⬚ EASY (10 Questions)

Q1. What is Active Directory primarily used for?
A. File compression
B. Centralized authentication and authorization
C. Disk management
D. Backup automation

Q2. Which Active Directory component defines object structure and attributes?
A. Domain
B. Forest
C. Schema
D. OU

Q3. What is the smallest administrative unit in Active Directory?
A. Forest
B. Domain
C. Site
D. Organizational Unit

Q4. Which service must be installed to create a domain controller?
A. DNS
B. DHCP
C. AD DS
D. IIS

Q5. What type of account is used by end users to log in to a domain?
A. Local account
B. Guest account
C. Domain user account
D. Service account

Q6. Which Active Directory object is used to group users for permissions?
A. OU
B. Group
C. Schema
D. Site

Q7. What does a Domain Controller store?
A. User documents
B. AD database and authentication data
C. Application logs
D. Backup files

Q8. Which folder stores Group Policy objects on a DC?
A. NTDS

B. SYSVOL
C. Program Files
D. Temp

Q9. Which protocol is used by AD for authentication by default?
A. NTLMv1
B. LDAP
C. Kerberos
D. HTTPS

Q10. What is the purpose of an Additional Domain Controller (ADC)?
A. Backup storage
B. Redundancy and load balancing
C. DNS forwarding
D. Software deployment

☐ MEDIUM (15 Questions)

Q11. What is the security boundary in Active Directory?
A. OU
B. Domain
C. Forest
D. Site

Q12. Which FSMO role is responsible for time synchronization?
A. RID Master
B. Schema Master
C. PDC Emulator
D. Infrastructure Master

Q13. Which group scope is best for assigning permissions to resources?
A. Global
B. Universal
C. Domain Local
D. Built-in

Q14. What is the primary purpose of an OU design?
A. Replication
B. Delegation and GPO management
C. Authentication
D. DNS resolution

Q15. Which database file stores Active Directory data?
A. boot.ini

B. sysvol.mdf
C. ntds.dit
D. ad.db

Q16. What happens if DNS is misconfigured in an AD environment?
A. Slow boot
B. Authentication failures
C. Disk errors
D. Backup failure

Q17. Which tool is commonly used to check AD replication health?
A. gpedit.msc
B. repadmin
C. diskpart
D. nslookup

Q18. What is the Global Catalog used for?
A. Backup recovery
B. Forest-wide object searches
C. Password encryption
D. DNS resolution

Q19. Which group strategy follows best practice in AD?
A. AGUDLP
B. AGDLP
C. UDGAPL
D. DLPAG

Q20. Which type of domain controller is used in branch offices with limited security?
A. Primary DC
B. Backup DC
C. Read-Only DC (RODC)
D. Virtual DC

Q21. What is the function of Sites in Active Directory?
A. Logical grouping
B. Physical network optimization
C. Security delegation
D. Schema management

Q22. Which service must be running for AD replication?
A. DHCP
B. Netlogon
C. DFS Replication
D. Print Spooler

Q23. Which account should NOT be used for daily administrative tasks?
A. Domain User
B. Service Account
C. Domain Admin
D. Managed Service Account

Q24. Which AD feature allows centralized policy enforcement?
A. FSMO
B. Trusts
C. Group Policy
D. LDAP

Q25. Which authentication protocol replaced NTLM in modern AD?
A. SSL
B. IPsec
C. Kerberos
D. TLS

⬤ HARD (15 Questions)

Q26. Why is a single-forest design recommended for most enterprises?
A. Faster replication
B. Reduced licensing
C. Simplified security boundary
D. Improved DNS resolution

Q27. What happens if the RID Master becomes unavailable for a long time?
A. Users cannot log in
B. New objects cannot get SIDs
C. DNS fails
D. SYSVOL stops

Q28. Which attack exploits Kerberos ticket forgery in AD?
A. Pass-the-Hash
B. Golden Ticket
C. LDAP Injection
D. DNS Spoofing

Q29. Why are multiple DCs deployed per domain?
A. Increase schema size
B. Improve authentication speed only
C. Provide fault tolerance and replication
D. Reduce OU complexity

Q30. Which AD misconfiguration leads to privilege escalation?
A. Excessive group membership
B. NTFS permissions
C. DHCP scope overlap
D. DNS scavenging

Q31. Which AD restore requires booting into DSRM?
A. File restore
B. Authoritative AD restore
C. Non-authoritative restore
D. System image restore

Q32. What is the main risk of enabling NTLMv1?
A. Performance drop
B. Weak encryption and replay attacks
C. Disk corruption
D. Replication latency

Q33. Which FSMO role updates cross-domain object references?
A. Schema Master
B. Domain Naming Master
C. Infrastructure Master
D. RID Master

Q34. What is the primary benefit of using gMSA?
A. Easier password guessing
B. Automatic password management
C. Interactive logon
D. Reduced AD size

Q35. Which AD component stores Group Policy templates?
A. Registry
B. SYSVOL
C. NTDS.DIT
D. Event Logs

Q36. Why should DCs not host additional roles like IIS?
A. Licensing issues
B. Performance impact
C. Increased attack surface
D. Storage limitations

Q37. What happens during non-authoritative restore?
A. DC overwrites other DCs
B. DC accepts updates from replication partners

C. Schema is rebuilt
D. SYSVOL is deleted

Q38. Which scenario requires a forest trust?
A. Same domain access
B. Same forest access
C. Separate security boundaries
D. OU delegation

Q39. Why is time synchronization critical in AD?
A. Backup accuracy
B. Kerberos authentication
C. DNS resolution
D. Group Policy refresh

Q40. Which AD security practice reduces lateral movement?
A. Single admin account
B. Tiered administrative model
C. Universal groups only
D. Shared service accounts