SYSTEM AND NETWORK ADMINISTRATION

SHORT QUESTIONS

When a device is turned on and connected to a network that has a DHCP server, it sends a request to the server, called a DHCPDISCOVER request.
After the DISCOVER packet reaches the DHCP server, the server holds on to an IP address that the device can use, then offers the client the address with a DHCPOFFER packet.
Once the offer has been made for the chosen IP address, the device responds to the DHCP server with a DHCPREQUEST packet to accept it. Then, the server sends an ACK to confirm that the device has that specific IP address and to define the amount of time that the device can use the address before getting a new one.

1. **Is it easy to manage dynamic DNS with DHCP?**
   We're unimpressed by DHCP systems that update dynamic DNS servers. This flashy feature adds unnecessary complexity and security risk.
2. **Write two major benefit of LYNC? * 2019**
3. **Define SLA and its procedure?** Service Level Aggreeement
   An SLA is a written document that specifies what kind of service and performance that service providers commit to providing. This policy should be written in dialogue with your customers. Once the SLA is determined, it can be turned into a policy specifying how the SLA will be achieved.
4. **Discuss hot swap component and what is the benefit of using hot swap component? * 2019**
   Hot-swap refers to the ability to remove and replace a component while the system is running. Normally, parts should be removed and replaced only when the system is powered off. The first benefit of hot-swap components is that new components can be installed while the system is running.
5. **What is cryptography?**
   Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of adversarial behavior.
   Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
   Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information.
6. **Why IPSec used?**
   IPsec is a framework of related protocols that secure communications at the network or packet processing layer. It can be used to protect one or more data flows between peers. IPsec enables data confidentiality, integrity, origin authentication and anti-replay.
7. **How syslog is managed?**
   A Syslog server needs to receive messages sent over the network. A listener process gathers syslog data sent over UDP port. UDP

   Syslog is the best way to consolidate data over a single location.Syslog uses listner process to listen logs and data over to udp port and store them in a single database

messages aren't acknowledged or guaranteed to arrive, so be aware that some network devices will send Syslog data via TCP to ensure message delivery.

8. **List down any two network services?**

   - Directory services.
   - e-Mail.
   - File sharing.
   - Instant messaging.

9. **Why network monitoring tool is used?**

   Network monitoring tools offer multiple technologies to monitor all the network layers and different types of devices in the network. They can quickly detect and report issues such as application delivery failure, routing problems, bandwidth consumption, and hardware malfunctions, and can help resolve the problems.

10. **What are IP tables?**

    iptables is a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall, implemented as different Netfilter modules. The filters are organized in different tables, which contain chains of rules for how to treat network traffic packets.

11. **What is difference between root user and other user?**

    The **root user** is allowed to access all files and programs in the system, whether or not root owns them. The root user is often called a superuser.

    Normal users can access only what they own or have been given permission to run; permission is granted because the user either belongs to the file's group or because the file is accessible to all users.

12. **Discuss difference between open cable management and close cable management?**

    Open cable management has a series of large split hoops that all the cables go behind. Cables are slotted through the gaps in the hoops as they are run from one place to the other. The hoops keep the cables within a confined channel or area. Closed cable management consists of a channel with a cover.

    Closed cable management consists of a channel with a cover. The cover is removed, cables are placed in the channel, and then the cover is replaced. Open cable management can look messier if not

maintained well, but closed cable management often is used to hide huge loops of cables that are too long.

13. **What is crypt analysis?**

    Cryptanalysis refers to the process of analyzing information systems in order to understand hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

14. **Why we use IDS sensors?** Intrusion Detection Sensors

    IDS sensors can detect network devices and hosts, they can inspect the data within the network packets and identify the services or operating systems that are being utilized. This saves a lot of time when compared to doing it manually. An IDS can also automate hardware inventories, further reducing labor.

15. **What are difference permission groups associated with file?**

    The following access types are possible:

    - (r) Read permission
    - (w) Write permission
    - (x) Execute permission
    - (-) No permission or no access

16. **Write down the command to visualize network addresses?**

    To see all of the devices connected to your network, type arp -a in a Command Prompt window. This will show you the allocated IP addresses and the MAC addresses of all connected devices.

---

17. **What are different types of server OS available now days?**

    - Microsoft Windows servers
    - Linux / Unix servers.
    - NetWare
    - Cloud servers.

18. **Write the scope of system and network administration? * 2019**

    Network administrators install, support and manage the network and computer systems that keep information flowing. They implement and maintain network hardware and software, troubleshoot network

problems, and ensure network security, availability & performance standards.

19. **Which file contain information about password policies such as expiry? * 2019**
    A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account and is therefore less of a security risk.
20. **What is the factor involve for baying server hardware?**
    Extensibility.
    More CPU performance.
    High-performance I/O.
    Upgrade Options
    Rack Mountable
    No Side Access Needs
    High Availability
    Maintenance
    Management Options

    Demand specific Hardware
21. **Write the difference between NTFS and FAT32?**
    FAT32 stands for File Allocation Table. FAT32 is an extension of previous file systems in which the data is stored in chunks of 32 bits. FAT32 is an upgraded version of FAT16 designed to overcome the limitations of FAT16 and add support for larger media.
    NTFS stands for New Technology File System. First introduced in 1993, it is used in newer versions of operating systems such as Windows NT and 2000 and later versions of Windows.

    NTFS:
    it provides a way for system changes to be written to a log, or a journal, before the changes are actually written. This feature allows the file system to revert to previous, well-working conditions if a failure occurs because the new changes have yet to be committed.
22. **What are the difference between passwd and shadow file?**
    on UNIX systems, the **/etc/shadow** file that stores the password has stricter protection than the **/etc/passwd** file that stores the UID, person's full name, home directory, and preferred shell.
23. **Why mountable racks are important while buying servers for networks?**
    Servers should be rack-mountable. Choosing rack-mountable and reasonably sturdy racks to bolt it into rather than putting equipment on shelves can significantly reduce the impact of a minor earthquake for little or no extra cost.
24. **Define data security?**

Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

25. **How windows and linux trace route do differ?**
    The difference between tracert(windows) and traceroute(linux) is that: tracert(windows) will only use ICMP echo requests. traceroute(linux) [and somewhat dependent on linux distro] default to UDP echo requests.
26. **What is meant by authentication and authorization?**
    Authentication is the act of validating that users are whom they claim to be. This is the first step in any security process.
    Authorization in system security is the process of giving the user permission to access a specific resource or function. This term is often used interchangeably with access control or client privilege.
27. **Discuss about the need for bash shell?**
    In many cases, we'll use Bash to issue commands one-by-one at a command prompt. Bash allows us to combine these commands, along with control structures and other basic programming constructs, into scripts. Text files which contain a series of commands, and can be run like programs. And can also be shared with others.
28. **What is difference between cron job and bash scripting?**
    The **cron** command-line utility, also known as cron job is a job scheduler on Unix-like operating systems. Users who set up and maintain software environments use cron to schedule jobs to run periodically at fixed times, dates, or intervals.
    A shell script is a computer program designed to be run by the Unix shell, a command-line interpreter. The various dialects of shell scripts are considered to be scripting languages. Typical operations performed by shell scripts include file manipulation, program execution, and printing text.
29. **Write down the command the change the permission of file?**
    The **chmod** command enables you to change the permissions on a file. You must be superuser or the owner of a file or directory to change its permissions.
30. **What is meant hot swapping?**

Hot swapping is the replacement or addition of components to a computer system without stopping, shutting down, or rebooting the system; hot plugging describes the addition of components only.

31. **Why ip tables are needed? * 2019**

    iptables allows the system administrator to define tables containing chains of rules for the treatment of packets. Each table is associated with a different kind of packet processing. Packets are processed by sequentially traversing the rules in chains.

32. **How administrator assign disk quota to users? * 2019**

---

33. **What is DHCP?**

    The dynamic host configuration protocol (DHCP) is the application responsible for requesting and offering IP addresses. A DHCP client automatically requests an IP address from a DHCP server when a network is detected. A DHCP server typically runs in a router and offers IP addresses to DHCP clients.

34. **What are integrated multiple operating system?**

    MULTOS (which stands for "Multiple Operating System") is an operating system that allows multiple application program s to be installed and to reside separately and securely on a smart card . ... These keys prevent unauthorized applications from being loaded into a card or deleted without the issuer's permission.

    Example: MS DOS

35. **Give the difference between LILO and GRUB?**

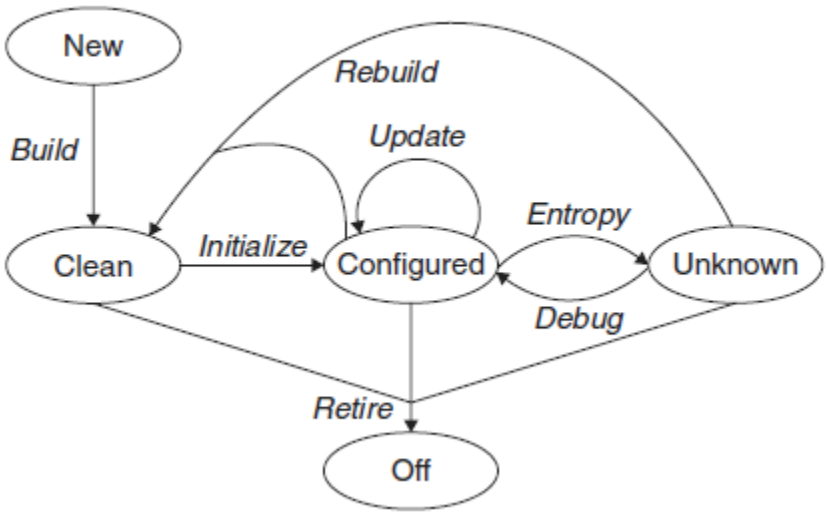
    LILO is a boot manager that allows you to boot multiple operating systems, provided each system exists on its own partition. In addition to booting multiple operating systems with LILO, you can choose various kernel configurations or versions to boot.

    Most modern Linux distributions use **GRUB** as the default boot loader during installation, including Fedora, Red Hat Enterprise Linux (RHEL), openSUSE, Debian, Mandrake, CentOS, Ubuntu, and a host of other Linux distributions. GRUB aims to be compliant with the Multiboot Specification and offers many features.

36. **What is linux shell?**

The shell is the Linux command line interpreter. It provides an interface between the user and the kernel and executes programs called commands. ... The shell can also execute other programs such as applications, scripts, and user programs (e.g., written in c or the shell programming language).

37. **Draw Evard's life cycle of machine and its OS?**



38. **Define SNMP?**

SNMP stands for Simple Network Monitoring Protocol. Nobody is sure whether the simple refers to networks or to protocol.

39. **What is KVM switches?**

A KVM switch is a device that lets many machines share a single keyboard, video screen, and mouse (KVM). For example, you might be able to fit three servers and three consoles into a single rack. However, with a KVM switch, you need only a single keyboard, monitor, and mouse for the rack.

40. **What are three time saving policies?**

Three Time-Saving Policies

- How do people get help?
- What is the scope of responsibility of the SA team?
- What's our definition of emergency?

41. **What are the difference between local and universal groups?**

Domain local groups are the direct descendants of Windows NT groups; the membership of these groups is only available from domain controllers of the domains in which they are created.

Universal group membership is available both from the domain controllers of the domains in which they are created in and from all Global Catalogs in the forest.

42. **What is fragmentation?**
    Fragmentation most generally means the process of fragmenting—breaking into pieces or being divided into parts. It can also refer to the state or result of being broken up or having been divided.

---

43. **Define sticky bit?**
    Programs can be tagged with what's called a SetUID bit (also called a sticky bit), which allows a program to be run with permissions from the program's owner, not the user who is running it. Using ls as an example.
44. **Define mask? How many type of Umask are there?**
    Umask, or the user file-creation mode, is a Linux command that is used to assign the default file permission sets for newly created folders and files. The term mask references the grouping of the permission bits, each of which defines how its corresponding permission is set for newly created files
45. **How does booting differ from shutting down?**
    Restart is the process of shutting down or powering off the computer temporarily and starting it again. It is necessary for tasks such as installing updates and installing new software to the computer. Restarting helps to confirm that the updates have installed correctly. Furthermore, it ensures that the software works as required.
    Shut down is the process of closing all the programs on the computer and turning off the computer's power. The last program to close is the operating system. It is essential to shut down the computer properly to avoid data corruption.
46. **If you want to check out the health of OS write down process in linux?**
    Step 1: Check for Swapping or Paging. ...
    Step 2: Check for Run Queue Greater than 1. ...
    Step 3: Check for Long Running Tasks with High CPU Usage. ...
    Step 4: Check for Excessive Physical Disk Input and Output. ...
    Step 5: Check for Excessive Spawning of Short Lived Processes.

Step 6: Check/Clean the Cooling Fans and Heatsinks

47. **What is yum?**

    Yum is one of the more popular packaging/updating tools for managing software on Linux systems. It is basically a wrapper program for RPM, with great enhancements.

48. **What are shadow copies?**

    Shadow Copy is a technology included in Microsoft Windows that can create backup copies or snapshots of computer files or volumes, even when they are in use. It is implemented as a Windows service called the Volume Shadow Copy service.

49. **What is port forwarding?**

    In computer networking, port forwarding or port mapping is an application of network address translation that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

    The complete syntax for the port-forwarding command is

    ```
    ssh -L local_port:destination_host:destination_port ssh_server
    ```

50. **What is the process of block facebook.com domain?**

    Locate your Windows hosts file, at
    C:\WINDOWS\system32\drivers\etc\hosts
    Open this file in your favorite text editor, Notepad works fine
    Add the following lines to the hosts file:
    127.0.0.1 facebook.com
    127.0.0.1 login.facebook.com
    127.0.0.1 www.facebook.com
    Reboot your Windows PC and try to access Facebook, it should be blocked.

51. **How to allow SSH access to specific MAC?**

    - Open the Apple menu in the upper left corner of the screen, and select "System Preferences...".
    - Under "Internet & Wireless", select "Sharing".
    - In the left column of services, enable "Remote Login".

- Highlight the "Remote Login" service and enable access for the users you would like to have SSH access.
- You can select all users, or specific users by selecting "Only these users:" and adding the appropriate users by clicking "+".
- Take note of the command displayed underneath the words "Remote Login: On" in the upper middle part of the screen.
- Write this command down as you will need it to log in from a different system.
- If your firewall is enabled (which it is by default), you may need to restart the firewall to allow SSH communications to pass through port 22.
- Open "System Prefrences", click "Security", and restart the Firewall.
- Test that the firewall is not blocking SSH access by going to a different system and entering the ssh login command in step 6 above.
- If you cannot login, restart the firewall or reboot.

52. Explain touch command?

We use the touch command to create an empty file called foo.txt in the user yyang's home directory:

```
[yyang@server ~]$ touch foo.txt
```

53. Write down the benefit of linux over window?

6 Reasons Why Linux is Better than Windows For Servers

- Free and Open Source. Linux or GNU/Linux (if you like) is free and open source; you can see the source code used to create Linux (kernel). ...
- Stability and Reliability. ...
- Security. ...
- Flexibility. ...
- Hardware Support. ...
- Total Cost of Ownership (TCO) and Maintenance.

54. What are command to combine two or more file in another file?

Type the cat command followed by the file or files you want to add to the end of an existing file. Then, type two output redirection symbols (>>) followed by the name of the existing file you want to add to.

55. Write down the command to copy file and remove directory?

The cp command is used to copy files.

To remove a directory called mydir, you'd type this:

```
[yyang@server ~]$ rmdir mydir
```

56. **How to reset system services?**
    - Open the command line.
    - Enter ls /etc/init.d or ls /etc/rc.d/
    - Find the name of the service you want to restart.
    - Enter sudo systemctl restart service where service is the service name.
    - Enter your password.

57. **Define user and its types?**

    Under Linux, every file and program must be owned by a user. Each user has a unique identifier called a user ID (UID). Each user must also belong to at least one group, a collection of users established by the system administrator.

    - Normal User
    - Root User or Super User

58. **What is rpm?**

    RPM stands for Red Hat Package Manager. It was developed by Red Hat and is primarily used on Red Hat-based Linux operating systems (Fedora, CentOS, RHEL, etc.). An RPM package uses the . rpm extension and is a bundle (a collection) of different files.

LONG QUESTIONS

Q1. Define Disaster and risk analysis? Also Explain data integrity in details? * 2019

Disaster

A disaster is a catastrophic event that causes a massive outage affecting an entire building or site. A disaster can be anything from a natural disaster, such as an earthquake, to the more common problem of stray backhoes cutting your cables by accident. A disaster is anything that has a significant impact on your company's ability to do business.

Risk Analysis

A risk analysis involves determining what disasters the company is at risk of experiencing and what the chances are of those disasters occurring. The analyst determines the likely cost to the company if a disaster of each type occurred. The company then uses this information to decide approximately how much money is reasonable to spend on trying to mitigate the effects of each type of disaster.

Data Integrity

Data integrity means ensuring that data is not altered by external sources. Data can be corrupted maliciously by viruses or individuals. It can also be corrupted inadvertently by individuals, bugs in programs, and undetected hardware malfunctions. For important data, consider ways to ensure integrity as part of day-to-day operations or the backup or archival process.

For example

Data that should not change can be checked against a read-only checksum of the data. Databases that should experience small changes or should have only data added should be checked for unexpectedly large changes or deletions.

Examples include source code control systems and databases of gene sequences. Exploit your knowledge of the data on your systems to automate integrity checking.

Disaster planning also involves ensuring that a complete and correct copy of the corporate data can be produced and restored to the systems. For

disaster recovery, it must be a recent, coherent copy of the data with all databases in sync. Data integrity meshes well with disaster recovery.

Industrial espionage and theft of intellectual property are not uncommon, and a company may find itself needing to fight for its intellectual property rights in a court of law. The ability to accurately restore data as it existed on a certain date can also be used to prove ownership of intellectual property. To be used as evidence, the date of the information retrieved must be accurately known, and the data must be in a consistent state. For both disaster-recovery purposes and use of the data as evidence in a court, the SAs need to know that the data has not been tampered with. It is important to make sure that the implementers put in place the data integrity mechanisms that the system designers recommend. It is inadvisable to wait for corruption to occur before recognizing the value of these systems.

Q2. What is network management? What are different types of firewall? Give commands for filtering? Also specify the filtering features? * 2018 * 2019

Network Management:

Network management is the process of administering and managing computer networks. Services provided by this discipline include fault analysis, performance management, provisioning of networks and maintaining quality of service.

Firewall:

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Different Types of Firewall: https://www.javatpoint.com/types-of-firewall

There are four types of firewalls, which are all available on Linux platforms. These are, in order of complexity and features, packet filtering, application proxies, stateful inspection, and hybrid.

Packet Filtering: These are the first generation of firewalls, generally what you see on modern routers these days. While useful, they are generally

trivial to circumvent an attacker using a number of common attack methods.

Application Proxies: This is the second generation of firewall technology, although it could be said this is actually the first in some ways. An application layer firewall is a proxy server, like the HTTP proxy server, Squid, for example. They also provide a layer of granularity into security policy that you won't find in stateful inspection or packet filtering firewalls.

Basically, an application proxy is an application that runs on your firewall or gateway that relays traffic between you and your destination. The added advantage here is that the traffic is being sent/received between both endpoints by a third-party application, meaning you can enforce very specific guidelines on the way the traffic is crafted between both points.

Stateful Inspection: This would be the third generation of firewall technology, this is related to the packet filtering method, but it extends the capabilities of firewalling by continuing to inspect the packets as they pass through the firewall. Net filter/iptables is a stateful inspection type firewall.

- Net filter/iptables' main features are
- stateful packet filtering (connection tracking)
- all kinds of network address translation
- flexible and extensible infrastructure
- large number of additional features as patches

Hybrids: Hybrids are the fourth generation. They are a combination of the previous three, giving the users more control of the methods they intend to employ to carry out their firewall policy.

Filtering Commands

`iptables -t table -A chain rule-spec [ options ]`	Append ***rule-spec*** to ***chain***.
`iptables -t table -D chain rule-spec`	Delete ***rule-spec*** from ***chain***.
`iptables -t table -I chain [ rulenum ] rule-spec [ options ]`	Insert ***rule-spec*** at ***rulenum***. If no rule number is specified, the rule is inserted at the top of the ***chain***.
`iptables -t table -R chain rulenum rule-spec [ options ]`	Replace ***rulenum*** with ***rule-spec*** on ***chain***.

`iptables -t table -L chain [ options ]`	List the rules on ***chain***.
`iptables -t table -F chain [ options ]`	Flush (remove all) the rules on ***chain***.
`iptables -t table -Z chain [ options ]`	Zero all the counters on ***chain***.
`iptables -t table -N chain`	Define a new chain called ***chain***.
`iptables -t table -X [ chain ]`	Delete ***chain***. If no chain is specified, all nonstandard chains are deleted.
`iptables -t table target -P chain`	Define the default policy for a chain. If no rules are matched for a given chain, the default policy sends the packet to target.
`iptables -t table -E chain [new-chain]`	Rename ***chain*** to ***new-chain***.

Q3. Elaborate comparative analysis among operating systems, windows 2008, windows server 2008 and Red hat Linux? * 2019

Microsoft Windows Server:

Pros:

- "I would say Microsoft operating systems are more stable correctly than they were before, they have made some improvements over the years."
- "The most valuable features are the file transfer protocol (FTP) and the secure file transfer protocol (SFTP)."
- "I like that Windows Server is easy to use."
- "It is very useful, and it is easy to use."
- "The installation of the solution is becoming easier every year after new releases. The first installation can take an hour but you can use templates to make the installation very quick."
- "I'm using all the features within it and find them all quite helpful."
- "Windows Server is easy to use. It's user friendly for the admin guys."

- "The solution is stable. The performance has been great over the years."

Cons

- "The solution would be better by implementing more security and integration."
- "The security could be improved."
- "It would be better if they improved the user interface."
- "The solution could have better security features."
- "Windows Server could be more secure."
- "The solution could improve by having more integration and some of the new features that are being released in Windows 11."
- "Windows Server could improve by having a faster browser, IE is too slow. There are better alternatives, such as Chrome."
- "Better integration with more platforms would be useful."

Red Hat Linux:

Pros:

- "This is a very robust product that doesn't require a lot of handling. It just works."
- "Its security is the most valuable. It is very stable and has many features. It also has good performance.
- "The feature that I like the most is that we can integrate it easily with our existing infrastructure.
- "It is a well-established operating system. We have tried to implement almost every feature of a version in our environment, and it has been very reliable.
- "The best system I've ever used is Red Hat, in terms of its ability and consistency of the operating system.
- "Its scalability and ease of setup and configuration are most valuable. When we have a hardware failure, we just save the configuration files, and in about half an hour, we have another server running with the same configuration. It is really easy to replace servers. This is the best feature."

- "The integrated solution approach reduces our TCO tremendously because we are able to focus on innovation instead of operations."
- "The most valuable features are the specification and technical guides, they are most important the security."

Cons

- "There should be the ability to add other databases to be installed and configured instead of going to other virtual machines. They should be better integrated so they are all in one place."
- "Right now what is needed on the server-side is an easier release process. Every year or every third year they are releasing a newer version and it could go smoother."
- "Sometimes we face some overload on the server."
- "We are finding some of the configurations inside the group policy not very straightforward. We had some difficulties."
- "The system needs to offer better integration capabilities."
- "The security could be improved."
- "The cost to use the solution is quite high."
- "The Active Directory synchronization on Azure."

Q4. Write Configuration steps for establishing Samba server and LYNC? * 2018

The Common Internet File System (CIFS) is such a protocol, and it is offered by the Linux Samba server. below we'll discuss how to set up a Samba server to offer file shares.

Samba is a very versatile service that you can use for different purposes on your network. Apart from sharing fi les, it can share printers and also offer Windows domain services such as directory services. You can even integrate Samba into an Active Directory domain and make it a member server of Active Directory. This means that all users in Active Directory get easy access to the resources you offer on the Samba server. The most popular use of Samba, however, is as a file server.

1.Setting Up a Samba File Server

Setting up a Samba fi le server is fairly straightforward. To set one up, you need to do the following:

- Create a directory on the Linux file system on the Samba server.
- If needed, create Linux users and give the appropriate permissions to the directory you just created.
- Install the Samba server.
- Define the share in /etc/samba/smb.conf.
- Create a Samba user account that has access to the share.
- (Re)start the Samba service.
- Tell SELinux to give access to the Samba share.

A few of the previous steps require further explanation. Let's start with the user account. There are different ways to offer user access on Samba. To set up a basic Samba server, you'll need both a Linux user and a Samba user. The Linux user is used for Linux permissions on the local Linux file system. A Windows user cannot authenticate with the credentials of a Linux user, however. This is why you'll also need a Samba user with the same name as the Linux user. Typically, the Windows user needs to work only with the Samba user, which also means that only the password of the Samba user is relevant. The Linux user is for local Linux access only.

To define the Samba share, you'll put it in Samba's main configuration file, which is /etc/samba/smb.conf. The basic share definition is very simple: it gives a name to the share, and it tells Samba what to share. A minimum share definition might appear as follows:

[myshare]

path=/mysharedfolder

When defining a share, you can also use many options to defi ne to whom and with which access permissions the share should be available. It could, for example, appear as follows:

[myshare]

path = /mydatafiles

comment = some shared files

allow hosts = 192.168.1.

writable = yes

public = yes

write list = +mygroup

2.Samba and SELinux

You've just created a Samba share, but for now it won't work. This is because you must apply some SELinux settings before being able to use Samba on Red Hat. Apart from some Booleans, which you can use, the most important change required is that you set the directories that you want to share with Samba to the samba_share_t context type. If you want to grant access to a Samba shared directory to other fi le-sharing services, you can also set the context type to public_content_t.

To set the appropriate Samba context type, use the following two commands:

semanage fcontext -a -t samba_share_t "/sambashare(/.*)?"

restorecon -R -v /sambashare

After making these changes, the Samba share should now be accessible.

3.Samba Advanced Authentication Options

When working with Samba, you can use different security options. This option is set in the [global] section of the /etc/samba/smb.conf file, and it determines where Samba looks for user authentication information. The default setting is security = user, which means that Samba needs a local Samba user account that is stored in a smbpasswd file.

The following authentication options are availabl:

security = share: When using this option, a user does not need to send a username and password to a share before connecting to it. You can set it up so that a user has to enter a password before connecting.

security = user: This is the default security option, where a user must log in to the share before getting access.

security = domain: This option works if your Samba server has been added to a Windows domain.

security = server: This option uses an external server (such as another Samba server) to handle Samba authentication requests.

security = ads: This option makes Samba a member in a Windows Active Directory domain.

4.Accessing Samba Shares

After setting up the Samba server, you'll need to access it. From Windows, you can set up a network share and point to the Samba server.

There are also some tools that you can use to access Samba shares on Linux. First you can use graphical tools, such as Nautilus, to connect to a Samba share. To list the Samba shares that are offered by a specifi c server, you can use smbclient -L. This shows the names of all shares that are offered, and it also provides an option to log into the Samba server.

Q5. Write a detail note of Network Management Services and Network monitoring tools?

1.What Are Network Management Services?

Network management involves the monitoring and maintenance of a business's information technology. You can have an in-house network management team or hire the services of network management providers. Vendors of network management services provide a wide range of services:

- implementing upgrades
- monthly status reporting
- user administration
- network maintenance

All this helps you assess the network's performance and optimize operations.

Also, a variety of tools and software solutions are available for network monitoring. Data from such software help you streamline network operations, repair reported issues, and manage network devices continuously. The aim is to reduce network infrastructure downtime and keep devices functioning correctly.

Network management services include providing solutions to different components of the network. Below are some examples.

Network administration: This covers tracking of network resources, such as switches, servers, and routers. Software updates and performance monitoring are also part of network administration.

Network maintenance: This includes fixes and upgrades to network resources. Remediation activities and proactive measures are executed here. They may include replacing switches, routers, or other network gears.

Network operation: This ensures the smooth running of the network. The network manager closely monitors activities to identify and fix issues as they happen.

Network provisioning: Often, you'll need to configure network resources to support the requirements of specific services. Network provisioning lets you do that. For instance, you can increase bandwidth requirements to accommodate more users.

Benefits of Network Management Services

- Keeping Your Data Safe at All Times
- Identifying Security Threats and Enhancing Network Security
- Saving Money
- Having a Proactively Managed Network

2.Network Monitoring Tools

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages or other trouble. Network monitoring is part of network management.

Q6. Explain in detail the advanced file system Management in red hat Linux?

File System Management Tasks

Essentially, everything on your RHEL server is stored in a text or ASCII file. Therefore, working with files is a very important task when administering Linux. Below, we'll discuss about file system management.

1.Working with Directories

Since fi les are normally organized within directories, it is important that you know how to handle these directories. This involves a few commands.

cd Use this command to change the current working directory. When using cd, make sure to use proper syntax. First, names of commands and directories are case-sensitive; therefore, /bin is not the same as /BIN. Next, you should be aware that Linux uses a forward slash instead of a backslash. So, use cd /bin and not cd \bin to change the current directory to /bin.

pwd The pwd command stands for Print Working Directory. You can often see your current directory from the command line, but not always. If the latter is the case, pwd offers help.

mkdir If you need to create a new directory, use mkdir. With Linux mkdir, it is possible to create a complete directory structure in one command using the -p option, something that you cannot do on other operating systems.

rmdir The rmdir command is used to remove directories. Be aware, however, that it is not the most useful command available, because it will work only on directories that are already empty.

2.Working with Files

Using ls to List Files

To manage files on your server, you must first know what files are available. For this purpose, the ls command is used. If you just use **ls** to show the contents of a given directory, it will display a list of files. These files, however, also have properties.

ls has many other options as well. One useful option is **-d**. The example that follows shows clearly why this option is so useful. Wildcards can be used when working with the **ls** command. For example, **ls *** will show a list of all files in the current directory, **ls /etc/*a.*** will show a list of all files in the directory **/etc** that have an a followed by **a. (dot)** somewhere in the file

name, and **ls [abc]*** will show a list of all files where the name starts with either a, b, or c in the current directory. Now without the option **–d**, something strange will happen. If a directory matches the wildcard pattern, the entire contents of that directory are displayed as well. This isn't very useful, and for that reason, the **-d** option should always be used with the **ls** command when using wildcards.

When displaying files using **ls**, note that some files are created as hidden files. These are files where the name starts with a dot. By default, hidden files are not shown. To display hidden files, use the **ls -a** command.

Removing Files with rm

Cleaning up the file system is a task that also needs to be performed on a regular basis. The **rm** command is used for this purpose. For example, use **rm /tmp/somefile** to remove **somefile** from the **/tmp** directory. If you are at the root and have all the proper permissions for this file (or if you are the root), you will succeed without any problem. Since removing files can be delicate (imagine removing the wrong files), the shell will ask your permission by default. Therefore, it may be necessary to push the rm command a little. You can do this by using the **-f (force)** switch. For example, use rm **-f somefile** if the command states that some file cannot be removed for some reason.

The **rm** command can also be used to wipe entire directory structures. In this case, the **-r** option has to be used. When this option is combined with the **-f** option, the command becomes very powerful. For example, use **rm -rf /somedir/*** to clear out the entire contents of **/somedir.**

Copying Files with cp

If you need to copy files from one location on the file system to another location, use the **cp** command. This straightforward command is easy to use. For example, use **cp ~/* /tmp** to copy all files from your home directory (which is referred to with the ~ sign) to the directory **/tmp.** If subdirectories and their contents need to be included in the copy command, use the option **-r.** You should, however, be aware that **cp** normally does not copy hidden files where the name starts with a dot. If you need to copy hidden fi les as well, make sure to use a pattern that starts

with **a .(dot)**. For example, use **cp ~/.* /tmp** to copy all files where the name starts with a dot from your home directory to the directory **/tmp.**

Moving Files with mv

An alternative method for copying files is to move them. In this case, the file is removed from its source location and placed in the target location. For example, use **mv ~/somefile/tmp/otherfile** to move the filename somefile to **/tmp**. If a subdirectory with the name otherfile exists in **/tmp**, somefile will be created in this subdirectory. If, however, no directory with this name exists in **/tmp**, the command will save the contents of the original file somefile under its new name, otherfile, in the directory **/tmp**.

Viewing the Contents of Text Files

cat This command displays the contents of a file by dumping it to the screen.

tac This command does the same thing as cat but inverts the result; that is, not only is the name of tac the opposite of cat, but the result is the opposite as well.

tail This command shows only the last lines of a text file. If no options are used, this command will show the last 10 lines of a text file.

head This command is the opposite of tail. It displays the first lines of a text file. less The last command used to monitor the contents of text files is less.

more This command is similar to less but not as advanced.

Creating Empty Files

It is often useful to create files on a file system. This is a useful test to check to see whether a file system is writable. The touch command helps you do this. For example, use touch somefile to create a zero-byte file with the name somefile in the current directory.

Q7. How can we access the server remotely? What will be the issues in remote access?

A remote access service gives authorized individuals a way to access the company network from home, customer sites, or other locations around the

country, the continent, or the world. In the early days, it was something that weird technical people wanted so that they could do extra work from home out of normal working hours. More recently, it has become a core service that everyone in a company uses. Now telecommuters and road warriors work outside the office, connecting only for specific services.

Remote access is achieved in many ways, but there are two main categories. Some forms connect a computer directly into the network: dial-up modems, ISDN, and so on. Others connect to the Internet—WiFi, cable modems, DSL, Ethernet, and so on—and then from there somehow tunnel or VPN into your network.

The Basics

To provide a remote access service, you should start by understanding your customers' many and varied requirements. You should also decide with your customers what service levels the SAs will provide for the various aspects of the system and document those decisions for future reference.

Once you have defined the requirements and the service levels, you are ready to build the service or to not build it. One of the basics of building a remote access system is to outsource as much of it as possible. However, several components must be built or managed internally to the company. In particular, the security aspects of authentication, authorization, and maintaining perimeter security should be managed internally.

Requirements for Remote Access

The first requirement of a remote access service typically will be assumed and not explicitly stated by your customers: Everyone must have access to a lowcost, convenient remote access solution. If the SA team does not provide one, customers will build something for themselves that will not be as secure or well managed as the service that the SAs would provide. It is quite likely that the SAs will ultimately be expected to support the service that their customers have built when it develops problems. It typically also will be more difficult to support than an SA-built service.

The other requirements are based on how the customers intend to use the remote access system. The most common customers of remote access are people who are traveling and want to check or send email. Other common customers are people who want to log in for an hour or two in the evening

to catch up on a few things. These different groups of people have something in common: They use the remote access service only for fairly short periods of time. They differ in that one group expects to be able to use the service from anywhere; the other, to use it from home. The requirement that they both introduce is that they need a reliable and economical way to connect to the office network for short-duration connections.

Policy for Remote Access

Before starting to provide a remote access service, the company must define a policy for remote access. The policy should define acceptable use of the service, the security policies surrounding the service, and the responsibilities attached to having access to the service. The policy should also state who gets what kind of remote access and who pays for it.

Issues in Remote access

Remote access, however, is not a perfect solution. Let's look at some of the top challenges faced by users of remote access:

Connection quality. If the user has a poor internet connection or a weak Wi-Fi signal, both of which are common at hotels or public hotspots for example, then the remote desktop connection will also be slow. Accessing applications or files becomes cumbersome.

VPNs. VPNs, or virtual private networks, are very sensitive. Many public internet connections will not allow users to work at all, making remote connection almost impossible.

Performance. There are many low-cost methods available, that simply do not have the speed necessary for accomplishing work. The delays inherent in these solutions mean they are only viable options for quick tasks or small amounts of work. In addition, they may not allow for local file and printer access.

Security. Public hotspots are common at coffee shops, airports, hotels, and even public parks. While they are convenient, they are also highly susceptible to hackers who would be able to access any of the data you're working on while using the shared Wi-Fi.

Application availability. Systems like Citrix and Terminal Server only allow access to certain programs that have been configured by the IT administrator. Often times, users need access to applications they installed themselves, special plugins, configurations, or files from their desktop, or other resources that are not on the remote access server.

Open applications. If a user left files or applications open on their business desktop, they are locked there. It is impossible to log in to them a second time from a remote access system.

HQ must be online. In the case that a natural disaster takes down the internet or power at your business, or worse, that the server crashes, the systems are not accessible remotely or locally.

Cost. Instituting and maintaining a remote access system is expensive. It requires hardware, software, ongoing maintenance, upgrades, training, and support.

Q8. Explain scenario for picking appropriate maintenance contracts for server?

Consider Maintenance Contracts

When purchasing a server, consider how repairs will be handled. All machines eventually break.4 Vendors tend to have a variety of maintenance contract options. For example, one form of maintenance contract provides on-site service with a 4-hour response time, a 12-hour response time, or next-day options. Other options include having the customer purchase a kit of spare parts and receive replacements when a spare part gets used.

Following are some reasonable scenarios for picking appropriate maintenance contracts:

Non-critical server. Some hosts are not critical, such as a CPU server that is one of many. In that situation, a maintenance contract with next-day or 2-day response time is reasonable. Or, no contract may be needed if the default repair options are sufficient.

Large groups of similar servers. Sometimes, a site has many of the same type of machine, possibly offering different kinds of services. In this case, it may be reasonable to purchase a spares kit so that repairs can be done by local staff. The cost of the spares kit is divided over the many hosts. These hosts may now require a lower-cost maintenance contract that simply replaces parts from the spares kit.

Controlled introduction. Technology improves over time, and sites described in the previous paragraph eventually need to upgrade to newer models, which may be out of scope for the spares kit. In this case, you might standardize for a set amount of time on a particular model or set of models that share a spares kit. At the end of the period, you might approve a new model and purchase the appropriate spares kit.

Critical host. Sometimes, it is too expensive to have a fully stocked spares kit. It may be reasonable to stock spares for parts that commonly fail and otherwise pay for a maintenance contract with same-day response. Hard drives and power supplies commonly fail and are often interchangeable among a number of products.

Large variety of models from same vendor. A very large site may adopt a maintenance contract that includes having an on-site technician. This option is usually justified only at a site that has an extremely large number of servers, or sites where that vendor's servers play a keen role related to revenue. However, medium-size sites can sometimes negotiate to have the regional spares kit stored on their site, with the benefit that the technician is more likely to hang out near your building. An SA can ensure that the technician will spend all his or her spare time at your site by providing a minor amount of office space and use of a telephone as a base of operations. In exchange, a discount on maintenance contract fees can sometimes be negotiated.

Highly critical host. Some vendors offer a maintenance contract that provides an on-site technician and a duplicate machine ready to be swapped into place. This is often as expensive as paying for a redundant server but may make sense for some companies that are not highly technical.

Q9. Give the configuration of Apache server in Linux?

Configuring the Apache Web Server:

Apache is one of the most used services on Red Hat Enterprise Linux. A basic installation of an Apache website is easy to perform, but by using

modules you can make Apache as sophisticated as you need. Below, we'll discuss how to set up a basic Apache web server, which offers access to a simple website.

1.Creating a Basic Website

Configuring an Apache server that services just one website is not hard to do—you just have to install the Apache software and create some content in the Apache document root. The default document root is set to /var/www/html on a Red Hat Enterprise Linux server. Just put a file in this directory with the name index.html, and it will be served by your Apache server.

Creating a Basic Website

Below, we'll learn how to configure Apache to serve a basic website.

1. Use **yum -y install httpd** to install the Apache web server.

2. Use **chkconfig httpd** on to put the Apache web server in your server's run levels, and have it star t at boot in your run levels.

3.Open a root shell, and go to the directory /var/www/html. In this directory, create a file with the name index.html. In this file, put the content "welcome to my website" and then use **service httpd start** to start the Apache web server.

4. Still from the root shell, use **elinks http://localhost** to access the website you just created. You'll notice that your web server is up and running!

2.Understanding the Apache Configuration Files

It's easy to set up a basic Apache web server, as long as you can retain all of the default settings. To be able to configure the web server in more complex scenarios, we'll need to understand how the Apache configuration files are organized.

Everything related to the configuration of your Apache server is in the /etc/httpd directory. In this directory, you'll find two subdirectories: **conf and conf.d**. In **/etc/httpd /confd**, you'll find the main Apache configuration fi le **httpd.conf**. From the **httpd.conf** file, many configuration files are included, and by default, they are **in /etc/httpd/conf.d**. This **httpd.conf** file is designed to contain the entire Apache configuration. However, because Apache can take advantage of many additional features, parts of the configuration are stored in additional configuration fi les in Red Hat Enterprise Linux. To understand how these additional configuration fi les are organized, you need to appreciate that Apache is modular. Installing additional modules can extend the functionality of the **httpd process**.

Apache Mode

Apache can be star ted in two different modes: the prefork mode and the worker mode. The prefork mode is the default mode. In this mode, a master httpd process is started, Configuring the Apache Web Server 391 and this master process will start different httpd servers. As an alternative, the worker mode can be used. In this mode, one httpd process is active, and it uses different threads to serve client requests. Even if the worker mode is a bit more efficient with regard to resource usage, some modules cannot handle it, and therefore the prefork mode is used as default.
To change the default mode that Apache uses, you can modify the HTTPD parameter in **/etc/sysconfig/httpd**. To use the worker mode, you have to start the **/usr/sbin/httpd.** worker binary instead of **/usr/sbin/httpd.**

Modules

Among the features that make the Apache web server attractive is the fact that it is modular. By including modules, functionality can be added to Apache. To include Apache modules, they first need to be installed. By default, some of the most common modules are installed to the /etc/httpd/modules directory. To tell Apache that it should load a specific module, you need to use the Load Module directive. By default, this directive is used to include many modules.
If a module is loaded, it can also have a specific configuration. There are three ways to load additional configurations for modules:

- Use the IfModule directive in httpd.conf.
- Put it in an include file.
- If a module is common, its parameters can be entered in httpd.conf without further specification.

Setting Directory Options

The administrator can also set different directory options on an Apache web server. These options are used to define how the contents of a directory on the httpd server should be presented to users who access that directory. The default behavior is that the httpd processes look in the document root to see whether there is a fi le whose name starts with index. The DirectoryIndex directive can be used to specify that other fi les should also be considered. If this is the case, it will show the contents of this fi le, and if not, a list of files in the directory is shown.
To modify this behavior, the DirectoryIndex and Options directives can be used.

3.Apache Log Files

To help you troubleshoot Apache issues, two log files are used by default. You can find these files in the /var/log/httpd directory. The access_log file contains information about users who have accessed your server. Note that it can grow very fast on busy web servers! The error_log file has error messages that can be useful in troubleshooting your Apache web server.

4.Apache and SELinux

As an administrator, SELinux can often be an annoyance. This is because it defines in a very strict way what is allowed and what isn't allowed. Moreover, if anything happens that isn't allowed specifically in the policy, SELinux will deny it. To make sure that Apache runs smoothly with SELinux, there are a few things that need to be addressed. First you'll need to make sure that the appropriate context types have been applied. Typically, these are httpd_sys_content_t on directories where Apache can access documents, and httpd_sys_script_exec_t on directories from where Apache needs to run scripts.

5.Getting Help

The number of options that Apache offers can be overwhelming for a new user. Fortunately, there is excellent documentation available in the httpd-manual package. Every task an Apache administrator will ever undertake is documented in the online documentation that is available on your web server after installing the httpd-manual package.

Q10. How the Linux file system works?

1.Linux File System

A Linux file system is a structured collection of files on a disk drive or a partition. A partition is a segment of memory and contains some specific data. In our machine, there can be various partitions of the memory. Generally, every partition contains a file system.

The general-purpose computer system needs to store data systematically so that we can easily access the files in less time. It stores the data on hard disks (HDD) or some equivalent storage type. There may be below reasons for maintaining the file system:

- Primarily the computer saves data to the RAM storage; it may lose the data if it gets turned off. However, there is non-volatile RAM (Flash RAM and SSD) that is available to maintain the data after the power interruption.

- Data storage is preferred on hard drives as compared to standard RAM as RAM costs more than disk space. The hard disks costs are dropping gradually comparatively the RAM.

The Linux file system contains the following sections:

- The root directory (/)
- A specific data storage format (EXT3, EXT4, BTRFS, XFS and so on)
- A partition or logical volume having a particular file system.

What is the Linux File System?

Linux file system is generally a built-in layer of a Linux operating system used to handle the data management of the storage. It helps to arrange the file on the disk storage. It manages the file name, file size, creation date, and much more information about a file.

2.Linux File System Structure

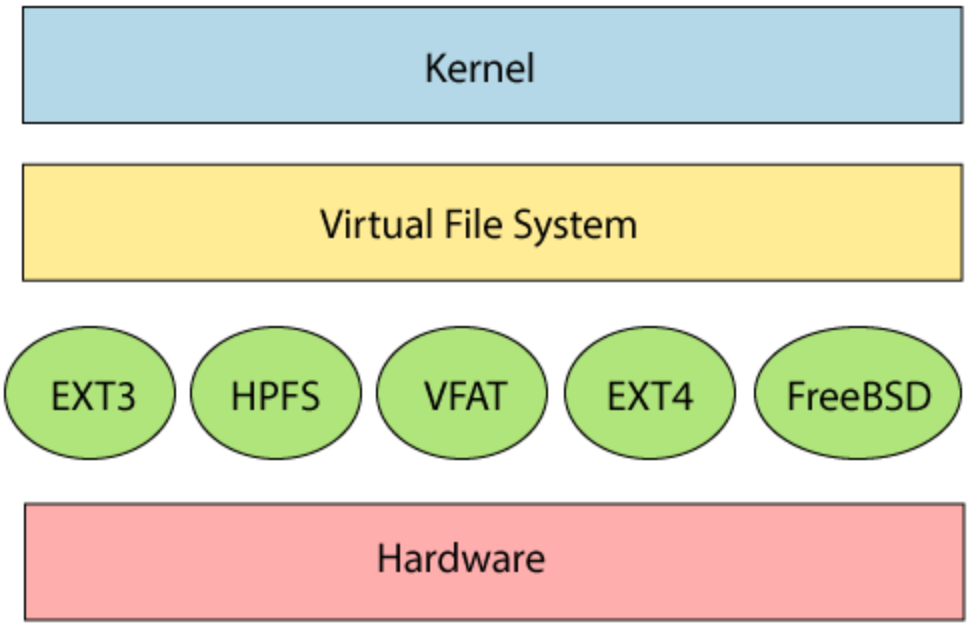
Linux file system has a hierarchal file structure as it contains a root directory and its subdirectories. All other directories can be accessed from the root directory. A partition usually has only one file system, but it may have more than one file system.

A file system is designed in a way so that it can manage and provide space for non-volatile storage data. All file systems required a namespace that is a naming and organizational methodology. The namespace defines the naming process, length of the file name, or a subset of characters that can be used for the file name. It also defines the logical structure of files on a memory segment, such as the use of directories for organizing the specific files. Once a namespace is described, a Metadata description must be defined for that particular file.

The data structure needs to support a hierarchical directory structure; this structure is used to describe the available and used disk space for a particular block. It also has the other details about the files such as file size, date & time of creation, update, and last modified.

Also, it stores advanced information about the section of the disk, such as partitions and volumes. The advanced data and the structures that it represents contain the information about the file system stored on the drive; it is distinct and independent of the file system metadata.

Linux file system contains two-part file system software implementation architecture. Consider the below image:



3.Linux File System Features

In Linux, the file system creates a tree structure. All the files are arranged as a tree and its branches. The topmost directory called the **root (/) directory**. All other directories in Linux can be accessed from the root directory.
Some key features of Linux file system are as following:
Specifying paths: Linux does not use the backslash (\) to separate the components; it uses forward slash (/) as an alternative. For example, as in Windows, the data may be stored in C:\ My Documents\ Work, whereas, in Linux, it would be stored in /home/ My Document/ Work.
Partition, Directories, and Drives: Linux does not use drive letters to organize the drive as Windows does. In Linux, we cannot tell whether we are addressing a partition, a network device, or an "ordinary" directory and a Drive.
Case Sensitivity: Linux file system is case sensitive. It distinguishes between lowercase and uppercase file names. Such as, there is a difference between test.txt and Test.txt in Linux. This rule is also applied for directories and Linux commands.
File Extensions: In Linux, a file may have the extension '.txt,' but it is not necessary that a file should have a file extension. While working with Shell, it creates some problems for the beginners to differentiate between files and directories. If we use the graphical file manager, it symbolizes the files and folders.

Hidden files: Linux distinguishes between standard files and hidden files, mostly the configuration files are hidden in Linux OS. Usually, we don't need to access or read the hidden files. The hidden files in Linux are represented by a dot (.) before the file name (e.g., .ignore). To access the files, we need to change the view in the file manager or need to use a specific command in the shell.

4.Types of Linux File System

When we install the Linux operating system, Linux offers many file systems such as **Ext, Ext2, Ext3, Ext4, JFS, ReiserFS, XFS, btrfs,** and **swap**.

1. Ext, Ext2, Ext3 and Ext4 file system

The file system Ext stands for **Extended File System**. It was primarily developed for **MINIX OS**. The Ext file system is an older version, and is no longer used due to some limitations.

Ext2 is the first Linux file system that allows managing two terabytes of data. **Ext3** is developed through Ext2; it is an upgraded version of Ext2 and contains backward compatibility.

Ext4 file system is the faster file system among all the Ext file systems. It is a very compatible option for the SSD (solid-state drive) disks, and it is the default file system in Linux distribution.

2. JFS File System

JFS stands for **Journaled File System**, and it is developed by **IBM for AIX Unix**. It is an alternative to the Ext file system. It can also be used in place of Ext4, where stability is needed with few resources. It is a handy file system when CPU power is limited.

3. ReiserFS File System

ReiserFS is an alternative to the Ext3 file system. It has improved performance and advanced features. In the earlier time, the ReiserFS was used as the default file system in SUSE Linux, but later it has changed some policies, so SUSE returned to Ext3. This file system dynamically supports the file extension, but it has some drawbacks in performance.

4. XFS File System

XFS file system was considered as high-speed JFS, which is developed for parallel I/O processing. NASA still using this file system with its high storage server (300+ Terabyte server).

5. Btrfs File System

Btrfs stands for the **B tree file system**. It is used for fault tolerance, repair system, fun administration, extensive storage configuration, and more. It is not a good suit for the production system.

6. Swap File System

The swap file system is used for memory paging in Linux operating system during the system hibernation. A system that never goes in hibernate state is required to have swap space equal to its RAM size.

Q11. Write different steps of configuring DNS?

Understanding DNS

Domain Name System (DNS) is the system that associates hostnames with IP addresses. Thanks to DNS, users and administrators don't have to remember the IP addresses of computers to which they want to connect but can do so just by entering a name, such as www. example.com.

Setting Up a DNS Server

The Berkeley Internet Name Domain (BIND) service is used to offer DNS services on Red Hat Enterprise Linux. Below, we'll learn how to set it up. First we'll read how to set up a cache-only name server. Next we'll learn how to set up a primary name server for your own zone. Then we'll learn how to set up a secondary name server and have it synchronize with the primary name server.

1.Setting Up a Cache-Only Name Server

Running a cache-only name server can be useful when optimizing DNS requests in your network. If you run a BIND service on your server, it will do the recursion on behalf of all clients. Once the resource record is found, it is stored in cache on the cache-only name server. This means that the next time a client needs the same information, it can be provided much faster. Configuring a cache-only name server isn't difficult. You just need to install the BIND service and make sure that it allows incoming traffic. For cache-only name servers, it also makes sense to configure a forwarder.

Configuring a Cache-Only Name Server

Below, we'll install BIND and set it up as a cache-only name server. You'll also configure a forwarder to optimize speed in the DNS traffi c on your network. To complete this, you need to have a working Internet connection on your RHEL server.

1. Open a terminal, log in as root, and run yum -y install bind-chroot on the host computer to install the bind package.
2. With an editor, open the configuration file /etc/named.conf. You need to change some parameters in the configuration file to have BIND offer its services to external hosts.
3. Change the fi le to include the following parameters: listen-on port 53 { any; }; and allow-query { any; };. This opens your DNS server to accept queries on any network inter face from any client.
4. Still in /etc/named.conf, change the parameter dnssec-validation; to dnsserver- validation no;.
5. Finally, insert the line forwarders x.x.x.x in the same confi guration fi le, and give it the value of the IP address of the DNS server you normally use for your Internet connection.

This ensures that the DNS server of your Internet provider is used for DNS recursion and that requests are not sent directly to the name servers of the root domain.

6. Use the service named restart command to restart the DNS server.
7. From the RHEL host, use dig redhat.com. You should get an answer, which is sent by your DNS server. You can see this in the SERVER line in the dig response. Congratulations, your cache-only name server is operational!

2.Setting Up a Primary Name Server

To set up a primary name server, you'll need to define a zone. This consists of two parts. First you'll need to tell the DNS server which zones it has to service, and next you'll need to create a configuration file for the zone in question. To tell the DNS server which zones it has to service, you need to include a few lines in **/etc/named.conf**. In these lines, you'll tell the server which zones to service and where the configuration files for that zone are stored. The first line is important. It is the directory line that tells **named.conf** in which directory on the Linux fi le system it can find its configuration. All file names to which you refer later in **named.conf** are relative to that directory. By default, it is set to **/var/named**. The second relevant part tells the named process the zones it services. On Red Hat Enterprise Linux, this is done by including another file with the name **/etc/named.rfc192.conf.**

Setting Up a Primary DNS Server

In this exercise, you'll learn how to set up a primary DNS server. You'll configure the name server for the example.com domain and then put in some resource records. At the end of the exercise, you'll check that it 's all working as expected.

1. Make sure that the bind package is installed on your host computer.
2. Open the /etc/named.conf file, and make sure the following parameters are included:
   - directory is set to /var/named
   - listen-on port 53 is set to any
   - allow-query is set to any
   - forwarders contains the IP address of your Internet provider's DNS name server
   - dns-sec validation is set to no
3. Open the /etc/named.rfc1912.zones file, and create a definition for the example.com domain.
4. Create a fi le /var/named/example.com, and give it contents similar to those in Listing
5. Make sure that the DNS resolver in /etc/resolv.conf is set to your own DNS server.
6. Use dig yourhost.example.com, and verify that your DNS server gives the correct information from your DNS database.

3.Setting Up a Secondary Name Server

A secondary server is one that synchronizes with the primary. Thus, to enable this, you must first allow the primary to transfer data. You do this by setting the allow-transfer parameter for the zone as you previously defined it in the /etc/named.rfc1912.conf file. It's also a good idea to set the notify yes parameter in the definition of the master zone. This means that the master server automatically sends an update to the slaves if something has changed. After adding these lines, the definition for the example.com zone should appear.

Creating a DNS slave configuration

```
zone "example.com" IN {
type slave;
masters {
192.168.1.220;
};
file "example.com.slave";
};
```

Q12. Give the configuration of FTP server in Linux?

Offering FTP Server Services

Samba and NFS are commonly used services designed to offer access to shared files within the same network. If you also want to share files with external users, FTP is a more suitable option. On Red Hat Enterprise Linux, vsftpd is the preferred FTP server. Deploying vsftpd to offer access to shared files is easy to do. After installing the vsftpd package, it uses its default home directory, /var/ftp. If you create a /pub subdirectory within that directory, you can start putting fi les in it that will be accessible for anonymous FTP users. Remember that FTP is clear text, so extra security precautions should be taken. To open vsftpd for authenticated users, you can change the settings in the configuration file /etc/vsftpd.conf. This is very readable configuration file, which contains many settings examples and good documentation on how to use these settings.

vsftpd Setting

anonymous_enable: Use to enable anonymous users (enabled by default).
local_enable Use to enable access for authenticated local users (enabled by default). Because it is insecure, this option should be disabled.
Set ting Description
write_enable Allows w rite access (by default only for authenticated users).
anon_upload_enable Use this if you want to allow anonymous users to upload files. (Be sure you know what you're doing if you're planning to enable this option because using it has some security risks!)
xferlog_enable Logs all FTP transfers.
chown_uploads Change the owner of uploaded files. (This parameter can be useful if you want to allow anonymous users to upload files.)

After applying the required settings to your FTP server, you'll also need to make sure it is accessible. This requires setting the appropriate firewall rules and the SELinux settings as well.

First you'll need to open the firewall. Remember that if you've made custom modifications to your firewall configuration, you shouldn't use system-

config-firewall anymore, so make sure to apply the proposed changes manually.
You'll need to load two firewall modules for FTP: **nf_conntrack_ftp** and **nf_nat_ftp**. The first allows FTP to track connections, which is an absolute requirement for opening both ports 20 and 21 on the firewall and the higher ports that are needed for active/passive connection.
The second module, **nf_nat_ftp,** is required only if you want to offer FTP services through a NAT. To load these modules at all times when the fi rewall is initialized, put the following line of code in **/etc/sysconfig/iptables_config:**
IPTABLES_MODULES=**"nf_conntrack_ftp nf_nat_ftp"**
After adding these two modules, you'll need to restart the firewall service, so use service iptables restart before continuing. Next you can open the FTP ports in the firewall. The following two commands allow you to do just that:
iptables -A INPUT -p tcp --dport 21 -j ALLOW
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ALLOW

Enabling an Anonymous FTP Server
Below, we'll learn how easy it is to set up your server for anonymous FTP access.
1. Use **yum -y install vsftpd.**
2. Use **service vsftpd start** to star t the FTP server, and use **chkconfig vsftpd on** to make sure it starts when you reboot your server.
3. Use **yum -y install lftp** to install the lftp FTP client to your computer.
4. From a console, type **lftp localhost**. This opens an anonymous FTP client interface.
From this inter face, use **ls** to see the contents of the current directory, use **cd** to change directories, and use the **get** and **put** commands to download and upload files.