**MCSA ASSIGNMENT**

**Module 3**

**Active directory domain services**

* 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.

Doneinlab

* 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.