Republic of Rwanda
Ministry of Education

RTB | RWANDA TVET BOARD

SWDWS 401

WINDOWS SERVER ADMINISTRATION

Perform Basic Windows Server Administration

Competence

RQF Level:	4
Learning Hours	90
Credits:	9
Sector:	ICT and Multimedia
Trade:	Software Development
Module Type:	Specific
Curriculum:	ICTSWD4002 – TVET Certificate IV in Software Development
Copyright:	© Rwanda TVET Board, 2023

Issue Date: August 2023

Learning outcome 1: Manage Server Services

1.1 Introduction to server administration

Server administration manages information on a company's servers, updates hardware and software, and protects against cyberattacks. Server administration is crucial in maintaining and securing a company's digital services and information.

1.1.1 Description of key terms

- **Server:** In the context of computer networks, a server refers to a computer or a system that provides services or resources to other computers or devices on the network. It is designed to handle and respond to requests from clients, such as serving web pages, managing files, or hosting applications.
- **Client:** A client, also known as a client computer or client device, is a computer or device that accesses and utilizes services or resources provided by a server. It can be a desktop computer, laptop, smartphone, or any other network-enabled device. Clients send requests to servers and receive responses to access data, files, applications, or other services.
- **Network Operating System (NOS):** A Network Operating System is a specialized operating system designed to manage and control network resources and services. It provides functionalities like file sharing, printer sharing, user authentication, and network administration. NOS enables multiple computers or devices to communicate and share resources within a network effectively.
- **Hypervisor:** A hypervisor, also known as a virtual machine monitor (VMM), is software or firmware that enables the creation and management of virtual machines (VMs). It allows multiple operating systems to run simultaneously on a single physical computer or server. The hypervisor provides isolation, resource allocation, and management capabilities, allowing multiple VMs to coexist and operate independently.

- **Virtualization:** is the process of creating a virtual version or representation of a physical resource, such as a server, operating system, storage device, or network. It enables the consolidation of multiple virtual resources on a single physical infrastructure, improving resource utilization, scalability, and flexibility. Virtualization technology allows for the efficient allocation and management of resources, leading to cost savings and increased efficiency in IT environments.

1.1.2 Server virtualization

- **Hypervisor Technologies**

1. **Type 1 Hypervisor (Bare Metal Hypervisor):** This hypervisor runs directly on the physical hardware, without the need for an underlying operating system. It provides direct access to hardware resources and manages the virtual machines (VMs) independently. Examples of type 1 hypervisors include VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

2. **Type 2 Hypervisor (Hosted Hypervisor):** This hypervisor runs on top of an existing operating system. It relies on the underlying operating system for hardware access and manages the VMs as processes within the host operating system. Examples of type 2 hypervisors include Oracle VirtualBox, VMware Workstation, and Parallels Desktop.

3. **Full Virtualization:** This hypervisor technology allows for the emulation of complete hardware environments, enabling the execution of multiple operating systems on a single physical machine. It provides isolation and allows different operating systems to run simultaneously without modification. Type 1 hypervisors typically support full virtualization.

4. **Para-virtualization:** In para-virtualization, the guest operating systems are modified to be aware of the virtualization layer. This allows for more efficient communication between the guest operating systems and the hypervisor, resulting in improved performance compared to full virtualization. Xen is an example of a hypervisor that supports para-virtualization.

5. **Hardware-assisted Virtualization:** This technology utilizes hardware extensions, such as Intel VT-x and AMD-V, to enhance the virtualization capabilities of the hypervisor. These extensions provide direct support for virtualization, improving performance and security. Most modern hypervisors leverage hardware-assisted virtualization.

Types of server virtualization

There are primarily three types of server virtualization techniques commonly used:

1. **Full Virtualization:** Full virtualization, also known as native virtualization, allows multiple virtual machines (VMs) to run on a single physical server while emulating the complete hardware environment. Each VM operates as if it has its own dedicated hardware resources, including CPU, memory, storage, and network interfaces. Examples of hypervisors that support full virtualization include VMware ESXi, Microsoft Hyper-V, and KVM (Kernel-based Virtual Machine).

2. **Para-virtualization:** Para-virtualization involves modifying the guest operating systems to be aware of the virtualization layer. This allows for more efficient communication between the guest operating systems and the hypervisor, resulting in better performance compared to full virtualization. Para-virtualization requires specific guest operating system support. Xen is a popular hypervisor that supports para-virtualization.

3. **Container-based Virtualization:** Container-based virtualization, also known as operating system-level virtualization, is a lightweight virtualization technique. It allows for the creation and running of multiple isolated user-space instances, called containers, on a single host operating system. Containers share the host's operating system kernel, libraries, and resources, making them more efficient and lightweight than full virtualization. Docker and Kubernetes are examples of popular containerization platforms.

Each type of server virtualization **has its own advantages and use cases**.

Full virtualization provides the highest level of isolation and flexibility, making it suitable for running different operating systems and applications on the same physical server.

Para-virtualization offers better performance but requires guest operating system modifications.

Container-based virtualization is ideal for deploying and managing lightweight, scalable applications in a shared environment.

Notes: Organizations choose the type of server virtualization based on factors such as performance requirements, compatibility, resource utilization, and management capabilities.

Benefits of server virtualization

Server virtualization offers several benefits to organizations. Here are some key advantages:

1. **Increased Efficiency and Resource Utilization:** Server virtualization allows for the consolidation of multiple virtual machines (VMs) on a single physical server. This consolidation leads to better utilization of hardware resources, as multiple VMs can share the same physical server, reducing hardware costs and energy consumption. It enables organizations to make more efficient use of their infrastructure.

2. **Cost Savings:** By reducing the number of physical servers needed, server virtualization helps organizations save on hardware costs, power consumption, cooling, and maintenance expenses. It eliminates the need for dedicated servers for each application or workload, resulting in significant cost savings over time.

3. **Improved Flexibility and Scalability:** Virtualization enables easy provisioning and deployment of new VMs, allowing organizations to quickly scale their IT infrastructure to meet changing demands. It provides the flexibility to

allocate resources dynamically, adjusting CPU, memory, and storage as needed, without disrupting running applications.

4. **Enhanced Disaster Recovery and Business Continuity:** Server virtualization simplifies the backup and recovery processes. VMs can be easily backed up, replicated, and restored, enabling faster disaster recovery and minimizing downtime. It also allows for the creation of failover clusters and high availability configurations, ensuring business continuity in case of hardware failures or disasters.

5. **Simplified Management and Maintenance:** Virtualization platforms provide centralized management tools that simplify the administration and monitoring of VMs. It allows for efficient resource allocation, performance optimization, and security management. Virtual machines can be easily migrated or moved between physical servers without interrupting services, making maintenance tasks easier.

6. **Testing and Development:** Virtualization provides a sandbox environment for testing and development purposes. It allows developers to create isolated VMs to test new applications, software updates, or system configurations without impacting the production environment. This helps reduce risks and improves the quality of software releases.

Overall, server virtualization offers increased efficiency, cost savings, flexibility, improved disaster recovery, simplified management, and enhanced testing capabilities. These benefits make it a popular choice for organizations looking to optimize their IT infrastructure and streamline operations.

1.1.3 Server requirements

- **Hardware requirements**

1. **Processing Power (CPU):** The CPU is a crucial hardware component that determines the server's processing capabilities. The required CPU power depends on the workload and applications that will run on the server. High-performance

servers may require multiple CPUs or processors with multiple cores to handle demanding tasks efficiently.

2. **Memory (RAM):** Sufficient memory is essential for smooth and efficient server operation. The amount of RAM required depends on the workload and the number of concurrent processes or virtual machines running on the server. Memory-intensive applications or virtualization environments typically require larger amounts of RAM.

3. **Storage:** Consider the storage requirements based on the amount of data that needs to be stored and accessed by the server. Determine the type of storage needed, such as hard disk drives (HDDs) or solid-state drives (SSDs), and the required capacity. Additionally, organizations may need to consider storage redundancy and backup solutions for data protection.

4. **Network Connectivity:** Servers require reliable network connectivity to communicate with other devices and provide services. Assess the network requirements based on factors such as the number of users or clients accessing the server, the expected network traffic, and the required network speed (e.g., Gigabit Ethernet, 10 Gigabit Ethernet).

5. **Redundancy and High Availability:** For critical applications or services, organizations may require redundant server configurations to ensure high availability and minimize downtime. This can involve redundant power supplies, network connections, and storage solutions.

- **Software requirements**

1. **Operating System (OS):** Choose an appropriate server operating system based on the organization's needs and compatibility with the applications and services to be hosted. Popular server OS options include Windows Server, Linux distributions (such as Ubuntu Server, CentOS, or Red Hat Enterprise Linux), or specialized server OS like VMware ESXi.

2. **Server Software:** Install the necessary server software based on the intended purpose of the server. This can include web server software (e.g., Apache HTTP Server, Microsoft IIS), database server software (e.g., MySQL, Microsoft SQL Server), email server software (e.g., Microsoft Exchange Server, Postfix), or other specialized server applications.

3. **Security Software:** Implement appropriate security measures to protect the server and its data. This may include firewall software, antivirus software, intrusion detection/prevention systems, and regular security updates.

4. **Server Management Tools:** Choose server management tools to efficiently monitor and administer the server infrastructure. This can include remote administration tools, monitoring software, backup and recovery solutions, and configuration management tools.

5. **Application Compatibility:** Consider the compatibility of the server software with the applications and services that will be hosted. Ensure that the server software supports the required programming languages, frameworks, and dependencies.

1.2 Installation of Server OS

1.2.1 Creation of virtual storage (RAID)

- **Identification of RAID Levels**

RAID stands for **Redundant Array of Independent Disks**. It is a technology that combines multiple physical hard drives into a single logical unit to improve performance, data protection, and storage efficiency. RAID achieves this by distributing or replicating data across the drives in various configurations called RAID levels.

There are several RAID levels, each offering different levels of performance, fault tolerance, and capacity. Here are some commonly used RAID levels:

1. **RAID 0 (Striping):** RAID 0 provides increased performance and capacity by striping data across multiple drives. It does not offer any fault tolerance or redundancy. Data is divided into blocks and distributed across the drives, allowing for parallel read/write operations. However, if one drive fails, all data is lost.

2. **RAID 1 (Mirroring):** RAID 1 provides data redundancy by creating an exact copy (mirror) of data on two or more drives. It offers high read performance and fault tolerance, as data can be read from any of the mirrored drives. If one drive fails, data remains accessible from the remaining drives. However, it has lower capacity due to the need for duplicating data.

3. **RAID 5 (Striping with Parity):** RAID 5 combines striping and parity to provide both performance and fault tolerance. Data is striped across multiple drives, and parity information is distributed across the drives as well. Parity allows for data reconstruction in case of a single drive failure. RAID 5 requires at least three drives and offers a good balance between performance, capacity, and fault tolerance.

4. **RAID 6 (Striping with Dual Parity):** RAID 6 is similar to RAID 5 but provides higher fault tolerance by using dual parity. It requires at least four drives and can withstand the failure of two drives simultaneously. RAID 6 offers better data protection but has slightly lower write performance compared to RAID 5.

5. **RAID 10 (Mirrored Striping):** RAID 10 combines mirroring (RAID 1) and striping (RAID 0). It requires at least four drives, where data is mirrored across pairs of drives, and then the mirrored pairs are striped. RAID 10 offers high performance, fault tolerance, and capacity utilization. It can withstand the failure of one or more drives in each mirrored pair.

6. **RAID 50 and RAID 60:** RAID 50 and RAID 60 are combinations of RAID 5 and RAID 0 (RAID 50) or RAID 6 and RAID 0 (RAID 60). They provide better performance and fault tolerance by striping data across multiple RAID 5 or RAID 6 arrays.

These are some of the commonly used RAID levels. Each RAID level has its own advantages and considerations, and the choice depends on the specific requirements, performance needs, and desired fault tolerance of the system.

Advantages and disadvantages of RAID technology

Advantages of RAID Technology:

1. **Improved Performance:** RAID can enhance read and write performance by distributing data across multiple drives. This allows for parallel access to data, resulting in faster data transfer rates and improved overall system performance.

2. **Data Redundancy and Fault Tolerance:** RAID provides data redundancy, which protects against drive failures. In certain RAID levels, such as RAID 1, RAID 5, RAID 6, and RAID 10, data is mirrored or parity information is stored to allow for data reconstruction in case of a drive failure. This ensures that data remains accessible and minimizes the risk of data loss.

3. **Increased Storage Capacity:** RAID allows for combining the storage capacity of multiple drives into a single logical volume. This enables the creation of larger storage spaces without relying on a single drive. It offers efficient utilization of storage capacity and scalability options for future expansion.

4. **Flexibility and Customization:** With different RAID levels available, organizations have the flexibility to choose the level that best suits their specific needs. RAID configurations can be customized based on performance requirements, fault tolerance, and capacity considerations.

5. **High Availability and Data Access:** RAID technology provides high availability by allowing the system to continue functioning even if one or more drives fail. This ensures uninterrupted access to data and minimizes downtime in critical environments.

Disadvantages of RAID Technology:

1. **Cost:** Implementing RAID can involve additional costs, especially for hardware RAID solutions that require dedicated RAID controllers. The cost of purchasing multiple drives and maintaining redundancy can be higher compared to a single drive setup.

2. **Complexity:** RAID configurations can be complex to set up and manage, especially for more advanced RAID levels. Proper configuration and monitoring are essential to ensure optimal performance and data protection. It may require technical expertise or specialized knowledge to implement and maintain RAID systems effectively.

3. **Performance Impact in Some RAID Levels:** While RAID can enhance performance in certain configurations, some RAID levels, such as RAID 1 and RAID 5, may have a performance impact due to the overhead of mirroring or parity calculations. The trade-off between performance and fault tolerance should be considered when choosing a RAID level.

4. **Limited Protection Against Multiple Drive Failures:** Although RAID provides protection against drive failures, it may not protect against multiple drive failures in certain RAID levels. For example, RAID 5 can tolerate the failure of a single drive, but if multiple drives fail simultaneously, data loss can occur.

5. **RAID Rebuild Time:** In the event of a drive failure, the process of rebuilding data onto a replacement drive can take time, during which the system may be vulnerable to further failures. RAID rebuild

Configuration of RAID on physical server

To configure RAID on a physical server, you typically need to follow these steps:

Step 1. Identify RAID Controller: Determine if your server has a built-in hardware RAID controller or if you need to install a separate RAID controller card. Check the server's specifications or consult the manufacturer's documentation to confirm the presence of a RAID controller.

Step 2. Install RAID Controller (if applicable): If your server does not have a built-in RAID controller, install the RAID controller card into an available slot on the server's motherboard. Ensure it is properly seated and securely connected.

Step 3. Access RAID Configuration Utility: Restart the server and enter the RAID controller's configuration utility. This is typically done by pressing a specific key combination during the server's boot process. The specific key combination and access method vary depending on the RAID controller manufacturer. Common keys include Ctrl+R, Ctrl+M, or Ctrl+G.

Step 4. Create RAID Array: Once inside the RAID configuration utility, you can create a RAID array. The exact steps may vary depending on the RAID controller, but typically involve selecting the drives to include in the array, specifying the RAID level (e.g., RAID 0, RAID 1, RAID 5), and configuring any additional settings such as strip size or cache settings. Follow the prompts and instructions provided by the RAID controller's configuration utility.

Step 5. Initialize and Format the RAID Array: After creating the RAID array, you need to initialize and format it to make it usable by the operating system. This step is typically performed using the operating system's disk management tools. Initialize the RAID array and then format it with the desired file system (e.g., NTFS, ext4).

Step 6. Install Operating System: Once the RAID array is initialized and formatted, you can proceed with installing the operating system on the RAID array. During the installation process, the RAID array should be recognized as a single logical disk, and you can proceed with the installation as you would on a regular disk.

Step 7. Verify and Test: After the operating system is installed, it's important to verify the RAID configuration and conduct tests to ensure proper functioning. Check the RAID controller's management software or utility to monitor the status of the RAID array, ensure all drives are functioning correctly, and conduct performance tests to validate the RAID configuration.

Notes: It's important to consult the documentation provided by the RAID controller manufacturer for detailed instructions specific to your RAID controller model. Following the manufacturer's guidelines will ensure a successful RAID configuration on your physical server.

1.2.2. Installation of Hypervisor

Certainly! Here are the steps for installing VMware ESXi Hypervisor:

Step 1. Check hardware compatibility: Before installing VMware ESXi, ensure that your hardware meets the compatibility requirements specified by VMware. You can find the Hardware Compatibility Guide on the VMware website.

Step 2. Download the VMware ESXi ISO image: Visit the VMware website and download the VMware ESXi installation ISO image. Make sure to choose the version that is compatible with your hardware.

Step 3. Create a bootable USB drive or burn the ISO image to a DVD: Use a tool like Rufus or Etcher to create a bootable USB drive with the VMware ESXi ISO image. Alternatively, you can burn the ISO image to a DVD.

Step 4. Configure BIOS/UEFI settings: Restart your computer and enter the BIOS/UEFI settings. Ensure that virtualization technology (e.g., Intel VT-x or AMD-V) is enabled. Save the changes and exit the BIOS/UEFI settings.

Step 5. Boot from the installation media: Insert the bootable USB drive or DVD into your computer and restart it. Make sure your computer is set to boot from the installation media. The exact steps to change the boot order may vary depending on your computer's manufacturer.

Step 6. Start the VMware ESXi installation: Once the installation media is booted, you will see the VMware ESXi installer. Select the appropriate keyboard layout and press Enter to continue.

Step 7. Accept the End User License Agreement (EULA): Read and accept the EULA to proceed with the installation.

Step 8. Select the installation destination: Choose the destination disk where you want to install VMware ESXi. This will typically be a local disk or a RAID array.

Step 9. Set a root password: Provide a secure password for the root user account, which will be used to manage the VMware ESXi host.

Step 10. Confirm the installation: Review the installation settings and confirm that you want to proceed with the installation. This will begin the installation process.

Step 11. Reboot the system: Once the installation is complete, remove the installation media and reboot the system.

Step 12. Configure network settings: After the system restarts, you will be prompted to configure the network settings for the VMware ESXi host. Provide the necessary network details, such as IP address, subnet mask, gateway, and DNS settings.

Step 13. Access the VMware ESXi host: Open a web browser on a computer connected to the same network and enter the IP address of the VMware ESXi host. This will allow you to access the VMware ESXi management interface, known as the vSphere Client.

Step 14. Install VMware vSphere Client: Download and install the VMware vSphere Client on your computer. This client software allows you to manage and configure virtual machines on the VMware ESXi host.

Step 15. Configure additional settings: Use the VMware vSphere Client to configure additional settings, such as storage, networking, and security options.

Notes: That's it! These steps should guide you through the installation process of VMware ESXi Hypervisor. Remember to refer to the official VMware documentation for detailed instructions and any specific requirements for your environment.

1.2.3 Creation of virtual machines

To create virtual machines (VMs) on VMware ESXi, you can follow these steps:

Step 1. Access the VMware vSphere Client: Open the VMware vSphere Client on your computer and connect to the VMware ESXi host by entering its IP address or hostname.

Step 2. Navigate to the "Hosts and Clusters" view: In the vSphere Client interface, locate the "Hosts and Clusters" view, which displays the available hosts and clusters.

Step 3. Select the host or cluster: Expand the tree view and select the host or cluster where you want to create the virtual machine.

Step 4. Click on "Create/Register VM": Right-click on the selected host or cluster and choose the "Create/Register VM" option. This will open the virtual machine creation wizard.

Step 5. Choose the creation type: In the creation wizard, select whether you want to create a new virtual machine or clone an existing one. For a new VM, choose the "Create a new virtual machine" option.

Step 6. Specify the name and location: Provide a name for the virtual machine and choose the location where it should be stored on the datastore.

Step 7. Select the guest operating system: Choose the guest operating system that you plan to install on the virtual machine. This selection helps optimize the VM's settings for the chosen OS.

Step 8. Configure the virtual hardware: Specify the virtual hardware settings such as CPU, memory, disk size, network adapter, and other devices. Adjust these settings based on your requirements.

Step 9. Customize advanced options (optional): If needed, you can configure advanced options like resource allocation, virtual machine compatibility, and boot options.

Step 10. Configure storage options: Choose the datastore where the virtual machine's virtual disks will be stored. You can also select thin provisioning or thick provisioning for disk allocation.

Step 11. Configure networking: Select the network adapter and configure the network settings for the virtual machine. You can choose to connect it to a specific virtual network or leave it disconnected.

Step 12. Review and finish: Review all the settings you've configured for the virtual machine and make any necessary changes. Once you're satisfied, click "Finish" to create the virtual machine.

Step 13. Install the guest operating system: Power on the virtual machine and follow the prompts to install the guest operating system using an ISO image or other installation media.

Step 14. Customize the VM (optional): After the guest OS is installed, you can further customize the virtual machine by installing VMware Tools and configuring additional settings.

Notes: Repeat these steps to create additional virtual machines on the VMware ESXi host as needed. Remember to allocate resources appropriately and consider the capacity of your host when creating multiple VMs.

1.2.4 Installation of guest OS

To install a guest operating system (OS) in VMware ESXi, you can follow these steps:

Step 1. Prepare the installation media: Obtain the installation media for the guest OS you want to install. This can be an ISO image, DVD, or other installation media.

Step 2. Access the VMware vSphere Client: Open the VMware vSphere Client on your computer and connect to the VMware ESXi host by entering its IP address or hostname.

Step 3. Navigate to the "Hosts and Clusters" view: In the vSphere Client interface, locate the "Hosts and Clusters" view, which displays the available hosts and clusters.

Step 4. Select the virtual machine: Expand the tree view and select the virtual machine (VM) where you want to install the guest OS.

Step 5. Power on the virtual machine: Right-click on the selected VM and choose "Power" > "Power On" to start the virtual machine.

Step 6. Connect the installation media: With the VM powered on, right-click on it and select "Edit Settings". In the settings window, select the "CD/DVD Drive" option and choose the appropriate option to connect the installation media (ISO image, client device, or datastore ISO file).

Step 7. Configure boot options: In the VM settings, make sure the "CD/DVD Drive" is set to boot first in the boot order. This ensures that the VM boots from the installation media.

Step 8. Save the settings and exit: Click "OK" to save the VM settings and exit the settings window.

Step 9. Install the guest OS: The virtual machine will now boot from the installation media. Follow the prompts and instructions provided by the guest OS installer to install the operating system on the VM.

Step 10. Customize the guest OS installation: During the installation process, you may be prompted to provide information such as language, keyboard layout, disk partitioning, and network settings. Customize these settings according to your requirements.

Step 11. Complete the installation: Once the guest OS installation is complete, the VM will restart. Remove the installation media from the CD/DVD drive or disconnect it from the VM settings.

Step 12. Install VMware Tools (optional): After the guest OS is installed, it is recommended to install VMware Tools. This software enhances the VM's performance and provides additional features. To install VMware Tools, right-click on the VM, select "Guest" > "Install/Upgrade VMware Tools", and follow the on-screen instructions.

Notes: That's it! The guest OS is now installed on the VMware ESXi virtual machine. You can repeat these steps to install different guest operating systems on other virtual machines as needed.

1.3 Creation of domain controller

A domain controller (DC) is a server that runs the Active Directory Domain Services (AD DS) role in a Windows Server environment. Its primary function is to authenticate and authorize users and computers within a domain network. A domain controller stores and manages user accounts, security policies, group memberships, and other directory information.

1.3.1 Description of Server Administrative tools

Server Administrative Tools, also known as Remote Server Administration Tools (RSAT), are a set of tools provided by Microsoft to manage and administer Windows Server operating systems remotely. These tools enable system administrators to perform various administrative tasks and configure server roles and features from a remote computer.

Here are some of the commonly used Server Administrative Tools:

1. **Active Directory Users and Computers (ADUC):** This tool allows administrators to manage users, groups, organizational units (OUs), and other objects in an Active Directory domain. It provides a graphical interface to create, modify, and delete user accounts, reset passwords, manage group memberships, and more.

2. **Active Directory Sites and Services (ADSS):** This tool enables administrators to manage the replication topology and site configuration in an Active Directory environment. It allows the creation and management of sites, subnets, site links, and connection objects to control how Active Directory data is replicated between domain controllers.

3. **DNS Manager:** DNS Manager is used to manage the Domain Name System (DNS) infrastructure. It allows administrators to create and manage DNS zones, configure DNS server properties, create and edit DNS records, and troubleshoot DNS-related issues.

4. **DHCP Manager:** DHCP Manager is used to manage the Dynamic Host Configuration Protocol (DHCP) server. It provides a graphical interface to configure DHCP scopes, manage IP address leases, set DHCP options, and monitor DHCP server activity.

5. **Group Policy Management Console (GPMC):** GPMC is used to manage Group Policy Objects (GPOs) in an Active Directory environment. It allows administrators to create, edit, and link GPOs, configure Group Policy settings, and manage Group Policy preferences.

6. **Hyper-V Manager:** Hyper-V Manager is used to manage and administer virtual machines running on Windows Server with the Hyper-V role installed. It provides a centralized interface to create, configure, start, stop, and monitor virtual machines, as well as manage virtual networks and storage.

7. **Remote Desktop Services Manager:** This tool is used to manage Remote Desktop Services (formerly known as Terminal Services). It allows administrators to view and manage user sessions, disconnect or log off users, monitor server performance, and manage RemoteApp programs.

8. **Server Manager:** Server Manager is a central management console that provides an overview of the server roles and features installed on a Windows Server machine. It allows administrators to add or remove server roles and

features, view server status and performance, and access various administrative tools.

Roles

The role is the services needed to run Active Directory Domain Services (ADDS). That is, a server role is a set of software programs that, when installed and properly configured, lets a computer perform a specific function for multiple users or other computers within a network.

Feature

Features are optional Windows Server components that provide helper functionality and are just some frontend programs to work with the services once installed and configured.

1.3.2 Installation of Active Directory Domain Services (ADDS)

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.

2. 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. Promote the Server to a Domain Controller: After the installation, the wizard will prompt you to promote the server to a domain controller. 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.

1.3.3 Promotion of server to a domain controller

Promoting a server to a domain controller is an important step in setting up a Windows Server environment. It allows the server to manage user accounts, security policies, and other resources within a domain.

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.

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

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.

1.4 Installation of server roles and features

1.4.1 Description of server roles and features

DNS stands for **Domain Name System**. In the context of Windows Server administration, DNS refers to the service and protocol used to translate domain names (such as www.example.com) into IP addresses (such as 192.168.0.1) and vice versa.

In Windows Server, the DNS service is typically provided by the DNS Server role, which can be installed and configured on a Windows Server machine. The DNS Server role allows the server to act as a DNS server, providing name resolution services to clients on the network.

DHCP stands for **Dynamic Host Configuration Protocol**. In the context of Windows Server administration, DHCP refers to the service and protocol used to automatically assign IP addresses and network configuration settings to devices on a network.

In Windows Server, the DHCP Server role can be installed and configured on a server to provide DHCP services to clients on the network. When a client device connects to the network and requests an IP address, the DHCP server dynamically assigns an available IP address from a predefined pool, along with other network configuration parameters such as subnet mask, default gateway, and DNS server addresses.

- **DNS**

- Queries: DNS is responsible for translating domain names (e.g., www.example.com) into IP addresses. DNS queries are requests made by clients to DNS servers to resolve domain names. There are different types of DNS queries, such as recursive queries (where the DNS server resolves the query on behalf of the client) and iterative queries (where the DNS server provides a referral to another DNS server).

- Operation: DNS operates using a distributed hierarchical database system. It consists of various DNS server types, including authoritative DNS servers (which hold the information for specific domains) and recursive DNS servers (which resolve queries on behalf of clients).

- **Roles:** DNS servers can serve different roles, such as being authoritative for a specific domain or acting as a caching server to improve query performance by storing recently resolved queries.

- **Root Hints:** Root hints are a list of IP addresses that DNS servers use to locate the root DNS servers. These root servers hold information about the top-level domains (.com, .org, etc.) and provide referrals to authoritative DNS servers for specific domains.

- **Zones and Zone Files:** DNS zones are portions of the DNS namespace that are managed by a specific DNS server. Each zone has a corresponding zone file, which contains the DNS resource records (such as A, CNAME, MX records) for that zone.

DHCP

- **Messages and Operation:** DHCP is responsible for dynamically assigning IP addresses and other network configuration parameters to clients on a network. DHCP messages include discover, offer, request, and acknowledgement messages. The DHCP server receives a client's request for an IP address, offers an available IP address, and then acknowledges the client's acceptance of that IP address.

- **Fault Tolerance Implementations:** DHCP fault tolerance can be achieved through various methods, such as using DHCP failover, where two DHCP servers share the lease information and can take over the DHCP service if one fails. Other methods include using DHCP clustering or implementing a split scope configuration.

- **Security Considerations:** DHCP security considerations include preventing unauthorized DHCP servers from operating on the network, ensuring the integrity of DHCP messages, and protecting against IP address lease exhaustion and IP address conflicts.

- **Relay Agent:** A DHCP relay agent is a network device that forwards DHCP messages between DHCP clients and DHCP servers that are on different subnets. It helps DHCP clients on one subnet to obtain IP addresses from DHCP servers on another subnet.

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.

- **DHCP**

1. Open the Server Manager on your Windows Server.

2. Click on "Add roles and features" or a similar option.

3. Proceed through the Add Roles and Features Wizard.

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

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

6. 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.

1.5 Configuration of DNS

1.5.1 Lookup zones

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.

6. Additionally, you can configure other zone-specific settings, such as aging and scavenging, dynamic updates, zone delegation, and more, based on your requirements.

Difference between Reverse Lookup Zone and Forward Lookup Zone The main difference between forward lookup zone and reverse lookup zone is that forward lookup zone is used to resolve forward lookup queries where the client requests an IP address by providing the host name, while reverse lookup zone is used for resolving reverse lookup queries where a client requests a host name by providing an IP address. The forward lookup zone contains A type resource records that can point out an IP address for a given host name. The reverse lookup zone contains PTR records that can point out a host name for a given IP address.

1.5.2 Creation of Alias (CNAME)

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.

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

Notes: It's important to note that the Alias (CNAME) record allows you to create an alias for a domain name or hostname. When clients request the alias, DNS will resolve it to the fully qualified domain name or hostname specified in the target host field.

Remember to allow sufficient time for DNS propagation, as changes to DNS records may take some time to propagate across the network.

1.5.3 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. 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. Here's a brief description of each record type:

- **A** Record: Associates a domain name with an IPv4 address. Provide the hostname and the corresponding IPv4 address.
- **AAAA** Record: Associates a domain name with an IPv6 address. Provide the hostname and the corresponding IPv6 address.
- **CNAME** Record: Creates an alias for a domain name. Provide the alias name and the **fully qualified domain name** (FQDN) or hostname to which it should point.

- **MX** Record: Specifies the mail exchanger responsible for accepting incoming email for a domain. Provide the priority, mail server hostname, and optionally, the preference.
- **PTR** Record: Maps an IP address to a hostname. This is used in reverse DNS lookup. Provide the IP address and the corresponding hostname.
- **NS** Record: Specifies the authoritative **name servers** for a domain. Provide the hostname or FQDN of the name server.
- **SOA** Record: Specifies the Start of Authority for a DNS zone. It includes information about the primary DNS server, contact details, serial number, and other parameters.

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."

1.6 Configuration of DHCP parameters

1.6.1 Scope

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:

- **Scope Name:** Provide a descriptive name for the scope to identify it easily.

- **IP Address Range:** Specify the starting and ending IP addresses that will be leased by the DHCP server. This defines the range of addresses available for DHCP assignment.
    - **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.
- **Subnet Mask:** Set the subnet mask for the IP addresses in the scope. It determines the network portion of the IP address.
- **Exclusions:** Exclude specific IP addresses or ranges from the scope if you want to reserve them for static assignment or other purposes.
- **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.
- **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.

Notes: Remember to review and adjust the DHCP scope parameters based on your network requirements and IP addressing scheme.

1.6.2 Reservation

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

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.

Notes: Remember to review and adjust the reservation settings based on the specific device's MAC address and the desired IP address assignment.

1.6.3 Failover

To configure DHCP failover for high availability and redundancy, 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.

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.

Notes: Remember to review and adjust the failover settings based on your network requirements and the desired level of redundancy.

DHCP reservation and DHCP failover are both techniques used in managing and ensuring the availability and stability of DHCP (Dynamic Host Configuration Protocol) services in a network.

DHCP Reservation: DHCP reservation is a feature in DHCP servers that allows the administrator to reserve a specific IP address for a particular device. This ensures that the device always receives the same IP address when it requests an address from the DHCP server. DHCP reservations are typically used for devices that require static IP addresses for specific applications or services.

DHCP Failover: DHCP failover is a mechanism used to provide redundancy and high availability for DHCP services. In a DHCP failover setup, two DHCP servers are configured to share DHCP lease information and address allocation responsibilities. If one DHCP server fails or becomes unavailable, the other server can take over and continue serving DHCP requests without interruption. DHCP failover helps ensure that DHCP services remain available even in the event of server failures or maintenance activities.

Both DHCP reservation and DHCP failover are important components of network management, helping to improve reliability and simplify administration in large-scale network environments.

1.7 Monitoring of Server services

1.7.1 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:

- Open a command prompt on your client machine.
- Type "**nslookup**" followed by the domain name or IP address you want to resolve.
- Press Enter to execute the command.
- 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

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:

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

Example: ipconfig

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.

What is the Windows DNS server's primary, Secondary, and Stub zone?

In Windows DNS server:

Primary Zone: The file is saved as a standard text file with filename (.dns) in the Primary Zone.

Secondary Zone maintains a read-only copy of the zone database on another DNS server. Also, it acts as a backup server to the primary server by giving fault tolerance and load balancing.

Stub Zone includes the server copy, and S.O.A. (Start of Authority) records used to minimize the DNS search orders.

Learning outcome 2: Manage Users

2.1 Creation of User Accounts

- ✓ **Define User account policies**

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 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. Some common user account policies in Windows Server include:

1. **Password policies:** These policies specify the requirements for creating and managing passwords, such as complexity, length, expiration, and history. They help enforce strong passwords to prevent unauthorized access.

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.

3. **Kerberos policies:** Kerberos is a network authentication protocol used in Windows Server environments. Kerberos policies define settings related to ticket-granting tickets (TGTs), session tickets, and ticket lifetimes, ensuring secure authentication and authorization.

4. **Logon policies**: Logon policies control the behavior and restrictions for user logon sessions. They include settings such as logon hours, logon workstation restrictions, and logon scripts, allowing administrators to manage user access and session control.

5. **Account auditing policies**: Account auditing policies enable administrators to track and monitor user account activities, such as successful or failed logon attempts, changes to user accounts, and access to sensitive resources. They help in identifying security breaches and detecting suspicious behavior.

✓ 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**: An administrator account, as the name suggests, has full control and unrestricted access to the Windows Server system. Users with administrator accounts can perform all tasks, including installing and uninstalling software, modifying system settings, managing other user accounts, and accessing all files and folders. Administrator accounts have elevated privileges and can make changes that affect the entire system. It is important to use administrator accounts with caution and only provide them to trusted individuals who require advanced system management capabilities.

✓ Creation of New Account

To create a new user account in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Open the "Server Manager" by clicking on the Server Manager icon on the taskbar or by selecting it from the Start menu.

3. In the Server Manager window, click on "Tools" in the top-right corner and select "Computer Management" from the dropdown menu. This will open the Computer Management console.

4. In the Computer Management console, expand the "Local Users and Groups" folder and click on the "Users" folder.

5. Right-click on an empty area in the right-hand pane and select "New User" from the context menu. This will open the New User dialog box.

6. In the New User dialog box, enter the required details for the new user account, including the user name, full name, and description. You can also set a password for the account and choose whether the user should change the password at the next logon.

7. Optionally, you can configure additional settings for the account, such as account expiration, account options, and group membership, by clicking on the "Profile," "Member Of," or "Account" tabs in the New User dialog box.

8. Once you have entered all the necessary information, click the "Create" button to create the new user account.

9. The new user account will now be listed in the Users folder of the Computer Management console.

Notes: You have successfully created a new user account in Windows Server 2012 R2. The user can now log in to the server using the provided username and password.

- ✓ **Copy Account**

If you want to create a copy of an existing user account in Windows Server 2012 R2, you can use the "Copy" feature available in the Computer Management console. Here's how you can do it:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Open the "Server Manager" by clicking on the Server Manager icon on the taskbar or by selecting it from the Start menu.

3. In the Server Manager window, click on "Tools" in the top-right corner and select "Computer Management" from the dropdown menu. This will open the Computer Management console.

4. In the Computer Management console, expand the "Local Users and Groups" folder and click on the "Users" folder.

5. Right-click on the user account that you want to copy and select "Copy" from the context menu. This will open the Copy User dialog box.

6. In the Copy User dialog box, enter a new username for the copied account. You can also modify other details such as the full name and description if needed.

7. Click the "Create" button to create the copy of the user account.

8. The copied user account will now be listed in the Users folder of the Computer Management console.

Notes: Please note that the copied user account will have the same group memberships and permissions as the original account. You may need to modify these settings as per your requirements for the new user account.

2.2 Management of user accounts

- ✓ **Changing user account password**

To change a user account password in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Users" in the left-hand pane to display a list of user accounts in the right-hand pane.

4. Right-click on the user account for which you want to change the password and select "Set Password" from the context menu. This will open the Set Password dialog box.

5. In the Set Password dialog box, enter the new password for the user account in both the "New password" and "Confirm password" fields.

6. Optionally, you can check the "User must change password at next logon" box if you want the user to change the password the next time they log in.

7. Click the "OK" button to change the password for the user account.

- ✓ **Remove account**

To remove a user account in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Users" in the left-hand pane to display a list of user accounts in the right-hand pane.

4. Right-click on the user account that you want to remove and select "Delete" from the context menu. This will open a confirmation dialog box.

5. In the confirmation dialog box, click the "Yes" button to confirm the deletion of the user account.

6. The user account will now be removed from the Users list in the Local Users and Groups Manager.

Notes: Please note that when you delete a user account, all associated user data, including files, folders, and settings, will be permanently deleted. Make sure to back up any important data before removing the account. Additionally, exercise caution when deleting user accounts to avoid accidentally removing critical system accounts or accounts that are still in use.

- ✓ **Activate Account**

To activate a disabled user account in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Users" in the left-hand pane to display a list of user accounts in the right-hand pane.

4. Right-click on the disabled user account that you want to activate and select "Properties" from the context menu. This will open the Properties dialog box for the user account.

5. In the Properties dialog box, go to the "General" tab.

6. Uncheck the "Account is disabled" checkbox.

7. Click the "OK" button to save the changes and activate the user account.

Notes: The disabled user account will now be activated and the user will be able to log in using their credentials.

- ✓ **Deactivate account**

To deactivate or disable a user account in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Users" in the left-hand pane to display a list of user accounts in the right-hand pane.

4. Right-click on the user account that you want to deactivate and select "Properties" from the context menu. This will open the Properties dialog box for the user account.

5. In the Properties dialog box, go to the "General" tab.

6. Check the "Account is disabled" checkbox.

7. Click the "OK" button to save the changes and deactivate the user account.

The user account will now be disabled, and the user will not be able to log in using their credentials until the account is reactivated.

- ✓ **Customization of User Account Parameters**

To customize user account parameters in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Users" in the left-hand pane to display a list of user accounts in the right-hand pane.

4. Right-click on the user account for which you want to customize parameters and select "Properties" from the context menu. This will open the Properties dialog box for the user account.

5. In the Properties dialog box, you can customize various parameters based on your requirements. Here are a few commonly customized parameters:

- **General tab**: You can modify the user's full name, description, and user logon name.

- **Member Of tab**: You can add or remove the user from different groups to manage their access and permissions.

- **Account tab**: You can set options such as password expiration, account expiration, and account lockout settings.

- **Profile tab**: You can specify a user profile path, logon script, and other profile-related settings.

- **Dial-in tab**: If you are configuring remote access, you can set up dial-in permissions for the user.

6. Make the necessary changes to the parameters based on your requirements.

7. Click the "OK" button to save the changes and apply the customized parameters to the user account.

<u>Notes</u>: By customizing user account parameters, you can tailor the user's experience, access, and security settings to meet your specific needs within the Windows Server 2012 R2 environment.

2.3 Management of user groups

User groups are a way to manage and organize users with similar permissions, access rights, and privileges. User groups allow administrators to simplify the management of user accounts by applying permissions and settings to groups rather than individual users.

- ✓ **Creation of group**

To create a group in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Groups" in the left-hand pane to display a list of groups in the right-hand pane.

4. Right-click on an empty area in the right-hand pane and select "New Group" from the context menu. This will open the New Group dialog box.

5. In the New Group dialog box, enter a name for the group in the "Group name" field.

6. Optionally, you can enter a description for the group in the "Description" field.

7. Click the "Add" button to add members to the group. This will open the Select Users dialog box.

8. In the Select Users dialog box, enter the usernames of the users you want to add to the group, or click the "Advanced" button to search for users in the Active Directory.

9. After adding the desired users to the group, click the "OK" button to close the Select Users dialog box.

10. Click the "Create" button to create the group.

Notes: The group will now be created and listed in the Groups section of the Local Users and Groups Manager. You can manage the group's membership, permissions, and other settings by selecting the group and using the context menu options available.

- ✓ **Adding users in groups**

To add users to a group in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Groups" in the left-hand pane to display a list of groups in the right-hand pane.

4. Double-click on the group to which you want to add users. This will open the Properties dialog box for the group.

5. In the Properties dialog box, go to the "Members" tab.

6. Click the "Add" button to open the Select Users dialog box.

7. In the Select Users dialog box, enter the usernames of the users you want to add to the group, or click the "Advanced" button to search for users in the Active Directory.

8. After adding the desired users to the group, click the "OK" button to close the Select Users dialog box.

9. The selected users will now be added to the group. You can verify the membership by checking the list of users in the Members tab of the Properties dialog box.

Notes: By adding users to groups, you can manage their access rights, permissions, and privileges more efficiently. Group membership allows you to apply consistent settings and permissions to multiple users at once, simplifying user management within the Windows Server 2012 R2 environment.

✓ Removing users from group

To remove users from a group in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "lusrmgr.msc" and press Enter. This will open the Local Users and Groups Manager.

3. In the Local Users and Groups Manager, click on "Groups" in the left-hand pane to display a list of groups in the right-hand pane.

4. Double-click on the group from which you want to remove users. This will open the Properties dialog box for the group.

5. In the Properties dialog box, go to the "Members" tab.

6. Select the user(s) you want to remove from the group by clicking on their name(s) in the list.

7. Click the "Remove" button to remove the selected user(s) from the group.

8. Confirm the removal by clicking the "Yes" button in the confirmation dialog box.

9. The selected user(s) will now be removed from the group. You can verify the membership by checking the list of users in the Members tab of the Properties dialog box.

Notes: By removing users from a group, you can revoke their access rights, permissions, and privileges associated with that group. This allows you to manage user access and permissions more effectively within the Windows Server 2012 R2 environment.

2.4 Management of Organization Units (OU)

Organizational Unit (OU) is a container within the Active Directory hierarchy that allows administrators to organize and manage objects, such as user accounts, computer accounts, and groups, in a logical and hierarchical manner.

- ✓ **Creation of OU**

To create an Organizational Unit (OU) in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "dsa.msc" and press Enter. This will open the Active Directory Users and Computers console.

3. In the Active Directory Users and Computers console, right-click on the domain name or an existing OU where you want to create the new OU. Select "New" and then click on "Organizational Unit" from the context menu. This will open the New Object - Organizational Unit dialog box.

4. In the New Object - Organizational Unit dialog box, enter a name for the new OU in the "Name" field.

5. Optionally, you can enter a description for the OU in the "Description" field.

6. Click the "OK" button to create the OU.

Notes: The new OU will now be created under the selected domain or existing OU in the Active Directory Users and Computers console. You can further customize and manage the OU by creating sub-OUs, adding users or groups, applying Group Policy settings, and more.

- ✓ **Adding Users in OU**

To add users to an Organizational Unit (OU) in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "dsa.msc" and press Enter. This will open the Active Directory Users and Computers console.

3. In the Active Directory Users and Computers console, navigate to the OU where you want to add users.

4. Right-click on the OU and select "New" and then click on "User" from the context menu. This will open the New Object - User dialog box.

5. In the New Object - User dialog box, enter the required details for the new user, such as the first name, last name, and user logon name.

6. Optionally, you can enter additional information such as the password, user principal name, and other attributes as needed.

7. Click the "Next" button to proceed to the next step.

8. Set the desired password for the user account and configure any other password-related settings as required.

9. Click the "Next" button to proceed to the next step.

10. Review the summary of the new user account details and click the "Finish" button to create the user account.

Notes: The user account will now be created and added to the specified OU in the Active Directory Users and Computers console. You can further manage the user account properties, group memberships, and other settings as needed. Repeat these steps to add more users to the OU if necessary.

- ✓ **Removing users from Organization unit**

To remove users from an Organizational Unit (OU) in Windows Server 2012 R2, you can follow these steps:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Press the Windows key + R on your keyboard to open the Run dialog box. Type "dsa.msc" and press Enter. This will open the Active Directory Users and Computers console.

3. In the Active Directory Users and Computers console, navigate to the OU from which you want to remove users.

4. Locate the user account(s) that you want to remove from the OU.

5. Right-click on the user account(s) and select "Move" from the context menu. This will open the Move dialog box.

6. In the Move dialog box, select the destination where you want to move the user account(s). This can be another OU or the main domain container.

7. Click the "OK" button to move the user account(s) out of the current OU.

8. The user account(s) will now be removed from the selected OU and placed in the new location.

Notes: By removing users from an OU, you are changing their location within the Active Directory structure. This can affect the application of Group Policy settings and other specific configurations associated with the OU. Make sure to consider the implications before removing users from an OU and ensure that their access and permissions are appropriately managed in the new location.

2.5 Assignment of Permission to Users

✓ 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.

In summary, granting permissions means giving someone access to resources, while revoking permissions means taking away their access to those resources.

To grant and revoke user account permissions in Windows Server 2012 R2, you can follow these steps:

Granting User Account Permissions:

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Right-click on the file, folder, or resource for which you want to grant permissions.

3. Select "Properties" from the context menu. This will open the Properties dialog box.

4. Go to the "Security" tab in the Properties dialog box.

5. Click the "Edit" or "Advanced" button to modify the permissions.

6. In the Permissions dialog box, click the "Add" button to add users or groups to the permission list.

7. Enter the name of the user or group in the "Enter the object names to select" field and click the "Check Names" button to validate.

8. Select the desired permissions for the user or group from the permission list.

9. Click the "OK" button to save the changes and grant the permissions.

- **Revoking User Account Permissions:**

1. Log in to the Windows Server 2012 R2 system using an account with administrative privileges.

2. Right-click on the file, folder, or resource from which you want to revoke permissions.

3. Select "Properties" from the context menu. This will open the Properties dialog box.

4. Go to the "Security" tab in the Properties dialog box.

5. Click the "Edit" or "Advanced" button to modify the permissions.

6. In the Permissions dialog box, select the user or group from the permission list.

7. Click the "Remove" button to revoke the permissions.

8. Click the "OK" button to save the changes and revoke the permissions.

Notes: By granting and revoking user account permissions, you can control access to files, folders, and resources on your Windows Server 2012 R2 system. It's important to carefully manage permissions to ensure proper security and access control.

Topic2.5.2.Change remote access permissions for a user account

To change remote access permissions for a user account on a Windows Server, you can follow these steps:

1. Open Server Manager: Launch Server Manager from the taskbar or search for it in the Start menu.
2. Navigate to Local Users and Groups: In Server Manager, click on "Tools" in the top-right corner and select "Computer Management." In the Computer Management window, expand "Local Users and Groups," and then click on "Users."
3. Find the User Account: Locate the user account for which you want to change remote access permissions.
4. Open Properties: Right-click on the user account and select "Properties."
5. Modify Remote Access Permissions:
   - Go to the "Member Of" tab.
   - Click on "Remote Desktop Users" or another appropriate group depending on your requirements.
   - Click on "Add" and then type the name of the user or group that you want to grant remote access to.
   - Click "OK" to save the changes.
6. Confirm Changes: Close the properties window and any other open windows.
7. Restart Remote Desktop Services (Optional): Sometimes, changes to remote access permissions may require a restart of the Remote Desktop Services. You can do this by opening a Command Prompt with administrative privileges and running the command net stop termservice && net start termservice

IC2.6.Management of client machines

Topic2.6.1. Joining a client computer to the domain

A. Setting of the client computer's name

When joining a client computer to a domain in Windows Server, the client computer's name typically remains the same unless it conflicts with an existing computer name in the domain. In that case, Windows will prompt you to enter a new name for the client computer.

Here's a step-by-step overview of how the process typically works:

1. Open System Properties: On the client computer, right-click on "This PC" or "My Computer" (depending on your Windows version) and select "Properties".
2. Change Settings: In the System window, click on the "Change settings" link next to the "Computer name, domain, and workgroup settings".
3. Join a Domain: In the System Properties window, go to the "Computer Name" tab and click the "Change" button.
4. Enter Domain Information: Select the "Domain" option and enter the name of the domain you want to join. You'll need appropriate credentials (usually domain administrator credentials) to join the domain.
5. Restart: After entering the domain information and credentials, Windows will attempt to join the domain. If successful, it will prompt you to restart the computer.
6. Computer Name: After restarting, the computer name should remain the same unless there's a conflict. If there's a conflict, Windows will prompt you to enter a new name for the computer.
7. Domain Authentication: Upon restart, the computer will authenticate with the domain controller, and the domain administrator can manage the computer's settings and policies through Active Directory.

B. Establishing connectivity between client and server

Establishing connectivity between a client computer and a domain server in a Windows environment involves several steps.

Here's a general guide:

1. Physical Connectivity:

- Ensure that the client computer is physically connected to the network where the domain server resides. This usually involves connecting an Ethernet cable to a switch or router.

2. Network Configuration:
    - Make sure that the client computer has the correct network settings, including IP address, subnet mask, default gateway, and DNS server address. These settings can be configured manually or obtained automatically from a DHCP server.
3. Domain Join:
    - On the client computer, go to "Control Panel" > "System and Security" > "System" (or right-click on "This PC" and select "Properties").
    - Click on "Change settings" next to "Computer name, domain, and workgroup settings".
    - In the System Properties window, select the "Computer Name" tab, then click the "Change" button.
    - Choose the "Domain" option, enter the name of the domain you want to join, and click "OK".
    - You will be prompted to enter credentials with permissions to join the domain. Enter the username and password of an account with appropriate permissions, usually a domain administrator account.
    - After successfully joining the domain, you will be prompted to restart the computer.
4. Domain Controller Configuration:
    - Ensure that the domain controller is properly configured, running, and accessible on the network.
    - Check network connectivity to the domain controller from the client computer using tools like Ping or by trying to access shared resources on the server.
5. DNS Configuration:

  - Verify that the client computer's DNS settings point to the domain controller. DNS resolution is crucial for domain authentication and name resolution.
  - You can configure DNS settings manually on the client computer or through DHCP options provided by the network.
6. Firewall and Security Settings:
   - Make sure that firewall settings on both the client and server allow necessary traffic for domain communication. Windows usually prompts you to allow domain-related traffic when joining a domain.
7. Testing Connectivity:
   - After restarting the client computer, log in with a domain user account to verify that the domain connectivity is established correctly.
   - Test access to domain resources, such as shared folders or printers, to ensure proper integration with the domain.

C.Changing from Workgroup to domain

To change a client computer from a Workgroup to a domain and join it to a Windows Server domain, follow these steps:

1. Ensure Connectivity: Ensure that the client computer is connected to the network where the domain controller resides.
2. Domain Information: Have the domain name, username, and password of an account that has permissions to join computers to the domain.
3. Access Control Panel: On the client computer, go to Control Panel.
4. System Settings: Click on "System and Security" or simply "System", depending on your Control Panel view settings.
5. Change Settings: Look for the option "Change settings" or "Change settings on the computer name, domain, and workgroup settings".
6. Computer Name/Domain Changes: Click on "Change settings" to open the System Properties window. In the "Computer Name" tab, click the "Change" button.

7. Join Domain: In the Computer Name/Domain Changes window, select the "Domain" option. Enter the domain name in the appropriate field.
8. User Authentication: You will be prompted for credentials to join the domain. Enter the username and password of an account with permissions to join computers to the domain.
9. Domain Join Confirmation: After entering the correct credentials, you should receive a confirmation message indicating that the computer has successfully joined the domain.
10. Restart: Restart the computer for the changes to take effect.

<u>Topic2.6.2.Implementation of Delegation of control</u>

Delegation of control in Windows Server allows administrators to assign specific administrative tasks to non-administrative users or groups without granting them full administrative privileges. This can help distribute administrative responsibilities and enhance security by limiting access to only the necessary functions.

Here's a general outline of how to implement delegation of control in Windows Server:

1. **Identify tasks to delegate**: Determine which administrative tasks you want to delegate. These could include creating user accounts, managing printers, resetting passwords, etc.
2. **Create security groups:** Create security groups in Active Directory Users and Computers (ADUC) to represent the users or groups that will be granted delegated permissions. For example, you might create a "Help Desk Operators" group for users who will manage password resets.
3. **Delegate control:**

   a. Open Active Directory Users and Computers.
   b. Right-click on the Organizational Unit (OU), domain, or specific object (like a user or group) to which you want to delegate control.
   c. Select "Delegate Control" from the context menu.
   d. Follow the wizard to specify the users or groups to whom you want to delegate control and the specific tasks you want to delegate.

4. **Review and test permissions:** After delegating control, review the permissions assigned to ensure they align with your intended delegation. Test the delegated tasks with a user account to verify that the permissions work as expected.
5. **Regularly review and update**: Periodically review delegated permissions to ensure they remain appropriate and aligned with your organization's requirements. Remove any unnecessary delegations and update permissions as needed.
6. **Document:** Document the delegation of control including which tasks have been delegated, to whom, and any relevant policies or procedures.
7. **Monitor:** Implement monitoring mechanisms to track delegated activities and ensure compliance with organizational policies and security standards

Topic2.6.3.Description of Group Policy Object (GPO)

A.Types (Local, NonLocal, Starter)

Group Policy Objects (GPOs) are a crucial component of managing and configuring user and computer settings within a Windows Server environment.

There are three main types of GPOs:

1. Local GPOs:
    - Local GPOs are stored on individual computers and are applicable only to those specific machines.
    - They are typically used to define settings that are specific to a single computer and do not need to be applied across an entire domain.
    - Local GPOs can be configured using the Group Policy Editor (gpedit.msc) on individual computers.
2. Non-local GPOs:
    - Non-local GPOs are stored on a domain controller and are applicable to multiple computers within a domain.

   - These GPOs are applied to users and computers based on their location in the Active Directory (AD) hierarchy.
   - Non-local GPOs are commonly used to enforce uniform settings across an entire domain or organizational unit (OU).
3. Starter GPOs:
   - Starter GPOs serve as templates for creating new GPOs with pre-configured settings.
   - They can help streamline the process of creating new GPOs by providing a starting point with commonly used configurations.
   - Starter GPOs are stored in the Group Policy Objects container within the Group Policy Management Console (GPMC) and can be imported into a domain for use.

B.Hierarchy (local, Site, Domain, OU)

In Windows Server environments, Group Policy Objects (GPOs) are used to manage and configure various settings for users and computers within Active Directory domains. In Windows Server environments, particularly in Active Directory (AD), there's a hierarchical structure that helps organize and manage resources.

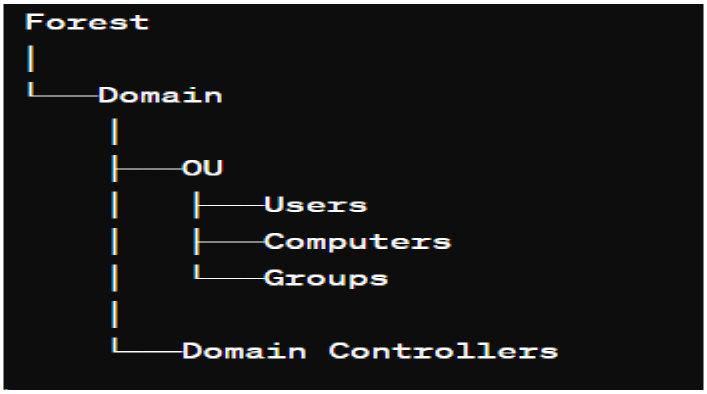
Here's a breakdown of the GPO hierarchy:

1. **Local**: This refers to settings or resources specific to an individual computer. It includes configurations like user accounts, groups, and security policies that are local to that machine.
2. **Site**: A site in Active Directory represents one or more IP subnets connected by fast and reliable network links. Sites help optimize network traffic and replication between domain controllers by grouping them based on their physical network topology. Sites are essential for distributed environments with multiple physical locations.
3. **Domain**: A domain is a logical grouping of computers, users, and devices in a network. It's administered as a unit with common rules and security settings. Domains can contain organizational units (OUs) and are typically

managed by domain controllers. They establish the security boundaries for authentication and access to resources within a network.

4. **Organizational Unit (OU)**: OUs are containers within a domain that can hold users, groups, computers, and other OUs. They provide a way to organize and manage resources with common administrative requirements. OUs are often used to delegate administrative tasks, apply Group Policy settings, and organize resources based on business or departmental structure.

Here's a visual representation:



```
Forest
|
└───Domain
     |
     ├───OU
     |    ├───Users
     |    ├───Computers
     |    └───Groups
     |
     └───Domain Controllers
```

- **Forest** represents the highest level and contains one or more domains.
- **Domain** represents a logical grouping of objects within a network.
- **OU** represents a container within a domain used for organizing objects and delegating administrative tasks.

C. Group Policy Object (GPO) and Group Policy Template (GPT)

Group Policy Object (GPO) and Group Policy Template (GPT) are essential components in managing and configuring Windows environments, particularly in a networked setting. Here's a breakdown of each:

i. **Group Policy Object (GPO):**
    - A Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for users and computers in a network.

- GPOs are primarily used in Windows Active Directory environments to enforce security settings, deploy software, configure system settings, and more.
- They provide a centralized way to manage configurations across multiple computers or users within a domain.
- GPOs can be linked to organizational units (OUs) in Active Directory, allowing administrators to target specific sets of users or computers with particular configurations.
- GPOs are stored on domain controllers and are replicated to all other domain controllers in the domain, ensuring consistency across the network.

ii. **Group Policy Template (GPT):**

- The Group Policy Template (GPT) is the physical storage location where Group Policy settings and configurations are stored on a Windows system.
- It consists of files and folders stored within the SYSVOL folder on domain controllers.
- The GPT contains two main folders: "Machine" and "User."

  -"Machine" contains settings that apply to computer objects in Active Directory.

  -"User" contains settings that apply to user objects in Active Directory.
- Within these folders, you'll find policy settings configured using Administrative Templates, Security Settings, Software Installation, Scripts, and more.
- The GPT is replicated to all domain controllers in a domain, ensuring that Group Policy settings are consistently applied across the network.
- When Group Policy is applied to a system, the GPT is read by the client machine, and the appropriate policies are enforced.

<u>Topic2.6.4.Manage GPO settings</u>

A.Creation of GPO

Creating a Group Policy Object (GPO) in Windows Server allows you to manage various settings and configurations for users and computers within an Active Directory domain.

Here's a basic guide on how to create a GPO:

1. Open Group Policy Management Console (GPMC):
   - On your Windows Server, open the "Server Manager" dashboard.
   - Go to "Tools" and select "Group Policy Management" from the list.
2. Navigate to the Domain:
   - In the GPMC, expand the forest and domain that you want to work with.
3. Create a New Group Policy Object:
   - Right-click on the Organizational Unit (OU) or domain where you want to link the GPO.
   - Select "Create a GPO in this domain, and Link it here."
4. Name the GPO:
   - Provide a descriptive name for the new GPO and click "OK".
5. Edit the GPO (Optional):
   - Right-click on the newly created GPO.
   - Select "Edit" to open the Group Policy Management Editor.
   - Here you can configure various settings under User Configuration and Computer Configuration.
6. Configure Settings:
   - Navigate through the settings available in the Group Policy Management Editor.
   - Configure the desired policies according to your requirements. You can control a wide range of settings related to security, network, software installation, etc.
7. Link the GPO to OUs:
   - After configuring the GPO, you need to link it to the appropriate Organizational Units (OUs) or domains.

- Right-click on the OU where you want to apply the GPO.
- Select "Link an Existing GPO" and choose the GPO you just created.

8. Enforce or Block Inheritance (Optional):
   - You can enforce the GPO to override conflicting settings from higher-level OUs or block inheritance if you don't want settings from parent OUs to affect the linked OU.
9. Apply and Test:
   - Once the GPO is linked, it will start applying to the users or computers in the specified OU.
   - Test the GPO thoroughly to ensure it behaves as expected.
10. Monitor and Troubleshoot:
    - Monitor the application of the GPO using tools like Group Policy Results or Group Policy Modeling.
    - If any issues arise, troubleshoot them by reviewing event logs and GPO settings.

B.GPO Editor

Group Policy Object (GPO) Editor in Windows Server is a management console that allows administrators to define and enforce system settings for users and computers within an Active Directory environment.

Here's how you can access and use the GPO Editor:

1. Open Group Policy Management Console (GPMC):
   - On Windows Server, you can access the GPMC by clicking on the Start menu and typing "Group Policy Management Console" or by running gpmc.msc in the Run dialog box.
2. Navigate to Group Policy Objects:
   - Once in the GPMC, expand your forest, domain, and organizational unit (OU) structure to locate the Group Policy Objects node.
3. Create or Edit a GPO:
   - Right-click on Group Policy Objects and select "New" to create a new GPO, or right-click on an existing GPO and select "Edit" to modify its settings.

4. Modify Group Policy Settings:
    - The Group Policy Management Editor will open, allowing you to configure various settings categorized under Computer Configuration and User Configuration. These settings cover a wide range of options, including security settings, software installation, script execution, and more.
5. Link the GPO:
    - Once you've configured the desired settings, you can link the GPO to the appropriate OU(s) by right-clicking on the OU and selecting "Link an Existing GPO."
6. Enforce or Block Inheritance:
    - You can enforce or block inheritance of GPOs at the OU level to control which policies apply to specific sets of users or computers.
7. Apply the GPO:
    - After linking the GPO, it will be applied to the users or computers within the specified OU(s) during the next Group Policy refresh interval.
8. Test and Verify:
    - It's essential to test the GPO changes in a non-production environment before applying them in a production environment. You can use tools like Group Policy Modeling and Group Policy Results to simulate and verify the application of GPOs.

C.Use of GPMC (Group Policy Management Console) to manage users

The Group Policy Management Console (GPMC) is a powerful tool in Windows Server for managing Group Policy Objects (GPOs) within Active Directory environments. While it primarily focuses on managing computer configurations, it can also be used to manage user configurations through the use of User Configuration settings within GPOs.

Here's a basic outline of how you can use GPMC to manage users in Windows Server:

1. Open GPMC: First, you need to open the Group Policy Management Console. You can do this by clicking on the Start button, then selecting Administrative Tools, and finally selecting Group Policy Management.
2. Create a New GPO: In the GPMC, you can create a new Group Policy Object by right-clicking on the domain or organizational unit (OU) where you want to apply the policy, then selecting "Create a GPO in this domain, and Link it here..." You can give the GPO a descriptive name.
3. Edit GPO Settings: Once you've created the GPO, you can edit its settings by right-clicking on it and selecting "Edit." This will open the Group Policy Management Editor, where you can configure various settings.
4. Configure User Settings: Within the Group Policy Management Editor, navigate to User Configuration settings. Here, you can configure policies that apply specifically to users within the scope of the GPO. These settings can include restrictions, permissions, software deployment, folder redirection, and more.
5. Apply GPO to Users: After configuring the desired user settings, close the Group Policy Management Editor. The GPO will automatically be applied to the users within the scope of the GPO (based on the domain or OU where it's linked).
6. Link GPO to OUs: If you want the GPO to apply to specific OUs containing user accounts, you can link the GPO to those OUs by right-clicking on the OU and selecting "Link an Existing GPO," then choosing the GPO you've created.
7. Enforce or Block Inheritance: You can enforce or block inheritance of GPOs at the OU level to control which GPOs apply to users within specific OUs. This allows for fine-grained control over policy application.
8. Test and Monitor: After configuring GPOs, it's important to test their effects in a controlled environment before deploying them widely. You can also use tools like Group Policy Results and Group Policy Modeling to monitor the application of policies and troubleshoot any issues.

LO3: Deploy web application

IC3.1.Introduction to Web Servers

Topic3.1.1. Definition of Web server

A **web server** is a software application or hardware device that serves content (such as web pages, images, videos, etc.) over the internet in response to requests from web browsers or other client applications. 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.

Topic3.1.2.Types of Web Servers/Web hosting Platform

1. IIS (Internet Information Services): Developed by Microsoft, IIS is a web server software for Windows servers. It's commonly used for hosting websites and web applications on Windows-based systems.
2. Apache HTTP Server: Apache is one of the most popular open-source web servers worldwide. It's known for its flexibility, stability, and robustness. Apache can run on various operating systems like Linux, Unix, Windows, and others.
3. Nginx (pronounced "Engine-X"): Nginx is a high-performance, open-source web server and reverse proxy server. It's well-known for its ability to handle a large number of concurrent connections efficiently. Nginx is often used as a reverse proxy server in front of other web servers like Apache to improve performance.
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"): Lighttpd is an open-source web server optimized for speed-critical environments. It's designed to be lightweight and efficient, making it suitable for serving high-traffic websites while consuming fewer system resources than some other web servers.

Topic3.1.3.Explain benefits and drawbacks of IIS

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

➢ **Benefits:**

1. Integration with Windows Environment: IIS is tightly integrated with the Windows operating system, making it easy to manage and administer for Windows administrators. It leverages features like Active Directory for authentication and authorization.
2. Scalability: IIS is highly scalable, capable of handling a large number of concurrent requests. It supports various application frameworks like ASP.NET, PHP, and Node.js, allowing developers to build scalable web applications.
3. Security Features: IIS provides robust security features, including SSL/TLS support, request filtering, IP address restrictions, and integration with Windows authentication mechanisms. It also supports advanced security configurations like Application Pool Identity and URL Authorization.

4. Performance Monitoring: IIS includes built-in performance monitoring tools that allow administrators to monitor server performance, diagnose issues, and optimize configurations for better performance.
5. Modular Architecture: IIS is built on a modular architecture, allowing administrators to install only the required components, reducing the attack surface and conserving system resources.

- **Drawbacks:**

1. License Cost: While IIS is included with Windows Server, some advanced features may require additional licensing costs. For example, using features like Microsoft Application Request Routing (ARR) for load balancing may require additional licensing.
2. Learning Curve: Configuring and managing IIS effectively requires knowledge of various components and configuration options. Administrators who are new to IIS may face a learning curve in understanding its features and best practices.
3. Resource Consumption: Like any web server, IIS consumes system resources such as CPU and memory. Improperly configured or overloaded IIS servers can lead to performance issues and downtime.
4. Limited Cross-Platform Support: While IIS is a robust web server for Windows environments, it has limited support for other operating systems. If you require cross-platform compatibility, alternatives like Apache or Nginx may be more suitable.
5. Vendor Lock-In: Using IIS ties you to the Windows ecosystem, which may limit your flexibility in adopting other platforms or technologies. If your organization prefers or requires a more heterogeneous IT environment, this could be a drawback.

IC3.2.Configure IIS With Windows Server

Topic3.2.1.Enabling DNS Server

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

Answer: Enabling the DNS server alongside configuring IIS on a Windows Server allows you to manage domain name resolution for your websites. DNS (Domain Name System) translates human-readable domain names into IP addresses, allowing clients to access websites using easy-to-remember names rather than numerical IP addresses.

Steps are involved in enabling the DNS server alongside configuring IIS are:

1. **Open Server Manager**: Go to the Start menu, click on "Server Manager" to open it.
2. **Add Roles and Features**: In Server Manager, click on "Manage" from the top-right menu and select "Add Roles and Features".
3. **Role-based or feature-based installation**: Choose "Role-based or feature-based installation" and click "Next".
4. **Select a server**: Ensure that the correct server is selected and click "Next".
5. **Select server roles**: Scroll down and select "DNS Server" from the list of roles. A pop-up window may appear asking you to add features that are required for DNS Server. Click on "Add Features" and then click "Next".
6. **Install DNS Server**: Review the information about the DNS Server role and click "Next".
7. **Confirmation**: Click "Install" to start the installation process. Once the installation is complete, click "Close".
8. **Configure DNS**: After the installation is finished, you can configure the DNS Server settings by opening the DNS Manager from the Tools menu in Server Manager.
9. **Configure DNS Zones**: Configure DNS zones, records, and other settings based on your network requirements.
10. **Verify Configuration**: Verify that the DNS Server is functioning correctly by performing DNS queries and ensuring that DNS resolution is working as expected. After the installation, you may want to configure your

DNS server settings as per your network requirements. This involves tasks such as creating forward and reverse lookup zones, configuring forwarders, setting up DNS records, etc.

11. **Testing:** Finally, it's essential to test your DNS server to ensure that it's functioning correctly. You can use tools like nslookup or perform DNS queries to verify proper functionality.

Other ways

Steps are involved in enabling the DNS server alongside configuring IIS are:

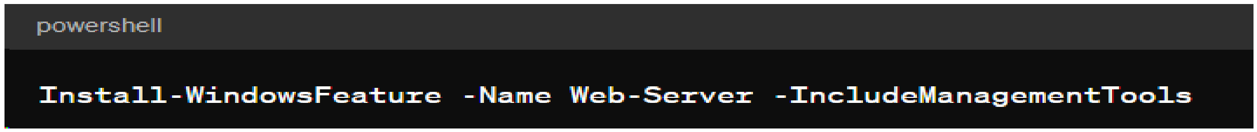
1. Install the DNS Server role on your Windows Server.
2. Open DNS Manager and create forward and reverse lookup zones for your domain.
3. Configure DNS records within these zones, such as A records for IPv4 addresses, AAAA records for IPv6 addresses, CNAME records for aliases, and MX records for mail servers.
4. Update IIS bindings to point to the appropriate hostnames or domain names, ensuring your websites are accessible via the configured names.
5. Test connectivity to verify DNS resolution is working correctly and your websites are accessible via domain names.

Topic3.2.2. Install IIS Role in selected Server

To install the IIS (Internet Information Services) role on a Windows Server and enable specific features like Enable HTTP Features, Enable ASP.NET, CGI Interface, Add FTP Feature, Enable HTTP Health and Diagnostics, Confirmation of IIS installation, Verify that IIS is installed successfully, you can use PowerShell commands.

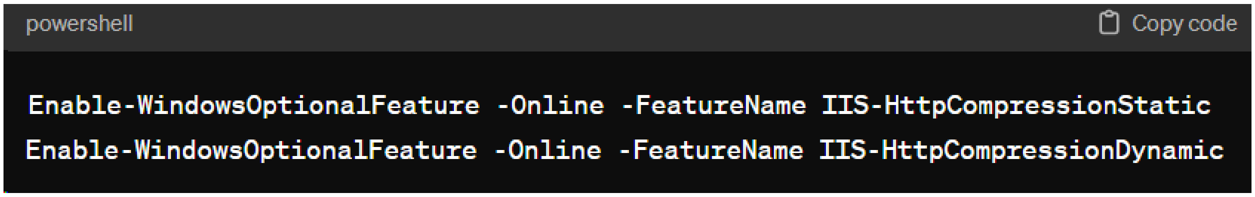
Here's a step-by-step guide:

1. **Open PowerShell as Administrator**: Right-click on the PowerShell icon and select "Run as Administrator" to open a PowerShell window with elevated privileges.
2. **Install the IIS Role:**



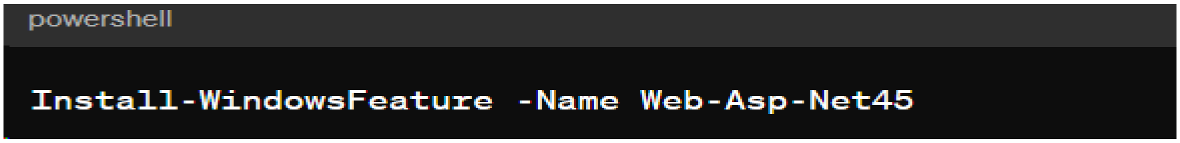
```powershell
Install-WindowsFeature -Name Web-Server -IncludeManagementTools
```

3. Enable HTTP Features:



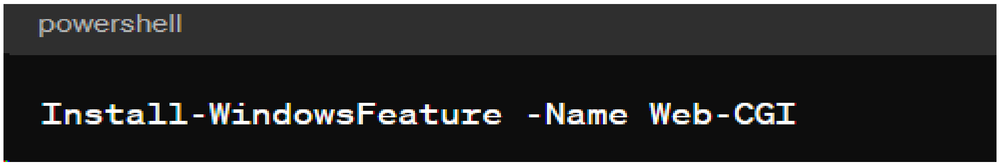
```powershell
Enable-WindowsOptionalFeature -Online -FeatureName IIS-HttpCompressionStatic
Enable-WindowsOptionalFeature -Online -FeatureName IIS-HttpCompressionDynamic
```

4. Enable ASP.NET:



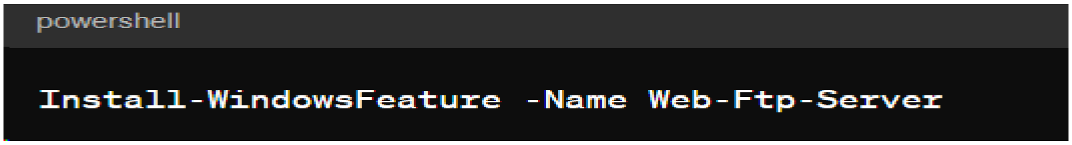
```powershell
Install-WindowsFeature -Name Web-Asp-Net45
```

5. Enable CGI Interface:



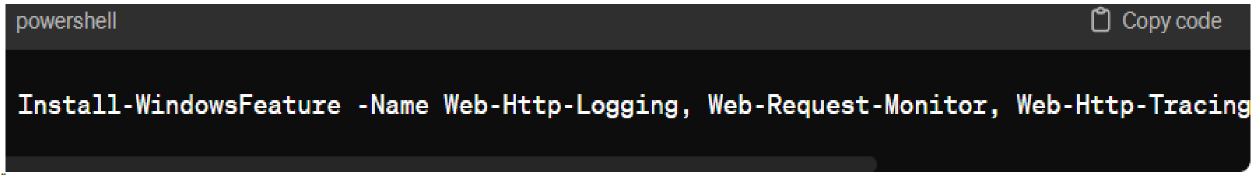
```powershell
Install-WindowsFeature -Name Web-CGI
```

6. Add FTP Feature:



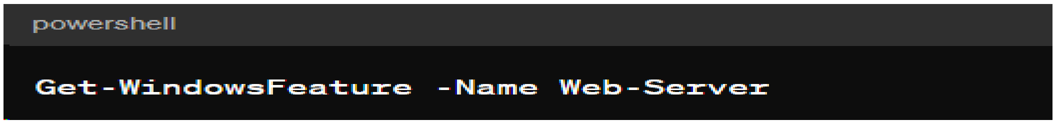
```powershell
Install-WindowsFeature -Name Web-Ftp-Server
```

7. Enable HTTP Health and Diagnostics:



```powershell
Install-WindowsFeature -Name Web-Http-Logging, Web-Request-Monitor, Web-Http-Tracing
```

8. Confirmation of IIS Installation:



```powershell
Get-WindowsFeature -Name Web-Server
```

9. **Verify that IIS is installed successfully**: You can open a web browser and navigate to **http://localhost**. If IIS is installed correctly, you should see the default IIS welcome page.

IC3.3.Management of IIS Web Server

Topic3.3.1.Explain 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). In simpler terms, it's like telling the server how to respond to different types of requests.

Here's how it works:

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: 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. If the request is for a dynamic web page (e.g., ASP.NET), IIS might pass the request to the ASP.NET handler for processing.
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.

Topic3.3.2.Explain 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. This ensures that the server can communicate properly within the network environment.
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). Connection tasks in this context involve configuring and managing these remote access methods, setting up user permissions, and ensuring secure remote connections.
3. **Firewall Configuration**: Windows Server includes a built-in firewall that helps protect the server from unauthorized access and malicious network traffic. Connection tasks related to the firewall include configuring firewall rules to allow or block specific types of traffic, opening ports for specific services, and monitoring firewall logs for suspicious activity.
4. **Network Monitoring and Troubleshooting**: Connection tasks also include monitoring network performance, identifying bottlenecks or connectivity issues, and troubleshooting network problems. This may involve using built-in Windows Server tools like Performance Monitor, Event Viewer, or Network Monitor, as well as third-party network monitoring software.
5. **DNS Configuration**: Domain Name System (DNS) is crucial for translating human-readable domain names into IP addresses. Connection tasks related to DNS involve configuring DNS servers, managing DNS zones and records, and troubleshooting DNS resolution issues.

6. **Active Directory Integration**: In a Windows Server environment, Active Directory (AD) is used for centralized authentication and management of network resources. Connection tasks in this context involve integrating servers with Active Directory domains, managing user accounts and group policies, and ensuring proper authentication and access control.
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. Connection tasks in virtual networking involve configuring virtual network settings, connecting virtual machines to virtual networks, and ensuring proper isolation and security between virtual networks.

Topic3.3.3.Explain FTP protocol

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.

Topic3.3.4.Explain 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. When you host multiple websites or web applications on a single server, site binding allows you to specify how incoming HTTP or HTTPS requests are routed to the appropriate site based on factors like domain name, IP address, and port number.

Here's how it works:

1. Domain Name: With HTTP or HTTPS site binding, you can associate each website hosted on the server with one or more domain names. When a request comes in, IIS examines the domain name specified in the request header and forwards the request to the corresponding site based on the binding configuration.
2. IP Address: You can also bind websites to specific IP addresses on the server. This means that if the server has multiple IP addresses assigned to it, you can control which website responds to requests on each IP address.
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. However, you can configure IIS to listen on alternative ports if needed.

4. Protocol (HTTP or HTTPS): Site binding allows you to specify whether a website should handle HTTP requests, HTTPS requests, or both. For HTTPS, you also need to configure SSL certificates to encrypt the data transmitted between the server and the client.

Topic3.3.5.Configure 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.
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.

IC.3.4. Setting environment of developed web app

Topic3.4.1. Explain hosting platforms available

A. Free hosting

Free hosting on a Windows server typically refers to the provision of web hosting services at no cost, where the server's operating system is based on Microsoft Windows. involves utilizing software packages like Internet Information Services (IIS) and SQL Server Express Edition, both of which are available at no cost.

B. Paid hosting

Paid hosting on a Windows server refers to the service of renting server space and resources from a hosting provider that runs Windows Server operating system

Topic3.4.2. Analysis of technical requirements for each hosting platforms:

A. Without backend server side

When analyzing technical requirements for hosting platforms on Windows Server without backend server-side processing, it's important to consider factors such as scalability, performance, security, and ease of management

B. With backend server side

Analyzing the technical requirements for hosting platforms on Windows Server with backend server-side functionality involves considering various factors such as server specifications, software dependencies, scalability options, security measures, and management tools.

Topic3.4.3. Verification of local web app to be deployed to the server.

To verify and deploy a local web application to a Windows Server, you can follow these general steps:

1. Prepare the Web Application:
   - Ensure your web application is properly developed and tested locally.
   - Make sure all necessary dependencies are included and configured.
   - Compile/minify your code if necessary.
2. Set Up the Server:
   - Make sure the Windows Server has Internet Information Services (IIS) installed. If not, you'll need to install it via Server Manager.
   - Configure IIS to serve your web application. You may need to set up a new website or application pool.
3. Transfer Files:
   - Copy your web application files (HTML, CSS, JavaScript, etc.) to the appropriate directory on the server. This is typically within the wwwroot folder of your IIS site.
4. Database Setup:
   - If your application requires a database, ensure it's set up on the server or on a separate database server. Update connection strings accordingly.
5. Configuration:
   - Update any configuration files (like web.config for .NET applications) to reflect server-specific settings such as database connection strings, API URLs, etc.
6. Testing:

- Test your deployed application to ensure everything is working as expected. Pay attention to any server-specific issues that may arise.

7. Security:
    - Implement necessary security measures, such as HTTPS, firewalls, and user authentication, depending on your application's requirements and the server environment.
8. Monitoring and Maintenance:
    - Set up monitoring tools to keep an eye on server performance and application health.
    - Establish a maintenance schedule for regular updates, backups, and security patches.

Topic3.4.4. Configuration of backend technology in IIS web Server

A. PHP Environment variables

Configuring a backend technology like PHP in IIS (Internet Information Services) on a Windows Server involves several steps, including setting up PHP environment variables.

Here's a basic guide to do that:

1. Install PHP:
    - Download the PHP installer for Windows from the official PHP website (https://www.php.net/downloads.php).
    - Follow the installation instructions provided with the installer. Make sure to note the installation directory.
2. Configure PHP:
    - Locate the php.ini file in the PHP installation directory. This file contains various settings for PHP.
    - Edit php.ini to configure PHP settings as needed. You may need to set options like extension_dir, error_log, display_errors, etc.
    - Save your changes to php.ini.
3. Configure IIS:

- Open Internet Information Services (IIS) Manager on your Windows Server.
- Navigate to your website/application in the Connections pane.
- Double-click on "Handler Mappings".
- Click on "Add Module Mapping..." from the Actions pane.
- Fill out the required fields:
    - Request path: *.php
    - Module: FastCgiModule
    - Executable: Path to php-cgi.exe (usually located in the PHP installation directory)
    - Name: PHP_via_FastCGI (or any preferred name)
- Click OK to save the mapping.

4. Set up Environment Variables:
    - Right-click on "This PC" or "My Computer" and select "Properties".
    - Click on "Advanced system settings" on the left-hand side.
    - In the System Properties window, click on the "Environment Variables..." button.
    - Under "System variables", click on "New..." to add a new variable.
    - Set the variable name to PHPRC and the variable value to the directory path where your php.ini file is located.
    - Click OK to save the variable.
5. Restart IIS:
    - After making these changes, it's recommended to restart IIS to ensure that the changes take effect.

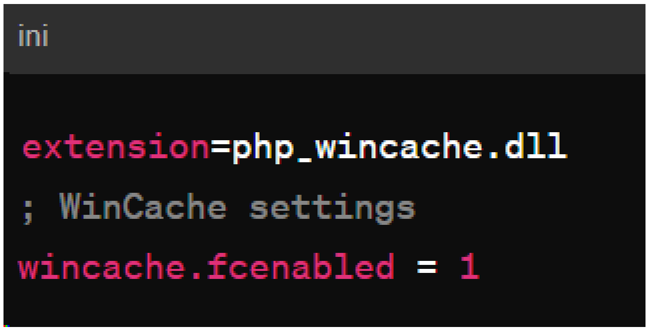
B. Configure WinCache for php web app

Configuring WinCache for a PHP web application on IIS involves several steps.

Here's a basic guide to get you started:

1. **Install PHP:** Make sure PHP is installed on your Windows Server and properly configured with IIS. You can download PHP from the official PHP website and follow their installation instructions.

2. **Install WinCache:** Download the appropriate version of WinCache for your PHP version and architecture (x86 or x64) from the Microsoft website. After downloading, run the installer and follow the installation instructions.
3. **Configure PHP to Use WinCache:** Open your php.ini file (located where PHP is installed, often in C:\PHP) and add or modify the following lines to enable WinCache:



```ini
extension=php_wincache.dll
; WinCache settings
wincache.fcenabled = 1
```

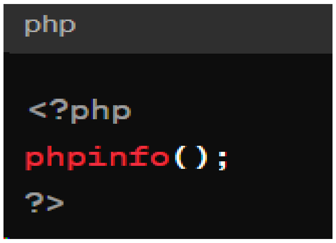
   You can adjust other WinCache settings as needed for your application.
4. **Configure IIS**: Open IIS Manager and select your website. Go to the "Handler Mappings" feature and ensure that PHP is mapped correctly. If not, you can add a FastCGI module mapping to point to the PHP-CGI executable.
5. **Restart IIS**: After making changes, it's a good idea to restart IIS to ensure that the changes take effect.
6. **Test**: Finally, test your PHP application to ensure that WinCache is working correctly. You can monitor WinCache statistics using tools like the WinCache admin dashboard or by checking performance metrics in Windows Performance Monitor.

C. FastCGI handler mapping for php web app

Configuring a PHP web application on an IIS web server in Windows Server via FastCGI handler mapping involves several steps.

Here's a general guide to help you set it up:

1. **Install PHP:** First, you need to install PHP on your Windows Server. You can download the PHP installer from the official PHP website (https://www.php.net/downloads.php) and follow the installation instructions.
2. **Install IIS:** Ensure that Internet Information Services (IIS) is installed on your Windows Server. You can install it through the 'Server Manager' dashboard in Windows.
3. **Install FastCGI Extension:** FastCGI is required to handle PHP requests efficiently. You can install the FastCGI extension through the 'Server Manager' dashboard by adding the 'CGI' feature.
4. **Configure FastCGI Settings:**
    - Open Internet Information Services (IIS) Manager.
    - Select your server in the Connections pane.
    - Double-click on "Handler Mappings" in the middle pane.
    - Click on "Add Module Mapping" in the Actions pane.
    - Fill out the required fields:
        - Request path: *.php
        - Module: FastCgiModule
        - Executable: Browse to the location of the PHP CGI executable (e.g., C:\PHP\php-cgi.exe)
        - Name: PHP_via_FastCGI
    - Click OK to save the mapping.
5. **Configure PHP Settings:**
    - Open the PHP configuration file (php.ini) located in the PHP installation directory.
    - Adjust settings such as cgi.fix_pathinfo (set it to 0 for security reasons), extension_dir, etc., according to your requirements.
    - Save the changes and close the file.
6. **Test Configuration:** Create a simple PHP file (e.g., info.php) with the following content:



```php
<?php
phpinfo();
?>
```

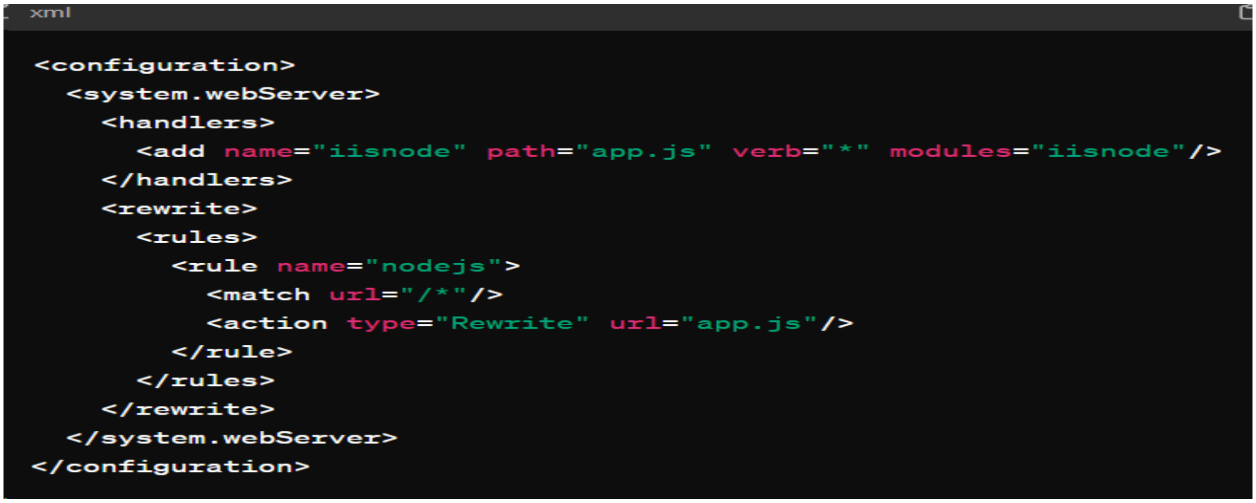
Place this file in your web directory (e.g., C:\inetpub\wwwroot).

7. **Restart IIS**: After making changes, it's a good practice to restart IIS to apply the configuration changes.
8. **Test PHP**: Open a web browser and navigate to http://localhost/info.php. You should see the PHP configuration information displayed. If it works, PHP is configured correctly on your IIS server.
9. **Security Considerations**: Ensure that you configure security settings appropriately, such as restricting access to sensitive files and directories, setting proper permissions, and configuring firewalls.

D. IISNode module for Node.Js web app

To configure a Node.js web application with IIS on a Windows server using the IISNode module, you'll need to follow these general steps:

1. **Install IIS**: Ensure that Internet Information Services (IIS) is installed on your Windows server. You can do this via Server Manager or PowerShell.
2. **Install Node.js:** Install Node.js on the server if it's not already installed. You can download the installer from the Node.js website and follow the installation instructions.
3. **Install IISNode:** Download and install the IISNode module for IIS. You can download it from the official GitHub repository or use a package manager like npm.
4. **Configure IISNode:** Once installed, you'll need to configure IISNode to work with your Node.js application. This typically involves creating a web.config file in the root directory of your Node.js application with specific settings for IISNode. Here's a basic example:



```xml
<configuration>
  <system.webServer>
    <handlers>
      <add name="iisnode" path="app.js" verb="*" modules="iisnode"/>
    </handlers>
    <rewrite>
      <rules>
        <rule name="nodejs">
          <match url="/*"/>
          <action type="Rewrite" url="app.js"/>
        </rule>
      </rules>
    </rewrite>
  </system.webServer>
</configuration>
```

Replace **app.js** with the entry point file of your Node.js application.

5. **Configure Node.js Application**: Ensure your Node.js application is set up properly. This includes installing dependencies using **npm**, setting up your server code, and configuring any environment variables.
6. **Start Node.js Application**: Start your Node.js application. You can do this manually by running the Node.js script, or you can configure it to run as a service using tools like **pm2**.
7. **Test Configuration**: Once everything is set up, test your configuration by accessing your web application through a browser. Ensure that it's running as expected without any errors.
8. **Monitoring and Maintenance**: Regularly monitor your Node.js application and server to ensure they are running smoothly. Set up logging and monitoring tools to track performance and diagnose any issues.

E. Configure web app environment security

Configuring backend technology in IIS (Internet Information Services) on a Windows Server involves several steps, especially when it comes to securing the web application environment. **Here's a general outline of the process:**

1. Install and Configure IIS:

- Ensure that IIS is installed on your Windows Server.
- Configure basic settings like ports, bindings, and website directories.

2. Install Backend Technology:
    - Depending on your application requirements, install the necessary backend technologies like ASP.NET, PHP, Node.js, etc.
    - Configure these technologies to work with IIS. For example, if you're using ASP.NET, ensure that the .NET framework is installed and properly configured.
3. Secure Communication:
    - Utilize HTTPS to encrypt communication between clients and the server.
    - Acquire and install an SSL/TLS certificate from a trusted certificate authority.
    - Configure IIS to use HTTPS and enforce SSL/TLS.
4. Authentication and Authorization:
    - Implement appropriate authentication mechanisms such as Windows Authentication, Forms Authentication, or OAuth.
    - Configure authorization rules to control access to resources based on user roles and permissions.
5. Firewall Configuration:
    - Configure the Windows Firewall to allow traffic on necessary ports for your web application.
    - Limit access to only the required ports and protocols.
6. Application Pool Security:
    - Create separate application pools for different web applications.
    - Set appropriate permissions for each application pool identity to restrict access to system resources.
7. Secure File System:
    - Apply the principle of least privilege by granting only necessary permissions to web application files and directories.

- Regularly monitor and audit file system permissions to prevent unauthorized access.

8. Secure Configuration Settings:
   - Review and secure configuration files such as web.config for ASP.NET applications, php.ini for PHP applications, etc.
   - Disable unnecessary features and services to reduce the attack surface.
9. Monitoring and Logging:
   - Enable logging in IIS to monitor and track web server activity.
   - Implement intrusion detection systems and security information and event management (SIEM) solutions to detect and respond to security incidents.
10. Regular Updates and Patch Management:
    - Keep the operating system, web server software, and backend technologies up to date with the latest security patches and updates.
    - Establish a patch management process to regularly apply updates and security fixes.
11. Security Testing:
    - Perform regular security assessments such as vulnerability scanning, penetration testing, and code reviews to identify and address security weaknesses.
12. Backup and Disaster Recovery:
    - Implement a robust backup and disaster recovery plan to ensure data integrity and business continuity in case of security breaches or system failures.

IC.3.5.Verify Server environment requirement

Topic3.5.1.Testing on local/remote computer/Server

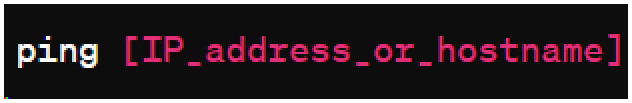
A. Network

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.

Here's a general guide:

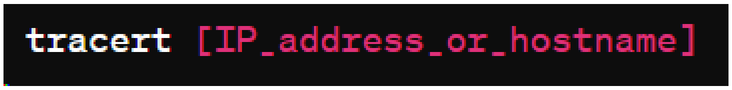
1. **Ping:** Use the ping command to check the connectivity between your server and other computers/servers on the network. Open Command Prompt and type:

   ```
   ping [IP_address_or_hostname]
   ```

   Replace **[IP_address_or_hostname]** with the IP address or hostname of the computer/server you want to test connectivity to.

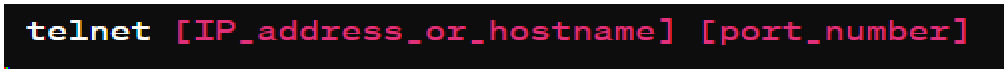
2. **Tracert**: Use the **tracert** command to trace the route that packets take from your server to the destination server. This can help identify network issues along the way. Open Command Prompt and type:

   ```
   tracert [IP_address_or_hostname]
   ```

   Replace **[IP_address_or_hostname]** with the IP address or hostname of the destination server.

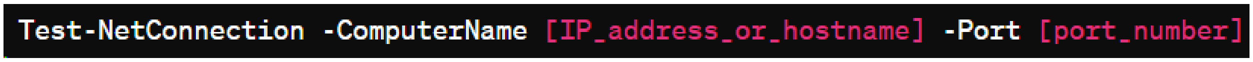
3. **Telnet**: Telnet can be used to test connectivity to a specific port on a remote server. Open Command Prompt and type:

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

   Replace **[IP_address_or_hostname]** with the IP address or hostname of the remote server, and **[port_number]** with the port you want to test.

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]
   ```

   Replace **[IP_address_or_hostname]** with the IP address or hostname of the remote server, and **[port_number]** with the port you want to test.

5. **Remote Desktop**: If you have Remote Desktop access to the remote server, you can connect to it and perform various tests directly on the server.
6. **Network Monitoring Tools**: Utilize network monitoring tools like Wireshark or Microsoft Message Analyzer to capture and analyze network traffic for troubleshooting purposes.

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.

Here's a general outline of how you might approach this:

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:
    - 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.
    - 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.
    - Security: Scan files with antivirus software to check for any potential threats or malicious content.
2. Remote Testing:

- File Transfer: Transfer the files to the remote server using secure methods like SSH or SFTP.
- File Integrity: After transferring, perform integrity checks on the remote server to ensure the files haven't been corrupted during transfer.
- Functionality: If applicable, execute the files on the remote server and verify their behavior.
- 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:
    - File Permissions: Ensure that the appropriate permissions are set on the server for accessing and executing the files.
    - Integration Testing: If the files are part of a larger system, conduct integration testing to ensure they work correctly within the server environment.
    - 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:
    - Keep detailed logs of the testing process, including any issues encountered and their resolutions.
    - Generate reports summarizing the testing results, including any anomalies or failures detected.

D.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:
    - Open Command Prompt.
    - Type ping localhost and press Enter. This tests basic network connectivity to your own machine.
2. Check Firewall:
    - Ensure that the firewall settings allow communication on the desired ports.
    - You can use the Windows Defender Firewall with Advanced Security tool to configure firewall rules.
3. Network Sharing:
    - If you're testing file sharing or any network service, ensure they're properly configured and accessible locally.

Testing Remote Visibility:

1. Ping Test:
    - From another machine on the same network, open Command Prompt.
    - 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:

- Review Event Logs: Look into the Event Viewer on the server for any relevant logs or errors that might indicate connectivity issues.
- Check DNS Settings: Ensure that DNS settings are correct, both on the server and the client machines, to resolve hostnames properly.
- Firewall Rules: Double-check that firewall rules on the server allow incoming connections on the required ports.
- 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.

Topic3.5.2.Verify 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.
3. Check Accessibility: Press Enter to navigate to the URL. If the URL is accessible locally, you should see the webpage or content associated with that URL displayed in the web browser.
4. Verify Content: Once the page loads, verify that the content displayed is what you expect. This confirms that the URL is accessible from the local server.
5. Firewall Settings: Ensure that any firewall settings on the server allow traffic on the port used by the web server or service hosting the content you're trying to access. If necessary, adjust firewall settings to allow access.

6. DNS Resolution: If you're using a domain name instead of IP addresses, ensure that DNS resolution is properly configured to resolve the domain name to the correct IP address.

B. Browsers

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

1. **Open a Web Browser**: Launch the web browser you want to verify. Common web browsers on Windows Server include Internet Explorer, Microsoft Edge, and Google Chrome (if installed).
2. **Enter the Local URL**: In the address bar of the web browser, type the URL of the local resource you want to access. For example, if you have a web server running on the local machine, you might type **http://localhost** or **http://127.0.0.1**.
3. **Check Access**: Press Enter to navigate to the local URL. If the web browser successfully loads the content from the local resource, it indicates that the browser is able to access local URLs on the Windows Server.
4. **Test with Different Browsers**: Repeat the above steps with other web browsers installed on the Windows Server to ensure they can also access local URLs.
5. **Firewall and Security Settings**: Ensure that any firewall or security settings on the Windows Server are configured to allow access to local resources via web browsers.
6. **Additional Troubleshooting**: If you encounter any issues, check the web browser's settings, network configuration, and any relevant logs for error messages that might provide clues to the problem.

C. 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

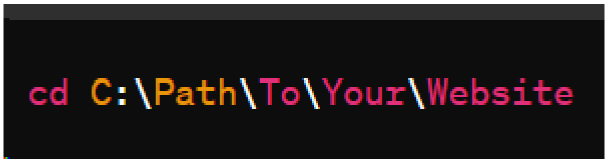
reload the page. You'll see a list of all the resources loaded by the page along with their load times.

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.
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.
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.

D. Website size

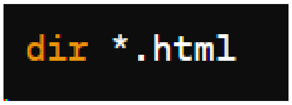
To verify the size of a local website hosted on a Windows server, you can follow these steps:

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

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.

IC.3.6. Hosting Web app

Topic3.6.1.Upload Web app to window Server

Sure, here's a general outline of the steps you would typically follow to upload a web application to a Windows Server:

1. Prepare Your Application: Make sure your web application is ready for deployment. This includes ensuring that all necessary files are included and any dependencies are installed.
2. Access Your Windows Server: Log in to your Windows Server where you want to deploy the web application. You can do this either directly or through remote desktop access.
3. Install Required Software: Ensure that the necessary software is installed on your Windows Server. This typically includes a web server like Internet Information Services (IIS) and any other runtime environments or frameworks your application requires.

4. Configure IIS: If you're using IIS, you'll need to configure it to host your web application. This involves creating a new site or application pool and setting up the appropriate bindings and permissions.
5. Copy Your Application Files: Transfer your web application files to the appropriate directory on the Windows Server. This could be the root directory for the default website or a subdirectory for a specific site or application.
6. Test Your Application: Once your application is deployed, test it to ensure that it's working correctly. Check for any errors or issues that may arise in the deployment process.
7. Set Up DNS: If your web application will be accessible over the internet, you may need to configure DNS settings to point to your Windows Server's IP address or hostname.
8. Monitor and Maintain: Regularly monitor your web application and server for performance, security, and any updates or maintenance tasks that may be required.

Topic3.6.2.Specify the physical path

To specify the physical path in Windows Server, you typically do so when configuring settings for web servers like Internet Information Services (IIS) or when working with file directories in general. Here's how you can specify a physical path:

1. **In Internet Information Services (IIS):**

a. Open the IIS Manager.

b. Navigate to the site or application for which you want to specify the physical path.

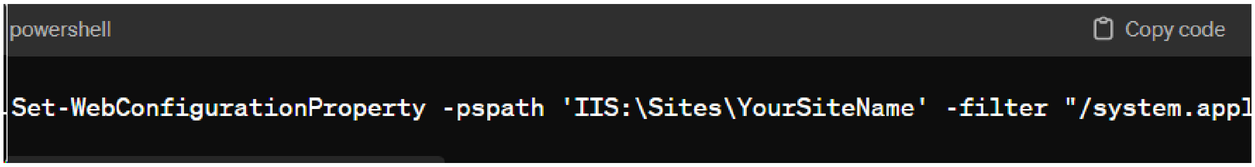
c. In the Features View, double-click on "Physical Path" under the "Basic Settings" for a site or application.

d. Enter the desired physical path in the text box provided.

e. Click "OK" to apply the changes.

2. **Using Command Line:**

You can also use the command line or PowerShell to specify the physical path. For example, in PowerShell, you can use the Set-WebConfigurationProperty cmdlet to modify the physical path of a site or application.



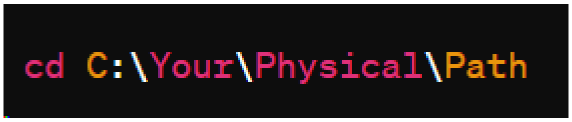
```
Set-WebConfigurationProperty -pspath 'IIS:\Sites\YourSiteName' -filter "/system.appl
```

Replace 'YourSiteName' with the name of your site/application and "C:\Your\Physical\Path" with the desired physical path.

3. **For File Directories:**

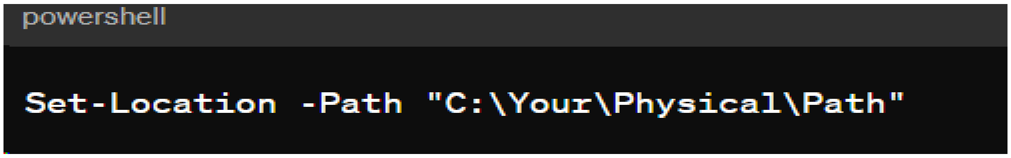
When working with file directories outside of web servers, you specify the physical path when creating, moving, or accessing files and folders using File Explorer or command-line tools like Command Prompt or PowerShell.

For example, to specify a physical path in Command Prompt:



```
cd C:\Your\Physical\Path
```

Or in PowerShell:



```
Set-Location -Path "C:\Your\Physical\Path"
```

These are general methods, and the exact steps may vary slightly depending on the specific version of Windows Server you are using and the configuration of your system.

Topic3.6.3.Select the protocols

Selecting protocols on a Windows Server involves enabling or disabling various networking protocols based on your requirements. Here's a general guide:

1. Open Network Connections: Press Windows Key + X and select "Network Connections" from the menu, or search for "Network Connections" in the Start menu.

2. Access Network Adapter Properties: Right-click on the network adapter you want to configure and select "Properties".
3. Select Protocols: In the Properties window, you'll see a list of items such as "Client for Microsoft Networks", "File and Printer Sharing for Microsoft Networks", "Internet Protocol Version 4 (TCP/IPv4)", "Internet Protocol Version 6 (TCP/IPv6)", etc. These represent different protocols and services.
4. Enable/Disable Protocols: Check or uncheck the box next to the protocol you want to enable or disable.
5. Configure Protocol Properties: For protocols like TCP/IP (both IPv4 and IPv6), you can click on them and then click the "Properties" button to configure settings such as IP address, subnet mask, default gateway, DNS server addresses, etc.
6. Apply Changes: After making changes, click "OK" or "Apply" to apply the changes and close the dialog boxes.
7. Restart if Necessary: In some cases, you might need to restart your network adapter or even the server for the changes to take effect.

Topic3.6.4.Specify the Ip Address

To specify an IP address in Windows Server, you can follow these steps:

1. Open Network Connections: Go to the Control Panel or use the search function to find "Network Connections" and open it.
2. Select the Network Adapter: You'll see a list of network adapters. Right-click on the one you want to configure and select "Properties."
3. Select IPv4 or IPv6: Depending on whether you want to configure an IPv4 or IPv6 address, select the appropriate option. Usually, you'll be dealing with IPv4.
4. Specify the IP Address: In the properties window, you'll see a section for IPv4 or IPv6 settings. Select "Use the following IP address" and enter the IP address you want to assign to the server.

5. Specify Subnet Mask and Default Gateway: Along with the IP address, you'll need to specify the subnet mask (which defines the network portion of the IP address) and the default gateway (the router's IP address for sending traffic outside the local network).
6. DNS Configuration (Optional): You may also want to specify DNS server addresses if you're not using DHCP for DNS resolution. You can do this in the same properties window by selecting "Use the following DNS server addresses" and entering the appropriate DNS server IPs.
7. Apply Changes: After entering all the necessary information, click "OK" or "Apply" to save the changes.
8. Verify Configuration: Once the changes are applied, it's a good idea to verify the configuration by opening a command prompt and using commands like ipconfig or ping to ensure that the server can communicate with other devices on the network.

Topic3.6.5.Configure Web app DNS

Configuring DNS for a web application on a Windows Server involves several steps.

Here's a basic guide to get you started:

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.
2. 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.
4. Test DNS Resolution:
    - Once you've added the DNS records, it's essential to test DNS resolution to ensure that your web application's domain name resolves to the correct IP address.
        - You can use tools like nslookup from the command line to perform DNS queries and verify the resolution.
5. Configure Web Server:
    - Ensure your web server (e.g., IIS) is configured to respond to requests for your domain name.
        - In IIS, you would typically set up a site binding for your domain name to direct incoming HTTP/HTTPS requests to the appropriate website or application.
6. Update Domain Registrar:
    - If your domain name is registered with a domain registrar, you need to update the DNS settings there to point to your Windows Server's DNS.
7. Monitor and Maintain:

- Regularly monitor your DNS configuration to ensure it's working correctly.
- Update DNS records as needed, especially if there are changes to your web application's infrastructure.

Topic3.6.6.Configure port number

To configure port numbers in Windows Server, you typically need to modify firewall rules or application settings, depending on what exactly you want to achieve. Here are some common scenarios:

1. **Windows Firewall:** If you want to allow traffic through a specific port on the Windows Firewall:
    - Go to Control Panel > System and Security > Windows Defender Firewall.
    - Click on "Advanced settings" on the left panel.
    - In the Windows Defender Firewall with Advanced Security window, click on "Inbound Rules" or "Outbound Rules" depending on your requirement.
    - Click on "New Rule..." on the right panel.
    - Choose "Port" as the rule type and click "Next."
    - Select either TCP or UDP and specify the port number(s) you want to configure. Click "Next."
    - Choose whether the rule should apply to all profiles or specific profiles (Domain, Private, Public). Click "Next."
    - Provide a name and description for the rule and click "Finish" to create it.
2. **Application Settings:** If you're configuring a specific application to use a different port, you'll usually need to consult the documentation for that application. Typically, there will be a configuration file or settings within the application itself where you can specify the port number it should listen on.

3. **IIS (Internet Information Services):** If you're configuring ports for websites hosted on IIS:
    - Open Internet Information Services (IIS) Manager.
    - In the Connections pane, expand the server node and click on "Sites."
    - Select the site you want to configure.
    - In the Actions pane, click on "Bindings."
    - Here you can add, edit, or remove bindings which include the port number.
4. **SQL Server:** If you're configuring SQL Server to listen on a specific port:
    - Open SQL Server Configuration Manager.
    - Navigate to SQL Server Network Configuration > Protocols for [Instance Name].
    - Double-click on TCP/IP.
    - In the TCP/IP Properties dialog, go to the "IP Addresses" tab.
    - Scroll down to find the IP Address section for the desired network interface.
    - Enter the desired port number in the "TCP Port" field.
    - Click "OK" to save the changes.

Topic3.6.7.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:

1. 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.
2. 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.

3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. Implement Preventive Measures: Take steps to prevent similar errors from occurring in the future. This may include implementing monitoring

tools, improving system redundancy, or revising procedures to avoid common pitfalls.

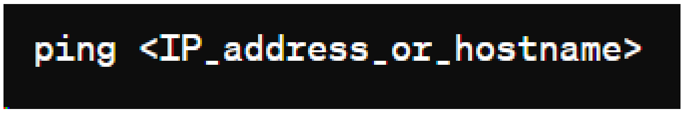
12. Monitor for Recurrence: After resolving the error, monitor the system for any recurrence of the issue. This ensures that the problem has been fully addressed and helps identify any lingering or related issues.

IC3.7. Verification of successfully hosted Web app

Topic3.7.1.Testing accessibility within a local Network

To test accessibility within a local network on a Windows Server, you can perform several checks and use various tools. Here are some common methods:

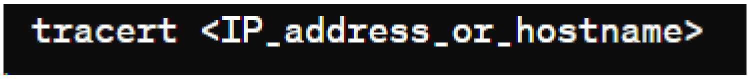
1. **Ping Command:** Use the ping command to test connectivity between devices within the network. Open Command Prompt and type:



```
ping <IP_address_or_hostname>
```

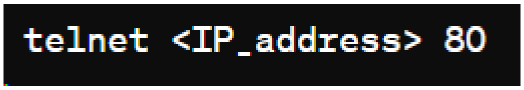
Replace **<IP_address_or_hostname>** with the IP address or hostname of the target device you want to test connectivity with.

2. **Tracert Command**: This command traces the route that packets take to reach a destination. It can help identify where connectivity issues occur. Use:



```
tracert <IP_address_or_hostname>
```

3. **Telnet**: Telnet can be used to check if a specific port is open and reachable on a remote device. For example, to test if port 80 (HTTP) is open on a device with IP address **<IP_address>**, use:

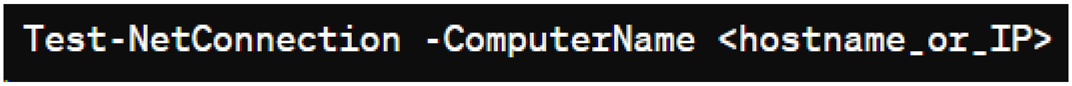


```
telnet <IP_address> 80
```

If the command succeeds, it means the port is open and reachable.

4. **Advanced IP Scanner**: This is a GUI-based tool that scans your network and shows connected devices along with their IP addresses. It's useful for visually identifying devices on the network.

5. **Windows PowerShell**: PowerShell provides various cmdlets for network testing. For example, you can use **Test-NetConnection** to diagnose connectivity to a remote host:



```
Test-NetConnection -ComputerName <hostname_or_IP>
```

   This command tests the connection to the specified hostname or IP address.

6. **Network Monitoring Tools**: Tools like Wireshark or Microsoft Message Analyzer can help diagnose network issues by capturing and analyzing network traffic.
7. **Firewall Settings**: Ensure that the Windows Firewall (or any other firewall software) is properly configured to allow traffic within the local network.

Topic3.7.2.Testing online accessibility

Testing online accessibility in a Windows Server environment involves ensuring that users can connect to and interact with resources and services hosted on the server over a network connection. Here are some steps you can take to test online accessibility:

1. Ping Test: Use the ping command from a client computer to check if it can reach the Windows Server. Open the command prompt and type ping <server_ip> replacing <server_ip> with the actual IP address of the server. If successful, it indicates that there is network connectivity between the client and the server.
2. Remote Desktop Connection: If Remote Desktop is enabled on the Windows Server, attempt to establish a Remote Desktop session from a client computer. Go to "Start" > "Remote Desktop Connection" and enter the IP address or hostname of the server. If successful, you'll be prompted to enter your credentials and will gain access to the server desktop.
3. File Sharing: Share a folder on the Windows Server and attempt to access it from a client computer. This will test whether file sharing is functioning

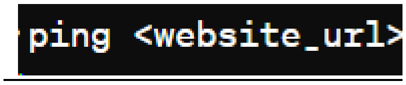
correctly. Try accessing the shared folder by navigating to \\<server_ip> in File Explorer and see if you can view and access the shared files.

4. Web Services: If the server hosts any web services or websites, try accessing them from a web browser on a client computer. Enter the URL of the website hosted on the server and ensure that it loads without any errors.
5. Database Connectivity: If the server hosts a database, ensure that clients can connect to it. Test database connectivity from client applications or utilities using the appropriate connection string and credentials.
6. Firewall Configuration: Check the Windows Firewall settings on the server to ensure that necessary ports are open for communication. Depending on the services hosted, you may need to open specific ports to allow inbound traffic.
7. VPN Connection: If the server is accessible via VPN, connect to the VPN from a client computer and then attempt to access server resources as if you were on the local network.
8. Network Monitoring Tools: Utilize network monitoring tools to analyze traffic between the client and the server. This can help identify any issues such as packet loss or latency that may be impacting accessibility.

Topic3.7.3.Testing online website speed

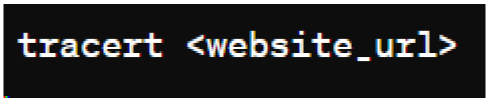
To test the speed of an online website on a Windows Server, you can use various tools and methods. Here's a basic approach using command-line tools:

1. **Ping Command**: This will give you an idea of the latency between your server and the website.



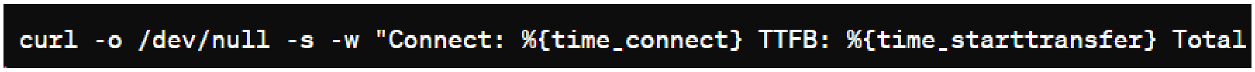
```
ping <website_url>
```

2. **Traceroute Command**: This will show you the path that packets take from your server to the website, indicating any delays or bottlenecks.

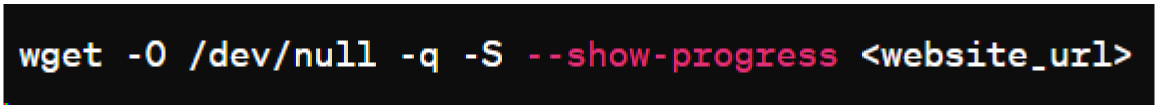


```
tracert <website_url>
```

3. **curl or wget Command**: These tools allow you to download content from a website and measure the time it takes



```
curl -o /dev/null -s -w "Connect: %{time_connect} TTFB: %{time_starttransfer} Total
```



```
wget -O /dev/null -q -S --show-progress <website_url>
```

4. **Third-party Online Tools**: There are many online services like GTmetrix, Pingdom, or Google PageSpeed Insights that can provide comprehensive website speed tests. These tools often offer detailed analysis and recommendations for improvement.
5. **Windows Performance Monitor**: You can use Performance Monitor to monitor various performance metrics of your server while accessing the website to identify any resource constraints or bottlenecks.

Topic3.7.4.Verify size of online web app

To verify the size of an online web application hosted on a Windows server, you can follow these steps:

1. Remote Desktop Connection: Connect to the Windows server where the web application is hosted using Remote Desktop Connection or any other remote access tool you prefer.
2. Navigate to the Web Application Directory: Once connected, navigate to the directory where your web application is stored. Typically, web applications are stored in directories like C:\inetpub\wwwroot for IIS (Internet Information Services).
3. Check Directory Size: Right-click on the folder containing your web application, select "Properties," and it should display the size of the folder, including all files and subdirectories within it.
4. Analyze Specific Files: If you want to analyze the size of specific files within the web application, you can navigate into the directory and check the properties of individual files or subdirectories.
5. Command Line Option (Optional): Alternatively, you can also use command-line tools like PowerShell to get the size of directories and files.

For example, you can use the Get-ChildItem cmdlet in PowerShell with the -Recurse parameter to get the size of all files and directories recursively.