
Guru99 Provides [FREE ONLINE TUTORIAL](#) on Various courses like

[Java](#) | [MIS](#) | [MongoDB](#) | [BigData](#) | [Cassandra](#) | [Web Services](#)

[SQLite](#) | [JSP](#) | [Informatica](#) | [Accounting](#) | [SAP Training](#) | [Python](#)

[Excel](#) | [ASP Net](#) | [HBase](#) | [Testing](#) | [Selenium](#) | [CCNA](#) | [NodeJS](#)

[TensorFlow](#) | [Data Warehouse](#) | [R Programming](#) | [Live Projects](#) | [DevOps](#)

Top 17 Active Directory Interview Questions & Answers

1) Mention what is Active Directory?

An active directory is a directory structure used on Microsoft Windows based servers and computers to store data and information about networks and domains.

2) Mention what are the new features in Active Directory (AD) of Windows server 2012?

- **dcpromo (Domain Controller Promoter) with improved wizard:** It allows you to view all the steps and review the detailed results during the installation process
- **Enhanced Administrative Center:** Compared to the earlier version of active directory, the administrative center is well designed in Windows 2012. The exchange management console is well designed
- **Recycle bin goes GUI:** In windows server 12, there are now many ways to enable the active directory recycle bin through the GUI in the Active Directory Administrative Center, which was not possible with the earlier version
- **Fine grained password policies (FGPP):** In windows server 12 implementing FGPP is much easier compared to an earlier It allows you to create different password policies in the same domain
- **Windows Power Shell History Viewer:** You can view the Windows PowerShell commands that relates to the actions you execute in the Active Directory Administrative Center UI

3) Mention which is the default protocol used in directory services?

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

4) Explain the term FOREST in AD?

Forest is used to define an assembly of AD domains that share a single schema for the AD. All

DC's in the forest share this schema and is replicated in a hierarchical fashion among them.

5) Explain what is SYSVOL?

The SysVOL folder keeps the server's copy of the domain's public files. The contents such as users, group policy, etc. of the sysvol folders are replicated to all domain controllers in the domain.



6) Mention what is the difference between domain admin groups and enterprise admins group in AD?

Enterprise Admin Group	Domain Admin Group
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

7) Mention what system state data contains?

System state data contains

- Contains startup files

- Registry
- Com + Registration Database
- Memory page file
- System files
- AD information
- SYSVOL Folder
- Cluster service information

8) 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.

9) Explain where does the AD database is held? What other folders are related to AD?

AD database is saved in %systemroot%/ntds. In the same folder, you can also see other files; these are the main files controlling the AD structures they are

- dit
- log
- res 1.log
- log
- chk

10) 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

11) Mention what are lingering objects?

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

12) 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.

13) 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.

14) Explain what is a child DC?

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

15) Explain what is RID Master?

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

16) Mention what are the components of AD?

Components of AD includes

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

17) Explain what is Infrastructure Master?

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