Bachelor of Science in Computer Science

Linux Server Administration

Sem 5 (NOV-2022)

Subject Code : 82902

Ql. Attempt All (10 Marks)

(a) Multiple Choice Questions:

i) Which Command is used to change the priority of a process?

a)crontab

b)tar

c)ln

d)nice

Ans: d)nice

ii) Which command is used to save work in the vi editor mode?

a)q

b):!q

c):q

d):wq!

Ans: d):wq!

iii) What is the maximum logical Partition per disk can be created?

a)7

b)9

c)14

d)11

Ans: a) 7.

iv) VNC stands for?

a)Virtual Network Clone

b)Virtual Nested config

c)Virtual Network Computing

d)Virtual Network Control

Ans: c) Virtual Network Computing.

V) What is the name of samba server identified by the Windows Computer?

a) Samba name

b)net-name-bios

c)net.bio.sambaname

d)netbios name

Ans: d)netbios name

Vi) Which of the following is commercial Distro?

a)Fedora

b)OpenSuSE

c)Ubuntu

d)RHEL

Ans: d)RHEL

vii) Is an_automatic updater and package installer/remover for RPM systems?

a)apt-get

b)yum

c)dpkg

d)dpms

Ans: b)yum

viii) Which of the following is a type of Firewall?

a)Stateless Firewall

b)Interface Firewall

c)Default Gateway

d)Packet Filtering Gateway

Ans: a)Stateless Firewall

xi) Which DataBase is responsible for configuration of the database in Apache?

a)DBMS

b)MYSQL

c)RDBMS

d)DBA

Ans: c) RDBMS (Relational Database Management System).

x) Which of this is a part of DNS hierarchy?

a)System

b)IP Address

c)Host

d)Root

Ans: d) Root.

(b) Fill in the blanks: (5M)

(netstatus, Greate Unified Rooter, icp, groupadd, ssh, FTP server, groupmod, Grand Unified Bootloader, netstat,rsa)

1.The **ssh** is a collection of tools using a secure protocol for communication with

remote Linux computer.

2.The groups can be created with the **groupadd** command.

3.GRUB stands for **Grand Unified Bootloader.**

4.The vsftpd package is used for the **FTP server** software.

5.The **netstat** program is used to display the status of all of the network connection

on a host.

Q2. Attempt the following (Any THREE) (Each of 5 Marks) (15M)

a)What is the importance of /etc/fstab in linux file system?

Answer]

- The "/etc/fstab" file is an important configuration file in the Linux file system**.** It is a configuration file that mounts uses which has a list of all partitions that the
- system uses. Format of /etc/fstab is.
  /dev/device/dir/to/mountfstypeParametersfs_freqfs_passno
- Mounting file systems: The "/etc/fstab" file is used to define the file systems that should be mounted at boot time. Each entry in the file specifies the device to be mounted, the mount point, the file system type, and any mount options that should be used.
- Simplifying file system management: By defining how block devices should be mounted into the file system, the "/etc/fstab" file simplifies the process of managing file systems. Administrators can use this file to automatically mount external storage devices or network shares, for example.
- Ensuring consistency: The "/etc/fstab" file ensures that the same file systems are mounted in the same way every time the system starts up. This helps to ensure consistency and reliability in the file system.
- Improving security: By specifying mount options in the "/etc/fstab" file, administrators can improve the security of the file system. For example, they can mount file systems with read-only permissions or with restricted access to certain users or groups.
- In summary, the "/etc/fstab" file is a critical component of the Linux file system, responsible for managing the mounting of block devices and ensuring consistency and security in the file system.

---

b) Explain booting process in Linux.

Answer]

- Power-on self-test (POST): When the computer is powered on, the hardware components go through a self-test called POST. The POST checks the system's hardware, including the CPU, memory, and peripherals, to ensure they are functioning properly.

- For boot process of any operating system you need boot loader. It is the first softwareprogram which runs firstly when your computer starts which takes control of the system.

- Boot loader: After the POST, the boot loader program is loaded into memory. The boot loader's primary purpose is to load the Linux kernel into memory and start its execution. The most commonly used boot loaders in Linux are GRUB (Grand Unified Bootloader) and LILO (Linux Loader).
- Kernel initialization: Once the boot loader has loaded the Linux kernel into memory, the kernel takes control of the booting process. It initializes various subsystems, sets up memory management, and detects and configures hardware devices. The kernel is responsible for managing the system's resources and provides an interface between the hardware and software.
- Init process: Once the kernel initialization is complete, the kernel starts the init process, which has a process ID of 1. The init process is responsible for starting and managing other system processes. In modern Linux distributions, the init process is usually replaced by systemd, which serves as the init system and manages the system services.
- Runlevels and services: Linux uses runlevels to determine the state of the system. A runlevel defines the set of services and processes that should be running at a given time. The init process or systemd identifies the default runlevel and starts the corresponding services. Different runlevels can be used for different purposes, such as single-user mode for system maintenance or multi-user mode for regular operation.
- User space initialization: Once the essential system services are started, the user space is initialized. This involves starting login managers, display managers, and other components that provide the graphical user interface (GUI). In command-line-based systems, this step may involve starting a terminal interface or a login prompt.
- User login: After the user space is initialized, the system is ready for user login. Users can enter their credentials, such as username and password, to access the system.
- User session: Once logged in, the user session begins, and the user can interact with the system, launch applications, and perform various tasks

---

c) Explain ARP protocol.

Answer]

- The Address Resolution Protocol allows IP to map the Ethernet addresses to IP addresses. ARP has its own Ethernet header type (0806). The Steps Of ARP are,
- The client sees in ARP cache to check a mapping between its IP address and its Ethernet address.

- If requested IP address is not found, a broadcast packet is sent out requesting a response.
- If IP address is there, it will respond to the ARP request.
- The client saves the information in its cache further builds a packet for transmission.
- ARP provides a mechanism for devices to dynamically resolve IP addresses to MAC addresses, allowing for efficient and seamless communication within a local network.
- It is a fundamental protocol in Ethernet-based networks and is widely supported by various operating systems and network devices.
- However, it can also be exploited by attackers to perform ARP spoofing attacks, where they send fake ARP packets to impersonate another device on the network and intercept or modify network traffic.
- To prevent ARP spoofing attacks, network administrators can use techniques such as static ARP entries or dynamic ARP inspection to validate ARP packets and prevent unauthorized access to the network.
- ARP is primarily used in IPv4 networks, where it serves as a fundamental mechanism for resolving IP addresses to MAC addresses.

---

d) Explain what is cron program.

Answer]

- User schedules a program to run on any date, at any time, or on a particular day of week which automates the system to generate reports on regular basis, and perform other periodic tasks.
  [root@fedora-serverA~]#ps aux I grepcrond I grep -v grep
  root 1897 0.0 0.4 5088 1152 ? Ss Dec09 0:06 crond
- The cron checks each user's crontab file which consist of the user's list of events that they want executed at a particular date and time.
- The crond daemon acts as background service that enables cron functionality.
- Crontab edits entries that are executed by crond. It verifies permission to modify cron settings invokes a text editor for making the changes.
- Then crontab puts the file in proper location and brings back prompt. The crontab checks /etc/cron.allow and /etc/cron.deny files for proper permission.
- The crontab format is as follows,

➢ **Minute Hour Day Month Day of Week Command**

- If there is many entries in particular column then values are separated by comma where space should not be there.
- For eg. if program is running at 2am, 6pm & 8pm then hours entries are 2,6,8. If process Runs every three minutes then the entry is /2.
- In Day_Of_Week entry, Sunday entry is represented by 0 and following other Monday to Saturday as from I to 6.

➢ **Editing the crontab file**

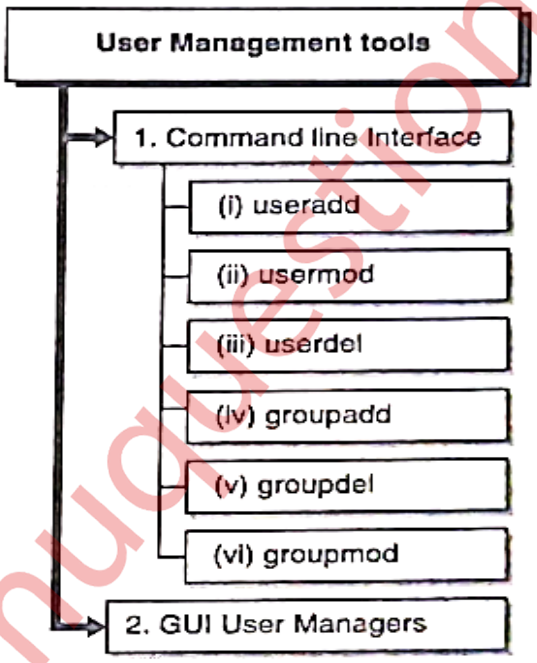
- Editing a crontab file is an easy task. As vi is the default editor for Linux, but you can
- change the editor as per your choice by setting the EDITOR or VISUAL environment variable.
- Following crontab command is used to edit the file,
- [kbp@serverA~]$ crontab —e
  To display the content of current crontab file type,
- [kbp@serverA~]$ crontab -l
  nocrontab for kbp
- To remove the crontab entry type.
  [kbp@serverA~]$ crontab -r

---

e) Explain the user management commands in linux

Answer]

- In Linux, user accounts are managed through a set of commands that allow administrators to create, modify, and delete user accounts. Here are some of the most commonly used user management commands in Linux:



(i) useradd: The "useradd" command is used to create a new user account on a Linux system. It helps you add a new user with a specific username to the system. This command sets up the necessary user information and creates a home directory for the user.

(ii) usermod: The "usermod" command is used to modify user account settings in Linux. It allows you to make changes to existing user accounts. For example, you can use it to add a user to additional groups, change the user's home directory, or modify other attributes associated with the user.

(iii) userdel: The "userdel" command is used to delete a user account from the system. It helps you remove a user's account, including their home directory and any associated files or settings. Be cautious when using this command, as it permanently deletes the user account and its data.

(iv) groupadd: The "groupadd" command is used to create a new group on a Linux system. Groups are used to organize users and assign permissions to shared resources. This command allows you to create a new group with a specific name, which can then be used to manage access and permissions for a set of users.

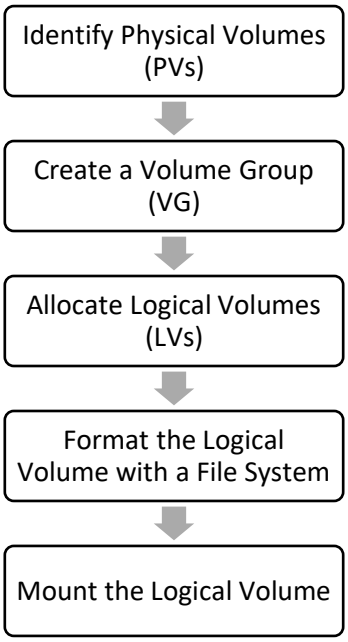
(v) groupdel: The "groupdel" command is used to delete a group from the system. When you no longer need a particular group, you can use this command to remove it from the system. If any users were associated with the group, they will no longer have that group affiliation after deletion.

(vi) groupmod: The "groupmod" command is used to modify existing group attributes. It allows you to make changes to a group's name or group ID (GID). This command helps you update the details of a group without needing to delete and recreate it.

---

f) Diagrammatically explain the steps involved in creating a logical volume

Answer]



Identify Physical Volumes (PVs):

- Identify the physical storage devices (such as hard drives or solid-state drives) that will be used to create the logical volume.
- These physical volumes will be combined to form a volume group.

Create a Volume Group (VG):

- Combine the identified physical volumes into a volume group.
- The volume group serves as a pool of storage from which logical volumes can be allocated.
- You can specify the name of the volume group and set various attributes.

Allocate Logical Volumes (LVs):

- From the created volume group, allocate logical volumes as needed.
- Specify the size and name of each logical volume.
- You can create multiple logical volumes within a volume group.

Format the Logical Volume with a File System:

- After creating the logical volume, format it with a file system.
- Common file systems in Linux include ext4, XFS, and Btrfs.
- Formatting makes the logical volume ready to store files and directories.

Mount the Logical Volume:

- Once the logical volume is formatted, you can mount it to a directory in the file system hierarchy.
- Mounting makes the logical volume accessible within the directory structure.
- You can specify the mount point and other options, such as read-only or read-write access.

Q3. Attempt the following (Any THREE)(Each of 5 Marks) (15M)

a)What is DNS Server? Explain how it works.

Answer]

- A DNS (Domain Name System) server is a crucial component of the internet infrastructure that translates human-readable domain names into the numerical IP addresses required for locating and communicating with computer services and resources. It serves as a distributed database that maps domain names to IP addresses, allowing users to access websites and other online services using easy-to-remember domain names instead of complex IP addresses.

➢ **Here's how a DNS server works:**

- DNS Query Initiation: When a user enters a domain name (e.g., example.com) in a web browser or any application that requires a network connection, the DNS resolution process begins. The application sends a DNS query to the configured DNS server.
- Recursive DNS Servers: The DNS query first reaches a recursive DNS server .Recursive DNS servers perform the bulk of the DNS resolution process by recursively querying other DNS servers to obtain the final IP address.
- Caching and DNS Hierarchy: Recursive DNS servers often have a cache to store previously resolved DNS records. If the requested domain name is found in the cache, the recursive DNS server can directly provide the corresponding IP address without further queries. If not found, the recursive DNS server starts traversing the DNS hierarchy.
- DNS Hierarchy: The DNS system has a hierarchical structure consisting of multiple types of DNS servers:
    - Root DNS Servers: At the top of the hierarchy are the root DNS servers. They maintain a list of authoritative DNS servers responsible for top-level domains (e.g., .com, .org, .net).
    - TLD DNS Servers: Below the root DNS servers are the TLD (Top-Level Domain) DNS servers. They store information about the authoritative DNS servers responsible for specific top-level domains (e.g., .com TLD servers).
    - Authoritative DNS Servers: These servers hold the actual DNS records for specific domain names. When the recursive DNS server receives a query, it iteratively

contacts the appropriate authoritative DNS servers in a top-down manner until it finds the IP address for the requested domain.

- DNS Response: Once the recursive DNS server obtains the IP address from the authoritative DNS server, it sends the response back to the requesting application or client. The IP address is then used to establish the necessary network connection to the requested resource (e.g., website, email server).
- DNS Record Time-to-Live (TTL): DNS records often have a Time-to-Live value specified, indicating the duration for which the record can be cached by DNS servers. This TTL value helps manage the caching of DNS records across the DNS infrastructure, ensuring timely updates.

---

b) Describe the Apache. Write its benefits.

Answer]

- Apache web server is a widely-used open source web server software that is designed to provide a highly reliable, scalable and secure web server environment.
- It is a popular choice for hosting dynamic websites and web applications.
- Apache web server works by receiving HTTP requests from clients (web browsers) and serving them with the appropriate web pages or resources in response. It supports various programming languages such as PHP, Python, Perl, and others through modules that can be enabled or disabled as needed.

➢ **Benefits and advantages provided by the Apache server software:**

- It is stable.
- Several major web sites, including amazon.com and IBM, are using it.
- The entire program and related components are open source.
- It works on a large number of platforms (all popular variants of Linux/UNIX, some of the not so popular variants of UNIX, and even Microsoft Windows).
- It is extremely flexible.

---

c) Explain OpenSSH.

Answer]

- Most servers are in datacenters—hostile environments that are noisy and cold. This means that as an administrator of a Red Hat Enterprise Linux Server, you probably want to access the server from a distance.
- The Secure Shell (SSH) protocol is the default service to obtain remote access to a server. To use SSH, you need an SSH server and an SSH client.

- SSH server is a process that runs on your server.
- On most Linux distributions, the name of this process is sshd.
- To connect to it from a client computer, you can use the ssh client utility if the client is Linux, or you can use PuTTY if you're on a Windows client.

➢ **Enabling the SSH Server**

- The SSH service is installed on your Red Hat Enterprise Linux server. It isn't enabled by default, however, so you should make sure to start it manually using the service sshd start command.
- After doing that, make sure that it is also started after a reboot of your server by using chkconfig sshd on. After performing these tasks, you can first do a basic connection test and connect to it using the ssh command.
- You've seen that it's not hard to enable SSH on your server.
- An SSH server that has been enabled with all the default settings isn't a secure SSH server, however. To make the SSH server secure, there are at least two modifications you should make to the /etc/ssh/sshd_config file: the Port setting and the AllowRootLogin parameter Make sure you consider at least the following SSH security settings:
- Port
- ListenAddres
- PermitRootLogin
- PasswordAuthentication
- AllowUsers

---

d) Write a short note on ftp.

Answer]

- The File Transfer Protocol (FTP) has existed for the Internet since around 1971.
- Remarkably, the underlying protocol itself has undergone little change since then.
- Clients and servers, on the other hand, have been almost constantly improved and refined. The vsftpd program is a fairly popular FTP server implementation and is being used by major FTP sites such as kernel.org, redhat.com, isc.org, and openbsd.org.
- The fact that these sites run the software attests to its robustness and security. As the name implies, the vsftpd software was designed from the ground up to be fast, stable, and secure.
- vsftpd offers the additional security features and usability enhancements listed here:
  1. Support for virtual IF configurations
  2. Support for so-called virtual users
  3. Can run as a standalone daemon or from inetd or xinetd
  4. Configurable on a per-user or per-IP basis

5. Bandwidth throttling
6. IPv6-ready

- FTP can operate in two modes: Active FTP mode and Passive FTP mode.
- **Active FTP**
  The client connects from a temporary port to the FTP server's command port. The server opens a connection from its data port to IP address and temporary port combination provided by the client when it is ready to transfer data. The PORT command is issued as the client does not make the actual data connection to the server but instead informs the server of its own port.
- **Passive FTP**
  PASV command is issued by FTP client to access data in the passive mode, and server responds with an IP address and temporal port number on itself to which the client can connect in order to do the data transfer.

---

e) Write a short note on Kerberos.

Answer]

- Kerberos is a network authentication system based on the principal of a trusted third party.
- The other two parties being the user and the service the user wishes to authenticate to. Not all services andapplications can use Kerberos, but for those that can, it brings the network environment one step closer to being Single Sign On(SSO).
- There are a few terms that are good to understand before setting up a Kerberos server:
- Principal: any users, computers, and services provided by servers need to be defined as Kerberos Principals.
- Instances: are used for service principals and special administrative principals.
- Realms: the unique realm of control provided by the Kerberos installation. Think of it as the domain or group your hosts and users belong to. Convention dictates the realm should be in uppercase. By default, ubuntu will use the DNS domain converted to uppercase (EXAMPLE.COM) as the realm.
- Key Distribution Center: (KDC) consist of three parts, a database of all principals, the authentication server, and the ticket granting server. For each realm there must be at least one KDC.
- Ticket Granting Ticket(TGT): issued by the Authentication Server (AS), the Ticket Granting Ticket (TGT) is encrypted in the user's password which is known only to the user and the KDC.
- Ticket Granting Server: (TGS) issues service tickets to clients upon request.

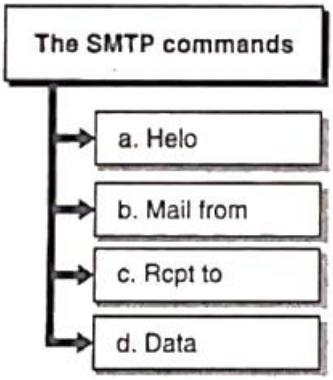
- Tickets: confirm the identity of the two principals. One principal being a user and the other a service requested by the user. Tickets establish an encryption key used for secure communication during the authenticated session.
- Keytab Files: are files extracted from the KDC principal database and contain the encryption key for a service or host.

---

f) Describe SMTP Protocol.

Answer]

- SMTP stands for Simple Mail Transfer Protocol.
- It is the standard for mail transport across the Internet. It specifies the method through which mail is sent from one host to another. It does not specify how the mail should be stored and displayed to the recipient.
- SMTP is also independent of operating systems, which means each system can use its own style of storing mail without worrying about how the sender of a message stores his mail



- The SMTP commands are,
- HELO
  It is used when a client introduces itself to the server
- MAIL FROM
  It requires the sender's e-mail address as its argument.
- RCPT TO
  It requires the receiver's e-mail address as an argument
- DATA
  The server knows who the sender and recipient are thus needs to know what message to send.

➢ **Mail service has following components:**

- Mail user agent
  It only reads mail and allows users to compose mail.
- Mailtransport agent

It handles the process of getting the mail from one site to another.

- Mail delivery agent
  It takes the message, once received at a site,and gets it to the appropriate user mailbox.

Q4. Attempt the following (Any THREE) (Each of 5 Marks) (15M)

a) Explain how to install and configure NFS server and client.

Answer]

Configuring NFS Server :

There are two steps in configuring NFS server :

- Step 1: create the /etc/exports file. This file defines the parts of the server's disk to be shared with the rest of the network and the rules by which they get shared. For example, is a client allowed only read access to the file system or Are they allowed to write to the file system?
- Step 2: start the NFS server processes that read the /etc/exports file.
- The /etc/exports Configuration File This is the primary configuration file for the NFS server. This file lists the partitions that are sharable, the hosts they can be shared with, and with what permissions. The file specifies remote mount points for the NFS mount protocol. The format for the file is simple. Each line in the file specifies the mount point(s) and export flags within one local server file system for one or more hosts. Here is the format of each entry in the /etc/exports file:
- **/directory/to/export client|ip_network(permissions) client|ip_network(permissions)**

Telling the NFS Server Process about /etc/exports

- Once you have an /etc/exports file written up, use the exportfs command to tell the NFS server processes to reread the configuration information. The parameters for exportfs are as follows:
- exportfs Command Option Description
  - -a Exports all entries in the /etc/exports file. It can also be used to unexport the exported file systems when used along with the u option, e.g., exportfs -ua.
  - -r Re-exports all entries in the /etc/exports file. This synchronizes /var/lib/nfs/xtab with the contents of the /etc/exports file. For example, it deletes entries from /var/lib/nfs/xtab that are no longer in /etc/exports and removes stale entries from the kernel export table.

- -u clientA:/dir/to/mount Unexports the directory /dir/to/mount to the host clientA.
- -o options Options specified here are the same as described in Table 22-1 for client permissions. These options will apply only to the file system specified on the exportfs command line, not to those in /etc/exports.
- -v Be verbose.

After you have configured your /etc/exports file and exported all of your file systems using exportfs, you can run showmount -e to see a listing of exported file systems on the local NFS server. The -e option tells showmount to show the NFS server's export list. For example #showmount -e localhost.

Configuring NFS Client :

- NFS clients configuration don't require any new or additional software to be loaded.
- But the kernel needs to be compiled to support the NFS file system.
- In most of the Linux distributions this feature is enabled by default.
- Along with the kernel support, the other important factor is the options used with the mount command.

The mount command :

- To mount the server share on the client machine, the mount command is used.
- The important parameters to use with the mount command are the specification of the NFS server name, the local mount point, and the options specified after the -o on the mount command line.
- The following is an example of a mount command line:
- **[root@clientA~]# mount -o rw server:/home /mnt/home**
- Here, server is the NFS server name

---

b) What is DHCP server? How is it configured?

Answer]

- DHCP stands for Dynamic Host Configuration Protocol
- It is a network protocol that is used to enables a server to automatically assign an IP address to a computer from a defined range of IP addresses configured for a given network.
- Using DHCP, you can have an IP address, default gateway, subnet mask, broadcast address and the other information automatically assigned to the hosts connected to your network.
- DHCP makes sure that every host on your network has a valid IP address, subnet mask, broadcast address, and gateway, with minimum efforts.

- To use DHCP there should be a server configured for each of your subnets and each host on the subnet needs to be configured as a DHCP client.

Configuring DHCP Server :

- Dhcpd is the daemon that runs on the server and is included as an RPM on Red Hat installation CDs.
- You can install it using the Package Management tool by following the instructions:

  - Choose Applications ⟶System Settings⟶ Add/Remove Applications from the panel.
  - Scroll down the list until you see a listing for Network Servers.
  - Click the Detail Link for Network Servers.
  - Click close; then click update and finally continue
  - Insert the requested numbered installation CD when prompted and click OK.
  - After the package is installed, click Close to exit the Package Management Tool

The DHCP server is controlled by its configuration file which is /etc/dhcpd.conf.

```
The following is an example of a simple DHCP configuration file:
subnet 192.168.1.0 netmask 255.255.255.0
# Options
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
option domain-name "example.org";
option domain-name-servers ns1.example.org;
# Parameters
default-lease-time 21600;
max-lease-time 43200;
# Declarations
range dynamic-bootp 192.168.1.25 192.168.1.49;
# Nested declarations
host clientA
hardware ethernet 00:80:c6:f6:72:00;
fixed-address 192.168.1.50;
```

- **option domain-name :** Mention Domain Name eg : elinuxbook.com
- **option domain-name-servers** : Mention DNS Servers eg: 192.168.0.100, 192.168.0.101
- **default-lease-time :** The Default time in Seconds till the time DHCP Server will assign a IP to Client Computer.
- **max-lease-time :** The Maximum time in Seconds till the time DHCP Server will assign a IP to Client Computer.
- **subnet :** Mention the Subnet IP Address eg : 192.168.0.0
- **netmask :** Mention the Subnet Mask eg : 255.255.255.0

- **range :** Mention the IP Range which will dynamically assigned by Linux DHCP Server to Client Computers. eg : 192.168.0.2 to 192.168.0.240
- **option routers :** Mention the Gateway IP Address eg : 192.168.0.1
- **option broadcast-address :** Mention your Broadcast Address eg : 192.168.0.255
- **hardware ethernet :** Mention your MAC Address OR Physical Address eg : 00:0C:29:F7:BE:27
- **option host-name :** Your systems Hostname OR Computer Name eg : dhcpserver

- You can create it using a text editor, if this file does not exist on your server,
- Make sure to use the proper addresses for your network.
- To start the server, run the command dhcpd.
- To enable dhcpd at the time system is booted, chkconflg command is used as
- chkconflg -level 3 5 dhcpd on .

---

c) What is LDAP? Explain.

Answer]

- The Lightweight Directory Access Protocol (LDAP) is actually a set of open protocols used to access and modify centrally stored information over a network.
- LDAP was developed by the University of Michigan in 1992 as a lightweight alternative to the Directory Access Protocol (DAP)
- LDAP is based on the X.500 standard (X.500 is an Industry Standards Organization [ISO] standard that defines an overall model for distributed directory services) but is a more lightweight version of the original standard.
- RFC 2251 explains the relationship like so: “LDAP is designed to provide access to directories supporting the X.500 models, while not incurring the resource requirements of the X.500 directory access protocol. Like traditional databases, an LDAP database can be queried for the information it stores.”
- LDAP itself does not define the directory service. It instead defines the transport and format of messages used by a client to access data in a directory (such as the X.500 directory).
- LDAP is a protocol for accessing a specially tailored database that is used for a variety of things, such as directory service.
- But unlike traditional databases, an LDAP database is especially suited for read, search, and browse operations instead of write operations. It is with reads that LDAP shines.

  Here are some popular LDAP implementations:

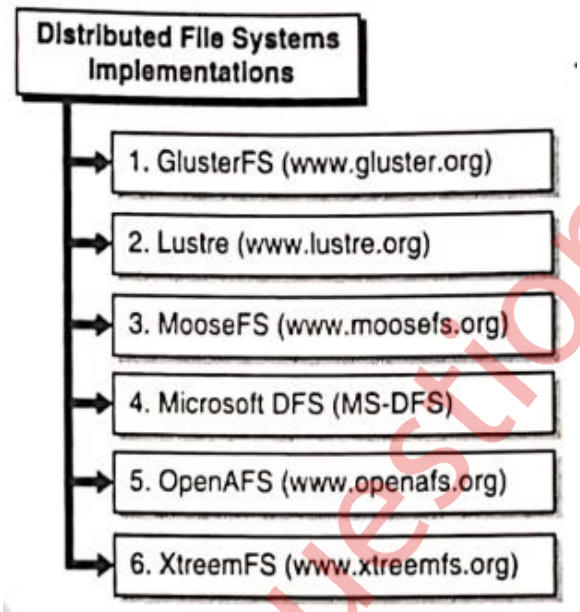
- OpenLDAP, an open-source LDAP suite
- Novell's NetWare Directory Service (eDirectory)
- Microsoft's Active Directory
- iPlanet Directory Server (split between Sun and Netscape a while back, but then Netscape Directory Server was acquired by Red Hat, which released it to the open-source community)
- IBM's SecureWay Directory

---

d) Write different Distributed File System (DFS) implementations.

Answer]

- Following are DFS implementations



1. **GlusterFS (www.gluster.org)**
It is a popular open source distributed file system that is easy to set up and use. The packaged binaries of GlusterFS are readily available for most of the popular Linux distributions. It is best suited for high-performance and cloud computing applications.

2. **Lustre (www.lustre.org)**
This high performance DFS implementation is mostly used for LAN environments. It is a little complicated to install, configure, and maintain in comparison to some other DFS solutions. A standard Lustre setup includes : Metadata Server (MDS), Metadata Target (MDT), Object storage Server (OSS), Object Storage Target (OST), and Lustre clients.

3. **MooseFS (www.moosefs.org)**
This DFS implementation is simple-to-use and fault-tolerant . It is easy to install and setup on most Linux-based distributions, A typical MooseFS implementation in a production environment consists of these components: master server, chunk servers, metalogger server, and clients.

4. **Microsoft DFS (MS.DFS)**
It a Microsoft product that is easy to install in a pure Windows environment. The Open source project Samba can emulate some of the features of the proprietary MS-DFS in its implementation .

5. **OpenAFS (www.openafs.org)**
One of the older DFS implementations, OpenAFS is robust and well supported on multiple platforms—MS Windows, Linux, and Macs. It is not easy to install and configure.

6. **XtreemFS (wwwxtreemfs.org)**
It is simple to set up and manage. XtreemFS workload is best suited for cloud-computing environments.

---

e) Explain the showmount command with options and example.

Answer]

- When configuration of NFS is done, the showmount command can be used to see if everything is working correctly.
- The command shows the mount information for an NFS server.
- After you have configured your /etc/exports file and exported all of your file systems using exportfs, you can run showmount -e to see a listing of exported file systems on the local NFS server.
- The -e option tells showmount to show the NFS server's export list.
- For example #showmount -e localhost.
- Here are some common options for the showmount command:

- `-e`: Displays a list of all exports from the NFS server, including the path to the directory being exported and any access restrictions.

- `-a`: Displays the list of NFS clients that are currently accessing any exported NFS shares.

- `-d`: Displays a list of all directories that have been exported by the NFS server.

---

f) What is LAMP? Write the steps to install LAMP applications

Answer]

- To budding dynamic web applications we may need to use web server. database and any server side and client side scripting language.
- LAMP is an open source Web development platform that uses Linux as operating system. Apache as the Web server. MySQL as the relational database and PHP as the object-oriented scripting language.
- Now a day's sometimes python is used instead of PHP.

Installation of LAMP :

1. Install Apache: The first step is to install the Apache web server using the package manager for your Linux distribution. For example, on Ubuntu, you can use the following command:

```` ```***sudo apt-get install apache2*** ``` ````

2. Configure Apache: After installation, you may need to modify the Apache configuration file, which is located at `/etc/apache2/apache2.conf`. This file specifies the server settings, such as the document root, virtual hosts, and server modules.

3. Install MySQL: Next, youll need to install the MySQL database server using the package manager for your Linux distribution. For example, on Ubuntu, you can use the following command: ```` ```***sudo apt-get install mysql-server*** ``` ````

4. Configure MySQL: After installation, you may need to modify the MySQL configuration file, which is located at `/etc/mysql/mysql.conf.d/mysqld.cnf`. This file specifies the server settings, such as the port number, data directory, and security options.

5. Secure MySQL: To improve the security of your MySQL server, you should run the MySQL Secure Installation script. This script will prompt you to set a root password, remove anonymous users, and disable remote root access. ```` ```***sudo mysql_secure_installation*** ``` ````

6. Install PHP: Finally, you'll need to install the PHP programming language and associated modules using the package manager for your Linux distribution. For example, on Ubuntu, you can use the following command: ```` ```***sudo apt-get install php libapache2-mod-php php-mysql*** ``` ````

7. Test LAMP: Once you've completed the installation and configuration, you can test your LAMP stack by creating a simple PHP script and accessing it through a web browser. By following these steps, you can install and configure a LAMP stack on a Linux system for web development.
````

Q5. Attempt the following (Any five) (Each of 3 Marks) (15M)

a) Discuss any one boot loader used in Linux in detail.

Answer]

Most Linux distributions such as Fedora, Red Hat Enterprise Linux (RHEL), OpenSUSE. Mandrake and Ubuntu they use GRUB as the default boot loader.
GRUB boot process takes place in stages which are important. In GRUB device names are shown in parenthesis

Stage 1

- An image file which is named as Stage 1 used for booting up GRUB in the first place which is important. It is implanted in the MBR Of a disk or in the boot sector of a partition.

Stage 2

- This stage has two types of Stages i.e. optional (which is called as Stage 1.5) and actual Stage 2 image file. Stage 1.5 acts as a bridge between Stage I and Stage 2 and also allows GRUB to access various file systems.

- Stage 2 .is the core Of the GRUB which contains the actual code to load the kernel that boots the OS. It also contains the GRUB shell which is interactive and flexible from which GRUB commands can be entered.

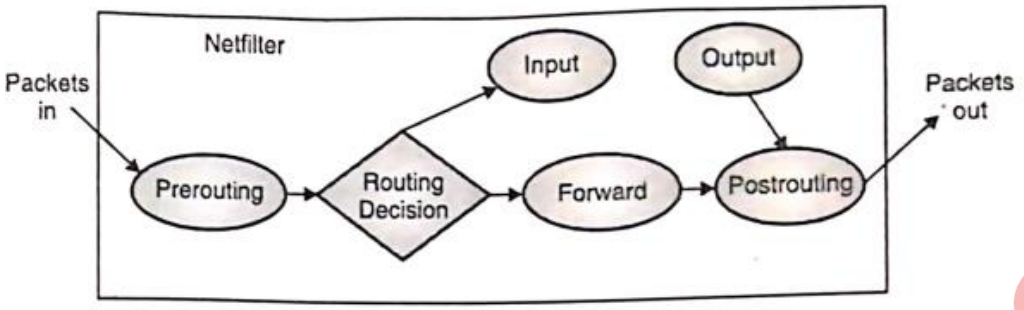
---

b) Write five predefined chains of iptables.

Answer]

Packet goes through a series of chains in each table which are list of rules that act on a packet flowing through the system.

Administrators can add more chains to the system if they want. There are five chains in iptables which are as follows



Prerouting : Packet first hits PREROUTING chain when it enters the system.

Forward : When IP forwarding is enabled and the packet is destined for a system other than the host itself the FORWARD chain is invoked.

Input : When a packet is destined for the host itself, INPUT chain is called.

Output : When packets are sent from applications running on the host itself, OUTPUT chain is invoked.

Postrouting : Here administrators can alter source IP address for the purposes of Source NAT.

---

c) Explain ext2 file System in detail.

Answer]

- Ext2 has become the standard file system for Linux.
- It is the next generation of the ext file system.
- The ext2 implementation has not changed much since it was introduced with the 1.0 kernel back in 1993.
- ext2 is flexible, can handle file systems up to 4TB large, and supports long filenames up to 1,012 characters long. In case user processes fill up a file system, ext2 normally reserves about 5 percent of disk blocks for exclusive use by root so that root can easily recover from that situation.

Advantages of ext2:

- Simple and stable: ext2 is a simple and stable file system that has been in use for many years.
- Compatible: ext2 is compatible with many operating systems, including Linux, Windows, and macOS.

- Efficient: ext2 is optimized for fast file access and can handle large files and partitions.

Disadvantages of ext2:

- No journaling: ext2 does not have built-in journaling capabilities, which can make it more vulnerable to data corruption in the event of a system crash or power failure.
- Fragmentation: Like most file systems, ext2 can suffer from fragmentation over time, which can lead to slower performance.
- Limited metadata: ext2 has limited support for extended attributes and other advanced file system features.

---

d) Explain the format of following files.

i)/etc/passwd

ii)/etc/group

Answer]

/etc/passwd :

- The user's login, encrypted password entry, UID. default GID. name home directory. and login shell are in /etc/passwd file. The fields are as follows:
- **Username:** Also called as login field or the account field which stores the name of the user on the system where as a common method to generate user login name is to use the first letter Of the user' s first name and append the user's last name.

- **Password:** It contains the encrypted password for the user which is compared against the user' s password entry when login is done.

- **User-ID:** It is a unique number to identify the user and determine access privileges. User with UID O hrs root access.

- **Group -ID:** It is number of the primary group that the user belongs to which determines user access privileges.

- **GECOS:** It stands for General Electric Comprehensive Operating System. It is an optional field which stores different pieces of information like user description, full name, telephone number etc.

- **Directory:** It's a home directory where users are allowed to keep configuration and regular files.

- **Shell:** It provides an interface between user and system. The default user shell is BASH.

etc/group :

- This file consists Of a list of groups. Each user belongs to one group, additional groups may be added if necessary. The fields in /etc/group are,
- **Group name:** The name Of the group
- **Group password :** This is optional, if set, it allows users who are not part of the group to join.
- **Group ID (GID)** : The number of the group name.
- **Group members :** It is a comma-separated list

---

e) Explain uses of various Samba daemons?

Answer]

1. smbd: This is the Samba daemon that provides file and print sharing services to clients. It is responsible for handling file and printer requests from clients, as well as authentication and access control. The smbd daemon is the core of Samba and is required for Samba to function.

2. nmbd: This is the NetBIOS name server daemon. It provides name resolution services to clients by mapping NetBIOS names to IP addresses. The nmbd daemon is required for Samba to support older Windows clients that rely on NetBIOS for name resolution.

3. winbindd: This daemon provides integration with Windows domains. It allows Samba to authenticate users against a Windows domain controller and provide access to Windows resources such as printers and file shares. The winbindd daemon is required for Samba to support domains and provides a bridge between Unix and Windows authentication systems.

4. smbclient: smbclient is a command-line tool that acts as a client for accessing and managing shared files and directories on Samba servers.It allows Linux/Unix users to connect to Samba shares, browse directories, upload/download files, and perform various file operations. smbclient provides a similar experience to the Windows command prompt and can be used for scripting or manual file operations.

---

f) Describe RPM.

Answer]

- RPM was written in 1997 by Erik Troan and Marc Ewing.
- In RPM i.e. Red Hat Package Manager you can easily install and remove software packages that consist logs of files and other metadata.
- Red Hat Package Manager (RPM) file is a package that consists files like configuration files, binaries and even pre- and postscript which are needed for the software to function correctly.
- Various Linux Distribution use this type tool for distributing and packaging their software.
- Red Hat Package Manager tool performs installation and uninstallation of RPMs. RPM packages are installed from, http://rpm.pbone.net etc. Fedora,OpenSuSE, comes with RPM

.

Functions of RPM

- To install and uninstall software
- To maintain a database which stores various items of information about the packages
- To package other software into an RPM form
- To update programs with original RPM installed are easy.

---

g) Explain mount command?

Answer]

- The mount command in Linux is used to connect and make a filesystem accessible within the Linux file system hierarchy.
- It establishes a link between a device (such as a disk partition or network share) and a directory (known as the mount point) to enable reading from and writing to the files within that filesystem.
- The general syntax is "mount [options] device directory". This command is essential for accessing and using storage devices and network shares in Linux.

option	Description
-a	It mounts all file system listed in /etc/fstab
-t fstype	Specifies the file system being mounted
-o options	It specifies options applying to the mount process
1) ro	Mounts the partition as read-only
2) rw	Mounts the partition as read/write
3) exec	Permits the execution

h) What is use of runlevel?

Answer]

A runlevel is a preset operating state in a Linux-based operating system. Each runlevel specifies a different configuration of system services and processes that are started during the boot process. In Linux, the runlevel is identified by a number from 0 to 6.

Here are the different use of runlevels in Linux:

Runlevel 0: This runlevel is used for system shutdown. When the system enters runlevel 0, all services are stopped, and the system is powered off or halted. It is used for a controlled and safe shutdown of the system.

Runlevel 1: Runlevel 1 is known as single-user mode or system maintenance mode. It starts with minimal services and provides a basic command-line interface. Runlevel 1 is used for system maintenance, troubleshooting, or repairing the system when it encounters critical issues.

Runlevel 2: Runlevel 2 is typically configured as a multi-user mode without a graphical user interface (GUI). It starts essential services without networking capabilities. It is commonly used in server environments where a GUI is unnecessary, focusing on providing essential server functionalities.

Runlevel 3: Runlevel 3 is the default multi-user mode with a command-line interface. In this runlevel, the system starts all essential services, including networking, file sharing, and user logins. It is commonly used for server installations, providing a robust and efficient environment for server operations.

Runlevel 4: Runlevel 4 is typically undefined and left for system administrators or distributions to define according to their specific needs. It does not have a predetermined purpose and can be customized to fit the requirements of the system or organization.

Runlevel 5: Runlevel 5 is commonly used for systems that require a graphical user interface (GUI). It starts all services from runlevel 3 along with a display manager that provides a graphical login screen. Runlevel 5 is often used in desktop or workstation installations, allowing users to interact with the system through a graphical interface.
