



RQF LEVEL 4



SWDWS401
SOFTWARE
DEVELOPMENT

Windows Server Administration

TRAINEE'S MANUAL

October 2024



WINDOWS SERVER ADMINISTRATION

AUTHOR'S NOTE PAGE (COPYRIGHT)

The competent development body of this manual is Rwanda TVET Board ©, reproduce with permission.

All rights reserved.

- This work has been produced initially with the Rwanda TVET Board with the support from KOICA through TQUM Project.
- This work has copyright, but permissions are given to all the Administrative and Academic Staff of the RTB and TVET Schools to make copies by photocopying or other duplicating processes for use at their own workplaces.
- This permission does not extend to making of copies for use outside the immediate environment for which they are made, nor making copies for hire or resale to third parties.
- The views expressed in this version of the work do not necessarily represent the views of RTB. The competent body does not give warranty nor accept any liability.
- RTB owns the copyright to the trainee and trainer's manuals. Training providers may reproduce these training manuals in part or in full for training purposes only. Acknowledgment of RTB copyright must be included on any reproductions. Any other use of the manuals must be referred to the RTB.

© **Rwanda TVET Board**

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 Software Development, specifically for the module " **SWDWS401: 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

BAKANIRORA Philipe

MANIRIHO Edouard

Validation

NIYONGOMBWA Jean d'Amour

MALAYIKA Sylvie

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

NTEZIMANA Aimable

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe

SUA Lim

SAEM Lee

SOYEON Kim

WONYEONG Jeong

NDAYISABA Olivier

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

AUTHOR’S NOTE PAGE (COPYRIGHT)-----	ii
ACKNOWLEDGEMENTS-----	iii
TABLE OF CONTENT -----	vi
ACRONYMS-----	viii
INTRODUCTION -----	1
MODULE CODE AND TITLE: SWDWS401-WINDOWS SERVER ADMINISTRATION -----	2
Learning Outcome 1: Manage Server Services-----	3
Key Competencies for Learning Outcome 1: Manage Server Services-----	4
Indicative content 1.1: Introduction to Server Administration-----	6
Indicative content 1.2: Installation of Server OS-----	10
Indicative content 1.3: Creation of Domain Controller-----	41
Indicative content 1.4: Installation of Server Roles and Features -----	54
Indicative content 1.5: Configuration of DNS -----	70
Indicative content 1.6: Configuration of DHCP Parameters-----	82
Indicative content 1.7: Monitoring of Server Services -----	98
Learning outcome 1 end assessment -----	102
References-----	107
Learning Outcome 2: Manage Users -----	108
Key Competencies for Learning Outcome 2: Manage Users -----	109
Indicative content 2.1: Creation of User Accounts-----	111
Indicative content 2.2: Management of User Accounts-----	117
Indicative content 2.3: Management of User Groups -----	122
Indicative content 2.4: Management of Organization Units (OU) -----	129
Indicative content 2.5: Assignment of Permission to Users-----	132
Indicative content 2.6 Management of client machines-----	140
Learning outcome 2 end assessment -----	162
References-----	164
Learning Outcome 3: Deploy Web Application -----	165

Key Competencies for Learning Outcome 3: Deploy Web Application -----	166
Indicative content 3.1: Introduction to Web Servers -----	168
Indicative content 3.2: Configure IIS with Windows Server -----	172
Indicative content 3.3: Management of IIS Web Server -----	179
Indicative content 3.4: Setting Environment of Developed Web App -----	190
Indicative content 3.5: Verify Server Environment Requirement -----	200
Indicative content 3.6: Hosting Web App -----	210
Indicative content 3.7: Verification of Successfully Hosted Web App -----	216
Learning outcome 3 end assessment -----	222
References-----	225

ACRONYMS

AD: Active Directory
ADDS: Active Directory Domain Services
ADSS: Active Directory Sites and Services
ADUC: Active Directory Users and Computers
BIOS: Basic Input/Output System
CBT: Competency-Based Training
CD: Compact Disc
CGI: Common Gateway Interface
C Name: Canonical Name
CPU: Central Processing Unit
CSS: Cascading Style Sheets
DHCP: Dynamic Host Configuration Protocol
DNS: Domain Name System
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
HDDs: Hard Drives
HTTPS: Hypertext Transfer Protocol Secure
IIS: Internet Information Services
IP: Internet Protocol
IP Config: Internet Protocol Configuration
IPV4: Internet Protocol Version 4
IPV6: Internet Protocol Version 6
KOICA: Korea International Cooperation Agency
MAC: Media Access Control Address
MX: Mail Exchange
MySQL: My Structured Query Language
NOS: Network Operating System
NS: Name Server
OS: Operating System
OU: Organizational Unit
PTR: Pointer Record
RAID: Redundant Array of Independent Disks
RAM: Random Access Memory

RRA: Rwanda Revenue Authority
RSAT: Remote Server Administration Tools
RTB: Rwanda TVET Board
SOA: Start Of Authority
SOD: Software Development
SQL: Structured Query Language
SSDs: Solid-State Drives
TQUM: TVET Quality Management Project
UEFI: Unified Extensible Firmware Interface
UTB: University of Tourism, Technology and Business Studies
VMs: Virtual Machines
WIN: Window
WSUS: Windows Server Update Services
WWW: World Wide Web

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Software Development 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: SWDWS401-WINDOWS SERVER ADMINISTRATION

Learning Outcome 1: Manage Server Services

Learning Outcome 2: Manage Users

Learning Outcome 3: Deploy web Application

Learning Outcome 1: Manage Server Services



Indicative contents

- 1.1 Introduction to Server Administration**
- 1.2 Installation of Server OS**
- 1.3 Creation of Domain Controller**
- 1.4 Installation of Server Roles and Features**
- 1.5 Configuration of DNS**
- 1.6 Configuration of DHCP Parameters**
- 1.7 Monitoring of Server Services**

Key Competencies for Learning Outcome 1: Manage Server Services

Knowledge	Skills	Attitudes
● Description of Windows Server ● Description of Active Directory (AD) ● Identification of Server Services and Roles Overview ● Description of Hypervisor ● Description of Virtualization ● Description of RAID	● Installing windows server OS ● Configuring RAID ● Creating virtual machines ● Creating domain controller ● Installing Hypervisor ● Configuring DNS ● Configuring DHCP ● Monitoring server services ● Installing server roles and features	● Being attentive to Details ● Having adaptability ● Being patient ● Having Customer Service Orientation ● Having Teamwork ● Having Time Management ● Having Troubleshooting ● persistence ● Having ethical Conduct ● Being Resourceful ● Being calm Under Pressure ● Having ownership and Accountability



Duration: 35hrs

Learning outcome 1 objectives:



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

1. Describe correctly key concepts that are used in server administration.
2. Describe clearly Windows Server in server administration.
3. Describe correctly Active Directory (AD) in server administration.
4. Identify correctly Server Services and Roles Overview in server administration.
5. Describe clearly Hypervisor and virtualization in server administration.
6. Describe correctly RAID as used in server administration.
7. Install properly windows server OS in virtual machine
8. Configure effectively RAID on physical server
9. Create appropriately virtual machines on server
10. Create effectively domain controller in windows server
11. Install properly Hypervisor in virtual machine
12. Configure properly DNS and DHCP in windows server
13. Monitor appropriately server services in client machine



Resources

Equipment	Tools	Materials
● Computer ● Server machine	● VMWare workstation ● VMWare ESXI ● Oracle VirtualBox ● VMWare V-Sphere ● Windows Server OS bootable image ● Browser ● Flash disk ● CD/DVD Drive ● PowerISO ● ImgBurn	● Electricity ● Internet



Indicative content 1.1: Introduction to Server Administration



Duration: 5hrs



Theoretical Activity 1.1.1: Description of server administration



Tasks:

- 1: You are requested to answer the following questions:
 - i. How does a server differ from a client?
 - ii. What is Network Operating System? Give three examples.
 - iii. Define the following:
 - a) Server administration
 - b) Virtualization
 - c) Hypervisor
 - iv. What are hypervisor technologies? Provide examples of each type?
 - v. Explain the types and benefits of server virtualization.
 - vi. What are the hardware and software requirements used in windows server administration?
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 1.1.1 in the trainee's manual



Key readings 1.1.1.: Description of server administration

1. Basic Concepts

A. Server: A computer or system that provides resources, data, or services to other computers (clients) over a network.

B. Client: A computer or device that requests resources or services from a server.

C. Network Operating System (NOS): Software that manages network resources and services, enabling communication between servers and clients. Examples include Windows Server, Linux, and UNIX.

D. Virtualization

1. Server administration involves managing and maintaining computer servers, which are powerful computers that provide services to other computers on a network.

2. Virtualization: The process of creating virtual versions of physical resources (servers, storage, networks) to maximize efficiency and flexibility.

3. Hypervisor: Software that creates and manages virtual machines by abstracting physical hardware.

Hypervisor Technologies

1. Type 1 Hypervisor (Bare-Metal): Runs directly on the hardware without needing a host OS (e.g., VMware ESXi, Microsoft Hyper-V).

2. Type 2 Hypervisor (Hosted): Runs on top of a conventional operating system (e.g., VMware Workstation, Oracle VirtualBox).

A) Types of Server Virtualization

- 1. Full Virtualization:** Provides a complete simulation of hardware to VMs, allowing them to run unmodified guest operating systems.
- 2. Para-Virtualization:** Requires modifications to the guest OS, offering better performance but less isolation.
- 3. Hardware-Assisted Virtualization:** Utilizes CPU features (e.g., Intel VT-x, AMD-V) to enhance virtualization performance.

B) Benefits of Server Virtualization

- 1. Resource Utilization:** Maximizes physical server resources by running multiple VMs on a single server.
- 2. Cost Efficiency:** Reduces hardware and energy costs through server consolidation.
- 3. Scalability:** Facilitates easy scaling up or down by adjusting the number of VMs.
- 4. Disaster Recovery:** Simplifies backup and recovery through snapshots and cloning.
- 5. Isolation:** Enhances security and stability by isolating VMs from each other.

C) Hardware and software requirements for servers

1. Hardware Requirements

The specific hardware requirements for a Windows Server virtual machine will depend on the intended workload and performance expectations. However, here are some general guidelines:

Processor:

Minimum: A 64-bit processor with at least two cores.

Recommended: A 64-bit processor with four or more cores, especially for demanding workloads like database servers or virtualization hosts.

Memory:

Minimum: 4 GB of RAM.

Recommended: 8 GB or more of RAM, depending on the workload. For example, a database server might require 16 GB or more of RAM.

Storage:

Minimum: A solid-state drive (SSD) with at least 120 GB of storage for the operating system and essential applications.

Recommended: A larger SSD or a combination of SSD and hard disk drive (HDD) for storing data and applications. SSDs offer faster performance, while HDDs can be more cost-effective for bulk storage.

Network:

Minimum: A network interface card (NIC) with at least 1 Gbps bandwidth.

Recommended: Multiple NICs for redundancy and improved performance, especially for servers that handle heavy network traffic.

2. Software Requirements

Operating System: Windows Server (e.g., Windows Server 2022, Windows Server 2019). The specific version will depend on your needs and compatibility requirements.

Hypervisor: A virtualization platform like Hyper-V (built-in to Windows Server) or VMware ESXi to create and manage virtual machines.

Applications: The specific applications required will depend on the server's role. For example, a web server might need IIS, a database server might need SQL Server, and a file server might need File Server Resource Manager.



Points to Remember

- Server administration: Involves managing and maintaining computer servers, which are powerful computers that provide services to other computers on a network.
- Virtualization: The process of creating virtual versions of physical resources to maximize efficiency and flexibility.
- Hypervisor: Software that creates and manages virtual machines by abstracting physical hardware.
- There are different types of server virtualization such as: Full Virtualization, Para-Virtualization and Hardware-Assisted Virtualization
- In server virtualization there are different technologies which include: Type 1 Hypervisor (Bare-Metal) and Type 2 Hypervisor (Hosted)



Application of learning 1.1.

XYZ Company is planning to set up a new server and needs guidance to understand more about server administration. The company is looking for a system administrator who can describe the windows server administration and both hardware and software requirements. You are hired as a system administrator to help company to get information needed.



Indicative content 1.2: Installation of Server OS



Duration: 5hrs



Theoretical Activity 1.2.1: Description of server OS



Tasks:

- 1: You are requested to answer the following questions:
 - i. What is RAID?
 - ii. What are the levels of RAID?
 - iii. What are the advantages and disadvantages of using RAID?
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 1.2.1



Key readings 1.2.1.: Description of virtual storage

- **RAID (Redundant Array of Independent Disks)** combines multiple physical disks into a single logical unit to improve performance, redundancy, and/or storage capacity.
- **Identification of RAID Levels:**
 1. RAID 0 (Striping): Data is split into blocks and distributed across multiple drives.
 2. RAID 1 (Mirroring)

Function: Data is duplicated across two or more drives. Each piece of data is written to all drives.

3. RAID 5 (Striping with Parity)

Function: Data and parity information are striped across three or more drives. Parity allows for data recovery in case of a single drive failure.

4. RAID 6 (Striping with Double Parity) recovery from two simultaneous drive failures.

Function: Similar to RAID 5, but with two sets of parity information, allowing for

5. RAID 10 (1+0) (Striping and Mirroring)

Function: Combines RAID 1 and RAID 0. Data is mirrored across pairs of drives and then striped across those pairs.

- **Advantages of RAID:** Performance, redundancy, storage efficiency
- **Disadvantages of RAID:** Cost, complexity, performance Trade-offs.



Practical Activity 1.2.2: Creating virtual storage (RAID)



Task:

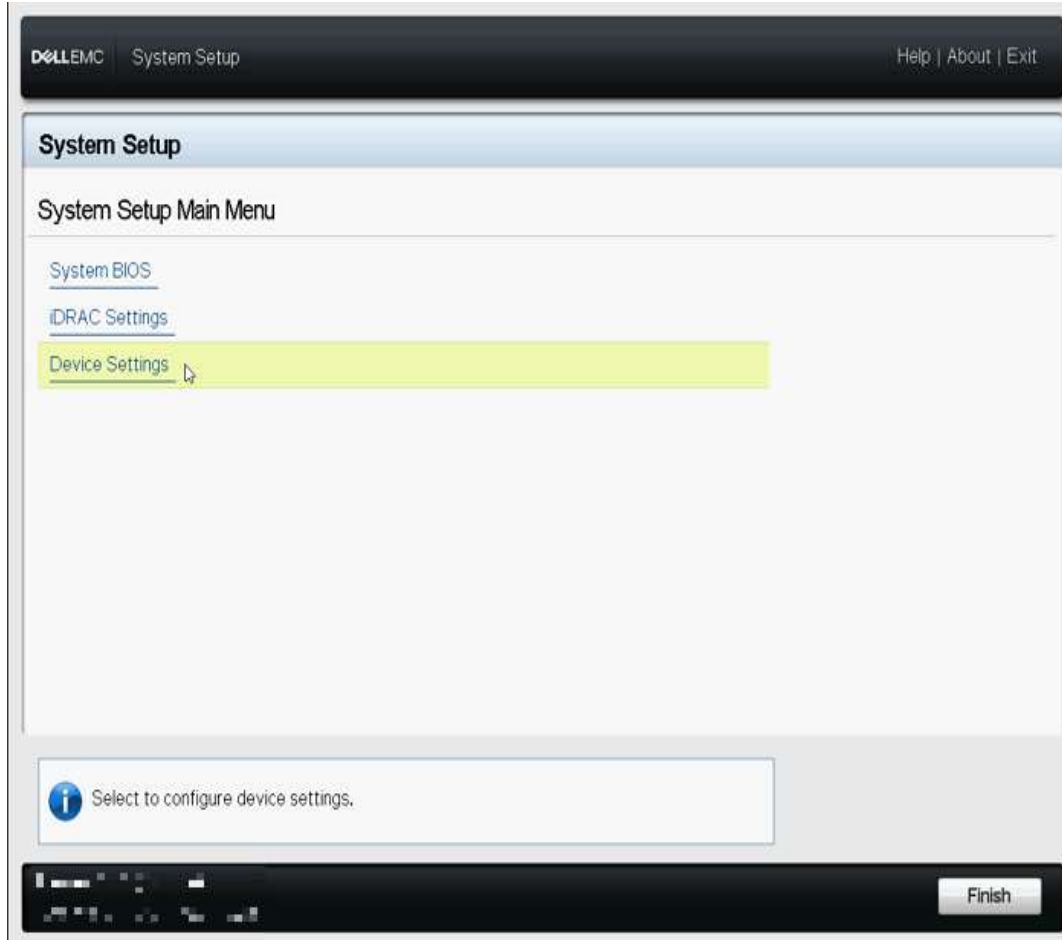
1. You are requested to go to the computer lab and do the task below individually.
As the server administrator for your organization, you are tasked with improving data redundancy and performance on the company's physical server. The server has multiple hard drives, and you must create a RAID 1 array to ensure both data protection and optimized storage usage.
2. Read the key readings 1.2.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



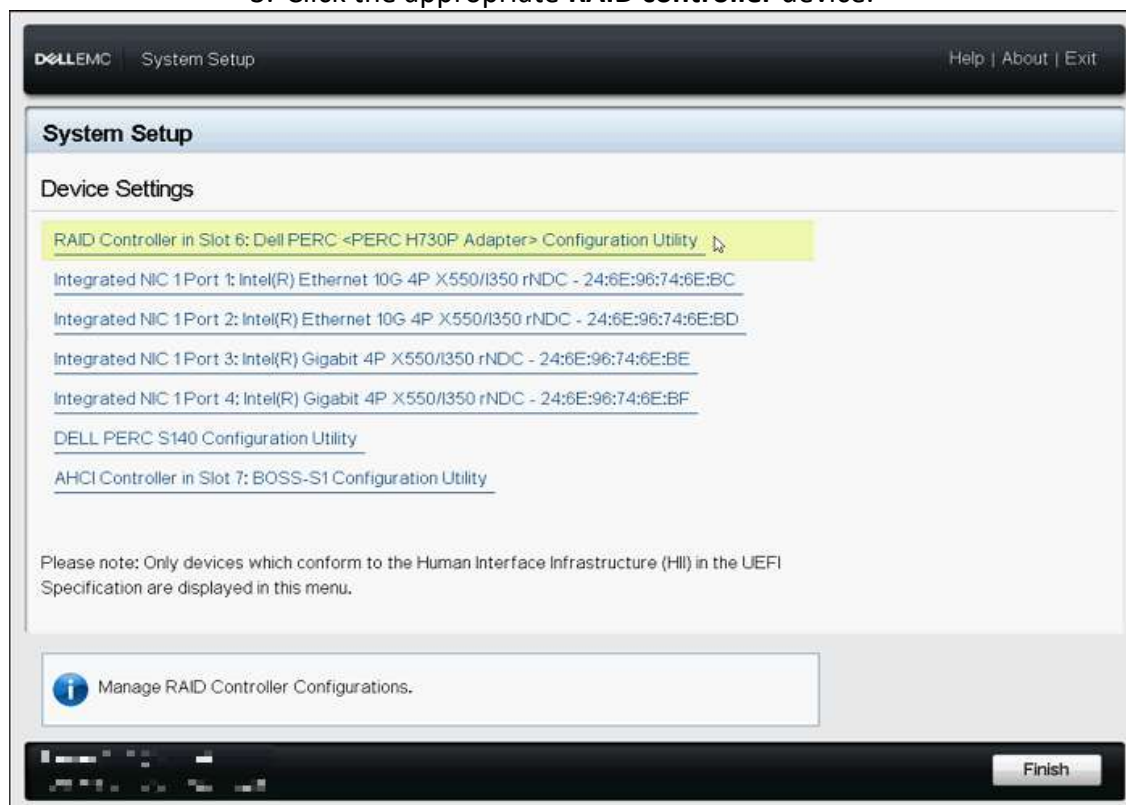
Key readings 1.2.2

Creating virtual storage (RAID)

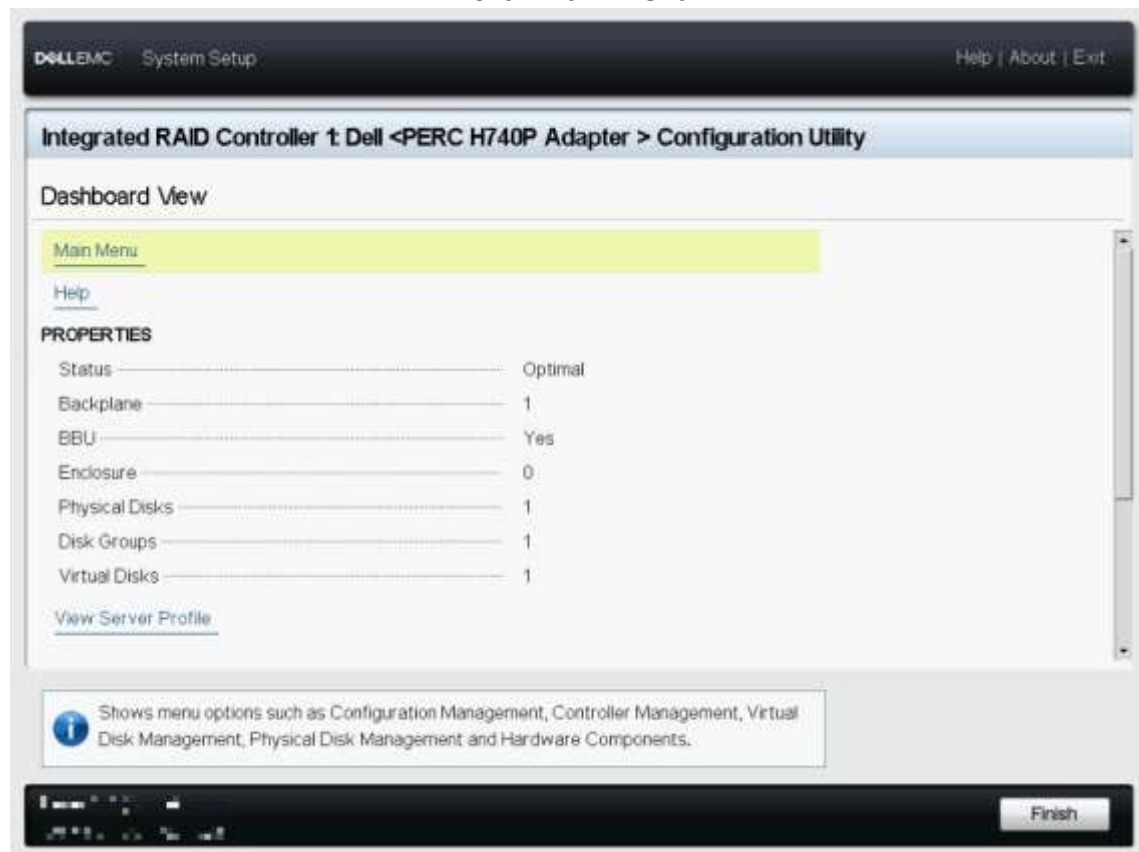
1. Enter the **System Setup** by pressing **F2** during system start.
 2. Click **Device Settings**.



3. Click the appropriate **RAID controller** device.



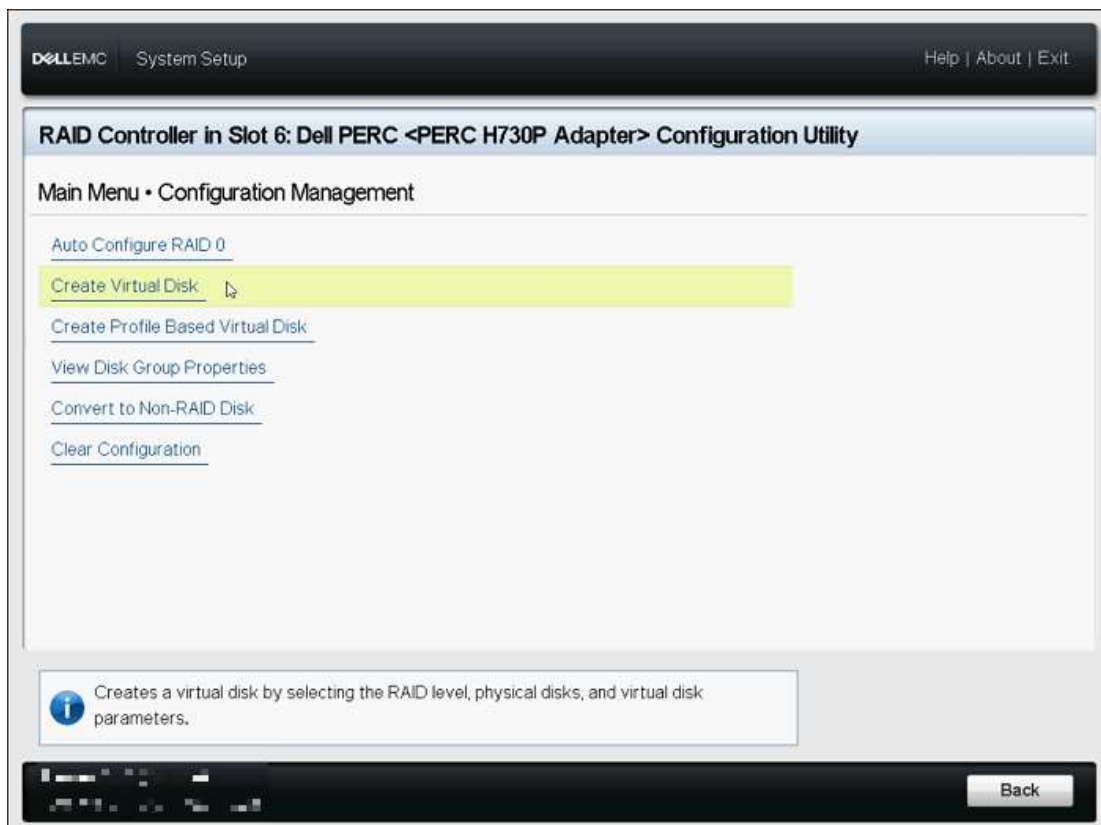
4. Click **Main Menu**.



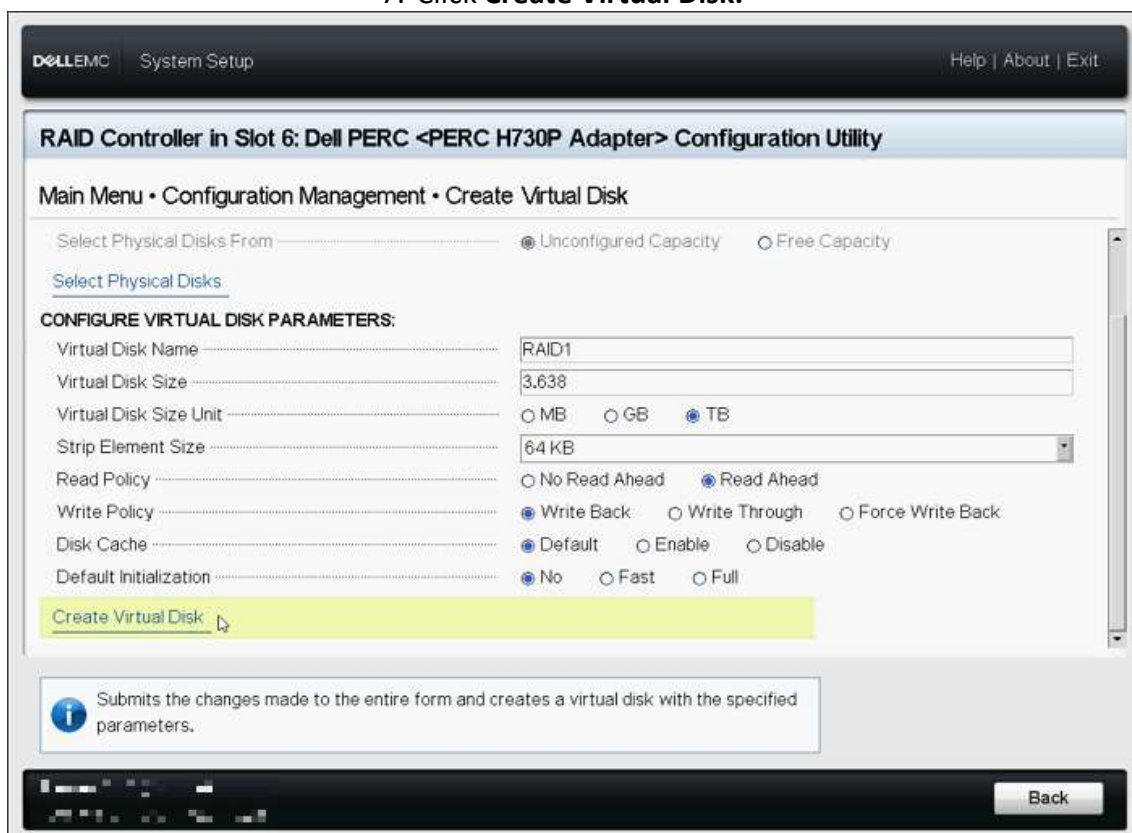
5. Click **Configuration Management**.



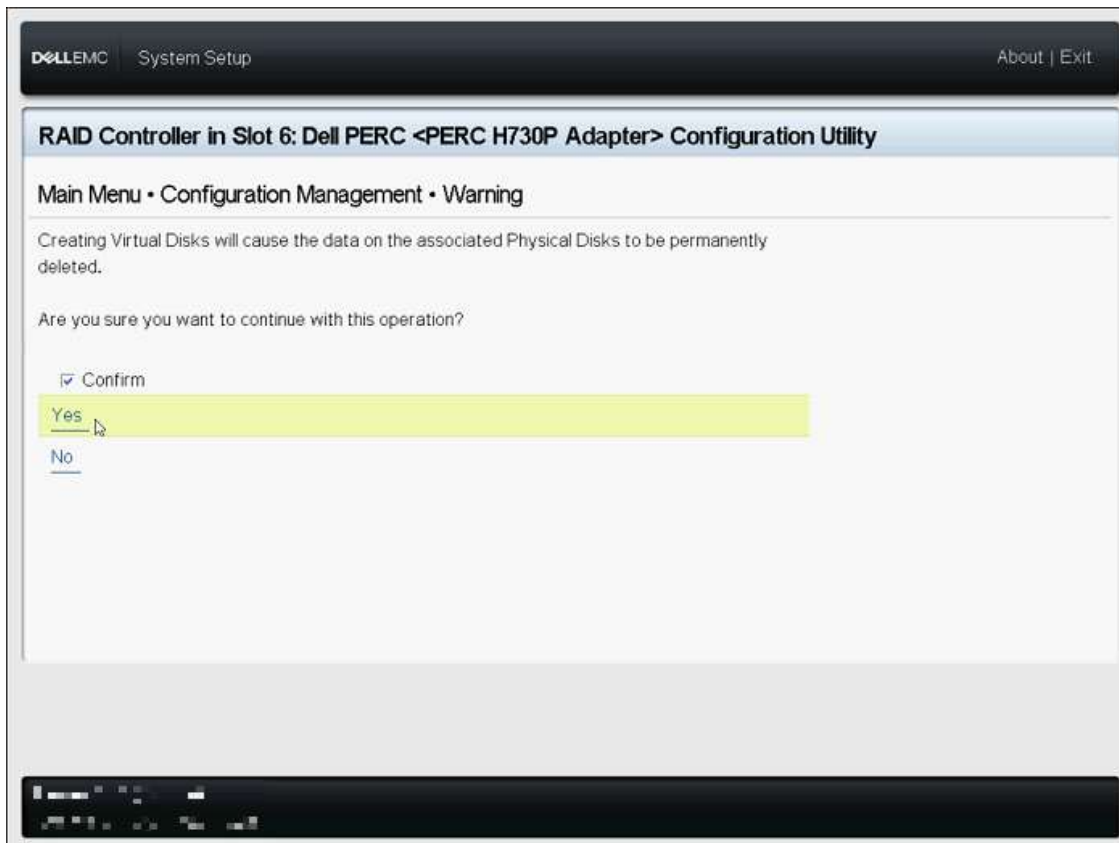
6. Click **Create Virtual Disk**



7. Click **Create Virtual Disk**.



8. Check **Confirm** and click **Yes**.



9. The **Virtual Disk** is created successfully. Click **Ok**.



Practical Activity 1.2.3: Installation of Hypervisor



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Trainee in Level 4 software development, you are tasked with installing of Hypervisor on the server administration.

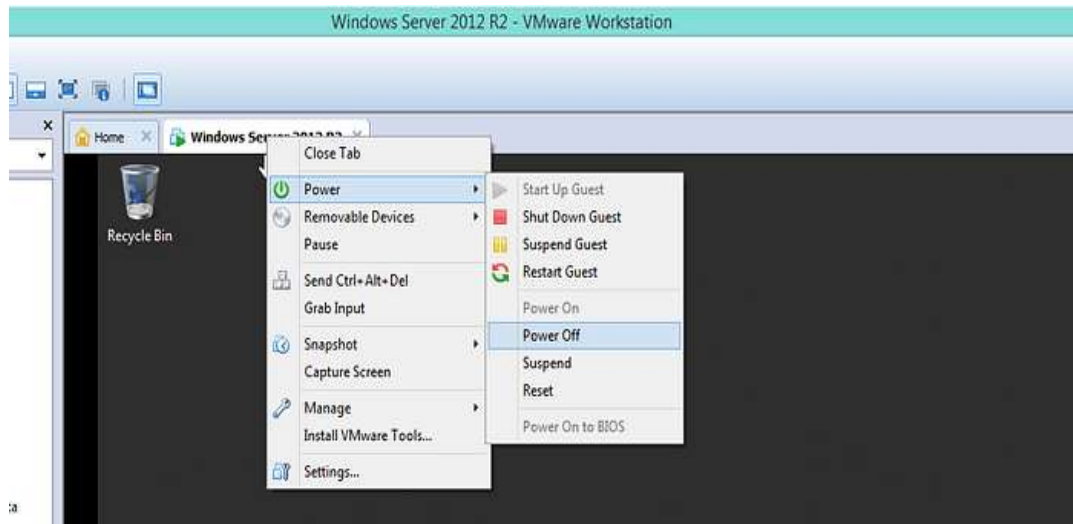
2. Read the key readings 1.2.3 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



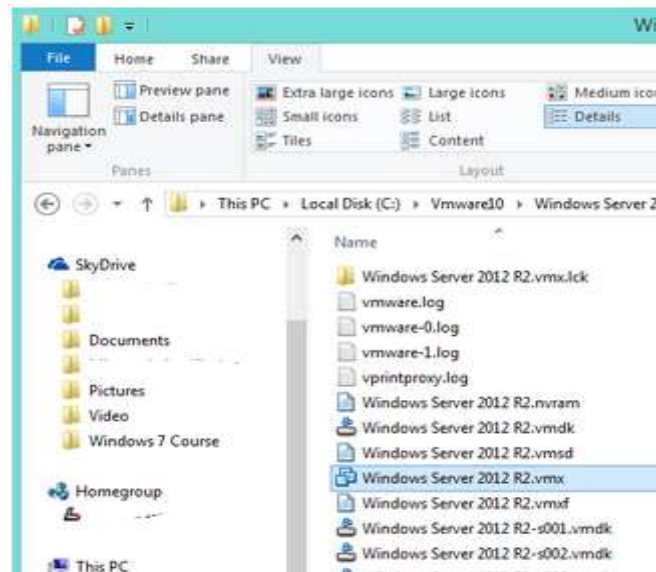
Key readings 1.2.3: Installation of Hypervisor

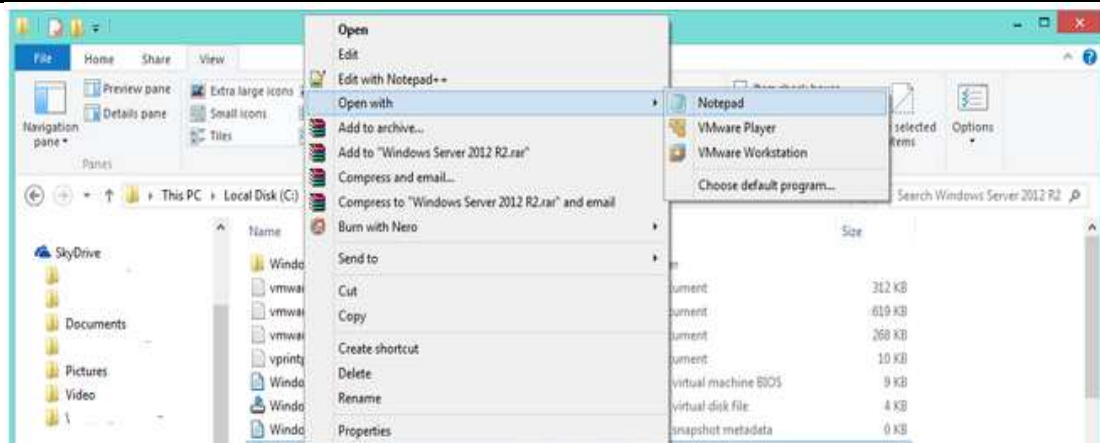
- To install a hypervisor, you'll generally follow these steps:

Step 1: Now Right Click on Virtual Machine and Power -> Power off the VM.



Step2: Now open the file Location for this Virtual Machine and open the file Extension (*.vmx) and open it with Notepad.



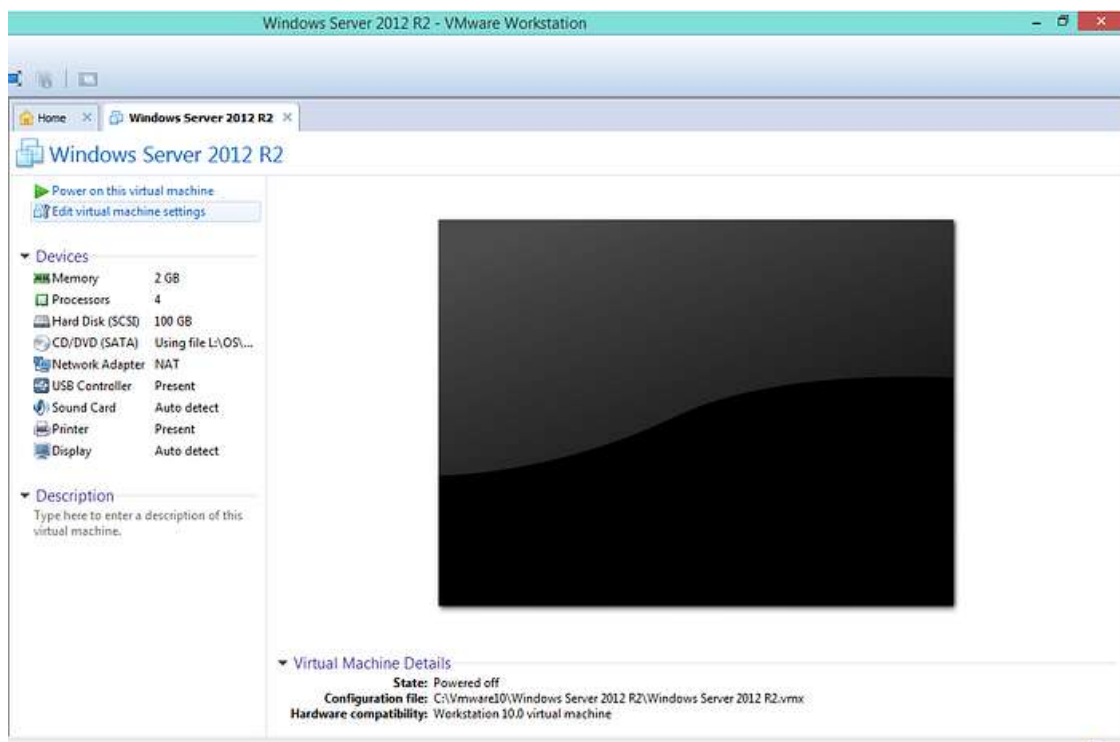


Step 3: In the last line we will add this code and save it: `hypervisor.cpuid.v0 = "FALSE"`
`mce.enable = "TRUE"`
`vhu.enable = "TRUE"`

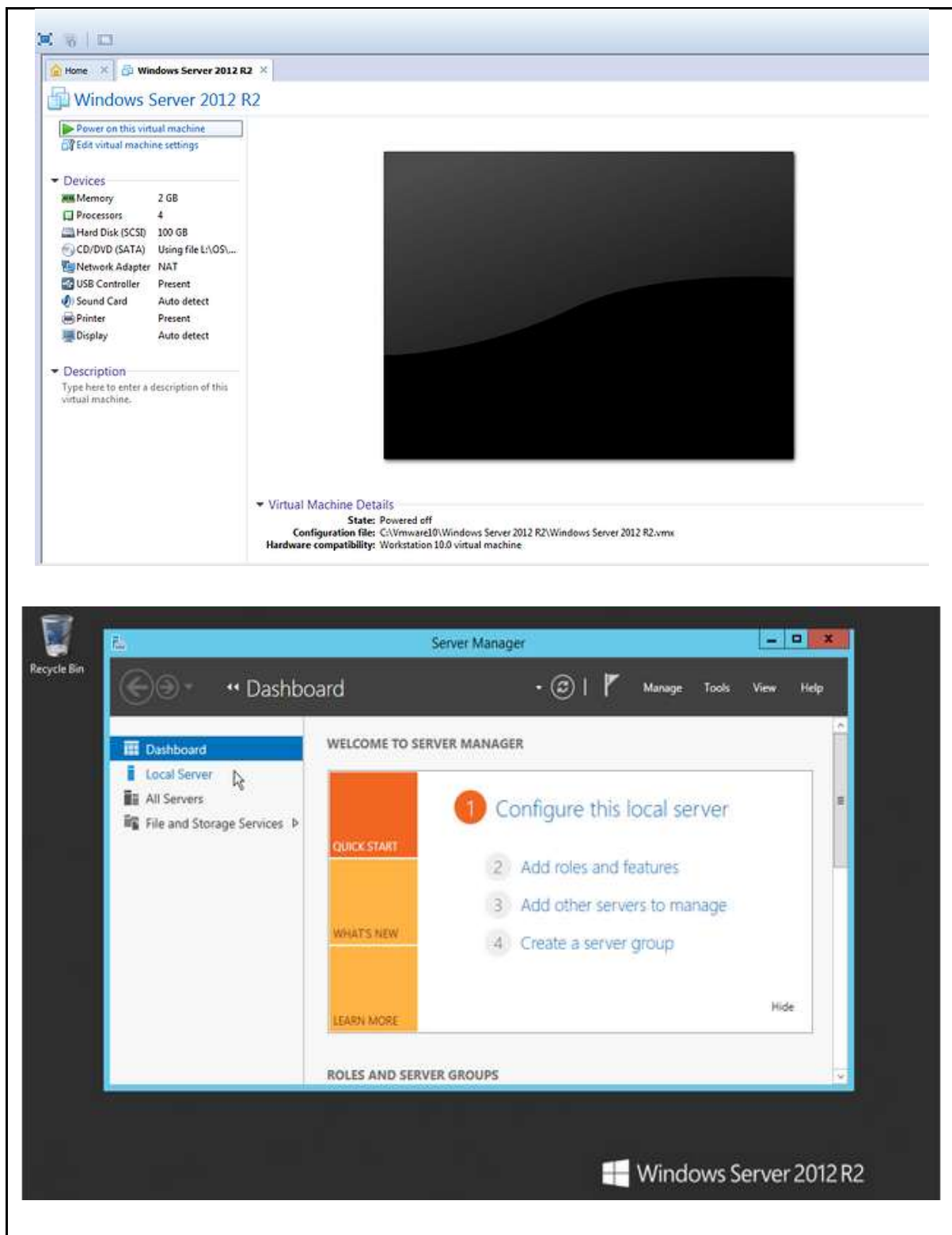
Step 4: After that edit the setting on VM from vmware workstation select Processors and check:

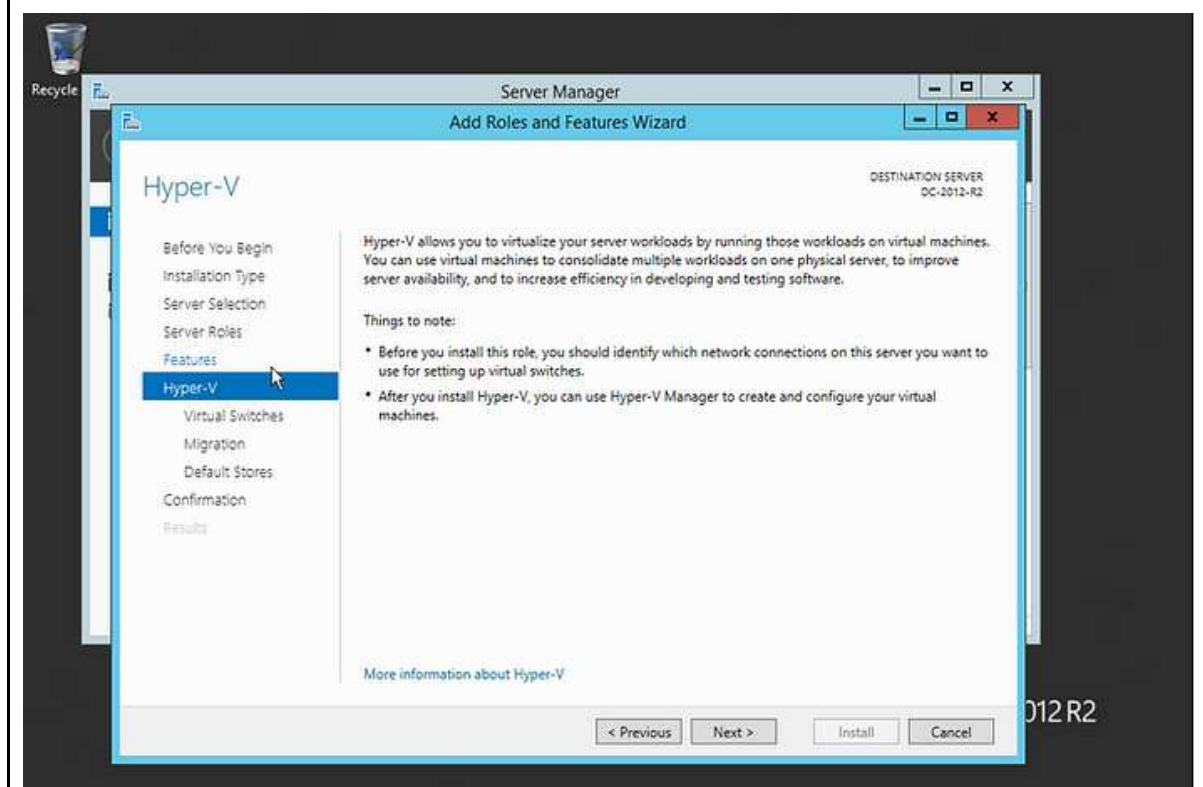
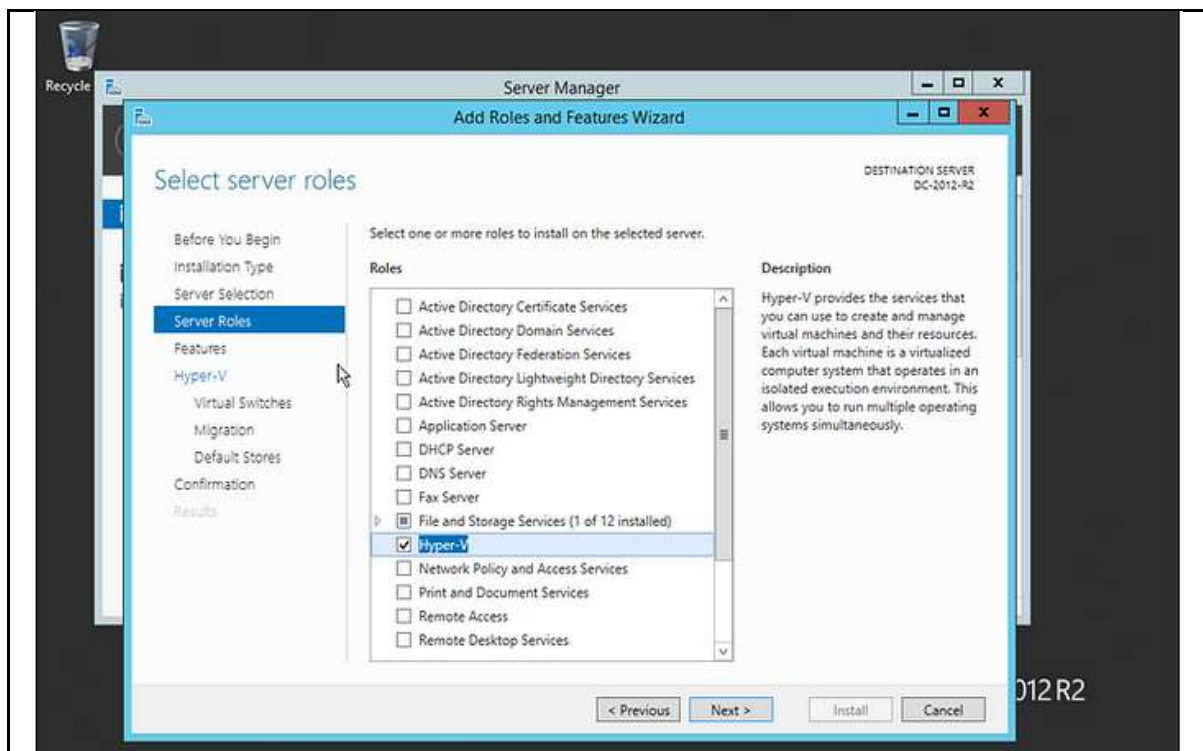
Virtualize Intel VT-x/EPT or AMD-V/RVI.

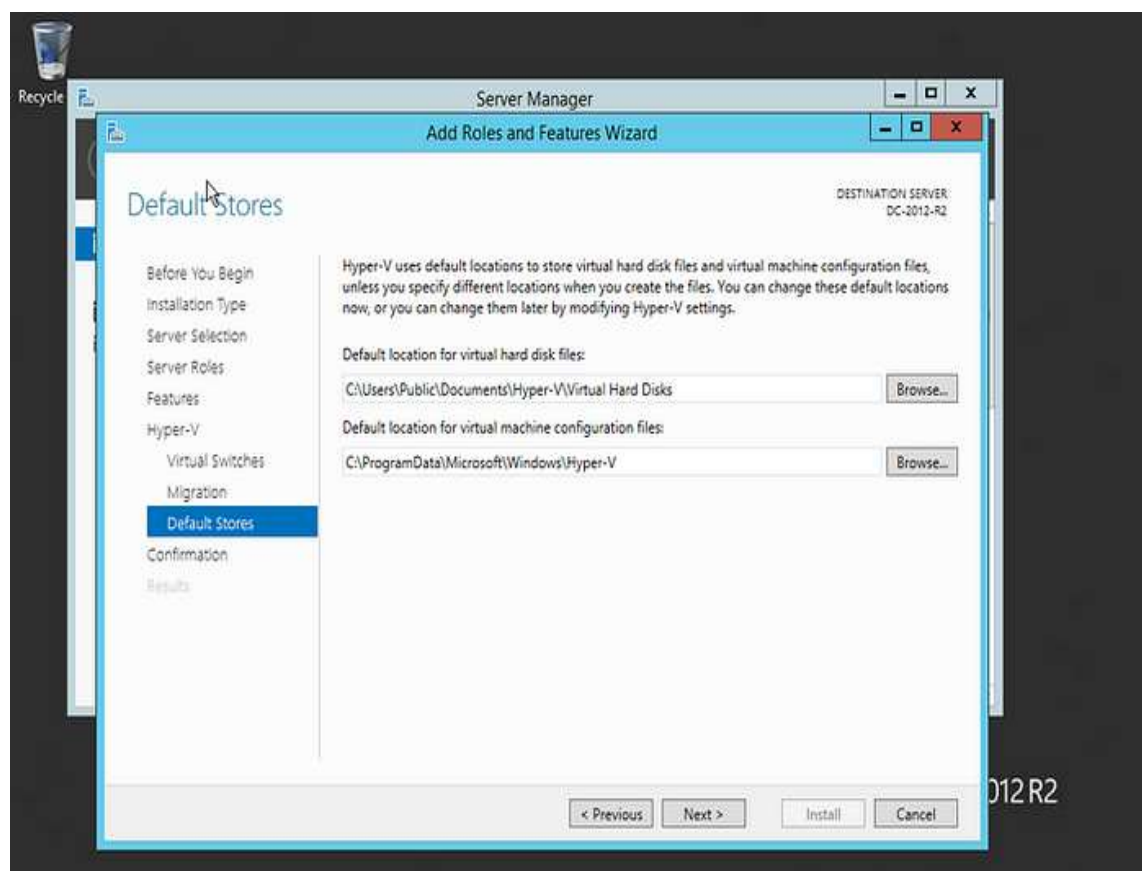
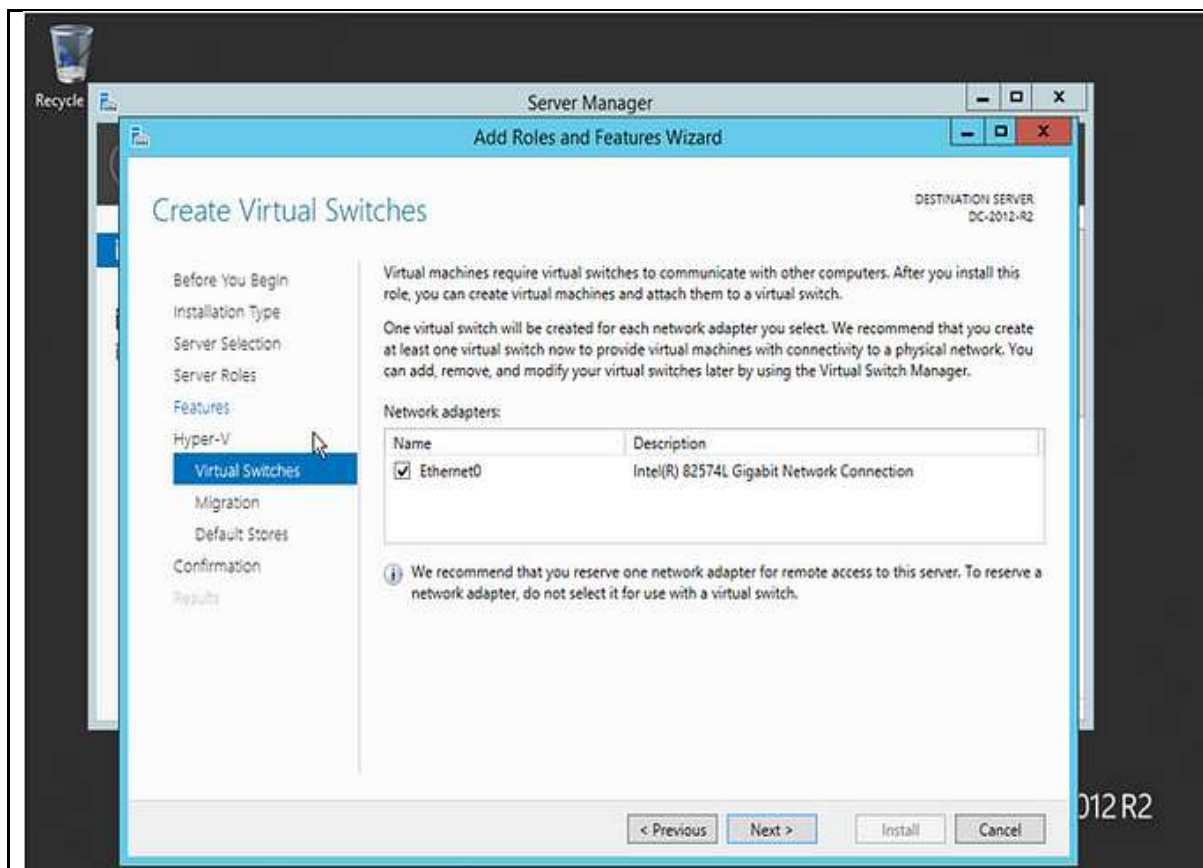
Virtualize CPU Performance counters.



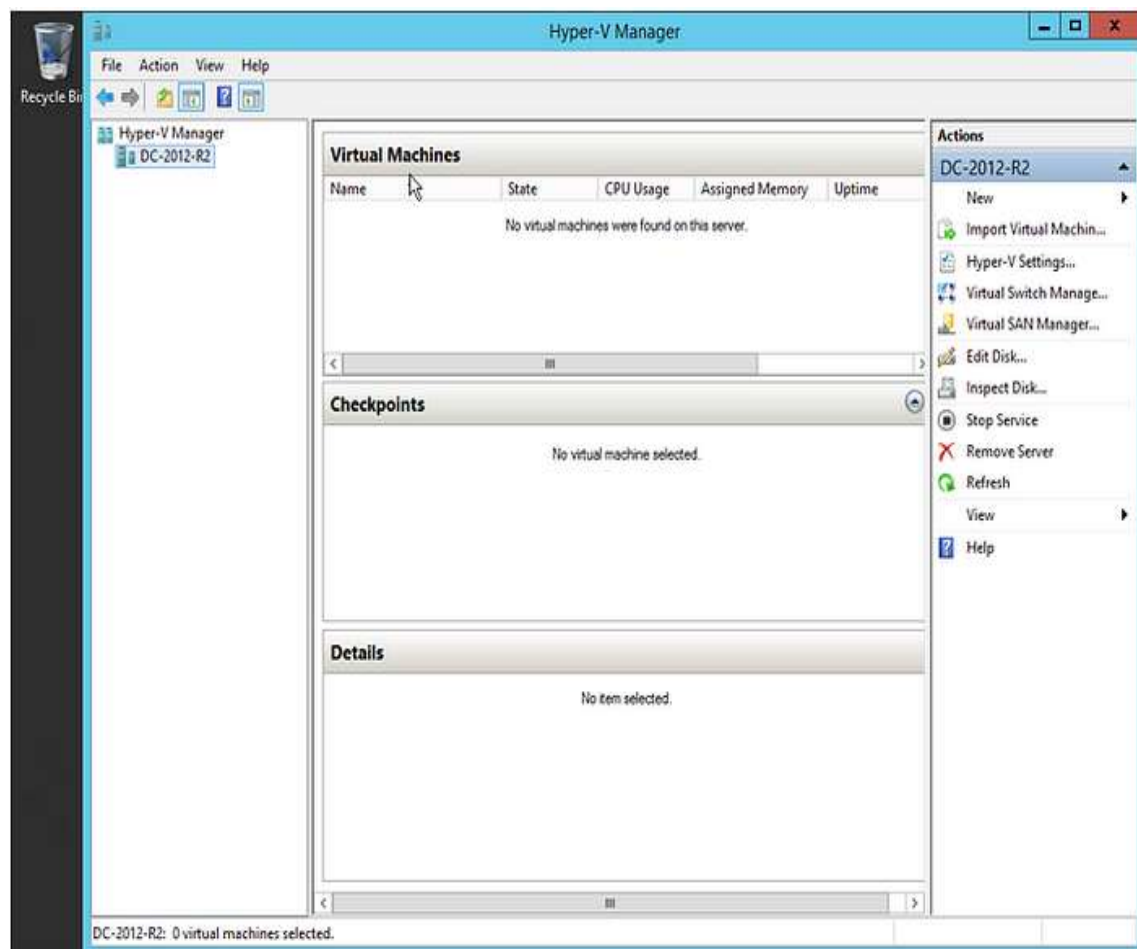
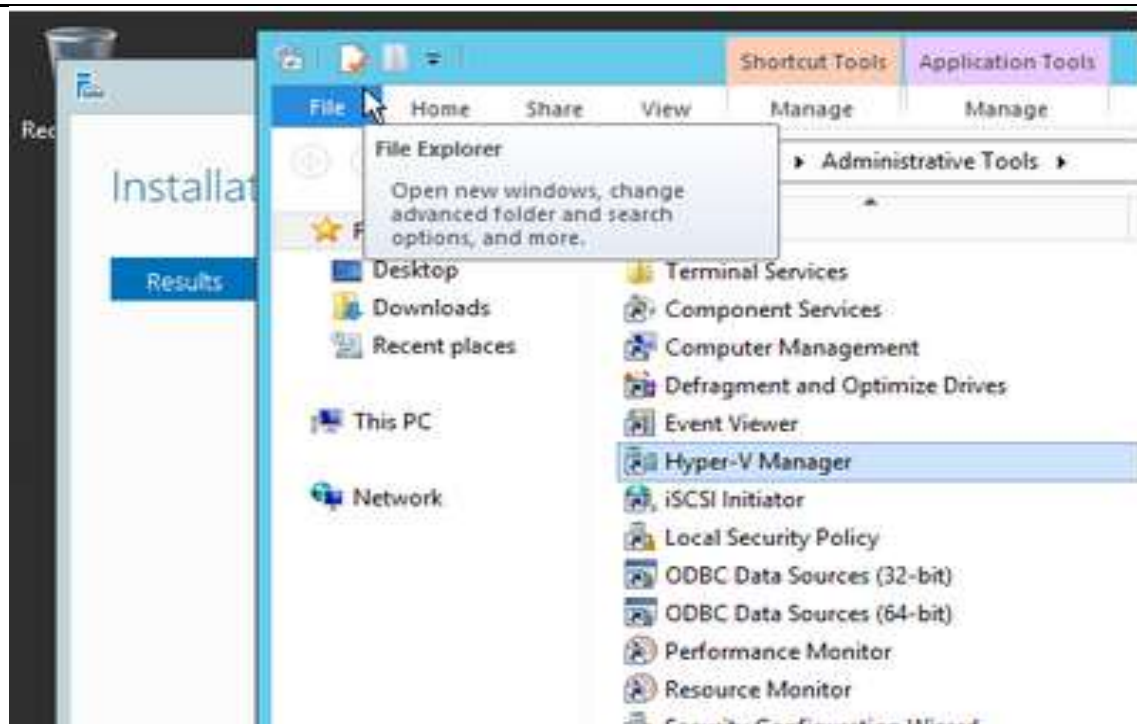
Step 5: Now the configurations is done, now Power on this virtual machine and install Hyper-V Role.



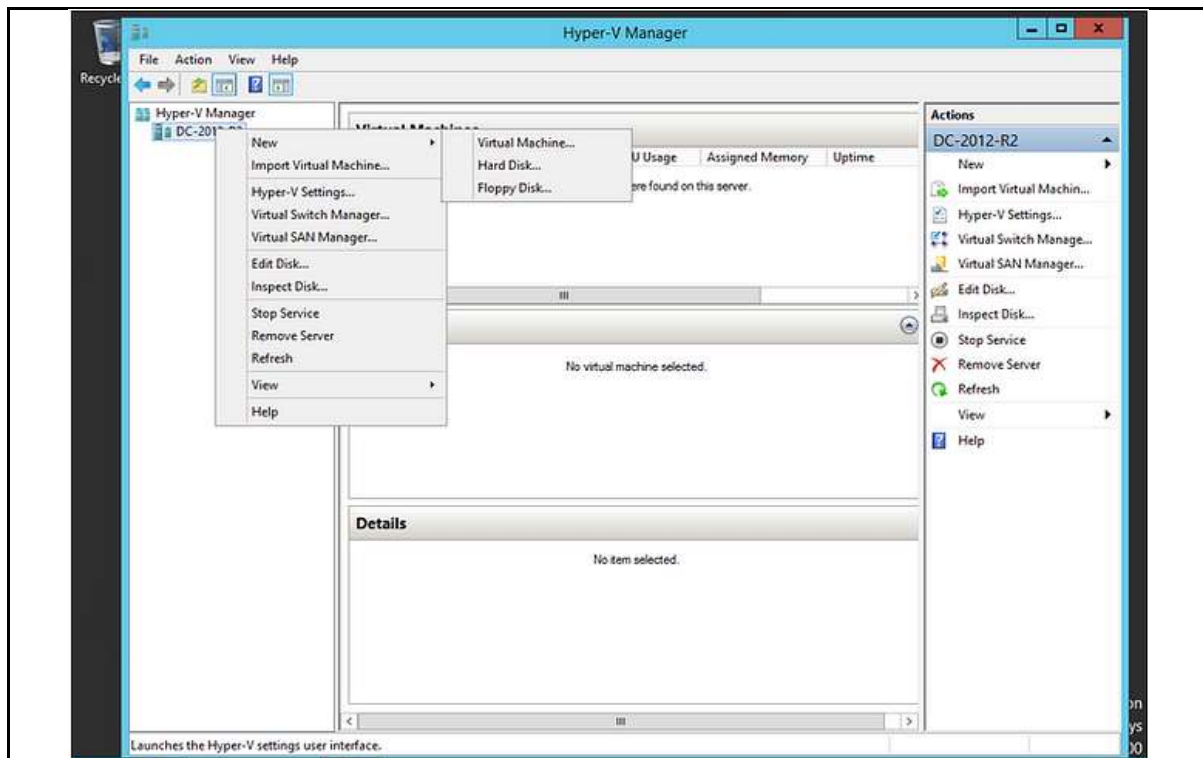




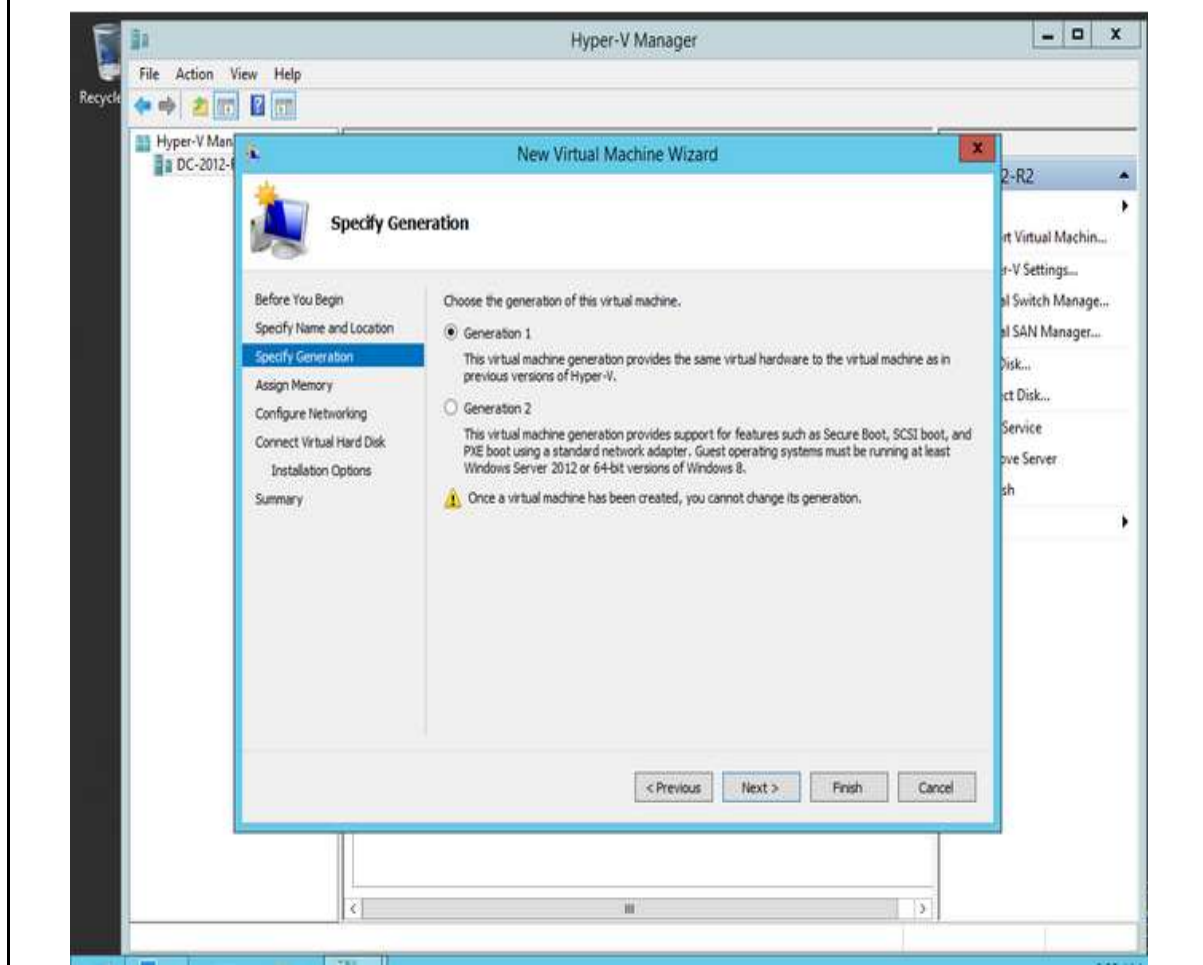
Step 6: After installing Hyper-V open the Hyper-V Manager from Administrative Tools.

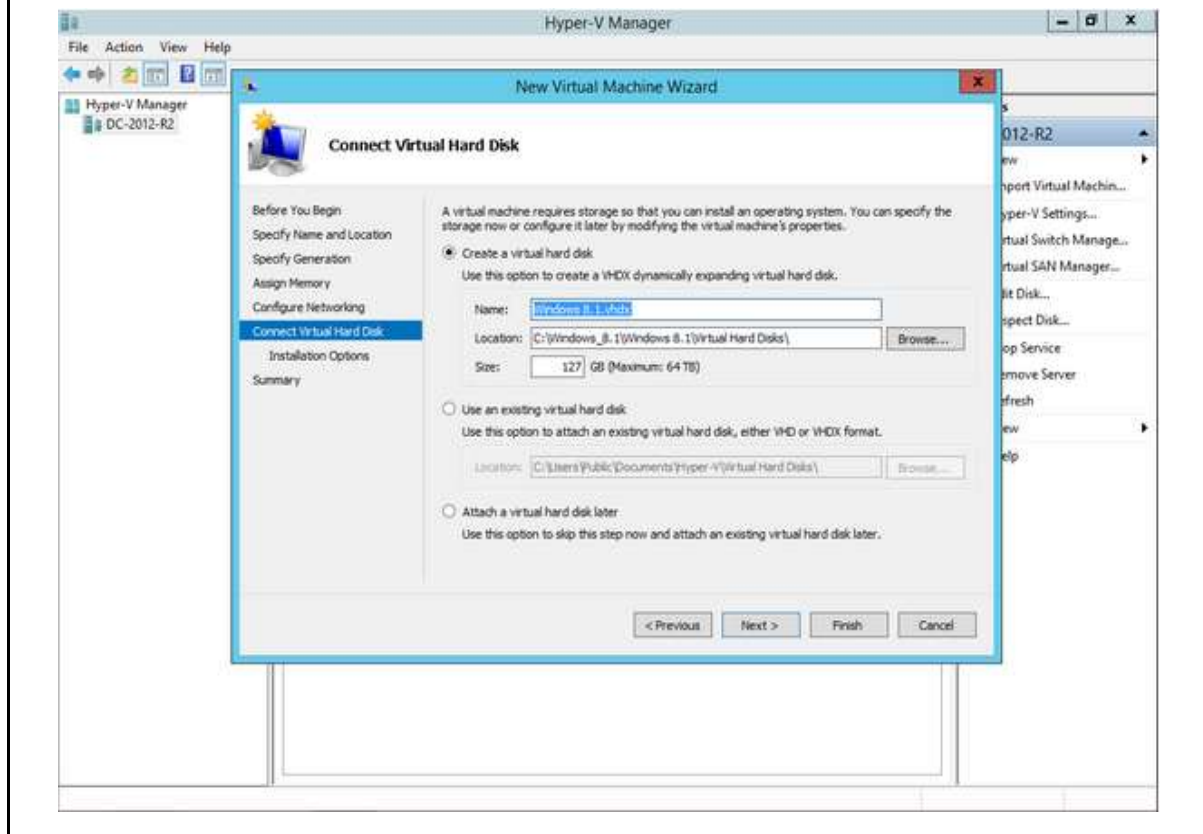
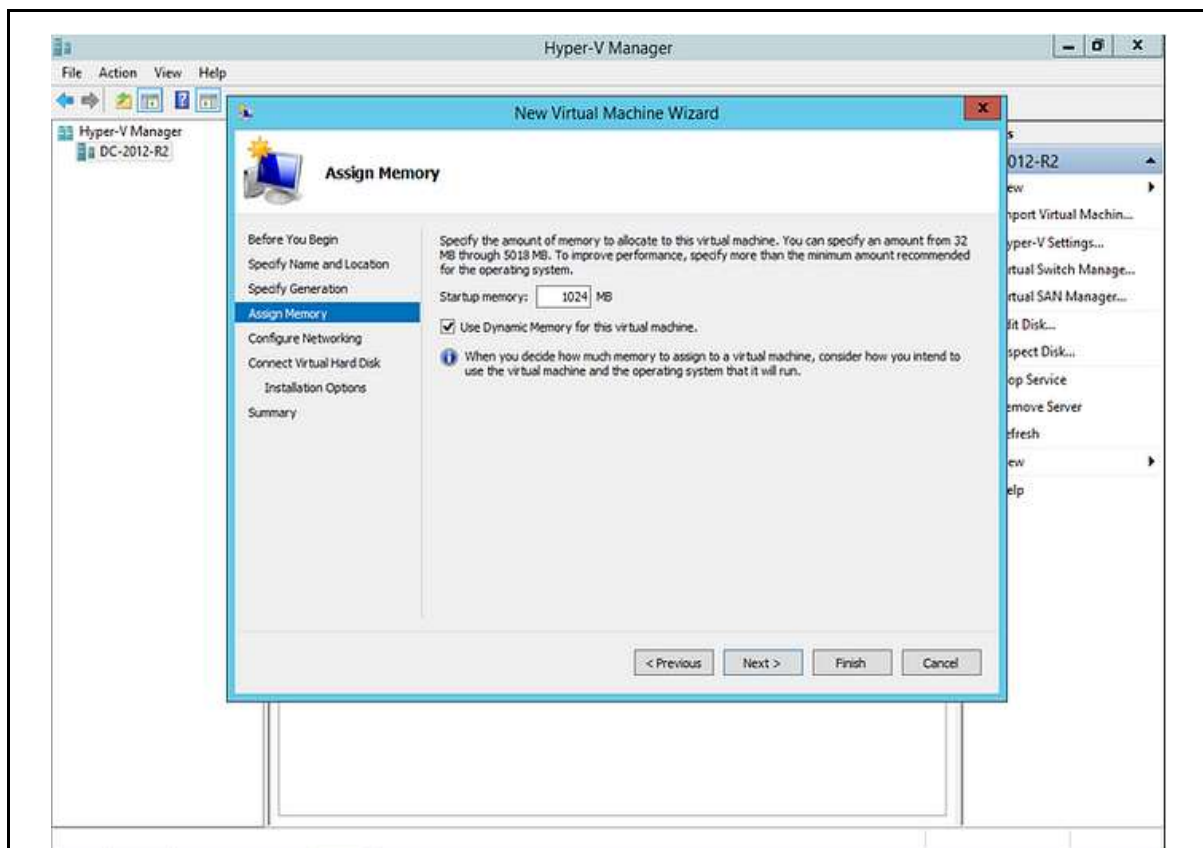


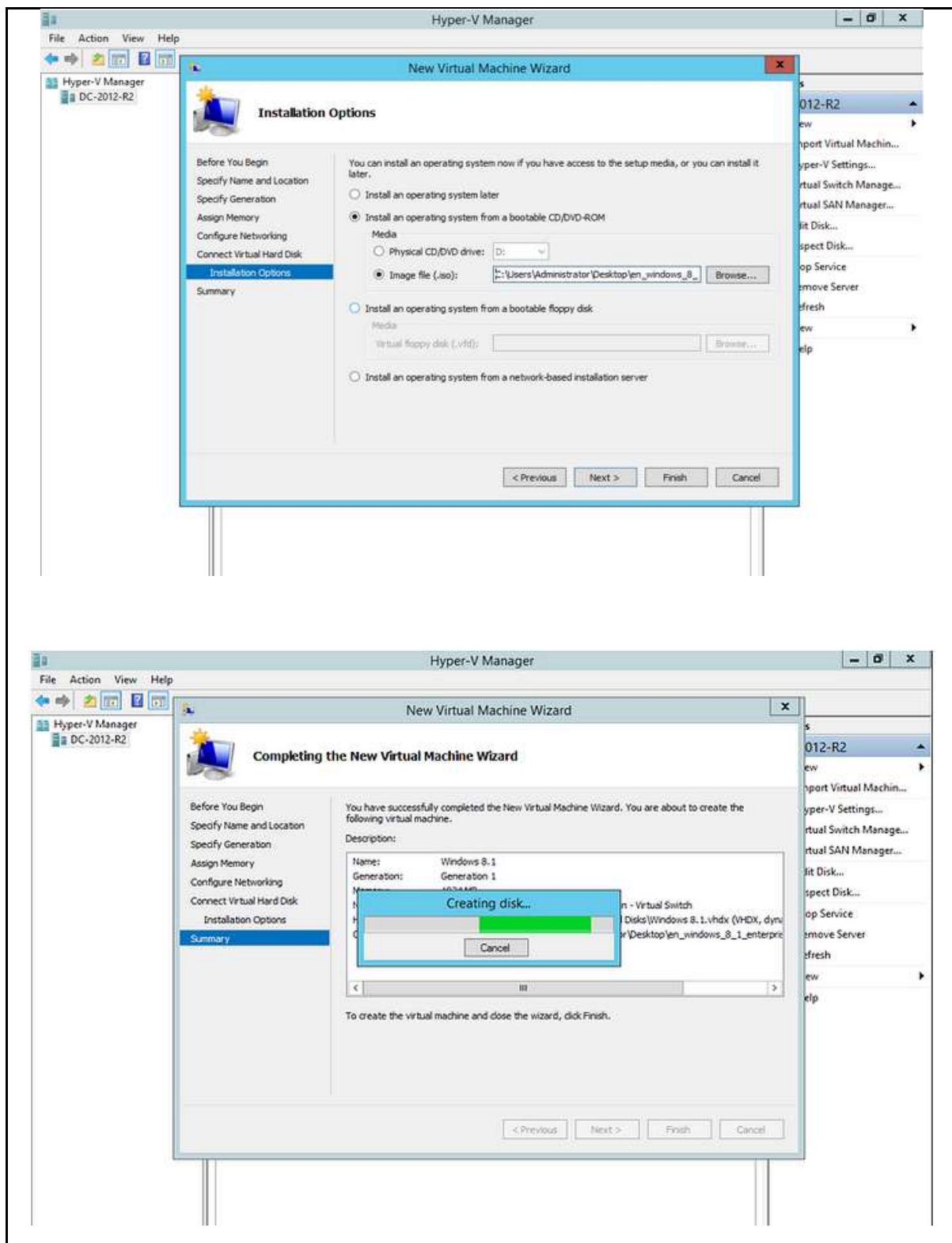
Step 7: And Create a New Virtual Machine for test.



Launches the Hyper-V settings user interface.









Practical Activity 1.2.4: Creating of virtual machines



Task:

1. You are asked to go to the computer lab and do the task below individually:
As a Trainee in Level 4 software development, you are requested to create a virtual machine on server.
2. Read the key readings 1.2.4 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

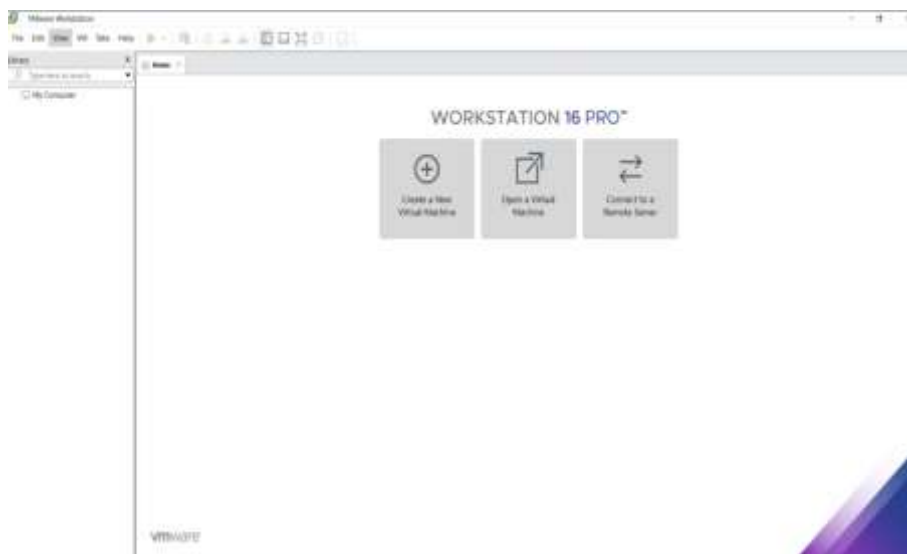


Key readings 1.2.4: Creation of virtual machines

Creating virtual machines (VMs) on VMware workstation

- **Creation of virtual machines**

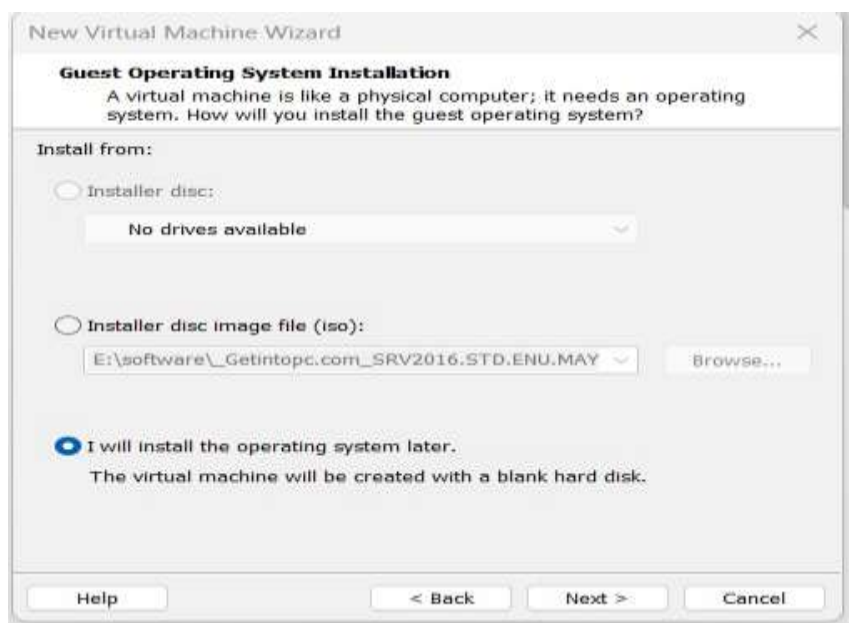
1. Open VMWare Workstation Pro
2. From the **Home** tab, click on the “**Create a New Virtual Machine**”



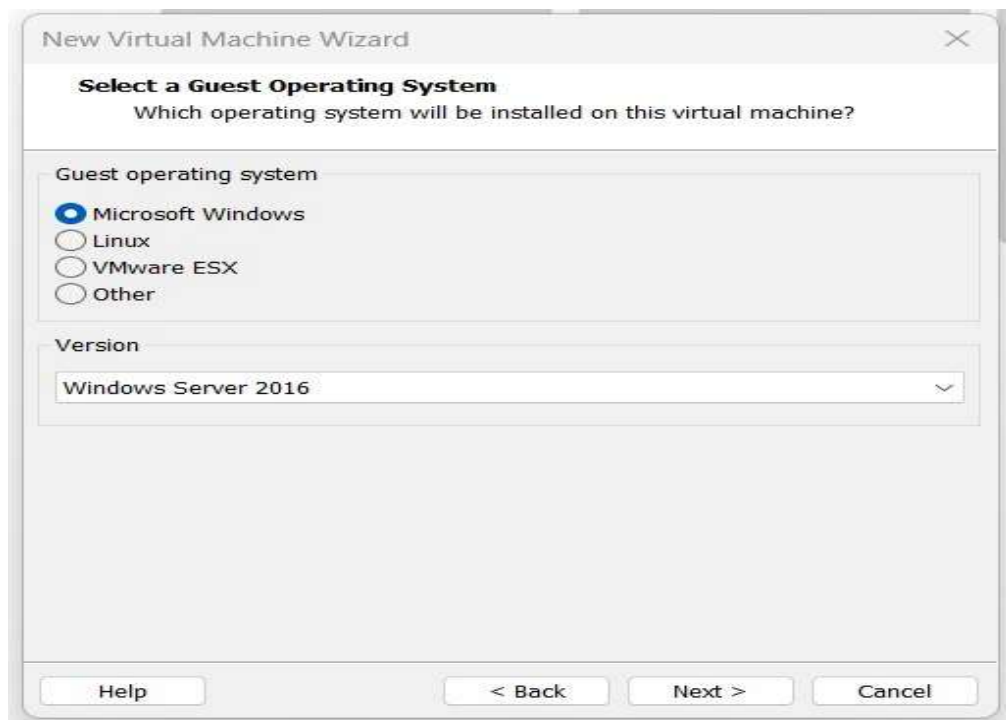
3. In a new window that opened asking What type of configuration do you want, select the “Typical (recommended)” and click Next



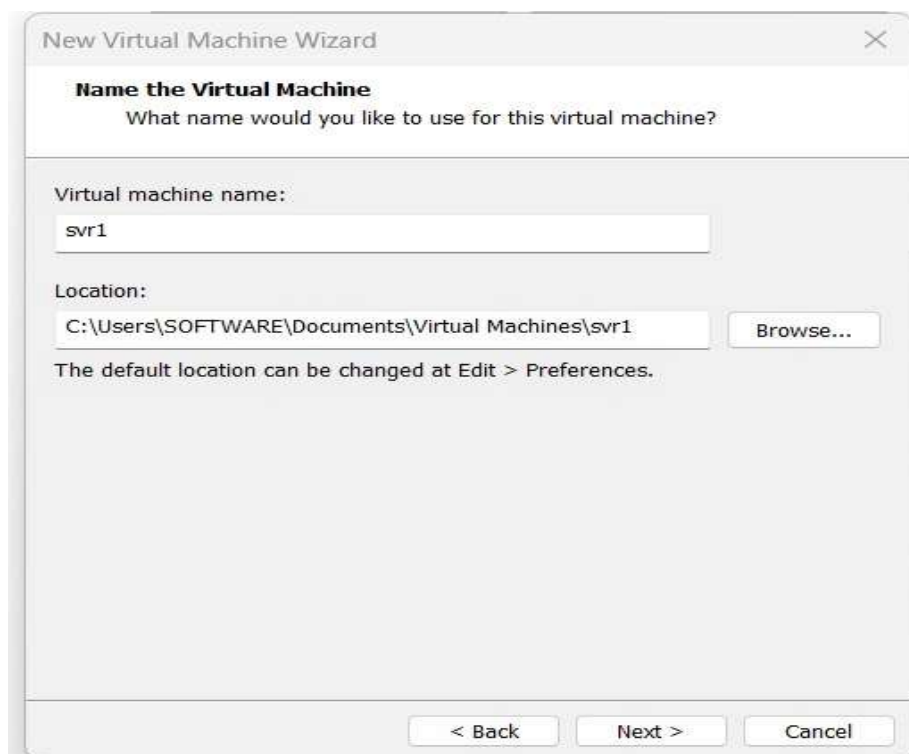
4. Then, select “I will install the operating system later” and click Next



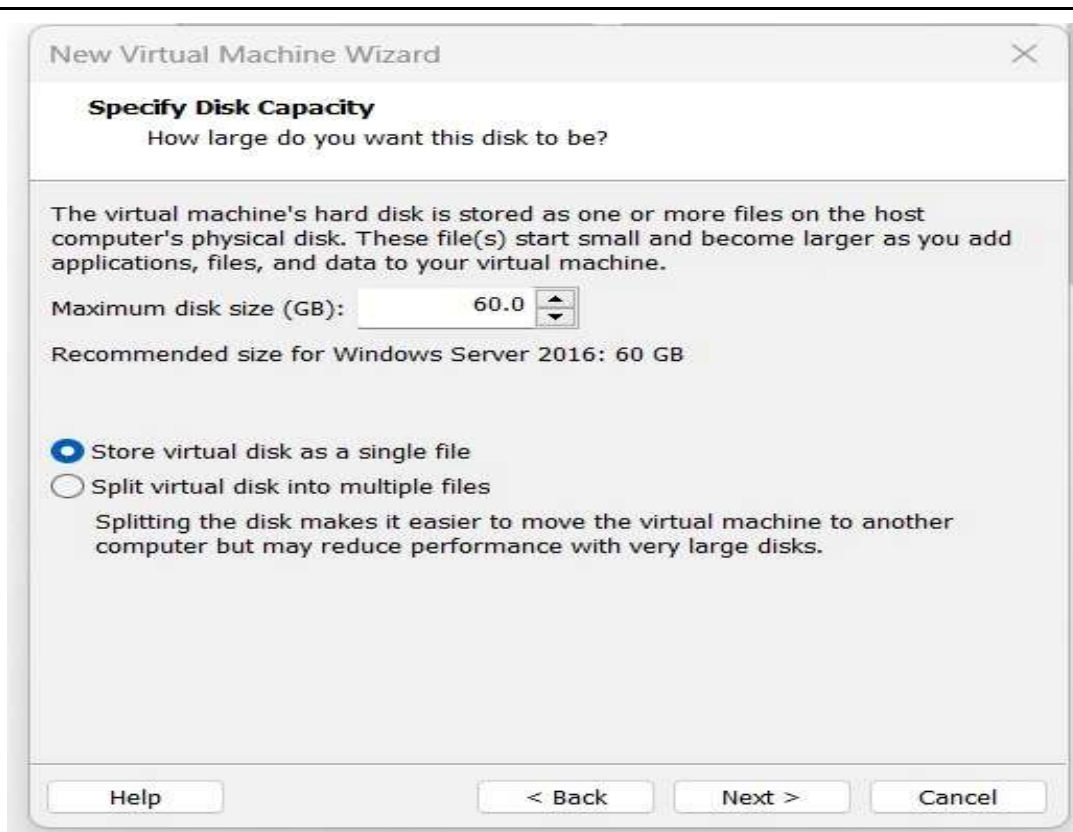
5. After that, select “Microsoft Windows”, set the Version to “Windows 10 x64” and click Next



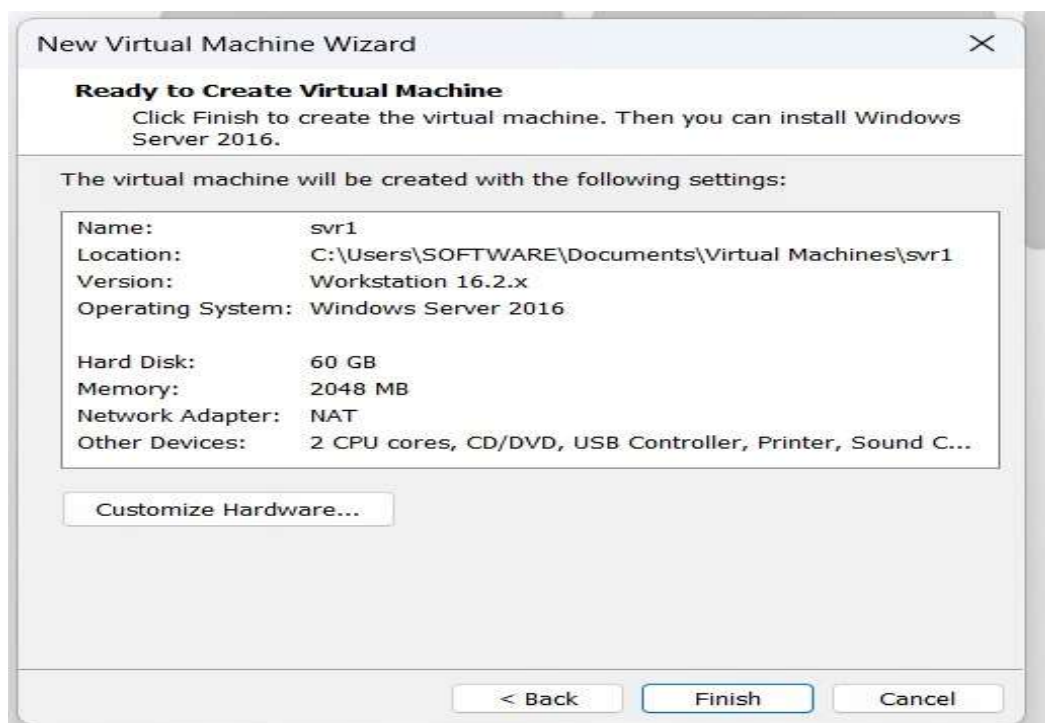
6. In the next screen you can give your Virtual Machine a unique name and select a different location. For this lab we will leave it as is and click on Next



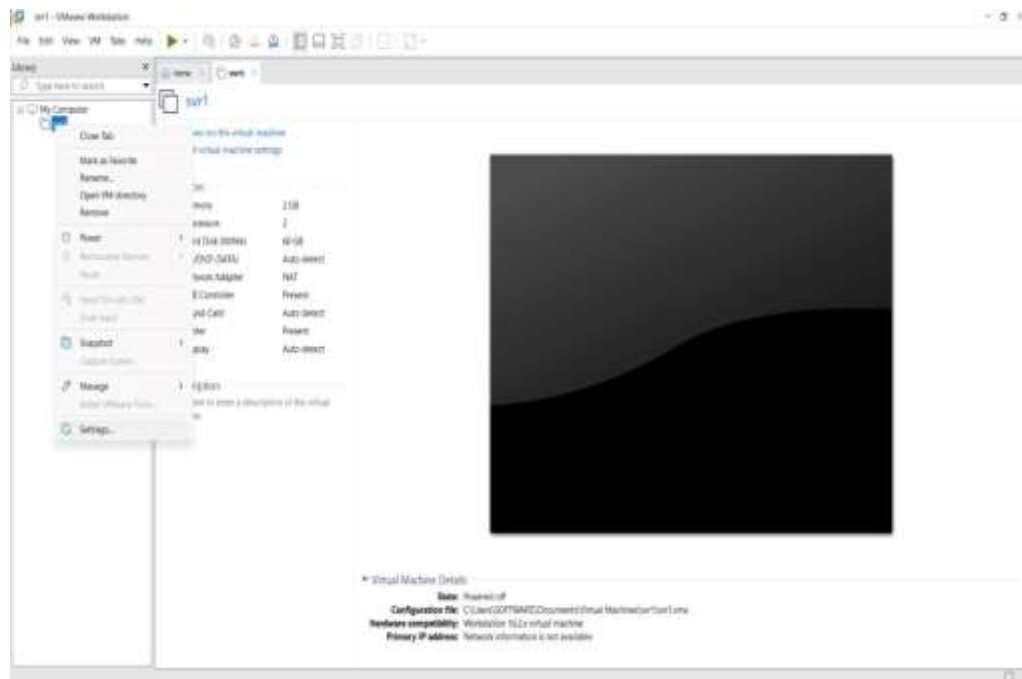
7. Next, set the Maximum disk size (GB): to 60.0, select "Store virtual disk as a single file" and click Next



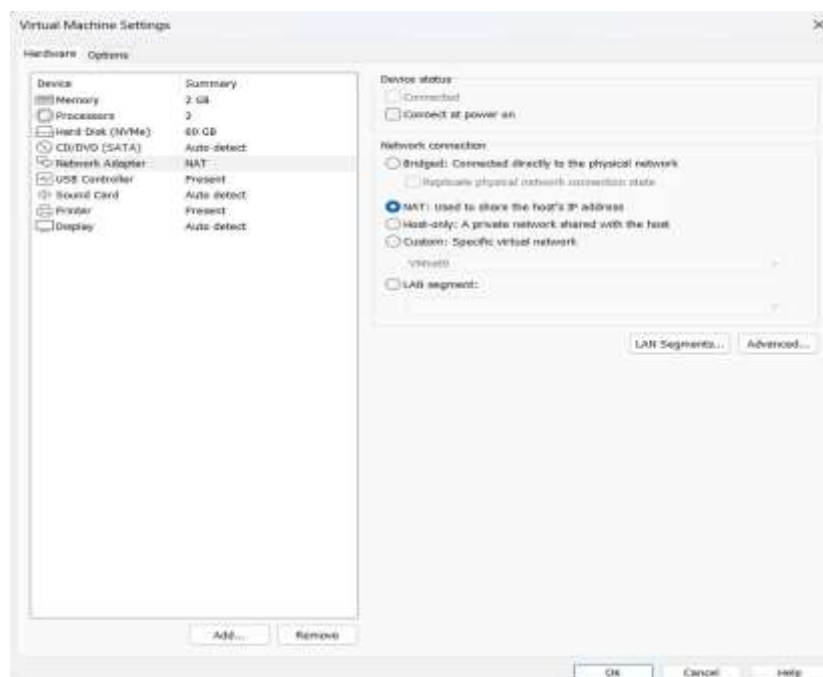
8. Check the final settings and click Finish



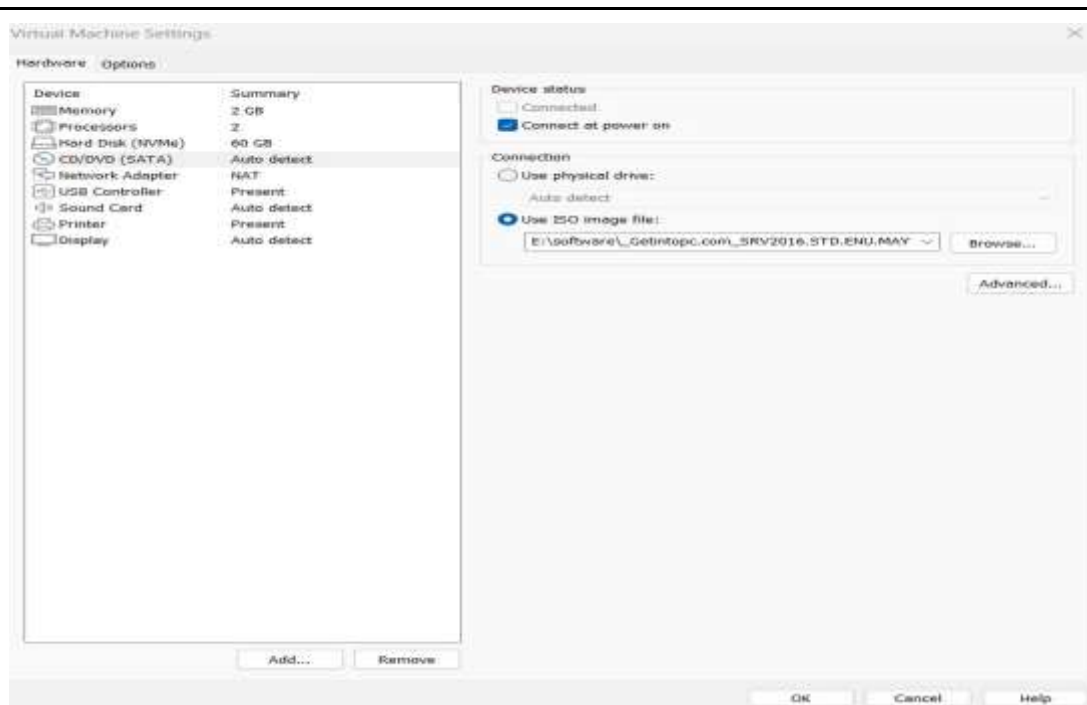
9. In the main VMWare Workstation view, right-click on your VM and from the drop-down menu select "Settings"



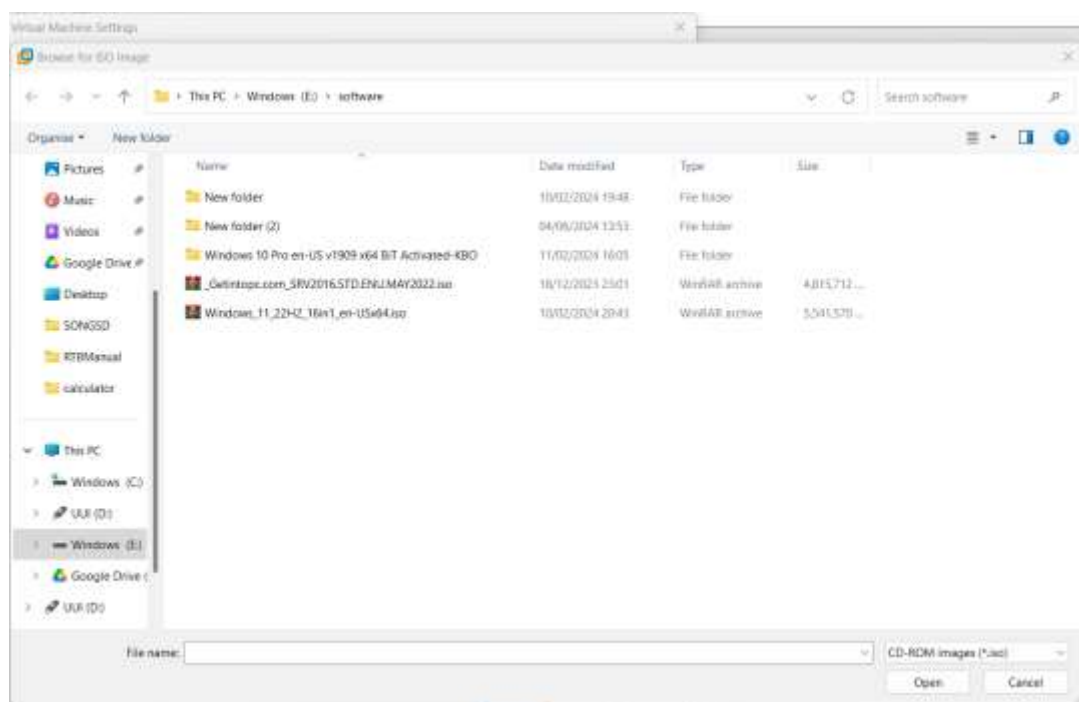
10. Temporarily disable the network adapter on your VM by selecting the Network Adapter from the list on the left and unchecking the "Connect at power on" option (on the right, under the Device status)



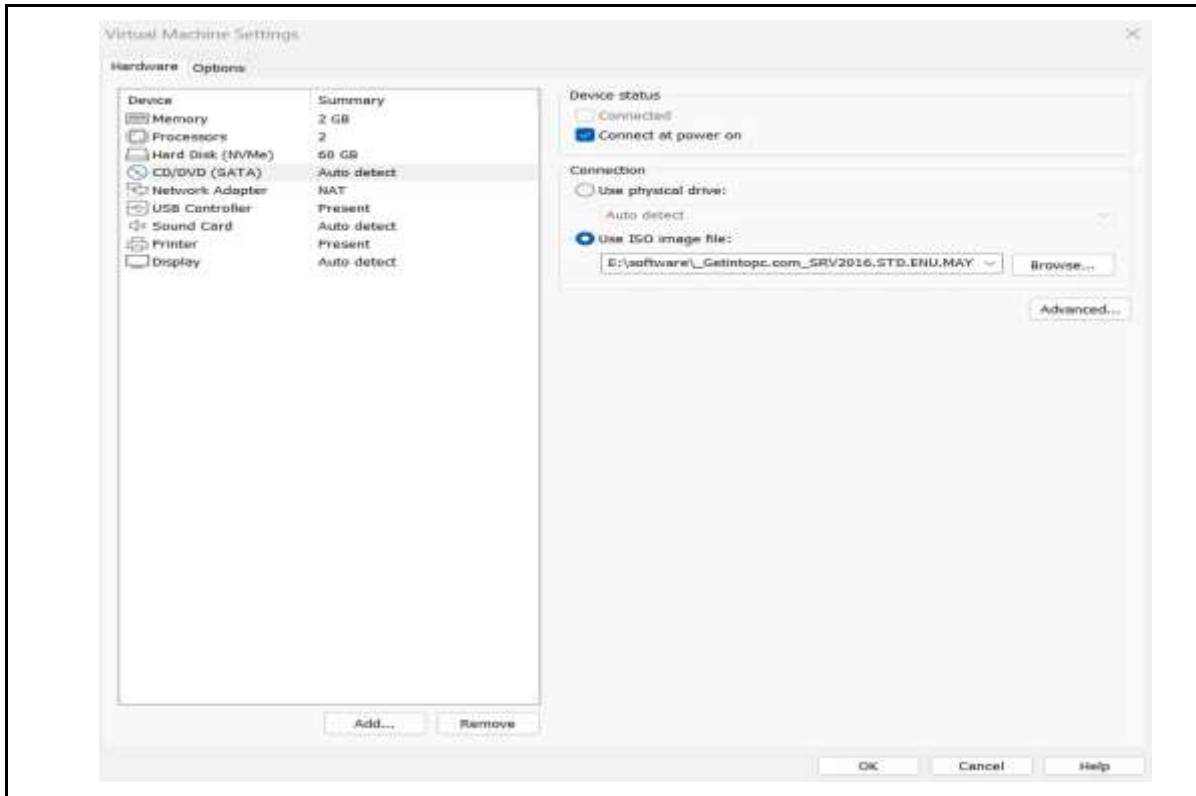
11. Select the CD/DVD (SATA) from the list on the left and select the "Use ISO image file"



12. Click on Browse to navigate to the iso image file on your PC, select the correct iso file and click Open



13. This will take you back into Virtual Machine Settings window from where you can click on OK to save the settings.



Practical Activity 1.2.5: Installation of guest OS



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Trainee in Level 4 software development, you are asked to Install the guest OS (win 7 or win 10) in VMware workstation.

2. Read the key readings 1.2.5 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



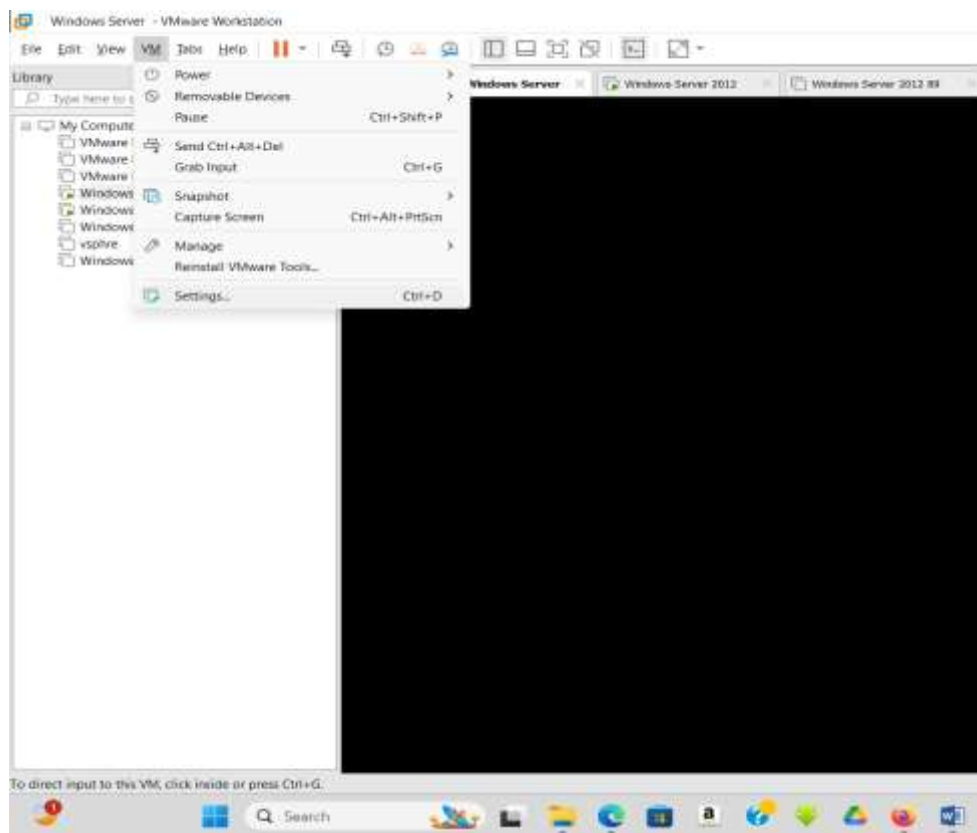
Key readings 1.2.5: Installation of guest OS

The steps to install a guest operating system (OS) in VMware Workstation:

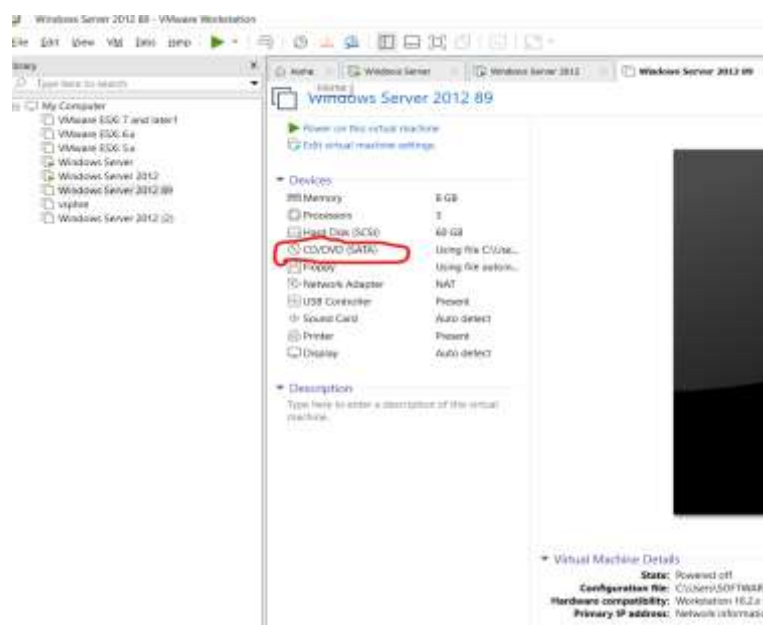
If you are installing the guest operating system from an ISO image file, configure the CD/DVD drive in the virtual machine to point to the ISO image file and configure the

drive to connect at power on.

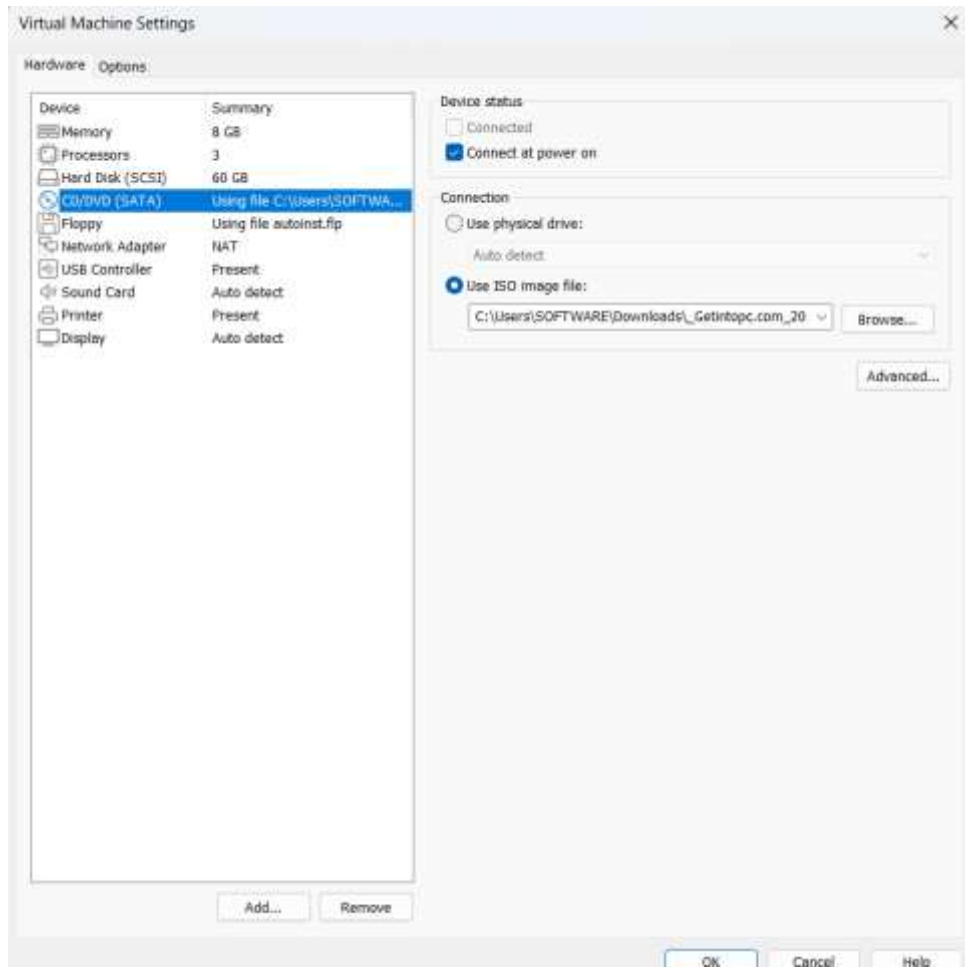
1. Select the virtual machine and select **VM > Settings**.



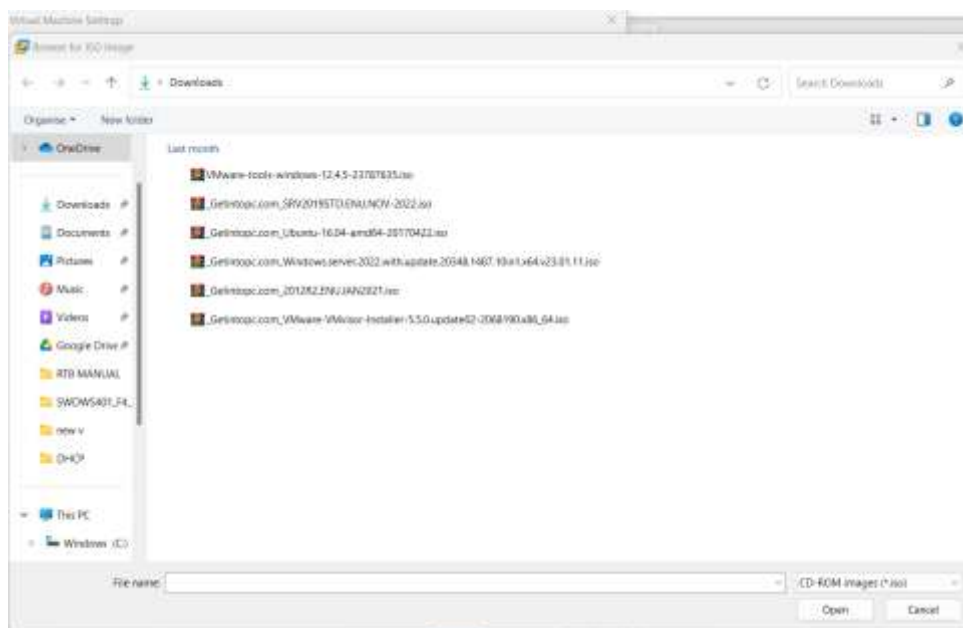
2. On the **Hardware** tab, select **CD/DVD drive**.



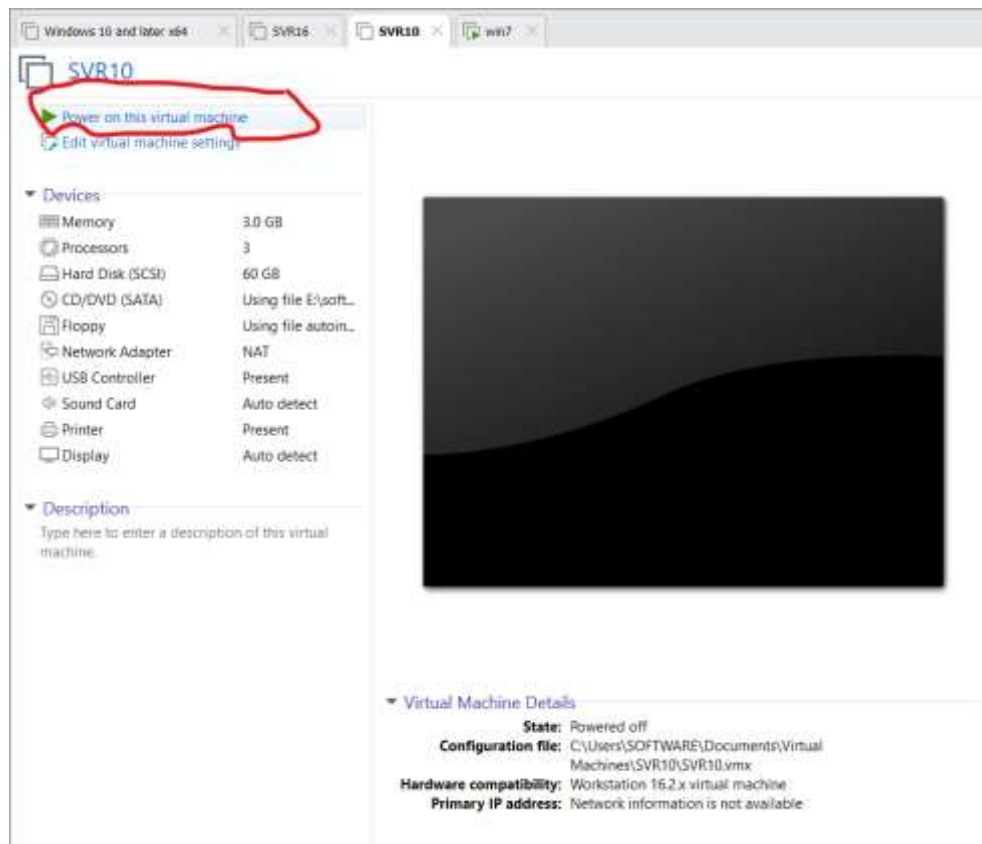
3. (Remote virtual machine only) Select the location of the ISO image file.



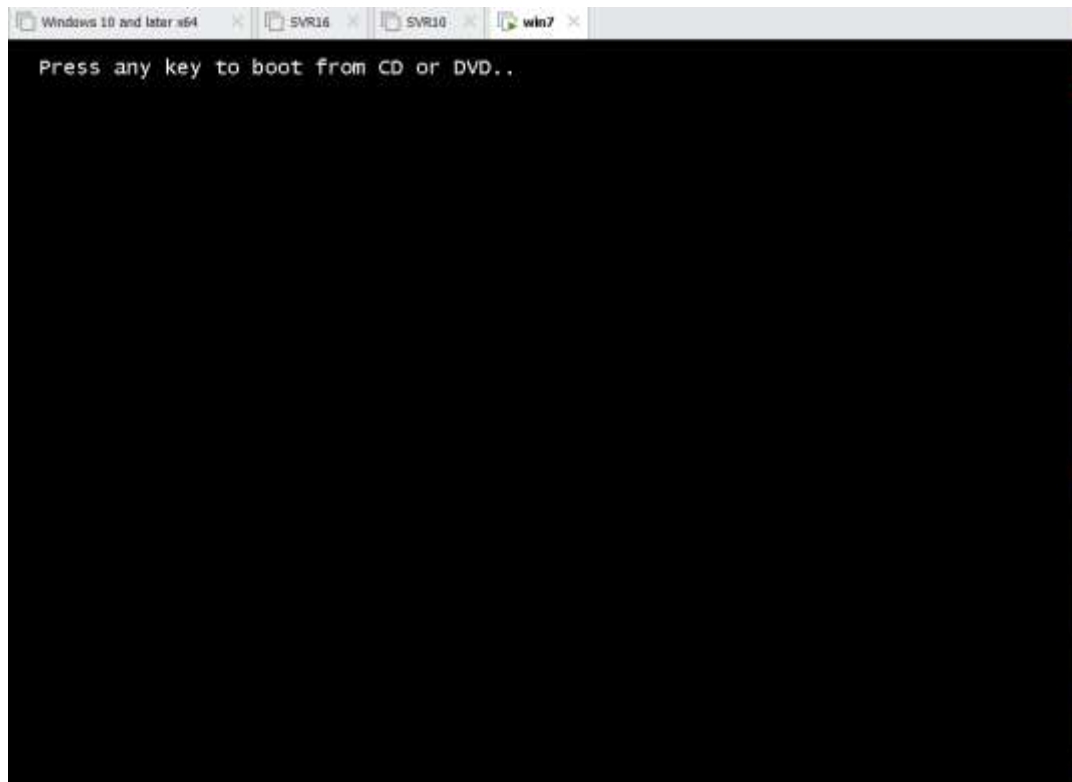
4. Select **Use ISO image file** and browse to the location of the ISO image file.

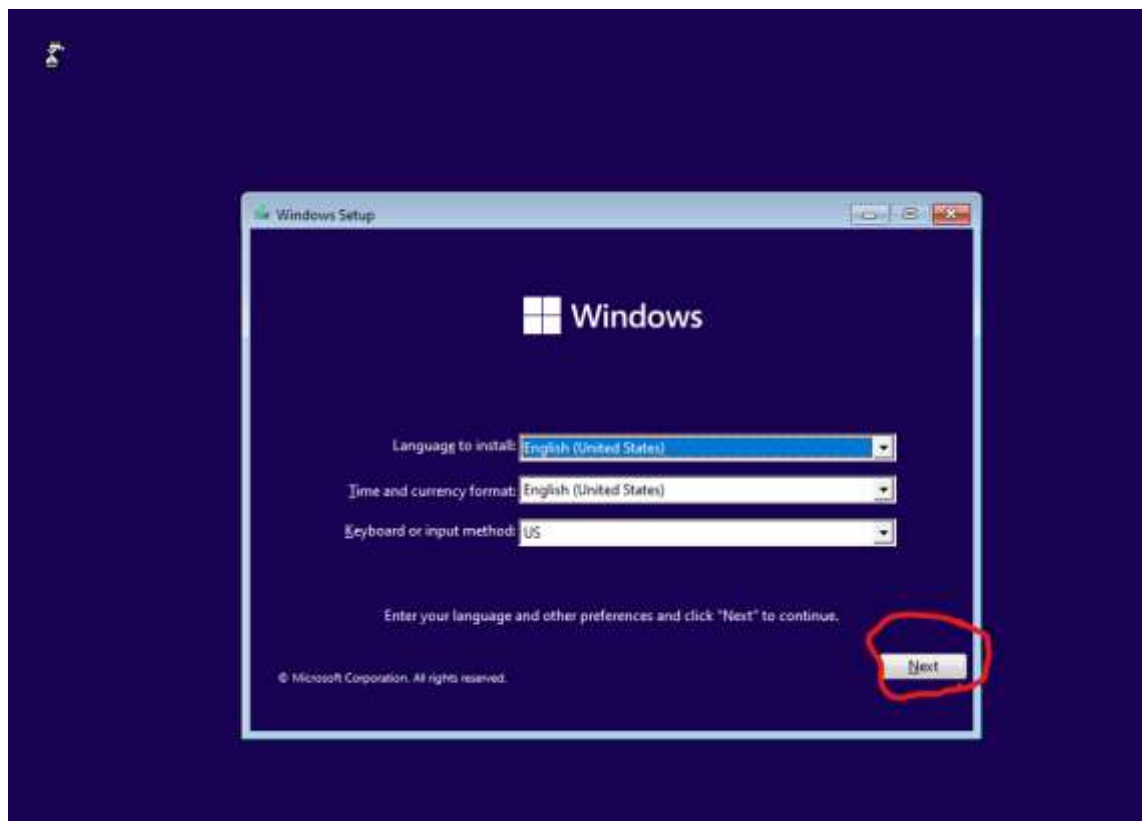


5. Select **Connect at power on.**

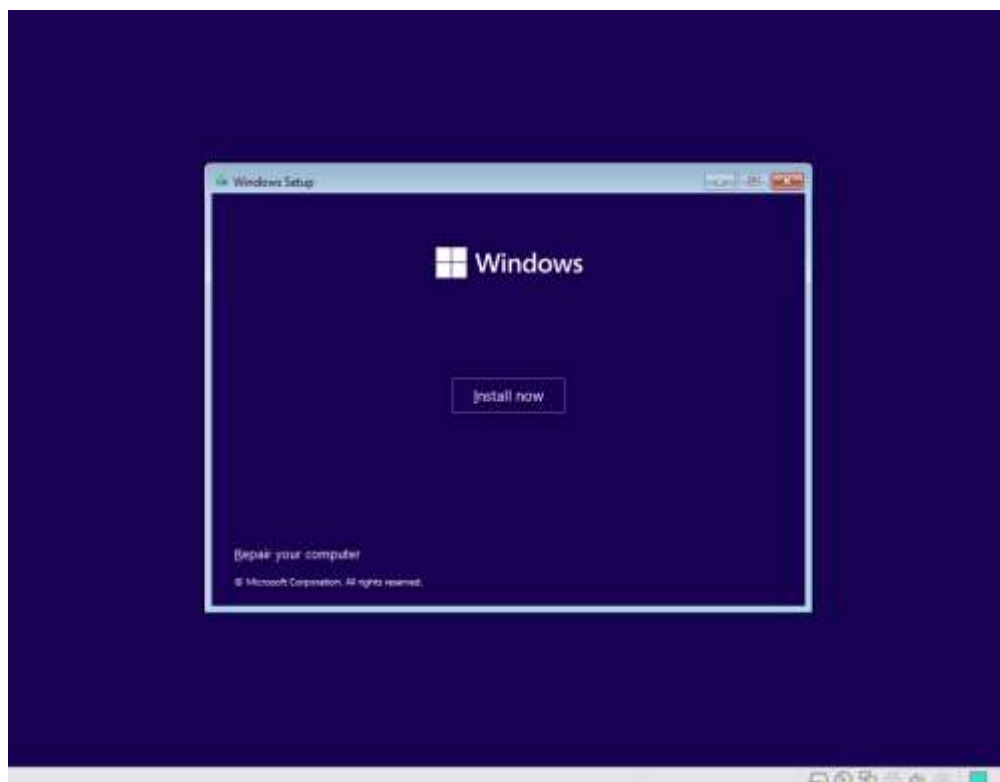


6. Press any key

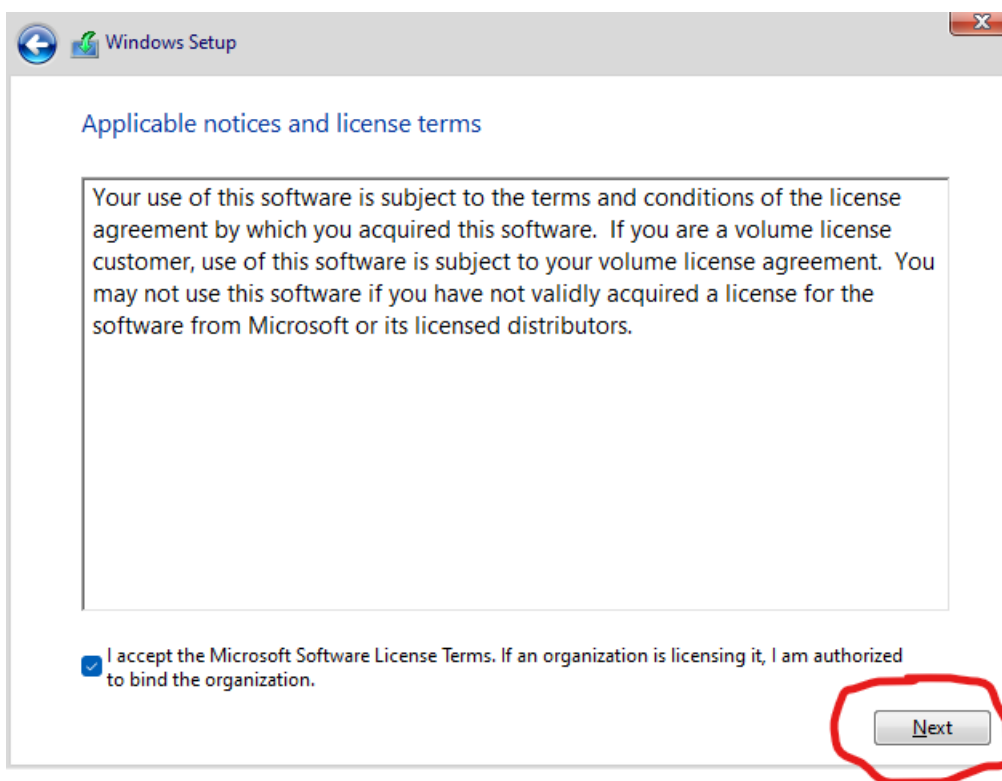
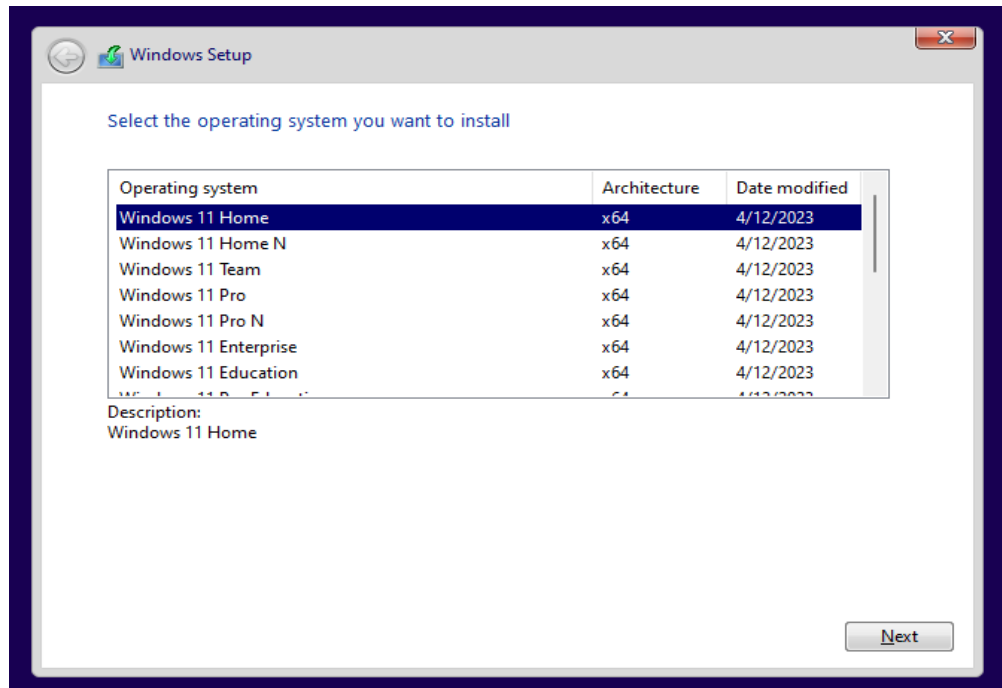


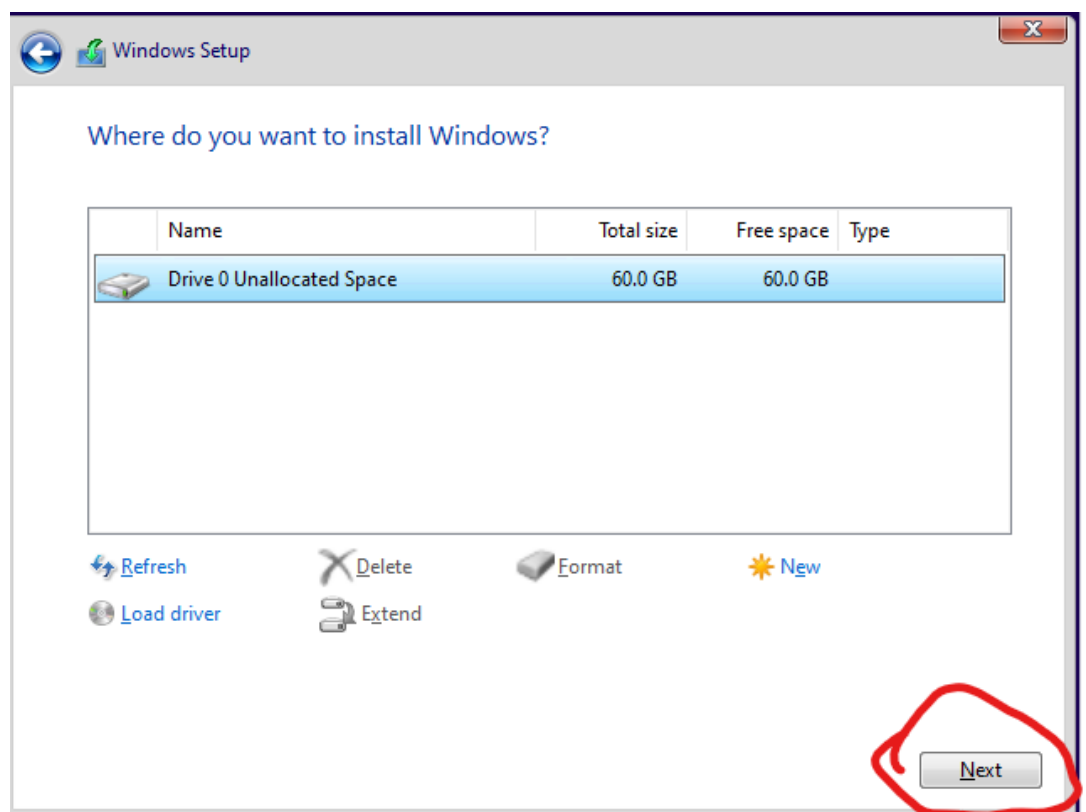
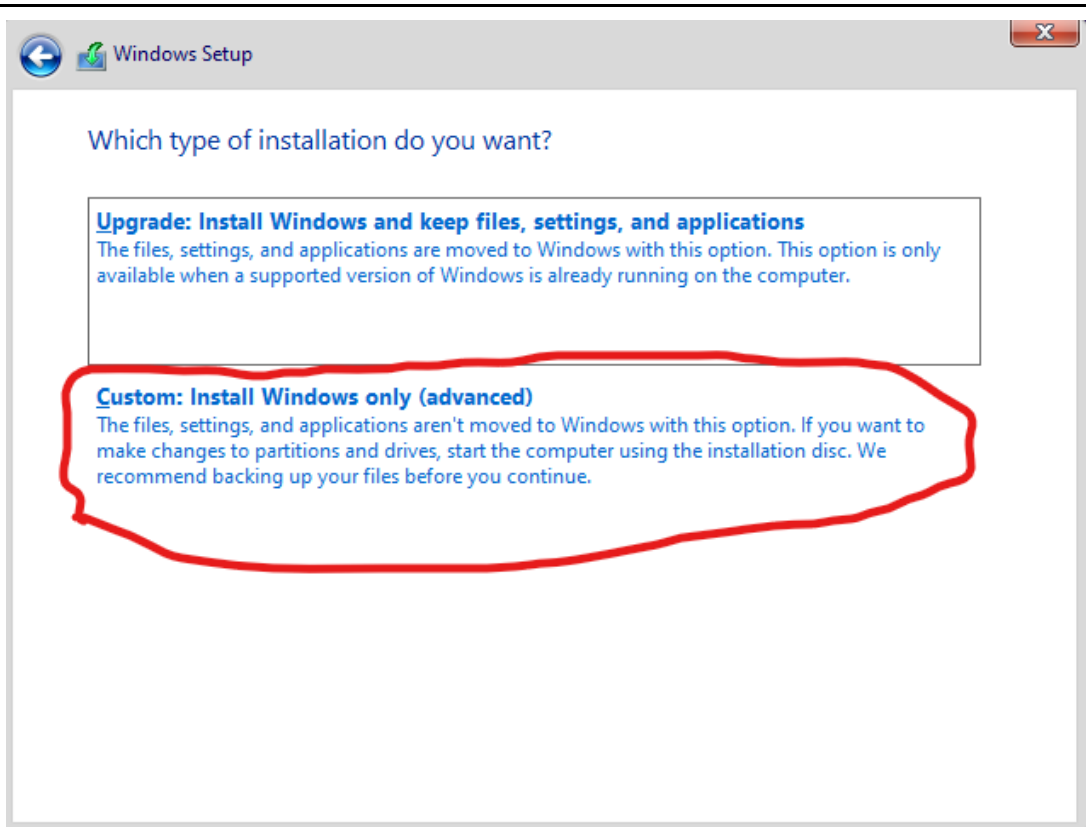


7. Install windows 7/10/11

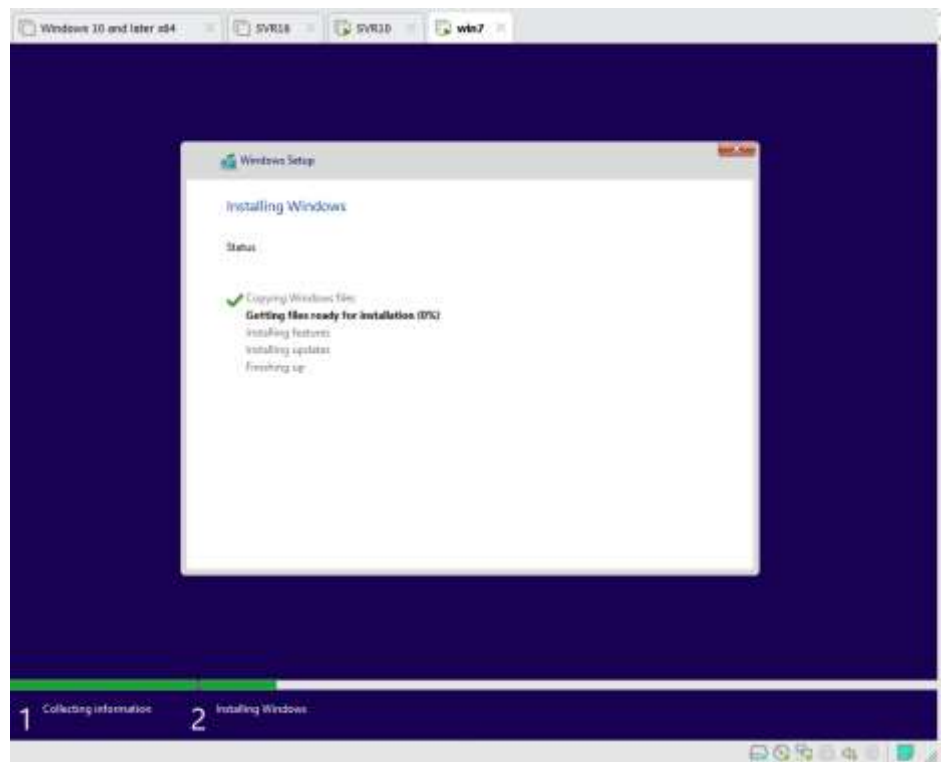


8. Select the operating system you want to install





9. Install windows (Dauti, 2024)



Points to Remember

Description of server OS

- RAID (Redundant Array of Independent Disks) combines multiple physical disks into a single logical unit to improve performance, redundancy, and/or storage capacity.
- RAID Levels are RAID 0 (Striping), RAID 1 (Mirroring), RAID 5 (Striping with Parity), RAID 6 (Striping with Double Parity), RAID 10 (1+0) (Striping and Mirroring).
- Advantages of RAID Technology are: Performance, redundancy, storage efficiency.
- Disadvantages of RAID Technology are: Cost, complexity, performance Trade-offs.

Creating virtual storage (RAID)

- To Create of Virtual Storage (RAID) on physical server follow steps:
 - ✓ Enter System Setup by pressing F2 at startup.
 - ✓ Navigate to **Device Settings**.
 - ✓ Select the appropriate **RAID controller**.
 - ✓ Access the **Main Menu**.

- ✓ Go to **Configuration Management**.
- ✓ Select **Create Virtual Disk**
- ✓ Confirm by checking the box and clicking **Yes**.
- ✓ The virtual disk is created successfully; click **Ok** to finish.

Installation of Hypervisor

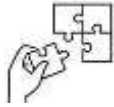
- To install a hypervisor in a virtual machine (VM), you'll generally follow these steps:
 - ✓ Prepare Your Environment
 - ✓ Create a New Virtual Machine
 - ✓ Install the Operating System
 - ✓ Install the Hypervisor: choose a hypervisor like VMware ESXi, Hyper-V, or another one.
 - ✓ Configure the Hypervisor
 - ✓ Test and Verify

Creation of virtual machines

- To Create of virtual machine, follow these steps:
 - ✓ Open VMWare Workstation Pro
 - ✓ From the **Home** tab, click on the "**Create a New Virtual Machine**"
 - ✓ In a new window that opened, select the "Typical (recommended)" and click Next
 - ✓ Then, select "I will install the operating system later" and click Next

Installation of guest OS

- To install a guest operating system (OS) in VMware workstation follow steps:
 - ✓ Select the virtual machine and go to **VM > Settings**.
 - ✓ Select **CD/DVD drive**, choose **Use ISO image file**, and browse to the ISO location.
 - ✓ Enable **Connect at power on**.
 - ✓ Press any key to start the OS installation and follow the prompts.



Application of learning 1.2.

Bxz Solutions Inc. is a company specializing in providing IT solutions for small and medium businesses. It aims to enhance its infrastructure by setting up a new server environment to improve its virtualization capabilities and manage its data efficiently. As a System Administrator, you are requested by Bxz Solutions Inc. to Configure RAID on the Physical Server, Install a Hypervisor, Create a Virtual Machine (VM) and Install Guest Operating System (OS) to establish a robust server environment.



Indicative content 1.3: Creation of Domain Controller



Duration: 5hrs



Theoretical Activity 1.3.1: Description of Server Administrative tools



Tasks:

1. You are requested to answer the following questions:
 - a) Define domain controller
 - b) Explain Server Administrative Tools.
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to read more on key reading 1.3.1 in the trainee's manual



Key readings 1.3.1: Description of Server Administrative tools

A Domain Controller (DC) is a server that runs Active Directory Domain Services (AD DS), which is responsible for handling authentication, authorization, and directory services within a Windows domain.

Server Administrative Tools in Windows Server are a collection of utilities and features designed to help system administrators manage server roles, configurations, and resources effectively. These tools provide interfaces for handling various aspects of server management, including:

- 1. Server Manager:** A central console used for managing server roles, features, and overall server performance.
- 2. Active Directory Administrative Center (ADAC):** A graphical interface for managing Active Directory environments, including user and group management.
- 3. Active Directory Users and Computers (ADUC):** A traditional tool for managing user accounts, groups, and computers within Active Directory.
- 4. Group Policy Management Console (GPMC):** A tool for managing and configuring Group Policy Objects (GPOs) across the network.
- 5. DNS Manager:** Used for configuring and managing Domain Name System (DNS) settings and records.

- 6. Hyper-V Manager:** Provides management of virtual machines and virtualization settings within the server.
- 7. Task Scheduler:** Automates administrative tasks by allowing the scheduling and management of tasks.
- 8. Performance Monitor:** Monitors and tracks system performance metrics and resource usage.
- 9. Windows Admin Center:** A modern, web-based management interface for Windows Server and Windows 10.
- 10. Event Viewer:** Provides access to logs of system and application events for troubleshooting and monitoring.
- 11. Windows PowerShell:** A command-line interface for scripting and automating server management tasks.



Practical Activity 1.3.2: Installation of Active Directory Domain Services (ADDS) and Promotion of server to a domain controller

Task:

1. You are requested to go to the computer lab and do the task below individually.
As a Trainee in Level 4 software development, you are requested to go to the computer lab to install Active Directory Domain Services (ADDS) and Promotion of server to a domain controller in the windows server.
2. Read the key readings 1.3.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present the work to trainer and the whole class



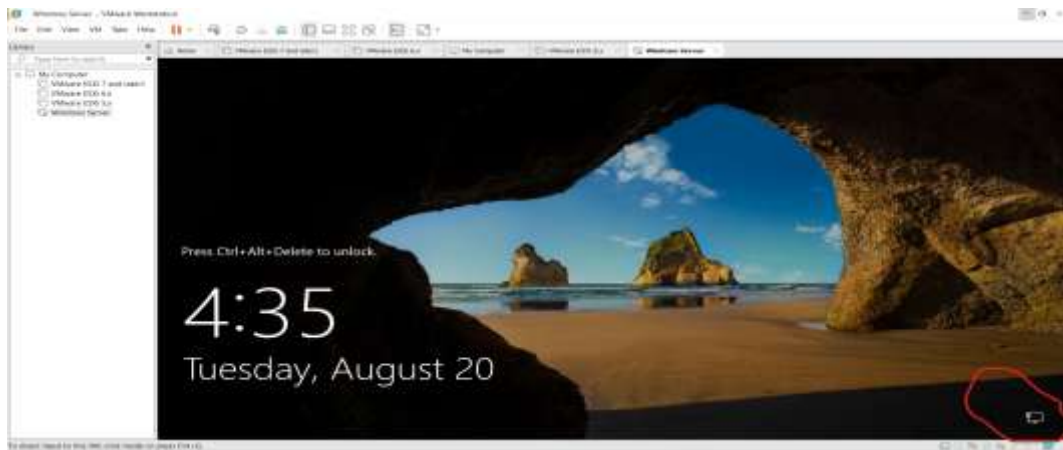
Key readings 1.3.2: Installation of Active Directory Domain Services

To install Active Directory Domain Services (AD DS) on a Windows Server, you can follow these steps:

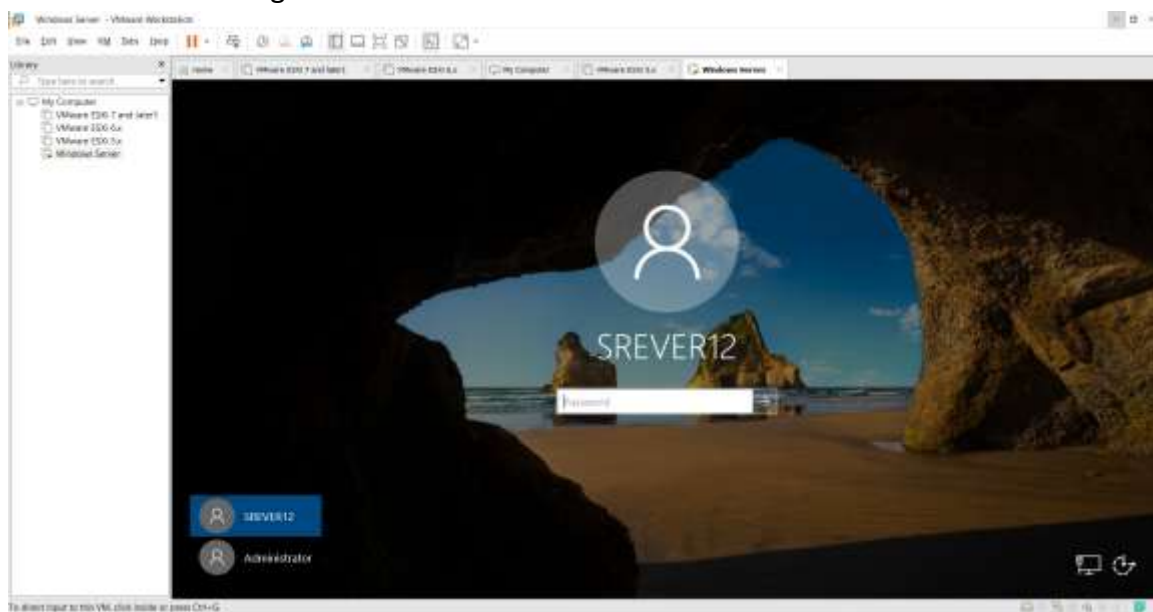
- 1. Prepare the Server:** Ensure that the server meets the minimum hardware requirements and is running a supported version of Windows Server.

Additionally, assign a static IP address to the server and ensure it has connectivity to the

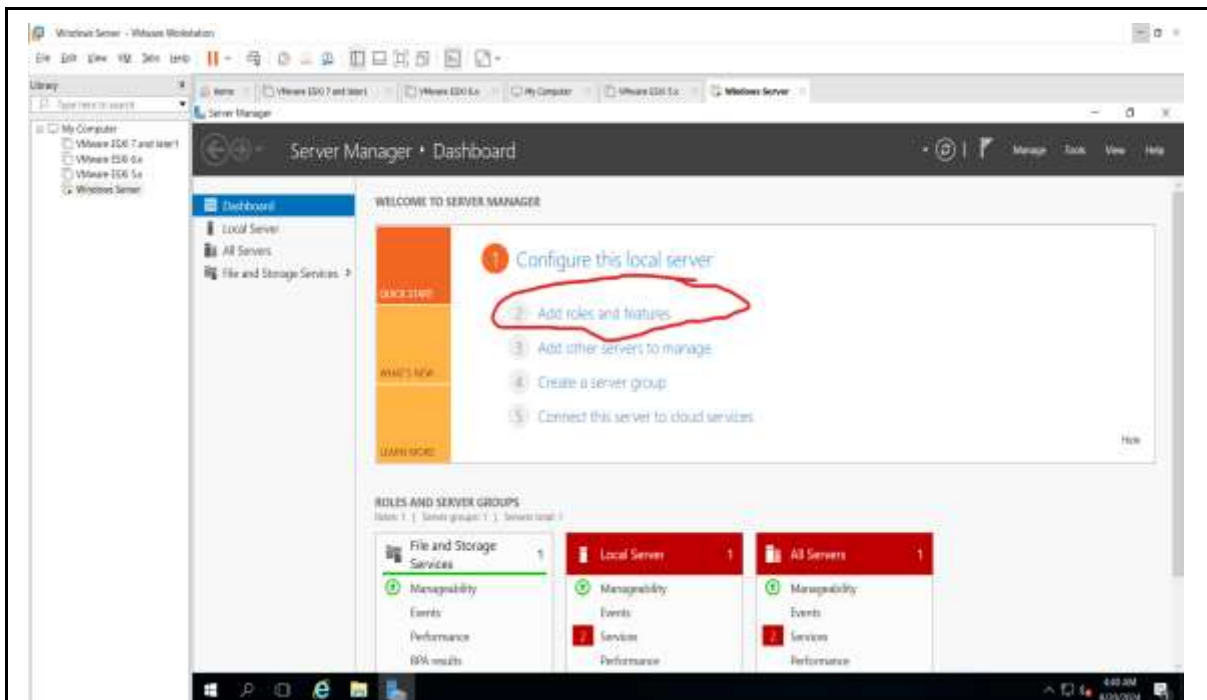
network.



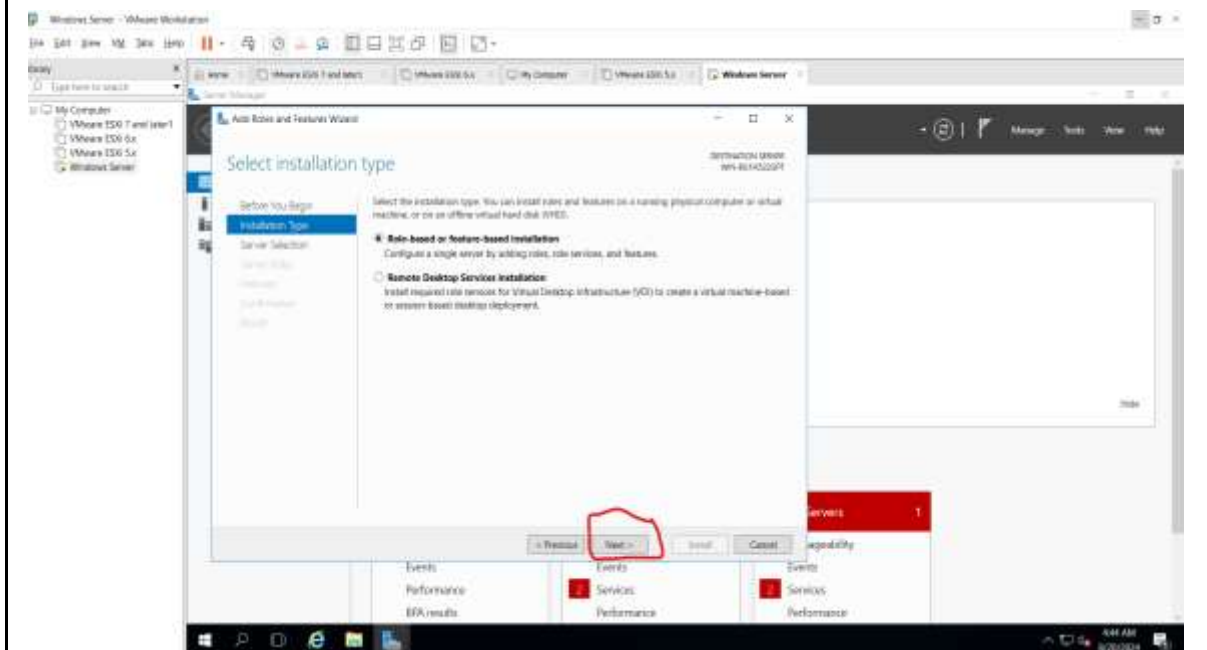
1. **Access Server Manager:** Log in to the server with administrative privileges and open Server Manager. This can be done by clicking on the Start menu and selecting "Server Manager."



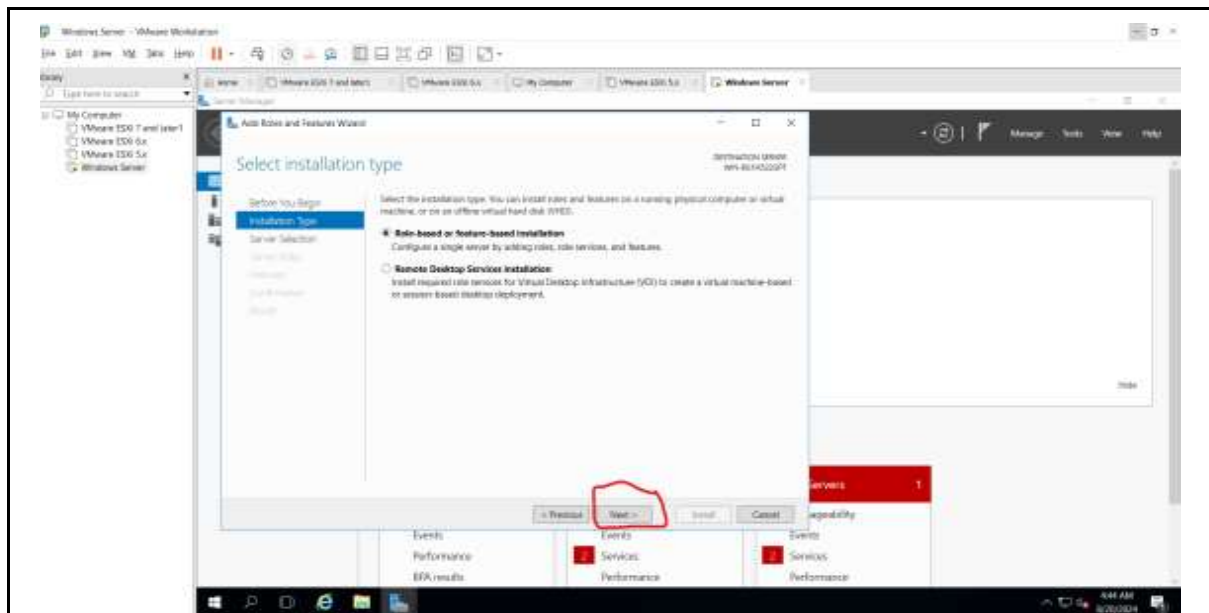
3. **Add the AD DS Role:** In Server Manager, click on "Add roles and features" from the dashboard or the Manage menu. This will open the Add Roles and Features Wizard.



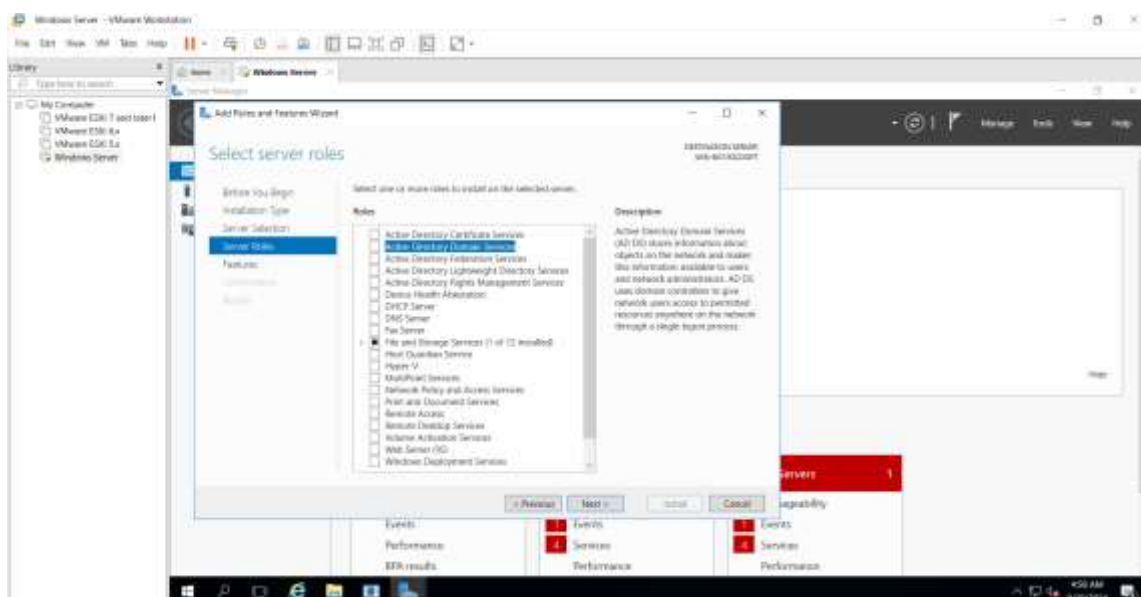
4. Select Installation Type: In the wizard, select "Role-based or feature-based installation" and click "Next."



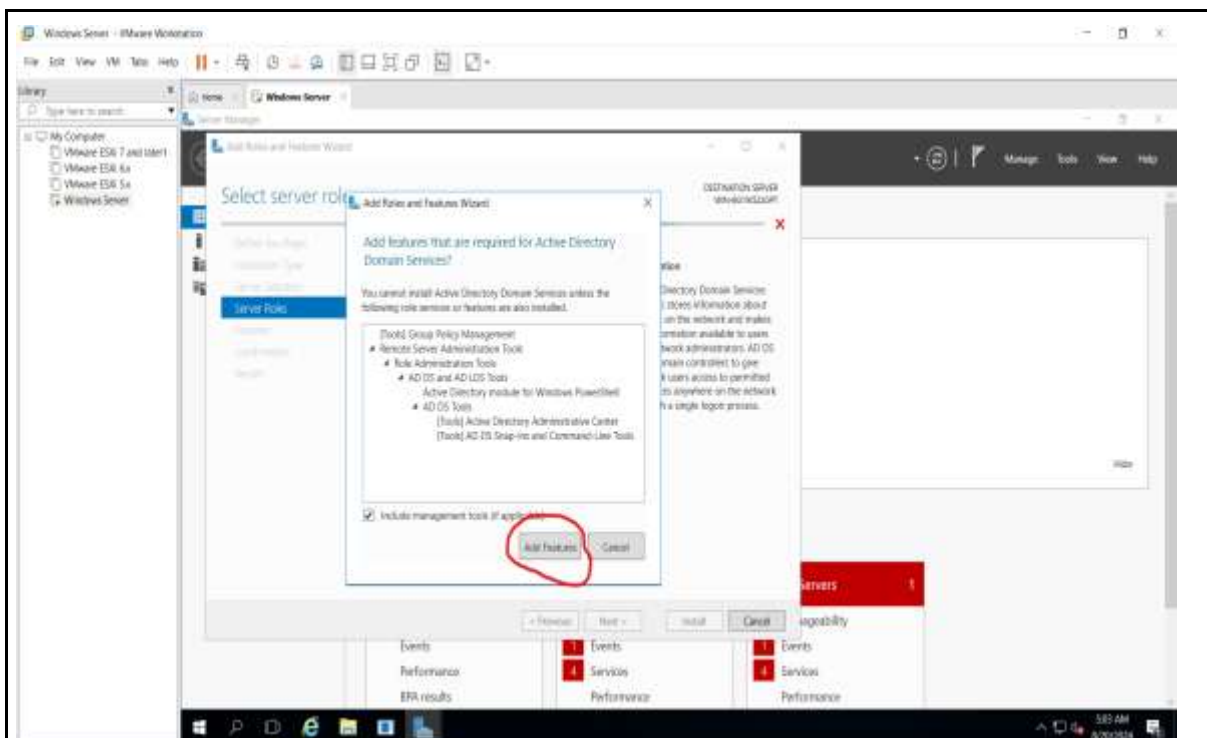
5. Select the Server: Choose the server on which you want to install AD DS and click "Next."



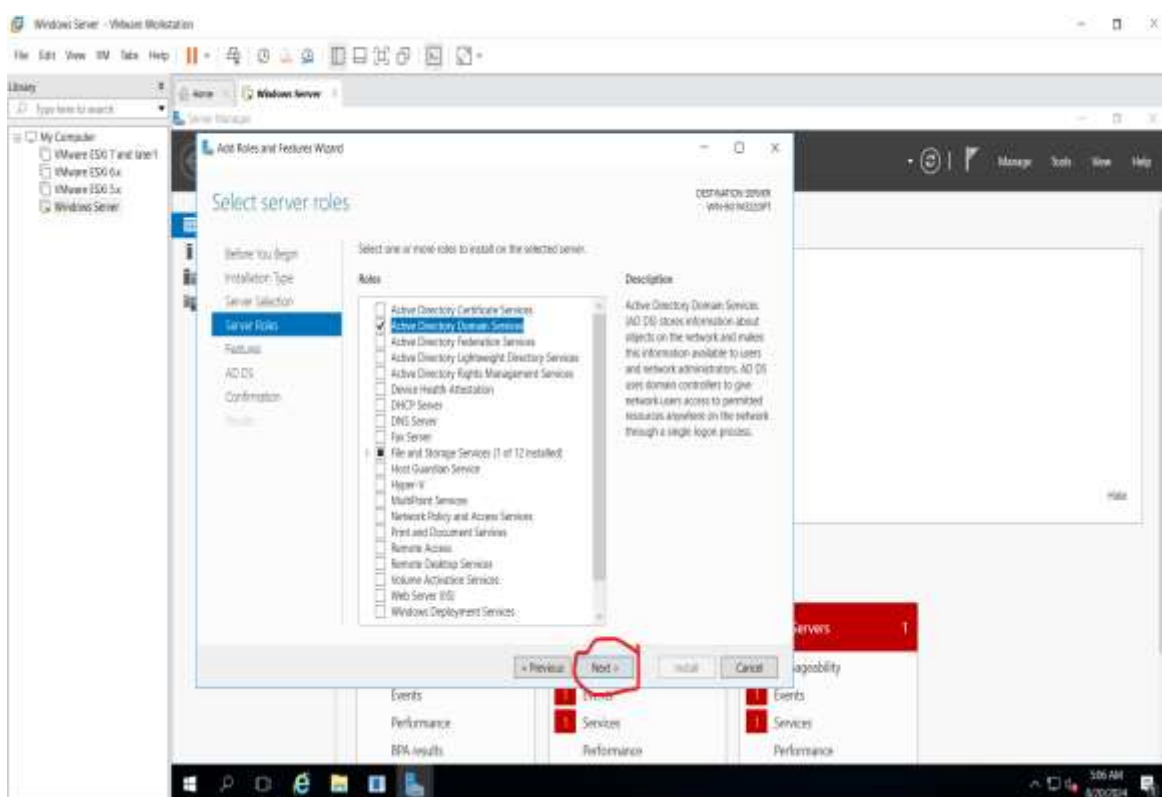
6. Select Role: From the list of server roles, select "Active Directory Domain Services" and click "Next."



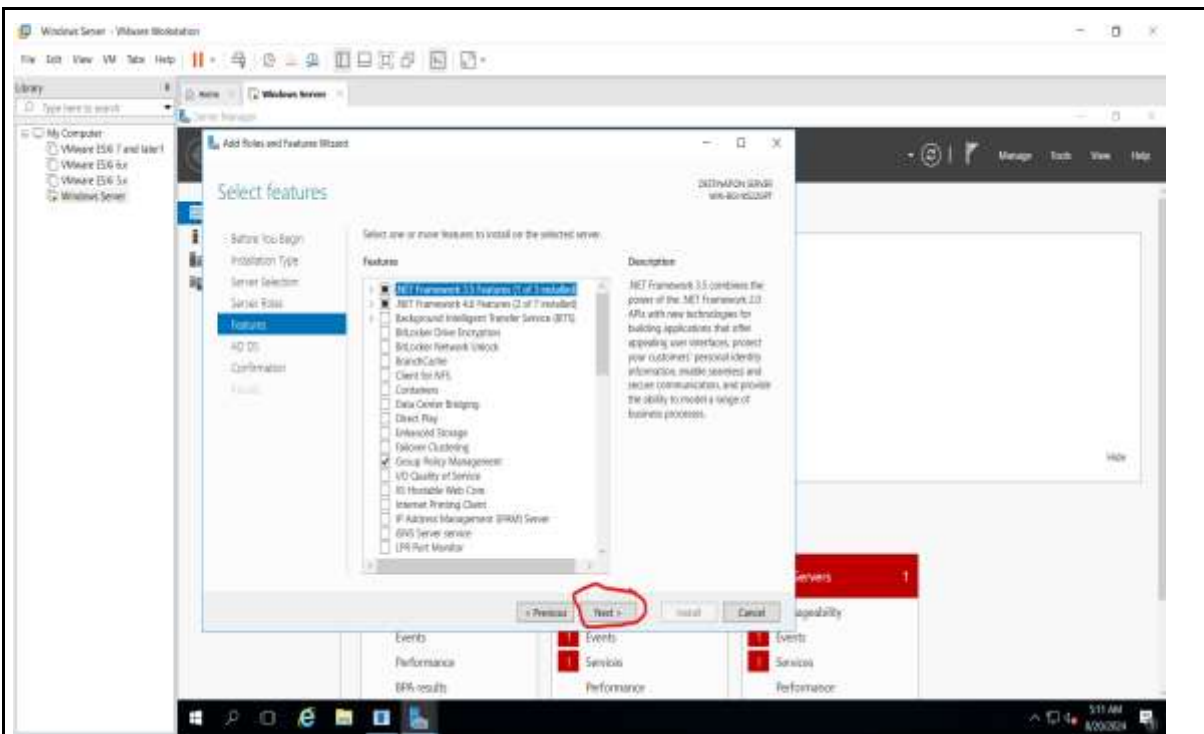
7. Add Features: The wizard may prompt you to add additional features required by AD DS. Review the features and click "Add Features" to include them. Then, click "Next."



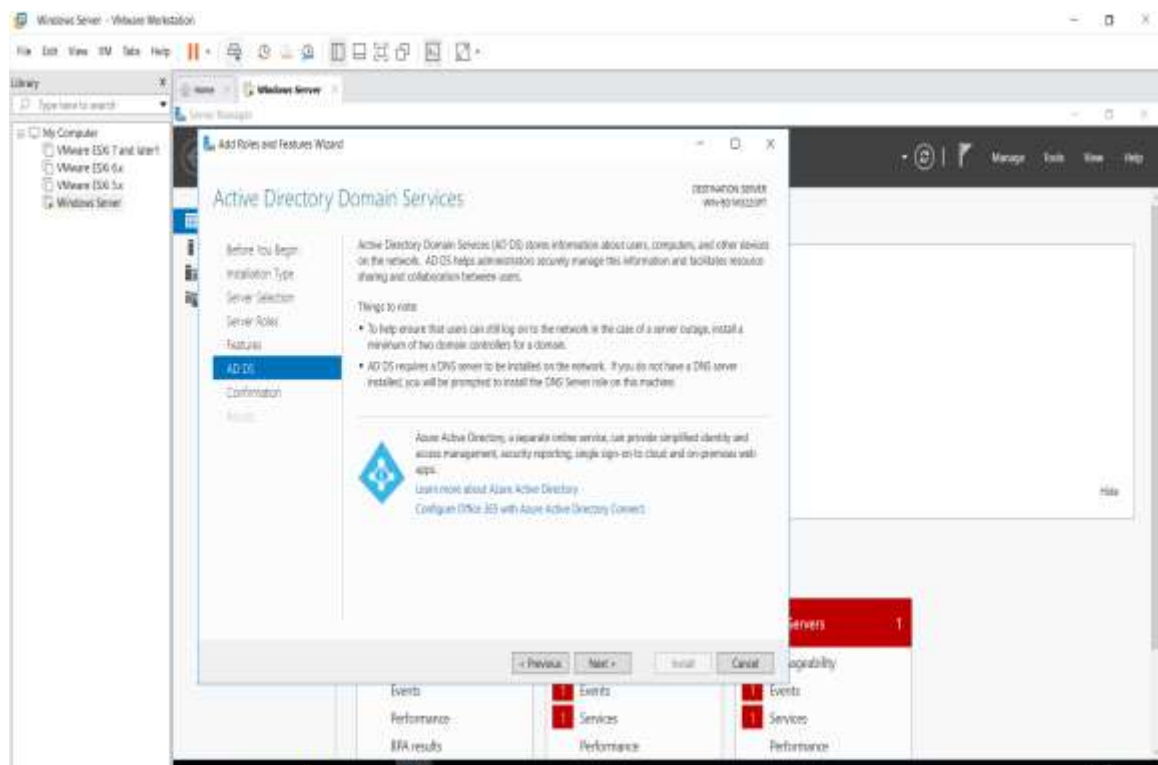
8. Confirm Installation: Review the information on the AD DS page and click "Next" to proceed.



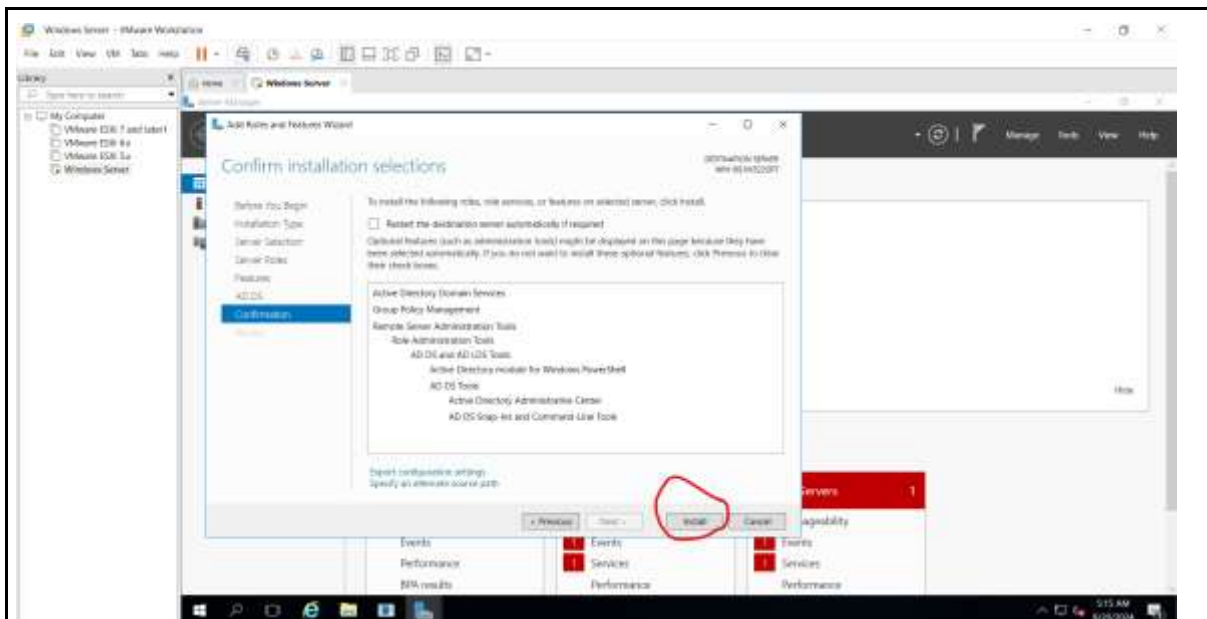
9. Select Features: On the Features page, leave the default selections and click "Next."



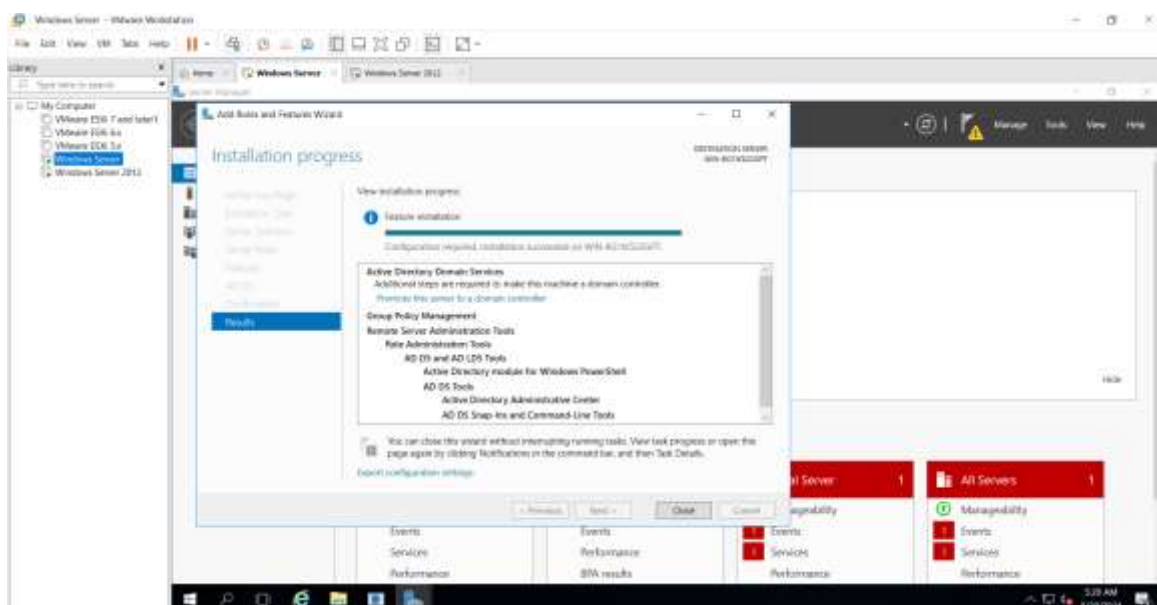
10. Confirm AD DS Role: Review the information about the AD DS role and click "Next."



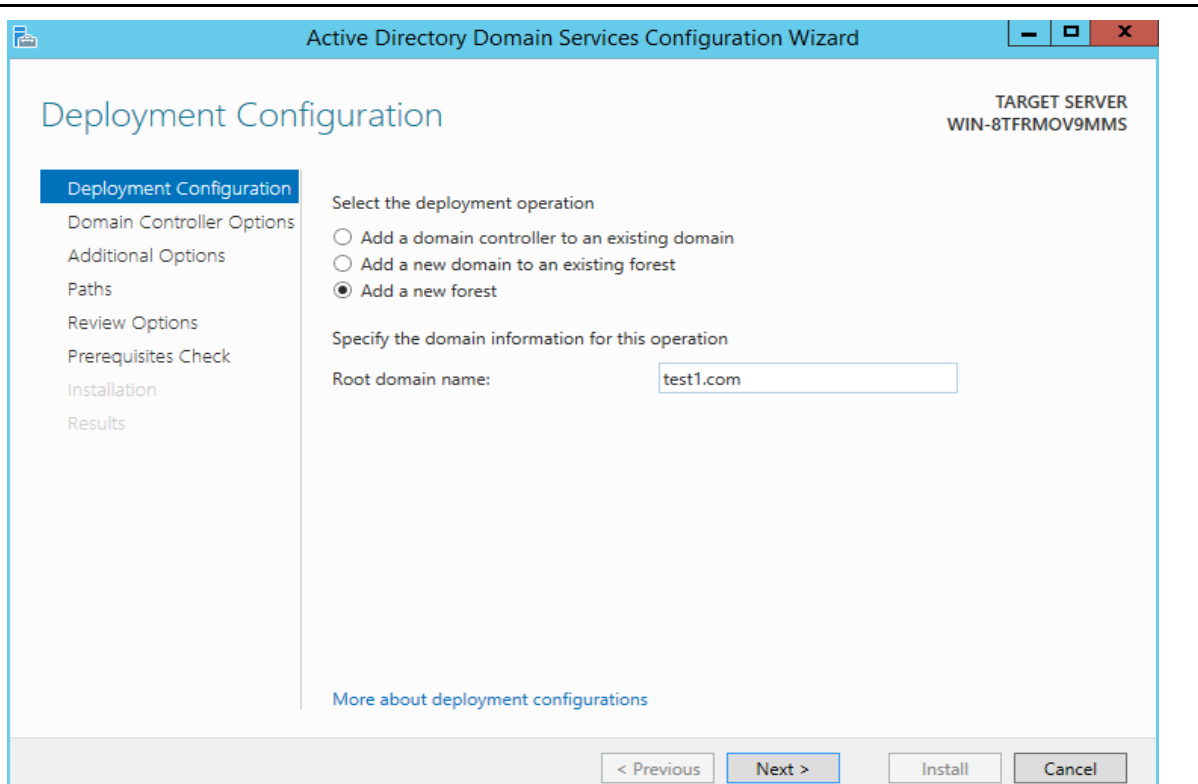
11. Confirm Installation: Review the summary of the installation and click "Install" to begin the installation process.



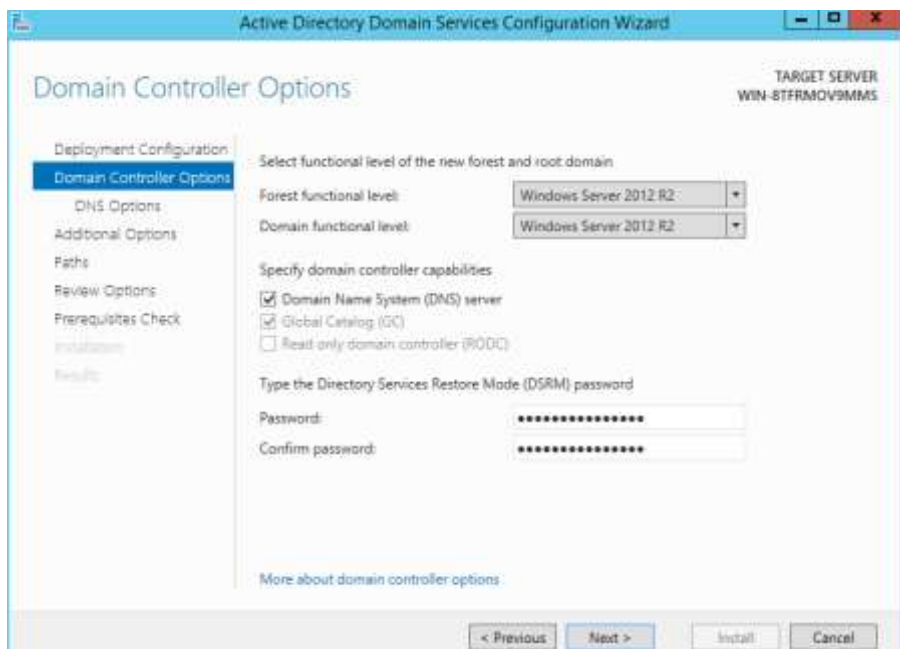
12. Installation Progress: The wizard will now install AD DS and any selected features. Wait for the installation to complete.



13. Select "Add a new forest" if you are creating a new domain or "Add a domain controller to an existing domain" if you are joining an existing domain. Provide the necessary information, such as the domain name and the domain controller options, and follow the prompts to complete the promotion process.



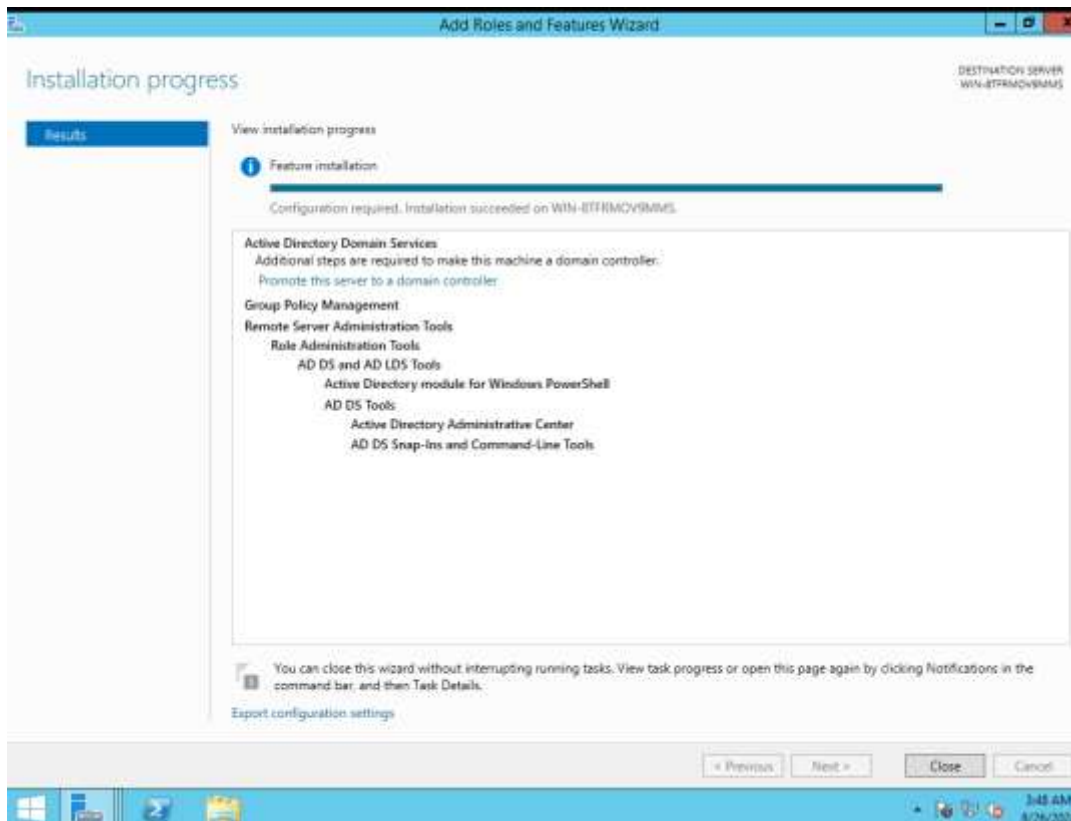
14. Set Directory Services Restore Mode (DSRM) Password: During the promotion process, set the password for the Directory Services Restore Mode (DSRM) administrator account. This account is used for recovery purposes.



15. Review and Confirm: Review the summary of the configuration and click "Next" to proceed.

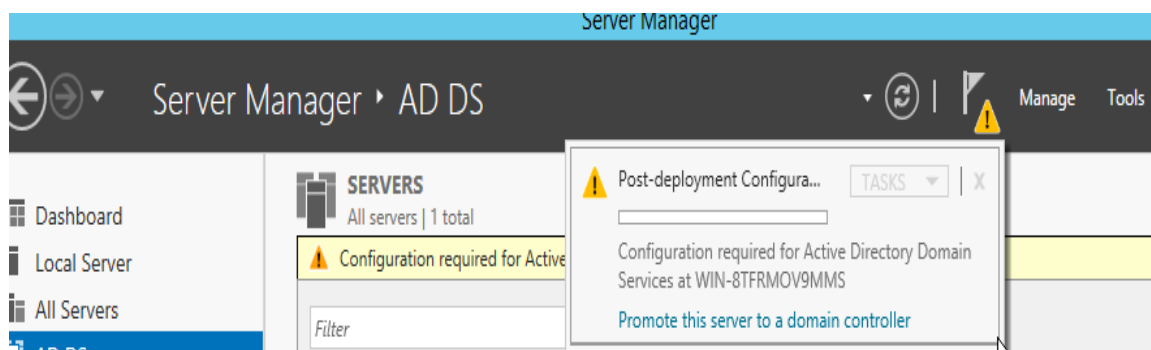
16. Installation Progress: The wizard will now configure the domain controller settings. Wait for the process to complete.

17. Restart the Server: After the configuration is complete, the server will need to be restarted. You can choose to restart immediately or do it later.

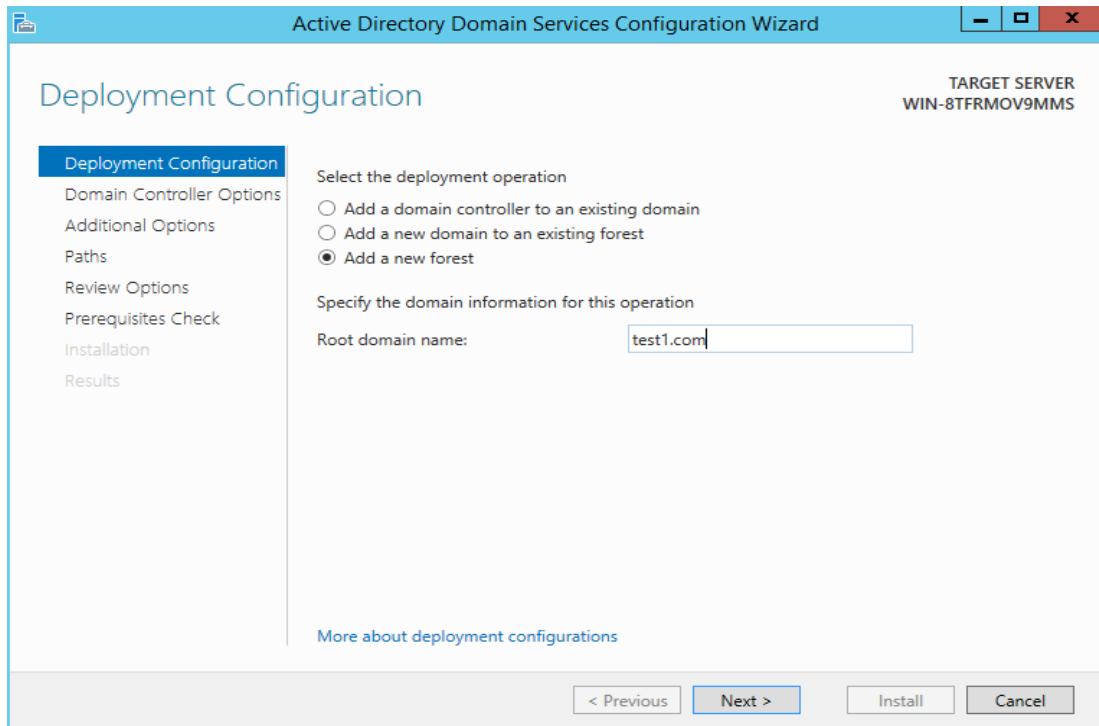


To promote a server to a domain controller, you can follow these general steps:

1. Ensure that the server meets the hardware and software requirements for being a domain controller.
2. Install the Active Directory Domain Services (AD DS) role on the server.
3. Run the Active Directory Domain Services Configuration Wizard to promote the server to a domain controller.

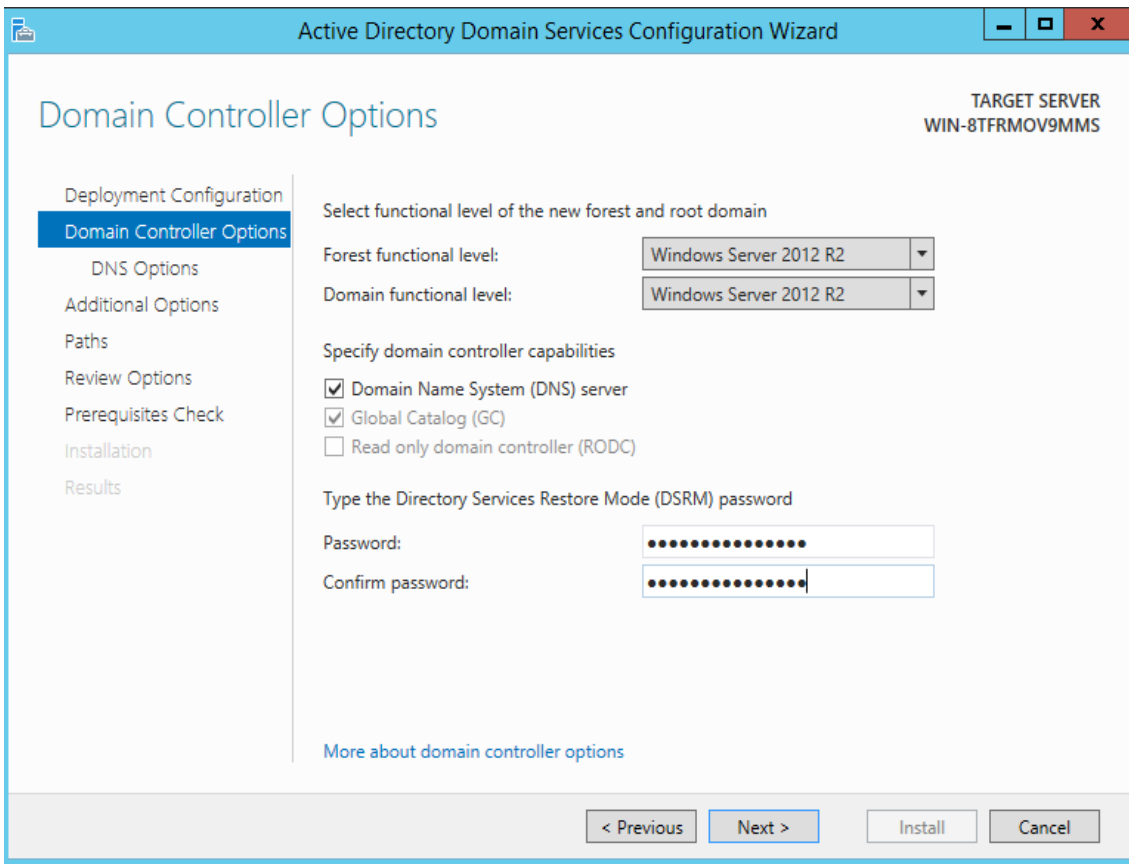


4. Select the appropriate configuration options, such as creating a new domain or joining an existing one.



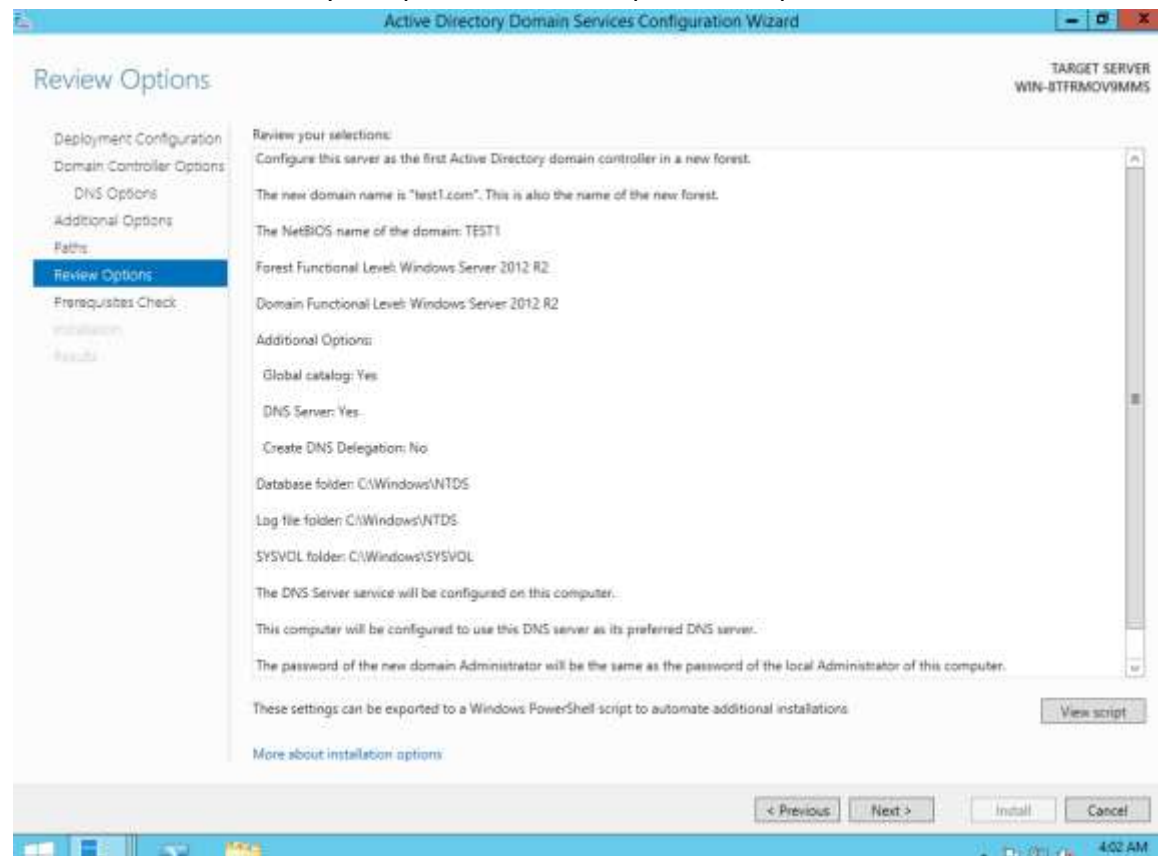
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the text 'Active Directory Domain Services Configuration Wizard' and standard window controls. The main window has a blue header with the title 'Deployment Configuration' and a 'TARGET SERVER' label with the value 'WIN-8TFRMOV9MMS'. On the left is a navigation pane with links: 'Deployment Configuration' (highlighted), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this is a section titled 'Specify the domain information for this operation' with a label 'Root domain name:' and a text box containing 'test1.com'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about deployment configurations' is located at the bottom of the main content area.

5. Specify the domain controller's DNS settings and provide necessary credentials.

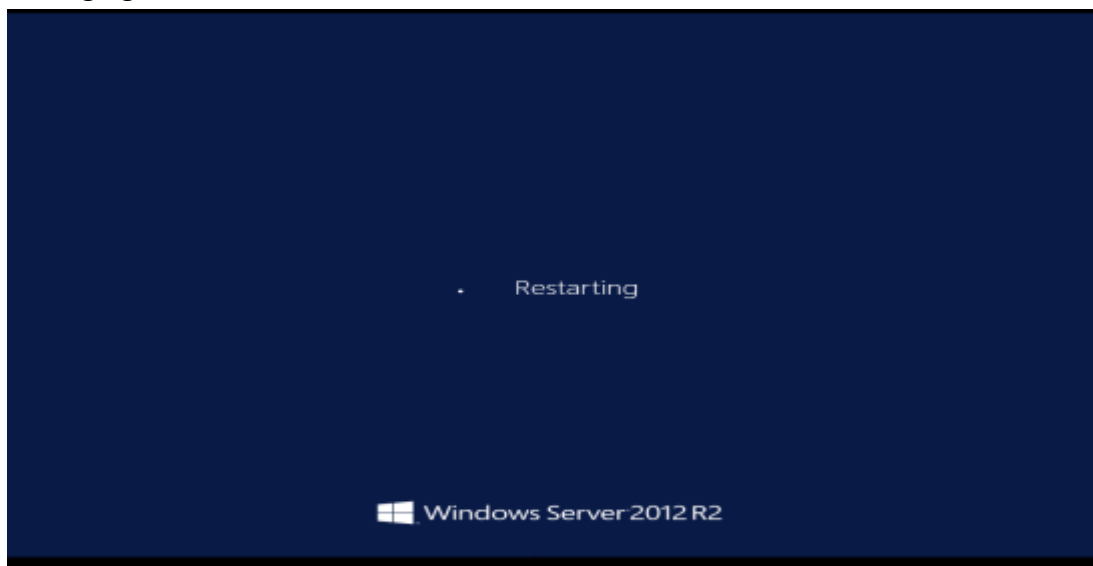


The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'Domain Controller Options' step. The title bar is the same as the previous screen. The main window has a blue header with the title 'Domain Controller Options' and the same 'TARGET SERVER' label 'WIN-8TFRMOV9MMS'. The navigation pane on the left now has 'Domain Controller Options' highlighted. The main content area is titled 'Select functional level of the new forest and root domain' and contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2012 R2'. Below this is a section titled 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Further down is a section titled 'Type the Directory Services Restore Mode (DSRM) password' with two text boxes labeled 'Password:' and 'Confirm password:', both filled with dots. At the bottom are the same four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about domain controller options' is at the bottom of the main content area.

6. Review the summary and proceed with the promotion process.



7. Once the promotion is complete, the server will be a domain controller and can start managing the domain's resources.





Points to Remember

- **Description of Server Administrative tools**
 - i. **A domain controller (DC)** is a server that runs the Active Directory Domain Services (AD DS) role in a Windows Server environment.
 - ii. **Server Administrative tools are:** Server Manager, Active Directory Administrative Center (ADAC), Active Directory Users and Computers (ADUC), Group Policy Management Console (GPMC), DNS Manager, Hyper-V Manager, Task Scheduler, Performance Monitor, Windows Admin Center, Event Viewer, Windows PowerShell
- A. Install ADDS Role follow the following steps:
 - ✓ Open Server Manager
 - ✓ Add Roles and Features
 - ✓ Role-Based or Feature-Based Installation
 - ✓ Select Destination Server
 - ✓ Select Server Roles
 - ✓ Complete Installation
- B. Promote the Server to a Domain Controller
 - ✓ Access AD DS Configuration Wizard
 - ✓ Deployment Configuration
 - ✓ Domain Controller Options
 - ✓ Additional Options
 - ✓ Review Options
 - ✓ Prerequisites Check
 - ✓ Server Restart



Application of learning 1.3.

Bxz Solutions Inc. is a company specializing in providing IT solutions for small and medium businesses. Located in Rwanda, Eastern area, Bxz Solutions Inc. aims to enhance its infrastructure by setting up a new server environment to improve its data management and network capabilities.

As an IT technician hired by Tech Solutions Inc., you are tasked with the following:

- Tasks:
1. Install Active Directory Domain Services (AD DS)
 2. Promote the Server to a Domain Controller



Indicative content 1.4: Installation of Server Roles and Features



Duration: 5hrs



Theoretical Activity 1.4.1: Description of server roles and features



Tasks:

- 1: You are requested to answer the following questions:
 - i. What is the primary function of a DNS server?
 - ii. What are DNS root hints used for?
 - iii. How do zones and zone files work in DNS?
 - iv. Discuss the key messages involved in the DHCP communication process.
 - v. Why is DHCP fault tolerance important?
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 1.4.1 in the trainee's manual



Key readings 1.4.1: Description of server roles and features

DNS (Domain Name System)

The Domain Name System (DNS) is a critical service that translates human-readable domain names (e.g: www.example.com) into IP addresses that computers use to identify each other on the network. DNS helps users and devices find and communicate with each other over a network or the internet.

Queries: DNS queries are requests made by clients (usually DNS resolvers) to a DNS server to translate a domain name into an IP address. There are two types of DNS queries: recursive and iterative. In a recursive query, the DNS server provides a complete answer, while in an iterative query, the DNS server may provide a referral to another server.

Operation: DNS servers respond to queries by consulting their own records, forwarding the request to other DNS servers, or caching responses from previous queries to provide faster responses in the future.

Roles:

- 1. Authoritative DNS Server:** Holds the definitive records for a particular domain and answers queries about that domain.
- 2. Caching-only DNS Server:** Does not hold any domain records but caches responses from other DNS servers to improve performance.
- 3. Forwarding DNS Server:** Forwards queries it cannot resolve to another DNS server, reducing the workload on higher-level servers.

Root Hints: A list of root DNS servers that a DNS server can use to resolve queries for domains it doesn't know. The root hints direct the DNS server to the root zone of the domain, from which it can continue resolving queries down the DNS hierarchy.

Zones and Zone Files:

- 1. Zones:** A zone is an administrative space within a domain that a DNS server manages. It contains all the DNS records for the domain or a portion of it.
- 2. Zone Files:** Text files that store DNS records for a zone. They include records like A, MX, and CNAME that map domain names to IP addresses or other resources.

DHCP (Dynamic Host Configuration Protocol)

The **Dynamic Host Configuration Protocol (DHCP)** is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices on the network, allowing them to communicate with each other.

- DHCP Messages and Operation:



- 1. DHCP Discover:** A client sends a broadcast message to discover available DHCP servers.
- 2. DHCP Offer:** A DHCP server responds with an offer, including an available IP address and configuration options.
- 3. DHCP Request:** The client requests the offered IP address.
- 4. DHCP Acknowledgment:** The server acknowledges and finalizes the IP address assignment.
 - **Fault Tolerance Implementations:** To ensure continuous DHCP service availability, administrators can implement fault tolerance using methods like:
 - 1. DHCP Failover:** Two DHCP servers share the load and provide redundancy by replicating their lease databases.
 - 2. Split Scope:** Distributes the IP address pool between two servers, with each handling a portion of the scope.
 - 3. Hot Standby:** One server is active, and the other is on standby to take over if the primary server fails.
 - **Security Considerations:** DHCP security issues include unauthorized DHCP servers, address spoofing, and denial-of-service attacks. To mitigate these risks, security measures include:
 - 1. DHCP Snooping:** Prevents unauthorized DHCP servers from operating on the network.
 - 2. MAC Address Filtering:** Ensures that only devices with authorized MAC addresses receive IP addresses.
 - 3. IP Address Tracking:** Monitors and logs which devices are assigned which IP addresses for accountability.
 - **Relay Agent:** A DHCP Relay Agent is a network device that forwards DHCP requests and replies between clients and DHCP servers when they are not on the same local network. This allows DHCP clients on different subnets to communicate with a central DHCP server without needing a server on each subnet.



Practical Activity 1.4.2: Installation of server roles and features



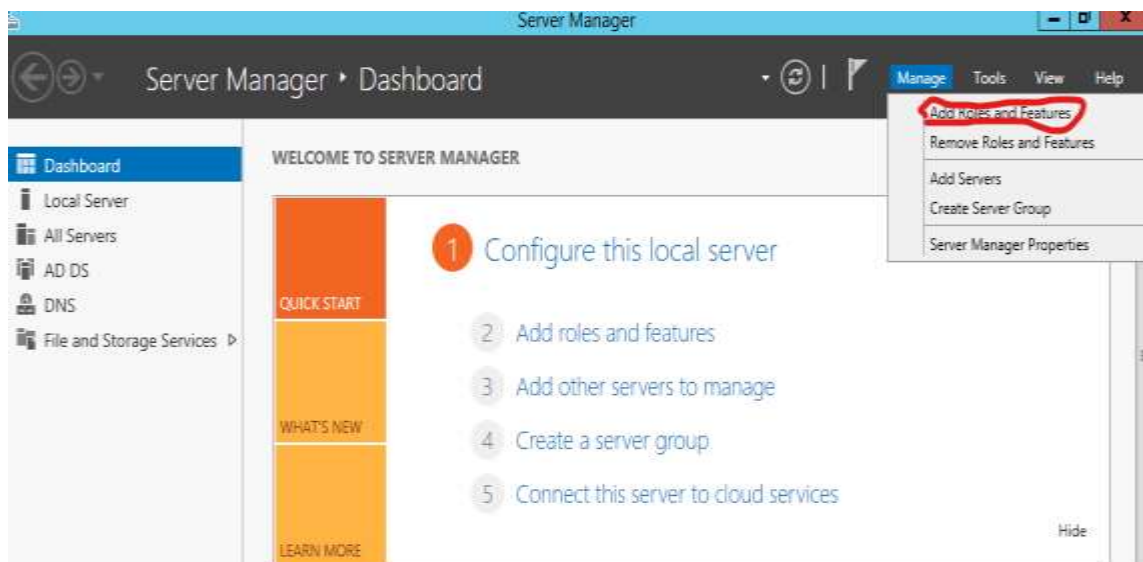
Task:

1. You are requested to go to the computer lab and do the task below individually.
As a Trainee in Level 4 software development, you are requested to go to the computer lab to install DNS and DHCP in server administration.
2. Remember to read the key readings 1.4.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class

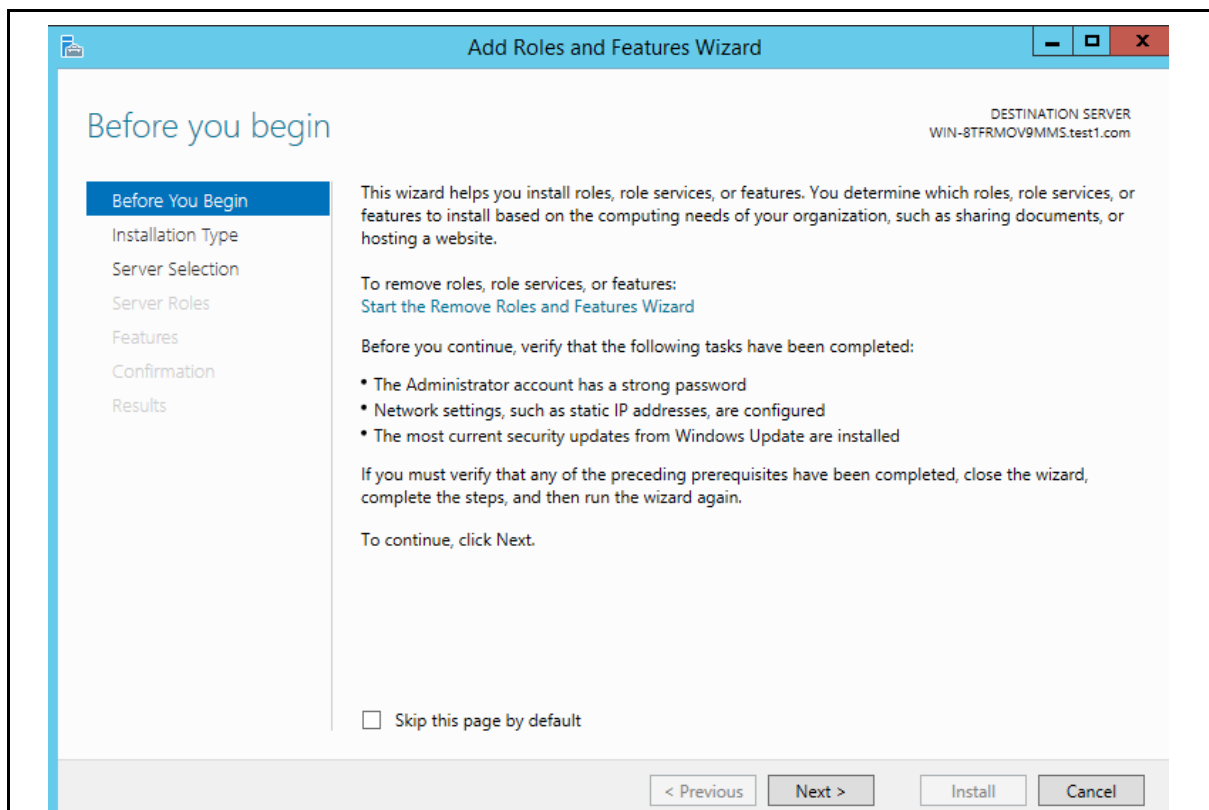


Key readings 1.4.2: Installation of server roles and features DNS

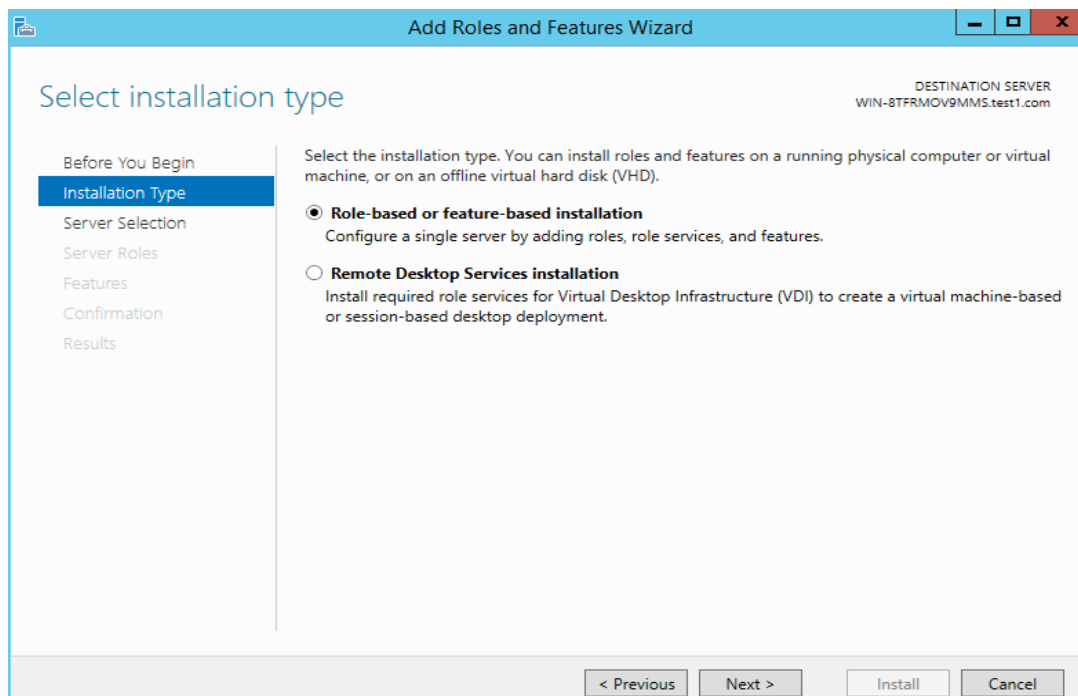
1. Open the Server Manager on your Windows Server. You can find it in the taskbar or access it through the Start menu.
2. In the Server Manager window, click on "Add roles and features" or a similar option.



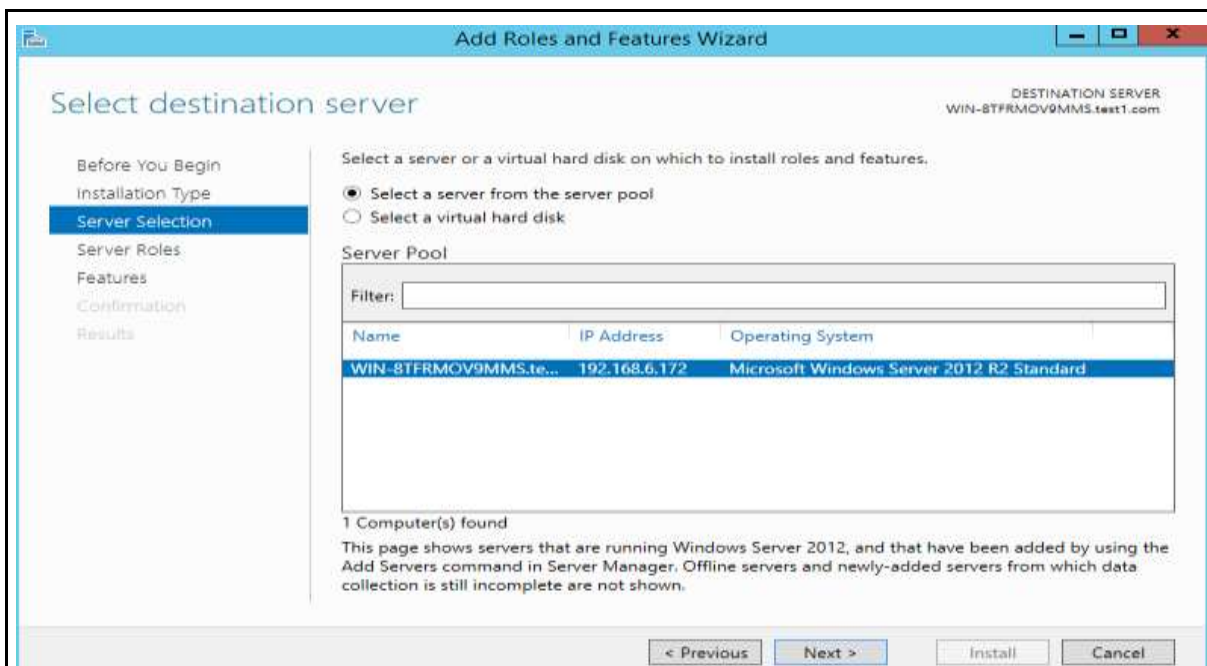
3. The Add Roles and Features Wizard will open. Click "Next" to proceed.



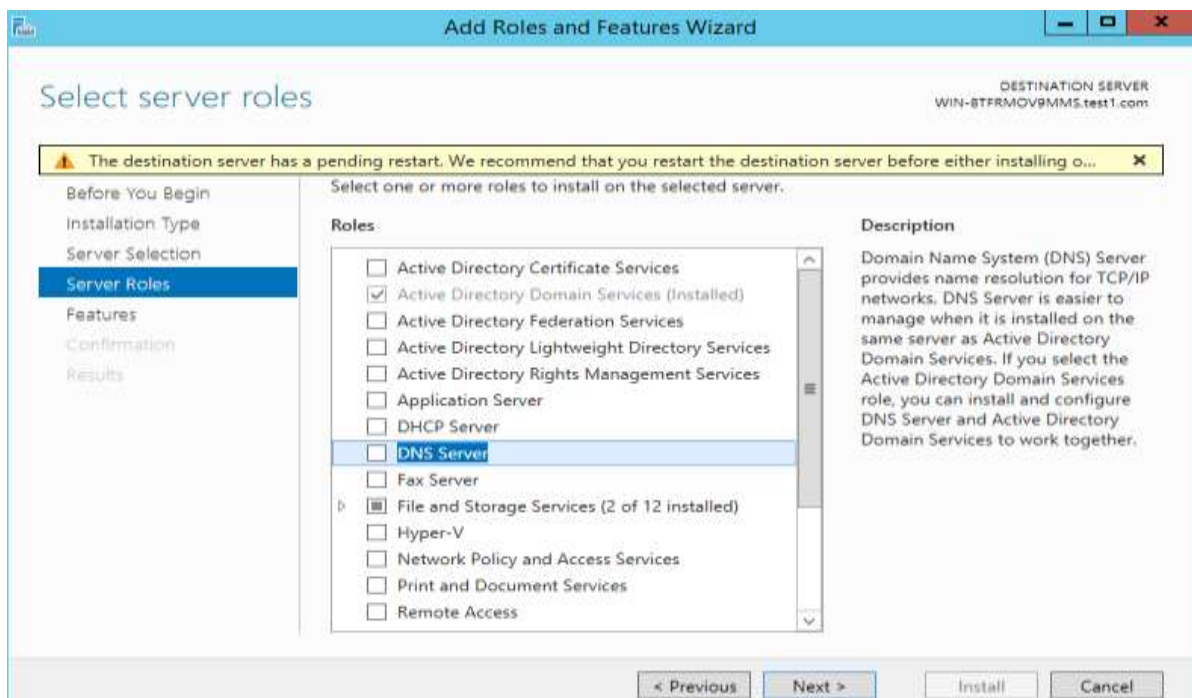
4. Select the installation type. Choose "Role-based or feature-based installation" and click "Next."



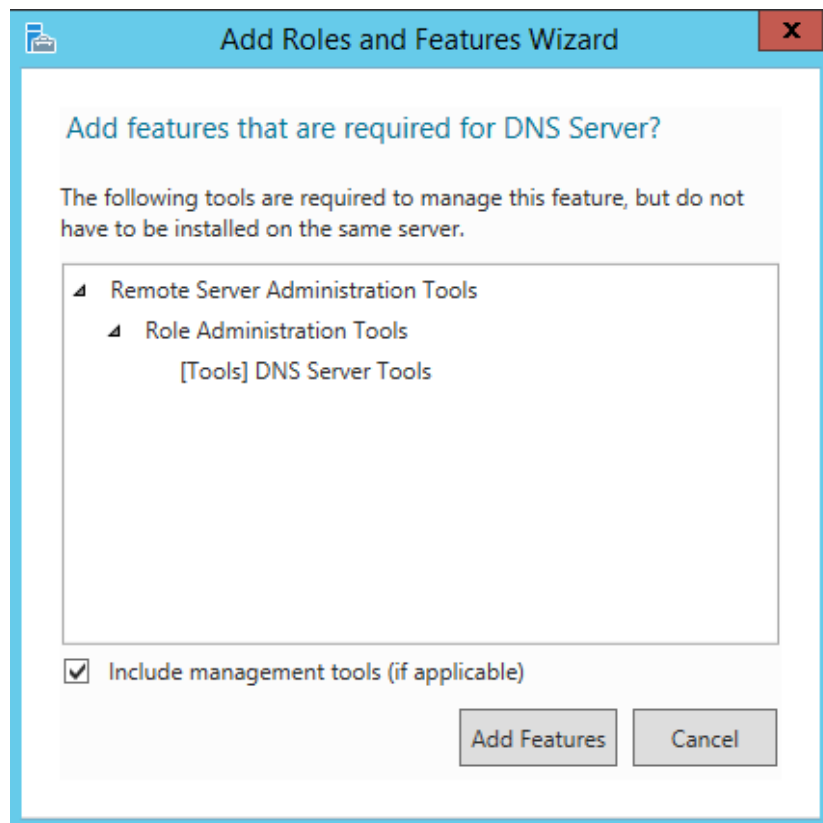
5. Select the appropriate server from the server pool and click "Next."



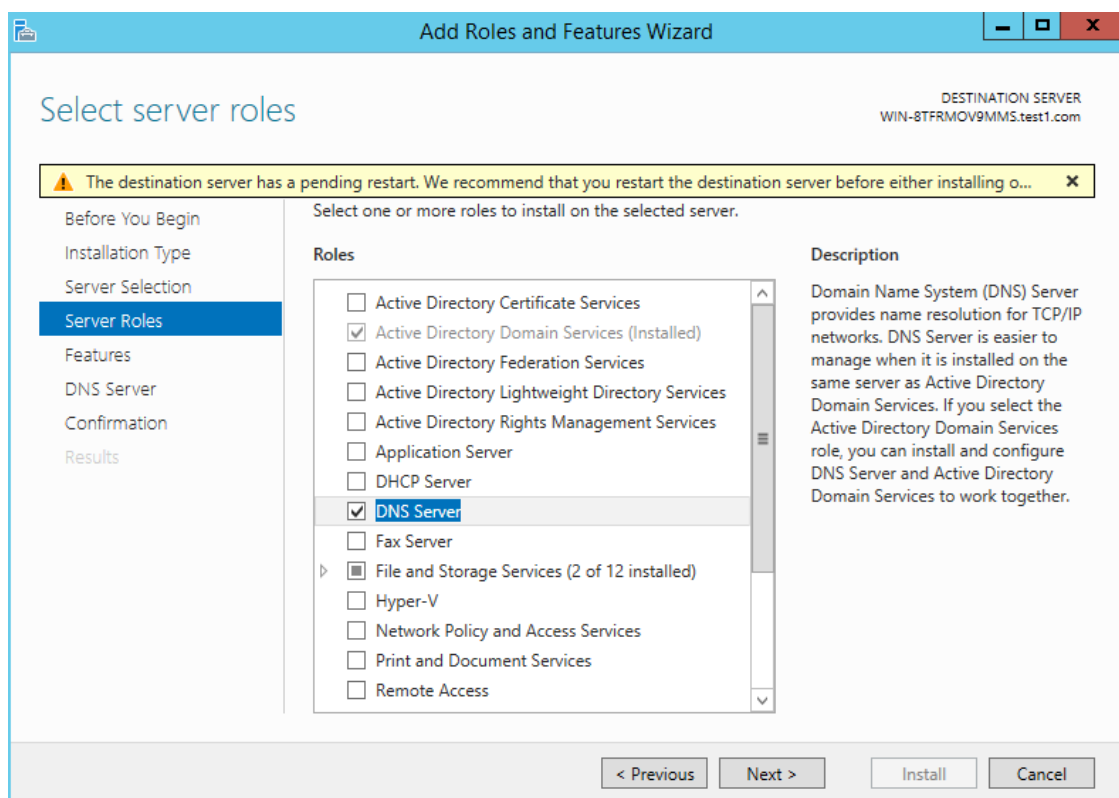
6. Scroll down and find the "DNS Server" role. Check the box next to it to select it.



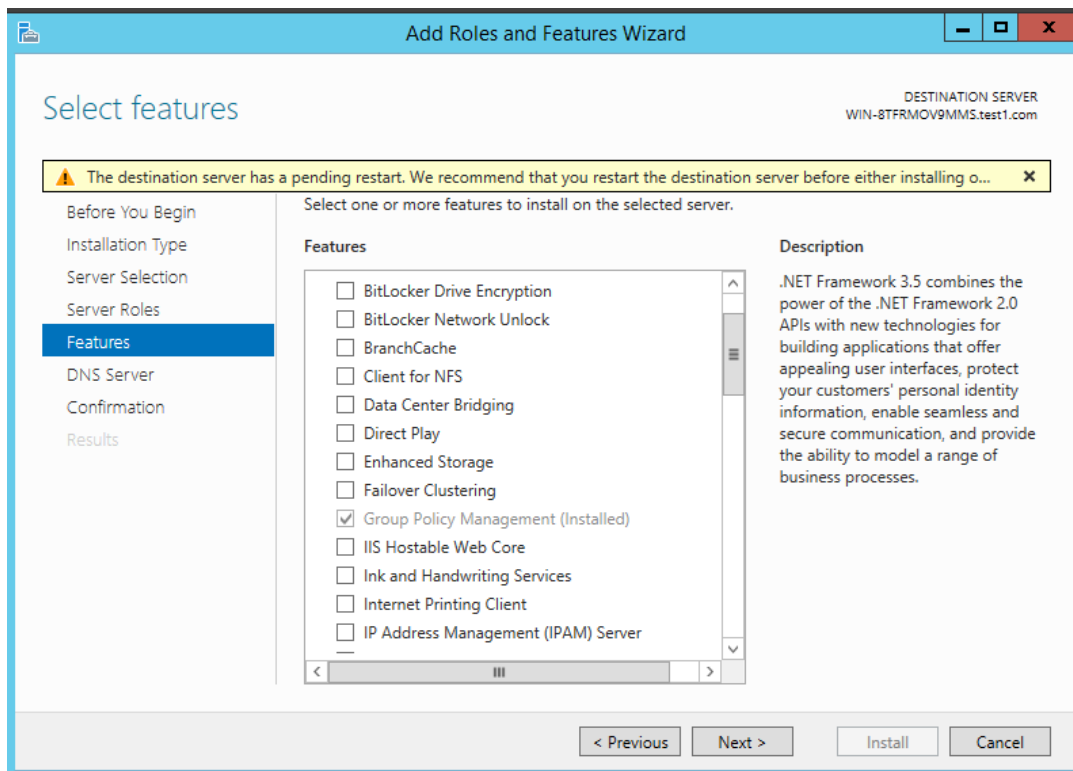
7. A prompt will appear asking to add the required features for the DNS role. Click "Add Features" to include the necessary features.



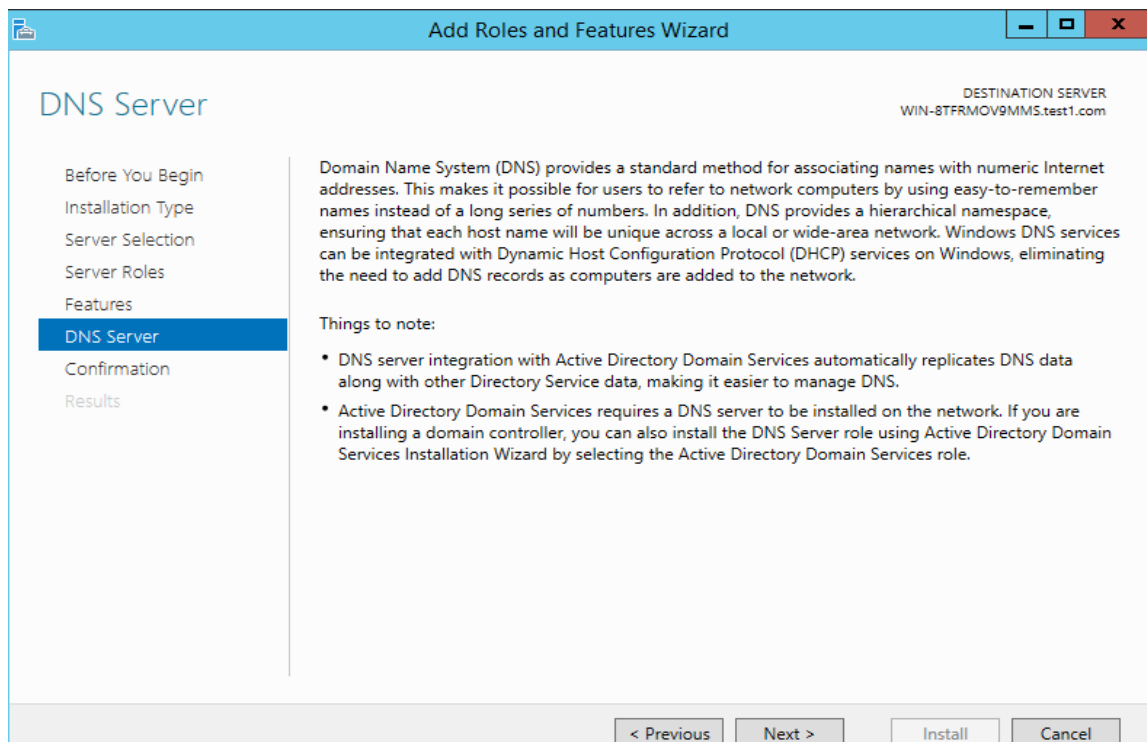
8. Click "Next" to proceed.



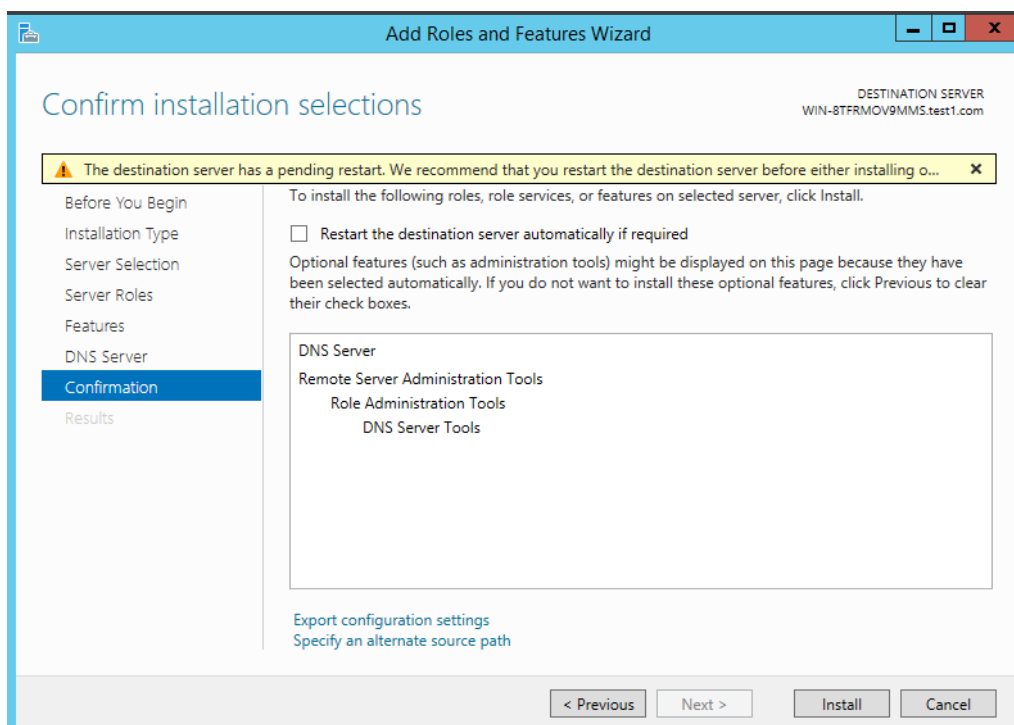
9. In the Features section, you can review the features that will be installed alongside the DNS role. Click "Next" to continue.



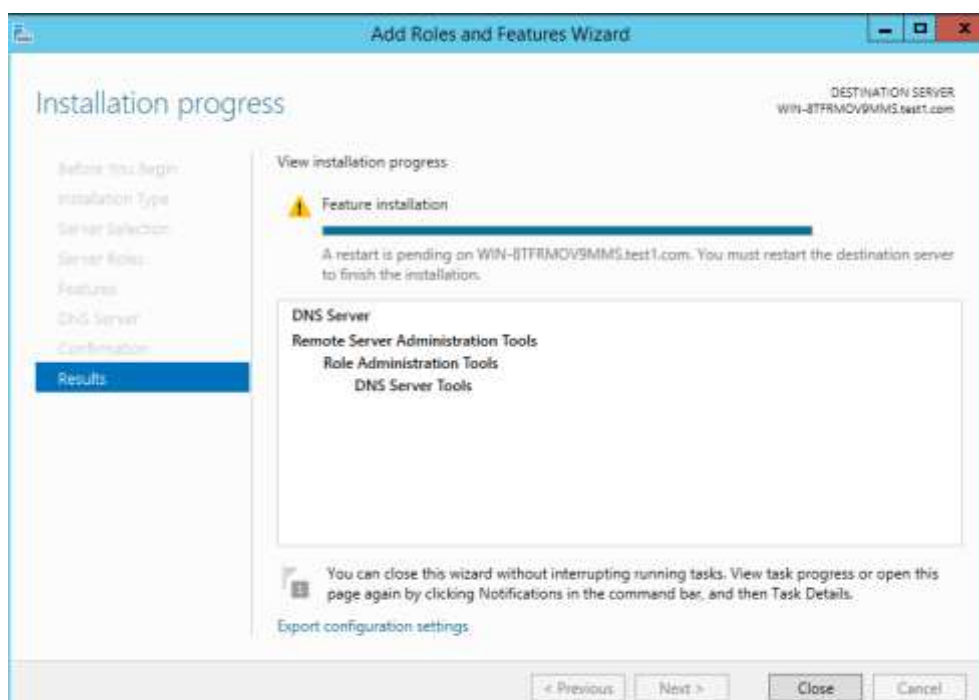
10. On the DNS Server page, read the information provided and click "Next."



11. Review the summary of your selections and click "Install" to begin the installation process for the DNS server role and features.



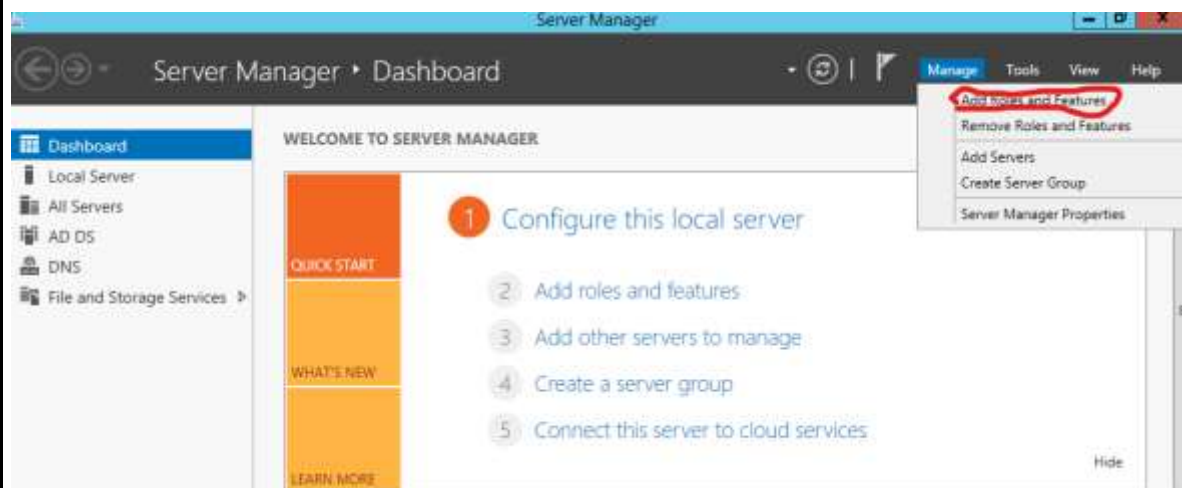
12. Once the installation is complete, you can configure and manage the DNS server using the DNS Manager tool. To promote a server to a domain controller, you can follow these general steps:



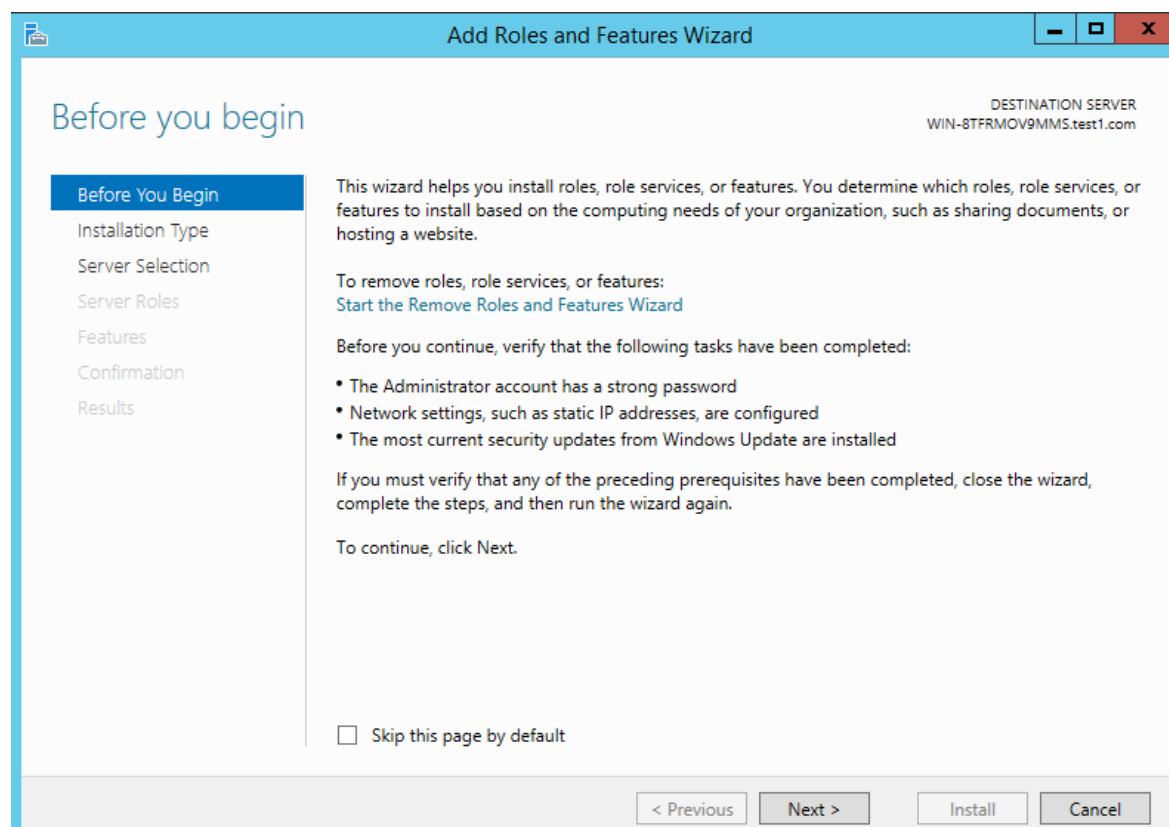
Then configuration of DNS Manager is Done

DHCP

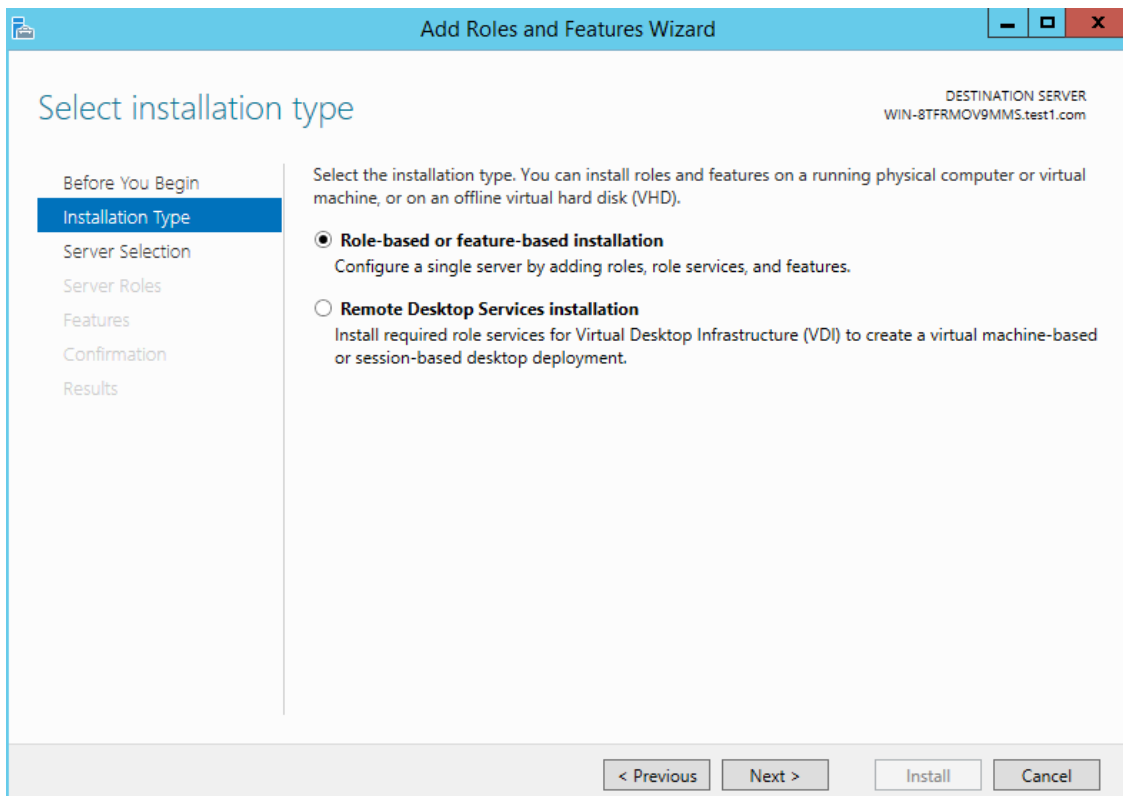
1. Open the Server Manager on your Windows Server.
2. In the Server Manager window, click on "Add roles and features" or a similar option.



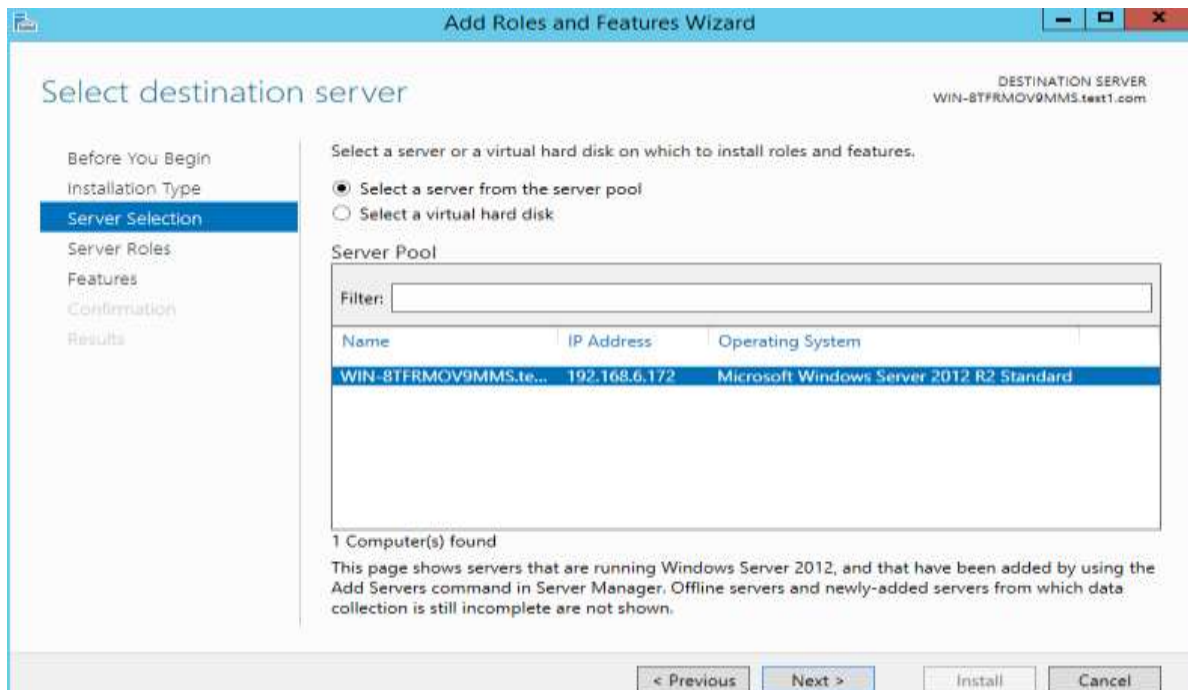
3. The Add Roles and Features Wizard will open. Click "Next" to proceed.



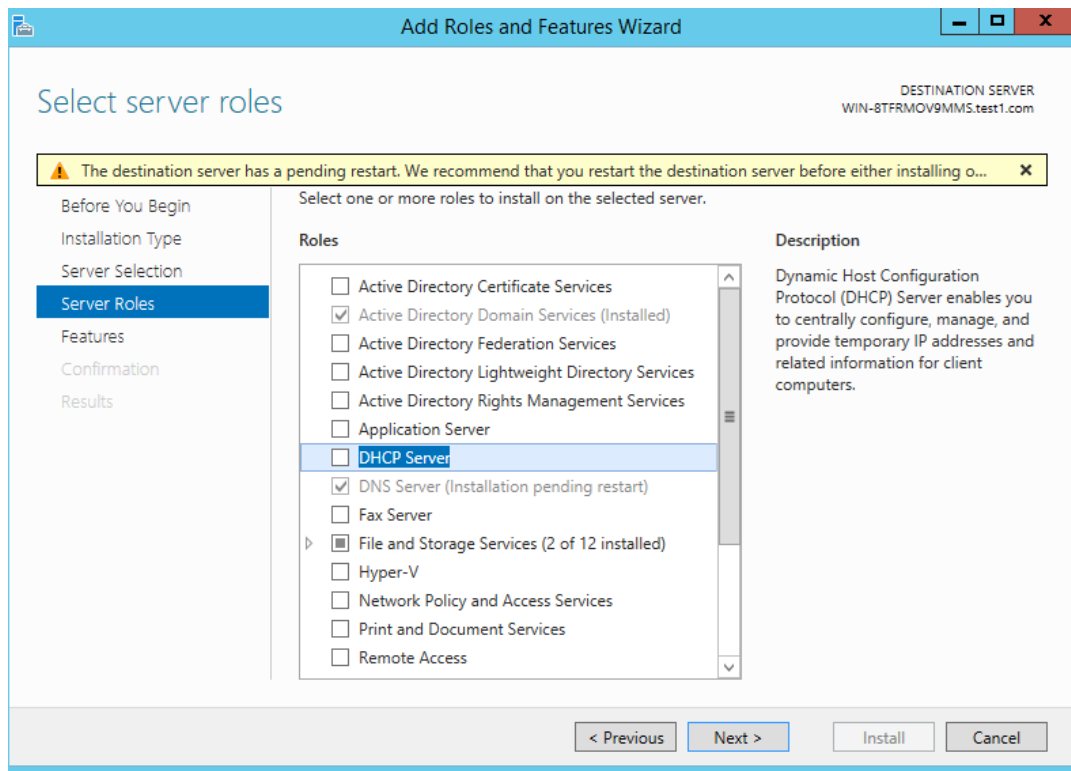
4. Select the installation type. Choose "Role-based or feature-based installation" and click "Next."



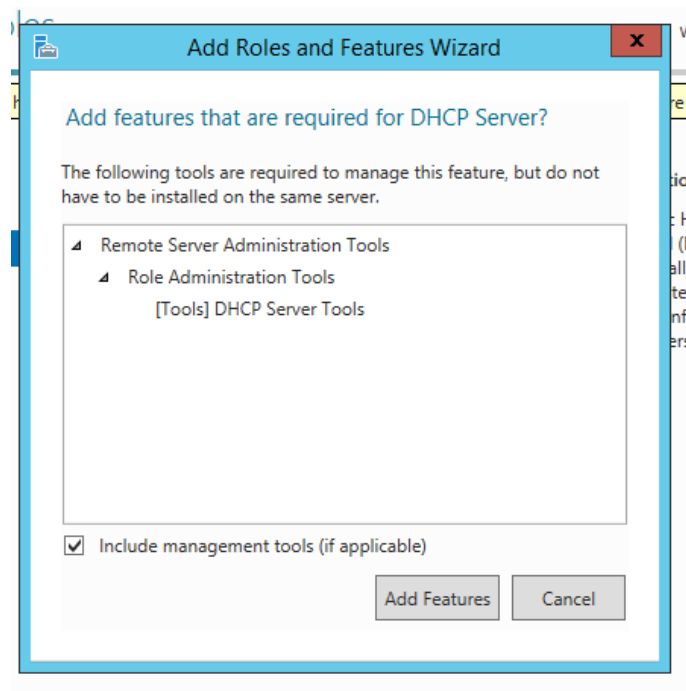
5. Select the appropriate server from the server pool and click "Next."



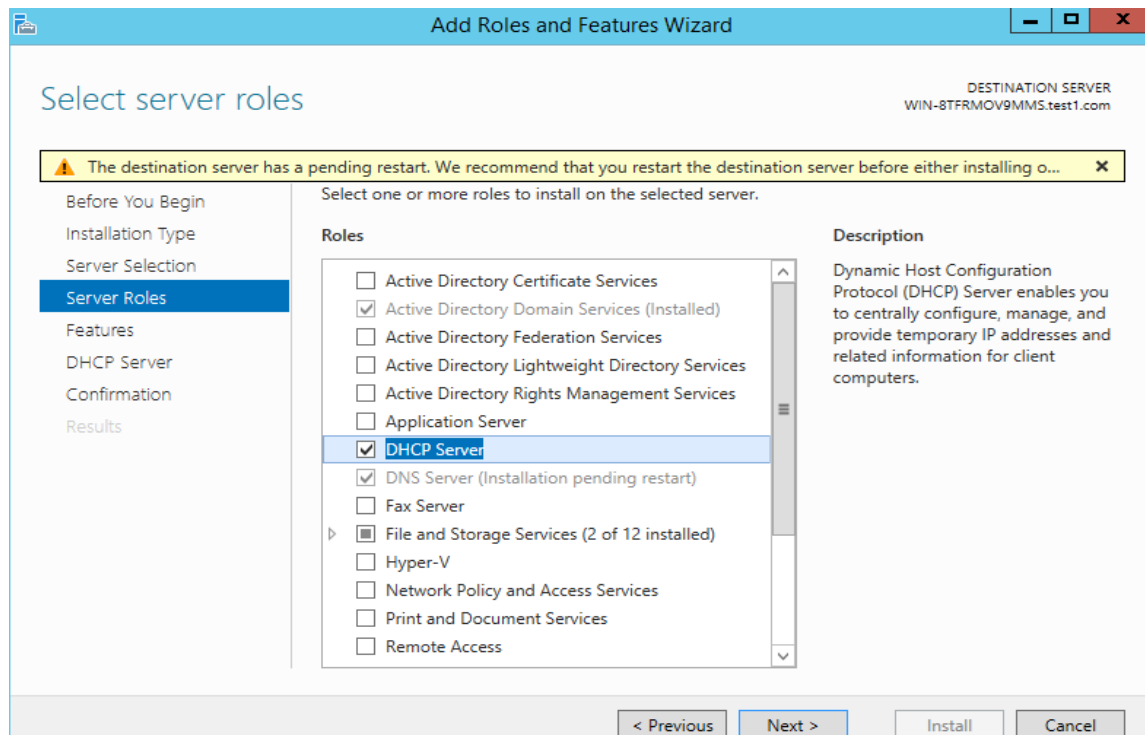
1. Scroll down and find the "DHCP Server" role. Check the box next to it to select it.



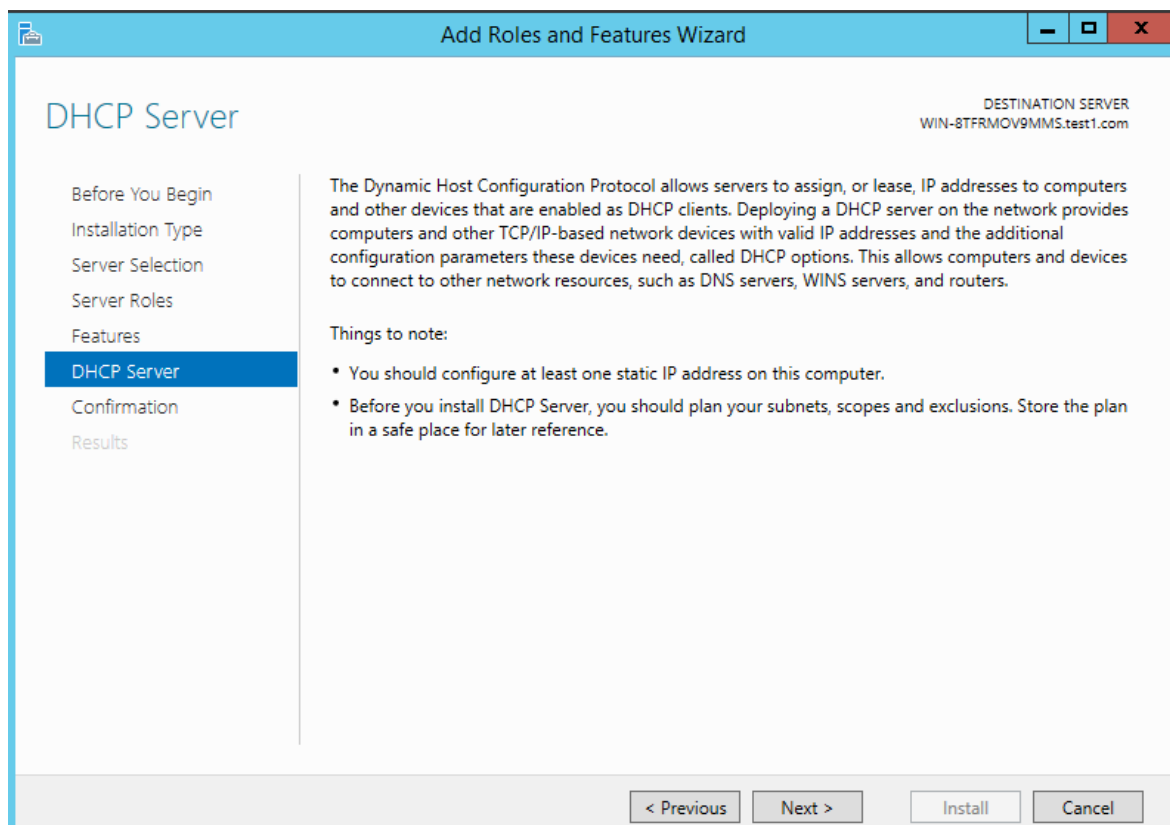
7. A prompt will appear asking to add the required features for the DHCP role. Click "Add Features" to include the necessary features.



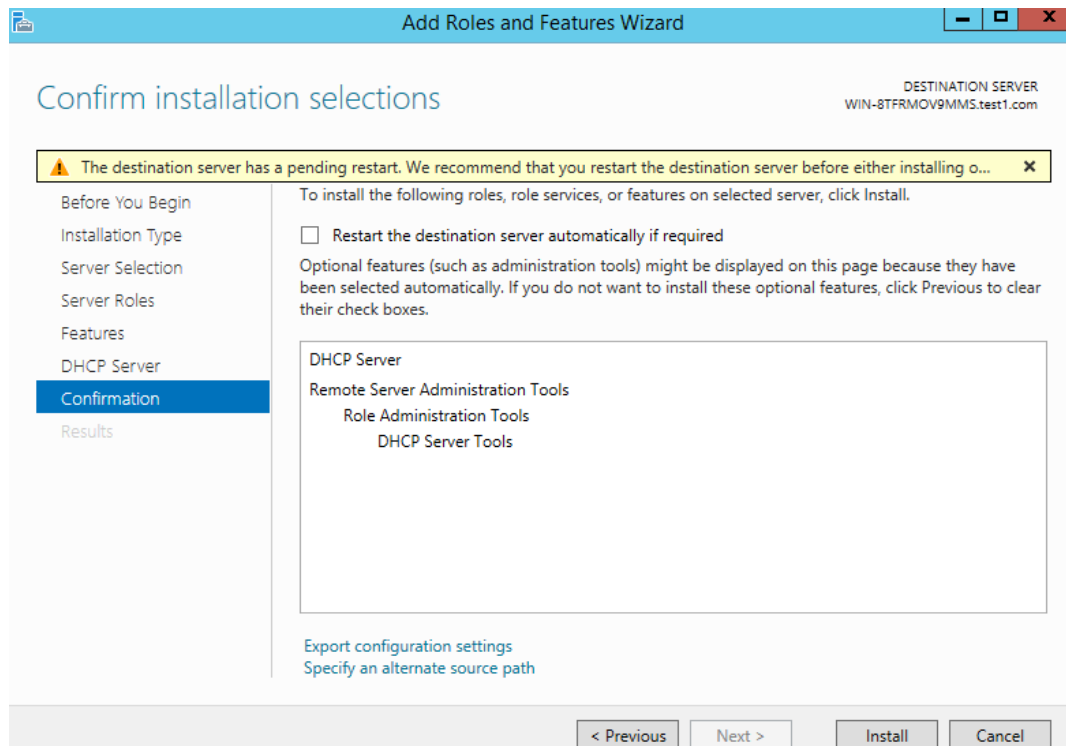
8. Click "Next" to proceed.



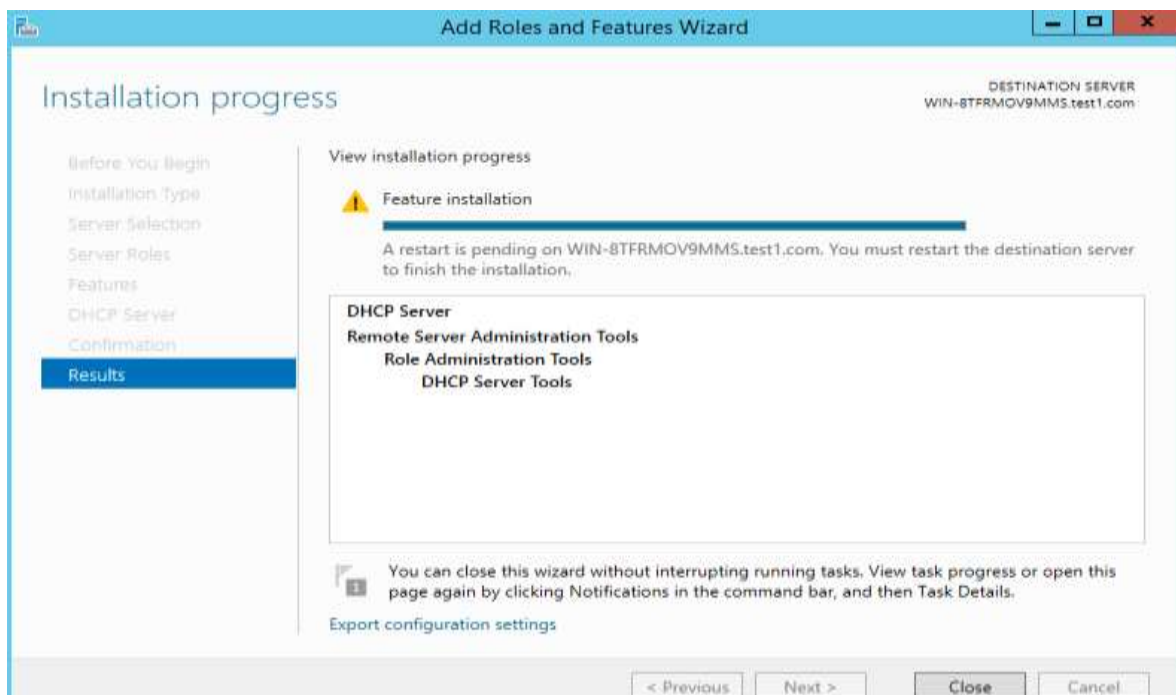
9. On the DHCP Server page, read the information provided and click "Next."



10. Review the summary of your selections and click **"Install"** to begin the installation process for the DHCP server role and features.



11. Once the installation is complete, you can configure and manage the DHCP server using the DHCP Manager tool.



Then configuration of DHCP Server is Done (Krause, 2024)



Points to Remember

- Description of server roles and features

1. The Domain Name System (DNS) is a critical service that translates human-readable domain names (e.g: www.example.com) into IP addresses.

2. Root Hints: A list of root DNS servers that a DNS server can use to resolve queries for domains it doesn't know.

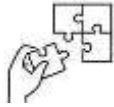
3. Zones and Zone Files

4. Key messages involved in the DHCP communication process are:DHCP Discover, DHCP Offer, DHCP Request, DHCP Acknowledgment

5. Fault Tolerance Implementations: To ensure continuous DHCP service availability, administrators can implement fault tolerance

Installation of server roles and features

- Installing DNS Server Role:
 - ✓ Open Server Manager.
 - ✓ Click on Add roles and features.
 - ✓ Proceed through the wizard by clicking Next.
 - ✓ Select Role-based or feature-based installation and click Next.
 - ✓ Choose the local server and click Next.
 - ✓ Check DNS Server and click Add Features.
 - ✓ Click Next through the subsequent screens.
 - ✓ Click Install.
 - ✓ Once installation completes, close the wizard.
- Installing DHCP Server Role:
 - ✓ Open Server Manager.
 - ✓ Click on Add roles and features.
 - ✓ Proceed through the wizard by clicking Next.
 - ✓ Select Role-based or feature-based installation and click Next.
 - ✓ Choose the local server and click Next.
 - ✓ Check DHCP Server and click Add Features.
 - ✓ Click Next through the subsequent screens.
 - ✓ Click Install.
 - ✓ Once installation completes, close the wizard.



Application of learning 1.4.

Bxz Solutions Inc. is a company specializing in providing IT solutions for small and medium businesses. Located in Rwanda, Eastern area, **Bxz Solutions Inc.** aims to enhance its network infrastructure by setting up essential server roles, including DNS and DHCP, to improve network management and efficiency.

As a system Administrator hired by Tech Solutions Inc., you are tasked with the following:

Tasks: Installation of Server Roles and Features (DNS and DHCP)



Indicative content 1.5: Configuration of DNS



Duration: 6hrs



Practical Activity 1.5.1: Configuring the lookup zones



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Trainee in Level 4 software development, you are requested to go to the computer lab to configure the Lookup zones in server administration.

2. Remember to read the key readings 1.5.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class



Key readings 1.5.1: Configuring the lookup zones

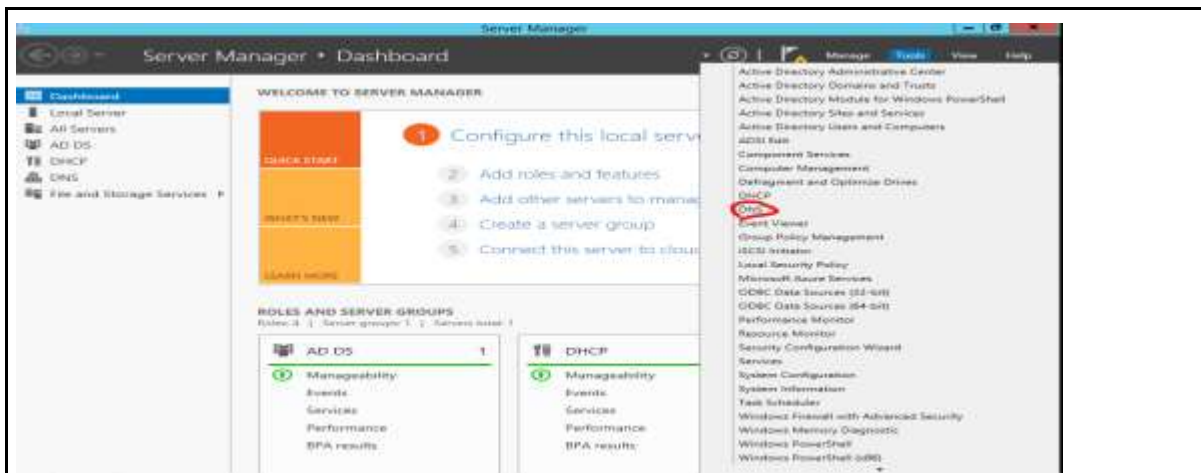
Lookup Zones in DNS refer to databases that store domain name information and are used to resolve domain names to IP addresses or vice versa.

Lookup zones in DNS are divided into two types:

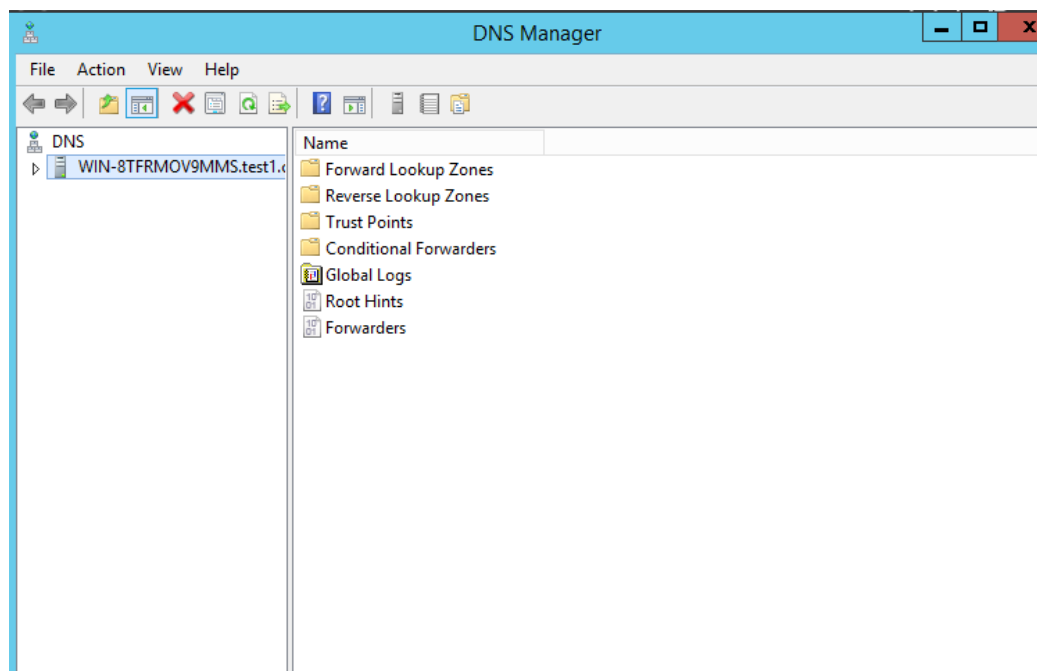
- 1. Forward Lookup Zone:** This zone resolves domain names to IP addresses. It is the most common type of DNS zone.
- 2. Reverse Lookup Zone:** This zone resolves IP addresses to domain names. It is used to perform reverse DNS lookups, mapping an IP address to its associated hostname.

To configure DNS lookup zones, you can follow these steps:

1. Open the DNS Manager on your Windows Server. You can access it through the Server Manager or directly from the Start menu.

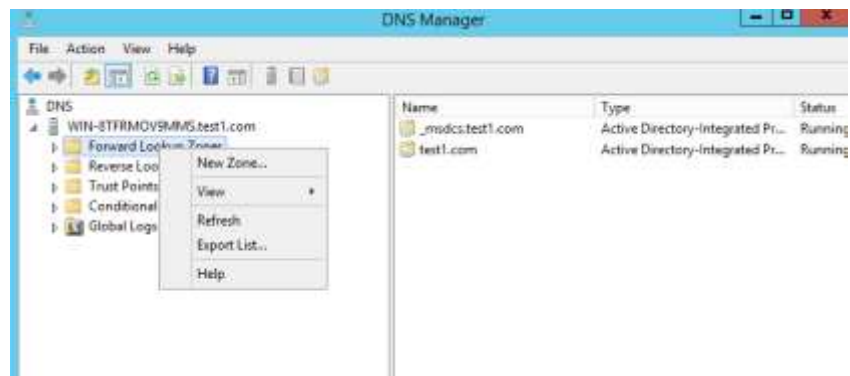


2. In the DNS Manager, you will see different sections such as Forward Lookup Zones, Reverse Lookup Zones, and Conditional Forwarders.

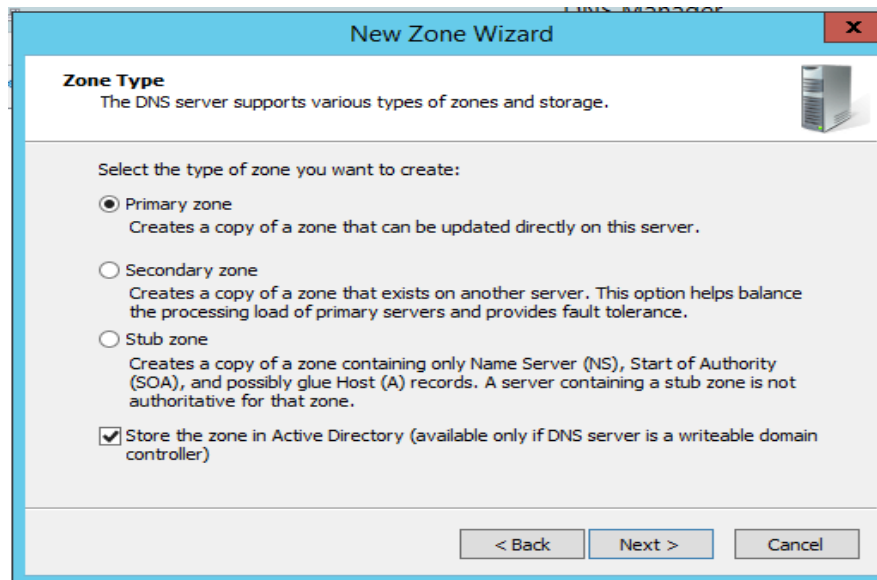


3. To configure a Forward Lookup Zone:

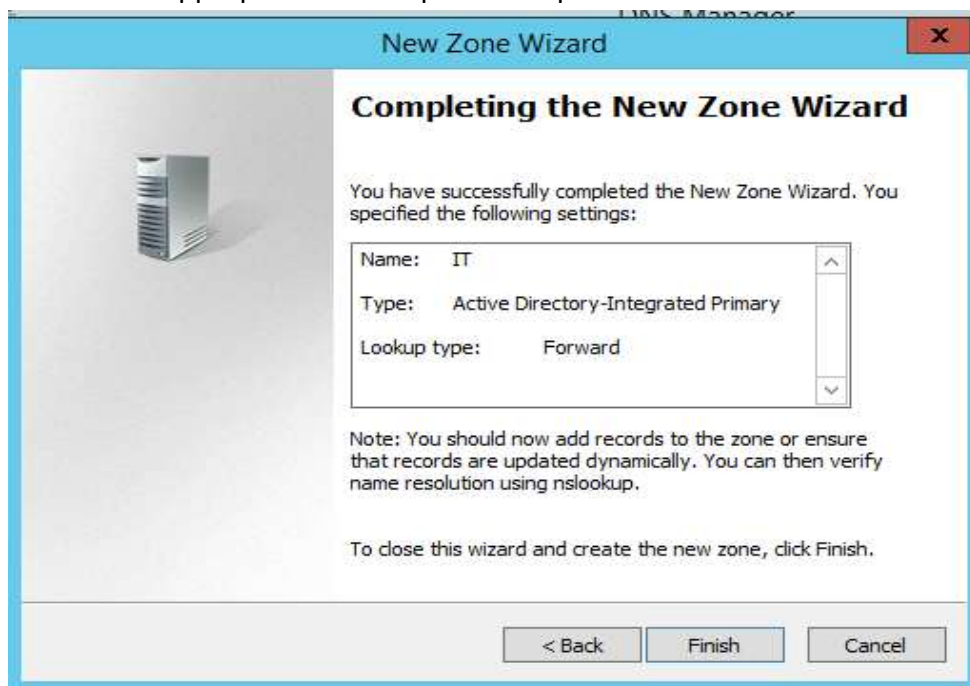
- ✓ Right-click on "Forward Lookup Zones" and select "New Zone."



- ✓ Follow the wizard to create a new zone and specify the zone type (primary, secondary, or stub) and the zone name (e.g., yourdomain.com).



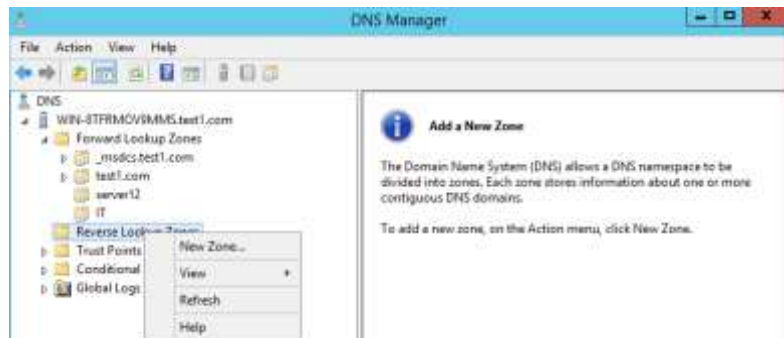
- ✓ Choose the appropriate zone replication options and DNS database file location.



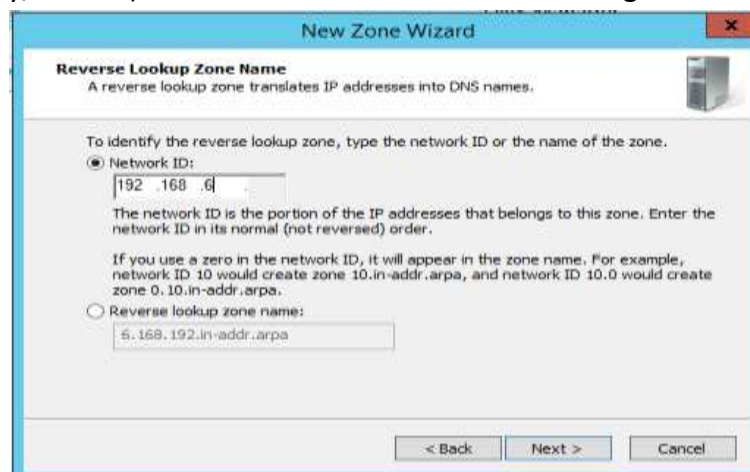
- ✓ Once the zone is created, you can manage its properties, add resource records, and configure other settings.

4. To configure a Reverse Lookup Zone:

- ✓ Right-click on "Reverse Lookup Zones" and select "New Zone."



- ✓ Follow the wizard to create a new zone and specify the zone type (primary, secondary, or stub) and the network ID or IP address range.

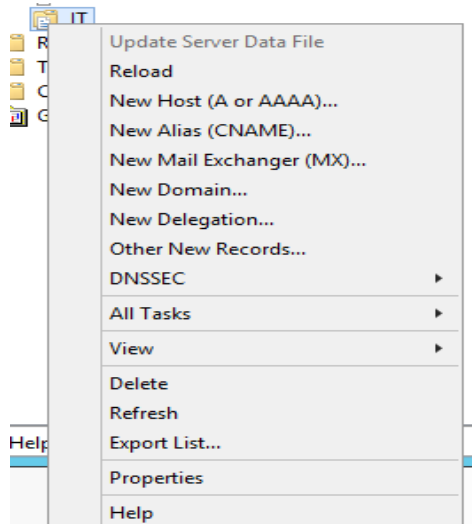


- ✓ Choose the appropriate zone replication options and DNS database file location.
- ✓ Once the zone is created, you can manage its properties, add resource records, and configure other settings.

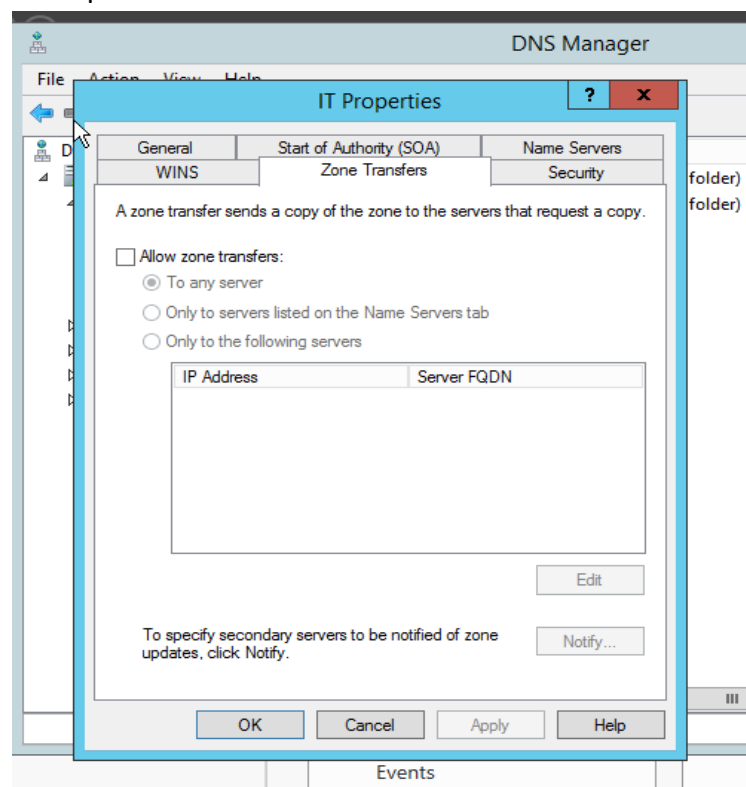


5. You can also configure zone transfer settings for each zone to control how the zone information is replicated between DNS servers.

- ✓ Right-click on the zone and select "Properties."



- ✓ Go to the "Zone Transfers" tab and configure the settings for allowing or denying zone transfers to specific DNS servers.





Practical Activity 1.5.2: Creation of Alias (CNAME)

Task:

1. You are requested to go to the computer lab and do the task below individually.
As a Trainee in Level 4 software development, you are requested to go to the computer lab to create an Alias (CNAME) record in DNS server administration.
2. Ask to read the key readings 1.5.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class

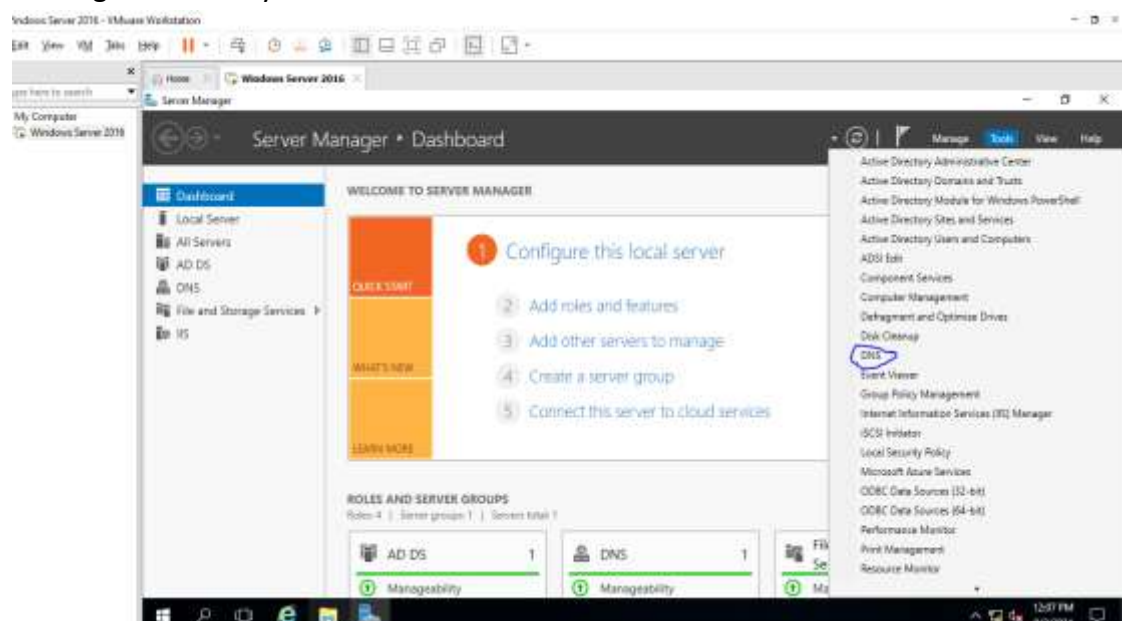


Key readings 1.5.2: Creation of Alias (CNAME)

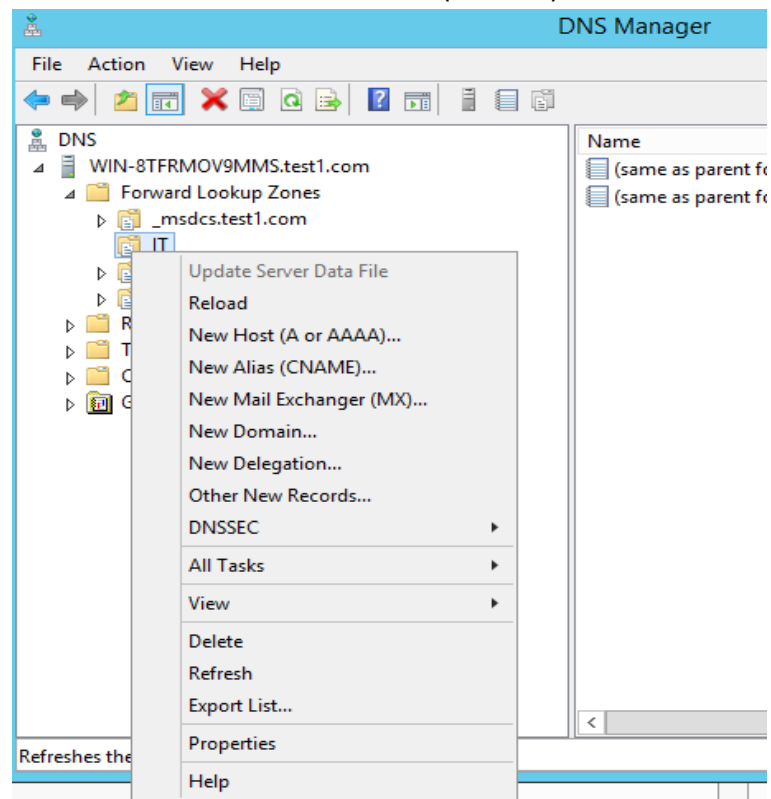
A **CNAME (Canonical Name)** record is used to create an alias for another domain name. It allows you to point multiple domain names to the same IP address or web server, making management easier. For example, you can have **www.example.com** point to **example.com** using a CNAME record.

To create an Alias (CNAME) record in DNS, you can follow these steps:

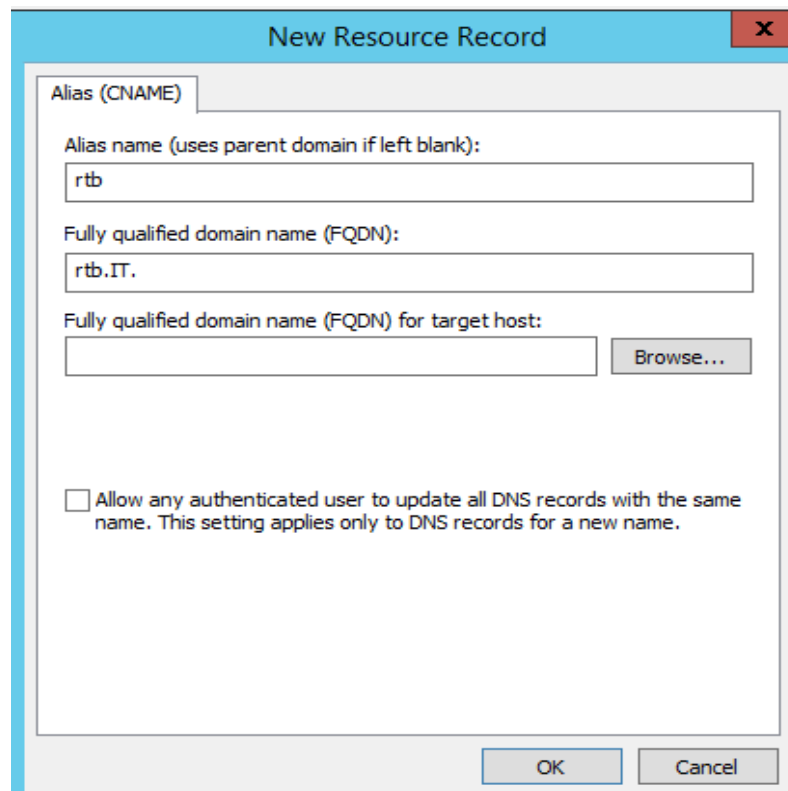
1. Open the DNS Manager on your Windows Server. You can access it through the Server Manager or directly from the Start menu.



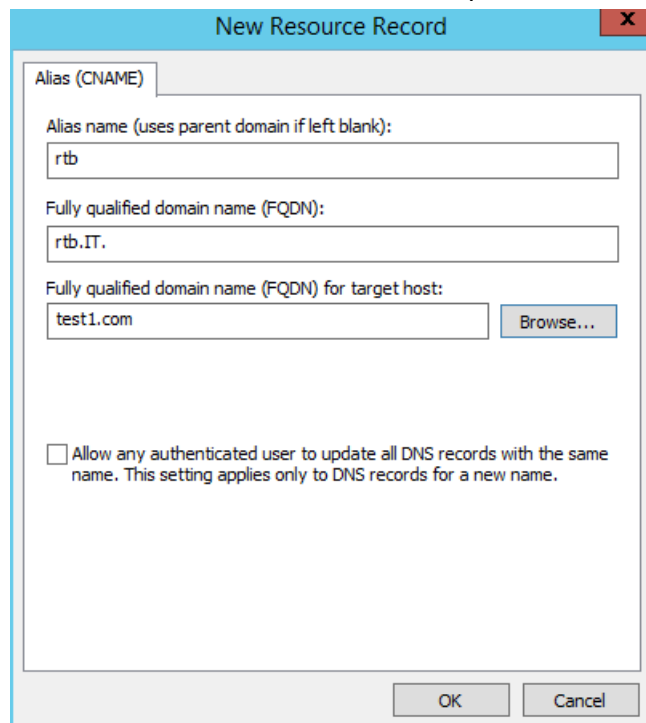
2. In the DNS Manager, navigate to the Forward Lookup Zone where you want to create the Alias (CNAME) record.
3. Right-click on the zone and select "New Alias (CNAME)" from the context menu.



4. In the New Resource Record window, enter the Alias name. This is the domain name or hostname for which you want to create an alias.



5. In the Fully qualified domain name (FQDN) for target host field, enter the fully qualified domain name or hostname to which the alias should point.



6. Click "OK" to create the CNAME record.

6. The Alias (CNAME) record will now be added to the DNS zone.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], win-8tfrm
(same as parent folder)	Name Server (NS)	win-8tfrmov9
rtb	Alias (CNAME)	test1.com



Practical Activity 1.5.3: Configuring DNS records



Task:

1. You are requested to go to the computer lab and do the task below individually.
As a Trainee in Level 4 software development, you are requested to go to the computer lab to configure different types of DNS records, including A, AAAA, CNAME, MX, PTR, NS, and SOA in server administration.
2. Remember to read the key readings 1.5.3 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task

5. Perform the task on your computer
6. Present the work to the whole class

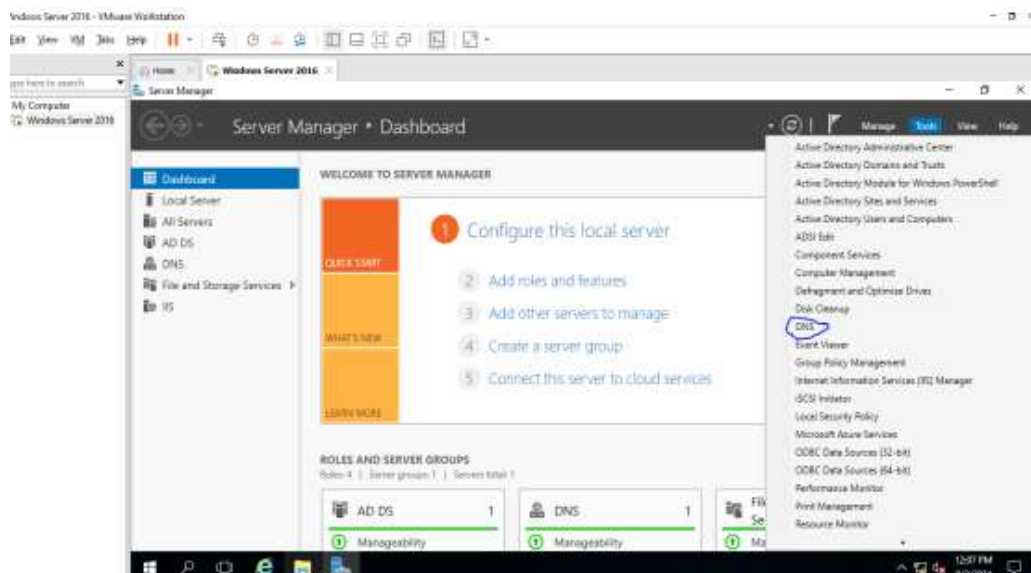


Key readings 1.5.3: Configuring DNS records

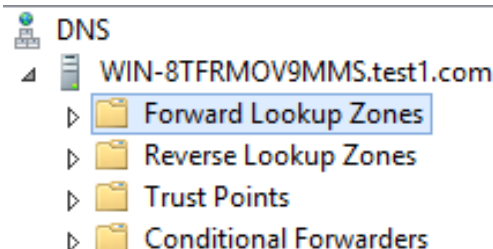
DNS records are the fundamental components of DNS zones. They define the relationships between domain names and IP addresses or other resources.

To configure different types of DNS records, including A, AAAA, CNAME, MX, PTR, NS, and SOA, you can follow these steps:

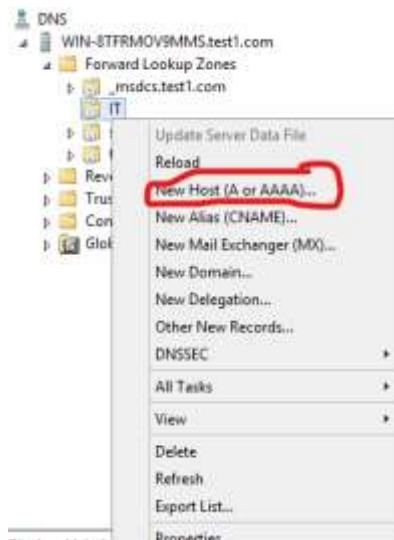
1. Open the DNS Manager on your Windows Server. You can access it through the Server Manager or directly from the Start menu.



2. In the DNS Manager, navigate to the appropriate Forward Lookup Zone or Reverse Lookup Zone where you want to create the DNS record.



3. Right-click on the zone and select the type of record you want to create (e.g., "New Host (A or AAAA)," "New Alias (CNAME)," "New Mail Exchanger (MX)," etc.).



4. Follow the wizard or the prompt to provide the necessary information for the specific record type you are creating.

 A screenshot of the 'New Host' dialog box. It has a title bar 'New Host' with a close button. The dialog contains three text input fields: 'Name (uses parent domain name if blank):' with the value 'rtb2', 'Fully qualified domain name (FQDN):' with the value 'rtb2.baka.com.', and 'IP address:' with the value '192.168.10.15'. Below these fields are two checkboxes: 'Create associated pointer (PTR) record' which is checked, and 'Allow any authenticated user to update DNS records with the same owner name' which is unchecked. At the bottom right are two buttons: 'Add Host' and 'Cancel'.

Here's a brief description of each record type:

A Record: Maps a domain name to an IPv4 address. This is the most common DNS record used to point a domain name to a web server.

AAAA Record: Maps a domain name to an IPv6 address. Similar to an A record but for IPv6 addresses.

CNAME (Canonical Name) Record: Points one domain name to another domain name (an alias). For example, *www.example.com* could point to *example.com*.

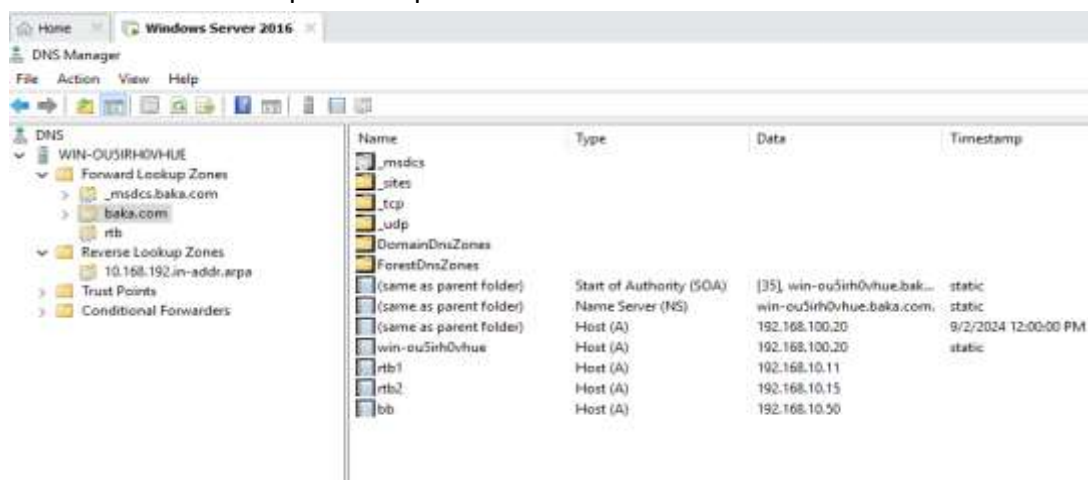
MX Record: Directs email to the mail server for a domain. This record specifies the mail servers responsible for receiving email on behalf of a domain

PTR (Pointer) Record: Used in reverse lookup zones to map an IP address to a domain name. It provides the reverse mapping for A records.

NS (Name Server) Record: Specifies the authoritative name servers for a domain. These servers are responsible for resolving queries for that domain.

SOA (Start of Authority) Record: Contains administrative information about the domain, including the primary name server, the email of the domain administrator, and other important details about the domain's DNS settings.

5. Complete the process to create the DNS record.



6. You can manage and modify the properties of the DNS record by right-clicking on it and selecting "Properties."



Points to Remember

- **Configuring lookup zones**

1. Open DNS Manager: Access via Server Manager or Start menu.
2. Sections such as Forward Lookup Zones, Reverse Lookup Zones
3. Configure Forward Lookup Zone
4. Configure Reverse Lookup Zone
5. Configure Zone Transfer Settings

- **Creation of Alias (CNAME)**

You can follow these steps:

1. Open the DNS Manager on your Windows Server.
2. In the DNS Manager, navigate to the Forward Lookup Zone where you want to create the Alias (CNAME) record.
3. Right-click on the zone and select "New Alias (CNAME)" from the context menu.

4. In the New Resource Record window, enter the Alias name.
5. In the Fully qualified domain name (FQDN) for target host field, enter the fully qualified domain name or hostname to which the alias should point.
6. Click "OK" or finish to create the CNAME record.

- **Configuring DNS records**

To configure different types of DNS records, including A, AAAA, CNAME, MX, PTR, NS, and SOA, you can follow these steps:

1. Open the DNS Manager on your Windows Server.
2. In the DNS Manager, navigate to the appropriate Forward Lookup Zone or Reverse Lookup Zone where you want to create the DNS record.
3. Right-click on the zone and select the type of record you want to create (example "New Host (A or AAAA)," "New Alias (CNAME)," "New Mail Exchanger (MX)," etc.).
4. Follow the wizard or the prompt to provide the necessary information for the specific record type you are creating.
5. Complete the process to create the DNS record.
6. You can manage and modify the properties of the DNS record by right-clicking on it and selecting "**Properties**"



Application of learning 1.5.

Bxz Solutions Inc. is a company specializing in providing IT solutions for small and medium businesses. Located in Rwanda, Eastern area, Bxz Solutions Inc. aims to enhance its network infrastructure by setting up essential server roles, including DNS Configuration to improve network management and efficiency. As an System Administrator hired by Bxz Solutions Inc., you are tasked with the following:

Task: Configure DNS Zones, Create Alias (CNAME) Records, Manage DNS Records.



Indicative content 1.6: Configuration of DHCP Parameters



Duration: 6hrs



Practical Activity 1.6.1: Configure DHCP scope parameters



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Trainee in Level 4 software development, you are requested to go to configure DHCP scope parameters in server administration.

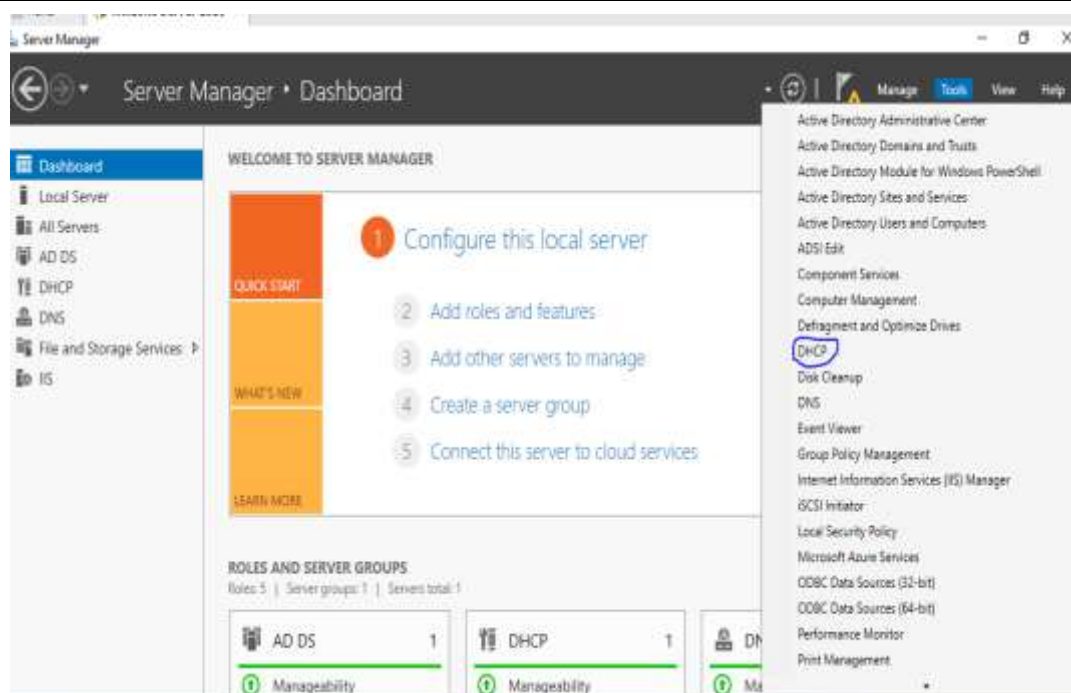
2. Read the key readings 1.6.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class
6. Remember to perform practical activity 1.6.1



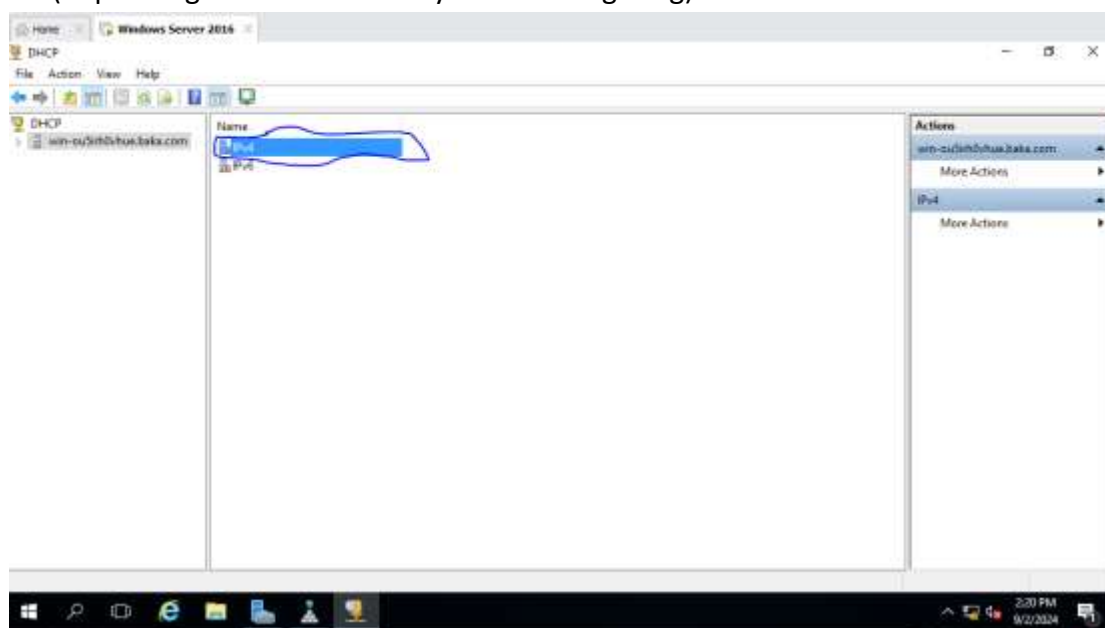
Key readings 1.6.1: Configure DHCP scope parameters

To configure DHCP scope parameters, including scope name, range of IP addresses, subnet mask, exclusions, lease time, and starting the DHCP service, you can follow these steps:

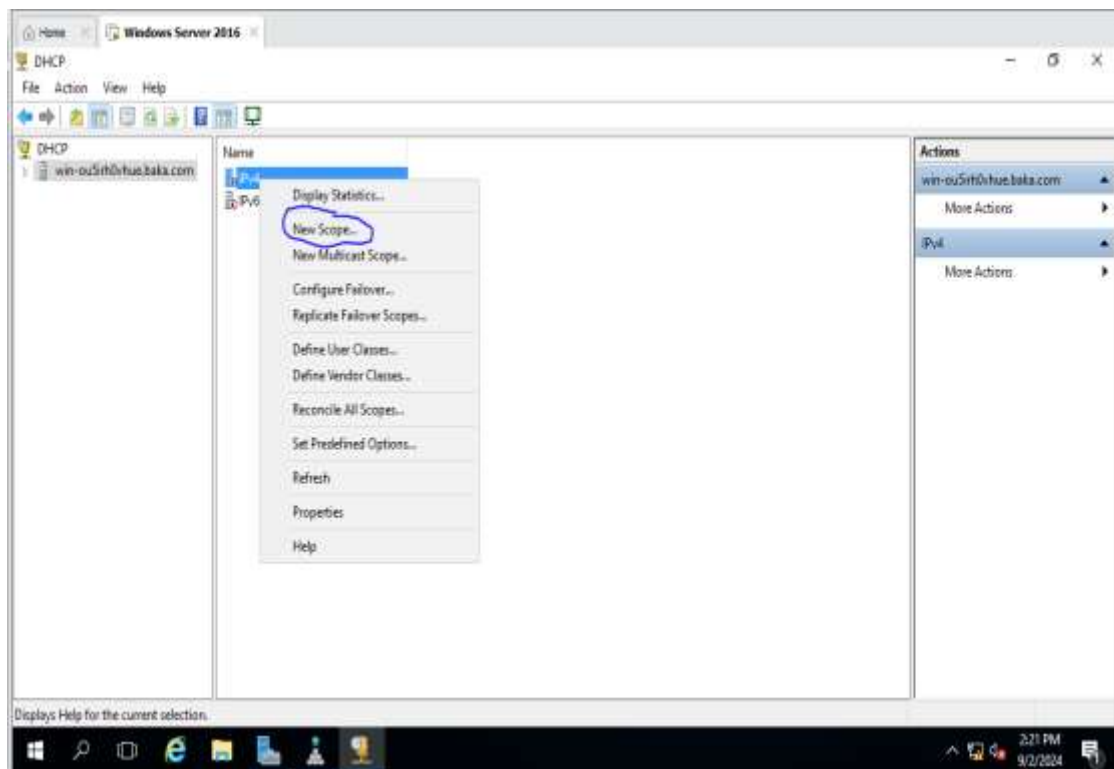
1. Open the DHCP Manager on your Windows Server. You can access it through the Server Manager or directly from the Start menu.



2. In the DHCP Manager, expand the server name and navigate to "IPv4" or "IPv6" (depending on the IP version you are configuring).



3. Right-click on "IPv4" or "IPv6" and select "New Scope" from the context menu.



4. Follow the New Scope Wizard to configure the DHCP scope parameters. Here's how you can set the key parameters:

The Scope Name is a descriptive label that identifies the scope within the DHCP server. It helps differentiate between various scopes, especially in networks with multiple subnets or VLANs.

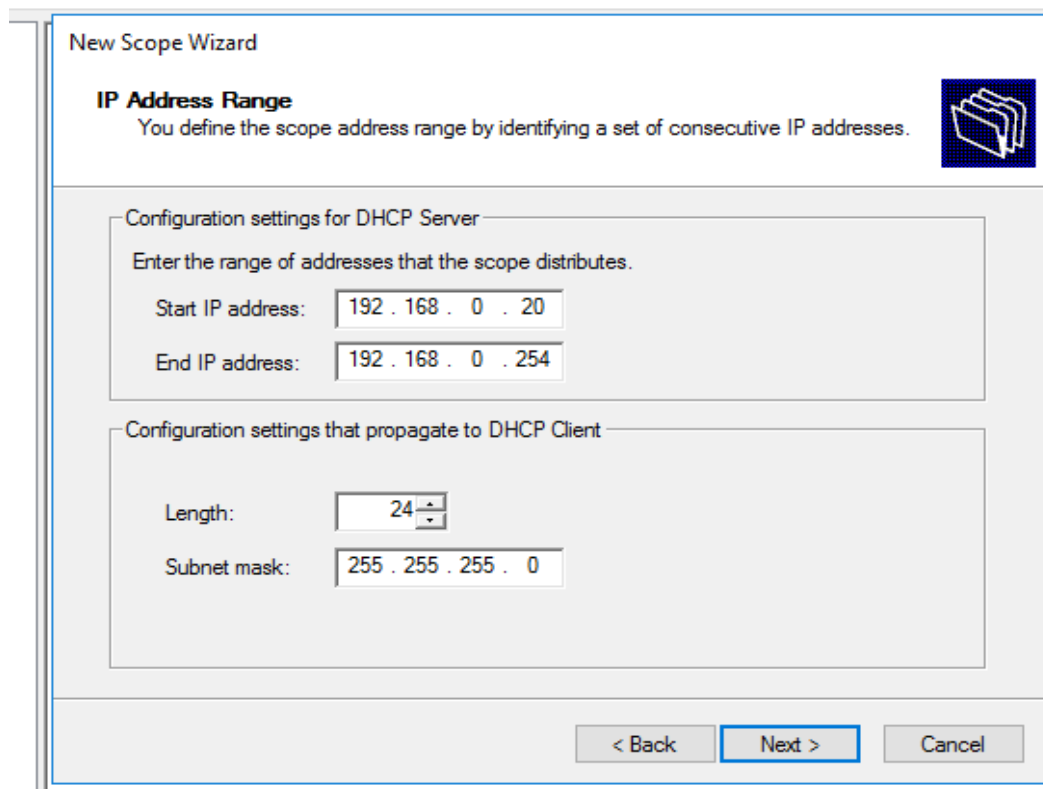
 A screenshot of the 'New Scope Wizard' dialog box, specifically the 'Scope Name' step. The dialog has a title bar 'New Scope Wizard' and a subtitle 'Scope Name'. Below the subtitle, it says 'You have to provide an identifying scope name. You also have the option of providing a description.' To the right of this text is a folder icon. Below this, a larger text box says 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' There are two input fields: 'Name:' with the text 'RTB' and 'Description:' with the text 'RWANDA TVET BOARD'. At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

The Range of IP Addresses defines the available IP addresses that the DHCP server can assign to network devices. For example, a range of 192.168.0.20 to 192.168.0.254 allows any IP address within that range to be assigned.

Starting IP Address: Specify the first IP address in the range that will be assigned by the DHCP server.

Ending IP Address: Specify the last IP address in the range.

The Subnet Mask determines which part of an IP address belongs to the network and which part identifies the host. It ensures that devices receiving IP addresses are correctly segmented into their respective networks.



The screenshot shows the 'New Scope Wizard' window in the Windows Server DHCP console. The title bar reads 'New Scope Wizard'. The main heading is 'IP Address Range' with a sub-instruction: 'You define the scope address range by identifying a set of consecutive IP addresses.' To the right of this text is a blue icon of a folder with a document. Below this, there are two sections: 'Configuration settings for DHCP Server' and 'Configuration settings that propagate to DHCP Client'. The first section contains the instruction 'Enter the range of addresses that the scope distributes.' and two input fields: 'Start IP address:' with the value '192 . 168 . 0 . 20' and 'End IP address:' with the value '192 . 168 . 0 . 254'. The second section contains two input fields: 'Length:' with a dropdown menu showing '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Exclusions: are IP addresses or address ranges excluded from the DHCP scope, ensuring they are not assigned to clients. This is essential for avoiding conflicts with statically assigned IP addresses.

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

Excluded address range:

Subnet delay in milli second:

< Back **Next >** Cancel

Lease Duration: Set the lease time, which determines how long an IP address is leased to a client before it must be renewed. Specify the lease duration in hours, days, or weeks.

The Lease Time specifies how long a client can use an IP address before the lease expires and the address needs to be renewed. For example, a lease time of 8 hours means that after 8 hours, the client must either renew the lease or request a new IP address.

Lease duration for DHCP clients

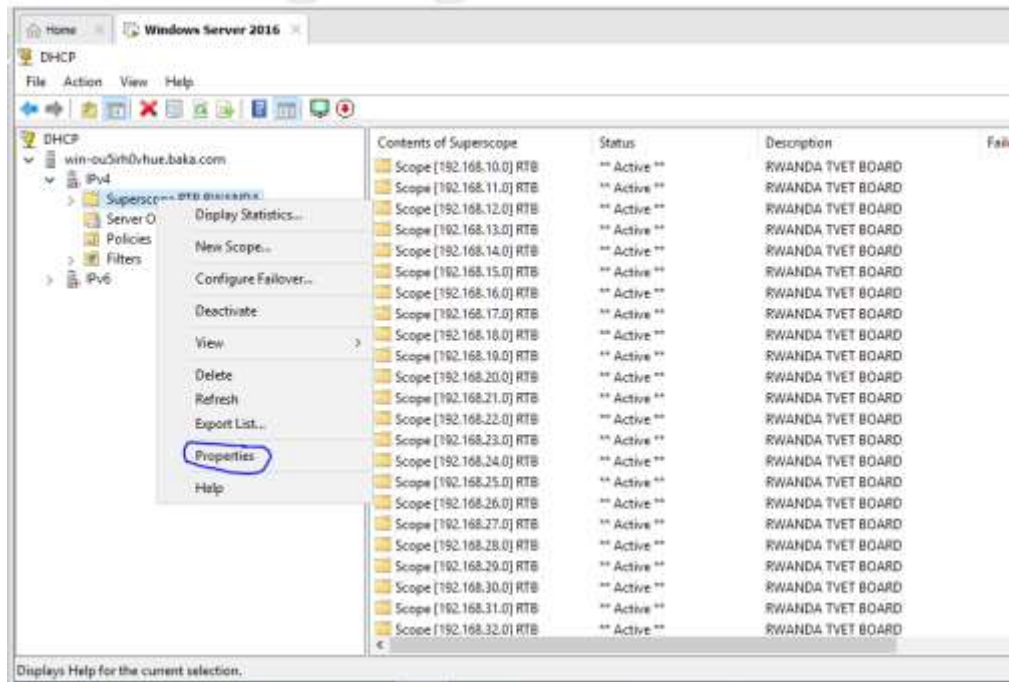
☒ Limited to:

Days: Hours: Minutes:

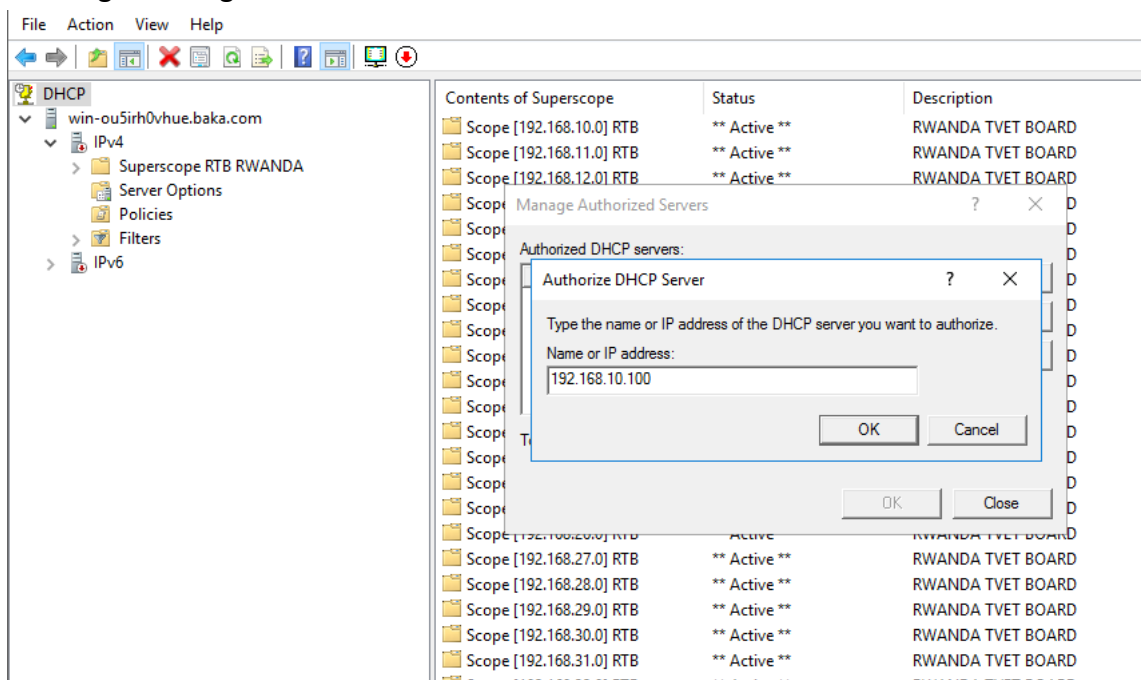
☐ Unlimited

Activate the Scope: Enable the scope to start leasing IP addresses.

5. Complete the wizard to create the DHCP scope with the specified parameters.
6. Once the scope is created, you can modify its properties by right-clicking on it and selecting "Properties." This allows you to make changes to the scope settings, such as lease duration, exclusions, and more.



7. To start the DHCP service, right-click on the DHCP server name and select "Authorize" or "Start" from the context menu. This will activate the DHCP service and allow it to begin leasing IP addresses to clients.





Practical Activity 1.6.2: Configuring DHCP reservations



Task:

1. You are requested to go to the computer lab and do the task below individually. As a Trainee in Level 4 software development, you are requested to go computer Lab to configure DHCP reservations in server administration.
2. Read the key readings 1.6.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the Trainer and whole class



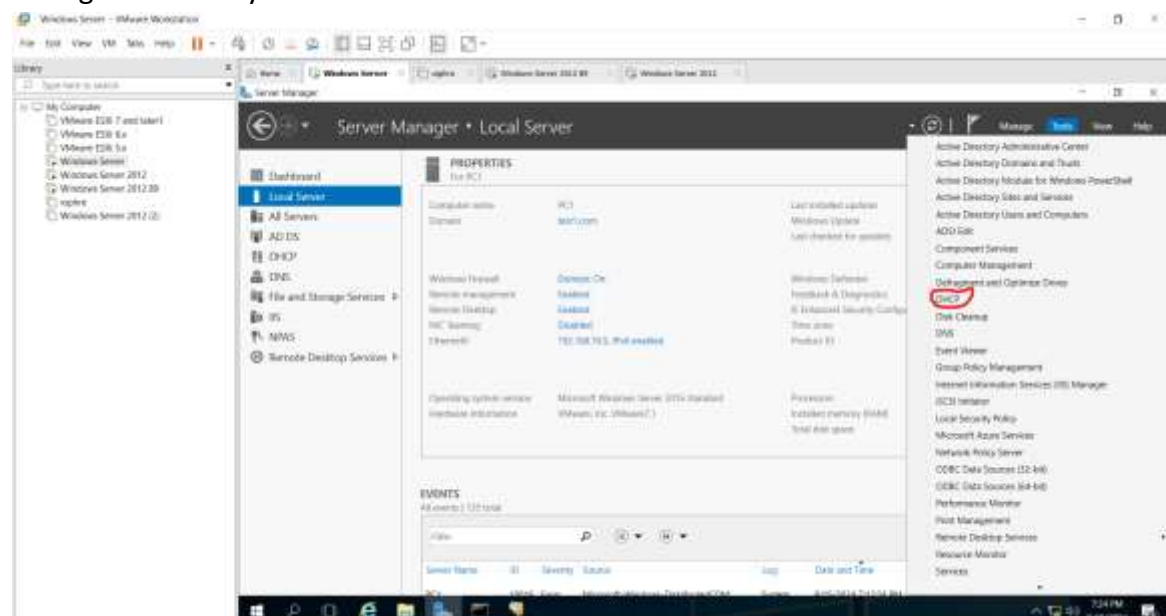
Key readings 1.6.2: Configuring DHCP reservations

To configure DHCP reservations, which assign specific IP addresses to specific devices based on their MAC addresses,

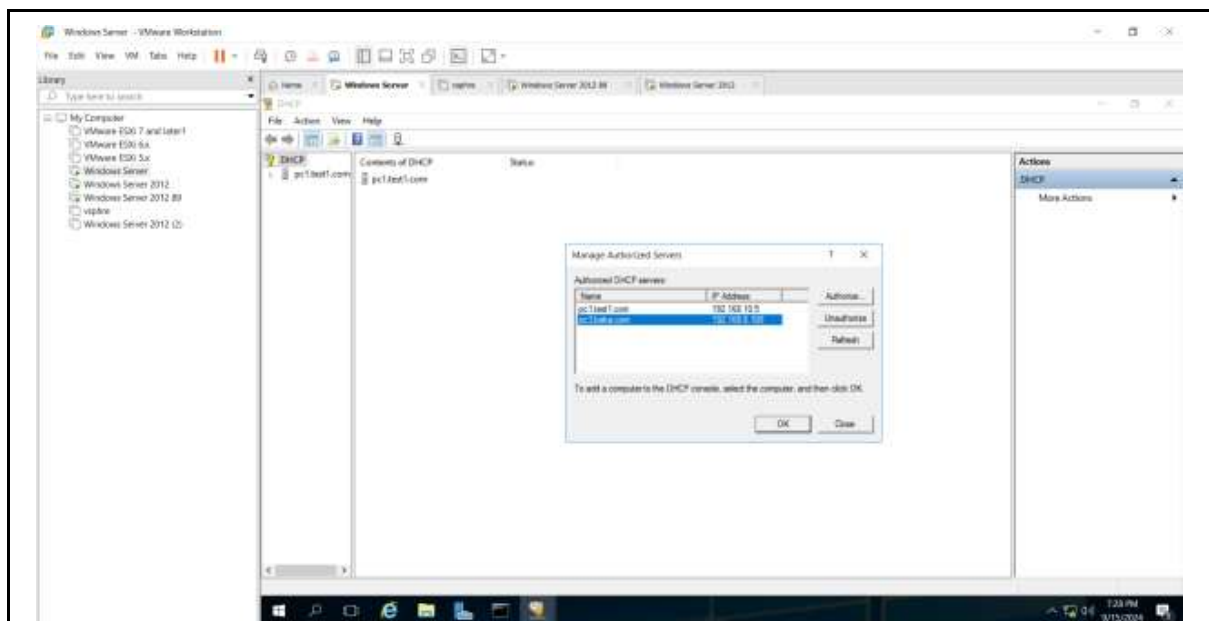
Reservation: Ensures that a specific device always receives the same IP address from the DHCP server. This is done by associating the device's MAC address with a fixed IP address within the DHCP scope. Useful for devices that require a consistent IP, such as printers or servers.

you can follow these steps:

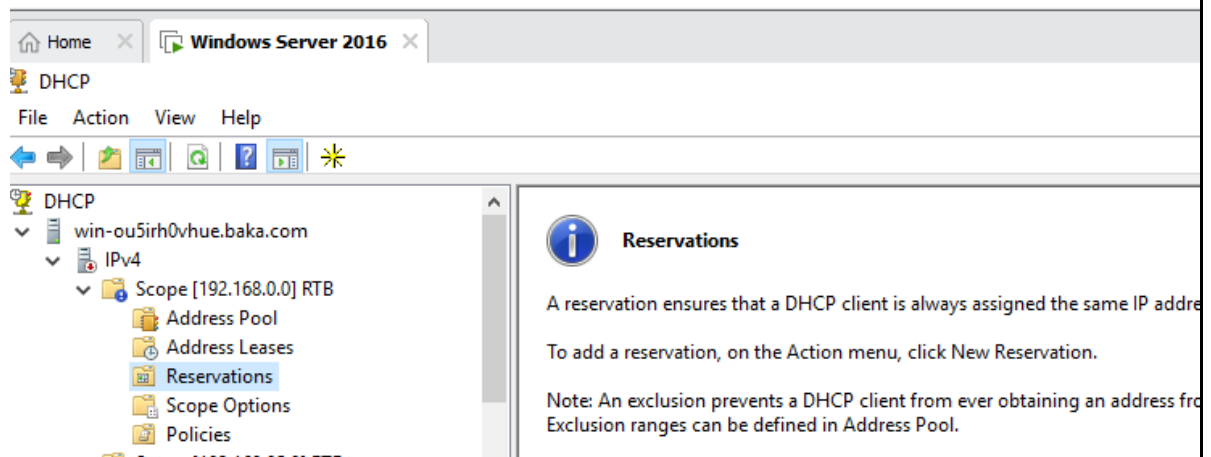
1. Open the DHCP Manager on your Windows Server. You can access it through the Server Manager or directly from the Start menu.



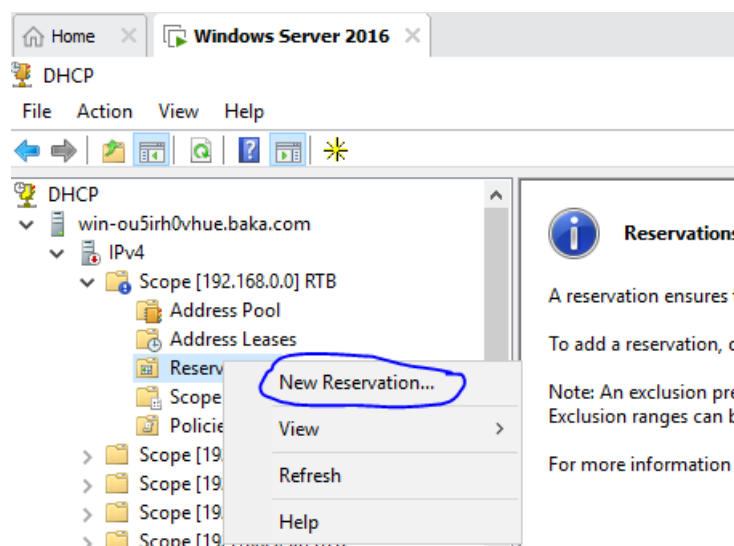
2. In the DHCP Manager, expand the server name and navigate to "IPv4" or "IPv6" (depending on the IP version you are configuring).



3. Expand the DHCP scope where you want to create the reservation.



4. Right-click on "Reservations" and select "New Reservation" from the context menu.



5. In the New Reservation window, provide the following information:

Reservation Name: Provide a descriptive name for the reservation to identify it easily.

IP Address: Enter the specific IP address you want to assign to the device.

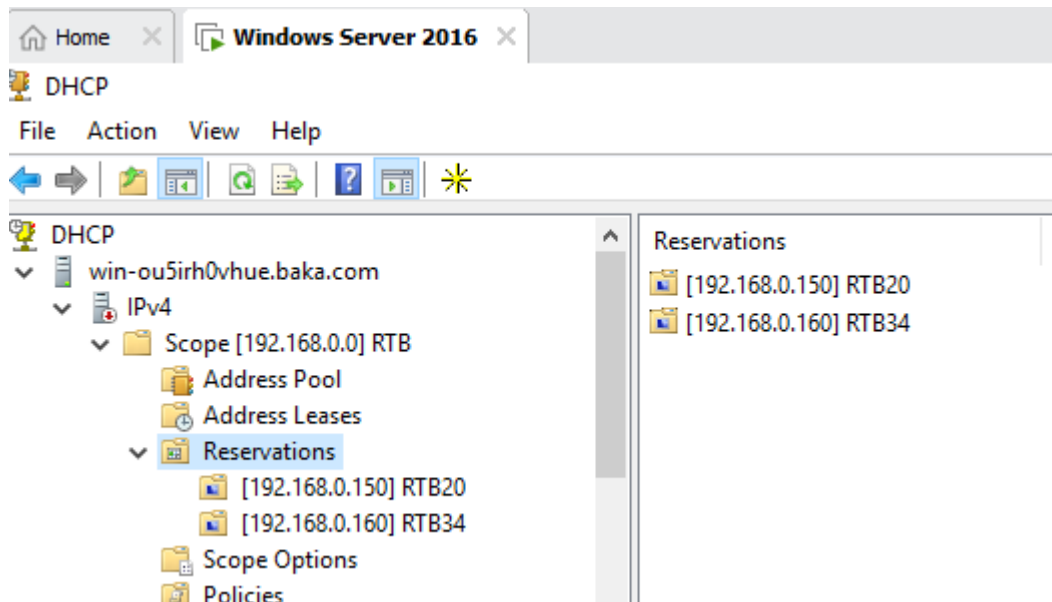
MAC Address: Enter the MAC address of the device for which you want to reserve the IP address.

Description (optional): Add an optional description to provide additional information about the reservation.

The 'New Reservation' dialog box is shown with the following details:

- Reservation name:** RTB34
- IP address:** 192 . 168 . .
- MAC address:** 080028B299B1
- Description:** RTB RWNDAL
- Supported types:** ☒ Both, ☐ DHCP, ☐ BOOTP
- Buttons:** Add, Close

6. The reservation will now be added to the DHCP scope, ensuring that the specified device always receives the assigned IP address.





Practical Activity 1.6.3: Configuring DHCP failover



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Trainee in Level 4 software development, you are requested to go to configure DHCP failover for high availability and redundancy in server administration.

2. You are asked to read the key readings 1.6.3 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the Trainer and whole class



Key readings 1.6.3: Configuring DHCP failover

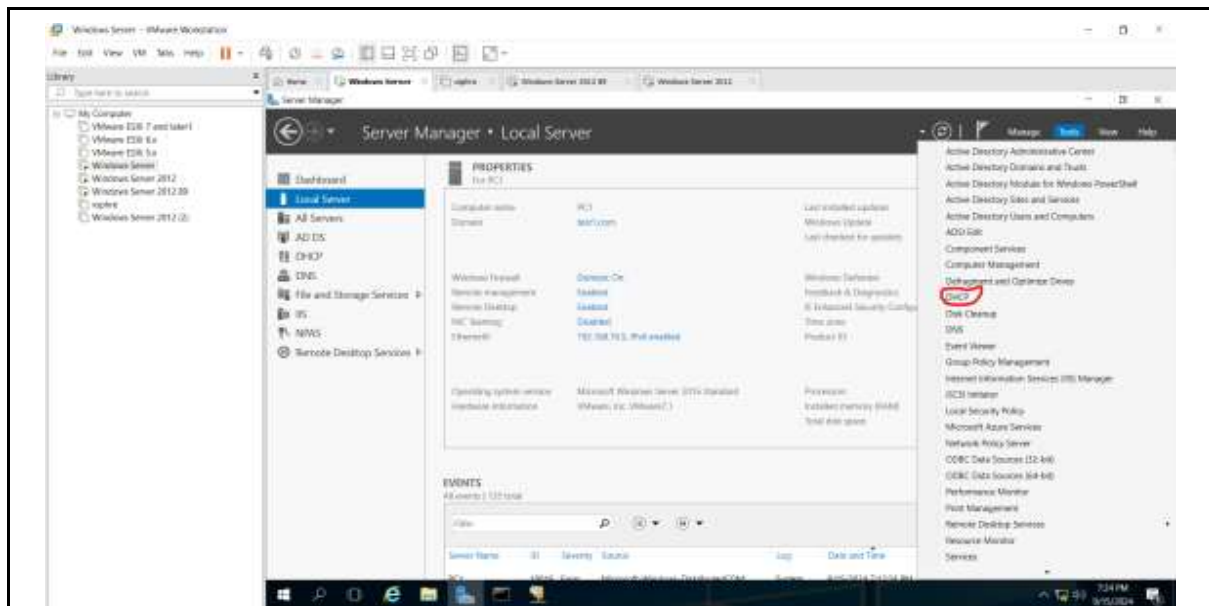
To configure DHCP failover for high availability and redundancy,

DHCP Failover is a setup where two DHCP servers work together to provide continuous service. If one server stops working, the other can take over.

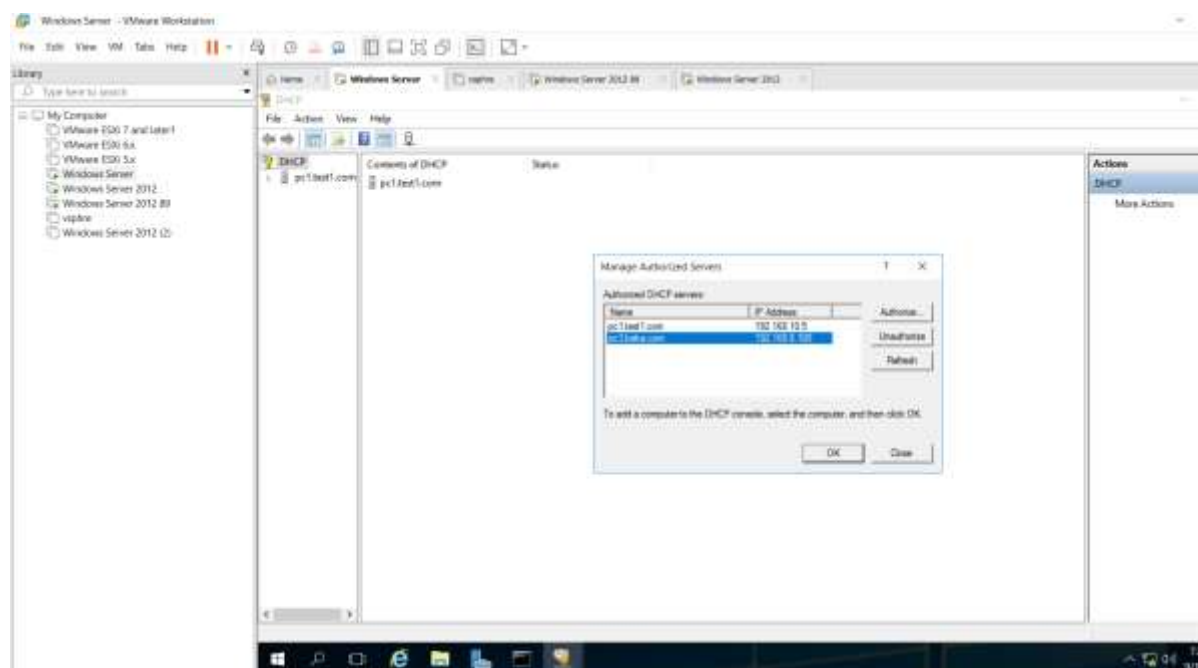
Failover is a backup system for DHCP servers, making sure that if one server fails, the other can continue to provide IP addresses and keep your network running smoothly.

you can follow these steps:

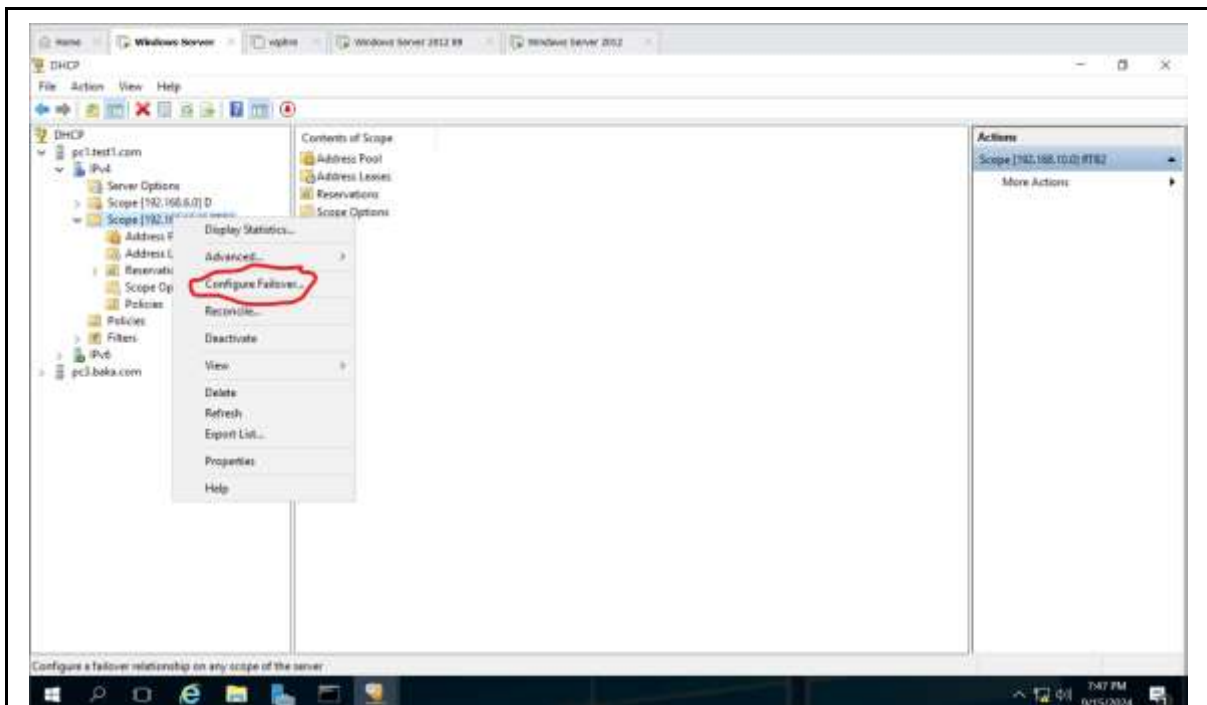
1. Open the DHCP Manager on your Windows Server. You can access it through the Server Manager or directly from the Start menu.



2. In the DHCP Manager, expand the server name and navigate to "IPv4" or "IPv6" (depending on the IP version you are configuring).



3. Right-click on "IPv4" or "IPv6" and select "Configure Failover" from the context menu.



4. In the Configure Failover Wizard, choose the appropriate options for your failover configuration:

- Select the DHCP scope to configure failover for.
- Choose the partner server: Specify the IP address or hostname of the partner server that will participate in the failover.
- Specify the relationship name: Provide a descriptive name for the failover relationship.
- Choose the mode: Select the failover mode, such as Load Balance or Hot Standby, based on your requirements.
- Specify the communication protocol and port: Choose the protocol (IPv4 or IPv6) and the port number for the failover communication.
- Set the relationship authentication: Specify the shared secret for authentication between the DHCP servers.
- Configure the failover settings: Set the percentage of load balancing, the maximum client lead time, and other parameters based on your needs.

Configure Failover

Select from failover relationships which are already configured on this server



There are existing failover relationships configured on this server with win-8tfmov9mms

Please select one of the existing relationships to use:

Relationship name:

win-bg1k522gpt.test1.com-win-8tfmov9mms

Maximum Client Lead Time:

1 hrs 0 mins

Mode:

Load balance

State switchover interval:

Disabled

Load Balance Percentage

Local Server:

50 %

Partner Server:

50 %

< Back

Next >

Cancel

5. Complete the wizard to configure the DHCP failover relationship.

Configure Failover

Failover will be set up between pc1.test1.com and win-8tfmov9mms with the following parameters.

Scopes:

192.168.10.0

Relationship Name: win-bg1k522gpt.test1.com-win-8tfmov9mms

Maximum Client Lead Time: 1 hrs 0 mins

Mode: Load balance

State Switchover Interval: Disabled

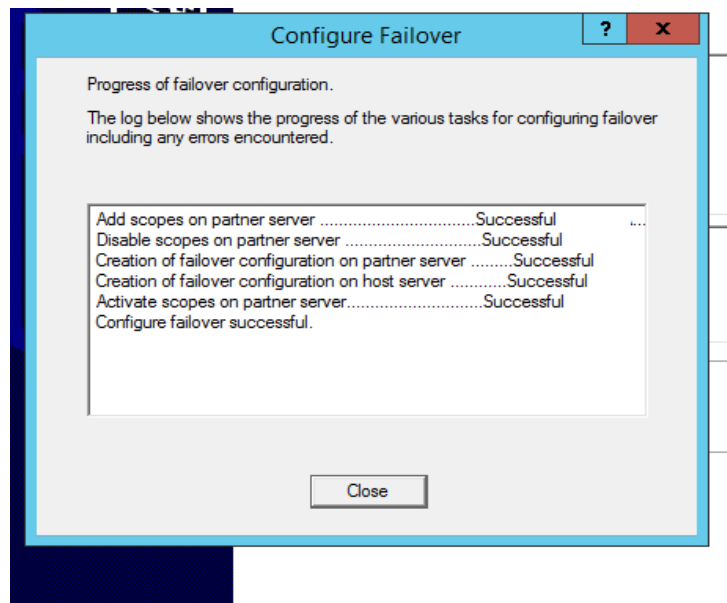
Load Balance Percentage

Local Server: 50 %

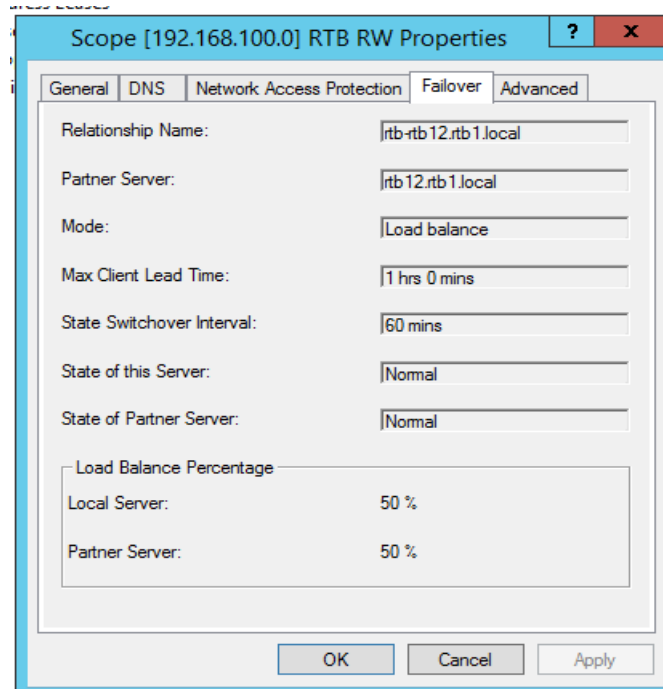
Partner Server: 50 %

< Back Finish Cancel

6. The DHCP failover relationship will now be established between the primary and partner servers, providing redundancy and high availability for DHCP service.



7. You can monitor and manage the DHCP failover relationship by right-clicking on the DHCP scope and selecting "Manage Failover" from the context menu. This allows you to view the status, modify settings, and monitor the failover relationship.





Points to Remember

- **Configure DHCP scope parameters**

You can follow these steps:

1. Open the DHCP Manager on your Windows Server.
2. In the DHCP Manager, expand the server name and navigate to "IPv4" or "IPv6".
3. Right-click on "IPv4" or "IPv6" and select "New Scope" from the context menu.
4. Follow the New Scope Wizard to configure the DHCP scope parameters.
5. Complete the wizard to create the DHCP scope with the specified parameters.
6. Once the scope is created, you can modify its properties by right-clicking on it and selecting "Properties".
7. To start the DHCP service, right-click on the DHCP server name and select "Authorize" or "Start" from the context menu.

- **Configuring DHCP reservations**

You can follow these steps:

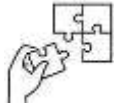
1. Open the DHCP Manager on your Windows Server.
2. In the DHCP Manager, expand the server's name and navigate to "IPv4" or "IPv6" (depending on the IP version you are configuring).
3. Expand the DHCP scope where you want to create the reservation.
4. Right-click on "Reservations" and select "New Reservation" from the context menu.
5. In the New Reservation window, provide the following information:
 - a) Reservation Name
 - b) IP Address.
 - c) MAC Address
 - d) Description (optional)
6. Click "Add" or "OK" to create the reservation.
7. The reservation will now be added to the DHCP scope, ensuring that the specified device always receives the assigned IP address.

- **Configuring DHCP failover**

You can follow these steps:

1. Open the DHCP Manager on your Windows Server.
2. In the DHCP Manager, expand the server name and navigate to "IPv4" or "IPv6"
3. Right-click on "IPv4" or "IPv6" and select "Configure Failover" from the context menu.
4. In the Configure Failover Wizard, choose the appropriate options for your failover
5. Complete the wizard to configure the DHCP failover relationship.
6. The DHCP failover relationship will now be established between the primary and partner servers, providing redundancy and high availability for DHCP service.

7. You can monitor and manage the DHCP failover relationship by right clicking on the DHCP scope and selecting "**Manage Failover**" from the context menu. This allows you to view the status, modify settings, and monitor the failover relationship.



Application of learning 1.6.

Bxz Solutions Inc. is a company specializing in providing IT solutions for small and medium businesses. Located in Rwanda, Eastern area, Tech Solutions Inc. aims to enhance its network infrastructure by setting up essential server roles, including DNS and DHCP, to improve network management and efficiency.

As an System Administrator hired by Bxz Solutions Inc., you are tasked with implementing best practices for configuring DHCP Scopes, Reservations, and Failover in Windows Server.



Indicative content 1.7: Monitoring of Server Services



Duration: 3hrs



Practical Activity 1.7.1: Use nslookup command for resolving DNS



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Trainee in Level 4 software development, you are requested to go to use nslookup command is a useful tool for troubleshooting and monitoring DNS resolution in server administration.

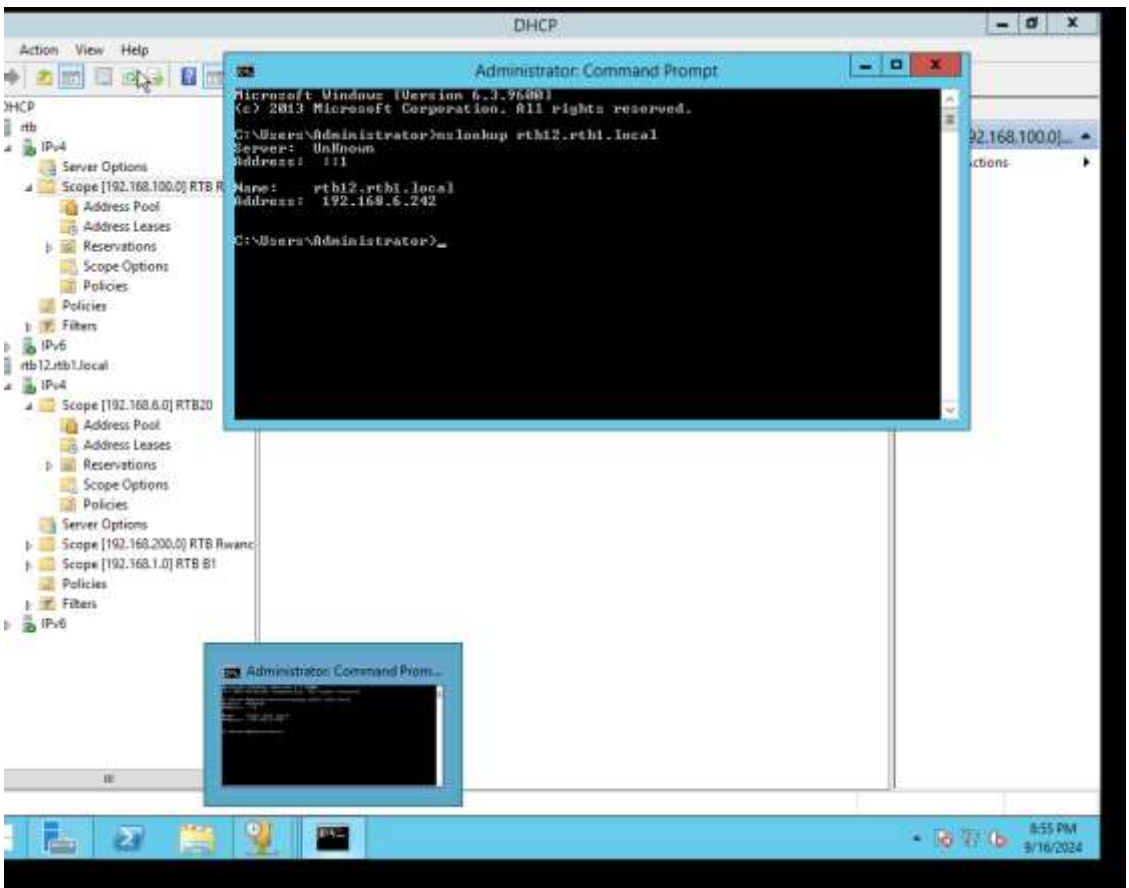
2. Remember to read the key readings 1.7.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class



Key readings 1.7.1: Use nslookup command for resolving DNS

The nslookup command is a useful tool for troubleshooting and monitoring DNS resolution. It allows you to query DNS servers and retrieve information about domain names and IP addresses. Here's how you can use it:

1. Open a command prompt on your client machine.
2. Type "nslookup" followed by the domain name or IP address you want to resolve.



The screenshot shows the Windows DHCP console on the left, displaying a tree view of DHCP scopes and servers. Overlaid on this is an 'Administrator: Command Prompt' window. The command prompt shows the following text:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup rth12.rth1.local
Server: Unknown
Address: 111

Name: rth12.rth1.local
Address: 192.168.6.242

C:\Users\Administrator>
```

Below the Command Prompt, there is a smaller, partially visible Command Prompt window. The taskbar at the bottom shows the system clock as 8:55 PM on 9/16/2024.

3. Press Enter to execute the command.
4. The command will display the corresponding IP address or domain name, along with additional information such as the DNS server used for the lookup. Example: nslookup www.example.com



Practical Activity 1.7.2: Checking IP DHCP configuration on client



Task:

1. You are requested to go to the computer lab and do the task below individually.

As a Level 4 software development trainee, you are requested to check the IP DHCP configuration on a client machine using Windows.

2. Remember to read the key readings 1.7.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class



Key readings 1.7.2: Checking IP DHCP configuration on client

To check the IP DHCP configuration on a client machine using Windows, you can use the following commands:

1. Open a command prompt.
2. Type "ipconfig" and press Enter.
3. The command will display the IP address, subnet mask, default gateway, and other network configuration details for all active network interfaces. Example: ipconfig

The screenshot shows a Windows 7 desktop. On the left, a Command Prompt window titled 'Administrator: Command Prompt' displays the output of the 'ipconfig' command. The output shows details for three network adapters: Tunnel adapter Local Area Connection* 11, Ethernet adapter Ethernet0, and Tunnel adapter isatap.{...}. The Ethernet adapter is the active one, showing an IP address of 192.168.6.242, a subnet mask of 255.255.255.0, and a default gateway of 192.168.6.2. On the right, the Windows Update window is open, showing the 'TASKS' tab with various update-related settings and a list of updates. The taskbar at the bottom shows the date and time as 8/16/2024 8:35:37 PM.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Tunnel adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::278b:1d22:9cac:4150:bc12
IPv4 Address. . . . . : 192.168.6.242
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.6.2

Tunnel adapter isatap.localdomain:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Ethernet adapter isatap.{15183FDD-3AEB-48B6-876D-P5E851A178D6}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\Administrator>
```

Notes: By using these commands, you can gather information about DNS resolution and DHCP configuration on client machines, helping you monitor and troubleshoot server services effectively.



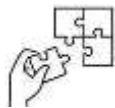
Points to Remember

- **Use nslookup command for resolving DNS**

1. Open a command prompt on your client machine.
2. Type "nslookup" followed by the domain name or IP address you want to resolve.
3. Press Enter to execute the command.
4. The command will display the corresponding IP address or domain name, along with additional information such as the DNS server used for the lookup.
Example: nslookup rtb.local

- **Checking IP DHCP configuration on client**

1. Open a command prompt.
8. Type "ipconfig" and press Enter.
9. The command will display the IP address, subnet mask, default gateway, and other network configuration details for all active network interfaces. Example: ipconfig



Application of learning 1.7.

FFF Ltd company, located in Gicumbi District, Northern Province, is hiring a System Administration Technician to use nslookup command is a useful tool for troubleshooting and monitoring DNS resolution and check the IP DHCP configuration on a client machine in windows server administration. The technician will also be responsible for documenting the entire process. All tasks must be completed within a three-hour timeframe.



Learning outcome 1 end assessment

Theoretical assessment

Question 1. Circle the letter corresponding to the correct answer:

i. What is a primary function of a server in a network?

- A) To request data from clients
- B) To provide resources, data, or services to clients
- C) To manage network operating systems
- D) To run on top of a hypervisor

ii. What type of hypervisor runs directly on the physical hardware without needing a host operating system?

- A) Type 2 Hypervisor
- B) Hosted Hypervisor
- C) Bare-Metal Hypervisor
- D) Managed Hypervisor

iii. Which of the following is an advantage of server virtualization?

- A) Increased hardware costs
- B) Decreased resource utilization
- C) Improved disaster recovery
- D) Reduced scalability

iv. What is the key characteristic of RAID 0?

- A) It provides redundancy by duplicating data across multiple disks.
- B) It splits data into blocks and distributes them across multiple disks without redundancy.
- C) It combines mirroring and striping for performance and redundancy.
- D) It uses double parity to protect against up to two disk failures.

v. Which RAID level offers protection against up to two disk failures?

- A) RAID 0
- B) RAID 1
- C) RAID 5
- D) RAID 6

vi. What does a Type 2 Hypervisor require to operate?

- A) Direct access to physical hardware
- B) A host operating system
- C) Additional storage drives
- D) Higher network bandwidth

vii. Which RAID level combines striping and mirroring for high performance and fault tolerance?

- A) RAID 0
- B) RAID 1
- C) RAID 5
- D) RAID 10

viii. What is a disadvantage of RAID 5?

- A) It requires double storage capacity.
- B) It offers no redundancy.
- C) It has slower write performance due to parity calculations.
- D) It does not support multiple disk failures.

ix. Which software component is essential for managing a network and enabling communication between servers and clients?

- A) Web Server Software
- B) Virtualization Software
- C) Network Operating System (NOS)
- D) Backup Software

x. What is the primary function of a domain controller (DC) in a Windows Server environment?

- A) To manage virtual machines
- B) To authenticate and authorize users and computers
- C) To configure DHCP scopes
- D) To troubleshoot DNS issues

xi. Which RSAT tool is used to manage users, groups, and organizational units in Active Directory?

- A) DNS Manager
- B) Active Directory Users and Computers (ADUC)

- C) Group Policy Management Console (GPMC)
- D) Remote Desktop Services Manager

xii. Which RSAT tool would you use to manage DNS zones and records?

- A) DHCP Manager
- B) Hyper-V Manager
- C) Active Directory Sites and Services (ADSS)
- D) DNS Manager

xiii. What is the purpose of the Group Policy Management Console (GPMC)?

- A) To manage virtual networks
- B) To configure DHCP scopes
- C) To manage Group Policy Objects (GPOs)
- D) To oversee server performance

xiv. Which tool is used to configure and manage DHCP scopes and IP address leases?

- A) Server Manager
- B) DHCP Manager
- C) Active Directory Sites and Services (ADSS)
- D) Hyper-V Manager

xv. What role does Active Directory Domain Services (AD DS) serve in a server environment?

- A) It manages the replication topology and site configuration.
- B) It provides virtual machine management and storage.
- C) It handles user authentication and authorization.
- D) It manages server roles, features, and performance.

xvi. What is the purpose of server roles in a Windows Server environment?

- A) To provide additional features to enhance server capabilities
- B) To manage user sessions and server performance
- C) To enable the server to perform specific functions for users or other computers
- D) To troubleshoot and configure DNS issues

xvii. Which RSAT tool would you use to manage virtual machines and virtual networks?

- A) Hyper-V Manager
- B) Server Manager

- C) Remote Desktop Services Manager
- D) Group Policy Management Console (GPMC)

xviii. What do server features in Windows Server do?

- A) They allow remote management of the server operating system.
- B) They provide optional components that enhance server capabilities.
- C) They manage the replication and site configuration.
- D) They handle user authentication and authorization.

xix. Which RSAT tool provides an overview and management of server roles, features, status, and performance?

- A) Active Directory Sites and Services (ADSS)
- B) DNS Manager
- C) Server Manager
- D) Remote Desktop Services Manager

Question 2. Fill in the Blanks space with the appropriate words. Select from the given choices

- i. A _____ query involves the DNS server handling the entire resolution process and returning the final result to the client. (Root Hints, Caching, Recursive)
- ii. In DNS operations, _____ helps improve performance by storing recently resolved query results. (Root Hints, Caching, Recursive)
- iii. _____ are lists of IP addresses of root DNS servers used by DNS servers to start the resolution process.(Root Hints, Caching, Recursive)
- iv. An _____ DNS server provides definitive answers for queries about domains it is responsible for.
- v. A _____ file contains DNS resource records such as A, CNAME, and MX records for a zone.(message, Zone, Authoritative)
- vi. The DHCP client starts the process by sending a _____ message to locate available DHCP servers.(Discover, message, Zone)
- vii. The DHCP server confirms the assignment of an IP address and provides additional configuration settings with a _____ message.(Acknowledgement, Discover, Zone)
- viii. The DHCP process begins with the client sending a _____ message.

ix. DHCP _____ involves configuring two DHCP servers to share lease information, allowing one server to take over if the other fails.(Failover, Discover, Acknowledgement)

x. To prevent unauthorized DHCP servers from providing IP addresses, network administrators use _____ on switches. (Forwarding, Relay, operates, DHCP Snooping)

xi. A DHCP _____ agent forwards DHCP messages between clients and servers when they are on different subnets. (Forwarding, Relay, operates, DHCP Snooping)

xii. The DHCP relay agent operates by receiving DHCP requests from clients and _____ them to the appropriate DHCP server.(Forwarding, Relay, operates)

Practical assessment

Bxz Solutions Inc. is a company specializing in providing IT solutions for small and medium businesses. Located in Rwanda, Eastern area, Bxz Solutions Inc. aims to enhance its network infrastructure by setting up essential server roles, including Active Directory and various network services, to improve network management and efficiency.

As an System Administrator hired by Bxz Solutions Inc., you are tasked with the following:

- i. Prepare the Windows Server OS Environment
- ii. Install and Configure Active Directory
- iii. Install and Configure Services and Features.

END



References

Dauti, b. B. (2024). *Windows Server 2022 Administration Fundamentals*. Third Edition.

Krause, J. (2024). *Mastering Windows Server 2022*.

Lee, T. (2024). *Windows Server Automation with PowerShell Cookbook*.

Abacus. (n.d.). **Three types of server virtualization explained**. Retrieved from https://goabacus.com/three-types-of-server-virtualization-explained/#:~:text=So%20what%20are%20the%20three,and%20hypervisor%20each%20type%20employs

Boitnott, J. (2019). **The Intrapreneur's Journey: Empowering Employees to Drive Growth**. Retrieved from https://books.google.rw/books?id=sagNDwAAQBAJ&pg=PA23&source=gbs_selected_pages&cad=1#v=onepage&q&f=false

GeeksforGeeks. (n.d.). **Difference between virtualization and hypervisor**. Retrieved from https://www.geeksforgeeks.org/difference-between-virtualization-and-hypervisor/

HostArmada. (n.d.). **9 questions to ask your brand new web hosting provider before signing up**. Retrieved from https://www.hostarmada.com/blog/9-questions-to-ask-your-brand-new-web-hosting-provider-before-signing-up/

Openprovider. (n.d.). **SSL installation on MS IIS (Windows powered systems)**. Retrieved from https://support.openprovider.eu/hc/en-us/articles/360014563220-SSL-Installation-on-MS-IIS-Windows-powered-systems

vsphere-land. (n.d.). **What is SAHF and LAHF and why do I need it to install vSphere 5.1?** Retrieved from https://vsphere-land.com/news/what-is-sahf-and-lahf-and-why-do-i-need-it-to-install-vsphere-51.html

Learning Outcome 2: Manage Users



Indicative contents

- 2.1 Creation of Users Accounts
- 2.2 Management of Users Accounts
- 2.3 Management of User Groups
- 2.4 Management of Organization Units (OU)
- 2.5 Assignment of Permission to Users
- 2.6 Management of Client Machines

Key Competencies for Learning Outcome 2: Manage Users

Knowledge	Skills	Attitudes
■ Description user account policies ■ Differentiate user account levels ■ Description of Group Policy Object (GPO)	■ Creating account ■ Managing user accounts ■ Managing user groups ■ Applying permission to users ■ Joining client to the domain ■ Managing GPO settings ■ Applying delegation of control	■ Being problem solver ■ Having ethical conduct ■ Being patience ■ Being calm ■ Working in a Team ■ Engaging in Continuous Learning.



Duration: 30hrs

Learning outcome 2 objectives:



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

1. Describe clearly user accounts in windows server
2. Differentiate properly user account levels used in server
3. Create properly user accounts in windows server
4. Manage properly user accounts in windows server
5. Manage properly the user groups in windows server
6. Manage properly organization units in windows server
7. Join properly client to the domain in windows server
8. Describe clearly Group Policy Object (GPO) used in client machine
9. Manage properly GPO settings in server machine
10. Apply clearly delegation of control in server machine
11. Assign clearly permissions on user accounts control
12. Manage appropriately client machine based on ICT policies



Resources

Equipment	Tools	Materials
• Computer • Server	• VMWare workstation, • VMWare ESXI • Oracle Virtual Box	• windows • Internet



Indicative content 2.1: Creation of User Accounts



Duration: 5 hrs



Theoretical Activity 2.1.1: Description of user accounts



Tasks:

- 1: You are requested to answer the following questions:
 - a) Define user account and user account policies
 - b) Differentiate standard and Administrator account
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications to the trainer
6. Remember to ready more on key reading 2.1.1 in trainee's manual



Key readings 2.1.1.: Description of user accounts

A user account refers to an individual's account within the Active Directory or local user database. A user account is created for each user who needs access to the system, resources, and services.

User: a user is an individual who has been granted access to the system. Users can log in to the system and perform various tasks, such as running applications, accessing files, and managing system settings. Each user has a unique username and password that is used to authenticate their identity and control their access to the system.

User account policies in Windows Server refer to a set of rules and configurations that govern the security and management of user accounts within a Windows Server environment. These policies help ensure the confidentiality, integrity, and availability of resources and data by defining various restrictions and requirements for user accounts.

Account Policies are classified into two categories:

- 1. Password policies:** Password Policies are a set of policies that determine how a password should be set for an AD user account. it's better to have stronger password policies to ensure that it is not easy for an attacker to guess the passwords.
- 2. Account lockout policies:** These policies determine the number of failed login attempts allowed before an account gets locked out, as well as the duration of the

lockout period. They help protect against brute-force attacks and unauthorized access attempts.

Identification of user account level of access

In Windows Server, there are two common levels of user account access: Standard and Administrator.

1. Standard User Account: A standard user account is a non-administrative account with limited privileges. Users with standard accounts can perform regular tasks such as running applications, accessing files and folders, and customizing their own settings. However, they do not have the authority to make system-wide changes, install or uninstall software, or modify critical system settings. This level of access is suitable for everyday users who do not require administrative privileges.

2. Administrator Account: Administrator accounts are special accounts that are used for making changes to system settings or managing other people's accounts. They have full access to every setting on the computer. Every computer will have at least one Administrator account, and if you're the owner you should already have a password to this account.



Practical Activity 2.1.2: Creation of user account in windows server



Task:

1. You are requested to go to the computer lab and do the task below individually.
As a learner in Level 4 software development, you are tasked with managing student accounts within an Active Directory environment. Your first task is to create a new user account for a new student. After that, you need to copy an existing student account to create a second account.
2. Read the key readings 2.1.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

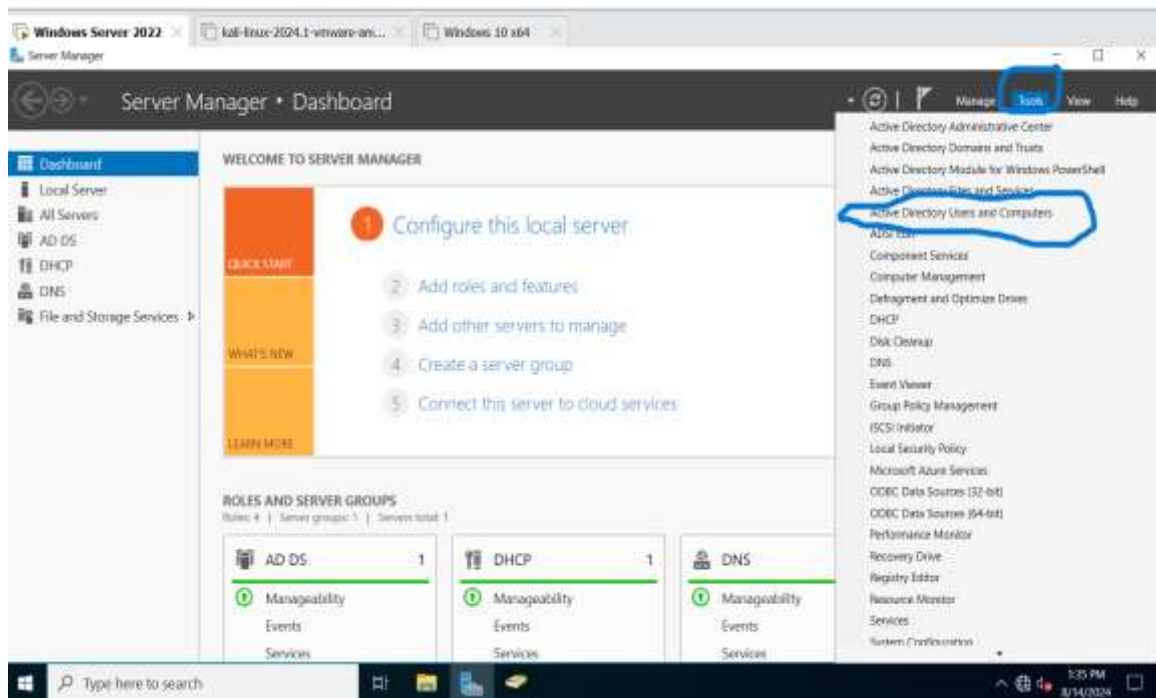


Key readings 2.1.2: Creation of user account in windows server

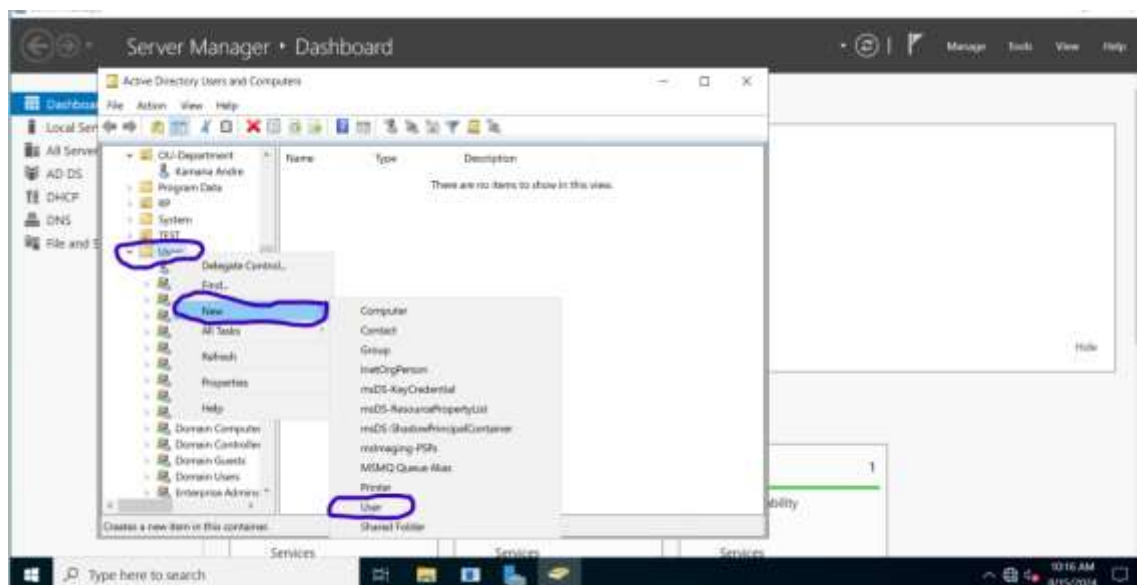
Create New User Account

This Article will show you how to create a user on the Windows Server step by step:

Step 1. Run **Server Manager** and click on **Tools** then click on **Active Directory Users and Computers** and **Computers**:

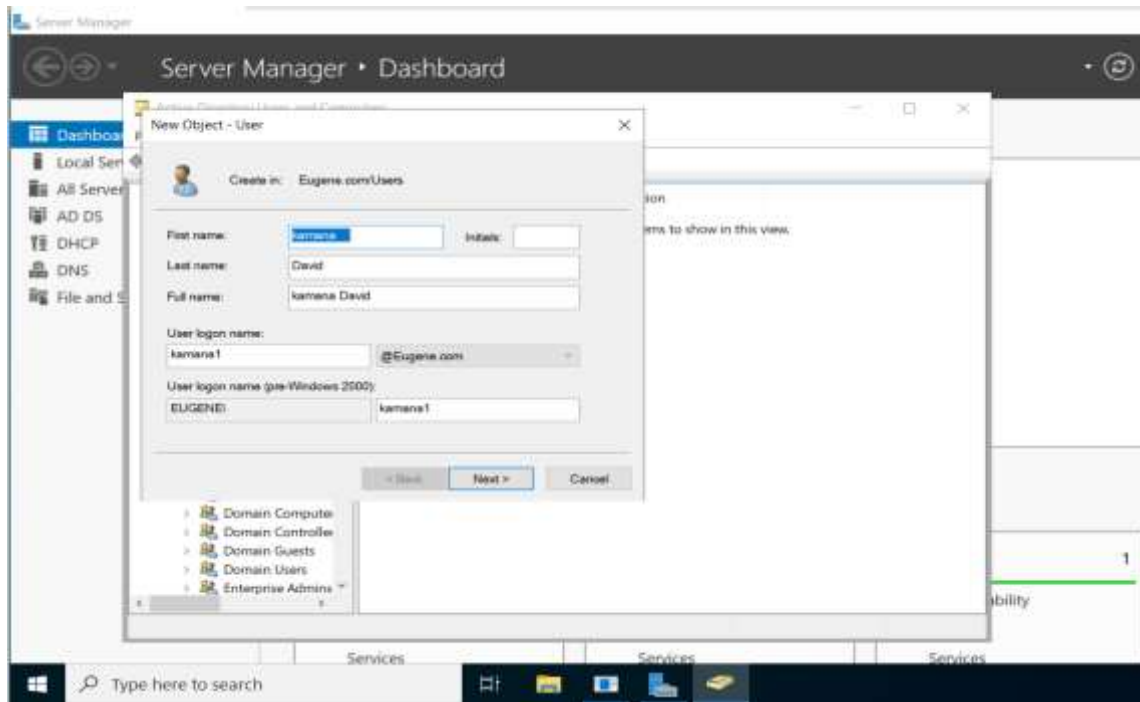


Step 2. Under **Local Users and Groups** Right click on **Users** then select **New**, then click on **User**.



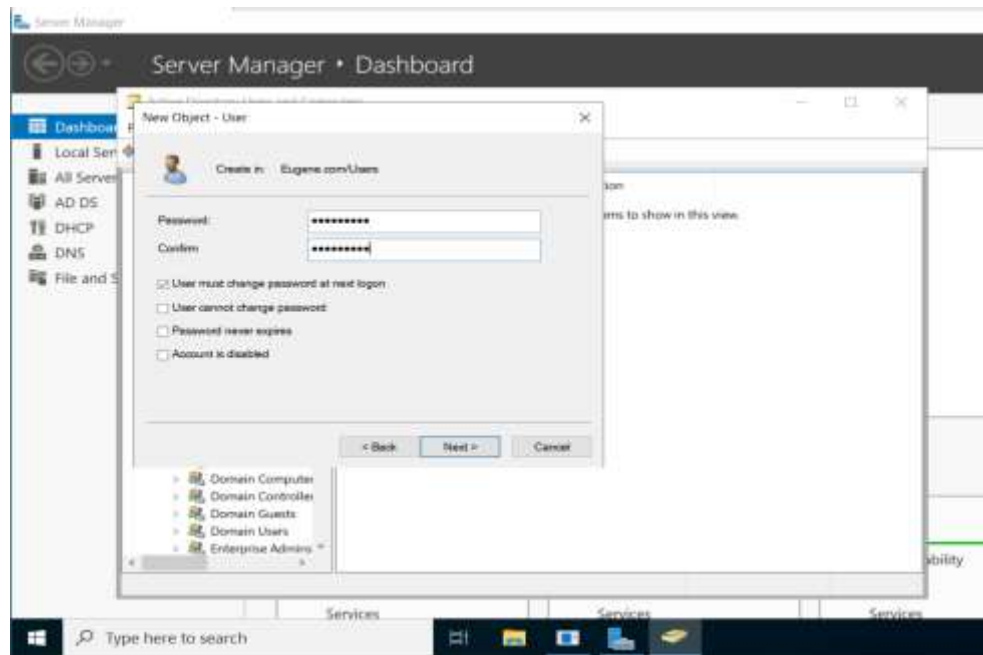
Step 3: Fill in User Information.

1. First Name: Enter the user's first name.
2. Last Name: Enter the user's last name.
3. User logon name: Enter the username. You can also choose the logon name format (e.g., username@domain.com).



Step 4: Set the Password.

1. Enter the password for the new user in the Password and Confirm password fields.



Step 5: Complete the Wizard.

1. Review the information you have entered.
2. Click **Finish** to create the user account.

Copy Account

Copying an account allows you to create a new user account with similar properties to an existing one.

Steps for copying an account in windows server administration :

Step 1. Right-click on the user account you want to copy and select **“Copy”**.

Step 2. Fill in the new user account's details such as **“First Name”**, **“Last Name”**, and **“User logon name”**.

Step 3. Set the Password and Complete: Set the new user's password, and choose the relevant password options:

1. **User must change password at next logon:** Recommended for security.
2. **User cannot change password:** Useful for service accounts.
3. **Password never expires:** Use cautiously, mainly for service accounts.
4. **Account is disabled:** Enable the account later if needed.

Step 5. Click on **“Next”** and **“Finish”** to create the copied account.



Points to Remember

- Description of user accounts:
 - ✓ **A user account** refers to an individual's account within the Active Directory or local user database.
 - ✓ **User account policies** in Windows Server refer to a set of rules and configurations that govern the security and management
 - ✓ User account levels are: Standard user account and Administrator Account
- To Create New User Account follow the steps bellow:
 1. Run Server Manager and Open Tools.
 2. Under Local Users and Groups Right click on Users
 3. Fill in User Information
 4. Set the Password
 5. Complete the Wizard



Application of learning 2.1.

Company Named **Rwanda Revenue Authority** is hiring an IT System Administrator to manage their Active Directory environment. As part of the assessment, the candidate is required to complete two tasks within a 1-hour timeframe: Firstly, create a new user account for **Eric Murindwa** with the username eric.murindwa and password Kigali@123. Secondly, copy the Eric Murindwa account to create a new user named **Pepe Uwitonze** with the username pepe.uwitonze and the same password. The tasks will perform in 1hour.



Indicative content 2.2: Management of User Accounts



Duration: 5hrs



Practical Activity 2.2.1: Managing user account



Task:

1. You are requested to go to the computer lab and do the task below individually:
As the system administrator for a medium-sized company, you need to manage the user account for **Kamana** in a Windows Server environment. Your tasks include resetting Kamana's password, reactivating the account, deactivating it temporarily, and customizing account parameters.
2. Read the key reading 2.2.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating the steps to perform the task
5. Perform the task on your computer
6. Present the work to the whole class



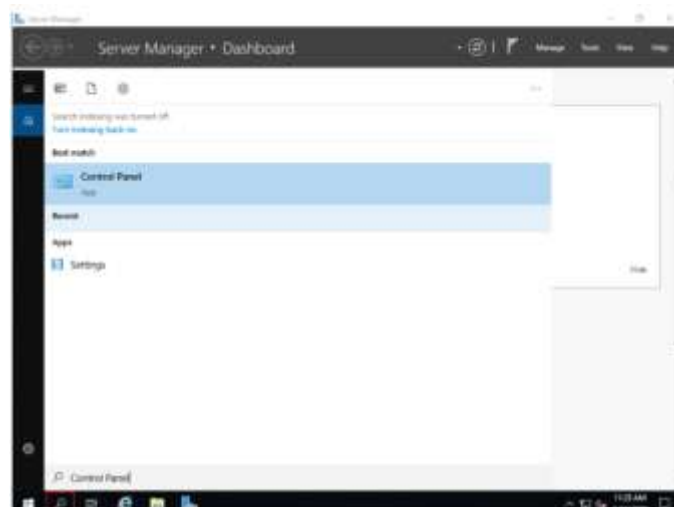
Key readings 2.2.1.: Managing user account

Changing user account password

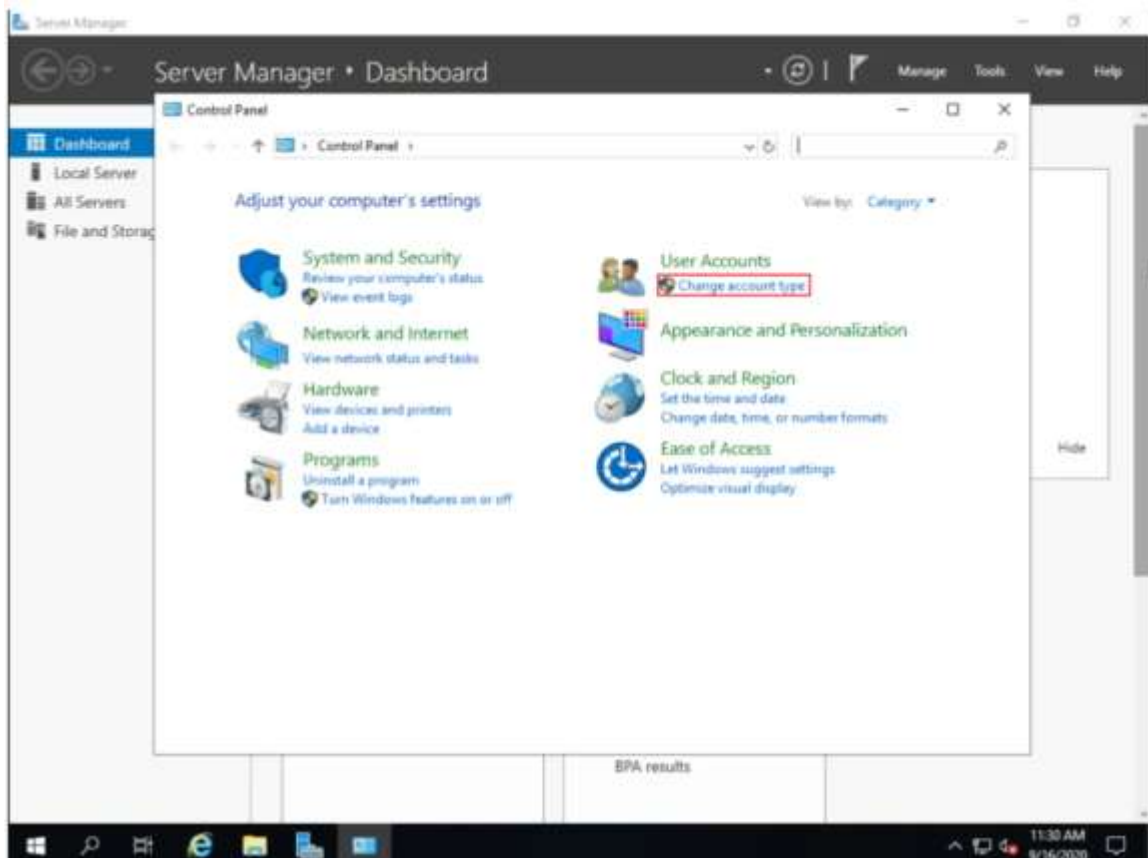
For changing user account password follow these steps bellow:

Step 1: Log in: Connect to your server with the login credentials which direct you to client area.

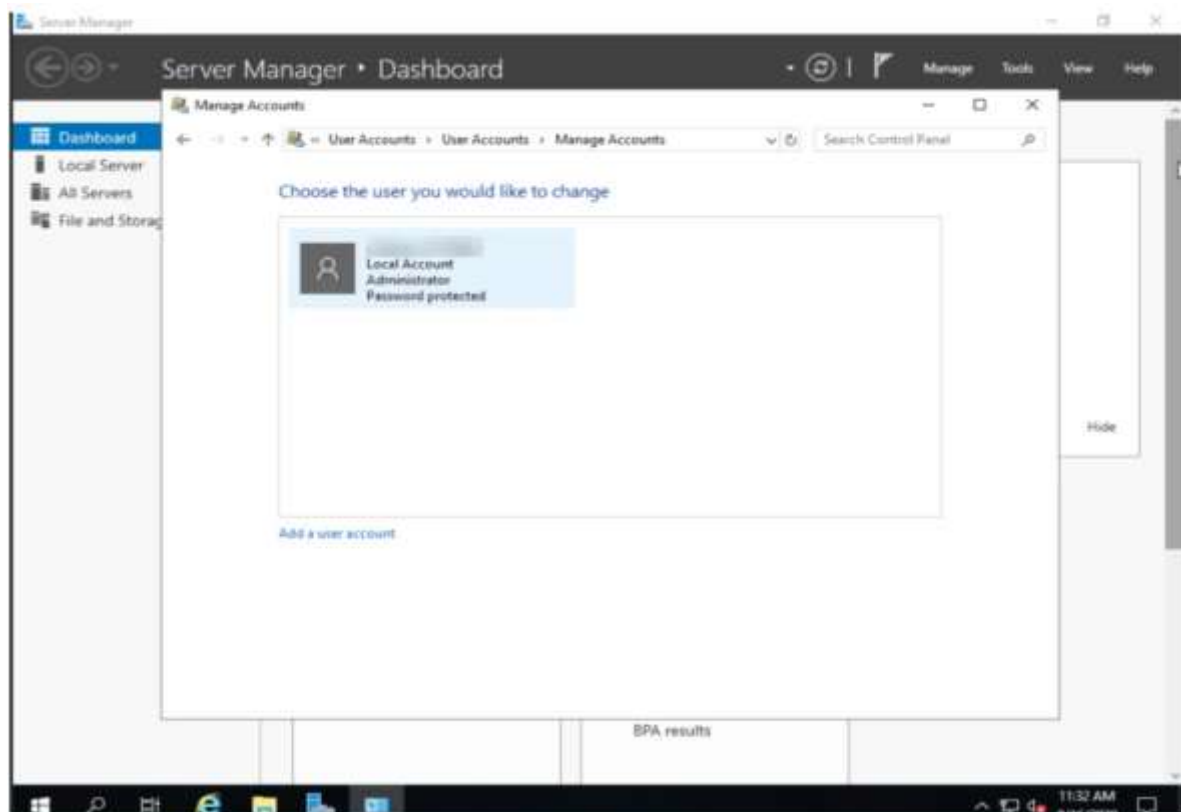
Step 2: Changing a password: Click on the **windows icon** in the lower-left corner, and search **Control Panel**.



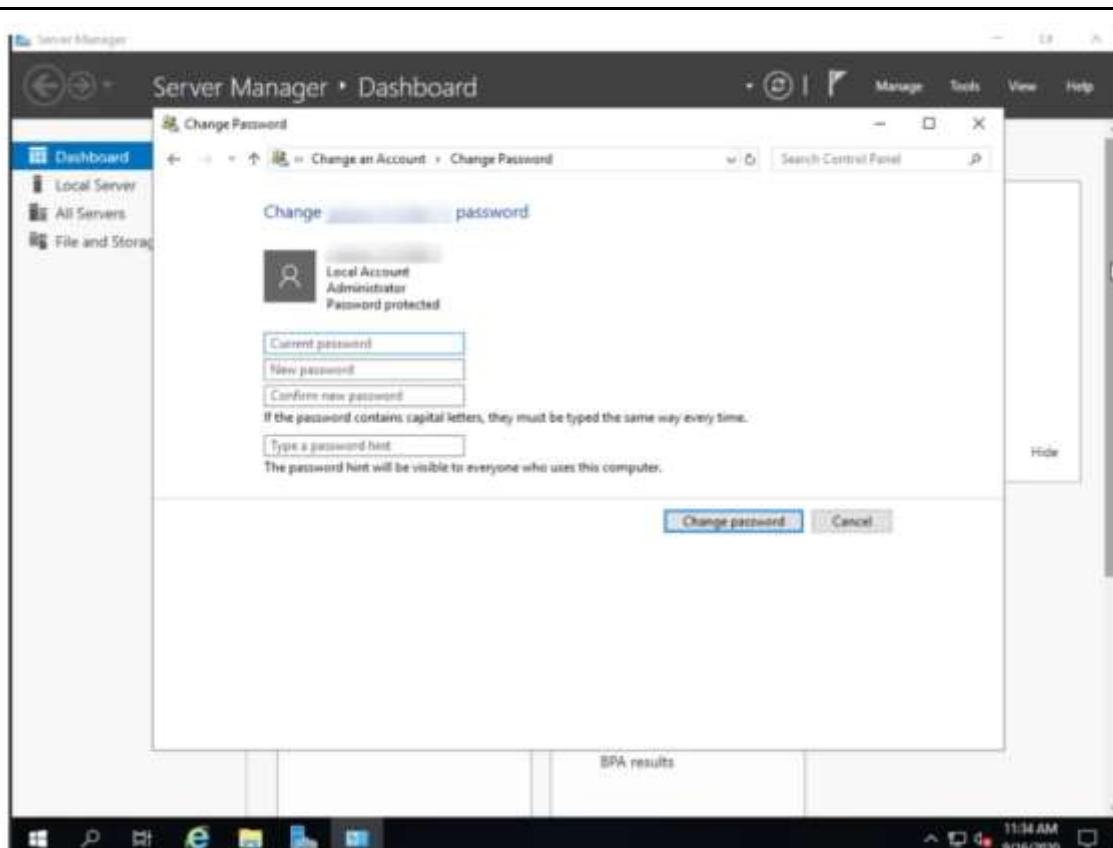
Step 3: Under User Account headings, click on Change account type.



Step 4: Click on the user you want to change the password.



Step 5: Click on Change the password and fill password fields .



Step 6: Click on Change password

- **Remove account**

Login to the Windows Server machine using an account with administrative privileges.

Follow these steps to delete a user account on a Windows Server

- 1. Open ADUC from Server Manager:** Open **Server Manager**> Go to **Tools** and select **Active Directory Users and Computers**.
- 2. Navigate the Default Container:** Expand the domain node and select the **Users** container or other relevant containers where users might be located.
- 3. Find and Delete the User Account:** Right-click the user account and click on **Delete**, and Confirm the deletion.

- **Activate account**

When you activate a user account, the assigned user can log on to the network and access network resources to which the account has permission, such as shared folders and the Remote Web Access site.

To activate a user account

1. Open the Windows Server Essentials Dashboard.

2. On the navigation bar, click **Users**.
3. In the list view, select the user account that you want to activate.
4. In the <User Account> Tasks pane, click **Activate the user account**.
5. In the confirmation window, click **Yes** to confirm your action.

- **Deactivate a user account**

When you deactivate a user account, account access to the server is temporarily suspended. Because of this, the assigned user cannot use the account to access network resources such as shared folders or the Remote Web Access site until you activate the account.

To deactivate a user account

1. Open the Windows Server Essentials Dashboard.
2. On the navigation bar, click **Users**.
3. In the list view, select the user account that you want to deactivate.
4. In the <User Account> Tasks pane, click **Deactivate the user account**.
5. In the confirmation window, click **Yes** to confirm your action.



Points to Remember

- **To Change user account password, follow the following steps:**
 - ✓ Log in
 - ✓ Changing a password
 - ✓ Under user Account headings, then click on **Change account type**
 - ✓ Click on the user you want to change the password.
 - ✓ Click on Change the password and fill password fields
 - ✓ Click on Change password.
- **To remove a user account, follow the steps**
 - ✓ Open ADUC from Server Manager
 - ✓ Navigate the Default Container
 - ✓ Find and Delete the User Account
- **To activate a user account, follow the steps:**
 - ✓ Open the Windows Server Essentials Dashboard.
 - ✓ On the navigation bar, click **Users**.
- **To deactivate a user account, follow the steps**

- ✓ Open the Windows Server Essentials Dashboard.
- ✓ On the navigation bar, click **Users**.



Application of learning 2.2.

As the system administrator, you are tasked with managing a single user account for **Kamana** in a Windows Server environment. The tasks include resetting Kamana's password to Gisenyi@100, reactivating the account, temporarily deactivating it, and customizing account parameters such as setting logon hours from 8:00 AM to 6:00 PM and updating the home directory to [\\Server\Home\Kamana](#).



Indicative content 2.3: Management of User Groups



Duration: 5 hrs.



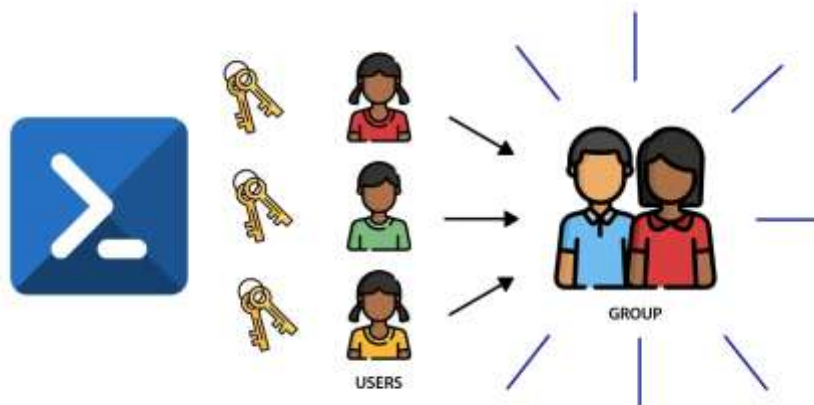
Theoretical Activity 2.3.1: Description of user groups



Tasks:

1. You are requested to answer the following questions:

- A. Define term groups in windows server
- B. Explain types of user groups in windows server



2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 2.3.1 in the trainee's manual.



Key readings 2.3.1.: Description of user groups

- **Creation of group**

A group is a collection of user accounts, and possibly other groups, that can be managed as a single unit.

Groups can be assigned permissions just like users, and all members of the group automatically receive those permissions.

Groups can be useful for the separation of users, allowing you the ability to manage access to certain files/folders/applications on a group basis both locally and in a domain environment.

- **Types of groups**

1. **Security Groups:** Used to assign permissions to resources. Members of a security group receive the permissions assigned to the group.
2. **Distribution Groups:** Used primarily for email distribution lists in environments like Microsoft Exchange. These groups are not used for assigning security permissions.



Practical Activity 2.3.2: Managing user groups



Task:

1. You are requested to go to the computer lab and do the task below individually:

As trainees in L4SOD, you are tasked with managing user groups within a Windows Server virtual machine. Your objective is to create a new group named L4SOD, add a previously created user to this group, and subsequently remove the user. Document each step of this process by capturing screenshots after creating the group, adding the user, and removing the user.

2. Read more on key reading 2.3.2 in Trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

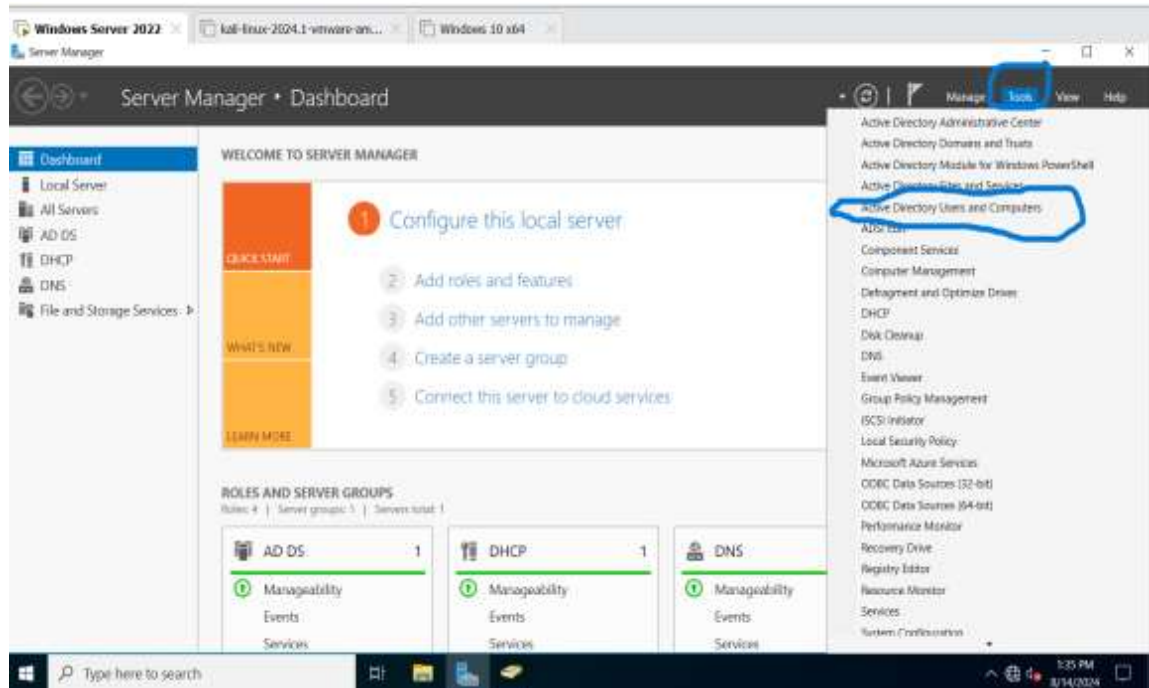


Key readings 2.3.2: Managing users in group

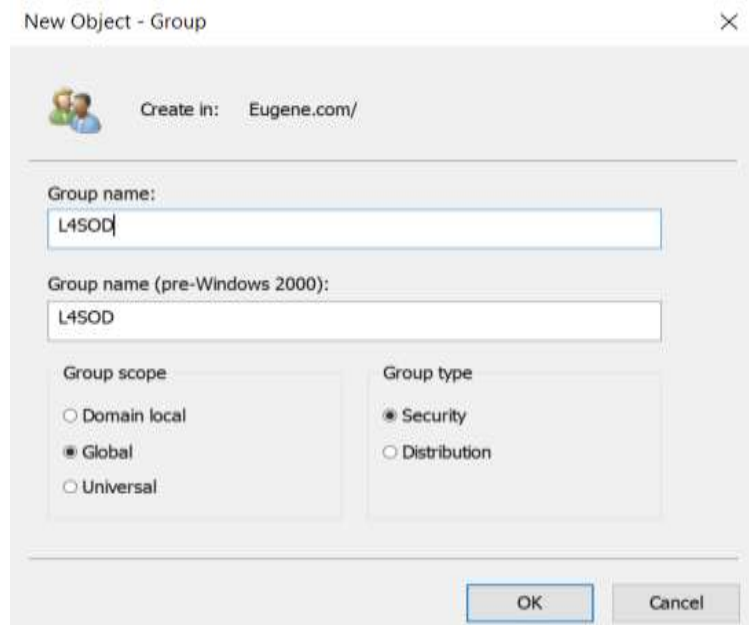
Creation of group

Steps for creating group in windows server administration:

1. In Server Manager, click on "**Tools**" and select "**Active Directory Users and Computers.**"



2. Right click on domain name, then Select **"New" > "Group"**.
3. In the **New Object - Group** window, Add **Group name**(e.g. L4SOD) and select **Group scope**: Global, **Group type**: Security



4. Click **OK** to create the group.

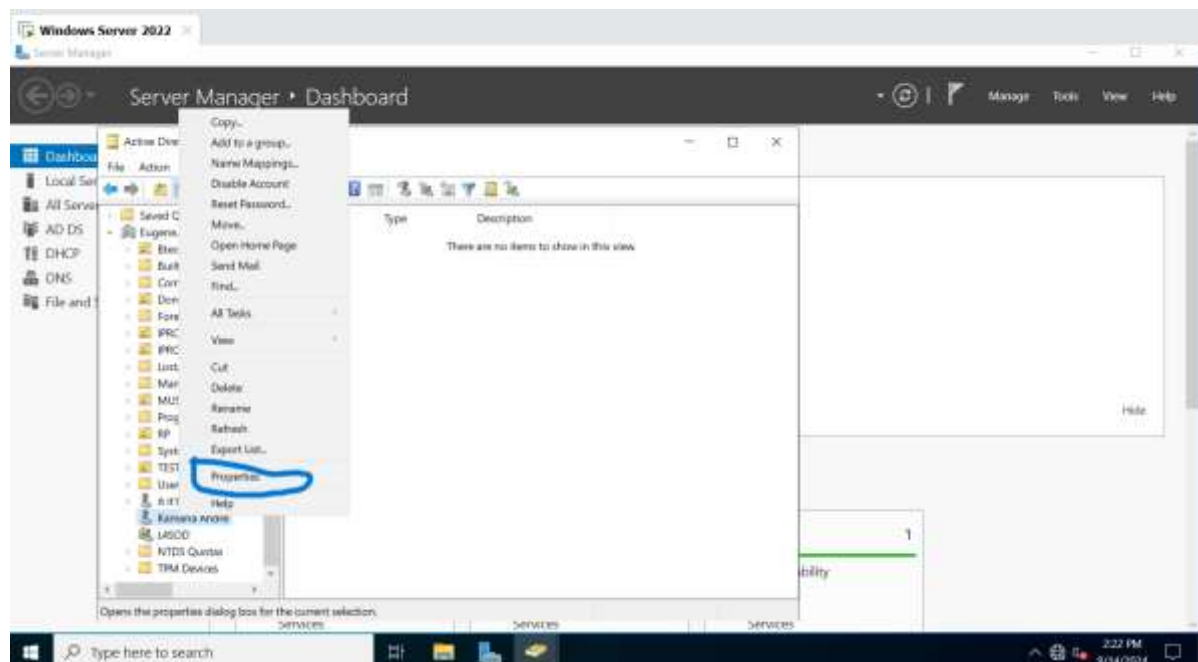
➤ Adding users in groups

Add User (**Kamana Andre**) to the Group(**L4SOD**) through the following steps:

1. In Server Manager, click on **"Tools"** and select **"Active Directory Users and**

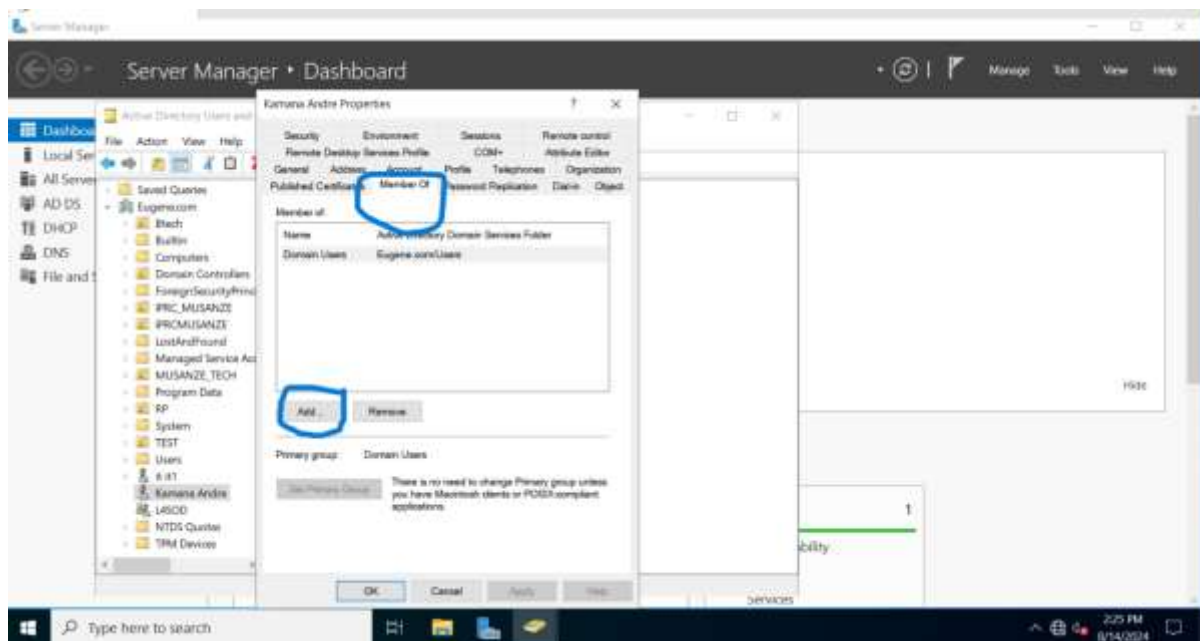
Computers."

2. Right-click on User (**Kamana Andre**) and select "**Properties.**"

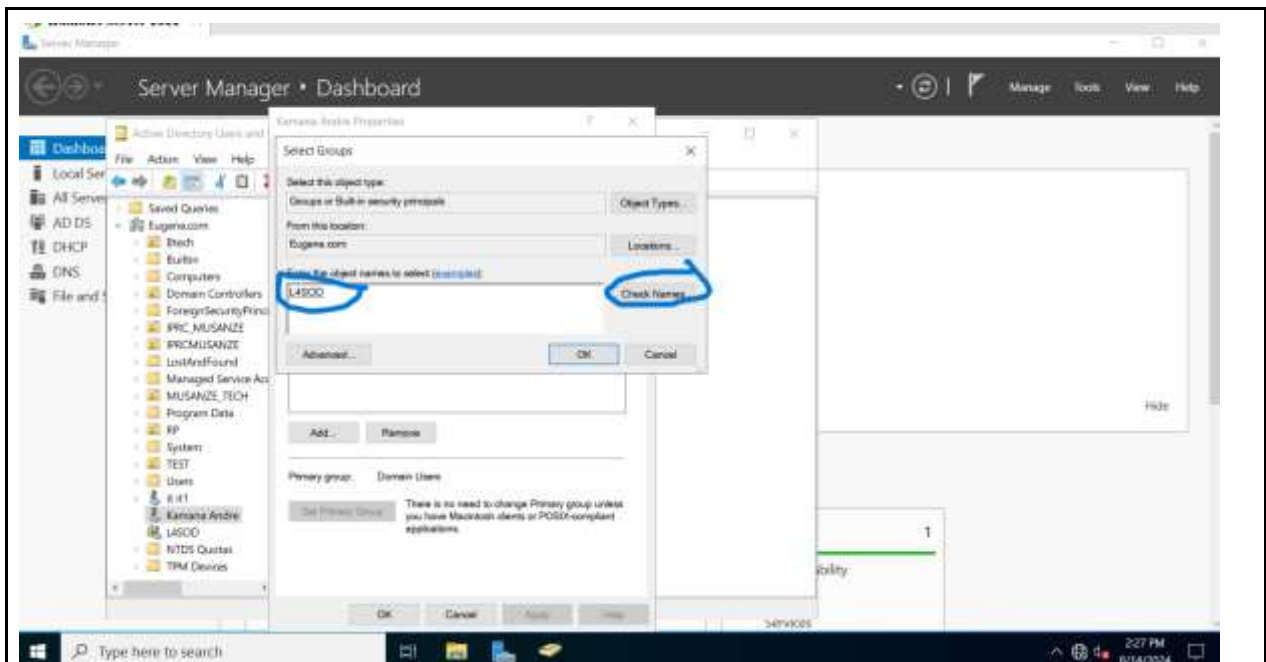


3. In the User (**Kamana Andre**) Properties window, go to the "**Member Of**" tab.

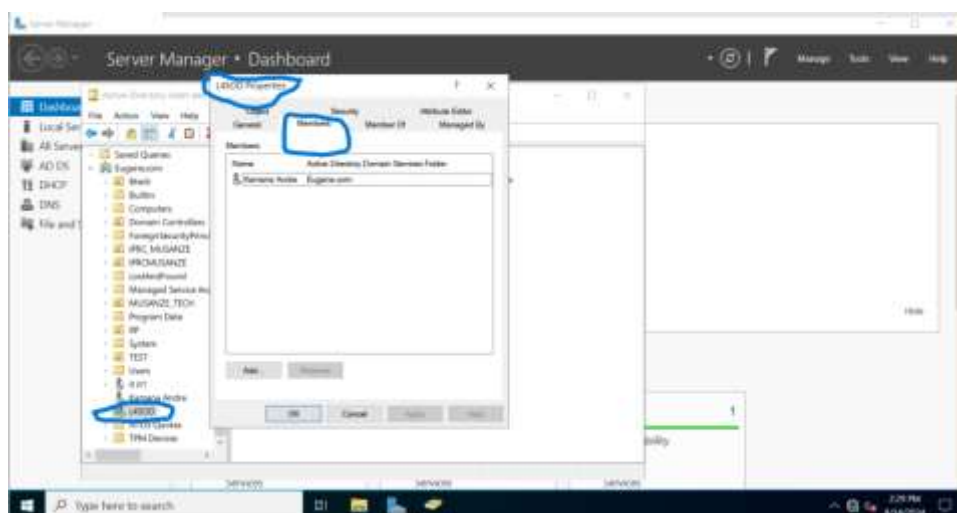
4. Click on "**Add.**"



5. In the **Select Groups** window: Type **L4SOD** in the "Enter the object names to select" field. Click "**Check Names**" to resolve the group name. Once the name resolves, click **OK**.



6. You will see **L4SOD** listed in the "**Member Of**" tab.



7. Click **Apply** and then **OK** to save the changes.

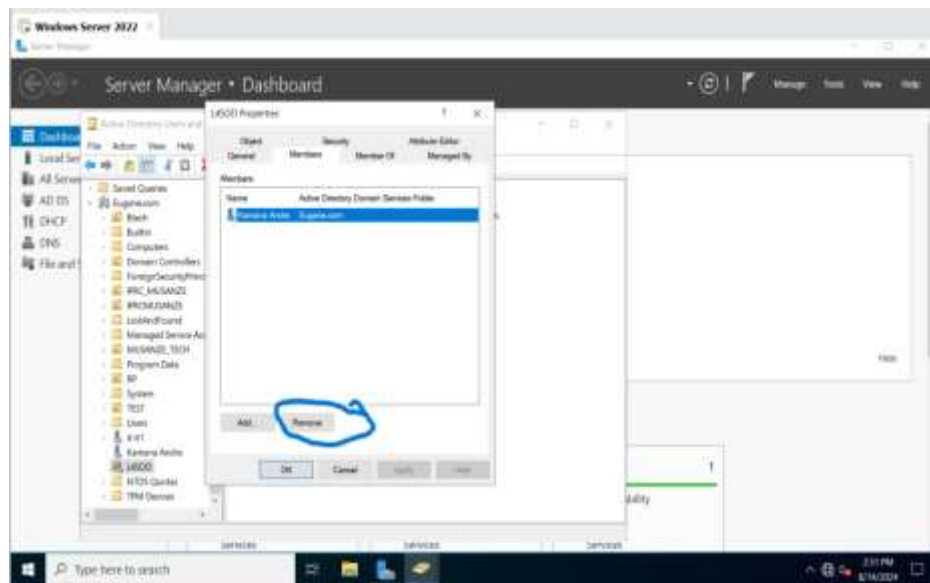
8. To Verify Right-click on the **L4SOD** group, select "**Properties**," and go to the "**Members**" tab. Ensure that User (**Kamana Andre**) is listed as a member of the group.

➤ Removing users from group

If you need to remove User (**Kamana Andre**) from the **L4SOD** group:

1. In the **Active Directory Users and Computers** window, right-click on the **L4SOD** group. Select "**Properties**"
2. Go to the "**Members**" tab.
3. Select User (**Kamana Andre**) from the list of members.

4. Click **"Remove"**.



5. Click **OK** to save the changes.



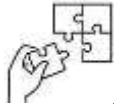
Points to Remember

- **Description of user groups**

- ✓ A group is a collection of Active Directory objects. The group can include users, computers, other groups and other AD objects.
- ✓ Types of groups in windows server are: Security Groups and Distribution Groups

- **To Manage users in group, follow the following steps:**

- ✓ In Server Manager, click on **"Tools"** and select **"Active Directory Users and Computers."**
- ✓ Right click on click on domain name then Select **"New" > "Group"**.
- ✓ In the **New Object - Group** window: type **Group name**, **Group scope**: Global, **Group type**: Security.



Application of learning 2.3.

Company Rwanda TVT Board (RTB), dedicated to promoting quality education in technical and vocational training from levels one (1) to five (5), RTB is hiring an IT System Administrator. As part of the assessment, the IT System Administrator must complete the following tasks within 1 hour: Create a new group named students in Active Directory. Then, add the users **Eric Murindwa** and **Pepe Uwitonze** to the students group. Finally, remove **Eric Murindwa** from the students group. These tasks will demonstrate the IT System Administrator's ability to manage group memberships and use Active Directory tools effectively.



Indicative content 2.4: Management of Organization Units (OU)



Duration: 5hrs



Practical Activity 2.4.1: Creation of Organization Units



Task:

- 1: You are requested to go to the computer lab and do the task below individually:
You are L4 SOD trainees, your school is expanding its IT infrastructure. As part of this expansion, you need to organize users into specific Organizational Units (OUs) for better management and security. You have been tasked with creating an OU named “OU-Department”, adding created user **kamana** Andre to this OU, and then removing **kamana** from this OU. Document each step with screenshots.
2. Read key reading 2.4.1 in trainee’s manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 2.4.1 Creation of Organization Units

Organizational Units (OUs) are Active Directory containers that can contain users, groups, computers, and other OUs.

An **OU** is a container within a Microsoft Windows Active Directory (AD) domain that can hold users, groups and computers and other organizational units. It is the smallest unit to which an administrator can assign Group Policy settings or account permissions.

An AD organizational unit can have multiple OUs within it, but all attributes within the containing OU must be unique. Active Directory OUs cannot contain objects from other [domains](#).

OUs are used to:

1. Represent your organization hierarchically and logically
2. Manage a collection of objects in a consistent way
3. Delegate permissions to administer groups of objects

4. Apply policies

- **Creation of an Organizational Unit (OU):**

1. Open Server manager > Tools > Active Directory users and computers >
2. In the ADUC console, right-click on the domain name (e.g., Eugene.com) in the left pane.
3. Select **New > Organizational Unit** from the context menu.
4. In the dialog box, name the OU (e.g. **OU-Department**).
5. Optionally, check the box for "Protect container from accidental deletion" to prevent accidental removal.
6. Click **OK** to create the OU.

- **Adding Users in OU**

Step 1: Navigate to the location where the user's name (e.g. **Kamana Andre**) is stored in ADUC

Step 2: Right-click on user (Kamana Andre) and select **Move**.

Step 3: In the **Move** dialog box, browse to and select the newly created organization unit (**OU-Department**).

Step 4: Click **OK** to move user (Kamana Andre) to the OU.

- **Remove the User from the Organizational Unit (OU)**

Step 1: Navigate to **organization unit (OU-Department)** in ADUC.

Step 2: Right-click on user (**Kamana Andre**) and click on **Remove**.

Step 3: In the **Remove** dialog box, select the container where you want to move user (**Kamana Andre**)

Step 4: Click **OK** to remove user (**Kamana Andre**) from **organization unit (OU-Department)**.

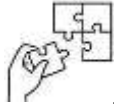


Points to Remember

- **Creation of Organization Units:**

- ✓ In **Active Directory Users and Computers**, select the top-level organizational unit you created
- ✓ Right-click and select **New > Organizational Unit**.
- To Create user in organization Units follow the following steps:

- ✓ In the 'Active Directory Users and Computers' console, navigate to the OU where you want to create the users.
- ✓ Right-click on the OU and select '**New**' > '**User**'.



Application of learning 2.4.

RISA has the mission of digitizing the Rwandan society through increased usage of Information and Communication Technologies and innovation technology as a cross-cutting enabler for the development of other sectors, spearheading Rwanda's digital and social economic transformation. As part of the hiring process for an IT System Administrator at RISA, you are required to complete the following tasks within 1 hour: Create a new Organizational Unit (OU) named "**Training Department**", add the users "**Eric Murindwa**" and "**Pepe Uwitonze**" to this OU, and then remove "Pepe Uwitonze" from the "Training Department" OU.

N.B: Capture screenshots of each step.



Indicative content 2.5: Assignment of Permission to Users



Duration: 5hrs



Practical Activity 2.5.1: Granting and revoking User account permissions



Task:

1: You are requested to go to the computer lab and do the task below individually:

In this practical task, you are requested to manage user account permissions for **Kamana Andre** within your company's Active Directory, specifically related to the **L4SOD** group. Your goal is to grant **Kamana Andre** full permissions related to the **L4SOD** group, ensuring he has comprehensive access. After verifying that Kamana has been granted full permissions, you will then revoke these permissions to remove his access. Document each step with screenshots

2. Read key reading 2.5.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 2.5.1: Grant and Revoke Users account permissions

Grant: To grant means to give or provide someone with certain rights, permissions, or privileges. When you grant permissions to a user or group, you are allowing them access to specific resources, such as files, folders, or system settings. Granting permissions typically involves specifying the type and level of access that the user or group should have.

Revoke: To revoke means to take back or remove previously granted rights, permissions, or privileges. When you revoke permissions from a user or group, you are removing their access to specific resources. Revoking permissions is

done when you want to restrict or deny access to certain files, folders, or system

Settings that were previously granted.

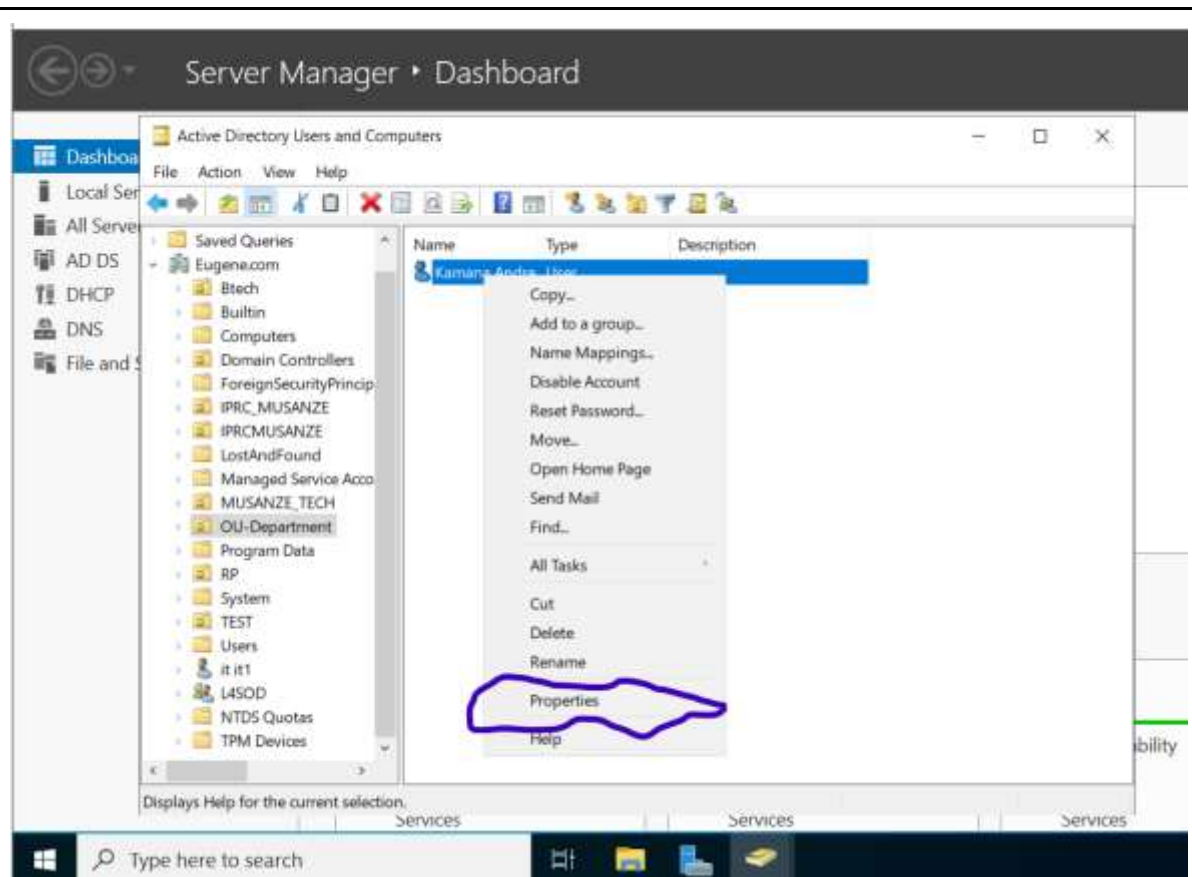
Grant Users account permissions

Step 1: Open Active Directory Users and Computers (ADUC): Click on **Start** menu, Search for "**Active Directory Users and Computers**" and click on it to open.

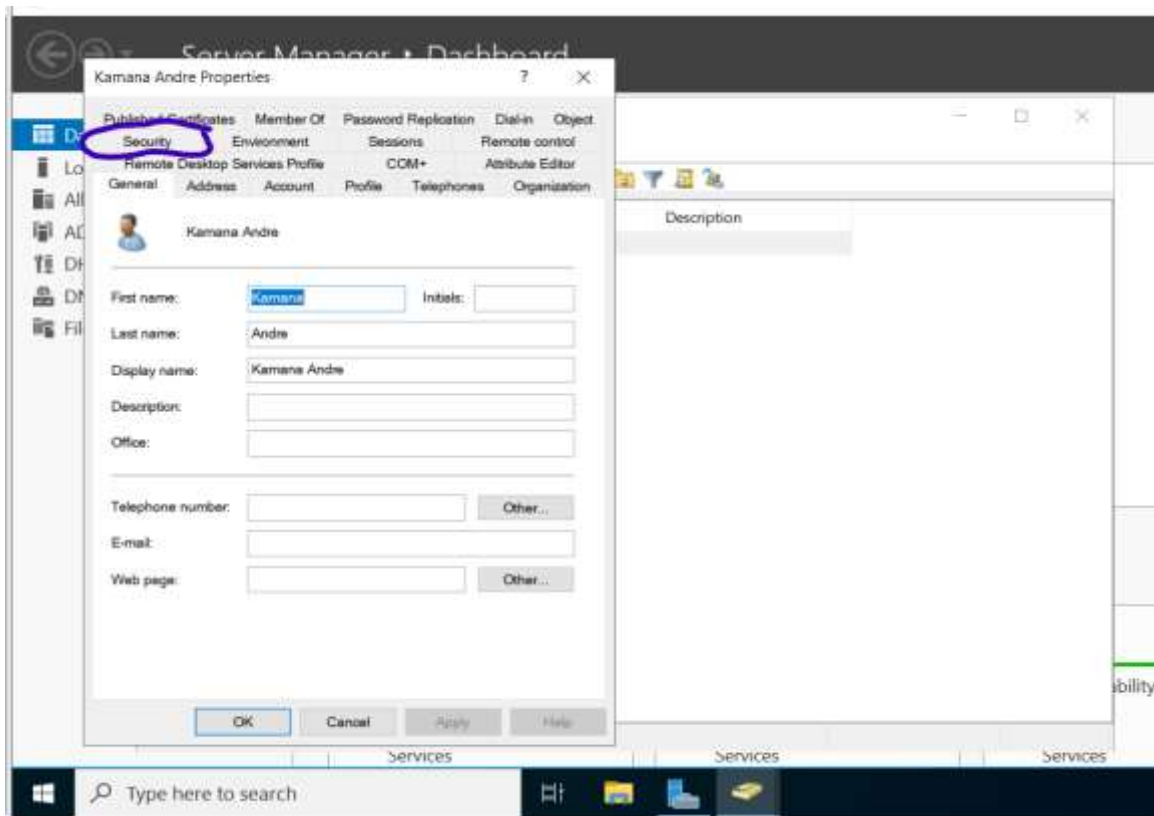
Step 2: Locate the Object (User, Group, or Organizational Unit)

- In the ADUC console, expand the appropriate Organizational Unit (OU) where the object (user, group, or OU) is located.
- Find and select the object to which you want to assign permissions.

Step 3: Open **Properties** of the Object: Right-click on the selected object (e.g., a user, group, or OU) and click on "**Properties**."

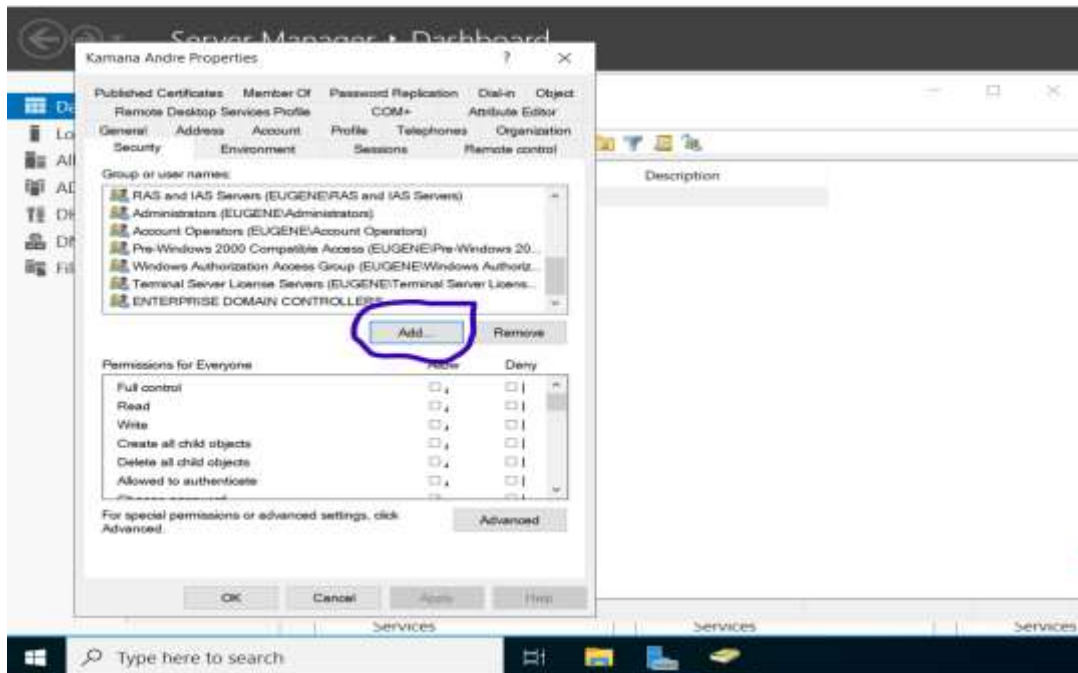


- Navigate to the "Security" tab.

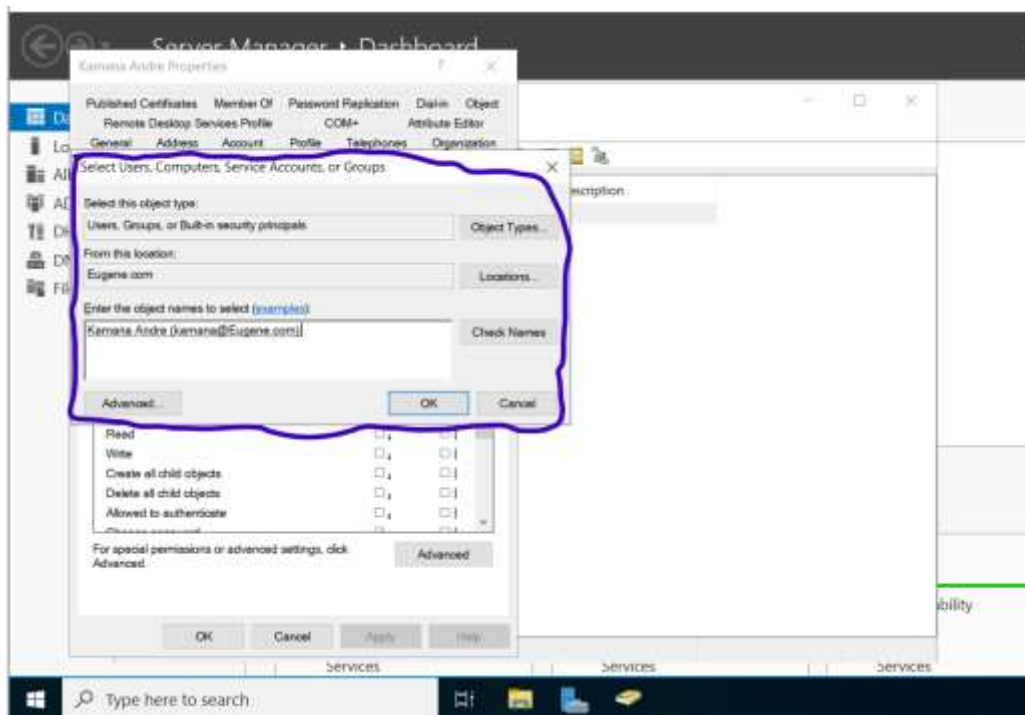


Step 4: Add the User to the Object

- Click "Add..." to open the "Select Users, Computers, Service Accounts, or Groups" dialog.

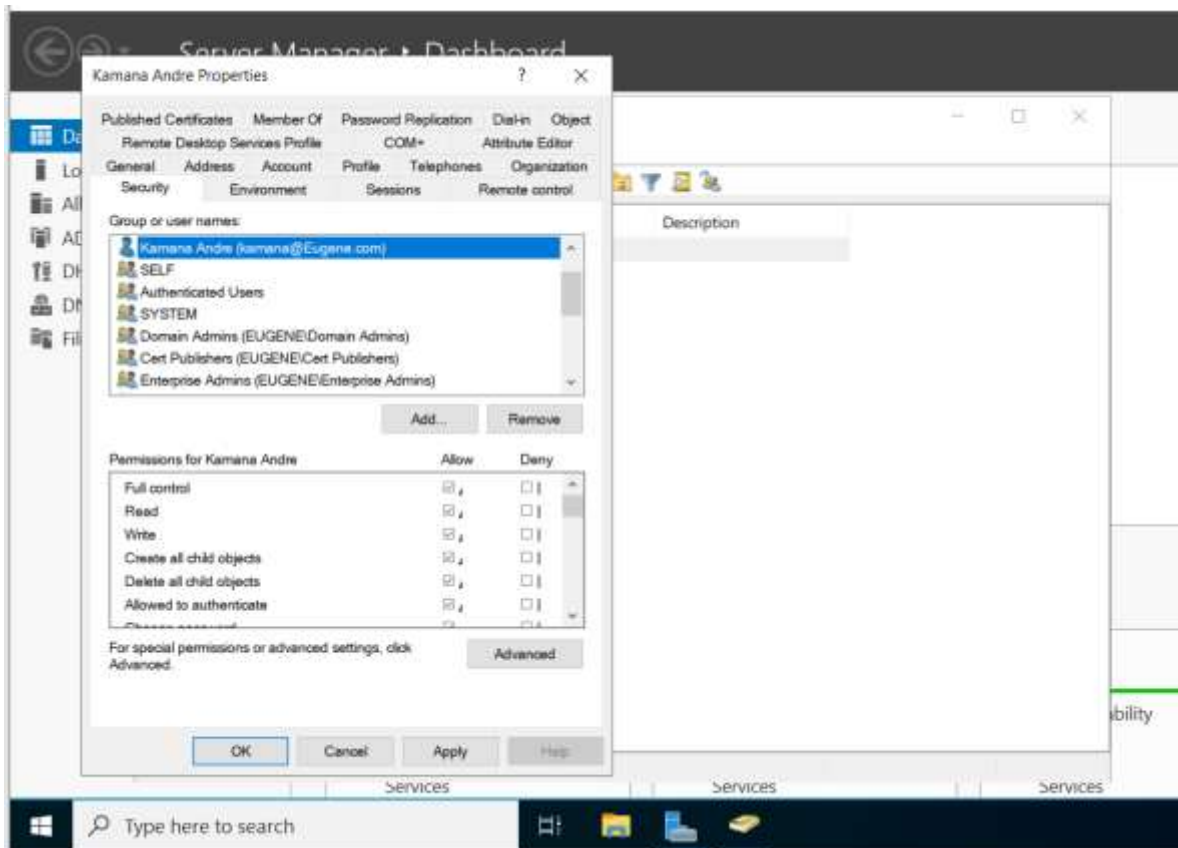


- Enter the name of the user you want to assign permissions to in the search field.
- Click "**Check Names**" to verify the user account.
- Click "**OK.**"



Step 5: Assign Permissions to the User

- With the user selected in the "**Group or user names**" list, check the appropriate permission boxes in the "**Permissions for [User]**" section.
 - ❖ **Common permissions include:**
 1. **Full Control:** Grants all permissions.
 2. **Read:** Allows the user to read the object's properties.
 3. **Write:** Allows the user to modify the object's properties.
 4. **Modify:** Allows the user to make changes without full control.
- After selecting the necessary permissions, click "**Apply**" and then "**OK.**"



Step 6: Verify Permissions

- Go back to the "**Security**" tab and review the permissions assigned to the user.
- Ensure that the user has the correct level of access.

Revoke Users account permissions

Step 1: Open Active Directory Users and Computers (ADUC): Click on **Start** menu, Search for "**Active Directory Users and Computers**" and click on it to open.

Step 2: Locate the Object (User, Group, or Organizational Unit)

- In the ADUC console, expand the appropriate Organizational Unit (OU) where the object (user, group, or OU) is located.

- Find and select the object from which you want to revoke permissions.

Step 3: Open **Properties** of the Object: Right-click on the selected object (e.g., a user, group, or OU) and select "**Properties.**"

- Navigate to the "**Security**" tab.

Step 4: Revoke the User's Permissions

- In the "**Group or user names**" list, select the user whose permissions you want to revoke.
- Uncheck the boxes for the permissions you want to revoke (e.g. Full Control, Read, and Write).

Step 5: After modifying or removing permissions, click "**Apply**" and then "**OK.**"

Step 6: Go back to the "**Security**" tab and review the list to ensure the user's permissions have been correctly revoked.

- **Change remote account permission for a user account**

To change the remote account permissions for a user account in Active Directory, follow these steps:

Step 1: Open Active Directory Users and Computers (ADUC)

- Click on **Start** menu, Search for "**Active Directory Users and Computers**" and click on it to open.

Step 2: Locate the User Account

- In the ADUC console, expand the appropriate Organizational Unit (OU) where the user account is located.
- Find and select the user account for which you want to change remote permissions.

Step 3: Open Properties of the User Account

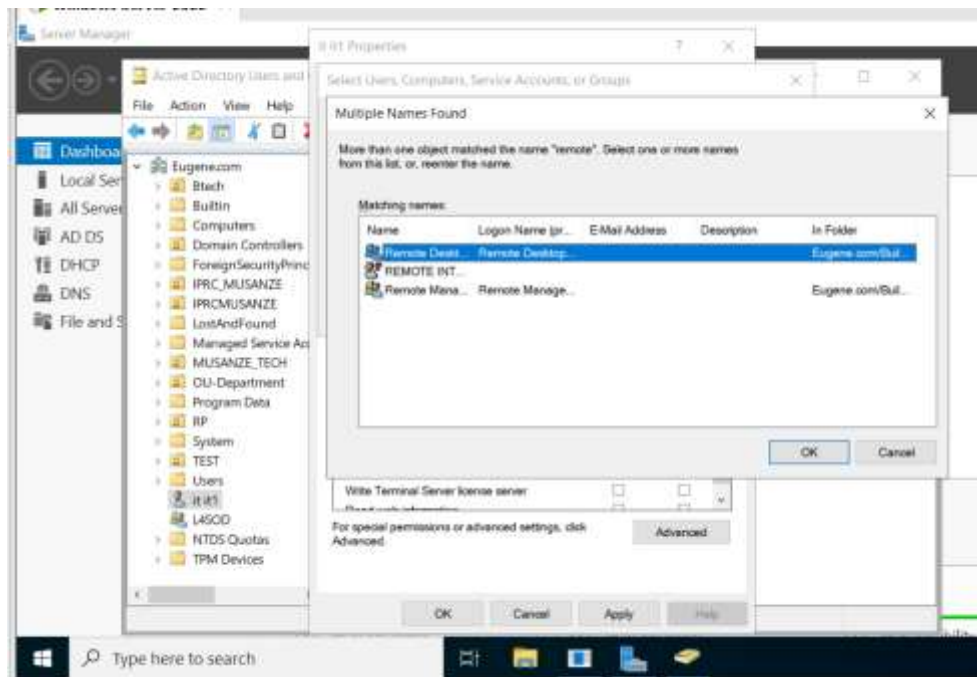
- Right-click on the user account and select "**Properties.**"
- Navigate to the "**Security**" tab.

Step 4: Modify Remote Account Permissions

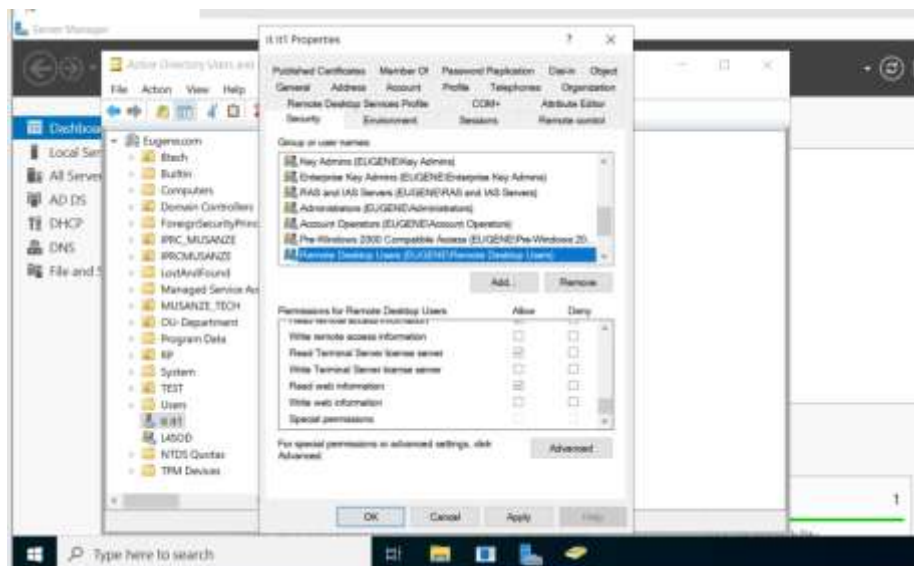
- In the "**Group or user names**" list, ensure that the user or group that needs remote access is listed. If the user or group is not listed, click "**Add.**" to include
 - Once the correct user or group is selected, check or uncheck the relevant permission boxes.

❖ **Common permissions for remote access might include:**

1. **Remote Desktop Users:** Allows the user to log in remotely via Remote Desktop.
2. **Allow log on through Remote Desktop Services:** Ensures that the user can access the system remotely.



Step 5: After selecting or modifying the permissions, click "**Apply**" and then "**OK.**"



Step 6: Go back to the "**Security**" tab or check the "**Remote Desktop Users**" group to ensure the user's permissions have been correctly modified.



Points to Remember

■ Granting and revoking User account permissions:

Grant: To grant means to give or provide someone with certain rights, permissions, or privileges.

Revoke: To revoke means to take back or remove previously granted rights, permissions, or privileges.

a. Grant Users account permissions steps:

- ✓ Open Active Directory Users and Computers (ADUC) from the Start menu.
- ✓ Locate and select the desired object (user, group, or OU) in the ADUC console.
- ✓ Right-click the object, go to "Properties," and under the "Security" tab, click "Add" to find the user.
- ✓ Assign the necessary permissions to the user, apply changes, and verify the permissions.

b. Revoke Users account permissions steps:

- ✓ Open Active Directory Users and Computers (ADUC) from the Start menu.
- ✓ Locate the user, group, or Organizational Unit (OU) and open its properties.
- ✓ In the "Security" tab, select the user and uncheck the permissions to revoke.
- ✓ Click "Apply" and "OK," then review to ensure permissions are removed.

c. Change remote account permission for a user account

- ✓ Open **Active Directory Users and Computers (ADUC)**, locate and right-click the user account, then select **Properties**.
- ✓ Go to the **Security** tab and check if the user or group needing remote access is listed; if not, click **Add** to include them.
- ✓ Modify the permissions by checking or unchecking relevant boxes like **Remote Desktop Users** or **Allow log on through Remote Desktop Services**.
- ✓ Click **Apply**, then **OK**, and verify the changes in the **Security** tab or the **Remote Desktop Users** group.



Indicative content 2.6 Management of client machines



Duration: 5hrs



Practical Activity 2.6.1: Joining a client computer to the domain



Task:

1. You are requested to go to the computer lab and do the task below individually:

As trainees, you practice key tasks related to managing client machines, including changing the computer name to your family name, establishing connectivity between a client and server, and changing the client's membership from a Workgroup to a Domain.

2. Read the key reading on Practical Activity 2.6.1
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 2.6.1: Joining a client computer to the domain

How to join a client to domain



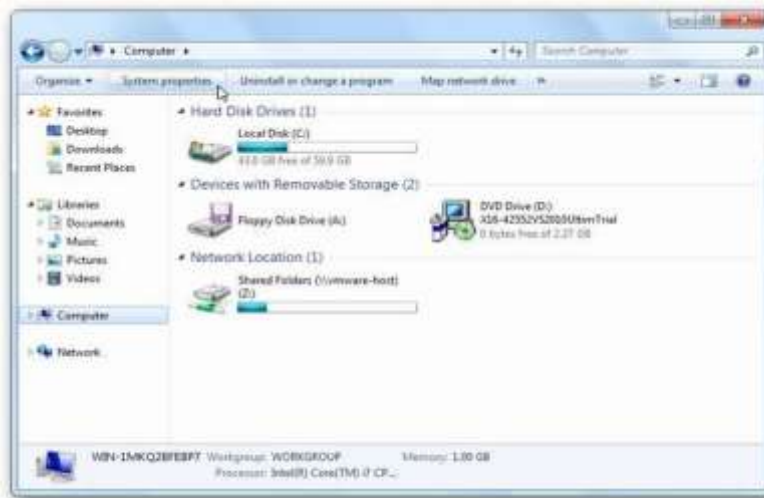
We have shown you how to install Active Directory on your network, but it's pointless to have a DomainController unless you add your machines to the Domain, so today we're going to cover how to do that.

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

1. Rename the machine to a user friendly, recognizable name before adding it to the Domain.
2. Make sure your DNS settings are pointing to the correct DNS Server for the domain.
3. You have to have access to a Domain account that is part of the Domain Admins security group.

Joining a client to a Domain

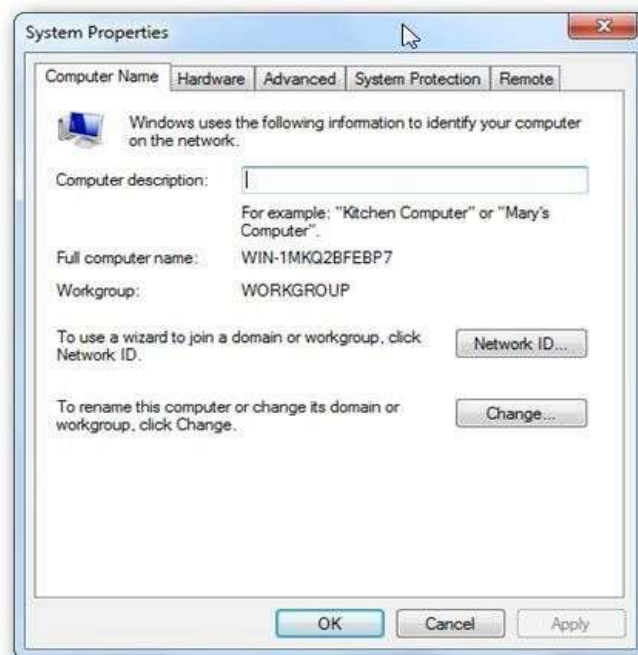
1. Open Computer and click on the **System Properties** button.



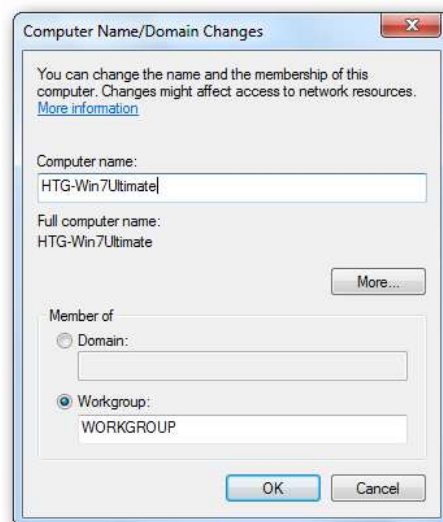
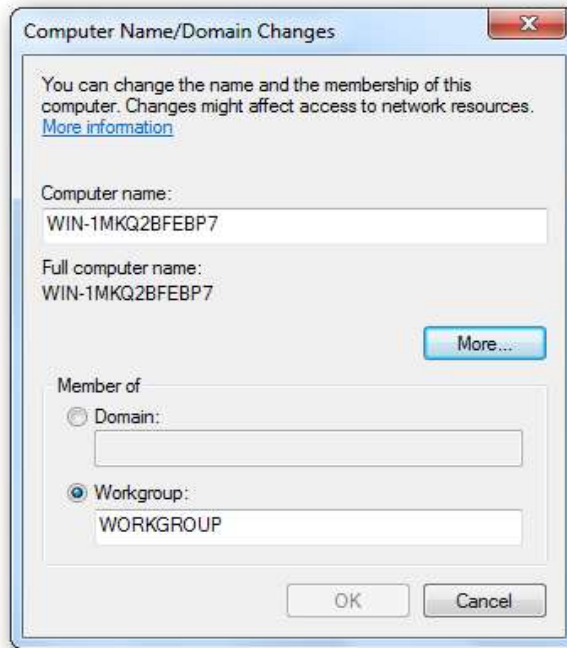
2. Now click on the **advanced system settings** link on the left-hand side



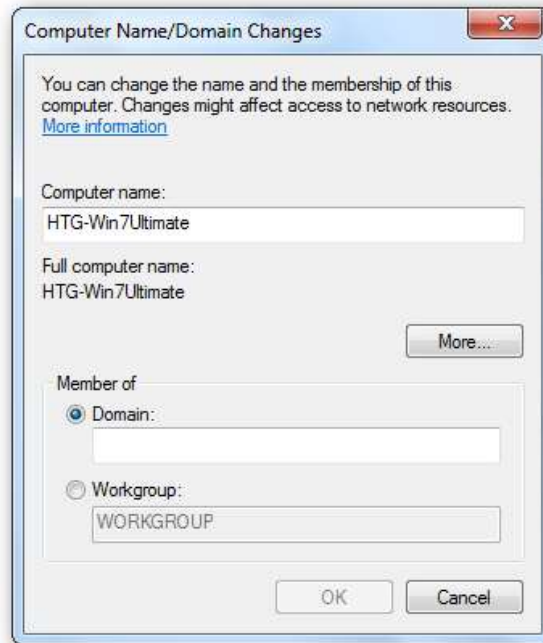
3. When the advanced system settings open, switch to the computer name tab.



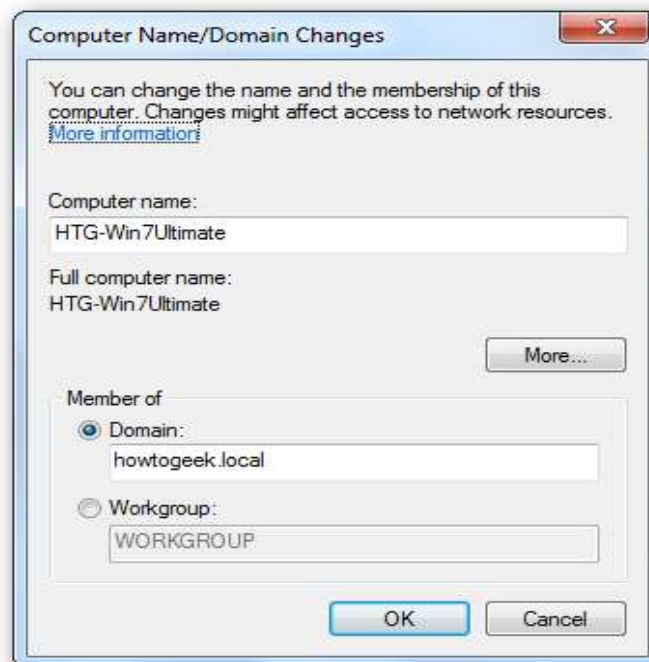
4. Click on the **change** button, from here you can change your Computers Name to a more friendly name.



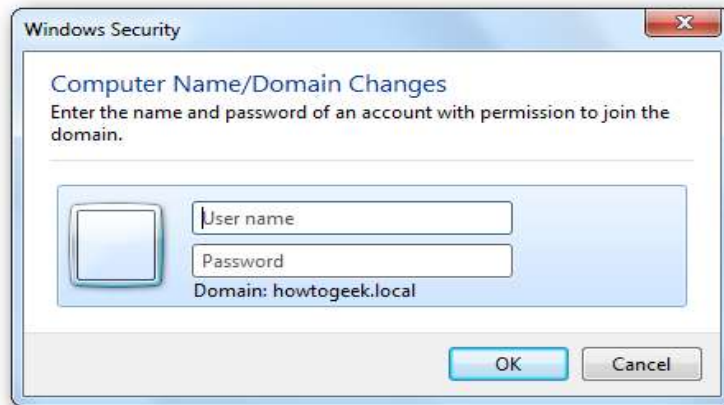
5. Now switch the radio button, in the bottom section, from Workgroup to Domain. This will make the text box become available.



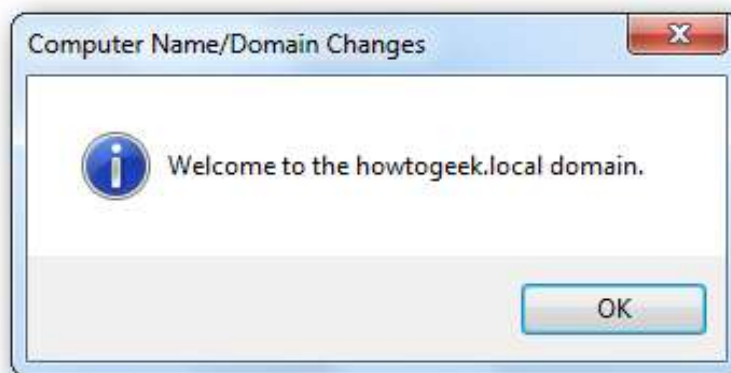
6. Now type in the name of your domain, ours is **howtogeek.local**, but yours will be whatever you made it when you set up Active Directory



When you hit enter, or click ok, you will be asked for the user name and password of a Domain Admin user account.



If you specify the correct credentials, you will be welcomed to the Domain. (Lee, 2024)



Practical Activity 2.6.2: Implementation of delegation of control

Task

1. You are requested to go to the computer lab and do the task below individually:
"As a system administrator, use the Delegation of Control Wizard to assign **Kamana** from the 'HelpDesk' group permissions to create, delete, and manage user accounts, as well as reset user passwords and force password changes at the next logon. Ensure that these permissions are limited to the specified organizational unit (OU). Document the steps and permissions configured."
2. Read key reading 2.6.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 2.6.2: Implementation of delegation of control

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

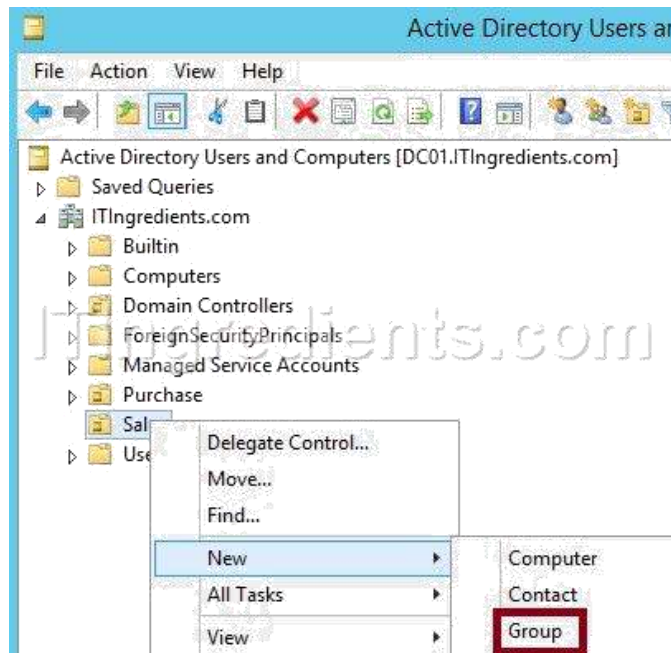
First option is that, we will add any other user into the **Domain Admins group**. This would assign Domain Admin permissions to the newly added user, these rights are sufficient to perform any domain level change in the environment. But do you really want to give **keys of kingdom to anyone**? In my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

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

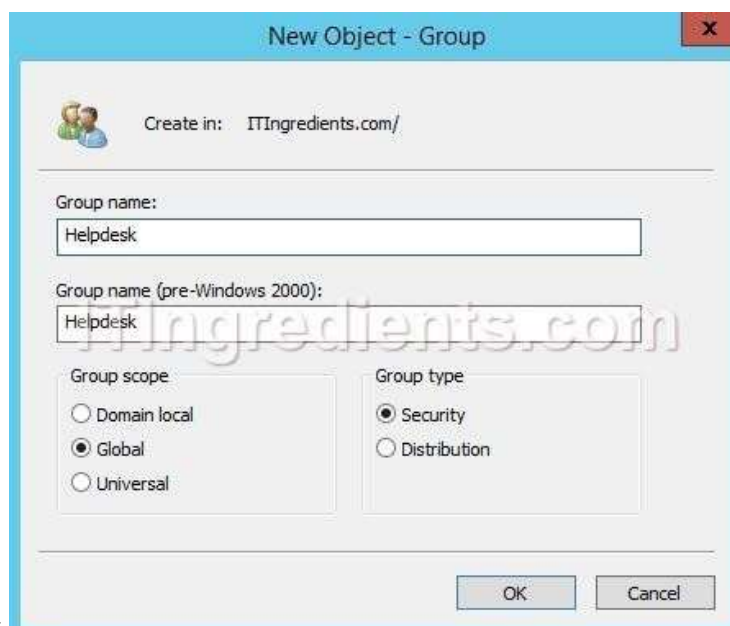
Steps to Delegate Control to Domain Users

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

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



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



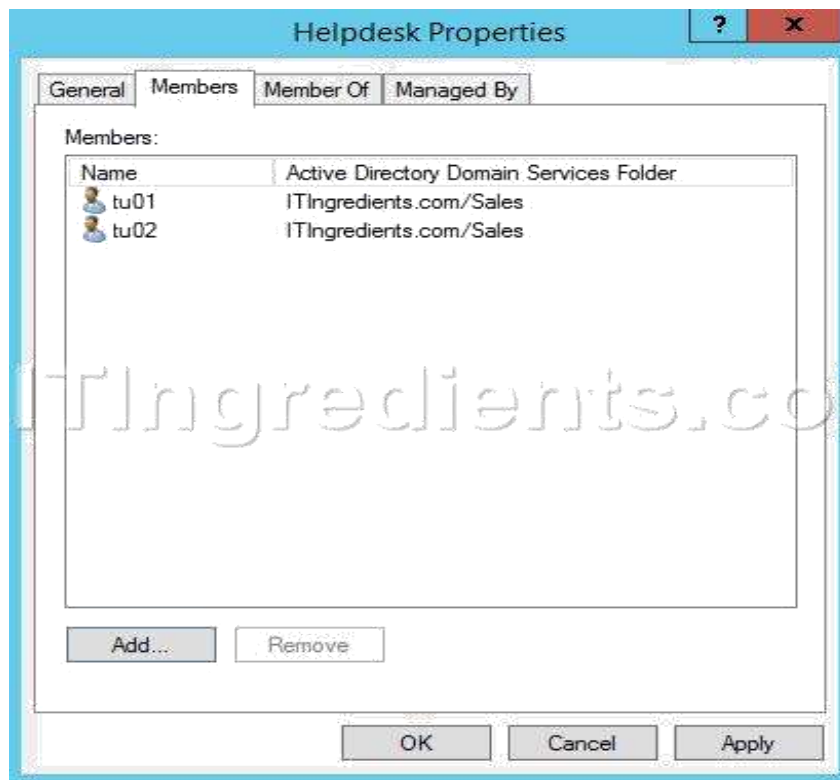
Helpdesk.



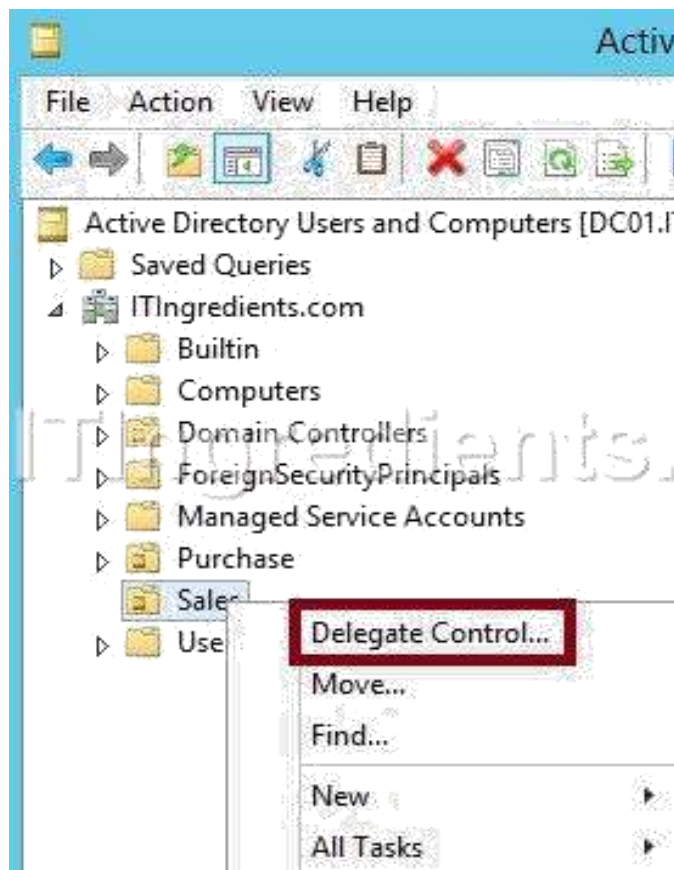
3. Right click on the group (Helpdesk) and click on Properties to open the properties console to modify various group settings.



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



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



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



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

Click on next to continue.

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



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



Conclusion:

Delegate access would enable set of users to perform the tasks that are normally performed by Domain Admins.

It would only restrict the user to the OU on which rights are delegated.



Theoretical Activity 2.6.3: Description of Group Policy Object (GPO)



Tasks:

1. You are requested to answer the following questions:
 - i. Compare term Group policy and Group Policy Object (GPO)
 - ii. Describe 3 types of Group Policy Object
 - iii. Discuss on the following Hierarchy finds on Group Policy Object:
 - a) Local
 - b) Site
 - c) Domain
 - d) OU
 - iv. What is group Policy Template (GPT)?
 - v. Where group policy template stored?
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
- 6 Remember to ready more on key reading 2.6.3 in the trainee's manual



Key readings 2.6.3: Description of Group Policy Object (GPO)

What is a **GPO**?

Group Policy is a tool that allows you to specify managed configurations for users and computers through Group Policy settings and Group Policy Preferences.

Local Group Policy Editor is used to configure Group Policy Settings that affect only local computer or user.

GPO is managed in ADDS environment through the Group Policy Management Console (GPMC).

GPO types

There are three types of GPO:

1. Local Group Policy Objects: Refers to the collection of group policy settings that only apply to the local computer and to the users who log on to that computer. Local

GPOs are used when policy settings need to apply to a single Windows computer or user. Local GPOs exist by default on all Windows computers.

2. Non-local Group Policy Objects: Is used when policy settings have to apply to one or more Windows computers or users. Non-local GPOs apply to Windows computers or users once they're linked to Active Directory objects, such as sites, domains or organizational units.

3. Starter Group Policy Objects: Introduced in Windows Server 2008, starter GPOs are templates for Group Policy settings. These objects enable an administrator to create and have a pre-configured group of settings that represent a baseline for any future policy to be created.

A starter GPO is a type of nonlocal group policy object that's used as a template when creating a new GPO within ADDS. Starter GPOs can be used when an organization has a requirement that certain mandatory settings should always be in place. Having a starter GPO would then ensure that as each GPO is created, the mandatory settings are already pre-populated within it. This helps to save time for administrators.

Because they're used as templates, Starter GPOs can't be linked to ADDS objects like nonlocal GPOs. The amount of starter GPOs that can be used within ADDS is unlimited. However, only one Starter GPO can apply to a group policy object.

GPO Hierarchy/Precedence

Precedence in group policy, like the name suggests, simply refers to the order or rank that policy applies.

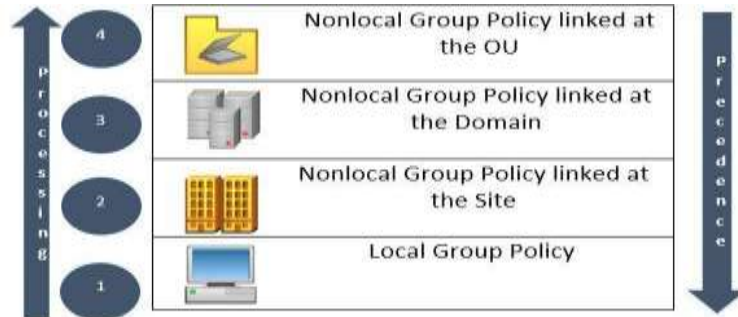
Group Policy objects are applied in a hierarchical manner, and often multiple Group Policy objects are combined together to form the effective policy. Local Group Policy objects are applied first, followed by site level, domain level, and organizational unit level Group Policy objects.

Group policy is processed in the following order:

1. Local GPO (least important)
2. Site
3. Domain
4. Organization unit; sub-Organization Unit
5. Enforcement GPO is applied to domain (most important)

GPO Order of Precedence

The group policy that is processed first has the least precedence. The one that is processed last has the most as shown in the following figure.



The group policy that is processed first has the least precedence. The one that is processed last has the most as shown in the above figure.

GPO Hierarchy are:

1. **Local:** GPOs that are applied to the computer's local policy for each user; **Local** is applied since nothing else is configured.
2. **Site:** GPOs that are applied to the site of which the computer is a member.
3. **Domain:** GPOs that are applied to the domain of which the computer is a member
4. **OUs:** GPOs that are applied to the OUs on which the computer is placed

N.B The last GPO to be applied wins

Regardless of whether the computer for which GPOs are applied is or is not a member of the domain, we encounter the following two ways to apply GPOs:

- ✓ **Non-domain computer:** The computer on which the GPO is applied locally
- ✓ **Domain computer:** The computer on which the GPO is applied through Active Directory

• Group Policy Template (GPT)

The Group Policy template (GPT) is a file system folder that includes policy data specified by **.adm** files, security settings, script files, and information about applications that are available for installation.

The **GPT** is located in the system volume folder (**SysVol**) in the domain \Policies subfolder.

The Group Policy template is a collection of files that is stored in the SYSVOL of each domain controller.



Practical Activity 2.6.4: Managing GPO settings



Task:

1: You are requested to answer the following activity individually:

As Level 4 trainees, you are tasked with managing Group Policy Objects (GPOs) in a Windows Server environment. Your goal is to create and configure a GPO named "**Student-GPO**", utilize the Group Policy Editor, and manage user settings through the Group Policy Management Console (GPMC).

2. Read the key readings 2.6.4 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

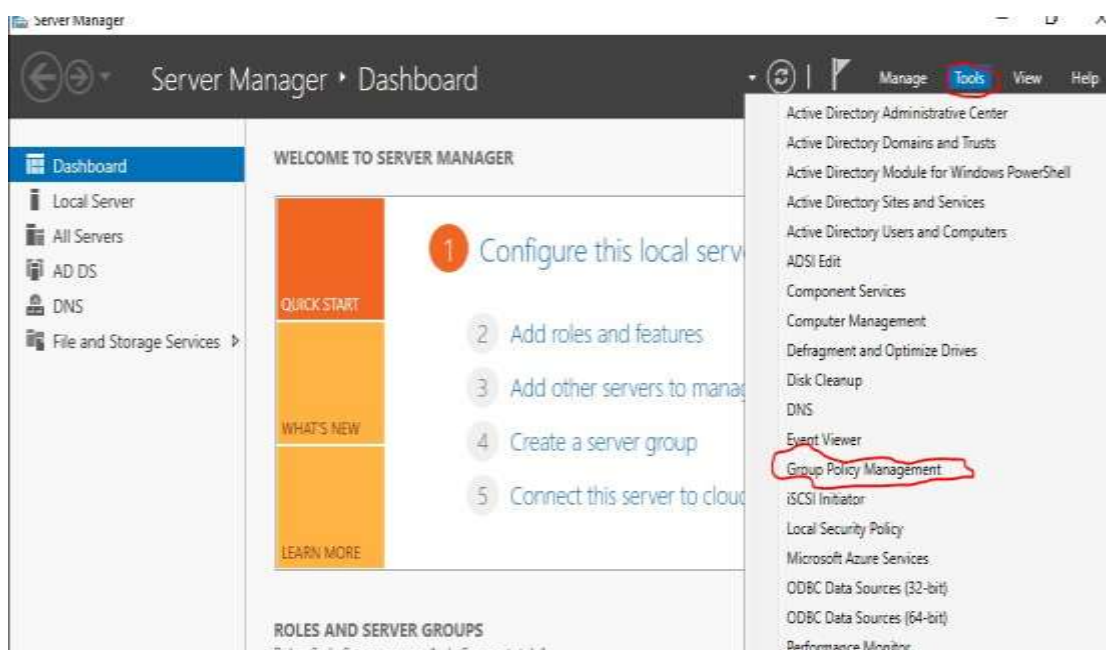


Key readings 2.6.4: Managing GPO settings

- **Create GPO**

GPOs are applied recursively, and this means that the settings will also be applied to all sub-OUs beneath the original OU the GPO was applied to.

1. To start Group Policy, you need to click **Tools > Group Policy Management** within Server Manager.



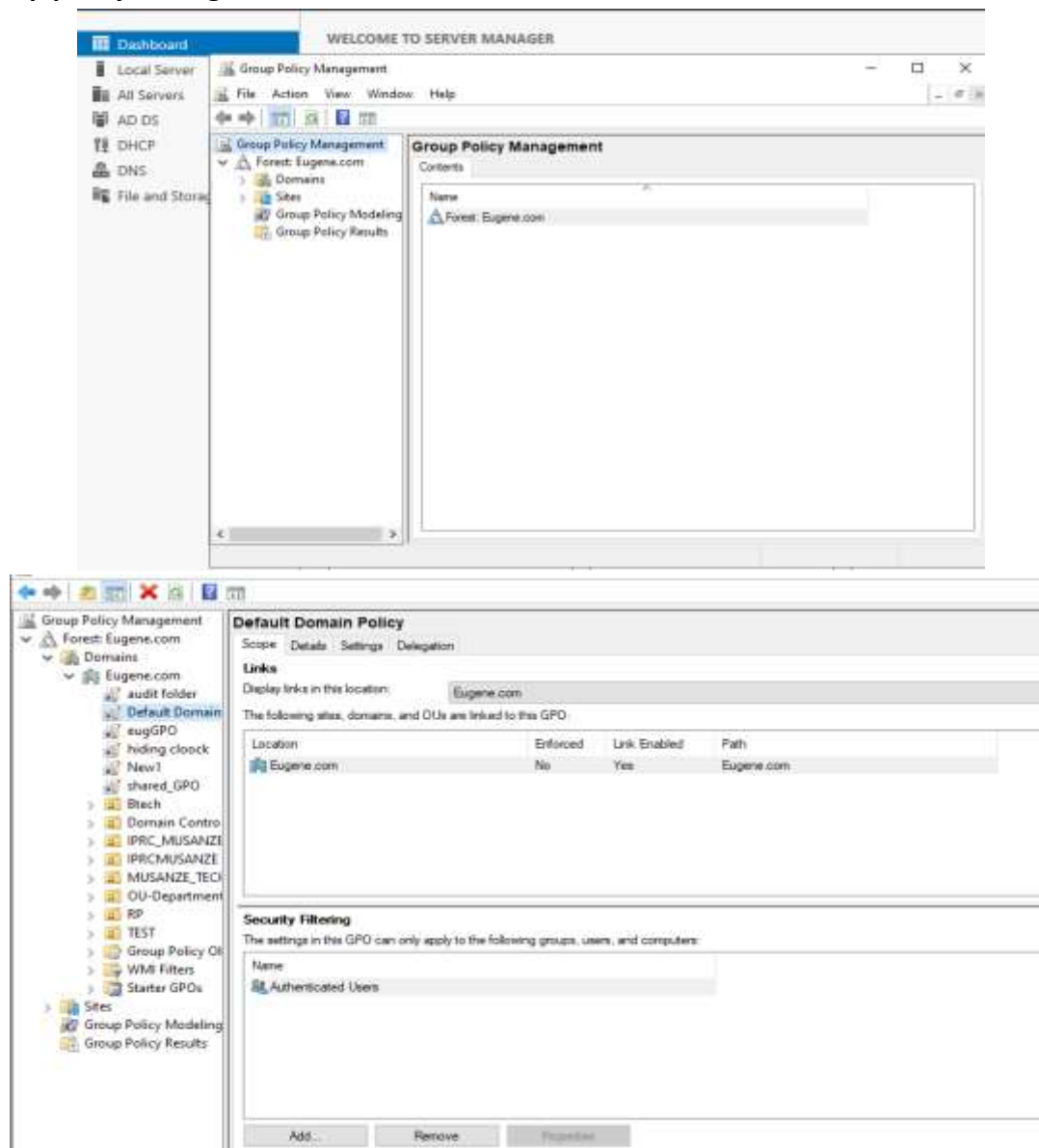
2. Once the console loads, you will need to expand the Forest **Eugene.com** by clicking the arrow. Now you see Domains, Sites, Group Policy Modeling and Group Policy Results.

Domain: Folder contains all the domains that are underneath the forest

Sites: Folder contains all your sites that you may have configured through Active Directory Sites and Services, in short, this is used when you have servers that are physically in a different location

Group Policy Modeling and **Group Policy Results:** are both tools that can be used to troubleshoot any Group Policy issues that may arise.

Group policy management console



Under Eugene.com

- **domain Default Domain Policy GPO:** group policy created automatically when a new domain is created. Since it is directly underneath the domain, it will be applied to all the Active Directory objects beneath the root of the domain.

- The Group Policy Objects folder contains ALL the GPOs that are inside this domain whether they are in use or not.
- **WMI Filters** allow you to add specific rules of when a specific GPO should be applied or not.

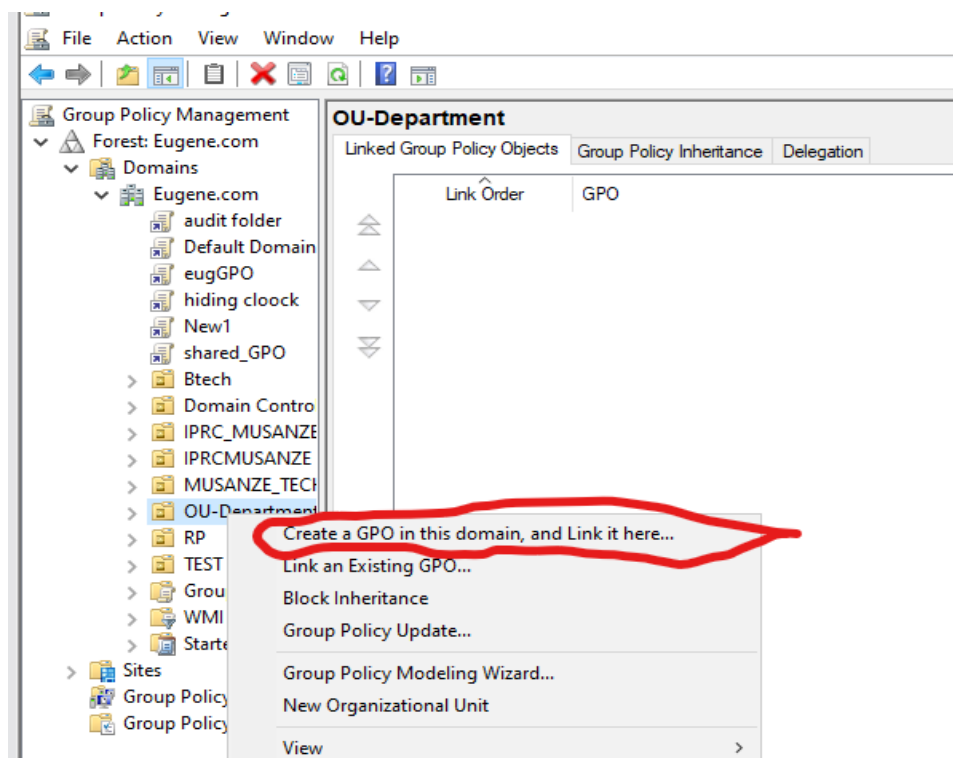
For example, you could only apply a particular GPO if the computer is using an operating system of Windows 7 or newer.

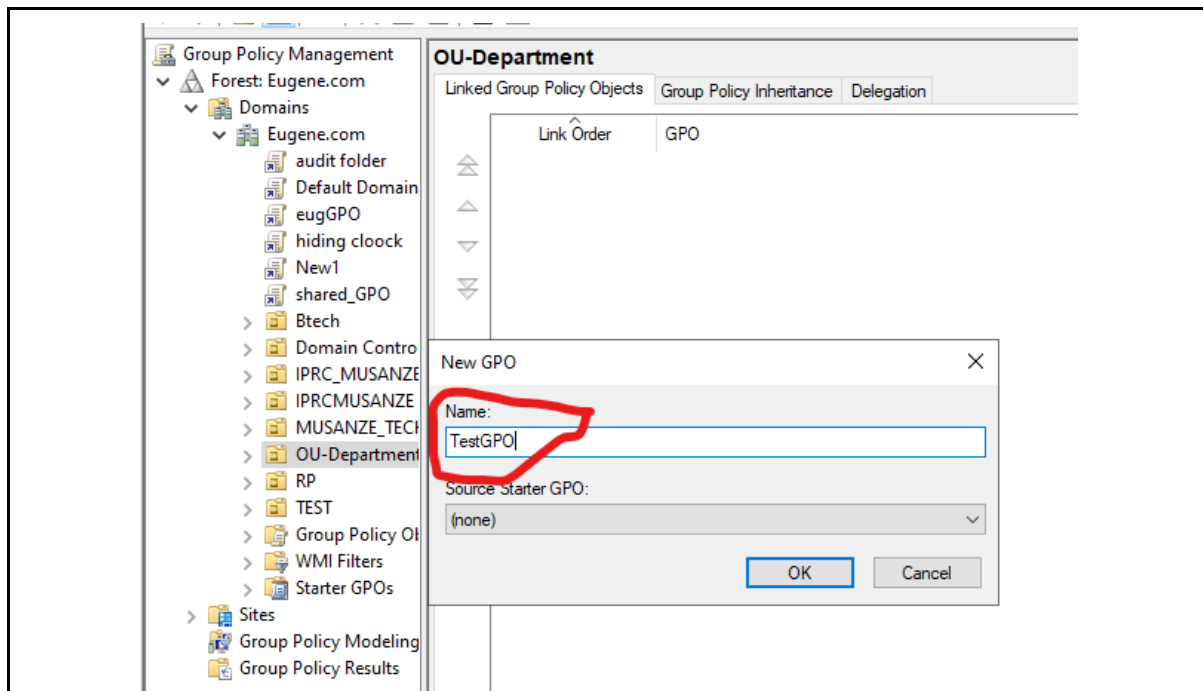
The Starter GPOs folder is used when you want to import or export GPOs for distribution to other environments.

GPOs are often used in a modular sense, meaning that an administrator might create several GPOs, and apply them to OUs as needed. For example, you could create a GPO that installs Adobe Flash Player, and apply the GPO to all the OUs that contain computers which would need Adobe Flash Player installed. Or you could create a GPO that prevents users from launching Internet Explorer, and you could link that GPO to all the OUs where you don't want the users to launch Internet Explorer. Creating a GPO is very similar to creating a user account or organizational unit in Active Directory.

You simply need to right-click on a domain or OU and choose Create a GPO in this domain, and Link it her.

Creating GPO





2. Using the GPO Editor

Step 1: After creating the GPO, right-click the newly created GPO under the appropriate OU in the GPMC.

Step 2: Select **"Edit"** from the context menu to open the Group Policy Management Editor (GPO Editor).

Step 3: In the GPO Editor, navigate through the policy settings under **Computer Configuration** or **User Configuration** depending on the policy you want to manage.

Step 4: Make the necessary changes to the policy settings. For example, you can configure password policies, software installation policies, or security settings.

Step 5: After editing, close the GPO Editor to save your changes.

3. Using GPMC to Manage GPO

Step 1: In the GPMC, you can manage existing GPOs by right-clicking on a GPO and selecting **"Edit," "Delete," "Back Up,"** or other management options.

Step 2: You can also **"Link an Existing GPO"** to other OUs or domains by right-clicking the desired OU or domain and selecting **"Link an Existing GPO..."**.

Step 3: Use the **"Group Policy Results"** and **"Group Policy Modeling"** features in GPMC to simulate and analyze the impact of GPOs on specific users or computers.

Step 4: Monitor GPO status and replication by using the **"Status"** tab in the GPMC, which provides information on the GPO's deployment and status.



Points to Remember

- **Joining a client to a Domain follow the following steps:**
 - ✓ Open **System Properties** on the computer and click **Advanced system settings**.
 - ✓ Under the **Computer Name** tab, click **Change** and update the computer's name if needed.
 - ✓ Switch from **Workgroup** to **Domain** and enter your domain name.
 - ✓ Enter the **Domain Admin** username and password when prompted.
 - ✓ If the credentials are correct, you'll be welcomed to the domain.
- **Implementation of Delegation of control**
 - ✓ Open **Active Directory Users and Computers**, right-click on the **Organizational Unit (OU)** (e.g: Sales) and create a new group (e.g: Helpdesk) by selecting **New > Group**.
 - ✓ Set the group scope to **Global** and type to **Security**, then add users to the group through the **Properties** console.
 - ✓ Right-click the **OU (Sales)** again and select **Delegate Control** to launch the wizard.
- **Description of Group Policy Object (GPO)**
 - ✓ **Group Policy** is a tool used by system administrators to quickly and easily make configuration changes to users and computers within Active Directory.
 - ✓ **Group Policy** works by applying GPO (Group Policy Objects) to the OU structure you have created in Active Directory
 - ✓ A **Group Policy Object** contains configuration settings for both users and computers. When a GPO is applied to an OU, the settings configured in the GPO are applied the users and computers that are within the OU.
- **There are three types of GPO:**
 - ✓ **Local Group Policy Objects.** Refers to the collection of group policy settings that only apply to the local computer and to the users who log on to that computer.
 - ✓ **Non-local Group Policy Objects.** Is used when policy settings have to apply to on or more Windows computers or users.
 - ✓ **Starter Group Policy Objects.** A starter GPO is a type of nonlocal group policy object that's used as a template when creating a new GPO within ADDS.
- **GPO Hierarchy/Precedence:** ***Precedence*** in group policy, like the name suggests, simply refers to the order or rank that policy applies.
 - ✓ **Local:** GPOs that are applied to the computer's local policy for each user; Local is applied since nothing else is configured.
 - ✓ **Site:** GPOs that are applied to the site of which the computer is a member.
 - ✓ **Domain:** GPOs that are applied to the domain of which the computer is a member
 - ✓ **OUs:** GPOs that are applied to the OUs on which the computer is placed

- **Manage GPO settings**

Steps to Create a Group Policy Object (GPO):

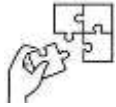
- ✓ Open Group Policy Management and navigate to the desired container (site, domain, or OU).
- ✓ Right-click the container, select "Create a GPO in this domain," and name the GPO.
- ✓ Click OK, then right-click the new GPO and select "Edit" to configure the settings.
- ✓ Close the editor after making your changes.
- ✓ Verify the GPO application using the Group Policy Results tool to ensure it's linked to the correct container.

- **Using the GPO Editor**

- ✓ After creating the GPO, right-click the newly created GPO under the appropriate OU in the GPMC.
- ✓ Select **"Edit"** from the context menu to open the Group Policy Management Editor (GPO Editor).
- ✓ In the GPO Editor, navigate through the policy settings under **Computer Configuration** or **User Configuration** depending on the policy you want to manage.
- ✓ Make the necessary changes to the policy settings. For example, you can configure password policies, software installation policies, or security settings.

Using GPMC to Manage GPO

- ✓ In the GPMC, you can manage existing GPOs by right-clicking on a GPO and selecting **"Edit," "Delete," "Back Up,"** or other management options.
- ✓ You can also **"Link an Existing GPO"** to other OUs or domains by right clicking the desired OU or domain and selecting **"Link an Existing GPO..."**.
- ✓ Use the **"Group Policy Results"** and **"Group Policy Modeling"** features in GPMC to simulate and analyze the impact of GPOs on specific users or computers.
- ✓ Monitor GPO status and replication by using the **"Status"** tab in the GPMC, which provides information on the GPO's deployment and status.



Application of learning 2.6

FFF Ltd company, located in Gicumbi District, Northern Province, FFF Ltd has a problem that there no way to manage their client's machines hence, they need to join a client computer to domain the access to their system they have recently developed so that all users in the company will be able to access it from the server in order to manage their client's machine and user accounts. As an IT technician, you are hired by FFF Ltd to Create and configure Group Policy Objects (GPOs) in server that will manage user settings through the Group Policy Management Console (GPMC).

Tasks:

- To change the client's membership from a Workgroup to a Domain "**DDance**"
- To use the Delegation of Control Wizard to assign **Kamana** from the '**HelpDesk**' group permissions to create, delete, and manage user accounts, as well as reset user passwords and force password changes at the next logon.
- To create and configure a GPO named "**Student-GPO**"



Learning outcome 2 end assessment

Written assessment

Question 1. Circle the letter corresponding to the correct answer:

- i. Which of the following is a security group in Windows Server?
 - a) Distribution Group
 - b) Global Group
 - c) Universal Group
 - d) All of the above
- ii. What is the purpose of an Organizational Unit (OU) in Active Directory?
 - a) To group users for email distribution
 - b) To provide security permissions to objects
 - c) To organize objects hierarchically and logically
 - d) To create a backup of Active Directory
- iii. Which of the following is not a common user account permission in Active Directory?
 - a) Full Control
 - b) Modify
 - c) Read and Write
 - d) Administrator
- iv. What is the default user account type created when a new user is added to Active Directory?
 - a) Administrator
 - b) Standard User
 - c) Guest
 - d) Domain User

Question 2: Read the following statement related to carry out finishing activity and Answer following questions by using **True or False**

1. The Domain Admins group has full control over all objects in an Active Directory domain.
2. You can create a new user account by copying an existing one.

Question 3. Fill in the Blanks space with the appropriate words. Select from the given choices

1. A(n) _____ is a collection of user accounts and other objects in Active Directory.
2. The _____ tab in the user account properties dialog allows you to manage group memberships.
3. To change a user's password in Active Directory, you need to have _____ privileges.

Practical assessment

As the IT Administrator for Special Solutions, you are responsible for effectively managing user accounts, permissions, and network security. Create new user accounts for Umutoni Claudine (Sales Department), Kamali Emmanuel (IT Department), and Kanyana Viviane (Human Resources). Assign appropriate permissions based on their roles: Umutoni Claudine (access to sales-related systems and data), Kamali Emmanuel (full administrative privileges), Kanyana Viviane (access to HR systems and employee data). Set strong password policies for all accounts. Manage existing user accounts by resetting passwords, deactivating/activating accounts, and updating contact information. Create and manage user groups: "Sales Team" and "IT Support." Assign permissions to these groups based on their roles. Organize users into OUs: Sales, IT, and Human Resources. Move users to their respective OUs and apply specific policies or settings. Delegate permissions to a help desk technician for password resets and user account creation/deletion within the "Sales" and "IT" OUs. Ensure proper oversight and control over delegated permissions. Implement strong password policies, enable account lockout policies, and regularly review user permissions. Provide user training on proper password management, security practices, and the use of company systems. Maintain detailed documentation of all user accounts, permissions, and policies. Regularly audit user account activity to identify potential security threats and compliance issues. By successfully completing these tasks, you will demonstrate your ability to effectively manage user accounts, permissions, and OUs in a dynamic and growing business environment.

END



References

Books

Dauti, b. B. (2024). *Windows Server 2022 Administration Fundamentals*. Third Edition.

Krause, J. (2024). *Mastering Windows Server 2022*.

Lee, T. (2024). *Windows Server Automation with PowerShell Cookbook*.

Microsoft. (n.d.). *Microsoft Windows Server Administration Essentials*. Open Library.
Retrieved from

[https://openlibrary.org/books/OL29072895M/Microsoft_Windows_Server_Administration_Essentials](https://openlibrary.org/books/OL29072895M/Microsoft_Windows_Server_Administration_Essentials)

Microsoft. (n.d.). Manage online accounts for users. Microsoft Learn. Retrieved from
<https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-online-accounts-for-users>

Microsoft. (n.d.). Manage user accounts in Windows Server Essentials. Microsoft Learn.
Retrieved from <https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-user-accounts-in-windows-server-essentials>

Microsoft. (n.d.). Add Windows Server Essentials as a member server. Microsoft Learn.
Retrieved from <https://learn.microsoft.com/en-us/windows-server-essentials/install/add-windows-server-essentials-as-a-member-server>

WEB SERVER

Configuration, Deploy, Maintain and Troubleshoot



Indicative contents

- 3.1 Introduction to Web Servers
- 3.2 Configure IIS with Window Server
- 3.3 Management of IIS Web Server
- 3.4 Setting Environment of Developed Web App
- 3.5 Verify Server Environment Requirement
- 3.6 Hosting Web App
- 3.7 Verification of Successfully Hosted Web App

Key Competencies for Learning Outcome 3: Deploy Web Application

Knowledge	Skills	Attitudes
• Description of web servers • Description of FTP and HTTPs protocol • Description web hosting platforms	• Applying IIS with web server • Managing IIS web server • Setting up environment of web app • Verifying server environment • Hosting web app • Testing hosted app	• Being a team player • Being creative • Having attentiveness • Having persistence in troubleshooting • Being patient • Being effective in time management



Duration: 25hrs

Learning outcome 2 objectives:



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

1. Describe clearly web servers/hosting platform used in windows server
2. Describe clearly web servers/hosting platform used in windows server
3. Describe clearly FTP and HTTPs protocol used in communication
4. Describe correctly web hosting platforms used for hosting
5. Set up properly environment of web app in server
6. Verify clearly server environment used in windows server
7. Apply properly IIS in windows server to web server
8. Manage correctly web server for hosting application
9. Host correctly a web app in web server via windows server
10. Test clearly hosted app in web server



Resources

Equipment	Tools	Materials
• Computer • Server	• VMWare workstation • VMWare ESXI • Oracle VirtualBox	• Widow Server • Internet



Indicative content 3.1: Introduction to Web Servers



Duration: 3hrs



Theoretical Activity 3.1.1: Description of web server/hosting platforms



Tasks:

1: You are requested to answer the following questions:

- A. Define the term "**Web Server**"
- B. What does "**IIS**" stand for?
- C. Explain the following types of Web Servers/Web Hosting Platforms:
 - i. IIS Web Server
 - ii. Apache Web Server
 - iii. Nginx Web Server
 - iv. Litespeed Web Server
 - v. Apache Tomcat
 - vi. Node.js
 - vii. Lighttpd

D. Mention the benefits and drawbacks of IIS

2. Write answers on the paper or flipchart

3. Present your findings from discussion

4. Follow trainer on expert view

5. Ask any clarifications if any.

6. Remember to read more on key reading 3.1.1 in the trainee's manual



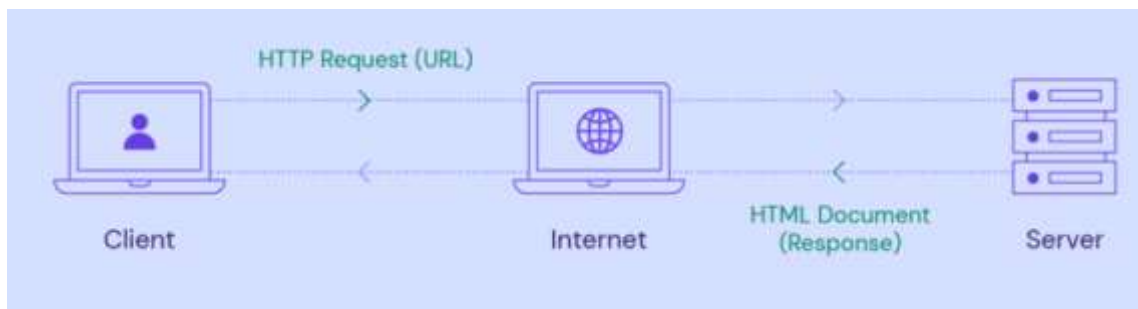
Key readings 3.1.1: Description of web server/hosting platforms

A. Definition of key terms

A web server is a computer that hosts web pages, making them accessible online.

A web server is a computer system capable of delivering web content to end users over the internet via a web browser. It functions by receiving HTTP (Hypertext Transfer Protocol) requests from clients, processing these requests, and delivering the requested resources back to the clients. Web servers are fundamental to the functioning of the World Wide Web, enabling websites and web applications to be accessible to users globally. Popular web server software includes Apache HTTP Server, Nginx, Microsoft Internet Information Services (IIS), and others.

B. IIS stands for Internet Information Services



C. Types of Web Servers/Web hosting Platform

1. IIS (Internet Information Services): Developed by Microsoft, Internet Information Services (IIS), is a web server designed for hosting web pages on Windows and Windows Server.

2. Apache HTTP Server: A free and open-source web server used for many operating systems, including Windows, Linux, and macOS.

3. Nginx (pronounced "Engine-X"): Initially designed only for HTTP web serving, this open-source software now also serves as a reverse proxy, HTTP load balancer, and email proxy. [NGINX](#) is known for its speed and ability to handle multiple connections, making it suitable for high-traffic websites.

4. LiteSpeed Web Server: LiteSpeed is a commercial web server known for its high performance and scalability. It's designed to be a drop-in replacement for Apache while offering better performance, especially under high load conditions.

5. Apache Tomcat: Apache Tomcat is an open-source web server and servlet container developed by the Apache Software Foundation. It's primarily used for deploying Java-based web applications and servlets.

6. Node.js: Node.js is not a traditional web server like the others listed. Instead, it's a JavaScript runtime built on Chrome's V8 JavaScript engine. Developers can use Node.js to build scalable network applications, including web servers, using JavaScript on the server-side.

7. Lighttpd (pronounced "Lighty"): A free and open-source web server software known for its fast data processing with less CPU power. Lighttpd is also popular for its small memory footprint, allowing the server to handle more requests while maintaining responsiveness and performance.

D. Explain benefits and drawbacks of IIS

Some benefits and drawbacks of using Internet Information Services (IIS) in Windows Server:

■ Advantages of IIS:

- 1. Windows Integration:** IIS integrates seamlessly with Windows Server and Active Directory, providing easy management and strong authentication/authorization capabilities within a Windows environment.

2. **Ease of Use:** It offers a user-friendly GUI, making it accessible even for those who are not experienced with command-line interfaces. Extensive documentation and community support further ease the learning process.
 3. **Security:** IIS comes with built-in security features like request filtering, authentication, and SSL certificate support, leveraging Windows security mechanisms like NTFS permissions for enhanced protection.
 4. **Scalability:** IIS is scalable and can handle everything from small websites to large enterprise applications. It supports load balancing and web farms, ensuring high availability and reliability.
 5. **Language Support:** While optimized for ASP.NET, IIS supports other web technologies such as PHP, JavaScript, and classic ASP, making it versatile for various development needs.
 6. **Management Tools:** Administrators can manage IIS servers remotely using IIS Manager, and PowerShell integration allows for automation and scripting, making server management more efficient.
- **Drawbacks (Disadvantages) of IIS:**
1. **Windows Dependency:** IIS is exclusive to Windows operating systems, which can be a limitation for organizations using Linux or other non-Windows systems. Additionally, Windows Server licenses can be costly.
 2. **Resource Intensive:** IIS can be demanding on system resources, particularly when running alongside other Windows services, potentially impacting performance in high-traffic environments.
 3. **Security Risks:** Due to its popularity, IIS is a common target for cyberattacks, necessitating frequent security updates and vigilant configuration to avoid vulnerabilities.
 4. **Learning Curve:** Despite its user-friendly interface, managing IIS, especially in large-scale or complex environments, can be challenging for beginners and may require significant learning.
 5. **Limited Customization:** Compared to open-source web servers like Apache or Nginx, IIS offers fewer third-party modules and plugins, which can limit customization and flexibility.
 6. **Compatibility Issues:** Some older web applications may not fully support the latest versions of IIS, leading to compatibility challenges that may require additional effort to resolve.



Points to Remember

- Description of web server/hosting platforms:
 - A. **A web server** is a computer that hosts web pages, making them accessible online.
 - B. **IIS** stands for Internet Information Services
- Types of Web Servers/Web hosting Platform are: IIS (Internet Information Services), Apache HTTP Server: Apache HTTP Server, Nginx (pronounced "Engine-X"), LiteSpeed Web Server, Apache Tomcat, Node.js, Lighttpd
- **Advantages of IIS are:** Windows Integration, Ease of Use, Security, Scalability and Language Support
- **Drawbacks (Disadvantages) of IIS are:** Windows Dependency, Resource Intensive, Security Risks, Learning Curve, Limited Customization and Compatibility Issues



Indicative content 3.2: Configure IIS with Windows Server



Duration: 4hrs



Practical Activity 3.2.1: Adding Roles and features during IIS configuration



Task:

1. You are requested to go to the computer lab and do the task below individually.

As trainees in L4 Software Development, you install and configure IIS and DNS Server on Windows Server 2022. You enable essential features for IIS, including HTTP functionality, ASP.NET, CGI, and FTP, and set up the DNS Server role. After installation, you verify the configurations by checking the IIS Welcome page and the DNS Server setup.

2. Read key reading 3.2.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 3.2.1: Adding Roles and features during IIS configuration

- Enabling DNS Server

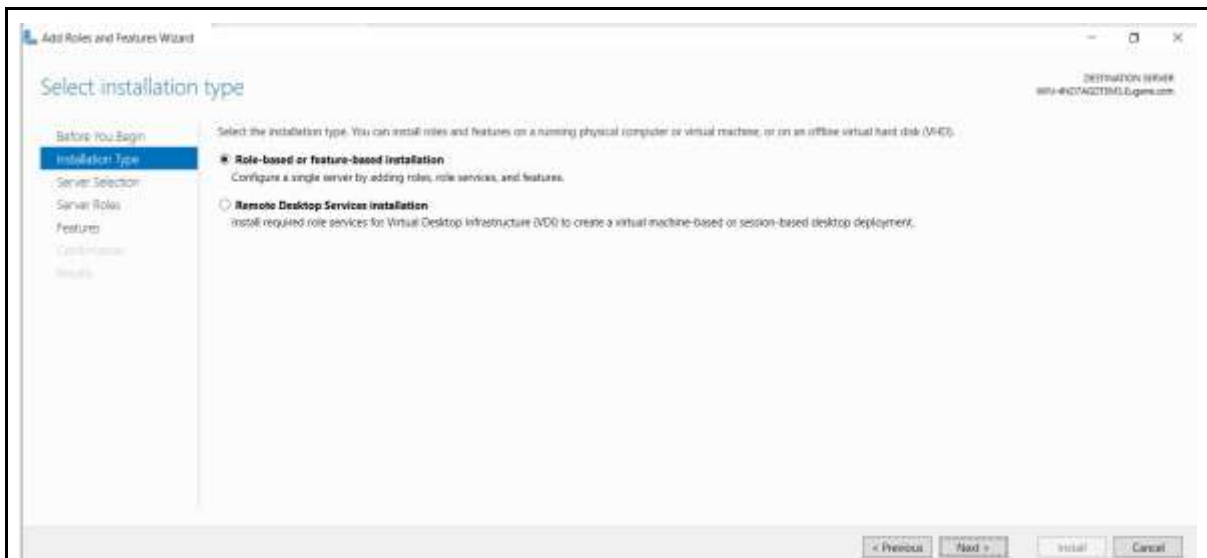
Why would you enable the DNS server when configuring IIS on a Windows Server?

DNS Server Role: DNS is responsible for translating human-friendly domain names (e.g., www.example.com) into IP addresses that computers use to communicate. If your IIS server is going to host websites, enabling DNS allows the server to manage its own domain names or resolve other domain names.

Steps to Enable DNS server in windows server

Step 1. Open **Server Manager** by clicking on the **Start** menu, searching for **Server Manager**, and selecting it.

Step 2. Choose Installation Type: Select **Role-based or feature-based installation** and click **Next**.



step1 Select Destination Server: Choose the server where you want to enable the DNS server, then click **Next**.

step2 Add DNS Server Role: In the Server Roles section, check the DNS Server box. If prompted, add any required features. This will allow your server to resolve domain names and manage DNS zones.

step3 Review and Confirm: After selecting the DNS Server role, review your choices, and click Install to begin the installation process.

step4 Complete Installation: Wait for the installation to complete, and ensure there are no errors.

3.2.1.2. Install IIS Role in selected Server

1. Open Server Manager

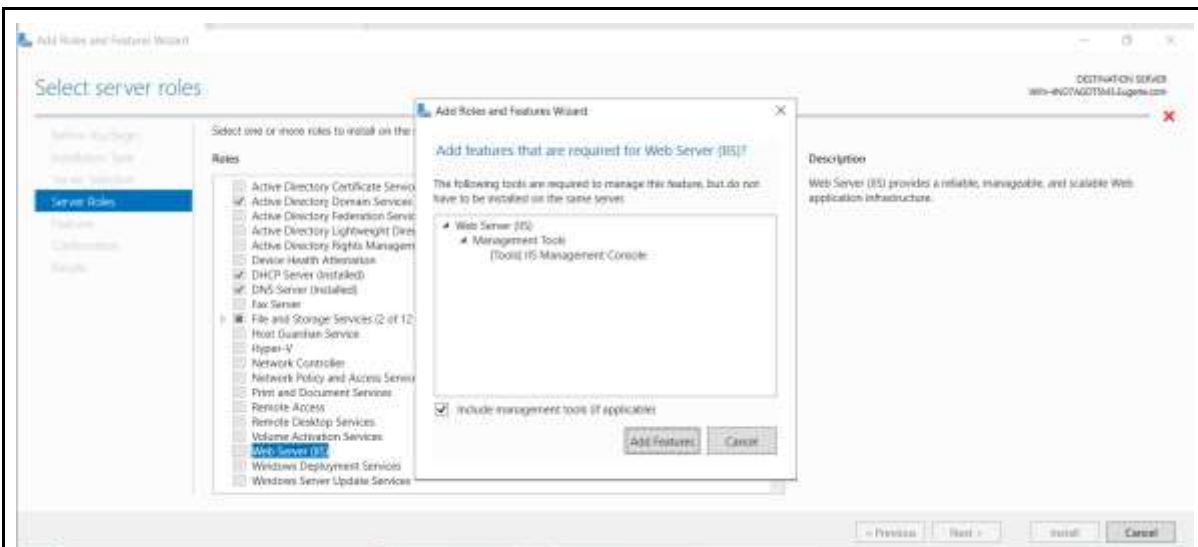
- Log in and open **Server Manager** from the **Start** menu.

2. Add Roles and Features

- Click Manage > Add Roles and Features.
- Click Next until you reach the Roles section.

3. Select Server Roles

- Check Web Server (IIS).
- Click Add Features when prompted, then click Next.



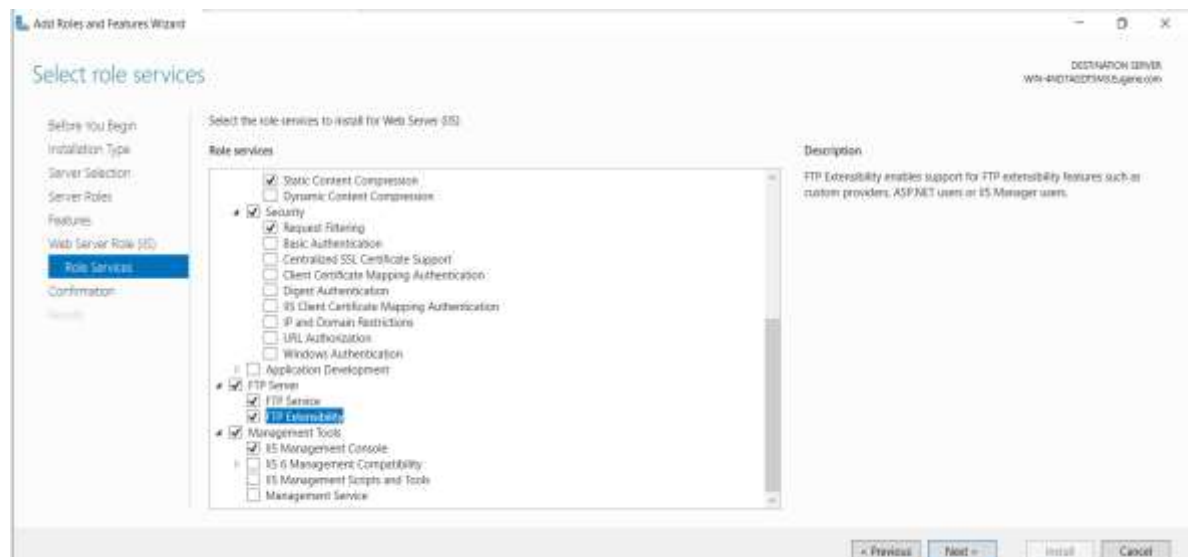
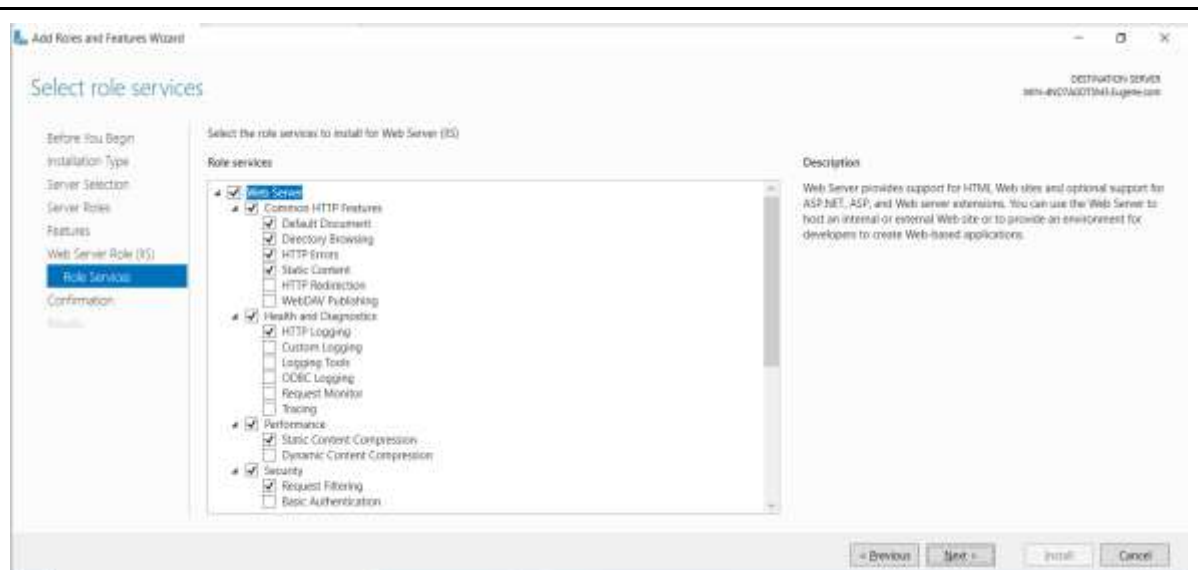
4. Skip Features Selection

- On the **Select features** page, click **Next**.

5. Configure IIS Role Services

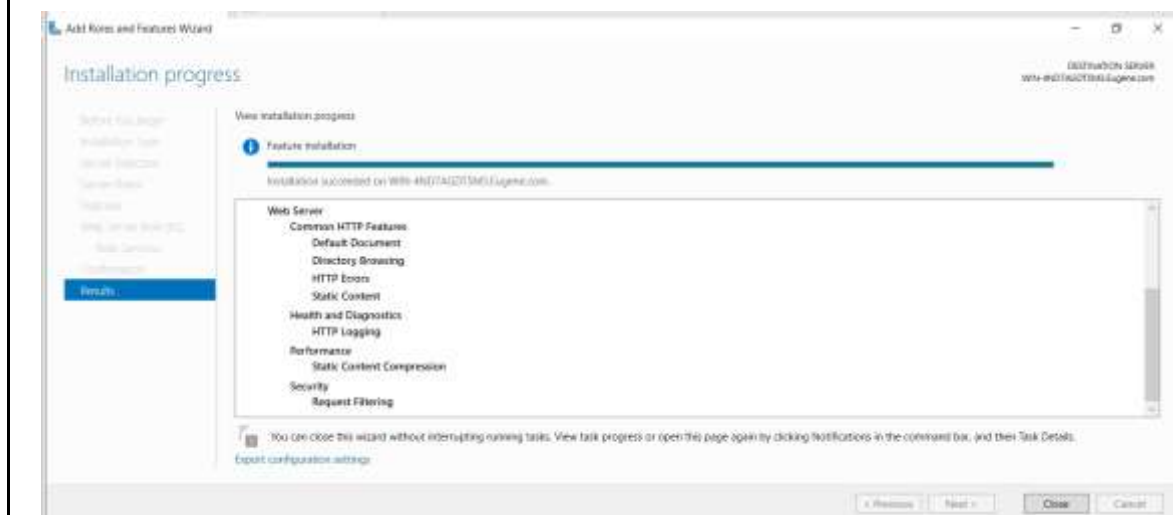
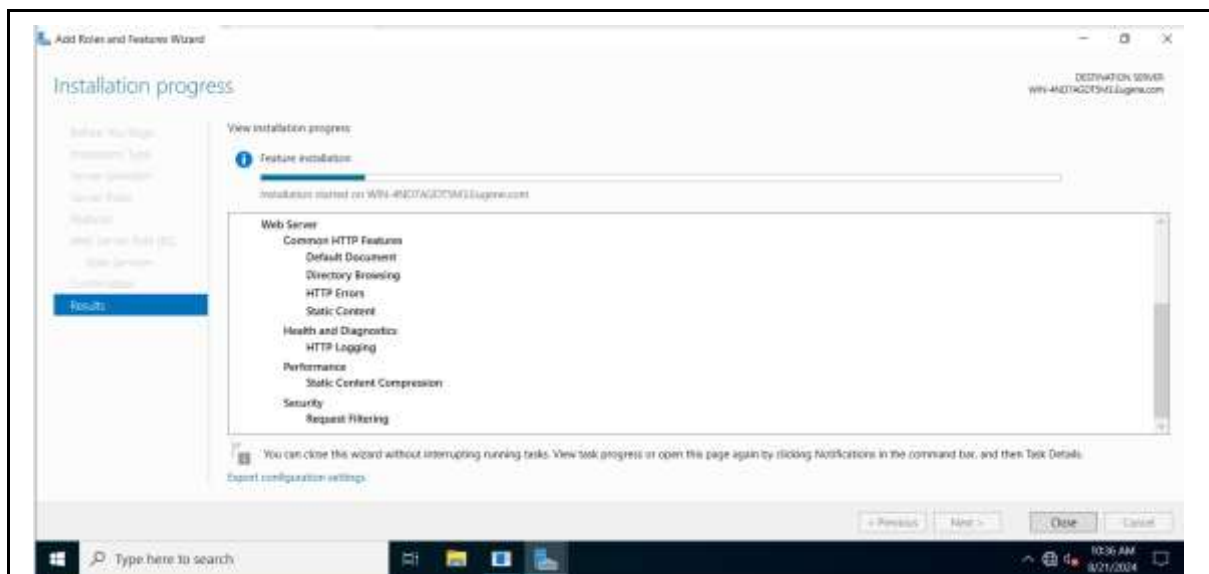
- Click Next on the Web Server Role (IIS) page.
- Under Role Services:
 - ✓ **Enable HTTP Features:** Default Document, Directory Browsing, HTTP Errors, Static Content.
 - ✓ **Enable ASP.NET:** Select ASP.NET version (e.g., ASP.NET 4.8).
 - ✓ **Enable CGI Interface:** Check CGI.
 - ✓ **Add FTP Feature:** Check FTP Service and FTP Extensibility.
 - ✓ **Enable HTTP Health and Diagnostics:** Check HTTP Logging and Request Monitor.
- Click **Next**.





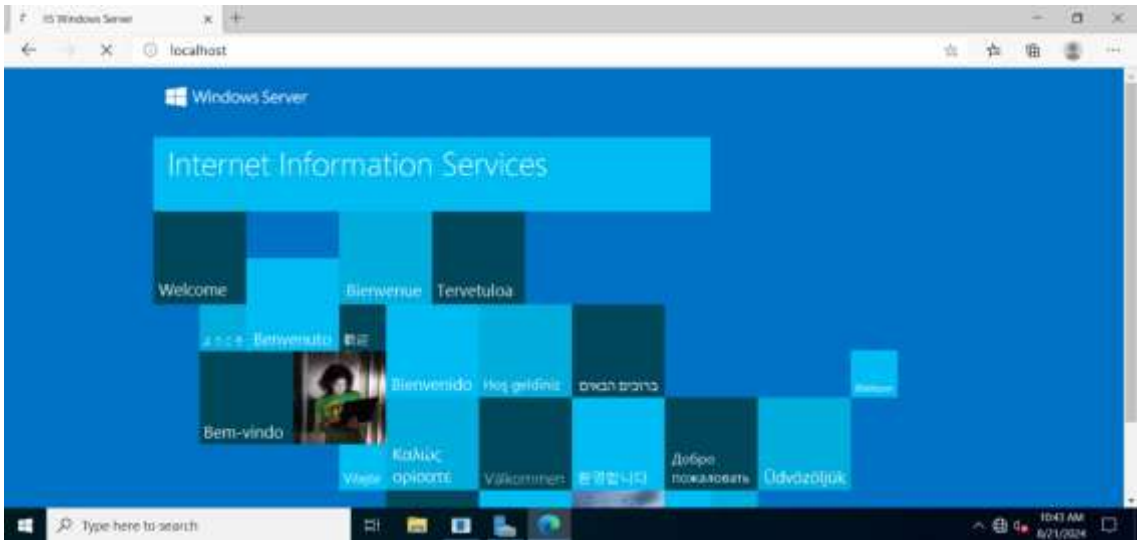
6. Confirm and Install

- Review selections on the confirmation page and click **Install**.
- Wait for the installation to complete, then click **Close**.



7. Verify IIS Installation

- Open a web browser and navigate to “<http://localhost>” or “http://<Server_IP_Address>” to see the IIS Welcome page.



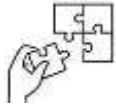
8. Check IIS Features

- Open IIS Manager from Server Manager > Tools.
- Verify the enabled features in IIS Manager.



Points to Remember

- DNS is responsible for translating human-friendly domain names into IP addresses that computers use to communicate.
- **Steps to Enable DNS server in windows server**
 - ✓ Open Server Manager
 - ✓ Choose Installation Type
 - ✓ Select Destination Server
 - ✓ Add DNS Server Role
 - ✓ Review and Confirm
 - ✓ Complete Installation
- **Steps to Install IIS Role in selected Server**
 - ✓ Open Server Manager: Log in and open Server Manager from the Start menu.
 - ✓ Add Roles and Features
 - ✓ Select Server Roles
 - ✓ Skip Features Selection > On the Select features page, click Next.
 - ✓ Configure IIS Role Services: Click Next on the Web Server Role (IIS) page.
 - ✓ Confirm and Install
 - ✓ Verify IIS Installation



Application of learning 3.2.

FFF Ltd company, located in Gicumbi District, Northern Province, FFF Ltd has a problem that there no way to configure their IIS with windows server hence, they need to install and configure IIS and DNS Server on Windows Server the access to their system they have recently developed so that all users in the company will be able to access it from webpage and DNS server. As an IT technician, you are hired by FFF Ltd to install and configure IIS and DNS Server on Windows Server



Indicative content 3.3: Management of IIS Web Server



Duration: 4hrs



Theoretical Activity 3.3.1: Explanation of handler mapping



Tasks:

1. You are requested to answer the following questions:
 - a. Explain handler mapping
 - b. Discuss on different types of requests
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 3.3.1 in the trainee's manual



Key readings 3.3.1: Explanation of handler mapping

- A. **Handler mapping in Windows Server:** Refers to the process of associating specific actions or handlers with particular types of requests in Internet Information Services (IIS). In simpler terms, it's like telling the server how to respond to different types of requests.
- B. **The types of requests**
 1. **Incoming Request:** When a request is made to the server (e.g., a request for a webpage), the server needs to know how to handle that request.
 2. **Handler Mapping:** is the mechanism by which IIS determines which module or program should handle a particular type of request. This mapping is usually based on the file extension or the URL of the request.
 3. **Mapping Rules:** In Windows Server, you can define mapping rules in the IIS Manager. These rules specify which handler should process requests for specific file types, directories, or URLs.
 4. **Choosing the Handler:** Once a request comes in, IIS checks its handler mappings to determine which handler should process the request. This handler could be a built-in IIS module, an ISAPI extension, a CGI script, or a custom program.
 5. **Processing the Request:** The chosen handler then processes the request according to its logic. For example, if the request is for a static HTML file, IIS might use a built-in handler to serve the file directly
 6. **Sending Response:** Finally, the handler generates the appropriate response (e.g., HTML content) and sends it back to the client that made the request.



Theoretical Activity 3.3.2: Explanation of Connection tasks

Tasks:

1. You are requested to answer the following questions:
 - a. Explain Connection tasks
 - b. Discuss on at least three (3) common connection tasks in Windows Server
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 3.3.2 in the trainee's manual



Key readings 3.3.2: Explanation of Connection tasks

- **Connection tasks** in Windows Server typically refer to various activities related to managing network connections, remote access, and communications within a network environment. These tasks encompass a range of activities aimed at configuring, monitoring, and troubleshooting network connections to ensure smooth operation and security.

Breakdown of some common connection tasks in Windows Server:

1. **Network Configuration:** This involves setting up and configuring network interfaces, IP addresses, subnets, and other network settings on the server.
2. **Remote Access Configuration:** Windows Server allows remote access to resources and services through protocols like Remote Desktop Protocol (RDP), Virtual Private Network (VPN), or Secure Shell (SSH).
3. **Firewall Configuration:** Windows Server includes a built-in firewall that helps protect the server from unauthorized access and malicious network traffic
4. **Network Monitoring and Troubleshooting:** Connection tasks also include monitoring network performance, identifying bottlenecks or connectivity issues, and troubleshooting network problems.
5. **DNS Configuration:** Domain Name System (DNS) is crucial for translating human-readable domain names into IP addresses.
6. **Active Directory Integration:** In a Windows Server environment, Active Directory (AD) is used for centralized authentication and management of network resources.
7. **Virtual Networking:** With technologies like Hyper-V, Windows Server allows for virtualization of networking resources, enabling the creation and management of virtual networks, switches, and network adapters.



Theoretical Activity 3.3.3: Explanation of FTP protocol



Tasks:

1. You are requested to answer the following questions:
 - a. Explain in detail the use of FTP protocol
 - b. Differentiate Authentication and Authorization as two vital information security
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 3.3.3 in the trainee's manual



Key readings 3.3.3: Explanation of FTP protocol

- A. **FTP (File Transfer Protocol)** is a standard network protocol used for the transfer of files between a client and a server on a computer network. In Windows Server, you can set up an FTP server using the built-in Internet Information Services (IIS) role.

General overview of how to set up FTP in Windows Server using IIS:

1. **Install the FTP Server Role:** You can do this through the Server Manager. Go to "Add Roles and Features" and select the FTP Server role.
2. **Configure FTP Site:** After installing the FTP Server role, you need to configure an FTP site. Open the Internet Information Services (IIS) Manager, right-click on "Sites," and select "Add FTP Site." Follow the wizard to specify a site name, physical path (where files will be stored), and bindings (IP address and port).
3. **Specify FTP Authentication:** Decide on the authentication method for your FTP site. You can choose between Anonymous Authentication, Basic Authentication, or Windows Authentication.
4. **Configure Authorization:** Determine who has access to your FTP site and what level of access they have. You can configure authorization rules based on user accounts or groups.
5. **Set Up Firewall Rules:** Ensure that the necessary firewall rules are in place to allow FTP traffic through. This typically involves opening port 21 for control connections and additional ports for data connections if you're using passive FTP.
6. **Test Your FTP Site:** Once configured, you can test your FTP site by connecting to it using an FTP client such as FileZilla or the command-line FTP client built into Windows.

7. **Monitor and Maintain:** Regularly monitor your FTP server for performance, security, and any potential issues. You may need to adjust settings or apply updates as necessary.

A. Difference between Authentication and Authorization

Authentication is the process of verifying who a user is, while **Authorization** is the process of verifying what they have access to.



Theoretical Activity 3.3.4: Explanation of Site binding used by HTTP or HTTPS protocols

Tasks:

1. You are requested to answer the following question:
 - a. Explain Site binding used by HTTP or HTTPS protocols
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to read more on key reading 3.3.4 in the trainee's manual



Key readings 3.3.4: Explanation of Site binding used by HTTP or HTTPS protocols

Site binding is a configuration setting used primarily with Internet Information Services (IIS), which is Microsoft's web server software.

Bindings are a collection of elements that define how your website will be accessed.

1. **Domain Name:** With HTTP or HTTPS site binding, you can associate each website hosted on the server with one or more domain names.
2. **IP Address:** You can also bind websites to specific IP addresses on the server.
3. **Port Number:** In addition to IP addresses, you can bind websites to specific port numbers on the server. By default, HTTP uses port 80, and HTTPS uses port 443.
4. **Protocol (HTTP or HTTPS):** Site binding allows you to specify whether a website should handle HTTP requests, HTTPS requests, or both.



Practical Activity 3.3.5: Configuration of site binding of HTTP or HTTPS Protocols



Task:

1. As trainee you are requested to perform the following activity individually:
As trainees in L4 Software Development, you configure site bindings for HTTP or HTTPS protocols in Windows Server, you typically use Internet Information Services (IIS)
2. Read the key readings 3.3.5 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

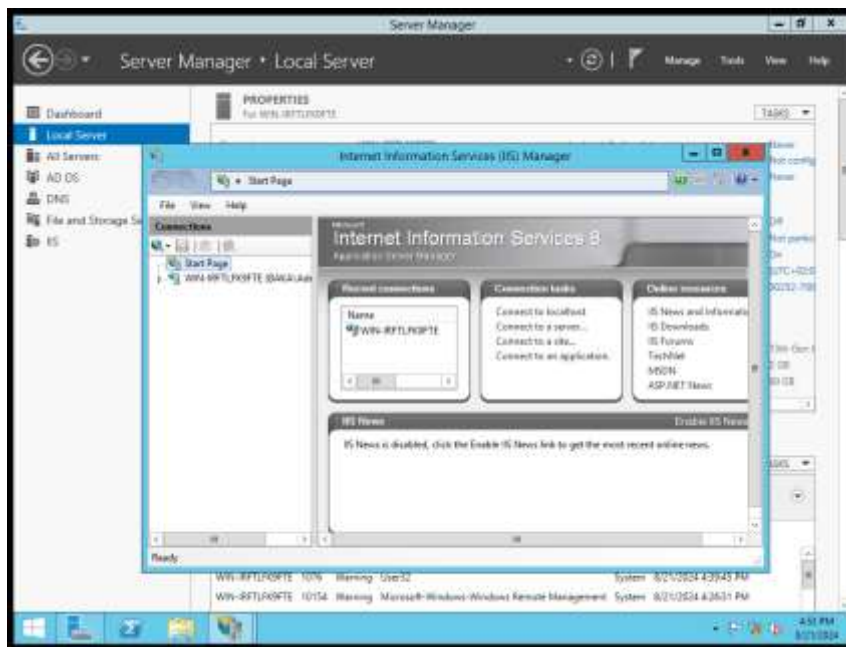


Key readings 3.3.5: Configuration of site binding of HTTP or HTTPS Protocols

To configure site bindings for HTTP or HTTPS protocols in Windows Server, you typically use Internet Information Services (IIS).

Here's how you can do it:

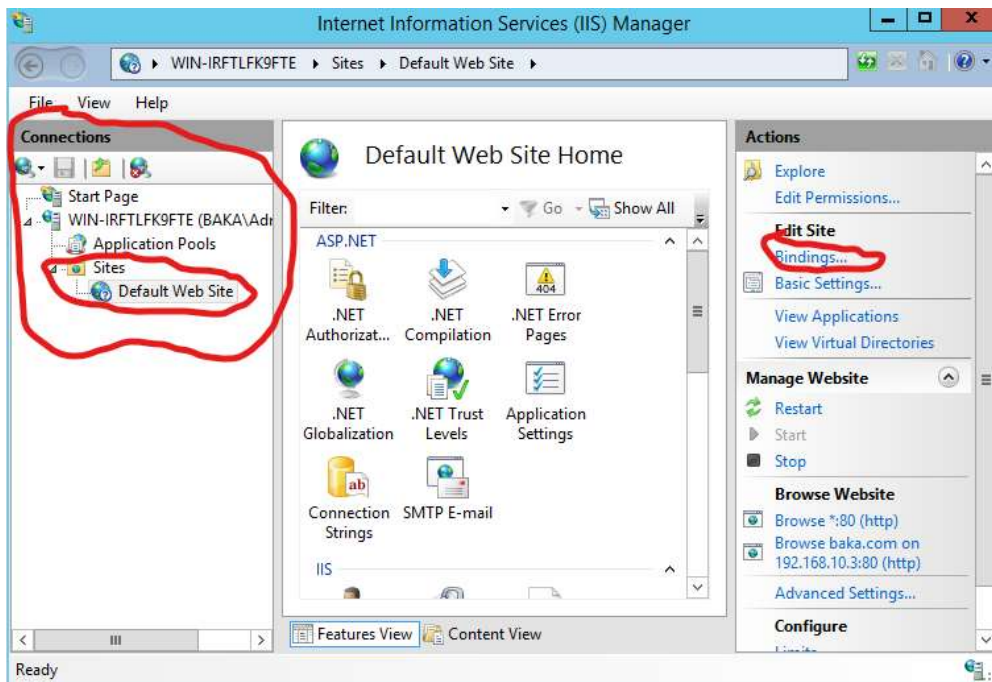
1. Open Internet Information Services (IIS) Manager:
 - You can open it by searching for "IIS" in the Start menu or by typing inetmgr in the Run dialog box (Win + R) and pressing Enter.



2. Select Your Website:

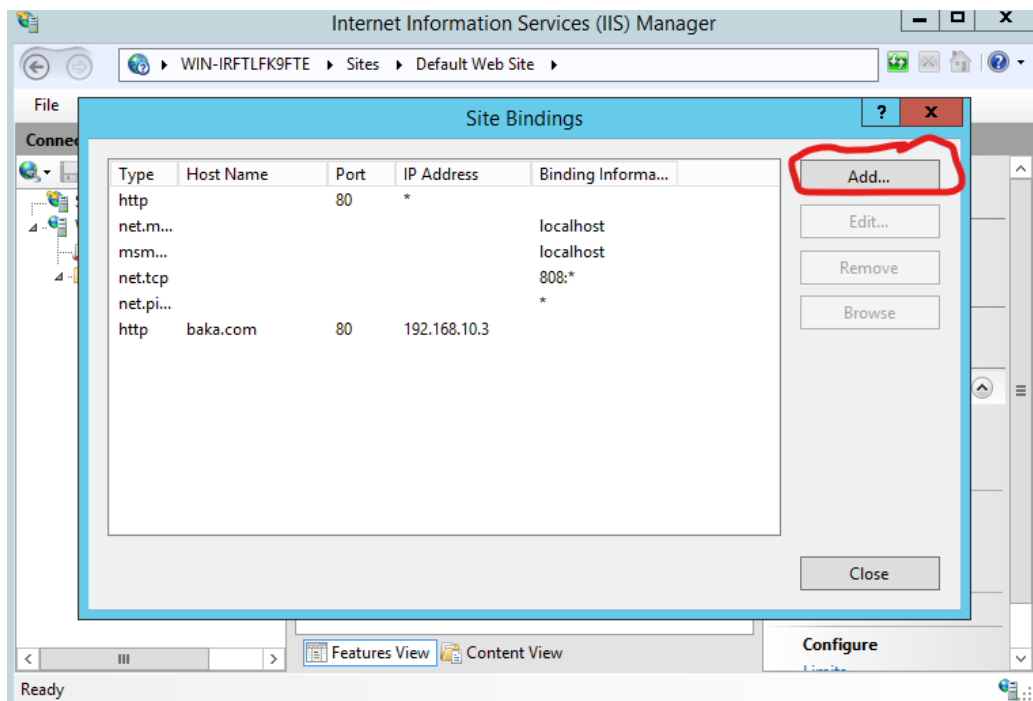
- In the Connections pane on the left-hand side, navigate to the site you want to

configure bindings for, and click on it to select it.



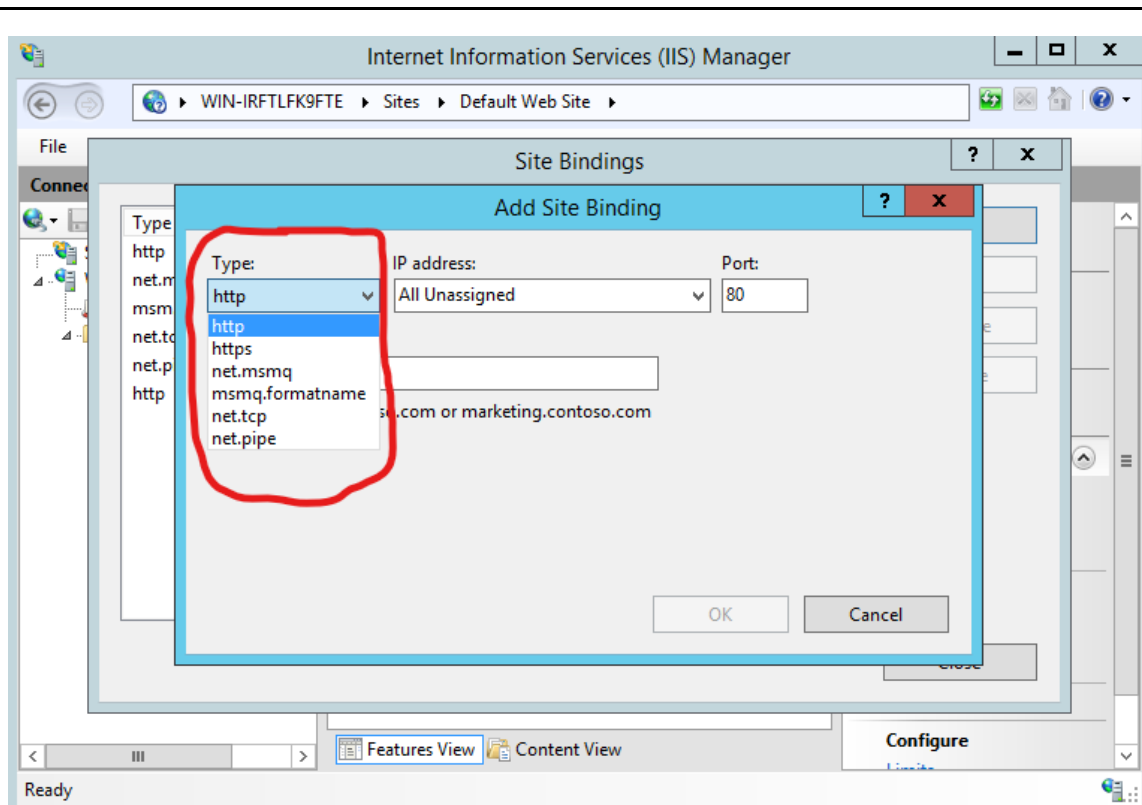
3. Add a Binding:

- In the Actions pane on the right-hand side, click on "Bindings."
- In the Site Bindings window, click "Add..." to add a new binding.



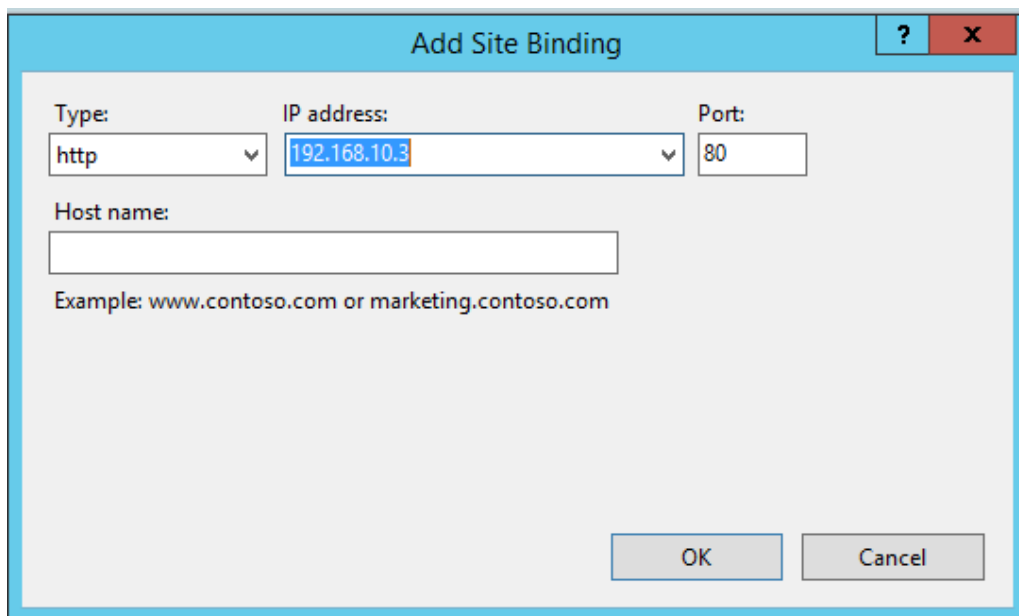
4. Choose Protocol:

- Select either HTTP or HTTPS, depending on your requirements.



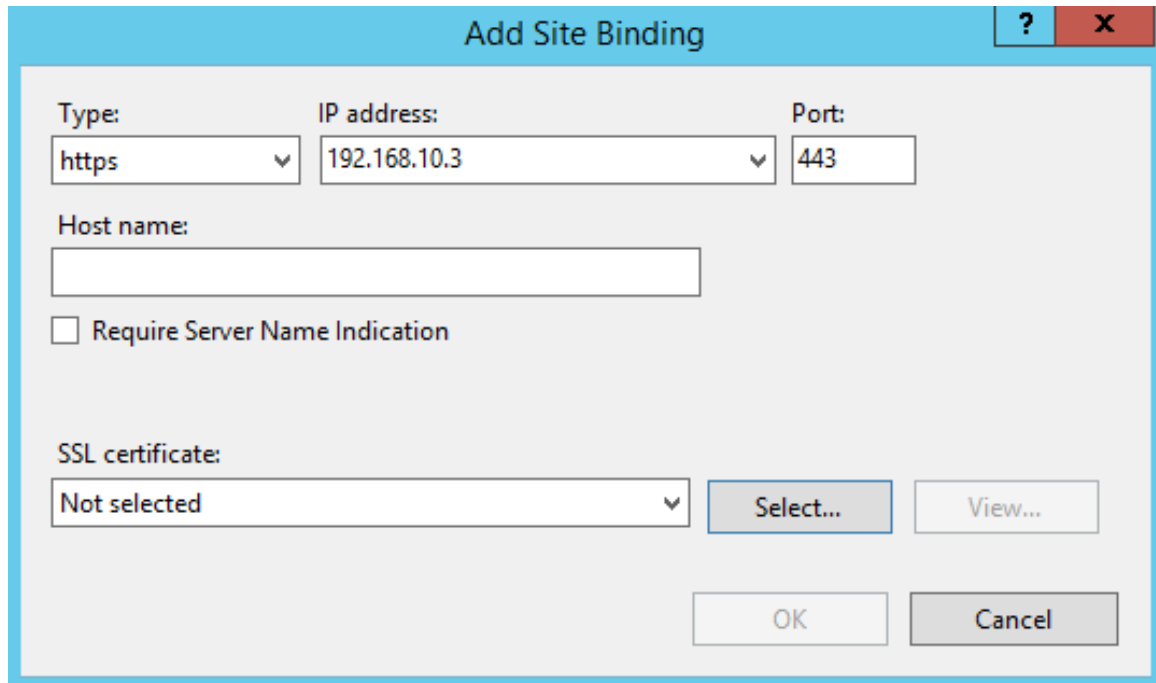
5. Specify IP Address and Port:

- If you have multiple IP addresses configured on your server, choose the appropriate one from the drop-down menu. Otherwise, leave it as "All Unassigned."
- Enter the port number. For HTTP, the default port is 80. For HTTPS, it's usually 443.



6. Select SSL Certificate (if configuring HTTPS):

- If you're configuring an HTTPS binding, you'll need to select an SSL certificate. If you haven't installed one yet, you'll need to do so before this step.

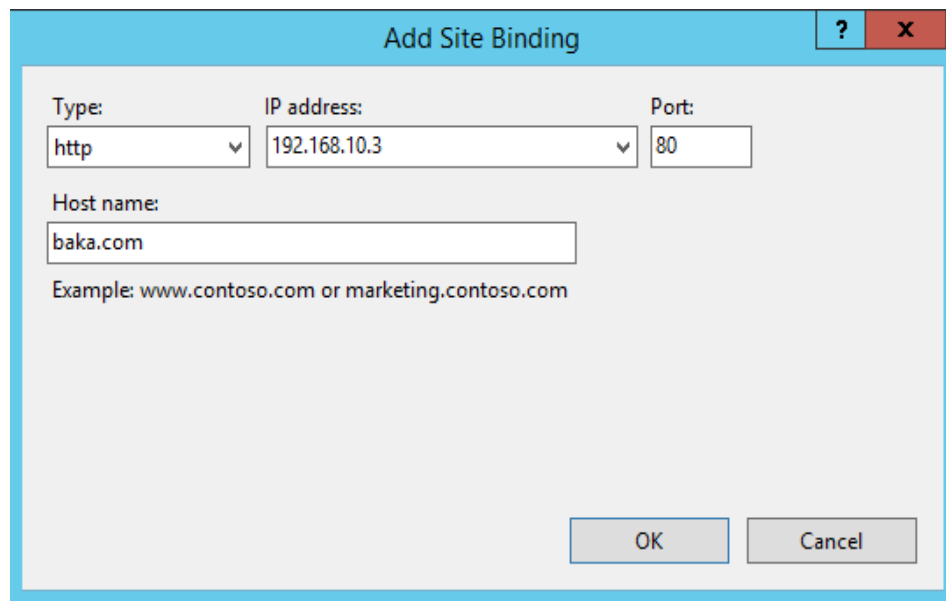


The screenshot shows the 'Add Site Binding' dialog box. It has a title bar with a question mark and a close button. The dialog contains the following fields and controls:

- Type:** A dropdown menu with 'https' selected.
- IP address:** A text box containing '192.168.10.3'.
- Port:** A text box containing '443'.
- Host name:** An empty text box.
- Require Server Name Indication:** An unchecked checkbox.
- SSL certificate:** A dropdown menu with 'Not selected' selected.
- Select...** and **View...** buttons next to the SSL certificate dropdown.
- OK** and **Cancel** buttons at the bottom right.

7. Host Name (Optional for HTTPS):

- If you want to configure host headers, you can specify the host name for the site. This is optional for HTTP but often required for HTTPS bindings if you're hosting multiple websites on the same IP address.

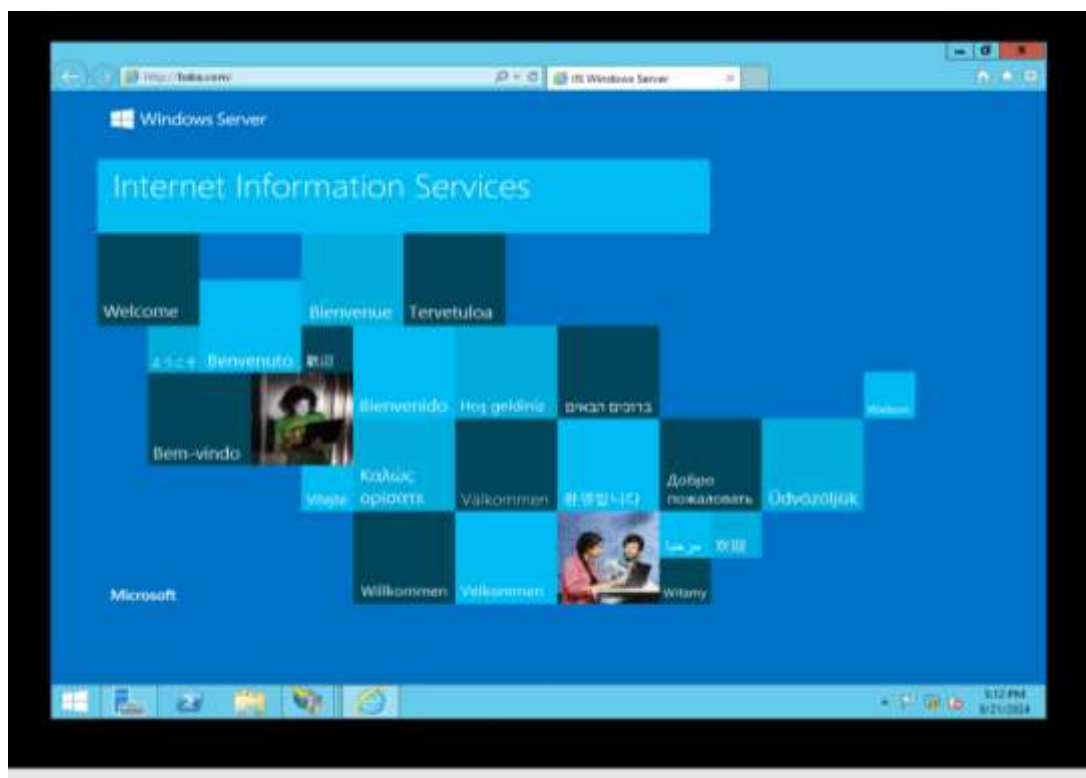


8. Apply and OK:

- Click "OK" to save the binding configuration.

9. Restart the Website:

- After adding or modifying bindings, it's a good practice to restart the website to apply the changes. You can do this by selecting the website in IIS Manager and then clicking "Restart" in the Actions pane.





Points to Remember

Explanation of handler mapping

- **Handler mapping in Windows Server** refers to the process of associating specific actions or handlers with particular types of requests in Internet Information Services (IIS).

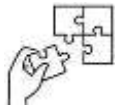
Explanation Connection tasks

- **Connection tasks** in Windows Server typically refer to various activities related to managing network connections, remote access, and communications within a network environment.

Breakdown of some common connection tasks in Windows Server:

- ✓ Network Configuration
- ✓ Remote Access Configuration
- ✓ Firewall Configuration
- ✓ Other connection tasks are: Network Monitoring and Troubleshooting, DNS Configuration, Active Directory Integration, Virtual Networking.
- Explanation FTP protocol
- ✓ **FTP (File Transfer Protocol)** is a network protocol used to transfer files between a client and a server over a TCP/IP network.
- ✓ **Authentication vs Authorization**
Authentication is the process of verifying who a user is, while Authorization is the process of verifying what they have access to.
- Explanation Site binding used by HTTP or HTTPS
- ✓ **Site binding** is a configuration setting used primarily with Internet Information Services (IIS), which is Microsoft's web server software. Here's how it works:
- ✓ Domain Name: With HTTP or HTTPS site binding, you can associate each website hosted on the server with one or more domain names.
- ✓ IP Address: You can also bind websites to specific IP addresses on the
- ✓ server.
- ✓ Port Number: By default, HTTP uses port 80, and HTTPS uses port 443. However, you can configure IIS to listen on alternative ports if needed.
- ✓ Protocol (HTTP or HTTPS): Site binding allows you to specify whether a website should handle HTTP requests, HTTPS requests, or both.
- To configure site bindings for HTTP or HTTPS protocols in Windows Server (IIS) follow steps below:

- ✓ Open Internet Information Services (IIS) Manager: You can open it by searching for "IIS" in the Start menu or by typing inetmgr in the Run dialog box (Win + R) and pressing Enter.
- ✓ Select Your Website
- ✓ Add a Binding
- ✓ Choose Protocol (HTTP or HTTPS)
- ✓ Specify IP Address and Port
- ✓ Select SSL Certificate (if configuring HTTPS)
- ✓ Host Name (Optional for HTTPS)
- ✓ Apply and OK
- ✓ Restart the Website



Application of learning 3.3.

FFF Ltd company, located in Gicumbi District, Northern Province, FFF Ltd has a problem that there no way to configure site binding of HTTP or HTTPS Protocols hence, they need to site binding of HTTP or HTTPS Protocols in Windows Server the access to their system they have recently developed so that all users in the company will be able to access it from site. As an IT technician, you are hired by FFF Ltd to configure site bindings for HTTP or HTTPS protocols in Windows Server.



Indicative content 3.4: Setting Environment of Developed Web App



Duration: 4hrs



Theoretical Activity 3.4.1: Describing web hosting platforms



Tasks:

1. You are requested to answer the following questions:
 - i. How would you define web hosting?
 - ii. What are the key differences between free and paid hosting platforms? provide 4 examples of each type.
 - iii. What are the key technical requirements for hosting a website that involves backend functionalities, and what are some examples of popular database clients that may be needed?
 - iv. How do the technical requirements differ between hosting a dynamic website with backend server support and a static website without backend server needs?
2. Write answers on the paper or flipchart
3. Present your findings from discussion
4. Follow trainer on expert view
5. Ask any clarifications if any.
6. Remember to ready more on key reading 3.4.1 in the trainee's manual



Key readings 3.4.1: Describing web hosting platforms

A. Web hosting is an online service that makes your website's content accessible on the internet. We have two main hosting platforms:

B. Free hosting Vs Paid hosting

Free hosting: Free hosting is when a web hosting company provides free access to web domains and hosting. Small businesses, startups, and personal bloggers are the primary audience for free hosting.

can be a good starting point for small, personal projects with low traffic and limited budgets. However, it typically comes with ads, limited storage and bandwidth, and less reliable performance.

Below is a list of examples of host providers that offers free hosting:

1. **WordPress.com:** WordPress.com offers free hosting with easy-to-use website building tools. Users can create blogs and basic websites without technical expertise.

2. **Wix.com:** Wix provides a free hosting option with a user-friendly website builder. It's known for its drag-and-drop design capabilities.
 3. **Weebly.com:** Weebly offers a free hosting plan that allows users to create simple websites and online stores using a simple website builder.
 4. **Blogger.com:** Blogger is a free blogging platform by Google. Users can create and publish blogs with ease.
 5. **000WebHost.com:** 000WebHost offers free web hosting with no ads. It's suitable for users looking for a more ad-free experience.
- Others are: X10Hosting.com, Bravenet.com, 5GBFree.com, Freehostia.com, FreeWebHostingArea.com

Paid hosting: Paid hosting is when you pay a fee for a web hosting services provider to host your website on their dedicated servers.

on the other hand, offers better performance, security, and reliability. It also provides more customization options, reliable customer support, and the ability to scale your website as it grows.

The following is a list of examples of popular web hosting providers (paid web hosting platform): BlueHost, HostGator, Namecheap, InMotion, GoDaddy, Hostinger, SiteGround, Digital Ocean.

C. Analysis of technical requirements for each hosting platforms:

Requirements of hosting platforms varies according to the website to host; the technologies used to develop the website, the amount of data to be processed, the script support required and many more other factors that defines the compatibility between your created website and your hosting server. If your website possesses a database, then you will need a host whose server supports backend functionalities otherwise, database server will not be required.

1. Hosting with backend server

All of the elements required for the website or application to perform as it should are the backend developer's responsibility. The backend consists of three parts: a server, an application, and a database.

Depending on the platform selected, the following is a list of popular database clients as requirements according to your chosen platform.

1. MySQL
2. Microsoft SQL Server
3. PostgreSQL
4. MONGO DB
5. Oracle
6. SQLite
7. PL/SQL

Dynamic Websites: Requires a server to process requests, manage databases, and execute backend code.

Requirements: Server hosting for PHP, Node.js, Python, or other backend languages; database support like MySQL, PostgreSQL.

2. Hosting without backend server

A website which only requires displaying pre-defined data essentially does not require any back-end logic. These websites are usually called static websites and does not require backend servers during their hosting processes, therefore the requirements are minimal: No database server required, disk space is minimal and load time may increase.

A few examples for such websites could be:

1. A website about a company.
2. A personal portfolio.
3. An events page.
4. An online journal/newspaper.

Static Websites: Suitable for free hosting or basic paid plans.

Requirements: HTML, CSS, JavaScript files, no need for server-side processing.



Practical Activity 3.4.2: Verifying a local web app and configuring backend

Technology in IIS web server

Task:

1. You are requested to go to the computer lab and do the task below individually:
Set up and verify a local web application stored in a folder named **“test1site”**, which contains an **“index.html”** file displaying the message **“Hello L4 SOD.”** Your goal is to ensure that this web app operates correctly in your local environment using IIS before it is deployed to a production server.
2. Read the key readings 3.4.2 in trainee’s manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

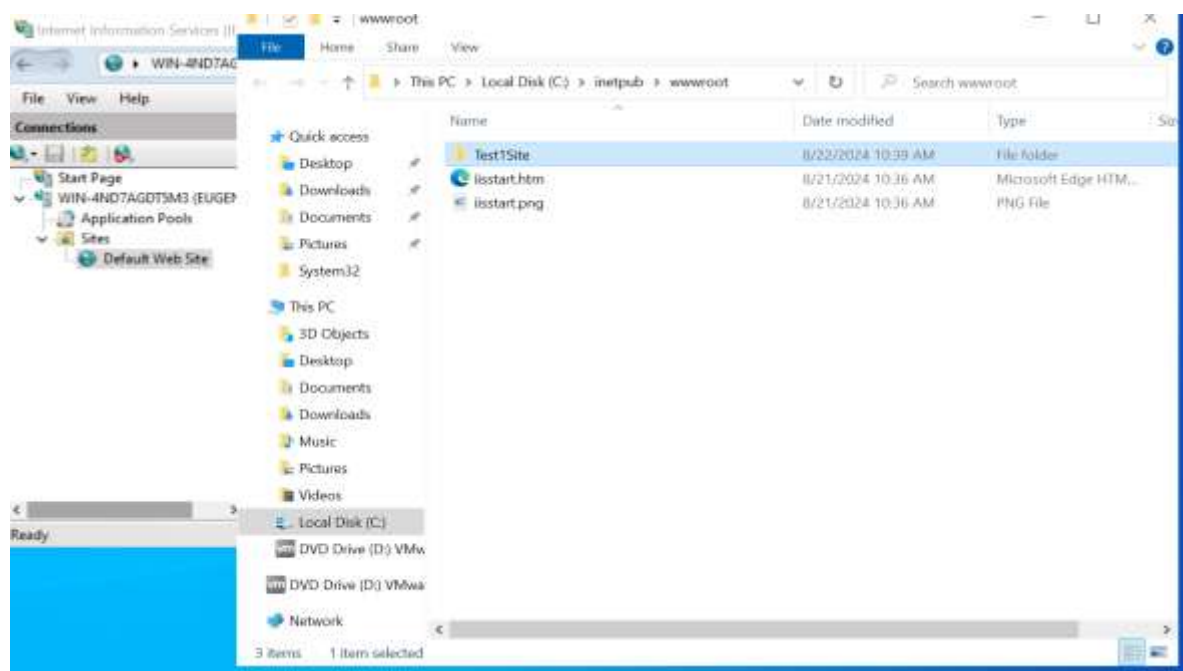


Key readings 3.4.2: Verification of Local Web App to Be Deployed to the Server

Step1. Prepare Your Local Environment

1. Ensure that IIS is installed and running on your local machine
2. Create a Local Directory for Your Web App:

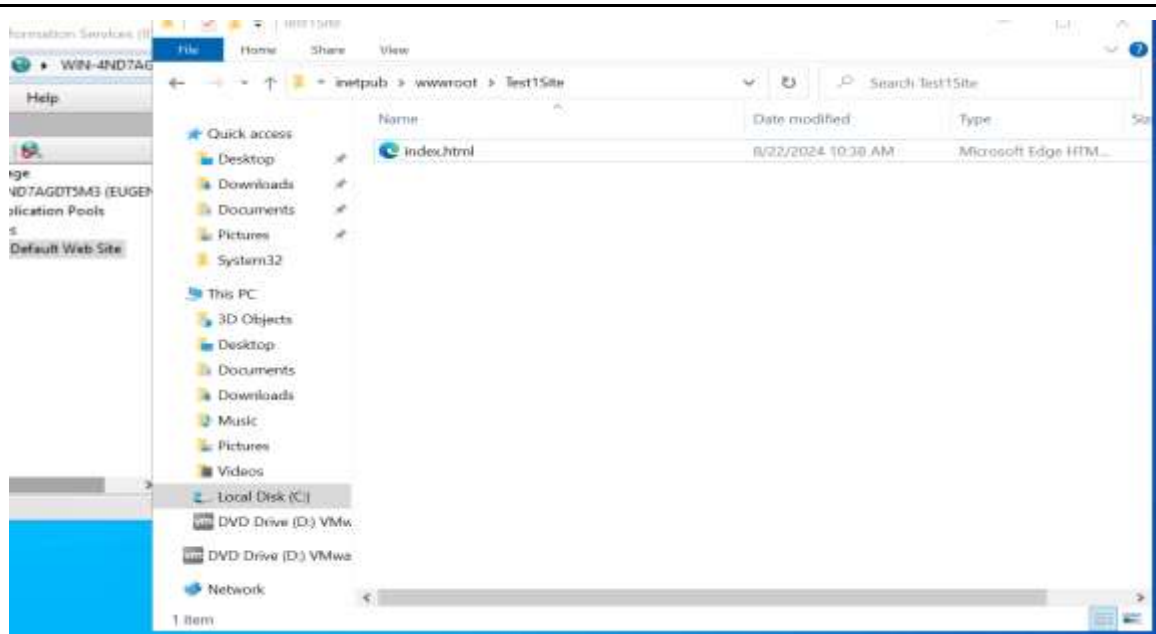
Create a directory named **test1site** where you'll place your web app files. For example: **"C:\inetpub\wwwroot\test1site."**



Step2. Deploy Web App Locally

1. Create Your Web App Files

Inside the **test1site** directory, create an **index.html** file with the following content:



Step3. Configure IIS for Local Verification

Open IIS Manager:

1. Go to **Start → Administrative Tools → Internet Information Services (IIS) Manager**.

2. Create a New Site:

In IIS Manager, right-click on Sites in the left panel and select Add Website.

- Site name: **Test1Site**
- Physical path: **C:\inetpub\wwwroot\test1site**
- Binding: Set the type to **http**, and **assign a port** (e.g., 80 if it is free). You can leave the hostname empty for local testing.
- Click **OK** to create the site.

Site name: Application pool:

Content Directory

Physical path:

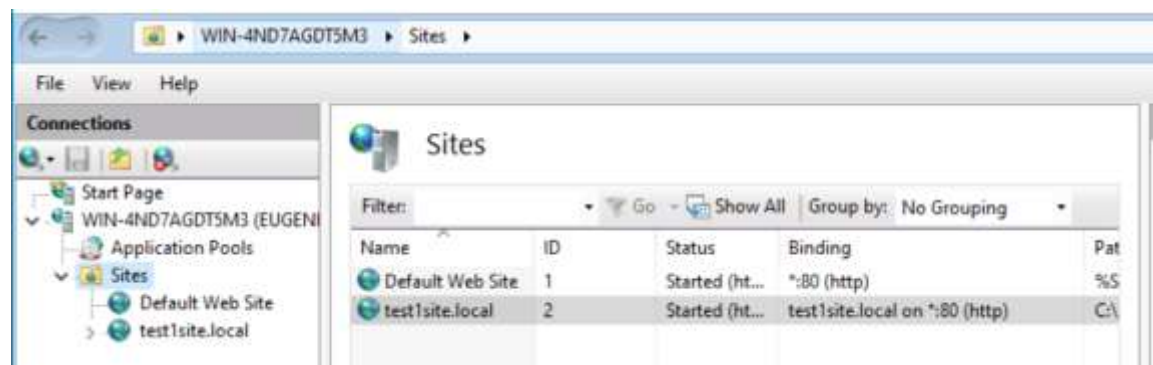
Pass-through authentication

Binding

Type: IP address: Port:

Host name:

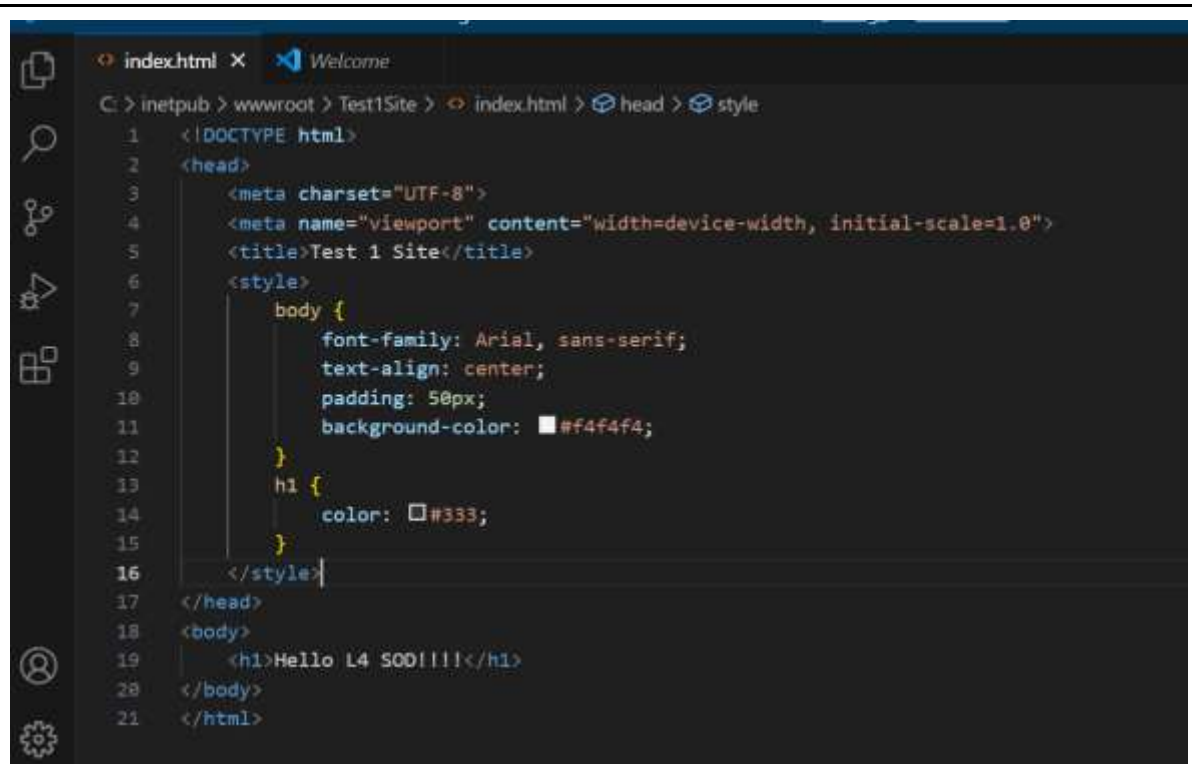
Example: www.contoso.com or marketing.contoso.com



Name	ID	Status	Binding	Pat
Default Web Site	1	Started (ht...	*:80 (http)	%S
test1site.local	2	Started (ht...	test1site.local on *:80 (http)	C:\

3. Set Default Document:

- In **IIS Manager**, select your new site (**Test1Site**) from the list.
- In the central panel, double-click on **Default Document**.
- Ensure that **index.html** is listed. If not, click **Add** and enter **index.html**.



```
1 <!DOCTYPE html>
2 <head>
3   <meta charset="UTF-8">
4   <meta name="viewport" content="width=device-width, initial-scale=1.0">
5   <title>Test 1 Site</title>
6   <style>
7     body {
8       font-family: Arial, sans-serif;
9       text-align: center;
10      padding: 50px;
11      background-color: #f4f4f4;
12    }
13    h1 {
14      color: #333;
15    }
16  </style>
17 </head>
18 <body>
19   <h1>Hello L4 SOD!!!</h1>
20 </body>
21 </html>
```

Step4. Test the Web App Locally

1. Open a Web Browser:

- Navigate to <https://localhost> or <http://localhost:80> (if you used port 80).

2. Verify the Output:

- You should see the **index.html** page with the message "Hello L4 SOD" displayed.



3. Troubleshooting:

- If the web page does not load, check IIS logs for errors.
- Ensure that the "test1site" folder and files have the correct permissions.
- Verify that IIS is configured correctly and that no other site is using the same port.

3.4.2.2. Configuration of backend technology in IIS web Server

1. PHP Environment Variables

- Go to Control Panel → System and Security → System → Advanced system settings → Environment Variables.
- Add a new system variable:
 - i. Variable name: PHPRC,

- ii. Variable value: Path to php.ini (e.g., C:\PHP\php.ini).

2. Configure WinCache for PHP

A. Download and Install WinCache: Obtain WinCache from the PHP website or PECL.

B. Update php.ini: Add extension=php_wincache.dll to php.ini.

C. Restart IIS: Open **IIS Manager** and restart the server.

3. FastCGI Handler Mapping for PHP

A. Open IIS Manager: Go to **Server** → **Handler Mappings**.

B. Add FastCGI Handler: Click **Add Module Mapping**:

- Request path: *.php
- Module: FastCGIModule
- Executable: Path to php-cgi.exe (e.g., C:\PHP\php-cgi.exe)
- Name: PHP_via_FastCGI

C. Click **OK** and restart IIS.

4. IISNode Module for Node.js

A. Install IISNode: Download and install IISNode.

B. Add Node.js Handler:

- In **IIS Manager**, select the server node.
- Go to **Handler Mappings** and click **Add Module Mapping**:
- **Request path:** *.js
- **Module:** iisnode
- **Executable:** Path to iisnode.dll (e.g., C:\Program Files\iisnode\iisnode.dll)
- **Name:** Node.js

Click **OK**

C. Create web.config for Node.js: Add the following content to “**web.config**” in your site's root directory:

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <configuration>
3      <system.webServer>
4          <handlers>
5              <add name="iisnode" path="app.js" verb="*" modules="iisnode" />
6          </handlers>
7          <iisnode watchedFiles="web.config;*.js" />
8      </system.webServer>
9  </configuration>
10 |

```

5. Configure web app environment security

A. Configure HTTPS:

- Obtain an SSL certificate.
- In IIS Manager, go to *Bindings* and add an HTTPS binding, selecting your SSL certificate.

B. Restrict File Access:

- Set appropriate file and directory permissions to limit access.

C. Regular Updates:

- Keep PHP, Node.js, and IIS updated to their latest versions.



Points to Remember

- Describing web hosting platforms

Explanation of hosting platforms available

- Web hosting is an online service that makes your website's content accessible on the internet.
- Free hosting is when a web hosting company provides free access to web domains and hosting.
- Paid hosting is when you pay a fee for a web hosting services provider to host your website on their dedicated servers.
- Hosting with backend server: All of the elements required for the website or application to perform as it should be the backend developer's responsibility. Dynamic Websites: Requires a server to process requests, manage databases, and execute backend code.
- Requirements: Server hosting for PHP, Node.js, Python, or other backend languages; database support like MySQL, PostgreSQL.

- Hosting without backend server: A website which only requires displaying pre-defined data essentially does not require any back-end logic.

Static Websites: Suitable for free hosting or basic paid plans.

Requirements: HTML, CSS, JavaScript files, no need for server-side processing.

- Testing on local/remote computer/Server

a) Network

To perform testing on local or remote computers/servers through a network in Windows Server, you can use various tools and methods depending on what you're trying to achieve.

Here's are the different tools:

- ✓ Ping
- ✓ Tracert
- ✓ Telnet
- ✓ PowerShell Test-NetConnection
- ✓ Remote Desktop
- ✓ Network Monitoring Tools



Indicative content 3.5: Verify Server Environment Requirement



Duration: 4hrs



Practical Activity 3.5.1: Testing on local/remote computer/Server



Tasks:

1. You are requested to go to the computer lab and do the task below individually. Testing on a local or remote computer/server according to network, security, files, and visibility criteria.
2. Read the key readings 3.5.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 3.5.1: Testing on local/remote computer/Server

a) Network

To perform testing on local or remote computers/servers through a network in Windows Server, you can use various tools and methods depending on what you're trying to achieve.

1. **Ping:** Use the ping command to check the connectivity between your server and other computers/servers on the network. Open Command Prompt and type:

```
ping [IP_address_or_hostname]
```

2. **Tracert:** Use the tracert command to trace the route that packets take from your server to the destination server. This can help identify network issues along the way. Open Command Prompt and type:

```
tracert [IP_address_or_hostname]
```

3. **Telnet:** Telnet can be used to test connectivity to a specific port on a remote server. Open Command Prompt and type:

```
telnet [IP_address_or_hostname] [port_number]
```

4. **PowerShell Test-NetConnection:** PowerShell provides the Test-NetConnection cmdlet, which allows you to diagnose connectivity to a remote server. Open PowerShell and type:

```
Test-NetConnection -ComputerName [IP_address_or_hostname] -Port [port_number]
```

b) Security

Testing on local or remote computers/servers through security in Windows Server typically involves various steps to ensure that systems are secure and protected from potential vulnerabilities or threats.

1. **Access Control and Permissions:** Ensure that access control mechanisms are properly configured. Use the principle of least privilege, granting users only the permissions they need to perform their tasks. Regularly review and update user permissions as needed.
2. **User Authentication:** Implement strong password policies and consider additional authentication measures such as multi-factor authentication (MFA) to enhance security.
3. **Network Security:** Configure firewalls, disable unnecessary network services, and segment your network to limit the potential impact of a security breach.
4. **Patch Management:** Regularly apply security patches and updates to the operating system and installed software to address known vulnerabilities.
5. **Antivirus and Antimalware:** Install and configure antivirus and antimalware software to detect and remove malicious software.
6. **Security Auditing and Logging:** Enable security auditing and logging to monitor user activity, system events, and potential security incidents. Regularly review logs for suspicious activities.
7. **Encryption:** Implement encryption for sensitive data, both in transit and at rest, using technologies such as BitLocker for disk encryption and TLS for network encryption.
8. **Backup and Disaster Recovery:** Implement regular backup procedures to ensure that critical data can be restored in the event of a security incident or data loss.
9. **Intrusion Detection and Prevention:** Deploy intrusion detection and prevention systems to monitor network traffic for signs of unauthorized access or malicious activity.
10. **Security Testing:** Conduct regular security assessments, including vulnerability scanning, penetration testing, and security audits, to identify and address potential security weaknesses.
11. **Security Policies and Procedures:** Develop and enforce security policies and procedures to guide the secure configuration and use of systems, as well as the response to security incidents.
12. **Employee Training and Awareness:** Provide security awareness training to employees to help them recognize and respond to security threats effectively.

c) Files

It sounds like you're asking about testing files on a Windows server, possibly in both local and remote environments. Testing files typically involves verifying their integrity, functionality, or security.

Here's a general guide on how you might approach this:

1. Local Testing:

- a) **File Integrity:** Use tools like checksums (MD5, SHA-1, SHA-256) to verify the integrity of files. You can generate checksums for files and compare them with known good values.
- b) **Functionality:** Execute the files in a controlled environment to ensure they perform as expected. For example, if it's an executable, run it and verify its behavior.
- c) **Security:** Scan files with antivirus software to check for any potential threats or malicious content.

2. Remote Testing:

- a) **File Transfer:** Transfer the files to the remote server using secure methods like SSH or SFTP.
- b) **File Integrity:** After transferring, perform integrity checks on the remote server to ensure the files haven't been corrupted during transfer.
- c) **Functionality:** If applicable, execute the files on the remote server and verify their behavior.
- d) **Security:** Ensure that the files don't pose any security risks to the remote server. Scan them with antivirus software after transfer.

3. Server Testing:

- a) **File Permissions:** Ensure that the appropriate permissions are set on the server for accessing and executing the files.
- b) **Integration Testing:** If the files are part of a larger system, conduct integration testing to ensure they work correctly within the server environment.
- c) **Performance Testing:** If relevant, test the performance impact of the files on the server's resources.

4. Automated Testing:

Consider automating some or all of these testing processes using scripts or specialized testing frameworks. This can help streamline the testing process, especially for repetitive tasks or large numbers of files.

5. Logging and Reporting:

- a) Keep detailed logs of the testing process, including any issues encountered and their resolutions.
- b) Generate reports summarizing the testing results, including any anomalies or failures detected.

6. Visibility

It seems like you're looking for guidance on testing visibility on a Windows Server, both locally and remotely.

Here's a general approach you can take:

Testing Local Visibility:

1. Ping Test:

- a) Open Command Prompt.
- b) Type ping localhost and press Enter. This tests basic network connectivity to your own machine.

2. Check Firewall:

- a) Ensure that the firewall settings allow communication on the desired ports.
- b) You can use the Windows Defender Firewall with Advanced Security tool to configure firewall rules.

3. Network Sharing:

- a) If you're testing file sharing or any network service, ensure they're properly configured and accessible locally.

Testing Remote Visibility:

1. Ping Test:

- a) From another machine on the same network, open Command Prompt.
- b) Type ping [server IP] and press Enter. Replace [server IP] with the actual IP address of your server.

2. Port Scanning:

You can use tools like nmap to scan for open ports on the server from a remote machine.

3. Remote Desktop Connection:

If Remote Desktop is enabled, try connecting to the server using Remote Desktop Protocol (RDP) from another machine.

4. File Sharing:

If testing file sharing, attempt to access shared folders from a remote machine.

5. Check Remote Access Permissions:

Ensure that remote access permissions are properly configured in the server settings.

Additional Tips:

- a) **Review Event Logs:** Look into the Event Viewer on the server for any relevant logs or errors that might indicate connectivity issues.
- b) **Check DNS Settings:** Ensure that DNS settings are correct, both on the server and the client machines, to resolve hostnames properly.
- c) **Firewall Rules:** Double-check that firewall rules on the server allow incoming connections on the required ports.
- d) **VPN Connection:** If you're testing connectivity over a VPN, ensure that the VPN connection is established successfully and that routing is set up correctly.



Practical Activity 3.5.2: Verifying Local URL accessibility



Task:

1. You are requested to go to the computer lab and do the task below individually

Verify local URL accessibility, browser compatibility, website speed, and website size. The goal is to ensure that everything works well.

2. Read the key readings 3.5.2 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

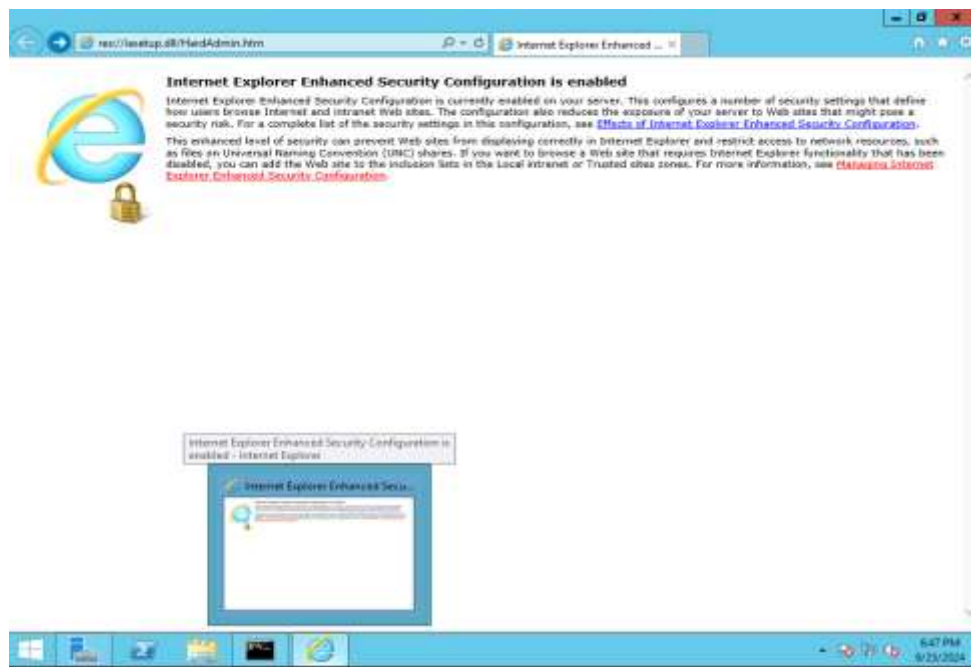


Key readings 3.5.2: Verification of Local URL accessibility

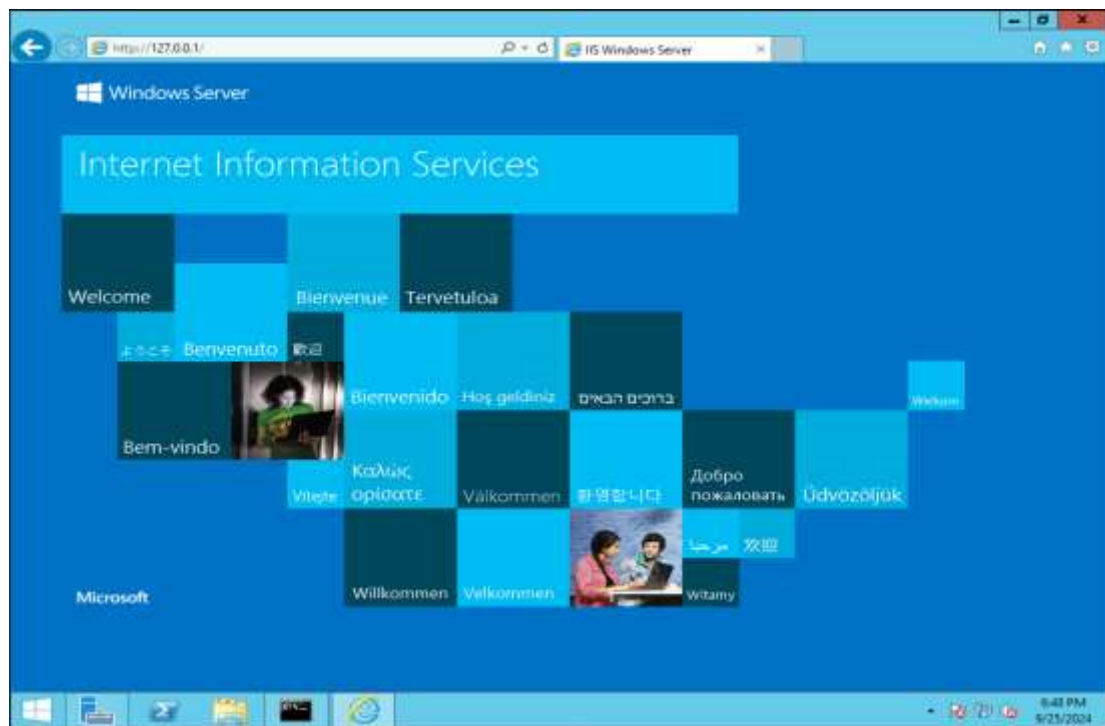
A. Accessibility

To verify local URL accessibility in a Windows Server environment, you can follow these steps:

1. **Open a Web Browser:** Open a web browser on the Windows Server machine.



2. **Enter URL:** In the address bar of the web browser, enter the URL you want to verify. Make sure to use the local address, such as <http://localhost>, <http://127.0.0.1>, or the actual local IP address of the server if applicable.



B. Website speed

To verify the speed of a local website hosted on a Windows Server, you can follow these steps:

1. Use Browser Developer Tools: Most modern browsers have built-in developer tools that include network monitoring. Open your website in a browser, right-click anywhere on the page, and select "Inspect" or "Inspect Element" to open the developer tools. Then, go to the "Network" tab and reload the page. You'll see a list of all the resources loaded by the page along with their load times.

Name / Path	Protocol	Method	Result / Description	Content type	Received	Time	Initiator / Type
http://www.test1.com/	HTTP	GET	200 OK	text/html	(from cache)	0 s	

2. Ping Command: You can use the Command Prompt (cmd) to ping your local server and check the response time. Open Command Prompt and type ping yourlocalwebsite.com replacing "yourlocalwebsite.com" with the actual local URL of your website. This will give you the round-trip time (in milliseconds) from your computer to the server.

```
C:\Users\Administrator>ping www.test1.com

Pinging www.test1.com [192.168.10.10] with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Traceroute Command: Similar to the ping command, you can also use the traceroute command to trace the route packets take to reach your server. This can help identify any network hops that might be causing delays. In Command Prompt, type `tracert yourlocalwebsite.com`.

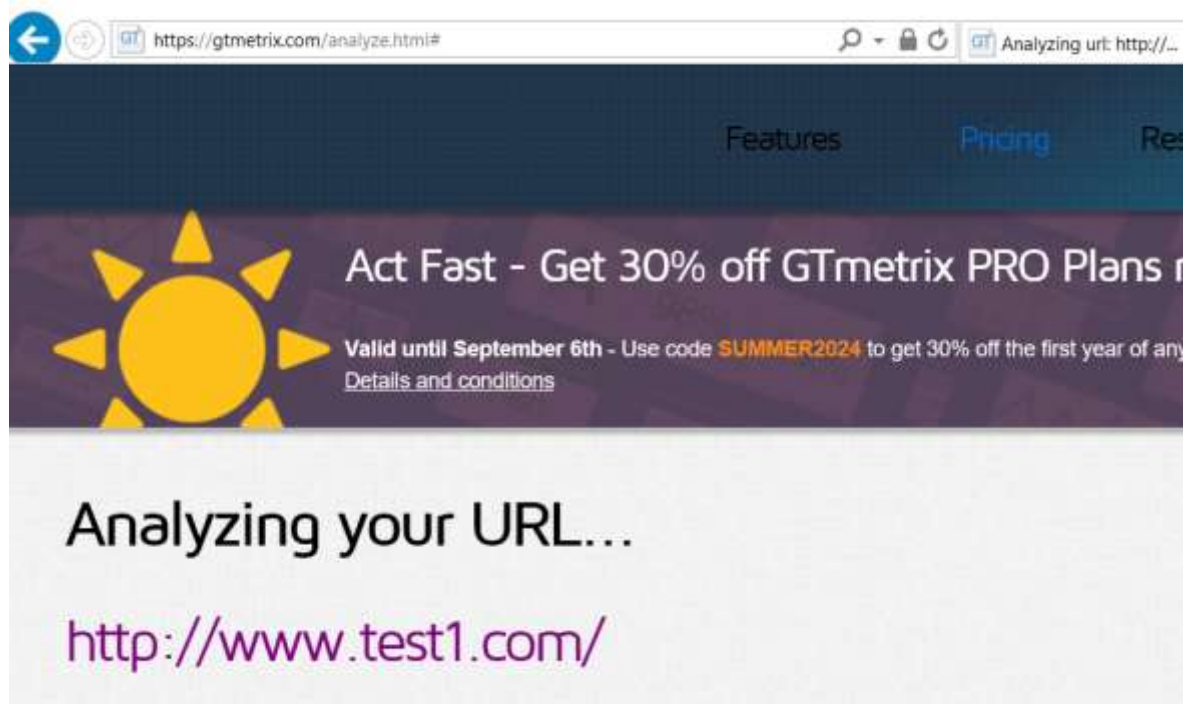
```
C:\Users\Administrator>tracert test1.com

Tracing route to test1.com [192.168.10.10]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  www.test1.com [192.168.10.10]

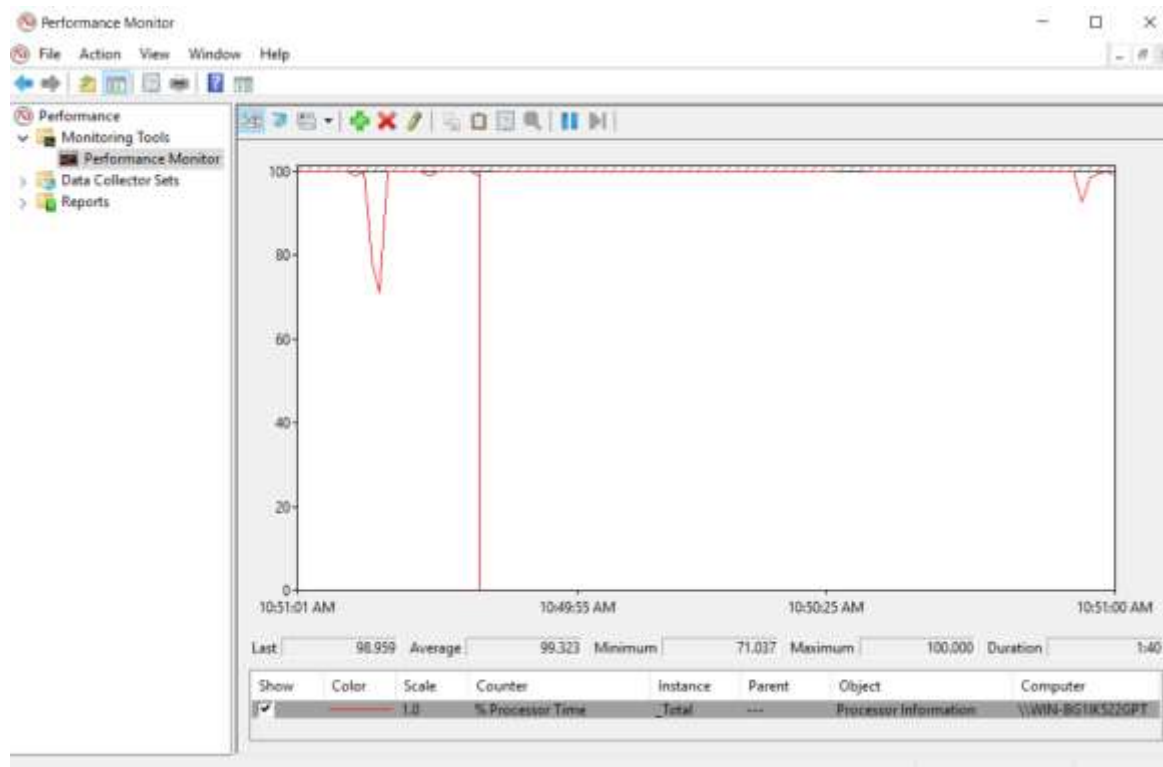
Trace complete.
```

4. Third-Party Tools: There are various online tools available that can analyze your website's speed and performance. While they are primarily designed for public websites, you can still use them to get an idea of your local website's performance. Tools like Google PageSpeed Insights, GTmetrix, or Pingdom Tools are commonly used for this purpose.



5. Performance Monitoring Software: Consider installing performance monitoring software on your Windows Server. These tools can provide detailed insights into your server's performance, including website speed.

Some popular options include New Relic, SolarWinds Server & Application Monitor, and Microsoft Application Insights.



C. Website size

To verify the size of a local website hosted on a Windows server, you can follow these steps:

1. Open Command Prompt: Press Win + R, type cmd, and press Enter.

Best match



Command Prompt
Desktop app

2. Navigate to the website directory: Use the cd command to navigate to the directory where your website files are located. For example

```
cd C:\Path\To\Your\Website
```

3. **Use the dir command:** Once you're in the directory, you can use the dir command to list all files and directories along with their sizes. You can filter by file extension or specific files if needed. For example, to list all .html files and their sizes, you can use:

```
dir *.html
```

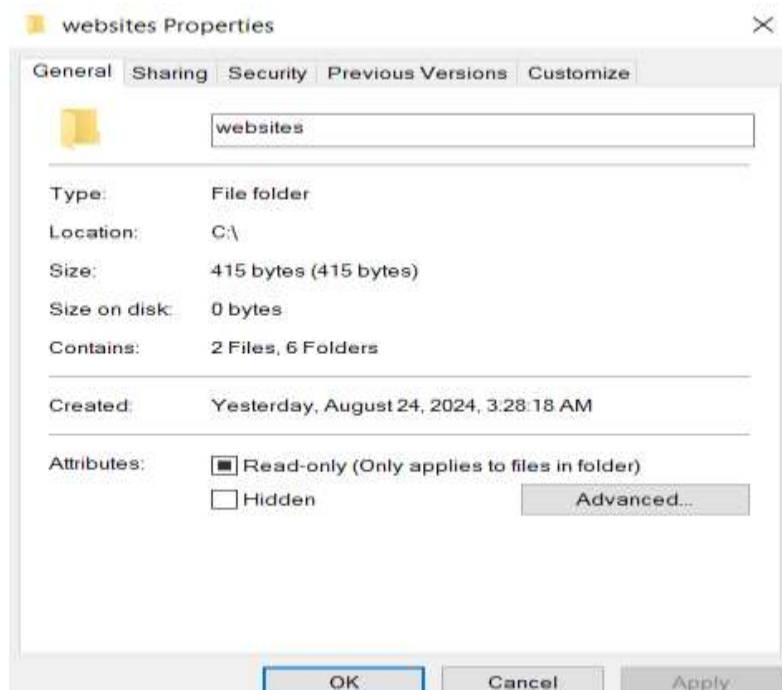
The out put

```
C:\websites\test1.com\wwwroot>dir *.html
Volume in drive C has no label.
Volume Serial Number is EE18-CE25

Directory of C:\websites\test1.com\wwwroot

08/24/2024  03:42 AM                172 index.html
               1 File(s)                172 bytes
               0 Dir(s) 34,970,697,728 bytes free
```

4. **Calculate the total size:** Add up the sizes of all the files to get the total size of your website. Alternatively, you can use Windows Explorer to view the properties of the folder containing your website files. Right-click on the folder, select "Properties," and it will show you the size of the folder, including all files and subfolders within it.





Points to Remember

A. Accessibility

To verify local URL accessibility in a Windows Server environment, you can follow these steps:

- ✓ Open a Web Browser
- ✓ Enter URL
- ✓ Check Accessibility
- ✓ Verify Content
- ✓ Firewall Settings
- ✓ DNS Resolution

B. Browsers

To verify local URL web browsers in Windows Server, you can follow these steps:

- ✓ Open a Web Browser
- ✓ Enter the Local URL
- ✓ Check Access
- ✓ Test with Different Browsers
- ✓ Firewall and Security Settings
- ✓ Additional Troubleshooting

C. Website speed

To verify the speed of a local website hosted on a Windows Server, you can follow these steps:

- ✓ Use Browser Developer Tools
- ✓ Ping Command
- ✓ Traceroute Command
- ✓ Third-Party Tools
- ✓ Performance Monitoring Software

D. Website size

To verify the size of a local website hosted on a Windows server, you can follow these steps:

- ✓ Open Command Prompt
- ✓ Navigate to the website directory
- ✓ Calculate the total size



Indicative content 3.6: Hosting Web App



Duration: 4hrs



Practical Activity 3.6.1: Hosting a Web Application on Windows Server:

Enabling HTTP and HTTPS Access



Task:

1. You are requested to go to the computer lab and do the task below individually.

Trainees are tasked with creating a simple web application that includes two HTML pages: ***"index.html"*** and ***"contact.html"***. These files should be stored in a folder named ***"rtbschools"***. The objective is to host this web app on a Windows Server, making it accessible using both HTTP and HTTPS protocols via the domain name ***"www.rtbschools.site"***. Students will need to specify the physical path for the web app in IIS, select the appropriate protocols (HTTP and HTTPS), specify the server's IP address, configure DNS settings to point the domain to the server, and set up the appropriate port numbers for HTTP (80) and HTTPS (443). Additionally, they should be prepared to handle and troubleshoot any errors that may arise during the setup process. After completing these steps, students should be able to access the website using both ***http://www.rtbschools.site*** and ***https://www.rtbschools.site***.

2. Read the key readings 3.6.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.

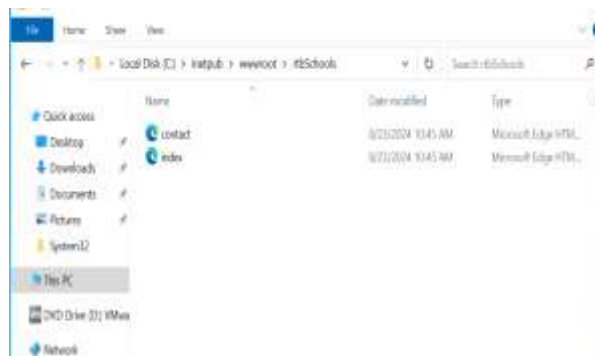


Key readings 3.6.1.: HTTP and HTTPS Access

1. Upload Web App to Windows Server

- **Using Remote Desktop:**

1. Connect to your Windows Server using **Remote Desktop Connection**.
2. Transfer the web application files to the server. Place them in the directory **C:\inetpub\wwwroot\rtbschools**.



2. Specify the Physical Path in IIS

1. Open IIS Manager:

- Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

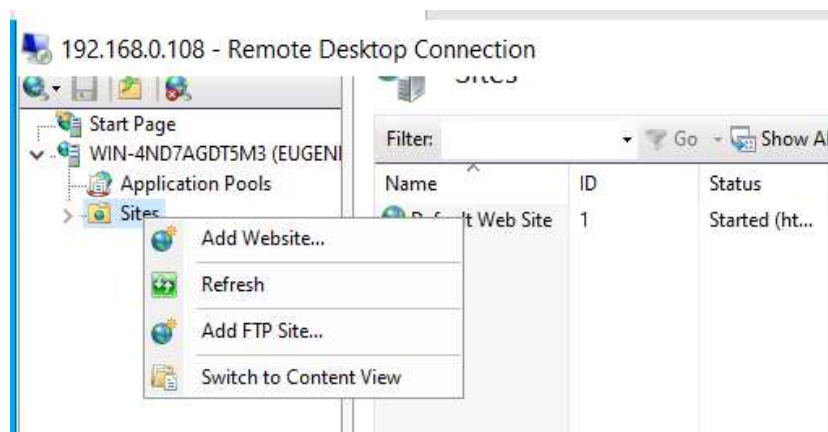
2. Create a New Website:

- In the **Connections** pane, right-click on **Sites** and select **Add Website**.

3. Specify Site Information:

- Site name:** Enter RtbSchools.
- Physical path:** Browse to C:\inetpub\wwwroot\RTB schools.
- Host name:** Enter your domain name: www.rtbschools.com.

4. Click OK to create the site.



Content Directory

Physical path:
rtbschools

Pass-through authentication

Connect as... Test Settings...

Binding

Type: http IP address: 192.168.0.108 Port: 80

Host name:
C:\inetpub\wwwroot\rtbSchools

Example: www.contoso.com or marketing.contoso.com

3. Select the Protocols

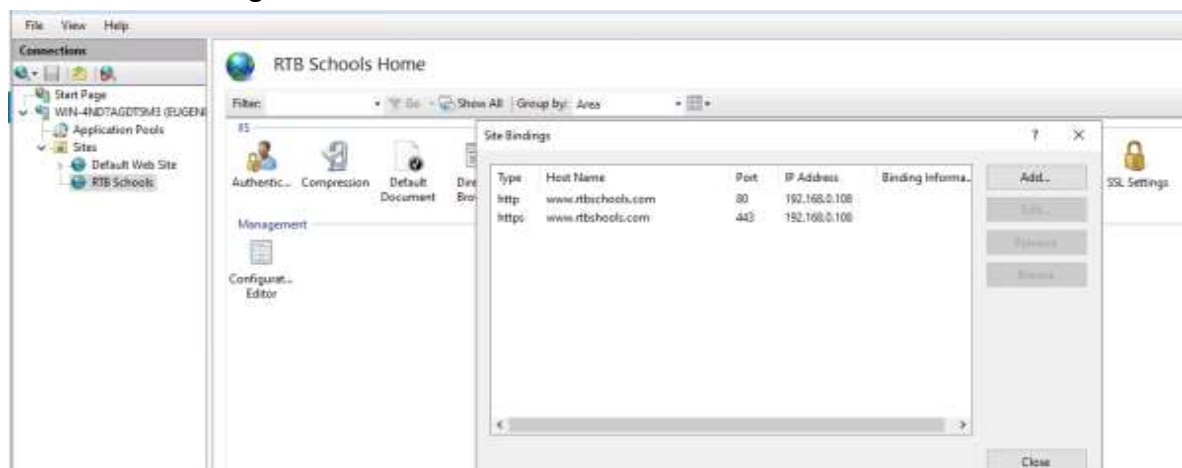
1. Add Protocol Bindings:

- In IIS Manager, select your website.
- Click on **Bindings** in the **Actions** pane.
- **HTTP (Port 80)**: Add a binding for HTTP using http, the appropriate IP address, and port 80.
- **HTTPS (Port 443)**: Add a binding for HTTPS using https, the appropriate IP address, port 443, and select the SSL certificate.

4. Specify the IP Address

1. Configure IP Address:

- In the **Site Bindings** window, specify the IP address where the website will be accessible. If necessary, use All Unassigned or a specific IP address assigned to the server.



5. Configure Web App DNS

Configuring DNS for a web application on a Windows Server involves several steps.

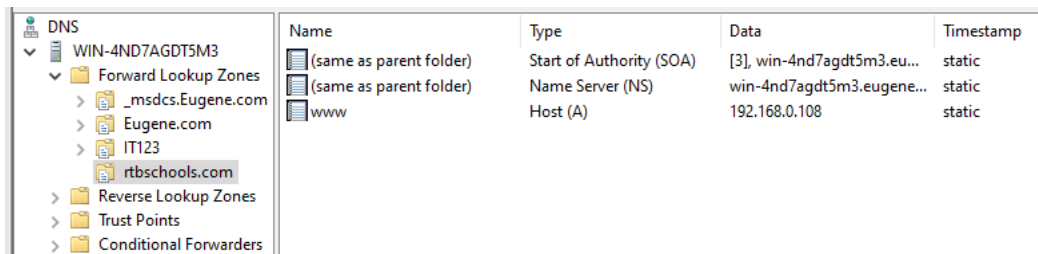
1. Install the DNS Server Role

First, you need to ensure that the DNS Server role is installed on your Windows Server. You can do this through the Server Manager:

- Open Server Manager.
- Click on "**Manage**" from the top right.
- Select "**Add Roles and Features.**"
- Follow the wizard to install the DNS Server role.
- Create a Forward Lookup Zone:

Once the DNS Server role is installed, you need to create a forward lookup zone for your domain:

- Open the DNS Manager.
- Right-click on "**Forward Lookup Zones**" and select "**New Zone.**"
- Follow the wizard to create a primary zone for your domain.
- Specify the zone name (e.g., example.com).
- Choose the zone type (primary zone).



3. Add DNS Records:

After creating the zone, you'll need to add DNS records for your web application:

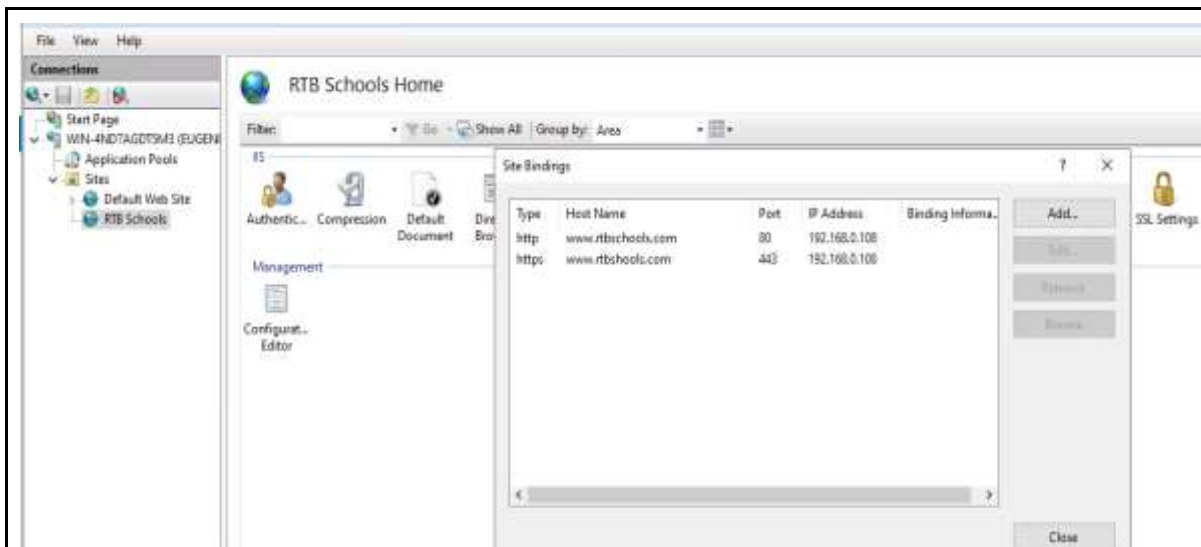
- Right-click on the newly created zone and select the type of record you want to add (e.g., A record for IPv4, AAAA record for IPv6).
- Enter the necessary information such as the hostname and IP address of your web server.
- You may also need to add other records like CNAME (alias) records if your application uses subdomains or additional services.

6. Configure Port Number

1. Configure Ports:

Ensure your site is configured to listen on ports 80 (HTTP) and 443 (HTTPS) in the **Bindings**.

- Open the ports in **Windows Firewall**:
- Go to **Control Panel > System and Security > Windows Defender Firewall > Advanced settings**.
- Ensure inbound rules allow traffic on ports 80 and 443.



7. Handle Discovered Errors

Handling errors on a Windows Server involves several steps to diagnose, troubleshoot, and resolve issues effectively. Here's a general guide on how to handle discovered errors:

- a) **Identify the Error:** Determine the nature of the error. This can often be done by reviewing system logs, event viewer, or error messages that appear on the screen.
- b) **Isolate the Issue:** Try to isolate the cause of the error. Determine if it's a hardware problem, software conflict, configuration issue, or a result of recent changes made to the system.
- c) **Check System Logs:** Windows Server logs events and errors in the Event Viewer. Look for critical or error-level events that coincide with the time of the issue. This can provide valuable information about what went wrong.
- d) **Research the Error:** Use online resources, Microsoft documentation, or community forums to research the error message or code. Often, others have encountered similar issues and may have posted solutions or workarounds.
- e) **Apply Updates and Patches:** Ensure that the server's operating system, drivers, and applications are up to date with the latest patches and updates. Sometimes, errors are caused by known issues that have been addressed in newer versions.
- f) **Check Hardware Health:** If the error seems hardware-related, such as disk failures or memory issues, use diagnostic tools to check the health of hardware components.
- g) **Review Configuration Changes:** If the error occurred after a configuration change, review recent changes to the system configuration, such as software installations, updates, or modifications to system settings.
- h) **Troubleshoot Software:** If the error is related to specific software or services, try troubleshooting steps provided by the software vendor. This may include restarting services, reinstalling software, or adjusting configuration settings.

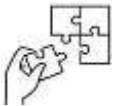
- i) **Restore from Backup:** If the error has caused data loss or corruption, consider restoring affected files or the entire system from backups. Regular backups are essential for recovering from unexpected errors or failures.
- j) **Document the Resolution:** Once the error is resolved, document the steps taken to diagnose and fix the issue. This documentation can be helpful for future reference or for sharing knowledge with other team members



Points to Remember

- **Hosting a Web Application on Windows Server: Enabling HTTP and HTTPS Access follow the following steps:**

5. Upload Web App to Windows Server
6. Specify the Physical Path in IIS
6. Select the Protocols
7. Specify the IP Address
8. Configure Web App DNS
9. Configure Port Number
10. Handle Discovered Errors



Application of learning 3.6.

FFF Ltd, located in Gicumbi District, Northern Province, is facing an issue with hosting a web application on their Windows Server. They need to enable both HTTP and HTTPS access so that all users within the company can access the newly developed system. As an IT technician, you have been hired by FFF Ltd to create and host the web application on the Windows Server, ensuring it is accessible via both HTTP and HTTPS protocols through the domain name "www.fffrwanda.site".

Tasks:

- Ensure access to the website via both <http://www.fffrwanda.site> and <https://www.fffrwanda.site>.



Indicative content 3.7: Verification of Successfully Hosted Web App



Duration: 4hrs



Practical Activity 3.7.1: Testing accessibility on local network and verify size, speed of online web app.



Task:

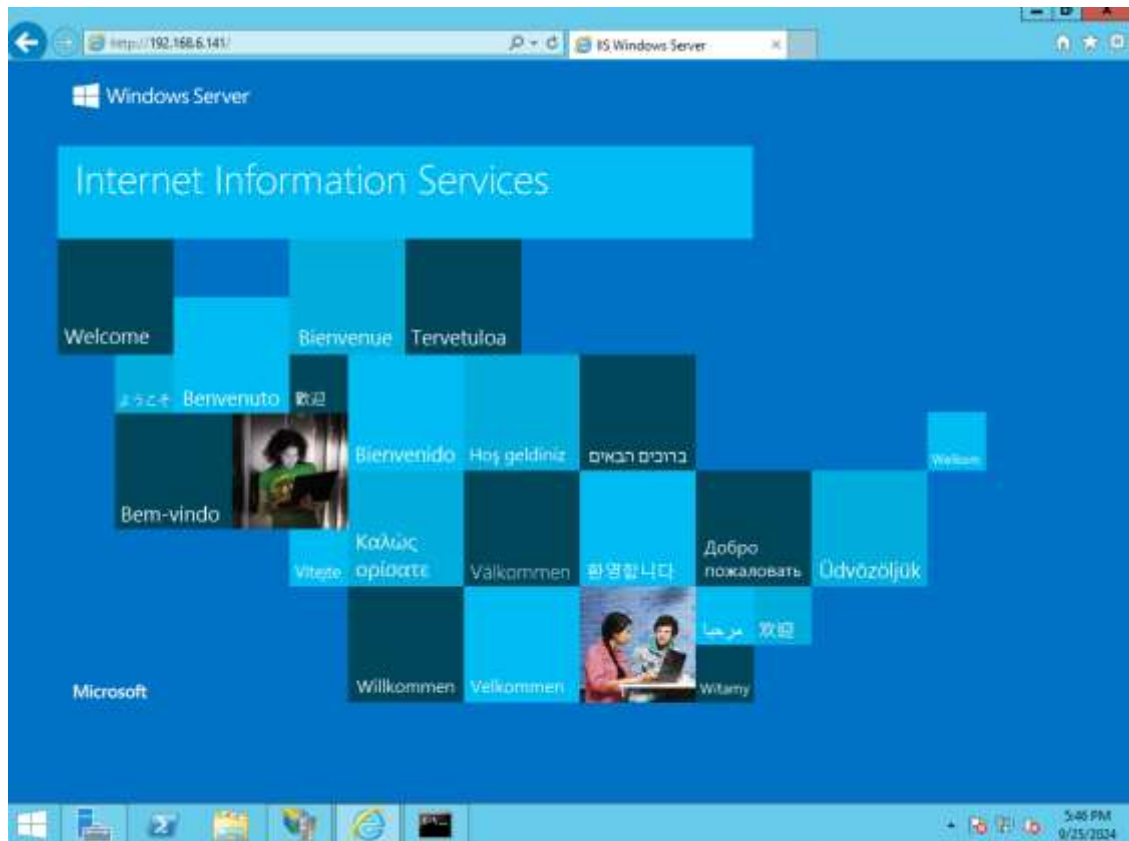
1. You are requested to go to the computer lab and do the task below individually.
Trainees are tasked to test accessibility within a local network on a Windows Server, you can perform several checks and use different various tools
2. Read the key readings 3.7.1 in trainee's manual
3. Follow explanations and instructions
4. Follow trainers while demonstrating how to perform the task
5. Perform the task on your computer
6. Present your work to the trainer and whole class.



Key readings 3.7.1: Verification of Successfully Hosted Web App

1. Testing Accessibility within a Local Network

Example: On a local machine within the same network, open a web browser and enter the server's local IP address (e.g., <http://192.168.1.10>).



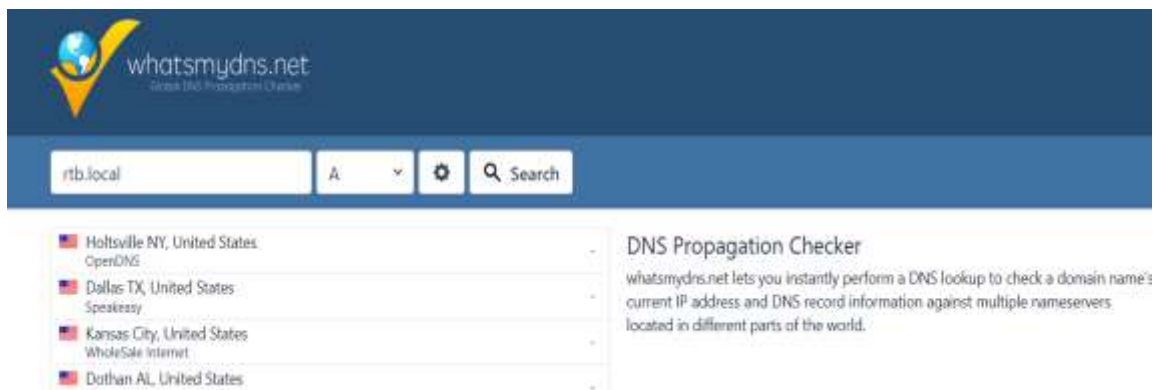
If the web app is accessible, it will load as expected. You may also test using the server's hostname (e.g., `http://rtb1.local`) if DNS is configured within the local network.



2. Testing Online Accessibility

Example: Open a browser on an external device (e.g., a smartphone or laptop connected to a different network) and enter the domain name you configured (e.g., <http://www.myapp.com>).

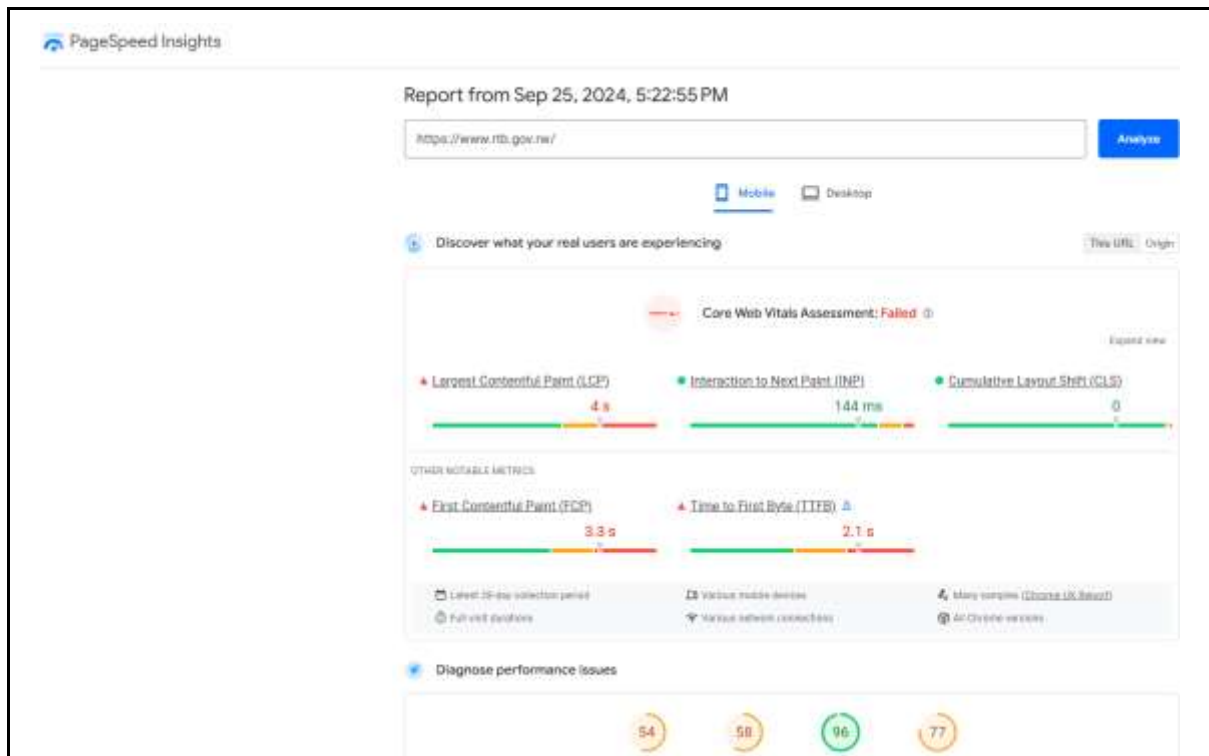
If the domain resolves correctly, your web app will load. If not, check DNS propagation using tools like **WhatsMyDNS.net** to verify that the DNS A record points to your server's public IP.



3. Testing Online Website Speed

Example: Use a tool like **Google PageSpeed Insights** (<https://pagespeed.web.dev/>) or **GTmetrix** (<https://gtmetrix.com/>) to test the speed of your web app.

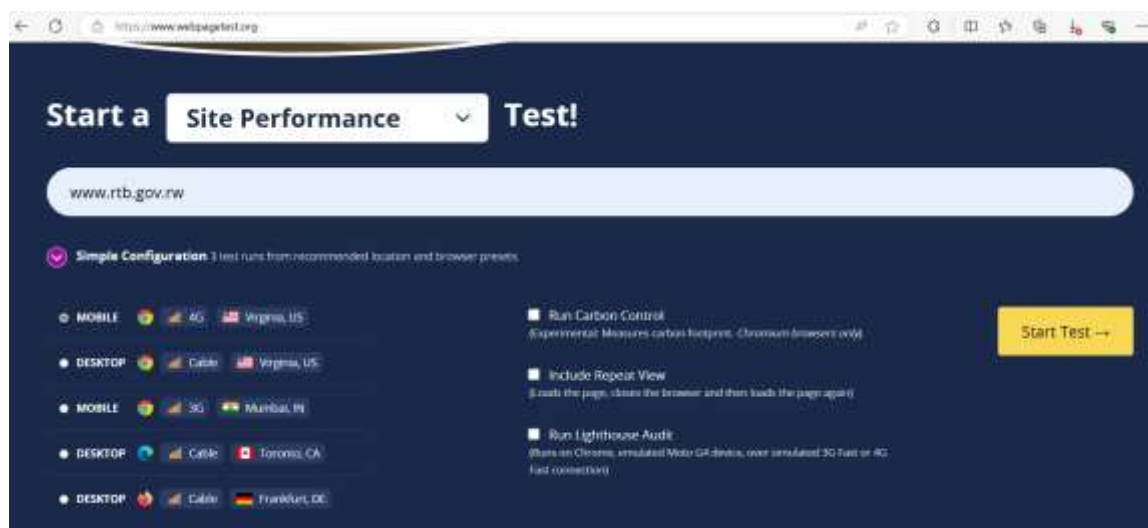
Enter the URL of your web app (e.g., <http://www.myapp.com>) and run the analysis. Review performance metrics like page load time, server response time, and suggestions for optimization.



4. Verify Size of Online Web App

Example: Use **WebPageTest** (<https://www.webpagetest.org/>) to analyze the size of your web app's resources. Enter the URL (e.g., <http://www.myapp.com>) and run a test.

Check the size of individual resources (HTML, CSS, JavaScript, images) and ensure the total page size is within an acceptable range (e.g., below 2MB for faster load times).







Points to Remember

Verification of Successfully Hosted Web App

- **Local Accessibility:**

Test using the server's local IP (e.g., `http://192.168.1.10`) or hostname (e.g., `http://rtb1.local`) to ensure the app loads.

- **Online Accessibility:**

- ✓ Access the domain (e.g., `http://www.myapp.com`) from an external device on a different network.
- ✓ Check DNS propagation with tools like [WhatsMyDNS.net](https://www.whatsmydns.net) if it doesn't load.

- **Website Speed Testing:**

Use tools like *Google PageSpeed Insights* or *GTmetrix* to analyze speed and performance metrics.

- **Resource Size Verification:**

- ✓ Analyze resource sizes using *WebPageTest*.
- ✓ Ensure the total page size is below 2MB for optimal loading.



Application of learning 3.7.

As a system administrator at **RRA**, you are responsible for verifying the deployment of a web app on the Windows Server. First, test its accessibility within the local network using the server's IP or hostname. Next, check its online availability by accessing the app through its public domain from an external device. Use *Google PageSpeed Insights* to evaluate the app's speed and performance. Lastly, verify the size of the web app by checking the file size on the server and reviewing the download size using browser Developer Tools. Document your results to ensure everything is functioning properly.



Learning outcome 3 end assessment

Written assessment

Question 1. Circle the letter corresponding to the correct answer:

i. What is Handler Mapping in IIS?

- a) Mapping IP addresses to domain names
- b) Assigning request handlers to specific types of requests
- c) Mapping users to their roles in the system
- d) Configuring network connections for the server

ii. Which of the following is NOT a type of web server?

- a) Apache
- b) IIS
- c) SQLite
- d) Nginx

iii. What protocol is used for secure communication between a client and a web server?

- a) HTTP
- b) FTP
- c) HTTPS
- d) SMTP

iv. Which of the following is a benefit of using IIS?

- a) Cross-platform compatibility
- b) Free licensing
- c) Tight integration with Windows and .NET
- d) Open-source availability

v. Which environment variable should be set to specify the configuration file for PHP in IIS?

- a) PHP_ENV
- b) PHP_INI_DIR
- c) PHP_CONF
- d) PHP_PATH

Question 2. Fill in the Blanks space with the appropriate words. Select from the given choices

- i. The default port number for HTTP is
 - a) 80
 - b) 443
 - c) 21
 - d) 22
- ii. The PHP handler in IIS is configured using
 - a) CGI
 - b) ISAPI
 - c) FastCGI
 - d) ASP.NET
- iii. Node.js applications in IIS are managed using the module.
 - a) PHP Handler
 - b) IISNode
 - c) Apache Tomcat
 - d) LiteSpeed
- iv. Free hosting platforms typically offer resources compared to paid hosting platforms.
 - a) Unlimited
 - b) Limited
 - c) Premium
 - d) High-performance
- v. The process of configuring an SSL certificate for secure communication in IIS involves setting up
 - a) HTTP binding
 - b) FTP binding
 - c) HTTPS binding
 - d) DNS binding

Question 3: Read the following statement related to carry out finishing activity and Answer following questions by using **True or False**

- i. IIS can be installed on Linux-based systems.
- ii. FTP is used to transfer files securely between a client and a server.
- iii. WinCache is a caching extension for PHP that can be used in IIS to improve performance.
- iv. Site binding in IIS is used to define how the server listens for incoming connections, specifying the protocol, IP address, port, and hostname.
- v. The SSL certificate is required to enable HTTP site binding in IIS.

Practical assessment

FFF Ltd company, located in Gicumbi District, Northern Province, FFF Ltd has a problem that there no way to Host a Web Application on Windows Server: Enabling HTTP and HTTPS Access hence, they need to access to their system they have recently developed so that all users in the company will be able to access it . As an IT technician, you are hired by FFF Ltd to create and host web application in the windows server, making it accessible using both HTTP and HTTPS protocols via the domain name “www.ffrwanda.site”.

Tasks:

To access the website using both ***http://*** www.ffrwanda.site and <https://www.ffrwanda.site> .



References

Dauti, b. B. (2024). *Windows Server 2022 Administration Fundamentals*. Third Edition.

Krause, J. (2024). *Mastering Windows Server 2022*.

Lee, T. (2024). *Windows Server Automation with PowerShell Cookbook*.

Microsoft. (n.d.). Add Windows Server Essentials as a member server. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/windows-server-essentials/install/add-windows-server-essentials-as-a-member-server>

Microsoft. (n.d.). Assessment and deployment kit for Windows Server Essentials. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/windows-server-essentials/install/assessment-and-deployment-kit-for-windows-server-essentials>

Microsoft. (n.d.). Customize and deploy Windows Server Essentials. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/windows-server-essentials/install/customize-and-deploy-windows-server-essentials>

Openprovider. (n.d.). SSL installation on MS IIS Windows-powered systems. Openprovider. Retrieved from <https://support.openprovider.eu/hc/en-us/articles/360014563220-SSL-Installation-on-MS-IIS-Windows-powered-systems>

Site24x7. (n.d.). DNS record types. Site24x7. Retrieved from <https://www.site24x7.com/learn/dns-record-types.html>

