[System Administrator interview questions and answers](http://sysadminreference.blogspot.com/2013/07/system-administrator-interview.html)

**1) Differentiate between NTFS & FAT.**  
NTFS is the current file system used by Windows. It offers features like security permissions (to limit other users' access to folders), quotas (so one user can't fill up the disk), shadowing (backing up) and many other features that help Windows.  
  
FAT32 is the older Microsoft filesystem, primarily used by the Windows 9X line and Window could be installed on a FAT32 parition up to XP. In comparision, FAT32 offers none of what was mentioned above, and also has a maximum FILE (not folder) size of 4GB, which is kind of small these days, especially in regards to HD video.  
  
**2) What Is VOIP.**  
  
  
VOIP - Short for Voice Over Internet Protocol, a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions.

**3) What is loop back.**

Loopback address is 127.0.0.1,

An address that sends outgoing signals back to the same computer for testing.

**4) What is Proxy Server.**   
  
A proxy server is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet. Proxy servers provide increased performance and security. In some cases, they monitor employees' use of outside resources.  
  
  
**5) Differentiate between FIREWALL/ANTIVIRUS.**  
  
**Antivirus:**  
The prime job of an anivirus is protect your system from computer viruses. Your computer may be standalone or part of network or connected to Internet you need an antivirus program. It actively monitors when you are using your system for any virus threat from different sources. if it found one it tries to clean or quarantine the virus ultimately keeping your system and data safe.  
  
**Firewall:**  
Firewall is in other hand a program which protects your system from outsider/intruder/hacker attacks. These attacks may not be virus type. In some cases hackers can take control of your system remotely and steal your data or important information from system. If your system is directly connected to internet or a large network than you can install a software firewall in your PC to protect your self from unauthorized access. Firewall is available either in software or in hardware form. For a single PC you may need a software firewall while a large corporate implements hardware firewall to protect all of their systems from such attacks.  
  
**6) Differentiate between Frond end & Back End Server.**  
  
**Backend server:**  
  
A back end server is a computer resource that has not been exposed to the internet. In this regard the computing resource does not directly interact with the internet user. It can also be described as a server whose main function is to store and retrieve email messages.  
  
**Frontend server:**    
  
A frontend server is a computer resources that has exposed to the internet.  
  
  
**7) What is APIPA.**  
  
Stands for Automatic Private IP Addressing  
APIPA is a DHCP fail over mechanism for local networks. With APIPA, DHCP clients can obtain IP addresses when DHCP servers are non-functional.   
  
APIPA exists in all modern versions of Windows except Windows NT.   
  
When a DHCP server fails, APIPA allocates IP addresses in the private range 169.254.0.1 to 169.254.255.254.  
  
  
**8) How Release and renew IP address from Command prompt.**  
  
Ipconfig / release  
ipconfig / renew  
  
  
**9) What is wins server.**  
  
Windows Internet Name Service (WINS) servers dynamically map IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of by IP address. If you want this computer to keep track of the names and IP addresses of other computers in your network, configure this computer as a WINS server.  
If you do not use WINS in such a network, you cannot connect to a remote network resource by using its NetBIOS name.  
  
  
**10)What is the Windows Registry.**  
  
The Windows Registry, usually referred to as "the registry," is a collection of databases of configuration settings in Microsoft Windows operating systems.  
  
  
**11) System Volume Information (SVI) Folder.**  
  
Windows XP includes a folder named System Volume Information on the root of each drive that remains hidden from view even when you choose to show system files. It remains hidden because it is not a normally hidden folder you can say it is a Super Hidden Folder. Windows does not shows Super Hidden Folders even when you select "Show Hidden Files."  
  
  
**12 ) What is MBR.**  
  
Short form Master Boot Record, a small program that is executed when a computer boots up. Typically, the MBR resides on the first sector of the hard disk. The program begins the boot process by looking up the partition table to determine which partition to use for booting  
  
  
**13) What is Bit Locker**.  
  
BitLocker is an encryption feature available in Ultimate and Enterprise versions of Windows 7 and Vista,  
To encrypt an entire drive, simply right-click on the drive and select Turn on BitLocker from the context menu.  
  
**14) Difference  b/w sata and IDE.**  
  
IDE and SATA are different types of interfaces to connect storage devices (like hard drives) to a computer's system bus. SATA stands for Serial Advanced Technology Attachment (or Serial ATA) and IDE is also called Parallel ATA or PATA. SATA is the newer standard and SATA drives are faster than PATA (IDE) drives. For many years ATA provided the most common and the least expensive interface for this application. But by the beginning of 2007, SATA had largely replaced IDE in all new systems.  
  
  
  
**15)Main Difference Between Windows server 2008 and 2012**  
  
1) New Server Manager: Create, Manage Server Groups  
  
2) Hyper-V Replication :  The Hyper-V Replica feature allows you to replicate a virtual machine from one location to another with Hyper-V and a network connection—and without any shared storage required. This is a big deal in the Microsoft world for disaster recovery, high availability and more. VMware does this, too, but the vendor charges new licensees extra for the capability.  
  
3) Expanded PowerShell Capabilities  
  
4)IIS 8.0  and IIS 7 in 2008  
5)Hyper-V 3.0  
6)PowerShell 3.0  
  
**16)How Long My Computer Has Been Running? Get to Know My Computer’s Uptime.**  
  
Start   Task manager,    and select    Performance tab .  
  
In performance tab we can see system up time  
  
Method 2: By typing systeminfo in command prompt we can find out up time of your server  
  
In system boot time.  
  
  
**17)Event viewer in Windows server**  
  
Control panel - Administrative tools - Computer Management - event Viewer  
  
Three types events  
Error.  
Warning.  
Information.  
  
  
**18)** **Manage Multiple, Remote Servers with Server Manager.**  
  
Server Manager is a management console in Windows Server® 2012 R2 Preview and Windows Server® 2012 that helps IT professionals provision and manage both local and remote Windows-based servers from their desktops, without requiring either physical access to servers, or the need to enable Remote Desktop protocol (RDP) connections to each server. Although Server Manager is available in Windows Server 2008 R2 and Windows Server 2008, Server Manager was updated in Windows Server 2012, to support remote, multi-server management, and help increase the number of servers an administrator can manage.   
  
  
**19) What happens when we type URL in browser**.

First the computer looks up the destination host. If it exists in local DNS cache, it uses that information. Otherwise, DNS querying is performed until the IP address is found.  
  
Then, your browser opens a TCP connection to the destination host and sends the request according to HTTP 1.1 (or might use HTTP 1.0, but normal browsers don't do it any more).  
  
The server looks up the required resource (if it exists) and responds using HTTP protocol, sends the data to the client (=your browser)  
The browser then uses HTML parser to re-create document structure which is later presented to you on screen. If it finds references to external resources, such as pictures, css files, javascript files, these are is delivered the same way as the HTML document itself.

**DHCP:**

**1) How DHCP work?**  
  
DHCP Stands for Dynamic host configuration protocol.  
DHCP is a protocol used for automatic configuration IP address in client computers connected to IP networks. DHCP operates on a client server model in four phases.  
  
Discover: A client broadcasts DHCP Discover message when it comes alive on the network.  
  
Offer: When a DHCP server receives the DHCP Discover message from the client, it reserves an I P address for the client and sends a DHCP Offer message to the client offering the reserved IP address.  
  
Request: The client receives the DHCP offer message and broadcasts a DHCP request message to show its consent to accept the offered IP address.  
  
Acknowledge: When the DHCP server receives the DHCP Request message from the client, it sends a DHCP Ack packet to the client. At this point the IP configuration process is complete.  
  
  
**2) What is DHCP Scope.**  
  
A range of IP address that the DHCP server can assign to clients that are on one subnet.  
  
  
  
**3) What protocol and port does DHCP use.**  
  
UDP protocol and 67 port in client and 68 port in server.  
  
  
**4) What is a DHCP lease.**  
  
A DHCP lease is the amount of time that the DHCP server grants to the DHCP  
client permission to use a particular IP address. A typical server allows its  
administrator to set the lease time.  
  
**5) Can DHCP support statically defined addresses**.  
  
Yes.  
  
6) Define Dora Process & why it is used.   
Discover, Offer, request and acknowledgement. it is used to assign ip address automatically to client systems.  
  
**7) What is Authorizing DHCP Servers in Active Directory.**  
  
If a DHCP server is to operate within an Active Directory domain (and is not running on a domain controller) it must first be authorized to Active directory.  
  
8)**How to Backup and Restore DHCP in Windows Server 2008**  
  
In Windows Server 2008, backup of DHCP database and settings has gotten simpler. You may want to backup your DHCP server from time to time to prepare for disaster recovery scenarios or when migrating DHCP server role to a new hardware.   
  
**Backup DHCP Server**  
1. Open Server Manager > DHCP role   
2. Right click server name, choose Backup..   
3. Choose a location for backup, click OK   
  
**Restore DHCP Server**  
1. Open Server Manager > DHCP role   
2. Right Click server name, choose Restore   
3. Choose the location of the backup, click OK   
4. Restart the DHCP Service   
  
  
  
  
  
  **DHCP Databse location**: C:\WINDOWS\System32\DHCP directory. 

**DNS**

**1) Define DNS .**  
  
 Domain Name System, DNS is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember.  
  
Two types of lookup in DNS.  
  
Forward lookup : it converts Domain name to ip address.  
Reverse lookup: it converts ip address to Domain name.  
  
Three types of zone.  
  
Primary zone  
secandary zone and stub zone.  
  
**what is the port no of DNS.**  
  
UDP and  port number - 53  
  
**What is NSlookup.**  
  
Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through Control Panel.    
  
MS-DOS utility that enables a user to look up an IP address of a domain or host on a network.

**Active directory and Domain**

**1) What is LDAP? Why it is used.**  
  
LDAP is the Lightweight Directory Access Protocol. Its an active directory protocal ,Basically, it's a protocol used to access data from a database    
  
  
**2) What is Active Directory? Why it used.**  
  
 Active Directory is a Directory Service created by Microsoft. It is included with most Windows Server operating systems.   
  
Active Directory is primarily used to store directory objects like users and groups and computers printers.  
Using Active Directory brings a number of advantages to your network,  
Centralized user account management  
Centralized policy management (group policy)  
Better security management  
  
  
**3) What Is Group Policy.**  
  
Group Policy is a feature of the Microsoft Windows NT family of operating systems that control the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. 

**4) What is the order in which GPOs are applied .**

   Local Group Policy object

   site ,

   Domain and

   organizational units.

**5) What is the difference between software publishing and          assigning.**

Assign Users : The software application is advertised when the user logs on. It is installed when the user clicks on the software application icon via the start menu, or accesses a file that has been associated with the   software application.

Assign Computers :The software application is advertised and installed   when it is safe to do so, s uch as when the computer is next restarted.

Publish to users : The software application does not appear on the start menu or desktop. This means the user may not know that the software is available. The software application is made available via the Add/Remove Programs option in control panel, or by clicking on a file that has been associated with the application. Published applications do not reinstall themselves in the event of accidental deletion, and it is not possible to publish to computers.

**6) Can I deploy non-MSI software with GPO.**

create the fiile in .zap extension.

**7) Name some GPO settings in the computer and user parts.**

Computer Configuration, User ConfigurationName

**8) Name a few benefits of using GPMC.**

Easy administration of all GPOs across the entire Active Directory Forest

View of all GPOs in one single list

Backup and restore of GPOs Migration of GPOs across different domains and forest.

**9) How frequently is the client policy refreshed ?**

90 minutes give or take.

**10) Where are group policies stored ?**

C:\Windows\System32\GroupPolicy.

**11) Group policy backup**

To backup a single GPO, right-click the GPO, and then click Back Up.

To backup all GPOs in the domain, right-click Group Policy Objects           and click Back Up All.

**12) Define DSRM Mode?**

Directory Services Restore Mode (DSRM) is a special boot mode for repairing or recovering Active Directory. It is used to log on to the computer when Active Directory has failed or needs to be restored.

To manually boot in Directory Services Restore Mode, press the F8 key repeatedly. Do this immediately after BIOS POST screen, before the Windows logo appears. (Timing can be tricky; if the Windows logo appears you waited too long.) A text menu menu will appear. Use the up/down arrow keys to select Directory Services Restore Mode or DS Restore Mode. Then press the Enter key.

**13) Where is the AD database held? What other folders are related            to AD?**

  The AD data base is stored in c:\windows\ntds\NTDS.DIT.

**14 ) Have you ever Installed AD?**

     To Install Microsoft Active Directory:

Ensure that you log on to the computer with an administrator account to perform installation.

Click electing Start > **Administration Tools** > **Server manager** > **Configure your Server.**

In the Welcome page, click Next.

In the Operating system compatibility panel, click Next.

On the Domain Controller Type panel, **select Domain controller for a new domain** and click Next.

On the Create New Domain panel, **select Domain in a new forest** and click Next.

On the New Domain Name panel, enter the **DNS suffix for your new Active Directory**. This name will be used during Tivoli Provisioning Manager installation, so make a note of it. Click Next.

On the NetBIOS Domain Name panel, enter the **NetBIOS name of the domain**. The first part of the DNS name is usually sufficient. Click Next.

On the Database and Logs panel, select the desired folders for the Database and Logs.**C:\Windows\NTDS is the default**. Click Next.

On the Shared System Volume panel, enter a valid directory for the system volume.**C:\Windows\Sysvol is the default**. Click Next to continue.

If you configured DNS successfully, the Permissions setting panel is displayed. Select Permissions compatible only with Windows 2000 or Windows Server 2003. Click Next.

On the Directory Services Restore Mode Administrator Password panel, enter a valid password to be used when running the Directory Services in Restore Mode. Click Next

Verify the settings and Click Next to begin the Active Directory configuration. The server will be rebooted as part of the process.

**15) What is the use of SYSVOL folder**

All active directory data base security related information store in SYSVOL folder and it’s only created on NTFS partition.

**16) What is global catalog**

The Global Catalog is a database that contains all of the information pertaining to objects within all domains in the Active Directory environment

**17) What is the difference between local, global and universal groups**

Domain local groups assign access permissions to global domain groups for local domain resources. Global groups provide access to resources in other trusted domains. Universal groups grant access to resoures in all trusted domains.

**18) 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

**19) What is Domain control?**

A domain controller (DC) is a server that handles all the security requests from other computers and servers within the Windows Server domain

there was a primary domain controller and a backup domain controller. The primary DC focused on domain services only to avoid the possibility of a system slow down or crash due to overtasking from managing other functionality and security requests. In the event of a primary DC going down, a backup DC could be promoted and become the primary DC to keep the rest of the server systems functioning correctly

**20) What is domain?**

A domain is a set of network resources (applications, printers, and so forth) for a group of users. The user needs only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network. The ‘domain’ is simply your computer address not to confuse with an URL. A domain address might look something like 211.170.469.

**21) What is Forest?**

A collection of one or more Active Directory domains that share a common schema, configuration, and global catalog.

**22) What is global catalog.**

The Active Directory Global Catalog is the central storage of information about objects in an Active Directory forest. A Global Catalog is created automatically on the first domain controller in the first domain in the forest. The Domain Controller which is hosting the Global Catalog is known as a Global catalog server.

**23) What is tree.**

An Active Directory tree is a collection of Active Directory domains that begins at a single root and branches out into peripheral, child domains. Domains in an Active Directory tree share the same namespace. An Active Directory forest is a collection of Active Directory trees, similar to a real world forest. Catalog Server.

**24) What is site.**

A Site object in Active Directory represents a geographic location that hosts networks.

**25)  Flexable Single Master Operation Roles (FSMO)**

The 5 FSMO server roles:

|  |  |  |
| --- | --- | --- |
| Schema Master | Forest Level | One per forest |
| Domain Naming Master | Forest Level | One per forest |
| PDC Emulator | Domain Level | One per domain |
| RID Master | Domain Level | One per domain |
| Infrastructure Master | Domain Level | One per domain |

**26) Command to Add client to Domain**

NETDOM /Domain:MYDOMAIN /user:adminuser /password:apassword MEMBER MYCOMPUTER /JOINDOMAIN

**27) Setting File Permissions on a Folder Using Group Policy**

The setting is located under Computer Configuration, Windows Settings, Security Settings, File System. Here's the procedure:

Go to the location in the Group Policy listed above.

Right-click File System.

Click Add File.

In the "Add a file or folder" window, select the folder (or file) for which you want the permissions to be set, and click OK.

In the security box that pops up, you can add a user or a group that needs permission to the folder.

**Vertualization**

**1)Define virtualization.**

Hyper-V virtualization will provide an environment in which we can run multiple operating systems at the same time on one physical computer, by running each operating system in its own virtual machine.

**2) What are the benefits of virtualization ?**

Reduce the number of physical servers

Reduce the infrastructure needed for your data center

**3) What is a Hypervisor.**

You can think of a Hypervisor as the kernel or the core of a virtualization platform. The Hypervisor is also called the Virtual Machine Monitor. The Hypervisor has access to the physical host hardware.

**4) What are a host, guest, and virtual machine.**

A host system (host operating system) would be the primary & first installed operating system.  If you are using a bare metal Virtualization platform like Hyper-V or ESX, there really isn’t a host operating system besides the Hypervisor. If you are using a Type-2 Hypervisor like VMware Server or Virtual Server, the host operating system is whatever operating system those applications are installed into.

A guest system (guest operating system) is a virtual guest or virtual machine (VM) that is installed under the host operating system. The guests are the VMs that you run in your virtualization platform.

Some admins also call the host & guest the parent and child.

**Hyper v Snap shot:**

**How to create Hyper v Snap shot:**

Just select the Virtual machine in Hyper-V Manager and select Snapshot from the Actions pane. The status of the virtual machine will change to “Taking Snapshot” and show the progress of the action using a percentage value.

**File extension = .avhd**

**Virtual Machine files**

The first thing to know is what files are used to create a virtual machine:

.XML files

These files contain the virtual machine configuration details.  There is one of these for each virtual machine and each snapshot of a virtual machine.  They are always named with the GUID used to internally identify the virtual machine or snapshot in question.

.BIN files

This file contains the memory of a virtual machine or snapshot that is in a saved state.

.VSV files

This file contains the saved state from the devices associated with the virtual machine.

.VHD files

These are the virtual hard disk files for the virtual machine

.AVHD files

These are the differencing disk files used for virtual machine snapshots