ACL

→ setfacl – Set file access control list

    - It is use to give multiple user access on one file.

        ▪ [root@localhost ~]# mount -a acl,remount /

        ▪ [root@localhost ~]# setfacl -m u:siddharth:rwx p_file.txt

        ▪ [root@localhost ~]# setfacl -m u:rutik:r p_file.txt

→ To check ACL:

        ▪ [root@localhost ~]# getfacl p_file.txt

→ To give same ACL to different file:

        ▪ [root@localhost ~]# getfacl p_file.txt | setfacl --set-file=-
        p_file1.txt

useradd Prajwal

    This command is used to create the user

passwd prajwal

    This is used to add password to the user which has been created, in this case for user RachanaM

su – Prajwal

    It is used to switch to the specified user

pwd

    It is used to retrieve the present directory path

    ⇨ home/Prajwal

cat > fileedit.txt

    this is an editable file to all

chmod o+w fileedit.txt

    This command grants write permission to others, meaning users who are neither the owner nor in the group can now modify the file.

chmod o+r fileedit.txt

This command gives read permission to others, allowing users outside the owner and group to read the file's contents.

chmod o+rwx fileedit.txt

This command provides read, write, and execute permissions to others, so any user can now read, modify, and run the file.

chmod o-w fileedit.txt

This command removes write permission from others, preventing users outside the owner and group from modifying the file, though they can still read or execute it if allowed.

chmod u+rwx fileedit.txt

This command gives the owner full control of the file by granting read, write, and execute permissions.

chmod g+rwx fileedit.txt

This command grants the group full access to the file, allowing users in the file's group to read, write, and execute it.

HTTP Server using Firewall

mount iso file

cd /etc/yum.repos.d

Navigates to the directory containing YUM repository configuration files on a Linux system.

mv *.*/opt/

This command moves all files with a .repo extension to the /opt/ directory

or

rm -f *.repo

This command forcefully deletes all files with a .repo extension in the current directory.

vi local.repo

Opens the file named local.repo in the vi text editor. If the file doesn't exist, it will create a new one.

Once in vi, you can:

Press **i** to enter insert mode and edit the file.

After editing, press **Esc** to exit insert mode.

Type **:wq** to save and quit, or **:q!** to quit without saving

Add the below contents:

[dvd1]

name=AppStream

baseurl=/run/media/root/CentOS-Stream-9-BaseOS-x86_64/AppStream

ggpgcheck=0

[dvd2]

name=BaseOS

baseurl=/run/media/root/CentOS-Stream-9-BaseOS-x86_64/BaseOS

gpgcheck=0

:wq

yum clean all

Used to clean up all cached data in YUM. This includes:

- Package metadata
- Downloaded packages
- Old headers

yum repolist all

Lists all configured YUM repositories, showing which are enabled and which are disabled.

yum update -y

The command updates all installed packages to their latest available versions without prompting for confirmation. The -y flag automatically answers "yes" to any prompts during the update process.

yum install httpd* -y

The command installs all packages that start with httpd, which typically includes the Apache HTTP Server and related modules. The -y flag automatically confirms the installation without prompting for user input.

systemctl enable httpd

The command enables the Apache HTTP Server (httpd) to start automatically at boot. This means that the service will be launched whenever the system is restarted.

systemctl start httpd

The command starts the Apache HTTP Server (httpd) immediately. This allows the web server to begin serving web pages without needing to reboot the system.

firewall-cmd --permanent --add-service=http

The command adds the HTTP service to the firewall's permanent rules, allowing incoming traffic on port 80 (the default port for HTTP).

firewall-cmd --permanent --add-service=https

The command adds the HTTPS service to the firewall's permanent rules, allowing incoming traffic on port 443 (the default port for HTTPS).

firewall-cmd --reload

The command reloads the firewall configuration, applying any changes made (such as adding or removing services) without restarting the system. This ensures that all new rules take effect immediately.

systemctl status httpd

The command displays the current status of the Apache HTTP Server (httpd). It shows whether the service is active (running), inactive, or failed, along with additional information such as the process ID, memory usage, and recent log entries. This helps you troubleshoot or verify that the web server is functioning properly.

ifconfig

It displays network configuration details for all network interfaces, including IP addresses and statuses.

- Copy the IP address and paste it in browser, then check the HTTP Server Test Page