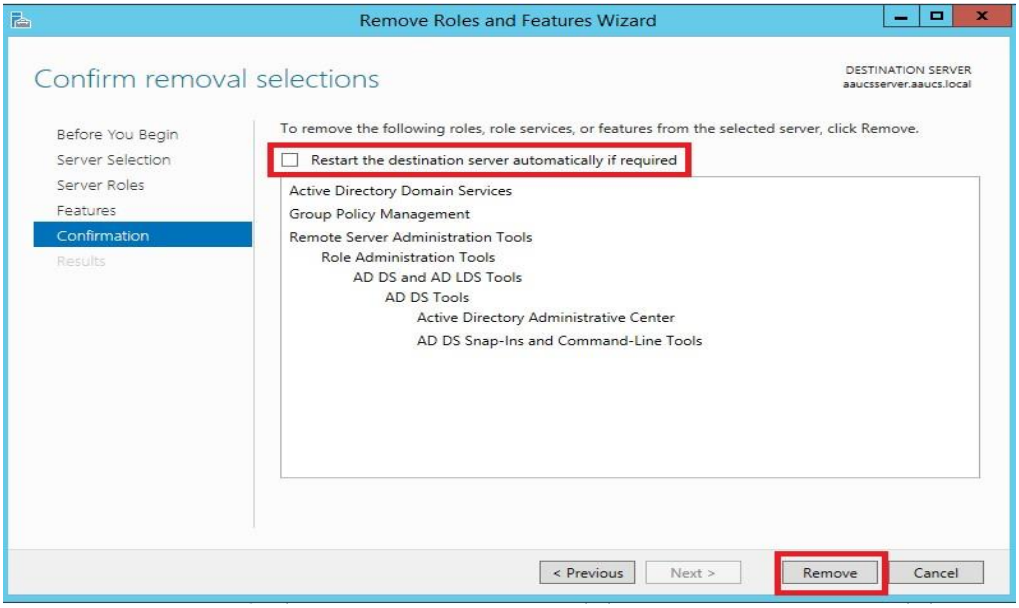



- The success of demoting the domain controller is not enough to remove an Active directory Domain Services from the server, there are some steps waiting us to remove the AD DS role totally from our server. The steps are:

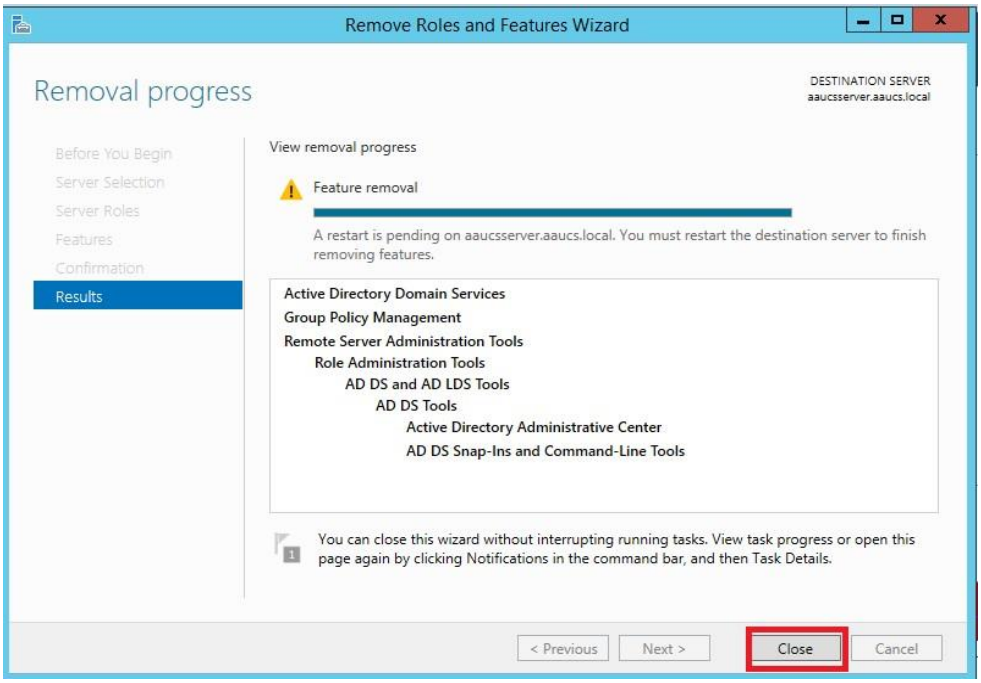
1. Go to **Manage** and click **Remove roles** and **features** on the **Server Manager** Dashboard.
2. Pass **Before you begin** and **Select destination server pages** by clicking **Next.**
3. Uncheck an **Active Directory Domain Services** from the **Server Roles** page and click **Next**.



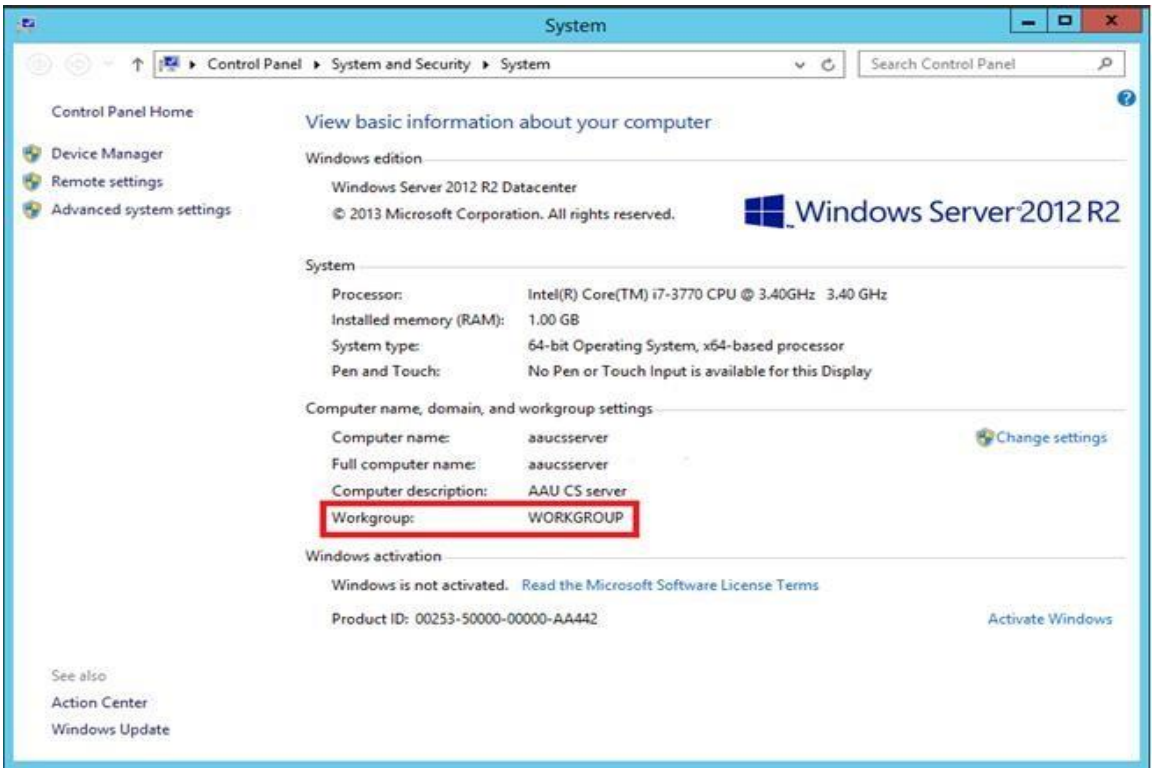
4. On the **Confirmation** page you can check "**Restart the destination server automatically if required**" or leave it as it is and restart the server manually after the removal process will be finished because the restart operation is required after the removal of AD DS role.




5. After the removal process successfully finished click **Close** button and **restart** the server manually if you didn't checked the "**Restart the destination server automatically if required**" check box in the previous step.



❖ Finally, you can check the server is back in to a member of workgroup through right click on **This PC** -> **Properties**.



# References:


1. Microsoft official Academic course, Networking fundamentals, Exam98-366

   193.140.54.45/network/NetworkingFundamentals.pdf

2. An Introduction to Computer Networks, Release 1.96, Peter L Dordal, September 05, 2017 https://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf
3. Microsoft Press eBook Introducing Windows Server 2012 R2

   https://download.microsoft.com/DOWNLOAD/4/8/A/48A3ADA5-063D-4C7F-AA11-F9A3AE8C8B55/MICROSOFT_PRESS_EBOOK_INTRODUCING_WINDOWS_SERVER_2012_R2_PDF.PDF

4. https://technet.microsoft.com/en-us/library
5. Installing and Configuring Windows Server 2012 R2 Exam Ref 70-410, Craig Zacker https://ptgmedia.pearsoncmg.com/images/9780735684249/.../9780735684249.pdf
6. https://docs.microsoft.com/en-us/windows-server
7. https://www.tutorialspoint.com/windows_server_2012/
8. https://theitbros.com/windows/windows-server/