Active Directory Knowledge Base

1. What is Active Directory?

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is a centralized system that automates network management of user data, security, and distributed resources. AD enables interoperation with other directories, stores information about objects on the network, and makes this information accessible to administrators and users. It uses a structured data store for a logical, hierarchical organization of directory information.

---

2. What are the main components of Active Directory?
The main components of Active Directory include:
- **Domain Controllers (DCs):** Host a copy of the AD database.
- **AD Database:** Stores all directory information.
- **Global Catalog (GC):** Contains information about every object in the directory.
- **LDAP (Lightweight Directory Access Protocol):** Used to query and modify items in AD.
- **Kerberos:** Provides authentication services.
- **DNS (Domain Name System):** Used to locate Domain Controllers and services.

---

3. What is a forest in Active Directory?
In Active Directory, a forest is the highest level of organization and represents the security boundary. It is a collection of one or more domains that share a common schema, configuration, and global catalog. Domains in a forest trust each other through transitive trust relationships. A forest allows centralized management while maintaining autonomy between domains.

---

4. What is the difference between a domain and an organizational unit (OU)?
- **Domain:** A collection of objects (users, devices, groups) that share the same directory database. It acts as a security and administrative boundary.
- **Organizational Unit (OU):** A container within a domain used to organize objects for easier management. OUs are primarily used for applying Group Policy settings and delegating administrative control.

---

5. What is Group Policy and how is it used in Active Directory?
Group Policy is a feature of Active Directory that provides centralized management and configuration of operating systems, applications, and user settings. It allows administrators to define how programs, network resources, and the operating system operate for users and computers in an organization. Group Policies can enforce security settings, install software, and more, and are applied to OUs, sites, domains, or local computers.

---

6. What is LDAP and how is it used with Active Directory?
LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining distributed directory information services over an IP network. In Active Directory:
- LDAP is the primary protocol for querying and modifying objects within the directory.
- It provides authentication and facilitates searching for and updating information.
- LDAP uses a hierarchical structure and supports operations like search, add, delete, and modify.

---

7. What is Kerberos and how does it work in Active Directory?
Kerberos is a network authentication protocol used by Active Directory to provide strong authentication for client/server applications. Key points:
- Kerberos uses tickets to authenticate users rather than transmitting passwords over the network.
- The **Key Distribution Center (KDC)** issues a **Ticket Granting Ticket (TGT)** when a user logs in.
- Users use the TGT to request service tickets for accessing network resources without re-entering credentials.

---

8. What is the Global Catalog in Active Directory?
The Global Catalog (GC) is a distributed data repository containing a searchable, partial representation of every object in every domain within a multi-domain AD forest. Its functions:
- Enables users to find directory information regardless of the domain storing the data.
- Provides information necessary for determining group membership for universal groups.
- The GC is hosted on designated Domain Controllers and is crucial for logon processes and locating resources across domains.

---

9. What is the Schema in Active Directory?
The Schema in Active Directory is a formal definition of all object types and their attributes within an AD forest. Key points:
- Defines the directory's structure, including the object types, properties, and information they store.
- Shared across all domains in a forest.
- Extensible, allowing custom object types and attributes to be defined as needed.

---

10. What is a trust relationship in Active Directory?
A trust relationship in Active Directory links two domains or forests, allowing users in one to access resources in the other. Types of trusts:
- **One-Way Trust:** Users in the trusting domain can access resources in the trusted domain, but not vice versa.

- **Two-Way Trust:** Users in both domains can access resources in the other.
- **Transitive Trust:** Automatically extends to other domains in the forest.
- **Non-Transitive Trust:** Limited to the two domains directly involved in the trust relationship.

12. What is the difference between a Security Group and a Distribution Group?
Security Groups and Distribution Groups serve different purposes in Active Directory:

- **Security Groups:**
  - Used to assign permissions to shared resources.
  - Can filter Group Policy settings.
  - Contain user accounts, computer accounts, and other groups.
  - Have a **Security Identifier (SID)**.

- **Distribution Groups:**
  - Used primarily for email distribution lists.
  - Cannot assign permissions to resources.
  - Contain only user accounts and other distribution groups.
  - Do not have a **SID**.

---

13. What is a Domain Controller and what are its roles?
A **Domain Controller (DC)** is a server that runs Active Directory Domain Services (AD DS) and stores a copy of the AD database. Its primary roles include:
- Authenticating users and computers.
- Storing directory data and security policies.
- Replicating updates to other Domain Controllers in the domain and forest.
- Acting as the central authority for domain security policies.
- Handling tasks like user logon processing, authentication, and directory searches.

---

14. What is the difference between a Read-Only Domain Controller (RODC) and a standard Domain Controller?
Read-Only Domain Controller (RODC):
- Hosts a **read-only** copy of the AD database.
- Does not process **write** operations.
- Does not store password hashes for users by default.
- Used in branch office scenarios or locations with potential physical security risks.
- Forwards write operations to writable DCs.

Standard Domain Controller:
- Hosts a **writable** copy of the AD database.
- Processes both **read** and **write** operations.
- Stores password hashes for users and can perform all DC operations.

---

15. What is Active Directory replication and why is it important?
Active Directory replication ensures that changes made to one Domain Controller are propagated to all others in the domain or forest. It is important because:
- Maintains **consistency** across the AD infrastructure.
- Balances load and provides **fault tolerance**.
- Improves access speed by allowing clients to query the nearest Domain Controller.
- Uses a **multi-master replication model**, allowing changes on any DC to be replicated.

---

16. What is the SYSVOL folder and what is its purpose?
The **SYSVOL folder** is a shared folder on all Domain Controllers that contains public files required for domain operations. Its purpose includes:
- Storing **Group Policy objects**, logon scripts, and other domain-wide data.
- Ensuring **replication** of important data across all Domain Controllers.
- Providing a consistent repository for files used in AD operations.

---

17. What is the tombstone lifetime in Active Directory?
The **tombstone lifetime** is the period during which deleted objects are retained in Active Directory before being permanently removed. Key points:
- Deleted objects are marked as **tombstones** for recovery purposes.
- Default tombstone lifetime is **60 days** (modifiable).
- After expiration, objects are permanently deleted during the **garbage collection** process.

---

18. What is the purpose of the Flexible Single Master Operation (FSMO) roles?
Flexible Single Master Operation (FSMO) roles are specialized tasks assigned to one or more Domain Controllers to ensure consistency and proper operation of Active Directory.

FSMO Roles:
- **Forest-Wide Roles:**
  1. **Schema Master:** Handles schema updates across the forest.
  2. **Domain Naming Master:** Manages domain additions or removals.

- **Domain-Specific Roles:**
  3. **PDC Emulator:** Synchronizes time, processes password changes, and handles legacy compatibility.
  4. **RID Master:** Allocates relative IDs (RIDs) to Domain Controllers for object creation.
  5. **Infrastructure Master:** Maintains referential integrity of objects across domains.

---

19. What is the difference between a workgroup and a domain?
Workgroup:
- Peer-to-peer network model.

- Each computer manages its own security and resources.
- No centralized authentication or resource management.

Domain:
- Centralized administration with common rules and procedures.
- Uses Active Directory for authentication and resource management.
- Allows users to log in to any domain computer with a single set of credentials.

---

20. What is a Site in Active Directory and why is it important?
A **Site** in Active Directory is a collection of **IP subnets** connected by high-speed links. It is used for:
- Optimizing **replication traffic** between Domain Controllers.
- Ensuring clients authenticate with the nearest DC for faster login times.
- Controlling replication **schedules** and traffic between geographically distributed locations.
- Improving overall performance and reducing network latency.

21. What is the Active Directory Recycle Bin?
The **Active Directory Recycle Bin** is a feature introduced in Windows Server 2008 R2 that allows administrators to recover deleted AD objects without the need for backups.

- Preserves all attributes of deleted objects, enabling full restoration to their original state.
- Reduces recovery time and effort for accidental deletions.
- Works by extending the lifetime of deleted objects and storing additional metadata for restoration.

---

22. What is ADSI (Active Directory Service Interfaces)?
Active Directory Service Interfaces (ADSI) is a set of COM interfaces that provide access to the features of directory services in a distributed computing environment.

- Provides a single, consistent interface for managing network resources across multiple directory services.
- Abstracts differences between directory services, offering uniform management capabilities.
- Commonly used in scripting and programming tasks related to AD management.

---

23. What is the difference between a user account and a computer account in AD?
User Account:
- Represents an individual needing access to network resources.
- Contains information such as username, password, and group memberships.
- Used for authentication and authorization of users.

Computer Account:

- Represents a computer joined to the domain.
- Automatically created during domain join operations.
- Authenticates the computer to the domain and allows it to download Group Policy settings.

---

24. What is a Group Policy Object (GPO) and how is it applied?
A **Group Policy Object (GPO)** is a collection of settings defining the behavior of users and systems in an Active Directory environment.

- Linked to AD containers such as sites, domains, or organizational units.
- Automatically applied during user logon or computer startup.
- Used for tasks such as configuring security settings, managing software installations, running scripts, and shaping user environments.

---

25. What is the purpose of the Primary Domain Controller (PDC) Emulator FSMO role?
The **PDC Emulator** FSMO role serves several critical functions:

- Acts as the primary DC for legacy systems and applications.
- Handles password changes and ensures password replication consistency.
- Serves as the master time source for domain synchronization.
- Preferred DC for Group Policy updates and modifications.
- In a forest, the PDC Emulator in the root domain is authoritative for time synchronization.

---

26. What is a Universal Group in Active Directory?
A **Universal Group** is a group type in AD that:

- Can contain members (users, groups, or computers) from any domain in the forest.
- Can be assigned permissions in any domain within the forest.
- Is stored in the Global Catalog for forest-wide accessibility.
- Best used in multi-domain environments to assign permissions across domains.
- Caution: Changes to Universal Groups trigger replication to all Global Catalogs, so their usage should be carefully managed to avoid excessive traffic.

---

27. What is the difference between a child domain and a tree root domain?
Child Domain:
- Created beneath an existing domain in the AD hierarchy.
- Shares a contiguous namespace with its parent domain.
- Inherits policies and trust relationships from its parent domain.

Tree Root Domain:
- The first domain in a new domain tree within a forest.
- Has its own distinct DNS namespace, which does not need to be contiguous with other domains.

- Used to incorporate separate DNS namespaces into a single forest.

---

28. What is the purpose of the Infrastructure Master FSMO role?
The **Infrastructure Master FSMO role** maintains references to objects in other domains.

- Ensures cross-domain references are updated and accurate.
- Compares its data with the Global Catalog and updates references as necessary.
- Critical in multi-domain forests where objects frequently reference each other.
- Not essential in single-domain forests or environments where all DCs are Global Catalogs.

---

29. What is the Global Catalog and why is it important?
The **Global Catalog (GC)** is a distributed repository containing partial representations of every object in every domain of an AD forest.

- Enables **forest-wide searches** for directory objects.
- Provides information needed to determine **group membership**, particularly for Universal Groups.
- Plays a vital role in **user logon** in multi-domain environments.
- Reduces time and network traffic for directory queries across domains.

---

30. What is the difference between a domain local group and a global group?
Domain Local Group:
- Can include user accounts, global groups, universal groups, and other domain local groups (from the same domain).
- Used to assign permissions to resources within the same domain.

Global Group:
- Can include user accounts and other global groups (from the same domain).
- Typically used to organize users by roles or functions.
- Designed for **cross-domain usage** to assign permissions in other domains.

31. What is Active Directory Federation Services (AD FS) and how does it relate to AD?
Active Directory Federation Services (AD FS) is a Microsoft technology for providing Single Sign-On (SSO) and authentication services across organizational boundaries.

- Extends Active Directory's authentication capabilities to external applications and services.
- Uses claims-based authentication to enable secure access without requiring separate credentials.
- Facilitates collaboration with partner organizations or cloud services by creating federation trusts.
- Maintains user credentials within the organization's AD, ensuring centralized management.

---

32. What is the Schema Master FSMO role responsible for?
The **Schema Master FSMO role** handles all updates and modifications to the Active Directory schema.

- The schema defines object classes and attributes in the AD database.
- Ensures consistency across the forest by centralizing schema updates.
- Required for actions such as extending the schema for new applications (e.g., Exchange or custom attributes).
- Only one Schema Master exists per forest.

---

33. What is a DNS zone and how does it relate to Active Directory?
A **DNS zone** is a portion of the DNS namespace managed by a DNS server.

- AD relies on DNS for locating domain controllers and services.
- Key DNS records, like SRV and A records, are stored in DNS zones to support AD functionality.
- **Active Directory-integrated DNS zones** store DNS data in the AD database, enabling secure and multi-master replication alongside other AD data.
- Integration enhances reliability and security for AD's DNS requirements.

---

34. What is the difference between a roaming profile and a mandatory profile?
Roaming Profile:
- Allows user settings and data to follow them to any computer on the network.
- Changes are saved back to a central server upon logoff.

Mandatory Profile:
- Pre-configured, unchangeable user profile.
- Changes made during the session are discarded on logoff.
- Useful for maintaining a consistent environment and preventing permanent modifications.

---

35. What is LDAP over SSL (LDAPS) and why is it important?
LDAP over SSL (LDAPS) secures LDAP communication using SSL/TLS protocols.

- Encrypts traffic between clients and AD servers, protecting sensitive data like usernames and passwords.
- Prevents interception and tampering during transmission.
- Uses port **636** (unlike standard LDAP, which uses port 389).
- Essential for securing directory services, especially over untrusted networks.

---

36. What is the purpose of the RID Master FSMO role?
The **RID Master FSMO role** allocates unique RID pools to domain controllers within a domain.

- RIDs are used to create unique Security Identifiers (SIDs) for AD objects (e.g., users, groups, computers).
- Centralized RID allocation ensures no duplicate SIDs are generated.
- If unavailable for extended periods, domain controllers may exhaust their RID pools, preventing the creation of new objects.

---

38. What is a fine-grained password policy and how does it differ from a domain-wide password policy?
Fine-Grained Password Policies (FGPP) allow for multiple password policies within a single domain.

- Introduced in Windows Server 2008 to offer flexibility.
- Can apply to specific users or groups, unlike domain-wide policies that apply to all users.
- Configurable settings include password complexity, expiration, and account lockout thresholds.
- Useful for scenarios requiring stricter or more lenient policies for specific user sets.

---

39. What is the Active Directory database file (NTDS.dit) and where is it located?
The **NTDS.dit** file is the primary database file for Active Directory.

- Contains all AD object data, including users, groups, and policies.
- Located in the `%SystemRoot%\NTDS` folder on domain controllers.
- Should only be managed using AD tools or APIs to prevent corruption.
- Integral to the operation of the directory service.

---

40. What is the purpose of the Domain Naming Master FSMO role?
The **Domain Naming Master FSMO role** manages the namespace of the Active Directory forest.

- Ensures all domains have unique names and prevents naming conflicts during domain additions or renaming.
- Manages cross-references for external trusts and other forests.
- Centralized to maintain the integrity of the forest-wide namespace.
- Only one Domain Naming Master exists per forest.

41. What is a bastion host in the context of Active Directory security?
A **bastion host** is a hardened server that acts as a gateway between untrusted networks (e.g., the internet) and the internal Active Directory environment.

- Used for secure remote administration of Active Directory.
- Configured with minimal services and strict security policies to reduce attack surfaces.
- Often serves as a **jump box** for administrators to access internal resources without exposing them directly.

- Enhances security by isolating administrative tasks from the external network.

---

42. What is the difference between a shadow group and a dynamic group in Active Directory?
Shadow Group:
- A security group with membership that mirrors another group or organizational unit (OU).
- Membership is updated through scripts or third-party tools.
- Explicitly stored and compatible with any AD-aware application.

Dynamic Group:
- Membership is determined in real-time using LDAP queries.
- Membership is not explicitly stored but calculated when the group is accessed.
- Provides flexibility and real-time accuracy but requires specific application support.

---

43. What is the purpose of the AdminSDHolder object in Active Directory?
The **AdminSDHolder** object ensures the protection of privileged accounts and groups by maintaining consistent security descriptors.

- Contains a template for security descriptors of protected accounts (e.g., Domain Admins, Enterprise Admins).
- The **SDProp** process (runs every 60 minutes by default) enforces the template on protected accounts.
- Prevents unauthorized changes to permissions, enhancing security for critical AD objects.

---

44. What is a read-only domain controller (RODC) and what are its benefits?
A **Read-Only Domain Controller (RODC)** hosts a read-only copy of the Active Directory database.

Benefits:
- Enhanced security for locations with limited physical security.
- Reduced replication traffic, as changes are not replicated back to writable DCs.
- Filters sensitive data using a **filtered attribute set.**
- Provides local authentication caching for better performance in remote sites.
- Suitable for branch offices with less secure environments.

---

45. What is the Default Domain Policy and why is it important?
The **Default Domain Policy** is a Group Policy Object (GPO) created during domain setup.

Key Features:
- Applies baseline security settings for all users and computers in the domain.
- Includes password policies, account lockout policies, and Kerberos settings.

Importance:
- Ensures consistent security standards across the domain.
- Changes to the Default Domain Policy should be minimal to avoid widespread impact.
- Best practices recommend creating custom GPOs for additional policies.

---

46. What is ADSI Edit and when would you use it?
ADSI Edit is a low-level Active Directory editor.

Uses:
- Troubleshooting complex AD issues.
- Modifying attributes not accessible through standard tools.
- Bulk editing AD objects.
- Viewing or altering the AD schema.

Caution:
- Incorrect changes can severely impact AD functionality.
- Reserved for advanced administrators and specific maintenance tasks.

---

47. What is the difference between a forest functional level and a domain functional level?
Forest Functional Level (FFL):
- Applies to the entire forest.
- Enables forest-wide features (e.g., cross-domain trusts).
- Cannot be lower than the highest Domain Functional Level in the forest.

Domain Functional Level (DFL):
- Applies to individual domains.
- Enables domain-specific features (e.g., advanced replication).

Raising functional levels is irreversible and requires domain controllers to meet the required server versions.

---

48. What is the purpose of the NETLOGON share in Active Directory?
The **NETLOGON share** exists on all domain controllers and supports domain-wide operations.

Functions:
- Stores logon scripts executed during user authentication.
- Provides Group Policy files accessible to client machines.
- Hosts other domain-wide resources needed during logon.

The NETLOGON share is replicated across domain controllers via SYSVOL, ensuring consistency.

---

49. What is a Security Identifier (SID) and why is it important in Active Directory?
A **Security Identifier (SID)** is a unique identifier assigned to security principals in Active Directory.

Key Points:
- Used for access control and auditing.
- SIDs remain consistent even if names or attributes change.
- Permissions are tied to SIDs, ensuring security policies remain intact across renames or moves.

The uniqueness of SIDs maintains security and prevents conflicts in AD environments.

---

50. What is the dsquery command and how is it used?
The **dsquery** command is a CLI tool for searching Active Directory objects.

Usage:
- Find objects like users, groups, computers, and OUs.
- Supports filtering by attributes (e.g., disabled accounts, unused computers).
- Commonly used in scripts for automation or bulk queries.

For example, to find all disabled users:
```cmd
dsquery user -disabled
```