RQF LEVEL 4

NITWA401

NETWORKING AND INTERNET TECHNOLOGIES

Windows Server Administration

TRAINEE'S MANUAL

October, 2024

WINDOWS SERVER ADMINISTRATION

KOICA Korea International Cooperation Agency

TQUM TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

Copies available from:

- *HQs: Rwanda TVET Board-RTB*
- *Web: www.rtb.gov.rw*
- **KIGALI-RWANDA**

Original published version: October 2024

ACKNOWLEDGEMENTS

The publisher would like to thank the following for their assistance in the elaboration of this training manual:

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate IV in Networking and Internet Technologies, specifically for the module **"NITWA401: Windows Server Administration."**

We extend our gratitude to KOICA Rwanda for its contribution to the development of these training manuals and for its ongoing support of the TVET system in Rwanda

We extend our gratitude to the TQUM Project for its financial and technical support in the development of these training manuals.

We would also like to acknowledge the valuable contributions of all TVET trainers and industry practitioners in the development of this training manual.

The management of Rwanda TVET Board extends its appreciation to both its staff and the staff of the TQUM Project for their efforts in coordinating these activities.

This training manual was developed:

Under Rwanda TVET Board (RTB) guiding policies and directives

Under Financial and Technical support of

COORDINATION TEAM

RWAMASIRABO Aimable
MARIA Bernadette M. Ramos
MUTIJIMA Asher Emmanuel

Production Team

Authoring and Review

KAREKEZI Gustave

UWIRINGIYIMANA Emmanuel

NTAKIRUTIMANA Samuel

Validation

UWANYAGASANI Jerome
SINDIKUBWABO Telesphore
GATETE Patrick

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Slvestre

NIYOMUGABO Silas

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe
SUA Lim
SAEM Lee
SOYEON Kim
WONYEONG Jeong
HAKIZAYEZU Adrien

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

AD LDS: Active Directory Lightweight Directory Services
AD: Active Directory
ADDS: Active Directory Domain Services
ADSS: Active Directory Sites and Services
ADUC: Active Directory Users and Computers
ARPA: Advanced Research Projects Agency
BIOS: Basic Input/ Output System
CBT/A: Competency-Based Training/Assessment
CD: Compact Disc
CGI: Common Gateway Interface
CName: Canonical Name
CPU: Central Processing Unit
CSR: Certificate Signing Request
DHCP: Dynamic Host Configuration Protocol
DNS: Domain Name System
DNSBL: Domain Name System-based Blackhole List
DSRM: Set Directory Services Restore Mode
DVD: Digital Video Disc or Digital Versatile Disc
FQDN: Fully Qualified Domain Name
FTP: File Transfer Protocol
GPMC: Group Policy Management Console
GPOs: Group Policy Objects
HTTPS: Hypertext Transfer Protocol Secure
IIS: Internet Information Services
IP: Internet Protocol
IPConfig: Internet Protocol Configuration
IPV4: Internet Protocol Version 4
IPV6: Internet Protocol Version 6
KOICA: Korea International Cooperation Agency
MAC: Media Access Control Address
MFT: Managed File Transfer
MTA: Message transfer agent
MX: Mail Exchange
NAT: Network Address Translation
NOS: Network Operating System
NS: Name Server
OS: Operating System

OU: Organizational Unit
PC: Personal Computer
PTR: Pointer Record
RTB: Rwanda TVET Board
SFTP: SSH File Transfer Protocol
SSL: Secure Sockets Layer
TLS: Transport Layer Security
TQUM Project: TVET Quality Management Project
TTL: Time To Live
UAC: User Account Control
UAT: User Acceptance Testing
WSUS: Windows Server Update Services

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Networking and Internet Technologies specifically for the module of **"Windows Server Administration."** Trainees enrolled in this module will engage in practical activities designed to develop and enhance their competencies. The development of this training manual followed the Competency-Based Training and Assessment (CBT/A) approach, offering ample practical opportunities that mirror real-life situations.

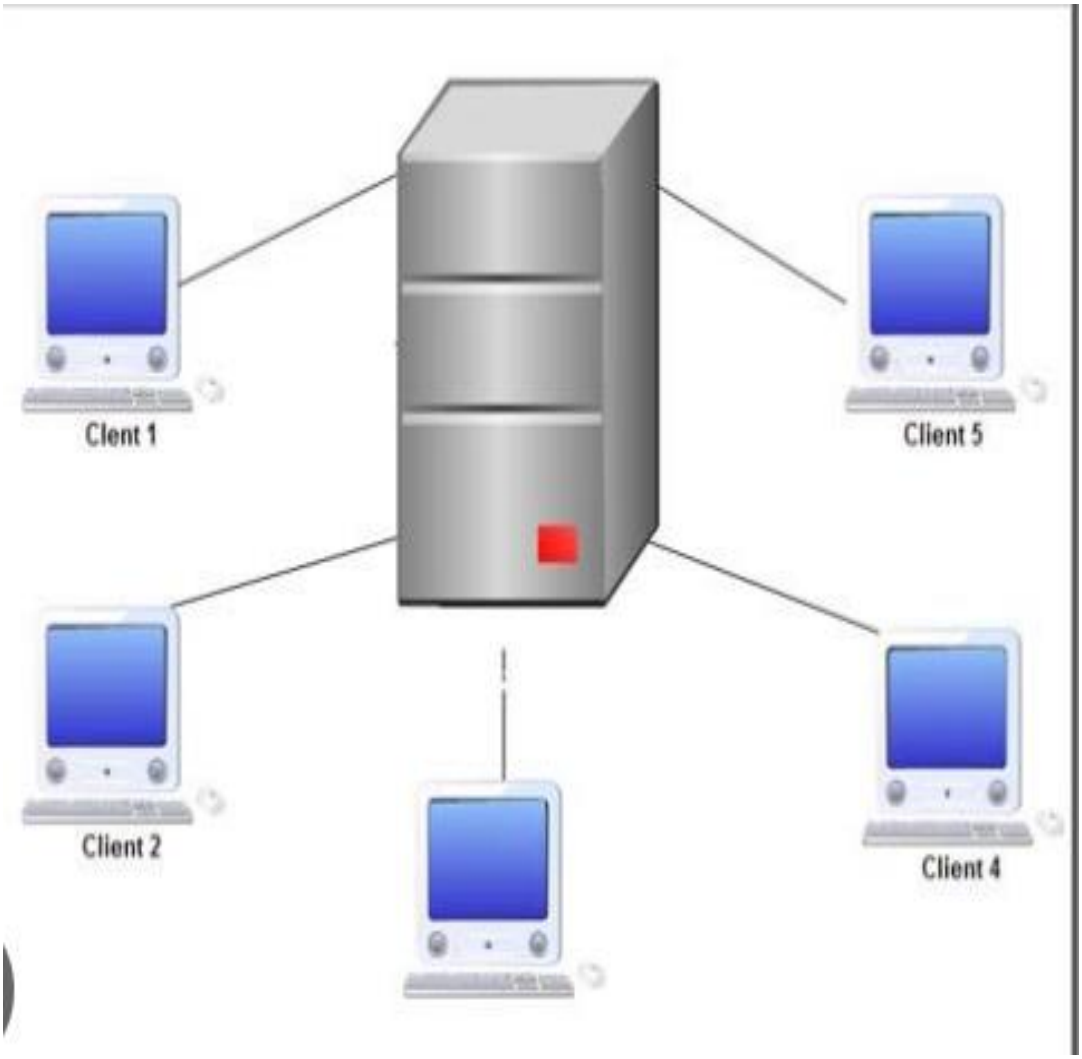
The trainee's manual is organized into Learning Outcomes, which is broken down into indicative content that includes both theoretical and practical activities. It provides detailed information on the key competencies required for each learning outcome, along with the objectives to be achieved.

As a trainee, you will start by addressing questions related to the activities, which are designed to foster critical thinking and guide you towards practical applications in the labor market. The manual also provides essential information, including learning hours, required materials, and key tasks to complete throughout the learning process.

All activities included in this training manual are designed to facilitate both individual and group work. After completing the activities, you will conduct a formative assessment, referred to as the end learning outcome assessment. Ensure that you thoroughly review the key readings and the 'Points to Remember' section.

MODULE CODE AND TITLE: NITWA401 WINDOWS SERVER ADMINISTRATION

Learning Outcome 1: Prepare server environment.
Learning Outcome 2: Deploy active directory services.
Learning Outcome 3: Deploy DHCP services.
Learning Outcome 4: Deploy DNS service.
Learning Outcome 5: Deploy web services.
Learning Outcome 6: Deploy FTP services.
Learning Outcome 7: Perform load balancing.
Learning Outcome 8: Perform server maintenance.


Client 1
Client 5
Client 2
Client 4

Indicative contents
1.1 Selection of Windows Server **1.2 Identification of Server Tools and Equipment** **1.3 Installation of Windows Server.**

Key Competencies for Learning Outcome 1: Prepare Server Environment

Knowledge	Skills	Attitudes
● Description of windows server concepts ● Description of virtualization concepts. ● Description of types of OS ● Identification of server tools and equipment ● Description of hardware server requirement ● Description of windows server requirements	● Installing virtualization software ● Selecting server based on criteria. ● Prepare Installation Media ● Selecting Installation type ● Configuring network adapter ● Updating server drivers and services	● Having Adaptability ● Having Teamwork ● Have self-motivation ● Being analytical thinker and details oriented ● Having Time management ability

Duration: 15 hrs

Learning outcome 1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly windows server concepts as used in server administration.
2. Describe clearly virtualization concepts used in server administration.
3. Install properly virtualization software based on server requirements.
4. Describe clearly the types of OS as used in server administration.
5. Select properly Server based on server criteria
6. Identify correctly server tools and equipment as used in server
7. Describe clearly hardware server requirements as used in windows server administration.
8. Describe clearly windows server requirements as used in windows server administration.
9. Install properly windows server OS in virtual machine based on hardware requirements
10. Configure correctly network adapter in server based on Microsoft standards
11. Update properly Server drivers and services based on Microsoft standards

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS ● Rack	● VMWare workstation ● VMWare ESXI ● Oracle VirtualBox ● VMWare V-Sphere ● Windows Server OS bootable image ● Browser ● Flash disk ● CD/DVD Drive ● Rufus ● PowerISO	● Electricity ● Data Cables ● Internet

Indicative content 1.1: Selection of Windows Server

Duration: 5 hrs

Theoretical Activity 1.1.1: Description of Windows Server concepts

Tasks:

1: Answer the following questions:

i. What do you understand by the following terms as used in windows server?
   a) Windows server
   b) Client-side
   c) Server-side
   d) Server core
   e) Server manager
   f) Hyper-V

ii. What is the different Version of Windows Server?

iii. Explain Window server editions

iv. Explain the benefits of server core

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.1.1 in their manuals.

Key readings 1.1.1: Description of Windows Server concepts

- **Windows Server concepts**

1. Introduction to windows server

Windows Server is a group of server operating systems developed by Microsoft that supports enterprise-level management, data storage, applications, and communications. It is designed to handle various server roles such as web hosting, file sharing, and application hosting.

2. Key concepts of windows server

2.1 Client-side: Refers to the components and services that run on the user's devices, allowing them to access server resources.

2.2 Client: The client is a device or application that requests services or resources from the server. It initiates communication with the server and processes the results returned by the server.

2.3 Server-side: Involves the backend services and processes that manage requests from client devices, including data processing and storage.

2.4 Server: The server is a powerful machine or application that provides services

or resources to clients. It processes client requests, performs the necessary

2.5 Hyper-V: is a Microsoft virtualization technology that enables users to create and manage virtual machines (VMs) on a physical server.

2.6 Server Manager: is a central administrative tool for managing multiple roles and features in a Windows Server environment.

2.7 Server Core: is a minimal installation option for Windows Server that was first introduced with Windows Server 2008.

3. Windows Server Versions

- **Windows Server 2003** or **2003 R2** - Introduced features like improved security and support for 64-bit computing.
- **Windows Server 2008** - Added Server Core, Hyper-V virtualization, and enhanced management tools.
- **Windows Server 2008 R2** - Introduced support for more memory, improved virtualization, and the Direct Access feature.
- **Windows Server 2012** - Brought a new interface, improved virtualization with Hyper-V 3.0, and enhanced cloud integration.
- **Windows Server 2012 R2** - Included updates to virtualization, storage, and cloud capabilities.
- **Windows Server 2016** - Featured containers, Nano Server, and improved security with Shielded VMs.
- **Windows Server 2019** - Focused on hybrid cloud features, security improvements, and Windows Admin Center.
- **Windows Server 2022** - Emphasized security enhancements, hybrid cloud support, and improved performance.

4. Editions of Windows Server

- **Essentials:** Designed for small businesses with up to 25 users and 50 devices. It offers simplified management and essential features.
- **Standard:** Suitable for physical or minimally virtualized environments, supporting two Operating System Environments (OSEs) per license.
- **Datacenter:** Intended for highly virtualized data centers and cloud environments, allowing unlimited OSEs.

5. **Benefits of a Server Core**

- **Minimal Installation:** Server Core has a stripped-down version of Windows Server, which includes only essential components and services.
- **Reduced Attack Surface:** Fewer installed features mean fewer vulnerabilities, enhancing security.
- **Lower Resource Consumption:** Server Core uses less disk space, memory, and CPU resources compared to a full GUI installation.
- **Improved Performance:** Without the overhead of a graphical interface, Server Core can deliver better performance for certain server roles.

- **Command-Line Management:** Administration is primarily done through Windows PowerShell or command-line tools, which can be more efficient for experienced administrators.
- **Remote Management:** Server Core can be managed remotely using tools like PowerShell Remoting and Windows Admin Center, allowing for greater flexibility.

Theoretical Activity 1.1.2: Description of virtualization concepts.

Tasks:

1: Answer the following questions related to virtualization concepts:

i. What is virtualization?
ii. What are the benefits of virtualization?
iii. What is virtual machine?
iv. Explain the types of Hypervisors?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.1.2 in their manuals.

Key readings 1.1.2.: Description of virtualization concepts

- **Virtualization concepts.**

1. Key Components of Virtualization

1.1 Virtualization is a technology that allows multiple virtual environments to run on a single physical hardware platform.

1.2 Hypervisor: A software layer that enables virtualization by managing and allocating hardware resources to virtual machines (VMs).

1.2.1 There are two main types of hypervisors:

- **Type 1 (Bare-metal)**: Runs directly on the hardware (e.g., VMware ESXi, Microsoft Hyper-V).
- **Type 2 (Hosted)**: Runs on top of an existing operating system (e.g., VMware Workstation, Oracle VirtualBox).

1.3 Virtual Machines (VMs): is a software-based emulation of a physical computer. It consists of virtualized hardware components such as CPUs, memory, and storage, allowing it to run its own operating system and applications independently from other VMs on the same host.

1.3.1 Types of Virtualizations

- **Server Virtualization**: This is the most common form, allowing multiple server environments to run on a single physical server.
- **Desktop Virtualization**: Centralizes desktop management by hosting user desktops on a server.
- **Network Virtualization**: Creates virtual networks that replicate physical network functions (like switches and routers) within software.
- **Storage Virtualization**: Combines multiple physical storage devices into a single virtual storage pool, simplifying management and improving resource allocation across different applications.

1.4 Benefits of Virtualization

- **Resource Efficiency**: Multiple VMs can share the same hardware resources, leading to better utilization rates compared to traditional setups.
- **Cost Reduction**: Decreases the need for physical servers, reducing capital expenditure on hardware as well as ongoing costs for power and cooling.
- **Flexibility and Scalability**: Organizations can quickly provision new VMs or adjust existing ones based on demand without needing additional physical infrastructure.
- **Disaster Recovery**: Features like snapshots allow for quick restoration of VMs to previous states, facilitating effective disaster recovery strategies

Theoretical Activity 1.1.3: Description of types of OS

Tasks:

1: Answer the following questions related to the types of OS:

i. Differentiate standalone from network operating system?
ii. List the four examples of network operating system

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.1.3 in their manuals.

Key readings 1.1.3.: Description of types of OS

- **Types of OS**

1. Standalone Operating System

- Runs on a single computer or device (e.g. desktop, laptop, mobile device)
- Manages resources for a single user at a time

- Examples: Windows 10, macOS, Android, iOS
- Provides basic networking capabilities but is not primarily designed for networked environments

2. Network Operating System

- Runs on a server to manage resources and services for multiple connected devices
- Enables sharing of files, printers, applications across a network
- Examples: Windows Server, Linux, Unix, Novell NetWare
- Provides advanced networking features like user authentication, access control, centralized management
- Allows remote access to shared resources
- Requires more technical maintenance and has higher setup costs compared to standalone OS

Practical Activity 1.1.4: Selecting windows server

Task:

1: Referring to the key reading 1.1.4, perform the following task:

As networking and internet technology trainee, you are asked to go to the computer lab to select windows server operating system.

2: Present the procedures of all step performed during selection

3: Present your work to the trainer and whole class.

4: for more information read key reading 1.1.4 and ask clarification where necessary

5: Perform the task provided in application of learning 1.1

Key readings 1.1.4: Selecting windows server

- **Windows server**

1.Server selection criteria

When selecting a Windows Server, there are several criteria to consider ensuring that the server meets your organization's technical requirements and business objectives. Below are the key selection criteria:

1.1. Assess Your Business or Technical Requirements

- **Determine Workload**: Identify the type of workloads your server will handle (e.g., database management, file storage, web hosting, virtualization).
- **Estimate Performance Needs**: Understand the performance you require in terms of CPU, memory (RAM), storage, and network bandwidth.
- **Determine the Number of Users/Devices**: Identify the number of users or devices that will connect to the server

1. 2. Server Edition

Windows Server offers multiple editions, each designed for different use cases:

- **Windows Server Standard**: Suitable for small to medium-sized businesses that need basic virtualization and storage features. It supports two virtual machines and Hyper-V containers.
- **Windows Server Datacenter:** Ideal for highly virtualized or cloud environments, offering unlimited virtualization rights and advanced features like Software-Defined Networking (SDN).
- **Windows Server Essentials:** Targeted at small businesses with up to 25 users and 50 devices. It offers simpler administration but fewer advanced features.
- **Windows Server Hyper-V**: A free, standalone edition focused entirely on providing a virtualization platform.1

1.3. Hardware Requirement

Ensure that your hardware meets the minimum and recommended requirements for running Windows Server efficiently:

- **Processor:** A compatible 64-bit processor with a minimum of 1.4 GHz, with support for x64 architecture.
- **Memory (RAM):** At least 512 MB, though 2 GB or more is recommended for better performance, depending on workload.
- **Storage:** A minimum of 32 GB of storage space, but additional space is recommended for installation, updates, and storage of user data.
- **Network Adapter:** A gigabit Ethernet adapter is recommended for fast and reliable network performance.

1.4. Virtualization Needs

Virtualization is a key feature of Windows Server. Consider the following aspects:

- **Hyper-V:** The built-in virtualization platform. Determine whether you need to run multiple virtual machines (VMs) on a single physical server.
- **Containers:** Windows Server supports both Windows and Linux containers. If you plan to use containers for application deployment, ensure your server edition supports this feature.
- **Licensing for VMs:** The Standard edition allows up to two virtual machines, while the Datacenter edition offers unlimited virtualization rights.

1.5. Storage Solutions

Evaluate the storage options provided by Windows Server:

- **Storage Spaces Direct (S2D):** A feature in Datacenter edition that allows you to create highly available, scalable software-defined storage.
- **ReFS (Resilient File System):** Optimized for handling large datasets, reducing data corruption, and providing better performance for modern workloads.

- **Data Deduplication:** Saves storage space by removing duplicate copies of data.

1. 6. Integration with Existing Infrastructure

Consider how Windows Server will integrate with your existing IT infrastructure:

- **Active Directory (AD):** Windows Server can manage users, devices, and resources through AD. Ensure that your choice of server will support or integrate with your existing AD environment.
- **Group Policy Management:** For organizations that need to apply settings and policies to multiple users or devices, Group Policy management is a critical feature.
- **DNS, DHCP, and File Services:** Ensure compatibility with existing network services like DNS and DHCP, especially if migrating from another server environment.

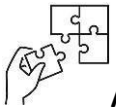
1.7. Cloud Integration and Hybrid Capabilities

Modern versions of Windows Server offer better cloud integration:

- **Azure Hybrid Benefit:** Allows you to use existing on-premises licenses for workloads in Azure, offering cost savings for businesses that use a hybrid cloud model.
- **Azure Integration:** Direct integration with Microsoft Azure services like Azure Backup, Azure Site Recovery, and Azure AD for cloud-based identity management.
- **Windows Admin Center:** A modern, browser-based interface that simplifies managing both on-premises and cloud-hosted servers.

Points to Remember

- While selecting windows server, take into consideration the following criteria:
    1. Assess Business/Technical Needs
    2. Select the Appropriate Edition
    3. Evaluate Hardware Requirements
    4. Consider Virtualization Needs
    5. Check Storage Options
    6. Focus on Security
    7. Consider Cloud Integration
    8. Ensure Infrastructure Compatibility



Application of learning 1.1.

Our school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for selecting windows sever operating system.

Indicative content 1.2: Identification of Server Tools and Equipment

Duration: 2 hrs

Theoretical Activity 1.2.1: Identification hardware requirement

Tasks:

1: Answer the following questions:

i. Which of the following is the minimum processor requirement for installing Windows Server 2022?

A. 1.4 GHz 64-bit processor
B. 2.0 GHz 32-bit processor
C. 1.3 GHz 64-bit processor
D. 2.5 GHz 64-bit processor

ii. What is the minimum RAM requirement for Windows Server 2022 installation?

A. 512MB
B. 1GB
C. 2GB
D. 4 GB

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.2.1 in their manuals.

Key readings 1.2.1: Identification hardware requirement

1.Hardware Requirements

The hardware requirements for Windows Server vary depending on the specific version and the workloads you intend to run. Below are the general minimum and recommended hardware requirements for Windows Server 2022, which is the latest version as of 2024. These requirements will help ensure that the server operates efficiently and meets your performance expectations.

1.1. Processor (CPU)

➢ **Minimum Requirements:**

- Processor architecture: x64-compatible processor with a minimum of 1.4 GHz.
- Processor support: The processor must support the following:
- NX (No Execute) bit.
- DEP (Data Execution Prevention).
- PAE (Physical Address Extension).

- SSE2 (Streaming SIMD Extensions 2).
- CMPXCHG16b (CompareExchange16b).

➢ **Recommended Requirements:**

- Processor architecture: 3.1 GHz or higher, multi-core processor (dual-core or better).
- Hyper-V support: If you plan to use Hyper-V for virtualization, ensure the CPU supports SLAT (Second Level Address Translation).

1.2. Memory (RAM)

➢ **Minimum Requirements:**

- Standard system: 512 MB of RAM.
- Server with desktop experience: 2 GB of RAM.

Note: If you are using a system with less than 800 MB of memory, the installation might fail or be inefficient.

➢ **Recommended Requirements:**

- General workloads: 4 GB or more.
- Virtualization/Heavy workloads: 16 GB or higher, depending on the number of virtual machines (VMs) or intensive applications.

1.3. Storage (Hard Drive)

➢ **Minimum Requirements:**

- **Disk space: 32** GB for the installation. Keep in mind that systems with the Server with Desktop Experience installation option may require more disk space (approximately 40 GB or more). For servers with minimal memory, more storage is required for paging, hibernation, and dump files.

➢ **Recommended Requirements:**

- System partition: 64 GB or more to account for future updates, applications, and system logs.
- SSD: Solid-State Drives (SSD) are recommended for faster boot times and better overall performance, especially for applications with high I/O needs (databases, file servers)

1.4. Rack Enclosures

Ensure that the rack enclosures are compatible with the hardware form factors being used (e.g., standard 19-inch racks). Consider the number of units (U) required based on the size and number of servers.

1.5. Uninterruptible Power Supply (UPS)

A UPS is critical for maintaining power during outages and ensuring hardware safety. The capacity should be chosen based on total wattage of all connected devices, typically providing at least **10-20% extra capacity.**

1.6. Form Factor and Rack Space

Common server form factors include:

- **1U:** Compact servers suitable for high-density environments.

•**2U or larger:** Offer more space for additional components like drives and cooling systems. Ensure that the total rack space required fits within the available rack dimensions while allowing for adequate airflow and maintenance access.

By carefully considering these hardware requirements, you can ensure that your setup will meet both current and future needs effectively.

Points to Remember

- About CPUMinimum Requirement is 1.4 GHz x64 processor with required extensions and Recommended Requirement are 3.1 GHz or higher multi-core processor. **Memory (RAM):** minimum Requirement are 512 MB (2 GB for desktop experience), Recommended requirement are 4 GB for general, 16+ GB for heavy workloads.
- **Storage:** 32 GB minimum (40+ GB for desktop experience) and 4 GB for general, 16+ GB for heavy workloads is recommended.
- By carefully considering these hardware requirements, you can ensure that your setup will meet both current and future needs effectively.

Theoretical Activity 1.2.2: Identification software requirement

Tasks:

1: Answer the following questions:

i. What is the role of Microsoft Management Console (MMC) in server management?
ii. Can you explain the importance of the .NET Framework in server management applications?
iii. Identify some popular virtualization platforms?

2: write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 1.2.2 in their manuals.

Key readings 1.2.2: Identification hardware requirement

1.Software Requirements

1.1. Server Management Software

Server management software enables administrators to monitor, control, and maintain server infrastructure. Here are some popular options:

- **Microsoft Windows Admin Center**: A browser-based management tool that allows for centralized management of Windows Server, Hyper-V, and clusters.
- **System Center**: A suite of tools for data center management, including Configuration Manager (SCCM), Virtual Machine Manager (SCVMM), and Operations Manager (SCOM).
- **SolarWinds Server & Application Monitor**: Monitors server health, performance, and applications.
- **ManageEngine OpManager**: Provides real-time server performance monitoring and network device management.
- **Puppet/Chef/Ansible**: Automates configuration management, allowing for infrastructure as code (IaC).
- **Nagios**: An open-source monitoring solution to keep track of server uptime, disk usage, and services.

1.2. Virtualization Software

Virtualization software allows multiple operating systems and applications to run on a single server, improving resource utilization and management flexibility.

Popular Virtualization Platforms:

- **Microsoft Hyper-V**: A built-in Windows Server feature offering hardware virtualization for multiple VMs (virtual machines).
- **VMware vSphere (ESXi)**: One of the most popular enterprise-grade hypervisors for running multiple VMs with advanced management capabilities.
- **Oracle VM VirtualBox**: A free, open-source option for both personal and commercial use.
- **Citrix Hypervisor (formerly XenServer)**: Provides robust server virtualization, including support for both Windows and Linux VMs.
- **Proxmox VE**: A free, open-source server virtualization management solution based on KVM and LXC.

Points to Remember

- Choosing the right server management and virtualization software is essential for optimizing your Windows Server environment. Built-in tools like Server Manager and Windows Admin Center offer robust capabilities. Ensure that your hardware meets the requirements for both management and virtualization software to achieve optimal performance.
- Windows Admin Center: A modern, browser-based tool that provides comprehensive management capabilities for Windows Server environments. Can be deployed locally without Azure or integrated into the Azure portal. Supports single-server deployments and hyper-converged clusters.

1. popular virtualization platforms:

2. Microsoft Hyper-V:
3. VMware vSphere (ESXi).
4. Oracle VM VirtualBox
5. Citrix Hypervisor (formerly XenServer)
6. Proxmox VE

Indicative content 1.3: Installation of Windows Server

Duration: 8 hrs

Practical Activity 1.3.1: Selecting windows server

Task:

1: Referring to the key reading 1.2.2 As networking and internet technology trainee, you are asked to go to the computer lab to prepare windows server installation media.
2: Present the procedures of all step performed installation.
3: Present your work to the trainer and whole class.
4: Read key reading 1.3.1 and ask clarification where necessary
5: Perform the task provided in application of learning 1.3 in their manuals.

Key readings 1.3.1.: Preparing the Installation Media

Prepare Installation Media

- **Download the Windows Server ISO Image:** Visit the Microsoft Volume Licensing Service Center or the Microsoft Store to download the desired Windows Server ISO image. Ensure you have the correct product key for the edition you've purchased.
- **Create a Bootable Installation Media:**
- **SB Drive**

Use a tool like Rufus or the Windows Media Creation Tool to create a bootable USB drive.

Steps to Create Bootable Installation Media with Rufus

Step 1: Download and Launch Rufus: Visit the Rufus download page and download the latest version. Double-click the downloaded file (e.g., Rufus-x.xx.exe) to launch the application.

Step 2: Prepare Your USB Drive: Insert your USB flash drive into your computer. In Rufus, under the **Device** section, select your USB drive from the dropdown menu.

Step 3: Select Boot Selection: Under the **Boot selection** section, click on the **Select** button. Choose your existing Windows ISO file from your computer or select **Download** to fetch a Windows image directly from Microsoft servers.

Step 4: Configure Image Options: If you are using an existing ISO, ensure you select **Standard Windows installation** from the **Image option** dropdown menu.

Step 5: Choose the appropriate partition scheme: **MBR** for BIOS or UEFI (non-CSM) or **GPT** for UEFI (recommended for modern systems).

Step 6: Click on the **Start** button to begin creating the bootable USB drive. You may receive a warning that all data on the USB drive will be destroyed; confirm to proceed.

Step 7: Once Rufus has finished creating the bootable USB drive, you will see a message indicating that it is ready. Safely eject your USB drive.

➢ **DVD**

Burn the ISO image to a DVD using a DVD burning software.

Step 1: Download and Install BurnAware: Visit the BurnAware website and download the free version of the software. Install it by following the on-screen instructions.

Step 2: Open the BurnAware application after installation.

Step 3: Insert a blank DVD into your DVD writer. Ensure that it is compatible (DVD-R, DVD+R, etc.).

Step 4: In BurnAware, select **"Burn ISO"** from the main menu. Click on the **"Browse"** button to locate and select the ISO file you want to burn.

Step 5: Ensure that your DVD drive is selected under the **"Destination"** dropdown. You can adjust settings such as burning speed if needed, although the default settings usually work well.

Step 6: Click on the **"Burn"** button to start the burning process. A progress bar will show you how much of the process is complete.

Step 7: 7. the burning is finished; you will receive a confirmation message. Safely eject your DVD from the drive.

Points to Remember

- **While prepare installation media, performs the following key steps:**
  1. Download the Windows Server ISO Image meet with your server requirements. If you haven't.
  2. Download and Launch Rufus:
  3. Prepare Your USB Drive
  4. Select Boot Selection
  5. Configure Image Options
  6. Choose the appropriate partition scheme
  7. Click on the **Start** button to begin creating the bootable USB drive.
  8. Completion

Practical Activity 1.3.2: Installing windows server

Task:

1: Referring to the key reading 1.3.1 As networking and internet technology trainee, you are asked to go to the computer lab to lab to installing windows server.
2: Present the procedures of all step performed installation.
3: Present your work to the trainer and whole class.
4: Read key reading 1.3.2 and ask clarification where necessary
5: Perform the task provided in application of learning 1.3

Key readings 1.3.2: Installing windows server

1.Physical machine

Ensure that your physical machine meets the minimum system requirements for the Windows Server edition you want to install. This typically includes a compatible processor, sufficient RAM, and storage. Connect the necessary peripherals, such as a keyboard, mouse, and monitor. If you have existing data on the machine, consider backing it up before proceeding with the installation.

The installation type you choose when installing Windows Server determines how the operating system will be installed on your physical machine. Here are the two main options:

1.1. Clean Installation:

This option erases all existing data on the selected partition or drive. It is recommended for new installations or if you want to start with a fresh system. If you choose a clean installation, you will need to back up any important data before proceeding.

1.2. Upgrade:

This option keeps your existing data and settings while installing Windows Server over the previous operating system. It is suitable for upgrading from an earlier version of Windows Server or another compatible operating system. However, some applications or drivers may not be compatible with the new version of Windows Server, so you may need to reinstall them after the upgrade.

➢ **Steps for Installing Windows Server 2012 R2**

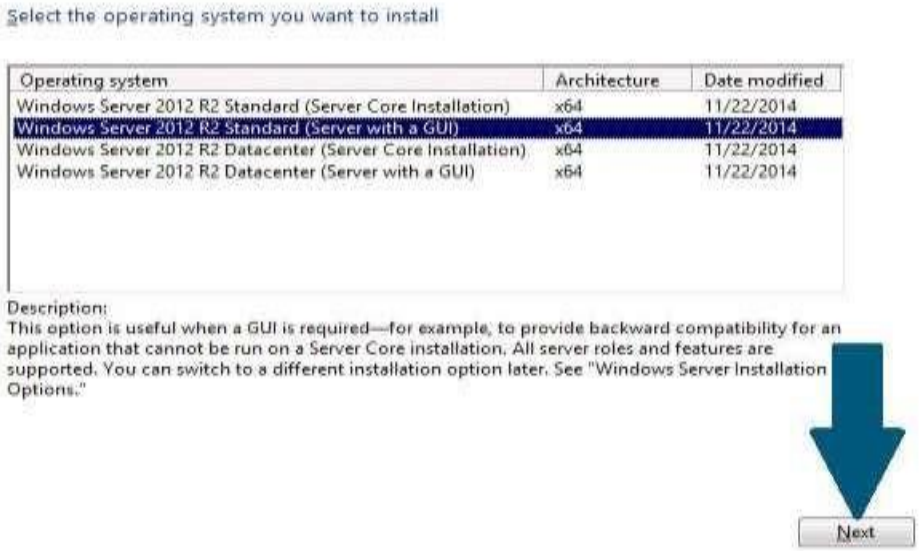
Step 1: Insert a DVD of Windows Server 2012 R2 into your system and start it. Once you get a message

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

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

Step 3: Click Install now

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

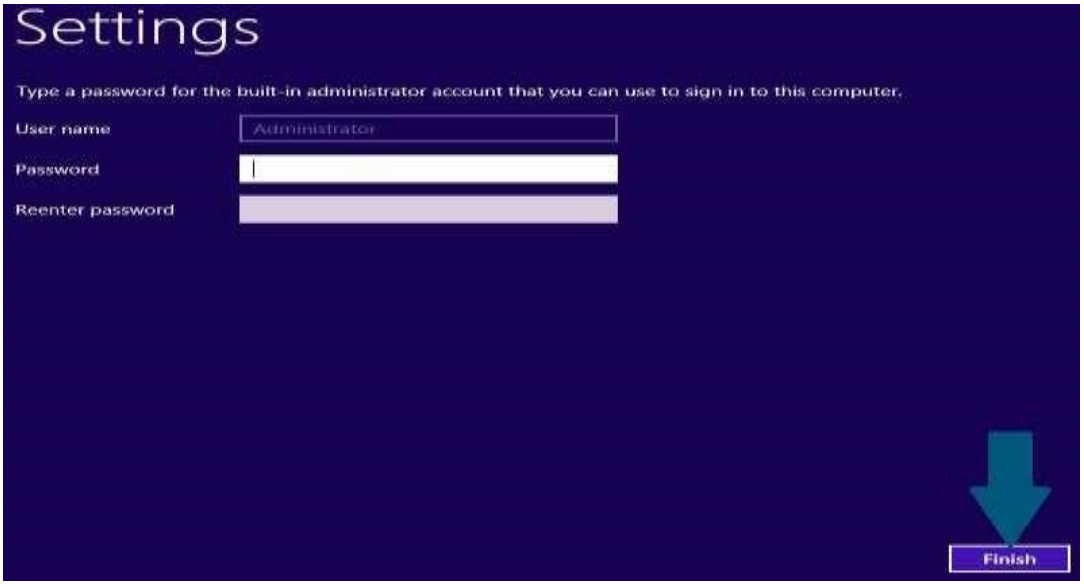


Step 5: Click Custom: Install Windows only (advanced)

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

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

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



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

➢ **Virtual machine**

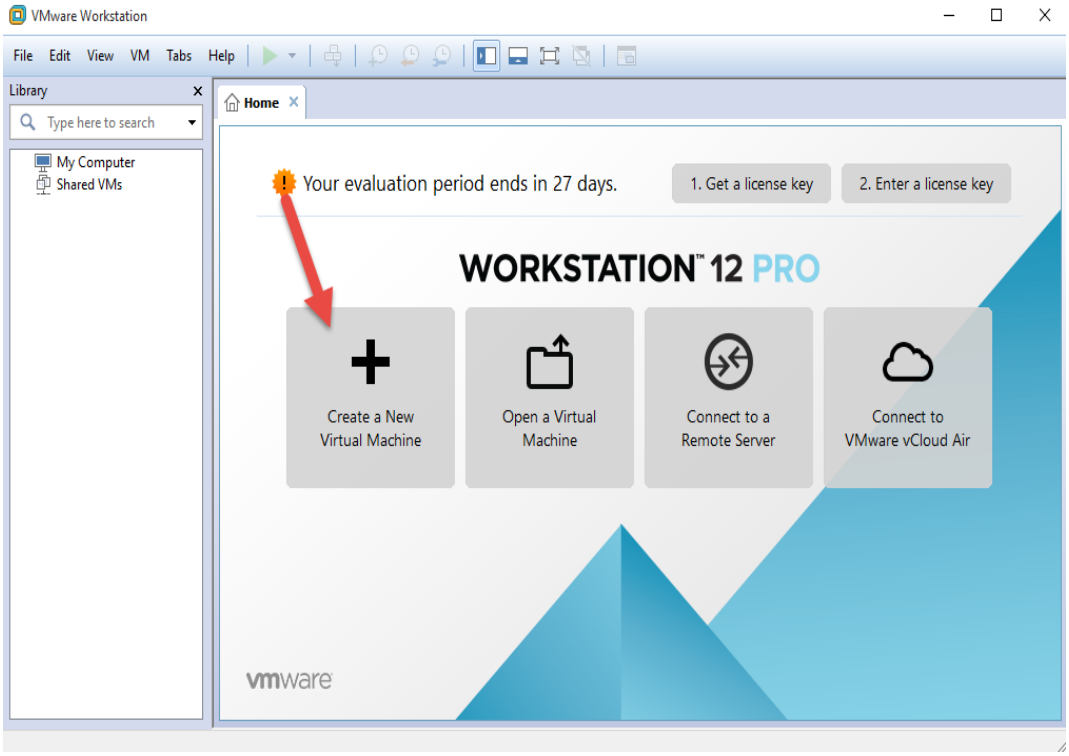
When installing Windows Server on a virtual machine, you typically perform a clean installation. This is because you are creating a new virtual hard disk (VHD) file to contain the Windows Server installation, and there is usually no existing data or operating system to upgrade from.

However, if you are cloning an existing virtual machine that already has Windows Server installed, you may have the option to upgrade the operating system within the cloned machine. In this case, you would be upgrading from an existing installation to a newer version of Windows Server**.**

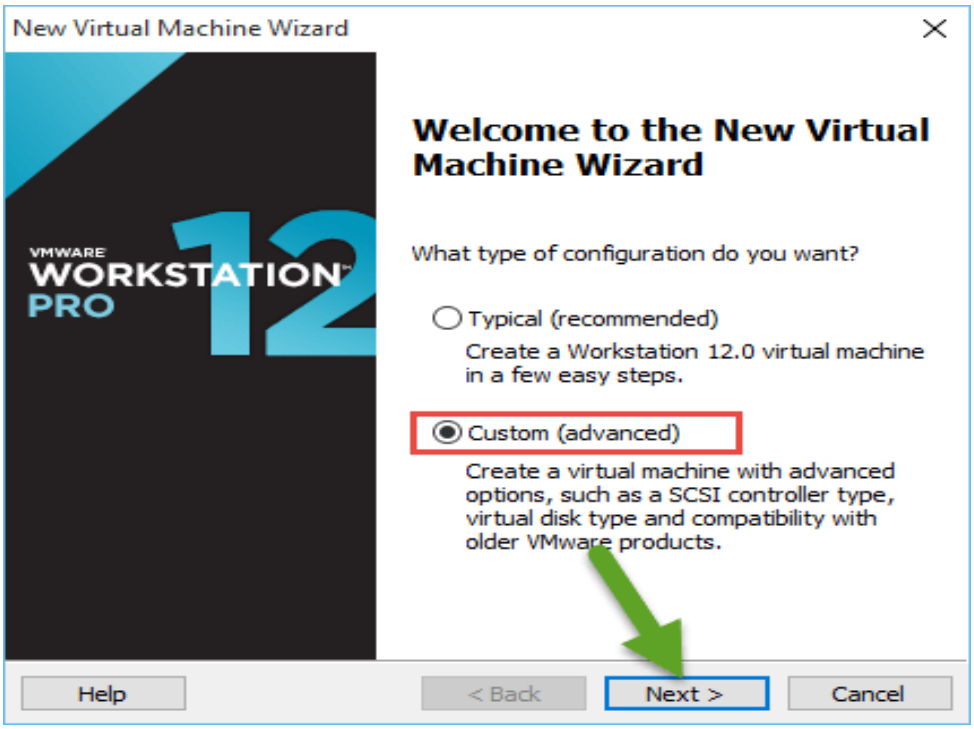
➢ **Installing Windows Server 2016 on VMware**

Step1. Open **VMware** and click on the **Create a New Virtual Machine**(Ctrl+N) icon. If you don't have VMware installed on your computer, click here to

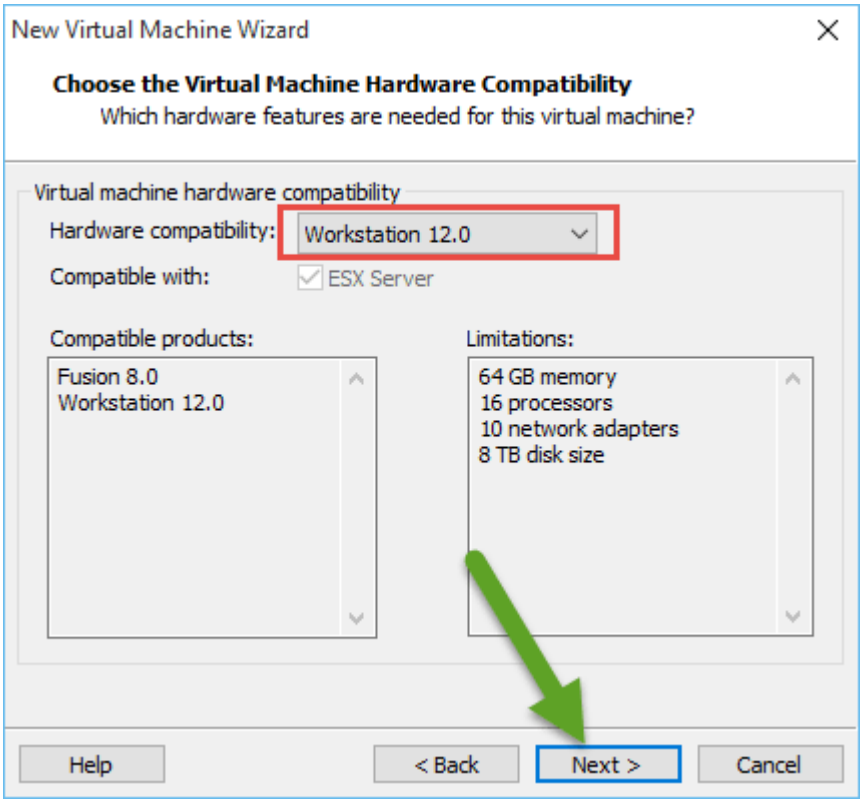
download one.



Step2. Now select **Custom (Advanced)** option to specify the virtual machine with advance options. If you want you can create virtual with less options, click on Typical option. When you are finished here, click on **Next** button.

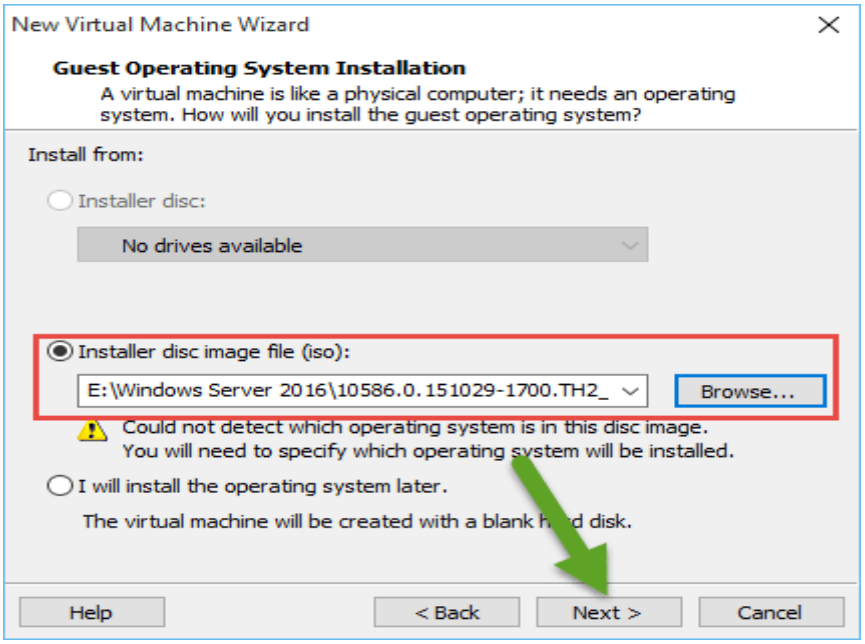


Step 3. Leave the **Virtual Machine Hardware Compatibility** settings as default. If you want you can select your VMware version. Then click **Next** button.



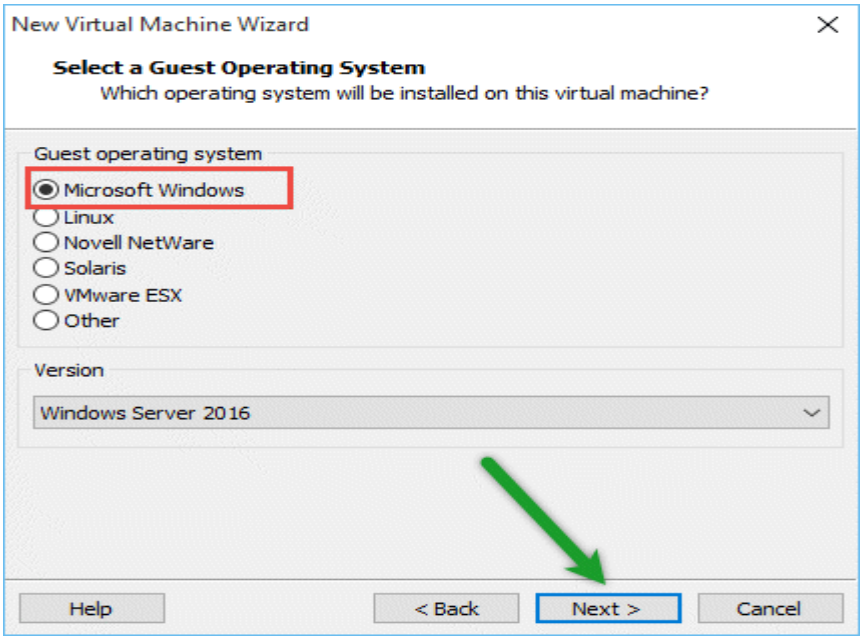
Step 4. Here you should add an installer image into the virtual machine. Select the **Installer disc image file (ISO)** option and click on the **Browse** button. Specify .iso file path and import it. Then click on **Next** button.

Note: Make sure that you are using an ISO image file, otherwise unzipped file won't boot.

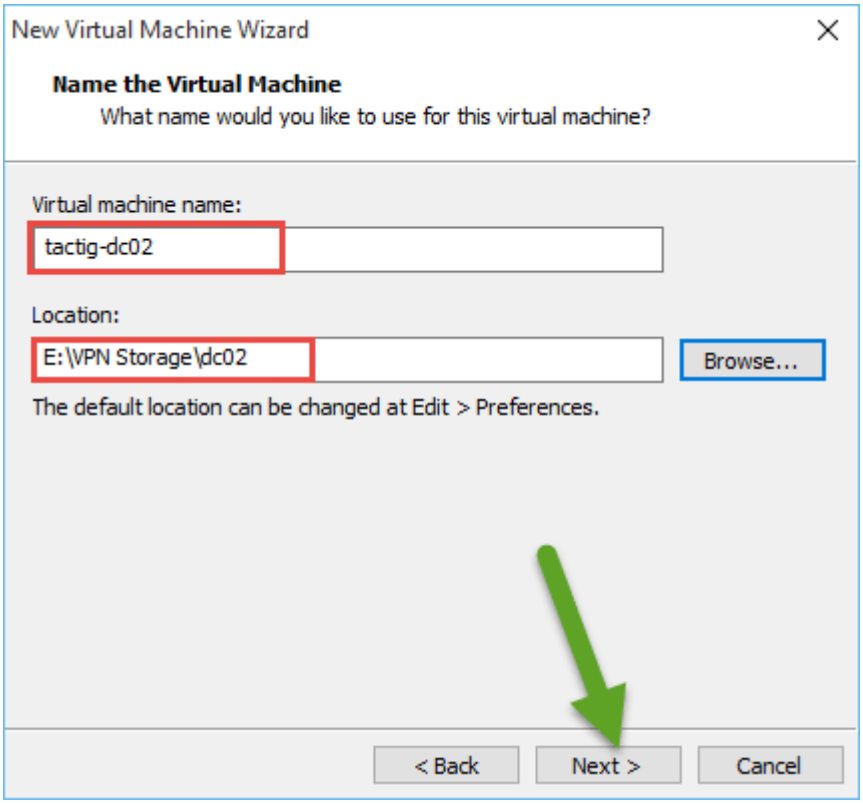


Step 5. Specify which operating system type you want to install on the virtual machine. Select **Windows Server 2016** version from the dropdown menu and

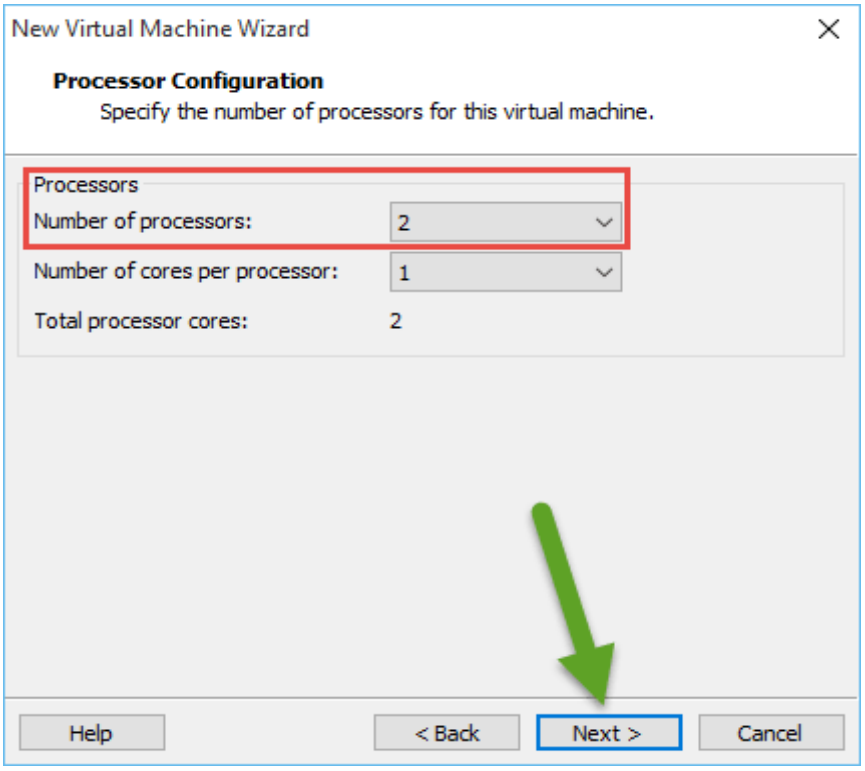
click on **Next** button.



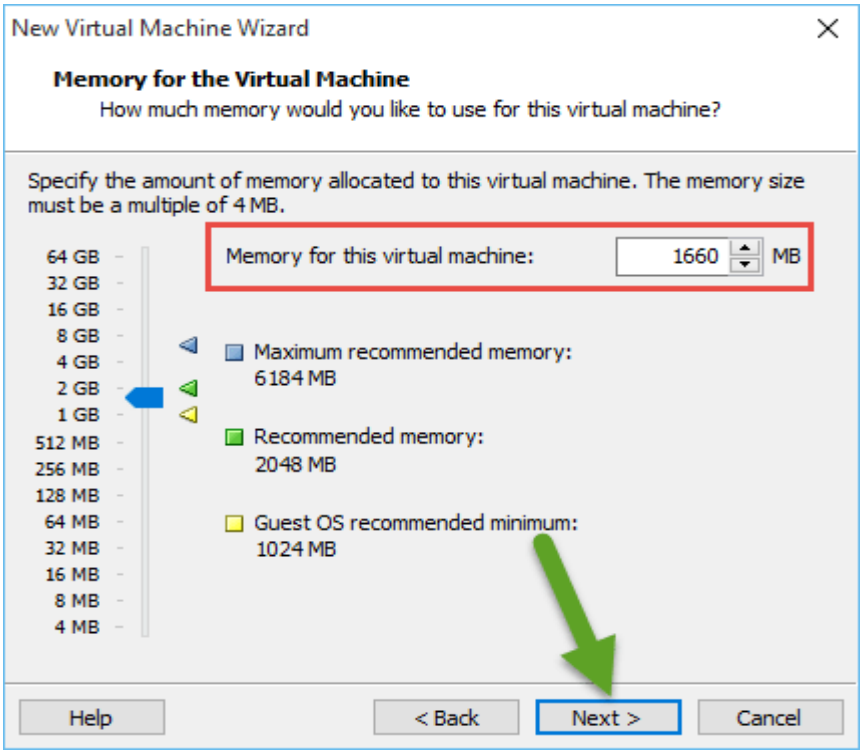
Step 6. Enter a name for the virtual machine and browse a place where you want to store the installation files. For the purpose click on **Browse** button and specify the place. When finished, click on **Next** button.



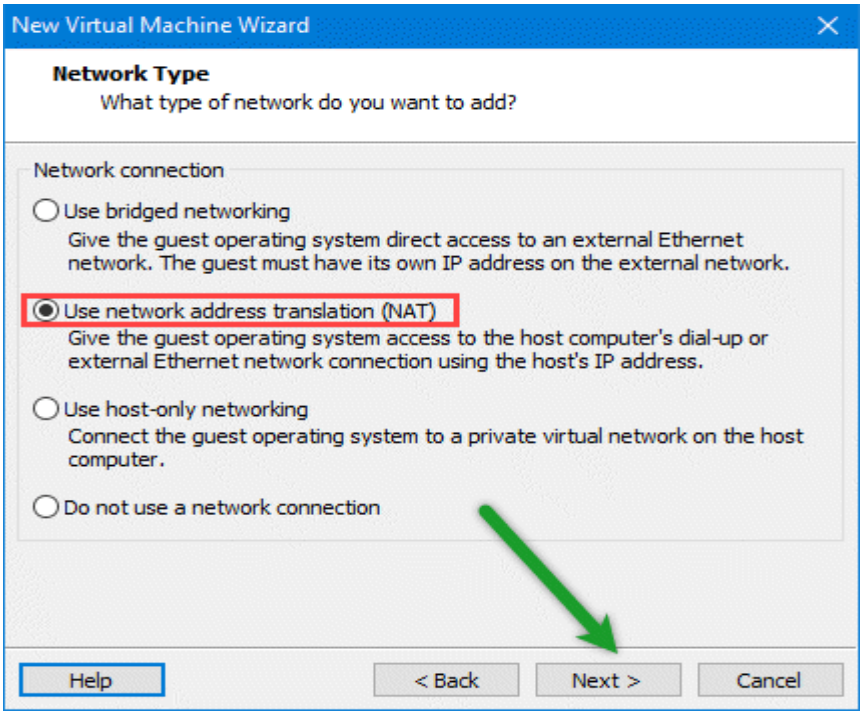
Step 7. On the **Processor Configuration** specify then number of processors your server need to use and click on **Next** button. Also notice that it refers to your virtual machine speed that how much speed the server should be.



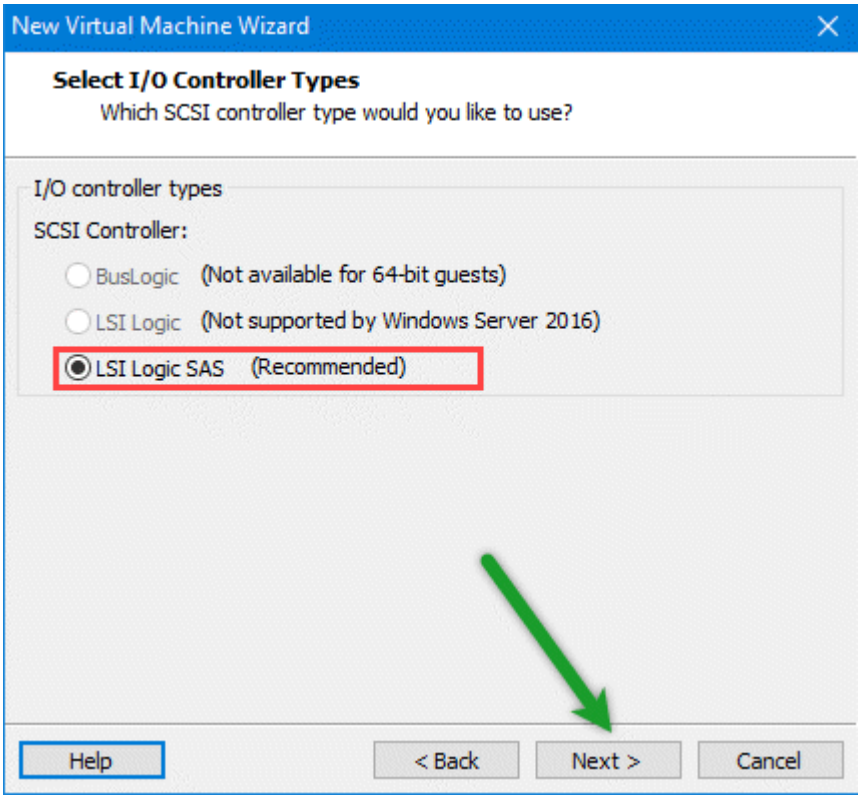
Step 8. Specify the amount of the memory for the virtual machine (based on MB) and click on **Next** button.



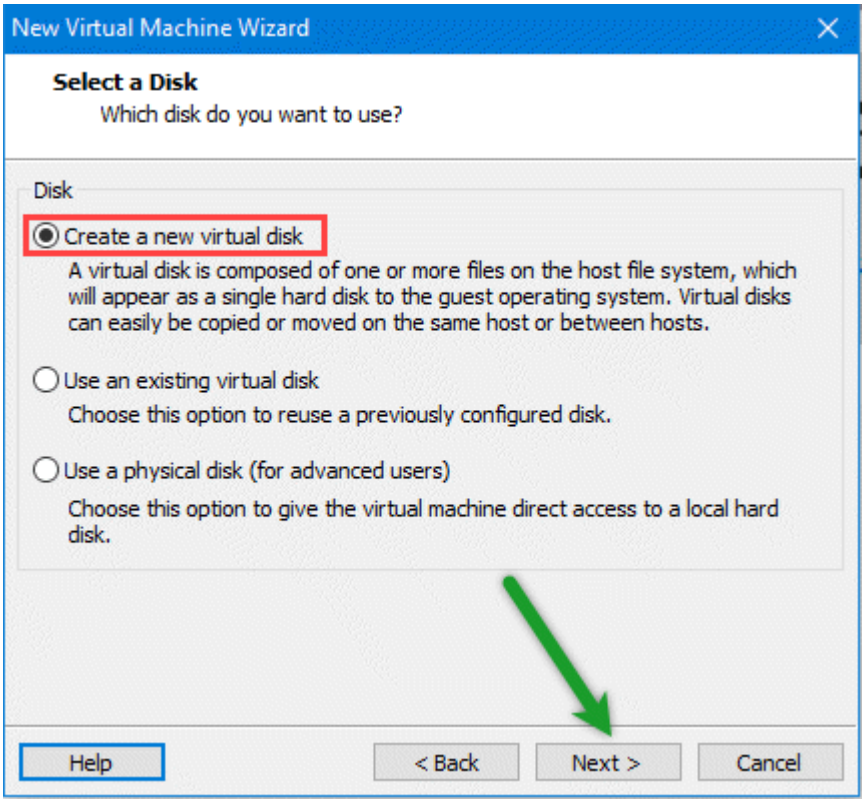
Step 9. Select **Use Network Address Translation (NAT)** or use bridged **networking** to directly connect and use internet, as a network type. Then hit **Next**.



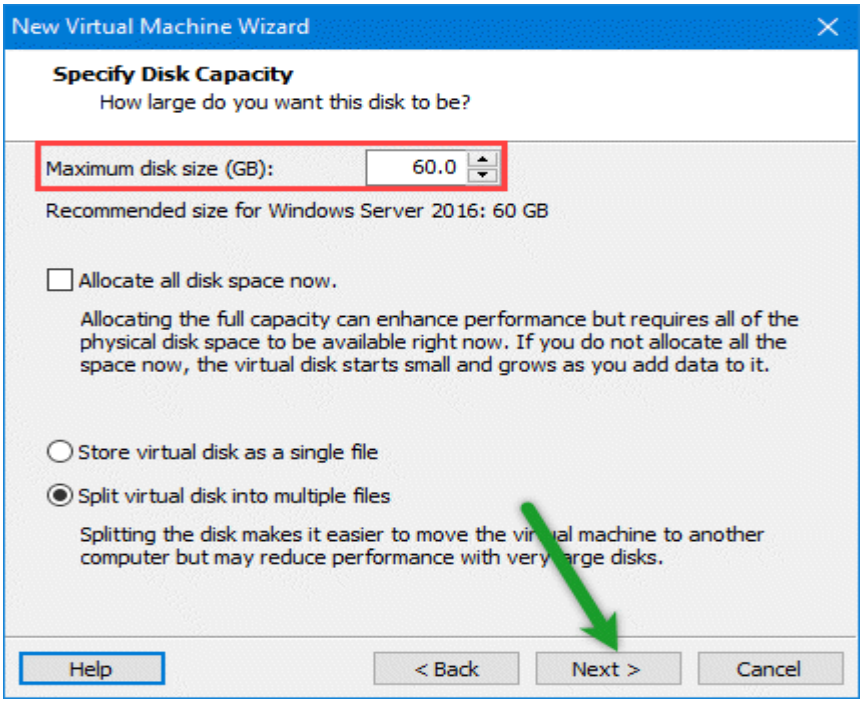
Step 10. Let the I/O Controller types by default because you don't have the option to change the SCSI type. just hit **Next**.



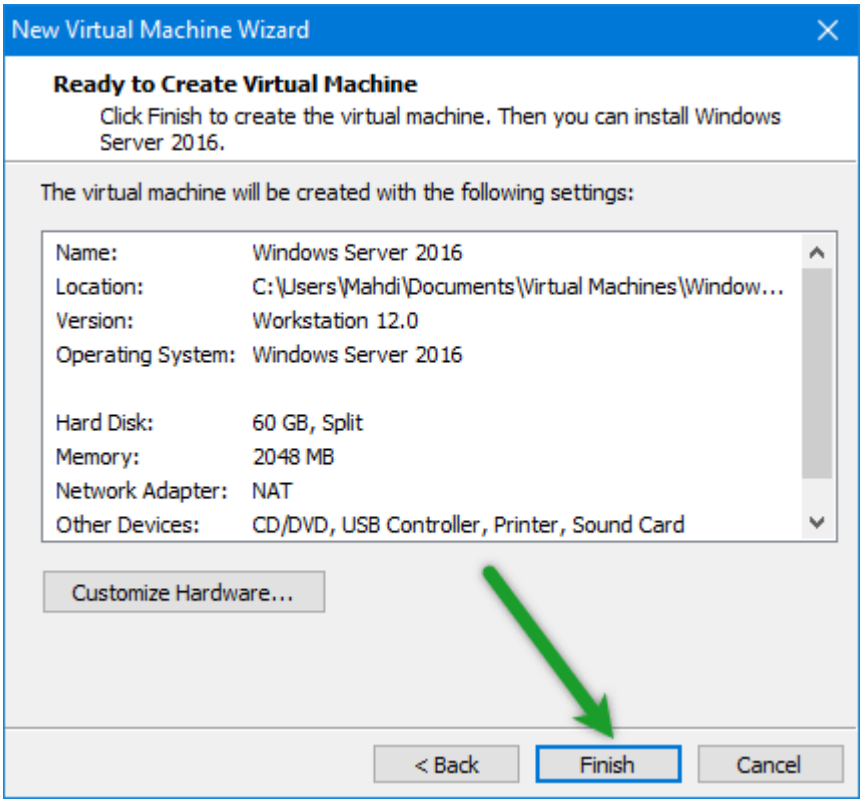
Step 11. Now to create new virtual disk, select **create a new virtual disk** for the virtual machine.



Step 12. Specify the **disk amount** by typing the disk size (Recommended 60 GB) and click on **Next** button.



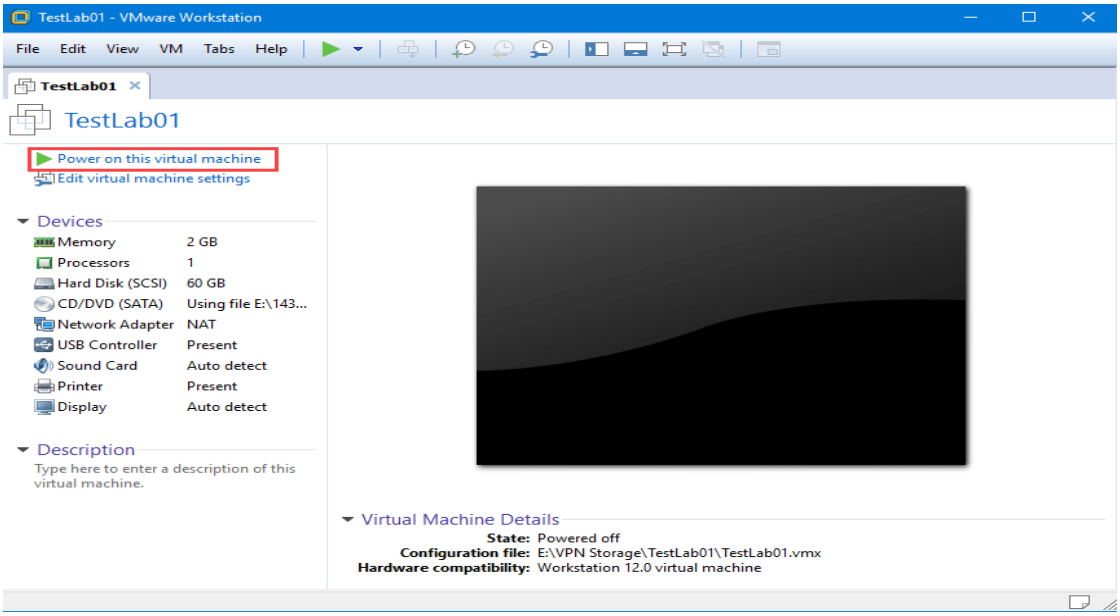
Step 13. At this point, just check out the settings you've done or you can customize if you want and click **Next**.



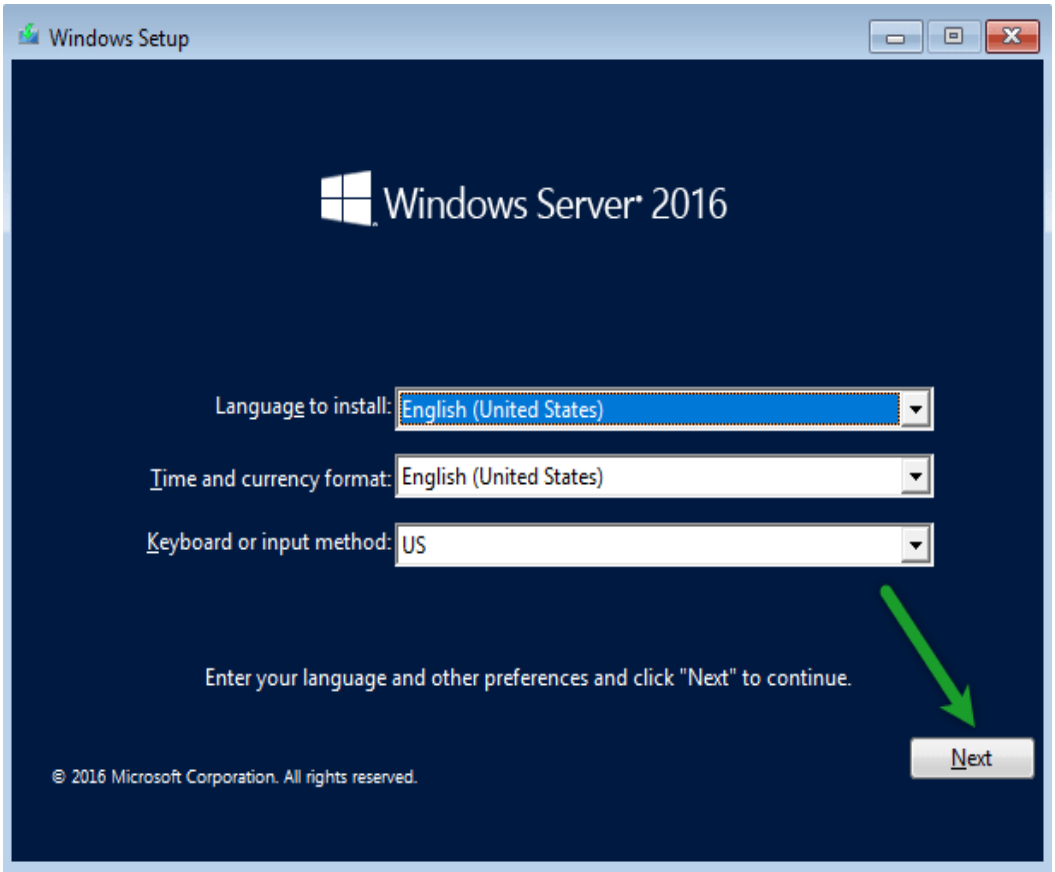
2.2. Install Windows Server 2016

Now it's time to boot up and start the virtual machine, just click on **Power on this virtual machine** then wait until it boots.

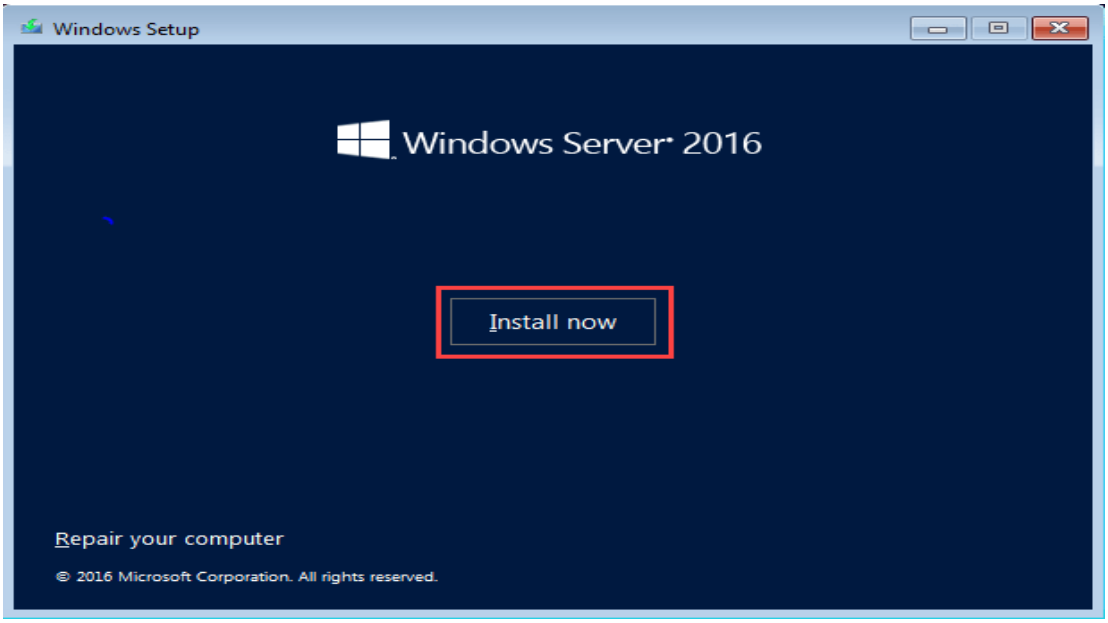
1. Open VMware Workstation on your host computer. Click on Power on this virtual machine in top left.



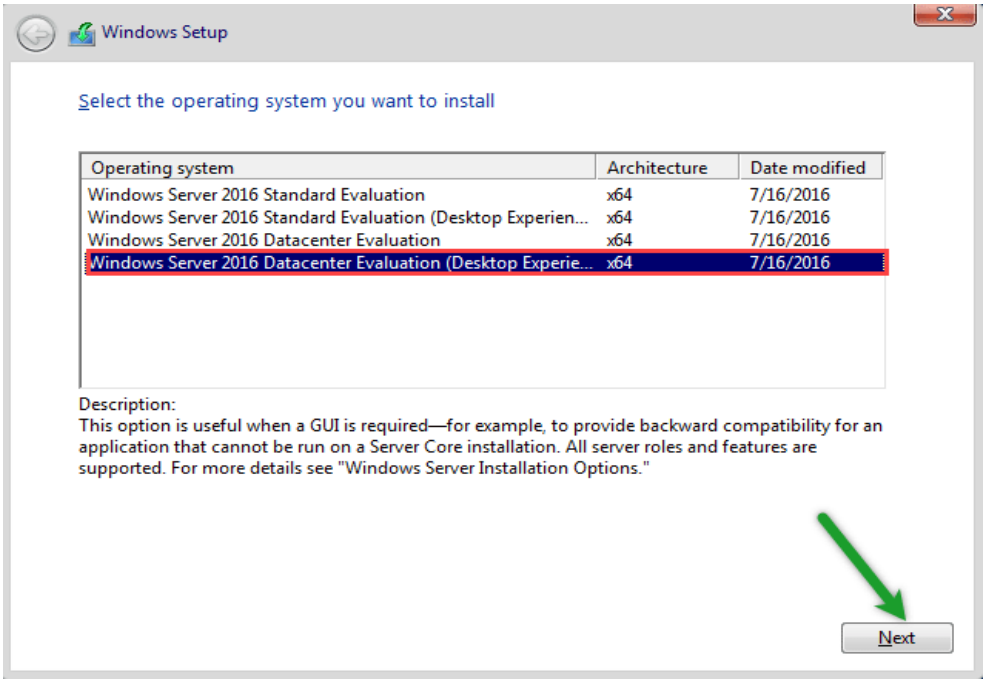
2. When the virtual machine powered on, specify the **language**, **time zone** and **keyboard** then click **Next**.



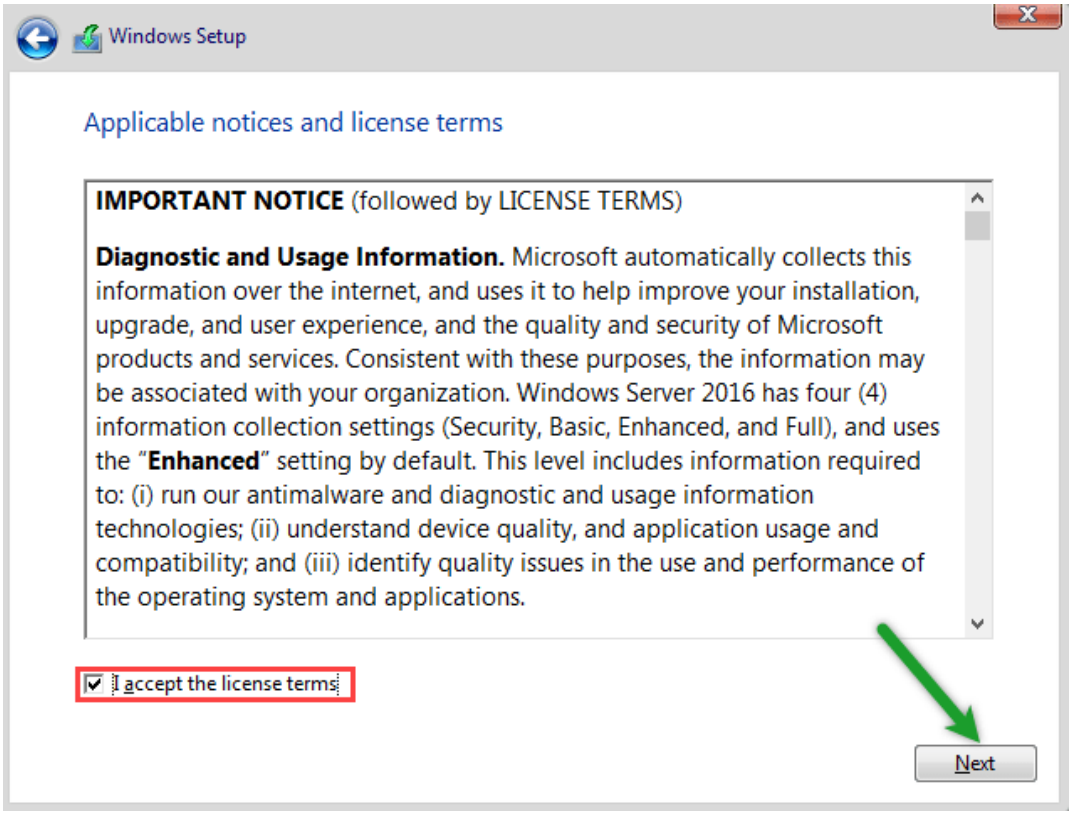
3. Install now to install the windows server 2016 on virtual machine.



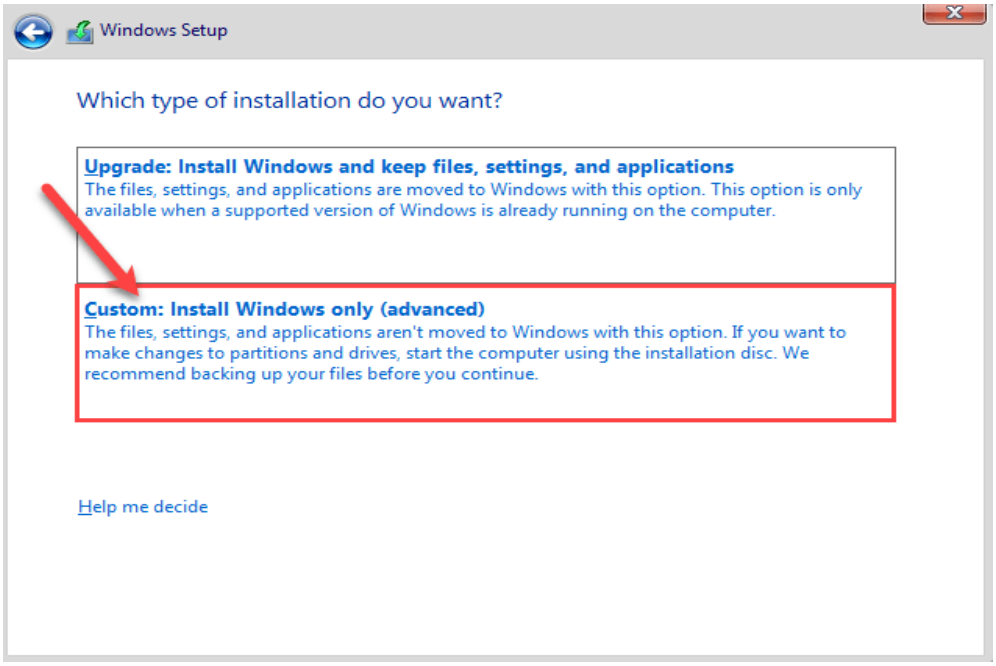
4. Select one the Windows Server editions you've decided and click on **Next** button.



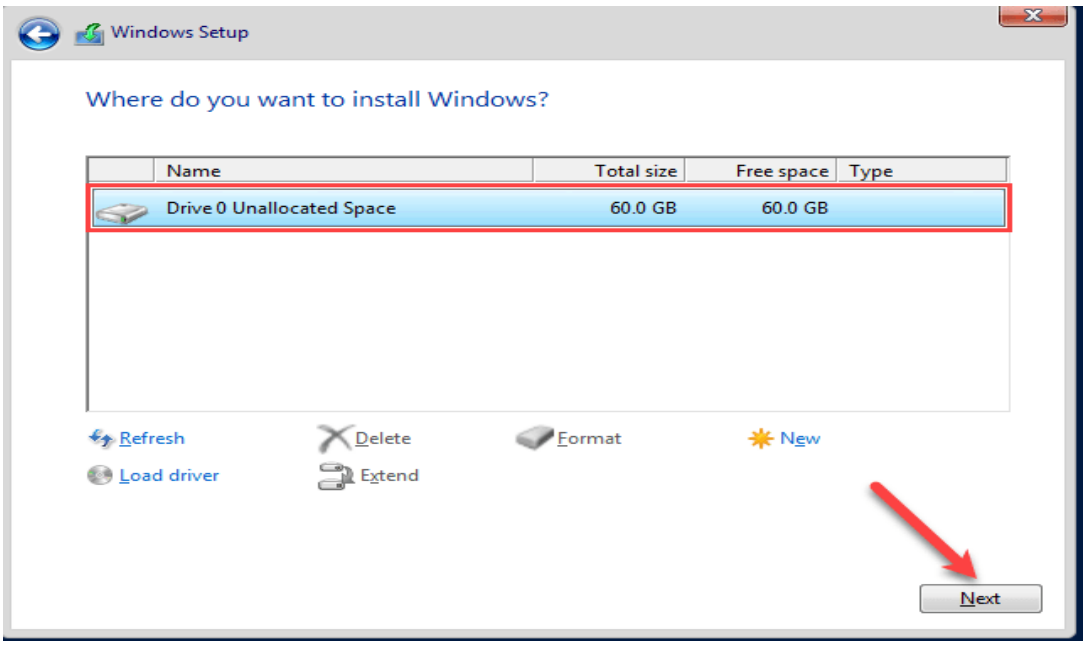
5. Put a mark in the box next to **I accept the license terms,** then click on the **Next** button.



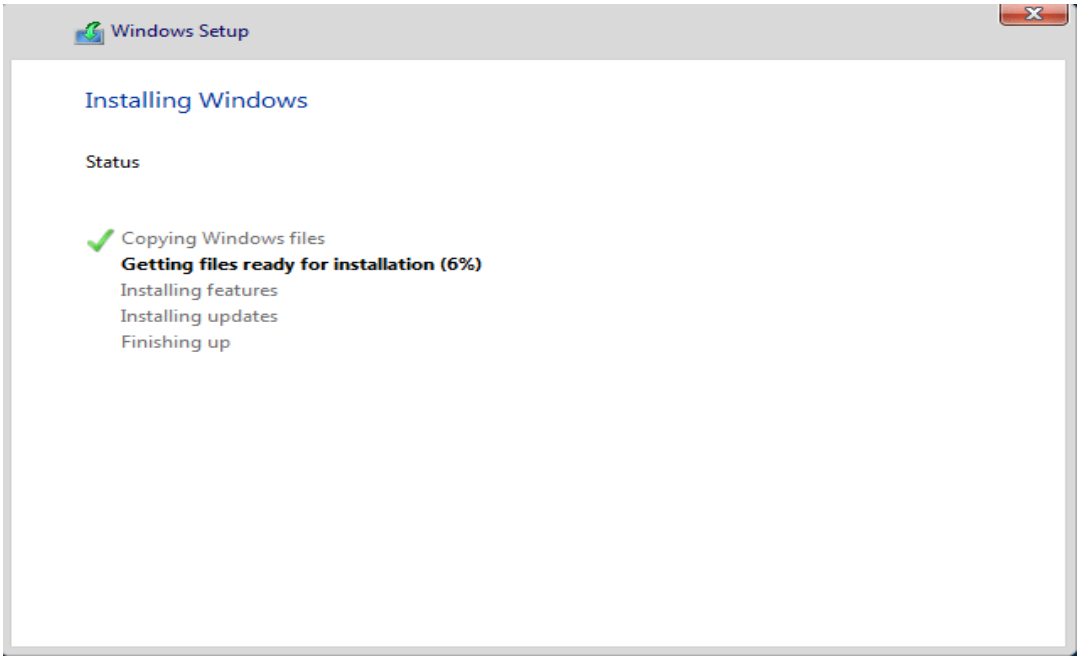
6. Go on and click on the **Custom: Install Windows only (Advanced)** option for installing the server custom.



7. Select the disk, you want to install the widows on and select the **disk**, click on **New**, then specify the amount (based on MB) and click on **Apply** button then click on **Next** button.

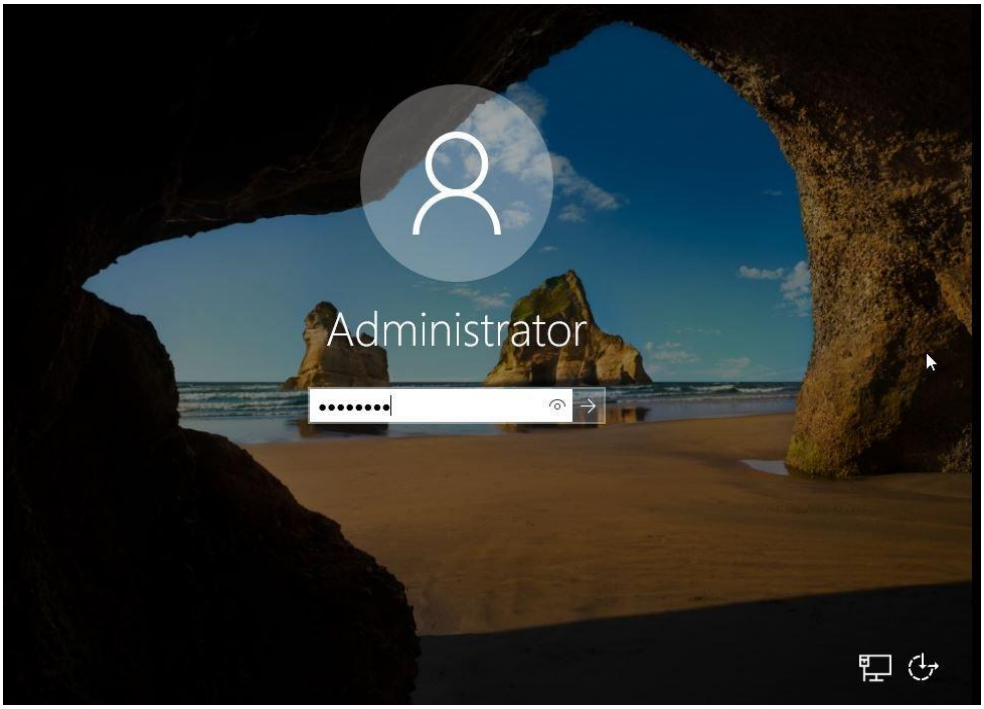


8. Now the server copies all the files to the disk, amount the files from the windows image, install features, updates, so it will take time and when finished it will reboot.

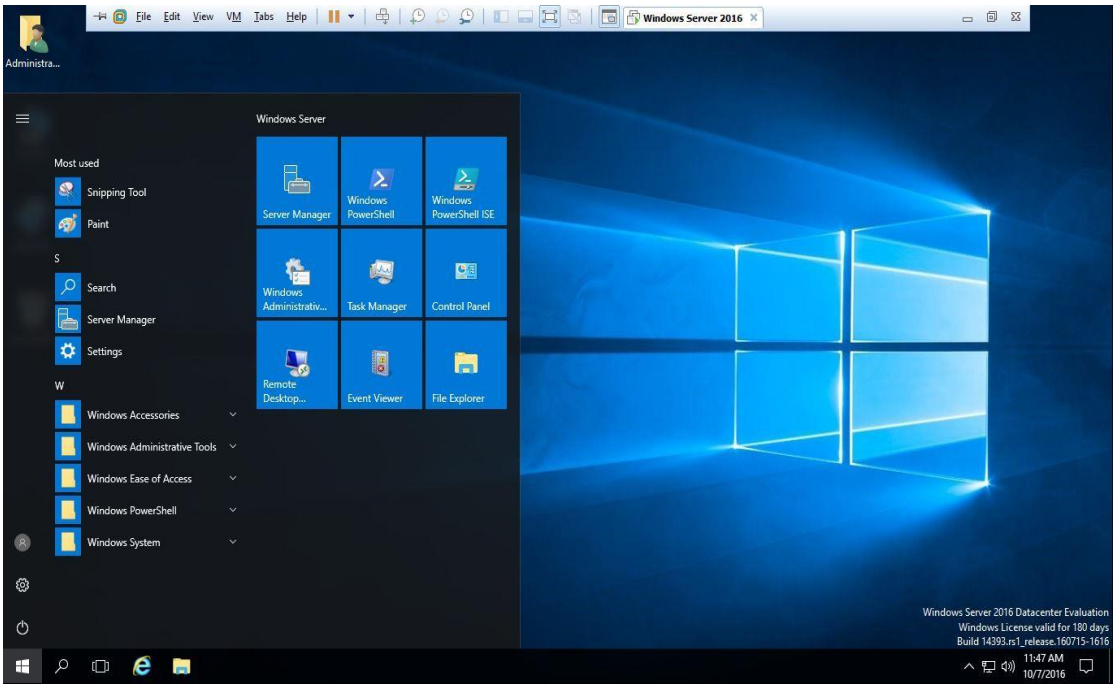


9. After the reboot, type a **complex password** composed of (uppercase, lowercase, symbols and numbers) and click on **Finish** button.

10. When the customization finished, now you'll need to sign in, but first click on the **button** that is composed of three buttons (**ctrl+alt+del**) shown in image below or simply press Ctrl+Alt+Del and sign in to Windows Server.



And that's it, after you have signed in, your windows server installation is completed like the shot below.



Points to Remember

- **Windows server installation methods:**

On Physical Machine, Clean Installation completely erases all existing data from the selected partition or drive, deal for new installations or when you want to start with a fresh system and Requires backing up any critical data before proceeding.

1. **Clean installation:** The most common option for virtual machines, as it creates a fresh installation of Windows Server on a new VHD file.
2. **Upgrade:** Only available if you are cloning an existing virtual machine with Windows Server installed.
3. **Consider your specific needs**: Determine whether you need a clean installation or an upgrade based on your goals and the existing configuration of your virtual machines.

- **Steps of installing windows server in physical machine:**

1. Insert a DVD or USB of Windows Server 2012 R2 into your system and start it.
2. Choose the language, time and currency format, keyboard or input method**.**
3. Click Install now
4 Choose the operating system you want to install
5. Click Custom : Install Windows only (advanced)
6. Create a new partition
7. Choose the drive other than Primary.
8. Upon reboot, provide an administrative password and click **Finish**

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

Practical Activity 1.3.3: performing network adapter configuration

Task:

1: Referring to the key reading 1.3.2 As networking and internet technology trainee, you are asked to go to the computer lab to lab to configure server network adapter.
2: Present the procedures of all step performed installation.
3: Present your work to the trainer and whole class.
4: Read key reading 1.3.3 and ask clarification where necessary
5: Perform the task provided in application of learning 1.3

Key readings 1.3.3: performing network adapter configuration

1. Physical Connection:

- **Ethernet Cable:** Ensure a secure connection between the server's network port and a network switch or router.
- **Fiber Optic Cable:** Use a fiber optic cable for longer distances or higher bandwidth requirements.

2. Access Network Settings:

- **Method 1: Control Panel**
  - Open the Control Panel.
  - Go to Network and Internet.

- Click Network and Sharing Center.
- Click Change adapter settings.

• **Method 2: Settings App**

- Open the **Settings** app.
- Go to **Network & Internet**.
- Click **Ethernet** or **Wi-Fi** (depending on your connection).

How to configure network settings in Windows Server 2016

Configuring network settings is one of the first steps you will need to take on Windows Server 2016. Whether you are using the GUI or Core version, changing the IP address, Subnet Mask, Default Gateway, and DNS Servers can be done in different ways depending on the case.

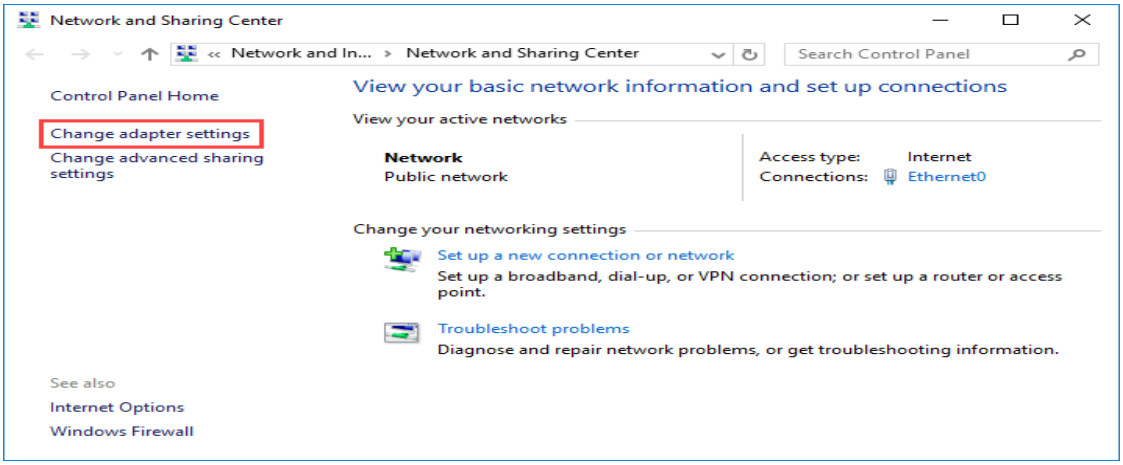
In today's article, you will see how to change the basic IPv4 network settings for your machine's adapters using the GUI, PowerShell, SConfig, and command prompt.

Configure network settings using the graphical user interface

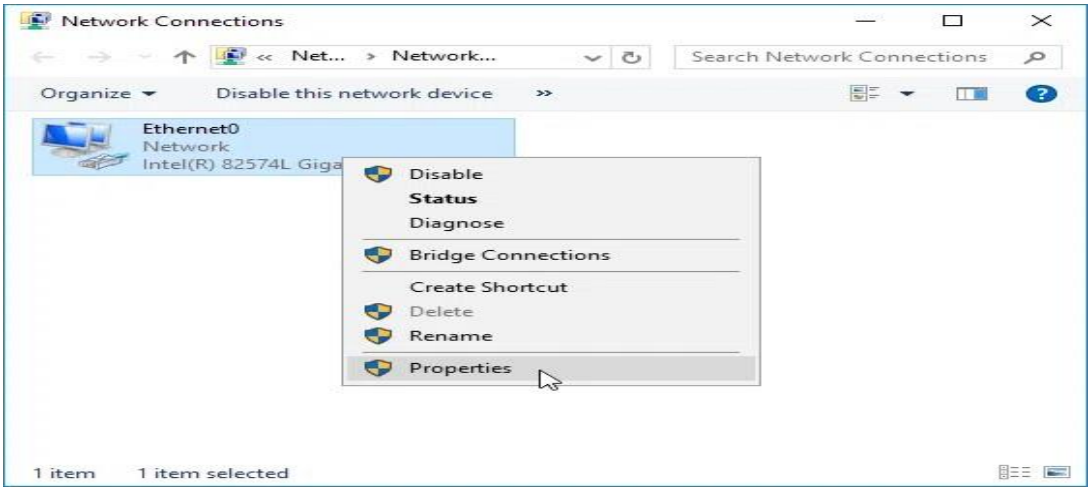
Ok, the process is more than simple, but I mention it to make the article more complete.

Right-click the network icon in the notification area, and then click **Open Network and Sharing Center**.

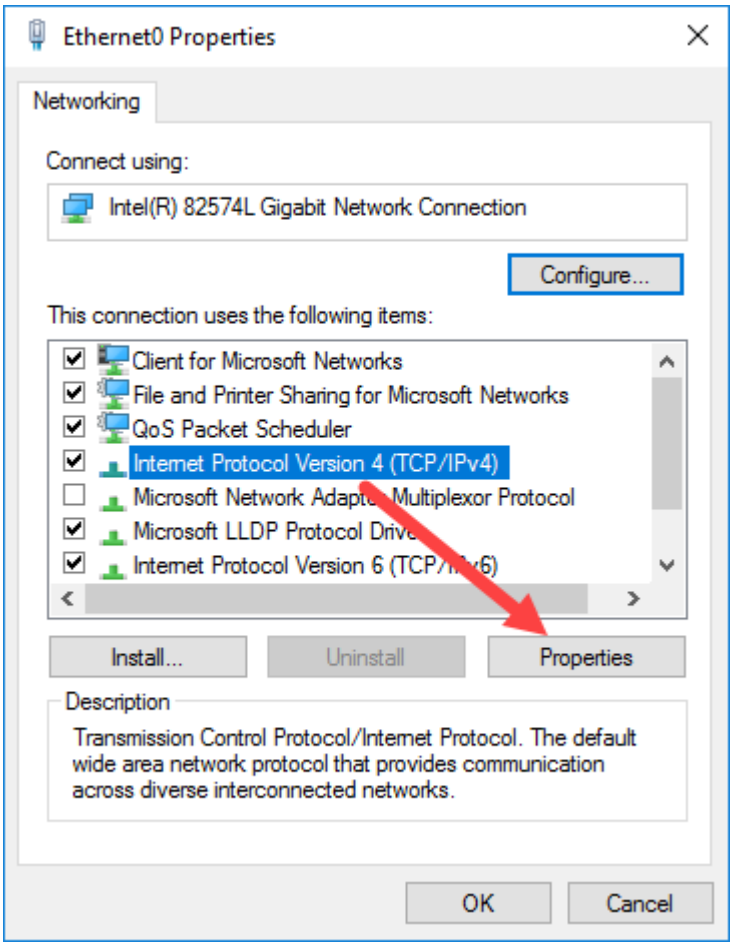
In the window that opens, click **Change adapter settings** to display the available network adapters of the machine.



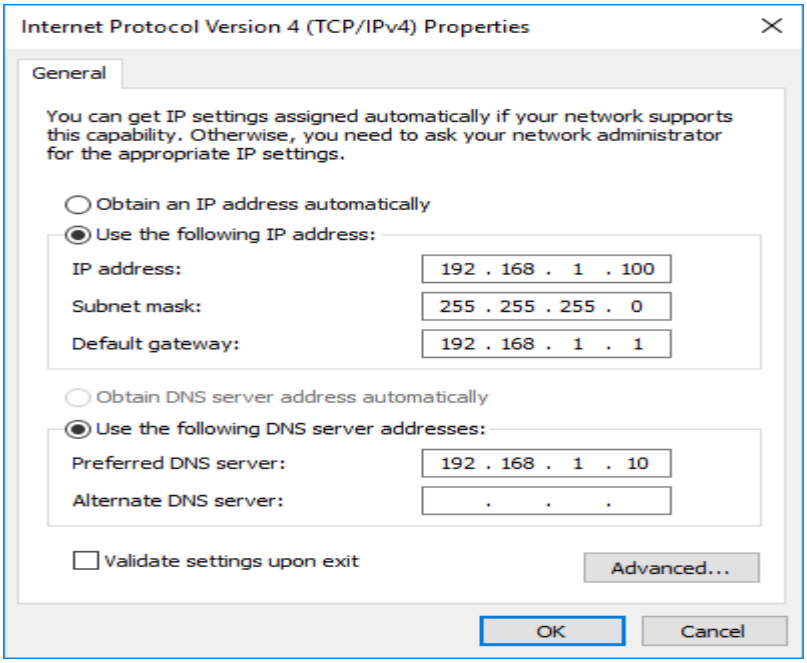
Right-click the adapter you are about to change the IP settings and then click **Properties**.



Click **Internet Protocol Version 4 (TCP / IPv4)** and then the **Properties** button.



Here, enable Use the following IP address and enter the static IP addresses for the server, subnet mask, default gateway and DNS servers.



3. Network sharing and Discovery

Windows Server handles a protocol called Network Discovery. In fact, as its name indicates, it allows you to see or find other computers and network devices. Additionally, it allows other computers on the network to see the server. However, the system may fail to detect other computers on the network. This circumstance is burdensome since it can affect the normal development of the system. Consequently, let's see how to activate network discovery in Windows Server 2019/2016

How to enable network detection in Windows Server 2019/2016.

Network discovery has three basic levels of configuration:

- **Enable:** This option allows the server to view other computers and devices on the network. In addition, let others see the active server
- **Disable:** This option prevents both seeing other devices on the network and others from seeing our server.
- **Customized:** With this option, we can adjust the settings associated with network discovery in order to allow only some of them.

we will enable definitively the network detection in Windows Server 2019/2016. Well, if you've come this far, it's because when you go to the file browser, the network detection has generated an error. But don't worry, let's see how we can fix this problem. First, it is necessary to enter the network settingsWindows Server handles a protocol called Network Discovery. In fact, as its name indicates, it allows you to see or find other computers and network devices. Additionally, it allows other computers on the network to see the server. However, the system may fail to detect other computers on the network. This circumstance is burdensome since it can affect the normal development of the system.

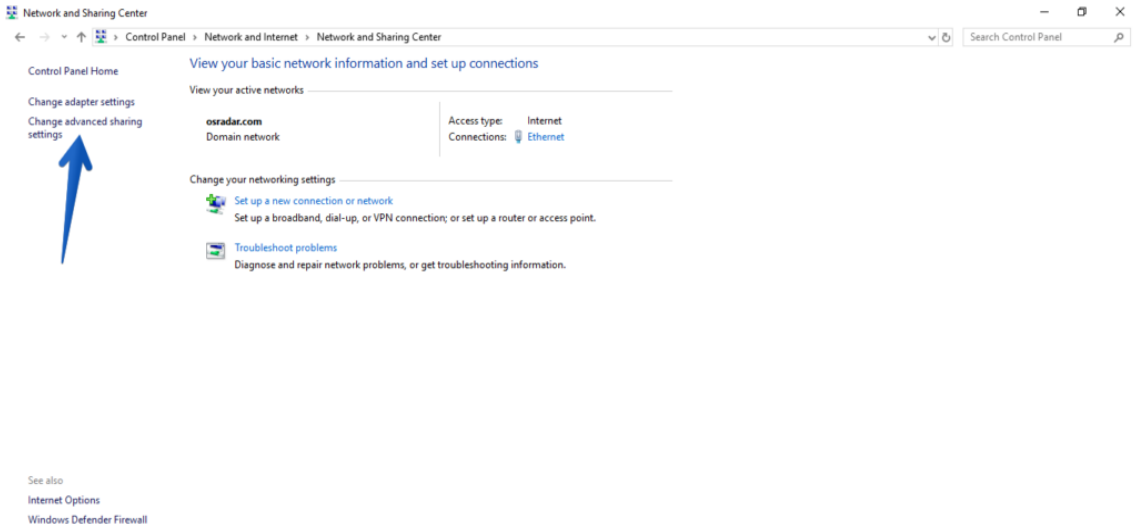
Consequently, let's see how to activate network discovery in Windows Server 2019/2016

How to enable network detection in Windows Server 2019/2016.

Network discovery has three basic levels of configuration:

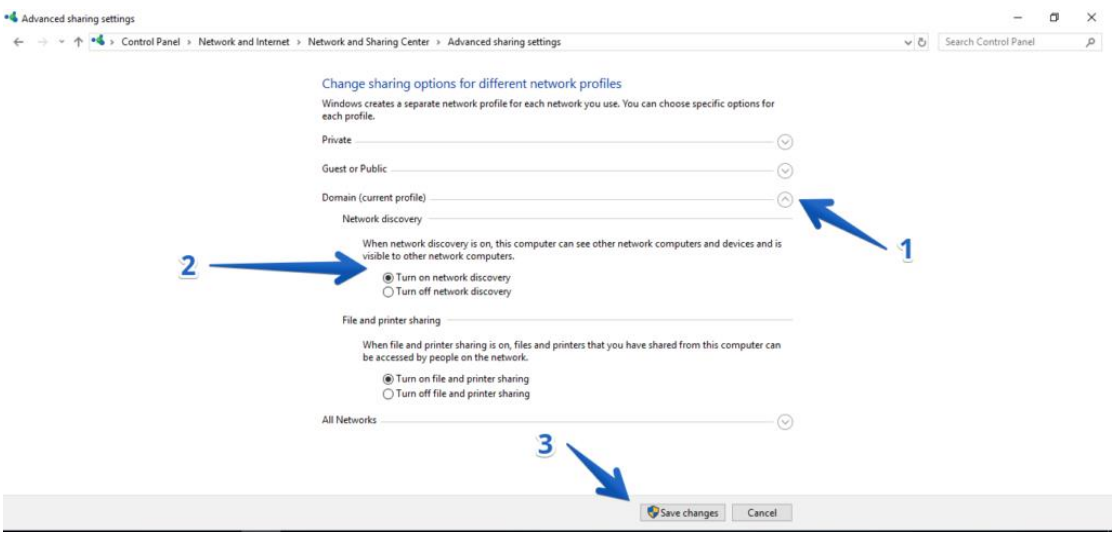
- **Enable:** This option allows the server to view other computers and devices on the network. In addition, let others see the active server
- **Disable:** This option prevents both seeing other devices on the network and others from seeing our server.
- **Customized:** With this option, we can adjust the settings associated with network discovery in order to allow only some of them.

In this opportunity, we will enable definitively the network detection in Windows Server 2019/2016. Well, if you've come this far, it's because when you go to the file browser, the network detection has generated an error. But don't worry, let's see how we can fix this problem. First, it is necessary to enter the network settings. With this in mind, follow the next path: Control Panel>Network and Internet>Network and Sharing Center. Once there, please click on Change advanced sharing settings.



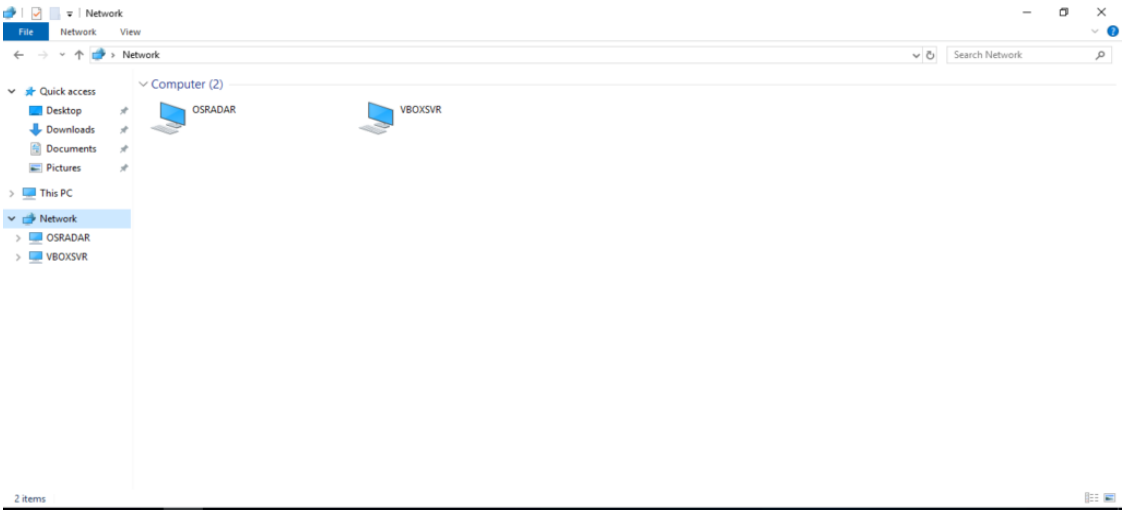
Go to network settings

In the next window, display the *Domain* section. Once there, check the *Enable network* detection box. Then click on *Save changes*.



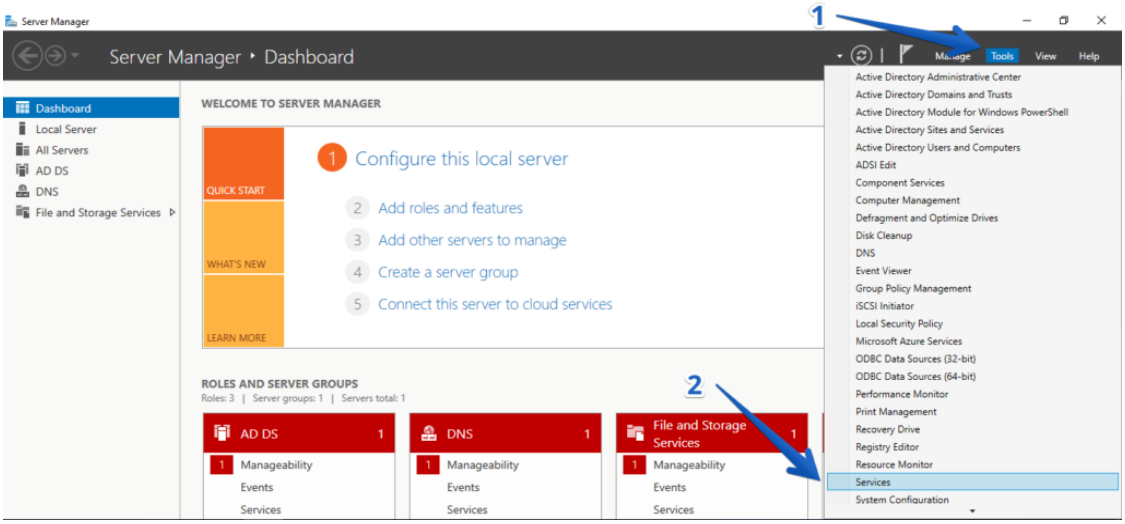
Please turn on the network discovery.

Now, go to the file browser and verify that devices are detected on the network.



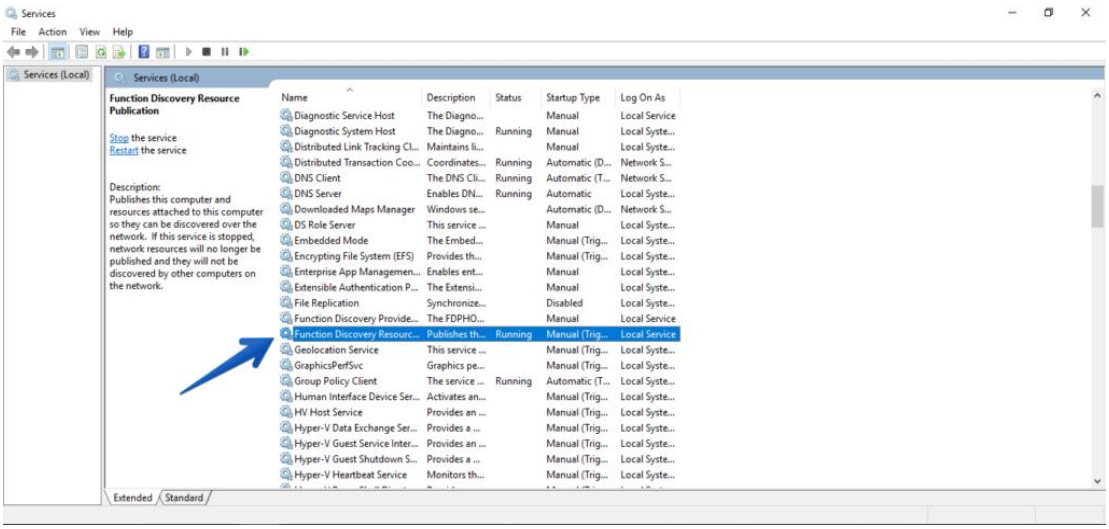
Activate services to improve network detection.

It is our intention, that your Windows Server works in an optimal mode. Therefore, we will give you some tips to ensure the optimal functioning of network discovery. With that intention, it is necessary to activate some services. For them, from the Dashboard go to *Tools* and from there select *Services.*

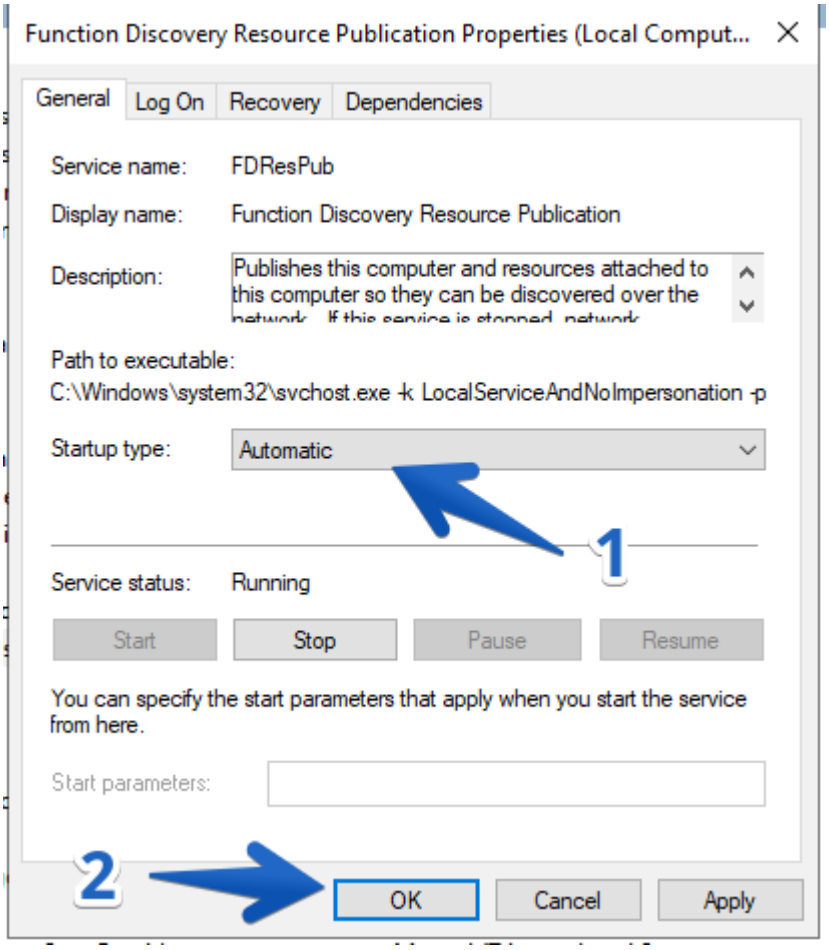


Go to Services

Now locate a service called Function Discovery Resource Publication

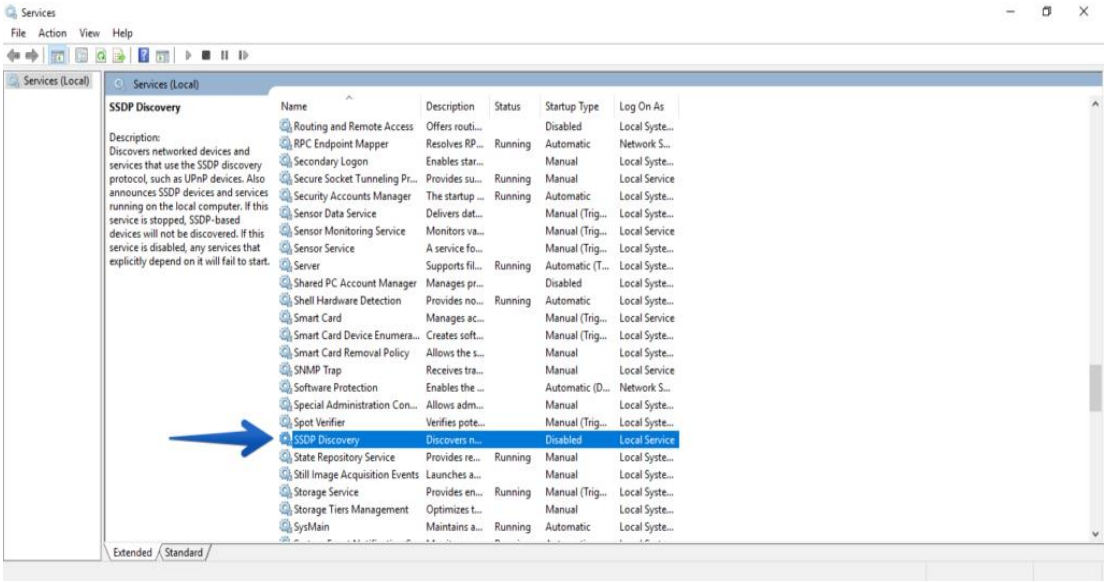


Then double-click on the service. Now in the *Startup Type*, set it to *Automatic*. Finally, click on OK.

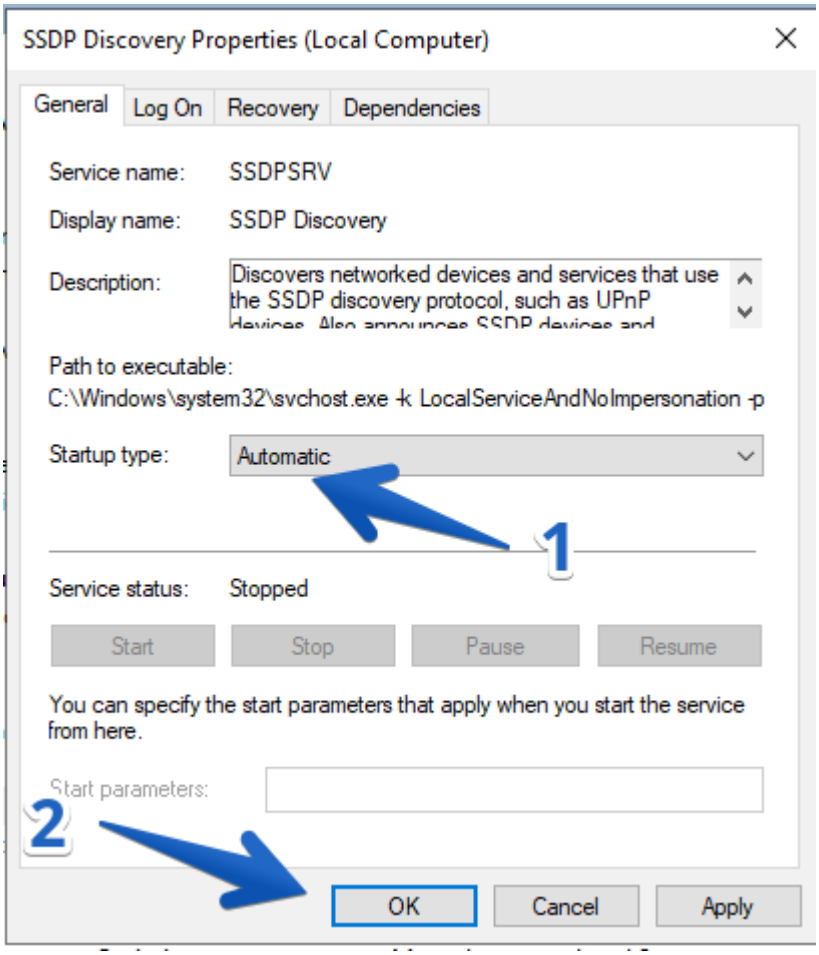


Sets the startup type to Automatic

Now locate a service called *SSDP Discovery*.

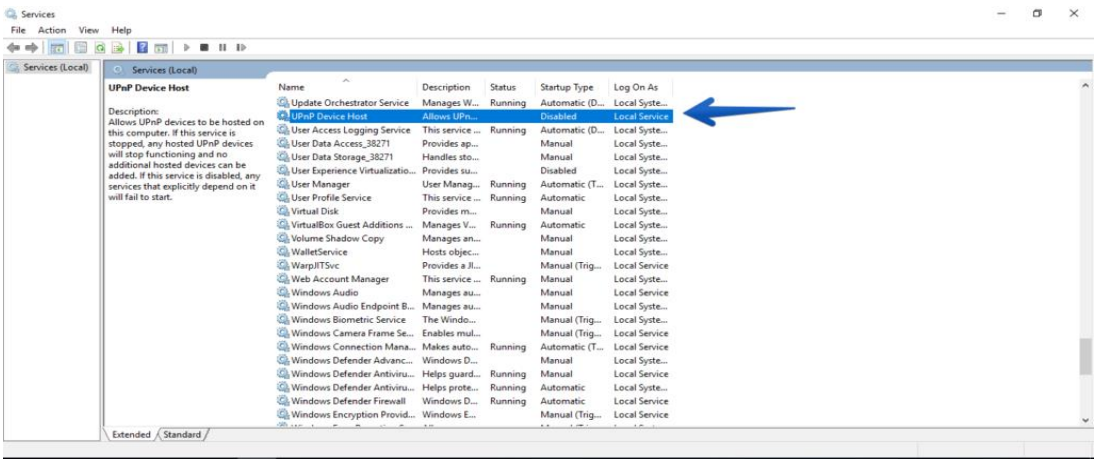


Next double-click on the service. Now in the *Startup Type*, set it to *Automatic*. Finally, click on OK.

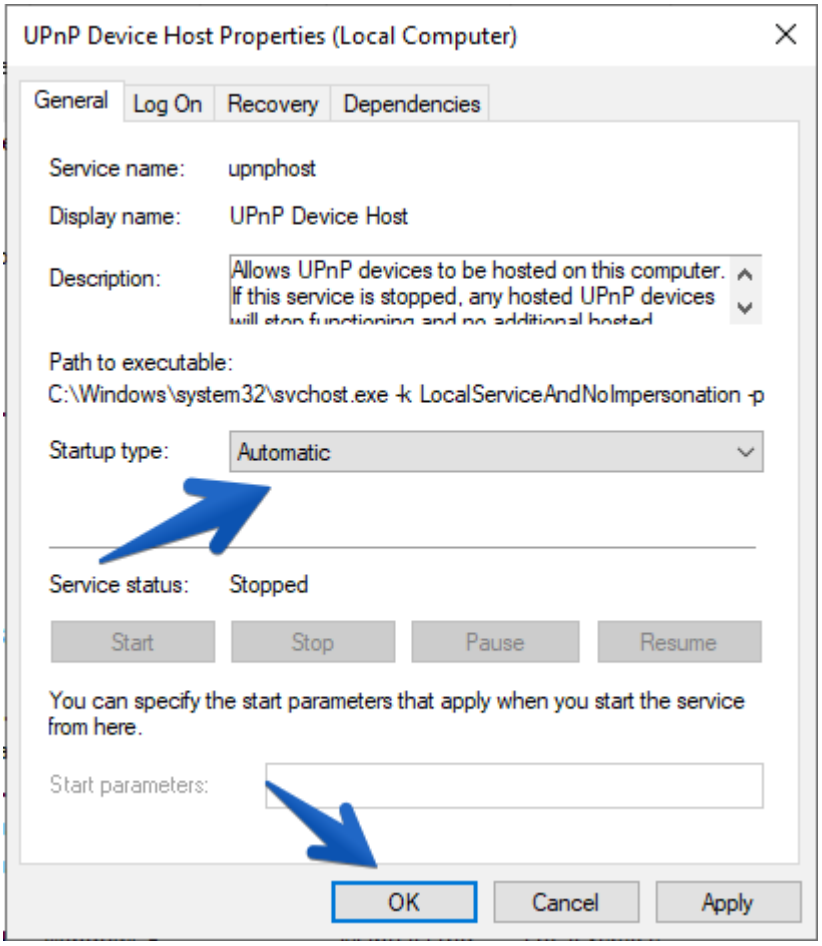


Sets the startup type to Automatic

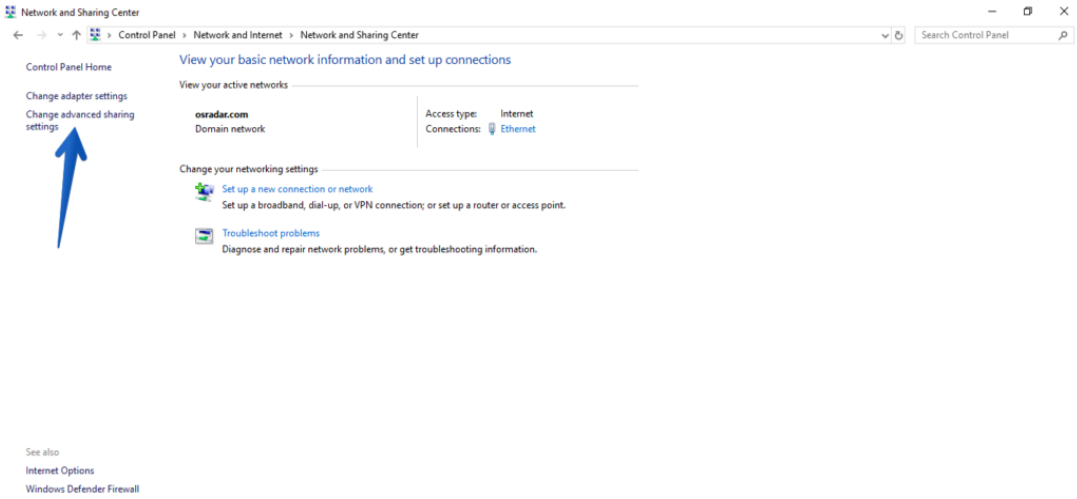
Then locate a service called UPnP Device Host.



Next double-click on the service. Now in the Startup Type, set it to Automatic. Finally, click on OK.

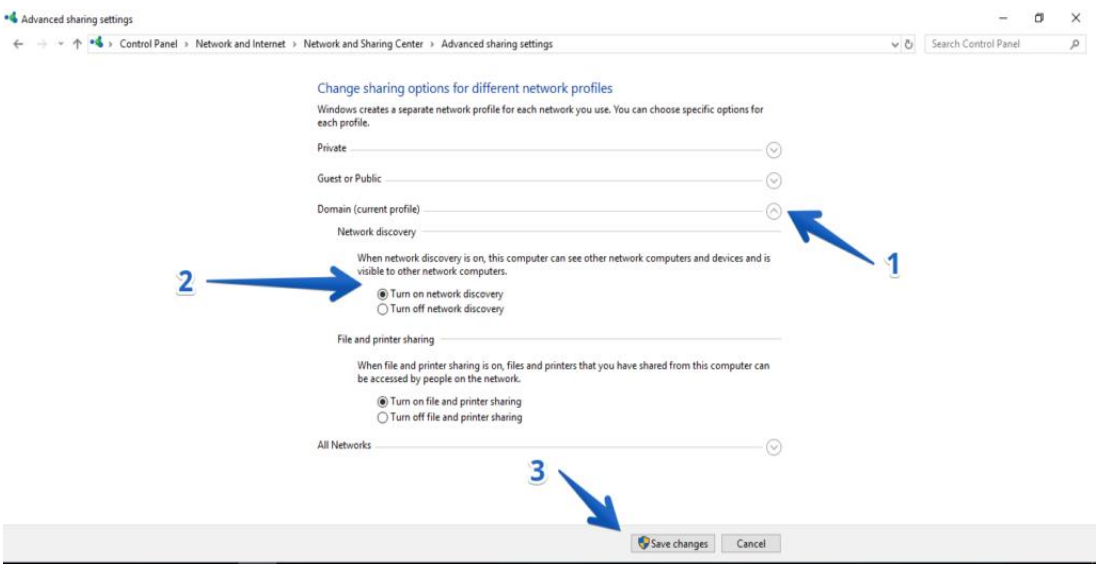


Internet>Network and Sharing Center. Once there, please click on Change advanced sharing settings.

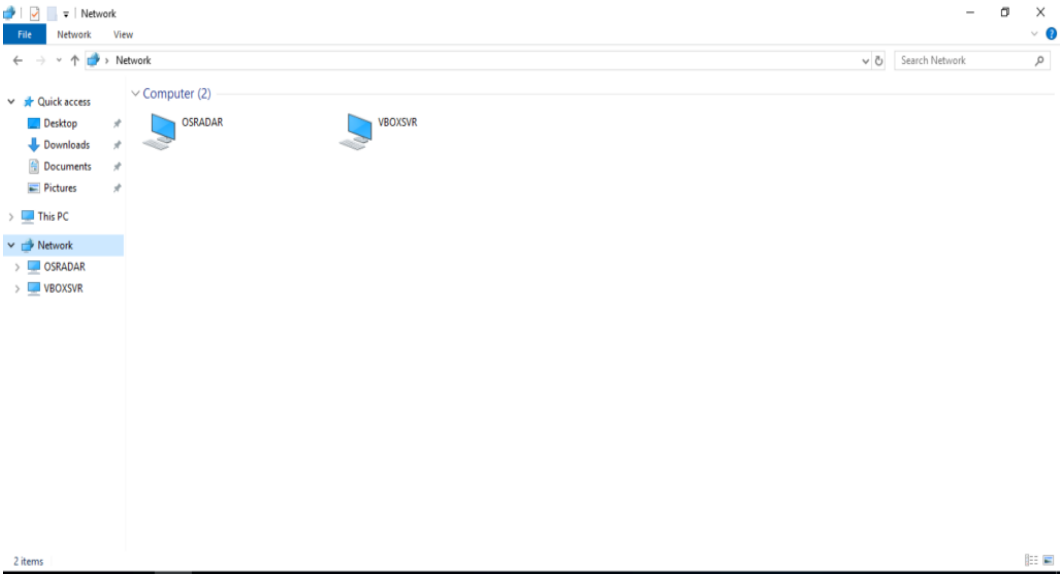


Go to network settings

In the next window, display the Domain section. Once there, check the Enable network detection box. Then click on Save changes.

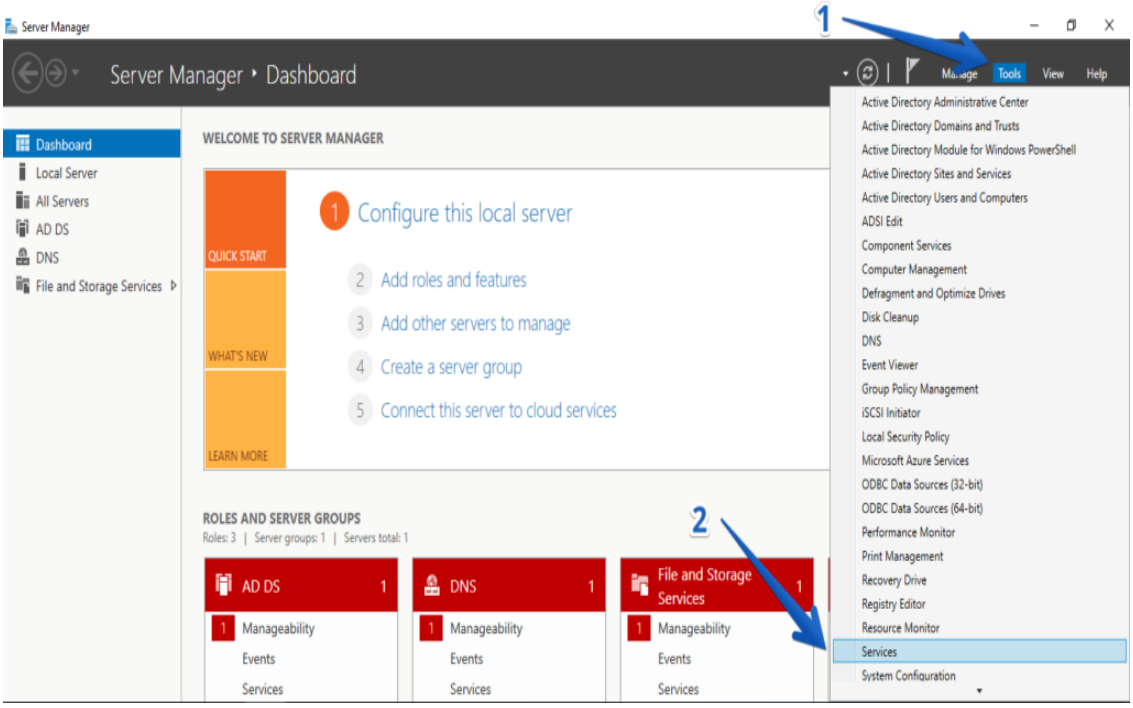


Please turn on the network discovery. Now, go to the file browser and verify that devices are detected on the network.



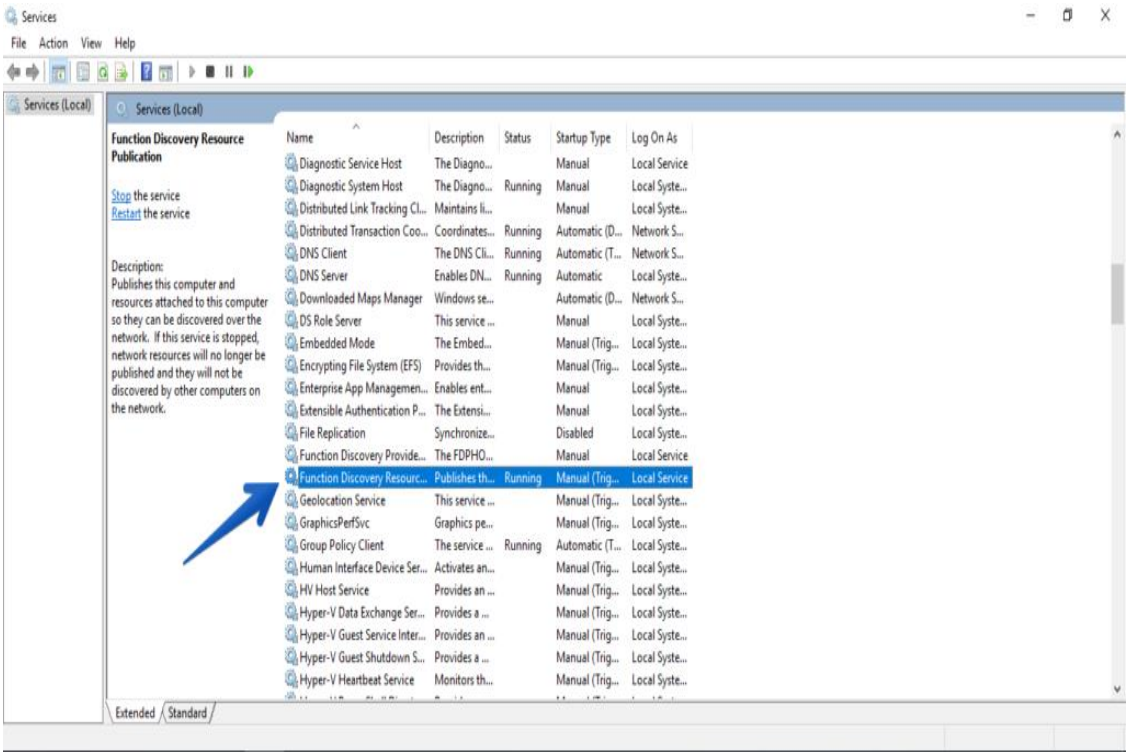
Activate services to improve network detection.

It is our intention, that your Windows Server works in an optimal mode. Therefore, we will give you some tips to ensure the optimal functioning of network discovery. With that intention, it is necessary to activate some services. For them, from the Dashboard go to Tools and from there select Services.

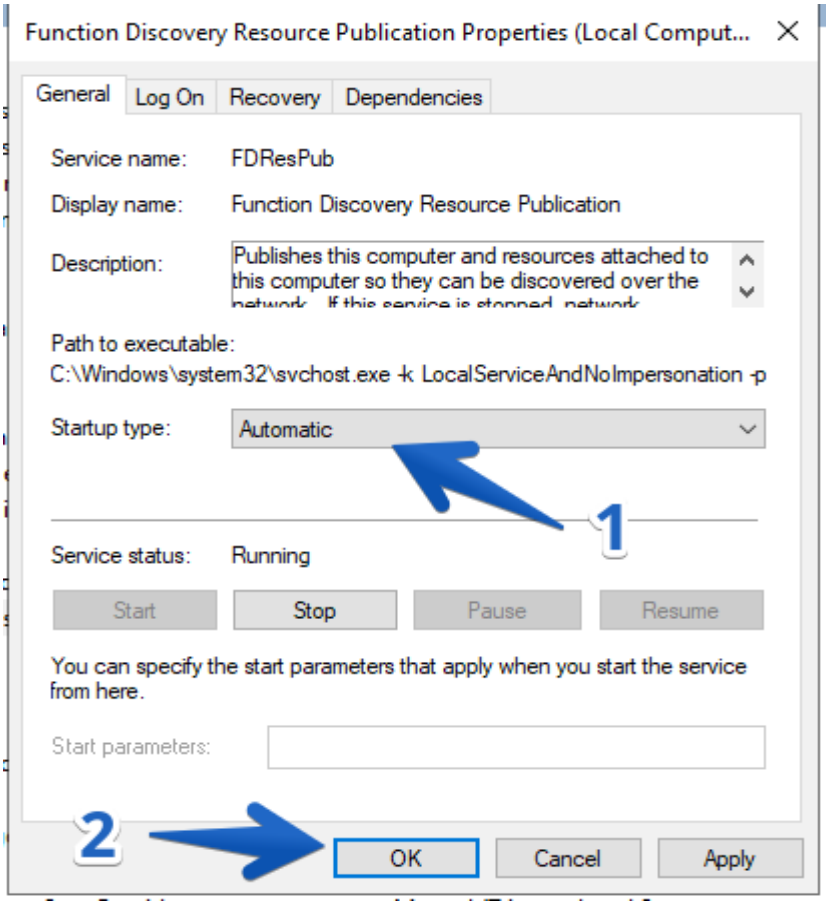


Go to Services

Now locate a service called Function Discovery Resource Publication

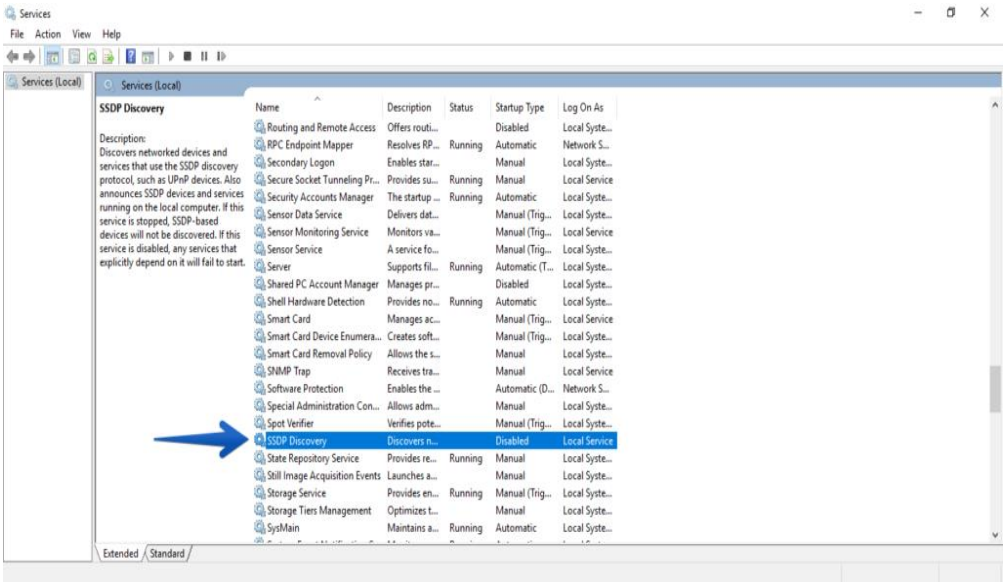


Then double-click on the service. Now in the Startup Type, set it to Automatic. Finally, click on OK.

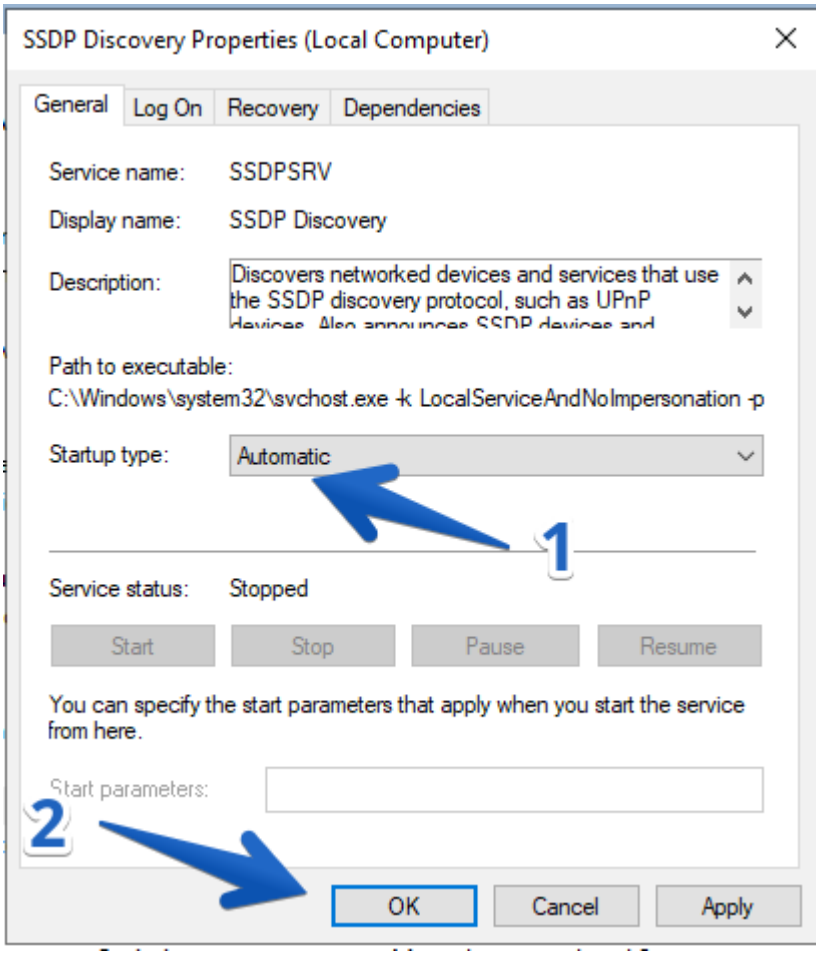


Sets the startup type to Automatic

Now locate a service called SSDP Discovery.

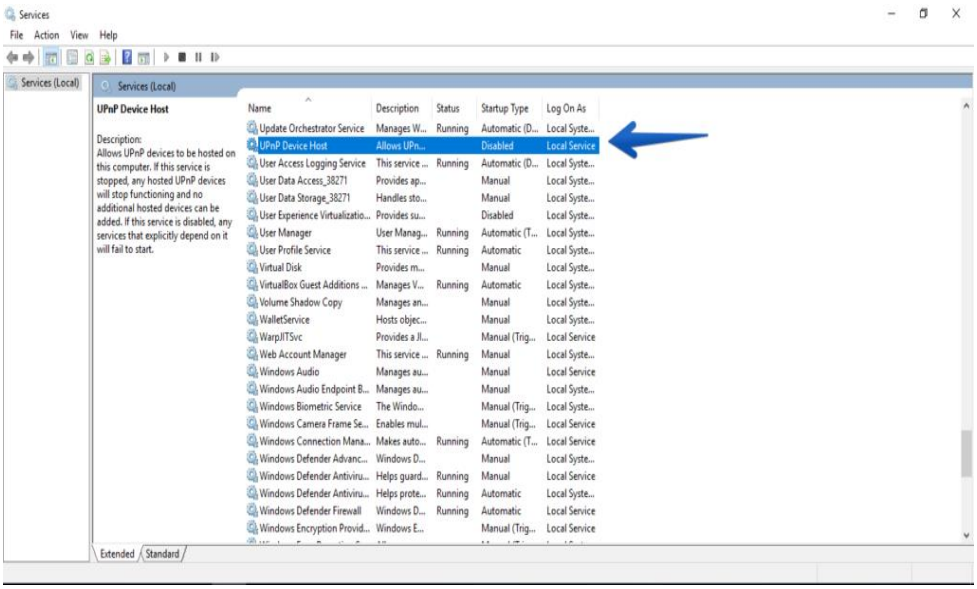


Next double-click on the service. Now in the Startup Type, set it to Automatic. Finally, click on OK.

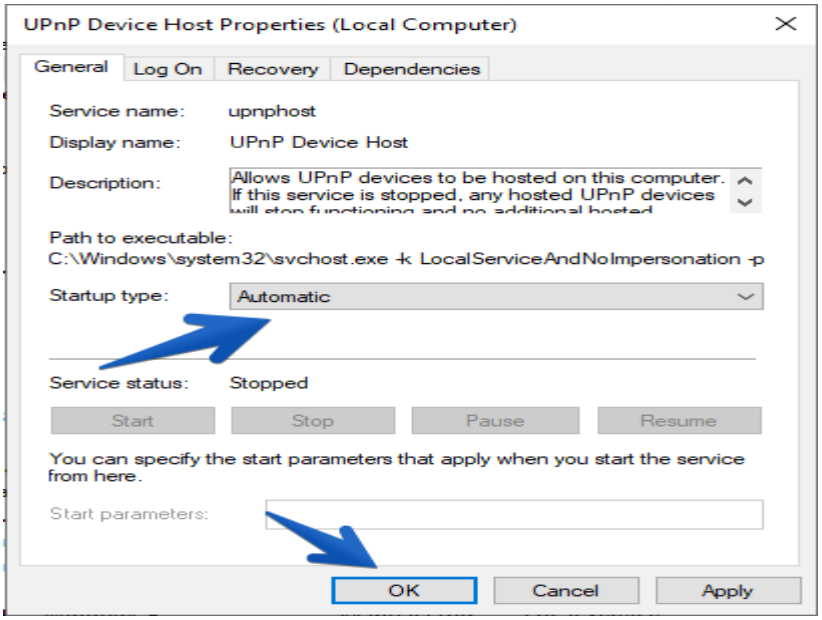


Sets the startup type to Automatic

Then locate a service called UPnP Device Host.



Next double-click on the service. Now in the Startup Type, set it to Automatic. Finally, click on OK.



4. Assign an IP Address:

➢ **Static IP Address (DHCP):**

- Right-click on the network adapter and select **Properties**.
- Double-click on **Internet Protocol Version 4 (TCP/IPv4)**.
- Select **Use the following IP address**.
- Enter the IP address, subnet mask, default gateway, and preferred DNS server addresses.
- Click **OK**.

➢ **Dynamic IP Address (DHCP):**

- Right-click on the network adapter and select **Properties**.
- Double-click on **Internet Protocol Version 4 (TCP/IPv4)**.
- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Click **OK**.

5.Firewall and Security

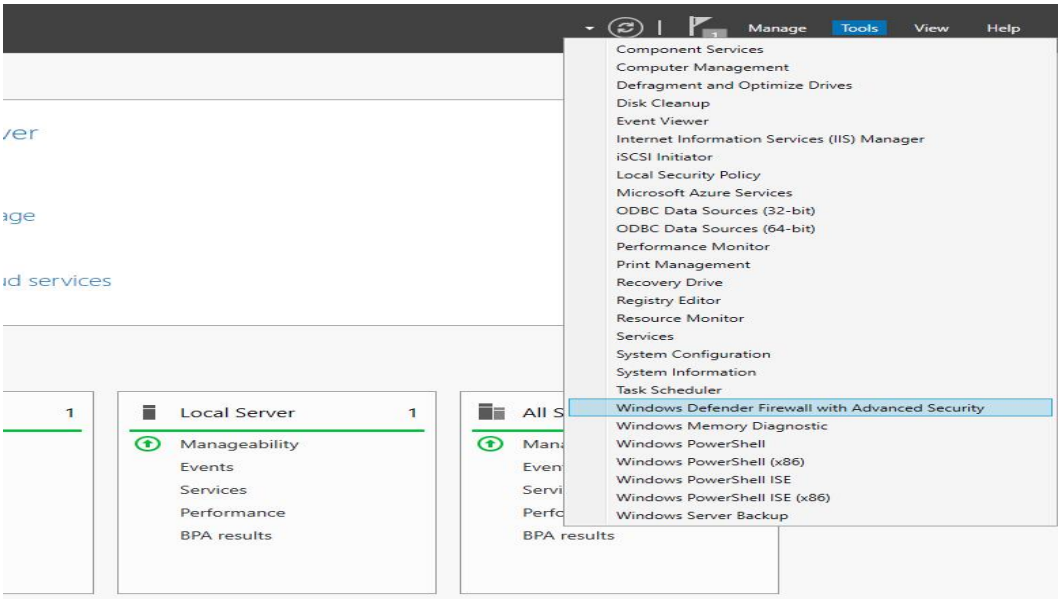
Prerequisites

- Deploy a Windows Server 2019 Instance on Vultr
- A Remote Desktop Connection App

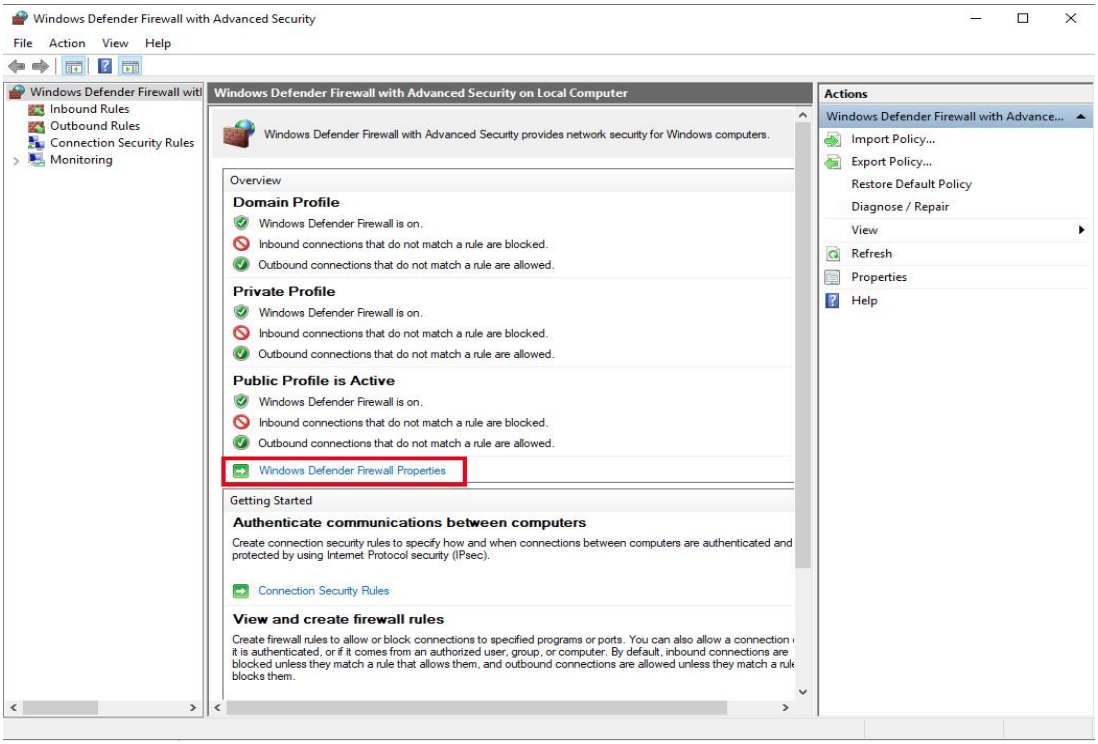
Establish a connection to your server by logging in through any remote desktop app or click the console on your Vultr dashboard to access your server. After you connect, you can start configuring your Windows server 2019 firewall rules.

Turn Windows Firewall ON

By default, Windows Defender Firewall is turned on, but in any case, you should confirm the current status and turn on firewall. To do this, click the tools node under server manager and select Windows Defender Firewall with Advanced Security from the drop down list.



From the open group policy management window, check the current status of Windows Firewall profiles if it is set to ON; otherwise, click the Windows Defender Firewall properties option and turn the service on per profile.



firewall Rules

Windows Firewall rules allow you to either permit or block specific incoming and outgoing network packets on your server. You can choose multiple parameters for each inbound or outbound rule. A rule can consist of a TCP or UDP port, program name, service, or a protocol to filter for every server profile.

Windows server profiles are grouped into, Domain, Private and Public. Domain represents your server's connection to a corporate domain

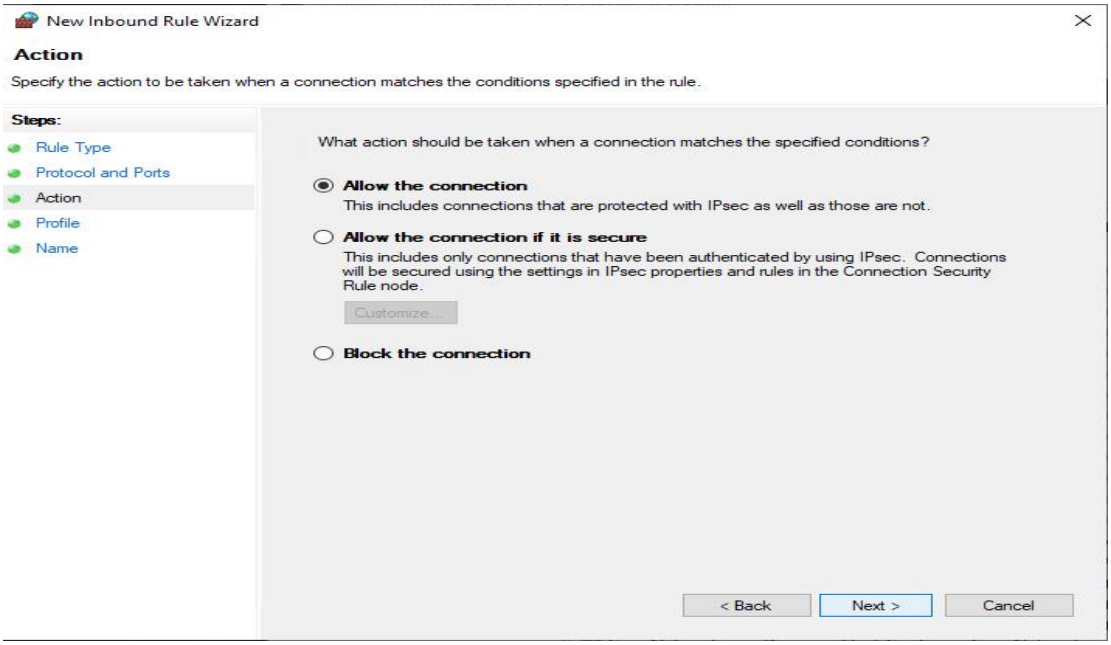
network, *Private* applies to your home or workplace network connection, and *Public* represents non-secure public network locations.

Open an Inbound Port (Incoming connections)

Launch windows defender firewall from the tools sub-menu under server manager. Then, select Inbound Rules on the left panel of the Firewall console.

A list of current rules will be displayed. Now, on the left Inbound Rules sub-menu under actions, click New Rule.

Define your TCP or UDP port rule.



- Allow the connection will allow incoming connections to the specified server port
- Allow the connection if it is secure will authenticate with IP security and either deny or allow the connection. For example, https connections will be allowed and http blocked.
- Block the connection will block all incoming connections to your server through the specified port

In this case, choose Allow the connection to open the port.

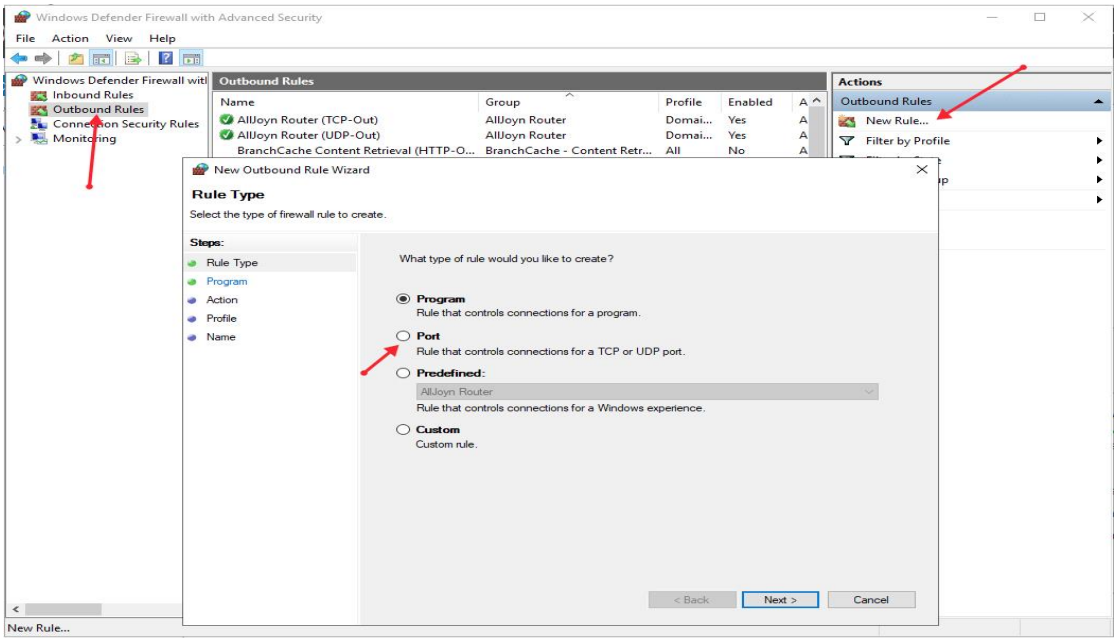
Click Next to assign the new rule to one or more profiles. You can select between Domain, Private, and Public, or choose all to apply the firewall rule on multiple profiles.

Next, give your new firewall rule a custom name and description for easy identification. Then, Click finish to enable the new rule. Your new Inbound (Incoming) port rule will be enabled, and all connections to the server that match the port will be accepted.

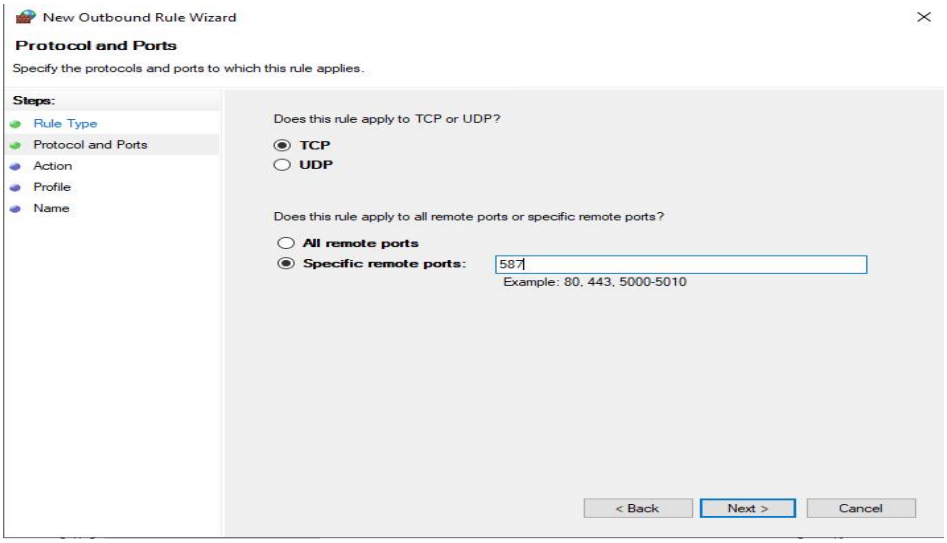
Open an Outbound Port (Outgoing connection)

From the Windows Defender Firewall console, click Outbound Rules on the left pane, and a list of available outgoing connection rules will be displayed.

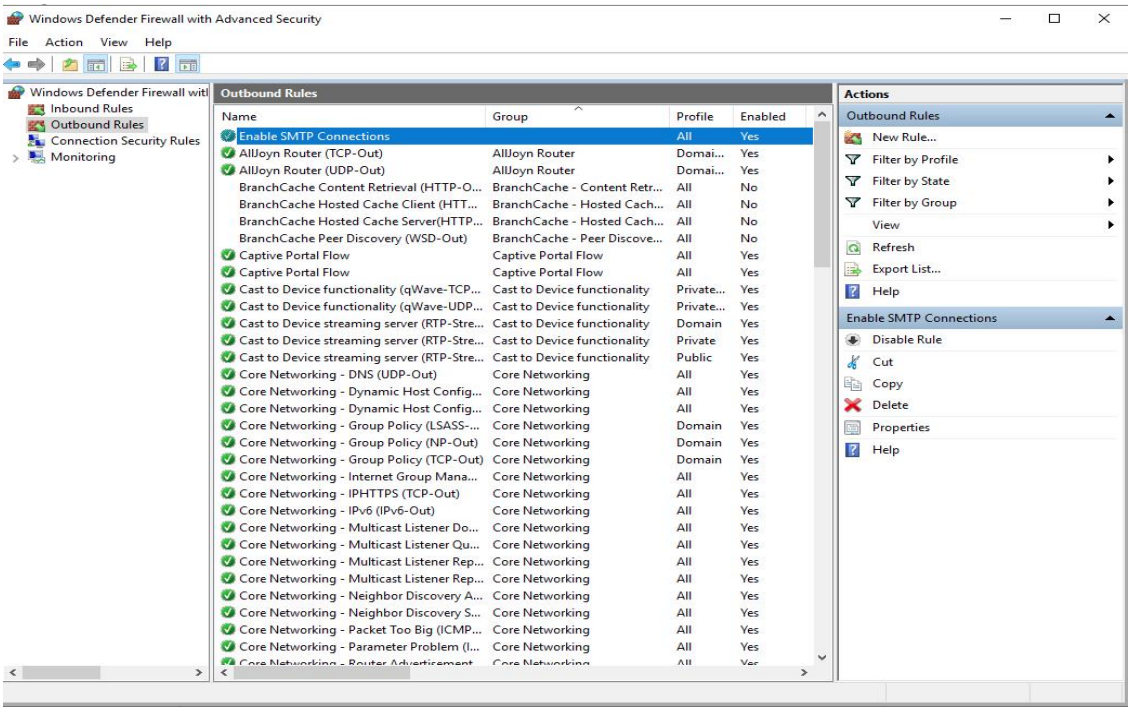
Now, click New Rule on the right pane under the outbound rules node.
In the new outbound rule wizard, select *Port* as the rule type and click Next.



Now, let's choose whether the new rule applies to a TCP or UDP port. Then, select specific remote ports and enter the target server port number; you can enter a range of ports, a single port, or multiple different ports you intend to open.



Next, on the Action page, select Allow the connection, then click next to select the server profile on which the rule should be enabled.
Give the new outbound rule a name and description that uniquely describes it. Then, click Finish to enable the outbound rule for the target port to be open on all selected server profiles.



6. Test Network Connectivity:

- **Ping Test:** Open a command prompt. Type ping **IP address (replace IP address)** with the IP address of a device on the network).
- **Web Browser:** Open a web browser and try to access websites.
- **Remote Desktop:** Use Remote Desktop to connect to the server remotely.

Points to Remember

- Network discovery has three basic levels of configuration:
  - Enable
  - Disable
  - Customized
- **Assign an IP Address to server:**
  - **Static IP Address (DHCP):**
    - Right-click on the network adapter and select **Properties**.
    - Double-click on **Internet Protocol Version 4 (TCP/IPv4)**.
    - Select **Use the following IP address**.
    - Enter the IP address, subnet mask, default gateway, and preferred DNS server addresses.
    - Click **OK**.
  - **Dynamic IP Address (DHCP):**
    - Right-click on the network adapter and select **Properties**.
    - Double-click on **Internet Protocol Version 4 (TCP/IPv4)**.

- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Click **OK**.

Practical Activity 1.3.4: Updating Server drivers and services

Task:

1: Referring to the key reading 1.3.3 As networking and internet technology trainee, you are asked to go to the computer lab to lab update server drivers and services.
2: Present the procedures of all step performed installation.
3: Present your work to the trainer and whole class.
4: Read key reading 1.3.4 and ask clarification where necessary
5: Perform the task provided in application of learning 1.3 in their manuals.

Key readings 1.3.4: Updating Server drivers and services

1. Get the drivers installed

Methods for Updating Server Drivers

1.1 Using Windows Update

This is the simplest method and ensures that you receive the latest drivers automatically.

- Press the Windows key + I to open Settings.
- Click on Update & Security.
- Select Windows Update from the sidebar.
- Click on Check for updates. If any driver updates are available, they will be downloaded and installed automatically.

1.2. Manually Updating via Device Manager

For more control over which drivers to update, use Device Manager.

Steps:

- Open Device Manager by right-clicking the Start button and selecting it.
- Expand the category of the device you want to update.
- Right-click on the specific device and select Update driver.
- Choose Search automatically for updated driver software. Follow the prompts if newer drivers are found.

1.3. Downloading from Manufacturer's Websites

This method ensures you get the most specific and up-to-date drivers directly from the source.

Identify the model number of your hardware component.

- Visit the manufacturer's official support page.

- Look for a section titled “Drivers” or “Downloads”.
- Download the appropriate driver for your operating system version and hardware model.
- Run the installer, checking release notes for improvements or fixes.

1.4. Using Automatic Driver Update Tools

These tools can simplify the process by scanning your system for outdated drivers and providing one-click solutions to update them.

1. Installation of services

To install services in Windows Server using the graphical user interface (GUI), follow these steps:

Steps to Install Services via GUI in Windows Server

Step 1: Open Server Manager>>Click on the Start menu. Select Server Manager from the list of applications.

Step 2: Access the Add Roles and Features Wizard: In the Server Manager dashboard, click on Manage in the top right corner. Select Add Roles and Features from the dropdown menu.

Step 3: Navigate Through the Wizard: On the Before you begin page, read any prerequisites and click Next.

Step 4: Select Installation Type: Choose Role-based or feature-based installation to install roles or features on a local server. Click Next.

Step 5: Select Destination Server: Choose the server from the server pool where you want to install the service. Click Next.

Step 6: Select Server Roles: On the Select server roles page, check the box next to the roles you want to install. Click Next.

Step 7: Select Features: On the Select features page, you can choose additional features that may be required for your service. Click Next.

Step 8: Confirm Installation Selections: Review your selections on the confirmation page. Click on Install to begin the installation process.

Step 9: Installation Progress, Monitor the installation progress. Once completed, you will see a confirmation message.

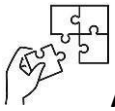
Step 10: 10. Verify Installation, after installation, you can verify that your service is installed by going back to the Server Manager dashboard.

Points to Remember

- **Steps to Install Services via GUI in Windows Server**
  a. Open Server Manager
  b. Select Add Roles and Features from the dropdown menu.
  c. On the Before you begin page, read any prerequisites and click Next.
  d. Select Installation Type

e. Select Destination Server
f. Select Server Roles
g. Select Features if is needed
h. Confirm Installation Selections
i. Installation Progress
j. Verify Installation

- **While you are performing manually update via device manager consider the following steps:**
  1. Open Device Manager by right clicking the Start button and selecting it.
  2. Expand the category of the device you want to update.
  3. Right-click on the specific device and select Update driver.
  4. Choose Search automatically for updated driver software. Follow the prompts if newer drivers are found.



Application of learning 1.3.

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for installing windows sever operating system and perform network adapter configuration.

Learning outcome 1 end assessment

Written assessment

Multiple choice questions: Circle the letter corresponding to the correct answer:

I. Which of the following is NOT a type of virtualization?
   a) Storage Virtualization
   b) Network Virtualization
   c) Application Virtualization
   d) Directory Virtualization

II. What is the role of a guest operating system in virtualization?
   a) To act as the primary server OS
   b) To run independently of any virtual environment
   c) To run on top of a virtual machine managed by the hypervisor
   d) To replace the physical machine's hardware

III. Which of the following is an advantage of virtualization?
   a) Reducing the number of physical servers
   b) Slower resource allocation
   c) Increased power consumption
   d) Increased hardware dependency

IV. Which of the following is a client-side operating system?
   a) Hyper-V
   b) Network OS
   c) Standalone

V. What is Hyper-V used for?
   b) Network management
   c) Virtualization
   d) File storage
   e) Web hosting

Practical assessment

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for selecting, installing windows sever operating system and perform network adapter configuration.

References

Springall, D., Durumeric, Z., & Halderman, J. A. (2016, June). FTP: The forgotten cloud. *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 503–513. IEEE. https://doi.org/10.1109/DSN.2016.54

Richards, J., Allen, R., & Lowe-Norris, A. G. (2006). *Active Directory*. O'Reilly Media.

Allen, R., & Lowe-Norris, A. (2003). *Active Directory*. O'Reilly Media.

Clines, S., & Loughry, M. (2008). *Active Directory for dummies*. John Wiley & Sons.

Desmond, B., Richards, J., Allen, R., & Lowe-Norris, A. G. (2008). *Active Directory: Designing, Deploying, and Running Active Directory*. O'Reilly Media.

Microsoft. (n.d.). How to install and uninstall services. Retrieved from https://learn.microsoft.com/en-us/dotnet/framework/windows-services/how-to-install-and-uninstall-services?redirectedfrom=MSDN

Microsoft. (n.d.). Set up environment for Windows containers. Retrieved from https://learn.microsoft.com/en-us/virtualization/windowscontainers/quick-start/set-up-environment

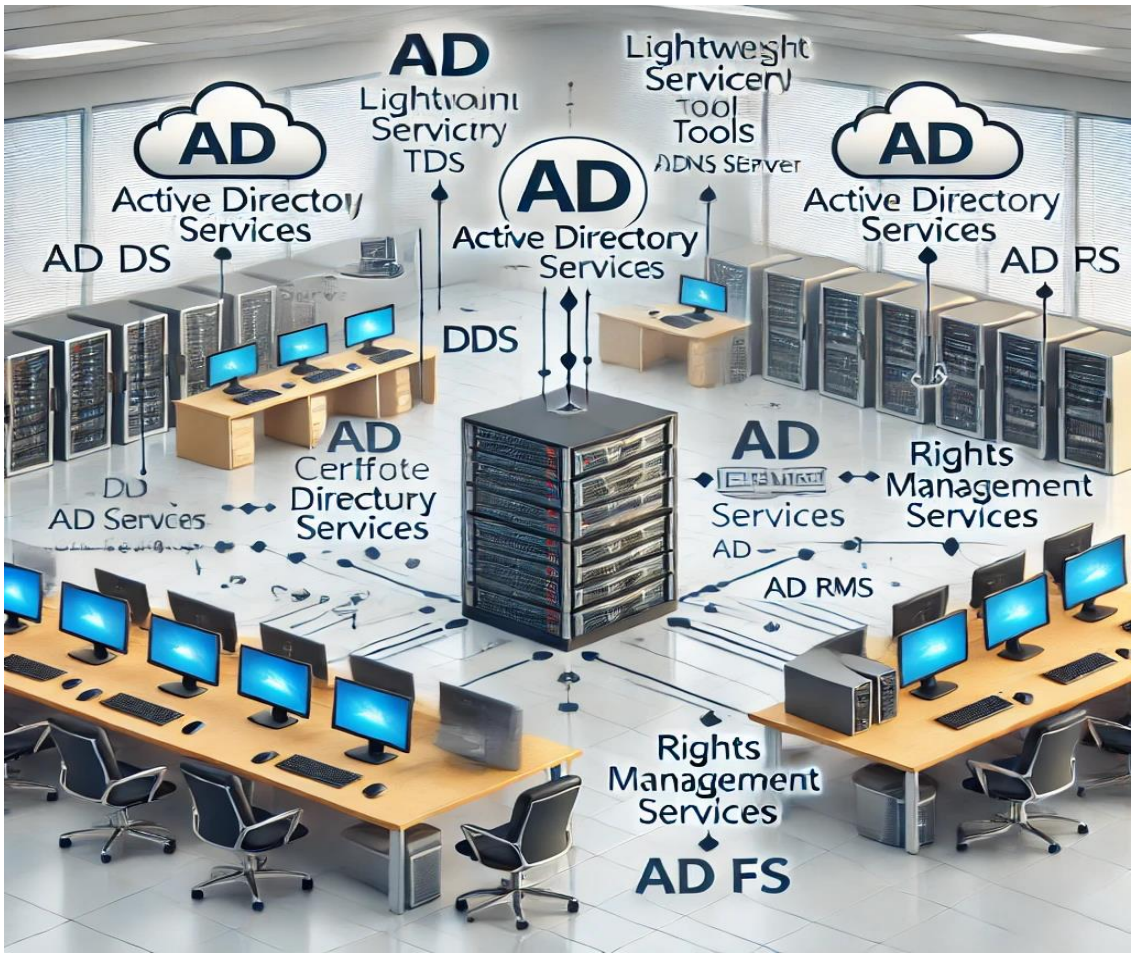
Microsoft. (n.d.). Install or uninstall roles, role services, or features. Retrieved from https://learn.microsoft.com/en-us/windows-server/administration/server-manager/install-or-uninstall-roles-role-services-or-features

Microsoft. (n.d.). Install and configure Windows Server Essentials. Retrieved from https://learn.microsoft.com/en-us/windows-server-essentials/install/install-and-configure-windows-server-essentials

Stack Overflow. (n.d.). Is there an official GUI way of installing and removing .NET services on Windows? Retrieved from https://stackoverflow.com/questions/3088234/is-there-an-official-gui-way-of-installing-and-removing-net-services-on-windows

Schunk, C. (n.d.). Step-by-step guide to building a fully functional Windows Server. LinkedIn. Retrieved from https://www.linkedin.com/pulse/step-by-step-guide-building-fully-functional-windows-server-schunk

Netwrix. (n.d.). Windows server hardening checklist. Retrieved from https://www.netwrix.com/windows-server-hardening-checklist.html


AD
Active Directory Services
AD DS
AD
Lightweight Servicery TDS
AD
Active Directory Services
DDS
Lightweight Servicery Tool
Tools
ADNS Server
AD
Active Directory Services
AD RS
AD
Certfote Directury Services
AD
Services
Rights Management Services
AD
AD RMS
Rights Management Services
AD FS

Indicative contents
2.1 Installation of Active Directory Domain Services
2.2 Configuration of Active Directory
2.3 Joining client Computer to the domain
2.4 Management of GPO
2.5 Deployment of Mail Exchange Server

Key Competencies for Learning Outcome 2: Deploy Active Directory Services

Knowledge	Skills	Attitudes
● Describe active directory concepts ● Description of Group policy object	● Installing Active Directory Domain Services (AD DS) ● Promoting the Server to a Domain Controller ● Post-Installation Configuration	● Having self-motivation ● Being analytical and details oriented

Duration: 20 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Install properly Active Directory Domain Services as used in windows server
2. Configure correctly Active Directory Domain Services based on windows server
3. Manage properly GPO settings in server machine based on windows server
4. Deploy properly of Mail Exchange Server used in windows server
5. Join properly client to the domain as used in windows server

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS	● Modem ● Router ● VMware Workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD ● USB	● Electricity ● Data Cables ● Internet

Indicative content 2.1: Installation of Active Directory Domain Services

Duration: 5 hrs

Theoretical Activity 2.1.1: Definition of active directory concepts

Tasks:

1: Answer the following questions:

I. What do you understand by the following terms as used in windows server?

a) Active Directory(AD)
b) Domain Controller (DC)
c) Organizational Unit (OU)
d) Global Catalog (GC)
e) Group Policy Object(GPO)
f) Active Directory Domain Service(ADDS)

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 2.1.1 in their manuals.

Key readings 2.1.1.: Definition of active directory concepts

1.Definition

1.1. Active Directory (AD)

- A directory service developed by Microsoft for Windows domain networks.
- It acts as a central database that stores information about network resources, users, and computers.
- AD provides authentication, authorization, and management of network resources.

1.2. Domain Controller (DC)

- A server running Active Directory Domain Services (AD DS).
- DCs are responsible for authenticating and authorizing users and computers within a domain.
- They store and replicate the Active Directory database.

1.3. Organizational Unit (OU)

- A container within Active Directory used to organize objects like users, computers, and other OUs.
- OUs help manage and delegate administrative control over groups of

objects.

- They can be nested within each other to create a hierarchical structure.

1.4. Global Catalog (GC)

- A special type of domain controller that stores a partial copy of every object in the Active Directory Forest.
- GCs enable users to search for objects across multiple domains.
- They are essential for large-scale Active Directory deployments.

1.5. Group Policy Object (GPO)

- A collection of settings that can be applied to user accounts and computers within Active Directory.
- GPOs are used to enforce security policies, configure software settings, and manage user preferences.
- They provide a centralized way to manage user and computer configurations.

1.6. Active Directory Domain Services (AD DS)

- The core service that provides the directory service functionality of Active Directory.
- AD DS is responsible for storing and managing information about objects in the Active Directory database.
- It enables authentication, authorization, and other directory-based services.

Theoretical Activity 2.1.2: Description of active directory concepts

Tasks:

1: Answer the following questions related to active directory concepts:

i. Define the following terms as used in windows server:

a) Domain
b) Forest
c) Tree
d) Trust Relationship

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 2.1.2

Key readings 2.1.2.: Description of active directory concepts

1.Definition

1.1. Domain

- A logical grouping of users, computers, and other objects that share a common database and security policies.
- Each domain has its own security boundary and is managed independently.
- Domains are the fundamental building blocks of Active Directory.

1.2. Domain Controller (DC)

- A server that runs the Active Directory Domain Services (AD DS) role.
- DCs store, replicate, and manage the domain's database.
- They authenticate user and computer accounts, enforce security policies, and provide other directory services.

1.3.Forest

- A collection of one or more domains that share a common schema, global catalog, and forest-wide configuration settings.
- Forests provide a way to organize multiple domains hierarchically and manage them as a single administrative unit.

1.4.Tree

- A contiguous set of domains in a forest that share a common root domain.
- Trees are used to organize domains within a forest and establish trust relationships between them.

1.5.Organizational Units (OUs)

- Containers within a domain that are used to organize objects like users, computers, and other OUs.
- OUs can be used to delegate administrative permissions, apply security policies, and simplify management of large domains.

1.6.Global Catalog (GC)

- A partial replica of the entire directory database that contains a subset of information about all objects in the forest.
- GCs enable users to search for objects across multiple domains and locate resources regardless of their physical location.

1.7.Trust Relationship

- A security association between two domains that allows users in one domain to access resources in another domain.
- Trust relationships can be transitive, meaning that trust can be extended to other domains within the same forest or to domains in different forests.

1.8.Group Policy (GPO)

- A collection of settings that define the configuration of operating systems,

applications, and user settings within a domain or OU.

- GPOs can be used to enforce security policies, deploy software, and manage user preferences.

1.9.User Accounts

- Represent individual users who are authorized to access network resources.
- User accounts store information such as user name, password, email address, and security permissions.

1.10.Computer Accounts

- Represent computers that are part of the domain.
- Computer accounts store information about the computer's hardware, operating system, and security settings.

1.11.Security Groups and Distribution Groups:

- Security groups are used to assign permissions to multiple users or computers at once.
- Distribution groups are used to send email messages to a group of users.

1.12.Schema:

- The underlying structure of the Active Directory database, defining the types of objects that can be stored and their attributes.
- The schema can be extended to add new object types or modify existing ones.

Practical Activity 2.1.3: Performing ADDC installation process

Task:

1: Read the following task:

Go to computer lab to install Active Directory Domain Services.

2: Present the procedures for all step performed during installation.

3: Present your work to the trainer and whole class.

4: Read key reading 2.1.3 and ask clarification where necessary

5: Perform the task provided in application of learning 2.1

Key readings 2.1.3: Performing ADDC installation process

Installation of Active Directory Domain Services (ADDS)

Active Directory Domain Services (AD DS) is a directory service that provides centralized management and security for networks. It's a core component of

Windows Server and is used to manage users, computers, and other resources in a domain environment.

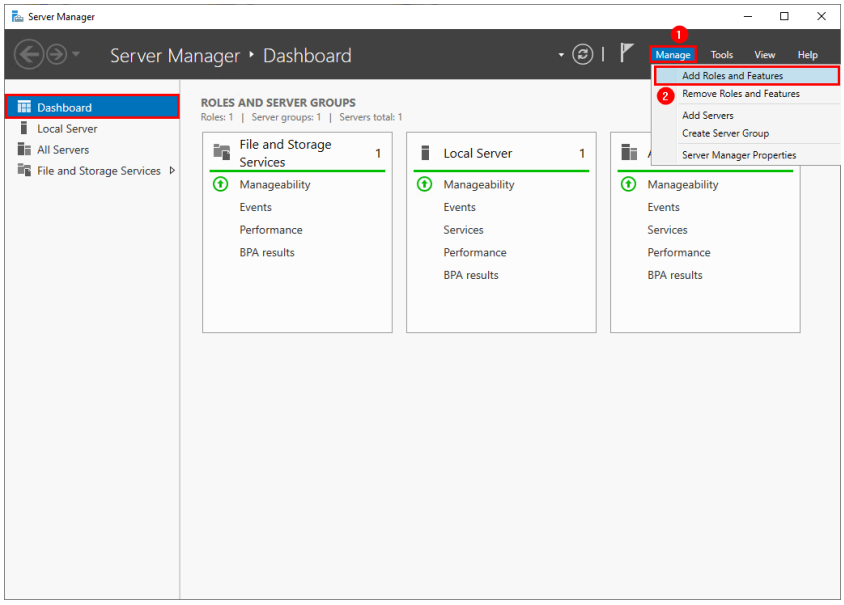
Prerequisites for AD DS Installation

Before you begin the installation process, ensure that your server meets the following requirements:

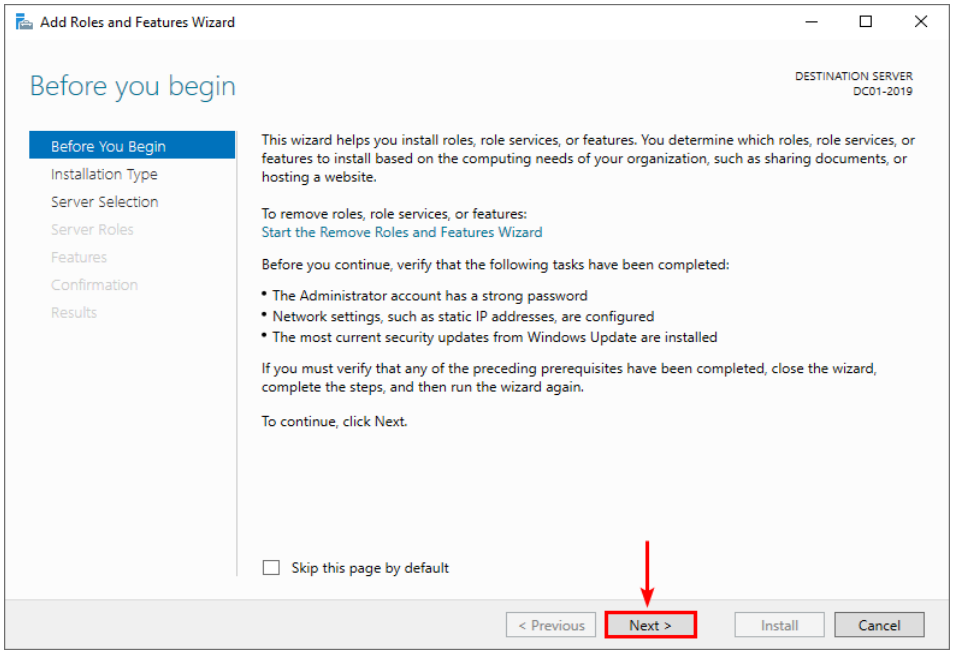
- **Operating System:** Windows Server 2012 R2 or later
- **Hardware:** Sufficient CPU, memory, and disk space
- **Network:** A stable network connection with a static IP address
- **DNS Server:** A functioning DNS server to resolve domain names
- **Domain Name:** A unique domain name for your organization

Follow the steps to install Active Directory Domain Services (AD DS) on Windows Server.

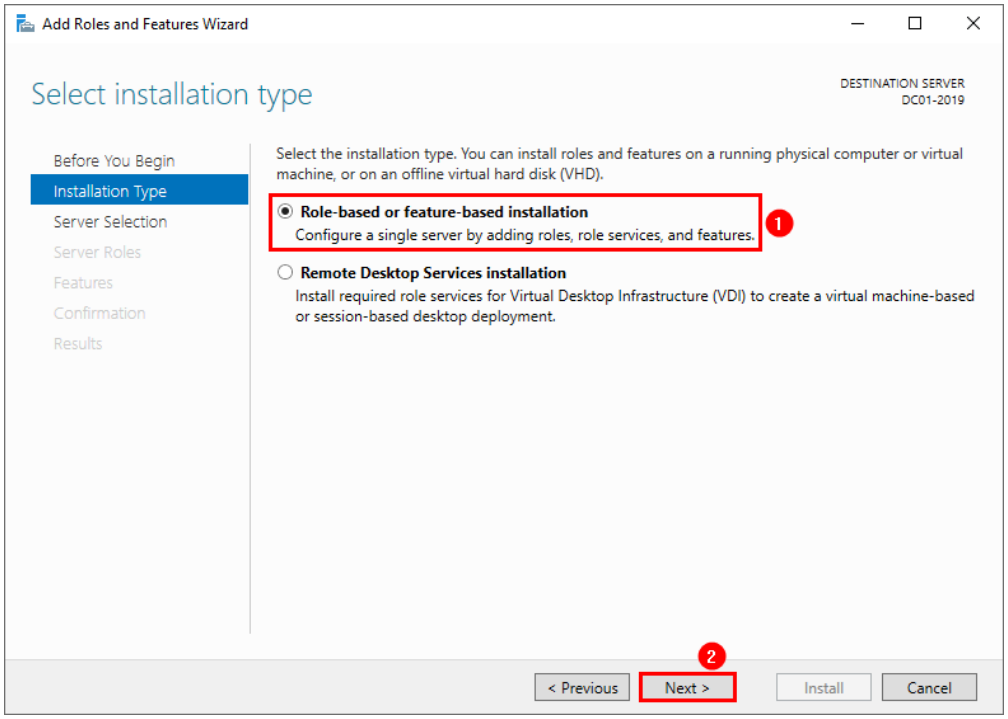
Start **Server Manager**. Go to **Dashboard > Manage > Add Roles and Features**.



Click **Next**.

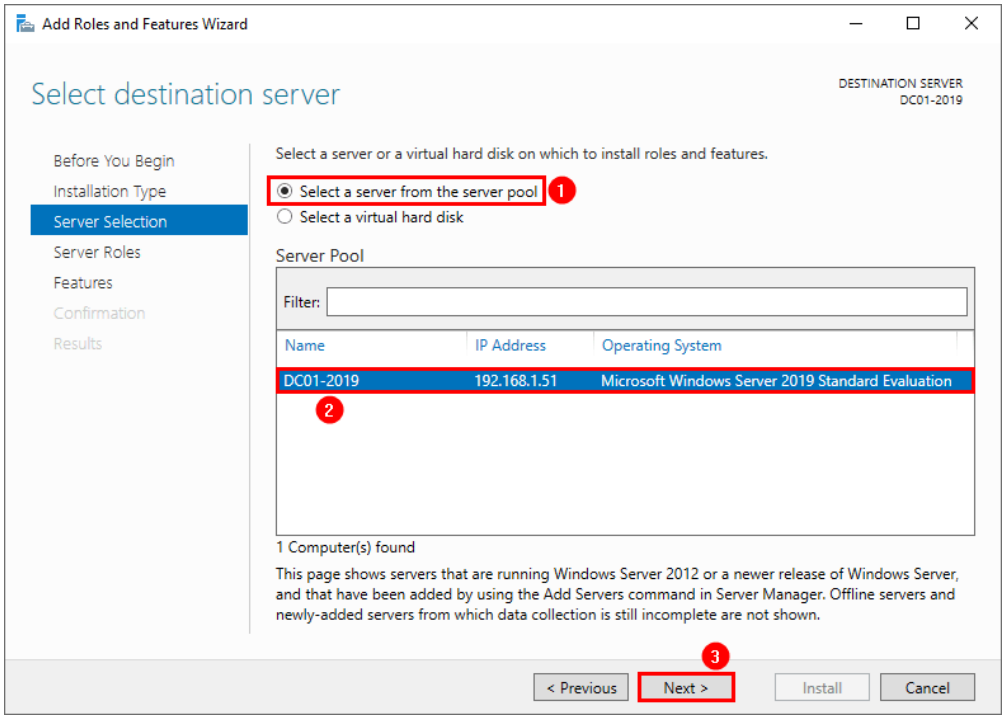


Select **Role-based or feature-based installation**. Click **Next**.

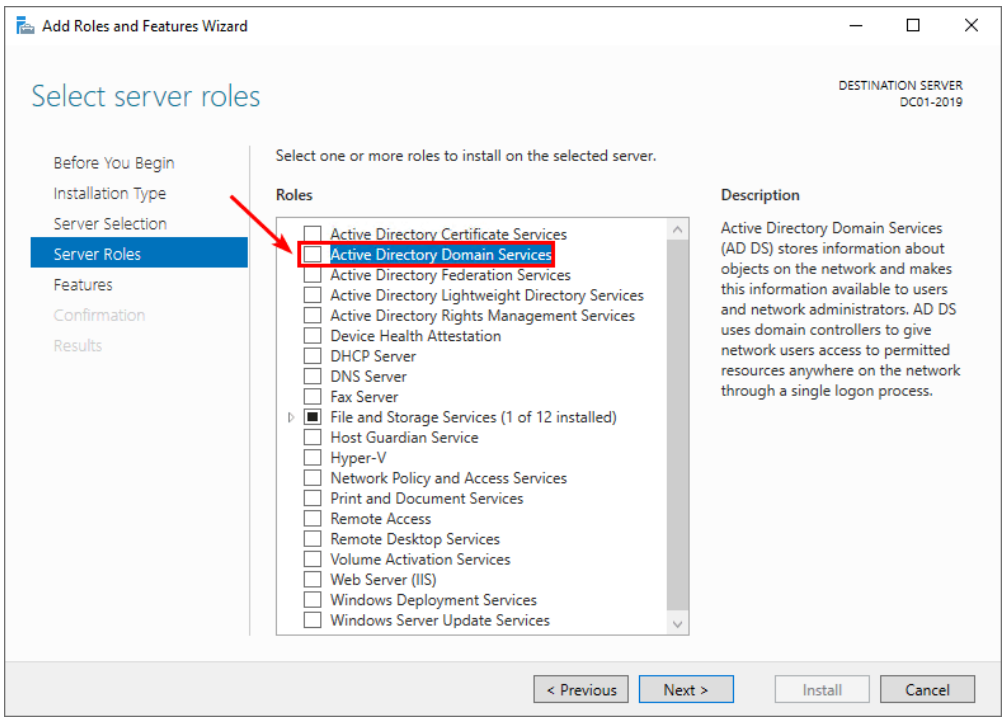


Select the server from the pool. Click on **Next**.

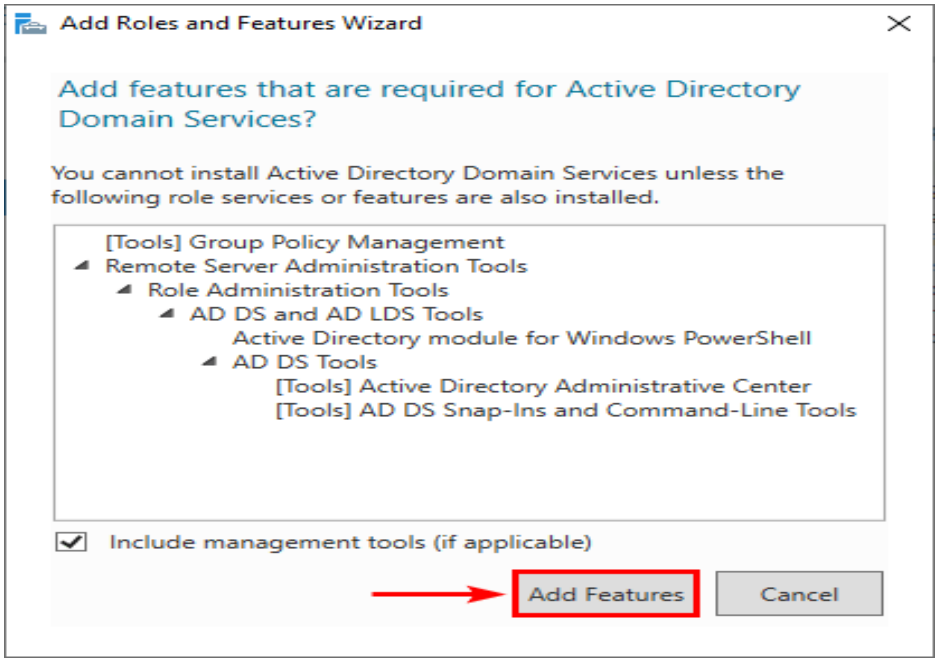
In our example, it's Windows Server **DC01-2019** with a fixed IP address **192.168.1.51**.



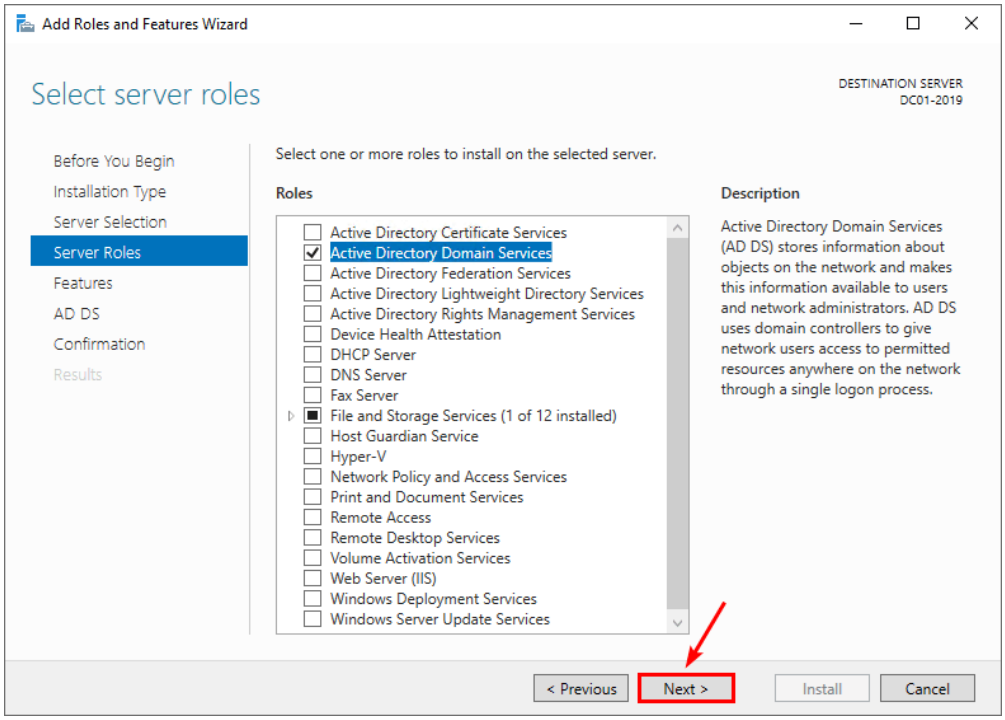
Check the checkbox **Active Directory Domain Services**.



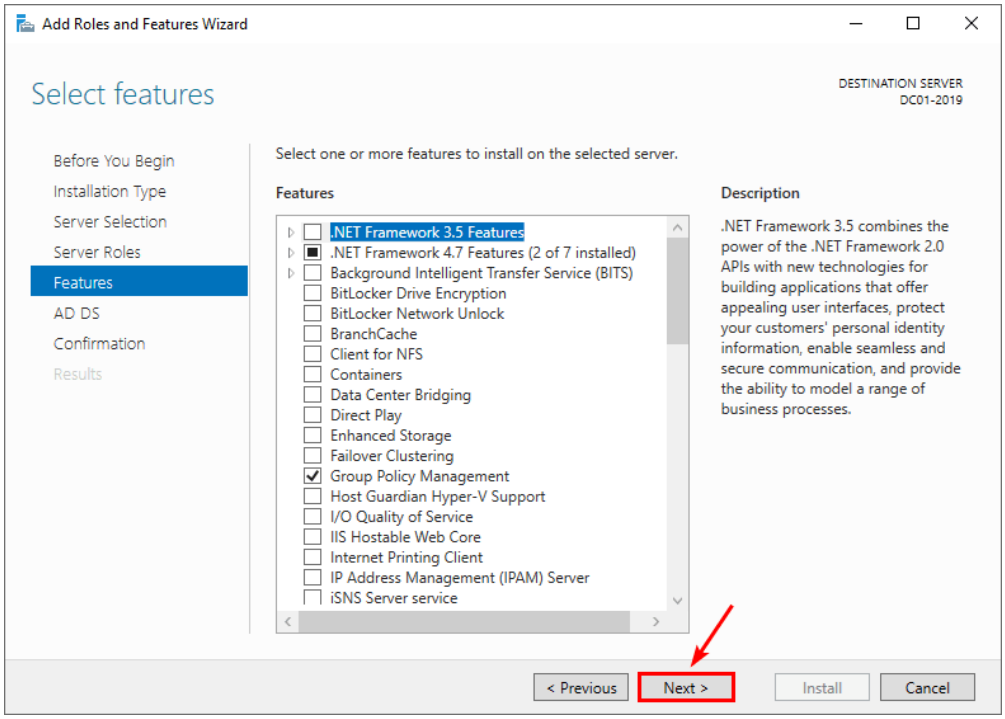
A window will show that it will add features that are required for Active Directory Domain Services. Click **Add Features**.



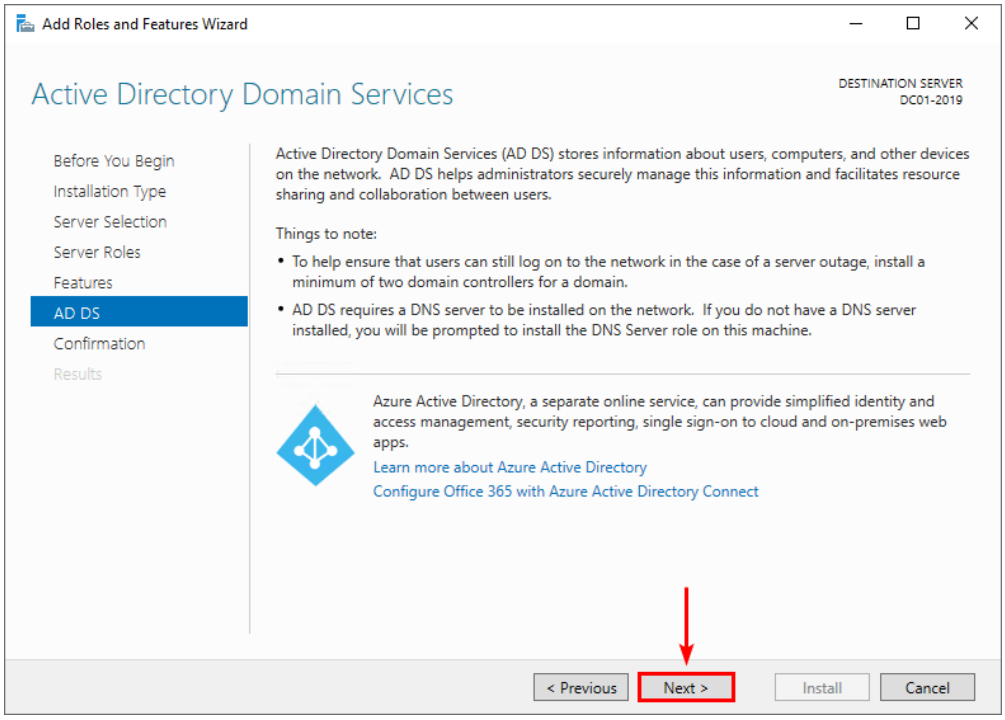
Click **Next**.



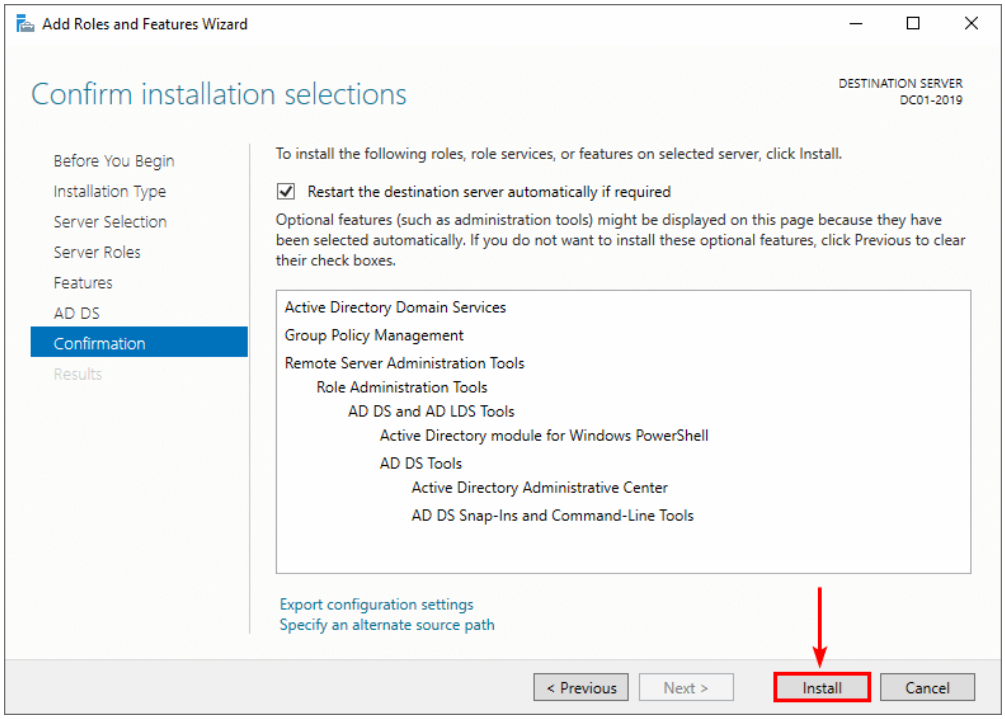
You don’t need to select any features. Click **Next**.



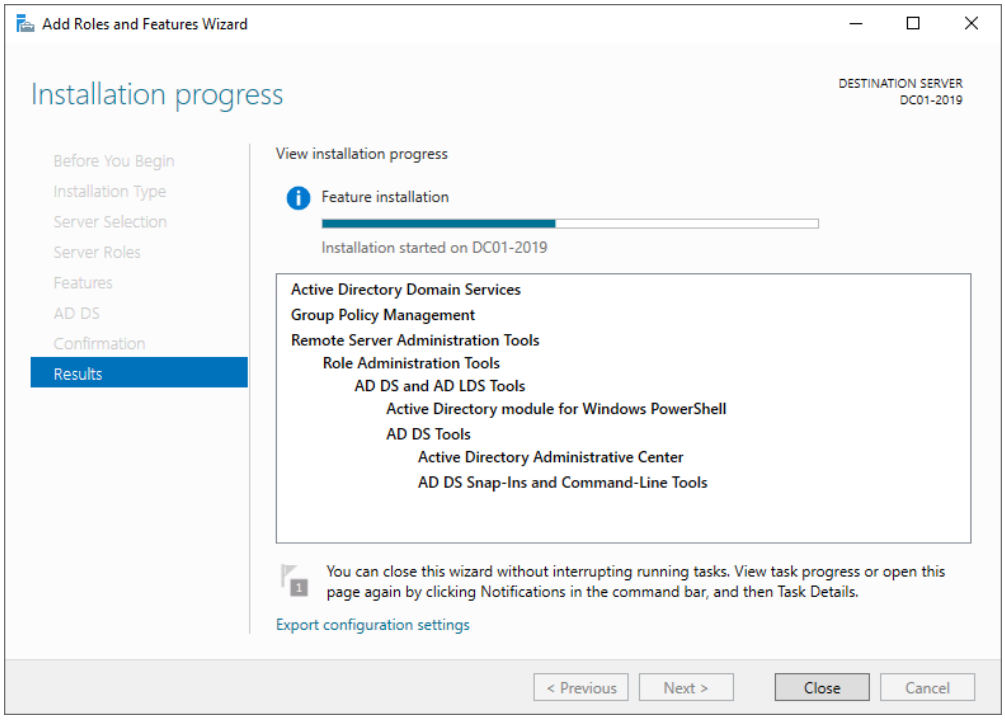
Proceed with **Next**.



Click **Install**.

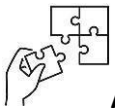


The installation will start.



Points to Remember

- **Steps of installing AD DS:**
  - ✓ In Server Manager, click **Manage** and then **Add Roles and Features.**
  - ✓ Choose **Role-based or feature-based installation** and click **next.**
  - ✓ Select the server where you want to install AD DS and click **next.**
  - ✓ Select **Active Directory Domain Services** and click **next.**
  - ✓ Click **Add Features** and then **Next.**
  - ✓ Review the installation selections and click **Install.**



Application of learning 2.1.

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for installing Active Directory Domain Services.

Indicative content 2.2: Configuration of Active Directory

Duration: 5 hrs

Theoretical Activity 2.2.1: Description of Active Directory

Tasks:

1: Answer the following questions:

1: Answer the following questions:

I. What is Active Directory?

II. What are the main components of Active Directory?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 2.2.1

Key readings 2.2.1: Description of Active Directory

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It serves as a centralized database that stores information about network objects, such as users, computers, groups, and resources. This information is organized in a hierarchical structure, making it easy to manage and access.

Key Components of Active Directory:

- **Domain:** A logical grouping of network objects, such as users, computers, and groups. A domain has its own security policies and administration.
- **Domain Controller:** A server that stores a copy of the Active Directory database and provides authentication, authorization, and other directory services.
- **Organizational Unit (OU):** A container within a domain that can be used to organize objects logically. OUs help in managing security policies and permissions.
- **User Account:** Represents a person or entity that can log into the network.
- **Computer Account:** Represents a computer that is part of the domain.
- **Group:** A collection of user and/or computer accounts that share common permissions and access rights.

Benefits of Active Directory:

- **Centralized Management:** AD provides a single point of administration for managing users, computers, and other network objects.
- **Enhanced Security:** AD offers robust security features, such as password policies,

access controls, and encryption, to protect sensitive information.

- **Scalability:** AD can be scaled to accommodate large and complex networks.
- **Simplified User Management:** AD automates many user management tasks, such as creating user accounts, assigning permissions, and resetting passwords.
- **Standardized Access:** AD ensures consistent access to network resources across the organization.

Common Use Cases:

- **User Authentication and Authorization:** AD verifies user identities and grants them appropriate access to network resources.
- **Group Policy Management:** AD allows administrators to define and enforce security policies and settings for users and computers.
- **Network Resource Management:** AD helps manage network resources, such as printers, file servers, and applications.
- **Single Sign-On (SSO):** AD enables users to log in once and access multiple applications and resources.

✓ **Active Directory Services**

- **Active Directory Domain Services:** Active Directory Domain Services (AD DS) is a core component of Active Directory and provides the primary mechanism for authenticating users and determines which network resources they can access. AD DS also provides additional features such as Single Sign-On (SSO), security certificates, LDAP, and access rights management.
- **Lightweight Directory Services:** AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service. It provides only a subset of the AD DS features, which makes it more versatile in terms of where it can be run.
- **Certificate Services:** You can create, manage and share encryption certificates, which allow users to exchange information securely over the internet.
- **Active Directory Federation Services:** ADFS is a Single Sign-On (SSO) solution for AD which allows employees to access multiple applications with a single set of credentials, thus simplifying the user experience.
- **Rights Management Services:** AD RMS is a set of tools that assists with the management of security technologies that will help organizations keep their data secure.

Practical Activity 2.2.2: Promoting windows server AD to DC

Task:

1: Read the following task:

Go to computer lab to Promote windows server AD to DC.

2: Present the procedures for all step performed during installation.

3: Present your work to the trainer and whole class.

4: Read key reading 2.2.2 and ask clarification where necessary

5: Perform the task provided in application of learning 2.2

Key readings 2.2.2: Promoting windows server AD to DC

Promote Windows Server 2016 to Domain Controller step by step

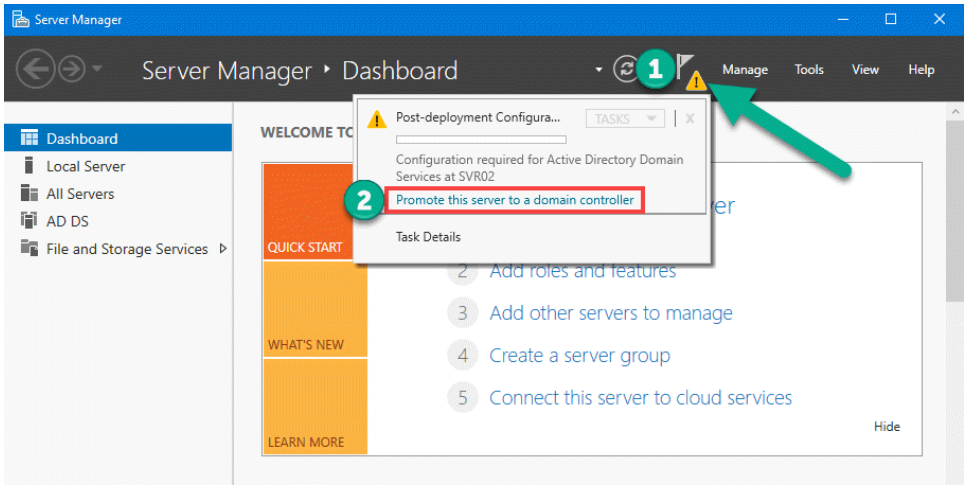
Prerequisites

Install Active Directory Domain Services (AD DS) role on the server you want to promote it to domain controller (DC).

Promote Server to Domain Controller

Follow the following steps to promote server to domain controller.

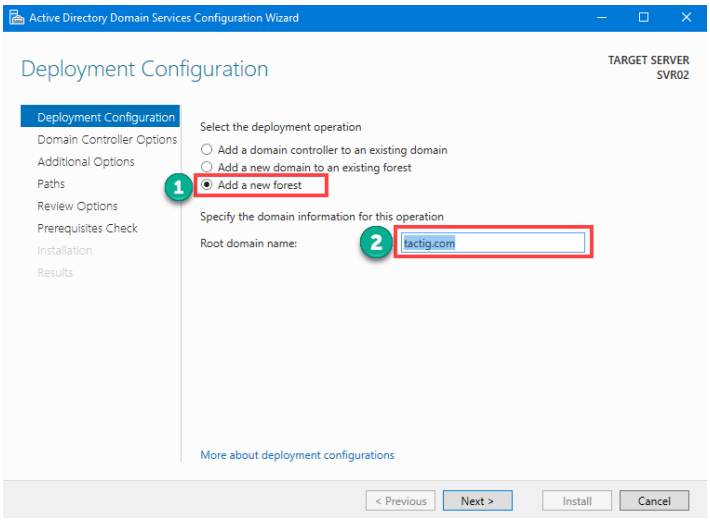
1. After the role installation, open Server Manager. Click on the flag, then click on **Promote this server to a domain controller** hyperlink.



2. When the Deployment Configuration page appears, you see three options.

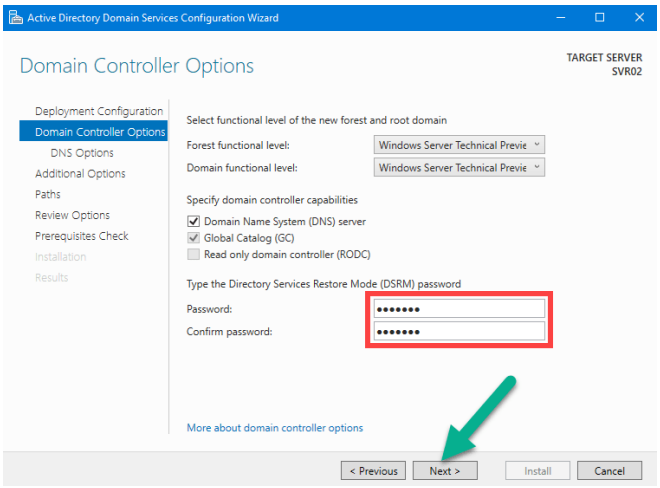
- **Add domain controller to existing domain:** This option is used when you want to add additional domain controller.
- **Add a new domain to an existing forest:** This option is used for adding a new domain to existing forest.
- **Add a new forest:** It is used for creating a new forest.

- Select the third option: **Add a new forest**. Enter a **Root domain name** and click on **Next** button.

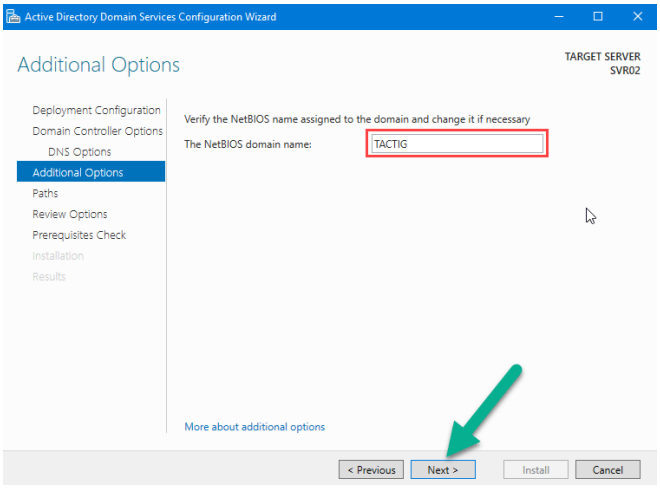


3. Specify the **forest and domain functional levels** (2008, 2008R2, 2012, 2o12R2, 2016). Type a complex password (composed of capital letters, small letters, numbers, symbols).

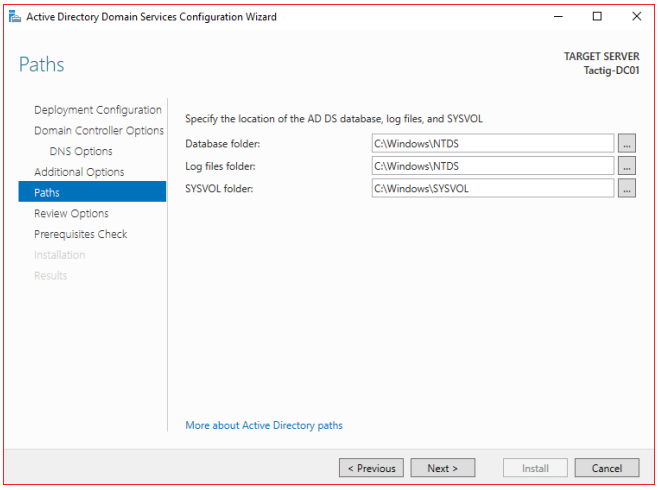
By default, Domain Name Services (DNS) server is installed at the same time when you are promoting the server to domain controller. If you want to install DNS server later, remove the selection from the box next to Domain Name Services (DNS) server. Click on **Next** button when you're finished here.



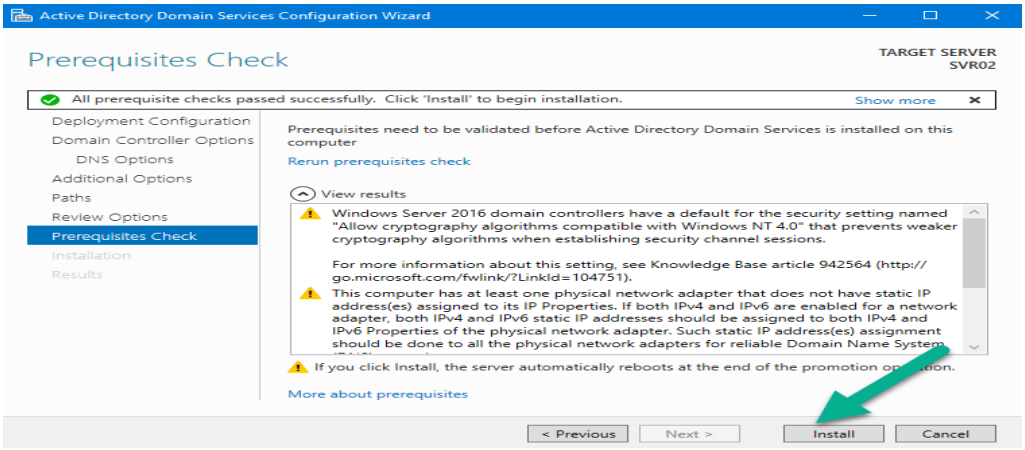
4. On the Additional options page, let the NetBIOS domain name as selected by default. If you want, you can change the NetBIOS name. Click on **Next** button to move on next page.



5. Thus, you can specify the path that you want to restore your Database files, log files and SYSVOL files. The path page give you the options to specify location of the sources to be restored. When you finished your work, click on **Next** button.



6. The next page is **Review options.** You go nothing to do. Click on **Next** button**.** The Prerequisites Check page shows you the summary of all prerequisites that are verified or not. If it's verified click **Next**. If not, recheck the steps you did just before and be sure you have done all correctly. Click on **Install** button. After the installation succeeded, the system automatically reboots.



Points to Remember

- **Steps of promoting windows server AD to DC:**
  - Launch the DC Promotion Wizard: Click it and select Promote this server to a domain controller
  - Select Deployment Operation
  - Configure Domain Controller Options
  - Configure DNS Options
  - Additional Options like SYSVOL Share Location and Database and Log Files Location
  - Review Options
  - Prerequisites Check
  - Promotion

Application of learning 2.2.

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required to promote active Directory to domain controller.

Indicative content 2.3: Joining Client Computer to the Domain

Duration: 5 hrs

Practical Activity 2.3.1: Adding client to the domain

Task:

1: Read the following task:

Go to computer lab to add client to the domain.

2: Present the procedures for all step performed during installation.

3: Present your work to the trainer and whole class.

4: Read key reading 2.3.1 and ask clarification where necessary

5: Perform the task provided in application of learning 2.3

Key readings 2.3.1: Adding client to the domain

To add a client to a domain, you'll need to follow these steps:

Prerequisites:

- **Domain Controller:** Ensure that you have an active and accessible Domain Controller (DC) set up.
- **Client Computer:** The client computer should be able to connect to the DC and have the necessary network connectivity.

Steps:

Step 1: **Log in to the Client Computer:** Use a local administrator account to log in.

Step 2: **Open System Properties:** Go to **Control Panel** > **System and Security** > **System**. Alternatively, you can right-click on **This PC** and select **Properties**.

Step 3: **Change Computer Name/Domain Settings:** Click on **Change settings**.

Step 4: **Join the Domain:**

- Under the **Computer Name** tab, click on **Change**.
- Select **Domain** from the **Member of** dropdown menu.
- Enter the **domain name** in the provided field.
- Click **OK**.

Step 5: **Provide Credentials:**

Step 6: You will be prompted to enter the credentials of a domain user account with the necessary permissions to join computers to the

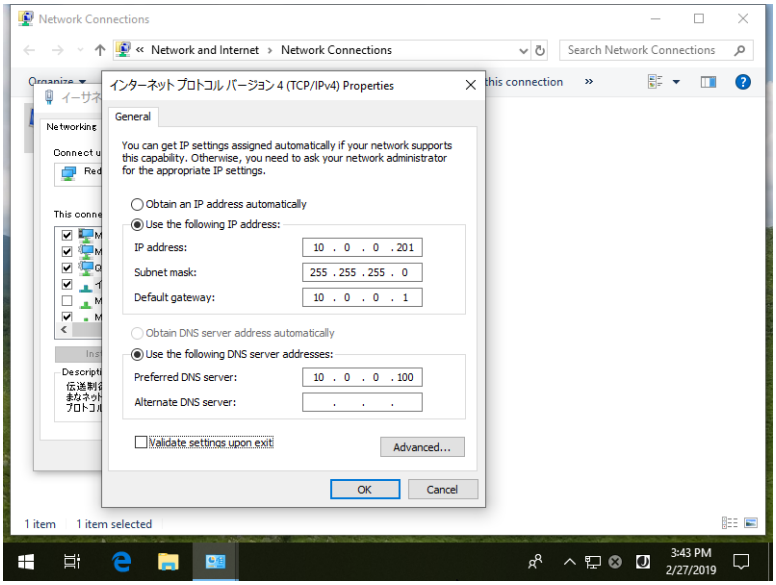
domain.

Step 7: Restart the Computer: After joining the domain, restart the computer for the changes to take effect.

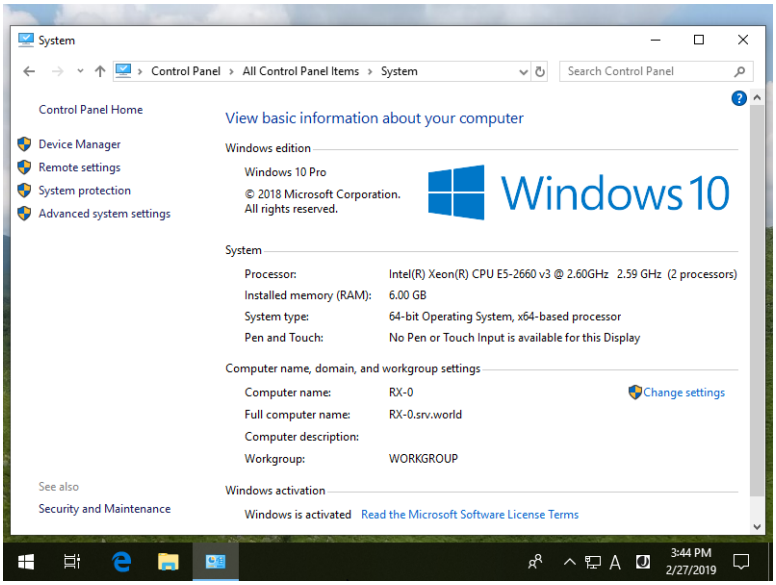
Join in Active Directory Domain from Other Windows Client Hosts.

This example is based on Windows 10

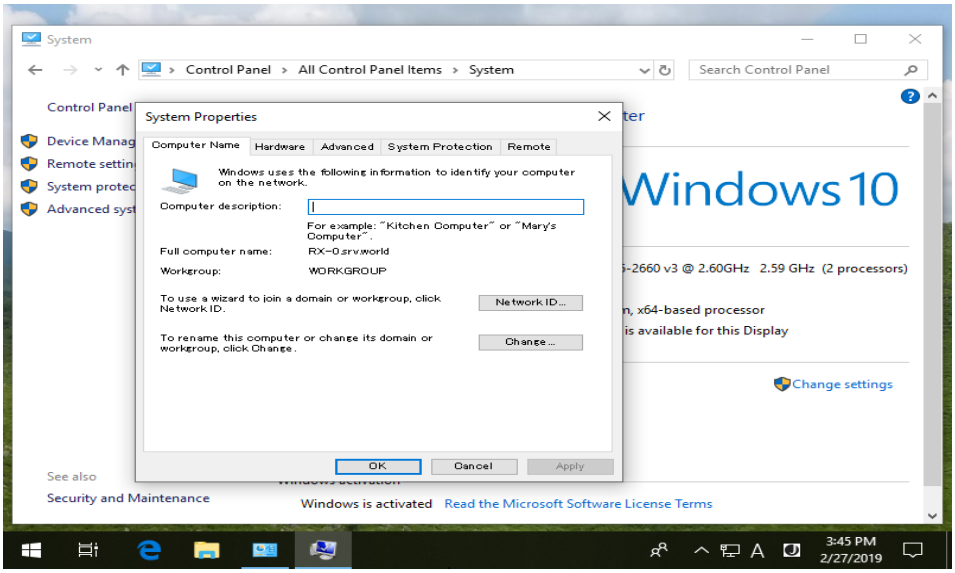
1.Before setting, change to DNS settings to refer Active Directory Host.



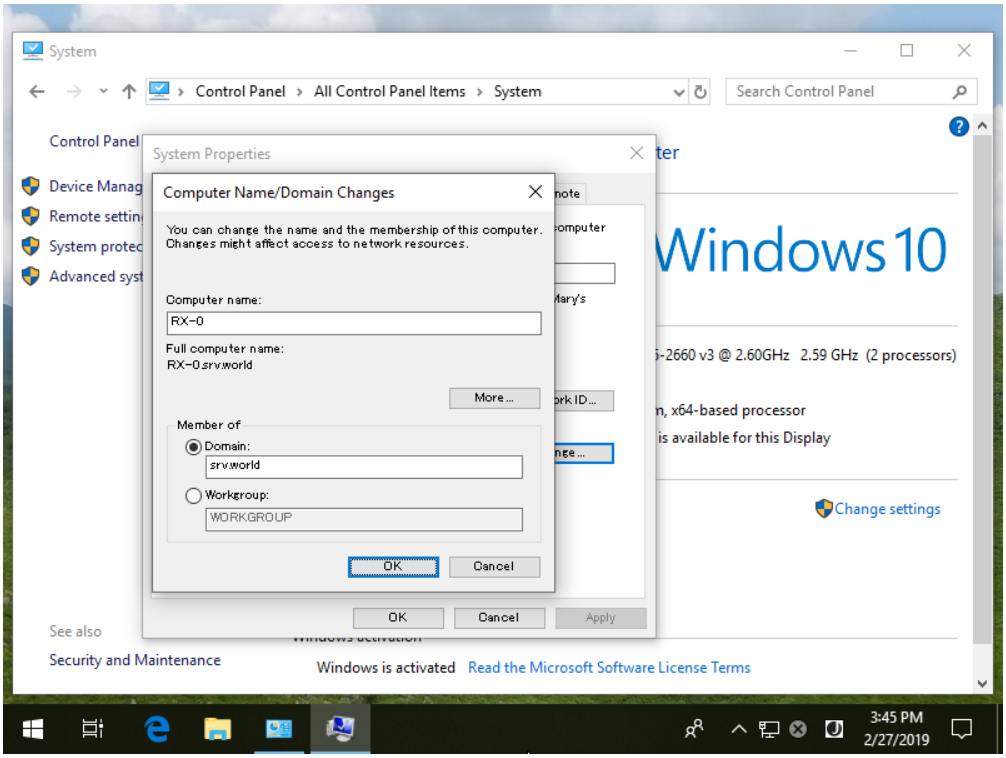
2. Open **System** and click **Change settings** link which is lower-right.



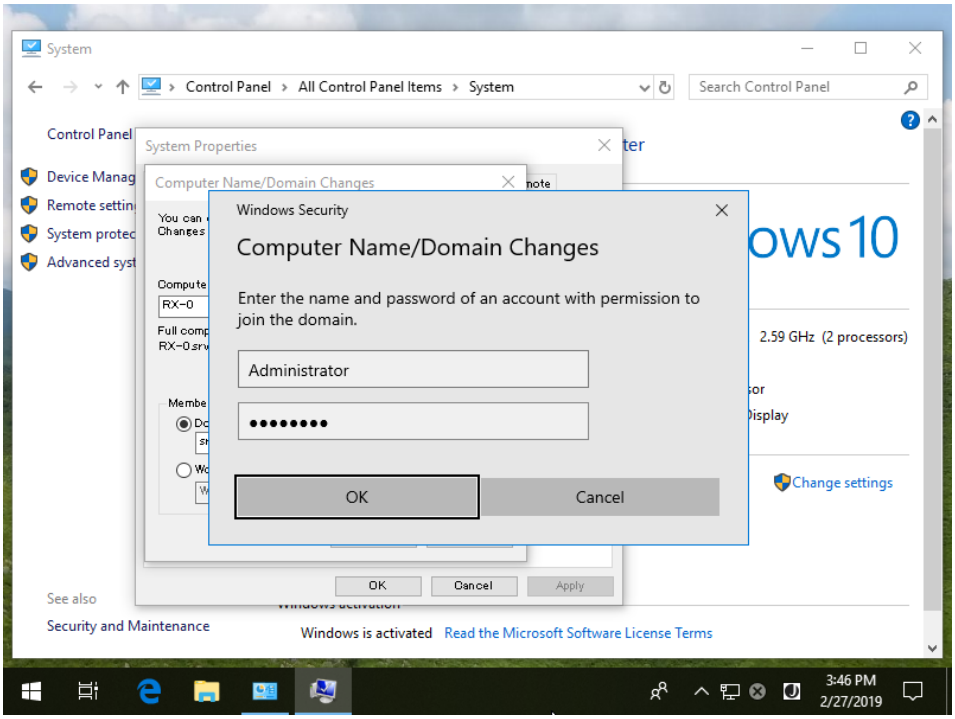
3. Move to **Computer Name** tab and click **Change** button.



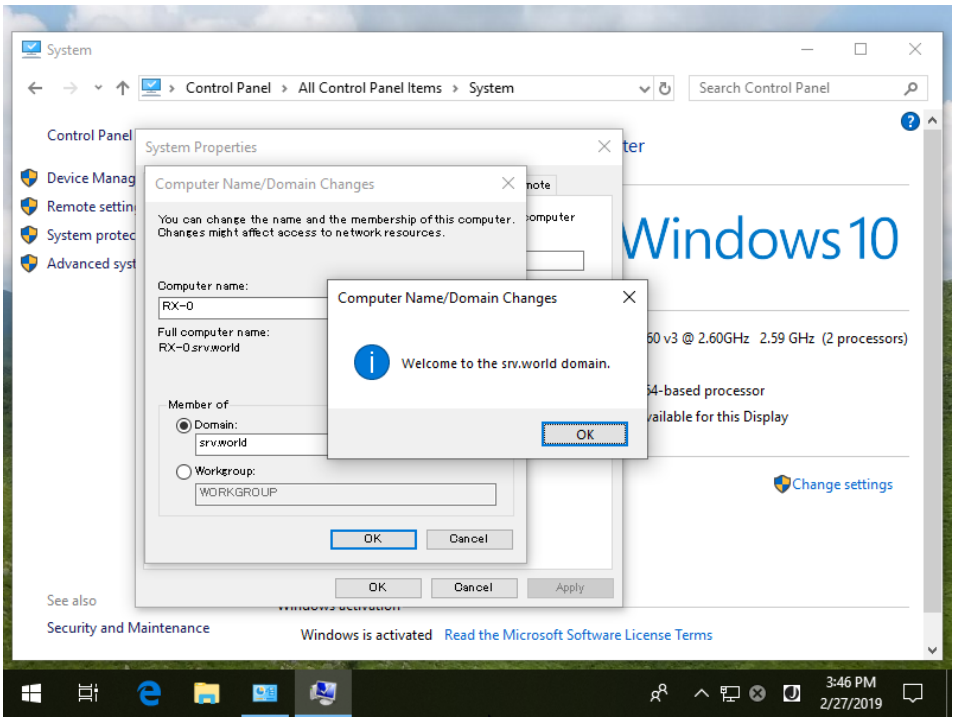
4. Check a box **Domain** and input domain name and next, click **OK** button.



5. Authentication is required, authenticate with a domain User in Active Directory.

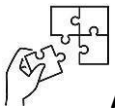


6. After successing authentication, Welcome message is shown like follows. Restart the Computer once.



Points to Remember

- **The steps for** adding **a client to a domain**
  - ✓ Log in to the Client Computer: Use a local administrator account to log in.
  - ✓ Open System Properties: Go to Control Panel > System and Security > System. Alternatively, you can right-click on This PC and select Properties.
  - ✓ Change Computer Name/Domain Settings: Click on Change settings.
  - ✓ Join the Domain:
  - ✓ Provide Credentials: You will be prompted to enter the credentials of a domain user account
  - ✓ Restart the Computer: After joining the domain, restart the computer for the changes to take effect.



Application of learning 2.3.

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for Configuring Active Directory and Joining client Computer to the domain.

Indicative content 2.4: Management of GPO

Duration: 5 hrs

Theoretical Activity 2.4 .1: Description of GPO

Tasks:

1: Answer the following questions:

i. What is a Group Policy Object (GPO)?
ii. What are the different types of GPOs?
iii. How does GPO processing order work?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 2.4.1

Key readings 2.4.1: Description of GPO

1.Definition

A Group Policy Object (GPO) is a collection of settings that can be applied to users and computers within an Active Directory domain. These settings can be used to configure various aspects of a Windows environment, including security settings, software installations, network settings, and more.

2.Types of GPOs

2.1. Local GPOs: Apply only to the local computer. Used for specific configurations that need to be isolated to a single machine. Primarily managed through the Local Group Policy Editor.

2.2. Non-Local GPOs: Linked to Active Directory objects (sites, domains, or OUs). Applied to users and computers that are members of those objects. Managed through the Group Policy Management Console (GPMC).

2.3. Starter GPOs: A template for creating new GPOs. Can be used to pre-configure settings that will be applied to multiple GPOs.

3.GPO Hierarchy and Policy Processing Order

GPOs are processed in a hierarchical order, with policies from higher levels taking precedence over lower-level policies. The order of processing is as follows:

3.1. Local Policy: Applies to the local computer only. Has the lowest priority.

3.2. Site Policy: Applies to all computers and users within a specific Active Directory site. Has a higher priority than local policy.

3.3. Domain Policy: Applies to all computers and users within a specific Active

Directory domain. Has a higher priority than site policy.

3.4. OU Policy: Applies to computers and users within a specific Organizational Unit (OU). Has the highest priority.

4.Benefits of Using GPOs

Implementing GPOs offers several advantages:

4.1. Centralized Management: Administrators can manage settings from a single interface, reducing the complexity of system administration.

4.2. Consistency: Ensures uniformity in user and computer configurations across the organization, which enhances stability.

4.3. Enhanced Security: Allows for the enforcement of security measures such as password policies, user rights assignments, and access restrictions.

4.4. Efficiency: Automates routine tasks like software deployment and system updates, saving time for IT staff.

4.5. Scalability: Suitable for organizations of all sizes, from small businesses to large enterprises

Practical Activity 2.4.2: Creating Accounts

Task:

1: Read the following task:

Go to computer lab to create accounts.

2: Present the procedures for all step performed during installation.

3: Present your work to the trainer and whole class.

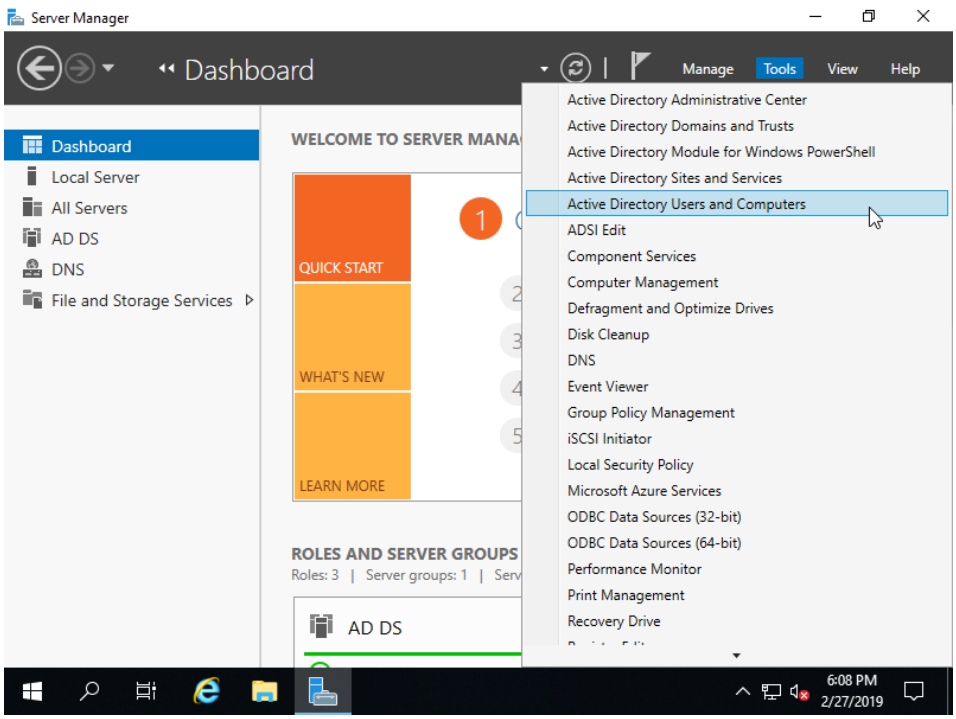
4: Read key reading 2.4.2 and ask clarification where necessary

5: Perform the task provided in application of learning 2.4

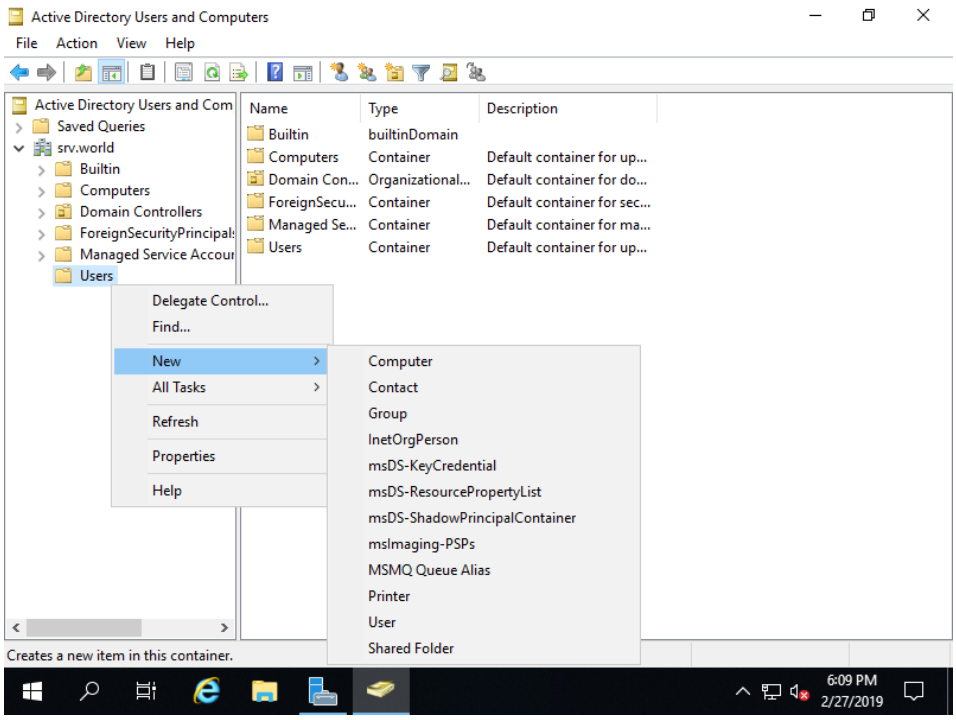
Key readings 2.4.1: Creating Accounts

Steps for Creating a Computer Account

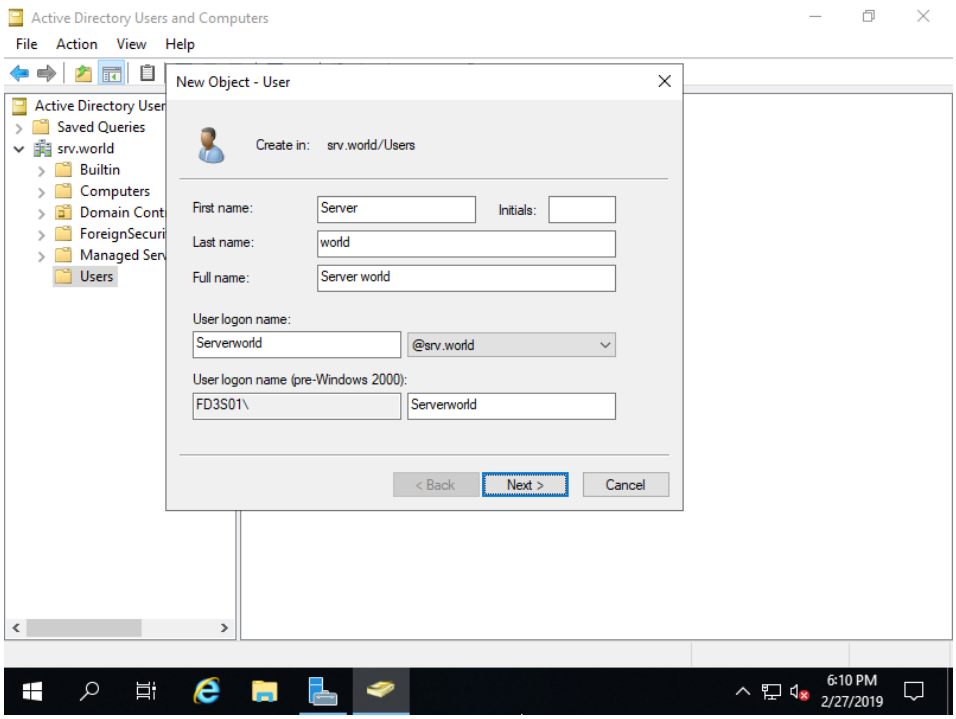
1. Run Server Manager and click Tools - Active Directory Users and Computers.



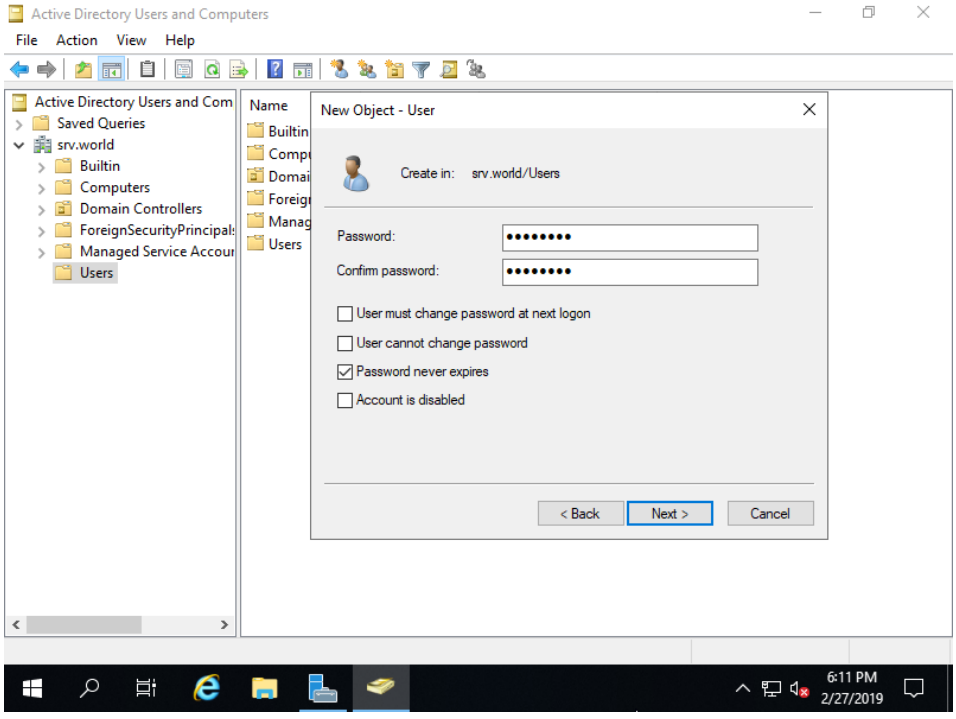
2. Right-Click **Users** on left tree and select **New** - **User**.



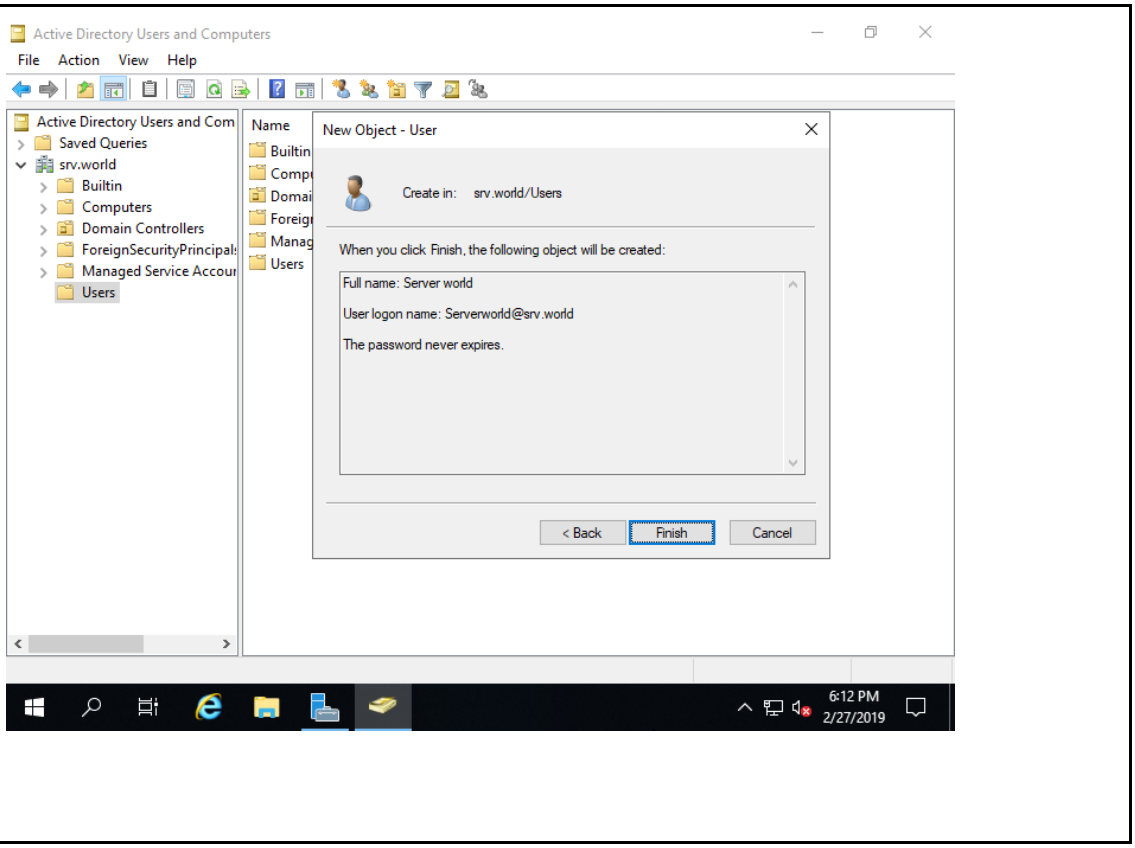
3. Input Username and Logon name for a new user.



4. Set initial password for a new User.



5. Check contents you set and click **Finish** button.



Points to Remember

- Understanding the types of GPOs and their hierarchical processing order is essential for effective management of policy settings in Windows Server environments
- **The steps of Joining Windows Server to An Active Directory Domain**
    1. click on Server Manager
    2. click on Local Server
    3. , click on the server's current computer name or the workgroup name.
    4. click the Change button
    5. Select the Domain option. Enter the name of the domain to which you want to join the server. Then click OK
    6. Enter the username and password of an account with domain join privileges. Then click OK

Application of learning 2.4.

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for installing Active Directory Domain Services promote windows server AD to DC

Learning outcome 2 end assessment

Written assessment

Multiple choice questions: Circle the letter corresponding to the correct answer:

1. What is the primary function of Active Directory Domain Services (AD DS)?
    a) To manage network resources and user accounts.
    b) To provide network security.
    c) To facilitate remote access to network resources.
    d) All of the above.
2. A hierarchical structure of domains that share a common namespace is known as a(n):
    a) Forest
    b) Tree
    c) Organizational Unit (OU)
    d) Domain
3. What is the role of a Domain Controller (DC)?
    a) To store and replicate Active Directory database.
    b) To authenticate users and computers.
    c) To authorize access to network resources.
    d) All of the above.
4. Which of the following is NOT a core component of Active Directory?
    a) Schema
    b) Global Catalog
    c) DNS Server
    d) File Server
5. What is the purpose of a Global Catalog server?
    a) To store a complete copy of the Active Directory database.
    b) To provide a single point of contact for user authentication.
    c) To store a partial copy of the Active Directory database, including attributes of all objects in the forest.
    d) To store user profiles and settings.
6. What is the process of transferring changes to Active Directory objects between Domain Controllers called?
    a) Replication
    b) Synchronization
    c) Propagation
    d) Mirroring
7. Which of the following is a security mechanism used in Active Directory to control access to resources?
    a) Kerberos

b) NTLM
c) Access Control Lists (ACLs)
d) All of the above.

8. What is the primary tool used to manage Active Directory?
    a) Active Directory Users and Computers
    b) Microsoft Management Console (MMC)
    c) PowerShell
    d) All of the above.
9. Which of the following is NOT a common AD DS administrative task?
    a) Creating and managing user accounts
    b) Configuring Group Policy Objects (GPOs)
    c) Managing DNS records
    d) Installing network drivers
10. What is the primary tool used to troubleshoot Active Directory replication issues?
    a) Repadmin
    b) DCDIAG
    c) Netdiag
    d) Event Viewer

Practical assessment

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for Configuring Active Directory and Joining client Computer to the domain.

References

Richards, J., Allen, R., & Lowe-Norris, A. G. (2006). *Active Directory*. O'Reilly Media, Inc.

Allen, R., & Lowe-Norris, A. (2003). *Active Directory*. O'Reilly Media, Inc.

Clines, S., & Loughry, M. (2008). *Active Directory for dummies*. John Wiley & Sons.

InvGate. (n.d.). *How to set up Active Directory*. Retrieved January 8, 2025, from https://blog.invgate.com/how-to-set-up-active-directory

PrimeKey. (n.d.). *Microsoft Auto Enrollment Configuration Guide: Part 1 - Configure Active Directory Domain Services*. Retrieved January 8, 2025, from https://doc.primekey.com/ejbca/ejbca-operations/ejbca-operations-guide/ca-operations-guide/enrollment-protocol-configuration/microsoft-auto-enrollment-operations/microsoft-auto-enrollmet-configuration-guide/part-1-configure-active-directory-domain-services

Keyfactor. (n.d.). *Part 1x: Configure Active Directory Domain Services*. Retrieved January 8, 2025, from https://docs.keyfactor.com/ejbca/latest/part-1x-configure-active-directory-domain-services

Jotelulu. (n.d.). *How to configure AD DS on your Windows Server*. Retrieved January 8, 2025, from https://jotelulu.com/en-gb/support/tutorials/how-to-configure-ad-ds-on-your-windows-server/

Microsoft. (n.d.). *Create an Active Directory server*. Retrieved January 8, 2025, from https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/create-an-active-directory-server

Microsoft. (n.d.). *Troubleshoot errors when joining a computer to a domain*. Retrieved January 8, 2025, from https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/troubleshoot-errors-join-computer-to-domain

Microsoft. (n.d.). *Install Active Directory Domain Services (Level 100)*. Retrieved January 8, 2025, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100


TESTING

Indicative contents
3.1 Installation of DHCP Services **3.2 Configuration of DHCP** **3.3 Testing DHCP Configuration**

Key Competencies for Learning Outcome 3: Deploy DHCP services

Knowledge	Skills	Attitudes
● Description DHCP concept ● Description of DHCP operations.	● Performing DHCP installation. ● Configuring DHCP scopes, IP ranges, and options (default gateway, DNS server). ● Enabling the DHCP server ● Start DHCP Service ● Testing DHCP Configuration.	● Being patience ● Being problem solver ● Working in a Team

Duration:10 hrs

Learning outcome 3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe properly DHCP operations based on Microsoft standard.
2. Perform correctly DHCP installation based on organisation requirements.
3. Configure clearly DHCP server as used in organisation.
4. Test effectively DHCP configuration based on organization requirement.

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS ● Router ● Switch	● Modem ● Router ● VMware Workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD ● USB	● Electricity ● Cables ● Internet

Indicative content 3.1: Installation of DHCP Services

Duration: 3 hrs

Theoretical Activity 3.1.1: Description of DHCP operations

Tasks:

1: Answer the following questions:

i. What do you understand by DHCP services?

ii. Explain DHCP operation performed to assign IP address to the client?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

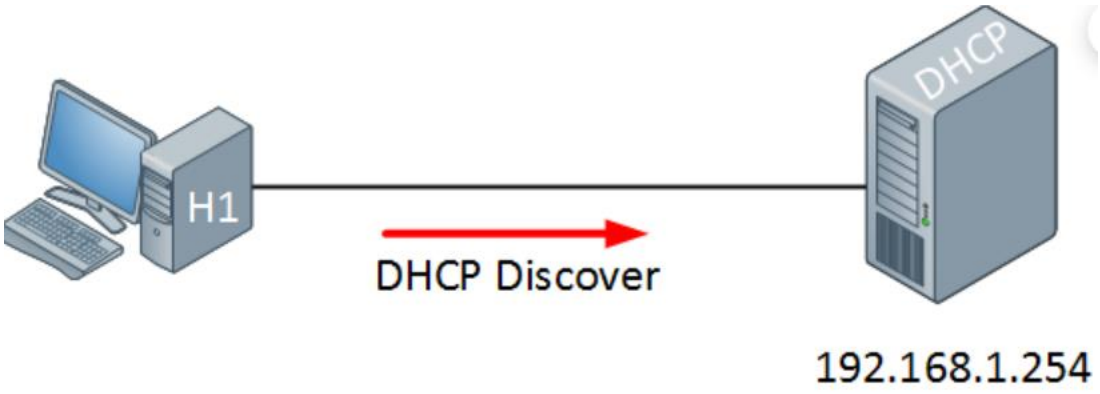
5: Read the key readings 3.1.1.

Key readings 3.1.1: Description of DHCP operations

1. Description of windows server

1.1. DHCP Discover

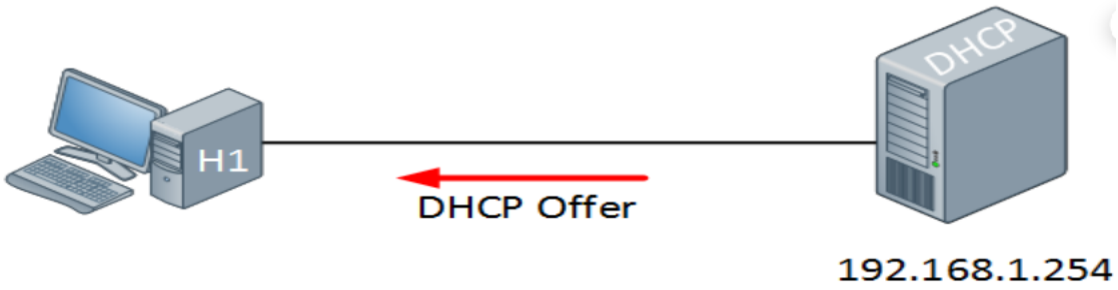
A DHCP server (Dynamic Host Configuration Protocol) is a server that automatically assigns IP addresses to computers and other devices on the network. When a client (PC) is booted, it broadcasts a DHCP Discover message over the Ethernet network to locate all available DHCP servers on the same subnet network (by setting the destination MAC address in the Ethernet header as Broadcast MAC=FF:FF:FF:FF:FF:FF), reaching all the DHCP servers on the same subnet network.



1.2 DHCP Offer

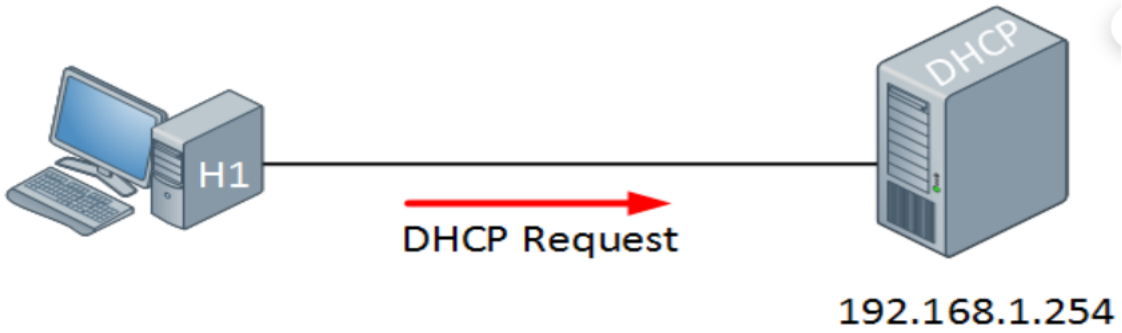
When a DHCP server receives the DHCP Discover message from the client, it also broadcasts a DHCP Offer message over the Ethernet network (because the client IP address has not been allocated yet), informing the client that it is available. This

message contains the network information, such as client IP address, subnet mask, default gateway IP address, DNS IP address, IP lease time and DHCP server IP address. The DHCP Offer message broadcasted is delivered to all the clients on the same subnet network, including the one that sent the DHCP Discover message.



1.3 DHCP Request

The client, having received the DHCP Offer message, recognizes there is a DHCP server available on the same subnet. Then it broadcasts a DHCP Request message to the server over the Ethernet network, requesting network configuration data including an IP address for itself. If more than one DHCP server responds on the same subnet and hence the client receives multiple DHCP Offer messages, it selects one of the DHCP servers, and enters the IP address of the selected DHCP server in the DHCP Server Identifier (option 54) field of the DHCP Request message. Then it informs all the DHCP servers on the subnet network about such selection by broadcasting the DHCP Request message. Typically, all DHCP servers internally store the network configuration data (i.e. IP address for the client and other information) when they send a DHCP Offer message. So, the client broadcasts the DHCP Request message to all the DHCP servers, so that those not selected can also receive the message and delete the stored network configuration data from their memory.



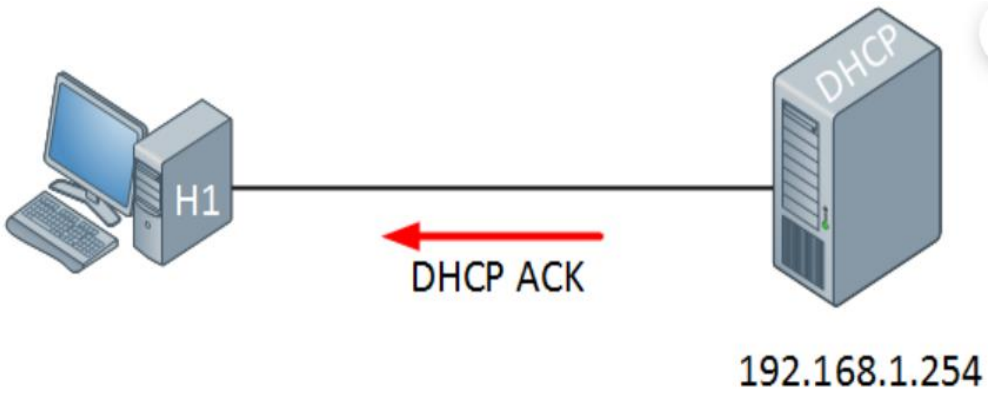
1.4 DHCP Acknowledgement

The DHCP server which received the DHCP Request message from the client checks if the IP address shown in the DHCP Server Identifier (option 54) field matches its own. If it does, it broadcasts a DHCP Ack message ensuring the client can receive

the message (Note: the client has NOT been allocated an IP address yet).

At this time, the DHCP server transfers all the network configuration data including the client IP address – the same data sent along with the DHCP Offer message - to the client. Then the client configures a network interface using the transferred data, finally connecting to the Internet. The typical network configuration data includes:

- IP address
- Subnet mask
- Default gateway IP address
- DNS server IP address
- Lease time (during which a client can use the IP address allocated/leased by a DHCP server)



Points to Remember

- Dynamic IP address assigning is performed by DHCP server by using DHCP discover, offer, lease, request and acknowledgement as main DHCP process.

Practical Activity 3.1.2:Performing DHCP installation

Task:

1: Referring to the previous theoretical activities (3.1.1) As a sever administrator, you are asked to go to the computer lab to install DHCP role and DHCP server.
2: Present the procedures of all step performed installation.
3: Present your work to the trainer and whole class.
4: Read key reading 3.1.2 and ask clarification where necessary
5: Perform the task provided in application of learning 3.1.2

Key readings 3.1.2 Performing DHCP installation

1.Perform DHCP installation process

A DHCP server (Dynamic Host Configuration Protocol) is a server that automatically assigns IP addresses to computers and other devices on the network. Without a DHCP server, each device on the network would need to be manually configured with an IP address.

Prerequisites:

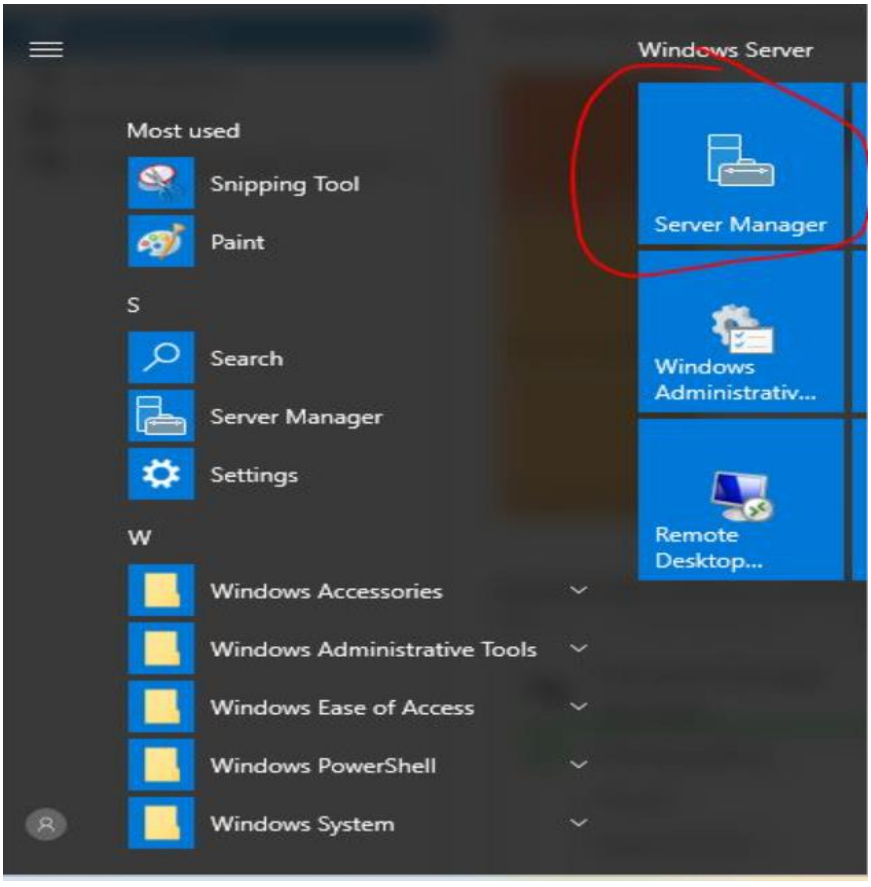
Before you can install your DHCP server, you must meet the following prerequisites:

- A computer running a supported version of Windows Server.
- A static IPv4 address.
- An IP address range for your DHCP scope.
- An account that's a member of the Administrators group, or equivalent.

This guide was created using Windows Server 2016. The steps should be similar for other server versions.

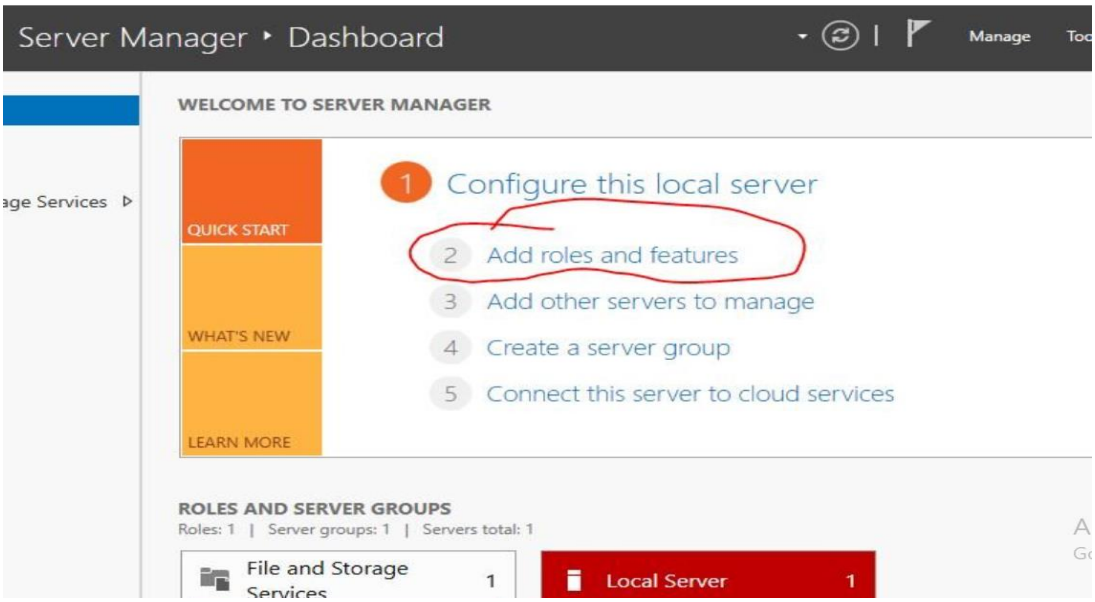
Step 1: Open Server Manager

Click the start button then click the Server Manager

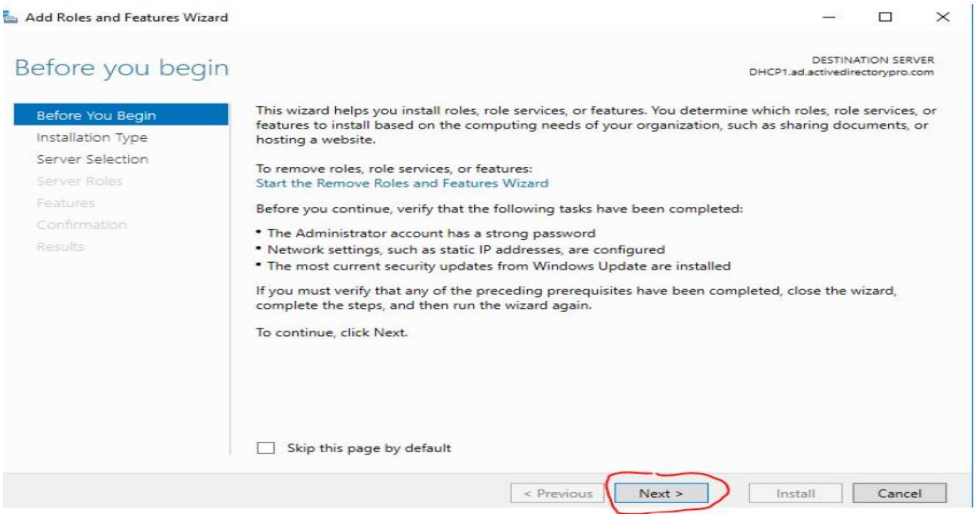


Step 2: Add roles and features

On the server manager dashboard click “Add roles and features” This will start the add roles and features wizard

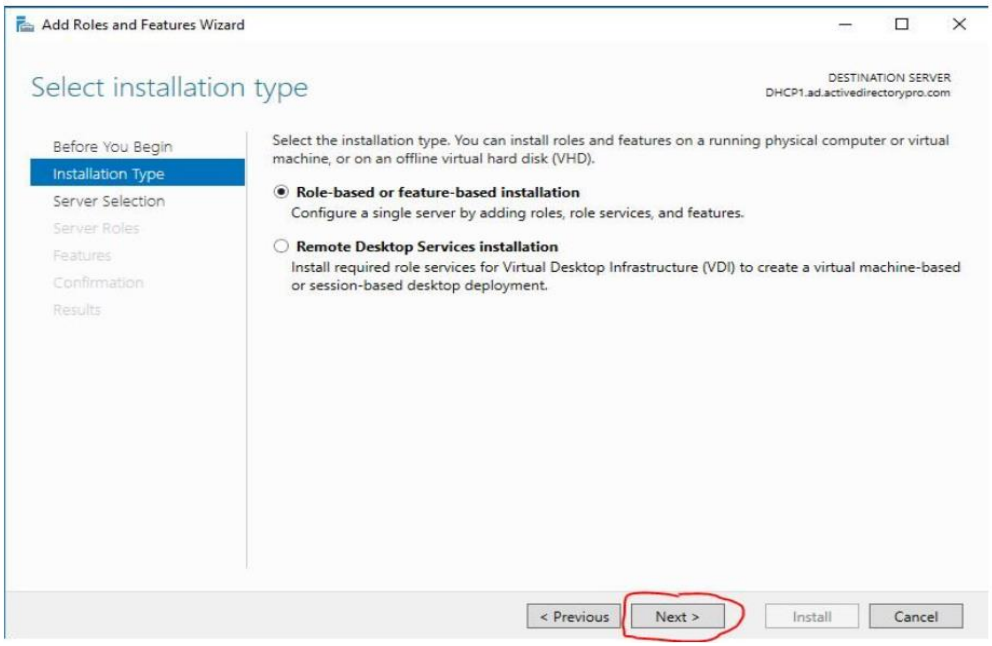


Click next on the before you begin page.



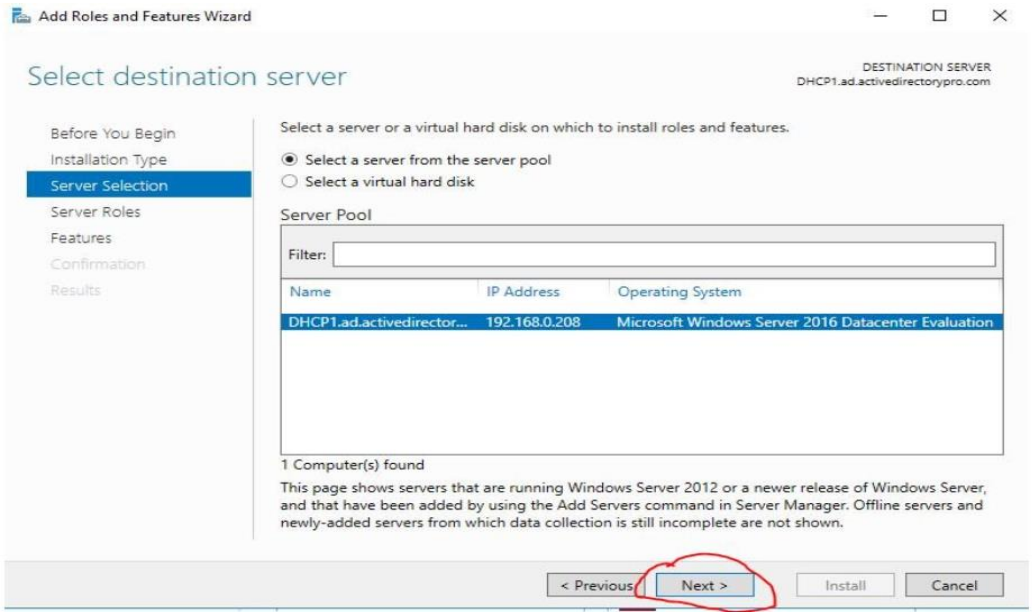
Step 3: Select Role-based or feature-based installation

Make sure “Role-based or feature-based installation is selected and click next



Step 4: Select the destination server

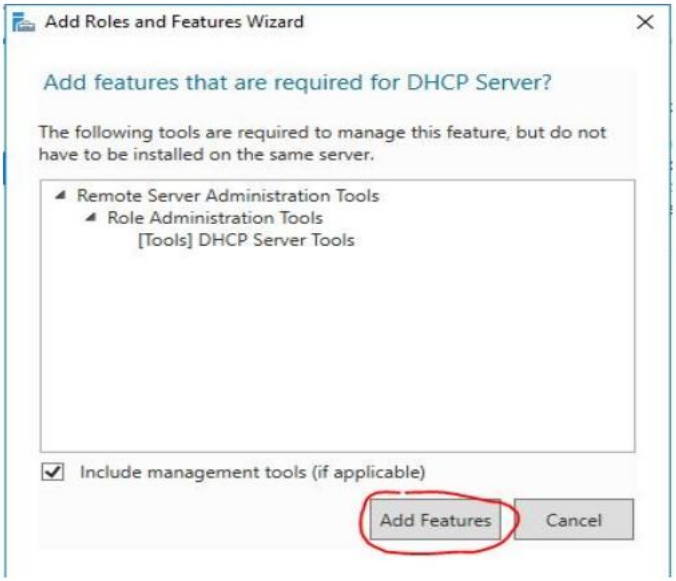
On this page choose the server you want the DHCP service installed on. In this example, I'll be choosing the local server.



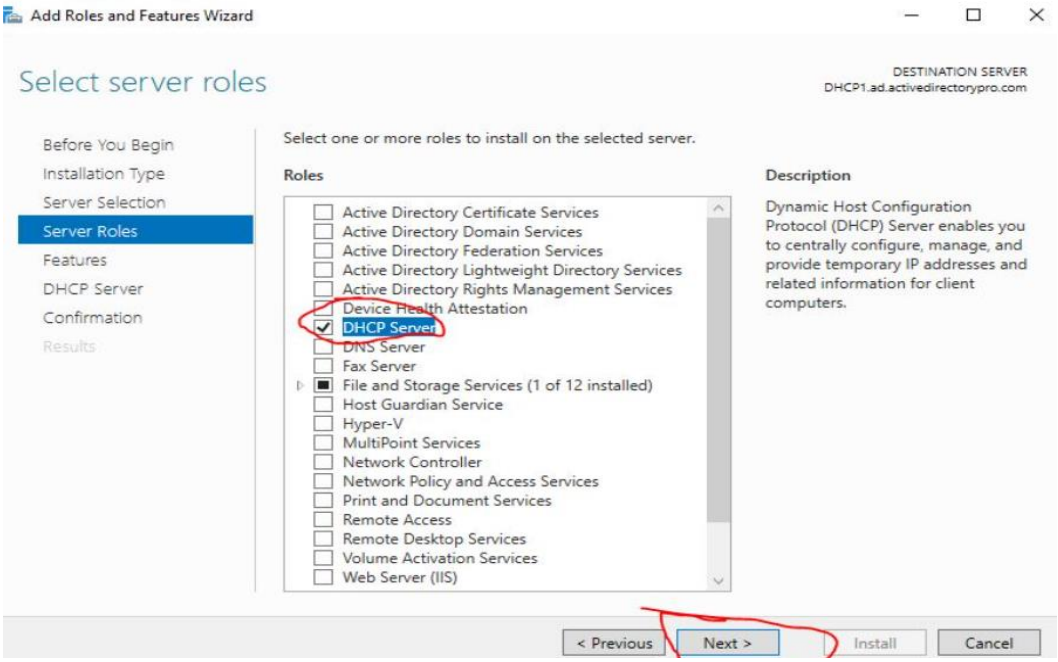
Step 5: Select server roles

On this page, you want to select the DHCP server roles and click next.

When you select the roll you will get a pop up asking to add features that are required for DHCP server. Click add features



Back on the select server roles page click next



Step 6: Feature, DHCP Server

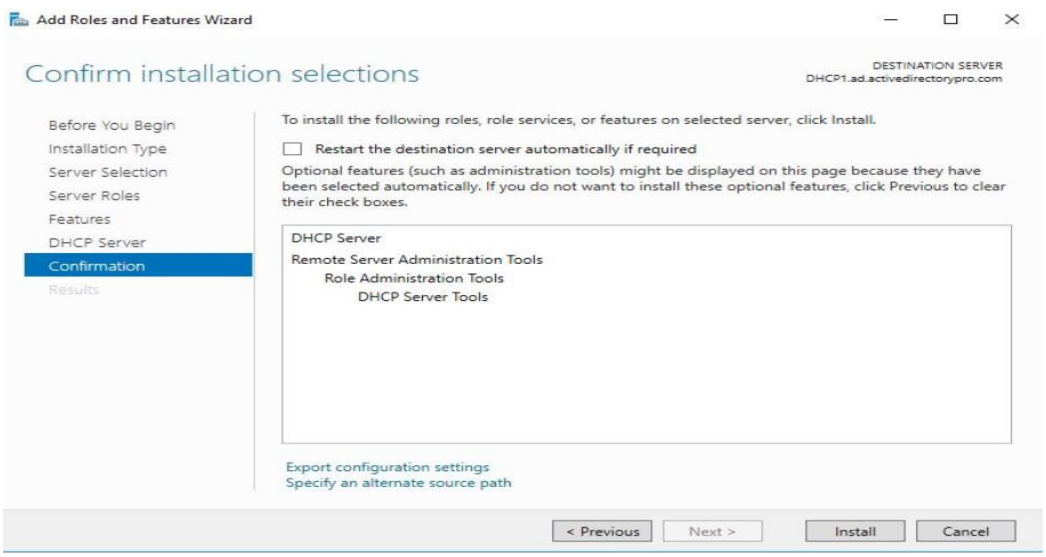
On the features screen click next

On the DHCP server click next

Step 7: Confirmation

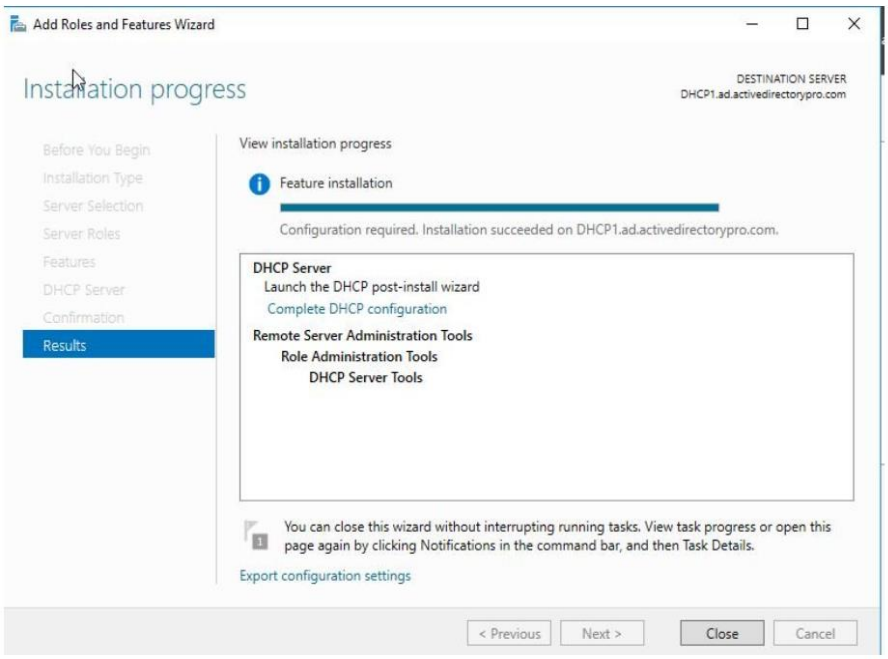
On the confirmation page, you can select to automatically restart the server if required.

On 2016 server it does not require a restart.



Click install and the install will start.

You will get an install progress page, it will say install succeeded when complete.



That completes the install of the DHCP role. Move onto the next section for steps on configuring the DCHP server.

2.Installation of DHCP roles

How to Install DHCP Server

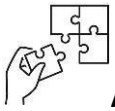
1. Step 1: Open Server Manager. Click the start button then click the Server Manager.
2. Step 2: Add roles and features.
3. Step 3: Select Role-based or feature-based installation.
4. Step 4: Select the destination server.
5. Step 5: Select server roles.

6. Step 6: Feature, DHCP Server.
7. Step 7: Confirmation.

Points to Remember

- During installation of DHCP server be carefully to select HDCP server roles and then you have to consider the following steps:

  Step 1: Open Server Manager. Click the start button then click the Server Manager.
  Step 2: Add roles and features.
  Step 3: Select Role-based or feature-based installation.
  Step 4: Select the destination server.
  Step 5: Select server roles.
  Step 6: Feature, DHCP Server.
  Step 7: Confirmation.



Application of learning 3.1

Suppose that your school needs to establish DHCP server, you are asked to install DHCP role and DHCP services for assign IP address to the computer lab's devices.
All tools, materials and equipment are available in computer lab.

Indicative content 3.2: Configuration of DHCP

Duration:4 hrs

Practical Activity 3.2.1: Configuring DHCP based on Microsoft

Task:

1: Referring to the key reading 3.1.2, As an internet and networking technology student, you are asked to go to the computer lab to configure DHCP server.

2: Present the procedures of all steps performed installation.

3: Present your work to the trainer and whole class.

4: Read key reading 3.1.2 and ask clarification where necessary

5: Perform the task provided in application of learning 3.2

Key readings 3.2.1 Configure DHCP based on Microsoft Standard

1. Enable the DHCP server

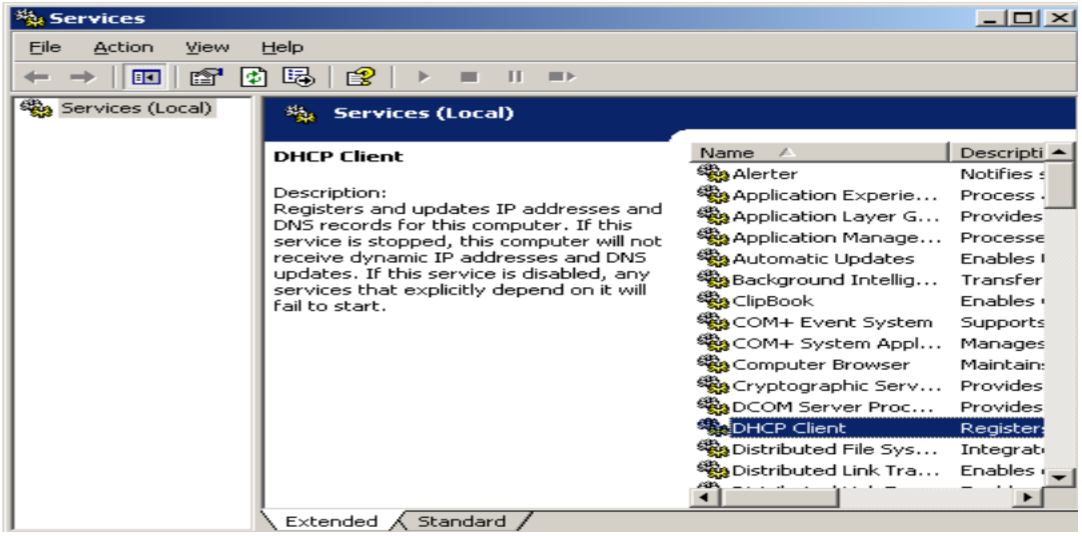
1.1. Enabling DHCP Client Service

For Windows Server 2012: run Windows PowerShell.

Then, execute the following command:

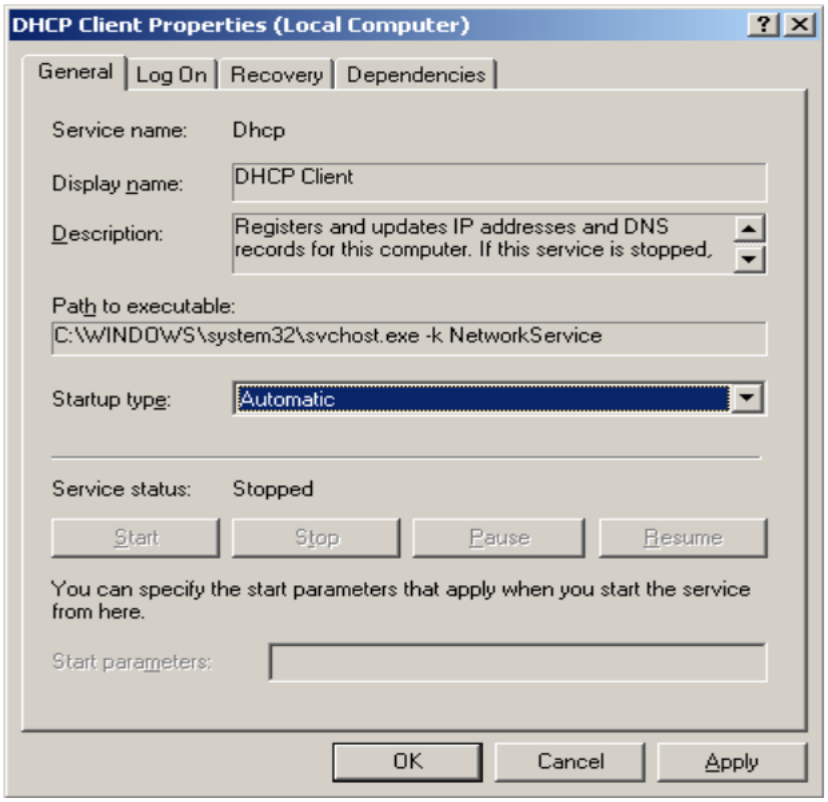
```
services.msc
```

In the Services management console, right-click the DHCP Client service.



In the opened menu, select **Properties**. The **DHCP Client Properties** dialog box opens.

In the **Startup type** drop-down box select **Automatic**.



Click Apply. The Start button becomes active.

Click the Start button.

After the indication bar disappears, click OK to close the dialog box.

2.Scope Configuration

After you have installed the DHCP service and started it, you must create a scope. The scope is a range of valid IP addresses available for lease to the DHCP client computers on the network. Microsoft recommends that, each DHCP server in your environment has at least one scope that does not overlap with any other DHCP server scope in your environment. In Windows Server 2003, DHCP servers in an Active Directory-based domain must be authorized to prevent *rogue* DHCP servers from coming online. Any Windows Server 2003 DHCP Server that determines itself to be unauthorized will not manage clients.

2.1. Create a New Scope

Step 1: Click Start, point to Programs, point to Administrative Tools, and then click DHCP.

Step 2: In the console tree, right-click the DHCP server on which you want to create the new DHCP scope, and then click New Scope.

Step 3: In the New Scope Wizard, click Next, and then type a name and description for the scope. The name can be anyone that you want, but it should be descriptive enough so that you can identify the purpose of the scope on your network (for example, you can use a name such as "Administration Building Client Addresses"). Click Next.

Step 4: Type the range of addresses that can be leased as part of this scope. For example, use a range of IP addresses from a starting IP address of 192.168.100.1 to an ending address of 192.168.100.100. Because these addresses are given to clients, they must all be valid addresses for your network and not currently in use. If you want to use a different subnet mask, type the new subnet mask. Click Next.

Step 5: Type any IP addresses that you want to exclude from the range that you entered. These addresses include any one in the range described in step 4 that may have already been statically assigned to various computers in your organization. Typically, domain controllers, Web servers, DHCP servers, Domain Name System (DNS) servers, and other servers, have statically assigned IP addresses. Click Next.

Step 6: Type the number of days, hours, and minutes before an IP address lease from this scope expires. It determines how long a client can hold a leased address without renewing it. Click Next, and then click Yes, I want to configure these options now to extend the wizard to include settings for the most common DHCP options. Click Next.

Step 7: Type the IP address for the default gateway that should be used by clients that obtain an IP address from this scope. Click Add to add the default gateway address in the list, and then click Next.

Step 8: If you are using DNS servers on your network, type your organization's domain name in the Parent domain box. Type the name of your DNS server, and then click Resolve to make sure that your DHCP server can contact the DNS server and determine its address. Click Add to include that server in the list of DNS servers that are assigned to the DHCP clients. Click Next, and then follow the same steps. If you are using a Windows Internet Naming Service (WINS) server, by adding its name and IP address, click Next.

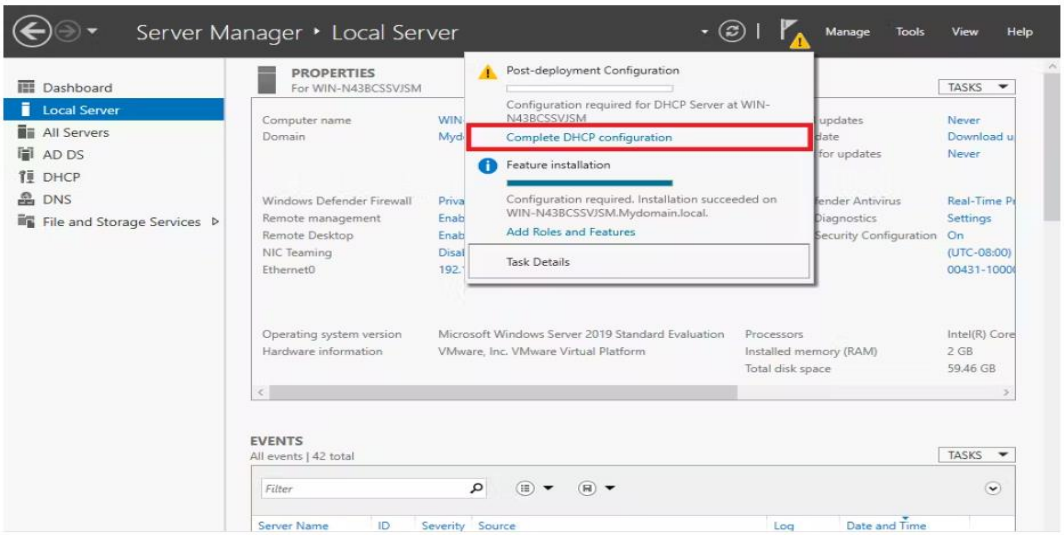
Step 9: Click Yes, I want to activate this scope now to activate the scope and allow clients to obtain leases from it, and then click Next.

Step 10: Click Finish.

Step 11: In the console tree, click the server's name, and then click Authorize on the Action menu.

Create IPv4 DHCP Scope:

- After installing the DHCP Server role, go back to Server Manager.
- In Server Manager, you'll see a yellow flag indicating that DHCP needs to be configured. Click on the flag or open the DHCP Server app directly from the Tools menu.



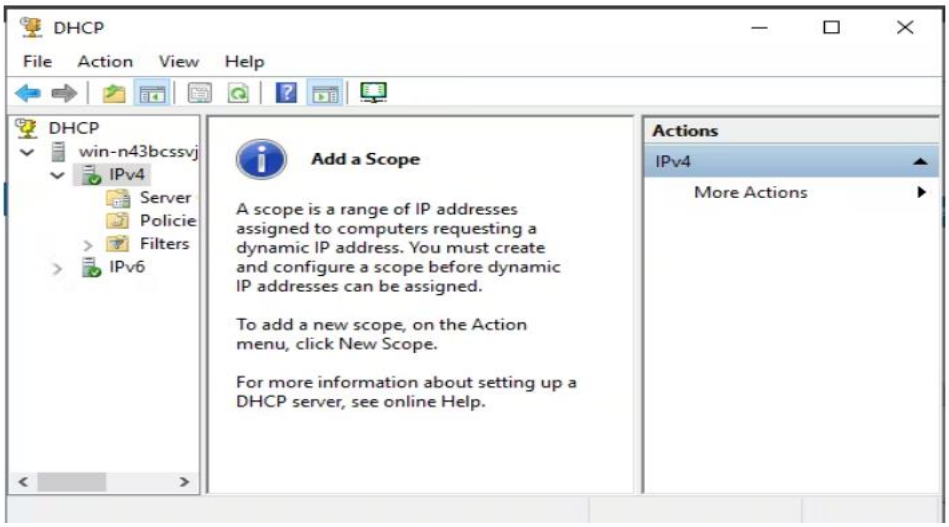
Authorize the DHCP Server:

•In the DHCP Server app, right-click on the DHCP server node in the left-hand pane and select "Authorize."

•Authorization is necessary to prevent unauthorized DHCP servers from assigning IP addresses on your network.

Create a DHCP Scope:

•In the DHCP Server app, right-click on the "IPv4" node in the left-hand pane and select "New Scope." The New Scope Wizard will open.



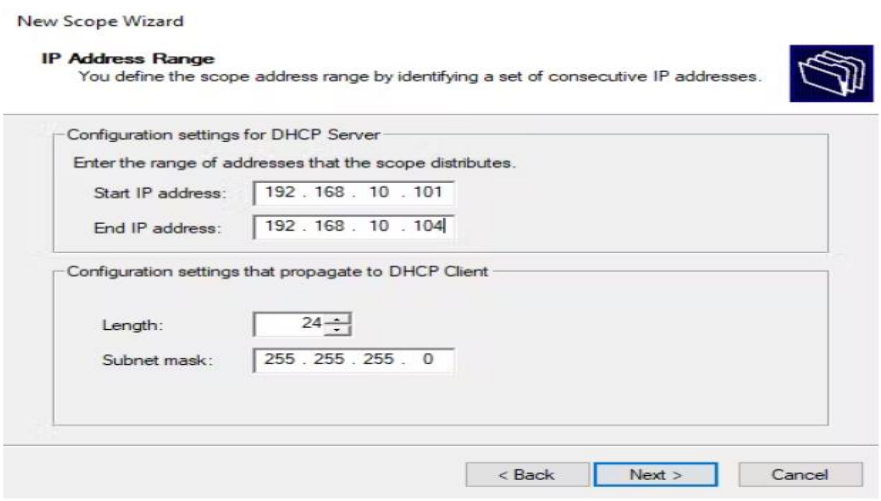
Follow the wizard to set up the scope:

•Provide a name and description for the scope.

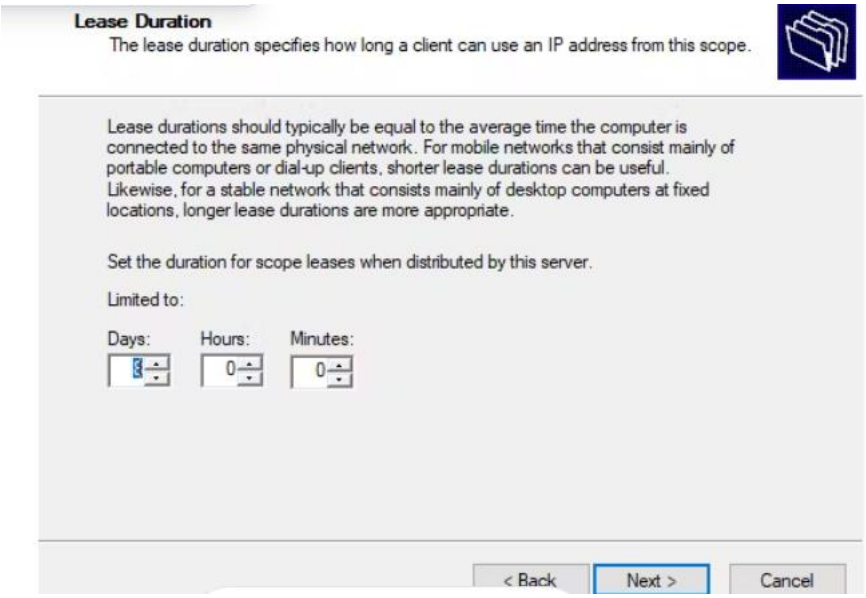
•Specify the range of IP addresses to be used in the scope.

•Set the subnet mask and default gateway.

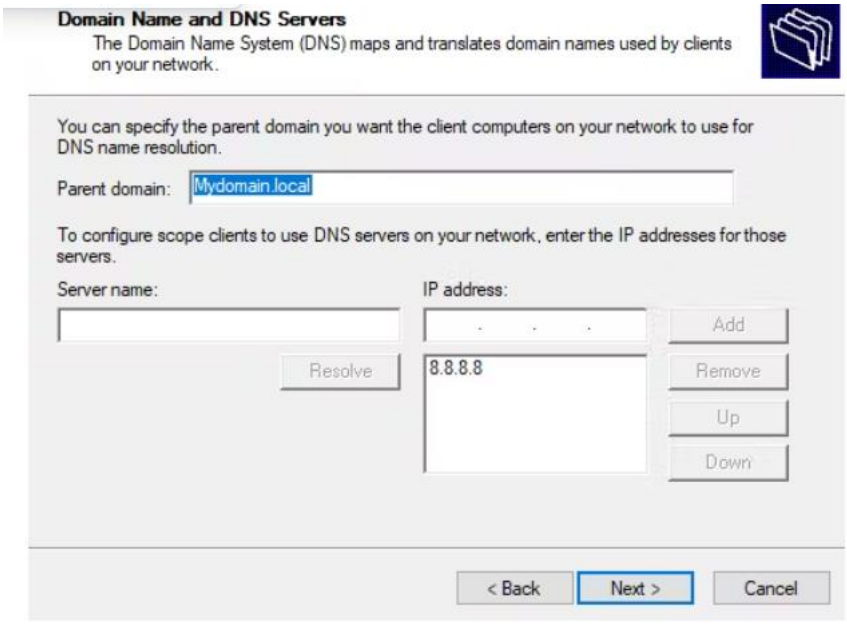
2.2. Range of IP address



2. Define the lease duration (how long IP addresses will be assigned to clients).

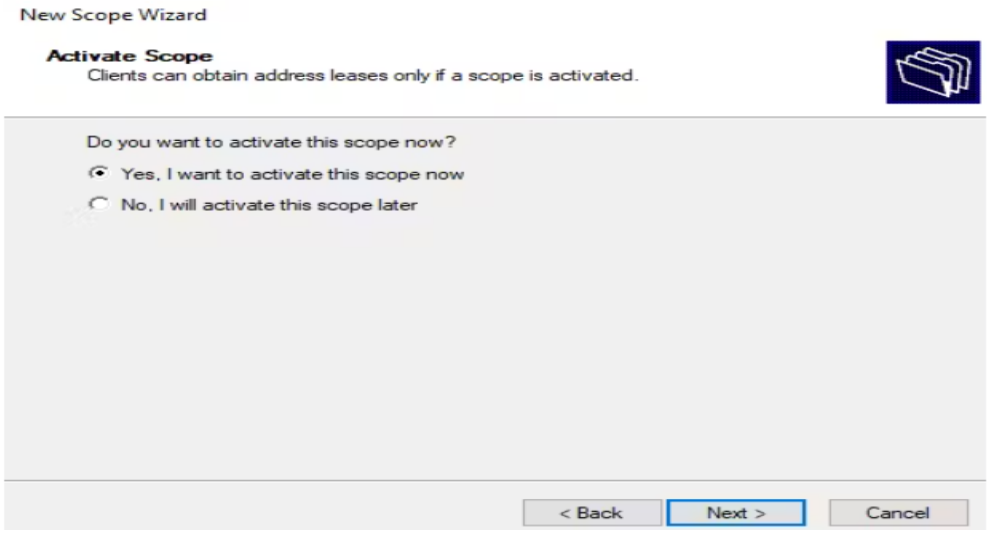


3. Specify any additional options, such as DNS server addresses.



Activate the Scope:

- After creating the scope, right-click on the scope name in the left-hand pane and select "Activate."
- This makes the scope available for assigning IP addresses to clients.



Configure DHCP Reservations:

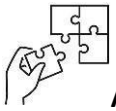
- Reservations allow you to assign specific IP addresses to particular devices based on their MAC addresses. This is useful for devices that require consistent IP addresses, such as printers or servers.

2.3. Start DHCP service

Right-click on DHCP Server and select Start if the service is not already running. If it is running and you need to restart it, select Restart instead.

Points to Remember

- The scope must be activated in order to broadcast IP address to the client.
- Use valid scope IP address range.
- During configuration of DHCP server scope be carefully to the following steps:
  1. open the DHCP management tool, and expand the tree on the left-hand side until you find IPv4. **Right-click on IPv4** (or IPv6 if this is what you're using) **and click on "New scope"**.
  2. **Click on "Next" to continue** .
  3. **Give a name and description for your new scope** .
  4. On the next screen, you will be asked to **enter a range of IP addresses**. These are the IP addresses that will be available for DHCP clients connected to this scope. All you need to do is **enter a start and an end IP address** .
  5. Assign a range of IP addresses and a subnet mask for your new DHCP scope
  6. Specify any excluded IP addresses within your IP range
  7. Set a lease duration for your new scope
  8. Choose to configure your DHCP options now
  9. Configure the default gateway for the scope
  10. Enter the domain name and DNS servers
  11. Add the WINS servers for your new scope
  12. Choose whether to activate the scope now or later
  13. finish



Application of learning 3.2.

Suppose that your school needs to establish DHCP server, you are asked to configure DHCP server by creating scope called **'I4NIT'** and assign IP address from range of 192.168.16.100 to 192.168.16.200 and DNS server address in 192.168.16.1.

Indicative content 3.3: Testing DHCP Configuration

Duration: 3 hrs

Practical Activity 3.3.1: Testing DHCP Configuration

Task:

1: Referring to the key reading 3.2.1, As an internet and networking technology student, you are asked to go to the computer lab to test DHCP configuration to assure that server is running properly.

2: Present the procedures of all step performed installation.

3: Present your work to the trainer and whole class.

4: Read key reading 3.3.1 and ask clarification where necessary

5: Perform the task provided in application of learning 3.3

Key readings 3.3.1: Testing DHCP Configuration

1.Start DHCP Service

Step 1. Open Server Manager: Click on the **Start** button, Select **Server Manager** from the list.

Step 2. Access DHCP Management Console: In Server Manager, navigate to **Tools** in the upper right corner, Click on **DHCP** to open the DHCP management console.

Step 3. Check Service Status: In the DHCP console, locate your DHCP server in the left pane, Right-click on your server's name and select **Properties**. Ensure that the **Service Status** is set to **Started** and that the **Startup Type** is set to **Automatic**.

Step 4. Start the Service if Necessary: If the service is not running, right-click on your server's name again. Go to **All Tasks**, then select **Start** to initiate the DHCP service.

Step 5. Verify Operation: After starting the service, you can verify its operation by checking for leases in the DHCP console or using PowerShell commands like:

```
Get-DhcpServerv4Lease -ScopeId <YourScopeID>
```

2.Check IP address of the DHCP client or Client devices

2.1. Windows command line

Open a command prompt or Windows PowerShell console, and then type ipconfig /all. Look for a line in the output that reads DHCP Enabled and a corresponding Yes or No value. Yes, means the device is a DHCP client and receives its IP address configuration from a DHCP server. A little further below

in the output are the DHCP server's IP address and info about when the lease was obtained and expired. Administrators can refresh the DHCP lease by using two simple commands:

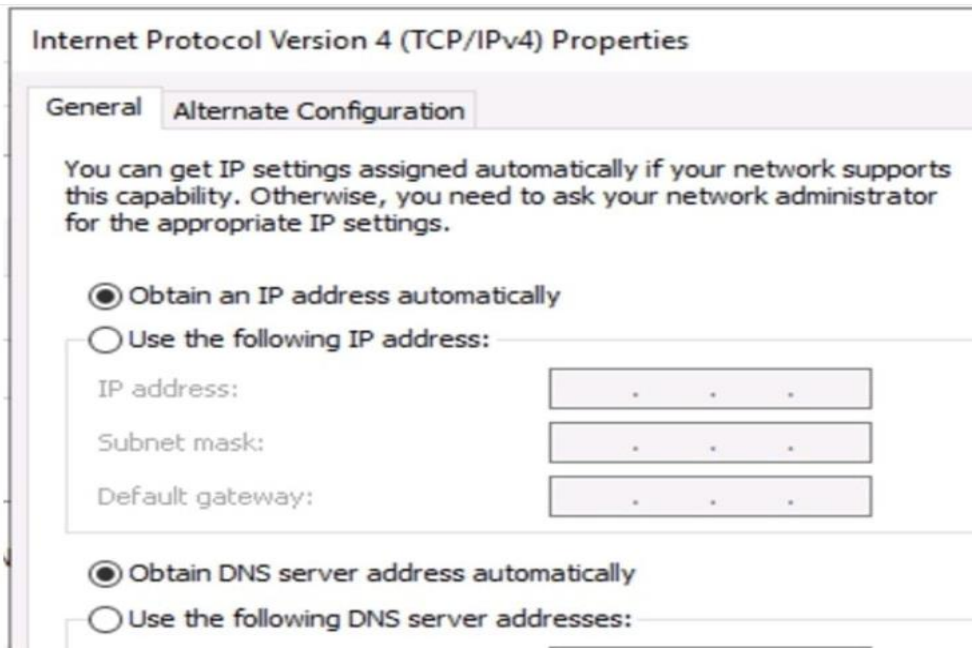
PS C:\> ipconfig /release

PS C:\> ipconfig /renew

The ipconfig /release command clears the current IP address configuration. The ipconfig /renew command causes the client to initiate the four-step DHCP lease generation process. This process provides the client with an updated IP address configuration, which likely includes the IP address, subnet mask, name resolution server and router information.

2.3. Windows GUI

For administrators who are more comfortable with the Windows GUI, various consoles display much of the same information. Admins can access network configuration information in Windows using several methods. On Windows Server, launch Server Manager, select Local Computer and then select the IP address information in the Ethernet entry. Likely, this information reads IPv4 address assigned by DHCP. The two available radio buttons configure the device as a DHCP client or a static IP address assignment.



To obtain a DHCP-assigned address:

- Type ipconfig /renew and press Enter to obtain a DHCP-assigned IP address.
- Use ipconfig /all to display all IP configuration information.
- Observe the updated DHCP lease information. The system should now have a valid IP address on the network, and the address will very likely be the same address as the one displayed in Activity 1.
- Close the command prompt to complete this activity.

3. Check IP addresses from the DHCP server

3.1. Check the following settings

- The DHCP server service is started and running. To check this setting, run the net start command, and look for DHCP Server.
- The DHCP server is authorized. See Windows DHCP Server Authorization in Domain
- Verify that IP address leases are available in the DHCP server scope for the subnet the DHCP client is on. To verify availability, see the statistic for the appropriate scope in the DHCP server management console.
- Check whether any BAD_ADDRESS listings can be found in Address Leases.
- Check whether any devices on the network have static IP addresses that haven't been excluded from the DHCP scope.
- Verify that the DHCP server binds to at least one IP address, and that this IP address is within the subnet of the scopes from which IP addresses must be leased out, unless using DHCP relay. To do this verification, run the Get-DhcpServerv4Binding or Get-DhcpServerv6Binding cmdlet. Server connection bindings are configured in the DHCP server management console under IPv4 / IPv6 Advanced Properties.
- Verify that only the DHCP server is listening on UDP port 67 and 68 by running the netstat -anb command. No other process or other services, such as WDS or PXE, should occupy these ports.
- Verify that the DHCP server IPsec exemption is added if you're dealing with an IPsec-deployed environment.
- Verify that the relay agent IP address can be pinged from the DHCP server.
- Enumerate and check configured DHCP policies and filters.

3.2. Event logs

Check the System and DHCP Server service event logs at Applications and Services Logs > Microsoft > Windows > DHCP-Server for reported issues that are related to the observed problem.

Depending on the kind of issue, an event is logged to one of the following event channels:

- DHCP Server Operational Events
- DHCP Server Administrative Events
- DHCP Server System Events
- DHCP Server Filter Notification Events
- DHCP Server Audit Events

3.3. DHCP Server log

The DHCP Server debug logs provide more information about the IP address lease assignment and the DNS dynamic updates that are done by the DHCP server. These logs by default are located in %windir%\System32\Dhcp. For more information, see **Analyze DHCP Server Log Files.**

Points to Remember

- To test DHCP configuration check client side by using ipconfig with option like /all, /release and renew.
- Don't forget to check DHCP server settings, by run the net start command, and look for DHCP Server.

Application of learning 3.3

Suppose that your school needs to establish DHCP server, you are asked to test if DHCP server is able to assign IP address dynamic to client. The scope to test is called **'I4NIT'** and has IP address from range of 192.168.16.100 to 192.168.16.200 and DNS server address in 192.168.16.1.

Learning outcome 3 end assessment

Written assessment

Multiple choice questions: Circle the letter corresponding to the correct answer:

1.What does DHCP stand for?

a) Dynamic Host Configuration Protocol
b) Dynamic Host Control Protocol
c) Dynamic Hypertext Configuration Protocol
d) None of the above

2. What is the primary function of a DHCP server?

a) To assign static IP addresses
b) To provide dynamic IP addresses to clients
c) To manage DNS records
d) To control network traffic

3. Which of the following is a benefit of using DHCP?

a) Reduces manual configuration errors
b) Provides faster internet speeds
c) Increases network security
d) None of the above

4. What happens when a client requests an IP address from a DHCP server?

a) The server immediately assigns the IP address without confirmation.
b) The server sends a DHCP Offer message.
c) The client must wait indefinitely for an IP address.
d) The server denies the request.

5. How long is an IP address typically leased to a client by DHCP?

a) For an unlimited period
b) For a limited period
c) Until the server shuts down
d) Only during active sessions

6. What is a DHCP scope?

a) A range of IP addresses that the DHCP server can assign to clients
b) A security feature of the DHCP server
c) A method for reserving IP addresses for specific devices
d) None of the above

7. What is required before a DHCP server can lease IP addresses in an Active Directory environment?

a) The server must be rebooted.
b) The DHCP server must be authorized in Active Directory.
c) The server must have a static IP address.
d) Both b and c are correct.

8. How can you test if your DHCP server is functioning correctly?
    a) By checking the event logs only
    b) By connecting a client device configured to obtain an IP address automatically
    c) By manually assigning IP addresses to clients
    d) By disabling the DHCP service

Practical assessment

Our school needs to establish DHCP server for assign IP addresses to all computer lab's machine dynamically from 192.168.1.100 to 192.168.1.200. however, assigned a static IP address. This ensures that the server's IP address is assigned statically. Your task is to configure DHCP server according to required addresses.

References

Alcott, N. (2001). *DHCP for Windows 2000*. O'Reilly Media, Inc.

Krause, J. (2019). *Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities*. Packt Publishing Ltd.

Krause, J. (2016). *Mastering Windows Server 2016*. Packt Publishing Ltd.

Droms, R. (1999). Automated configuration of TCP/IP with DHCP. *IEEE Internet Computing, 3*(4), 45–53. https://doi.org/10.1109/4236.777449

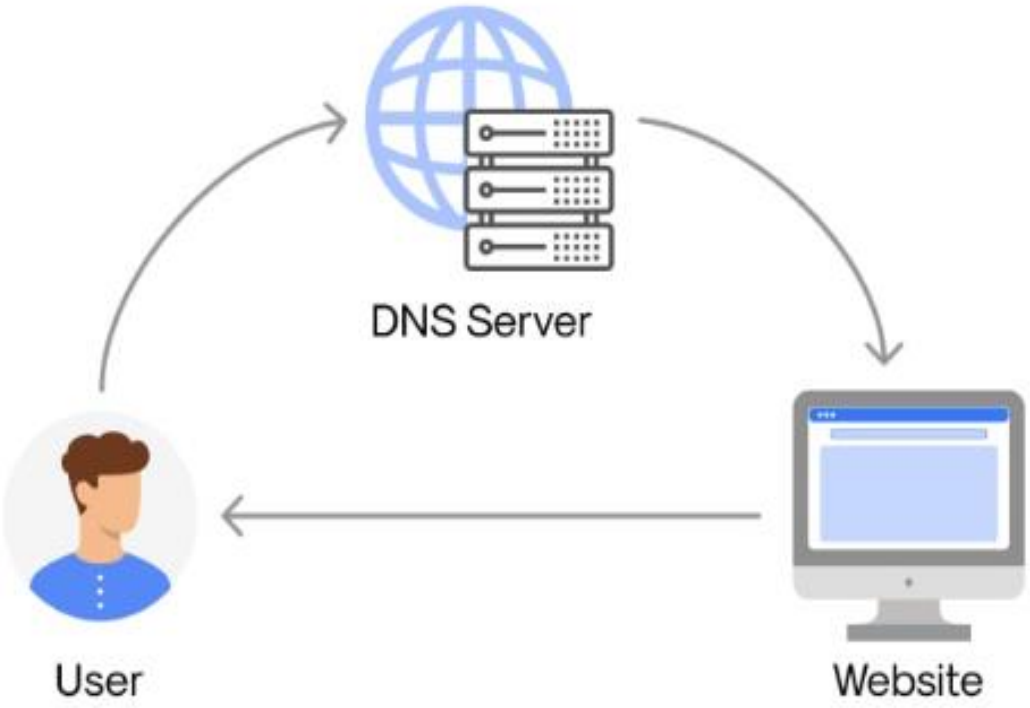
CSL Academy. (n.d.). *Windows Server interview questions*. Retrieved January 8, 2025, from https://csl.academy/job-interview-question/windows-server-interview-questions-3/

Saleem, F. (n.d.). *Setting up DHCP (Dynamic Host Configuration Protocol) on Windows Server 2019*. Retrieved January 8, 2025, from https://farkhandasaleem.hashnode.dev/setting-up-dhcp-dynamic-host-configuration-protocol-on-windows-server-2019

Jotelulu. (n.d.). *How to install DHCP server on Windows Server*. Retrieved January 8, 2025, from https://jotelulu.com/en-gb/support/tutorials/how-to-install-dhcp-server-on-windows-server/

Microsoft. (n.d.). *Install and configure a DHCP server in a workgroup*. Retrieved January 8, 2025, from https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/install-configure-dhcp-server-workgroup

Microsoft. (n.d.). *Quickstart: Install and configure a DHCP server*. Retrieved January 8, 2025, from https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server


DNS Server
User
Website

Indicative contents
4.1 Installation of DNS service **4.2 Configuration of DNS Settings** **4.3 Testing of DNS Configuration**

Key Competencies for Learning Outcome 4: Deploy DNS service

Knowledge	Skills	Attitudes
• Description of DNS records • Description of DNS queries • Description of DNS zones and zone files • Choose a DNS Hosting Provider	• Performing DNS installation. • Configuring of DNS Settings • Testing DNS configuration.	• Having Attention to detail • Being Adaptive • Being collaborative

Duration: 10 hrs

Learning outcome 4 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly DNS records as used in DNS server.
2. Install properly DNS server based on organization requirements.
3. Configure properly DNS server based on DNS records.
4. Test properly DNS server according to the domain functionality.

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS ● Router ● Switch	● Modem ● VMware Workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD ● USB	● Electricity ● Cables ● Internet

Indicative content 4.1: Installation of DNS Service

Duration: 4 hrs

Theoretical Activity 4.1.1: Description of DNS records

Tasks:

1: Answer the following questions**:**

i. What do you understand by DNS service?

ii. What do you understand by CNAME and PTR?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 4.1.1.

Key readings 4.1.1: Description of DNS records

1.Definitions

1.1. A record

The "A" stands for "address" and this is the most fundamental type of DNS record: it indicates the IP address of a given domain. For example, if you pull the DNS records of cloudflare.com, the A record currently returns an IP address of: 104.17.210.9. A record only holds IPv4 addresses. If a website has an IPv6 address, it will instead use an "AAAA" record.

Here is an example of an A record:

example.com	record type:	value:	TTL
@	A	192.0.2.1	14400

The "@" symbol in this example indicates that this is a record for the root domain, and the "14400" value is the TTL (time to live), listed in seconds. The default TTL for A records is 14,400 seconds. This means that if an A record gets updated, it takes 240 minutes (14,400 seconds) to take effect.

The vast majority of websites only have one A record, but it is possible to have several. Some higher profile websites will have several different A records as part of a technique called round robin load balancing, which can distribute request traffic to one of several IP addresses, each hosting identical content.

•Use of DNS A records

The most common usage of A records is IP address lookups: matching a domain name (like "cloudflare.com") to an IPv4 address. This enables a user's device to

connect with and load a website, without the user memorizing and typing in the actual IP address. The user's web browser automatically carries this out by sending a query to a DNS resolver.

DNS A records are also used for operating a Domain Name System-based Blackhole List (DNSBL). DNSBLs can help mail servers identify and block email messages from known spammer domains.

1.2. DNS CNAME record

A "canonical name" (CNAME) record points from an alias domain to a "canonical" domain. A CNAME record is used in lieu of an A record, when a domain or subdomain is an alias of another domain. All CNAME records must point to a domain, never to an IP address. Imagine a scavenger hunt where each clue points to another clue, and the final clue points to the treasure. A domain with a CNAME record is like a clue that can point you to another clue (another domain with a CNAME record) or to the treasure (a domain with an A record).

For example, suppose blog.example.com has a CNAME record with a value of "example.com" (without the "blog"). This means when a DNS server hits the DNS records for blog.example.com, it actually triggers another DNS lookup to example.com, returning example.com's IP address via its A record. In this case we would say that example.com is the canonical name (or true name) of blog.example.com.

Oftentimes, when sites have subdomains such as blog.example.com or shop.example.com, those subdomains will have CNAME records that point to a root domain (example.com). This way if the IP address of the host changes, only the DNS A record for the root domain needs to be updated and all the CNAME records will follow along with whatever changes are made to the root.

A frequent misconception is that a CNAME record must always resolve to the same website as the domain it points to, but this is not the case. The CNAME record only points the client to the same IP address as the root domain. Once the client hits that IP address, the web server will still handle the URL accordingly. So for instance, blog.example.com might have a CNAME that points to example.com, directing the client to example.com's IP address. But when the client actually connects to that IP address, the web server will look at the URL, see that it is blog.example.com, and deliver the blog page rather than the home page.

Example of a CNAME record:

blog.example.com	**record type:**	**value:**	**TTL**
@	CNAME	is an alias of example.com	32600

In this example you can see that blog.example.com points to example.com, and assuming it is based on our example A record we know that it will eventually

resolve to the IP address 192.0.2.1.

1.3. DNS MX record

A DNS 'mail exchange' (MX) record directs email to a mail server. The MX record indicates how email messages should be routed in accordance with the Simple Mail Transfer Protocol (SMTP, the standard protocol for all email). Example of an MX record:

example.com	record type:	priority:	value:	TTL
@	MX	10	mailhost1.example.com	45000
@	MX	20	mailhost2.example.com	45000

The 'priority' numbers before the domains for these MX records indicate preference; the lower 'priority' value is preferred. The server will always try mailhost1 first because 10 is lower than 20. In the result of a message send failure, the server will default to mailhost2.

The email service could also configure this MX record so that both servers have equal priority and receive an equal amount of mail:

example.com	record type:	priority:	value:	TTL
@	MX	10	mailhost1.example.com	45000
@	MX	10	mailhost2.example.com	45000

This configuration enables the email provider to equally balance the load between the two servers.

- **Process of querying an MX record**

Message transfer agent (MTA) software is responsible for querying MX records. When a user sends an email, the MTA sends a DNS query to identify the mail servers for the email recipients. The MTA establishes an SMTP connection with those mail servers, starting with the prioritized domains (in the first example above, mailhost1).

- **Backup MX record**

A backup MX record is just an MX record for a mail server with a higher 'priority' value (which means a lower priority), so that under normal circumstances mail will go to the more prioritized servers. In the first example above, mailhost2 would be the 'backup' server because email traffic will be handled by mailhost1 as long as it

is up and running.

•Can MX records point to a CNAME

A CNAME record is used for referencing a domain's alias instead of its actual name. CNAME records typically point to an A record (in IPv4) or AAAA record (in IPv6) for that domain. However, MX records have to point directly to a server's A record or AAAA record. Pointing to a CNAME is forbidden by the RFC documents that define how MX records function.

1.4. DNS PTR record

The Domain Name System, or DNS, correlates domain names with IP addresses. A DNS pointer record (PTR for short) provides the domain name associated with an IP address. A DNS PTR record is exactly the opposite of the 'A' record, which provides the IP address associated with a domain name.

DNS PTR records are used in reverse DNS lookups. When a user attempts to reach a domain name in their browser, a DNS lookup occurs, matching the domain name to the IP address. A reverse DNS lookup is the opposite of this process: it is a query that starts with the IP address and looks up the domain name.

•DNS PTR records stored

In IPv4:

While DNS A records are stored under the given domain name, DNS PTR records are stored under the IP address — reversed, and with ".in-addr.arpa" added. For example, the PTR record for the IP address 192.0.2.255 would be stored under "255.2.0.192.in-addr.arpa".

"in-addr.arpa" has to be added because PTR records are stored within the .arpa top-level domain in the DNS. .arpa is a domain used mostly for managing network infrastructure, and it was the first top-level domain name defined for the Internet. (The name "arpa" dates back to the earliest days of the Internet: it takes its name from the Advanced Research Projects Agency (ARPA), which created ARPANET, an important precursor to the Internet.)

in-addr.arpa is the namespace within .arpa for reverse DNS lookups in IPv4.

In IPv6:

IPv6 addresses are constructed differently from IPv4 addresses, and IPv6 PTR records exist in a different namespace within. arpa. IPv6 PTR records are stored under the IPv6 address, reversed and converted into four-bit sections (as opposed to 8-bit sections, as in IPv4), plus “. ip6.arpa".

1.5. DNS NS records

NS stands for ‘nameserver,’ and the nameserver record indicates which DNS server is authoritative for that domain (i.e. which server contains the actual DNS records). Basically, NS records tell the Internet where to go to find out a domain's IP address. A domain often has multiple NS records which can indicate primary and secondary nameservers for that domain. Without properly configured NS records, users will

be unable to load a website or application. Here is an example of an NS record:

example.com	record type:	value:	TTL
@	NS	ns1.exampleserver.com	21600

Note that NS records can never point to a canonical name (CNAME) record.

- **nameserver**

A nameserver is a type of DNS server. It is the server that stores all DNS records for a domain, including A records, MX records, or CNAME records.

Almost all domains rely on multiple nameservers to increase reliability: if one nameserver goes down or is unavailable, DNS queries can go to another one. Typically, there is one primary nameserver and several secondary nameservers, which store exact copies of the DNS records in the primary server. Updating the primary nameserver will trigger an update of the secondary nameservers as well. When multiple nameservers are used (as in most cases), NS records should list more than one server. Learn more about DNS servers.

1.6. DNS SOA records

The DNS 'start of authority' (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETF standards. SOA records are also important for zone transfers. Example of an SOA record:

name	example.com
record type	SOA
MNAME	ns.primaryserver.com
RNAME	admin.example.com
SERIAL	1111111111
REFRESH	86400
RETRY	7200
EXPIRE	4000000
TTL	11200

The 'RNAME' value here represents the administrator's email address, which can be

confusing because it is missing the '@' sign, but in an SOA record admin.example.com is the equivalent of admin@example.com.

- **zone serial number**

In the DNS, a 'zone' is an area of control over namespace. A zone can include a single domain name, one domain and many subdomains, or many domain names. In some cases, 'zone' is essentially equivalent with 'domain,' but this is not always true.

A zone serial number is a version number for the SOA record. In the example above, the serial number is listed next to 'SERIAL.' When the serial number changes in a zone file, this alerts secondary nameservers that they should update their copies of the zone file via a zone transfer.

- **Other parts of an SOA record**
  - **MNAME**: This is the name of the primary nameserver for the zone. Secondary servers that maintain duplicates of the zone's DNS records receive updates to the zone from this primary server.
  - **REFRESH**: The length of time (in seconds) secondary servers should wait before asking primary servers for the SOA record to see if it has been updated.
  - **RETRY**: The length of time a server should wait for asking an unresponsive primary nameserver for an update again.
  - **EXPIRE**: If a secondary server does not get a response from the primary server for this amount of time, it should stop responding to queries for the zone.

Points to Remember

DNS, or Domain Name System, is a fundamental component of the Internet that translates human-readable domain names into machine-readable IP addresses. This process allows users to access websites without needing to memorize complex numerical addresses.

A **CNAME record** is used to create an alias for a domain name. It maps one domain name (the alias) to another (the canonical name). This is particularly useful for pointing multiple subdomains to a single domain, simplifying DNS management.

Theoretical Activity 4.1.2: Describing DNS queries

Tasks:

1: Answer the following questions**:**

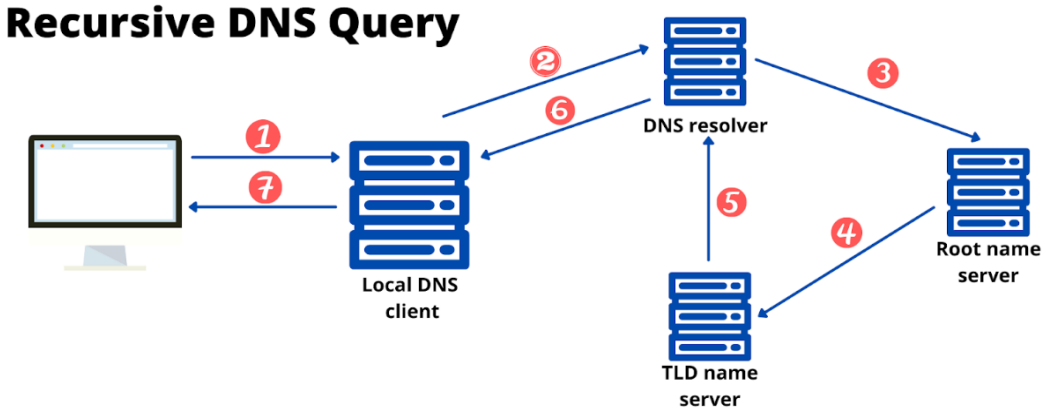
i. What do you understand by Recursive Query?
ii. What do you understand by Iterative Query and Non-Recursive Query?
iii. Differentiate DNS Resolver from DNS Root Server?

2: Write your answers on papers or flipchart.
3: Present your findings/answers to the whole class
4: Ask for clarification where necessary
5: Read the key readings 4.1.2.

Key readings 4.1.2: Description of DNS queries

1. Recursive DNS

Recursive query in a recursive query, a DNS client requires that a DNS server (typically a DNS recursive resolver) will respond to the client with either the requested resource record or an error message if the resolver can't find the record. A recursive DNS lookup is where one DNS server communicates with several other DNS servers to hunt down an IP address and return it to the client. This is in contrast to an iterative DNS query, where the client communicates directly with each DNS server involved in the lookup. While this is a very technical definition, a closer look at the DNS system and the difference between recursion and iteration should help clear things up. If you have enabled recursive DNS, the appliance uses the following logic to determine how to resolve a DNS host name and when to return an error to the client. If the DNS server response does not contain an A record with an IP address but instead contains authoritative server information (a referral), the appliance follows all referrals until it receives an answer. If the appliance follows more than eight referrals, it assumes that there is a recursion loop, aborts the request, and sends an error to the client.



- **Advantages of recursive DNS**

  Recursive DNS queries generally tend to resolve faster than iterative queries. This is due to caching. A recursive DNS server caches the final answer to every query it performs and saves that final answer for a certain amount of time (known as the Time-To-Live).

  When a recursive resolver receives a query for an IP address it already has in its cache, it can rapidly provide the cached answer to the client without communicating with any other DNS servers. Quickly serving responses from the

cache is very likely if a) the DNS server serves a lot of clients and/or b) the requested website is very popular.

- **Disadvantages of recursive DNS**

  Unfortunately, allowing recursive DNS queries on open DNS servers creates a security vulnerability, as this configuration can enable attackers to perform DNS amplification attacks and DNS cache poisoning.

2. Iterative Query

Iterative query in this situation the DNS client will allow a DNS server to return the best answer it can. If the queried DNS server does not have a match for the query name, it will return a referral to a DNS server authoritative for a lower level of the domain namespace. The DNS client will then make a query to the referral address. This process continues with additional DNS servers down the query chain until either an error or timeout occurs. An iterative DNS query is a request for a domain name's IP address sent to a name server (DNS resolver) that responds with the most relevant answer. This answer could be the IP address if it is stored in the DNS resolver's cache. Otherwise, the DNS resolver responds with another name server's details. As the term "iterative" suggests, this referral process continues until the requesting server receives the appropriate DNS response.

An iterative DNS query is also known as a "nonrecursive DNS query" since the name servers respond to the requesting server instead of querying another name server.

In the DNS, the iterative query typically follows these steps:

Step 1: You type "example[.]com" on your browser, telling your local DNS client to look for the domain name's IP address.

Step 2: Your local DNS client asks the DNS resolver for the IP address of example[.]com.

Step 3: If the DNS resolver has the answer in its cache, it responds with the IP address. If it does not know the answer, it responds with the IP address of the root server.

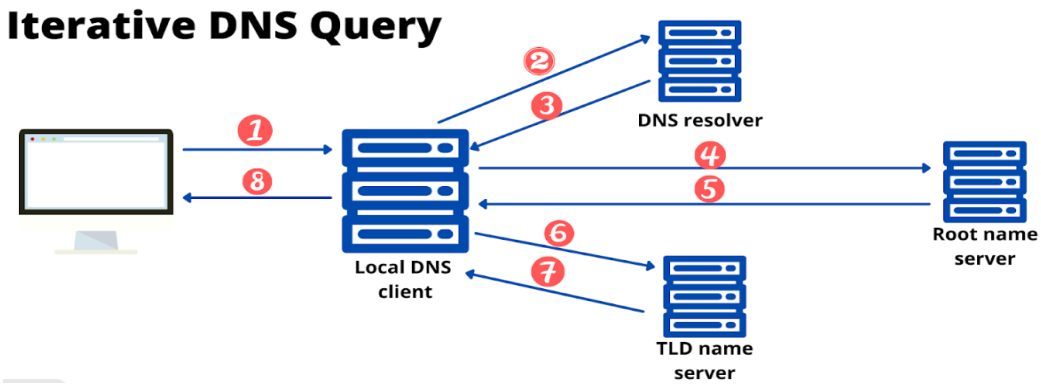
Step 4: Your local DNS client then asks the root name server for the details of the domain name's TLD name server.

Step 5: The root name server responds with the TLD server's IP address.

Step 6: Your local DNS client asks the TLD server for the domain name's IP address.

Step 7: The TLD name server responds with the corresponding IP address.

Step 8: Your local DNS client resolves the IP address, and your browser displays the website.



3. Non-Recursive Query

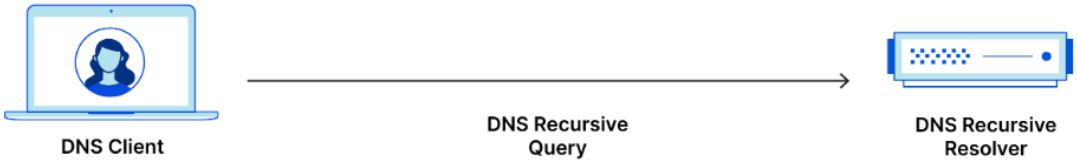
typically, this will occur when a DNS resolver client queries a DNS server for a record that it has access to either because it's authoritative for the record or the record exists inside of its cache. Typically, a DNS server will cache DNS records to prevent additional bandwidth consumption and load on upstream servers. non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client. This form of DNS query is able to respond immediately since the DNS resolver already knows how to obtain the answer to the query. This is because the DNS record is either stored in the local cache or a DNS name server has been queried which is authoritative and definitely holds the IP address for the hostname. In other words, a response is immediately returned to the client because unlike recursive and iterative queries, there is no need for additional rounds of queries.

4. DNS Resolver

The DNS resolver is the first stop in the DNS lookup, and it is responsible for dealing with the client that made the initial request. The resolver starts the sequence of queries that ultimately leads to a URL being translated into the necessary IP address.

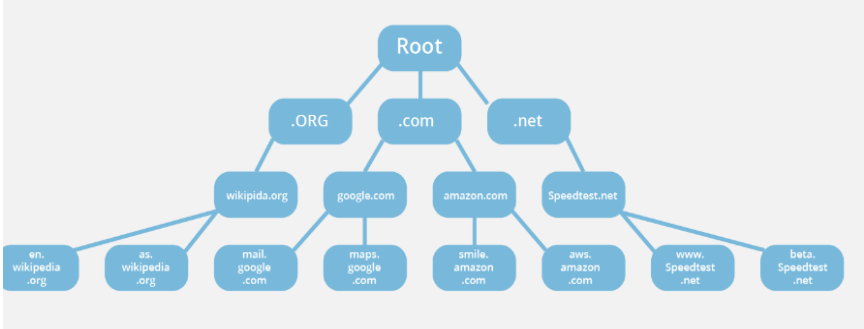
Note: A typical uncached DNS lookup will involve both recursive and iterative queries.

It's important to differentiate between a recursive DNS query and a recursive DNS resolver. The query refers to the request made to a DNS resolver requiring the resolution of the query. A DNS recursive resolver is the computer that accepts a recursive query and processes the response by making the necessary requests.



5.DNS Root Server

The administration of the Domain Name System (DNS) is structured in a hierarchy using different managed areas or "zones", with the root zone at the very top of that hierarchy. Root servers are DNS nameservers that operate in the root zone. These servers can directly answer queries for records stored or cached within the root zone, and they can also refer other requests to the appropriate Top Level Domain (TLD) server. The TLD servers are the DNS server group one step below root servers in the DNS hierarchy, and they are an integral part of resolving DNS queries.



During an uncached DNS query, whenever a user enters a web address into their browser, this action triggers a DNS lookup, and all DNS lookups start at the root zone. Once the lookup hits the root zone, the lookup will then travel down the hierarchy of the DNS system, first hitting the TLDs servers, then the servers for specific domains (and possibly subdomains) until it finally hits the authoritative nameserver for the correct domain, which contains the numerical IP address of the website being sought. This IP address is then returned to the client. Interestingly, despite the number of steps required, this process can happen very quickly.

Root servers are an essential part of the infrastructure of the Internet; web browsers and many other internet tools would not work without them. There are 13 different IP addresses that serve the DNS root zone, and hundreds of redundant root servers exist around the globe to handle requests to the root zone.

- **Who operates DNS root servers**

  The Internet Corporation for Assigned Names and Numbers (ICANN) operates servers for one of the 13 IP addresses in the root zone and delegated operation of the other 12 IP addresses to various organizations including NASA, the University

of Maryland, and Verisign, which is the only organization that operates two of the root IP addresses. Cloudflare actually helps provide DNS Anycast services to one of the root servers known as the F-Root; Cloudflare supplies additional F-Root instances under contract with ISC (the F-Root operator).

- **find DNS root servers**

  Since the DNS root zone is at the top of the DNS hierarchy, recursive resolvers cannot be directed to them in a DNS lookup. Because of this, every DNS resolver has a list of the 13 IP root server addresses built into its software. Whenever a DNS lookup is initiated, the recursor's first communication is with one of those 13 IP addresses.

- **DNS root server becomes unavailable**

  Thanks to the use of Anycast routing and heavy redundancy, the root servers are very reliable. But on rare occasions a root server will have to update its IP address. In this case, recursive resolvers can continue using the other 12 IP addresses in the root zone to perform DNS lookups until their software is updated with the correct addresses of all 13 servers. Since resolvers will retry until they reach a working root server, there is no disruption to the normal operations of the Internet when one root server is down.

6.Authoritative DNS Server

Authoritative DNS is the system that keeps official records corresponding to domain names such as IP addresses. Domain names are the human-readable names of IP addresses that direct applications such as browsers to websites such as www.example.com. IP addresses are designated by strings of numbers and periods like 123.45.67.189 that can be read by machines.

When a user types a domain name into a browser, the user's device queries the DNS system for the IP address for the domain name. If the address cannot be produced quickly from the initial DNS server, it contacts another nameserver to look for the answer. This process is known as the recursive lookup process.

Points to Remember

1. A **recursive query** in DNS is a type of request where a DNS resolver (also known as a recursive DNS server) takes on the responsibility of fully resolving a domain name into its corresponding IP address. This process involves the resolver making multiple queries to various DNS servers on behalf of the client, allowing the user to receive a complete answer without needing to manage each step.
2. **Non-Recursive Query**

   The term non-recursive query is often used interchangeably with iterative query. It emphasizes that the queried DNS server does not perform any additional queries on behalf of the client but responds directly with either an answer or a referral.
3. **Iterative Query**

   An **iterative query** is a type of DNS request where the DNS resolver queries a server and expects either a direct answer or a referral to another server. If the queried server does not have the requested information, it will respond with the address of another DNS server that may have the answer.

Theoretical Activity 4.1.3: Description of DNS zones and zone files

Tasks:

1: Answer the following questions**:**

i.What do you understand by zone files?

ii. Explain DNS zone?

iii. Differentiate DNS zones from zone file?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 4.1.3.

Key readings 4.1.3: Description of DNS zones and zone files

1. Forward lookup zone

A forward DNS lookup is the process of converting a domain name into its corresponding IP address. This is the most common type of DNS query. A forward DNS lookup zone is a DNS zone configured to facilitate mapping between domain names and IP addresses. It's essential for everyday internet usage, enabling users to access websites through domain names.

IPv4 and IPv6:

Both address types can be mapped in a DNS zone file using address records: A records for IPv4 and AAAA records for IPv6.

Example:

To access clouddns.manageengine.com, an A record is queried, which resolves to the IPv4 address 203.0.113.45.

To access blog.zylkercorp.com, an AAAA record is queried, which resolves to the IPv6 address 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

- **forward DNS lookup zones used**

Forward lookup zones are a fundamental component of the DNS, ensuring the smooth operation of the internet and private networks by making it easier for humans to access and use network resources through memorable domain names instead of exhaustive strings of IP addresses. These zones are used by DNS servers around the world to resolve client queries and direct traffic appropriately.

Forward lookup zones are utilized in a variety of situations, including:

✓ **Accessing websites:** When you type a website address (e.g., www.example.com) into your browser, a DNS query is made in a forward lookup zone to resolve the hostname to its IP address, allowing your browser to connect to the website's server.

✓ **Email services:** Email clients and servers use the DNS to resolve domain names in email addresses to the IP addresses of mail servers, ensuring that emails can be correctly routed and delivered to their destination.

✓ **Connecting to networked services:** Whether it's cloud services, remote databases, or online APIs, clients use forward DNS lookups to find the IP addresses of the servers hosting these services, based on their hostnames.

✓ **Network administration and operations:** In enterprise environments, forward lookup zones facilitate connections to internal servers, networked printers, file shares, and other resources by translating human-friendly domain names into IP addresses that only networked computers can understand.

✓ **Load balancing and redundancy:** Forward lookup zones can be configured to return multiple IP addresses for a single hostname, enabling traffic to be distributed across several servers or rerouted in case of a server failure; this enhances the availability and reliability of services.

2.Reverse lookup zone

Reverse lookup zones in the DNS are used for resolving IP addresses back into domain names, essentially performing the opposite function of the more common forward lookup zones, which map domain names to IP addresses. This process is known as a reverse DNS lookup, or rDNS. This is particularly important for services like email, where verifying the sender's domain against the IP address can help reduce spam.

Reverse lookup zones require careful setup to ensure accurate reverse lookups

and use PTR records in designated reverse zones. Each record will correlate an IP address to a hostname, with the IP block address portion written in reverse.

While not all IP addresses have reverse DNS setups, for many applications—especially in business or enterprise environments—setting up reverse lookup zones is a crucial part of managing the network infrastructure.

- **Reverse zones and PTR records for IPv4 addresses**

Say, for instance, in the IPv4 network block 192.168.1.0/24, there's a user named John with the employee ID 12345. A typical forward DNS lookup for John's hostname, using the format [hostname].[domainname].[TLD] (where TLD stands for top-level domain, like .com), would resolve to an IPv4 address as shown below:

john-12345.zylkercorp.com > 192.168.1.26

To create a reverse DNS lookup zone for John's IP address, you would start with the network portion of your IP block, reverse it, and then append .in-addr.arpa. So, for the /24 address block, 192.168.1 is the network address and the reverse lookup zone would be:

1.168.192.in-addr.arpa

Within this reverse lookup zone, a PTR record for John's IP address would be:

26.1.168.192. in-addr.arpa

The response for the PTR record should correctly point back to John's hostname:

john-12345.zylkercorp.com

- **Reverse zones and PTR records for IPv6 addresses**

For IPv6 addresses, the process is similar to IPv4, but the notation and the domain used for reverse DNS delegation are different. The domain used for IPv6 reverse DNS is .ip6.arpa. For the IPv6 address block 2001:0db8:85a3::/48, you first need to construct the reverse zone name by reversing the address block and formatting it according to the reverse lookup naming conventions for IPv6 in the DNS. For a /48 subnet, the network address involves only the first three groups of hexadecimal numbers.

✓ **Reverse DNS lookup zone name construction:**

- Start with the IPv6 prefix: 2001:0db8:85a3
- Reverse the hexadecimal groups of the network address and separate each digit with a dot: 3.a.5.8.8.b.d.0.1.0.0.2
- Append the standard reverse lookup suffix for IPv6: .ip6.arpa
- So, the reverse zone name is 3.a.5.8.8.b.d.0.1.0.0.2.ip6.arpa.

✓ **Sample PTR records within this zone:**

For example, let's create PTR records for an IPv6 address in this block:

2001:0db8:85a3:0000:0000:0000:0000:abcd

To create a PTR record, we need to reverse the unique part of the address (beyond the /48 prefix), which is the last four hexadecimal digits (abcd), omitting the zeros, otherwise you'll have to reverse the whole unique part. Following the

reverse DNS lookup conventions for IPv6:

1. Reverse the unique hexadecimal digits: d, c, b, a
2. Separate each digit with a dot: d.c.b.a
3. Append the reverse zone name constructed from the /48 prefix: 3.a.5.8.8.b.d.0.1.0.0.2.ip6.arpa

Therefore, the complete PTR record for 2001:0db8:85a3::abcd would be:
d.c.b.a.3.a.5.8.8.b.d.0.1.0.0.2.ip6.arpa

The PTR record above indicates that the IP address should reverse resolve to the hostname jade-56789.zylkercorp.com, which is in the format hostname.domainname.tld referring to the top-level domain name .com. Note: Typically, one IP address maps to one hostname, although having multiple PTR records for a single IP is not prohibited by the DNS standard.

3.Standard primary zone

A DNS server hosting a primary zone is the primary source for information about this zone. It stores the zone data in a local file or in AD DS. To create, edit, or delete resource records, you must use the primary zone. Secondary zones are read-only copies of primary zones.

You can store a standard primary zone in a local file, or you can store zone data in AD DS. When you store zone data in AD DS other features are available, such as secure dynamic updates and the ability for each domain controller that hosts the zone to function as a primary and be able to process updates to the zone. When the zone is stored in a file, by default the primary zone file is named zone_name.dns, and it's located in the %windir%\System32\Dns folder on the server.

4.AD-integrated zone

Active Directory-integrated DNS in Windows Server 2008 stores zone data in application directory partitions. (There are no behavioral changes from Windows Server 2003-based DNS integration with Active Directory.) The following DNS-specific application directory partitions are created during AD DS installation:

- A forest-wide application directory partition, called ForestDnsZones
- Domain-wide application directory partitions for each domain in the forest, named DomainDnsZones

5. Standard secondary zone

A secondary zone is a read-only copy of a primary zone. When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with

updated information about the zone. Because a secondary zone is only a copy of a primary zone that is hosted on another server, it can't be stored in AD DS as an Active Directory Integrated zone.

Points to Remember

1. A **zone file** is a plain text file stored on a DNS server that contains all the resource records for a particular DNS zone. This file is essential for the functioning of the DNS as it specifies how domain names are resolved to IP addresses and includes various types of records.
2. A DNS zone is a distinct administrative space within the DNS hierarchy that allows for the management of a specific portion of the domain namespace. It can encompass a domain and its subdomains, enabling administrators to control DNS records, name servers, and other components for that segment.

Practical Activity 4.1.4: Performing DNS installation

Task:

1: Referring to the key reading 4.1.3, As an internet and networking technology student, you are asked to go to install DNS server installation
2: Present the procedures of all step performed installation.
3: Present your work to the trainer and whole class.
4: Read key reading 4.1.4 and ask clarification where necessary
5: Perform the task provided in application of learning 4.1

Key readings 4.1.4: Performing DNS installation process

1. DNS installation process

1.1. DNS installation Prerequisites

•Our domain name.

•The IP address and hostname of each server that we want to provide name resolution for.

Additionally, before we configure our computer as a DNS, we need to verify that the following minimum conditions are proper:

•A server running Windows Server 2012R2, 2016, 2019, or 2022 operating system and an open Remote Desktop Protocol (RDP) 3389 port.

•A domain user with appropriate administrative privileges in configuring the DNS.

•Minimum of 4 GB of RAM and 2-core CPU.

1.2. Updating DNS client configuration

Client DNS settings are confined to DNS server IP addresses and are usually pre-configured as part of the process that allocates a device an IP address. Should DNS server settings need changing, follow the steps below relevant to your operating system:

Windows

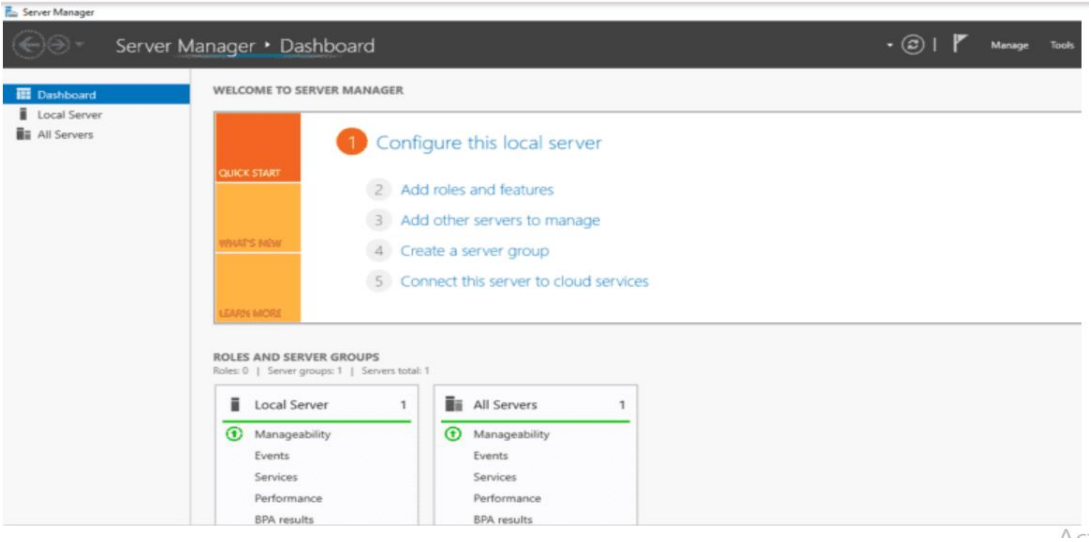
1. Open “Control Panel” and navigate to “Network and Sharing Center”.
2. Click the active network connection.
3. In the new window, click “Properties”.
4. Click “Internet Protocol Version 4 (TCP/IPv4)”, then navigate to “Properties.”
5. Choose “Use the following DNS server addresses,” then enter the desired DNS server IP addresses.
6. Click “OK”, then close the windows.

1.3. Installing DNS Server DNS Server Role

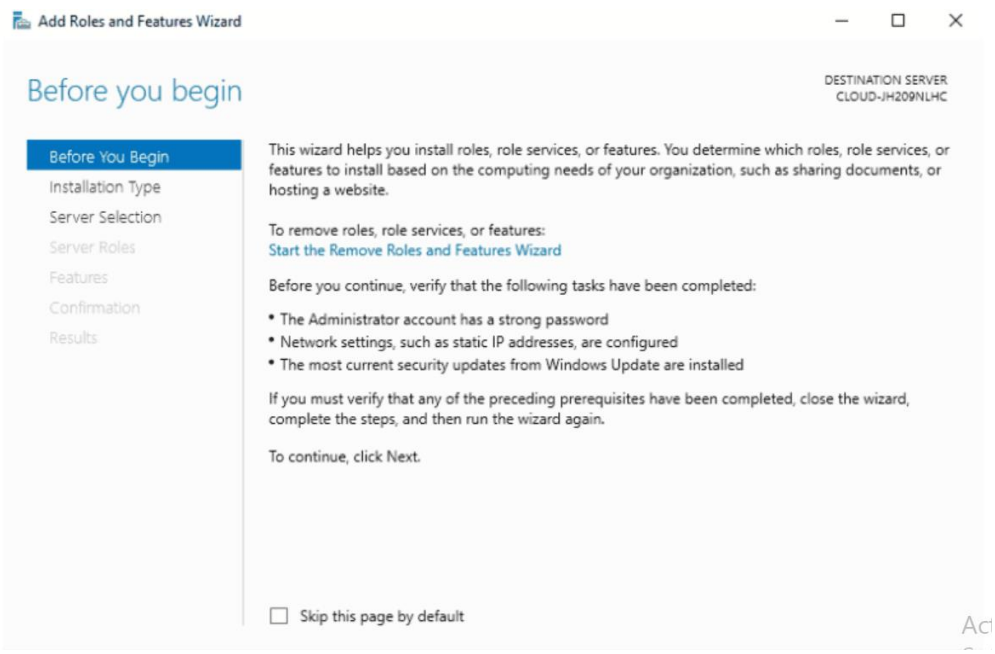
Basically, installing the DNS Server Role in Windows Server is a simple process that allows you to configure and manage a DNS server for your network. It involves adding the DNS server role to your Windows Server machine, configuring basic DNS settings, and creating and managing DNS records. First of all, log in as an administrator user to the Windows Server and follow the steps below to install the DNS server on our Windows Server:

Step 1: Launch the **Server Manager**, as illustrated below:

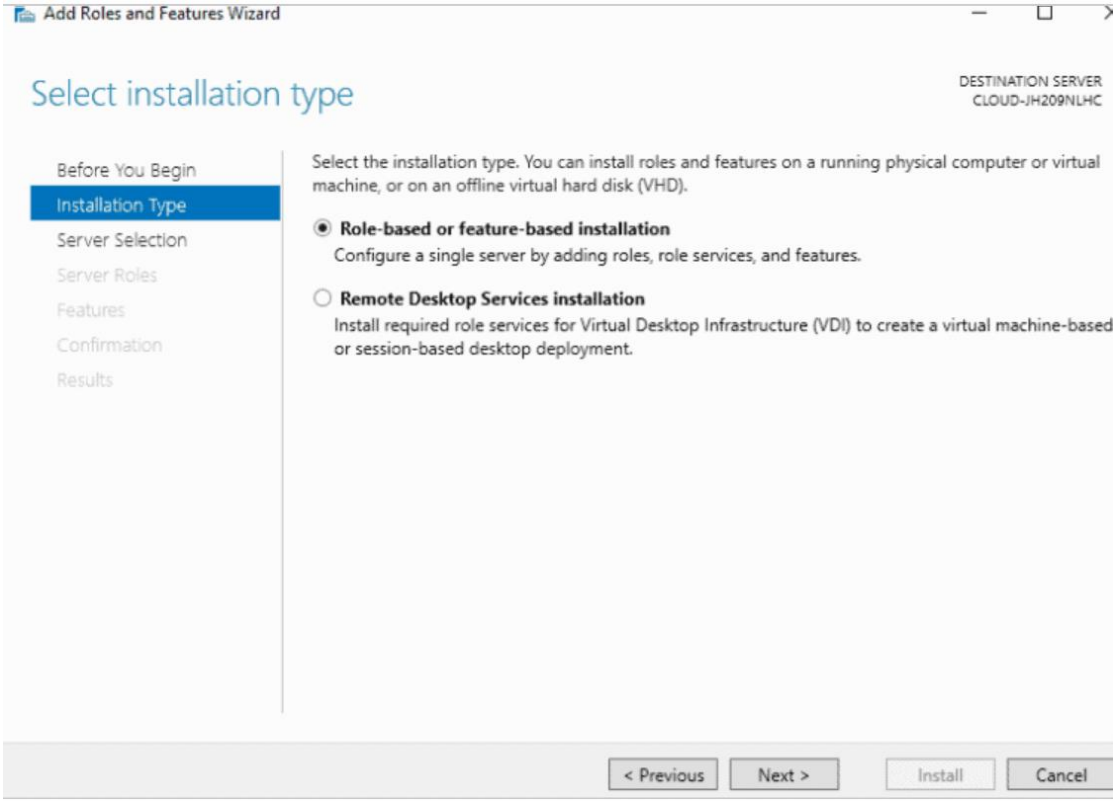
Step 2: Select **Add roles and features**.



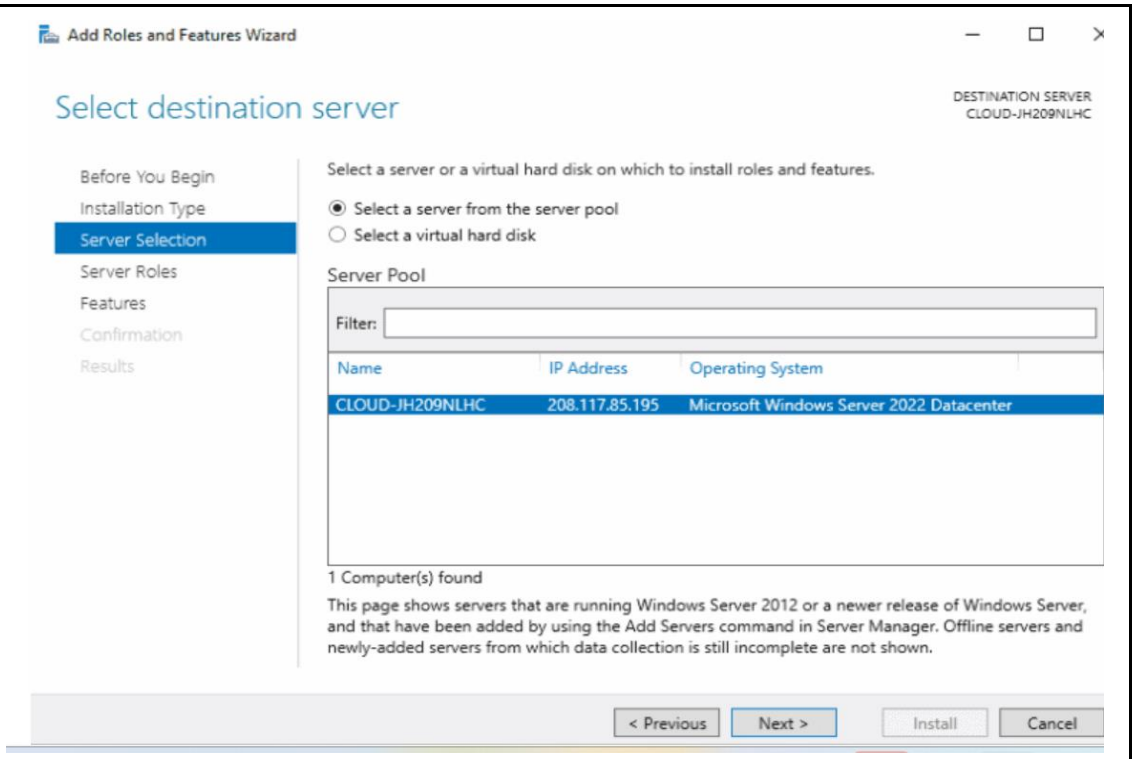
Step 3: Press **Next**



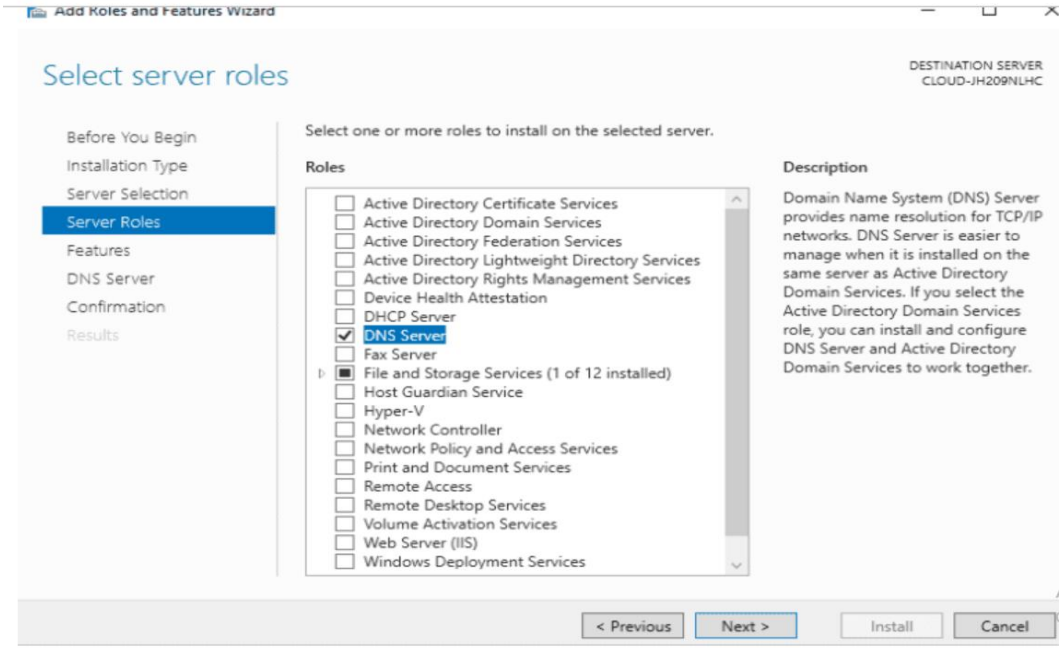
Step 4: Click on Next after selecting Role based and feature based installation.



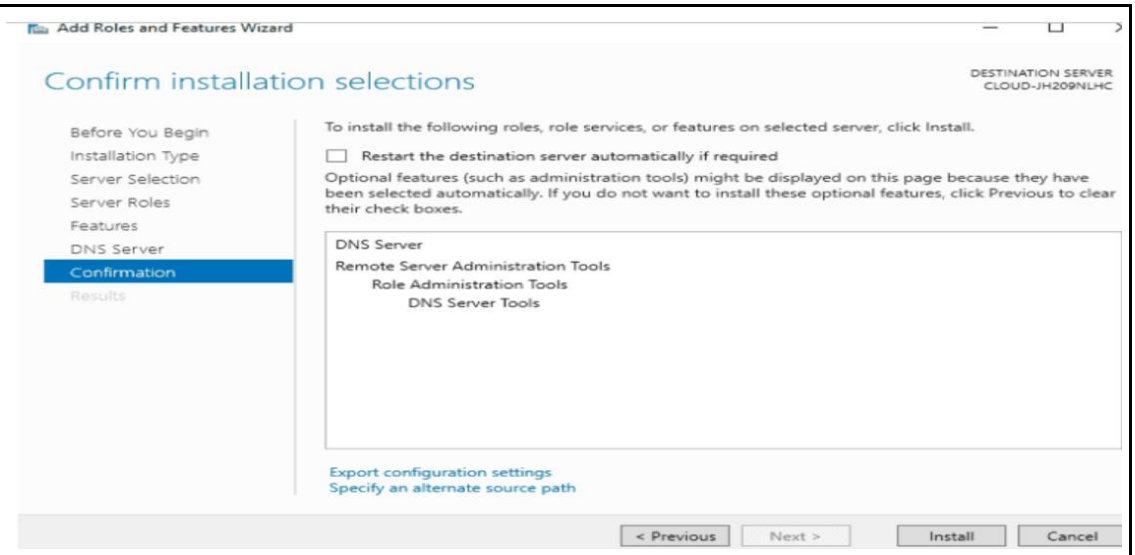
Step 5: Choose a server from the pool and press **Next**.



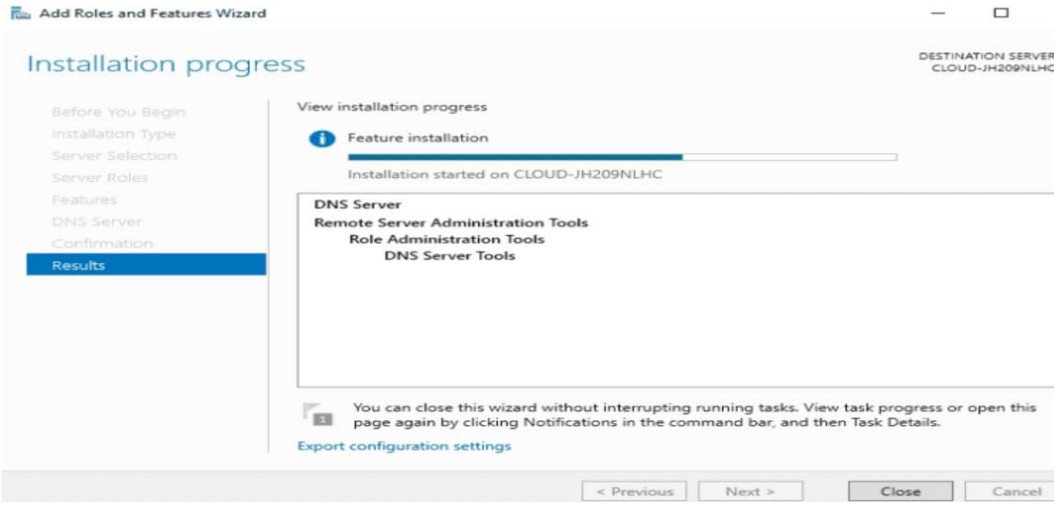
Step 6: Pick the DNS server and click **Next**.



Step 7: Double check all settings before clicking the **Install** button to begin the installation.



Step 8: Allow some time for the installation to complete. Once done, click the **Close** to exit the installation wizard.



Points to Remember

- DNS, or Domain Name System, is a fundamental component of the Internet that translates human-readable domain names into machine-readable IP addresses. This process allows users to access websites without needing to memorize complex numerical addresses.
- A **CNAME record** is used to create an alias for a domain name. It maps one domain name (the alias) to another (the canonical name). This is particularly useful for pointing multiple subdomains to a single domain, simplifying DNS management.

- A **recursive query** in DNS is a type of request where a DNS resolver (also known as a recursive DNS server) takes on the responsibility of fully resolving a domain name into its corresponding IP address. This process involves the resolver making multiple queries

to various DNS servers on behalf of the client, allowing the user to receive a complete answer without needing to manage each step.

- Non-Recursive Query
- The term non-recursive query is often used interchangeably with iterative query. It emphasizes that the queried DNS server does not perform any additional queries on behalf of the client but responds directly with either an answer or a referral.
- An iterative query is a type of DNS request where the DNS resolver queries a server and expects either a direct answer or a referral to another server. If the queried server does not have the requested information, it will respond with the address of another DNS server that may have the answer.
- A zone file is a plain text file stored on a DNS server that contains all the resource records for a particular DNS zone. This file is essential for the functioning of the DNS as it specifies how domain names are resolved to IP addresses and includes various types of records.
- A DNS zone is a distinct administrative space within the DNS hierarchy that allows for the management of a specific portion of the domain namespace. It can encompass a domain and its subdomains, enabling administrators to control DNS records, name servers, and other components for that segment.

Feature	**DNS Zone**	**Zone file**
Definition	An administrative spave in the DNS hierarchy	A text file containing resource records for a zone
Purpose	Manages a specific portion of the domain namespace	Provides data necessary for resolving domain names
Structure	Can contain multiple subdomains	Contains various types of DNC records
Control	Allows granular control by administrators	Represents actual data used in queries
Updates	Managed through zone file	Updated directly in the zone file

- **Prerequisites**

Before configuring our DNS, we must have the following information:

- Our domain name.
- The IP address and hostname of each server that we want to provide name resolution for.

Additionally, before we configure our computer as a DNS, we need to verify that the following minimum conditions are proper:

- A server running Windows Server 2012R2, 2016, 2019, or 2022 operating system and an open Remote Desktop Protocol (RDP) 3389 port.
- A domain user with appropriate administrative privileges in configuring the DNS.
- Minimum of 4 GB of RAM and 2-core CPU

- **Installing the DNS Server Role**

Step 1: Launch the Server Manager, as illustrated below:

Step 2: Select Add roles and features.

Step 3: Press Next.

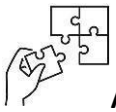
Step 4: Click on Next after selecting Role based and feature based installation.

Step 5: Choose a server from the pool and press Next.

Step 6: Pick the DNS server and click Next.

Step 7: Double check all settings before clicking the Install button to begin the installation

Step 8: Allow some time for the installation to complete. Once done, click the Close to exit the installation wizard.



Application of learning 4.1

Suppose that your school needs to establish DNS server, you are asked to install DNS role. All tools, materials and equipment are available in computer lab.

Indicative content 4.2: Configuration of DNS Settings

Duration: 3 hrs

Practical Activity 4.2.1: Configuring DNS Settings

Task:

1: Referring to the key reading 4.1.1, As an internet and networking technology student, you are asked to go to configure DNS server settings
2: Present the procedures of all step performed during DNS configuration.
3: Present your work to the trainer and whole class.
4: Read key reading 4.2.1 and ask clarification where necessary
5: Perform the task provided in application of learning 4.2

Key readings 4.2.1: Configuring DNS Settings

Configuring DNS (Domain Name System) settings involves several steps, including choosing a DNS hosting provider, configuring DNS records, and assigning the public DNS IP addresses. Here's a breakdown of the process:

4.2.1Choosing a DNS Hosting Provider

A DNS hosting provider manages the DNS records for your domain. Some popular DNS hosting providers include:

- Cloudflare
- Google Cloud DNS
- Amazon Route 53
- DigitalOcean DNS
- GoDaddy DNS
- Namecheap

Choose a provider based on your requirements (e.g., speed, global reach, DDoS protection, pricing).

4.2.1. Public DNS IP Addresses (IPv4)

Public DNS IP addresses allow the internet to locate and resolve your domain. If you're hosting your own DNS, or using third-party services, you may need to assign these. Here are the common DNS services with public IPv4 addresses:

Popular Public DNS IPv4 Addresses:

- **Google DNS (IPv4)**
- Primary: 8.8.8.8
- Secondary: 8.8.4.4

- **Cloudflare DNS (IPv4):**
- Primary: 1.1.1.1
- Secondary: 1.0.0.1
- **OpenDNS (IPv4):**
- Primary: 208.67.222.222
- Secondary: 208.67.220.220

3. Public DNS IP Addresses (IPv6)

As the world increasingly adopts IPv6, you should also configure DNS for IPv6 addresses.

Popular Public DNS IPv6 Addresses:

- Google DNS (IPv6):

- Primary: 2001:4860:4860::8888
- Secondary: 2001:4860:4860::8844

- Cloudflare DNS (IPv6):

- Primary: 2606:4700:4700::1111
- Secondary: 2606:4700:4700::1001

- OpenDNS (IPv6):

- Primary: 2620:119:35::35
- Secondary: 2620:119:53::53

Configuring the Forward Lookup Zone

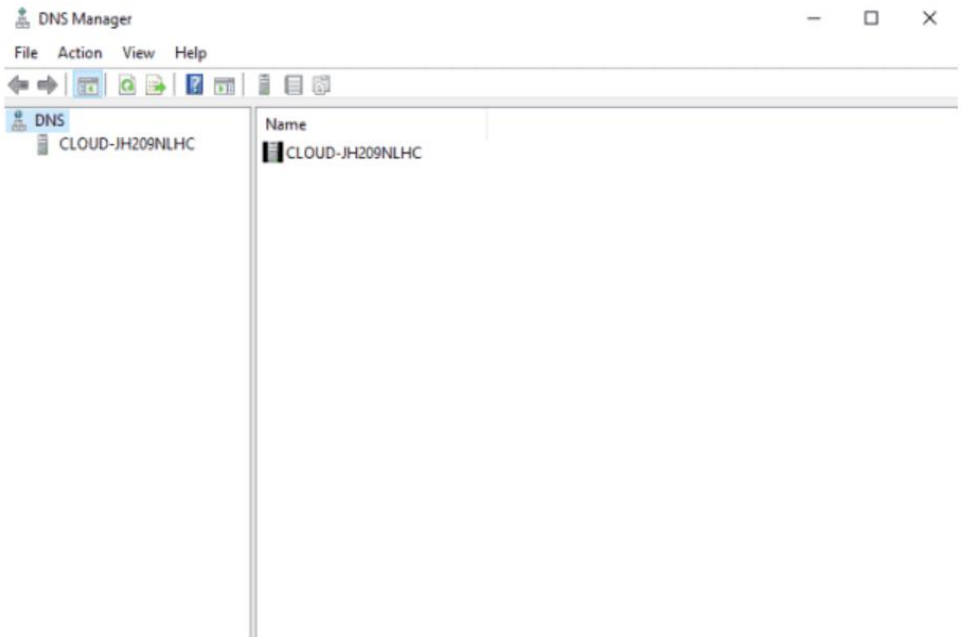
Evidently, a Forward Lookup Zone in DNS is a database of resource records that map domain names to IP addresses. Hence, we use it to resolve host names to IP addresses.

Certainly, the Forward Lookup Zone is vital because it enables clients to access network resources using domain names instead of IP addresses. This lookup zone makes it easier for users to remember and access network resources, and it helps improve the network's readability and maintainability.

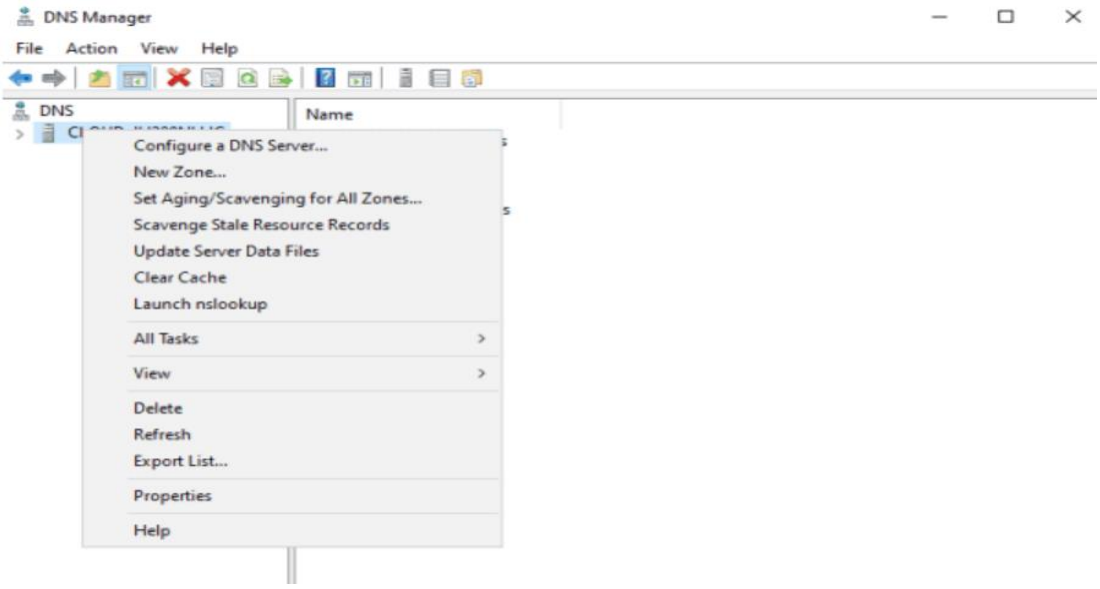
Steps

In order to create a forward lookup zone, follow the steps below:

Step 1: On the server manager, navigate to **Tools > DNS** to access the DNS manager, as shown below:

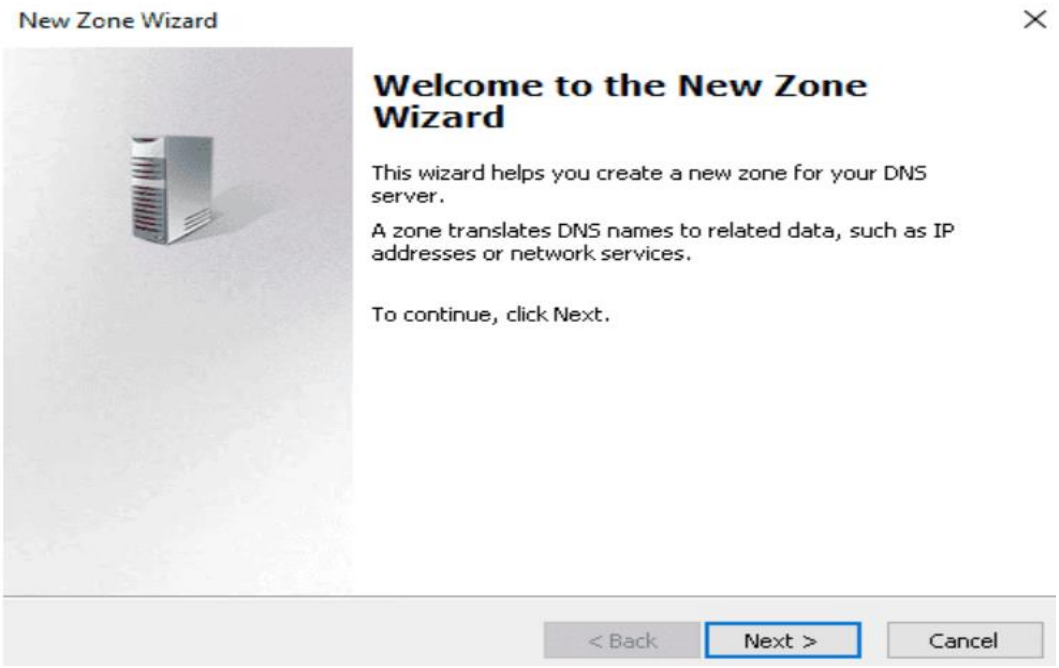


Step 2: Right click on the server name and select **Properties**.

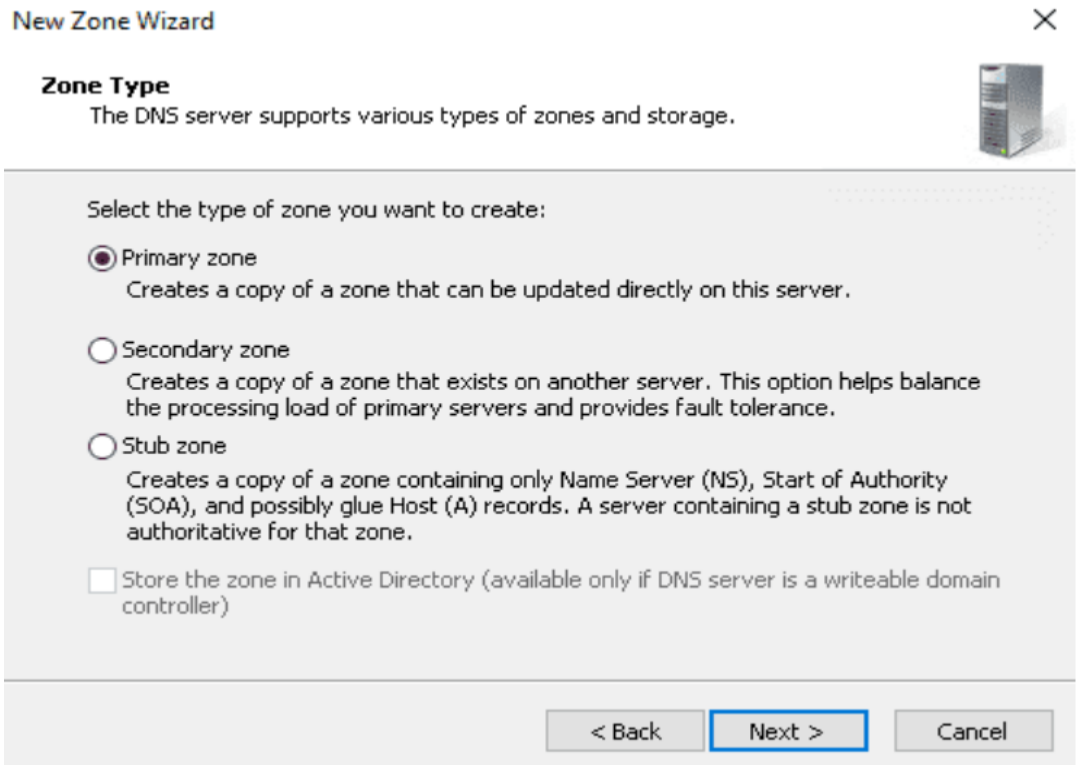


Step 3: Select the **New Zone** option.

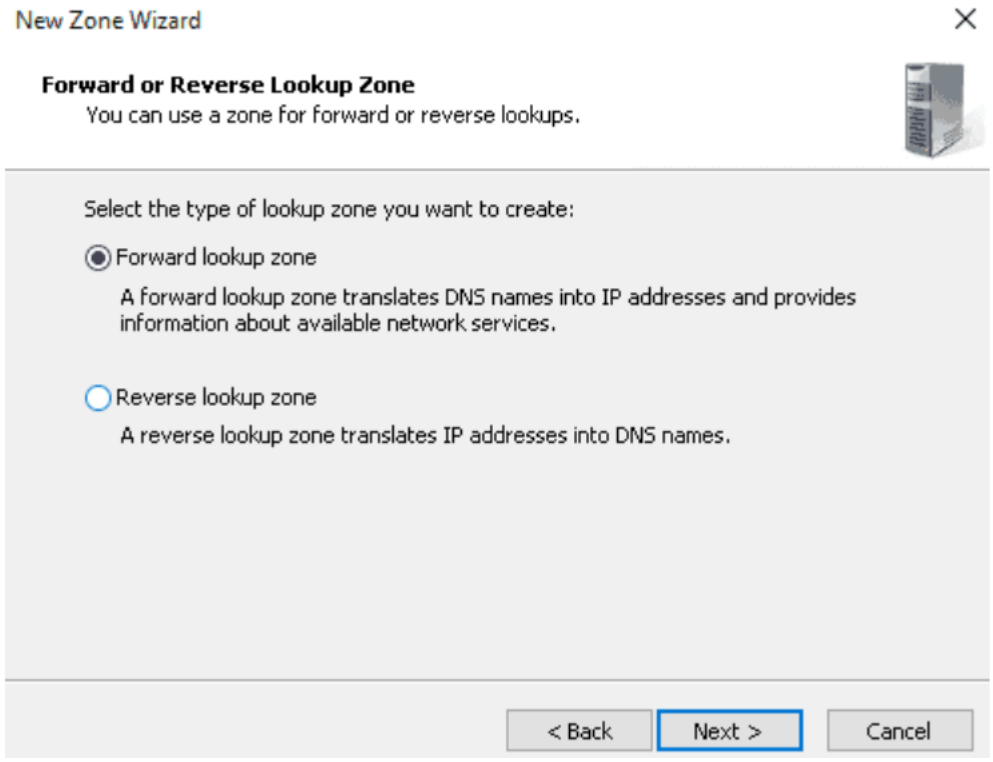
Step 4: Press **Next**.



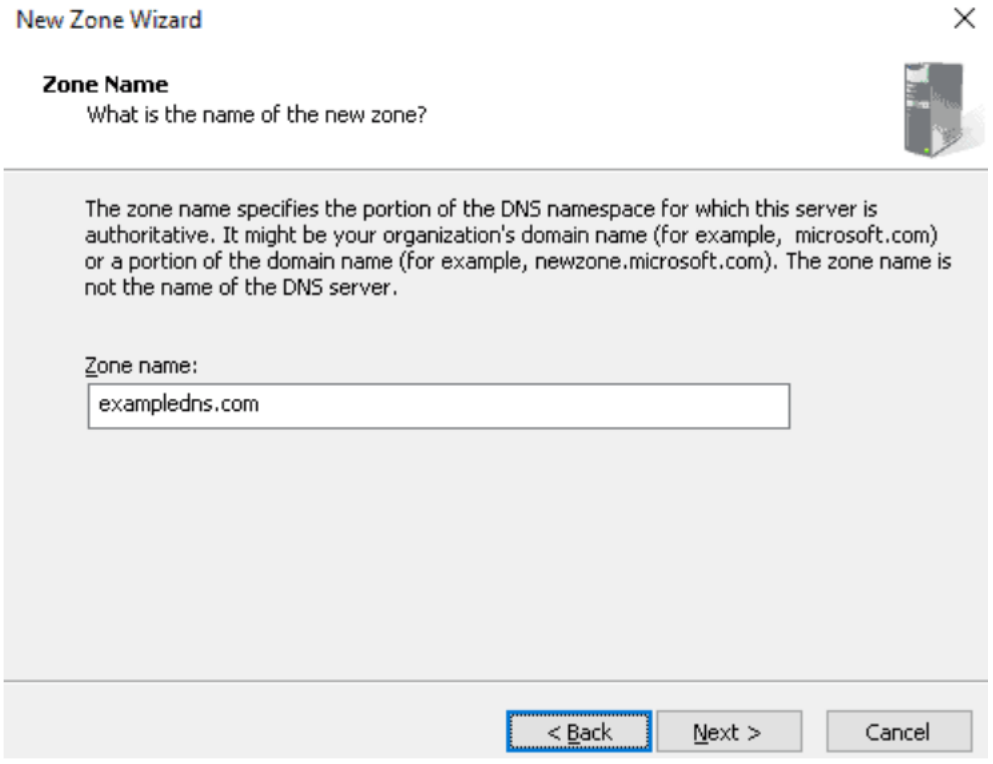
Step 5: Choose the Primary zone and press **Next**.



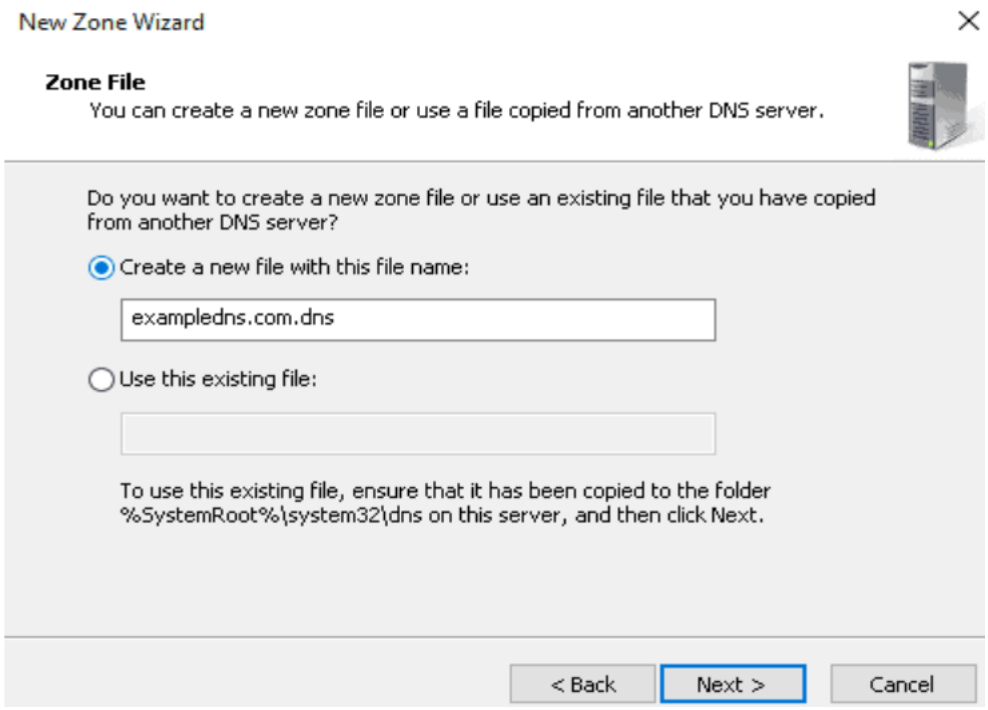
Step 6: Click **Next** after selecting the **Forward lookup zone**.



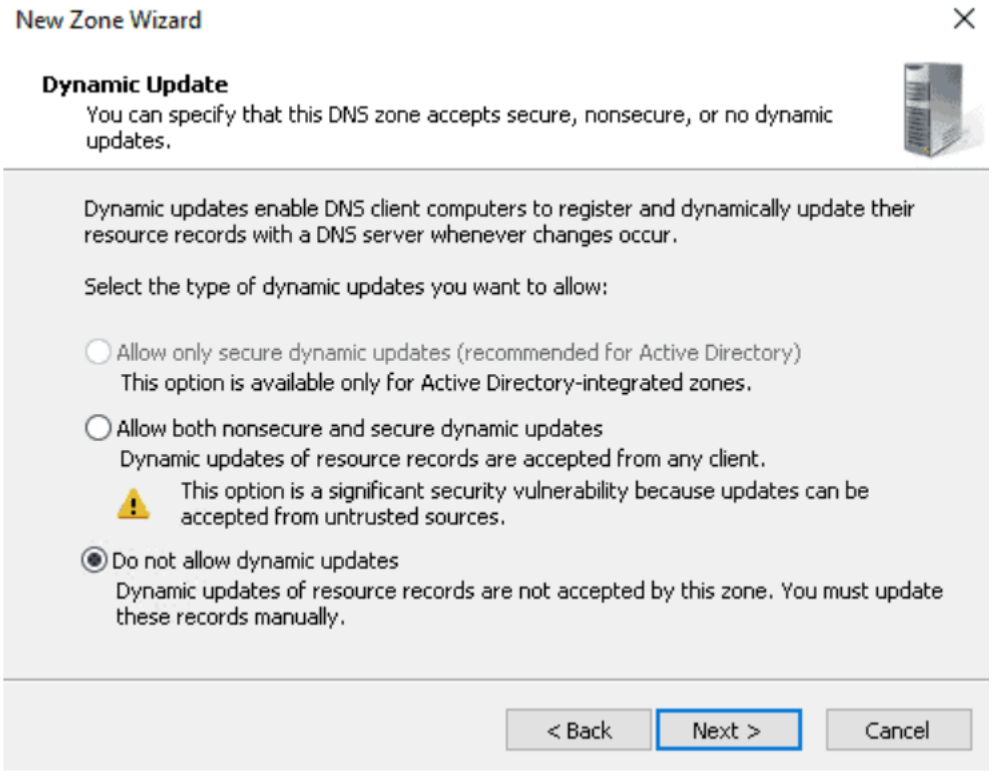
Step 7: Enter the name of our zone and press **Next**



Step 8: Choose **"Create a file with the file name"** and press **Next**.



Step 9: Check the box next to "Do not allow dynamic update" and click Next.



Step 10: Press the Finish button

Configuring the Reverse Lookup Zone

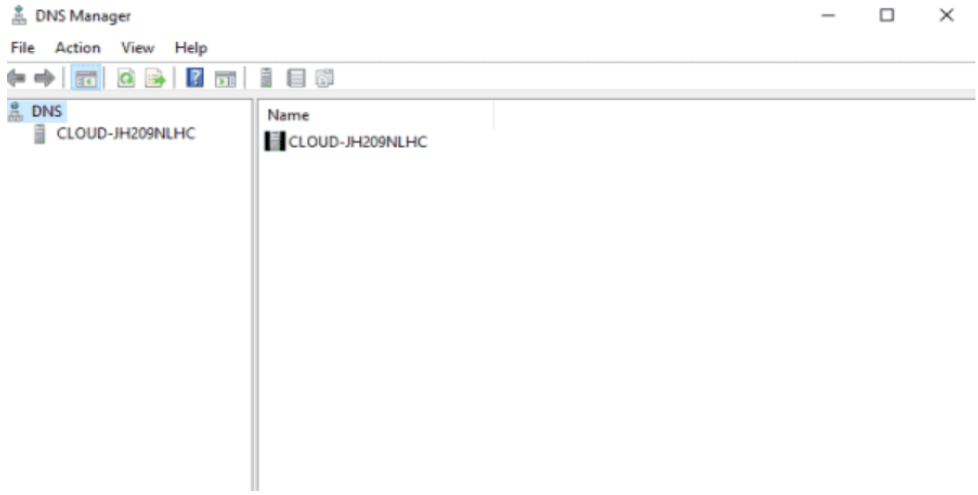
Following, a Reverse Lookup Zone in DNS is a database of resource records that map IP addresses to host names. By all means, we use this lookup zone to resolve IP addresses to hostnames.

Further, a Reverse Lookup Zone is different from the Forward Lookup Zone. In that it maps IP addresses to host names, while the Forward Lookup Zone maps host names to IP addresses. Additionally, the Reverse Lookup Zone is typically less frequently used than the Forward Lookup Zone, as clients are more likely to access network resources using host names rather than IP addresses.

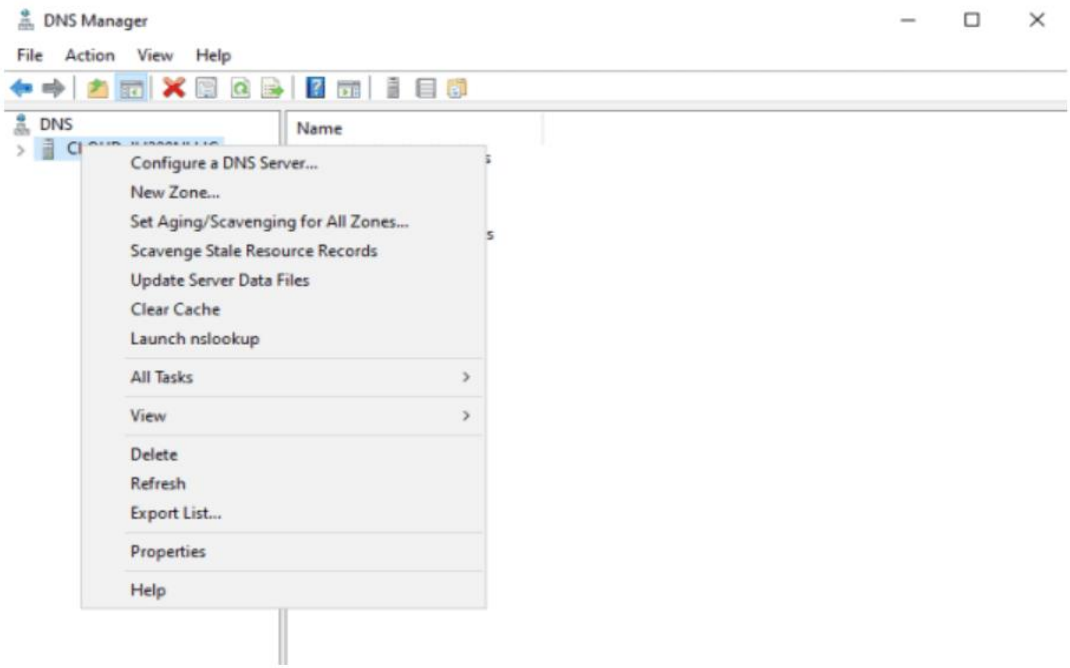
Steps

Indeed, to create a forward lookup zone, follow the steps below:

Step 1: On the server manager, navigate to **Tools > DNS** to access the DNS manager:

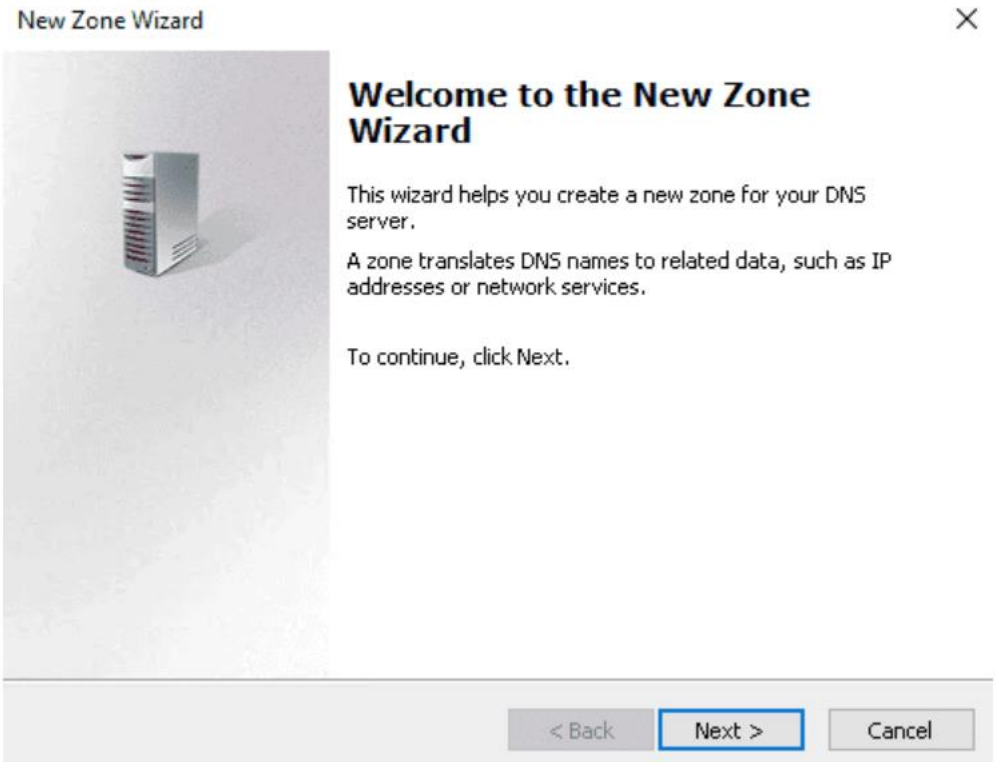


Step 2: Right click on the server name and select **Properties.**

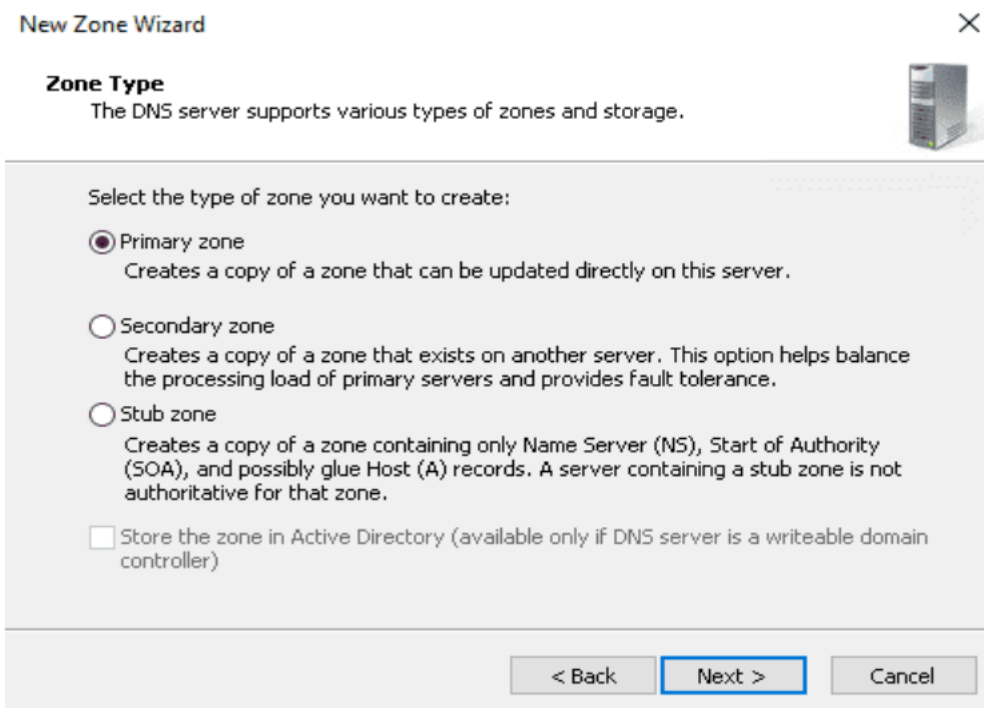


Step 3: Here, select the **New Zone** option.

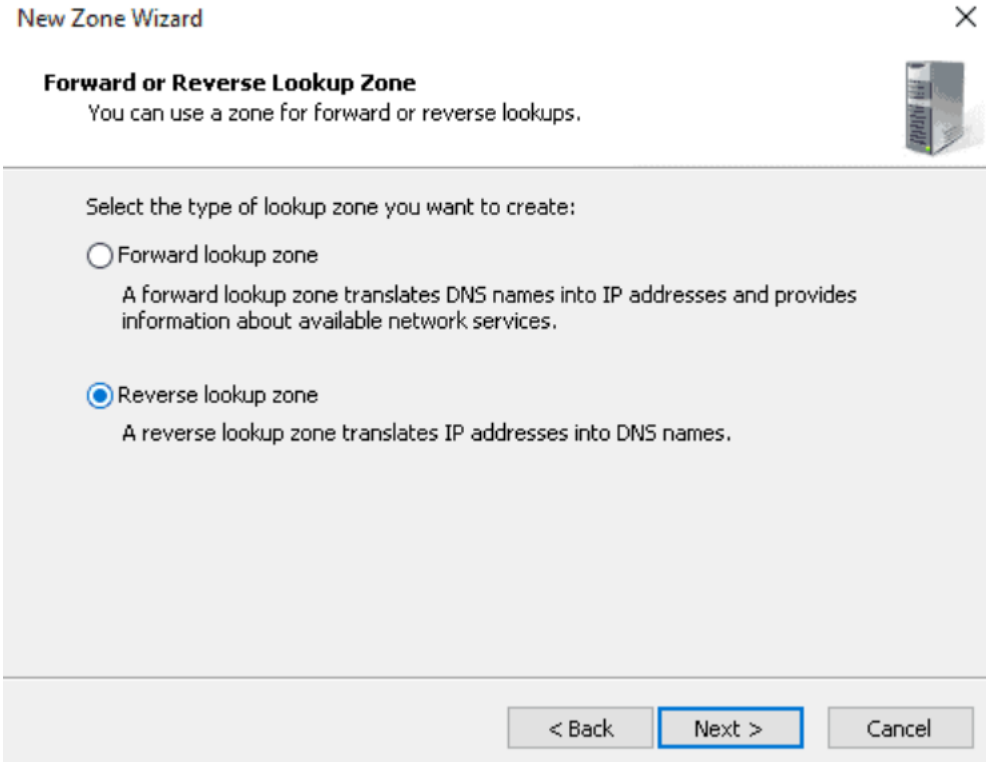
Step 4: Press **Next**.



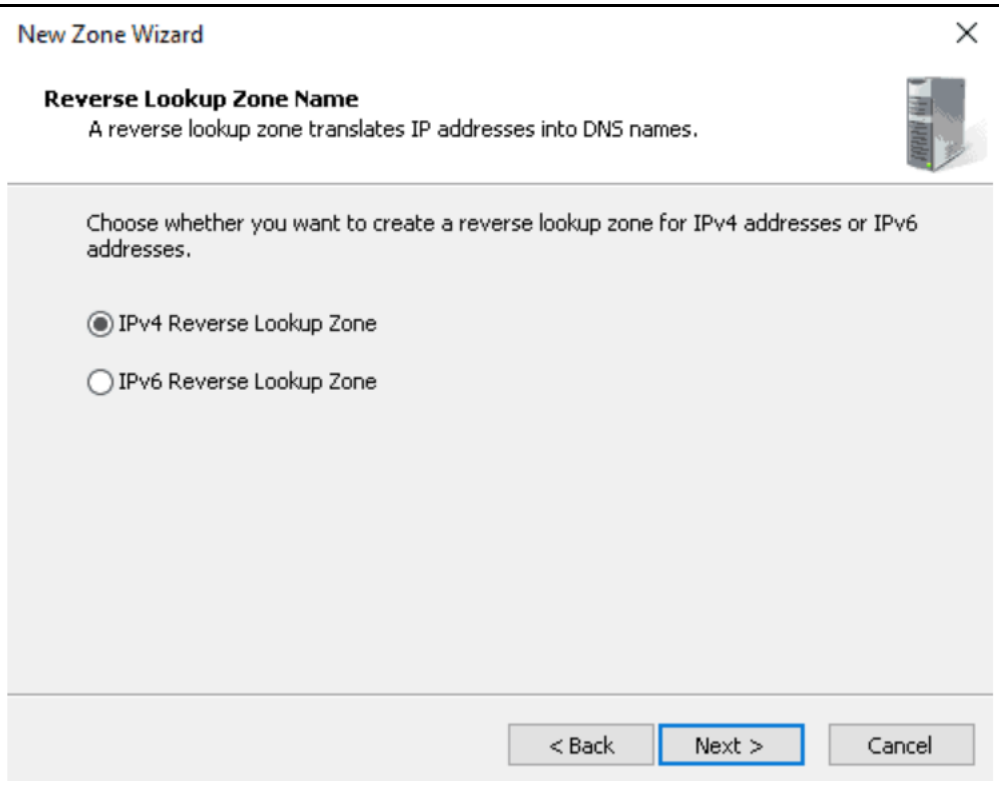
Step 5: Now, choose the Primary zone and press **Next**.



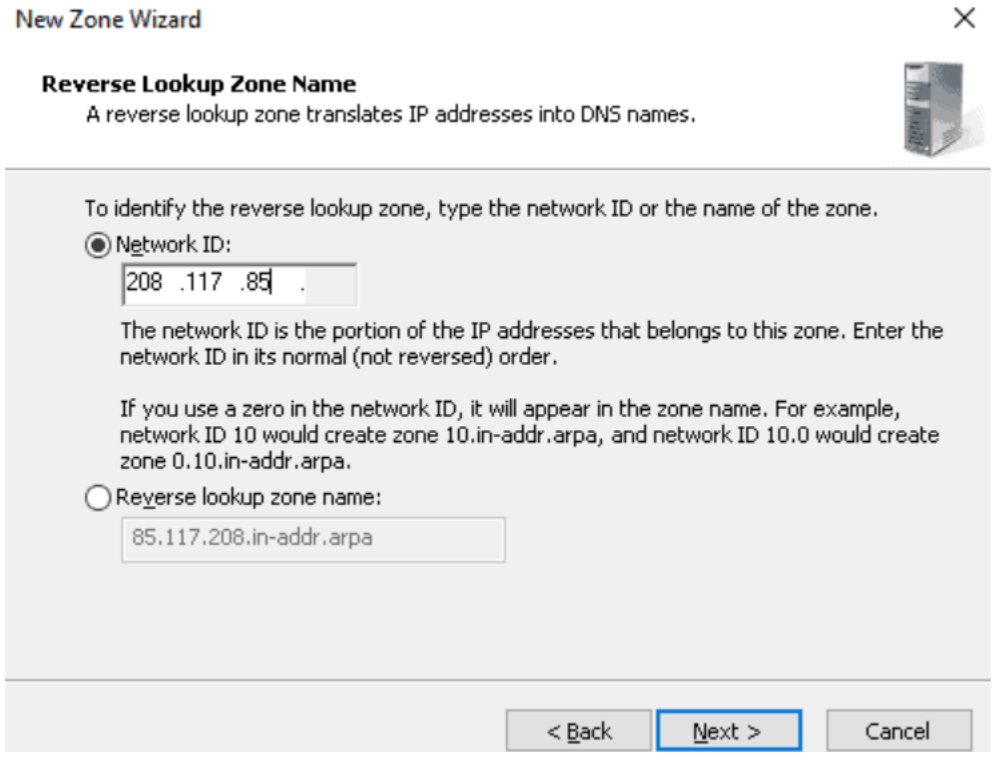
Step 6: From this step forward, the setup is different from our previous section. Next, click **Next** after selecting the **Reverse lookup zone**.



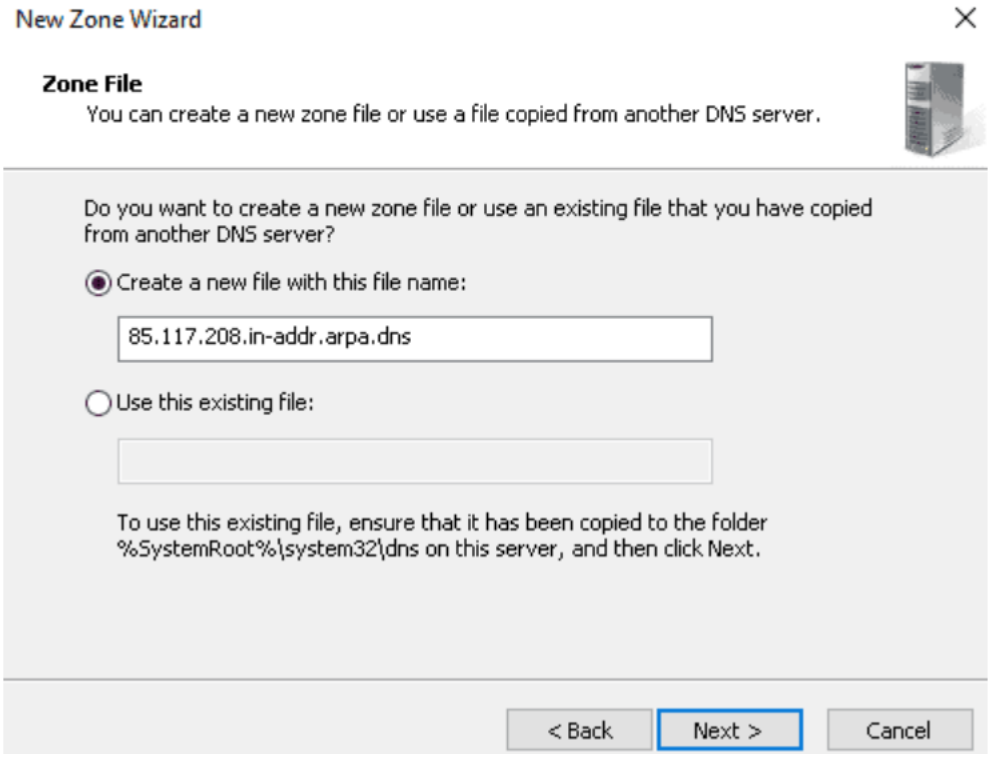
Step 7: After, select **IPv4 Reverse Lookup Zone** and click on **Next**.



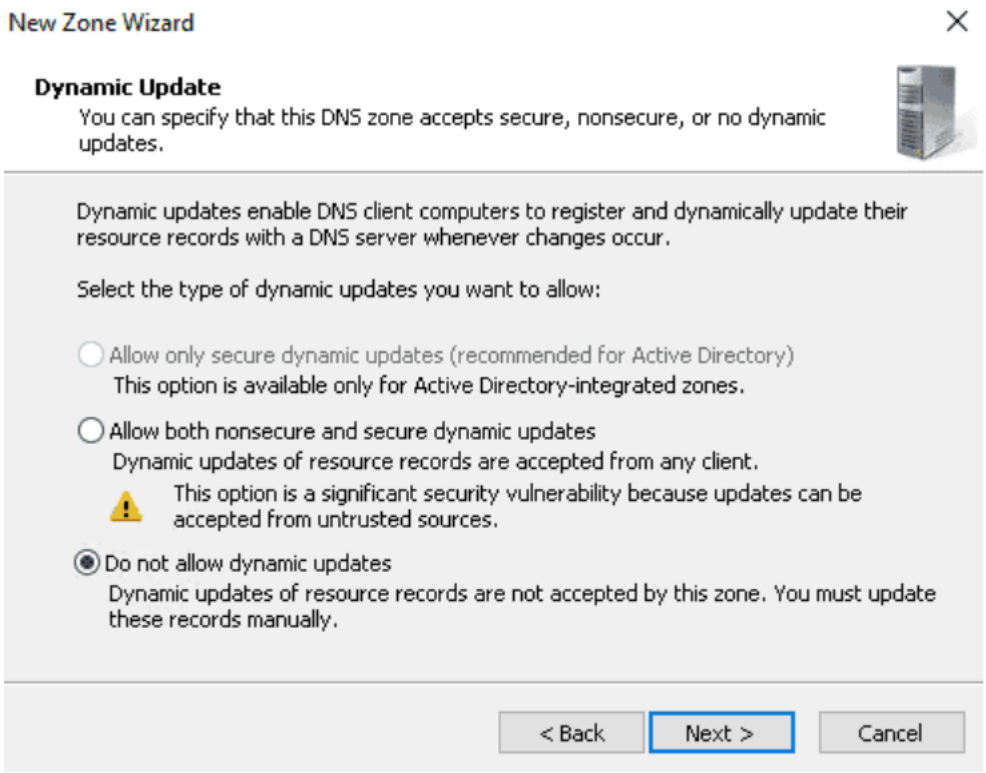
Step 8: Define your network ID and click **Next**.



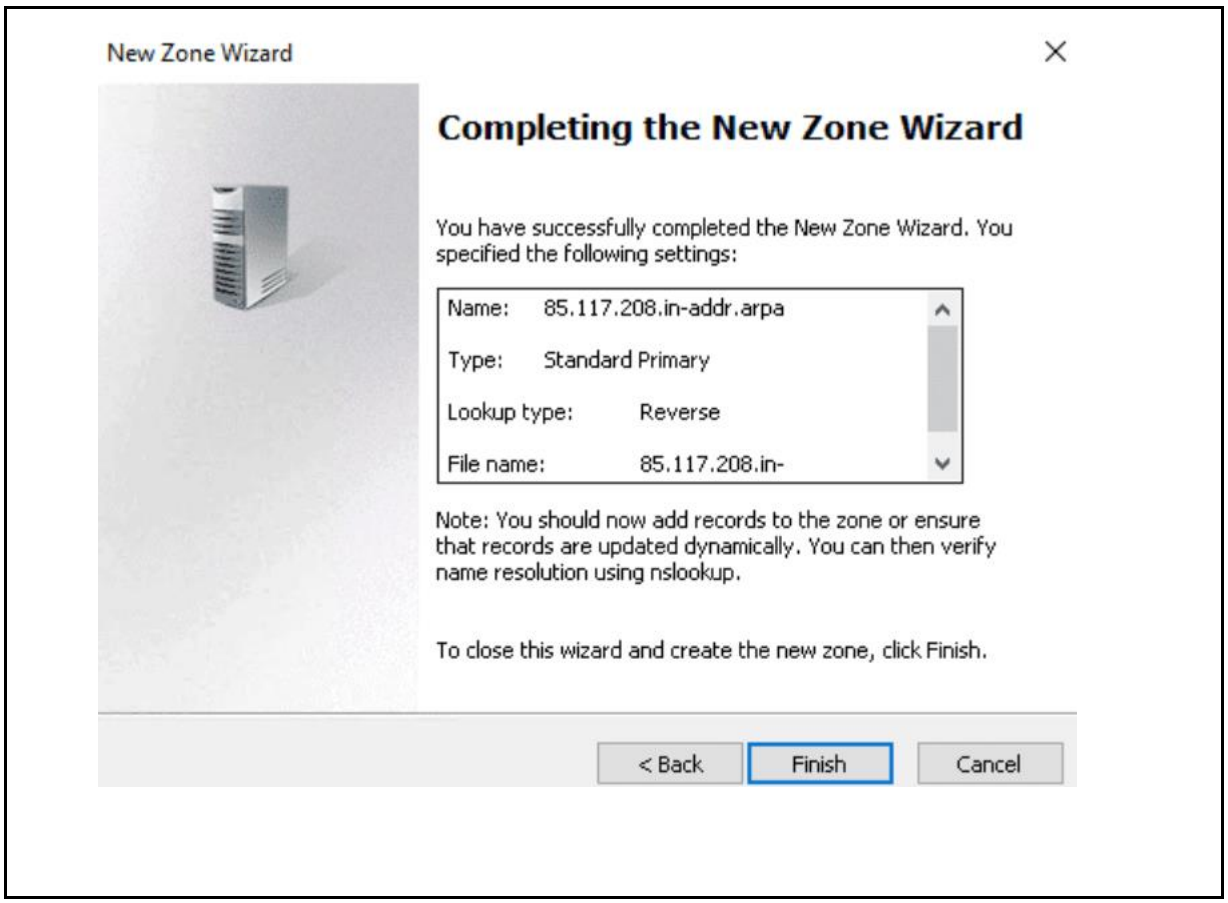
Step 9: Further**,** choose **"Create a file with the file name"** and press **Next**.



Step 10: Please check the box next to **"Do not allow dynamic update"** and click **Next**.



Step 11: In sum, press the **Finish** button



Points to Remember

- **Steps of DNS Settings Configuration**

Configuring the Forward Lookup Zone

Step 1: On the server manager, navigate to **Tools > DNS** to access the DNS manager

Step 2: Right click on the server name and select **Properties**.

Step 3: Select the **New Zone** option.

Step 4: Press **Next**.

Step 5: Choose the Primary zone and press **Next**.

Step 6: Click **Next** after selecting the **Forward lookup zone**.

Step 7: Enter the name of our zone and press **Next**

Step 8: Choose **"Create a file with the file name"** and press **Next**.

Step 9: Check the box next to "Do not allow dynamic update" and click Next.

Step 10: Press the Finish button

- **Configuring the Reverse Lookup Zone**

Step 1: On the server manager, navigate to **Tools > DNS** to access the DNS manager:

Step 2: Right click on the server's name and select **Properties.**

Step 3: Here, selects the **New Zone** option.

Step 4: Press **Next**.

Step 5: Now, choose the Primary zone and press **Next**.

Step 6: From this step forward, the setup is different from our previous section. Next, click **Next** after selecting the **Reverse lookup zone**.

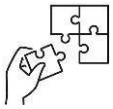
Step 7: After, select **IPv4 Reverse Lookup Zone** and click on **Next**.

Step 8: Define your network ID and click **Next**.

Step 9: Further**,** choose **"Create a file with the file name"** and press **Next**.

Step 10: Please check the box next to **"Do not allow dynamic update"** and click **Next**.

Step 11: In sum, press the **Finish** button.



Application of learning 4.2.

Suppose that your school needs to establish DNS server, you are asked to configure DNS role for domain name translation.

Indicative content 4.3: Testing of DNS Configuration

Duration: 3 hrs

Practical Activity 4.3.1: Testing DNS Configuration

Task:

1: Referring to the key reading 4.2.1, As an internet and networking technology student, you are asked to go to test DNS server configuration settings

2: Present the procedures of all step performed during DNS configuration.

3: Present your work to the trainer and whole class.

4: Read key reading 4.3.1 and ask clarification where necessary

5: Perform the task provided in application of learning 4.3

Key readings 4.3.1 Testing DNS Configuration

After configuring DNS settings, it is crucial to test them to ensure that everything is working correctly. Here's how you can verify DNS settings, ping a domain, and resolve domain names effectively:

1.1. Verify DNS Settings

You can verify DNS settings using several tools to ensure that your DNS records have been correctly propagated across the internet.

a. Using dig Command

The **dig** command (Domain Information Groper) is a powerful tool used to query DNS servers and verify DNS records.

- Check A Record (IPv4):

```
dig example.com
```

- **Check AAAA Record (IPv6):**

```
dig example.com AAAA
```

- Check CNAME Record:

```
dig www.example.com CNAME
```

- Check MX Record:

```
dig example.com MX
```

- Check NS Records:

```
dig example.com NS
```

- Checking TTL and Record Details:

The output from `dig` will show the TTL (Time to Live), IP addresses, and other relevant DNS record information.

b. Using `nslookup` Command

nslookup is another tool used to query DNS servers.

- Check A Record (IPv4):

```
nslookup example.com
```

- Specify DNS Server:

You can also query a specific DNS server:

```
nslookup example.com 8.8.8.8
```

c. Online DNS Lookup Tools

You can also use online tools to verify DNS settings:

- [Google Dig Tool](https://toolbox.googleapps.com/apps/dig/)
- [MXToolbox](https://mxtoolbox.com/DNSLookup.aspx)
- [DNSChecker](https://dnschecker.org/)

These tools allow you to check DNS records across multiple locations worldwide and confirm whether DNS propagation has occurred.

1.2. Ping a Domain Name

The **ping** command is used to check the network reachability of a domain or server by sending ICMP echo requests. While ping doesn't directly test DNS records, it can confirm that the domain name resolves to an IP address and that the server is reachable.

a. Ping using IPv4:

```
ping example.com
```

This command will resolve the domain name to its IPv4 address and send packets to test the network connection.

Example output:

```
PING example.com (93.184.216.34): 56 data bytes
64 bytes from 93.184.216.34: icmp_seq=0 ttl=56 time=25.2 ms
64 bytes from 93.184.216.34: icmp_seq=1 ttl=56 time=25.1 ms
```

b. Ping using IPv6:

```
ping6 example.com
```

This will resolve the domain name to its IPv6 address and test network connectivity over IPv6.

1.3. Resolve a Domain Name

Domain name resolution refers to converting a domain name (e.g., example.com) into its corresponding IP address (e.g., 93.184.216.34 for IPv4, or 2606:2800:220:1:248:1893:25c8:1946 for IPv6).

a. Using dig or nslookup to Resolve IP Addresses:

You can use the **dig or nslookup** commands as mentioned earlier to resolve domain names into their respective IP addresses.

For example:

```
dig example.com
```

This will return:

```
example.com.    300    IN    A    93.184.216.34
```

b. Resolve with host Command

The **host** command is another option for resolving domain names:

```
host example.com
```

Example output:

```
example.com has address 93.184.216.34
example.com has IPv6 address 2606:2800:220:1:248:1893:25c8:1946
```

1.4. Verify DNS Propagation

Sometimes DNS changes may take up to 24-48 hours to propagate across the global DNS system. To check whether DNS changes have been fully propagated:

- Use DNS Propagation Checker:

DNSChecker(https://dnschecker.org) allows you to verify whether DNS records have been propagated to multiple servers worldwide.

WhatsMyDNS(https://www.whatsmydns.net/) also shows global DNS status for various records.

These tools display results from multiple geographic locations, helping you determine whether the DNS changes have fully propagated.

Points to Remember

- To test your DNS configuration effectively, follow these steps:

Step 1: Verify DNS Settings: For Windows:

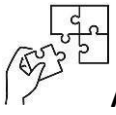
1. Open **Control Panel**.
2. Navigate to **Network and Internet > Network and Sharing Center.**
3. Click on Change **Adapter Settings**.
4. Right-click your active network connection and select **Properties**.
5. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
6. Ensure the settings are correct, either obtaining DNS server addresses automatically or using specific DNS servers.

Step 3: Resolve a Domain Name

To explicitly test DNS resolution, use tools like **nslookup** or **dig**.

Using nslookup:

1. Open a command prompt or terminal.
2. Type the following command:
3. nslookup www.example.com



Application of learning 4.3

Suppose that your school needs to establish DNS server, you are asked to test DNS server for domain name translation.

Learning outcome 4 end assessment

Written assessment

Multiple choice questions: Circle the letter corresponding to the correct answer:

1. What does DNS stand for?
    A) Domain Name System
    B) Dynamic Network Service
    C) Domain Network System
    D) Dynamic Name Service
2. Which of the following is an authoritative source of information about each DNS domain name**?**
    A) Perfmon
    B) Zone
    C) Record
    D) Sysprep
3. Which server is used to convert host names into IP addresses?
    A) DNS server
    B) Network server
    C) Web server
    D) File server
4. What type of DNS query requires the server to respond with the best information it possesses at that time?
    A) Recursive query
    B) Iterative query
    C) Action query
    D) Parameter query
5. Which of the following records maps a domain name to an IPv4 address?
    A) AAAA
    B) CNAME
    C) MX
    D) D)A
6. What is the purpose of a DNS forwarder?
    A) To cache DNS queries
    B) To forward DNS queries for external names to other DNS servers
    C) To resolve local DNS queries only
    D) To create new DNS zones
7. Which zone type contains the master copy of the zone database?
    A) Stub zone
    B) Secondary zone
    C) Primary zone

D) Hybrid zone

8. What is the Time to Live (TTL) in a DNS record used for?
    A) To specify how long the record is valid before being discarded
    B) To determine how long a resolver can cache the record
    C) To indicate when to refresh the record
    D) Both A and B
9. Which feature adds security to the DNS protocol by validating responses?
    A) DHCP
    B) DNSSEC
    C) Cache locking
    D) Forwarding
10. What type of query does a resolver use when it needs an immediate response?
    A) Iterative query
    B) Recursive query
    C) Action query
    D) Parameter query
11. Which of the following statements about Dynamic DNS (DDNS) is true?
    A) DDNS requires a Microsoft DHCP server to work.
    B) DDNS clients may not register their own addresses.
    C) DDNS works only with Microsoft clients and servers.
    D) The Windows Server 2012 DDNS server can interoperate with recent versions of BIND.
12. What does a CNAME record do in DNS?
    A) Maps an IP address to a domain name.
    B) Creates an alias for an existing record.
    C) Specifies mail exchange servers.
    D) Defines the start of authority for a zone.
13. Which command can be used to check if a specific domain name resolves correctly?
    A) nslookup
    B) ping
    C) ipconfig
    D) tracert
14. In Windows Server, which tool is primarily used for managing DNS zones and records?
    A) Active Directory Users and Computers
    B) DHCP Management Console
    C) DNS Manager
    D) Group Policy Management Console
15. What is the function of a stub zone in DNS?
    A) It contains all records for a domain.
    B) It holds only the necessary records to identify authoritative name servers.

C) It is used for caching purposes only.
D) It stores reverse lookup records exclusively.

Practical assessment

Suppose that your school needs to implement server based on windows server as a trainee in networking and Internet Technology you are required for performing DNS server installation, configure and testing server configuration.

References

Hao, S., Wang, H., Stavrou, A., & Smirni, E. (2015, November). On the DNS deployment of modern web services. *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*, 100–110. IEEE. https://doi.org/10.1109/ICNP.2015.7363514

Panek, W. (2018). *Installing Windows Server 2016*.

Krause, J. (2016). *Mastering Windows Server 2016*. Packt Publishing.

Krause, J. (2019). *Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities*. Packt Publishing.

Richards, J., Allen, R., & Lowe-Norris, A. G. (2006). *Active Directory*. O'Reilly Media.

Allen, R., & Lowe-Norris, A. (2003). *Active Directory*. O'Reilly Media.

Clines, S., & Loughry, M. (2008). *Active Directory for dummies*. John Wiley & Sons.

InfraSOS. (n.d.). Install and configure DNS server on Windows Server. Retrieved January 8, 2025, from https://infrasos.com/install-and-configure-dns-server-on-windows-server/

Jotelulu. (n.d.). Deploy DNS server using PowerShell commands. Retrieved January 8, 2025, from https://jotelulu.com/en-gb/blog/deploy-dns-server-using-powershell-commands/

Indicative contents
5.1 Installation of web server **5.2 Configure Web Server (IIS)** **5.3 Implement Security access control** **5.4 Deploying Web application** **5.5 Test Web application**

Key Competencies for Learning Outcome 5 : Deploy Web Services

Knowledge	Skills	Attitudes
● Description of web servers' software ● Identifications of web server installation prerequisites ● Description of deployment Method	● Selecting of web server hardware and software. ● Performing IIS installation. ● Configuring web services. ● Implementing server security	● Having self-motivation ● Being analytical and details oriented

Duration: 10 hrs

Learning outcome 5 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe correctly web servers' software based on Microsoft standard.
2. Identify clearly web server installation prerequisites based on Microsoft standard.
3. Describe clearly the deployment process as used in web services.
4. Perform properly web service installation process as used in windows server.
5. Perform correctly web service configuration as used in server administration.
6. Implement appropriately security access for web server based on Microsoft standard

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS ● Router ● Switch	● Router ● VMware Workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD ● USB	● ● Electricity ● Cables ● Internet

Indicative content 5.1: Installation of Web Server

Duration: 2 hrs

Theoretical Activity 5.1.1: Introduction To Web Server

Tasks:

1: Answer the following questions**:**

i. With your owner's word explain a web service?

ii. Enumerate three advantages of using web services?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 5.1.1.

Key readings 5.1.1: Introduction to Web Server

1.Describing web servers' software

A web server is a computer system that combines hardware and software to store, process, and deliver web content to clients over the Internet. When a user requests a web page through a web browser, the web server responds by retrieving the requested content and sending it back to the user's device. This interaction typically occurs using the Hypertext Transfer Protocol (HTTP) or its secure variant, HTTPS.

1.1. Apache Web Server

Apache HTTP Server, commonly referred to as Apache, is one of the most widely used web servers globally. It is open-source and cross-platform, making it versatile for various environments, including Linux and Windows.

- **Key Features**

- **Modular Architecture**: Apache operates on a modular system, allowing users to extend its functionality with various modules, such as mod rewrite for URL rewriting and mod_ssl for secure connections.
- **Virtual Hosting**: This feature enables a single Apache installation to host multiple websites, making it efficient for shared hosting environments.
- **Security:** Apache supports modern authentication methods and can encrypt web traffic using SSL/TLS.
- **Performance:** It can handle a significant number of connections, though it may not perform as well as some competitors under extremely high loads.

1.2. Internet Information Services (IIS)

IIS is a web server created by Microsoft, specifically designed for Windows Server environments. It is known for its integration with other Microsoft products and

services.

- **Key Features:**

- **User-Friendly Interface:** IIS provides a graphical user interface that simplifies management and configuration tasks.
- **Security Features**: It includes built-in security features such as request filtering, URL authorization, and SSL support.
- **Application Pooling**: IIS allows applications to run in isolated environments, enhancing security and stability by preventing one application from affecting others.
- **Integration with .NET**: IIS is optimized for hosting ASP.NET applications, making it a preferred choice for developers working within the Microsoft ecosystem.

1.3. Nginx Web Server

Nginx (pronounced "engine-x") is a high-performance web server and reverse proxy server known for its speed and efficiency in handling concurrent connections.

- **Key Features**

- **Event-Driven Architecture**: Nginx uses an asynchronous, event-driven approach, allowing it to handle many connections with low resource consumption.
- **Load Balancing**: Nginx can distribute incoming traffic across multiple servers, enhancing performance and reliability for high-traffic websites.
- **Static Content Serving**: It excels at serving static content quickly, making it a popular choice for content-heavy websites.
- **Reverse Proxy Capabilities**: Nginx can act as a reverse proxy, providing additional layers of security and load balancing for backend applications.

1.4. LiteSpeed Web Server

LiteSpeed is a commercial web server that offers high performance and low resource consumption, making it a popular choice for high-traffic websites.

- **Key Features:**

- **Dynamic Content Handling**: LiteSpeed can process dynamic content efficiently without requiring additional software like PHP-FPM.
- **HTTP/3 Support:** It supports the latest HTTP/3 protocol, enhancing speed and performance for modern web applications.
- **Built-in Caching**: LiteSpeed includes built-in caching mechanisms that improve response times and reduce server load.

1.5. Apache Tomcat

Apache Tomcat is an open-source application server that implements the Java Servlet and Java Server Pages (JSP) specifications. It is designed to run Java applications.

- **Key Features**

- **Java Support**: Tomcat is specifically designed for running Java-based web

applications, making it a popular choice for Java developers.

- **Servlet and JSP Support**: It provides a robust environment for executing servlets and JSPs, allowing for dynamic content generation.
- **Integration with Apache HTTP Server:** Tomcat can be used in conjunction with Apache HTTP Server to serve static content while handling dynamic requests through Java.
- **Management Tools:** Tomcat offers a web-based management interface for deploying and managing applications easily.

When preparing to install a web server, specifically Internet Information Services (IIS) on Windows Server, it is essential to meet certain hardware and software prerequisites to ensure a successful installation and optimal performance.

2.Installation prerequisites

2.1. Hardware Prerequisites

- **Processor**: minimum is 1.4 GHz 64-bit processor compatible with the x64 instruction set.
- **Recommended:** multi-core processors for better performance, especially under high load.
- **Memory (RAM**): minimum is 2 GB for Server with Desktop Experience.
- **Recommended:** More than 2 GB for better performance, particularly for hosting multiple sites or applications.
- **Disk Space**: minimum of 30 GB of available disk space is recommended for the operating system and IIS. Additional space may be required depending on the applications hosted and the amount of content served.

2.2. Software Prerequisites

- **Operating System**: Windows Server 2016, 2019, or 2022 (Standard or Datacenter editions). Ensure that the server is fully updated via Windows Update before installation.
- **IIS Installation:** The Web Server (IIS) role must be enabled. This can be done through Server Manager or PowerShell.
- **.NET Framework:** The Microsoft .NET Framework 4.6 or later is required for running ASP.NET applications. This is often included in the IIS installation.
- **Web Deployment Tool**: Install Web Deploy (version 2.1 or later) if you plan to use it for publishing and managing web applications.
- **Management Tools**: Install IIS Management Service for remote management capabilities.
- **Security Certificates:** If planning to use HTTPS, ensure you have the necessary SSL/TLS certificates installed.
- **Basic Authentication**: If needed, install the Basic Authentication module for IIS to manage user credentials securely.

Practical Activity 5.1.2: Installing web Server

Task:

1: Referring to the key reading 5.1.1, As a sever administrator, you are asked to go to the computer lab and install web server.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 5.1.2 and ask clarification where necessary

5: Perform the task provided in application of learning 5.1.2

Key readings 5.1.2 Installing web Server

1.Perform installation process

To install a web server on a Windows machine, you can choose between different options, such as Apache HTTP Server, Nginx, or Internet Information Services (IIS). Below are the installation steps for each.

1.1. Installing Apache HTTP Server

- **Download Apache:** Go to the Apache Lounge website and download the ZIP file for Apache.
- **Extract Files:** Unzip the downloaded file to a location on your computer, preferably to the root of the **C:\ drive (e.g., C:\Apache24).**
- **Installing Nginx**
- **Download Nginx:** Visit the [Nginx download page] (https://nginx.org/en/download.html) and download the latest version for Windows.
- **Extract Files:** Unzip the downloaded file to a preferred location (e.g., C:\nginx).

1.2. Installing IIS (Internet Information Services)

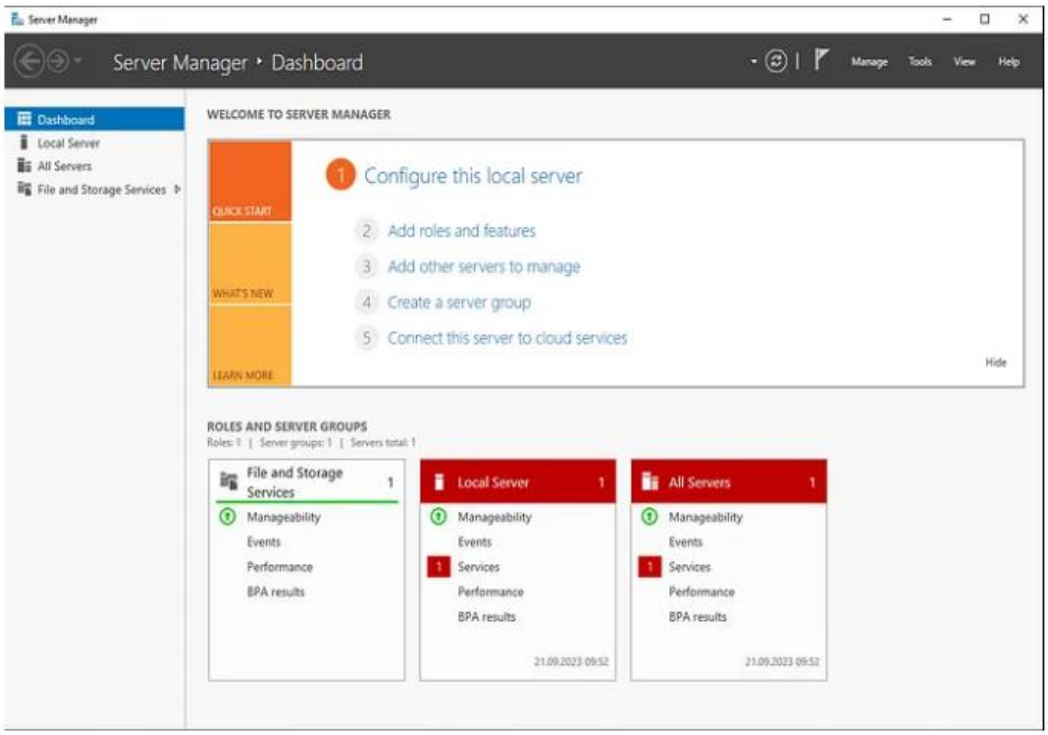
To install IIS (Internet Information Services) on Windows Server using Server Manager by following the steps below:

1. **Server Preparation:** Make sure you have Administrator privileges on your server if you are using a Windows Server operating system.

2. **Opening Server Manager:**

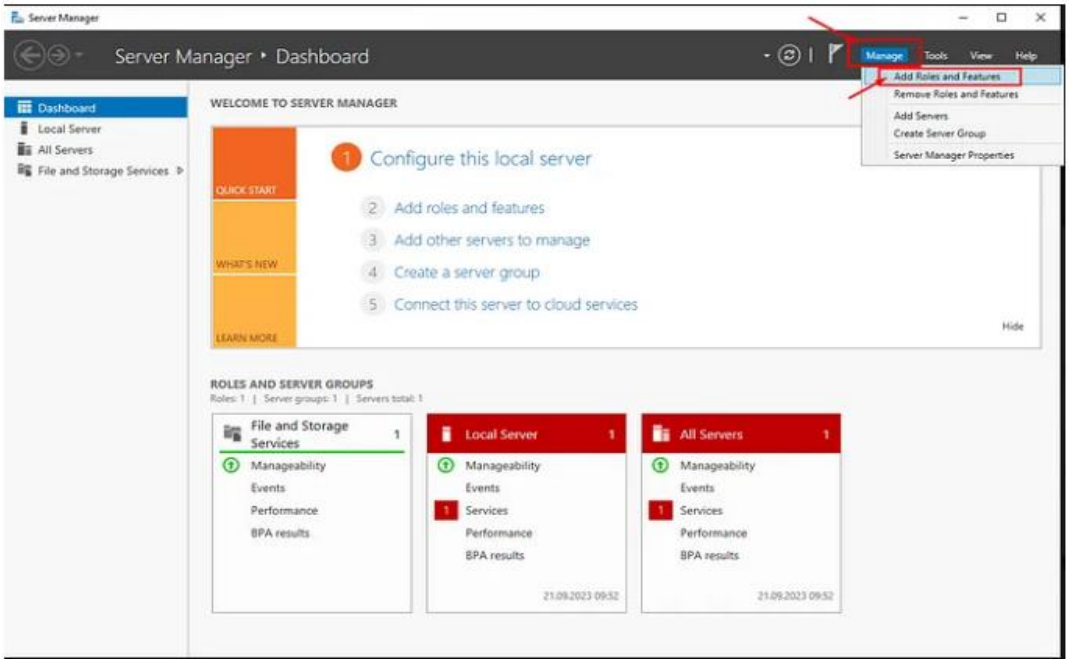
— Click on the Start button.

— Search for “Server Manager” and open it.



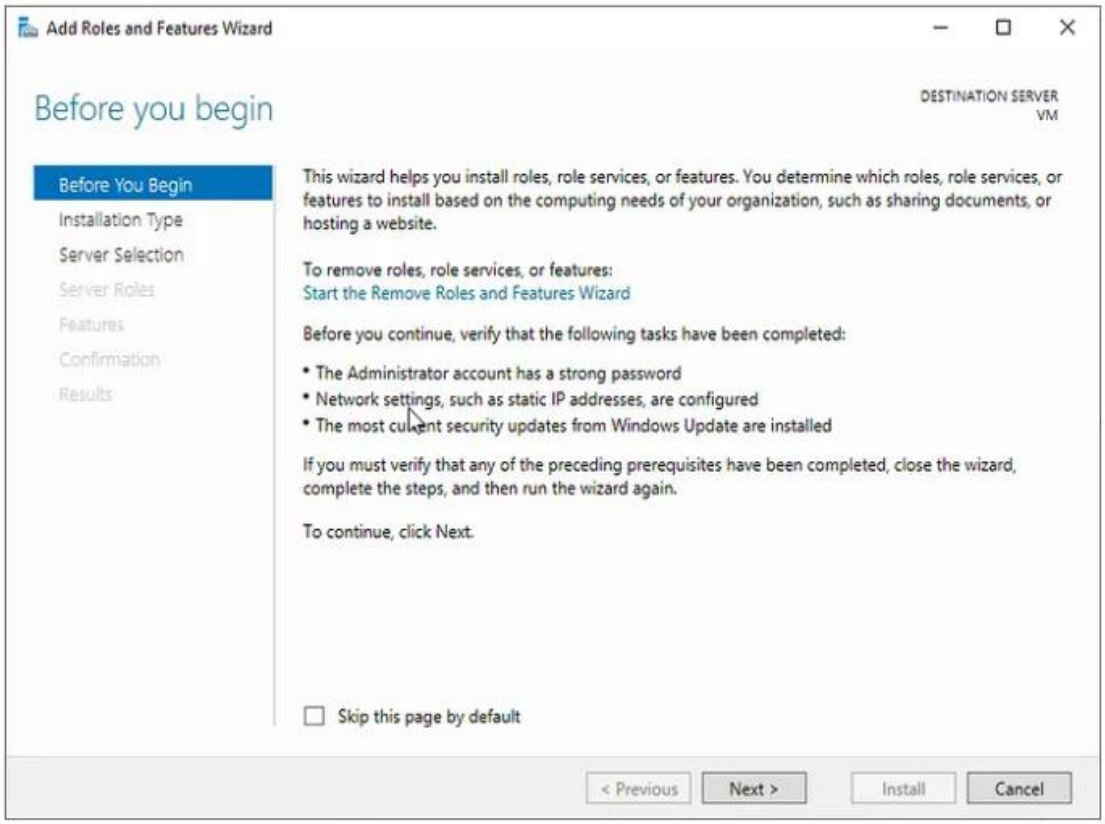
3. Select "Add Roles and Features" from the Left Menu:

In the Server Manager main window, locate "Upper Banners" and select "Add Roles and Features."



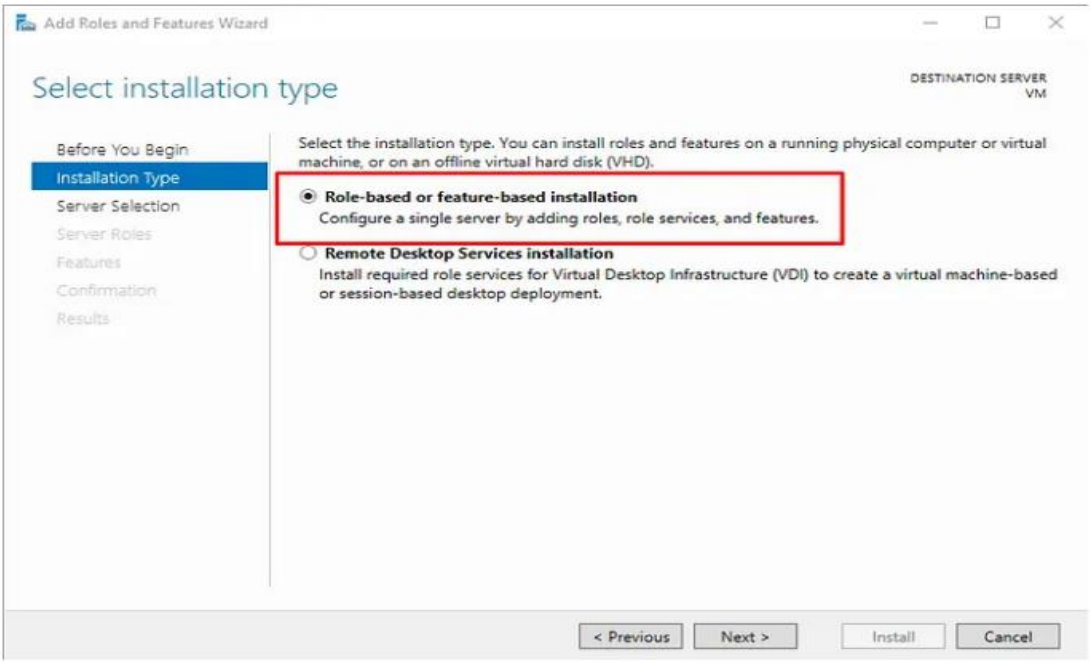
4. Launch the "Add Roles and Features Wizard":

The "Add Roles and Features Wizard" window will open. This wizard helps you add roles and features to your server.



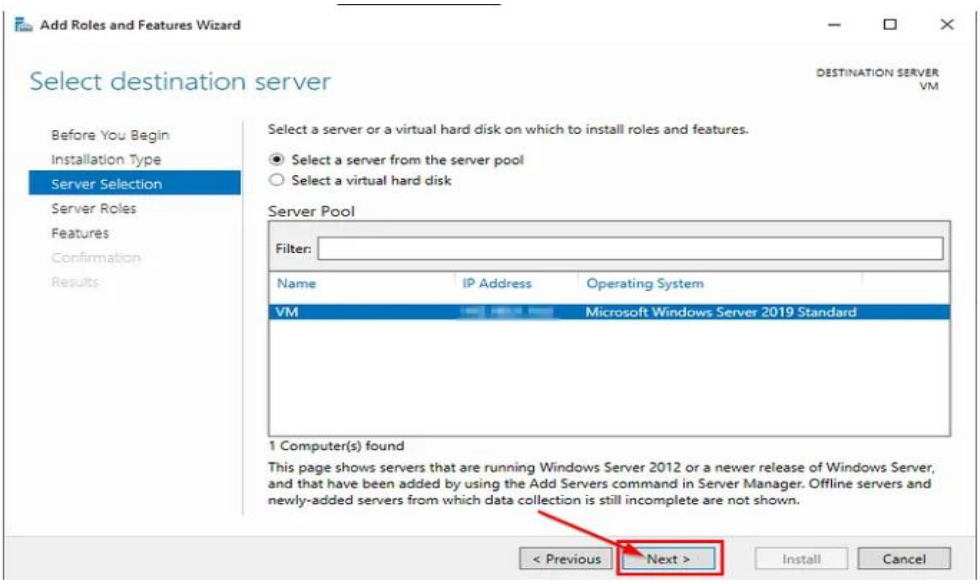
5. Select Features:

In the first step of the wizard, choose the "Installation Type." Typically, select "Role-based or feature-based installation," and proceed.



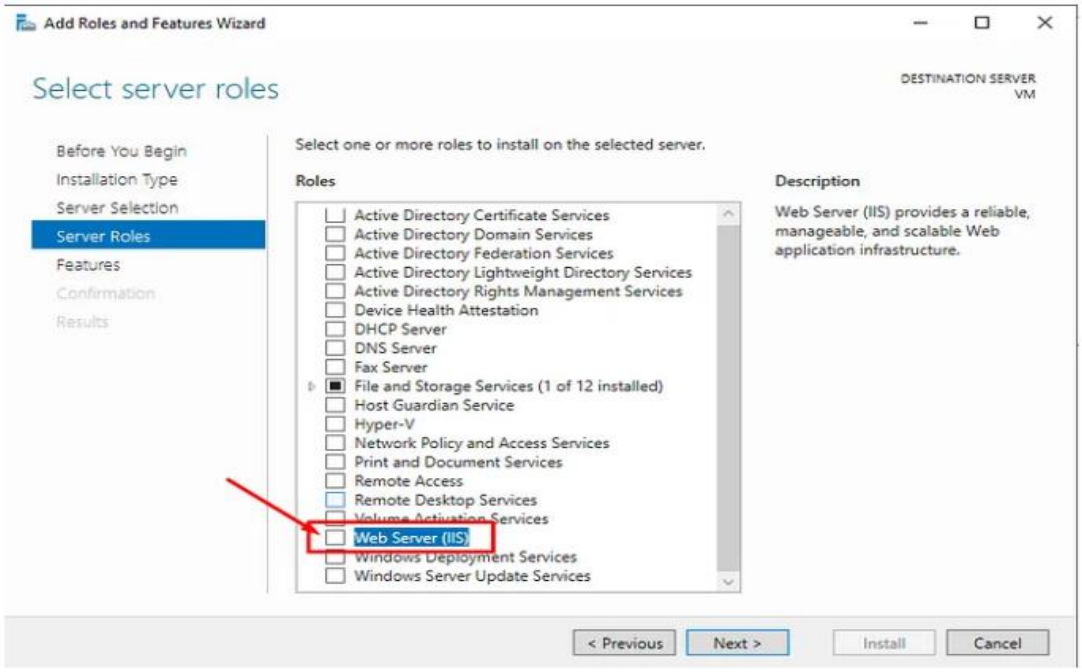
6. Choose the Target Server:

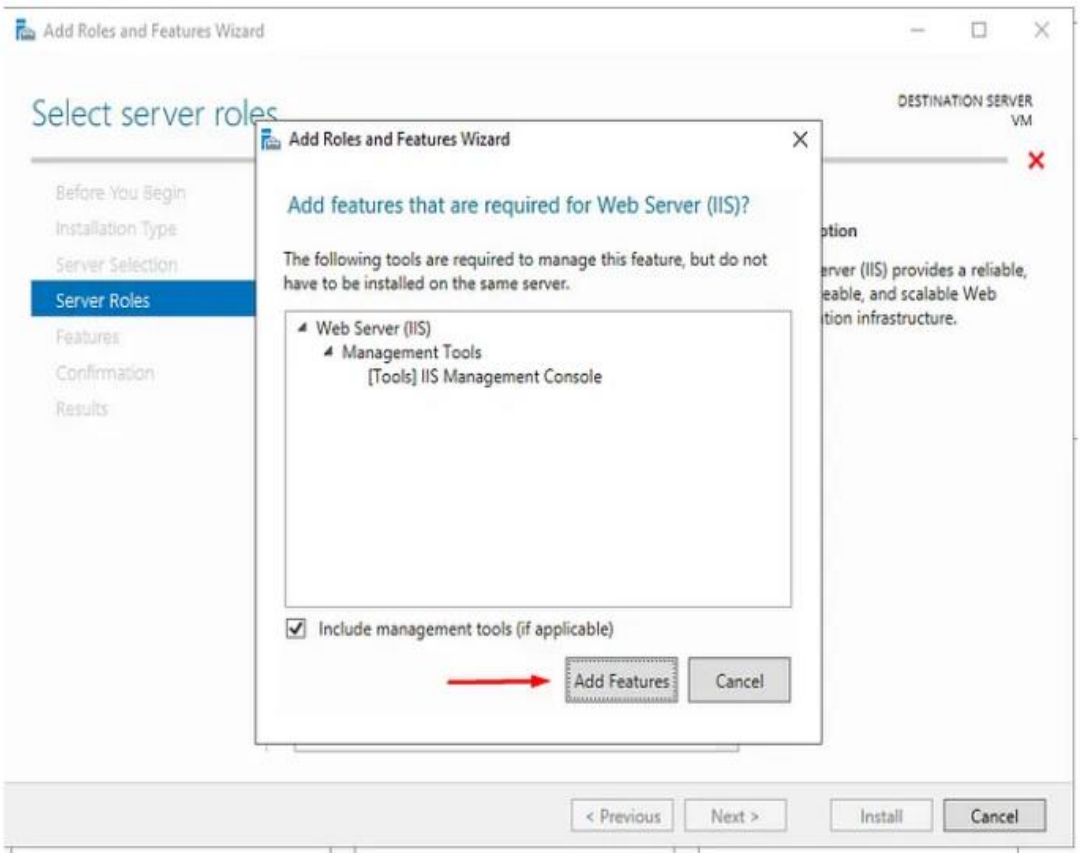
Select your server or specify the target server, then click "Next."



7. Select Roles:

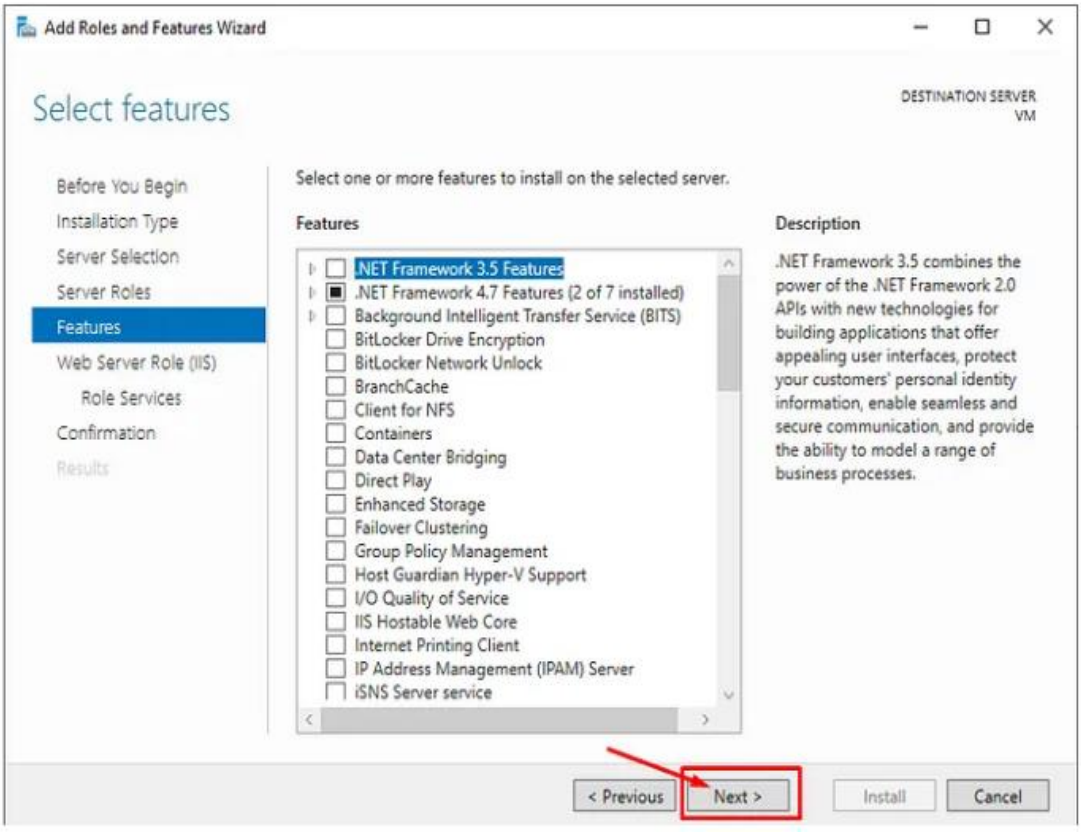
In the "Roles" section, find "Web Server (IIS)" and check the box. You can also select additional components if needed.





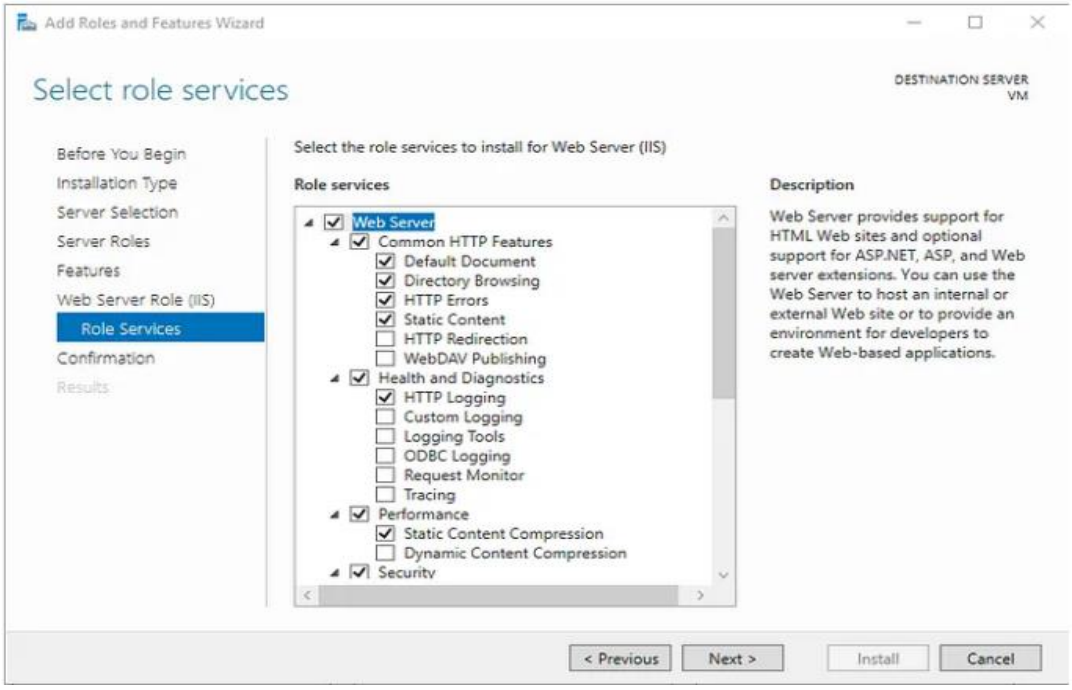
8. Review Accessibility Information:

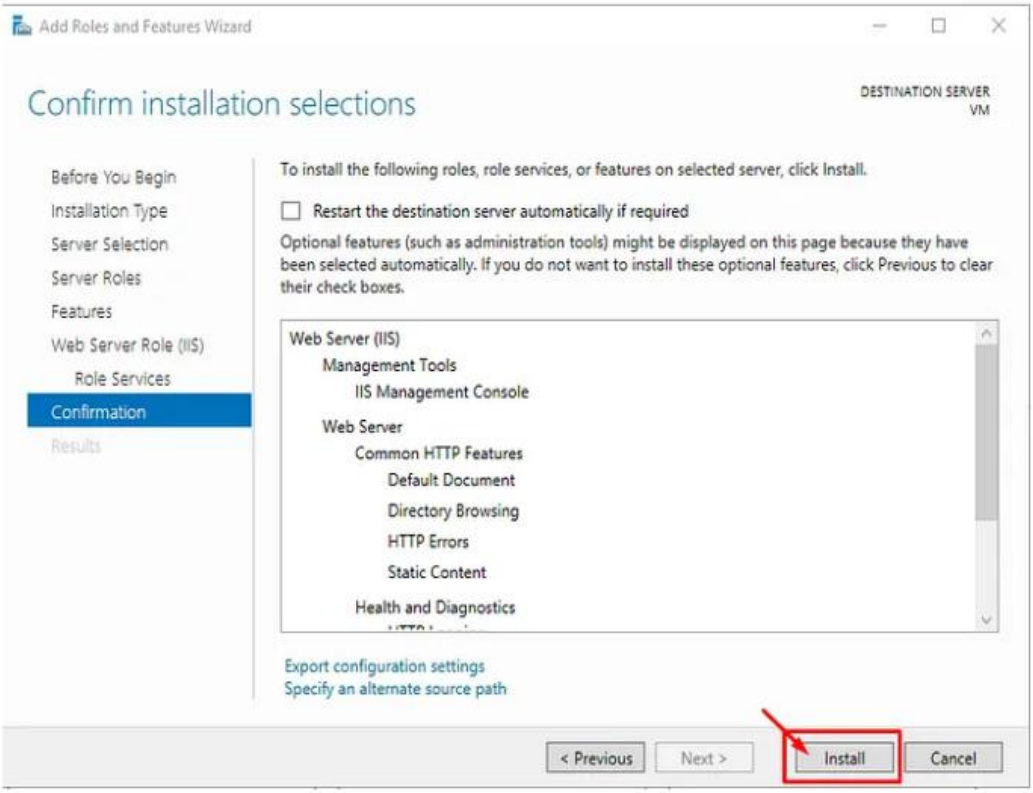
Follow the wizard's progression and configure necessary options when prompted.



9. Initiate the Installation:

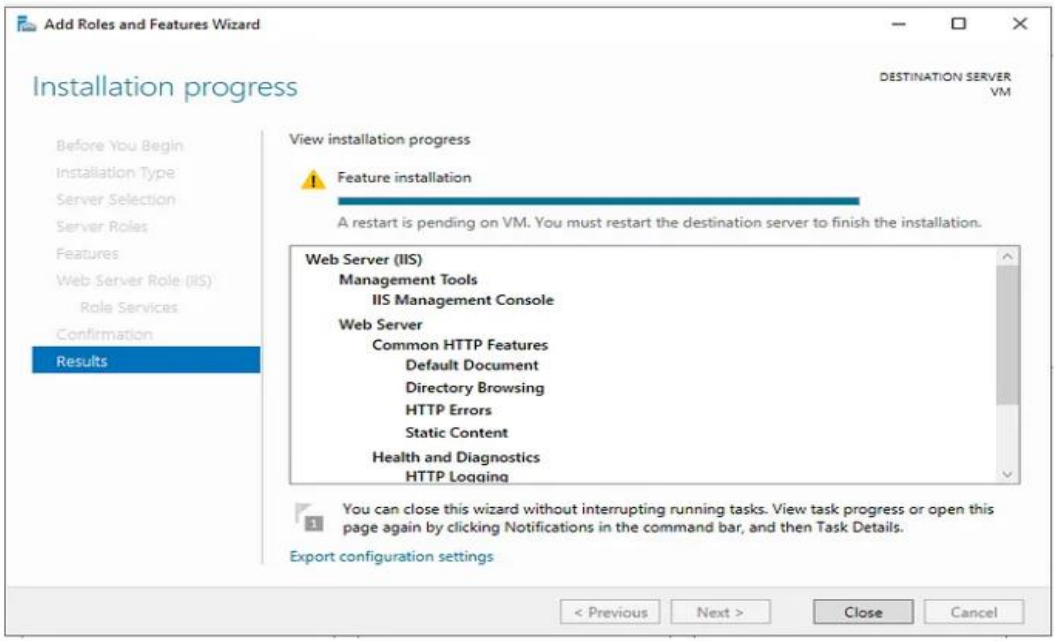
Start the IIS installation by clicking the “Install” button.





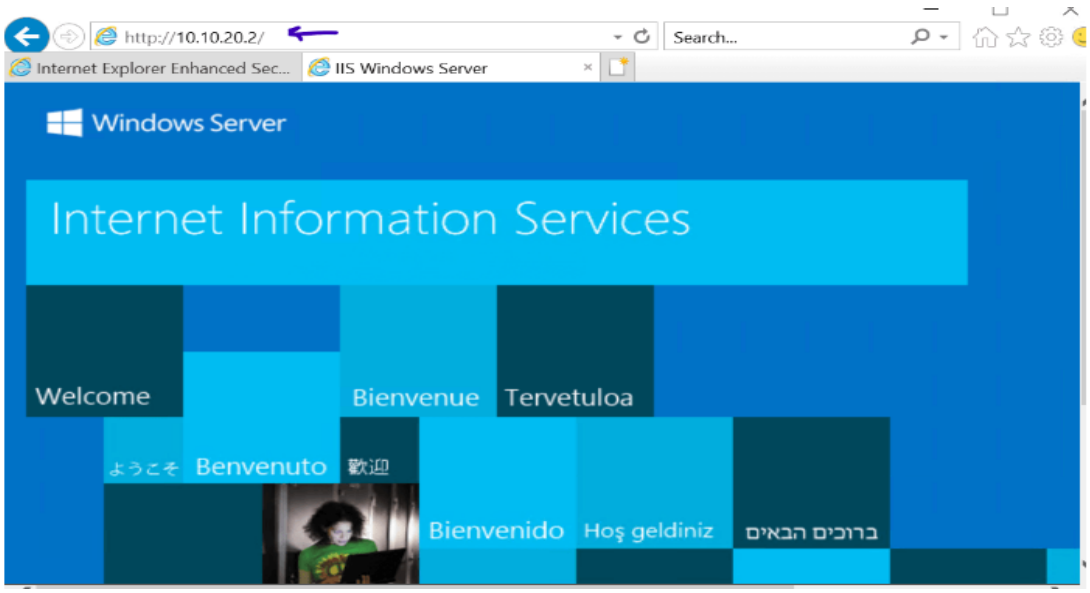
10. Completion of Installation:

Once the installation is complete, you will receive a confirmation message indicating successful installation. You will then be prompted for a reboot.



11. Prove the Web Server is running:

Open your browser either within the server or on a computer that can access your IIS Server network and input its IP Address on the browser's search as shown below.

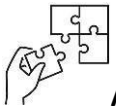


You can successfully install IIS by following these steps. Afterward, you can configure your websites and applications using the IIS Management Console.

Points to Remember

- Do not forget IIS (Internet Information Services) as the mean feature of webserver.
- Apache is basic element of web server.

- Do not forget Installation prerequisites while selecting web server hardware and software
- Make sure that IIS is selected during installation of web server.
- After web server (IIS) installation process, verify installation completion.



Application of learning 5.1.1

Suppose that your school needs to establish web server, you are asked to install web server within windows sever operating system.

Indicative content 5.2: Configure Web Server (IIS)

Duration: 2 hrs

Practical Activity 5.2.1: Creation real/virtual host and website hosting

Task:

1: Referring to the key reading 5.1.2, As a network administrator, you are asked to go to the computer lab to perform the followings: create real or virtual host, configure web server, make sample of website and host created website.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 5.2.1 and ask clarification where necessary

5: Perform the task provided in application of learning 5.2.1

Key readings 5.2.1: Creation real/virtual host and website hosting

1.Create real/virtual host

1.1. Real Host

A real host: typically refers to a dedicated server or a physical machine that hosts a website. This server is assigned a unique IP address and can serve one or more websites directly. In this setup, each website can operate independently, and resources are allocated specifically for that site.

1.2. Virtual Host

A virtual host, on the other hand, allows multiple websites to be hosted on a single physical server or IP address. This is achieved through a technique known as **virtual hosting**, which enables the server to differentiate between different domain names and serve the appropriate content based on the request received.

2.Host website

Step 1: Open IIS Manager

Click on the Start menu. Navigate to Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.

Step 2: Create a New Website (Real Host): In the **Connections** pane, expand the node for your server. Right-click on "**Sites**" and select **"Add Website".**

2.1. Configure the Website

In the "**Add Website"** dialog, fill in the following details:

- **Site name**: Enter a name for your new site (e.g., MyWebsite).

2.2. Physical path

• **Physical path**: Browse to the folder where your website files are stored (e.g., C:\inetpub\wwwroot\MyWebsite).

- **Binding:**

○ **Type:** Select http (or https if you have an SSL certificate).

○ **IP address**: Select **All Unassigned** or specify an IP address.

○ **Port:** Typically, this will be 80 for HTTP or 443 for HTTPS.

○ **Host name:** Enter the domain name you want to use for this site (e.g., **www.example.com**).

○ **Start Website immediately**: Ensure this option is checked. Click **OK** to create the website.

Step 3: Configure Host Headers for Multiple Websites (Virtual Hosts)

1. In the **Connections** pane, select the site you just created.
2. In the **Actions** pane on the right, click on **Bindings**.
3. In the **Site Bindings** dialog, click **Add**.

- **Configure the Binding**

In the Add Site Binding dialog, configure the following settings:

- **Type:** Select http or https.
- **IP address:** Select an IP address or leave as **All Unassigned**.
- P**ort**: Enter the port number (e.g**., 80 for HTTP**).
- **Host name**: Enter the domain name for the virtual host (e.g., www.anotherexample.com). Click **OK** to add the binding.

2.3. Test connectivity

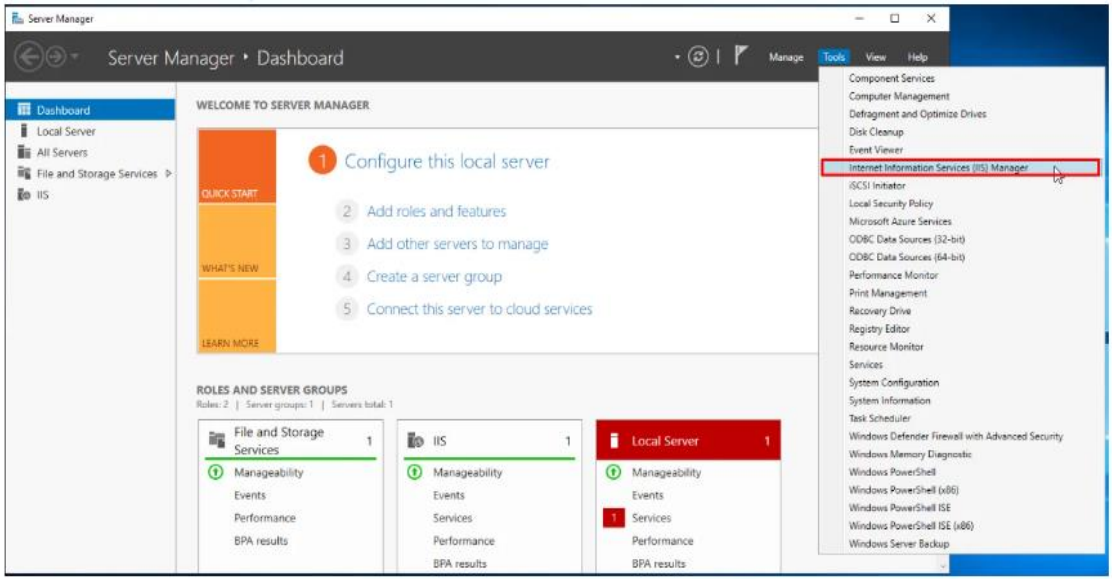
Step 4: Test Your Configuration

1. Open a web browser and enter the domain name you configured (e.g.,http://www.example.com).
2. You should see the content from the physical path you specified.

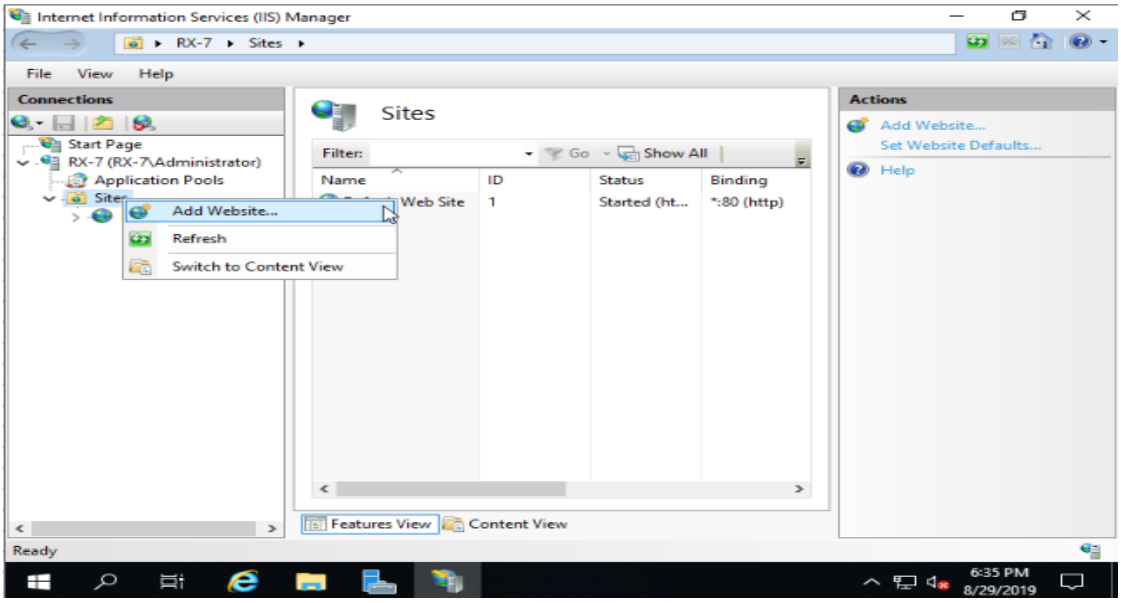
Step 5: Repeat for Additional Virtual Hosts

Repeat the steps to add more websites or virtual hosts as needed, ensuring each has a unique host name. By following these steps, you can successfully create real and virtual hosts in IIS 7.5, allowing you to host multiple websites on the same server using different domain names.

From the **Server Manager** application open the **IIS** services. Click on **tools** then click an **Internet Information Services (IIS) Manager**

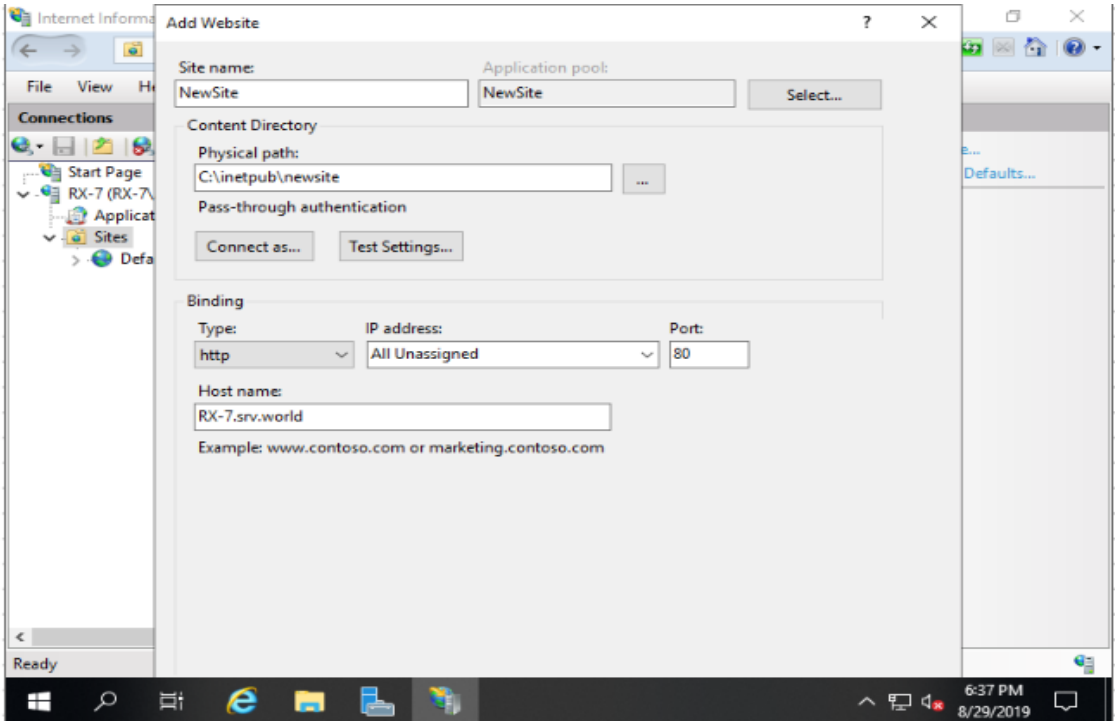


Once the IIS service is opened expand the **default Web Server**.

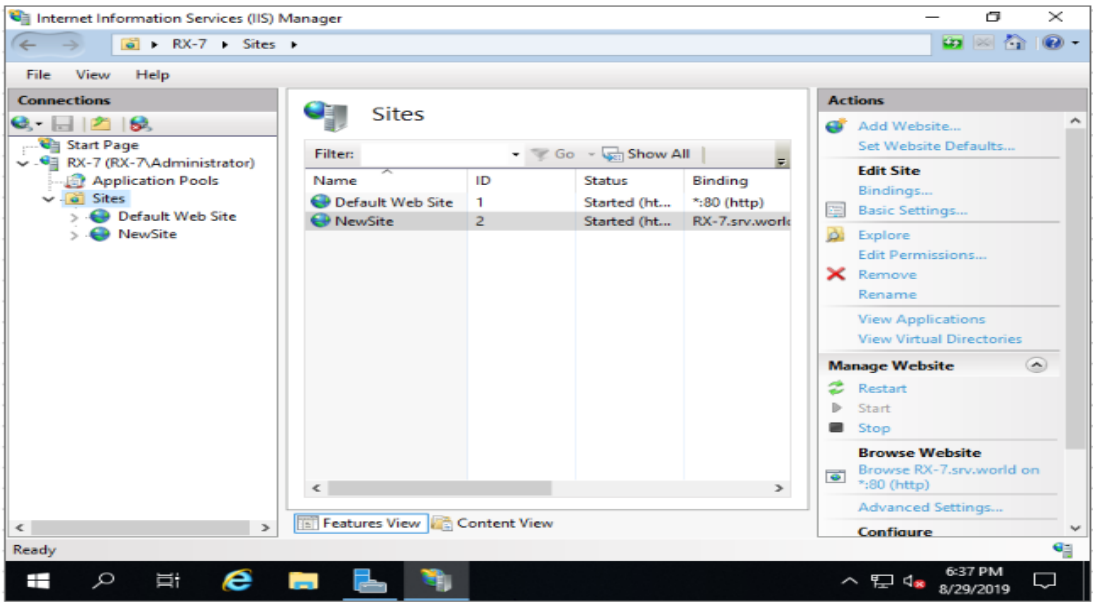


Right click the **Sites** to add site.

Input any Site name (it is used on IIS Manager) for Site name field, for **Physical path** field, input physical folder path for this new site, and for **Host name**, input server's hostname.



If added normally, new web Sete is displayed on Sites list.



Create a test page for new web Site and verify accesses

Points to Remember

- **Configure Virtual Hosts**

To set up virtual hosting (multiple websites on the same server):

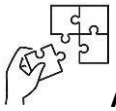
1. Edit Site Bindings:

- In IIS Manager, right-click on the newly created site and select Edit Bindings
- In the Site Bindings dialog, click on the Add. button to add a new binding for another hostname.
- Enter the new hostname (e.g., www.anotherexample.com) in the Host name field and ensure that the port is set to 80.
- Click OK to save changes.

2.Repeat for Additional Sites:

Repeat the process of adding websites with unique hostnames as needed.

- **steps of creating real/virtual host**
  1. Open IIS Manage: Navigate to **Control Panel**, select **Administrative Tools**, and then open **Internet Information Services (IIS) Manager**Add a New Website
  2. Add a New Site
  3. Configure firewall Settings
  4. Test your website
  5. Upload website



Application of learning 5.2.

Our school has website for break news and announcement, also school manger after setup local area network wishes to host a school website by using windows server and its web server role as networking and internet student you are required to configure and host a school web server.

Indicative content 5.3: Implement Security Access Control

Duration: 3 hrs

Theoretical Activity 5.3.1: Description of security access control concepts

Tasks:

1: Answer the following questions:

i. SSL stand for?
ii. Differentiate antimalware from the antivirus
iii. Explain mechanism of create uncrackable password.
iv. Give any four benefits of performing regular backup.

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: read the key readings 5.3.1.

Key readings 5.3.1.: Description of security access control concepts

Implementing security access control in a web server is crucial for protecting sensitive data and ensuring that only authorized users can access specific resources. Here are key strategies and best practices for establishing effective access control:

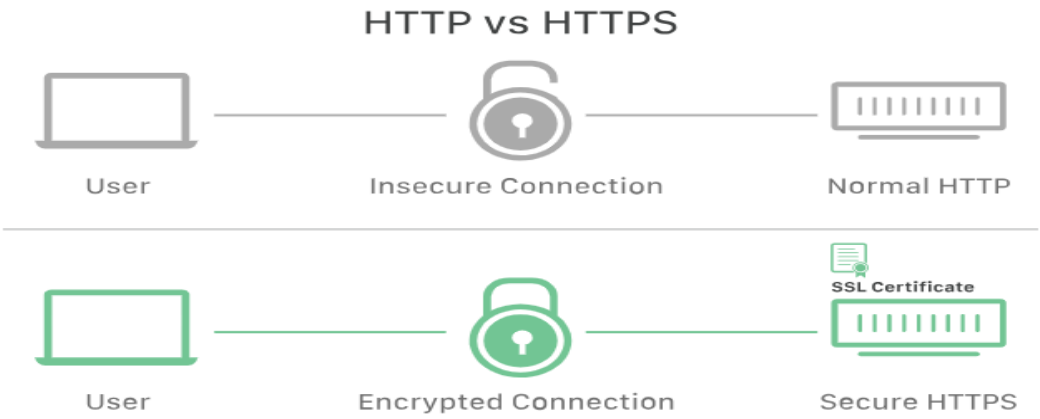
- **Key Concepts of Access Control**
  - **Authentication:** This is the process of verifying the identity of a user. Common methods include usernames and passwords, multi-factor authentication (MFA), and client certificates.
  - **Authorization:** After authentication, authorization determines what actions a user can perform. This is typically managed through roles and permissions.
  - **Access Control Models:**
    - **Role-Based Access Control (RBAC):** Users are assigned roles that dictate their permissions.
    - **Access Control Lists (ACLs):** Specific permissions are defined for users or groups for particular resources.
    - **Attribute-Based Access Control (ABAC**): Access is granted based on user attributes and environmental conditions.

1.1. SSL/TLS

SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are essential protocols for securing communications over the internet.

SSL is a security protocol that creates an encrypted link between a web server and

a browser, ensuring that all data transmitted remains private and integral. TLS is the updated version of SSL, designed to address vulnerabilities found in earlier SSL versions. Although SSL is largely deprecated, the term is still commonly used to refer to both protocols collectively.



Types of SSL certificates

- **Single-domain:** A single-domain SSL certificate applies to only one domain (a "domain" is the name of a website, like www.cloudflare.com).
- **Wildcard:** Like a single-domain certificate, a wildcard SSL certificate applies to only one domain. However, it also includes that domain's subdomains. For example, a wildcard certificate could cover www.cloudflare.com, blog.cloudflare.com, and developers.cloudflare.com, while a single-domain certificate could only cover the first.
- **Multi-domain:** As the name indicates, multi-domain SSL certificates can apply to multiple unrelated domains.

2. Make password uncrackable

To make passwords uncrackable in a web server implementation, it's essential to follow a comprehensive approach that includes strong password policies, secure storage practices, and additional security measures. Creating an uncrackable password is a challenging task, as no password can be entirely immune to cracking attempts. However, you can significantly enhance the strength and security of your passwords by following best practices.

2.1. Enforce Strong Password Policies

➢ **Password Complexity Requirements**

- Minimum Length: Require a minimum password length of at least 12-16 characters.
- Character Variety: Mandate the use of:
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (e.g., !, @, #, $, %, ^, &, *)

2.2. Password Creation Guidelines

Encourage users to create passphrases that combine unrelated words or phrases. Prohibit the use of easily guessable information such as names, birthdays, or common words.

Example Policy, Password must be at least 16 characters long and include:

- ✓ At least one uppercase letter
- ✓ At least one lowercase letter
- ✓ At least one number
- ✓ At least one special character

2.3. Implement Secure Password Storage

➢ Hashing Passwords: Use a strong hashing algorithm to store passwords securely. Recommended algorithms include bcrypt, Argon2, PBKDF2.

➢ Salting Passwords: Always add a unique salt to each password before hashing. This ensures that even identical passwords will produce different hashes.

Example Implementation (using bcrypt in Python)

```
import bcrypt
# Hashing a password
password = b"UserPassword123!"
salt = bcrypt.gensalt()
hashed_password = bcrypt.hashpw(password, salt)
# Verifying a password
def verify_password(stored_hash, user_password):
return bcrypt.checkpw(user_password.encode('utf-8'), stored_hash)
```

2.4. Enable Two-Factor Authentication (2FA)

➢ Adding an Extra Layer of Security: Implement 2FA to require users to provide a second form of verification, such as a code sent to their mobile device or generated by an authenticator app.

➢ **Implementation Steps:**

1. Choose a 2FA method (SMS, authenticator app, etc.).
2. Integrate a library or service that supports 2FA (e.g., Google Authenticator, Authy).
3. Update user accounts to allow for 2FA enrollment and verification.

➢ **Logging and Monitoring**

- Implement logging to track login attempts and access to sensitive areas of your application.
- Regularly review logs for suspicious activity, such as multiple failed login attempts.

➢ **Account Lockout Policy:** Implement an account lockout mechanism after a certain number of failed login attempts to prevent brute-force attacks.

➢ **Educate Users**

User Awareness Training: Provide guidance to users on creating strong passwords

and recognizing phishing attempts. Encourage the use of password managers to help users manage their passwords securely.

By implementing these strategies, you can significantly enhance the security of passwords in your web server environment, making them much harder to crack. Strong password policies, secure storage practices, two-factor authentication, and user education are essential components of a robust security framework that protects against unauthorized access.

3.Update Your Website

Keeping your website and its components up to date is crucial for security. Updates often include patches for vulnerabilities that could be exploited by attackers.

3.1. Update Your Website

a. Update Content Management System (CMS): If you're using a CMS (like WordPress, Joomla, or Drupal), regularly check for updates. Enable automatic updates if available, or set a schedule to check for updates manually.

b. Update Plugins and Themes: Regularly update all plugins and themes to their latest versions. Remove any unused or outdated plugins and themes to minimize potential vulnerabilities.

c. Update Server Software: Ensure that your web server software (e.g., Apache, Nginx) and database systems (e.g., MySQL, PostgreSQL) are up to date. Regularly check for updates to your programming languages and frameworks (e.g., PHP, Node.js).

d. Monitor Security Advisories: Subscribe to security advisories relevant to your CMS and any third-party libraries you use. This will help you stay informed about vulnerabilities and patches.

Example Update Process

1. Backup Your Website: Before making any updates, create a complete backup of your website.

2. Check for Updates: Log in to your CMS and check for available updates.

3. Apply Updates: Update the CMS, plugins, themes, and server software.

4. Test the Website: After updates, thoroughly test your website to ensure that everything functions correctly.

4. Do Regular Backups

Regular backups ensure that you can restore your website in case of data loss due to hacking, server failure, or accidental deletion.

4.1. Steps to Implement Regular Backups:

a. Choose a Backup Solution

- Select a backup solution that fits your needs. Options include:
- **Manual Backups**: Use FTP/SFTP to download files and export databases.
- **Automated Backup Plugins**: If using a CMS, consider plugins like UpdraftPlus

(WordPress) or Akeeba Backup (Joomla).

- **Server-Side Backups**: Use server management tools (like cPanel or Plesk) to schedule backups.

b. Define a Backup Schedule: Set a regular backup schedule based on how often your website content changes. For dynamic sites, daily or weekly backups are recommended.

c. Store Backups Securely

Store backups in multiple locations to ensure redundancy. Options include: Local storage (external hard drives), Cloud storage (Google Drive, Dropbox, AWS S3), Offsite storage for disaster recovery.

d. Test Backup Restoration: Regularly test your backup restoration process to ensure that you can successfully restore your website from backups when needed.

Example Backup Process:

1. Select Backup Tool: Choose a backup tool that meets your needs.

2. Schedule Backups: Set up automated backups to run daily or weekly.

3. Store Backups: Save backups to both local and cloud storage.

4. Verify Backups: Periodically check the integrity of your backups and perform test restorations.

Implementing security access control through regular website updates and backups is essential for protecting your web server from vulnerabilities and data loss. By following these practices, you can significantly enhance your website's security posture and ensure that you are prepared for any potential incidents. Regular updates keep your software secure, while consistent backups provide a safety net in case of emergencies.

Practical Activity 5.3.2: Perform security access control

Task:

1: Referring to the key reading 5.3.1, As a network administrator, you are asked to go to the computer lab, to perform the following: after configure web server in your windows server, install and configure SSL as security mechanism.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 5.3.2 and ask clarification where necessary

5: Perform the task provided in application of learning 5.3.2

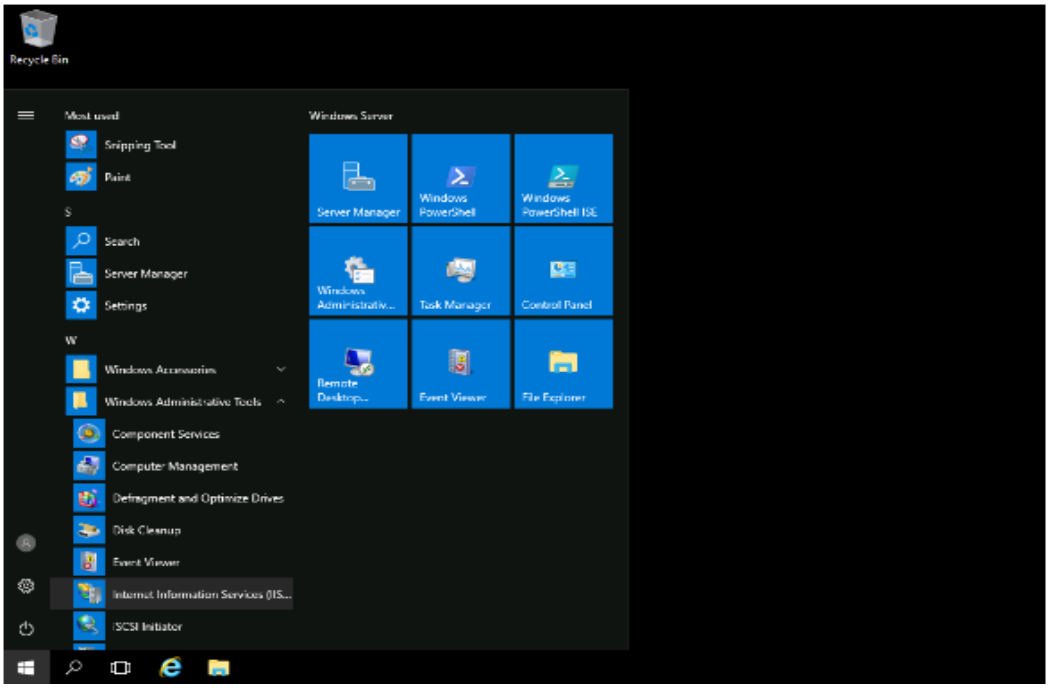
Key readings 5.3.2 Perform security access control

1.Create Certificate Signing Request Using IIS

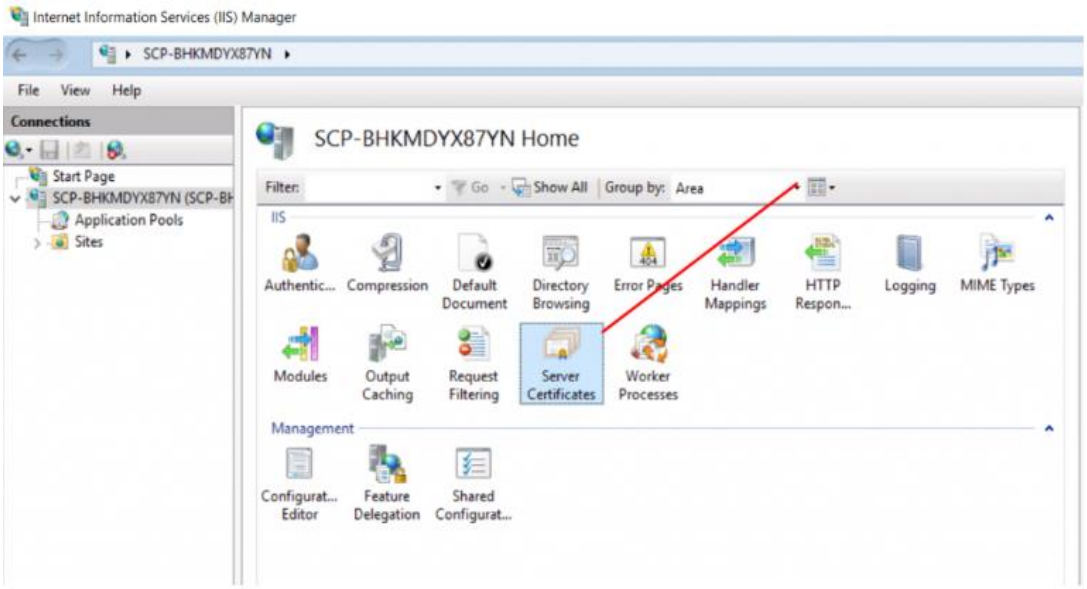
When you are applying or ordering an SSL certificate, you will need to create CSR (Certificate Signing Request) on your server and send it to a Certificate Authority. The CSR validates the information the CA requires to issue a certificate. After validating the CSR, the Certificate Authority will use this data to generate and issue the SSL certificate.

create a CSR by following the below steps:

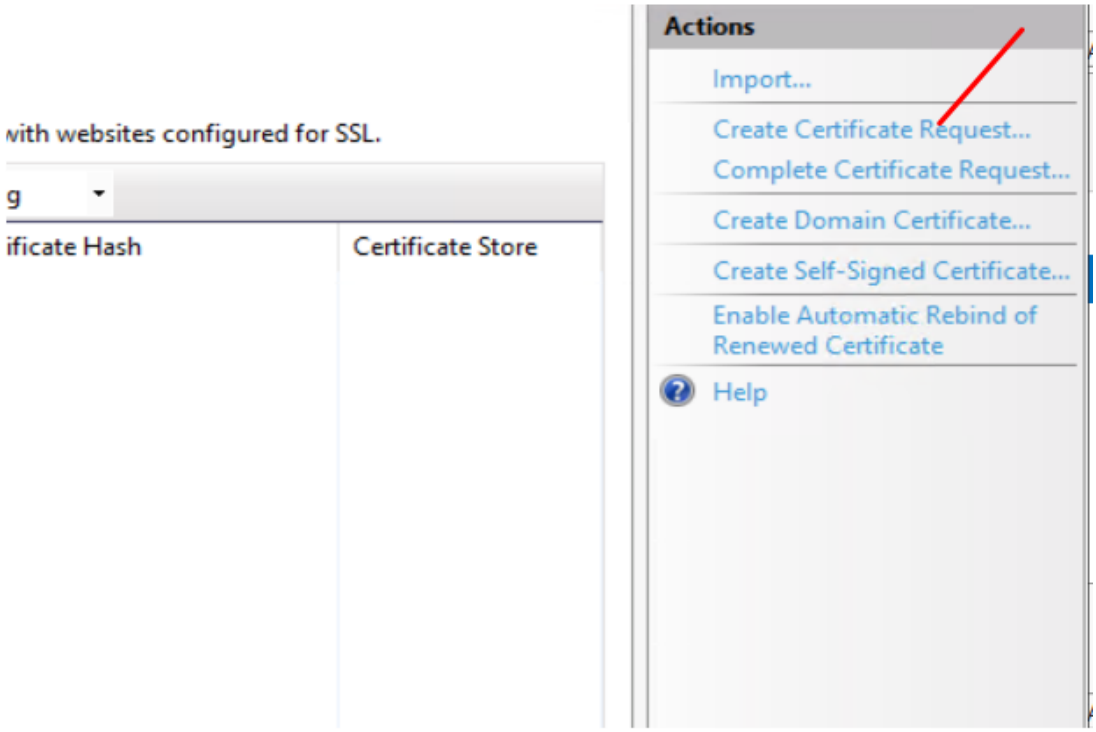
Step 1: Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**, as shown below:



Step 2: In the left pane, click on the **server's name** and double click on the **Server Certificates**. You should see the following page:



Step 3: In the right pane, click on the **Create Certificate Request**. You should see the following page:



Step 4: Provide your domain name, company name, department name, city, state, country name and click on the **Next** button. You should see the following page:

At this point, you will be asked for information about the certificate and the company requesting the certificate.

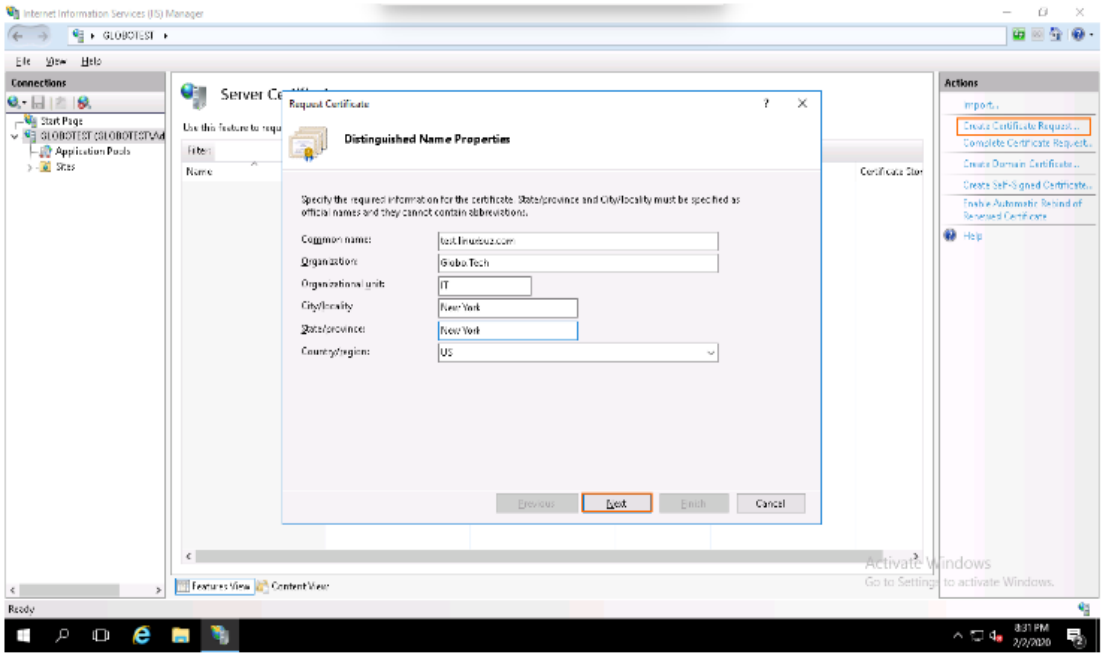
Once you have filled this out, click Next.

It will bring you to the following screen

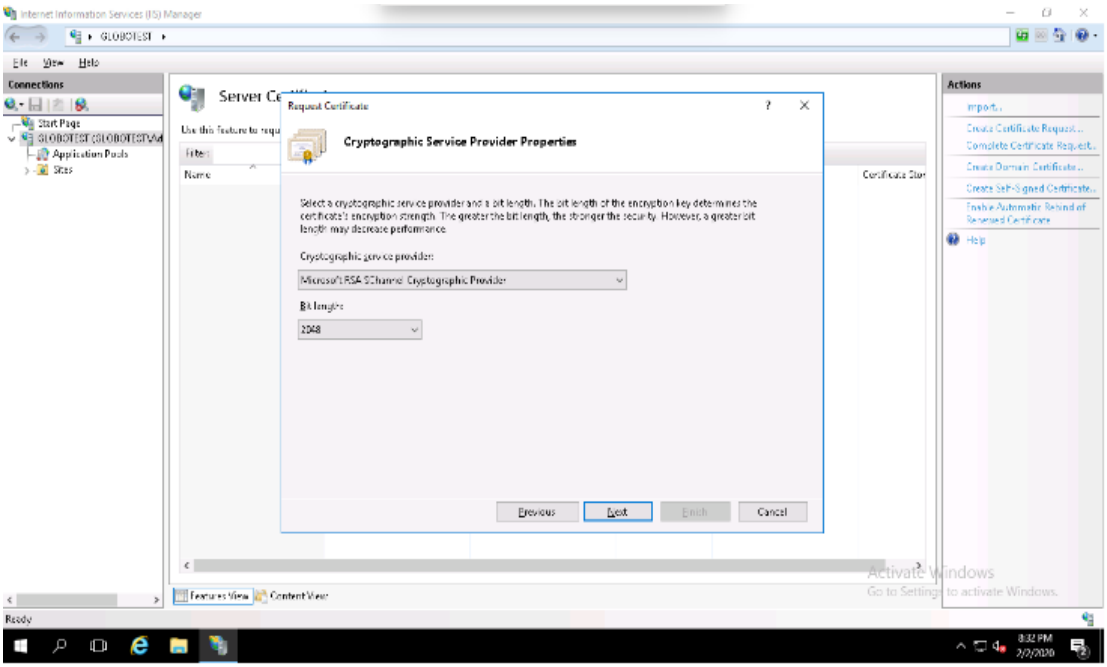
Common Name	Your domain name, this should be **www.example.com** or ***.example.com** if you are ordering a wildcard.
Organization	Your company's legal name, including any suffixes.
Organizational *Unit*	The department handling the certificate, this is usually IT.
City, State, Country	Should match the information where your company is located.

On the subsequent screen, you need to specify a filename where your Certificate Request or CSR can be exported.

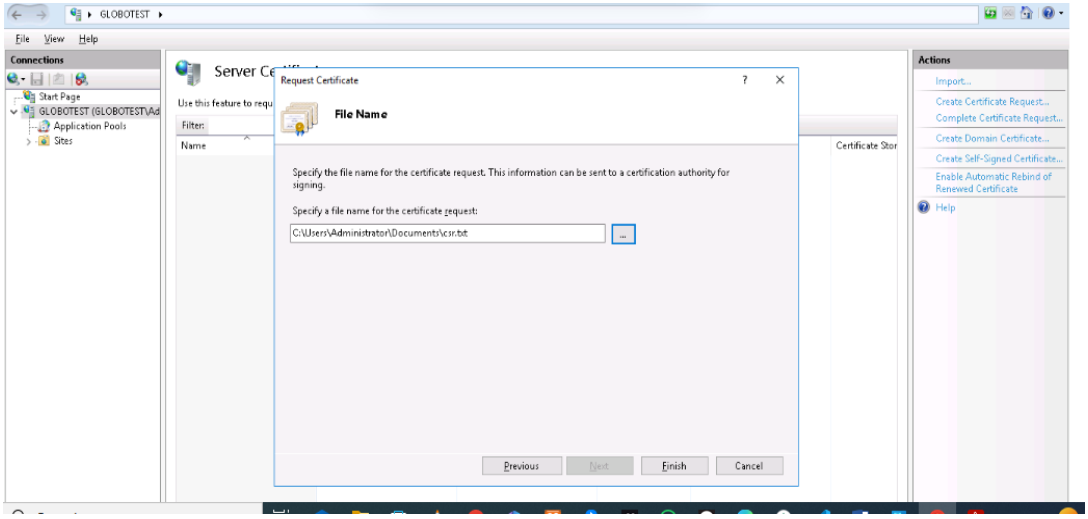
For example: we would like to export the CSR to *C:\example.com.csr.txt*



Step 5: Select the Cryptographic Service Provider, 2048 as a bit length and click on the **Next** button. You should see the following page:



Step 6: Specify the filename and the location where you want to save the CSR, and click on the **Finish** button to create a CSR certificate.



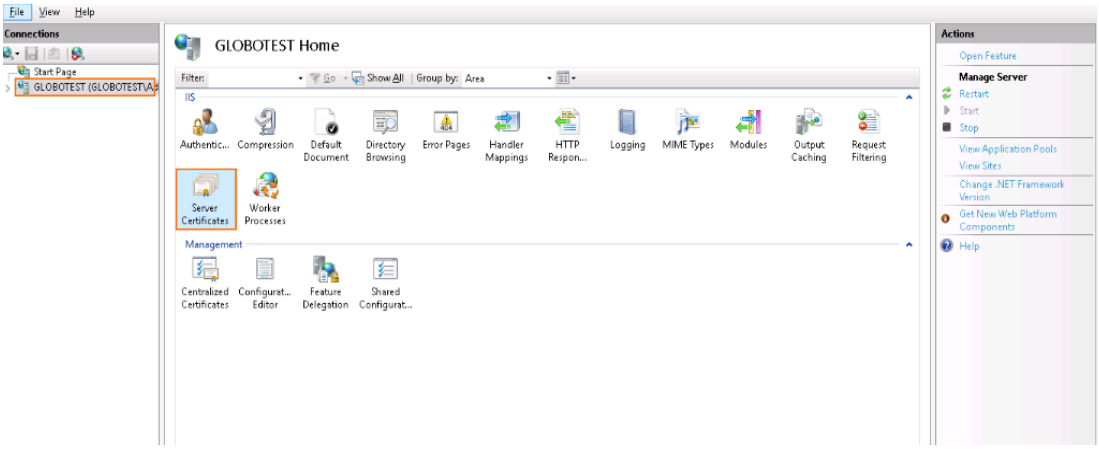
Step 7: After generating the CSR, you will need to give this CSR file to the Certificate Provider in order to purchase the new SSL certificate.

Make sure that you get an SSL certificate in P7B or CER format. Once you received the SSL certificate file from the Certificate Authority save it on the server where you created the CSR

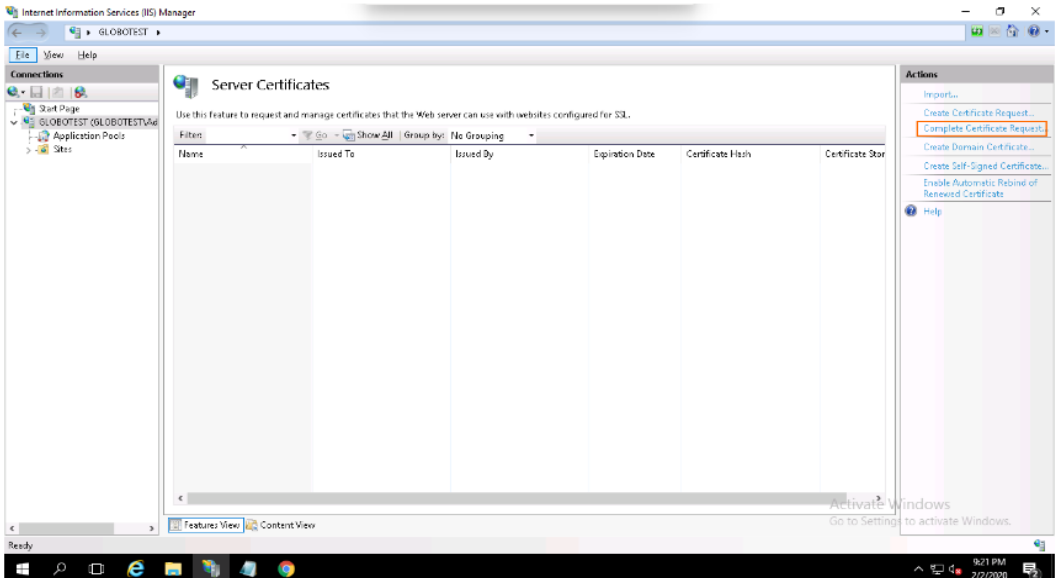
1.2. Install the SSL on IIS Website

Next, you will need to install the SSL certificate on your IIS website. You can install it by following the below steps:

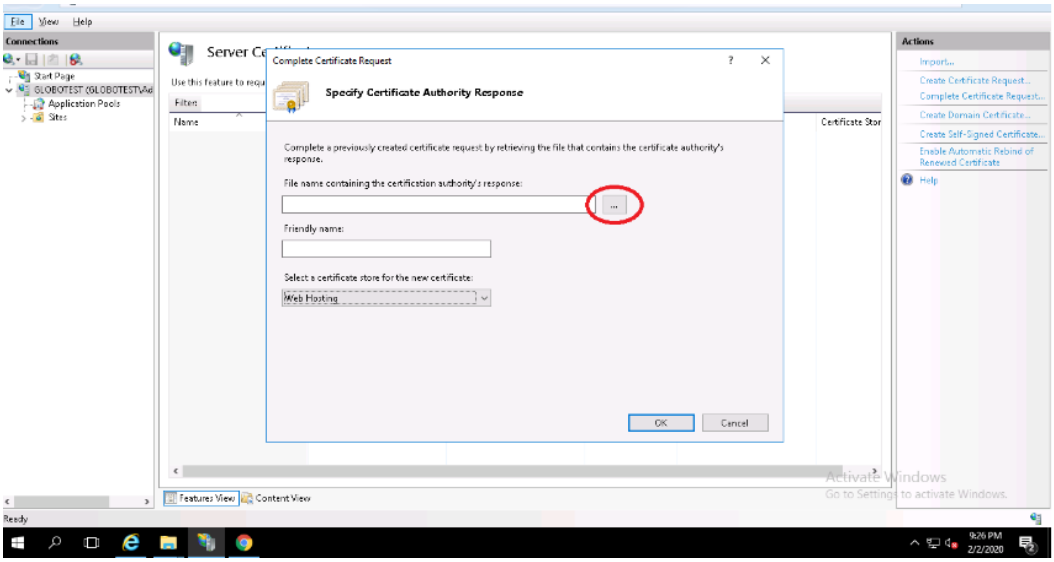
Step 1: Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager** as shown below



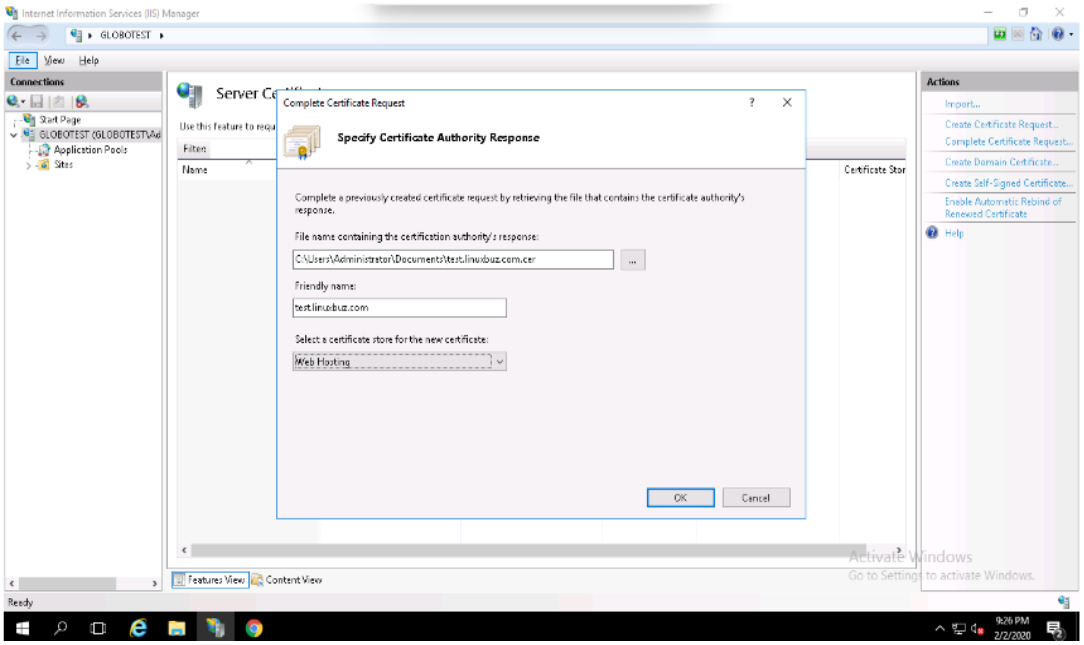
Step 2: In the left pane, click on the server's name and double click on the **Server Certificates**. You should see the following page:



Step 3: In the right pane, click on **Complete Certificate Request**. You should see the following page:



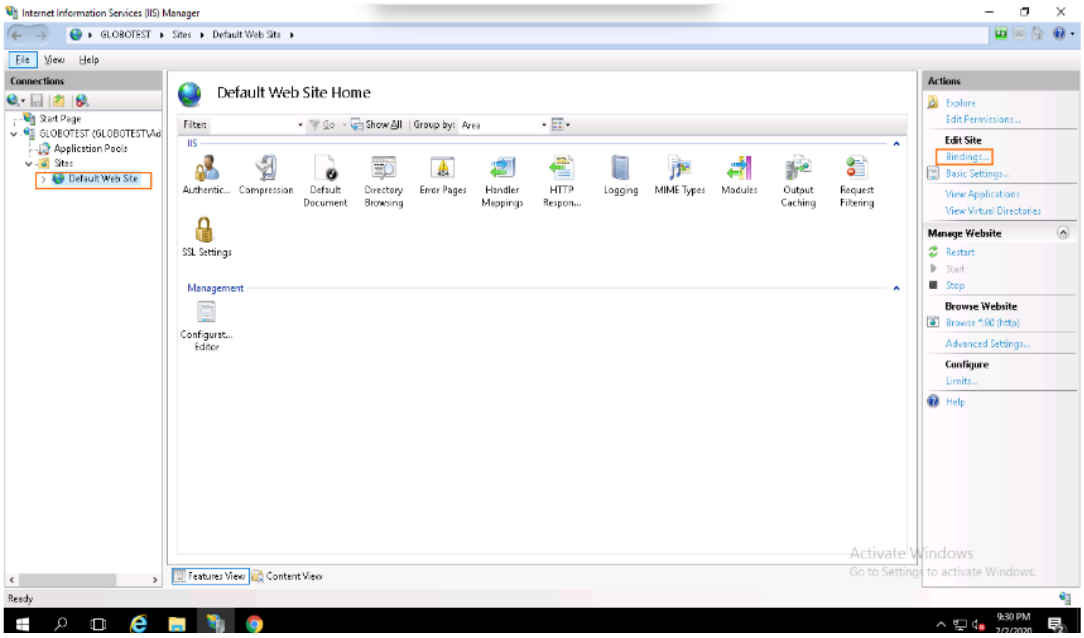
Step 4: Browse the certificate file (.cer), provide your domain name, select Web Hosting in the certificate store option and click on the **OK** button.



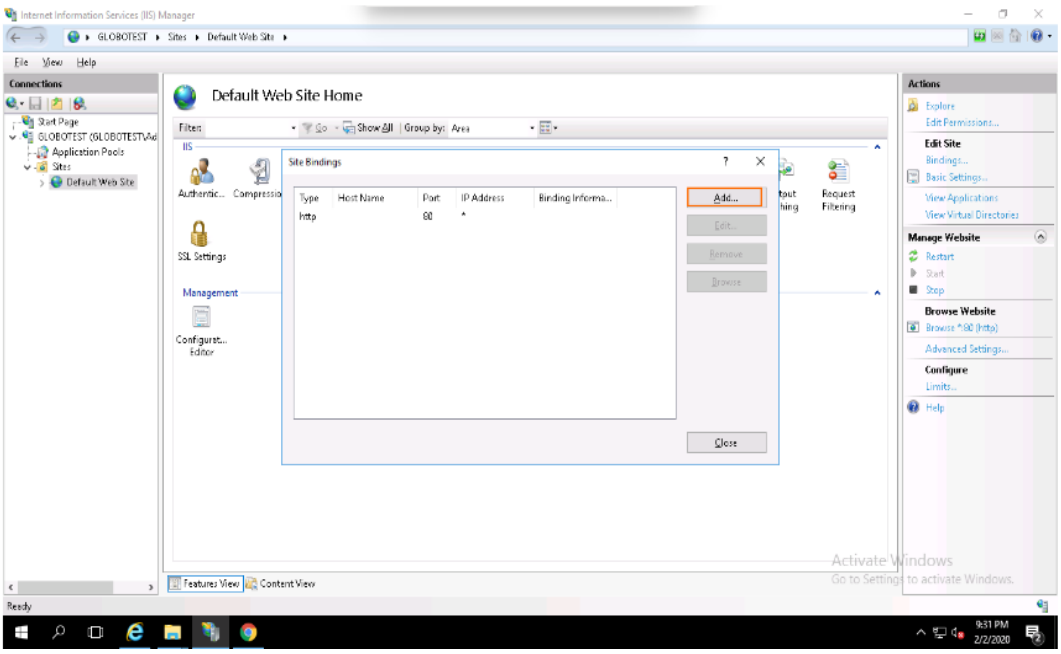
At this point, you have successfully installed your SSL certificate. Next, you will need to assign the certificate to your website.

2.To assign the certificate by following the below steps:

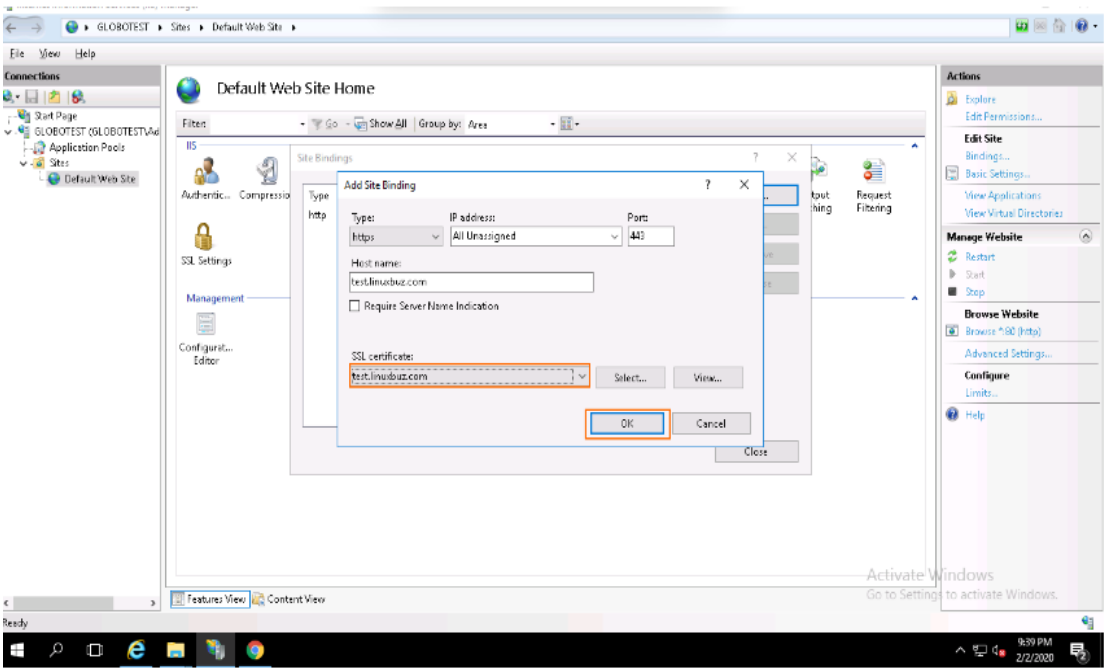
Step 1: Open the IIS Manager, expand the server's name and click on the Default Website then click on the **Bindings** in the right pane. You should see the following page



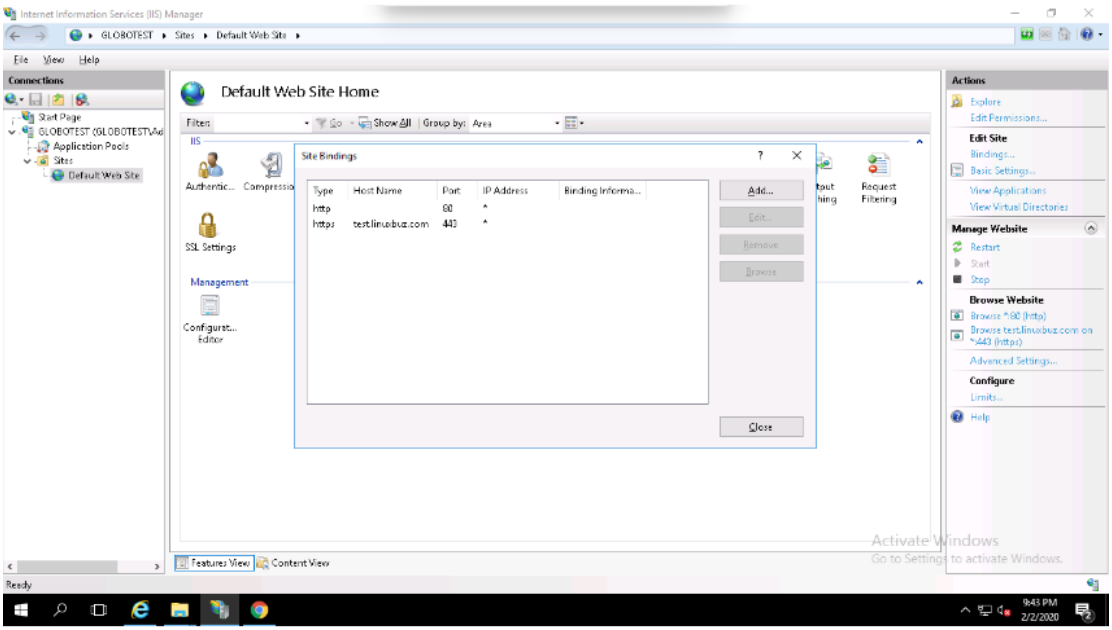
Step 2: Click on the **Add** button. You should see the following page:



Step 3: Select https, select the IP address of your website or leave it unassigned, type port 443, type your domain name, select the domain name on which you want to install SSL and click on the **OK** button to install the certificate.



Your SSL certificate is now installed and the website configured to accept secure connections as shown below:



3.Installation of Anti-viruses' software on windows server

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

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

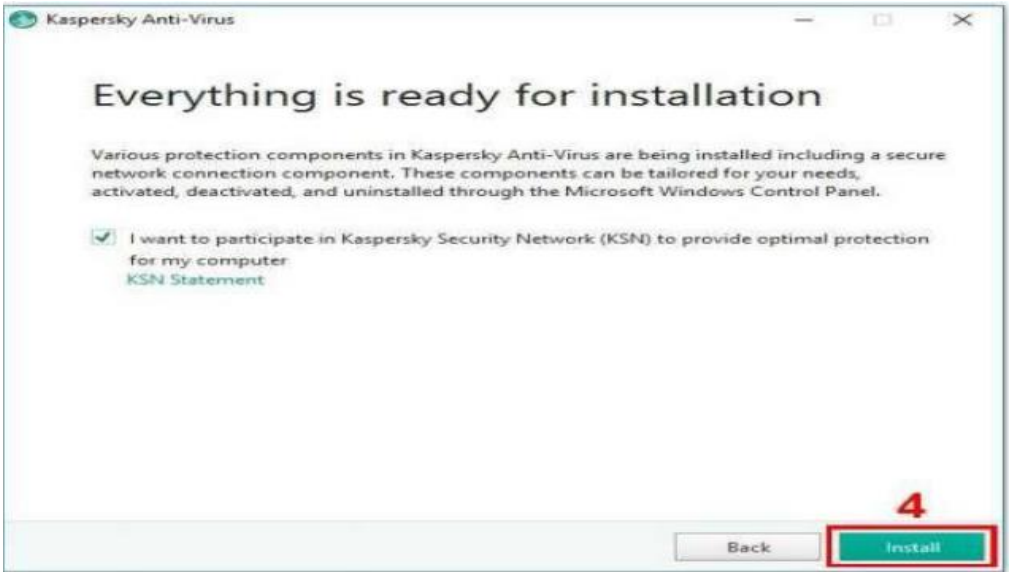
How to install Kaspersky Anti-Virus 2023

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

1. Click Run

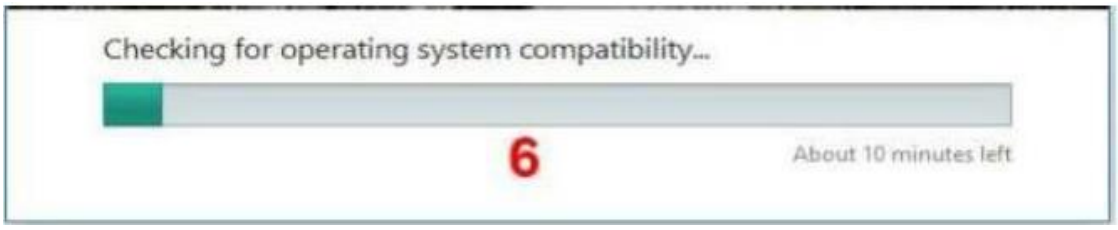
2. Click continue

3. Click Install

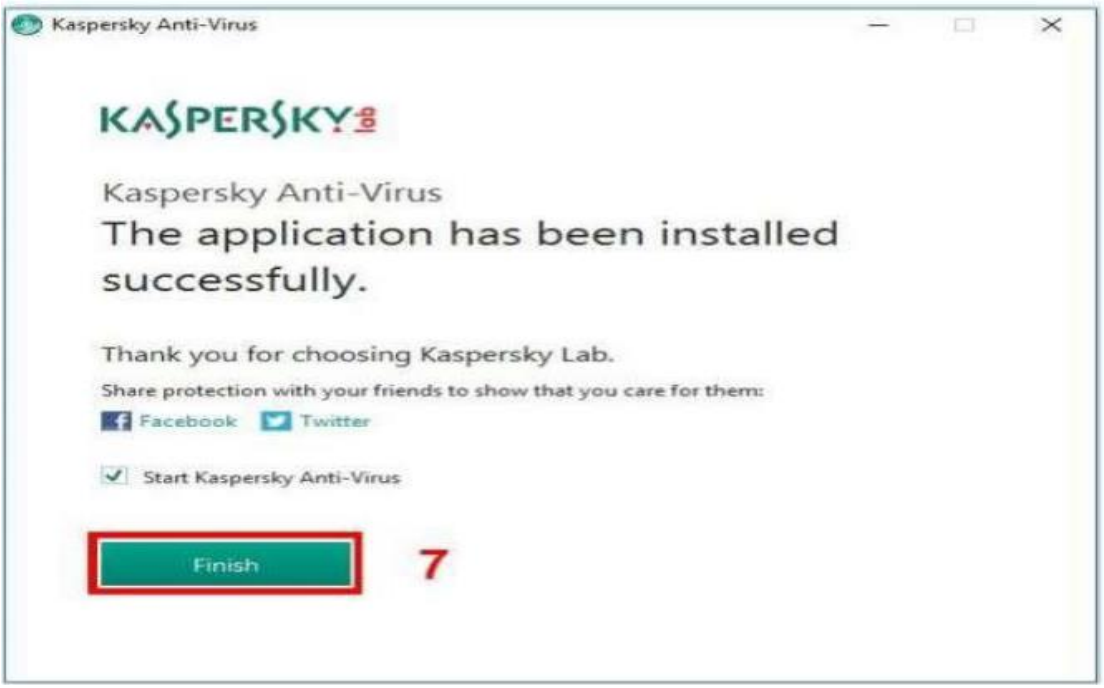


4. If you are installing the application under Windows server 2008, or Windows server 2012, you may see a notification from the User Account Control (UAC) service after you click the Install button. To proceed with the installation, enter your administrative password and click Yes.in the User account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

5. Wait for the installation to complete



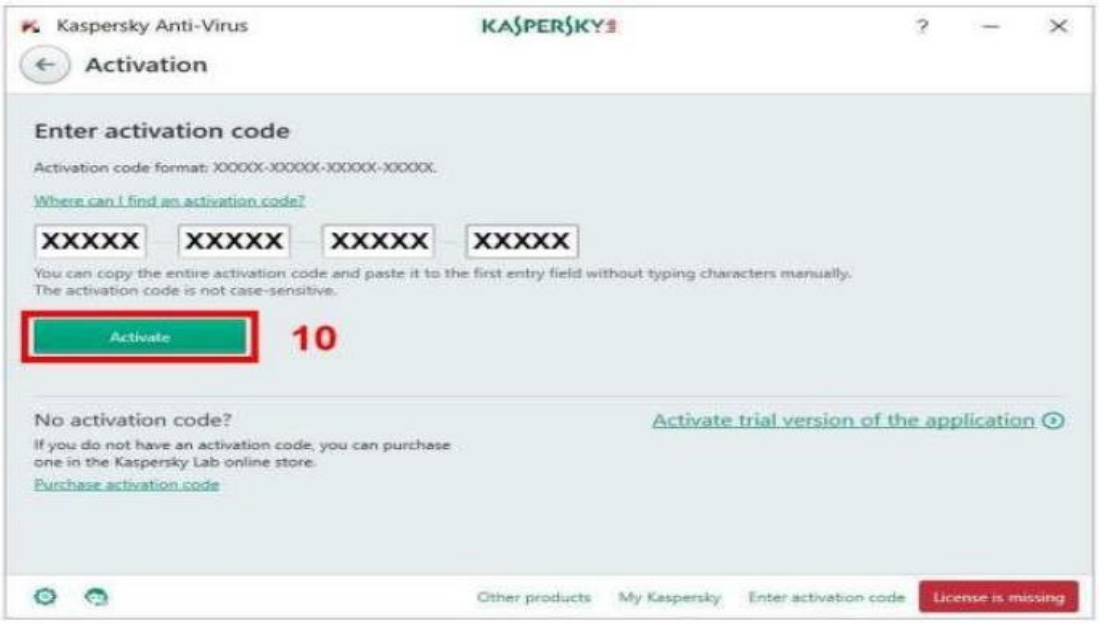
6. Make sure that the check box Run Kaspersky Anti-Virus is selected and click the Finish button to complete the installation.



7. Wait for loading the application

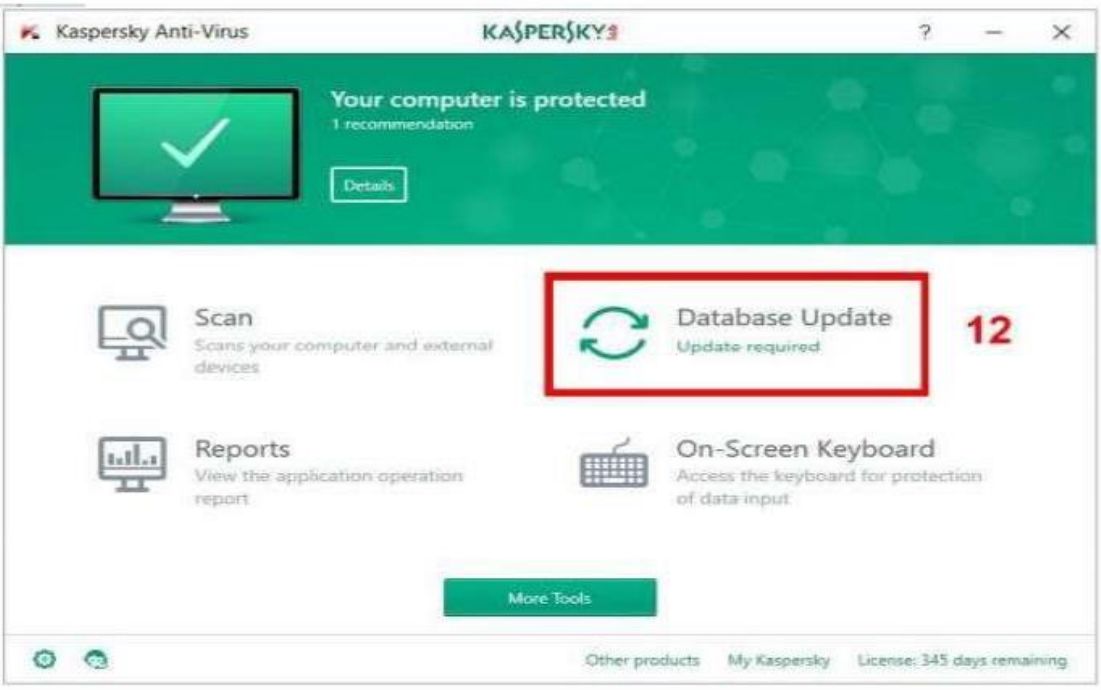
8. You can take a tour through the app features by clicking continue. Or Skip it.

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



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

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



Updating Antivirus in an Industrial Control System

When properly deployed and up-to-date, antivirus software is an important part of a defense in-depth strategy to guard against malicious software (malware) in industrial control systems (ICS)1.

Points to Remember

- **Install the SSL on IIS Website**

  step 1: Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**

  Step 2: In the left pane, click on the server's name and double click on the **Server Certificates**.

  Step 3: In the right pane, click on **Complete Certificate Request**.

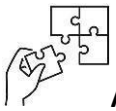
  Step 4: Browse the certificate file (.cer), provide your domain name, select Web Hosting in the certificate store option and click on the **OK** button.

- **To assign the certificate by following the below steps**

  Step 1: Open the IIS Manager, expand the server's name and click on the Default Website then click on the **Bindings** in the right pane.

  Step 2: Click on the **Add** button. You should see the following page:

  Step 3: Select https, select the IP address of your website or leave it unassigned, type port 443, type your domain name, select the domain name on which you want to install SSL and click on the **OK** button to install the certificate.



Application of learning 5.3.

Refer to the configuration made on application of learning 5.3 establish web server security feature by configure and enabling SSL certificate.

Indicative content 5.4: Deploy Web Application

Duration: 2 hrs

Theoretical Activity 5.4.1: Description of deployment method

Tasks:

1: Answer the following questions:

i. What do you understand by the following terms:
   a) Deployment
   b) Version control system
   c) containerization

ii. Explain manual deployment?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 5.4.1

Key readings 5.4.1.: Description of deployment method

1.Description of deployment Method

1.1. Manual Deployment

Manual deployment involves hands-on involvement of IT teams in every step of the deployment process. It requires human intervention to provision infrastructure, configure settings, and install software. While manual deployment provides flexibility, it is often time-consuming, error-prone, and lacks consistency across environments.

1.2. Version Control

Version control systems track changes to code over time, allowing multiple developers to collaborate on a project. Popular version control tools include Git, Subversion, and Mercurial. Using version control enables features like branching, merging, and rollbacks, which are essential for managing application deployments.

1.3. Containerization

Containerization packages an application's code, runtime, system tools and libraries into a single package called a container. Containers provide a consistent, isolated environment for running applications. Docker is the most widely used containerization platform. Containerized applications can be easily deployed across different environments, improving portability and scalability.

2. Testing the Deployment

Once your web application has been deployed, it’s crucial to conduct thorough

testing to ensure everything is functioning as expected. Here's a structured approach to testing your deployment:

1. Smoke Testing: To verify that the most critical functionalities of the application are working.

Steps:

- ✓ Access the application in a web browser.
- ✓ Check the homepage and key pages for loading issues.
- ✓ Test core functionalities such as user login, form submissions, and navigation links.

Example: **http://www.mynewsite.com.**

-**Outcome**: Confirm that the application is up and running without any critical errors.

2. Functional Testing: To ensure that all features work according to the requirements.

Steps:

- ✓ Execute test cases for each feature of the application.
- ✓ Validate inputs, outputs, and user interactions.
- ✓ Test edge cases and error handling scenarios.

Outcome: Verify that all functionalities meet the specified requirements and behave as expected.

3. Performance Testing: To assess the application's performance under various conditions.

Steps:

- Use tools like JMeter, LoadRunner, or Gatling to simulate user load.
- Measure response times, throughput, and resource utilization.
- Test under peak load conditions to identify bottlenecks.
- **Outcome**: Ensure the application can handle expected traffic and performs well under stress.

4. Security Testing: To identify vulnerabilities and ensure the application is secure.

Steps:

- Conduct penetration testing to find security weaknesses.
- Check for common vulnerabilities such as SQL injection, XSS, and CSRF.
- Review authentication and authorization mechanisms.
- **Outcome**: Confirm that the application is secure and meets compliance standards.

5. User Acceptance Testing (UAT): To validate the application from the end-user perspective.

Steps:

- Involve real users to test the application in a production-like environment.
- Gather feedback on usability and functionality.
- Address any concerns or issues raised by users.
- **Outcome**: Ensure the application meets user expectations and is ready for full-scale use.

  6. Monitoring and Logging: To track the application's performance and identify issues post-deployment.

  Steps:
- Set up monitoring tools (e.g., New Relic, Datadog, or Google Analytics) to track application health.
- Implement logging to capture errors and user interactions.
- Regularly review logs and monitoring dashboards for anomalies.

Practical Activity 5.4.2: Preforming web application deployment

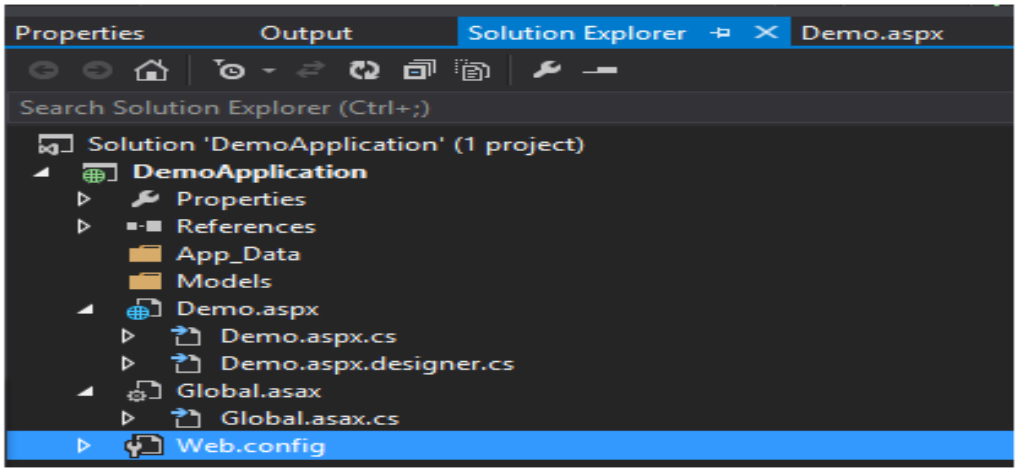
Task:

1: Referring to the key reading 5.4.1, As a server administrator, you are asked to go to the computer lab to perform the following: develop a web application and deploy it to the web server (IIS) by respecting all deployment steps.
2: Apply safety precautions
3: Present your work to the trainer and whole class.
4: Read key reading 5.4.2 and ask clarification where necessary
5: Perform the task provided in application of learning 5.4.2

Key readings 5.4.2: Preforming web application deployment

1.Step to deploy website in IIS via file copy

Step 1) Let's first ensure we have our web application 'DemoApplication' open in Visual Studio.



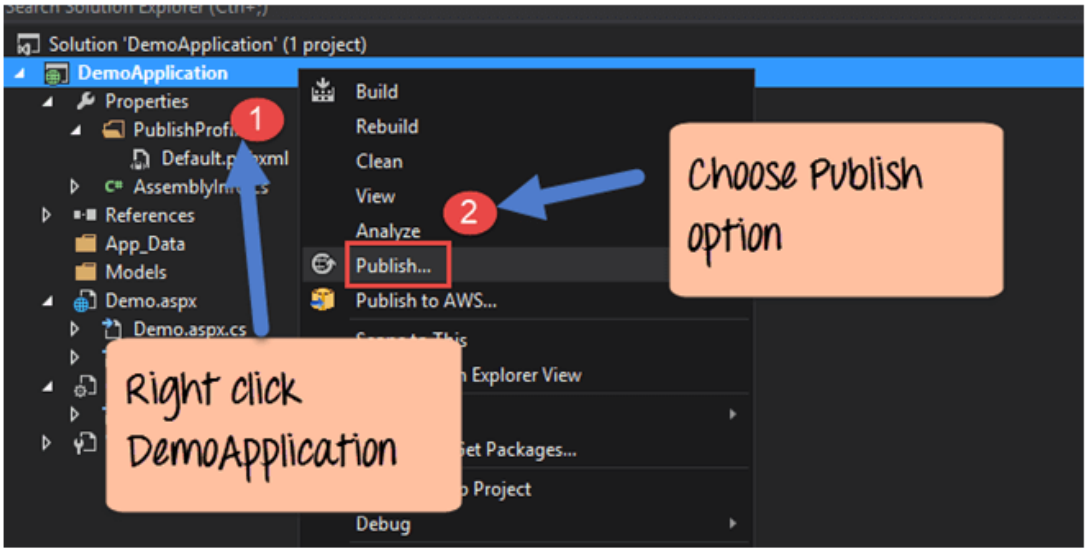
Step 2) Open the 'Demo.aspx' file and enter the string "hello.net."

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title></title>
</head>
                <body>
                    <form id="form1" runat="server">
                    <div>

                Guru 99 ASP.Net

                    </div>
                    </form>
                </body>
</html>
```

Display Text

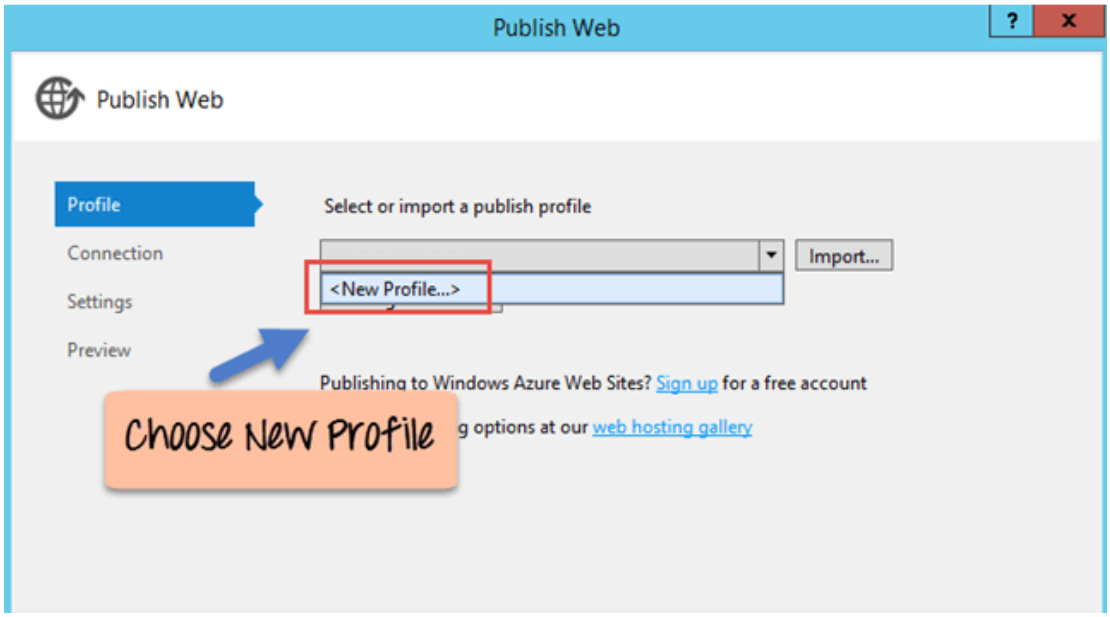
Step 3) Now it's time to publish the solution.

1. Right-click the 'DemoApplication' in the Solution Explorer
2. Choose the 'Publish' Option from the context menu.



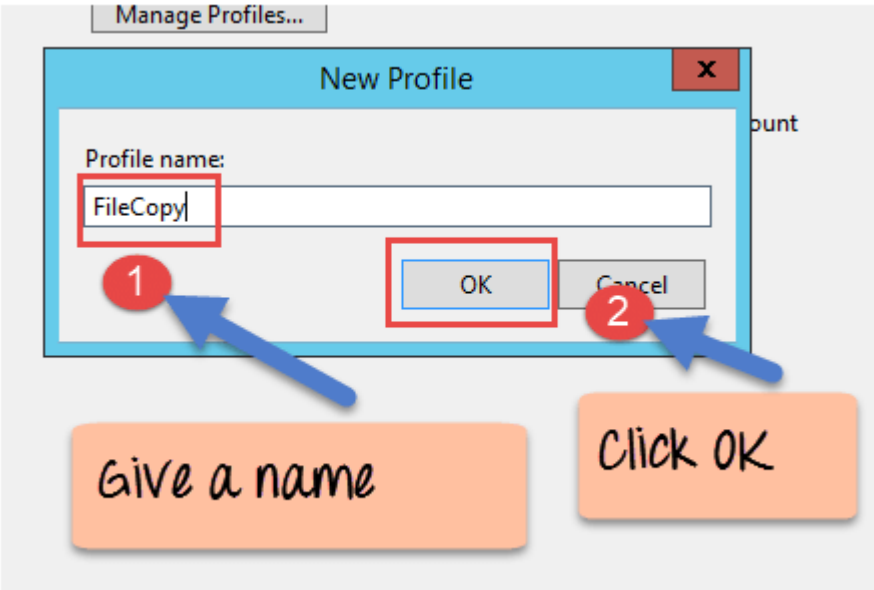
It will open another screen (see step below).

Step 4) In the next step, choose the 'New Profile' to create a new Publish profile. The publish profile will have the settings for publishing the web application via File copy.



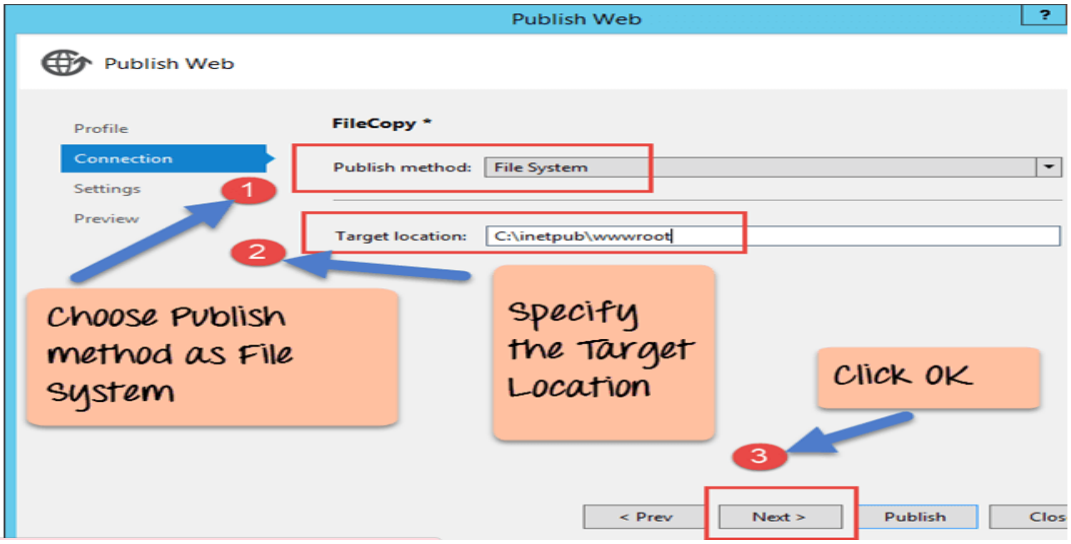
Step 5) In the next screen we have to provide the details of the profile.

1. Give a name for the profile such as FileCopy
2. Click the OK button to create the profile

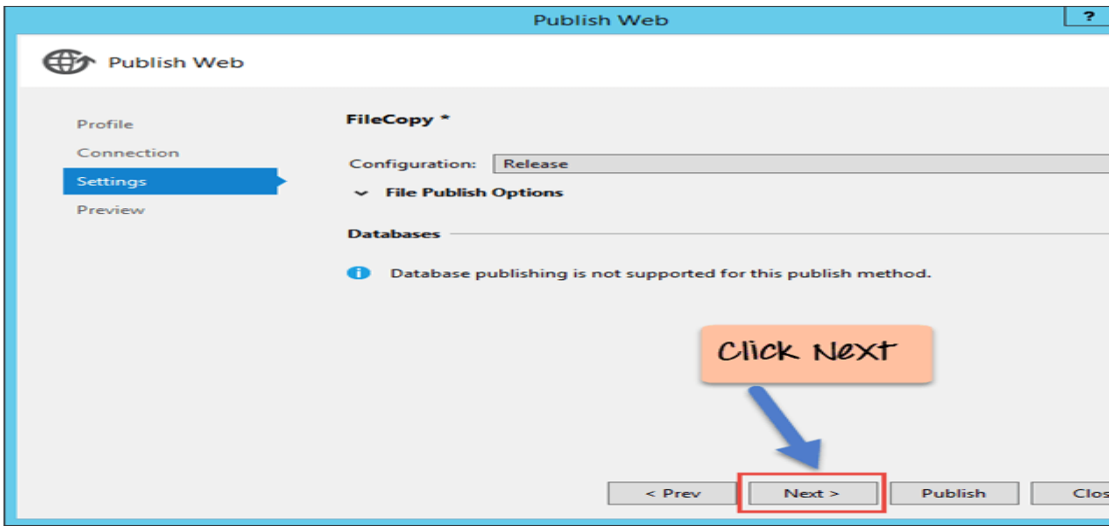


Step 6) In this step, we specifically mention that we are going to Publish website via File copy.

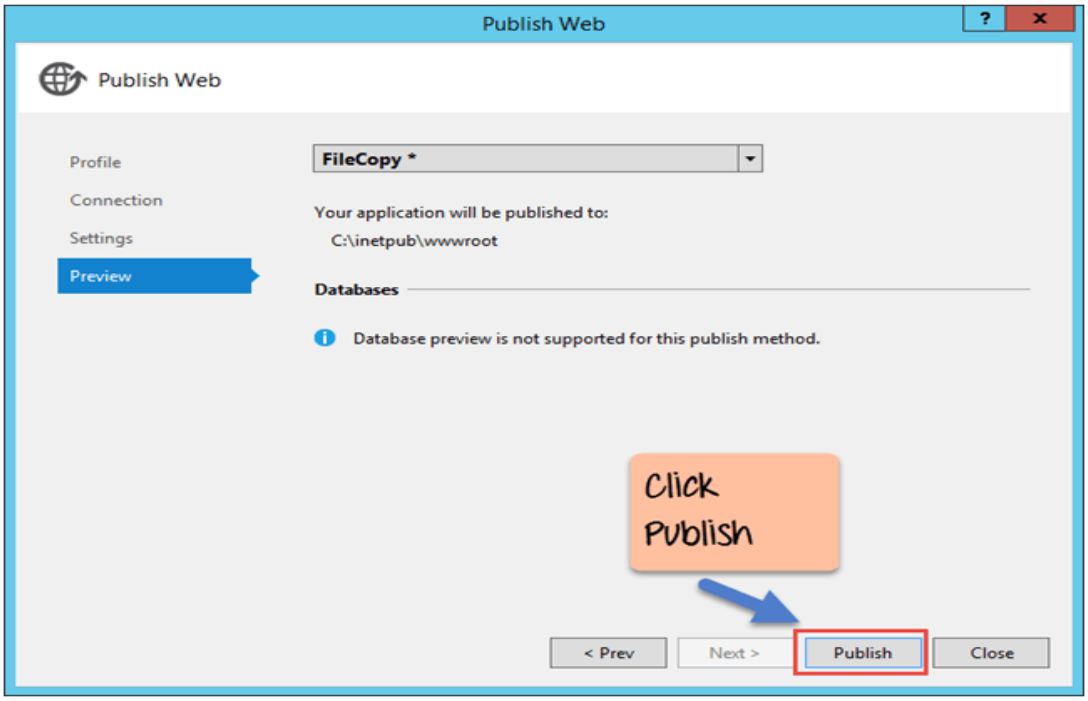
1. Choose the Publish method as File System.
2. Enter the target location as C:\inetpub\wwwroot – This is the standard file location for the Default Web site in IIS.
3. Click 'Next' button to proceed.



Step 7) In the next screen, click the Next button to proceed.



Step 8) Click the 'Publish' button in the final screen

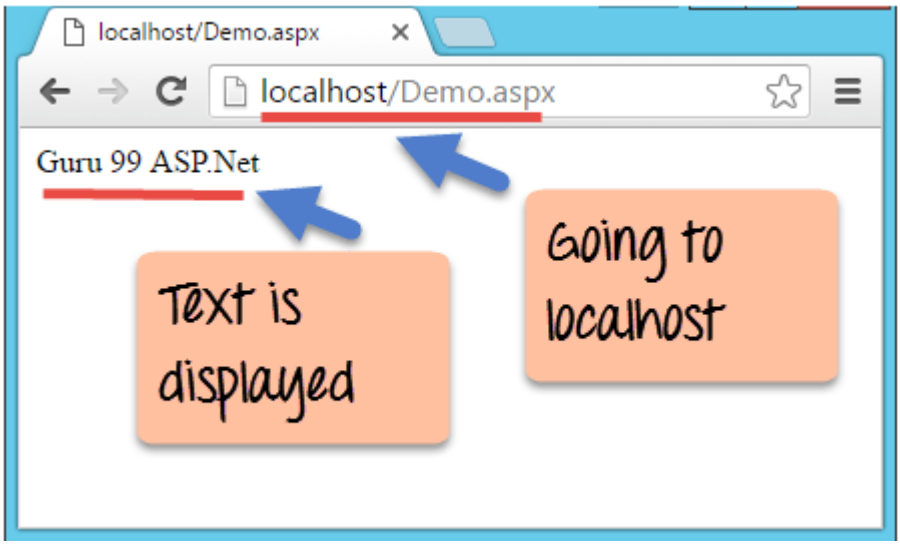


When all of the above steps are executed, you will get the following output in Visual Studio

Output:

From the output, you will see that the Publish succeeded.

Now just open the browser and go to the URL: http://localhost/Demo.aspx

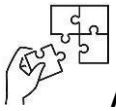


You can see from the output that now when you browse to **http://localhost/Demo.aspx**, the page appears. It also displays the text 'Guru 99 ASP.Net'.

Points to Remember

- Manual deployment involves hands-on involvement of IT teams in every step of the deployment process. It requires human intervention to provision infrastructure, configure settings, and install software.

- Version control systems track changes to code over time, allowing multiple developers to collaborate on a project. Popular version control tools include Git, Subversion, and Mercurial.
- Containerization packages an application's code, runtime, system tools and libraries into a single package called a container. Containers provide a consistent, isolated environment for running applications.
- **While deploying website in IIS via file copy, take into consideration the following steps:**
    1. Creation of web application
    2. Open your application into VS code
    3. Choose the 'Publish' Option from the context menu
    4. choose the 'New Profile' to create a new Publish profile.
    5. Provide the details of the profile.
    6. Choose plication method and the target location then next
    7. Click the Publish button in the final screen
    8. Test publication by browsing target URL:http://localhost/Demo.aspx place demo.sapx with your web application name



Application of learning 5.4

Suppose that your school needs to host web application, you are asked to deploy web application so that every classmate can access. All tools, materials and equipment will be provided by the school.

Indicative content 5.5: Test Web Application

Duration: 1 hr

Theoretical Activity 5.5.1: Identification of web application tools

Tasks:

1: Answer the following questions:

i. What do you understand by the following terms:

a) Monitoring tools

b) Maintenance tools

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 5.5.1

Key readings 5.5.1.: Identification of web application tools

1. Web application tools

Testing web applications on Windows Server involves a structured approach that includes monitoring, maintenance, security, performance, scalability, and documentation. Below is a detailed overview of each aspect.

1.1 . Monitoring Tools

Effective monitoring tools are essential for tracking the performance and health of web applications hosted on Windows Server. Key tools include:

1.2. Microsoft Test Base: Allows validation of applications against Windows Server 2016 and 2019. It supports uploading application packages for testing against security updates and provides insights into test results.

1.3. Application Insights: A part of Azure Monitor, it offers real-time monitoring and analytics for web applications, helping to identify performance issues and user behavior.

1.4. Nagios: An open-source tool that provides comprehensive monitoring of server resources, applications, and services.

2. Maintenance Tools

Maintenance tools facilitate the ongoing support and management of web applications:

- ✓ **Web Deploy**: This tool simplifies the deployment process of web applications to Windows Server. It supports automated deployment and configuration management.
- ✓ **IIS Manager:** Integrated with Windows Server, it allows administrators to manage web applications easily, configure settings, and monitor application

health.

- ✓ **SQL Server Management Studio (SSMS):** Essential for managing databases that support web applications, enabling backups, performance tuning, and query optimization.

2.3. Security

Security is critical in protecting web applications from vulnerabilities:

- ✓ **OWASP ZAP**: An open-source security scanner designed to find vulnerabilities in web applications. It integrates well with CI/CD pipelines for continuous security testing.
- ✓ **Nessus:** A widely used vulnerability assessment tool that identifies potential security flaws in web applications running on Windows Server.
- ✓ **Burp Suite**: A comprehensive platform for web application security testing that provides tools for scanning, crawling, and exploiting vulnerabilities.

2.4. Performance

To ensure optimal performance of web applications:

- ✓ **Apache JMeter**: A powerful tool for load testing that simulates heavy traffic to assess how the application behaves under stress. It supports various protocols including HTTP and HTTPS.
- ✓ **Microsoft Playwright**: This framework enables automated testing of web applications across different browsers, ensuring they perform well under various conditions.
- ✓ **New Relic:** Provides real-time performance monitoring and analytics to help identify bottlenecks in web applications.

2.5. Scalability

Scalability tools help ensure that web applications can handle increased loads:

- ✓ **LoadRunner:** A performance testing tool that simulates thousands of users to evaluate how the application scales under load.
- ✓ **Azure Load Testing**: A cloud-based service that helps test the scalability of applications by simulating user traffic from various locations.
- ✓ **Kubernetes on Windows Server:** For containerized applications, Kubernetes can manage scaling automatically based on demand.

2.6. Documentation

Comprehensive documentation is vital for maintaining clarity in processes:

- ✓ **Confluence or SharePoint:** These platforms provide collaborative documentation solutions where teams can create and share knowledge about application configurations, deployment processes, and troubleshooting guides.
- ✓ **Markdown or Wiki-based systems:** Lightweight documentation tools can be used to maintain logs of changes and updates made to web applications.

Points to Remember

- Effective monitoring tools are essential for tracking the performance and health of web applications hosted on Windows Server. Key tools include:
  - ✓ Microsoft Test Base.
  - ✓ Application Insights
  - ✓ Nagios
- Maintenance Tools: facilitate the ongoing support and management of web applications. These tools include Web Deploy, IIS Manager, SQL Server Management Studio (SSMS).

Learning Outcome 5 end Assessment

Written assessment

Multiple choice question: Circle the letter corresponding to the correct answer:

1. During IIS installation, which feature should be selected to enable HTTPS?
    a) WebDAV Publishing
    b) ASP.NET
    c) Request Filtering
    d) Security - SSL Certificate
2. What is the default directory path where IIS websites are stored on a Windows Server?
    a) C:\Windows\Web\IIS
    b) C:\Program Files\IIS
    c) C:\inetpub\wwwroot
    d) C:\IIS\Webroot
3. Which tool is primarily used to install IIS on Windows Server?
    a) PowerShell
    b) Server Manager
    c) Task Manager
    d) Windows Defender
4. What is the first step in deploying IIS on a Windows Server?
    a) Installing FTP service
    b) Configuring DNS settings
    c) Adding the Web Server (IIS) role
    d) Installing a database
5. Which tool in Windows Server can be used to monitor real-time IIS performance and resource usage?
    a) IIS Manager
    b) Event Viewer
    c) Performance Monitor
    d) Task Scheduler
6. What is Web Deploy used for in IIS?
    a) Monitoring website traffic
    b) Deploying websites and applications to IIS
    c) Configuring application pools
    d) Enabling HTTP redirection
7. How is load balancing implemented in IIS?
    a) Using Application Pools
    b) Configuring a Web Farm
    c) Using only one server

d) Disabling SSL

8. What does the HTTP Redirect feature in IIS allow you to do?
   a) Redirect HTTP requests to another server
   b) Host multiple websites on the same server
   c) Change website language settings
   d) Bind SSL certificates
9. How do you ensure that only authorized users can access a website hosted on IIS?
   a) Enable FTP
   b) Use Authentication and Authorization features
   c) Use IP filtering
   d) Configure DNS settings
10. What is the purpose of Application Initialization in IIS?
    a) It monitors website load time
    b) It ensures websites are initialized before the first request is made
    c) It compresses website content
    d) It limits the number of application pools

Practical assessment

Our school wants to hire you in the implementation of the following task in order to achieve the central administration of school information.
From Windows Server with IIS or another web server software, create and a website with "Student Report" message so that everyone can browse through the network.

References

Hao, S., Wang, H., Stavrou, A., & Smirni, E. (2015, November). On the DNS deployment of modern web services. In *2015 IEEE 23rd International Conference on Network Protocols (ICNP)* (pp. 100–110). IEEE. https://doi.org/10.1109/ICNP.2015.13

Panek, W. (2018). *Installing Windows Server 2016*.

Krause, J. (2016). *Mastering Windows Server 2016*. Packt Publishing Ltd.

Krause, J. (2019). *Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities*. Packt Publishing Ltd.

Richards, J., Allen, R., & Lowe-Norris, A. G. (2006). *Active Directory*. O'Reilly Media, Inc.

Allen, R., & Lowe-Norris, A. (2003). *Active Directory*. O'Reilly Media, Inc.

Clines, S., & Loughry, M. (2008). *Active Directory for dummies*. John Wiley & Sons.

Infrasos. (n.d.). Install and configure DNS server on Windows Server. Retrieved January 8, 2025, from https://infrasos.com/install-and-configure-dns-server-on-windows-server/

Jotelulu. (n.d.). Deploy DNS server using PowerShell commands. Retrieved January 8, 2025, from https://jotelulu.com/en-gb/blog/deploy-dns-server-using-powershell-commands/

Indicative contents
Installation of FTP server **Configure the FTP Server** **Implement FTP server file sharing**

Key Competencies for Learning Outcome 6: Deploy FTP Services

Knowledge	Skills	Attitudes
• Describe FTP services • Preparation of FTP services installation • Test the FTP server • Select an FTP Server Software • Test FTP File Sharing	• Configuring and installing FTP services • Installing FTP client • Installing FTP services • Setting permissions for Shared Directory	• Have self-motivation • Being analytical and details oriented

Duration: 10 hrs

Learning outcome 6 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe clearly the deployment process as used in FTP services
2. Perform properly FTP services installation as used in windows server.
3. Perform correctly FTP service configuration as used in server administration.
4. Implement appropriately permissions for Shared Directory as used in FTP server

Resources

Equipment	Equipment	Equipment
● Projector ● Computer ● UPS	● Modem ● Router ● VMware Workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD	● Electricity ● Cables ● Internet

Indicative content 6.1: Installation of FTP Server

Duration: 4 hrs

Theoretical Activity 6.1.1: Introduction of FTP services and section of FTP

Tasks:

1: Answer the following questions related to the description of FTP services Concepts:

i. i. Define FTP?.

ii. Discuss the advantages and disadvantages of using File Transfer Protocol over FileZilla

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 6.1.1

Key readings 6.1.1: Introduction of FTP services and selection of FTP client

1.Definition of key terms

1.1. FTP (File Transfer Protocol)

FTP, or File Transfer Protocol, is a standard network protocol used for transferring files between a client and a server over the Internet. It facilitates the exchange of commands and data, allowing users to upload or download files to and from a remote server. FTP operates using two modes: Active and Passive, which determine how data connections are established. While FTP is widely used for website management and file sharing, it does not encrypt data during transmission, making it vulnerable to interception. To enhance security, variations like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) are often used, which encrypt the data being transferred.

Types of FTP

- **FTP secure (FTPS):** Taking security one notch up from traditional FTP, FTP Secure (FTPS) ensures a secure file transfer. It provides an additional encryption layer using either Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols during data transmission across the network.
- **SSH file Transfer Protocol (SFTP):** This is a secure file transfer subsystem for the Secure Shell (SSH) protocol. SFTP is a widely used method for securely transferring files over remote systems. In SFTP, both data and commands are encrypted and transmitted in specifically formatted binary packets through a single, secured connection using SSH.

1.2. FileZilla

FileZilla is a popular open-source FTP client that enables users to connect to FTP servers to transfer files easily. It supports both standard FTP and secure protocols like FTPS and SFTP. FileZilla is known for its user-friendly interface and robust functionality, making it suitable for managing website files and sharing large data sets. The software is available on multiple platforms, including Windows, macOS, and Linux. Users can set up connections quickly using features like Quickconnect or Site Manager for frequent connections.

1.3. Hosting Account

A hosting account refers to a service provided by web hosting companies that allows individuals or organizations to store their websites or applications on a server. This account provides the necessary resources such as storage space, bandwidth, and access to an FTP server for uploading files. Hosting accounts can vary in features depending on the provider and plan chosen, catering to different needs such as personal blogs, business websites, or complex applications.

2. Select an FTP client

When choosing an FTP client, it's important to consider the following essential features:

1. **Speed and Reliability:** Look for an FTP client that offers fast and stable file transfer speeds, ensuring that your uploads and downloads are completed efficiently.

   Speed and reliability are crucial factors to consider when choosing an FTP client. A client with fast transfer speeds will save you valuable time, especially when dealing with large files or a high volume of data. Additionally, a reliable FTP client will ensure that your files are transferred without any interruptions or errors, minimizing the risk of data loss.
2. **Security:** Ensure that the FTP client supports secure connection protocols such as FTPS or SFTP to protect your file transfers from unauthorized access. Security is of utmost importance when transferring files over the internet. It is essential to choose an FTP client that supports secure connection protocols like FTPS (FTP over SSL/TLS) or SFTP (SSH File Transfer Protocol) to encrypt your data and protect it from potential threats.
3. **User-Friendly Interface:** A well-designed and intuitive interface can significantly improve your workflow by making it easy to navigate and perform file management tasks.

   The user interface of an FTP client plays a vital role in enhancing your overall experience.
4. A client with a user-friendly interface will allow you to navigate through directories, upload and download files, and manage your remote files effortlessly. Look for features such as drag-and-drop functionality, customizable layouts, and clear icons that make it intuitive and convenient to perform file

management tasks.

Compatibility: Consider the compatibility of the FTP client with your operating system to ensure seamless integration with your preferred platform. Compatibility is an essential aspect to consider when selecting an FTP client. Ensure that the client you choose is compatible with your operating system, whether it's Windows, macOS, Linux, or others.

Practical Activity 6.1.2: Installing of FTP client and FTP services

Task:

1: Referring to the key reading 6.1.1, As a server administrator, you are asked to go to the computer lab to perform the following: select FTP client and FTP server based on requirement and perform FTP installation on client side and server side.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 6.1.2 and ask clarification where necessary

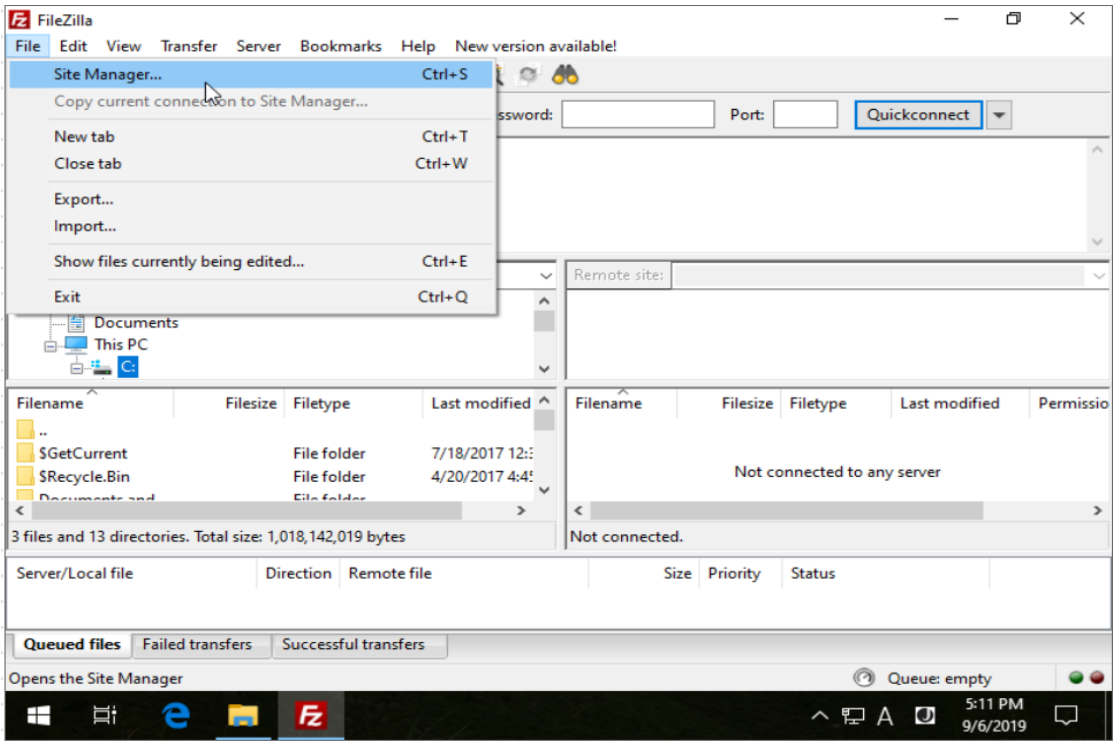
5: Perform the task provided in application of learning 6.1.2

Key readings 6.1.2: Installing FTP client and FTP

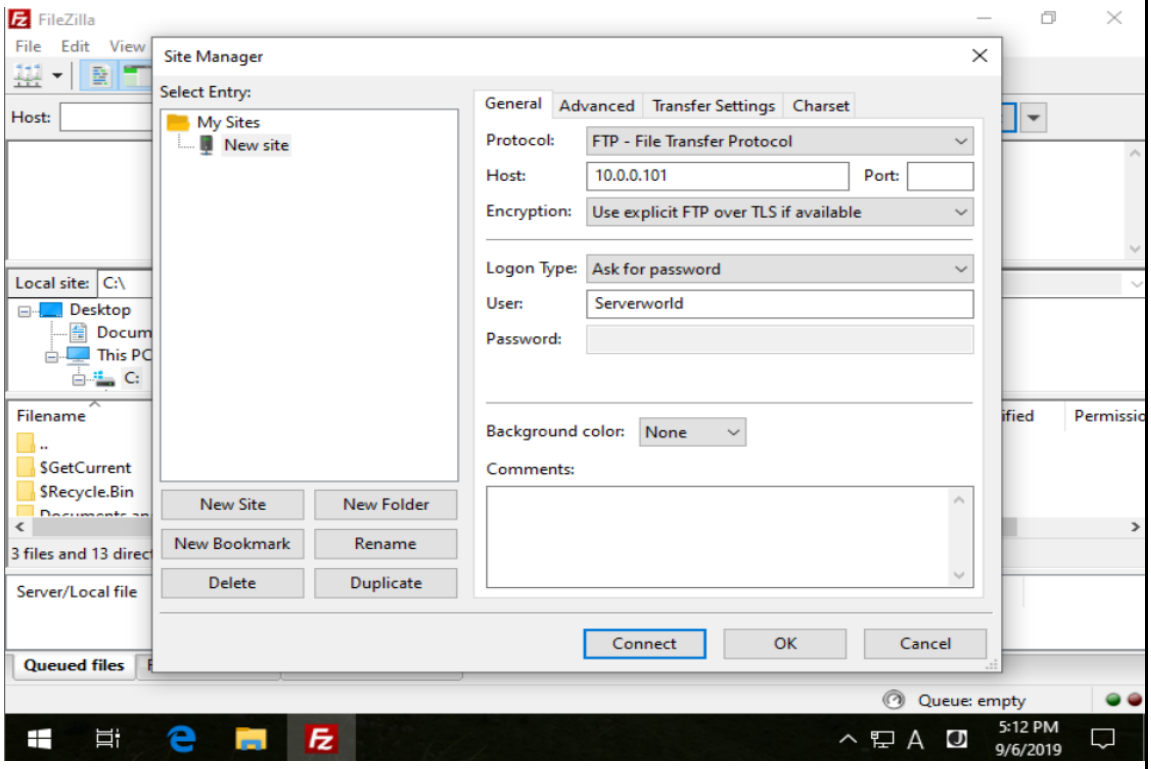
1.FTP Server: FTP Client

Connect to the FTP server from client computers. On passive mode connection, client program ftp command bundle in windows 10 or windows server 2019(tor old versions) cannot use passive mode (even if with [quote pasv]), so it needs to use other FTP client program. On this example, Use FileZilla. https://filezillaproject.org/download.php?type=client.

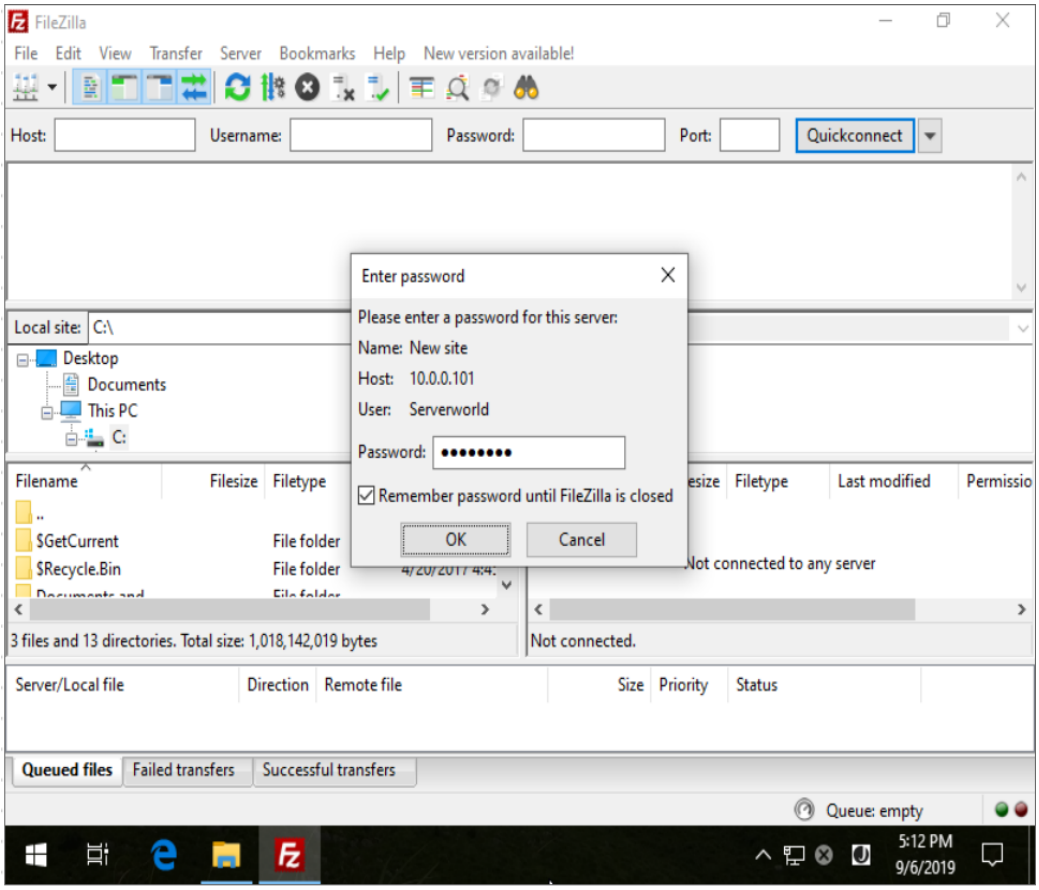
1.install FileZilla and run it, then open [File]-[Site Manager].



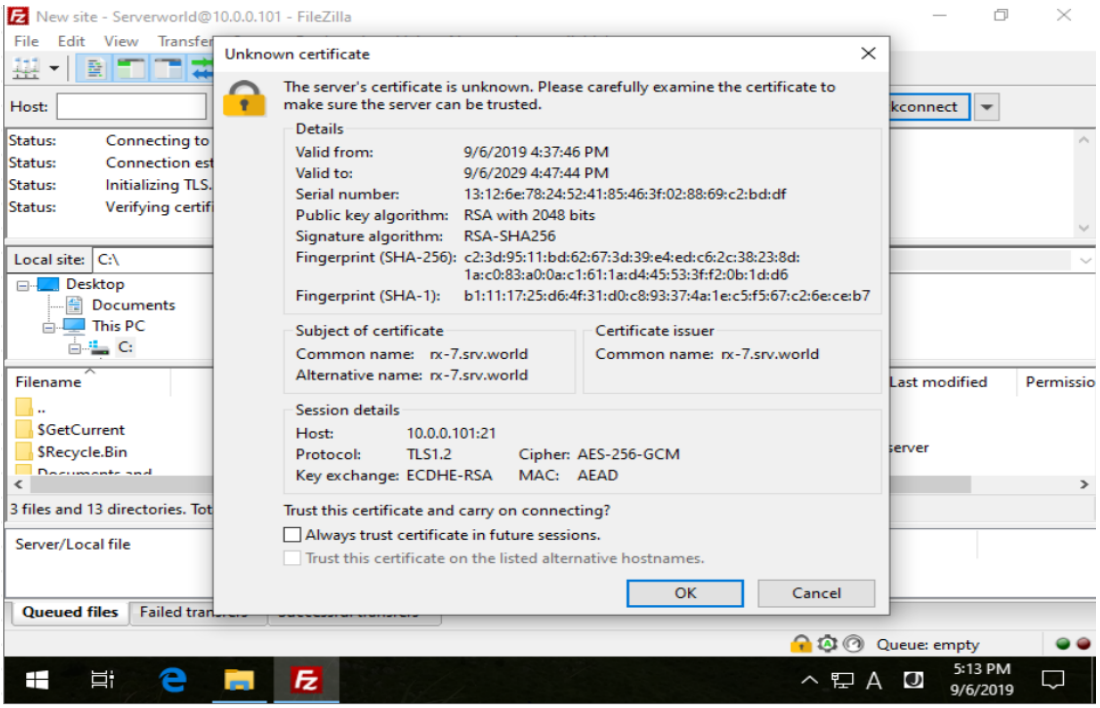
2. Click **New Site** button and input information for FTP connection. For host field, input Hostname or IP address of FTP server. For **Logon Type** filed, select **Ask for password** or other type except **Anonymous.**



3. password is required, input it of the connected user



4. if you use self-signed certificate, following warning is shown because it is self-signed one. Click **OK** to proceed



5. Just connected to FTP site. Try to transfer file.

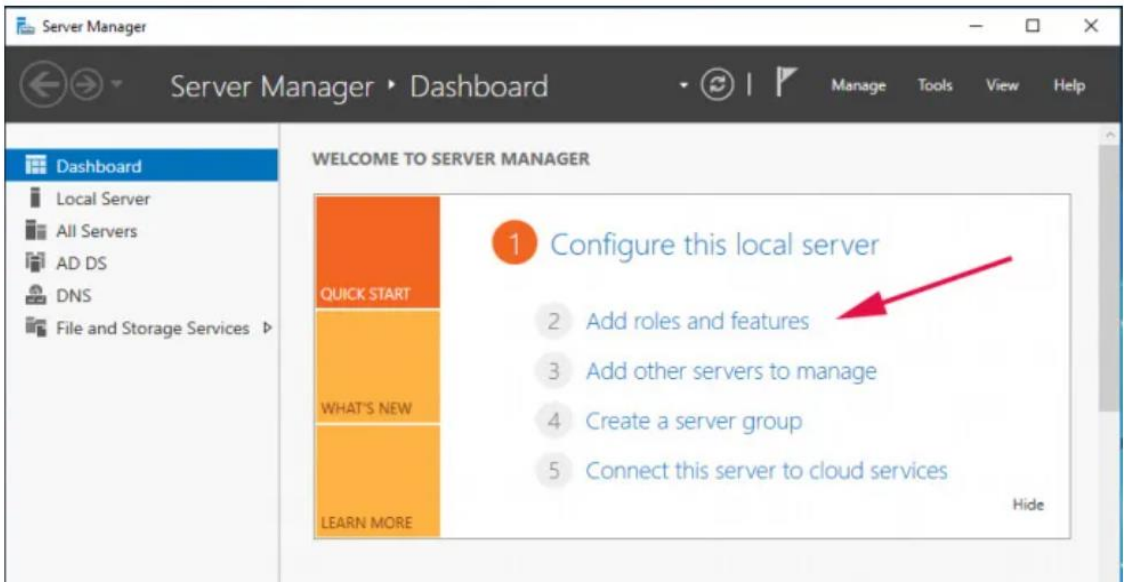
2.Install FTP Server

Server Manager is a graphical console that was introduced in Windows Server 2008. The objective was to help System Administrators easily install and manage various features and roles on the server. To install the FTP server using Server Manager, follow the steps as illustrated.

Step 1: Launch Server Manager

Usually, the server manager utility launches automatically upon logging in. Alternatively, you can click on the **Start** menu button and select **Server Manager** from the pull-up menu that appears.

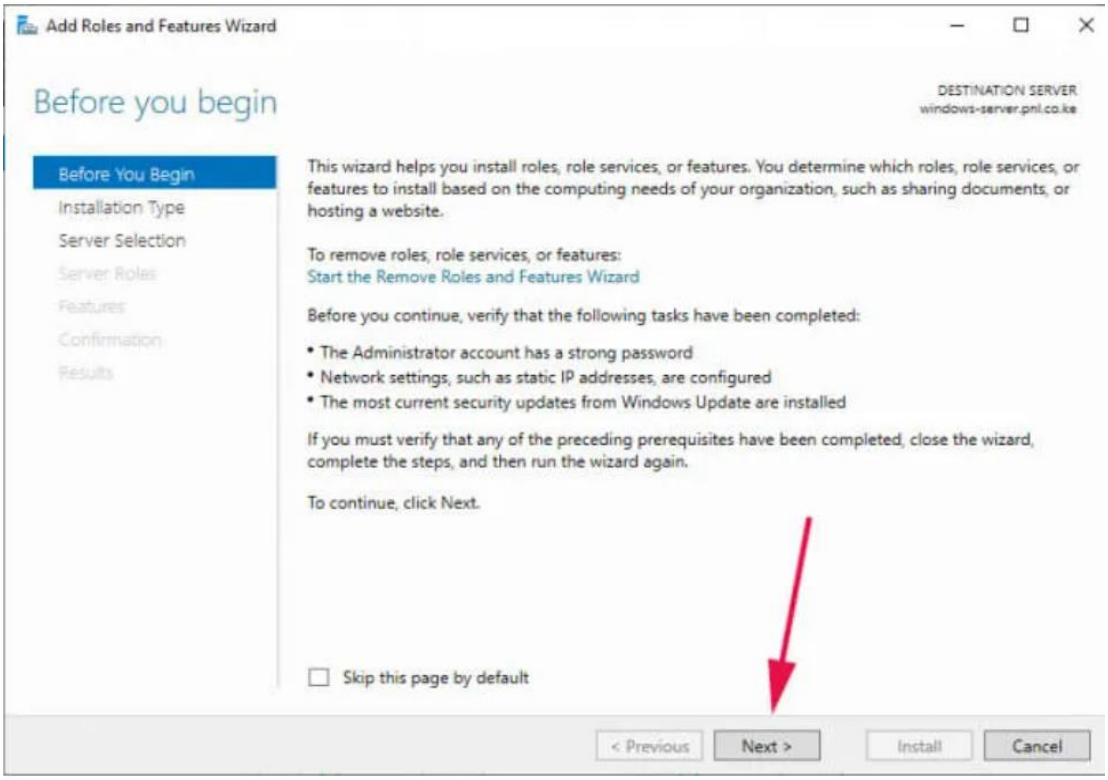
Once launched, click on the **Add roles and features** option as shown.



Step 2: Proceed with the installation

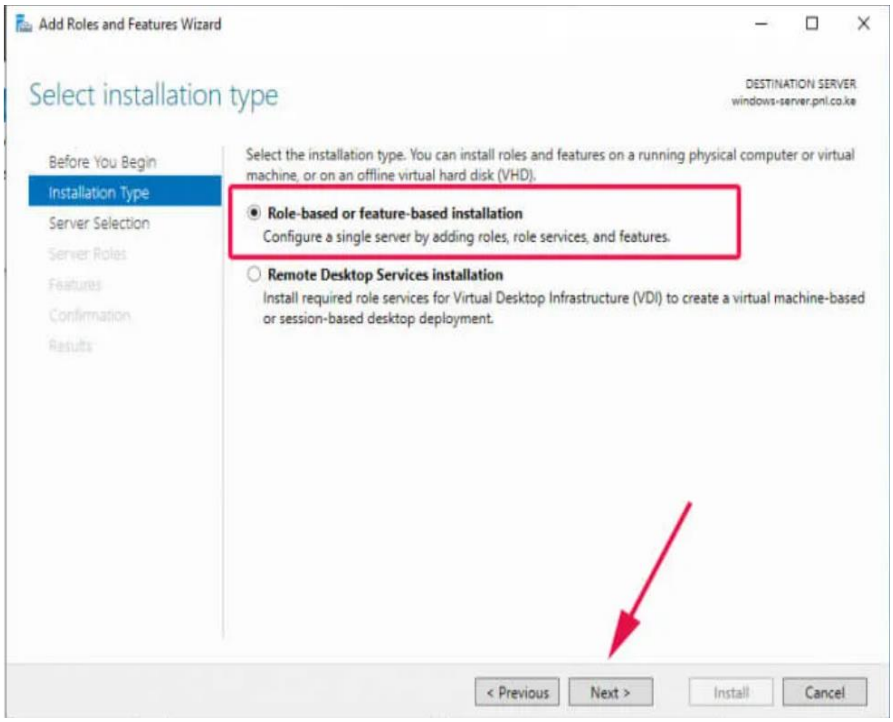
Clicking the '**Add roles and features**' option launches the installation wizard. The Wizard gives you a summary of the tasks you can perform such as adding/removing roles and features. You will be required to have a few prerequisites in order before proceeding.

Once you have gone over the summary, simply click '**Next'**.



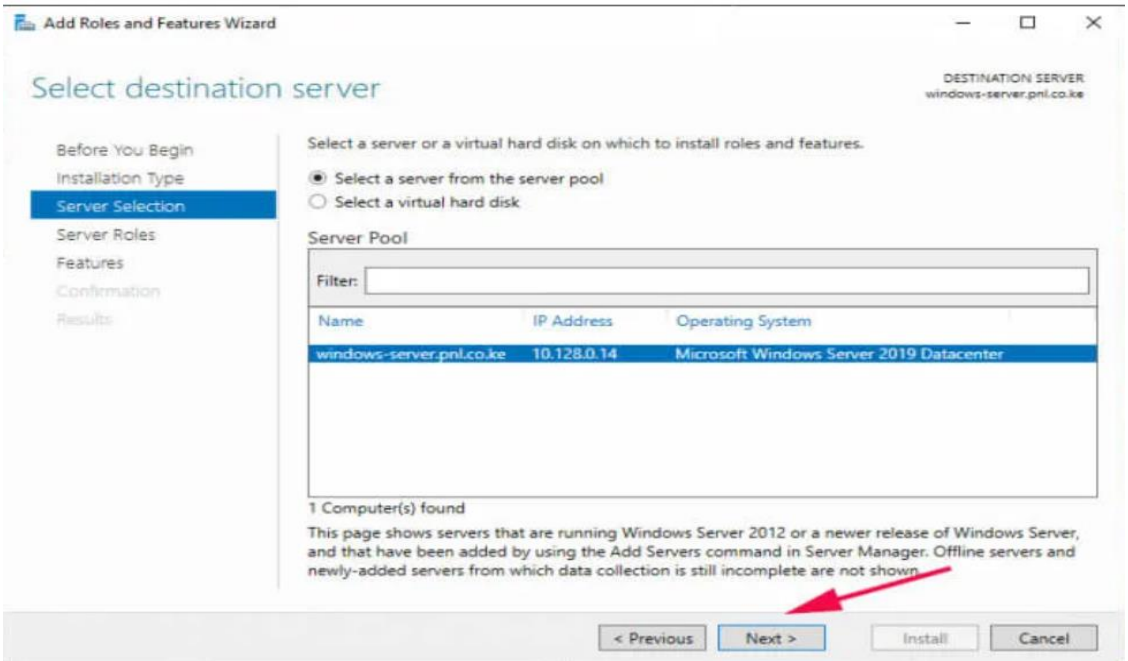
Step 3: Select the Installation Type

In the next step choose '**Role-based or feature-based**' installation and click **'Next**'.



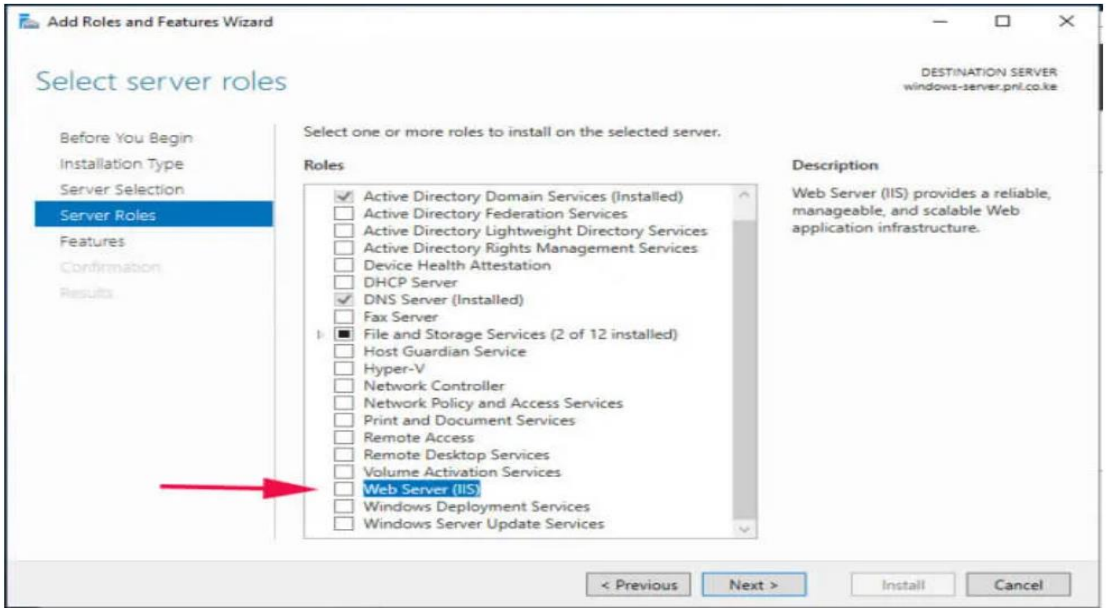
Step 4: Select the Destination Server

You will thereafter be required to select the server upon which you will install the roles and features. By default, the server you are working on will be selected. Just accept the defaults and hit '**Next**'.



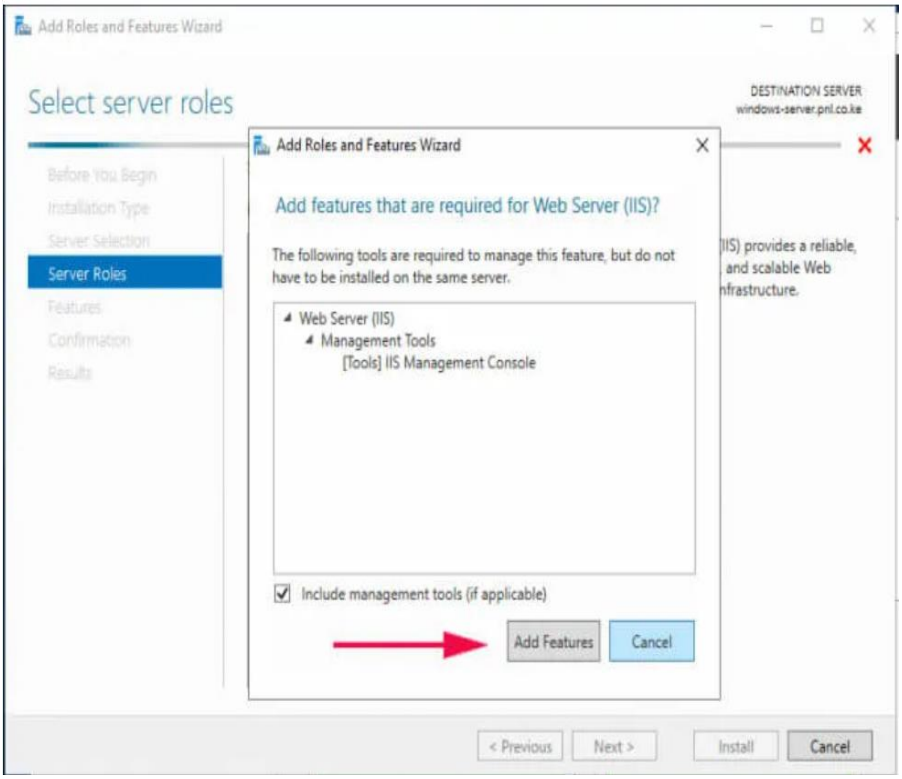
Step 5: Select Server Roles to be Installed

In the next step, a list of server roles will be listed. Click on the '**Web Server IIS**' option.



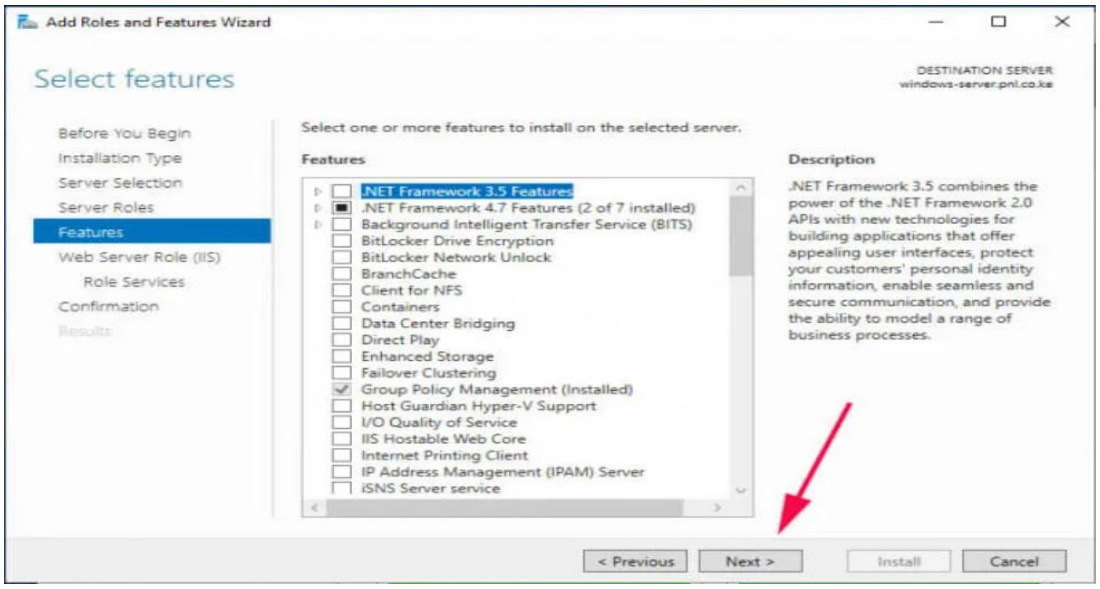
This launches a pop-up window that lists the roles to be installed as shown.

Click on '**Add features**' and hit the '**Next**' button to proceed to the next step.



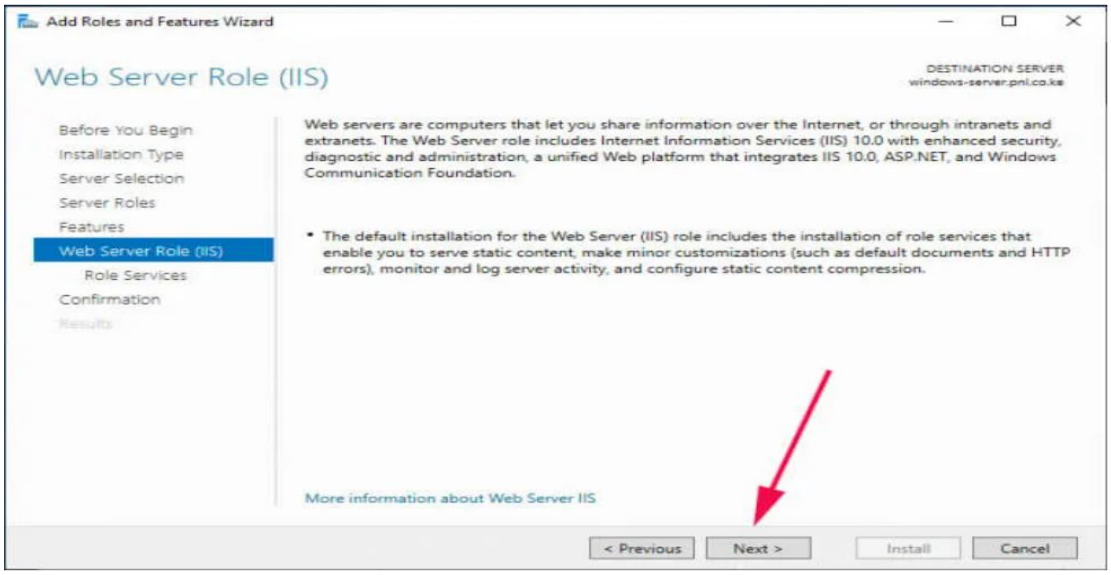
Step 6: Select Server Features

Nothing much is required in this step, so once again, click on the **'Next**' button.



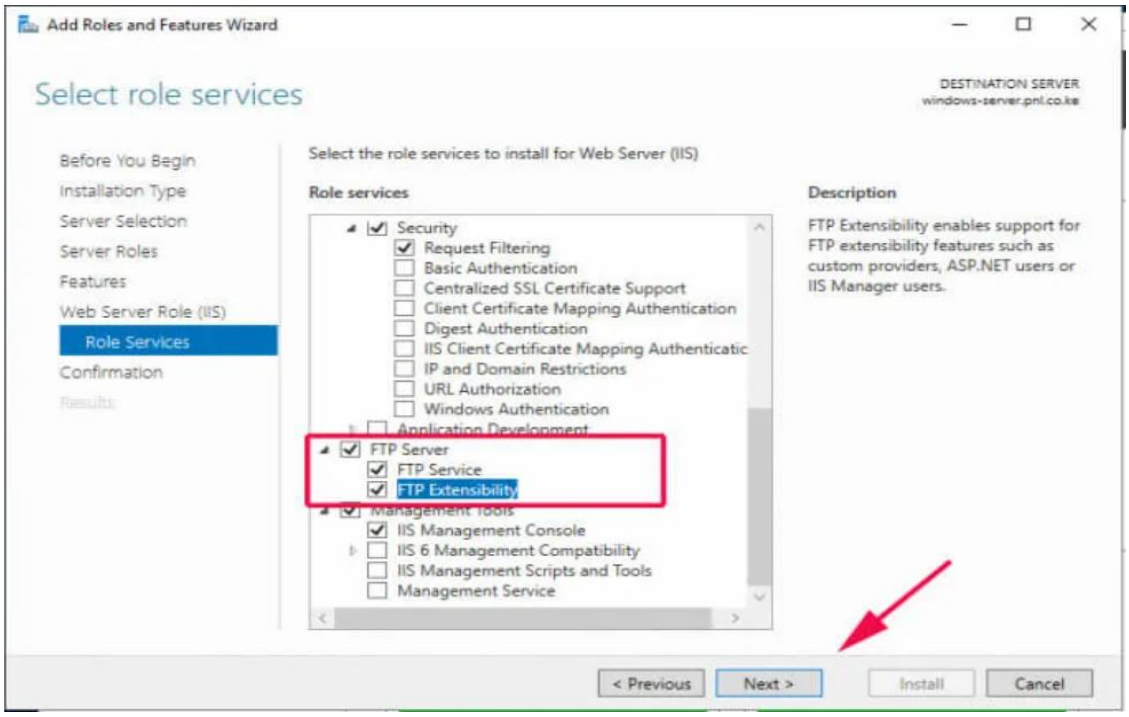
Step 7: Web IIS overview

The next step gives you a glance about what a web server is and the role it plays. So, once again, simply click '**Next**' to proceed to the next step.



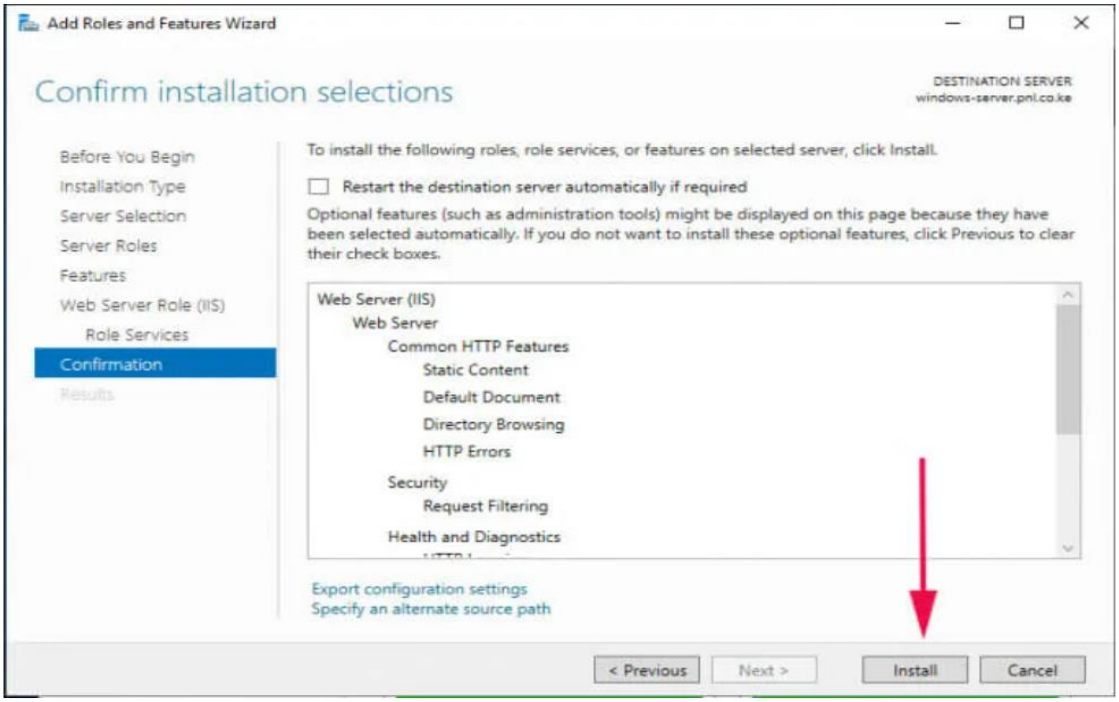
Step 8: Select Role Services

This is the quintessential step where we shall select the FTP feature. Simply scroll and check off the '**FTP Server**' checkbox and the corresponding FTP sub-options (**FTP service** and **FTP extensibility**). Then click '**Next**'.

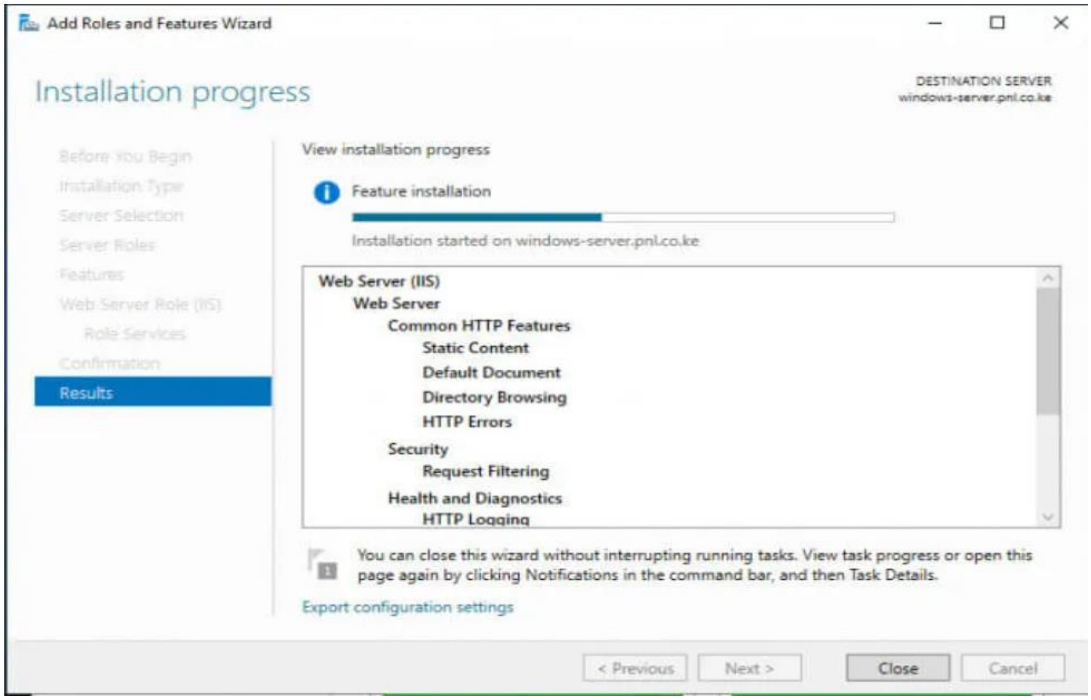


Step 9: Confirm Installation

Finally, you will be presented with a summary of the roles and features that you have selected to be installed. To confirm and initiate the installation process, click on the '**Install**' button.



The installation will take a while, so some patience will come in handy. Once the installation is complete, reboot your server for the roles and features to be fully enabled.



As we mentioned, we can install FTP using Windows Power shell. All the steps that we have just gone through can be summarized in one single command on Windows Power shell as follows:

Install-Windows Feature Web-FTP-Server -Include Management Tools

Points to Remember

- **File Transfer Protocol (FTP)**
  File Transfer Protocol (FTP) is a standard network protocol used for transferring files between a client and a server over a computer network.
- **FileZilla**
  FileZilla is a free, open-source FTP client that enables users to connect to FTP servers to transfer files securely.
- **Hosting Account**
  A hosting account refers to an online service provided by web hosting companies that allows individuals or organizations to store their website files on a server.

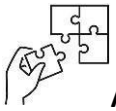
Select an FTP client

When choosing an FTP client, it's important to consider the following essential features:

- Speed and Reliability
- Security
- User-Friendly Interface
- Compatibility

- **Steps of FTP server installations**

  Step 1: Launch Server Manager
  Step 2: Proceed with the installation
  Step 3: Select the Installation Type
  Step 4: Select the Destination Server
  Step 5: Select Server Roles to be Installed
  Step 6: Select Server Features
  Step 7: Web IIS overview
  Step 8: Select Role Services
  Step 9: Confirm Installation



Application of learning 6.1.

As network administrator you are asked to establish a web Server for hosting your school website, select all requirement and install web server within windows sever operating system based on school objectives and available materials and equipment's.

Indicative content 6.2: Configure the FTP Server

Duration: 3 hrs

Practical Activity 6.2.1: Setup root directory for the FTP server

Task:

1: Referring to the previous theoretical activities (6.1.1) as a server administrator, you are asked to go to the computer lab to perform the following: configure FTP server root directory with its respected features.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 6.2.1 and ask clarification where necessary

5: Perform the task provided in application of learning 6.2.1

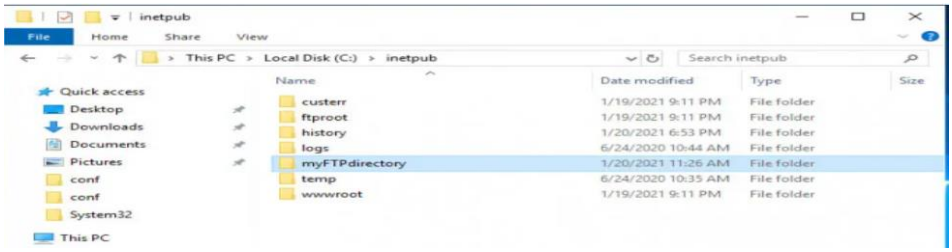
Key readings 6.2.1: Setup root directory for the FTP server

1.Root directory for the FTP server

To this point, we have installed the FTP server feature on the system, and a root default directory is created to that effect. The path of the root directory is at **C:\inetpub**.

We are going to create a custom FTP directory where we are going to place files and directories which can be accessed by authorized users across the network.

Therefore, navigate to the C:\inetpub path. Right click and select '**New**' then **'Folder**'. Give the folder your preferred name. In this case, we have created a folder called **myFTPdirectory.**



2.Access permissions

Access permissions for files and directories in an FTP server can be categorized into three main types: Read, Write, and Execute. Here's a detailed overview of each type of permission:

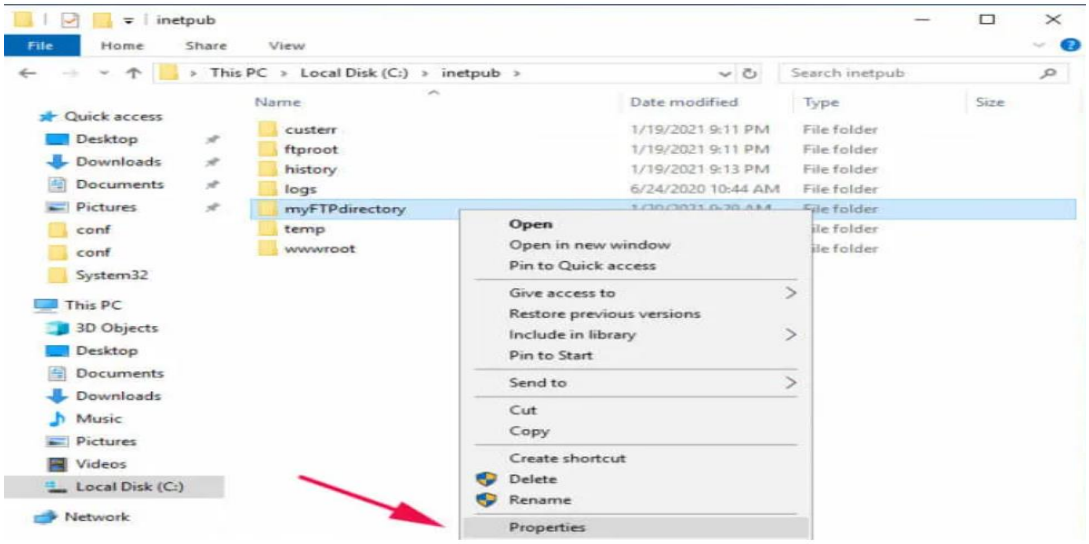
2.1. Read Permission (r): Allows users to view the contents of a file or directory. For directories, this permission enables users to list the files contained within that directory. Without read access, users cannot see or retrieve any files.

2.2. Write Permission (w): Grants users the ability to modify a file or directory.

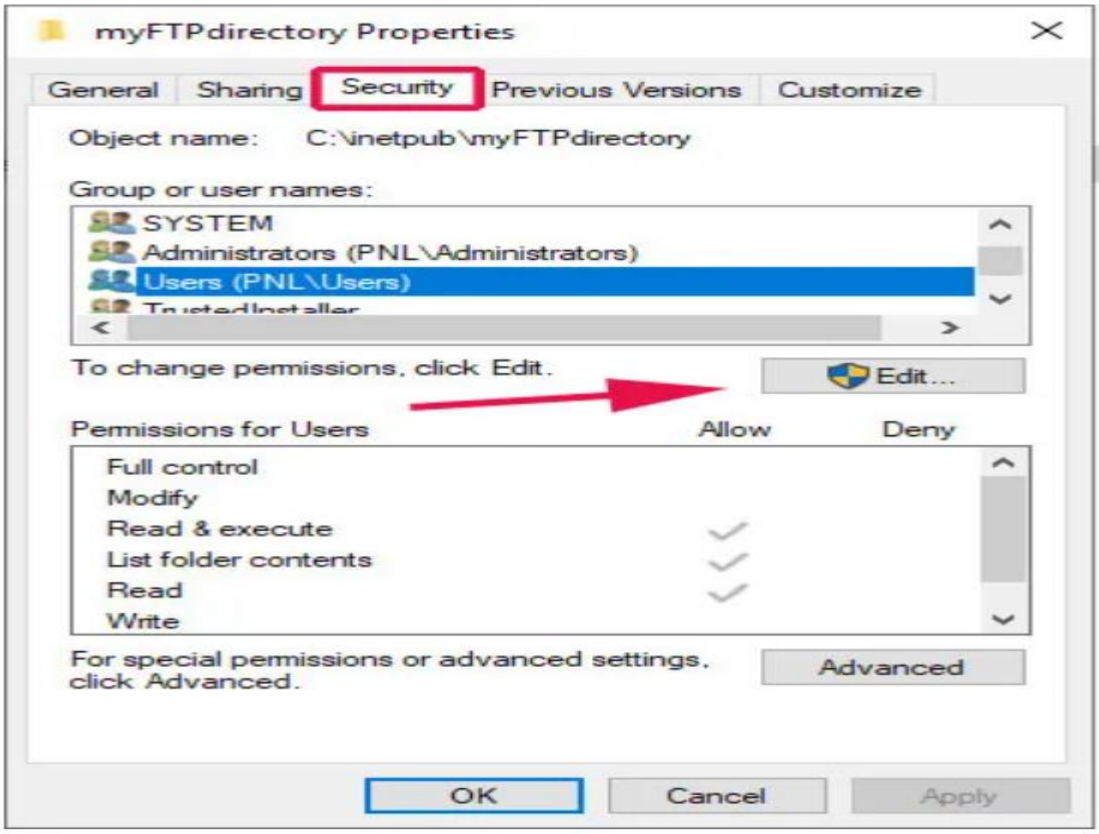
For files, this means they can edit the content or overwrite it. For directories, write permission allows users to create new files or subdirectories and delete existing ones.

2.3. Execute Permission (x): This permission is relevant primarily for directories in the context of FTP servers. It allows users to enter a directory and access its contents if they have read permission.

We need to assign this directory the required permissions so that an authorized user can read from its contents. To achieve this, right-click on the directory and select '**Properties**'.



In the **'Properties'** window pop-up, click on the **'Security**' tab to adjust the permissions. Select the group which you want to allow access to the directory. In this case, I have selected the '**Users**' group. Then click on the '**Edit**' button to assign permissions to the group.



For our example, we clicked on '**Full control'** and hit the **Apply** button.

2.4 Setting Permissions on Windows FTP Server

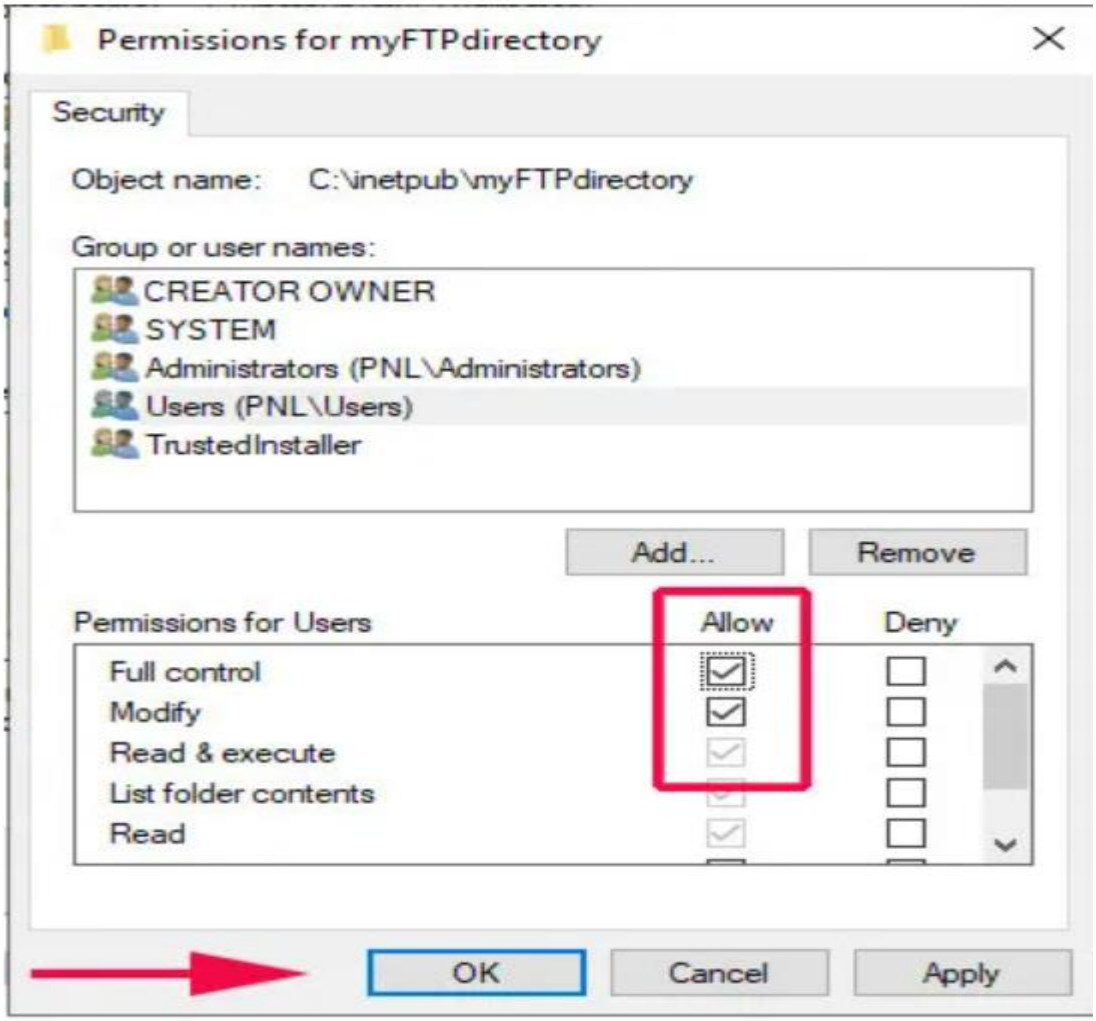
On a Windows Server running IIS for FTP services, permissions are managed through the file system's security settings:

- **Navigate to the Directory**: Locate your FTP root directory (e.g., C:\inetpub\ftproot).

- **Modify Security Settings:**

1. Right-click on the directory and select **Properties**.
2. Go to the **Security** tab.
3. Click on **Edit** to change permissions for specific users or groups.
4. Add or select a user/group and check the boxes for **Read**, **Write**, and **Modify** as needed.

- **Apply Changes:** After setting the desired permissions, click **OK** to apply changes.



Then click '**Ok**'. This takes you back to the Properties window where, once again, you will click on the '**Ok**' button.

Practical Activity 6.2.2: Configure Passive FTP Mode, Enable Logging (Optional) and Test the FTP Server

Task:

1: Referring to the key reading 6.2.1, As a server administrator, you are asked to go to the computer lab to perform the following: configure Passive FTP Mode, enable Logging and Test the FTP Server to achieve working goals.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 6.2.2 and ask clarification where necessary

5: Perform the task provided in application of learning 6.2.2

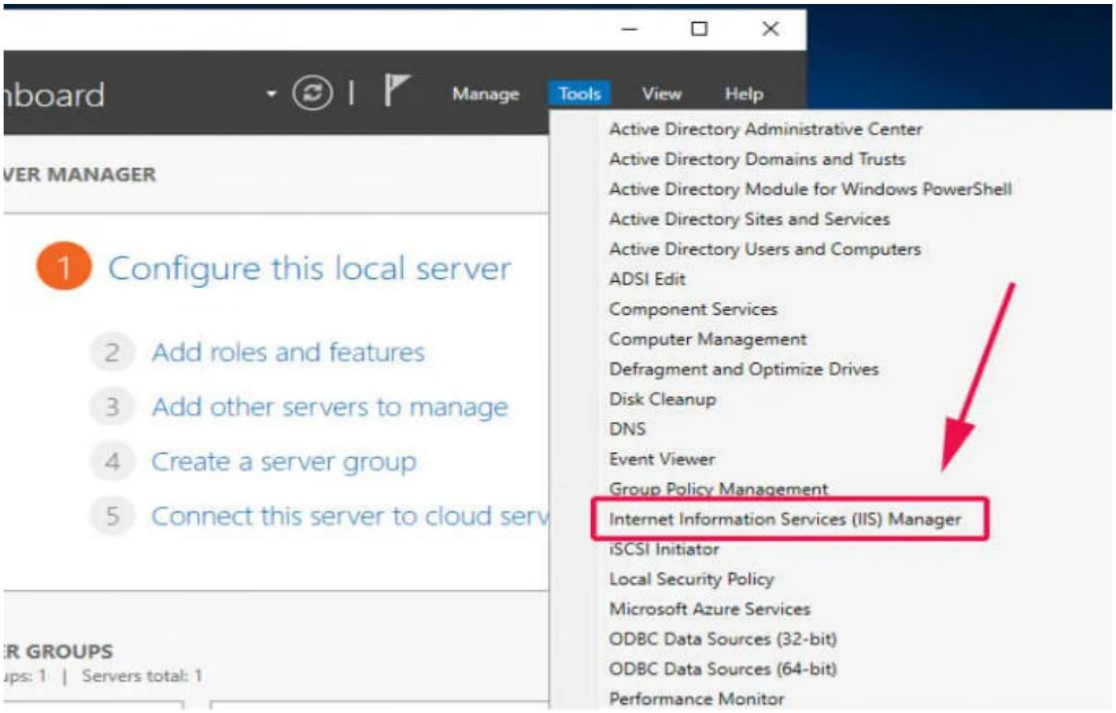
Key readings 6.2.2: Configure Passive FTP Mode, Enable Logging (Optional) and Test the FTP Server

1.Configure Passive FTP Mode (Optional)

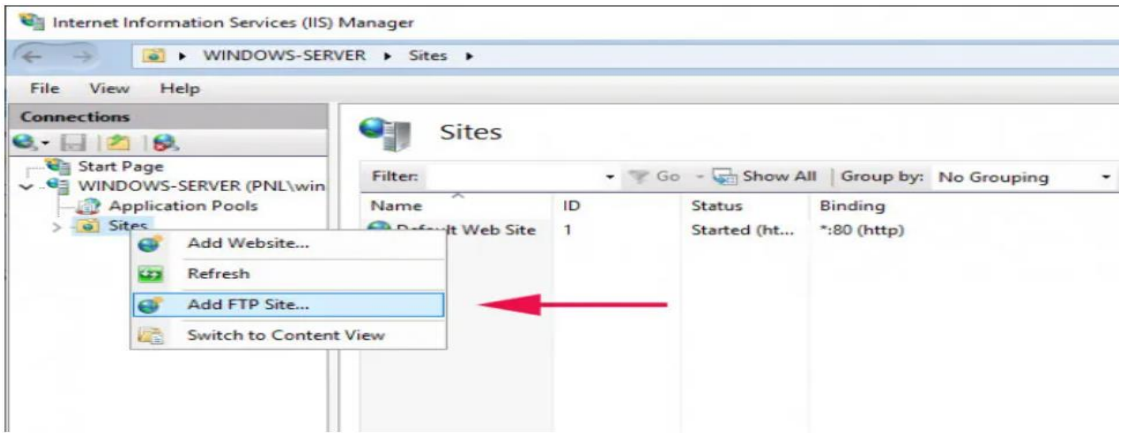
1.1 Create an FTP Site

We have assigned all permissions on our FTP directory to the Users group. The next step will be to create an FTP site which we shall map to the FTP directory. To configure Passive FTP mode on a Windows Server, follow these steps:

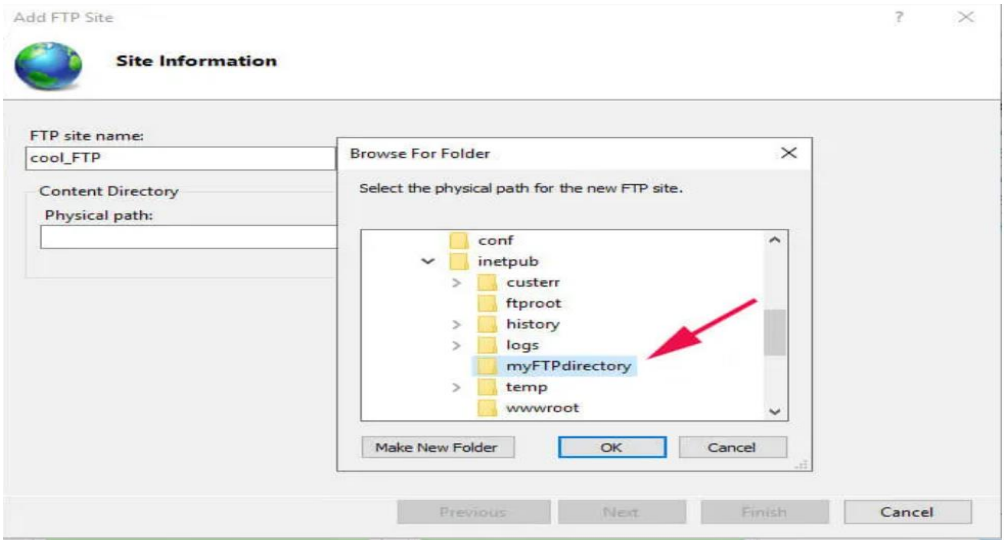
On the Server manager, click on '**Tools**' then select '**Internet Services Information (IIS) Manager**' option.



On the IIS Manager window that appears, click the server name at the left pane to reveal more options. Right-click on the '**Sites**' option and select '**Add FTP site**'.

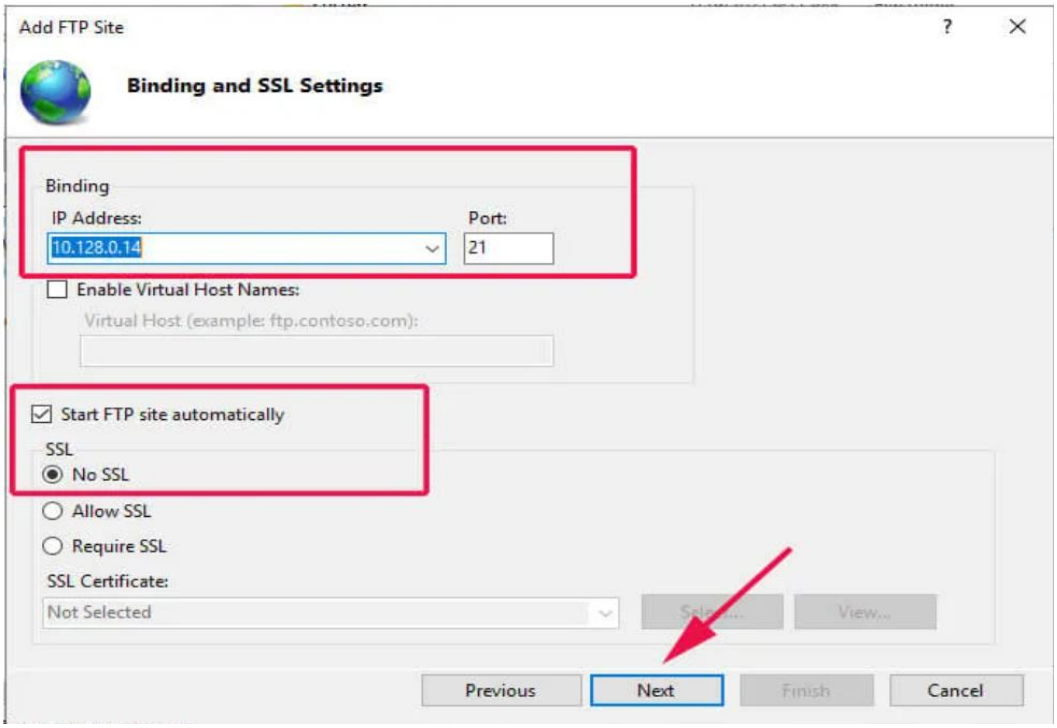


In the next step, provide the **FTP site name** and the **Physical Path** by clicking on the adjacent button with three dots and navigating to the FTP directory that we created in the previous step.



Then click '**Ok**' then '**Next**' to go to the next step.

In the '**Binding and SSL settings**' step, provide your server's IP address, FTP port. Be sure to select the -'**No SSL**' option since we are not using an SSL certificate to secure the site.

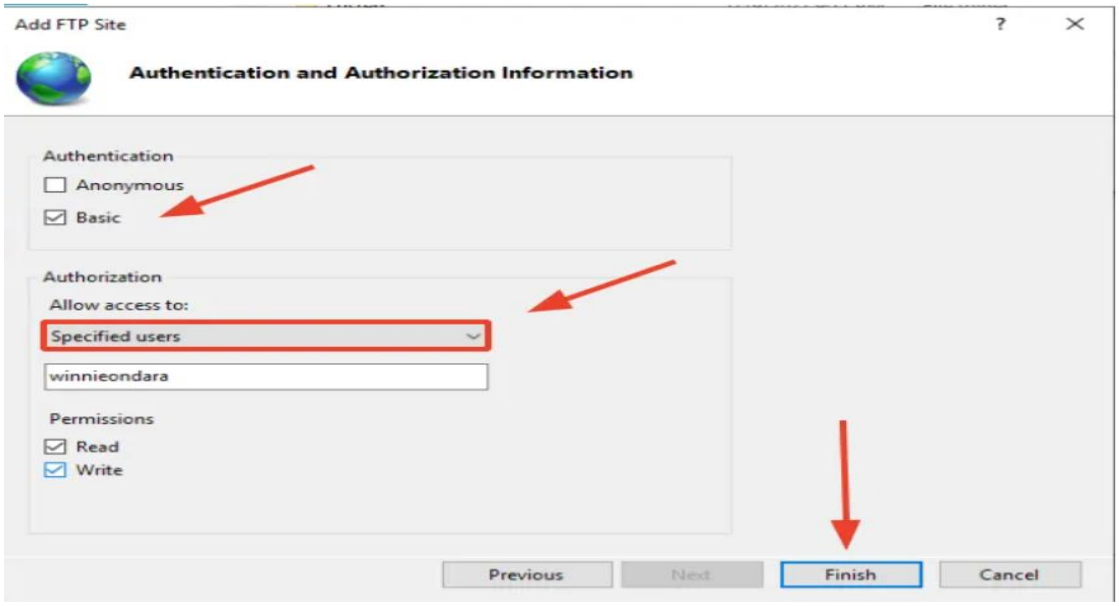


The final step requires you to select the authentication type and configure which users will have access to the FTP site. Select '**Basic'** authentication.

Under authorization, click on the '**Specified users**' option if you want a single user to access the site and right below that specify the username of the user.

Alternatively, you can allow a group of users by selecting '**Specified roles or user**

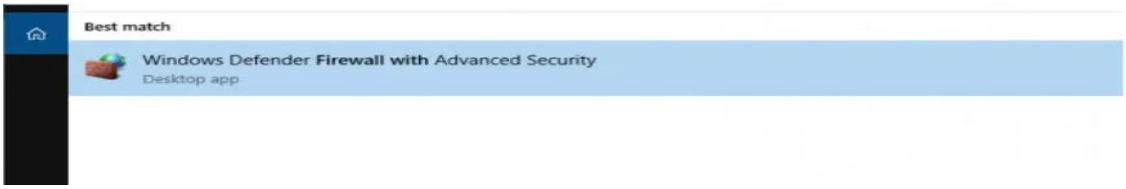
groups' and specifying the user group in the 'text field' provided. Then check off '**Read**' and '**Write**' permissions and hit '**Finish**'.



Up until this point, we have successfully configured the FTP server. The only bit remaining is to configure the firewall to allow remote users to access the FTP site.

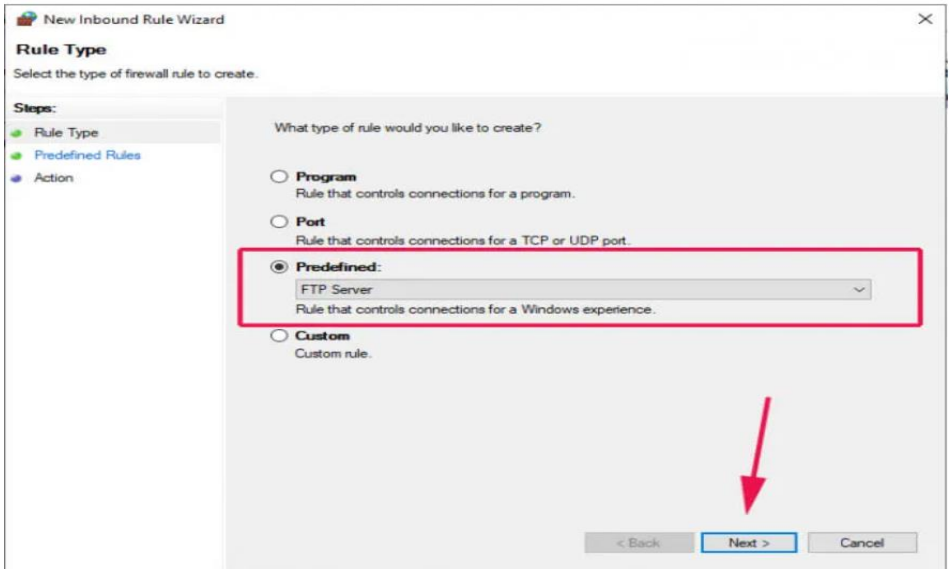
Step 2: Configure the Firewall

FTP listens on port 21, and therefore, we need to allow this port across the firewall. To start off, click on the '**Start**' menu button and search for '**Firewall with Advanced security**

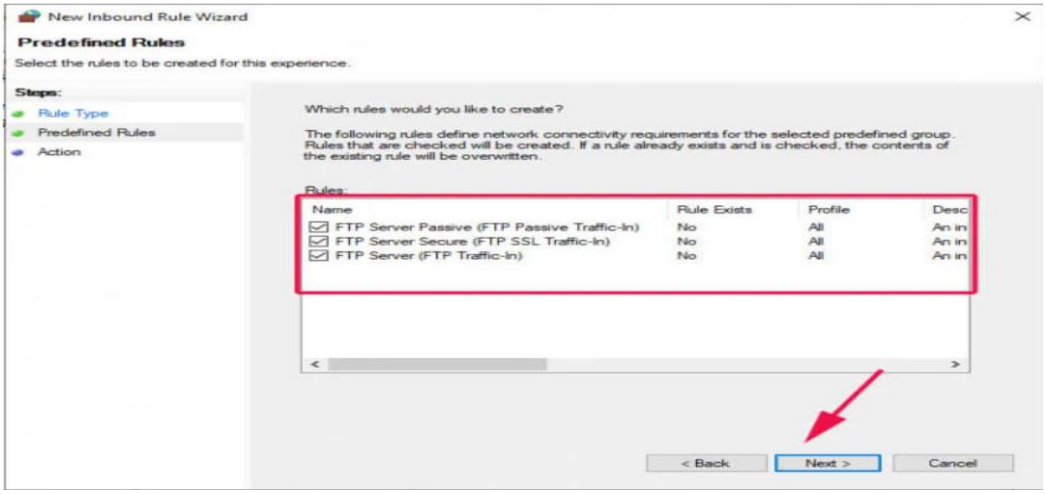


On the left pane, click on '**Inbound rules**' and the head over to the extreme right and click on **'New rule**'.

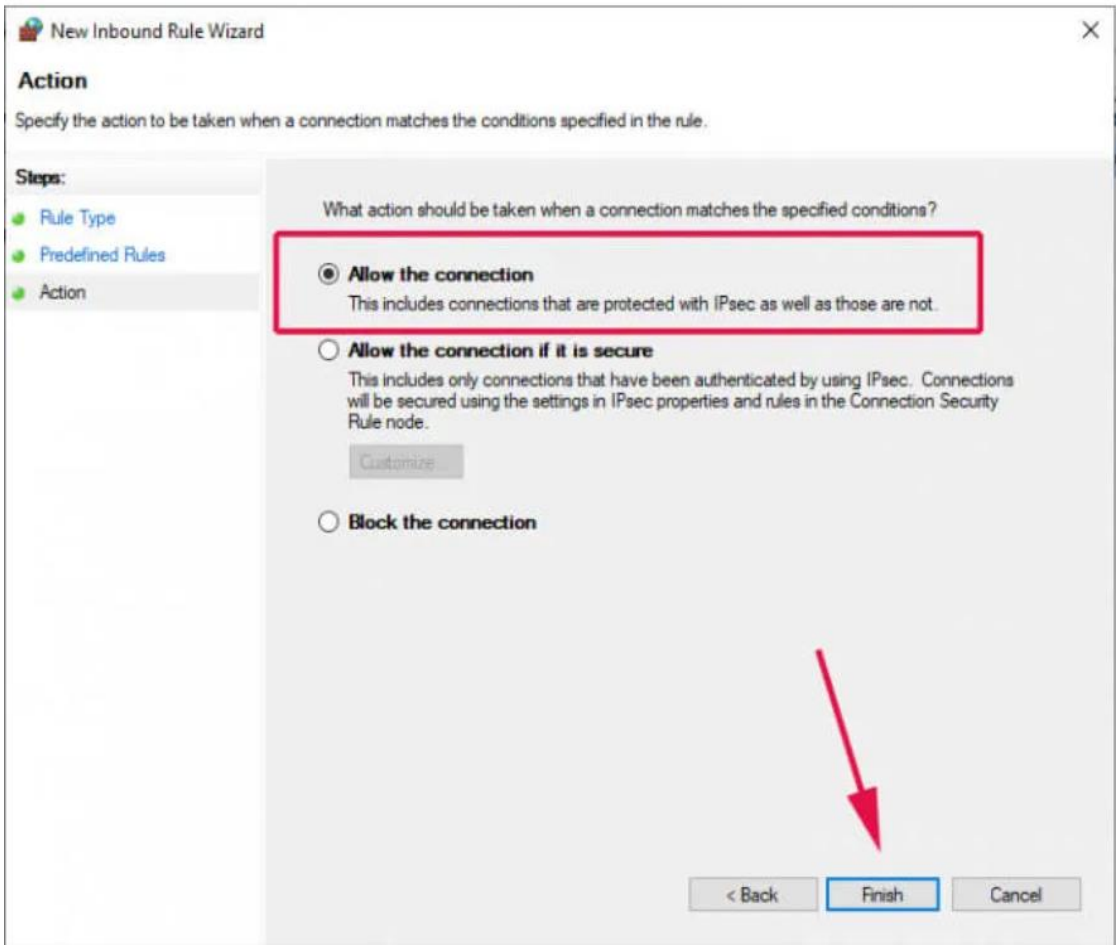
On the '**Rule Type**' window, select the '**Predefined**' option and select '**FTP server**' in the drop-down menu. Click '**Next**'.



Ensure that all the firewall rules are checked off and click '**Next**'.



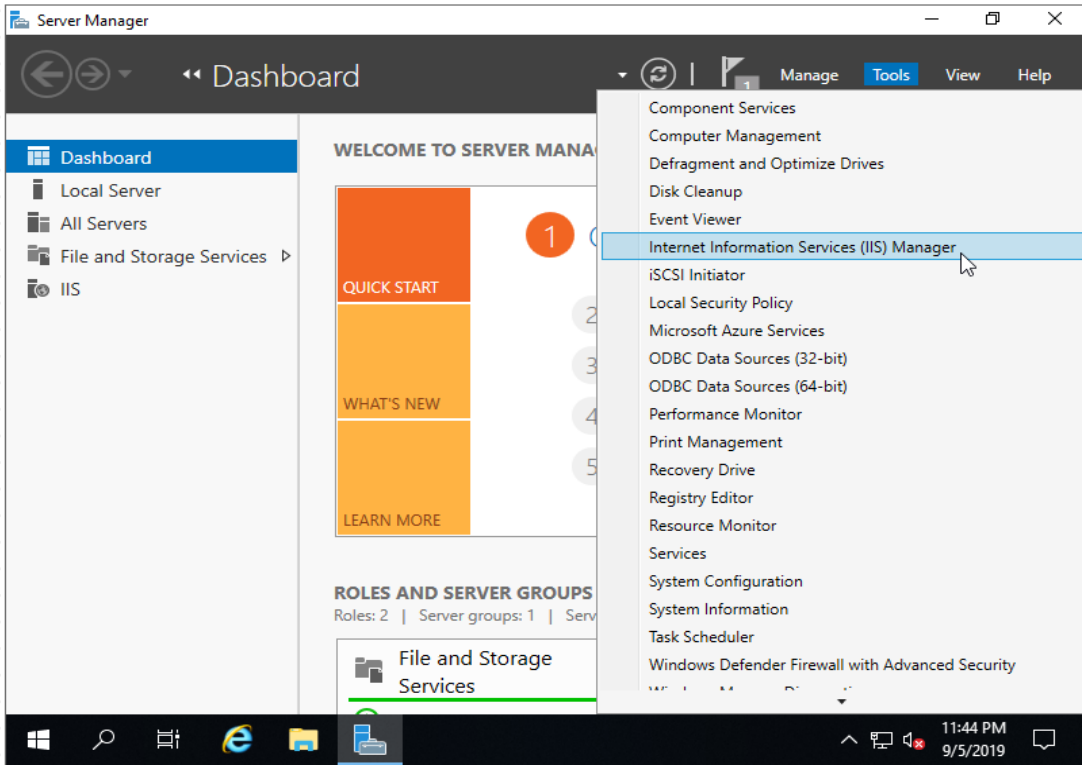
Finally, click on '**Allow the connection**' and click '**Finish**'.



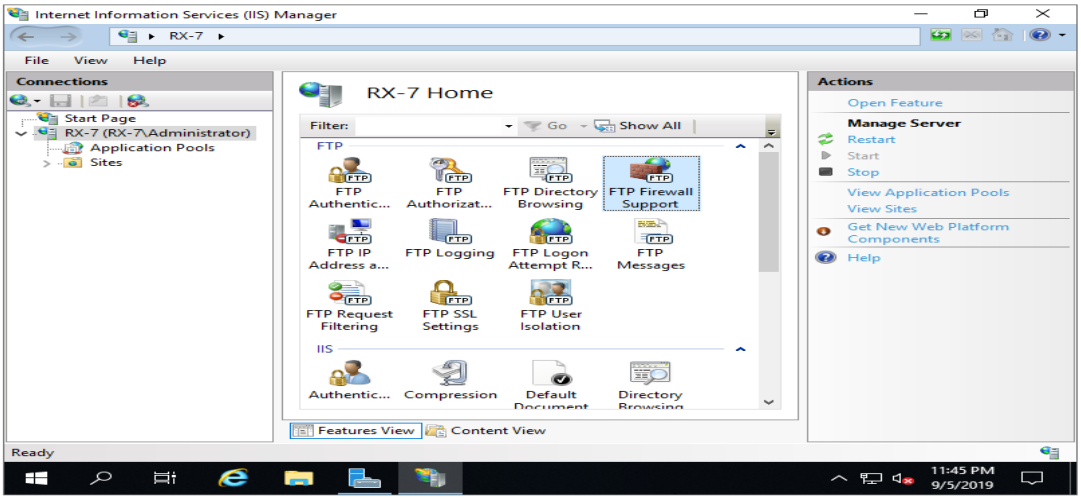
Our FTP server can now be accessed remotely from either a Windows or Linux/UNIX system. The only thing remaining is to test if we can make a connection to the server.

6. **Configure Passive FTP Mode**

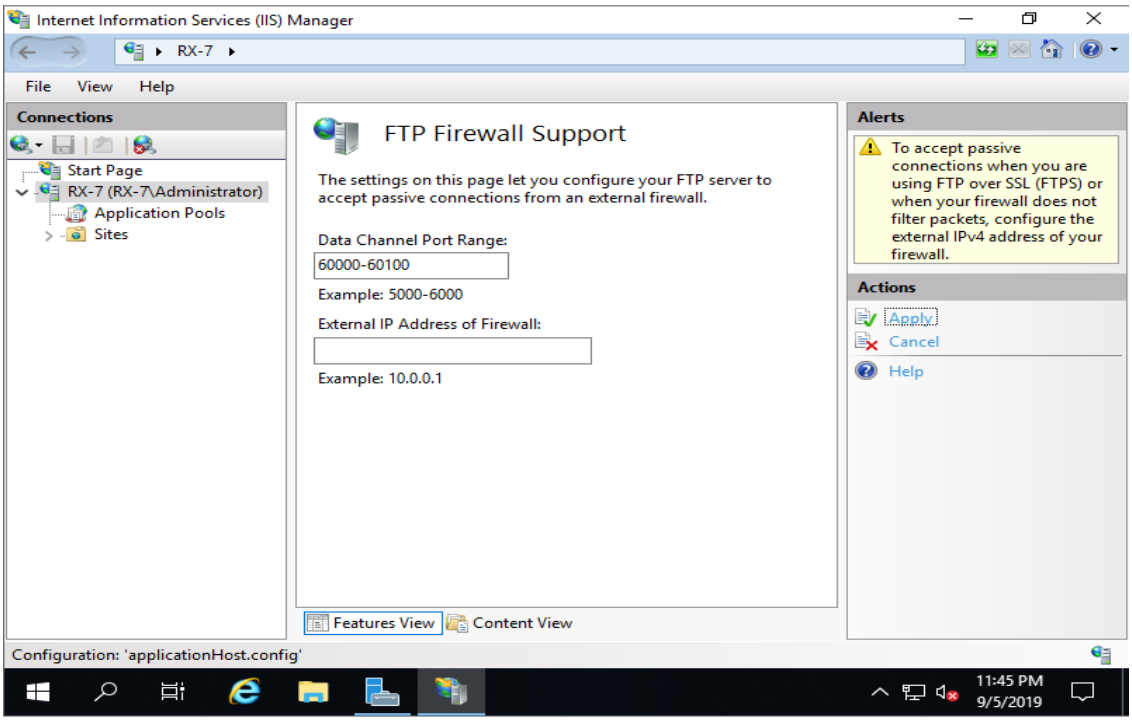
   Run **Start Server Manager** and Click **Tools** - **Internet Information Services (IIS) Manager**



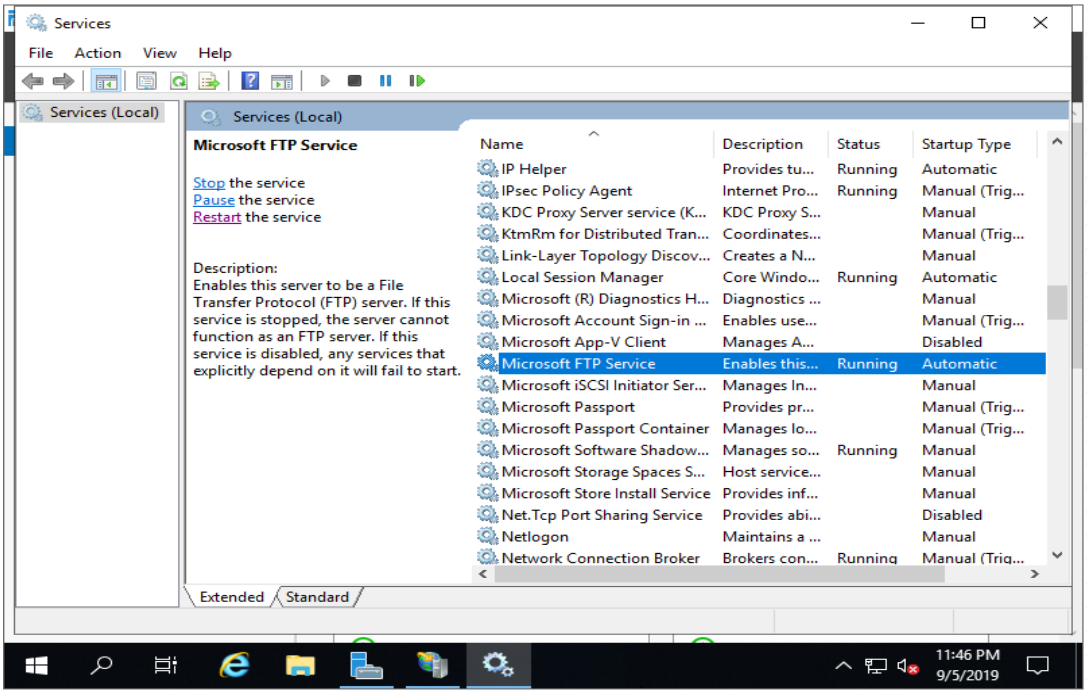
Select Hostname on the left pane and Click **FTP Firewall Support** on the center pane.



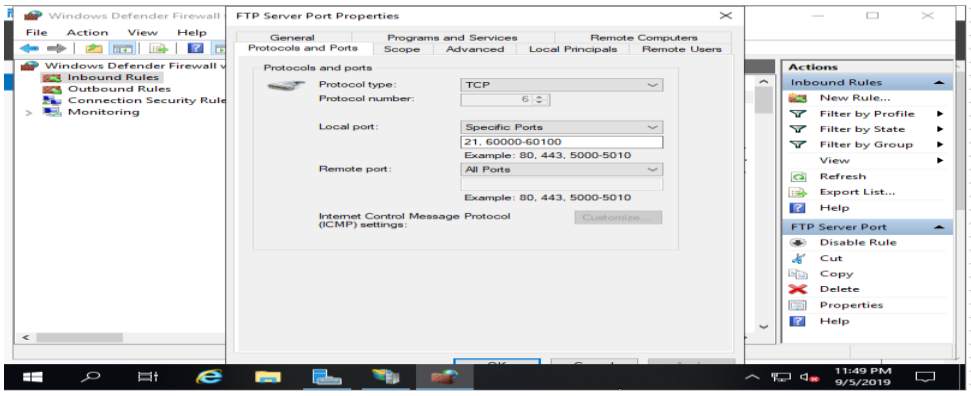
Input port range for **Data Channel Port Range** section. Specify any range that FTP Server Host does not use. (example below sets 60000 - 60100 range)



Open **Server Manager** - **Tools** - **Services** and restart FTP Service to apply changes.



Open **Server Manager** - **Tools** - **Windows Defender Firewall with Advanced Security** and add inbound rule to allow passible ports you set and also 21 port FTP Service uses like follows.



3.Enable Logging (Optional)

To enable logging for an FTP server on Windows Server, you can follow these steps to configure logging through the Internet Information Services (IIS) Manager:

- Open IIS Manager: Go to **Start** > **Server Manager** > Tools> **Internet Information Services (IIS) Manager.**
- Select Your FTP Site, In the IIS Manager, locate your FTP site under the **Sites** node.
- Configure Logging, with your FTP site selected, look for the **FTP Logging** feature in the middle pane. Double-click on **FTP Logging** to open the configuration settings.
- **Enable Logging,** Check the box for **Enable logging** if it is not already checked.
- **Choose Log File Format**, you can select the log file format. The default is usually W3C format, which is recommended for its compatibility with various log analysis tools.
- **Specify Log File Directory,** you can specify a custom directory for your log files if you wish. By default, logs are stored in: %SystemDrive%\inetpub\logs\LogFiles
- **Configure Log File Settings,** Set options for log file rollover and retention, such as:
- **Log file rollover:** Choose how often logs should be rolled over (daily, weekly, or monthly).
- **Log file size limits:** You can set limits on log file sizes to manage disk space effectively.
- Click **Apply** in the Actions pane to save your logging settings.
- **Restart FTP Service (if necessary):**
- If you made significant changes to the configuration, consider restarting the FTP service to ensure that all settings take effect:
- Open the **Services** snap-in (**Start > Administrative Tools > Services**).
- Find **Microsoft FTP Service**, right-click it, and select **Restart**.

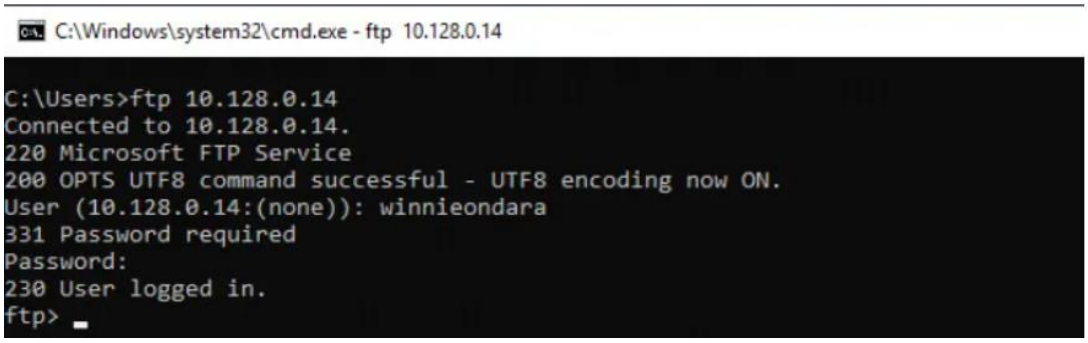
4.Test FTP server

To test if your FTP server is working as expected head over to a remote system

and launch command prompt. Next, type the command below:

ftp server-ip

You will be required to authenticate, so provide your username and password.



The output above confirms that we have been able to successfully log in.

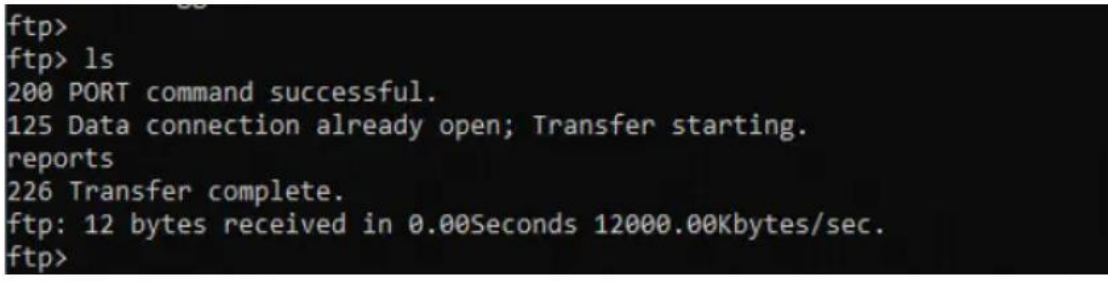
Let's try something more ambitious. We are going to create a directory and navigate into it using the commands shown:

ftp> mkdir reports

ftp> cd reports

To verify the existence of the directory, use the ls command, just as you would in a Linux system when listing files.

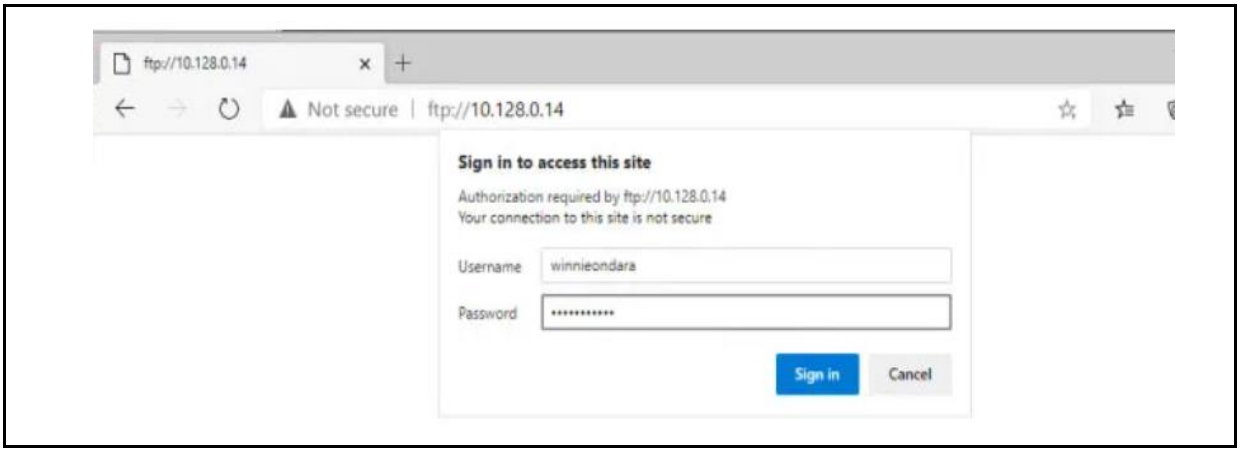
ftp> ls



Alternatively, You can head over to your browser and head over to the URL shown:

ftp://server-ip

In the authentication pop-up, provide your username and password and click on the 'Sign In' button.



Points to Remember

- **To Change User Permissions of an FTP Server**
  1. Access the server preferences in **Server Functions** > **FTP Configuration**.
  2. On the **FTP Users** tab, click the name of the user you want to modify.
  3. Click **Permissions**.
  4. Set the permissions of the user.
  5. Click **Apply**.
- **To Change User Permissions of an FTP Server**
  1. Access the server preferences in **Server Functions** > **FTP Configuration**.
  2. On the **FTP Users** tab, click the name of the user you want to modify.
  3. Click **Permissions**.
  4. Set the permissions of the user.
  5. Click **Apply**.
- **Setting Permissions on Windows FTP Server**

On a Windows Server running IIS for FTP services, permissions are managed through the file system's security settings:

Navigate to the Directory: Locate your FTP root directory (e.g., C:\inetpub\ftproot).

Modify Security Settings:

- ✓ Right-click on the directory and select **Properties**.
- ✓ Go to the **Security** tab.
- ✓ Click on **Edit** to change permissions for specific users or groups.
- ✓ Add or select a user/group and check the boxes for **Read**, **Write**, and **Modify** as needed.
- ✓ **Apply Changes:** After setting the desired permissions, click **OK** to apply changes.

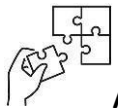
- **Passive FTP mode**

  Passive FTP mode is a method of transferring files using the File Transfer Protocol (FTP) where the client establishes both the command and data connections to the server. This mode is particularly useful in environments where firewalls or Network Address Translation (NAT) devices may block incoming connections.

- **Enable logging**

  Enable logging refers to the process of activating a logging mechanism within software applications or systems to record events, errors, and other significant information during their execution. This functionality is essential for debugging, monitoring performance, and maintaining system health.

  - **Test the FTP Server: Y**ou can use several methods depending on the tools you have at hand.



Application of learning 6.2

As network administrator you are asked to establish a web Server for hosting your school website, select all requirement and install web server within windows sever operating system based on school objectives and available materials and equipment's.
All tools, materials and equipment will be provided by the school

Indicative content 6.3: Implement FTP Server File Sharing

Duration: 3 hrs

Practical Activity 6.3.1: Choose FTP Server Software

Task:

1: Referring to the previous theoretical activities (6.2.1) as a server administrator, you are asked to go to the computer lab to perform the following: choose FTP software and set permissions to the directory.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 6.2.1 and ask clarification where necessary

5: Perform the task provided in application of learning 6.3.1

Key readings 6.3.1.: Choose FTP Server Software

1. **Choose an FTP server software**

   When choosing an FTP server software, several options stand out based on features, security, and usability. Here's a concise overview of some of the best FTP server solutions available:

   1.1. Top FTP Server Software

- **SolarWinds Serv-U Managed File Transfer (MFT):** comprehensive FTP server that offers robust encryption for secure file transfers. Supports SFTP and FTP/S for enhanced security. User-friendly interface with management tools for tracking file activity. Ideal for businesses needing compliance and secure file handling.
- **Cerberus FTP Server**: Designed for Windows, Cerberus is known for its ease of use and strong security features. Supports multiple protocols including SFTP, FTPS, and HTTPS. Features two-factor authentication and detailed user management options.
- **Complete FTP:** A versatile FTP server suitable for larger organizations with diverse file transfer needs. Supports various protocols (FTP, SFTP, FTPS) with enterprise-level options like clustering. High availability and scalability to handle extensive data transfers.
- **FileZilla Server:** An open-source solution that is popular for its simplicity and ease of use. Supports FTP and FTP over TLS for secure connections. Basic functionality suitable for internal file transfers but lacks advanced enterprise features.
- **Good Sync**: While primarily a backup solution, Good Sync can function as an FTP server with synchronization capabilities. Automated backup and synchronization

across multiple devices. Highly reliable for businesses with varied data management needs.

1.2. Considerations When Choosing an FTP Server

- Security: Ensure the server supports secure protocols like SFTP or FTPS to protect data in transit.

-Usability: Look for user-friendly interfaces that simplify management tasks.

-Support & Documentation: Reliable customer support and comprehensive documentation can ease the setup and maintenance process.

To implement FTP server file sharing, follow these steps, including choosing an FTP server software, setting permissions for a shared directory, and testing the setup.

Choose an FTP Server Software

For this implementation, we will use **FileZilla Server** due to its user-friendly interface and robust features. It supports both FTP and FTPS, making it suitable for secure file transfers.

Installation Steps:

-Download FileZilla Server: Obtain the installer from the official FileZilla website.

-Run the Installer: Follow the prompts to complete the installation.

-Launch FileZilla Server Interface: Open the application after installation.

2. Set Permissions for Shared Directory

2.1. Create a Shared Directory

- ✓ **Create a Directory**: On your server, create a directory that you want to share (e.g., C:\FTPShared).
- ✓ **Set Folder Permissions**:
  - Right-click on the folder and select **Properties**.
  - Go to the **Security** tab and set permissions for users or groups as needed (e.g., allowing read/write access).

2.2. Configure User Permissions in FileZilla

1. Open the **FileZilla Server Interface.**
2. Go to **Edit > Users.**
3. Click on **Add** to create a new user account (e.g., ftpuser).
4. Set a password for the user.
5. Under the **Shared folders** section:
   - -Click on **Add** to include your shared directory (C:\FTPShared).
   - -Set permissions:
   - **-Read:** Allows the user to view files.
   - **-Write:** Allows the user to upload files.
   - **-Delete:** Allows the user to delete files.
   - **-Create:** Allows the user to create new directories.
6. Click **OK** to save changes.

3. Test FTP File Sharing

Testing Steps:

1. Use an FTP client like **FileZilla Client,** WinSCP, or any other FTP client.
2. Connect to your FTP server using the following credentials:
    - **-Host:** Your server's IP address or hostname.
    - **-Username: ftpuser** (or whatever username you created).
    - **-Password:** The password you set for the user account.
    - **-Port:** 21 (default for FTP).
3. Once connected, navigate to the shared directory (`C:\FTPShared`).
4. Try uploading a file to ensure write permissions are correctly set.
5. Attempt to delete a file (if applicable) to confirm that delete permissions work as intended.

4. Verification

Ensure that you can view, upload, and delete files based on the permissions set for the user account. If any issues arise during testing, revisit the permission settings in both Windows and FileZilla Server.

Learning outcome 6 end assessment

Written assessment

Multiple choice question: Circle the letter corresponding to the correct answer:

1.Which role must be installed to set up an FTP server on Windows Server?

a) Web Server (IIS)
b) File and Storage Services
c) Remote Access
d) Active Directory

2.In Windows Server, which tool is used to manage IIS and FTP settings?

a) Server Manager
b) Task Manager
c) Control Panel
d) Windows Explorer

3.Which of the following authentication methods can be used for an FTP site?

a) Anonymous authentication
b) Basic authentication
c) Windows authentication
d) All of the above

4.After installing the FTP server, which command can be used to connect to the server from the command line?

a) ftp server_address
b) connect server_address
c) open server_address
d) link server_address

5.In an FTP client, what does the "Passive Mode" do?

a) Encrypts the data
b) Changes the transfer mode
c) Allows the client to open a data connection
d) Requires the server to open a data connection

6. What is the purpose of using a "home directory" for FTP users?

a) To restrict access to certain files
b) To provide a default directory for file transfers
c) To improve security
d) All of the above

7.In Windows Server, how can you restrict FTP access to specific IP addresses?

a) Change firewall settings
b) Set up IP restrictions in IIS
c) Use Windows Defender
d) Enable Anonymous FTP

8. What is the main difference between FTP and SFTP?
    a) FTP is faster
    b) SFTP uses a different protocol for secure connections
    c) FTP supports large file sizes
    d) SFTP allows more users
9. Which feature allows FTP connections to be encrypted?
    a) Basic authentication
    b) SSL/TLS
    c) Passive mode
    d) Anonymous access
10. What should be done after setting up the FTP server for testing?
    a) Change all passwords
    b) Disable the firewall
    c) Attempt to connect with an FTP client
    d) Restart the server

Practical assessment

Our school wants to hire you in the implementation of FTP server with the following tasks:

- Allow trainees and trainers to upload files as assignments to the dedicated folder called "**Assignments**" created on the server.
- Grant both "Trainees" and "Trainers." Read, write, execute permissions to the "**Assignments**" folder respectively.

References

Springall, D., Durumeric, Z., & Halderman, J. A. (2016, June). FTP: The forgotten cloud. *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 503–513. IEEE. https://doi.org/10.1109/DSN.2016.44

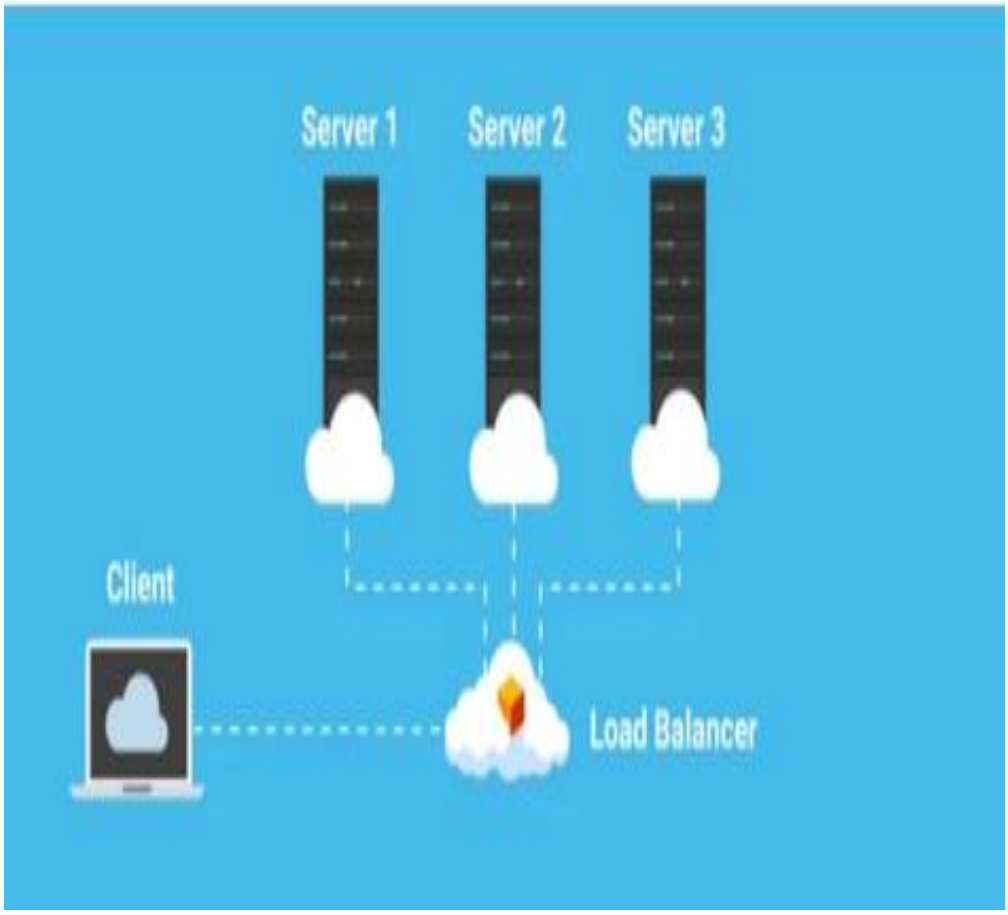
Sharapov, V. (2016). *Implementing a hybrid network deployment server for Windows and Linux*.

Panek, C. (2019). *Windows Server Administration Fundamentals*. John Wiley & Sons.

Lynn, S. (2012). *Windows Server 2012: Up and Running*. O'Reilly Media.

Krause, J. (2018). *Mastering Windows Server 2019*. Packt Publishing.V. K., & G. S. (2022, January 27). Windows-server. *Learn.microsoft.com*. Retrieved from https://www.server-world.info/en/note?os=Windows_Server_2019&p=install

Server, W. (2019, October 4). Note?os=Windows_Server_2019&p=hyper-v&f=1. *Server World*. Retrieved from https://www.server-world.info/en/note?os=Windows_Server_2019&p=hyper-v&f=1


Server 1
Server 2
Server 3
Client
Load Balancer

Indicative contents
7.1 Description of Load balancer Installation
7.2 Configuration of Windows Server Load Balancer
7.3 Management of Load Balancing Cluster

Key Competencies for Learning Outcome 7: Perform Load Balancing

Knowledge	Skills	Attitudes
• Description of load balancing concepts. • Identification of methods and technologies.	• Installing load balancing. • Installing windows software OS. • Configuring window server load balancer. • Maintaining load balancer cluster	• Being Flexible • Adaptability • Teamwork ability • Persistence • Time management

Duration: 10 hrs

Learning outcome 7 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify and describe properly load balancer.
2. Identify correctly methods and technologies.
3. Perform clearly installation of load balancer.

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS ● Router ● switch	● Modem ● Route ● VMware workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD ● USD	● Electricity ● Cables ● Internet

Indicative content 7.1: Description of Load Balancer Installation

Duration: 4 hrs

Theoretical Activity 7.1.1: Description of load balancer installation

Tasks:

1: Answer the following questions related to the Description of load balancing Key Concepts:

i. Define the following terms:
   a) Load balancing
   b) DNS-based load balancing
   c) Hardware load balancer
   d) Software load balancer

ii.Differentiate the following terms used in function:
   a) Layer 4 load balancing
   b) Layer 7 load balancing

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 7.1.1

Key readings 7.1.1.: Description of load balancer installation

1. Load balancing

Load balancing is the process of distributing traffic among multiple servers to improve a service or application's performance and reliability.

2. DNS-based load balancing

DNS-based load balancing is a specific type of load balancing that uses the DNS to distribute traffic across several servers.

3. **Hardware load balancers**

These are specifically designed to provide the best load balancing based on the task they are intended to address.

4. **Software load balancers**

These are the applications that can be installed and provisioned on more traditional compute resources like servers.

5. **Layer 4 load balancing**

It manages traffic based on network information such as protocols and application ports without requiring visibility into actual content of messages.

6. **Layer 7 load balancing**

It operates at the application layer of the OSI model, allowing for more sophisticated traffic management compared to Layer 4 load balancing.

Practical Activity 7.1.2: Perform load balancing installation

Task:

1. You are requested to go to the computer lab to install load balancing.
2: Present the procedures of all step performed during selection
3: Present your work to the trainer and whole class.
4: for more information read key reading 7.1.1 and ask clarification where necessary
5: Perform the task provided in application of learning 7.1

Key readings 7.1.2 Perform load balancing installation

To perform a load balancing installation, you need to follow a structured approach that involves setting up the necessary infrastructure, configuring the load balancer, and ensuring that your services are properly integrated. Here's a step-by-step guide:

Step 1: **Hardware Load Balancers**: Physical devices that manage traffic distribution.

- **Software Load Balancers**: Applications that run on standard servers or in the cloud.
- **Virtual Load Balancers**: Combine features of both hardware and software solutions.

Step 2: Prepare Your Environment

1. **Server Pool**: Ensure you have a pool of servers (server farm) ready to handle incoming requests.
2. **Load Balancer Selection**: Choose between hardware or software load balancers based on your needs and budget.

Step 3: Enable Load Balancing Feature

Using Command Line Interface (CLI)

To enable load balancing via CLI, execute the following commands:

```
bash
enable ns feature LB
show ns feature
```

This will enable the load balancing feature on your device.

Using Graphical User Interface (GUI)

1. Navigate to **System > Settings**.
2. In the **Configure Basic Features**, select **Load Balancing** to enable it

Step 4: Configure Services

1. **Create Services**: For each application server in your pool, create a service that specifies:

- Service name
- IP address
- Port number
- Type of data served (e.g., HTTP, TCP)

2. If you want to identify servers by name rather than IP, create server objects first.
3. **Set Up Health Monitoring**: Bind appropriate health monitors to your services (e.g., TCP default for TCP services) to ensure they are operational.

Step 5: Create Load Balancing Virtual Server

1. **Create a Virtual Server**: This acts as the entry point for client requests.
2. **Bind Services**: Attach each configured service to the virtual server you created.

Step 6: Verify Configuration

After completing the setup:

- Check that all services are correctly bound and operational.
- Use monitoring tools or logs to ensure traffic is being distributed as expected.

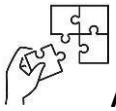
Step 7: Optimize Load Balancing Strategy

Choose an appropriate load balancing algorithm based on your application needs:

- **Round Robin**: Distributes requests sequentially across servers.
- **Least Connections**: Directs traffic to the server with the fewest active connections.
- **IP Hashing**: Ensures users are consistently directed to the same server based on their IP address for session persistence
- **Test Load Balancing:** To test network load balancing, connect a browser to the cluster IP address, for example: http://192.168.10.10. Refresh the screen multiple times. If the cluster is operating successfully, web pages from different machines in the cluster appear after each refresh. Start an Enterprise Server for.

Points to Remember

- Ensure that all servers in the NLB cluster have the same configuration and that the NLB feature is installed on each server.
- Monitor the performance and health of the cluster using the NLB Manager or PowerShell commands for ongoing management.



Application of learning 7.1.

BTEC LTD is a software development company located in Rusizi district, they want to manage all computers connected to the single server, due to different activities that they have, you are hired as system Administrator who is responsible for setting the working environment by installing and configuring the server load balancer, and set all other necessary settings in order to be ready for installation of server load balancer, testing the server.

All tools, materials and equipment will be provided by the company.

Indicative content 7.2: Configuration of Windows Server Load Balancer

Duration: 5 hrs

Theoretical Activity 7.1.2: Description of load balancing

Tasks:

1: Answer the following questions related to the Description of load balancing Key Concepts:

i. What do you understand by the Load balancing?
ii. What are the types of load balancing
iii. What are benefits of load balancing

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 7.1.2.

Key readings 7.1.2 Description of load balancing

Load balancing is the process of distributing traffic among multiple servers to improve a service or application's performance and reliability.

This process enhances the performance, reliability, and availability of applications and services.

Key Aspects of Load Balancing

1. **Purpose**:

Load balancing aims to optimize resource utilization, improve response times, and increase the availability of applications. By evenly distributing traffic, it prevents any single server from becoming a bottleneck, which can lead to performance degradation or downtime.

2.How It Works:

- A load balancer acts as an intermediary between clients and servers. When a client makes a request, the load balancer determines which server is best suited to handle that request based on various algorithms and criteria. It then forwards the request to the selected server.

3.**Types of Load Balancers**:

Load balancers can be hardware-based or software-based.

- **Hardware load balancers** are dedicated devices that provide high performance but can be expensive
- **Software load balancers** run on standard servers or virtual machines and are more flexible and scalable.

4.Load Balancing Algorithms:

Various algorithms dictate how requests are distributed among servers:

- **Round Robin**: Distributes requests sequentially across servers.
- **Least Connections**: Directs traffic to the server with the fewest active connections.
- **Least Response Time**: Chooses the server with the lowest average response time.
- **IP Hash**: Uses the client's IP address to determine which server will handle the request, ensuring session persistence.

5.Benefits:

- The primary benefits of load balancing include improved application performance, increased reliability through redundancy, better resource utilization, enhanced user experience due to faster response times, and scalability to handle varying levels of traffic.
- **In summary**, load balancing is essential for modern applications that require high availability and performance.
- load balancing helps organizations meet user demands while maintaining service quality.

Practical Activity 7.2.1: Installing NLB server manager feature

Task:

1: Referring to the key reading 7.2.1, As a server administrator, you are asked to go to the computer lab to perform the following: install NLB server manager.
2: Apply safety precautions
3: Present your work to the trainer and whole class.
4: Read key reading 5.4.2 and ask clarification where necessary
5: Perform the task provided in application of learning 7.2

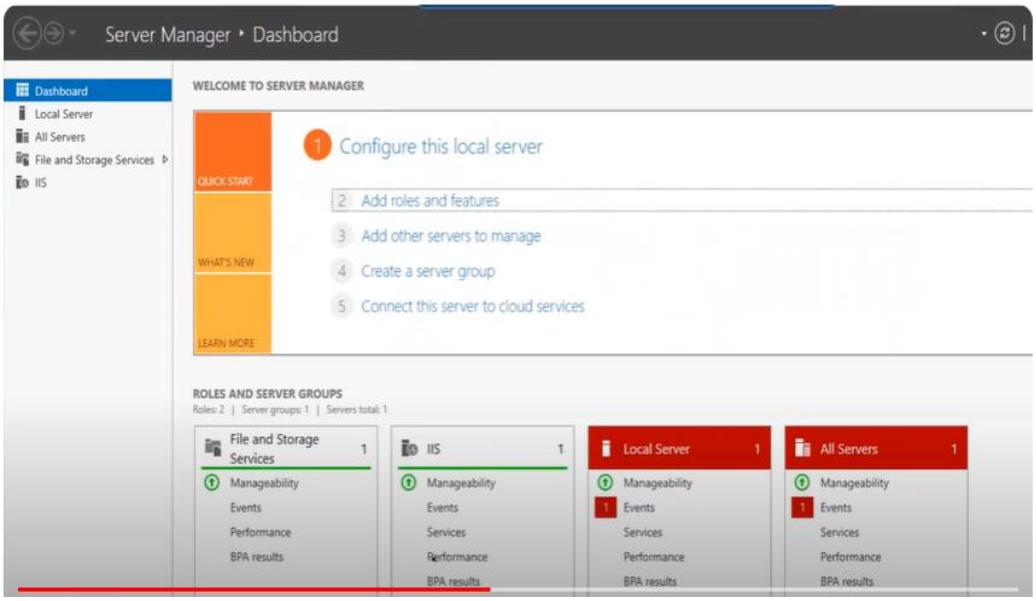
Key readings 7.2.1: Installing NLB server manager feature

To install the Network Load Balancing (NLB) feature using Server Manager on Windows Server, follow these detailed steps:

Step-by-Step Installation of NLB Feature

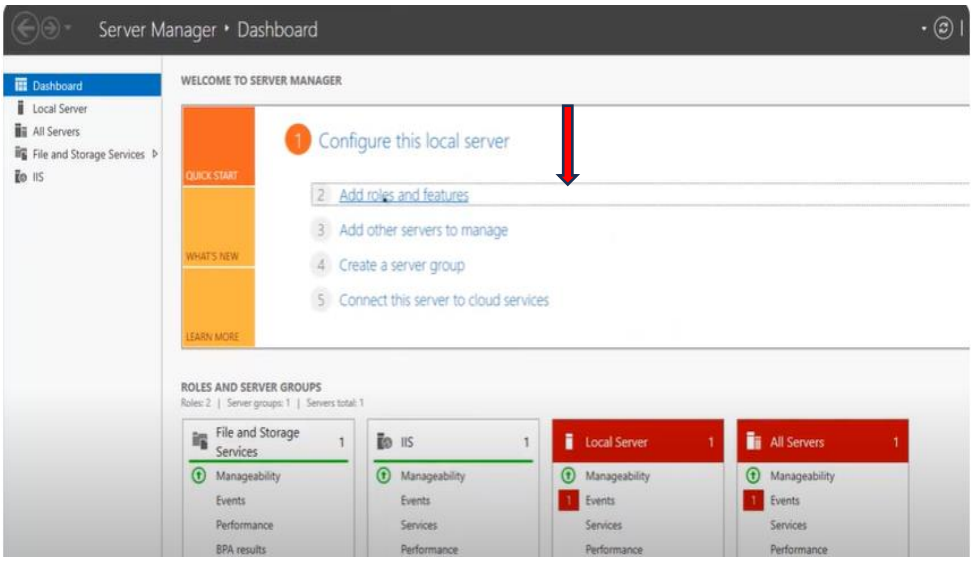
3. **Open Server Manager**:

- Click on the **Start** menu and select **Server Manager**.



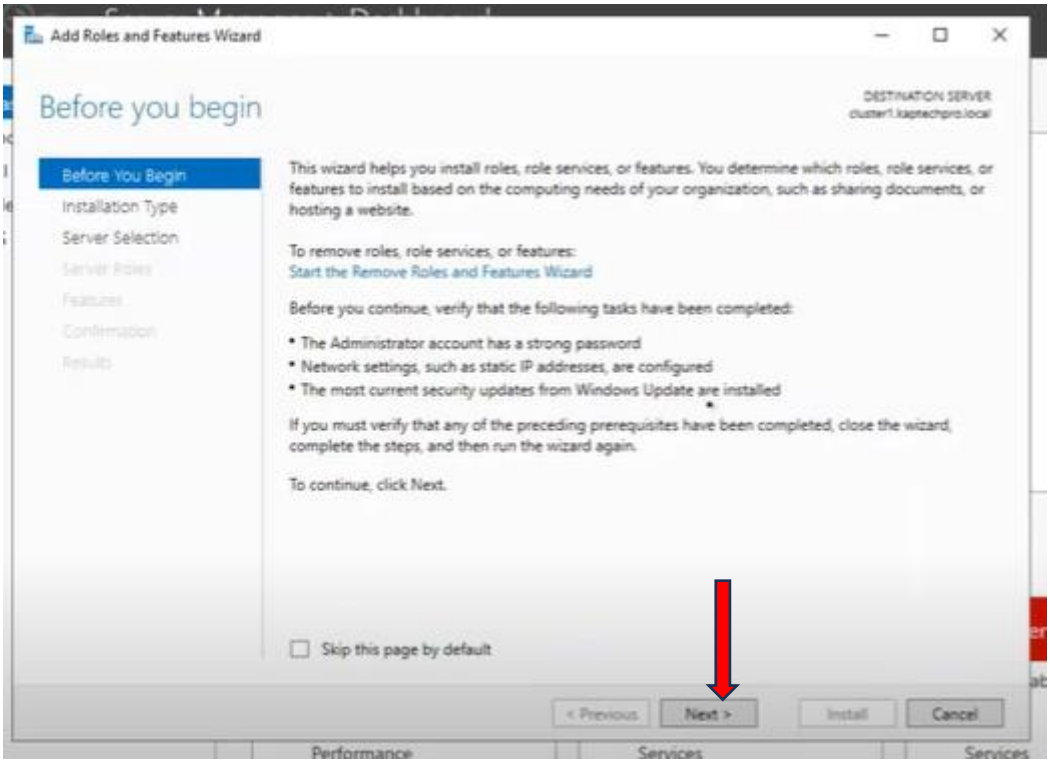
2.Add Roles and Features:

- Select **Add Roles and Features** from the dropdown menu.



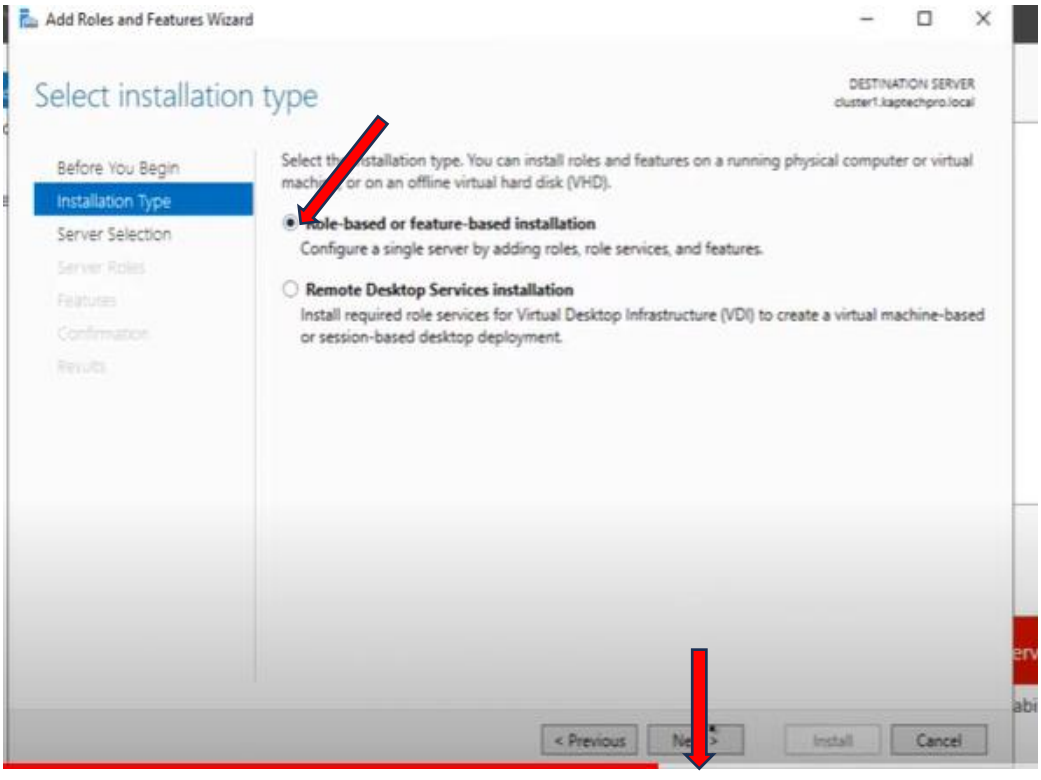
3.Before You Begin:

- On the "Before you begin" page, click **Next** to continue.



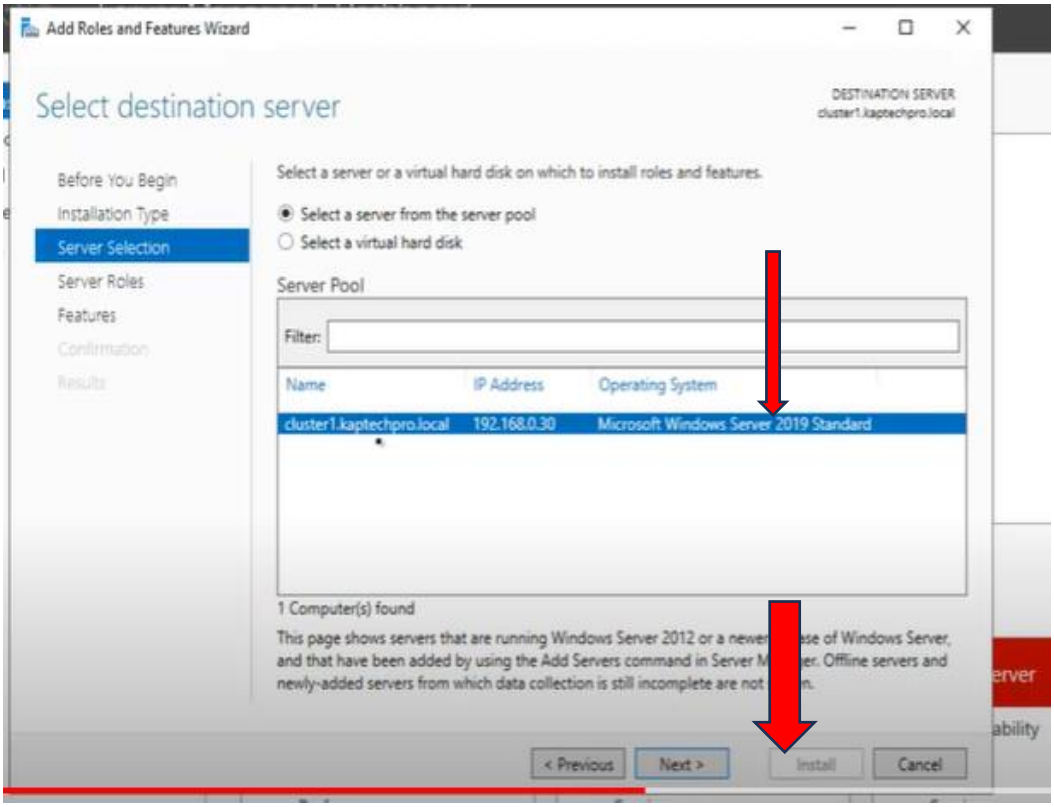
4.Installation Type:

- Choose **Role-based or feature-based installation** and click **Next**.



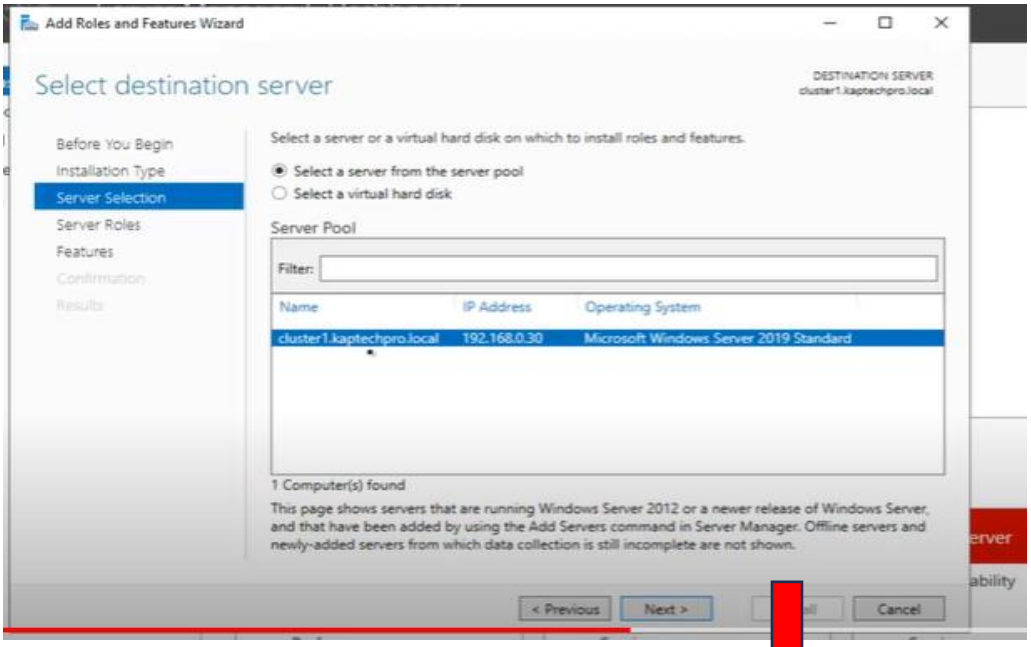
5.Select Destination Server:

- Select the server from the server pool where you want to install the NLB feature, then click **Next**.



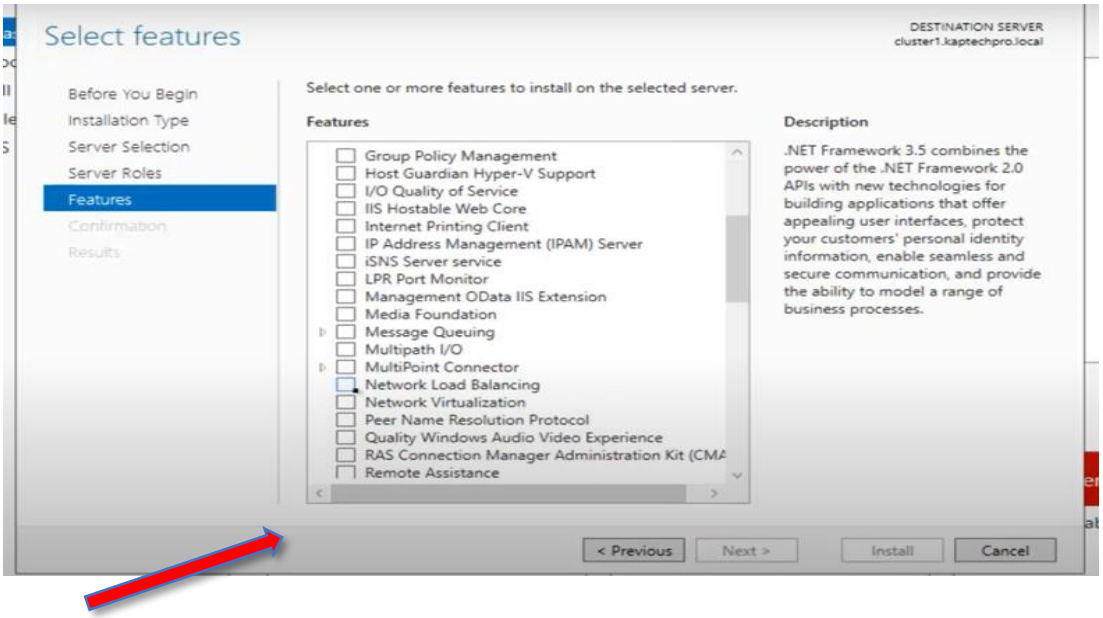
6.Server Roles:

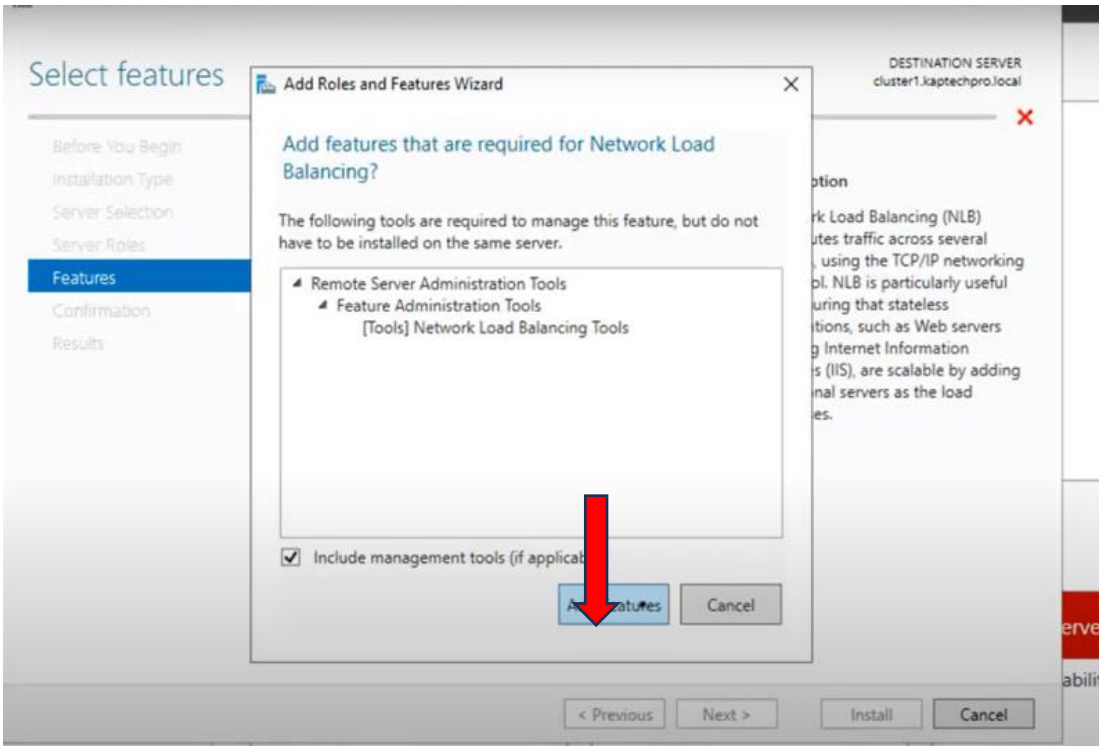
- On the "Select server roles" page, simply click **Next** (NLB is not a server role).



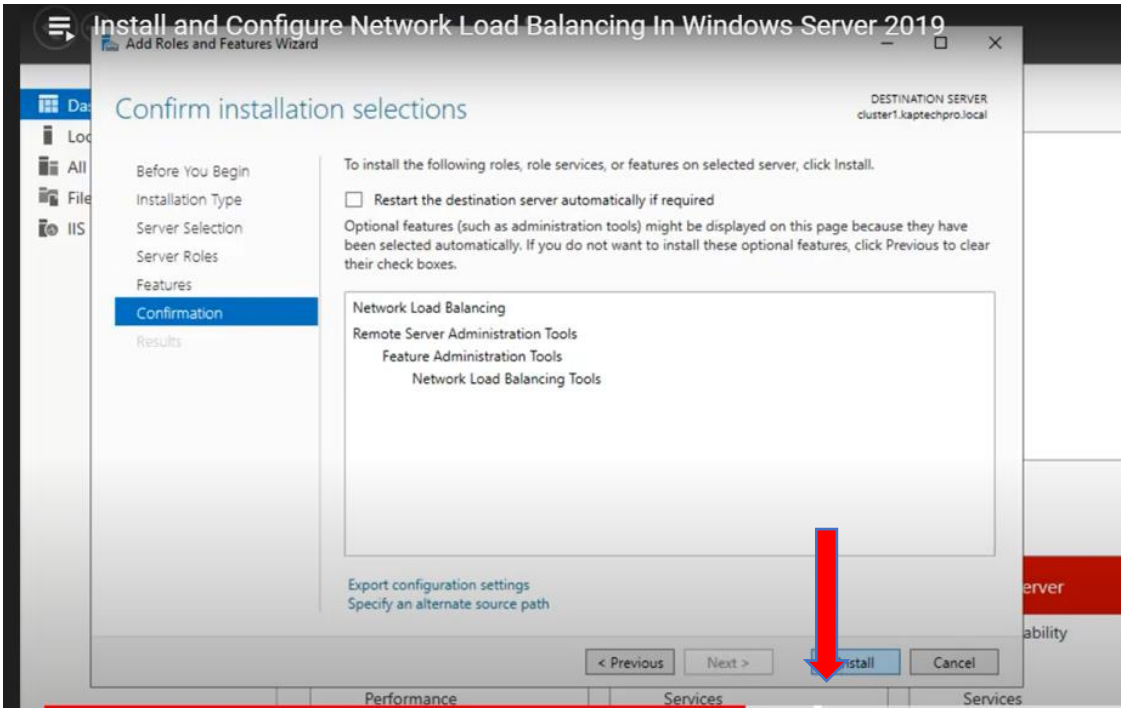
7.Select Features:

- On the "Select features" page, scroll down and check the box for **Network Load Balancing**.
- A new window will pop up asking to add features required for NLB; click on **AddFeatures, then click Next.**





8.Click install

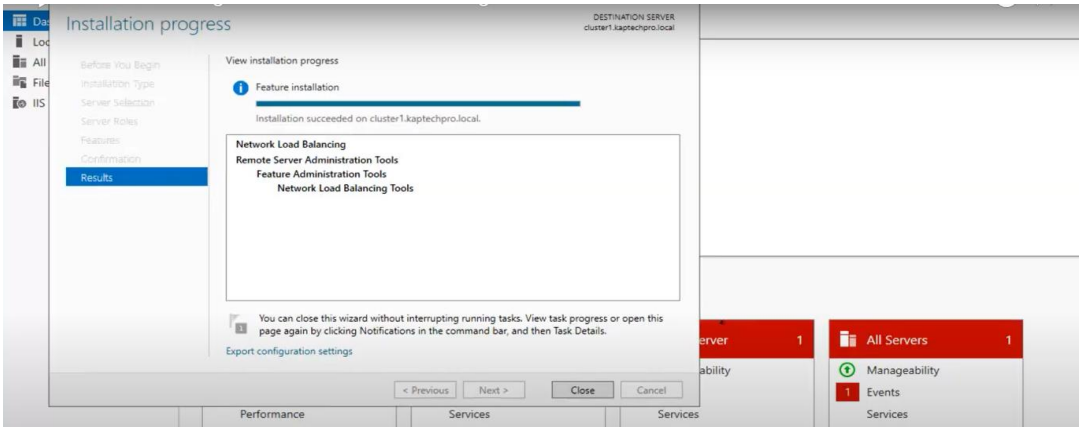


9.**Installation Progress**:

- Wait for the installation to complete. This may take a few moments.

9.**Close Installation Wizard**:

- Once the installation is finished, click on **Close** to exit the wizard.

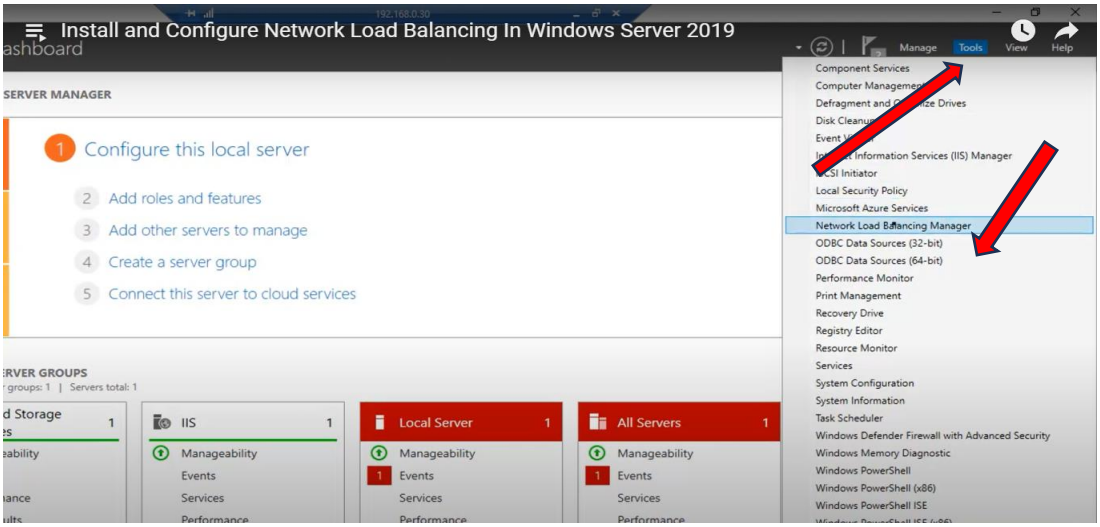


✓ Configure Network Load Balancing Manager

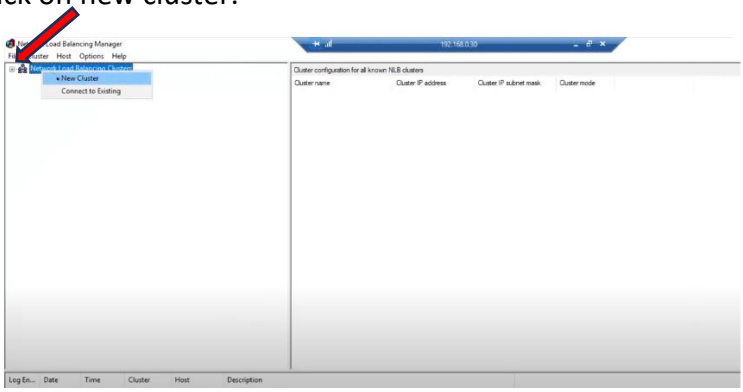
- Start the Cluster

A cluster: refers to a group of servers working together on one system to provide users with higher availability. These clusters are used to reduce downtime and outages by allowing another server to take over in an outage event.

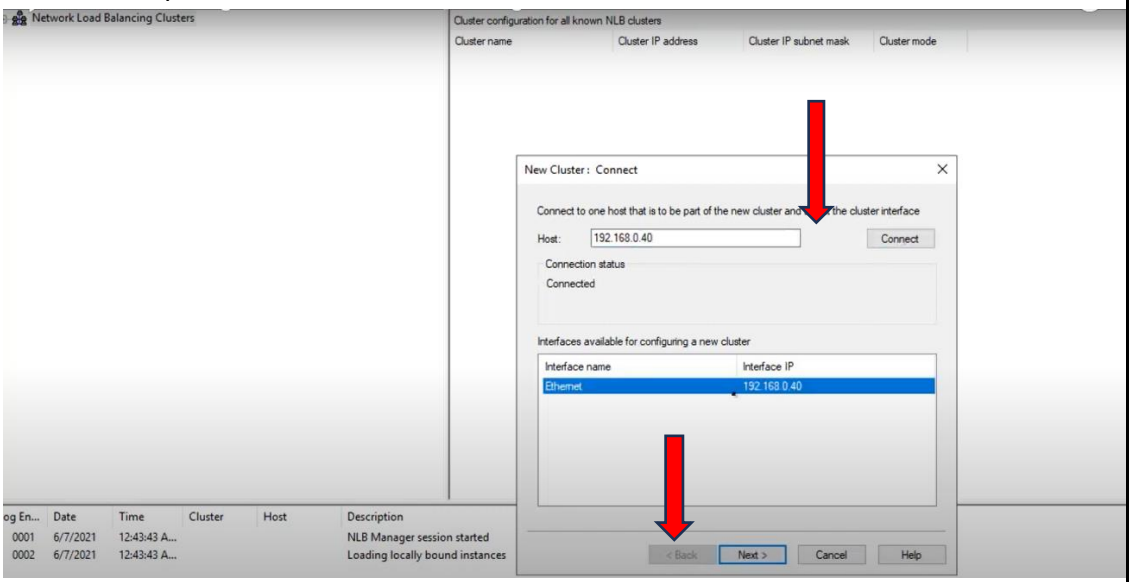
Step 1:click on Tools and select network load balancing manager.



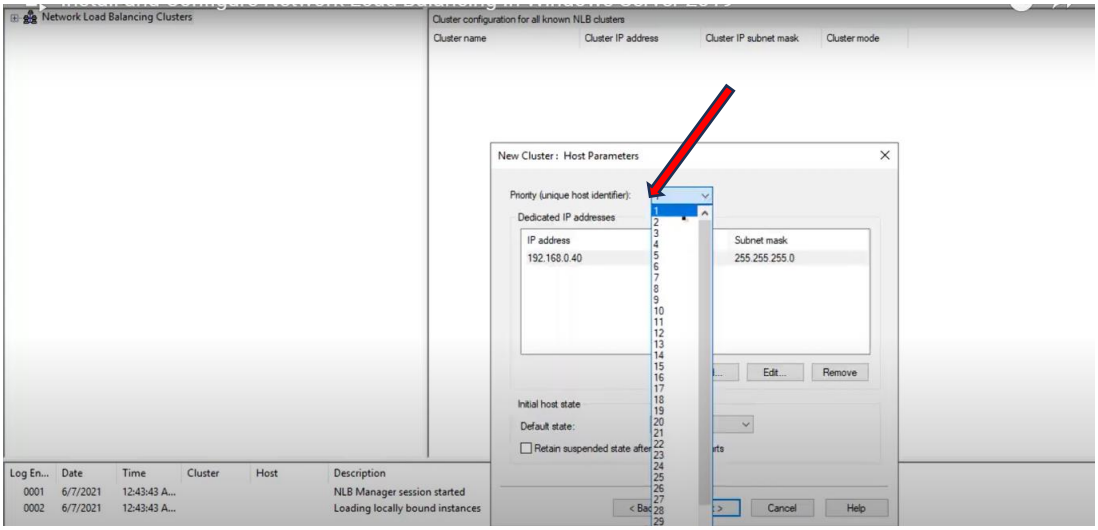
2.maximize opened page and right click on network load balancing cluster and click on new cluster.



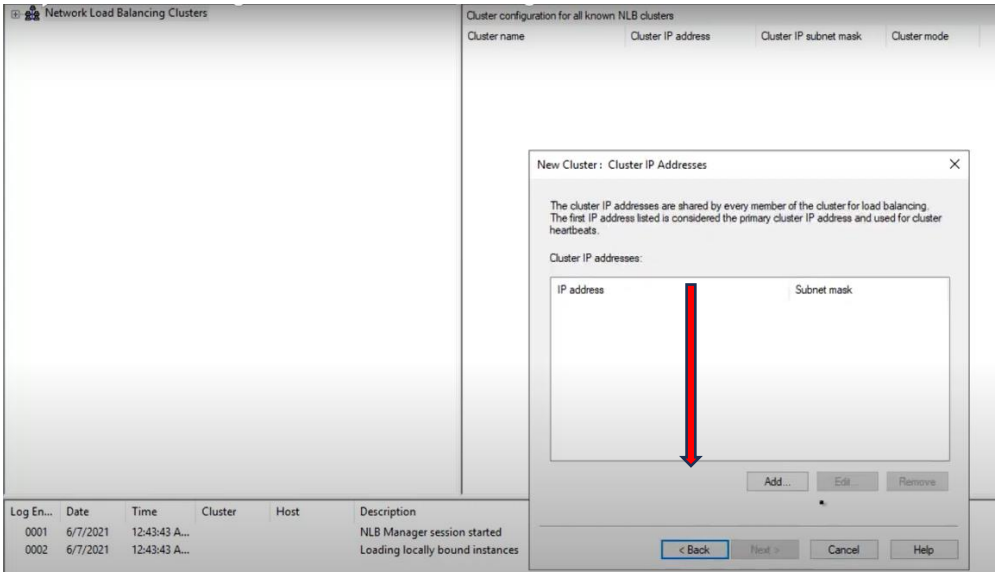
3.Enter the ip address of node click connect and next.

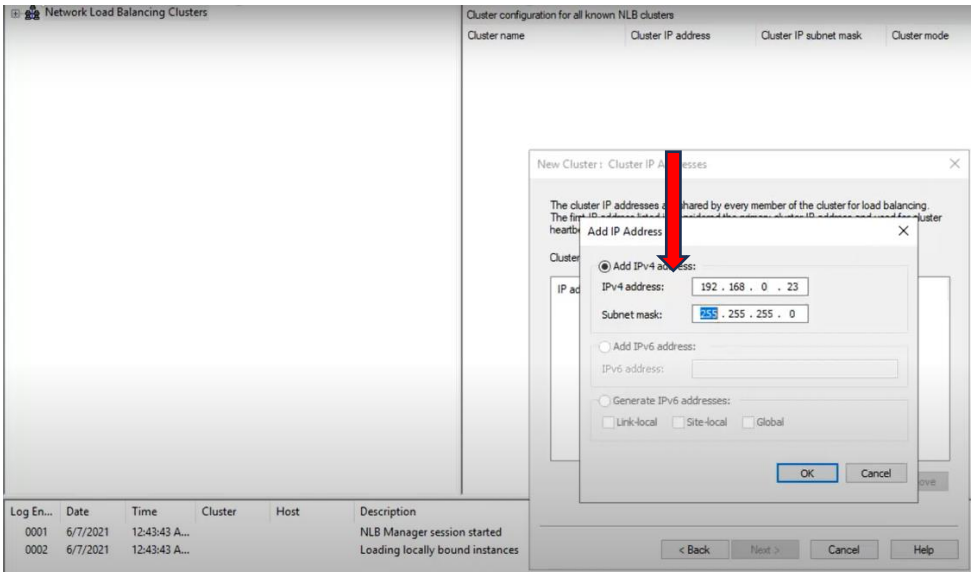


4.set priority and click next

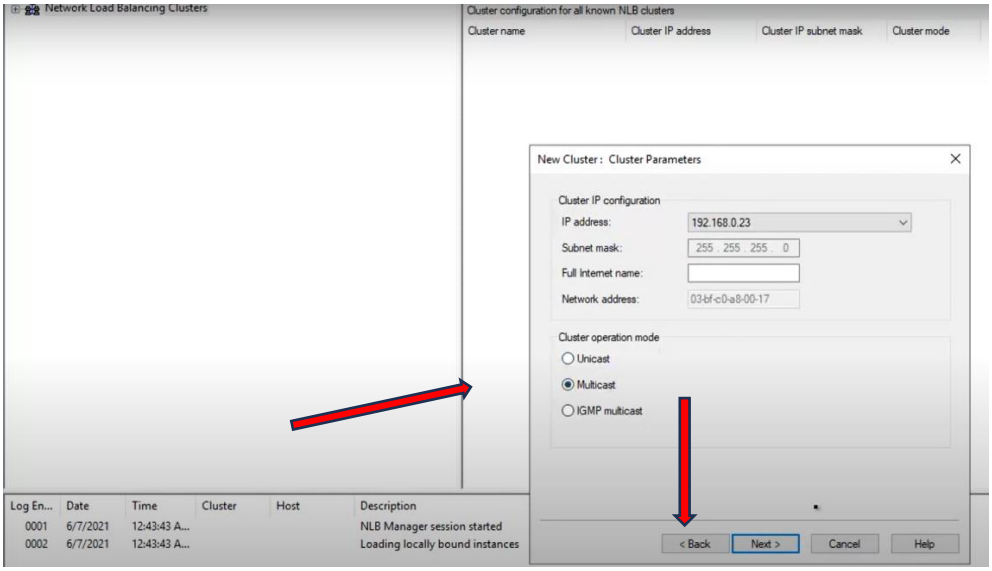


5.click add to assign new ip address to a cluster and click ok and click next.

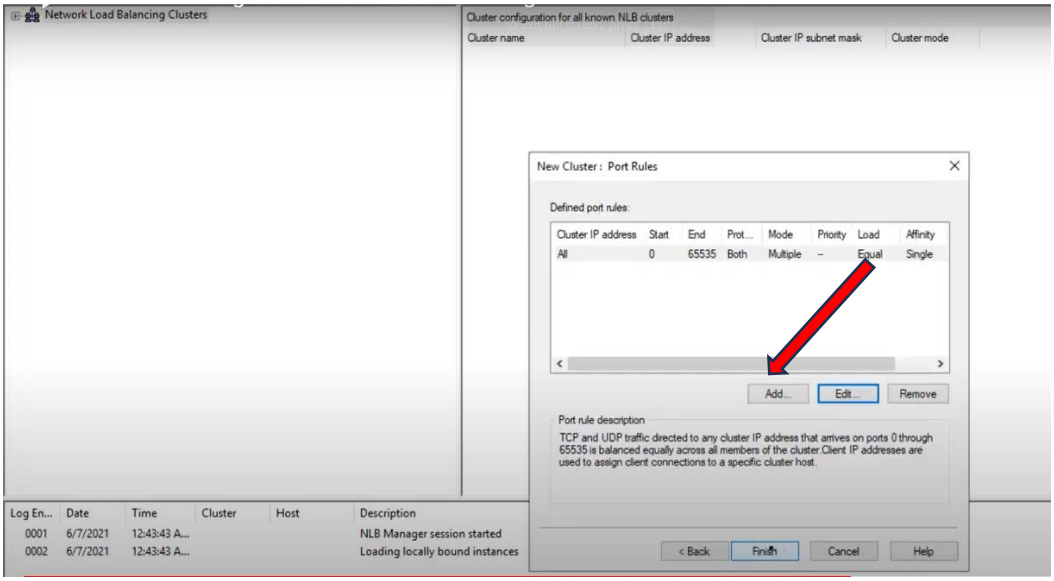




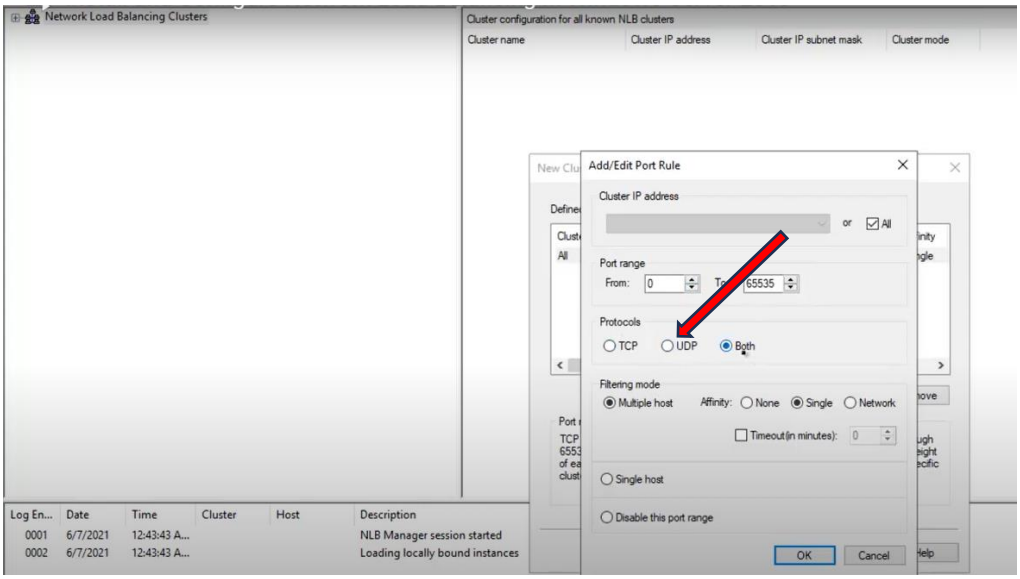
7.set cluster operation mode as **multicast** and click next.



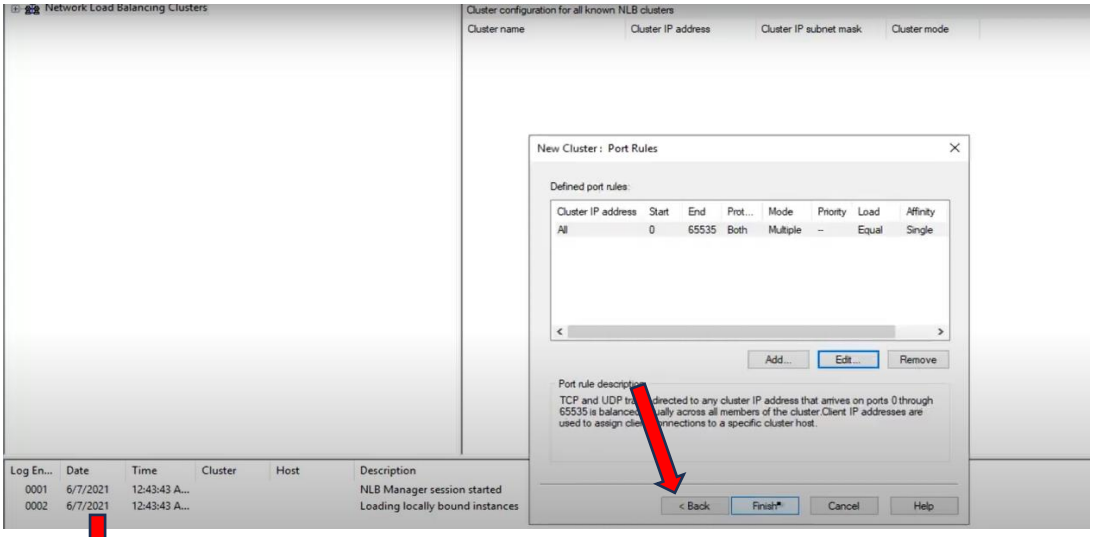
8.set port rules and click on edit



9.choose protocols by default use **both** ,click ok and finish.

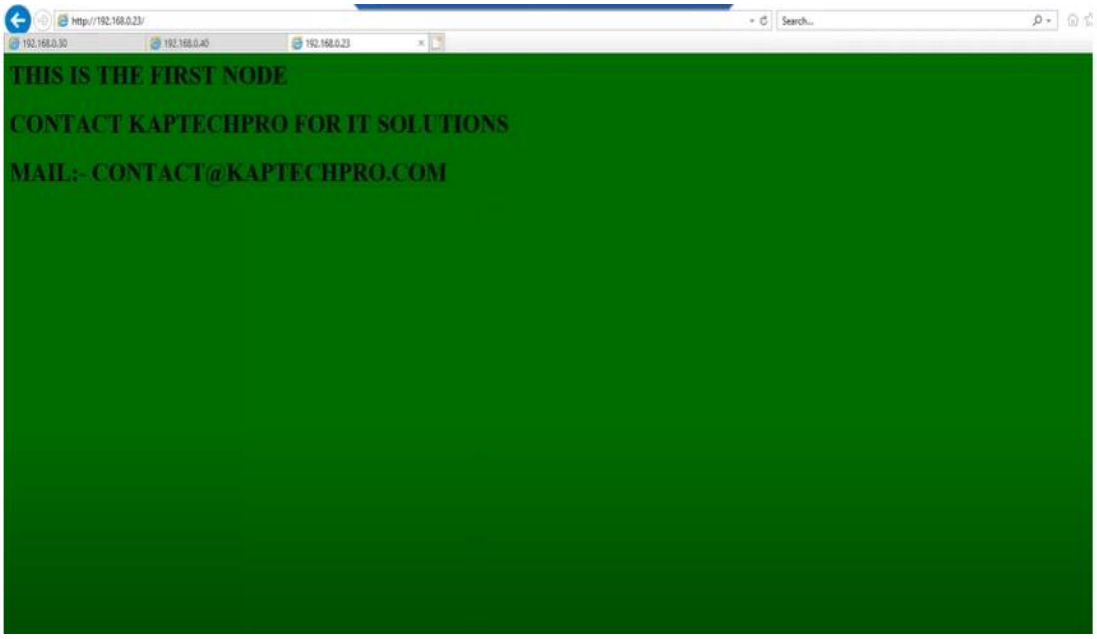


10.After selecting protocols and set port range click finish.



•Test Load Balancing

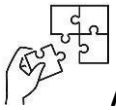
To test network load balancing, connect a browser to the cluster IP address, for example: http://192.168.0.23. Refresh the screen multiple times. If the cluster is operating successfully, web pages from different machines in the cluster appear after each refresh. Start an Enterprise Server for.



Points to Remember

- Make Ensure that all servers in the NLB cluster have the same configuration and that the NLB feature is installed on each server.
- After network load balancing (NLB) installation process, verify installation completion.

- Monitor the performance and health of the cluster using the NLB Manager or PowerShell commands for ongoing management.
- While testing NLB enables each host to detect and receive incoming TCP/IP traffic.
- Remember to connect a browser to the cluster IP address, for example: http://192.168.0.23.
- Do not forget to refresh the screen multiple times. If the cluster is operating successfully, web pages from different machines in the cluster appear after each refresh.
- Do not forget to set port range and selecting cluster operation mode during configuration of NLB.



Application of learning 7.2

Suppose that your school needs to install and configure load balancing, network load balancing based on windows server as a trainee in networking and Internet Technology you are required for performing this activity as it is required.
All tools, materials and equipment will be provided by the company.

Indicative content 7.3: Management of Load Balancing Cluster

Duration: 1 hr

Theoretical Activity 7.1.3: Management of load balancing cluster

Tasks:

1: Answer the following questions related to the Description of load balancing Key Concepts:

i. What do you understand the following term:

a) Capacity planning
b) Configuration
c) Disaster Recovery
d) Security
e) Maintenance
f) Scaling
g) monitoring

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 7.1.3

Key readings 7.1.3: Management of load balancing cluster

✓ **capacity planning** is a crucial aspect of managing a load balancing cluster. It enables organizations to prepare for future demands while optimizing current resource utilization, ensuring that applications remain responsive and available under varying load conditions.

Importance of Capacity Planning in Load Balancing

- **Performance Optimization**: Ensures that the load balancing cluster can efficiently handle traffic without delays or downtime.
- **Cost Efficiency**: Helps avoid unnecessary expenditures by aligning resource allocation with actual needs.
- **High Availability**: Enhances system reliability by ensuring that sufficient resources are available to manage failures or unexpected surges in traffic.

✓ Configuration

you can effectively configure and manage a load balancing cluster that enhances application performance and reliability.

✓ Disaster Recovery

Disaster Recovery is an organization's plan to protect its IT systems and data from disasters and recover quickly to minimize downtime and losses.

✓ **Security**

Security: refers to every aspect of protecting an organization and its employees and assets against cyber threats.

✓ **Maintenance**

By implementing a comprehensive maintenance strategy for load balancing clusters, organizations can ensure high availability, optimal performance, and efficient resource utilization. Regular health checks, capacity planning, software updates, and performance monitoring are key components that contribute to the overall reliability of applications served by the cluster.

✓ **Scaling**

Scaling refers to the ability of a system, application, or infrastructure to handle increased loads or demands by adjusting its resources accordingly.

✓ **Monitoring**

monitoring in a load balancing cluster is vital for maintaining optimal performance and reliability.

•It involves health checks, performance metrics analysis, alerting mechanisms, and user experience assessments to ensure that services remain available and responsive to user demands.

✓ **Importance of Monitoring in Load Balancing Clusters**

High Availability: Continuous monitoring ensures that any server failures are quickly detected and addressed, maintaining service availability.

Performance Optimization: By analyzing performance metrics, organizations can make informed decisions about scaling resources or optimizing configurations to enhance application performance.

Cost Efficiency: Effective monitoring can help identify underutilized resources, allowing organizations to optimize costs by scaling down unnecessary capacity.

Improved Troubleshooting: With detailed logs and real-time alerts, administrators can quickly pinpoint issues and resolve them before they impact users.

Points to Remember

- Configuration
  you can effectively configure and manage a load balancing cluster that enhances application performance and reliability.
- capacity planning
  It is a crucial aspect of managing a load balancing cluster
- Security
  It refers to every aspect of protecting an organization and its employees and assets against cyber threats.

- Maintenance
  for load balancing clusters, organizations can ensure high availability, optimal performance, and efficient resource utilization.
- monitoring in a load balancing cluster is vital for maintaining optimal performance and reliability.
- Scaling
  It refers to the ability of a system, application, or infrastructure to handle increased loads or demands by adjusting its resources accordingly.

Learning outcome 7 end assessment

Written assessment

I. Multiple choice question: Circle the letter corresponding to the correct

1. What is the primary purpose of load balancing.?
    a) Writing JavaScript code
    b) Debugging the application
    c) Load balancing is the process of distributing traffic among multiple servers to improve a service or application's performance and reliability.
    d) Creating a user interface
2. Read the following statements and choose the right answer?
    a) Software load balancers are applications that can be installed and provisioned on more traditional compute resources like servers.
    b) Software load balancers operate at the application layer of the OSI model, allowing for more sophisticated traffic management compared to Layer 4 load balancing.
    c) Software load balancers are specifically designed to provide the best load balancing based on the task they are intended to address.

3. Which of the following best defines NLB?
    a) It is a tool used by system administrators to detect when a cyberattack has occurred.
    b) It is a tool used for performing routine maintenance on servers.
    c) It is a Windows Server 2016 feature that is used to distribute network traffic across a cluster of servers.
    d) is a crucial technology used to distribute network traffic across multiple servers, enhancing both availability and scalability.

4. Which of the following best defines Server Manager?
    a) Server Manager is a vital management console in Windows Server, designed to help IT professionals manage both local and remote servers effectively.
    b) Server Manager is a management protocol in Windows Server, designed to help IT professionals manage both local and remote servers effectively.
    c) Server Manager is a Windows Server 2016 feature that is used to distribute network traffic across a cluster of servers.

5. Which is the types of load balancing depends on what you have seen?
    a) Hardware load balancers and Software load balancers
    b) Hyper-v and virtualization
    c) Least Connections and Least Response Time
    d) None of the above.

6.Which of the following is not Methods and technologies of load balancing?
    a) Dhcp
    b) DNS-based load balancing

c) Hardware load balancer
d) Software load balancer

II. Read the following statement related to perform load balancing in column A and B and write the letter corresponding to the correct answer

Answer	Column A	Column B
……..	**1.** is a crucial aspect of managing a load balancing cluster	A. PerformanceOptimization
……..	2. Ensures that the load balancing cluster can efficiently handle traffic without delays or downtime.	B. capacity planning
……	3. Helps avoid unnecessary expenditures by aligning resource allocation with actual needs.	C. Disaster Recovery
……	4. is an organization's plan to protect its IT systems and data from disasters and recover quickly to minimize downtime and losses.	D.Cost Efficiency:
……	5. refers to every aspect of protecting an organization and its employees and assets against cyber threats.	E. Security
		F. you can effectively configure and manage a load balancing cluster that enhances application performance and reliability

III. Read the following statement related to perform load balancing and answer True if the statement is correct and False if the statement is wrong

1.Both TCP and UDP are protocols used in installation of Network Load Balancing?

a) False
b) True

2.In installation of load balancing is it possible to set port range and select cluster operation mode.

a) True
b) False

3. NLB is not technology used to distribute network traffic across multiple servers, enhancing both availability and scalability.

a) True
b) False

4.To set cluster operation mode as multicast in installation of load balancing is it possible?

a) False
b) True

5.While testing NLB enables each host to detect and receive incoming TCP/IP traffic.

a) True
b) False

Practical assessment

ABC is a software development company located in Nyanza district, they want to manage all computers connected to the single server, due to different activities that they have, you are hired as system Administrator who is responsible for setting the working environment by installing and configuring the server load balancer, and set all other necessary settings in order to be ready for installation of server load balancer, testing the server.

All tools, materials and equipment will be provided by the company.

References

Shimonski, R. (2003). *Windows Server 2003: Clustering & Load Balancing*. McGraw-Hill/Osborne.

Bourke, T. (2001). *Server Load Balancing*. O'Reilly Media.

Bryhni, H., Klovning, E., & Kure, O. (2000). A comparison of load balancing techniques for scalable web servers. *IEEE Network, 14*(4), 58–64. https://doi.org/10.1109/65.857190

Ibrahim, I. M., Ameen, S. Y., Yasin, H. M., Omar, N., Kak, S. F., Rashid, Z. N., ... & Ahmed, D. M. (2021). Web server performance improvement using dynamic load balancing techniques: A review. *System, 19*, 21.

K., & G. S. (2022, January 27). Windows-server. *Learn.microsoft.com*. Retrieved from https://www.server-world.info/en/note?os=Windows_Server_2019&p=install

Krause, J. (2018). *Mastering Windows Server 2019*. Packt Publishing.

Server, W. (2019, October 4). Note?os=Windows_Server_2019&p=hyper-v&f=1. *Server World*. Retrieved from https://www.server-world.info/en/note?os=Windows_Server_2019&p=hyper-v&f=1

Indicative contents
8.1 Deployment of Windows Server Update Service
8.2 Configure WSUS
8.3 Perform Server Backup
8.4 Perform Troubleshooting
8.5 Perform Migration

Key Competencies for Learning Outcome 8: Perform Server Maintenance

Knowledge	Skills	Attitudes
● Description of windows server update service	● Installing necessary roles and features. ● Configuring WSUS. ● Performing server backup ● Performing troubleshooting ● Performing migration	● Being Flexible ● Being persistent ● Having Adaptability ● Having teamwork ability.

Duration:15 hrs

Learning outcome 8 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify and describe properly Windows server update service based on system requirements
2. Identify correctly necessary roles and features.
3. Perform clearly installation of roles and features.
4. Perform clearly migration according to the organization needs
5. Perform clearly troubleshooting based on server performance.
6. Perform clearly server backup according to the backup plan.

Resources

Equipment	Tools	Materials
● Projector ● Computer ● UPS ● Router ● Switch	● Modem ● Route ● VMware workstation ● Windows server 2016 OS ● Windows client OS ● Bootable device software ● DVD ● USD	● Electricity ● Cables ● Internet

Indicative content 8.1: Deployment of Windows Server Update Service

Duration:4 hrs

Theoretical Activity 8.1.1: Description of Windows server update service

Tasks:

1: Answer the following questions:

i. What do you understand by the following term?

a) Windows server update service

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 8.1.1

Key readings 8.1.1.: Description of Windows server update service

1.**Windows server update service**

This is a Microsoft tool that enables IT administrators to manage the distribution of updates released by Microsoft to computers in a corporate environment. It serves as a local update management system, where admins can decide which updates are approved for installation on networked devices. Here's a detailed overview:

Key Features:

Centralized Management:

WSUS allows administrators to manage the deployment of updates for Windows operating systems, Microsoft Office, and other Microsoft software products from a central server.

Administrators can approve, schedule, and control the distribution of updates to individual computers or groups of computers.

2.Update Categories:

- It supports updates for various categories such as critical updates, security updates, service packs, feature packs, and drivers.
- Administrators can select which types of updates they want to deploy based on their relevance and importance.

3.Control over Deployment:

- Administrators can test updates in a controlled environment before deploying them network-wide, ensuring that updates do not interfere with critical business functions.

- It allows granular control by offering the ability to approve or decline updates, automatically approve certain update types, and schedule installations.

4.Network Efficiency:

- By downloading updates from Microsoft once and distributing them locally, WSUS reduces bandwidth consumption, as each client does not need to connect to the internet for updates.

5.Reporting:

WSUS provides detailed reports on the status of updates, helping administrators track which updates have been installed and on which machines.

How WSUS Works:

Synchronization with Microsoft Update:

- WSUS connects to the Microsoft Update server to download the latest updates.
- Administrators can choose to synchronize all available updates or only those relevant to their environment.

Client-Side Interaction:

- Client computers are configured to contact the WSUS server instead of Microsoft's online update service for updates.
- Based on the policies set by the administrator, clients download and install approved updates.

Deployment and Monitoring:

Administrators can monitor the status of updates and generate reports to ensure that updates are successfully installed and that no issues arise during the process.

summary, WSUS is a powerful tool for managing updates in a Windows environment, offering centralized control, testing, and monitoring, making it an essential tool for IT administrators looking to maintain a secure and efficient network.

Practical Activity 8.1.2: Installing the necessary roles and features

Task:

1: Referring to the key reading 8.1.2, As a server administrator, you are asked to go to the computer lab to perform the following: install necessary roles and features.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 5.4.2 and ask clarification where necessary

5: Perform the task provided in application of learning 8.1

Key readings 8.1.2: Installing the necessary roles and features

steps of Installing the necessary roles and features in windows server 2019

Here's a step-by-step guide to installing roles and features in **Windows Server 2019**:

Method 1: Using Server Manager

Step 1: Open Server Manager

- Open **Server Manager** by clicking the Start button and selecting **Server Manager** from the menu.

Step 2: Add Roles and Features

- In **Server Manager**, click on **Manage** in the upper-right corner.
- Select **Add Roles and Features** from the dropdown menu.

Step 3: Before You Begin

- A "Before You Begin" window will appear. Review the information and click **Next**.

Step 4: Installation Type

- Choose **Role-based or feature-based installation**, then click **Next**.

Step 5: Select Destination Server

- Choose the server where you want to install the roles and features. Typically, it's your local server. Select the server from the **Server Pool** and click **Next**.

Step 6: Select Server Roles

- In the **Server Roles** window, you'll see a list of available roles. Check the box for the roles you want to install (e.g., **Active Directory Domain Services**, **DNS Server**, **Web Server (IIS)**, etc.).
- After selecting a role, you may be prompted to install additional features required for that role. Click **Add Features** when prompted, and then click **Next**.

Step 7: Select Features

- In the **Features** window, you can add additional features if necessary (e.g., **.NET Framework 3.5**, **Failover Clustering**).
- Once selected, click **Next**.

Step 8: Role Services (Optional)

- If installing a role like **Web Server (IIS)**, you will be asked to select **Role Services**. Check any additional services you need and click **Next**.

Step 9: Confirm Installation Selections

- Review your selected roles, features, and services. You can also choose to restart the server automatically if required. If you're ready, click **Install**.

Step 10: Installation Progress

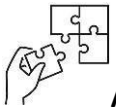
- The installation will begin. You can monitor the progress, and once it's complete, you'll receive a confirmation message.

Common Roles and Features to Install:

- **Active Directory Domain Services (AD DS):** Install-WindowsFeature -Name AD-Domain-Services
- **DNS Server:** Install-WindowsFeature -Name DNS
- **DHCP Server:** Install-WindowsFeature -Name DHCP
- **File and Storage Services:** Install-WindowsFeature -Name FS-FileServer
- **Web Server (IIS):** Install-WindowsFeature -Name Web-Server.

Points to Remember

- While installing roles and feature remember to Open **Server Manager** by clicking the Start button and selecting **Server Manager** from the menu.
- While installing roles and feature remember to check pre-installation requirements by setting strong administrator password and static Ip address.
- Don't forget to select destination server and installation type as main keywords.
- While installing roles and feature remember to select the roles you need (example: DNS, AD and DHCP.)
- While installing roles and feature remember to confirm installation selections by reviewing all selections on the confirmation page.
- While installing roles and feature remember to Open **Server Manager** by clicking the Start button and selecting **Server Manager** from the menu.
- While installing roles and feature remember to check pre-installation checks
- Don't forget to select destination server and installation type as main keywords
- Don't forget to restart if necessary and verify that the roles and features are functioning as expected by checking their status in Server Manager.



Application of learning 8.1.

XYZ LTD is a software development company located in Muhanga district, they want to manage all computers connected to the single server, due to different activities that they have, you are hired as system Administrator who is responsible for setting the working environment by installing roles and features on the server.
All tools, materials and equipment will be provided by the company.

Indicative content 8.2: Configure WSUS

Duration:3 hrs

Practical Activity 8.2.1: Configuration of WSUS

Task:

1: Referring to the key reading 8.1.2, As a server administrator, you are asked to go to the computer lab to perform the following: configure wsus.
2: Apply safety precautions
3: Present your work to the trainer and whole class.
4: Read key reading 5.4.2 and ask clarification where necessary
5: Perform the task provided in application of learning 8.2

Key readings 8.2.1: Configuration of WSUS

1.**Step Configure WSUS**

- **Open WSUS Console**:

In Server Manager, navigate to Tools > Windows Server Update Services.

2. Run Configuration Wizard:

The WSUS Configuration Wizard should start automatically. If it doesn't, you can manually launch it from the WSUS console under Options > WSUS Server Configuration Wizard.

3.Choose Upstream Server:

Select whether to synchronize updates from Microsoft Update or another WSUS server. For a new setup, choose to synchronize from Microsoft Update

4.Configure Group Policy Settings:

To direct client machines to your new WSUS server, configure Group Policy settings that specify the WSUS server's location (e.g., http://<YourServerName>:8530). This can be done through Group Policy Management Editor under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update

5.Finalize Configuration:

After configuration, approve updates in the WSUS console as needed and ensure clients are reporting correctly to your WSUS server.

- Approve Updates

After synchronization, review available updates in the WSUS console and approve them for installation on client machines.

- Configure Client Settings
- A client configuration provides settings that define a client and how it should

operate in the network. Each configuration includes settings for: The Software AG Directory Server that should be used by the client in its attempts to work with databases.

- Client Detection and Update
- Enable the policy **Automatic update detection frequency** to specify how often clients check for updates (in hours). This setting allows clients to check for updates at intervals you define, which can range from every hour to every few days.
- Once the Group Policy settings are configured, you can force clients to detect updates:
- On each client machine, open Command Prompt as an administrator.
- Run the following command to force detection:

```
bash
wuauclt /detectnow
```

- This command prompts the client to contact the WSUS server immediately for updates.
- Regularly review and approve new updates on the WSUS server.

✓ To regularly review and approve new updates on the WSUS server in Windows Server follow these steps

1.Open the WSUS Console:

- Launch the **Windows Server Update Services** console from the Start menu or by running wsus.msc

Reviewing Updates

2. Navigate to Updates:

- In the left pane, expand **Updates** and select **All Updates**. This view displays all updates that have been synchronized from Microsoft Update or an upstream WSUS server.

3.Filter Updates:

- Use the filtering options to display updates based on approval status, installation status, and other criteria. The default view shows unapproved updates needed by clients or those that had installation failures.

4.View Update Details:

- Select an update to view detailed information in the lower pane, including its title, classification, installation status, and any relevant.

Approving Updates

5. Select Updates to Approve:

- In the list of updates, select the updates you wish to approve. You can select multiple updates by holding down the **Shift** or **Ctrl** key while clicking.

6.Approve Selected Updates:

- Right-click on the selected updates and choose **Approve**. You will then be prompted to select the target computer group for which you want to approve

these updates.

7.Regular Review Schedule:

Establish a regular schedule (e.g., weekly) to review and approve new updates.

This ensures that your systems remain secure and up to date with the latest patches.

- **Monitor the health and performance of the WSUS server and its database.**

After approving updates, monitor their deployment by using the WSUS reporting feature. Navigate to Reports > Update Status Summary to see which updates have been installed on client machines and their status.

- **Periodically clean up expired and unneeded updates to save disk space:**

is a utility tool provided by the Windows operating system that helps you free up disk space on your computer. It scans your hard drive for unnecessary files, such as temporary files, system files, and files in the Recycle Bin, and allows you to safely delete them, reclaiming valuable storage space.

Points to Remember

- Don't forget to **Open WSUS Console**:
- While configuring WSUS remember to navigate to Tools > Windows Server Update Services.
- Remember to Select updates from Microsoft Update or another WSUS server. For a new setup, choose to synchronize from Microsoft Update.

Application of learning 8.2.

ABC LTD is a software development company located in Kirehe district, they want to manag e all computers connected to the single server, due to different activities that they have, you are hired as system Administrator who is responsible for setting the working environment b y configuring WSUS.

All tools, materials and equipment will be provided by the company.

Indicative content 8.3: Perform Server Backup

Duration: 3 hrs

Theoretical Activity 8.3.1: Description of server backup

Tasks:

1: Answer the following questions:

i. What do you understand by the following terms as used in windows server?

a) Server backup

b) Recovery strategies

ii. differentiate types of backups in windows server

iii. how to secure backup storage

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 8.3.31

Key readings 8.3.1.: Description of server backup

1.Definition of key terms

1. A server backup is a copy of the data stored on a server. The backup should be made to a different media and ideally stored in a different location. Backups provide an accessible copy of the data on the server, allowing it to be recovered if the original data is lost or corrupted.

2. **A recovery strategy** in computer science refers to a **plan designed to restore a database system to a working state after a failure or** disaster.

Assess data to be backed up

Identify critical data, including user files, system configurations, databases, and applications, that need to be backed up to ensure business continuity.

Plan the Backup and recovery strategies

Develop a comprehensive backup and recovery plan outlining the frequency of backups, retention policies, and recovery procedures.

Backup type

1.full backups

A full backup is the process of creating one or more copies of all organizational data files in a single backup operation to protect them.

incremental backups

is a backup type that only copies data that has been changed or created since the previous backup activity was conducted.

3. differential backups

is a data protection method that copies all files changed since the last full backup.

Select Backup Location

Determine where backups will be stored, considering factors like accessibility, security, and redundancy. For example, you may choose to store backups on local storage devices, network-attached storage (NAS), or cloud storage services like AWS S3 or Azure Blob Storage.

Schedule Backups

•Establish a backup schedule that ensures regular and consistent backups are performed according to the defined backup strategy. For example, you may schedule daily backups during non-business hours to minimize disruption.

✓ Secure Backup Storage:

•Implement security measures to protect backup data from unauthorized access, tampering, or loss. This may include encryption, access controls, and physical security measures for storage devices.

Test Restorations

Regularly test the restoration process to verify the integrity and effectiveness of backups. Conducting periodic recovery drills helps ensure that data can be successfully restored in the event of a disaster.

Documentation of backup

Maintain detailed documentation of the backup process, including backup schedules, storage locations, and recovery procedures. This documentation serves as a reference for IT staff and facilitates compliance with regulatory requirements.

Regularly review

Periodically review and evaluate the backup strategy to ensure it remains aligned with changing data and server requirements. Adjustments may be necessary as new applications are deployed or data volumes increase.

Update backup strategy as your data and server requirements evolve

Update the backup strategy as your data and server requirements evolve, incorporating lessons learned from past backup and recovery experiences.

Periodic mock drills

Conduct periodic mock drills to simulate various disaster scenarios and test the effectiveness of the backup and recovery procedures. This helps identify potential weaknesses and areas for improvement.

Produce DRP document

Develop a Disaster Recovery Plan (DRP) document that outlines the steps to be taken in the event of a server failure or data loss. This document should include roles and responsibilities, escalation procedures, and contact information for key stakeholders.

Practical Activity 8.3.2: performing server backup

Task:

1: Referring to the key reading 8.3.2, As a server administrator, you are asked to go to the computer lab to perform the following: perform server backup.
2: Apply safety precautions
3: Present your work to the trainer and whole class.
4: Read key reading 5.4.2 and ask clarification where necessary
5: Perform the task provided in application of learning 8.3

Key readings 8.3.2.: performing server backup

To perform server backup in Windows Server, follow these detailed steps using the built-in **Windows Server Backup** feature.

step 1: Install Windows Server Backup

1. Open Server Manager:

- Click on **Manage** in the top right corner and select **Add Roles and Features**.

2.Navigate through the Wizard:

- Click **Next** until you reach the **Features** section.
- **Navigate through the Wizard**: Check the box for **Windows Server Backup** and click **Next**.

4.Complete Installation:

- Click **Install**, and once the installation is complete, click **Close**.

Step 2: Perform a One-Time Backup

Open Windows Server Backup:

In the Start menu, search for "Windows Server Backup" and open it.

2.Initiate Backup:

In the right pane, click on **Backup Once.**

3.Choose Backup Options:

- In the Backup Once Wizard, select **Different options**, then click **Next**.

4.Select Backup Configuration:

- Choose either **Full server (recommended)** or **Custom**, then click **Next**.

5.**Specify Destination Type**:

- Select either **Local drives** or a **Remote shared folder**, then click **Next**.

6.Select Backup Destination:

- Choose the specific drive or folder where you want to store the backup, then click **Next**.

7.Review and Start Backup:

Confirm your settings and click on **Backup** to start the process. Wait for it to complete, then close the utility.

Step 3: Schedule Regular Backups

1.Open Windows Server Backup Again:

- Go back to Windows Server Backup from the Start menu.

2.Access Backup Schedule:

- In the right pane, click on **Backup Schedule**.

3.Choose Backup Configuration Type:

- Select either **Full server** or **Custom**, then click **Next**.

4.Set Frequency of Backups:

- Choose how often you want backups to occur (daily, multiple times a day), and specify the time for backups, then click **Next**.

5.Select Destination for Scheduled Backups:

- Choose where to save these backups (local drive or remote shared folder), then click **Next**.

6.Finalize Settings:

- Review your settings and click on **Finish** to create the scheduled backup task.

Step 4: Monitor and Manage Backups

- Regularly check your backup status in Windows Server Backup.

Ensure that backups are completing successfully and monitor available storage space on your backup destination.

- Consider testing restore procedures periodically to ensure that your backups can be reliably restored when needed.

Points to Remember

- Don’t forget to **automate backup processes**
- While perform server backup remember to implement backup strategy.
- Remember to Select backup options either local hard drives or cloud storage.
- Schedule backups to run automatically to minimize the risk of forgetting to perform them.
- Regularly test data restores
- Monitor backup status
- Secure and encrypt backups
- **Steps of performing server backup:**
    - Open Server Manager
    - Navigate through the Wizard and Click Next.
    - Complete Installation
    - Initiate Backup

- Choose Backup Options
- Specify Destination Type
- Select Backup Destination
- Review and Start Backup
- Finalize Settings

Application of learning 8.4.

Suppose that your school needs to implement server backup based on windows server as a trainee in networking and Internet Technology you are required for performing server backup.

All tools, materials and equipment will be provided by the company.

Indicative content 8.4: Perform Troubleshooting

Duration:3 hrs

Practical Activity 8.4.1: Performing server troubleshooting

Task:

1: Referring to the key reading 8.4.2, As a server administrator, you are asked to go to the computer lab to perform the following: **perform troubleshooting**.

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 5.4.2 and ask clarification where necessary

5: Perform the task provided in application of learning 8.4

Key readings 8.4.2: Performing server troubleshooting

1.Definition of key terms

Troubleshooting is a systematic approach to problem-solving that is often used to find and correct issues with complex machines, electronics, computers and software systems.

✓ To troubleshoot issues in Windows Server 2019 effectively, follow these structured steps:

Step 1: Identify the Issue

- **Gather Error Messages**: Document any specific error messages you encounter. Take screenshots or write down error codes as they can be critical for troubleshooting.
- **Review Event Logs**: Open the **Event Viewer** (Control Panel > Administrative Tools >

Event Viewer) to check for relevant logs:

- Look in the **System** and **Application** logs for errors around the time the issue occurred.
- Navigate to **Application and Service Logs > Microsoft > Windows > Windows Update Client > Operational** for Windows Update-related issues.

Step 2: Check for Pending Actions

- **Pending Reboot**: Ensure that there are no pending reboots. If the server has not been restarted after updates, do so to apply changes.

Step 3: Analyze Services

- **Check Service Status**: Use the Services management console (services.msc) to verify that all necessary services are running. If a service is stopped, attempt to

start it and check its dependencies.

- **Set Recovery Options**: Configure recovery options for critical services to automatically restart on failure.

Step 4: Remove Variables

- **Disable Non-Essential Hardware**: Temporarily disable or disconnect any non-essential hardware components to rule out hardware failures.
- **Uninstall Recent Updates**: If issues began after recent updates, consider rolling them back.

Step 5: Use Diagnostic Tools

- **Run Built-in Troubleshooters**: Utilize the Windows Update troubleshooter or other relevant troubleshooters available in Settings (Settings > Update & Security > Troubleshoot).
- **DISM and SFC Tools**: Run the following commands in an elevated Command Prompt to repair system files:

```
bash
DISM /Online /Cleanup-Image /RestoreHealth
sfc /scannow
```

Step 7: Monitor System Performance

- **Resource Monitoring**: Use Task Manager or Resource Monitor to check CPU, memory, and disk usage. High resource consumption can indicate underlying issues.

Step 8: Document Findings

- Keep a detailed record of all findings, changes made, and steps taken during troubleshooting. This documentation can be invaluable if further assistance is needed or if similar issues arise in the future.

Theoretical Activity 8.4.1: Description of Gathering information

Tasks:

1: Answer the following questions:

I. What do you understand by the following terms as used in windows server?
   a) Gather information
   b) Troubleshooting

ii.List four (4) Diagnostic Tools used in troubleshooting

iii.Differentiate Check Server Status from Network Connectivity?

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 8.4.1

Key readings 8.4.2: Description of Gathering information

1**.Definition of key terms**

Troubleshooting is a systematic approach to problem-solving that is often used to find and correct issues with complex machines, electronics, computers and software systems.

Gather Information: Collect relevant information to identify the root cause of the issue, including:

- Server hardware specifications (e.g., CPU, RAM, storage)
- Software configuration details (e.g., installed applications, services)
- Logs from system event logs, application logs, and error logs
- Error messages reported by users or system alerts
- Recent changes made to the server configuration or application

Check Server Status: Ensure that the server is operational and responsive by performing the following checks:

- Verify that the server is powered on and accessible.
- Monitor resource utilization to identify any performance bottlenecks:
- Check CPU usage to ensure its within normal limits.
- Monitor disk usage to ensure there's sufficient free issues.

✓ **Verify Network Connectivity:** Confirm that the server can communicate with other devices on the network by checking:

- DNS settings to ensure proper name resolution.
- Network configurations, including IP addresses, subnet masks, and gateways.

✓ Use Diagnostic Tools

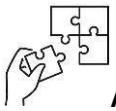
- Employ diagnostic tools to further troubleshoot and diagnose server issues, such as:
- Network diagnostic tools like ping, traceroute, and nslookup to diagnose network connectivity problems.

✓ **Document Findings and Solutions**

- Document the findings from troubleshooting efforts, including identified issues, potential causes, and solutions implemented.
- Maintain a log of troubleshooting activities and resolutions for future reference and knowledge sharing within the IT team.

Points to Remember

- When perform troubleshooting remember to gather detailed information.
- Don’t forget to identify the problem.
- Enable temporarily disconnect or disable unnecessary hardware components to see if they are causing conflicts.
- When perform troubleshooting remember to use rollback recent changes.
- When perform troubleshooting remember to use diagnostic tools.
- While perform troubleshooting remember to use performance monitoring tools to check CPU, memory and disk usage for any anomalies that could indicate underlying issues.
- When perform troubleshooting remember to gather detailed information.
- Don’t forget to identify the problem.
- Enable temporarily disconnect or disable unnecessary hardware components to see if they are causing conflicts.
- When perform troubleshooting remember to use rollback recent changes.
- When perform troubleshooting remember to use diagnostic tools.
- While perform troubleshooting remember to use performance monitoring tools to check CPU, memory and disk usage for any anomalies that could indicate underlying issues.



Application of learning 8.4.

XYZ is a software development company located in Musanze district, they want to manage all computers connected to the single server, due to different activities that they have, you are hired as system Administrator who is responsible for setting the working environment to perform troubleshooting on server.
All tools, materials and equipment will be provided by the company.

Indicative content 8.5: Perform Migration

Duration:2 hrs

Theoretical Activity 8.5.1: Description of migration

Tasks:

1: Answer the following questions:

i. What do you understand by the following terms as used in windows server?
   a) Migration
   b) Timeline
   c) Potential risks

ii. Differentiate FTP for files, and database migration for databases.

iii. How to monitor and validate migration process.

2: Write your answers on papers or flipchart.

3: Present your findings/answers to the whole class

4: Ask for clarification where necessary

5: Read the key readings 8.5.1

Key readings 8.5.1 Description of migration

1.definitions of migration

Migration in Windows Server refers to the process of transferring data, applications, and configurations from one server to another.

✓**Plan and prepare servers and services that need to be migrated**

- Timeline
- Establish a comprehensive plan for migrating servers and services, including:
- Setting a timeline for the migration process to minimize downtime and disruption.
- Potential risks
- Identifying potential risks and mitigation strategies to address any challenges that may arise during migration.

✓ Configure RAIDs

- Configure Redundant Array of Independent Disks (RAID) arrays to ensure data redundancy and fault tolerance, enhancing data integrity and availability during the migration process.

✓ **Perform migration process**

- Execute the migration process according to the established plan, ensuring a smooth transition of servers and services to the new environment.

Below we outline seven steps to a successful data migration.

- Identify the data format, location, and sensitivity. ...
- Planning for the size and scope of the project. ...
- Backup all data. ...
- Assess staff and migration tool. ...
- Execution of the data migration plan. ...
- Testing of final system. ...
- Follow-up and maintenance of data migration plan.
- Data Transfer methods (rsync or FTP for files, and database migration for databases)

  ✓ Utilize appropriate data transfer methods based on the nature of the data being migrated:

  - For files use FTP to transfer data securely and efficiently.
  - For databases, employ database migration techniques to ensure data consistency and integrity throughout the migration process.

  ✓ Monitoring and Validation
- Monitor the migration process closely to track progress and identify any issues that may arise.
- Validate the migrated servers and services to ensure that they function correctly and meet organizational requirements post-migration.

Real-life Example:

Consider a scenario where an organization decides to migrate its web hosting services to a new server infrastructure. In planning the migration, the IT team establishes a timeline for the migration process, identifies potential risks such as data loss or service disruption, and configures RAID arrays on the new servers to safeguard against data loss. During the migration process, they use rsync to transfer website files and database migration tools to migrate the underlying database.

Practical Activity 8.5.2: Performing migration process

Task:

1: Referring to the key reading 8.5.2, As a server administrator, you are asked to go to the computer lab to perform the following: to perform migration process

2: Apply safety precautions

3: Present your work to the trainer and whole class.

4: Read key reading 5.4.2 and ask clarification where necessary

5: Perform the task provided in application of learning 8.5

Key readings 8.5.2 performing migration process

The migration process in Windows Server refers to the transfer of roles, features, and data from one server to another. This process ensures minimal downtime and data integrity. Below is a general guide to performing a migration in a Windows Server environment.

Steps to Perform Migration in Windows Server

Step 1: Pre-Migration Planning

1. Determine what to migrate: Identify the roles (e.g., Active Directory, DNS, DHCP) and data to be migrated.
2. Check compatibility: Ensure the destination server is compatible with the roles and applications running on the source server.
3. Backup source server: Always back up the source server and its critical data before performing any migration.
4. Gather necessary tools: Install the Windows Server Migration Tools and other relevant migration software.

Step 2: Prepare Source and Destination Servers

1.Source Server (Old Server)

- Ensure the source server is stable and running the services you want to migrate.
- Check for pending updates or issues that may affect migration.
- Clean up unnecessary files or services that you do not want to migrate.

2.Destination Server (New Server)

- Install the same or newer version of Windows Server as the source server.
- Make sure it is properly configured, networked, and can communicate with the source server.
- Install the Windows Server Migration Tools:

1. Go to Server Manage
2. Click on Add roles and features
3. Select Windows Server Migration Tools under the Features section.

step 3: Install Windows Server Migration Tools

On both the source and destination servers

This installs the migration tools required to transfer roles, features, and data between the two servers.

Step 4: Export Data from the Source Server

1. Prepare the Source Server for Export:
   Run PowerShell and navigate to the migration tools directory: PowerShell d "C:\Windows\System32\ServerMigrationTools"
2. Export settings or data using specific PowerShell commands for the roles/services you're migrating. Example commands: For file services:

3. Back up any application-specific data (such as SQL databases) manually, if necessary.

Step 5: Import Data to the Destination Serve

1. Prepare the Destination Server

- Make sure Windows Server Migration Tools are installed, and the server is ready to accept incoming data.
- Navigate to the same migration directory as on the source server using PowerShell Power Shell cd "C:\Windows\System32\ServerMigrationTools"

2. Import the settings:

- Use the following command to import the settings or data exported from the source server: For file services:

3. Verify the Import: After the migration completes, ensure all the settings, roles, and data are correctly imported and running on the destination server.
4. You can verify the services using the Server Manager or running service-specific PowerShell checks.

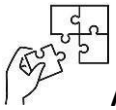
Tools and Methods for Migration

- **Windows Server Migration Tools**: Built-in set of tools for migrating roles and data between Windows Servers.
- **Active Directory Migration Tool (ADMT)**: Specialized for migrating Active Directory domains and users.
- **Storage Migration Service**: Facilitates the migration of file servers and associated data from older systems to newer systems.

Points to Remember

- While performing migration remember to assess your current environment by identifying all servers, their roles, applications and dependencies.
- When performing migration remember to choose a migration strategy by upgrading the existing server to a newer version.
- Don’t forget to use migration tools to facilitate data transfer and configuration replication.
- While performing migration remember to prepare migration to ensure that all data is backed up before starting the migration process.
- Remember to monitor migration progress to keep track of migration process to quickly identify and troubleshoot any issues that arise.
- Determine what to migrate
- Check compatibility
- Backup source server
- Gather necessary tools
- Prepare Source and Destination Servers

- Install Windows Server Migration Tools
- Export Data from the Source Server
- Import Data to the Destination Serve
- Verify the Import settings



Application of learning 8.5.

Suppose that your school needs to implement server migration based on windows server as a trainee in networking and Internet Technology you are required for performing server migration based on the requirements of your school.

All tools, materials and equipment will be provided by the company.

Learning outcome 8 end assessment

Written assessment

I. Multiple choice question: Circle the letter corresponding to the correct

1.What is the primary function of WSUS?

a) Writing JavaScript code
b) Debugging the application
c) It is a Microsoft tool that enables IT administrators to manage the distribution of updates released by Microsoft to computers in a corporate environment.
d) Creating a user interface

2.Read the following statements and choose the right answer about centralized management?

a) centralized management are applications that can be installed and provisioned on more traditional compute resources like servers.
b) centralized management operate at the application layer of the OSI model, allowing for more sophisticated traffic management compared to Layer 4 load balancing.
c) centralized management allows administrators to manage the deployment of updates for Windows operating systems, Microsoft Office, and other Microsoft software products from a central server.

3. Which of the following best defines Control over Deployment?

a. It is a tool used by system administrators to detect when a cyberattack has occurred.
b. It allows granular control by offering the ability to approve or decline updates, automatically approve certain update types, and schedule installations.
c. It is a tool used for performing routine maintenance on servers.
d. It is used to distribute network traffic across a cluster of servers.

4. Read the following statements and choose the right answer about assess data to be backed up?

a) Identify critical data, including user files, system configurations, databases, and applications, that need to be backed up to ensure business continuity
b) Least Connections and Least Response Time
c) Develop a comprehensive backup and recovery plan outlining the frequency of backups, retention policies, and recovery procedures.

5.Which of the following is not types of backups?

a) full backups
b) incremental backups
c) differential backups.
d) All above

II. Read the following statement related to perform load balancing in column A and B and write the letter corresponding to the correct answer

Answer	Column A	Column B
……..	**1.** Implement security measures to protect backup data from unauthorized access, tampering, or loss. This may include encryption, access controls, and physical security measures for storage devices.	A. Schedule Backups
……..	2. Establish a backup schedule that ensures regular and consistent backups are performed according to the defined backup strategy. For example, you may schedule daily backups during non-business hours to minimize disruption.	B. Secure Backup Storage:
……	3. Maintain detailed documentation of the backup process, including backup schedules, storage locations, and recovery procedures.	C. Regularly review
……	4. Periodically review and evaluate the backup strategy to ensure it remains aligned with changing data and server requirements.	D. Documentation of backup
……	5. Conduct periodic mock drills to simulate various disaster scenarios and test the effectiveness of the backup and recovery procedures.	E. Periodic mock drills
		F. you can effectively configure and manage a load balancing cluster that enhances application performance and reliability

III. Read the following statement related to perform load balancing and answer True if the statement is correct and False if the statement is wrong

1. Troubleshooting is a systematic approach to problem-solving that is often used to find and correct issues with complex machines, electronics, computers and software systems?

a) False
b) true

2. Configure Redundant Array of Independent Disks (RAID) arrays is to ensure data redundancy and fault tolerance, enhancing data integrity and availability during the migration process.

a) True
b) False

3. NLB is not technology used to distribute network traffic across multiple servers, enhancing both availability and scalability.

c) True
d) false

4. These tools (ping, traceroute, and nslookup) are network diagnostic tools?

a) False
b) True

5.To check server status is to Ensure that the server is operational and responsive by performing and verify that the server is powered on and accessible.

a) False
b) True

Practical assessment

AXZ LTD is a software development company located in Rubavu district, they want to manage all computers connected to the single server, due to different activities that they have, you are hired as system Administrator who is responsible for setting the working environment by. Perform migration and configure RAIDs.

All tools, materials and equipment will be provided by the company.

Further information to the trainer

Van Do, T., & Krieger, U. R. (2009). A performance model for maintenance tasks in an environment of virtualized servers: (Work in progress). In *NETWORKING 2009: 8th International IFIP-TC 6 Networking Conference, Aachen, Germany, May 11-15, 2009. Proceedings 8* (pp. 931–942). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-01399-7_73

Kherbache, V., Madelaine, E., & Hermenier, F. (2014). Planning live-migrations to prepare servers for maintenance. In *Euro-Par 2014: Parallel Processing Workshops: Euro-Par 2014 International Workshops, Porto, Portugal, August 25-26, 2014, Revised Selected Papers, Part II 20* (pp. 498–507). Springer International Publishing. https://doi.org/10.1007/978-3-319-14313-2_43

Liu, C., Zha, X. F., Miao, Y., & Lee, J. (2005). Internet server controller-based intelligent maintenance system for information appliance products. *International Journal of Knowledge-based and Intelligent Engineering Systems, 9*(2), 137–148.

Krause, J. (2018). *Mastering Windows Server 2019*. Packt Publishing.

Server, W. (2019, January 22). Note?os=Windows_Server_2019&p=install. *Server-world.info*. Retrieved from https://www.server-world.info/en/note?os=Windows_Server_2019&p=install

Ejaz, I., Alvarado, M., Gautam, N., Gebraeel, N., & Lawley, M. (2019). Condition-based maintenance for queues with degrading servers. *IEEE Transactions on Automation Science and Engineering, 16*(4), 1750–1762. https://doi.org/10.1109/TASE.2019.2903234

Hossain, M. M. (2016). *Networking & server maintenance of Abdul Monem Ltd* (Doctoral dissertation, East West University).

RTB | RWANDA TVET BOARD

October 2024