Frequently asked interview questions on Active Directory.

This is a compilation of question and answers
on Active Directory from various sources listed below.This provides a starting point in preparation for Windows Administration interview.

1. **Define Active Directory**

   Active Directory is a database that stores data pertaining to the users and objects within the network. Active Directory allows the compilation of networks that connect with AD, as well as the management and administration.

2. **What is a domain within Active Directory?**

   A domain represents the group of network resources that includes computers, printers, applications and other resources. Domains share a directory database. The domain is represented by address of the resources within the database. A user can log into a domain to gain access to the resources that are listed as part that domain.

3. **What is the domain controller?**

   The server that responds to user requests for access to the domain is called the Domain Controller or DC. The Domain Controller allows a user to gain access to the resources within the domain through the use of a single username and password.

4. **Explain what domain trees and forests are**

   Domains that share common schemas and configurations can be linked to form a contiguous namespace. Domains within the trees are linked together by creating special relationships between the domains based on trust. Forests consist of a number of domain trees that are linked together within AD, based on various implicit trust relationships. Forests are generally created where a server setup includes a number of root DNS addresses. Trees within the forest do not share a contiguous namespace.

5. **What is LDAP?**

   LDAP is an acronym for Lightweight Directory Access Protocol and it refers to the protocol used to access, query and modify the data stored within the AD directories. LDAP is an internet standard protocol that runs over TCP/IP.

6. **Mention which is the default protocol used in directory services?**

   The default protocol used in directory services is LDAP (Lightweight Directory Access Protocol).

7. **What tool would you use to edit AD?**

   Adsiedit.msc is a low level editing tool for Active Directory. Adsiedit.msc is a Microsoft Management Console snap-in with a graphical user interface that allows administrators to accomplish simple tasks like adding, editing and deleting objects with a directory service. The Adsiedit.msc uses Application Programming Interfaces to access the Active Directory. Since Adsiedit.msc is a Microsoft Management Console snap-in, it requires access MMC and a connection to an Active Directory environment to function correctly.

8. **How would you manage trust relationships from the command prompt?**

   Netdom.exe is another program within Active Directory that allows administrators to manage the Active Directory. Netdom.exe is a command line application that allows administrators to manage trust relationship within Active Directory from the command prompt. Netdom.exe allows for batch management of trusts. It allows administrators to join computers to domains. The application also allows administrators to verify trusts and secure Active Directory channels.

9. **Where is the AD database held and how would you create a backup of the database?**

   The database is stored within the windows NTDS directory. You could create a backup of the database by creating a backup of the System State data using the default NTBACKUP tool provided by windows or by Symantec’s Netbackup. The System State Backup will create a backup of the local registry, the Boot files, the COM+, the NTDS.DIT file as well as the SYSVOL folder.

10. **What is SYSVOL, and why is it important?**

    SYSVOL is a folder that exists on all domain controllers. It is the repository for all of the active directory files. It stores all the important elements of the Active Directory group policy. The File Replication Service or FRS allows the replication of the SYSVOL folder among domain controllers. Logon scripts and policies are delivered to each domain user via SYSVOL. SYSVOL stores all of the security related information of the AD.

11. **Briefly explain how Active Directory authentication works**

    When a user logs into the network, the user provides a username and password. The computer sends this username and password to the KDC which contains the master list of unique long term keys for each user. The KDC creates a session key and a ticket granting ticket. This data is sent to the user's computer. The user's computer runs the data through a one-way hashing function that converts the data into the user's master key, which in turn enables the computer to communicate with the KDC, to access the resources of the domain.

12. **Mention what is the difference between domain admin groups and enterprise admins group in AD?**

    Enterprise Admin Group

    - Members of this group have complete control of all domains in the forest.
    - By default, this group belongs to the administrators group on all domain controllers in the forest.
    - As such this group has full control of the forest, add users with caution.

    Domain Admin Group

    - Members of this group have complete control of the domain
    - By default, this group is a member of the administrators group on all domain controllers, workstations and member servers at the time they are linked to the domain.
    - As such the group has full control in the domain, add users with caution.

13. **Mention what is Kerberos?**

    Kerberos is an authentication protocol for network. It is built to offer strong authentication for server/client applications by using secret-key cryptography.

14. **Mention what are lingering objects?**

    Lingering objects can exists if a domain controller does not replicate for an interval of time that is longer than the tombstone lifetime (TSL).

15. **Mention what is TOMBSTONE lifetime?**

    Tombstone lifetime in an Active Directory determines how long a deleted object is retained in Active Directory. The deleted objects in Active Directory is stored in a special object referred as TOMBSTONE. Usually, windows will use a 60- day tombstone lifetime if time is not set in the forest configuration.

16. **Mention what is PDC emulator and how would one know whether PDC emulator is working or not?**

    PDC Emulators: There is one PDC emulator per domain, and when there is a failed authentication attempt, it is forwarded to PDC emulator. It acts as a “tie-breaker” and it controls the time sync across the domain. These are the parameters through which we can know whether PDC emulator is working or not.

    - Time is not syncing
    - User’s accounts are not locked out
    - Windows NT BDCs are not getting updates
    - If pre-windows 2000 computers are unable to change their passwords.

17. **Explain what is Active Directory Schema?**

    Schema is an active directory component describes all the attributes and objects that the directory service uses to store data.

18. **Explain what is a child DC?**

    CDC or child DC is a sub domain controller under root domain controller which share name space

19. **Explain what is RID Master?**

    RID master stands for Relative Identifier for assigning unique IDs to the object created in AD.

20. **Mention what are the components of AD?**

    Components of AD includes

    - Logical Structure: Trees, Forest, Domains and OU
    - Physical Structures: Domain controller and Sites

21. **Explain what is Infrastructure Master?**

    Infrastructure Master is accountable for updating information about the user and group and global catalogue.

22. **What is FSMO?**

    Flexible single master operation is a specialized domain controller (DC) set of tasks, used where standard data transfer and update methods are inadequate. AD normally relies on multiple peer DCs, each with a copy of the AD database, being synchronized by multi-master replication.

23. **Tel me about the FSMO roles?**

    - Schema Master
    - Domain Naming Master
    - Infrastructure Master
    - RID Master
    - PDC

Schema Master and Domain Naming Master are forest wide role and only available one on each Forest, Other roles are Domain wide and one for each Domain AD replication is multi master replication and change can be done in any Domain Controller and will get replicated to others Domain Controllers, except above file roles, this will be flexible single master operations (FSMO), these changes only be done on dedicated Domain Controller so it's single master replication.

24. **Which FSMO role is the most important? And why?**

Interesting question which role is most important out of 5 FSMO roles or if one role fails that will impact the end-user immediately Most amateur administrators pick the Schema master role, not sure why maybe they though Schema is very critical to run the Active Directory

Correct answer is PDC, now the next question why? Will explain role by role what happens when a FSMO role holder fails to find the answer

Schema Master – Schema Master needed to update the Schema, we don't update the schema daily right, when will update the Schema? While the time of operating system migration, installing new Exchange version and any other application which requires extending the schema So if are Schema Master Server is not available, we can't able to update the schema and no way this will going to affect the Active Directory operation and the end-user

Schema Master needs to be online and ready to make a schema change, we can plan and have more time to bring back the Schema Master Server

Domain Naming Master – Domain Naming Master required to creating a new Domain and creating an application partition, Like Schema Master we don't create Domain and application partition frequently. So if are Domain Naming Master Server is not available, we can't able to create a new Domain and application partition, it may not affect the user, user event didn't aware Domain Naming Master Server is down

Infrastructure Master – Infrastructure Master updates the cross domain updates, what really updates between Domains? Whenever user login to Domain the TGT has been created with the list of access user got through group membership (user group membership details) it also contain the user membership details from trusted domain, Infrastructure Master keep this information up-to-date, it update reference information every 2 days by comparing its data with the Global Catalog (that's why we don't keep Infrastructure Master and GC in same server) In a single Domain and single Forest environment there is no impact if the Infrastructure Master server is down

In a Multi Domain and Forest environment, there will be impact and we have enough time to fix the issue before it affect the end-user

RID Master –Every DC is initially issued 500 RID’s from RID Master Server. RID’s are used to create a new object on Active Directory, all new objects are created with Security ID (SID) and RID is the last part of a SID. The RID uniquely identifies a security principal relative to the local or domain security authority that issued the SID When it gets down to 250 (50%) it requests a second pool of RID’s from the RID master. If RID Master Server is not available the RID pools unable to be issued to DC’s and DC’s are only able to create a new object depends on the available RID’s, every DC has anywhere between 250 and 750 RIDs available, so no immediate impact

PDC – PDC required for Time sync, user login, password changes and Trust, now you know why the PDC is important FSMO role holder to get back online, PDC role will impact the end-user immediately and we need to recover ASAP The PDC emulator Primary Domain Controller for backwards compatibility and it’s responsible for time synchronizing within a domain, also the password master. Any password change is replicated to the PDC emulator ASAP. If a logon request fails due to a bad password the logon request is passed to the PDC emulator to check the password before rejecting the login request.

25. **What is Active Directory Partitions?**

Active Directory partition is how and where the AD information logically stored.

26. **What are all the Active Directory Partitions?**

- Schema
- Configuration
- Domain
- Application partition

27. **What is KCC?**

KCC (knowledge consistency checker) is used to generate replication topology for inter site replication and for intra-site replication. Within a site replication traffic is done via remote procedure calls over ip, while between sites it is done through either RPC or SMTP.

28. **Explain what intrasite and intersite replication is and how KCC facilitates replication**

The replication of DC's inside a single site is called intrasite replication whilst the replication of DC's on different sites is called Intersite replication. Intrasite replication occurs frequently while Intersite replication occurs mainly to ensure network bandwidth.

KCC is an acronym for the Knowledge Consistency Checker. The KCC is a process that runs on all of the Domain Controllers. The KCC allows for the replication topology of site replication within sites and between sites. Between sites, replication is done through SMTP or RPC whilst Intersite replication is done using procedure calls over IP.

29. **What is group policy?**

Group Policy is one of the most exciting -- and potentially complex -- mechanisms that the Active Directory enables. Group policy allows a bundle of system and user settings (called a "Group Policy Object" or GPO) to be created by an administrator of a domain or OU and have it automatically pushed down to designated systems.

Group Policy can control everything from user interface settings such as screen background images to deep control settings in the client such as its TCP/IP configuration and authentication settings. There are currently over 500 controllable settings. Microsoft has provided some templates as well to provide a starting point for creating policy objects.

A significant advantage of group policy over the old NT-style policies is that the changes they make are reversed when the policy no longer applies to a system. In NT 4, once a policy was applied to a system, removing that policy did not by itself roll back the settings that it imposed on the client. With Windows 2000, when a specified policy no longer applies to a system it will revert to its previous state without administrative interference.

Multiple policies from different sources can be applied to the same object. For example, a domain might have one or more domain-wide policies that apply to all systems in the domain. Below that, systems in an OU can also have policy objects applied to it, and the OU can even be further divided into sub-OU's with their own policies.

This can create a very complex web of settings so administrators must be very careful when creating these multiple layers of policy to make sure the end result -- which is the union of all of the applicable policies with the "closest" policy taking priority in most cases -- is correct for that system. In addition, because Group policy is checked and applied during the system boot process for machine settings and again during logon for user settings, it is recommended that GPO's be applied to a computer from no more than five "layers" in the AD to keep reboot and/or login times from becoming unacceptably long.

30. **Why do we need Netlogon?**

    Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records.

31. **What are the Groups types available in active directory ?**

    Security groups: Use Security groups for granting permissions to gain access to resources. Sending an e-mail message to a group sends the message to all members of the group. Therefore security groups share the capabilities of distribution groups.

    Distribution groups: Distribution groups are used for sending e-mail messages to groups of users. You cannot grant permissions to security groups. Even though security groups have all the capabilities of distribution groups, distribution groups still requires, because some applications can only read distribution groups.

32. **Explain about the groups scope in AD?**

    Domain Local Group: Use this scope to grant permissions to domain resources that are located in the same domain in which you created the domain local group. Domain local groups can exist in all mixed, native and interim functional level of domains and forests. Domain local group memberships are not limited as you can add members as user accounts, universal and global groups from any domain. Just to remember, nesting cannot be done in domain local group. A domain local group will not be a member of another Domain Local or any other groups in the same domain.

Global Group: Users with similar function can be grouped under global scope and can be given permission to access a resource (like a printer or shared folder and files) available in local or another domain in same forest. To say in simple words, Global groups can be use to grant permissions to gain access to resources which are located in any domain but in a single forest as their memberships are limited. User accounts and global groups can be added only from the domain in which global group is created. Nesting is possible in Global groups within other groups as you can add a global group into another global group from any domain. Finally to provide permission to domain specific resources (like printers and published folder), they can be members of a Domain Local group. Global groups exist in all mixed, native and interim functional level of domains and forests.

Universal Group Scope: These groups are precisely used for email distribution and can be granted access to resources in all trusted domain as these groups can only be used as a security principal (security group type) in a windows 2000 native or windows server 2003 domain functional level domain. Universal group memberships are not limited like global groups. All domain user accounts and groups can be a member of universal group. Universal groups can be nested under a global or Domain Local group in any domain.

33. **What is REPLMON?**

The Microsoft definition of the Replmon tool is as follows; This GUI tool enables administrators to view the low-level status of Active Directory replication, force synchronization between domain controllers, view the topology in a graphical format, and monitor the status and performance of domain controller replication.

34. **What is NETDOM ?**

NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels.

35. **Explain about Trust in AD ?**

To allow users in one domain to access resources in another, Active Directory uses trusts. Trusts inside a forest are automatically created when domains are created. The forest sets the default boundaries of trust, not the domain, and implicit, transitive trust is automatic for all domains within a forest. As well as two-way transitive trust, AD trusts can be a shortcut (joins two domains in different trees, transitive, one- or two-way), forest (transitive, one- or two-way), realm (transitive or nontransitive, one- or two-way), or external (nontransitive, one- or two-way) in order to connect to other forests or non-AD domains.

36. **Different modes of AD restore ?**

A **nonauthoritative restore** is the default method for restoring Active Directory. To perform a nonauthoritative restore, you must be able to start the domain controller in Directory Services Restore Mode. After you restore the domain controller from backup, replication partners use the standard replication protocols to update Active Directory and associated information on the restored domain controller.

An **authoritative restore** brings a domain or a container back to the state it was in at the time of backup and overwrites all changes made since the backup. If you do not want to replicate the changes that have been made subsequent to the last backup operation, you must perform an authoritative restore. In this one needs to stop the inbound replication first before performing the An authoritative restore.

37. **What is OU ?**

Organization Unit is a container object in which you can keep objects such as user accounts, groups, computer, printer . applications and other (OU). In organization unit you can assign specific permission to the user’s. organization unit can also be used to create departmental limitation.

38. **What is Global Catalog?**

The Global Catalog authenticates network user logons and fields inquiries about objects across a forest or tree. Every domain has at least one GC that is hosted on a domain controller. In Windows 2000, there was typically one GC on every site in order to prevent user logon failures across the network.

39. **When should you create a forest?**

Organizations that operate on radically different bases may require separate trees with distinct namespaces. Unique trade or brand names often give rise to separate DNS identities. Organizations merge or are acquired and naming continuity is desired. Organizations form partnerships and joint ventures. While access to common resources is desired, a separately defined tree can enforce more direct administrative and security restrictions.

40. **What is group nesting?**

Adding one group as a member of another group is called ‘group nesting’. This will help for easy administration and reduced replication traffic.

41. **How the AD authentication works ?**

When a user enters a user name and password, the computer sends the user name to the Key Distribution Centre (KDC). The KDC contains a master database of unique long term keys for every principal in its realm. The KDC looks up the user’s master key (KA), which is based on the user’s password. The KDC then creates two items: a session key (SA) to share with the user and a Ticket-Granting Ticket (TGT). The TGT includes a second copy of the SA, the user name, and an expiration time. The KDC encrypts this ticket by using its own master key (KKDC), which only the KDC knows. The client computer receives the information from the KDC and runs the user’s password through a one-way hashing function, which converts the password into the user’s KA. The client computer now has a session key and a TGT so that it can securely communicate with the KDC. The client is now authenticated to the domain and is ready to access other resources in the domain by using the Kerberos protocol.

42. **What is Global Catalog and its function?**

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

The global catalog provides the ability to locate objects from any domain without having to know the domain name. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the forest.

Forest-wide searches. The global catalog provides a resource for searching an AD DS forest. Forest-wide searches are identified by the LDAP port that they use. If the search query uses port 3268, the query is sent to a global catalog server. ***User logon***. In a forest that has more than one domain, two conditions require the global catalog during user authentication: Universal Group Membership Caching: In a forest that has more than one domain, in sites that have domain users but no global catalog server, Universal Group Membership Caching can be used to enable caching of logon credentials so that the global catalog does not have to be contacted for subsequent user logons. This feature eliminates the need to retrieve universal group memberships across a WAN link from a global catalog server in a different site.

- In a domain that operates at the Windows 2000 native domain functional level or higher, domain controllers must request universal group membership enumeration from a global catalog server.
- When a user principal name (UPN) is used at logon and the forest has more than one domain, a global catalog server is required to resolve the name.

Exchange Address Book lookups. Servers running Microsoft Exchange Server rely on access to the global catalog for address information. Users use global catalog servers to access the global address list (GAL).

43. **What are the physical components of Active Directory?**

Domain controllers and Sites. Domain controllers are physical computers which is running Windows Server operating system and Active Directory data base. Sites are a network segment based on geographical location and which contains multiple domain controllers in each site.

44. **What are the logical components of Active Directory?**

Domains, Organizational Units, trees and forests are logical components of Active Directory.

45. **What is RODC? Why do we configure RODC?**

Read only domain controller (RODC) is a feature of Windows Server 2008 Operating System. RODC is a read only copy of Active Directory database and it can be deployed in a remote branch office where physical security cannot be guaranteed. RODC provides more improved security and faster log on time for the branch office.

46. **What is role seizure? Who do we perform role seizure?**

Role seizure is the action of assigning an operations master role to a new domain controller without the support of the existing role holder (generally because it is offline due to a hardware failure). During role seizure, a new domain controller assumes the operations master role without communicating with the existing role holder. Role seizure can be done using repadmin.exe and Ntdsutil.exe commands.

47. **Tell me few uses of NTDSUTIL commands?**

We can use ntdsutil commands to perform database maintenance of AD DS, manage and control single master operations, Active Directory Backup restoration and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

48. **A user is unable to log into his desktop which is connected to a domain. What are the troubleshooting steps you will consider?**

Check the network connection on the desktop. Try to ping to the domain controller. Run and check if name resolution is working. Check Active Directory for the computer account of the desktop. Compare the time settings on the desktop and Domain controller. Remove the desktop from domain and rejoin to domain.

49. **A Domain Controller called ABC is failing replication with XYZ. How do you troubleshoot the issue?**

Active Directory replication issue can occur due to variety of reasons. For example, DNS issue, network problems, security issues etc. Troubleshooting can start by verifying DNS records. Then remove and recreate Domain Controller replication link. Check the time settings on both replication partners.

50. **What do you understand by Garbage Collection? Explain.**

Garbage collection is a process of Active Directory. This process starts by removing the remains of previously deleted objects from the database. These objects are known as tombstones. Then, the garbage collection process deletes unnecessary log files. And the process starts a defragmentation thread to claim additional free space. The garbage collection process is running on all the domain controllers in an interval of 12 hours.