Microsoft Active Directory Interview Questions

Whether you are a beginner or experienced candidate, you may come across a number of basic questions in the Active Directory interview.

So, here are the simple and straight most common 25+ Active Directory interview questions you should go through.

1. What is Active Directory?

Active Directory is a directory service that is used to store and manage network such as user accounts, passwords, and other security information. It is a central repository for all the users and computers in a network. Active Directory can be used to centrally manage large networks.

It also provides authentication and authorization for users to access network resources.

2. What are the main components of Active Directory?

The main components of Active Directory are Domain Name System (DNS), Lightweight Directory Access Protocol (LDAP), Kerberos, and Active Directory Domain Services (AD DS).

3. What is a domain in Active Directory?

A domain is a grouping of network resources that share a common security perimeter. In Active Directory, a domain is a logical grouping of computers, users, and other resources that are managed by a single set of administration tools and security policies.

4. What is a domain controller?

A domain controller is a server that is responsible for maintaining the security and integrity of an Active Directory (AD) domain. A domain controller authenticates and authorizes all user and computer access to resources in the domain. In addition, it enforces security policies for the domain, and provides a central point of administration for the domain. They also replicate Active Directory data to other domain controllers.

5. What is DNS in Active Directory?

DNS is a hierarchy of servers that converts human-readable domain names (such as example.com) into IP addresses (such as 192.0.2.1). Active Directory uses DNS to locate domain controllers and other resources in a domain.

6. What is LDAP in Active Directory?

LDAP is a protocol for accessing and manipulating directory information. Active Directory uses LDAP to communicate with other directory services, such as Novell Directory Services (NDS) and Unix-based directory services.

7. What is a forest in Active Directory?

When people talk about Active Directory, they often talk about forests.

A forest is the highest level of organization in Active Directory. It is a collection of one or more domain trees that share a common schema and a common global catalog. A forest can also be seen as a security boundary. Forests provide a measure of security and isolation between domains.

8. List out the benefits of using Active Directory?

Active Directory can help simplify network administration and security. By storing information in a central location, it is easier to manage and secure resources on a network. Additionally, Active Directory can provide single sign-on capabilities, meaning users can access multiple resources with a single set of credentials.

9. What is the Default Domain Policy?

The default domain policy is a group of rules that govern how a domain behaves. It can be used to control various aspects of the domain, such as user accounts, passwords, and security settings. The default domain policy is stored in the Active Directory database and is applied to all users and computers in the domain.

10. What is the Default Domain Controllers Policy?

The Default Domain Controllers Policy is the set of Group Policy settings that are applied to all Domain Controllers in an Active Directory Domain. These rules govern everything from how passwords are stored to how user accounts are managed. The purpose of the Default Domain Controllers Policy is to provide a consistent and secure environment for all users.

11. What are Group Policies?

Active Directory Group Policies are used to manage and configure computer accounts within a domain. Group Policies can be used to centrally manage a variety of settings on domain-joined computers, including:

-Security settings

-Software deployment

-Scripts

-Printer and drive mapping

Group Policies are a powerful tool for managing Active Directory environments, and can be used to make mass changes to computer configurations. If you need to make changes to a large number of computers, Group Policies can save you a lot of time and effort.

12. What is the Active Directory Recycle Bin?

The Active Directory Recycle Bin is a feature in Windows Server that allows you to recover accidentally deleted objects. When you delete an object from Active Directory, it is not immediately removed from the database. Instead, deleted object moved to the Recycle Bin, where it can be restored if necessary.

13. What is Active Directory Federation Services?

Active Directory Federation Services (ADFS) is a Microsoft identity management service that provides single sign-on (SSO) capabilities to internal and external users. It allows organizations to federate their Active Directory (AD) identities with other organizations, such as partners or suppliers. This enables users to access resources in a federated environment using their AD credentials. ADFS also provides a number of features to improve security and usability, such as multi-factor authentication and account recovery.

14. What is Active Directory Certificate Services?

Active Directory Certificate Services (AD CS) is a server role that allows an administrator to issue and manage digital certificates for their organization. AD CS provides a variety of services, including:

– Certificate issuance and renewal

– Certificate revocation

– Certificate template management

– Certification authority (CA) management

AD Certificate Services is an important part of any network security infrastructure and can help to provide a higher level of assurance for communication between devices and applications.

15. What is Active Directory Rights Management Services?

Active Directory Rights Management Services (AD RMS) is a Microsoft technology that provides a centralized way to manage digital rights for documents and other files. This enables organizations to control how their content is used, by whom, and for how long. Additionally, AD RMS can help prevent sensitive information from leaking outside of an organization.

16. What are the risks of using Active Directory?

There are several risks associated with using Active Directory. One of the biggest risks is that Active Directory can be a single point of failure for an organization. If Active Directory goes down, all of the services that depend on it will also go down.

Another risk is that Active Directory can be a target for attackers. If an attacker is able to compromise Active Directory, they can gain access to all of the resources that are protected by it. This can include sensitive data, such as customer data or financial information.

17. How can you secure Active Directory?

There are many ways to secure Active Directory, but some of the most important steps include:

1. Ensure that all domain controllers are running the latest version of the operating system and have all the latest security patches applied.
2. Configure Active Directory to use strong passwords and password policies.
3. Implement multifactor authentication for all users.
4. Use auditing to track changes made to Active Directory objects and monitor for suspicious activity.
5. Restrict access to Active Directory servers and data to only authorized personnel.

By taking these steps, you can help to ensure that your Active Directory environment is secure and protected against potential threats.

18. What are some common Active Directory problems?

There are several common Active Directory problems that can occur. One is that the Active Directory database can become corrupt. This can happen if the database is not properly maintained or if it becomes damaged. Another common problem is that Active Directory can become unresponsive. This can happen if the servers that host Active Directory are not working properly or if the network is congested.

19. What are some Active Directory troubleshooting tips?

There are a few Active Directory troubleshooting tips that can help you if you're having trouble with your AD setup. First, make sure that your DNS settings are correct. Often, problems with AD can be traced back to incorrect DNS settings. Second, check the event logs on your DCs. The event logs can give you valuable insights into what's happening with your AD environment. Finally, make sure to check the replication status of your DCs. Often, replication issues can cause problems with AD.

20. What are some Active Directory best practices?

Active Directory is a powerful tool for managing user accounts and access control in an enterprise environment. However, Active Directory can also be a potential security risk if not configured properly. Here are some best practices for securing Active Directory:

1. Use strong passwords for all accounts.
2. Enable two-factor authentication for all accounts.
3. Use Group Policy Objects (GPOs) to control access to sensitive data and resources.
4. audit all access to Active Directory.
5. Restrict physical access to servers and data centers where Active Directory is deployed.

By following these best practices, you can help to secure Active Directory and prevent unauthorized access to your network

21. What is the SYSVOL folder?

The SYSVOL folder is a critical part of Active Directory. It stores the Active Directory database and log files. Without the SYSVOL folder, Active Directory would not be able to function.

The SYSVOL folder is located on the server that hosts the Active Directory domain controller. The folder is typically located at C:\Windows\SYSVOL.

22. What is a Global Catalog in Active directory?

A global catalog is a database that contains a replica of every object in every domain in a forest. The global catalog is stored on a domain controller that has been designated as a global catalog server and is replicated to every other domain controller in the forest.

The global catalog provides a centralized repository of information that is used to facilitate searches for objects throughout the Forest.

When a user performs a search for an object, the query is directed to a global catalog server. The global catalog server then searches its database and returns a list of any objects that match the search criteria.

23. What is Kerberos in Active directory?

Kerberos is a widely used network authentication protocol. It is used by many large organizations to provide secure access to their networks. Kerberos is a standard component of Microsoft Windows Server and is used by Active Directory to authenticate users.

Kerberos uses a combination of encryption and tickets to provide a secure way for users to authenticate to a network. When a user attempts to log in to a Kerberos-protected system, they are first given a ticket by the Kerberos server. This ticket is then used to request a service from another server on the network.

The ticket is encrypted with the user's password, so only the user who requested the ticket can decrypt it. This ensures that only the intended user can access the network resources.

24. What is an Active Directory Snapshot?

An Active Directory snapshot is a read-only copy of an Active Directory database. It can be used to restore the contents of an Active Directory database in the event of data loss. Active Directory snapshots are made possible by the Volume Shadow Copy Service (VSS), which is a Windows service that creates point-in-time copies of files.

25. What is the difference between domain local, global and universal groups in Active Directory ?

When it comes to Active Directory, there are three different types of groups that you can use to manage user access: domain local, global, and universal.

Domain local groups are used to grant permissions to users within a single domain.

Global groups are used to give permissions to users across multiple domains.

Universal groups are used to give permissions to users across multiple domains and forests.

So, which group should you use? It really depends on your needs. If you only need to give permissions to users within a single domain, then a domain local group is probably all you need. If you need to give permissions to users across multiple domains, then you will need to use a global or universal group.