Top 45 System Admin Interview Questions and Answers – 2023

By Great Learning Team Updated on Nov 16, 2022 139182

A system administrator is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems, especially multi-user computers, such as servers. They work on the configuration and maintenance of the day-to-day operations and ensure that the server and client computers remain secure and perform well. This blog talks about the top system admin interview questions and answers divided into two sections, system admin interview questions and answers for freshers and system admin interview questions for experienced.

Top 10 System Admin Interview Questions that are frequently asked in interviews:

1. Can you tell us about the experience you have with hardware Components?
2. What, according to you, could be the personal characteristics of a person administering a system?
3. Can you give us one of the examples of the systems you have been working with as an Administrator?
4. What do you know about the active directory in the system administration?
5. Can you differentiate between firewall and antivirus?
6. According to you, what is the difference between FAT and NTFS?
7. Describe the concept of DHCP.
8. What is a domain controller?
9. What is group policy?
10. What do you know about proxy servers?

We have further classified system administrator interview Questions into 3 sub-sections, they are:

1. System admin interview questions for freshers
2. System admin interview questions for experienced
3. System Admin Interview Question FAQs

System admin interview questions for freshers

If you are a fresher looking to enter the field of system administration, here is a list of the top system admin interview questions and answers for freshers.

1. What do you know about the active directory in the system administration?

When talking about network security, one thing that matters is the centralized control of everything that the active directory can assure. The information and settings related to the development are stored in the central database.

For example, The database might list 100 user accounts with details like each person's job title, phone number, and password.

2. What is group policy?

Network administrators can use group policy to control the working environment of users and computer accounts in an active directory. It provides a central place for administrators to manage and configure operating systems, applications, and user settings. Using it properly enables you to increase the security of users' computers and help defend against insider and external threats.

3. Why is it said that we should restore a dc that was backed up 9 months ago?

We can face problems due to lingering objects because, when restoring a backup file, the active directory generally requires that the backup file should not be more than 180 days old.

4. Can you tell us about your experience with hardware Components?

A system administrator or system admin should be able to do installation and replacement operations with hardware. Sometimes, there can be a need to rebuild the hardware component.

5. What do forest, trees, and domain mean?

A domain is a logical group of network objects like computers, users, and devices with the same active directory database. A tree is a collection of domains within a Microsoft active directory network in which each domain has exactly one parent, leading to a hierarchical tree structure. A forest is a group of active directory trees.

6. What do you know about WINS servers?

WINS stands for Windows Internet Name Service. This will allow the users to access resources by a computer name rather than an IP address. It is an operating system that uses a centralized computer that will provide specific functions and predetermined rules for the users and the computers connected to a Network. For example, if you want your computer to keep track of the names and IP addresses of other computers in your network.

7. What, according to you, could be the personal characteristics of a person administering a system?

System administrators face a variety of challenges. They are the problem solvers and coordinators. They understand a computer's software, hardware, and networks

in-depth. Thus, they can instruct employees regarding technical issues. Their primary task is to monitor the system. They are able to keep track of the server performance and creative designs for computer systems and quickly arrange for replacement in case of any hardware failure.

8. Can you give us one of the examples of the systems you have been working with as an Administrator?

This typically may include Windows and Linux, which support asset management or GIS.

9. What is a lingering object? What is the command that we use to remove lingering objects? Why is it important to remove the lingering objects?

The lingering object is a deleted active directory that remains on the restored domain controller in its local copy of the active directory. When an object is deleted from the active directory, a Tombstone (which is temporary) is created, which then has to be replicated by the domain controller before it expires, i.e., they seem to occur when some changes are made to the directories after the system backups are created.

When we restore a backup file, the AD (ACTIVE DIRECTORY) generally requires that the backup should not be more than 180 days old. This may happen if, after the backup was done, the object was deleted on another DC more than 180 days ago. In such cases, if we want to remove the lingering object, we use windows server 2003 and windows server 2008 as they can manually remove the lingering objects using the console utility command REPADMIN.EXE. It is necessary to remove the lingering object as it puts an extra burden on the system's RAM and can create the problems like limited space availability.

10. Can you differentiate between firewall and antivirus?

Antivirus: We use antivirus to protect the system from computer viruses. When using your system, it actively monitors for any virus threats from different sources. If it finds any virus threats, it tries to clean or quarantine the virus and keeps your system and data safe.

Firewall: On the flip side, a firewall protects your system from outside/intruder/hacker attacks. Sometimes hackers may take control of your system remotely and steal your vital information or the data from the system. It happens mostly in cases when your system is connected directly to the internet or an extensive network. In that case, you should install a firewall on your pc to protect yourself from unauthorized access. It is either available in software or hardware form. If you have a single PC, the software firewall can do the work, but when you want to protect a large corporation, you have to install a hardware firewall to protect their system from such attacks.

11. According to you, why backing up an active directory is important, and how can you back up an active directory?

To maintain the proper health of the AD database, the backup of an active directory is important.

Windows Server 2003: In this, you can backup the active directory using the NTBACKUP tool that is inbuilt with windows server 2003, or we can also use any 3rd party tool that will support this feature.

Windows server 2008: There is no option to back up the system state data through the normal backup utility. Here we need to use the command line to backup the active directory.

- Step 1 – Open the command prompt by clicking on start, typing “cmd,” and then hitting the enter button.
- Step 2 – In the command prompt, type “wbadmin start systemstatebackup –backuptarget;e:” and then press the enter button.
- Step 3 – Input “y” and press the enter button to start the backup process.

When the backup is finished, you will get a message that the backup is completed if it has not been completed properly, you need to troubleshoot.

12. What is a domain controller?

A domain controller (DC) is a windows-based computer system that is used for storing user account data in a central database. The system administrator allows or denies users access to system resources, such as printers, documents, folders, network locations, etc.

13. According to you, what is the difference between FAT and NTFS?

FAT:

- There is no security when the user logs in locally.
- It usually supports file names with only 8 characters and does not support file compression.
- The partition and file size can be up to 4 GB, and there is no such security permission for file and folder levels.
- It doesn’t support bad cluster mapping, so it is not very reliable.

NTFS:

- There is security for both the local and the remote users.
- It usually supports file names that have 255 characters.
- It supports file compression, and the partition size can be up to 16 exabytes.
- There is security for file and folder levels.
- It supports bad cluster mapping and transaction logging and is highly reliable.

14. Can you tell me what is loopback address and in what sense is it useful?

It is an address that sends outgoing signals back to the same computer for testing purposes. It is managed entirely within the operating system so the client and the server process on a single system and can communicate. It is not physically connected to a network. It is useful because the loopback provides IT professionals with an interface to test the IP software without worrying about broken or corrupted drives or hardware.

15. What do you know about proxy servers?

It acts as the gateway between a local network (e.g., computers in a company) and a large-scale network (for ex: the internet). By using this server, there is an increase in performance and security as it can be used to prevent employees from browsing inappropriate and distracting sites.

16. Can you tell us about the windows registry?

It is often referred to as “the registry.” In the Microsoft Windows operating system, it is the collection of databases of configuration settings (low-level settings). It stores important information like the location of programs, files, etc. If you don’t understand what you are doing, you should not edit the Windows registry, or it will cause problems with the installed applications or the operating system.

17. What is the Sysvol Folder?

We can say that it is a type of shared folder that stores group policy information, or we can say that it contains public files of the domain controllers, and the domain users can access it. Its significant feature is that it is used to deliver policy and login scripts to the domain members.

18. Why is VOIP important?

VOIP is important as it makes the user adopt modern techniques over traditional infrastructure. Using it, the users can use the transmission medium by delivering the voice packets designed for telephone calls.

19. What do you know about Windows deployment services?

The name itself suggests that it is used to deploy the windows operating system (i.e., there is no need to install each operating system directly from CD or DVD. Some tools are used for managing the server.

- Windows deployment services MMC
- Windows PowerShell cmdlets for WDS

- WDSUTIL command-line tool

20. What is the difference between a workgroup and a domain?

In a workgroup, a particular system has a collection of systems having their own rules and local users' logins. Whereas in the domain, the centralized authentication server, which is a collection of systems, tells what the rules are. Workgroups are like P2P networks, whereas domains are like standard client/server relationships.

System Admin Interview Questions for Experienced

If you are an experienced professional looking to attend an upcoming system admin interview and don't know where to look for system admin interview questions, here is a list of the top system admin interview questions for experienced.

21. What can you tell us about the lightweight directory access protocol?

The LDAP (lightweight directory access protocol) is used to name the object in an AD (Active Directory) and makes it widely accessible for management and query applications. It is most commonly used to provide a central place to store the usernames and passwords.

22. What do you know about the PPP protocol?

PPP protocol stands for point-to-point protocol. This protocol helps us communicate between the two computers (routers). The two derivatives of the point-to-point protocol are:

1. Point-to-point protocol over Ethernet
2. Point-to-point protocol over ATM

It is a multilayer protocol that operates on the same communication link.

23. What is IP Spoofing, and what can we do to prevent it?

It is a type of mechanism that is used by attackers to get authorized access to the system. The intruder sends the message to the computer with an IP address from a trusted source/host. We can prevent it by filtering packets using special routers and firewalls that allow packets with recognized formats to enter the network.

24. What is garbage collection?

The memory that is occupied and is no longer in use is called garbage collection. One of the significant advantages of garbage collection is that it frees the user from dealing with memory deallocation. The higher level of programming languages has

more garbage collection, and resources other than memory are not handled by garbage collection.

25. Tell us something about frame relay.

In the OSI model, it operates at the physical and data link layer and is a high-speed data communication technology. It uses frames for the transmission of data in the network.

26. What is DNS?

The DNS stands for the domain name system. The IP addresses are constantly changing, so the DNS makes the IP address into human-friendly names so humans can remember them much more easily. This is less likely to change. For example, if you look at the standard phone book and search for a person's name, you will get their phone number. In this case, the DNS performs the same operation as a standard phone book but with updates on an hourly or daily basis. Due to the tiring nature of the DNS, it makes it possible to have repeated queries that can be responded to quickly.

27. Can you tell the difference between the domain admin groups and the Enterprise admin groups in the ad (active directory)?

Domain admin groups: The members of the domain admin group have complete control of the domain.

Enterprise admin group: The members of the enterprise admin group have complete control of the domains in the forest.

28. What is the authoritative restoration of the active directory?

To perform an authoritative restore, we first need to perform a non-authoritative restore process. As we know that the authoritative restore can increment the version number of the attributes, this will make us restore an object in the directory. On the flip side, when we discuss the non-authoritative restore to determine the changes since the last backup, it will contact the replication partners after a domain controller is back online.

29. What will be your daily routine if you are a system administrator?

Your answer should reflect that you are well aware of the responsibilities of the system administrator or the tasks to be performed by the system administrator.

For example, Tasks like software installation and updates, providing system access control, creating backups, data recovery, etc.

30. What do you know about the object server?

The application of the client/server is written in the form of communication objects. The client objects communicate with server objects using ORB (Object Request Broker). This server object provides support for concurrency and sharing.

31. What is the working of traceroute, and what protocol does it use?

Depending on the operating system, the Tracert, also called a traceroute, allows you to see what all the routers you touch when you move along the chain of connections to reach the final destination. If a case arrives in which you can't ping your final destination, tracers can be used as they can tell you exactly where the chain of connections stopped. You will be able to contact the correct people, may it be your firewall, your ISP, your destination's ISP, or anywhere in the middle. The traceroute uses ICMP protocol but is also having the ability to use the first step of the TCP to send the SYN requests for the response.

32. What do you know about NETBIOS and NetBEUI?

NETBIOS is referred to as the network basic input or output system. It is a layer 5 protocol that is non-routable. It allows the applications to communicate with one another over LAN, or we can call it a local area network. NETBIOS normally runs over a TCP/IP, resulting in a network with both an IP address and a NETBIOS name corresponding to the hostname.

There are three different services that NETBIOS provides:

- Name service: The name registration and resolution is made
- Datagram distribution service: It is generally used for connectionless communication
- Session service: It is used for connection-oriented communication

NETBUI: NetBEUI is an extended version of the NETBIOS. It is a networking protocol that IBM and Microsoft developed in 1985. It is a primary protocol for the Lan manager and windows for workgroups. It supports both connection-based and connectionless communication. It implements flow control and error detection. It is one of the fastest and most efficient protocols. The enhanced implementation of a protocol available on the Microsoft Windows NT operating system is called the NetBEUI frame. We should use it only on smaller network sizes as it relies more heavily on broadcast packets than on the TCP or an IP, i.e., it is unsuitable for WAN (wide area networks) and is also a non-routable protocol.

33. Can you tell us about RSVP and how it works?

RSVP refers to Resource Reservation Protocol. As the name suggests, it is used to reserve resources across a network, so when we look into the working of the RSVP. In the RSVP, the host's request is carried throughout the network and then visits each node. It has two local modules for reservation of resources: the admission

control module and the policy module. The admission module checks whether there are sufficient available resources, whereas the policy module checks the permission to make a reservation. After these two checks are performed, the RSVP uses the packet classifier and the packet scheduler for desired QoS requests.

34. Describe the concept of DHCP?

DHCP refers to dynamic host configuration protocol. This protocol is used to assign the IP address to the computers. So when we use the DHCP protocol, its IP address is changed whenever a computer is connected to a network. In other words, we can say that we will have different IP addresses. In some cases, the IP address is changed when the computer is in the network. We can say that a clear-cut advantage of the DHCP protocol is that rather than using the administrator to manage the IP address, we use the software.

35. Can you tell us the main email servers and which are their ports?

There are two types of email servers: incoming and outgoing mail servers.

1. **The incoming mail server:** This mail server is usually associated with the email address account. You should have the correct settings in your email client program to download the emails. In this server, there cannot be more than one incoming server.
2. **The outgoing mail server:** When we are talking about the outgoing mail server, the protocol used to send emails is SMTP, known as the simple mail transfer protocol. The main email portal includes: (POP3 – PORT 110, IMAP – port 143, STMP – port 25, HTTP – port 80, secure SMTP – PORT 465, Secure IMAP – port 585, IMAP4 over SSL – port 993, secure POP3 – port 995).

36. Can you differentiate between a hub and a switch?

Both the hub and the switch are roughly the same. They both have a more significant number of potential connections and are used for the same primary purpose of creating a network. The only difference is how they handle the connections in the hub case. They broadcast all the data to every port and hence, can cause serious security and reliability concerns and several collisions on that network. On the flip side, when we talk about switches, the connections are created dynamically, so the requesting portal only receives the information designed for it. We can consider a hub where all are talking at the same time, but this can be inconvenient as it can transmit or release information to the people whom you don’t want to have access to that information on the other side when we talk about switches they are creating the connections between the ports as in need.

37. What do you know about HTTPS, and what port does it use?

The HTTPS uses the SSL certificates to confirm that the server you are connecting to is the one it says. The HTTPS traffic goes over TCP port 443.

38. What can you tell us about TCP?

TCP/IP is not a protocol but is a member of the IP protocol suite. The TCP refers to Transmission Control Protocol and is a massively used protocol (for ex: HTTP, FTP & SSH). One of the benefits of TCP is that it establishes the connection on both ends before any data starts to flow. It is also used to sync up the data flow as if a case arrives when the packets arrive out of order, so the receiving system should be able to figure out what the puzzle of packets is supposed to look like.

39. What do you know about UDP?

We can call the UDP the twin of the TCP. The UDP stands for User Datagram Protocol. The UDP doesn't care if somebody is listening on the other end or not, and it is called the connectionless protocol. Whereas, when we talk about the TCP, it makes everybody stay on the same page. The transmission speed on a UDP is faster than the transmission speed of TCP. The TCP always needs confirmation from the other side that the message is received or not. On the other side, the UDP is like a television broadcast in which the transmitter doesn't care or know about the person on the other end.

40. What can you tell us about port forwarding?

When we want to communicate with the inside of a secured network, there is the use of a port forwarding table within the router or other connection management device that will allow the specific traffic to be automatically forwarded to a particular destination. It probably does not allow access to the server from outside directly into your network.

41. Can you differentiate between a PowerShell and a Command prompt?

Powershell: it was introduced in the year 2006. We can open the power shell by typing PowerShell. It operates on both the batch commands and the PowerShell commands. It allows the user to navigate easily between the functions by providing the ability to create aliases for cmdlets or scripts. The output comes in the form of an object and can be passed from one cmdlet to another. It can also execute a sequence of cmdlets that are put together in a script. It is built on a net framework, so it has access to the programming libraries and can be used to run all types of programs. It supports the Linux-based system, can connect with the Microsoft cloud products, and integrates directly with WMI. It also has an ISE.

Command Prompt: It was introduced in the year 1981. We can open a command prompt from running by typing cmd. It cannot operate on both the batch commands and the PowerShell commands; it only operates on batch commands. There is no support for the creation of aliases of commands. The output that is formed is in the form of text. We can not transfer or pass the output from one command to the other command. When we want to run a certain command, the command that is run first must be finished. In this case, there is no such command as the help command as in the case of PowerShell to get the information regarding the commands. There is no separate ISE; there is only a command line interface it can only run console type of

programs. It doesn't support the Linux-based system and cannot connect with the MS online products. There is a need for an external plugin for WMI interaction. It doesn't have access to the libraries.

42. Can you tell the difference between an RDP and a KVM?

The RDP stands for Remote desktop protocol, as the name itself suggests about the nature of this protocol. It is one of the primary methods by which we can access the windows system remotely for troubleshooting purposes and is a software-driven method. In contrast, when we talk about the KVM, it refers to keyboard video and mouse, and it allows fast-switching between different systems by using the same keyboard monitor and mouse. It is a hardware-driven method or system in which a junction box is placed between the user and the systems. The KVM does not require any active network connection, so it is very useful to use the same setup on multiple networks without doing the cross talk.

43. What do you know about FTP and SSH? What protocol do they use?

FTP – The FTP is referred to as the file transfer protocol. It is primarily designed for transferring large files and can resume the download if interrupted. We can access the FTP server using two techniques: Anonymous access and standard login. There is only one difference between the techniques: the anonymous doesn't require an active user login, whereas the standard login requires an active user login. The FTP uses ports 20 and 21 of TCP.

SSH – SSH stands for secure shell and is very well known by Linux users. The secure shell is used to create a secure tunnel between devices (for example:- systems, switches, thermostats, etc.) .it also can tunnel the other programs through it. So in case the programs having unsecured connections can be used in the secured state if we configure it correctly. The SSH uses port 22 of the TCP

44. What are ARP and EFS?

ARP refers to the address resolution protocol that allows the DNS to be linked to MAC addresses; the mapping of the human-friendly URLs to IP addresses is allowed by standard DNS. At the same time, the address resolution protocol allows the mapping of IP addresses to mac addresses. In this manner, the system goes from a regular domain name to an actual piece of hardware.

EFS: it refers to the encrypted file system. The encrypted files tied to the specific user become difficult when trying to decrypt a file without the user's assistance. There can also be a case when the user forgets their password or loses their password in such case. It becomes almost impossible to decrypt the file as the decryption process is tied to the user's login and password. It can only occur on NTFS formatted partitions. For a larger purpose, the better alternative is a Bitlocker.

45. What is an id?

IDs stand for an intrusion detection system that has two basic variations:

1. Host intrusion detection system (HIDS) runs as a background utility like an antivirus.
2. Network intrusion detection system: When they go across the network to start looking for things that are not ordinary, it sniffs packets.

46. What is Telnet?

It is one of the application protocols that allow the connection on any port and is a very small and versatile utility. It allows the admin to connect to the remote devices. In case telnet transfers data in the form of text. On a remote host, the telnet provides access to a command-line interface because of security concerns when we use the telnet over an open network source such as the internet. It is significantly in favor of SSH. It has a negotiable protocol architecture, because of which many extensions were adopted. Most telnet implementation has no authentication, ensuring that the communication Is carried out between the two desired hosts. It does not encrypt any data that has been sent over the connection. Generally, it is used to establish a connection to TCP (transmission control protocol) port 23, where the server application of the telnet is listening.

System Admin Interview Question FAQs

What is system administration?
System administration is the process of maintaining and managing a computer system. This includes the hardware, software, and network resources that make up a system. System administrators are responsible for ensuring the system is available and functioning correctly, and they may also be responsible for providing training and support to users.

What are the skills of a system administrator?
A system administrator should have many skills to be effective in their role. They should be able to manage and configure networks, servers, and storage systems, and they should also be able to troubleshoot and resolve issues that may arise. Additionally, system administrators should have strong communication and customer service skills to interact with users and other IT staff.

How do I prepare for a system administrator interview?
You can prepare for a system admin interview by reading this blog on the top 45 system admin interview questions. Further, you can head to Great Learning Academy and learn more about a system administrator career path.

What is the role of a system administrator?
The sysadmin's responsibilities include ensuring that system hardware, software, and related procedures adhere to organizational values and that the system's availability, performance, and security are continuously maintained. In larger

organizations, system administrators typically work in teams responsible for different areas of the network, such as storage, security, or email.