**Learning outcome 1: Manage Server Services**

* 1. **Introduction to server administration**
     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. **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. **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.

**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.

**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.

**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.