MICROSOFT SERVER

• Windows Server 2016 installation requirements

Windows Server 2016 installation requirements include a minimum of 512 MB of RAM for the Essentials edition and 2 GB for Standard and Datacenter editions. Additionally, you'll need at least 32 GB of available disk space for the installation.

• Describe Windows Server 2016 editions.

Windows Server 2016 offers several editions tailored to different organizational needs: Essentials, Standard, and Datacenter. Essentials is suited for small businesses with up to 25 users and 50 devices. Standard is suitable for physical or minimally virtualized environments, while Datacenter is ideal for highly virtualized and software-defined data center environments, providing unlimited virtualization rights.

• From which menu we can add and remove server roles?

From manage menu we can add and remove server role.

• What is workgroup?

A workgroup is a peer-to-peer network where individual computers share resources such as files, printers, and internet connections without the need for a centralized server. In a workgroup, each computer maintains its own security settings and user accounts, making it suitable for small networks or home environments.

• What is domain?

A domain is a centralized network infrastructure in which computers, users, and resources are managed and authenticated by a domain controller. It provides centralized security, management, and administration, allowing for seamless access to resources across the network.

• What is powershell?

It is designed to automate system administration tasks and manage various aspects of Windows operating systems and applications. PowerShell allows users to execute commands, access system objects, and perform tasks using a consistent syntax and framework.

• up gradation v/s migration

Upgradation involves moving from an older version to a newer version of software or operating system within the same environment, preserving existing settings and configurations. Migration, on the other hand, involves moving data, applications, or systems from one environment to another.

• license and activation model

The license and activation model for software typically involves acquiring a license to legally use the software and activating it to validate the license. Activation usually involves inputting a unique product key or license code provided by the software vendor to unlock the full functionality of the software.

• Precaution of up gradation.

1. Backup: Ensure that you have a complete backup of all important data and configurations before starting the upgrade process to prevent data loss.
2. Compatibility: Verify compatibility with existing hardware, software, and dependencies to avoid compatibility issues during or after the upgrade.
3. Testing: Conduct thorough testing in a non-production environment to identify and address any potential issues or conflicts before performing the upgrade in the production environment.

• Migration limitation.

Migration limitations include compatibility issues leading to functionality loss, potential data loss if not carefully managed, and required downtime impacting business operations. Additionally, the complexity of the migration process can result in increased costs, resource allocation, and potential errors.

• What is the advantages of server core.

Server Core offers advantages such as reduced resource usage, improved security due to a smaller attack surface, simplified management with fewer components to maintain, and increased reliability with fewer updates and reboots required.

• What is Nano server.

Nano Server is like a super-small version of Windows Server that's made for running specific tasks, especially in modern, cloud-based environments. It's incredibly streamlined, meaning it doesn't have all the extra features and bloat that you might find in a regular Windows Server installation. Because of this, it's faster, uses fewer resources, and is more secure. It's great for running things like cloud-native applications and containers, where efficiency and speed are really important. You usually control it remotely using special tools instead of directly interacting with it like you would with a regular computer.

• Purpose of Nano server.Top of Form

The purpose of Nano Server is to provide an extremely lightweight and efficient platform for running cloud-native applications and containerized workloads. It's designed to be highly scalable, fast, and secure, making it ideal for modern, dynamic IT environments.

• Compare GUI v/s core v/s Nano server.

1. **GUI (Graphical User Interface)**: Provides a full graphical interface, ideal for traditional server workloads.
2. **Server Core**: Minimal installation without the GUI, reduces attack surface, and is suitable for core infrastructure services.
3. **Nano Server**: Ultra-lightweight, headless, and designed for container hosts or specific workloads.

• Assign dual IP address on lan card.

1. Open the **Network Connections** window by pressing Windows Key + R, typing ncpa.cpl, and hitting Enter.
2. Right-click on the network adapter (Ethernet or Wi-Fi) and select **Properties**.
3. Scroll down to **Internet Protocol Version 4 (TCP/IPv4)** and click on it, then click **Properties**.
4. In the IPv4 properties window, select **Use the following IP address** and enter the first IP address, subnet mask, and default gateway.
5. Click on the **Advanced** button to open the Advanced TCP/IP Settings window.
6. Under the **IP Settings** tab, click on the **Add** button to enter additional IP addresses and subnet masks.
7. After adding the desired IP addresses, click **OK** on all windows to apply the changes.

• Upgrade server 2012 to server 2016.

1. **Backup and Recovery Plan**:
   * Before proceeding, **take a backup** of your server and ensure you have a **recovery plan** in place.
2. **Download Windows Server 2016 ISO**:
   * **Download the Windows Server 2016 ISO file** from the **Microsoft website**.
3. **Mount and Run Setup**:
   * **Mount the ISO file** (you can use tools like Virtual CloneDrive or built-in Windows features).
   * Run the setup.exe file from the mounted ISO.
4. **Select “Upgrade” Option**:
   * During the installation process, choose the **“Upgrade”** option.
   * This will perform an **in-place upgrade**, moving from Windows Server 2012 to Windows Server 2016 while staying on the same physical hardware.

• Change computer name.

Setting > system > about > rename this pc

* install nano server.

Done in lab.

* manage and configure a nano server.

Done in lab

* compare GPT and MBR

mbr = support up to 2 tb and four primary partition compatible with legacy bios

gpt = it support more than 2 tb and 128 partitions and compatible with uefi firmware.

* different between VHD and VHDX.

Certainly! Here’s a concise comparison between **VHD** and **VHDX**:

* **VHD**:
  + Older format.
  + Maximum drive size: Approximately 2.2TB.
  + Widely supported by third-party virtualization software.
  + Commonly used for testing and compatibility.
* **VHDX**:
  + Newer version of VHD.
  + Maximum drive size: Supports up to 64TB.
  + Offers data protection and better performance.
  + Mainly used in Hyper-V environments
* what is SMB and NFS.

SMB (Server Message Block) and NFS (Network File System) are file access storage protocols used for efficient file sharing over a network.

* what is sharing permission.

When user share a folder, user set the permissions for that folder, determining the type of access others have to it across the network. They typically have three different levels of sharing: Full Control, Change, and Read.

* what is NTFS permission.

NTFS permissions, introduced with Microsoft Windows NT, control access to files and folders on Windows systems formatted with the NTFS file system. They allow you to restrict who can access files using allow or deny permissions.

* what is resource ownership.

Resource ownership refers to the control and permissions assigned to users or groups for accessing files and folders within a file system. It determines who has the authority to read, write, or execute specific files or directories.

* what is storage pool.

A storage pool is a collection of physical storage devices, such as hard drives or solid-state drives, combined to function as a single storage unit.

* what is basic disk and dynamic disk.

Basic Disk: This is the traditional disk storage configuration in Windows. It supports primary partitions, extended partitions, and logical drives.

Dynamic Disk: Dynamic disks offer more advanced features compared to basic disks, such as support for volumes that span multiple disks (spanned, striped, and mirrored volumes), as well as fault tolerance through mirroring and striping. Dynamic disks are primarily used in environments requiring advanced disk configurations, such as RAID setups or dynamic volume management.

* what is simple volume , spanned volume.

simple volume is a single block of space, while a spanned volume combines space from multiple disks, but neither offers fault tolerance.

* describe RAID 0 , RAID 1 , RAID 5, RAID 6 , RAID 1 0.

Raid 0 = in this type data will be stored 50-50 % on both hdd.

Raid 1 = in this type data will be 100% copied to another hdd.

Raid 5/6 = in this type data stored in multiple hdd with comparession.

Raid 10 = this type is combination of 0 and 1 data will be stored 50-50 and this will be copied to another hdd.

* describe DAS, NAS and SAN.

DAS is directly connected to a single server, NAS provides file-level storage over a network, and SAN offers block-level storage accessible by multiple servers over a dedicated network.

* what is virtualization.

Virtualization is the process of creating a virtual (rather than actual) version of something, such as a server, storage device, network, or operating system.

* type of virtualization and compare it.

Virtualization encompasses various types, including server, desktop, storage, network, and application virtualization.

Server virtualization divides a physical server into multiple virtual servers, improving resource utilization and scalability.

Desktop virtualization centralizes desktop environments for flexibility and simplified management.

Storage virtualization abstracts storage resources, enhancing management and scalability.

Network virtualization creates logical network segments for easier management and resource optimization.

Application virtualization isolates applications for easier deployment and improved compatibility.

* Describe hyper v

Hyper-V is a hypervisor-based virtualization platform developed by Microsoft for creating and managing virtualized environments. It allows users to run multiple operating systems (such as Windows, Linux, and others) concurrently on a single physical machine.

* what is remote management of hyper v.

Remote management of Hyper-V refers to the ability to manage Hyper-V virtualization hosts and virtual machines (VMs) from a remote location using management tools or interfaces. This allows administrators to control Hyper-V servers without physically accessing them, improving efficiency and flexibility in managing virtualized environments.

* what is hyper v manager.  
  Hyper-V Manager is a graphical user interface (GUI) tool provided by Microsoft for managing Hyper-V virtualization hosts and virtual machines (VMs).
* what is virtual machine and nested virtualization

A virtual machine (VM) is a software-based emulation of a physical computer that runs its own operating system and applications as if it were a separate physical machine. Multiple VMs can run concurrently on a single physical host, sharing the underlying hardware resources such as CPU, memory, storage, and network interfaces.

Nested virtualization refers to the ability to run a virtual machine within another virtual machine. In other words, it allows you to create VMs inside VMs.

* what is dynamic memory.

Dynamic memory, also known as memory ballooning, is a feature in virtualization environments that allows the allocation of memory to virtual machines (VMs) to dynamically adjust based on workload demand.

* what is NUMA.

NUMA stands for Non-Uniform Memory Access. It's a computer memory design used in multiprocessor systems, where each processor has its own local memory. In a NUMA architecture, memory access times can vary depending on whether the data is stored locally to the processor accessing it or on a remote memory module accessed by another processor.

* describe Virtual Machine functions.

They facilitate workload consolidation, resource optimization, and flexibility in IT environments. VMs host guest operating systems and applications, enabling efficient resource management, mobility through features like live migration, and simplified backup and recovery with snapshot capabilities.

* describe Hyper v functions.

Hyper-V provides a comprehensive set of functions for creating, managing, and securing virtualized infrastructure, making it a versatile and widely used platform for server virtualization in both on-premises and cloud environments.

* what is check point.

a checkpoint refers to a snapshot or saved state of a virtual machine (VM) at a particular point in time. Checkpoints capture the VM's memory, disk, and device state, allowing users to revert to that state later if needed.

* hyper v networking—virtual nic , hyper v switch.

vNICs provide network connectivity within VMs, while Hyper-V Virtual Switches act as the conduit for network traffic between VMs, physical network adapters, and external networks in Hyper-V virtualized environments.

* hyper v storage---vhd ,vhdx , fixed size, dynamic expanding.

VHDX is the recommended disk format for new Hyper-V deployments due to its advanced features and improved performance. When provisioning virtual disks, administrators can choose between fixed-size and dynamic expanding options based on their storage requirements and performance considerations.

* create a checkpoint.

Done in lab

* P4 create a virtual hdd (vhd) and attach to virtual machine.

Done in lab.

* describe containers.

Containers are lightweight, portable, and isolated environments that package applications and their dependencies together. Unlike virtual machines (VMs), which include a full operating system, containers share the host operating system's kernel and resources, making them more efficient and faster to deploy.

* What is docker?  
  Docker is a platform for developing, shipping, and running applications using containerization technology. It allows developers to package applications and their dependencies into standardized units called containers, which can be easily deployed across different environments, such as development, testing, and production.
* hyper v containers and windows containers

Hyper-V containers provide stronger isolation through VM-level isolation, while Windows containers offer lightweight, process-level isolation.

* install windows container.

Done in lab.

* install container in core server.

Done in lab.

* install container in Nano server.

Done in lab.

* hyper v live migration

**Hyper-V Live Migration** is a powerful feature that allows you to seamlessly move running virtual machines (VMs) from one physical server to another without causing any noticeable downtime for users.

* What is high availability?

**High availability (HA)** refers to a system or service’s ability to remain operational and accessible even in the face of failures or disruptions. It ensures that critical applications or resources are consistently available to users, minimizing downtime and maintaining a reliable user experience.

* What is cluster, quorum and witness?

Cluster: A group of interconnected servers that provide high availability and fault tolerance. Clusters ensure seamless failover when one server fails.

Quorum: The minimum number of voting elements (nodes or resources) required for a cluster to function. It establishes majority decisions.

A witness is an additional resource used to achieve and maintain quorum, especially in clusters with an even number of members.

* describe cluster storage.

A cluster in the context of storage refers to a group of interconnected servers (also known as nodes) that work together as a single storage unit.

* What is NLB?

NLB efficiently balances network traffic, ensuring high availability and optimal resource utilization for critical applications.

* importance of network in Failover and NLB.

a robust network infrastructure is essential for both failover mechanisms and effective NLB operation, ensuring uninterrupted service delivery and optimal resource utilization.

* Install and configure failover cluster for hyper v.

Done in lab.

* install and configure NLB for web server.

Done in lab.

* What is WSUS and why is it important?

WSUS (Windows Server Update Services) is a tool by Microsoft for managing Windows and Microsoft product updates, crucial for network security by automating update distribution.

* Describe WSUS architecture.

WSUS architecture comprises server and client components. The server manages update distribution, while clients connect to retrieve and install updates.

* How does WSUS synchronize updates, products, and classifications?

WSUS synchronizes with Microsoft Update to download updates, categorizing them by product and classification for efficient deployment.

* What is a WSUS group and how is it useful?

WSUS allows administrators to organize computers into groups, simplifying targeted update deployment by managing updates based on group membership.

* What are the default port numbers and policies associated with WSUS?

Default port numbers for WSUS are 8530 for HTTP and 8531 for HTTPS. Policies define WSUS operation, including update approval and installation settings.

* Define backup and restore and list the types of backup.

Backup involves creating data copies for protection against loss, while restore retrieves data from backups. Types of backup include full, incremental, and differential.

* Explain the difference between incremental and differential backup. Incremental backups store changes since the last backup, while differential backups store changes since the last full backup, offering different approaches to data storage and recovery.
* What is a full server backup and why is it important?

Full server backup involves copying all data on a server, ensuring comprehensive recovery capability in the event of system failure, vital for data integrity and business continuity.

* What is a full server backup and why is it important?

Full server backup involves copying all data on a server, ensuring comprehensive recovery capability in the event of system failure, vital for data integrity and business continuity.

* What is the purpose of the Performance Monitor?

Performance Monitor is a Windows tool for monitoring system performance, including CPU, memory, disk, and network usage, aiding in troubleshooting and optimization efforts.

* install and configure wsus server.

Done in lab.

* apply update to particular client group through wsus.

Done in lab.

**Module: 2**

* Describe DNS operation.

DNS operation involves queries for translating domain names to IP addresses. Iterative queries involve the DNS server providing a referral to another server if it doesn't have the requested information, while recursive queries involve the DNS server resolving the query entirely on behalf of the client.

* DNS query—Iterative and Recursive.

There are two types of DNS queries: iterative and recursive. In an iterative query, the DNS server provides referrals to other servers if it doesn't have the requested information, requiring the client to continue the query process. In a recursive query, the DNS server resolves the query entirely on behalf of the client, obtaining the requested information from other servers if necessary.

* what is forward lookup zone and its resource type.

A forward lookup zone maps hostnames to IP addresses. Its resource type typically includes A (Address) records, AAAA (IPv6 Address) records, CNAME (Canonical Name) records, and others.

* what is reverse lookup zone and its resource type.

A reverse lookup zone maps IP addresses to hostnames. Its resource type usually includes PTR (Pointer) records.

* what is conditional forwarder .

A conditional forwarder is a DNS server configuration that forwards queries based on specific domain names to designated DNS servers rather than using standard DNS resolution methods.

* what is primary zone, secondary zone and stub zone.

Primary zone contains the master copy of the zone data, secondary zone contains a read-only copy of the zone data transferred from the primary server, and stub zone contains only information about authoritative name servers for the zone.

* what is active directory integrated zone.

An Active Directory integrated zone stores zone data in the Active Directory database, providing better integration and replication capabilities.

* primary server, secondary server, cache only server.

Primary servers host the original copies of zone data, secondary servers obtain zone data through zone transfers from primary servers, and cache-only servers do not store zone data but only cache DNS information temporarily.

* what is aging and scavenging .

Aging and scavenging are processes used to manage stale records in DNS zones by marking records as stale and eventually removing them from the DNS database.

* what is MX record.

An MX (Mail Exchange) record specifies the mail server responsible for receiving email on behalf of a domain, allowing email messages to be routed correctly across the internet.

* Purpose of dhcp?

DHCP (Dynamic Host Configuration Protocol) automates the assignment of IP addresses and other network configuration parameters to devices on a network, simplifying network administration and ensuring efficient IP address management.

* What is DORA process?

DORA (Discover, Offer, Request, Acknowledge) is the four-step process that DHCP clients and servers use to allocate IP addresses and other network configuration parameters. The client sends a Discover message to locate DHCP servers, servers respond with an Offer containing IP address leases, the client selects an offered lease and sends a Request, and the server acknowledges the lease with an Acknowledge message.

* What is authorized DHCP server?

An authorized DHCP server is a DHCP server that has been explicitly approved by an administrator to provide IP address leases on a specific network segment, ensuring network security by preventing unauthorized DHCP servers from operating on the network.

* What is dhcp relay agent?

A DHCP relay agent forwards DHCP messages between clients and DHCP servers across different network segments, allowing DHCP clients on one subnet to obtain IP address leases from DHCP servers on another subnet.

* Describe scope, lease duration, DHCP option, exclude address.

A DHCP scope is a range of IP addresses available for lease to clients on a specific subnet. Lease duration specifies the length of time a client can use an assigned IP address. DHCP options are additional configuration parameters, such as DNS server addresses or domain names, provided to clients along with their IP address lease. Exclude addresses are IP addresses within a DHCP scope that are reserved and not assigned to clients.

* describe ipconfig command.

The "ipconfig" command is used in Windows operating systems to display the current TCP/IP network configuration settings of a computer, including IP address, subnet mask, default gateway, and DNS servers.

* instal dhcp sever and make authorize.

Done in lab.

* create a scope and check on client by ipconfig.

Done in lab.

* dhcp database and take backup.

The DHCP database stores lease information, client configurations, and other DHCP server data. Regular backups of the DHCP database are essential to prevent data loss in case of server failure or corruption.

* dhcp failover.

DHCP failover is a feature that provides high availability for DHCP services by replicating DHCP configuration and lease information between two DHCP servers, ensuring continuity of service in the event of a server failure.

* dhcp filter.

DHCP filtering allows administrators to control which clients can obtain IP address leases from the DHCP server based on their MAC address or other criteria, enhancing network security by restricting access to authorized devices.

* dhcp reservation.

DHCP reservation is a feature that allows administrators to assign a specific IP address to a client device based on its MAC address, ensuring that the device always receives the same IP address lease from the DHCP server.

* what is IPAM and purpose of IPAM .

IPAM stands for IP Address Management, which is a framework for planning, tracking, and managing IP address space within a network. The purpose of IPAM is to efficiently allocate and utilize IP addresses, prevent IP address conflicts, and streamline network administration tasks.

* why need dedicated server.

A dedicated server for IPAM is necessary to ensure reliable and efficient management of IP addresses, as it requires dedicated resources and capabilities to handle IP address allocation, tracking, and monitoring effectively.

* policy for ipam sever .

IPAM servers typically have policies configured to enforce IP address assignment rules, subnet allocations, DHCP and DNS configurations, and security measures to safeguard IP address space and network infrastructure.

* which service monitor and manage by IPAM.

IPAM monitors and manages IP address assignment, DHCP (Dynamic Host Configuration Protocol) configuration, DNS (Domain Name System) services, subnet utilization, IP address conflicts, and overall network health to ensure efficient IP address management and optimal network performance.

* Install IPAM.

Done in lab.

* configure IPAM.

Done in lab.

* create dhcp scope using IPAM 4 create DNS zone.

Done in lab.

* check monitoring of services.

Done in lab.

* What is VPN?  
  VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, such as the internet, allowing users to access private networks and resources remotely.
* type of VPN.

Remote Access VPN: Allows individual users to connect to a private network securely over the internet.

Site-to-Site VPN: Establishes secure connections between multiple sites or networks over the internet.

* tunnelling protocol .

Tunneling protocols, such as PPTP (Point-to-Point Tunneling Protocol), L2TP/IPsec (Layer 2 Tunneling Protocol with IPsec), and OpenVPN, are used to encapsulate and encrypt data packets for secure transmission over the internet.

* authentication protocol .

Authentication protocols, such as PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), and EAP (Extensible Authentication Protocol), verify the identity of VPN users and ensure secure access to the network.

* what is routing

Routing is the process of determining the path that data packets should take from the source to the destination across a network. In the context of VPNs, routing involves directing encrypted data packets through the VPN tunnel to the appropriate destination within the private network.

* install routing and remote access.

Done in lab.

* configure LAN routing.
* Done in lab.
* configure vpn connection (VPN client).
* Done in lab.
* what is Radius server?

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting management for users attempting to access network resources.

* what is authentication authorization and accounting.

Authentication verifies the identity of users, authorization determines the resources users can access, and accounting tracks user activity for auditing and billing purposes.

* RADIUS server operation method and radius client

RADIUS servers operate by receiving authentication requests from RADIUS clients, such as network access servers or wireless access points, and then verifying the credentials against its database or forwarding the request to a backend server for authentication.

* RADIUS port number

The default port number for RADIUS is UDP port 1812 for authentication and UDP port 1813 for accounting.

* What is network policies (NPS)?

Network Policy Server (NPS) is Microsoft's implementation of a RADIUS server for Windows Server environments, providing centralized authentication, authorization, and accounting services for network access.

* P1 configure RADIUS for wireless client.

Done in lab.

* configure NPS for remote access.

Done in lab.

* What is ip address? And type of ip address.

An IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. Types of IP addresses include IPv4 and IPv6.

* class of ip address.

Class A: 0.0.0.0 to 127.255.255.255 (1.0.0.0 to 126.255.255.255 are usable addresses)

Class B: 128.0.0.0 to 191.255.255.255 (128.0.0.0 to 191.255.255.255 are usable addresses)

Class C: 192.0.0.0 to 223.255.255.255 (192.0.0.0 to 223.255.255.255 are usable addresses)

Class D: 224.0.0.0 to 239.255.255.255 (reserved for multicast addresses)

Class E: 240.0.0.0 to 255.255.255.255 (reserved for experimental use)

* public ip address and private ip address.

Public IP addresses are globally unique addresses assigned by ISPs, while private IP addresses are used within a private network and cannot be routed over the internet.

* What is NAT?

NAT (Network Address Translation) is a technique used to remap one IP address space into another by modifying network address information in the IP header of packets.

* What id gateway address?

A gateway address is the IP address of a device on a network that serves as an access point or router to another network.

* What is loopback address?

A loopback address (127.0.0.1 in IPv4) is a special IP address used to send network packets back to the same device for testing or troubleshooting purposes.

* different type of ipv6 address.

Different types of IPv6 addresses include unicast, multicast, and anycast addresses, each serving different purposes in IPv6 networking.

* ipv6 tunneling.

IPv6 tunneling is a technique used to encapsulate IPv6 packets within IPv4 packets for transmission over networks that do not yet support IPv6 natively.

* IPv6 address automatically.

IPv6 addresses can be configured automatically using stateless address autoconfiguration (SLAAC) or stateful DHCPv6.

* ping utility.

Ping utility is used to send ICMP Echo Request messages to test the reachability of a host on an IP network.

* Ipconfig.

Ipconfig is a command-line utility used to display the current TCP/IP configuration of a computer, including IP address, subnet mask, and default gateway.

* tracert / traceroute.

Tracert (Windows) or traceroute (Unix/Linux) is a command-line tool used to trace the route that packets take from one host to another on an IP network, showing the IP addresses of routers along the path.

* dhcpv6.

DHCPv6 is an extension of DHCP for IPv6 networks, used to automatically assign IPv6 addresses and other configuration parameters to devices on a network.

* What is DFS? And purpose of DFS.

DFS (Distributed File System) is a technology used to organize and manage distributed file resources across a network.

The purpose of DFS is to provide users with a unified view of files and folders from multiple file servers, improving accessibility, scalability, and fault tolerance.

* Define DFS namespace and DFS replication.

A DFS namespace is a logical view of shared folders from multiple servers as a single hierarchical structure, allowing users to access files and folders using a single UNC (Universal Naming Convention) path.

DFS replication is a feature of DFS that enables files to be replicated and synchronized between multiple servers, ensuring data availability and redundancy.

* What is folder target?

A folder target is a network share hosted on a file server that is part of a DFS namespace. It represents the physical location where files are stored and accessed by users, providing fault tolerance and load balancing capabilities within the DFS infrastructure.

* install DFS namespace and replication.

Done in lab.

* configure common namespace.

Done in lab.

* configure replication and check.

Done in lab.

* configure branch cache.

Done in lab.

* What is SDN?

SDN (Software-Defined Networking) separates network control from data forwarding, enabling centralized management and automation.

* What is SCVMM?

SCVMM (System Center Virtual Machine Manager) is a Microsoft tool for simplifying the management of virtualized infrastructure, including VM provisioning and monitoring in private cloud environments.

**Module = 3**

* what is domain controller?   
  A domain controller is a server that authenticates users, stores user account information, and manages access to network resources within a Windows domain.
* describe forest, domain, tree, schema, OU, container, site, subnet.

Forest: A collection of one or more domain trees that share a common schema, configuration, and global catalog.

Domain: A logical group of network objects, such as computers, users, and devices, that share a common namespace and security policies.

Tree: A hierarchical arrangement of domains in a Windows Active Directory environment where child domains are subdomains of a parent domain.

Schema: Defines the structure and attributes of objects in Active Directory, ensuring consistency and compatibility across the forest.

OU (Organizational Unit): A container within a domain used to organize and manage objects, such as users, groups, and computers, with common administrative requirements.

Container: A generic Active Directory object used to store other objects, such as users or groups, but does not support the application of Group Policy.

Site: A collection of well-connected IP subnets that represent physical locations in a network, used for optimizing replication traffic and facilitating client authentication.

Subnet: A range of IP addresses used to segment a network into smaller, manageable parts.

* what is active directory?

Microsoft's directory service that stores information about objects on a network and makes this information available to users and network administrators.

* what is global catalog server?

A domain controller that holds a full replica of all objects in the forest, facilitating cross-domain searches and authentication requests.

* what is ADC AND RODC?

ADC (Active Directory Domain Controller) and RODC (Read-Only Domain Controller) are different types of domain controllers, with RODCs designed for branch office deployments with limited physical security.

* what is operation master role?

Operation Master Role: Also known as FSMO (Flexible Single Master Operations), these roles are responsible for managing specific functions within an Active Directory forest.

* type of operation master role and describe all role.

Schema Master: Manages changes to the Active Directory schema.

Domain Naming Master: Controls the addition or removal of domains from the forest.

RID Master: Allocates unique security identifiers (SIDs) to objects within a domain.

PDC Emulator: Provides backward compatibility with earlier Windows clients and manages time synchronization.

Infrastructure Master: Maintains object references and group membership across domains.

* difference between transferring and seizing role.

Transferring a role involves gracefully moving the role from one domain controller to another, while seizing a role forcibly takes control of the role when the original holder is unavailable or unresponsive.

* password policy

Password policy defines the requirements for passwords, including length, complexity, and expiration settings, to enhance security.

* what id profile and type of profile?

Profile: Stores user-specific settings and configurations, including desktop appearance and application preferences.

Local Profile: Stored on the local computer and applicable only to that specific machine.

Roaming Profile: Stored on a network server and synchronized with the user's workstation, allowing consistent settings across multiple devices.

* group nesting and scope, type of group

Group nesting refers to the practice of placing one group as a member of another group, allowing for more granular control over permissions and access.

Types of groupe scope

Domain Local Group: Used to assign permissions within a domain.

Global Group: Used to organize users who share similar access requirements across multiple domains.

Universal Group: Used to organize users and groups from multiple domains for broader access management.

Top of Form

* install ADDS and create a new forest

done in lab.

* give membership of pc to domain

done in lab.

* create a ADC .

done in lab.

* create RODC and password replication.

done in lab.

* create a new user with GUI and CLI.

done in lab.

* create roaming profile.

done in lab.

* create OU and give delegation.

done in lab.

* create a group.

done in lab.

* transfer roles—PDC, RID , schema master.

done in lab.

* describe account policy.

Account policies in Windows environments define rules and settings related to user account security. They typically include password policies, such as minimum password length, complexity requirements, and password expiration settings. Additionally, account policies may include settings for account lockout thresholds and Kerberos authentication.

* describe account lockout policy .

The account lockout policy determines the conditions under which a user account is locked out after a certain number of failed login attempts. It includes parameters such as the maximum number of failed login attempts allowed, the duration of the lockout period, and whether to reset the lockout counter after a certain period of time.

* what is trust relationship &type of trust relationship describe all trust.

A trust relationship in a Windows domain environment establishes a secure communication pathway between domains, allowing users in one domain to access resources in another domain.

One-way incoming trust: Allows users in the trusting domain to access resources in the trusted domain.

One-way outgoing trust: Allows users in the trusted domain to access resources in the trusting domain.

Two-way trust: Allows users in both domains to access resources in each other's domains.

* What is site and subnet ?

a site is a logical grouping of well-connected network segments (subnets) that represent physical locations in a network. Sites are used to optimize replication traffic and facilitate client authentication by associating network resources with their physical locations. Subnets, on the other hand, are ranges of IP addresses used to divide a network into smaller, manageable parts, typically corresponding to specific physical locations or network segments.

* manage active directory offline.

Done in lab

* restore object of active directory from AD Recycle bin.

Done in lab.

* backup active directory.

Done in lab.

* manage active directory replication---repadmin DcDiag.

Done in lab.

* create multiple UPN suffix multidomain enviourment.

Done in lab.

* configure trust between forest check with login.

Done in lab.

* configure ADDS sites and subnet.

Done in lab.

* What is group policy?

Group Policy is a feature in Microsoft Windows that allows administrators to manage and enforce specific settings, configurations, and security policies across a network of computers.

* What is default policy? Default Domain and domain controller .

Default policies are predefined sets of configurations applied to all users or computers within a domain. The Default Domain Policy applies settings to all users and computers in the domain, while the Default Domain Controller Policy applies settings specifically to domain controllers.

* what is user configuration and computer configuration.

User Configuration and Computer Configuration are sections within Group Policy Objects (GPOs) that allow administrators to configure settings for user accounts and computer systems, respectively.

* What is GPO?

GPO (Group Policy Object) is a container for a collection of policy settings that can be linked to Active Directory containers, such as sites, domains, or organizational units (OUs), to apply configurations to users and computers.

* define software setting, windows setting, and administrative templates .

Software Settings, Windows Settings, and Administrative Templates are categories within Group Policy that organize different types of policy settings:

Software Settings: Policies related to software installation and deployment.

Windows Settings: Policies that control Windows operating system features and behaviors.

Administrative Templates: Preconfigured settings for various Windows components, applications, and services.

* link GPO.

Linking GPOs involves associating a GPO with an Active Directory container, such as a domain, OU, or site, to apply its configured settings to users and computers within that container.

* delegation GPO management.

Delegation of GPO management allows administrators to assign specific permissions to users or groups to manage GPOs, such as editing settings, linking GPOs, or viewing GPO results.

* inheritance policy.

Inheritance policy refers to the process by which settings from higher-level containers, such as domains or OUs, are inherited by lower-level containers, unless explicitly blocked or overridden.

* filtering .

Filtering allows administrators to control which users or computers within a container receive the settings defined in a GPO, based on criteria such as security group membership or WMI filters.

* script, template.

Scripts: Custom scripts (e.g., PowerShell scripts, batch files) that can be executed as part of GPO processing.

Templates: Configuration files containing predefined settings for specific applications or Windows components, such as Administrative Templates.

* backup restore import and copy GPO.

Done in lab.

* force group policy command.

Done in lab.

* check group policy settings.

Done in lab.

* configure folder redirection.

Done in lab.

* software installation ---assign and publish .

Done in lab.

* drive map through policy.

Done in lab.

* purpose of certification .

The purpose of certification is to validate and authenticate the identity of individuals, devices, or services within a network or online environment, ensuring secure communication and access to resources.

* certificate service and its role service –certificate authority, certificate enrolment policy web service.

Certificate Services is a Windows Server role that provides a framework for issuing and managing digital certificates. It includes the Certificate Authority (CA) role service, which issues and manages certificates, and the Certificate Enrollment Policy Web Service, which provides policy-based certificate enrollment services.

* standalone v/s enterprise CA .

Standalone CA operates independently and issues certificates for a single domain or organization, while Enterprise CA integrates with Active Directory and issues certificates based on predefined policies and templates.

* root CA and subordinate CA .

Root CA is the top-level authority in a certificate hierarchy, responsible for issuing and managing certificates for subordinate CAs. Subordinate CAs are lower-level authorities that issue certificates on behalf of the root CA, often for specific purposes or within defined organizational units.

* describe certificate templates and how to use it.

Certificate templates are predefined configurations that specify the format, properties, and intended use of certificates issued by a CA.

* install certified services ---certificate authority and web enrolment .

done in lab.

* issue certificate through web enrolment and make secure web site .

done in lab.

* self-signed certificate .

done in lab.

* mange certificate---using template and issue certificate for computer .

done in lab.

* backup CA

done in lab.

* what is federation services

Federation Services, commonly referred to as ADFS (Active Directory Federation Services), is a Windows Server role that provides single sign-on (SSO) and identity federation capabilities across organizational boundaries.

* ADFS service component .

Federation Server: Manages trust relationships with external identity providers and issues security tokens to enable SSO.

Federation Proxy: Allows external users to authenticate and access resources within the organization's network securely.

Web Application Proxy: Provides reverse proxy functionality for publishing internal web applications securely to external users.

* ADFS requirement

Active Directory Domain Services (AD DS)

Certificate services for SSL certificates

Server hardware meeting minimum requirements

DNS configuration for ADFS endpoints

* multifactor authentication

Multifactor authentication (MFA) enhances security by requiring users to provide additional verification beyond username and password, such as a code sent to a mobile device or biometric data.

* web application proxy .

Web Application Proxy (WAP) is a component of ADFS that allows organizations to securely publish internal web applications to external users without requiring VPN access.

* multifactor authentication.

Multifactor authentication (MFA) is a security feature that requires users to provide additional authentication factors, such as a code sent to a mobile device or biometric data, to access resources or services, enhancing security beyond just a username and password.

* what is ADRMS.

ADRMS (Active Directory Rights Management Services) is a server software for information rights management (IRM) that works with Active Directory to protect sensitive information from unauthorized access.

* how to secure data and type of security .

Encryption: Encrypting data to prevent unauthorized access or disclosure.

Rights Management: Applying specific permissions and restrictions to data, such as viewing, editing, or printing rights.

Policy Enforcement: Implementing policies that govern how data can be accessed, used, and shared.

* what is service account.

A service account is a special user account used by services or applications to access network resources or perform specific tasks. In the context of ADRMS, a service account may be used to run ADRMS-related services and processes, ensuring that they have the necessary permissions and access rights to function properly.