Module : 14 Identity With Windows Server

1) A domain controller (DC) is a server that manages network and identity security requests for a domain.
2) A forest can contain one or more domain container objects, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. The first domain in the forest is called the forest root domain.
3) A partition trust relationship in a server is a communication and administration link between two domains that allows users and groups to access resources in both domains.

- This is done through an Active Directory (AD) trust, which connects two Active Directory domains or forests.

4) Active Directory (AD) is a directory service that helps organizations manage and secure their IT infrastructure.
5) The global catalog is a feature of Active Directory (AD) that allows a domain controller (DC) to provide information on any object in the forest, regardless of whether the object is a member of its domain.
6) ADC stands for Application Delivery Controller

- RODC stands for Read-Only Domain Controller

7) The operation master role in a server is a Flexible Single Master Operation (FSMO) role, which is a task set that ensures the consistency of the Active Directory database.
8) In windows 5 FSMO roles

- Schema Master – one per forest. Domain Naming Master – one per forest. Relative ID (RID) Master – one per domain. Primary Domain Controller (PDC) Emulator – one per domain.

9) Difference of Transferring and Seizing FSMO Roles.

- Transferring makes the old DC know that it does not own the roles any more.
- If the DC is broken (e. g. hardware defect) and will never come back again, then you can seize the role on a remaining DC.

10) Password policies for servers, such as those in Active Directory, are a combination of security and user impact. They can be configured to meet a variety of requirements, including.
11) A server profile is a collection of key server configuration details, such as network connectivity, BIOS settings, and firmware levels. A profile can also refer to a runtime environment, which includes all the files that the server processes.
12) Group nesting is the process of putting one group inside another group in Active Directory (AD).

- The scope of a group in AD determines the area it covers within a domain tree or forest, and the types of groups it can contain.

13) An account policy is a set of security rules that govern how users interact with a computer or domain.

- Account policies can include rules for passwords, failed logins, and account lockouts.

14) An account lockout policy is a security measure that prevents unauthorized access to a user account by disabling it after a certain number of incorrect password attempts.

15) Trust relationships are an administration and communication link between two domains.

16) There are many types of trust relationships that can be used in a server.

- One-way trust
- Two-way trust
- Transitive trust
- Non-transitive trust
- Implicit trust
- Explicit trust
- Parent-child trust
- Tree-root trust
- Shortcut trust
- External trust
- Forest trust

17) A Site is a collection of subnets that are connected by high-speed links, while a subnet is a group of neighboring computers that are connected by routers.
18) Group Policy is a Microsoft Active Directory (AD) feature that allows IT administrators to manage user and computer settings across a domain.
19) A default policy is a set of rules that govern access to a device or system when no other policy applies.

- Default domain policy: A Group Policy Object (GPO) that applies to all users and computers in a domain. It's created automatically when a server is promoted to a domain controller. This policy is used to manage default account settings, such as password and account lockout policies.
- Domain controller: A computer that is a part of a domain.

20) Computer configuration and user configuration are settings that apply to a computer or a user, respectively, and are defined in Group Policy Objects (GPOs).
21) A Group Policy Object (GPO) is a collection of policy settings that can be used to control Windows operating systems and policies.
22) Software settings, Windows settings, and administrative templates are all policy settings that

can be used in Group Policy to manage machines and users in an Active Directory environment.

23) A GPO can be associated (linked) to one or more Active Directory containers, such as a site, domain, or organizational unit.

24) GPO delegation is a technique that allows you to assign different permissions and roles to different users or groups for managing GPOs.

25) Inheritance policy in a server allows you to reuse a policy without having to redefine it at each level of a policy tree.

26) Server-side filtering occurs on the web server after the user's input has been submitted.

- It's a crucial step in ensuring data integrity and security.

27) A script template is a packaged script that can be reused.

28) Server certificates enable encrypted connections, guaranteeing the confidentiality and integrity of data transferred between users and servers.

29) Certificate services on a server, such as Active Directory Certificate Services (AD CS), are responsible for issuing, managing, and validating digital certificates.

- Certification Authority (CA)

- Verifies the identity of users, computers, and organizations by issuing digitally signed certificates. CAs can also manage, revoke, and renew certificates.
- Certificate Enrollment Policy Web Service (CEP)
- Allows users and computers to retrieve information about their certificate enrollment policy. This includes the location of the CAs and the types of certificates requested from them.

30) The main difference between a standalone CA and an enterprise CA is that an enterprise CA requires Active Directory Domain Services (AD DS) membership, while a standalone CA does not.

31) The main difference between a root CA and a subordinate CA is that a root CA is not certified by any other CA, while a subordinate CA is certified by a root CA.

32) A certificate template is a set of rules and settings that a Certification Authority (CA) uses to process certificate requests.

33) Active Directory Federation Services (AD FS) is a single sign on (SSO) feature developed by Microsoft that provides safe, authenticated access to any domain, device, web application or system within the

organization's active directory (AD), as well as approved third-party systems.

34) 4 Type of ADFS service componet

- ADFS Server
- Federation Service
- ADFS Proxy server
- ADFS Web Server

35) ADFS requirements

- Certificate requirements
- Hardware requirements
- Proxy requirements
- AD DS requirements
- Configuration database requirements
- Browser requirements
- Network requirements
- Permissions requirements

36) Multi Factor authentication (MFA) is a security method that requires users to provide more than just a password to access an account or application.

37) A web application proxy works by providing application publishing capabilities to organizations.

38) Active Directory Rights Management Services (AD RMS) is a Microsoft technology that helps protect digital information from unauthorized access.

39) Service accounts enhance security by providing a separate identity for applications and services.

- Type of service account
- Access controls
- Cloud security
- Authentication
- Data loss prevention (DLP)
- Encryption
- Governance and accountability
- Vulnerability assessment
- Service account security