# Assignment 23-09-2024

**ACL Overview:**

➢ ACLs allow you to grant or restrict access to files or directories for specific users or groups beyond the traditional file permission system (user-group-other). It provides more granular control over who can access a file.

✚ setfacl – Set file access control list

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

  o [root@localhost ~]# mount -a acl,remount /
  o [root@localhost ~]# setfacl -m u:nikita:rwx p_file.txt
  o [root@localhost ~]# setfacl -m u:neha: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

```
-rw-rwxr--+  1 root root    0 Sep 23 15:37 p_file1.txt
-rw-rwxr--+  1 root root    0 Sep 23 15:09 p_file.txt
drwxr-xr-x.  2 root root    6 Sep 23 16:39 Pictures
drwxr-xr-x.  2 root root    6 Sep 23 16:39 Public
-rw-r--r--.  1 root root  129 Dec 29  2013 .tcshrc
drwxr-xr-x.  2 root root    6 Sep 23 16:39 Templates
drwxr-xr-x.  2 root root    6 Sep 23 16:39 Videos
[root@localhost ~]# touch mj1.txt
[root@localhost ~]# mount -a acl,remount /
[root@localhost ~]# setfacl -m u:mayank:rwx mj1.txt
[root@localhost ~]# setfacl -m u:deepak:r mj1.txt
[root@localhost ~]# getfacl mj1.txt
# file: mj1.txt
# owner: root
# group: root
user::rw-
user:mayank:rwx
user:deepak:r--
group::r--
mask::rwx
other::r--

[root@localhost ~]# touch mj2.txt
[root@localhost ~]# getfacl mj1.txt | setfacl --set-file=- mj2.txt
[root@localhost ~]# getfacl mj2.txt
# file: mj2.txt
# owner: root
# group: root
user::rw-
user:mayank:rwx
user:deepak:r--
group::r--
mask::rwx
other::r--

[root@localhost ~]#
```

➢ Mount .iso file, install Apache web server and allow that service using firewall.
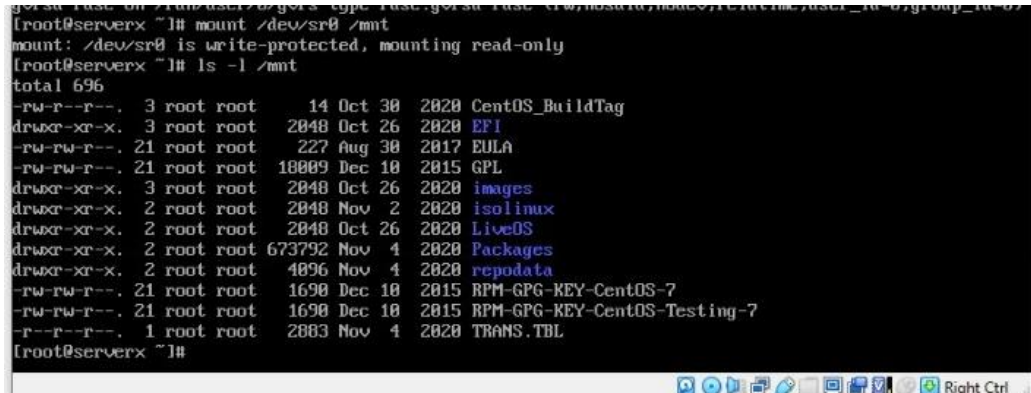
✚ Insert .iso file:
- o Select 'Machine' menu of server.
- o Select Storage.
- o Inside Controller iDE select Dropdown near Optical drive
- o Select 'Choose a disk file'.
- o Select centos .iso file.
- o Ok & Apply
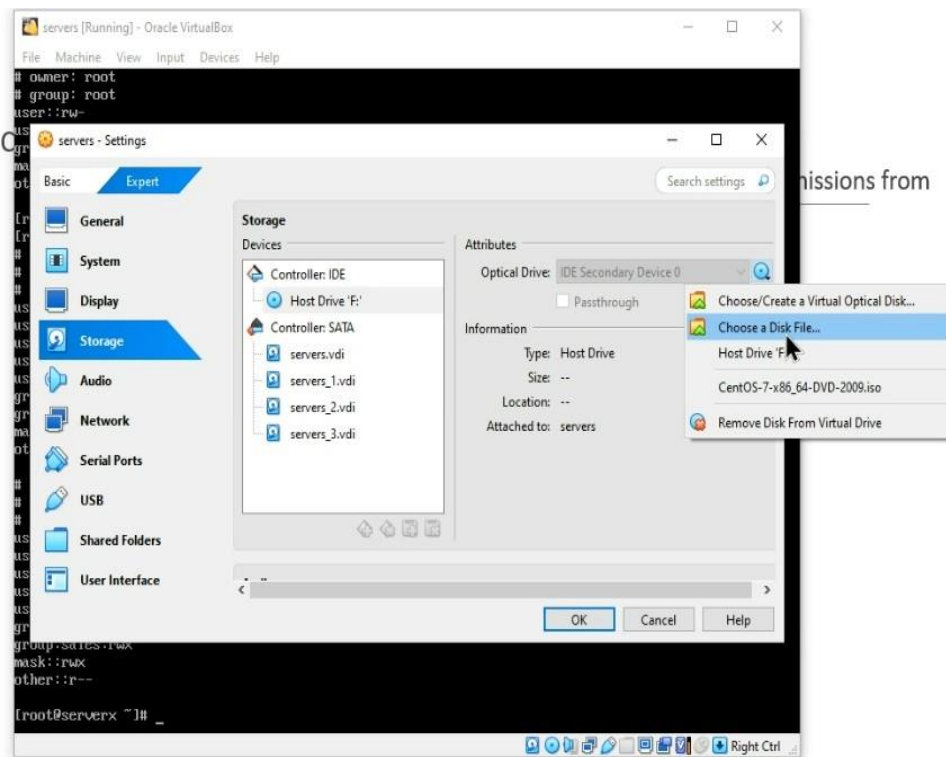
- In CLI of CentOS: [To open: ctl + alt +f2 & close: ctl + alt + f1]
    - To Mount:
        - [root@localhost ~]#mount /dev/sr0 /mnt
        - [root@localhost ~]#ls -l /mnt



- Open Terminal in CentOS:
    - Application => System Tool => Terminal
        - [root@localhost ~]#cd /etc/yum.repos.d
        - [root@localhost yum.repos.d]#ls –l

    - To remove all .repo files:
        - [root@localhost yum.repos.d]#rm -f *.repo
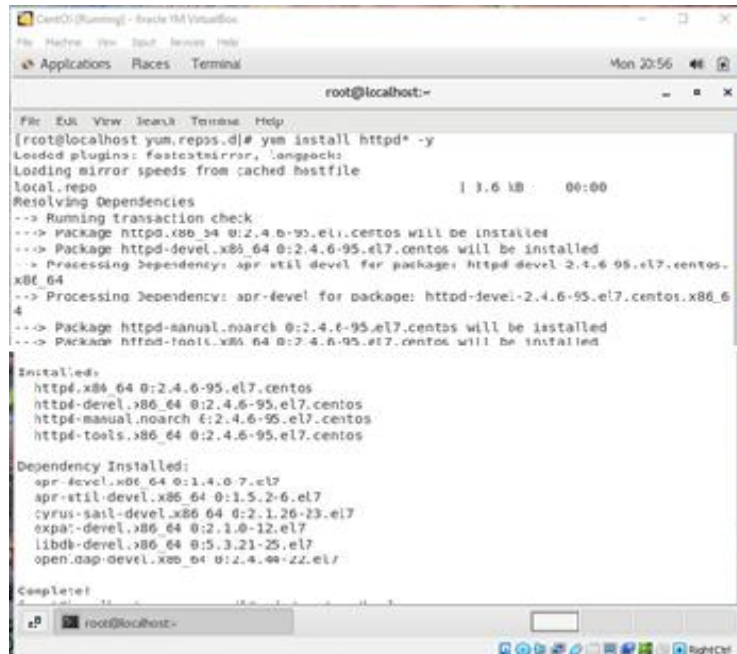
- Create new repo file:
    - [root@localhost yum.repos.d]# vi local.repo
    - In VI editor, Press 'i' to insert and write the below content:
    - [local.repo]
      name=centosrepo
      baseurl=file:///mnt
      enable=1
      gpgcheck=1
      gpgkey=file://mnt/RPM-GPG-KEY-CentOS-7
    - To exit: ESC + :wq
    - [root@localhost yum.repos.d]# yum repolist all
    - OUTPUT: "enabled:4070"

- To install Apache web server:
  - [root@localhost yum.repos.d]# yum install httpd* -y
  - OUTPUT: "Complete!"
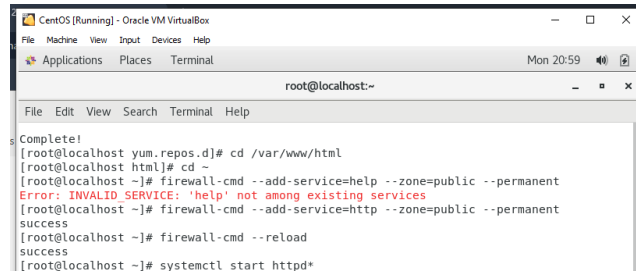


- To confirm it:
  - [root@localhost yum.repos.d]# cd /var/www/html
  - [root@localhost yum.repos.d]# cd ~
  - [root@localhost ~]#
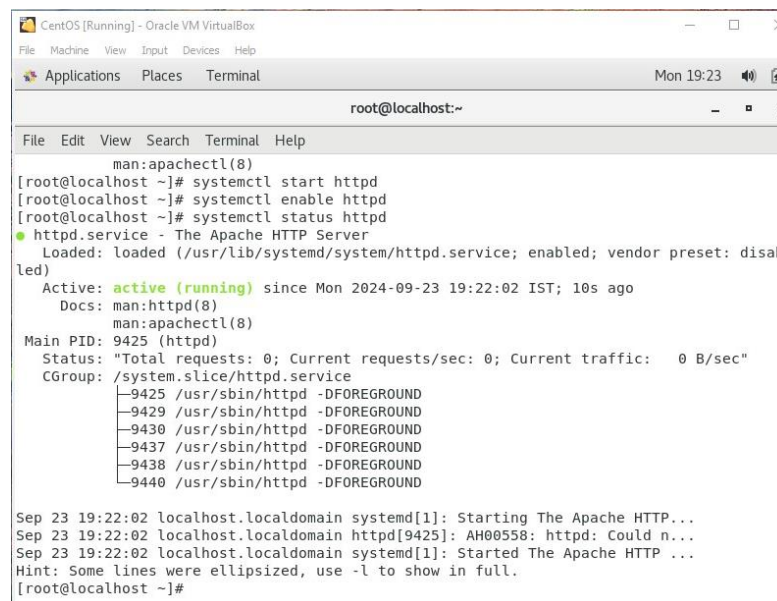
- Allow service by using Firewall:
    - [root@localhost ~]# firewall-cmd -add-service=httpd --zone=public --permanent
    - OUTPUT: "Success"
    - [root@localhost ~]# firewall-cmd --reload
    - OUTPUT: "Success"



    - [root@localhost ~]# systemctl start httpd
    - [root@localhost ~]# systemctl enable httpd
    - [root@localhost ~]# systemctl status httpd

- Try running last 3 command until you get output like:activate (running)