Most Asked Active Directory Interview Questions

Following is the list of most frequently asked Active Directory Interview questions and their best possible answers.

1) What do you understand by the term Active Directory?

The term active directory specifies an index structure or MetaData used in Microsoft Windows-based servers and computers to stock up data and information about domains and networks.

Active Directory is like a database that stores data such as user information, computer information, and other network object information. It is capable of managing and administers the complete network.

---

2) What is a domain?

A domain is a set of network resources for a group of users. The users need only to log in to the domain to access the resources, which may be located on different servers in the network. The 'domain' specifies a system address that may provide you a lot of information. A domain address might look something like 211.170.469. The concept of the domain was introduced in Windows NT, where a user may grant access to several computer resources using a single username and password combination.

---

3) What is the default protocol used in directory services?

The non-payment default protocol used in directory services is LDAP. Here, LDAP stands for Lightweight Directory Access Protocol.

---

4) What is the difference between domain local, global and universal groups?

Domain local groups have a scope that extends to the local domain and are used to assign permissions to local resources. The difference between domain local and global groups is that user accounts, global groups, and universal groups from any domain can be added to a domain local group. However, because of its limited scope, members can only be assigned permissions within the domain in which this group is created.

---

5) What is the Sysvol folder? Why is it used?

The Sysvol folder is used to store the server's copy of the domain's public files and deliver the policy and logon scripts to domain members. It replicates all the group policies from one domain to other domain controllers in a particular domain.

---

6) Can a user create a new universal user group?

The universal groups are allowed only in native-mode Windows Server 2003 environments. It requires promoting all domain controllers to Windows Server 2003 Active Directory to create a new universal user group.

---

7) What do you understand by the term "Forest" in AD?

The term forest describes an assembly of AD domains that split a separate schema for the AD. All DC's in the forest share this schema and are replicated in a hierarchical way among them.

---

8) What is the difference between enterprise admin group and domain admin group in AD?

Following is the list of differences between enterprise admin group and domain admin group in AD:

Enterprise Admin Group	Domain Admin Group

The members of the Enterprise Admin Group have complete control of all domains in the forest.	The members of the Domain Admin Group have complete control of the domain.
By default, the Enterprise Admin Group belongs to the Administrators group on all domain controllers in the forest.	By default, the Domain Admin Group is a member of the Administrators group on all domain controllers, workstations, and member servers when linked to the domain.
This group has complete control of the forest, so; the users should be added with caution.	This group has full control in the domain, so; the users should be added with caution.

9) What is ARP? What do you understand by ARP Cache Poisoning?

ARP stands for Address Resolution Protocol. It is a protocol used for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

ARP Cache Poisoning is a process where a table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

10) What do you understand by Kerberos?

The Kerberos is a verification protocol used for the network. It is built to provide secure verification for client applications by using secret-key cryptography.

11) What is LSDOU?

LSDOU is a group policy inheritance model where the policies are applied to Local machines, Sites, Domains, and Organizational Units. That's why it is called LSDOU.

12) What is Active Directory Schema?

Active Directory Schema is the blueprint of an Active Directory Network. All the objects created in an Active Directory Network reference the Active Directory Schema for its object type.

13) What are the different components of Active Directory Schema?

Three main components are used to make an AD Schema:

- **Objects:** Objects are the entities that Active Directory uses to store information about the resources in its network. In Active Directory, objects are used as references to the resources in the network. For example, if a computer belongs to the Active Directory network, there would be a computer object that will represent this computer in real life. The computer object will also store some information about the computer such as operating system, running status, etc.
- **Classes:** In an Active Directory Schema, attributes are grouped and categorized into object classes. Object classes are, therefore, hierarchical classifications of object definitions. There are three types of classes in an Active Directory schema:
    1. Abstract class
    2. Structural class
    3. Auxiliary class
- **Attributes:** Attributes are the entities that are used to store information about the objects in the Active Directory environment. For example, a user object can have attributes such as their first name, last name, telephone number, address, and other attributes that store data about the user. Some attributes also store information about other attributes than the object itself. There are several types of attributes, such as linked attributes, indexed attributes, and global attributes.

14) What are the newly added features in Active Directory (AD) of Windows Server 2012?

Following is a list of newly added features in Active Directory of Windows Server 2012:

- **dcpromo (Domain Controller Promoter) with the improved wizard:** It facilitates users to view all the steps and review the detailed results during the installation process.
- **Enhanced Administrative Center:** In the newer version of Windows 2012, the administrative center is well designed compared to the earlier version of the active directory. The exchange management console is well designed.
- **Recycle bin goes GUI:** The Windows Server 12 provides so many ways to enable the active directory to recycle bin through the GUI in the Active Directory Administrative Center, which was not possible in the earlier version.
- **Fine-grained password policies (FGPP):** Implementing FGPP is much easier in Windows Server 12 than in the earlier versions. It also facilitates us to create different password policies in the same domain.
- **Windows Power Shell History Viewer:** It also provides Windows PowerShell commands related to the actions executed in the Active Directory Administrative Center UI.

---

15) What system state data contains?

The system state data contains the following things:

- Registry
- Startup files
- System files
- Registration Database
- Memory page file
- AD information
- SYSVOL Folder
- Cluster service information etc.

---

16) What are the main components of Active Directory?

There are mainly two components of Active Directory:

- **Physical Structures:** It contains the Domain controller and Sites.
- **Logical Structure:** It contains the Trees, Forest, Domains, and OU.

---

17) What do you understand by Tombstone lifetime?

The Tombstone lifetime is used to determine how long a deleted object is retained in Active Directory. The deleted objects in Active Directory are stored in a special object called TOMBSTONE. By default, Windows uses a 60- day tombstone lifetime if time is not set in the forest configuration.

---

18) What do you understand by a child DC or CDC?

CDC or child DC stands for Child Domain Controller. It is a subdomain controller under the root domain controller, which is used to share a namespace.

---

19) What is the full form of APIPA? Why is it used?

APIPA stands for Automatic Private IP Addressing. It is a prominent feature of Windows 98, 98 SE, Me, and 2000. It is used to automatically assign an Internet Protocol address to a computer on which it is installed.

---

20) What do you understand by RID Master?

RID master stands for Relative Identifier Master. It is used to assign unique IDs to the object created in Active Directory.

---

21) What do you understand by Infrastructure Master?

The role of the Infrastructure Master is to update references from objects in the local domain to objects in other domains. There can be only one Infrastructure Master DC in each domain. In other words, we can say that the Infrastructure Master is accountable for updating information about the user and group and global catalog.

---

22) What do you understand by organizational units?

An Organizational Unit is a design factor that impacts policy, security, competence, and the charge of administration. Organizational Units are a kind of LDAP pot that can reflect as a sub-domain element with comparable properties to domains.

---

23) What is the use of Active Directory Recycle Bin?

The Active Directory Recycle bin is a characteristic of Windows Server 2008 AD. It is used to re-establish by chance deleted Active Directory objects without using a backed-up AD database, rebooting area controller.

---

24) What do you understand by domain trees and forests?

Domain trees and forests both are two important concepts of Active Directory. A domain tree is a collection of one or more domains that share a common namespace. For example, jobs.career.com and career.com both domains are a part of the career.com domain tree. If the domain you create does not contain the full name of the parent domain or forest root domain, it is considered part of a separate domain tree.

A forest is a collection of one or more domain trees. The domains in the career.com domain tree and the colleges.com domain tree could be part of the same forest. A domain tree is based on a common namespace, but a forest is not. A forest is named after the first domain created in the forest. Suppose career.com is the first domain created, then the forest is automatically named career.com. Later, you can create additional domains for jobs.career.com and colleges.com, all belonging to the career.com forest.

---

25) What is the purpose of replication in Active Directory?

The main purpose of replication is to share the data stored within the index throughout the organization for amplified availability, performance, and data defense.

---

26) What are the different ports used by Active Directory?

Following is the list of ports that Active Directory uses

- **RPC endpoint mapper:** port 135 TCP, UDP
- **NetBIOS name service:** port 137 TCP, UDP
- **NetBIOS datagram service:** port 138 UDP
- **NetBIOS session service:** port 139 TCP
- **SMB over IP (Microsoft-DS):** port 445 TCP, UDP
- **LDAP:** port 389 TCP, UDP
- **LDAP over SSL:** port 636 TCP
- **Global catalog LDAP:** port 3268 TCP
- **Global catalog LDAP over SSL:** port 3269 TCP
- **Kerberos:** port 88 TCP, UDP
- **DNS:** port 53 TCP, UDP
- **WINS resolution:** port 1512 TCP, UDP

- **WINS replication:** 42 TCP, UDP
- **RPC:** Dynamically-assigned ports TCP, unless restricted

---

27) What are the best tools that you would like to use to edit AD?

The Adsiedit.msc is one of the best low-level editing tools for Active Directory. It is a Microsoft Management Console snap-in with a graphical user interface that facilitates administrators to do simple tasks such as adding, editing, and deleting objects with a directory service. The Adsiedit.msc tool uses Application Programming Interfaces to access the Active Directory.

---

28) Which program is used to manage trust relationships from the command prompt?

The Netdom.exe is a program or a command-line application within Active Directory which administrators use to manage the Active Directory. This application facilitates administrators to manage trust relationships within Active Directory from the command prompt. It also allows administrators to join computers to domains for batch management of trusts and verify trusts and secure Active Directory channels.

---

29) What is the full form of SID? Why is it used?

SID stands for Security Identifier. It is a unique variable-length identifier used to recognize a trustee or refuge principal.

---

30) What do you understand by PDC emulator? How would one know whether the PDC emulator is working or not?

PDC Emulators are used as a "tie-breaker" and control the time sync across the domain. There is one PDC emulator per domain, and when there is a failed authentication attempt, it is forwarded to the PDC emulator.

Following are some parameters through which we can know whether the PDC emulator is working or not:

- If time is not syncing
- If user's accounts are not locked out
- If Windows NT BDCs are not getting updates
- If pre-windows 2000 computers are unable to change their passwords

---

31) What is Active Directory Schema?

Active Directory Schema is the blueprint of an Active Directory Network. All the objects created in an Active Directory Network reference the Active Directory Schema for its object type.

---

32) What are the different components of Active Directory Schema?

- **Objects:** Objects are the entities that Active Directory uses to store information about the resources in its network. In Active Directory, objects are used as references to the resources in the network. For example, if a computer belongs to the Active Directory network, there would be a computer object that will represent this computer in real life. The computer object will also store some information about the computer such as operating system, running status, etc.
- **Classes:** In an Active Directory Schema, attributes are grouped and categorized into object classes. Object classes are, therefore, hierarchical classifications of object definitions. There are three types of classes in an Active Directory schema:
    1. Abstract class
    2. Structural class
    3. Auxiliary class
- **Attributes:** Attributes are the entities that are used to store information about the objects in the Active Directory environment. For example, a user object can have attributes such as their first name, last name, telephone number,

address, and other attributes that store data about the user. Some attributes also store information about other attributes than the object itself. There are several types of attributes, such as linked attributes, indexed attributes, and global attributes.

---

33) What are the newly added features in Active Directory (AD) of Windows Server 2012?

Following is a list of newly added features in Active Directory of Windows Server 2012:

- **dcpromo (Domain Controller Promoter) with the improved wizard:** It facilitates users to view all the steps and review the detailed results during the installation process.
- **Enhanced Administrative Center:** In the newer version of Windows 2012, the administrative center is well designed compared to the earlier version of the active directory. The exchange management console is well designed.
- **Recycle bin goes GUI:** The Windows Server 12 provides so many ways to enable the active directory to recycle bin through the GUI in the Active Directory Administrative Center, which was not possible in the earlier version.
- **Fine-grained password policies (FGPP):** Implementing FGPP is much easier in Windows Server 12 than in the earlier versions. It also facilitates us to create different password policies in the same domain.
- **Windows Power Shell History Viewer:** It also provides Windows PowerShell commands related to the actions executed in the Active Directory Administrative Center UI.

---

34) What system state data contains?

The system state data contains the following things:

- Registry
- Startup files
- System files
- Registration Database
- Memory page file
- AD information
- SYSVOL Folder
- Cluster service information etc.

---

35) What are the main components of Active Directory?

There are mainly two components of Active Directory:

- **Physical Structures:** It contains the Domain controller and Sites.
- **Logical Structure:** It contains the Trees, Forest, Domains, and OU.

---

36) What do you understand by Tombstone lifetime?

The Tombstone lifetime is used to determine how long a deleted object is retained in Active Directory. The deleted objects in Active Directory are stored in a special object called TOMBSTONE. By default, Windows uses a 60- day tombstone lifetime if time is not set in the forest configuration.

---

37) What do you understand by a child DC or CDC?

CDC or child DC stands for Child Domain Controller. It is a subdomain controller under the root domain controller, which is used to share a namespace.

---

38) What is the full form of APIPA? Why is it used?

APIPA stands for Automatic Private IP Addressing. It is a prominent feature of Windows 98, 98 SE, Me, and 2000. It is used to automatically assign an Internet Protocol address to a computer on which it is installed.

---

39) What do you understand by RID Master?

RID master stands for Relative Identifier Master. It is used to assign unique IDs to the object created in Active Directory.