Short Questions

1. **What is DHCP?**
   The Linux DHCP (Dynamic Host Configuration Protocol) client and server can assist with these tasks. The client machine is configured to obtain its IP address from the network. When the DHCP client software is started, it broadcasts a request onto the network for an IP address. If all goes well, a DHCP server on the network will respond, issuing an address and other necessary information to complete the client's network configuration.
2. **How windows and Linux trace route do differ?**
   The Unix/Linux `traceroute` command and the Microsoft Windows `tracert` commands both accomplish the task of tracing network paths, but they do it in slightly different ways.
   Both of these tools for tracing network routes send out a packet wth TTL (Time To Live) set to 1 and report it's destnation. Then, they send out a packet with TTL=2 and report it's destination. They continue until the packets reach their final destination or the TTL limit is exceeded.
   The difference is that Unix/Linux `traceroute` uses UDP (User Datagram Protocol) packets to a random high port number, while Microsoft Windows uses ICMP (Internet Control Message Protocol) packets.
3. **What is meant by authentication and authorization?**
   In simple terms, authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.
   Comparing these processes to a real-world example, when you go through security in an airport, you show your ID to authenticate your identity. Then, when you arrive at the gate, you present your boarding pass to the flight attendant, so they can authorize you to board your flight and allow access to the plane.
4. **Give the difference between LILO and GRUB?**
   The main difference between GRUB and LILO is that GRUB can be used for various operating systems, while LILO is used only for the Linux operating system. Moreover, GRUB is new while LILO is old.
5. **Discuss hot swap components?**
   Redundant components should be hot-swappable. 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. Being able to hot-swap components is like being able to change a tire while the car is driving down a highway. It's great not to have to stop to fix common problems. The first benefit of hot-swap components is that new components can be installed while the system is running. Hot-swappable components increase the cost of a system.
6. **What is Linux shell?**
   When users log into the system, they expect an environment that can help them be productive. This first program that users encounter is called a shell. If you're used to the Windows side of the world, you might equate this with command.com, Program Manager, or Windows Explorer (not to be confused with Internet Explorer, which is a web browser).
   Under UNIX/Linux, most shells are text-based. A popular default user shell in Linux is the Bourne Again Shell, or BASH for short. Linux comes with several shells from which to choose—you can see most of them listed in the /etc/shells file. Deciding which shell is right for you is kind of like choosing a favorite beer—what's right for you isn't right for everyone, but still, everyone tends to get defensive about their choice!
7. **What are 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. Now more servers can fit there. You can save even more room by having one KVM switch per row of racks or one for the entire data center. However, bigger KVM switches are often prohibitively costly. You can save even more space by using IP-KVMs, KVMs that have no keyboard, monitor, or mouse. You simply connect to the KVM console server over the network from a software client on another machine.

8. Draw Evard's Life cycle of a machine and its OS?

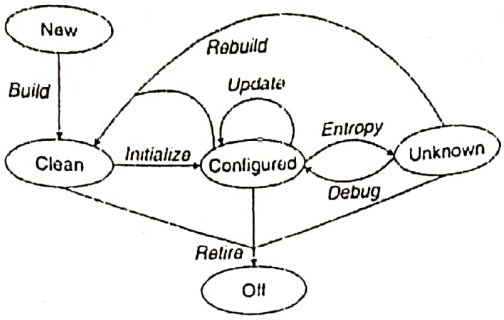


Figure 3.1 Evard's life cycle of a machine and its OS

9. Define SNMP?

SNMP stands for Simple Network Monitoring Protocol. Nobody is sure whether the simple refers to networks or to protocol. Problems with SNMP make it difficult to use on larger-than-simple networks. Although it attempted to be simple, the protocol itself is rather complex.
In SNMP's most basic form, a packet is sent to a network device, such as a router, with a question called a GET. The router replies with a packet containing the value.

10. What are three time saving policies?

Your management can put three policies in writing to help with the floor mopping.
1. How do people get help?
2. What is the scope of responsibility of the SA team?
3. What's our definition of emergency?

11. What is Fragmentation?

Moving the disk arm to a new place on the disk is extremely slow compared to reading data from the track where the arm is. Therefore, operating systems make a huge effort to store all the blocks for a given file in the same track of a disk. Since most files are read sequentially, this can result in the data's being quickly streamed off the disk. However, as a disk fills, it can become difficult to find contiguous sets of blocks to write a file. File systems become fragmented.

12. Write some tips for improving system administration?

Here are a few things you can do to break this endless cycle of floor mopping.
- Use a trouble-ticket system
- Manage quick requests right
- Adopt three time saving policies
- Start every new host in a known state
- Our other tips

If you aren't doing these things, you're in for a heap of trouble elsewhere. These are the things that will help you climb out of your hole.

13. Define 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.

14. How SA will keep customer and manager happy?

Keeping Customers Happy:
- Make sure that you make a good impression on new customers
- Make sure that you communicate more with existing customers
- Go to lunch with them and listen
- Create a System Status web page
- Create a local Enterprise Portal for your site

Keeping Management Happy:

- Make sure that their direct manager knows how to manage them well
- Make sure that executive management supports the management of SAs
- Make sure that the SAs are taking care of themselves
- Make sure that the SAs are in roles that they want and understand
- If SAs are overloaded, make sure that they manage their time well
- Fire any SAs who are fomenting discontent
- Make sure that all new hires have positive dispositions.

15. What are integrated multiple operating system?

Multiple Operating System (MULTOS) is an operating system that allows multiple application programs to be installed. And to reside separately and securely on a smart card.
MULTOS (which stands for "Multiple Operating System") is an operating system that allows multiple application programs to be installed and to reside separately and securely on a smart card. Each program is isolated by the operating system so that no application can interfere with another one. Whereas earlier smart card systems did not allow new applications to be installed or old ones deleted, MULTOS makes this possible.

16. Write the scope of system and network administration?

Network and computer systems administrators are responsible for the day-to-day operation of these networks. They organize, install, and support an organization's computer systems, including local area networks (LANs), wide area networks (WANs), network segments, intranets, and other data communication systems.

17. Why mountable racks are important while buying servers for the networks?

Servers should be rack-mountable. Although nonrackable servers can be put on shelves in racks, doing so wastes space and is inconvenient. Whereas desktop hardware may have a pretty, molded plastic case in the shape of a gumdrop, a server should be rectangular and designed for efficient space utilization in a rack. Any covers that need to be removed to do repairs should be removable while the host is still rack-mounted. More importantly, the server should be engineered for cooling and ventilation in a rack-mounted setting. A system that only has side cooling vents will not maintain its temperature as well in a rack as one that vents front to back. Having the word server included in a product name is not sufficient; care must be taken to make sure that it fits in the space allocated. Connectors should support a rack-mount environment; such as use of standard cat-5 patch cables for serial console rather than db-9 connectors with screws.

18. Which files contains information about password policies such as expiry?

The /etc/passwd File:

The /etc/passwd file stores the user's login, encrypted password entry, UID, default GID, name (sometimes called GECOS), home directory, and login shell. Each line in the file represents information about a user. The lines are made up of various standard fields, with each field delimited by a colon.

The /etc/shadow File:

This is the encrypted password file that stores the encrypted password information for user accounts. In addition to storing the encrypted password, the /etc/shadow file stores optional password aging or expiration information.

The /etc/group File:

The /etc/group file contains a list of groups, with one group per line. Each group entry in the file has four standard fields, each colon-delimited, as in the /etc/passwd and /etc/shadow files. Each user on the system belongs to at least one group, that being the user's default group. Users can then be assigned to additional groups if needed. You will recall that the /etc/passwd file contains each user's default group ID (GID). This GID is mapped to the group's name and other members of the group in the /etc/ group file. The GID should be unique for each group.

19. What is the difference between root user and other user?

The root user is basically equivalent to the administrator user on Windows – the root user has maximum permissions and can do anything to the system. Normal users on Linux run with reduced permissions – for example, they can't install software or write to system directories.

20. What are the differences between Local and Universal Groups?

Local Group:

Domain local security groups are most often used to assign permissions for access to resources. You can assign these permissions only in the same domain where you create the domain local group. Members from any domain may be added to a domain local group.
The domain local scope can contain user accounts, universal groups, and global groups from any domain. In addition, the scope can both contain and be a member of domain local groups from the same domain.

Global Group:

Global security groups are most often used to organize users who share similar network access requirements. Members can be added only from the domain in which the global group was created. A global group can be used to assign permissions for access to resources in any domain. The global scope can contain user accounts and global groups from the same domain, and can be a member of universal and domain local groups in any domain.

Universal Group:

Universal security groups are most often used to assign permissions to related resources in multiple domains. Members from any domain may be added. Also, you can use a universal group to assign permissions for access to resources in any domain. Universal security groups are not available in mixed mode. The full feature set of Windows 2000 and later Microsoft NT-based operating systems is available only in native mode. The universal scope can contain user accounts, universal groups, and global groups from any domain. The scope can be a member of domain local or universal groups in any domain.

21. Why IP tables are needed?

To make configuration easier, Netfilter provides a tool called iptables that can be run from the command line. The iptables tool specifically manages Netfilter for Internet Protocol version 4 (IPv4). The iptables tool makes it easy to list, add, and remove rules as necessary from the system.
IP-table is a firewall program for Linux that is monitor traffic from and to your server using tables. These tables contain sets of rules, called chains, that will filter incoming and outgoing data packets.

22. How administrator assign disk quota to user?

To implement disk quotas, use the following steps:

- Enable quotas per file system by modifying the /etc/fstab file.
- Remount the file system(s).
- Create the quota database files and generate the disk usage table.
- Assign quota policies.

23. Write two benefits of LYNC?

Microsoft Lync has a variety of benefits for businesses to help them improve internal and external communications.
There are following benefits of LYNC:

- Easy Access
- Mobile Access
- Availability Alert
- High Definition Video
- Simplicity
- Easy to setup Meetings

24. Discuss hot swap components and what is the benefits of using host swap component?

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. Being able to hot-swap components is like being able to change a tire while the car is driving down a highway. It's great not to have to stop to fix common problems.
The first benefit of hot-swap components is that new components can be installed while the system is running. You don't have to schedule a downtime to install the part. However, installing a new part is a planned event and can usually be scheduled for the next maintenance period. The real benefit of hot-swap parts comes during a failure.

25. Discuss the difference between open cable management and closed cable management?

Horizontal cable management usually screws into the mounting rails and can be open or closed. 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. 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. When closed cable management fills up, it becomes difficult or impossible to replace the covers, so they are left off, and it becomes even messier than open cable management. Closed cable management is also more tedious to work with and becomes a nuisance for very little gain.

26. What are different permissions group associated with file?

Permission groups associated with files are as follows:

- Read (r)
- Write (w)
- Execute (x)

Read: This permission give you the authority to open and read a file. Read permission on a directory gives you the ability to lists its content.

Write: The write permission gives you the authority to modify the contents of a file. The write permission on a directory gives you the authority to add, remove and rename files stored in the directory. Consider a scenario where you have to write permission on file but do not have write permission on the directory where the file is stored. You will be able to modify the file contents. But you will not be able to rename, move or remove the file from the directory.

Execute: In Windows, an executable program usually has an extension ".exe" and which you can easily run. In Unix/Linux, you cannot run a program unless the execute permission is set. If the execute permission is not set, you might still be able to see/modify the program code(provided read & write permissions are set), but not run it.

27. Write down the names of Linux file systems?

1. Ext, Ext2, Ext3 and Ext4 file system
2. JFS File System
3. ReiserFS File System
4. XFS File System
5. Btrfs File System
6. Swap File System

28. Why SSH command is used?

The SSH command is used to start the SSH client program that enables secure connection to the SSH server on a remote machine. The ssh command is used from logging into the remote machine, transferring files between the two machines, and for executing commands on the remote machine.

29. Define the term open source OS?

Open Source operating systems are released under a license where the copyright holder allows others to study, change as well as distribute the software to other people. This can be done for any reason. Open source software is software with source code that anyone can inspect, modify, and enhance. "Source code" is the part of software that most computer users don't ever see; it's the code computer programmers can manipulate to change how a piece of software—a "program" or "application"—works. Programmers who have access to a computer program's source code can improve that program by adding features to it or fixing parts that don't always work correctly.

30. What is the difference between /root and /?

/ is the parent directory of all files and directories on a Linux box including root.
On a standard Linux system /root is home directory of user root.
Home directory :- User lands in this directory as soon as he logs on the machine.

31. How file permissions of a file can be changed provide command?

The chmod command is used to change the permissions of a file or directory. To use it, we specify the desired permission settings and the file or files that we wish to modify.
You can use the chmod command to set permissions in either of two modes:

Absolute Mode – Use numbers to represent file permissions (the method most commonly used to set permissions). When you change permissions by using the absolute mode, you represent permissions for each triplet by an octal mode number.

Syantax: `$ chmod nnn filename`

Symbolic Mode – Use combinations of letters and symbols to add or remove permissions.

Syntax: `$ chmod who operator permission filename`

32. What is purpose of shadow and /passwd files?

The /etc/passwd file stores the user's login, encrypted password entry, UID, default GID, name (sometimes called GECOS), home directory, and login shell. Each line in the file represents information about a user. The lines are made up of various standard fields, with each field delimited by a colon. This is the encrypted password file that stores the encrypted password information for user accounts. In addition to storing the encrypted password, the /etc/shadow file stores optional password aging or expiration information. The introduction of the shadow file came about because of the need toseparate encrypted passwords from the /etc/passwd file. This was necessary because the ease with which the encrypted passwords could be cracked was growing with the increase in the processing power of commodity computers (home PCs). The idea was to keep the /etc/passwd file readable by all users without storing the encrypted passwords in it and then make the /etc/ shadow file readable only by root or other privileged programs that require access to that information. An example of such a program would be the login program.

33. How groups are managed in Linux OS?

On Linux, group information is held in the /etc/group file. You can use commands to create a group, add a user to a group, display a list of the users who are in the group, and remove a user from a group.

Create a new group:

To create a new group, use the **groupadd** command.

Type the following command:

```
groupadd -g group-ID group-name
```

where group-ID is the numeric identifier of the group, and group-name is the name of the group.

Adding new member in a group:

To add a member to a supplementary group, use the `usermod` command to list the supplementary groups that the user is currently a member of, and the supplementary groups that the user is to become a member of.

For example, if the user is already a member of the group groupa, and is to become a member of groupb, use the following command:

```
usermod -G groupa,groupb user-name
```

where user-name is the user name.

Display the member of a gropup:

To display who is a member of a group, use the `getent` command.

Type the following command:

```
getent group group-name
```

where group-name is the name of the group.

Remove a member from group:

To remove a member from a supplementary group, use the **usermod** command to list the supplementary groups that you want the user to remain a member of.

For example, if the user's primary group is users and the user is also a member of the groups mqm, groupa and groupb, to remove the user from the mqm group, use the following command:

```
usermod -G groupa,groupb user-name
```

where user-name is the user name.

34. List down to major network services?

The major network services include:

file, print, email, authentication, and name service.

35. Why IPSec used?

IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from.

36. What Is the key difference between Windows OS and Linux OS?

- Linux is an open source operating system so user can change source code as per requirement whereas Windows OS is a commercial operating system so user doesn't have access to source code.
- Linux is very well secure as it is easy to detect bugs and fix whereas Windows has a huge user base, so it becomes a target of hackers to attack windows system.
- Linux runs faster even with older hardware whereas windows are slower compared to Linux.
- Linux peripherals like hard drives, CD-ROMs, printers are considered files whereas Windows, hard drives, CD-ROMs, printers are considered as devices
- Linux files are ordered in a tree structure starting with the root directory whereas in Windows, files are stored in folders on different data drives like C: D: E:
- In Linux you can have 2 files with the same name in the same directory while in Windows, you cannot have 2 files with the same name in the same folder.
- In Linux you would find the system and program files in different directories whereas in Windows, system and program files are usually saved in C: drive.

37. What is the role of server in network?

A network server is a powerful computer used to store files and run programs centrally. A server can improve file management and security and make it easier for employees to collaborate.
A network server can have many roles:
Use a network server to:

- store and share your files;
- share a single internet connection between all your devices;
- manage incoming and outgoing email;
- allow staff to access files when out and about through a virtual private network (VPN);
- centralise printing, so the server manages print jobs and lets you share printers;
- run networked applications, such as your customer database;
- host an intranet (a kind of private website holding important information about your business).

38. What is NAS?

Network-Attached Storage (NAS) is a new term for something that's been around for quite a while: clients accessing the storage attached to a server. For example, UNIX clients that use NFS to access files on a server, or Microsoft Windows systems that use CIFS to access files on a Windows server. Many vendors package turnkey network file servers that work out of the box with several file-sharing protocols. Network Appliance and EMC make such systems for large storage needs; Linksys and other companies make smaller systems for consumers and small business.

39. How RAId works?

RAID (redundant array of independent disks) is a way of storing the same data in different places on multiple hard disks or solid-state drives to protect data in the case of a drive failure.
RAID works by placing data on multiple disks and allowing input/output (I/O) operations to overlap in a balanced way, improving performance. Because the use of multiple disks increases the mean time between failures (MTBF), storing data redundantly also increases fault tolerance.

40. Write a command for transferring a files through telnet?

```
cat <file_to_transfer> | base64
```

41. Discuss about the need for bash shell?

a Bash shell script is a computer program written in the Bash programming language. ... Shell scripts are commonly used for many system administration tasks, such as performing disk backups, evaluating system logs, and so on. They are also commonly used as installation scripts for complex programs.

42. Define SLA and its procedure?

A Service Level Agreement (SLA) is defined as an official commitment that prevails between a service provider and a client. Particular aspect of the service quality, availability, responsibilities and agreed between the service provider and the user.

Procedure for SLA:

The Service Desk Manager and the Service Contract Manager define and review service level agreements (SLAs).

From the Process Navigator, select the Manage Service Level Agreements task to access a wizard for creating or editing an SLA.

The topic walks you through this basic procedure.

- Start a new SLA or edit an existing SLA .
- Set basic parameters of the SLA.
- Set priority levels for the SLA.
- Set response procedures for the SLA.
- Set On Demand Work parameters (only for requests whose type is SERVICE DESK-MAINTENANCE).
- Set optional workflow steps:
  - Include an Edit and Approve step for service requests with a Requested status.
  - Include approvals for a service request status.
  - Include notifications for a service request status.
  - Include the option to accept or decline working on a service request
  - Include a satisfaction survey for completed service requests.
- Change the default ordering of the SLA (optional).

43. What is cryptography?

storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography is a method of conversion of data into a secret code for transmission over a public network. Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security. Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

44. Why Network monitoring tools are used?

Network monitoring tools are used to calculate network metrics that characterize a network. These will be used by the Grid middle-ware to optimize the performance of Grid applications; they will also be used by network research and developers, and network support personnel to maintain and manage the network upon which the operation of the Grid depends.

Measuring and monitoring of network performance is required for two important reasons. The first is to provide the tools necessary to view the network performance from a Grid applications standpoint and hence identify any strategic issues which may arise (such as bottlenecks, points of unreliability, Quality of Service needs). The second is to provide the metrics required for use by Grid resource broker services. This document outlines the requirements for network monitoring.

45. What is cryptanalysis?

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it; cryptanalysts also target secure hashing, digital signatures and other cryptographic algorithms.

46. Write a command to visualise network addresses?

```
ifconfig
```

47. Is it is easy to manage dynamic DNS with DHCP?

No, we are unimpressed by DHCP systems that update dynamic DNS servers. This flashy features adds unnecessary complexity and security risks. Dynamic DNS with DHCP creates a system that is more complicated more difficult to manage more prone to failure and less secure in exchange for a small amount of aesthetics pleasantness. It's not worth it.

48. What are IP tables?

IP tables 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.

49. How Syslog is managed?

Syslog is a great way to consolidate logs from multiple sources into a single location. Syslog servers uses listener process to listen the data sent over to udp/tcp port 514/1468. After listening the data is managed in the database.

50. How root password can be changed if somebody has forgotten that?

You can now reset your lost root password by using the following command:

```
passwd root
```

51. Write two advantages of using LYNC server?

The platform integrates with exchange email and Microsoft applications seamlessly but this is not only benefit of LYNC:

- Stay connected
- Simple and cost effective
- Customer care
- HD video conferencing

52. Define CIA?

The CIA Triad of confidentiality, integrity and availability is considered the core underpinning of information security. Every security control and every security vulnerability can be viewed in light of one or more of these key concepts. For a security program to be considered comprehensive and complete, it must adequately address the entire CIA Triad.

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.

53. What is the role of system administrator?

System Administrator responsibilities include:

- Installing and configuring software, hardware and networks
- Monitoring system performance and troubleshooting issues
- Ensuring security and efficiency of IT infrastructure

54. Difference between IPS / IDS and Snort?

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are both parts of the network infrastructure. The main difference between them is that IDS is a monitoring system, while IPS is a control system.

Intrusion Detection Systems (IDS): analyze and monitor network traffic for signs that indicate attackers are using a known cyberthreat to infiltrate or steal data from your network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviors like security policy violations, malware, and port scanners.

Intrusion Prevention Systems (IPS): live in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively deny network traffic based on a security profile if that packet represents a known security threat.

Snort:

Snort is a Network Intrusion Detection System (NIDS). It's quite popular and is open source software which helps in monitor network traffic in real-time, hence it can also be considered as a packet sniffer. Basically, it examines each and every data packet in depth to see if there are any malicious payloads. it

can also be used for protocol analysis and content searching. It is capable of detecting various attacks like port scans, buffer overflow, etc. It's available for all platforms i.e. Windows, Linux, etc.

55. **What is difference between cronjob and bash scripting?**
56. **List down any two network services?**
57. **Why we use IDS sensors?**
58. **What use the significance of IP tables and access list?**
59. **How files can be encrypted?**

Long Questions

1. **Define disaster and risk analysis? Explain data integrity in details?**

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:

The first step in building a disaster-recovery plan is to perform a risk analysis. Risk management is a good candidate for using external consultants because it is a specialized skill that is required periodically, not daily.

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.

2. **How the Linux file system works?**

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.

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.

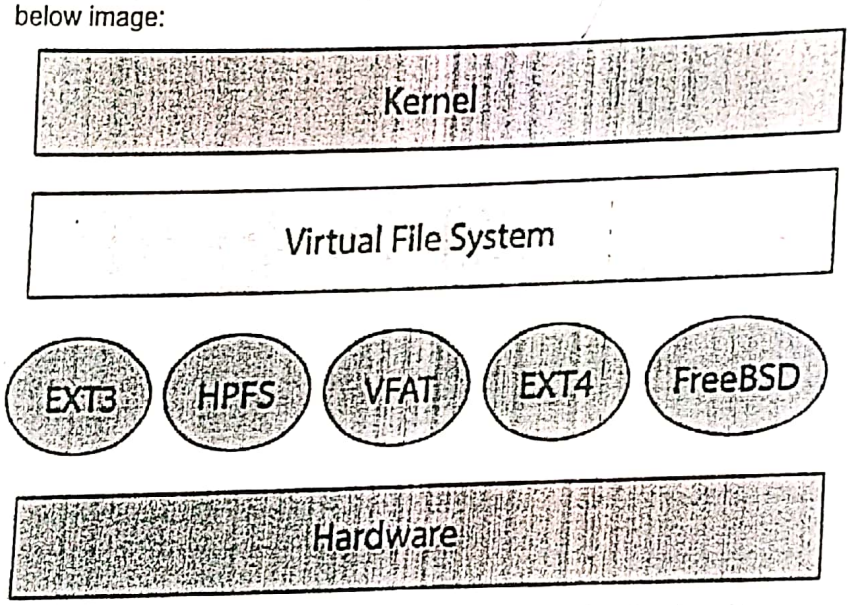
Linux file system is generally a built-in layer of a Linux operating system used to handle the data management of the storage. It helps to arrange the file on the disk storage. It manages the file name, file size, creation date, and much more information about a file.

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:



The file system requires an API (Application programming interface) to access the function calls to interact with file system components like files and directories. API facilitates tasks such as creating, deleting, and copying the files. It facilitates an algorithm that defines the arrangement of files on a file system.

The first two parts of the given file system together called a Linux virtual file system. It provides a single set of commands for the kernel and developers to access the file system. This virtual file system requires the specific system driver to give an interface to the file system.

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 as follows:

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. The major drawback of Ext3 is that it does not support servers because this file system does not support file recovery and disk snapshot.

   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. **JSF 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.

long

3. **Give the configuration of FTP server in Linux?**

FTP:

File transfer protocol is used to transfer files within or between machines.

1. FTP installation:

`yum install vsftpd`: is used to install ftp server.

`/var/ftp/pub` : is directory which automatically created by ftp after installation

2. Server services restart:

`systemctl start vsftpd.services`: is used to start the services of ftp.

`systemctl status vsftpd.services`: is used to check the status of ftp server.

notes

3. Server Services Enable:

`Systemctl enable vsftpd.services`: is used to enable the ftp services forever.

4. Allow Server Services in Firewall:

`Firewall-cmd--permanent--add.services=ftp`: is used to allow the server in firewall for security purposes.

`Firewall-cmd--reload`: is used add this rule in ftp directory for further traffic.

5. Server Configuartion:

`vsftpd.config` : is used to configure ftp file for example:

`cd/etc/vsftpd/` is used to enter in `vsftpd` directory than configure file by using vim editor

`vim vsfptd.config.`

6. Server services restart:

`systemctl restart vsftpd. services`: after configuration all the ftp services should be restart.

Long

4) **Write the different steps of configuring DNS?**

The DNS (Domain Name System) is a naming system for computers, the service that does that is the DNS server which translates an IP address to a human-readable address. Read more on the link https://likegeeks.com/linux-dns-server/#Setting-up-Linux-DNS-servert

5. **What is firewall? What different types of firewall exist? Give commands for filtering?**

A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

Types of Firewalls:

Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

- **Packet-filtering firewalls**
  As the most "basic" and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.
- **Circuit-level gateways**
  As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.
- **Stateful inspection firewalls**
  These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.
- **Application-level gateways (a.k.a. proxy firewalls)**
  Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name "application-level gateway." These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.
- **Next-gen firewalls**
  Many of the most recently-released firewall products are being touted as "next-generation" architectures. However, there is not as much consensus on what makes a firewall truly next-gen. Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.
- **Software firewalls**
  Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware (or a cloud server). The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.
- **Hardware firewalls**
  Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.
- **Cloud firewalls**
  Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewall-as-a-service (FaaS). Cloud firewalls are considered synonymous with proxy firewalls by many, since a cloud server is often used in a proxy firewall setup (though the proxy doesn't necessarily have to be on the cloud, it frequently is).
  The big benefit of having cloud-based firewalls is that they are very easy to scale with your organization. As your needs grow, you can add additional capacity to the cloud server to filter larger traffic loads. Cloud firewalls, like hardware firewalls, excel at perimeter security.