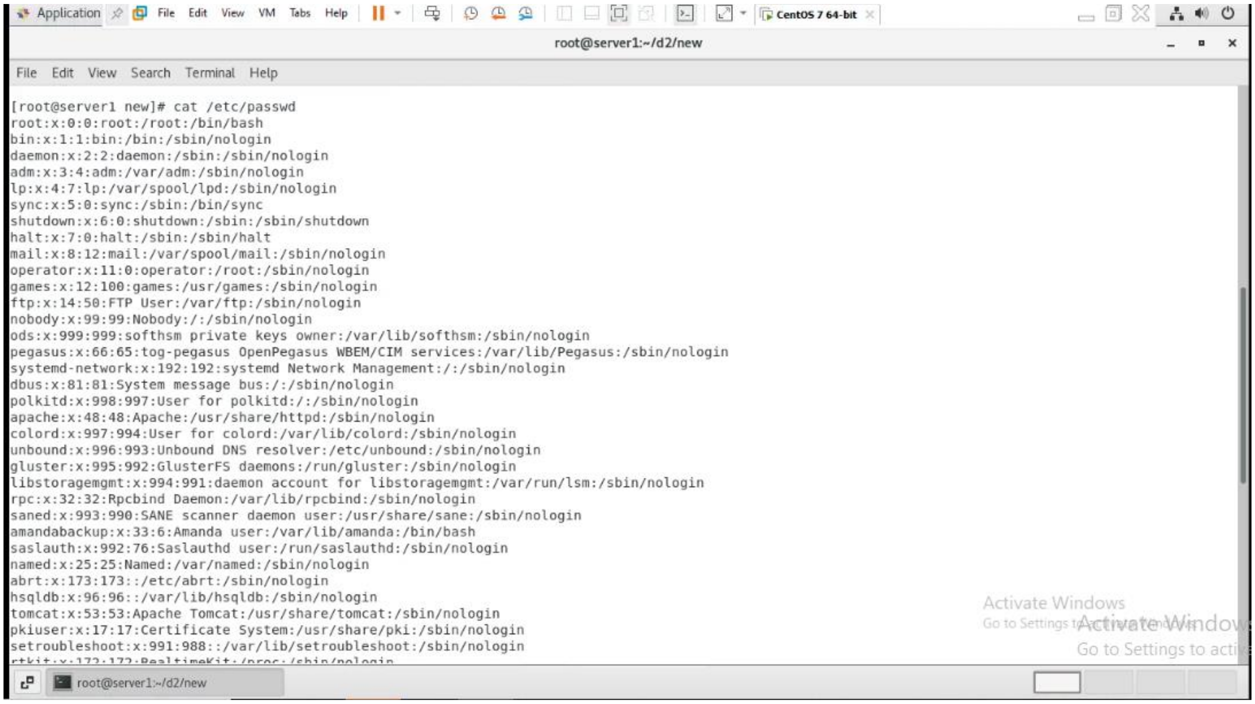
/etc/passwd

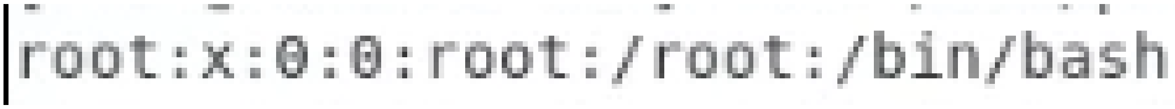
Its a file that stores essential information about user accounts .



Application
File Edit View VM Tabs Help
CentOS 7 64-bit
root@server1:~/d2/new
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
root@server1:~/d2/new

```
[root@server1 new]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
ods:x:999:999:softhsm private keys owner:/var/lib/softhsm:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:997:User for polkitd:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
colord:x:997:994:User for colord:/var/lib/colord:/sbin/nologin
unbound:x:996:993:Unbound DNS resolver:/etc/unbound:/sbin/nologin
gluster:x:995:992:GlusterFS daemons:/run/gluster:/sbin/nologin
libstoragemgmt:x:994:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
saned:x:993:990:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
amandabackup:x:33:6:Amanda user:/var/lib/amanda:/bin/bash
saslauth:x:992:76:Saslauthd user:/run/saslauthd:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
hsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin
tomcat:x:53:53:Apache Tomcat:/usr/share/tomcat:/sbin/nologin
pkiuser:x:17:17:Certificate System:/usr/share/pki:/sbin/nologin
setroubleshoot:x:991:988::/var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
```

- Here used the commant : cat /etc/passwd (To open and read the the passwd file)
- Here the file stores users information

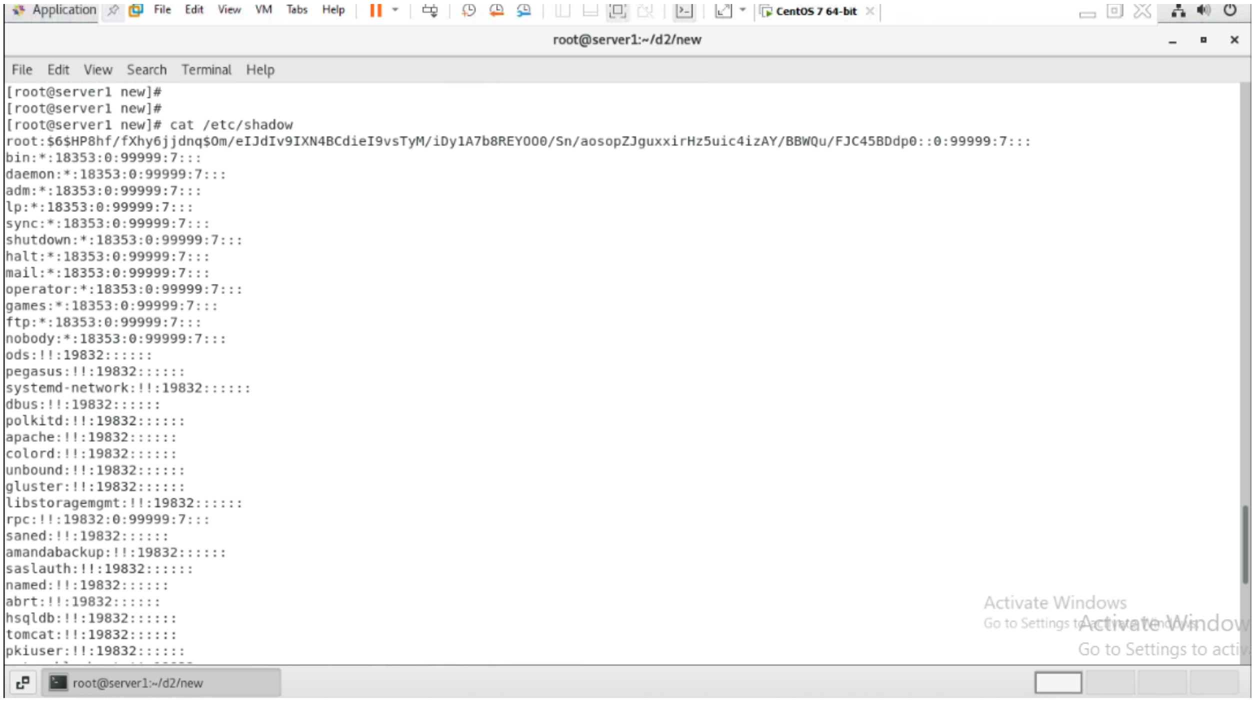


```
root:x:0:0:root:/root:/bin/bash
```

- It contains 7 columns , and they are seperated by “:”
- 1 - login user name
- 2 – referenced password - /etc/shadow
- 3 – user id
- 4 – group id
- 5 – fullname / description / comment
- 6 – default home directory
- 7 – default shell

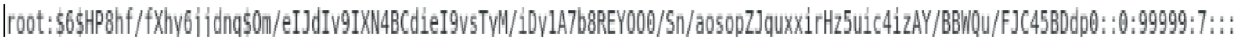
/etc/shadow

- It contains users encrypted password information



```
[root@server1 new]#
[root@server1 new]#
[root@server1 new]# cat /etc/shadow
root:$6$HP8hf/fXhy6jjdnq$Om/eIJdIv9IXN4BCdieI9vsTyM/iDy1A7b8REYOO0/Sn/aosopZJguxxirHz5uic4izAY/BBWQu/FJC45BDdp0::0:99999:7:::
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
ods:!!:19832::::::
pegasus:!!:19832::::::
systemd-network:!!:19832::::::
dbus:!!:19832::::::
polkitd:!!:19832::::::
apache:!!:19832::::::
colord:!!:19832::::::
unbound:!!:19832::::::
gluster:!!:19832::::::
libstoragemgmt:!!:19832::::::
rpc:!!:19832:0:99999:7:::
saned:!!:19832::::::
amandabackup:!!:19832::::::
saslauth:!!:19832::::::
named:!!:19832::::::
abrt:!!:19832::::::
hsqldb:!!:19832::::::
tomcat:!!:19832::::::
pkiuser:!!:19832::::::
```

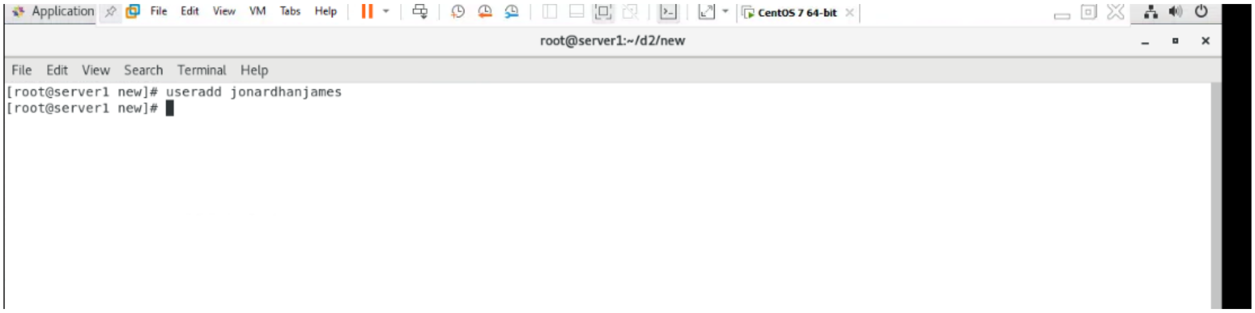
Here , cat /etc/shadow -- to open and read the shadow file



```
root:$6$HP8hf/fXhy6jjdnq$Om/eIJdIv9IXN4BCdieI9vsTyM/iDy1A7b8REYOO0/Sn/aosopZJguxxirHz5uic4izAY/BBWQu/FJC45BDdp0::0:99999:7:::
```

- It contains 9 columns .
- They are seperated by “:”
- 1 – login username
- 2 – True encrypted password
- 3 – Last password change --> Epoch date
- 4 – minimum password age
- 5 – maximum password age
- 6 – warning days
- 7 – inactive days (by default its 0 . If it changes to 1 then then after password expires the user is able to login for extra 1 day)
- 8 – account expiry
- 9 – unused till date (future purpose)

Creating a User in Linux

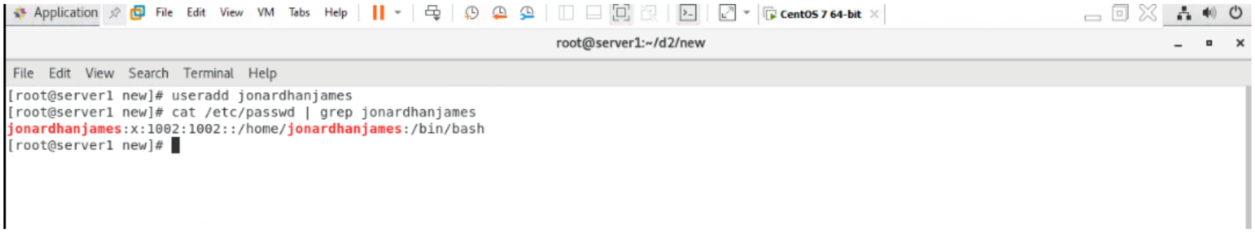


```
[root@server1 new]# useradd jonardhanjames
[root@server1 new]#
```

useradd jonardhanjames

Here jonardhanjames is the username .

Filter the user information using grep

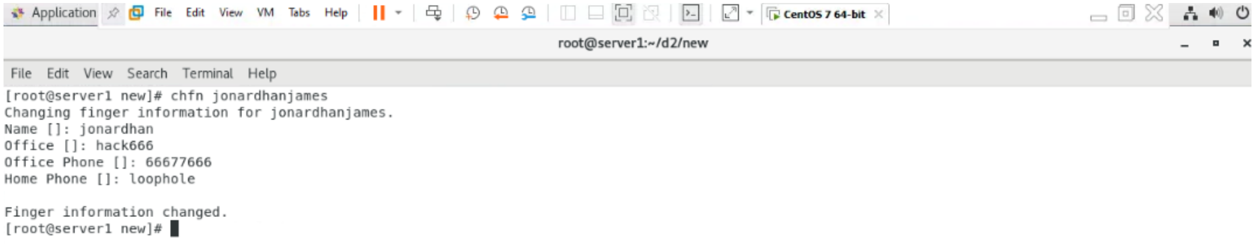


```
[root@server1 new]# useradd jonardhanjames
[root@server1 new]# cat /etc/passwd | grep jonardhanjames
jonardhanjames:x:1002:1002::/home/jonardhanjames:/bin/bash
[root@server1 new]#
```

Here we filtered the user information using grep from /etc/passwd file .

Also we can use another command ***# grep jonardhanjames /etc/passwd***

To add extra information like Fullname or comment (finger information)



```
[root@server1 new]# chfn jonardhanjames
Changing finger information for jonardhanjames.
Name []: jonardhan
Office []: hack666
Office Phone []: 66677666
Home Phone []: loophole

Finger information changed.
[root@server1 new]#
```

Here we add extra information to an existing user jonardhanjames . By using “chfn” command . Also we can use ***#usermod –c “description” jonardhanjames***

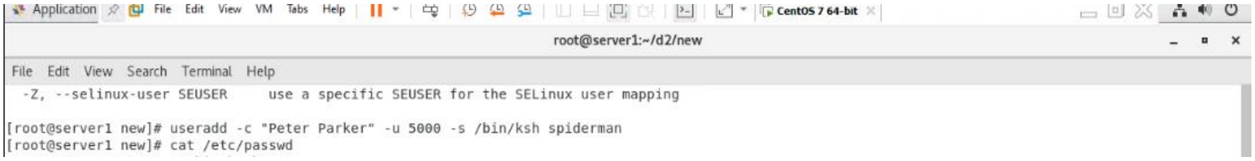
TASK – Create a user with below information with a single line command

Username = Spiderman

Comment = Peter Parker

UID = 5000

Default shell = /bin/ksh


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
root@server1:~/d2/new
File Edit View Search Terminal Help

```
 -Z, --selinux-user SEUSER     use a specific SEUSER for the SELinux user mapping

[root@server1 new]# useradd -c "Peter Parker" -u 5000 -s /bin/ksh spiderman
[root@server1 new]# cat /etc/passwd
```

Here i created user with some information by using single line .

If we want to change/modify anything then ,

# usermod –s /bin/bash spiderman -- Here i changed shell into bash

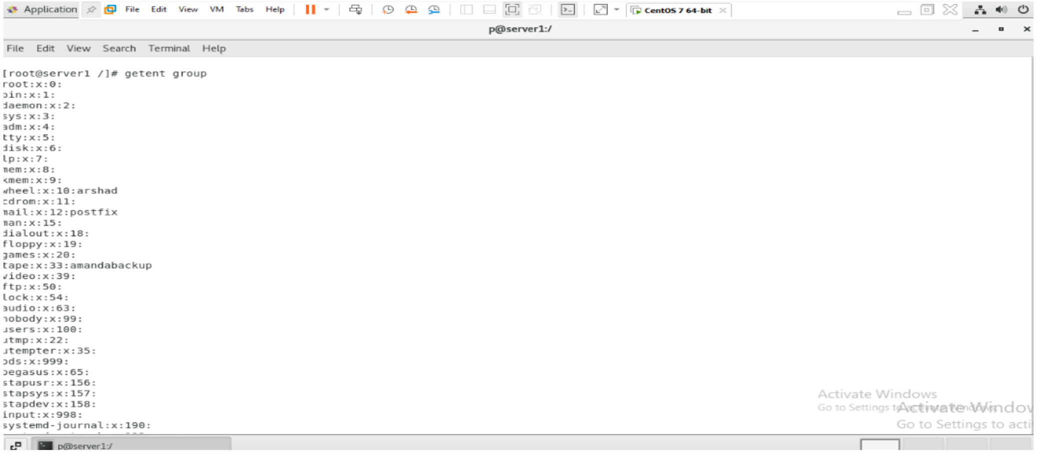
Also we can change the shell by using this command **# chsh spiderman** and enter shell.

Command To Delete a User

# userdel –r username

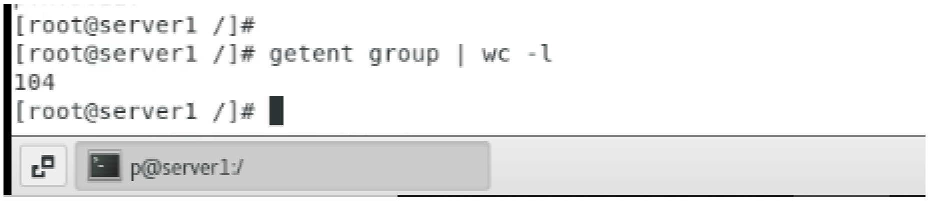
Group

#getent group --> Lo list all group


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
p@server1:/
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
p@server1:/

```
[root@server1 /]# getent group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:arshad
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:amandabackup
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
ods:x:999:
pegasus:x:65:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
input:x:998:
systemd-journal:x:190:
```

#getent group | wc –l --> To get count

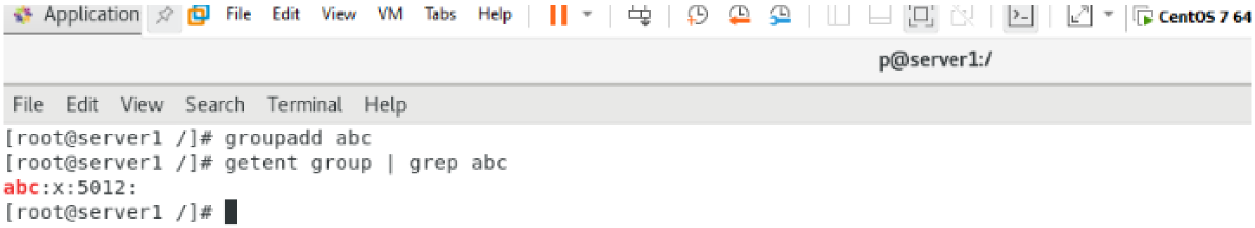


```
[root@server1 /]#
[root@server1 /]# getent group | wc -l
104
[root@server1 /]# █
```

#groupadd groupname --> To create a group

Eg : - #groupadd abc

#gentent group | group abc--> To filter the specific group

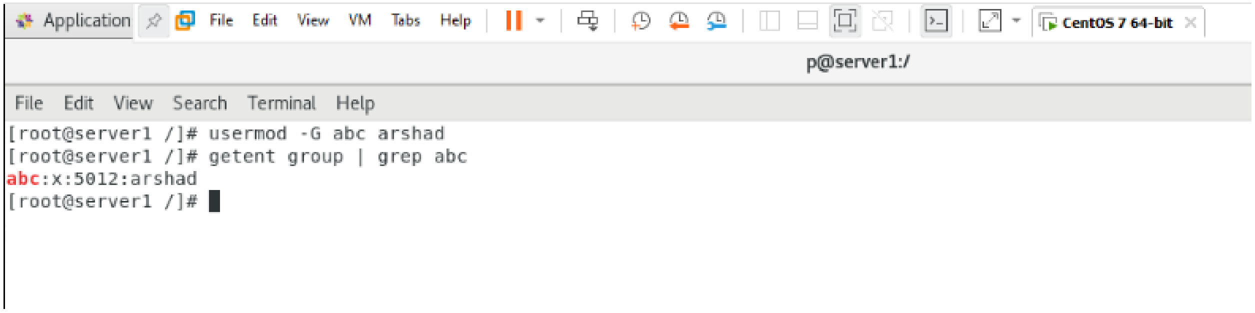


Application
File Edit View VM Tabs Help
CentOS 7 64
p@server1:/
File Edit View Search Terminal Help

```
[root@server1 /]# groupadd abc
[root@server1 /]# getent group | grep abc
abc:x:5012:
[root@server1 /]# █
```

To add Users to the group : **# usermod –G groupname username**

Eg : usermod –G abc arshad



Application
File Edit View VM Tabs Help
CentOS 7 64-bit
p@server1:/
File Edit View Search Terminal Help

```
[root@server1 /]# usermod -G abc arshad
[root@server1 /]# getent group | grep abc
abc:x:5012:arshad
[root@server1 /]# █
```

Command to add users to group while creating

#useradd –G groupname username

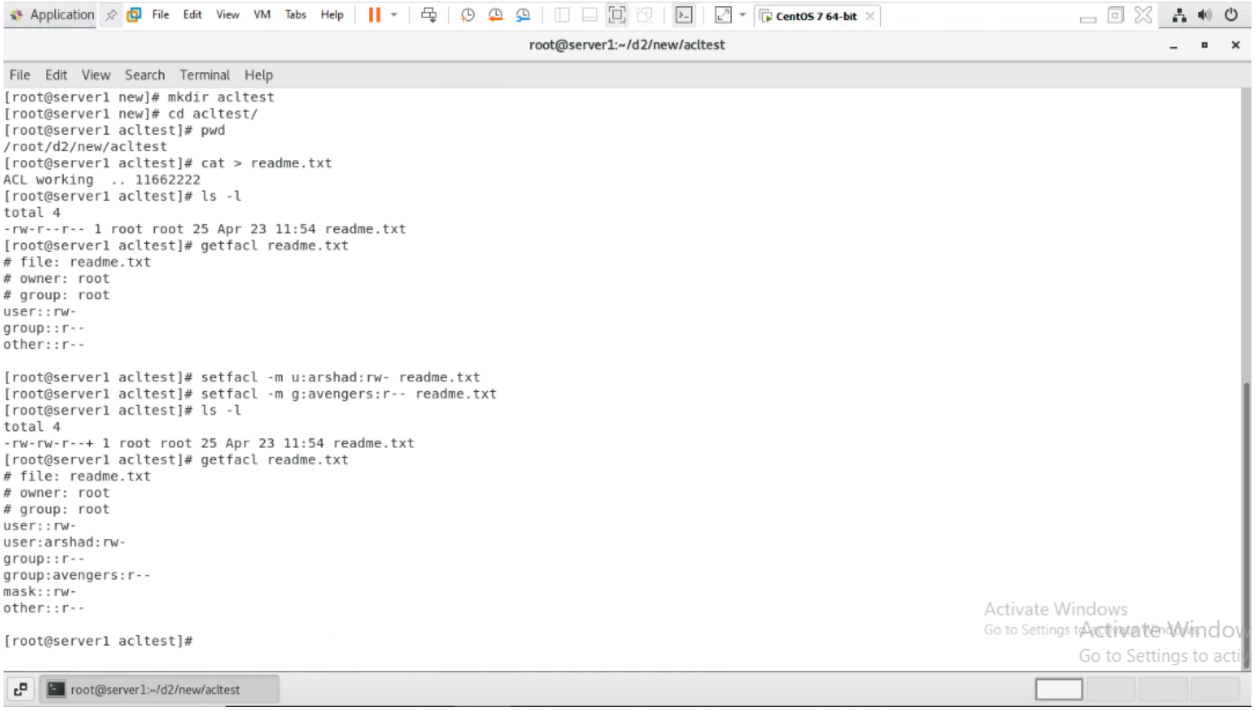
ACL – ACCESS CONTROL LIST

- It allows more grandular level permission to applied for a user or a group
- Commands are #getfacl and #setfacl
- #getfacl filename
- For users : #setfacl –m u:<username>:<permission> filename
- For groups : # setfacl –m g:<groupname>:<permission> filename

To remove ACL from a user or file:

#setfacl –b filename

TASK 1



```
[root@server1 new]# mkdir acltest
[root@server1 new]# cd acltest/
[root@server1 acltest]# pwd
/root/d2/new/acltest
[root@server1 acltest]# cat > readme.txt
ACL working  .. 11662222
[root@server1 acltest]# ls -l
total 4
-rw-r--r-- 1 root root 25 Apr 23 11:54 readme.txt
[root@server1 acltest]# getfacl readme.txt
# file: readme.txt
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@server1 acltest]# setfacl -m u:arshad:rw- readme.txt
[root@server1 acltest]# setfacl -m g:avengers:r-- readme.txt
[root@server1 acltest]# ls -l
total 4
-rw-rw-r--+ 1 root root 25 Apr 23 11:54 readme.txt
[root@server1 acltest]# getfacl readme.txt
# file: readme.txt
# owner: root
# group: root
user::rw-
user:arshad:rw-
group::r--
group:avengers:r--
mask::rw-
other::r--

[root@server1 acltest]#
```

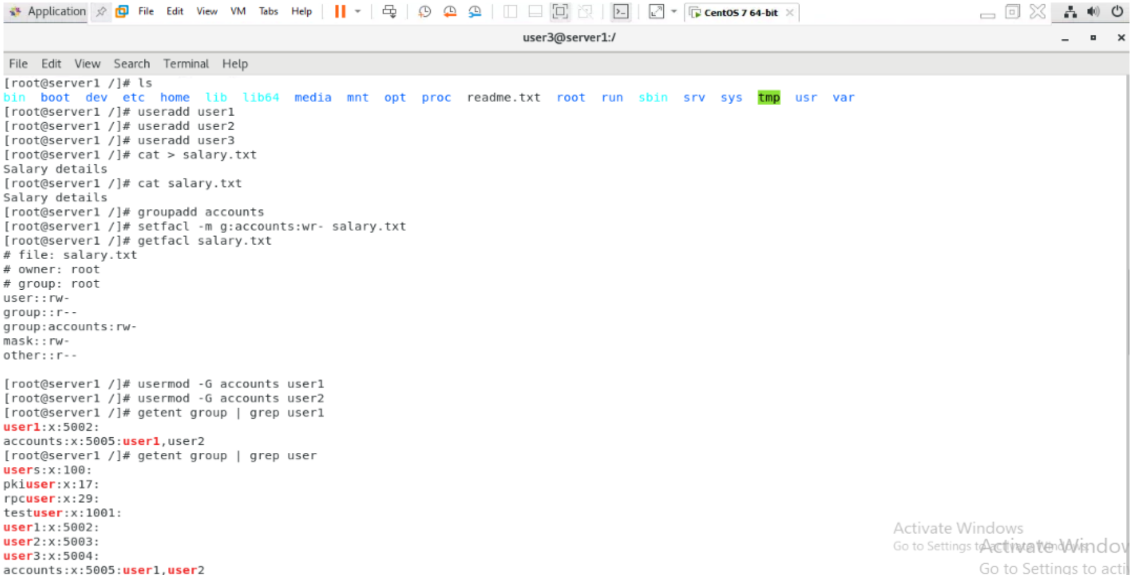
Here we created acl for file named readme.txt

TASK 2

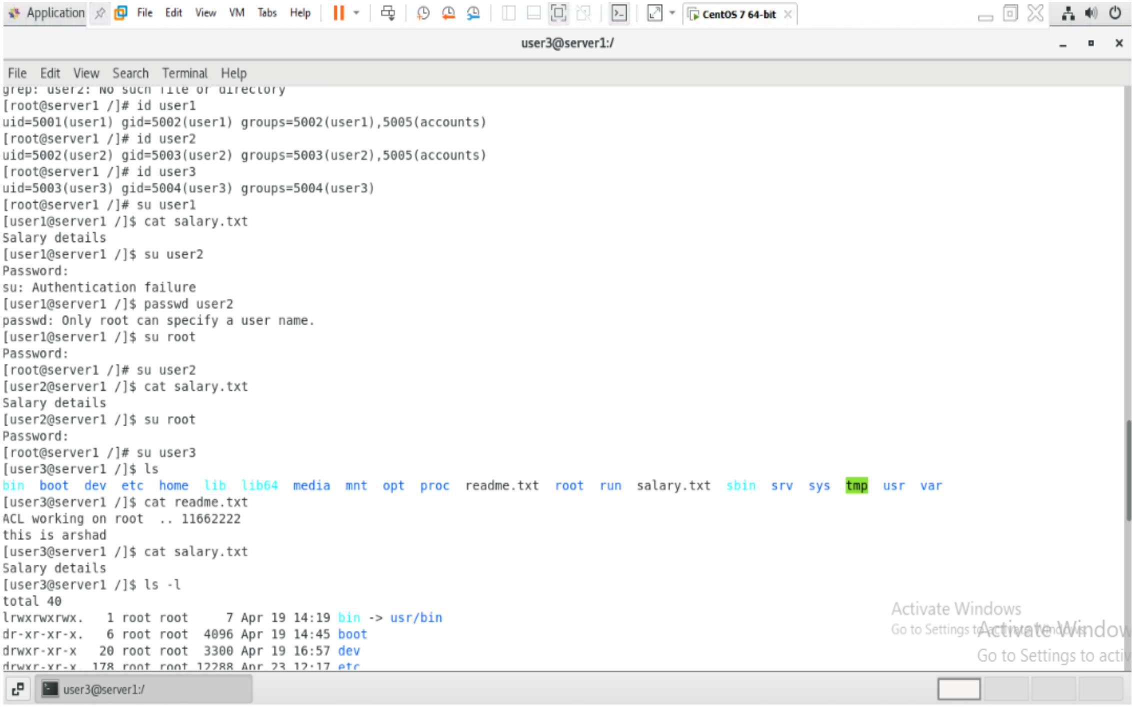
Here we need to create a file called /salary.txt . And Create a group called accounts

Create 3 users , and add 2 users into accounts .

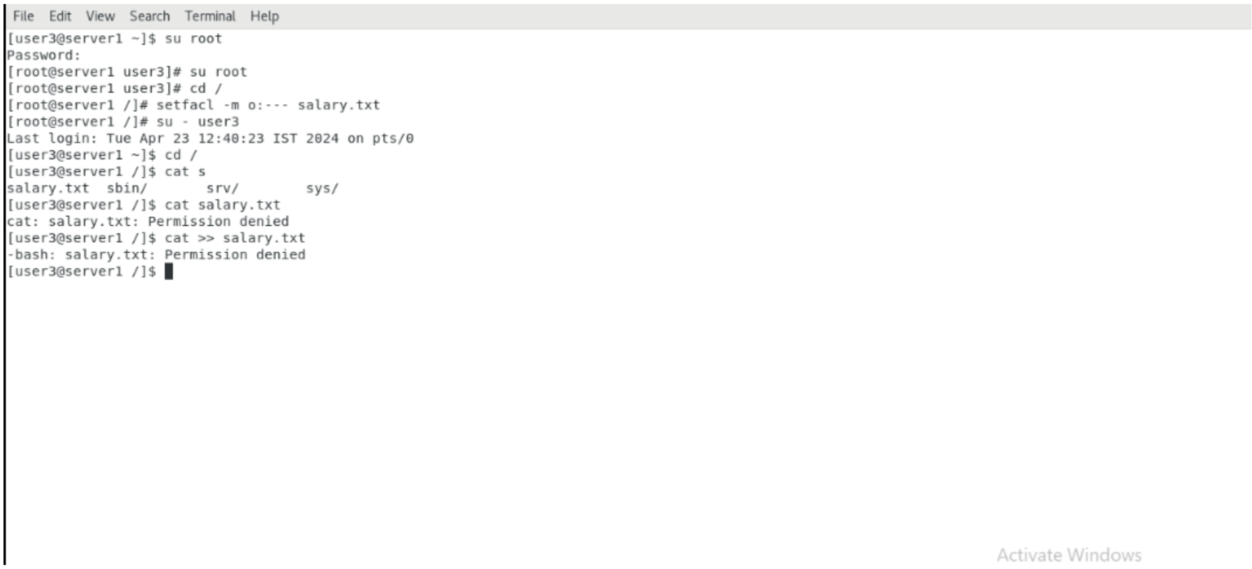
Gave read and write permission to accounts group (for salary.txt) and other user cannot acces the salary.txt


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
user3@server1:/
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.

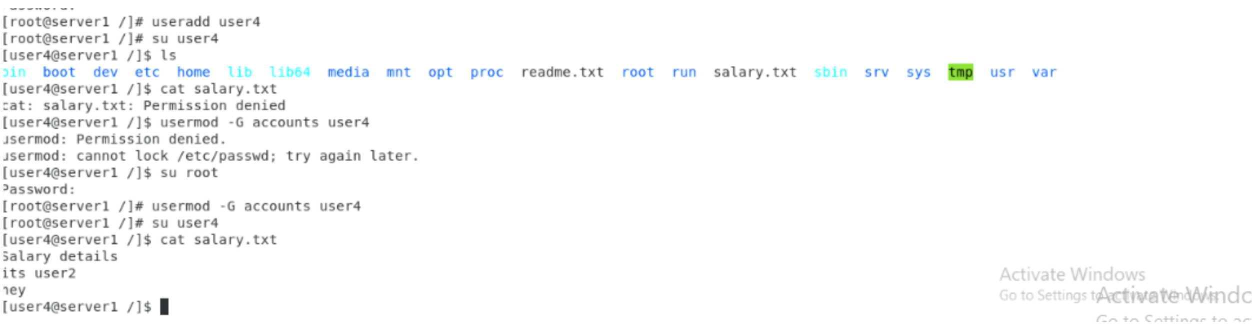
```
[root@server1 /]# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  readme.txt  root  run  sbin  srv  sys  tmp  usr  var
[root@server1 /]# useradd user1
[root@server1 /]# useradd user2
[root@server1 /]# useradd user3
[root@server1 /]# cat > salary.txt
Salary details
[root@server1 /]# cat salary.txt
Salary details
[root@server1 /]# groupadd accounts
[root@server1 /]# setfacl -m g:accounts:wr- salary.txt
[root@server1 /]# getfacl salary.txt
# file: salary.txt
# owner: root
# group: root
user::rw-
group::r--
group:accounts:rw-
mask::rw-
other::r--

[root@server1 /]# usermod -G accounts user1
[root@server1 /]# usermod -G accounts user2
[root@server1 /]# getent group | grep user1
user1:x:5002:
accounts:x:5005:user1,user2
[root@server1 /]# getent group | grep user
users:x:100:
pkiuser:x:17:
rpcuser:x:29:
testuser:x:1001:
user1:x:5002:
user2:x:5003:
user3:x:5004:
accounts:x:5005:user1,user2
```


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
user3@server1:/
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
user3@server1:/

```
grep: user2: No such file or directory
[root@server1 /]# id user1
uid=5001(user1) gid=5002(user1) groups=5002(user1),5005(accounts)
[root@server1 /]# id user2
uid=5002(user2) gid=5003(user2) groups=5003(user2),5005(accounts)
[root@server1 /]# id user3
uid=5003(user3) gid=5004(user3) groups=5004(user3)
[root@server1 /]# su user1
[user1@server1 /]$ cat salary.txt
Salary details
[user1@server1 /]$ su user2
Password:
su: Authentication failure
[user1@server1 /]$ passwd user2
passwd: Only root can specify a user name.
[user1@server1 /]$ su root
Password:
[root@server1 /]# su user2
[user2@server1 /]$ cat salary.txt
Salary details
[user2@server1 /]$ su root
Password:
[root@server1 /]# su user3
[user3@server1 /]$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  readme.txt  root  run  salary.txt  sbin  srv  sys  tmp  usr  var
[user3@server1 /]$ cat readme.txt
ACL working on root  .. 11662222
this is arshad
[user3@server1 /]$ cat salary.txt
Salary details
[user3@server1 /]$ ls -l
total 40
lrwxrwxrwx.   1 root root     7 Apr 19 14:19 bin -> usr/bin
dr-xr-xr-x.   6 root root  4096 Apr 19 14:45 boot
drwxr-xr-x   20 root root  3300 Apr 19 16:57 dev
drwxr-xr-x. 178 root root 12288 Apr 23 12:17 etc
```



```
[user3@server1 ~]$ su root
Password:
[root@server1 user3]# su root
[root@server1 user3]# cd /
[root@server1 /]# setfacl -m o:--- salary.txt
[root@server1 /]# su - user3
Last login: Tue Apr 23 12:40:23 IST 2024 on pts/0
[user3@server1 ~]$ cd /
[user3@server1 /]$ cat s
salary.txt  sbin/       srv/        sys/
[user3@server1 /]$ cat salary.txt
cat: salary.txt: Permission denied
[user3@server1 /]$ cat >> salary.txt
-bash: salary.txt: Permission denied
[user3@server1 /]$ 
```



```
Password:
[root@server1 /]# useradd user4
[root@server1 /]# su user4
[user4@server1 /]$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  readme.txt  root  run  salary.txt  sbin  srv  sys  tmp  usr  var
[user4@server1 /]$ cat salary.txt
cat: salary.txt: Permission denied
[user4@server1 /]$ usermod -G accounts user4
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
[user4@server1 /]$ su root
Password:
[root@server1 /]# usermod -G accounts user4
[root@server1 /]# su user4
[user4@server1 /]$ cat salary.txt
Salary details
its user2
hey
[user4@server1 /]$ 
```

Here we can see that user4 has no permission to access salary.txt file .

Because the user is not a member of group named accounts

Some other special permissions are

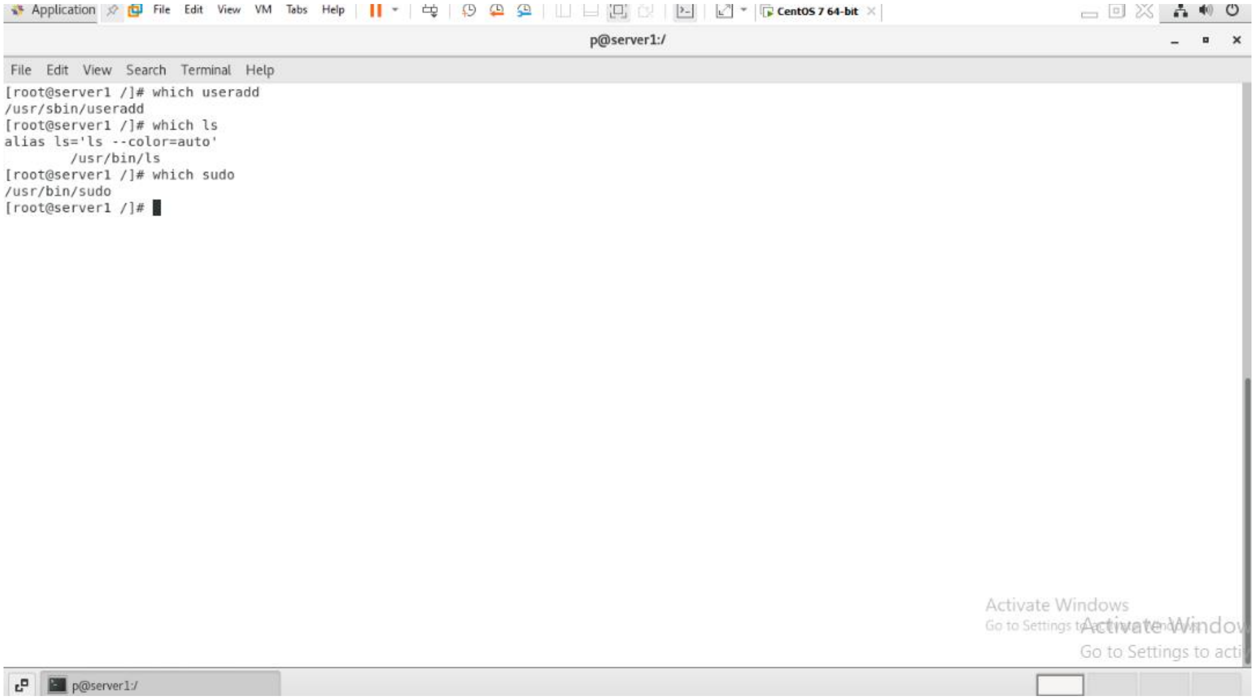
- SUID
- SGID
- Sticky Bit

SUDO USERS

- Super USer
- Its is regular user with limitted root permission
- Like network admins , storage admins , infra admins ....
- File : /etc/sudoers
- Command : #visudo /etc/sudoers

If we need check which user can do a particular command we can use “which” command

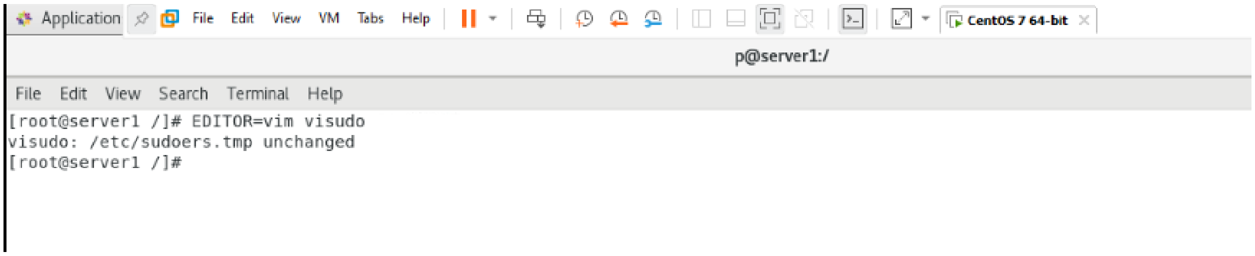
Eg : **# which useradd**



Application
File Edit View VM Tabs Help
CentOS 7 64-bit
p@server1:/
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
p@server1:/

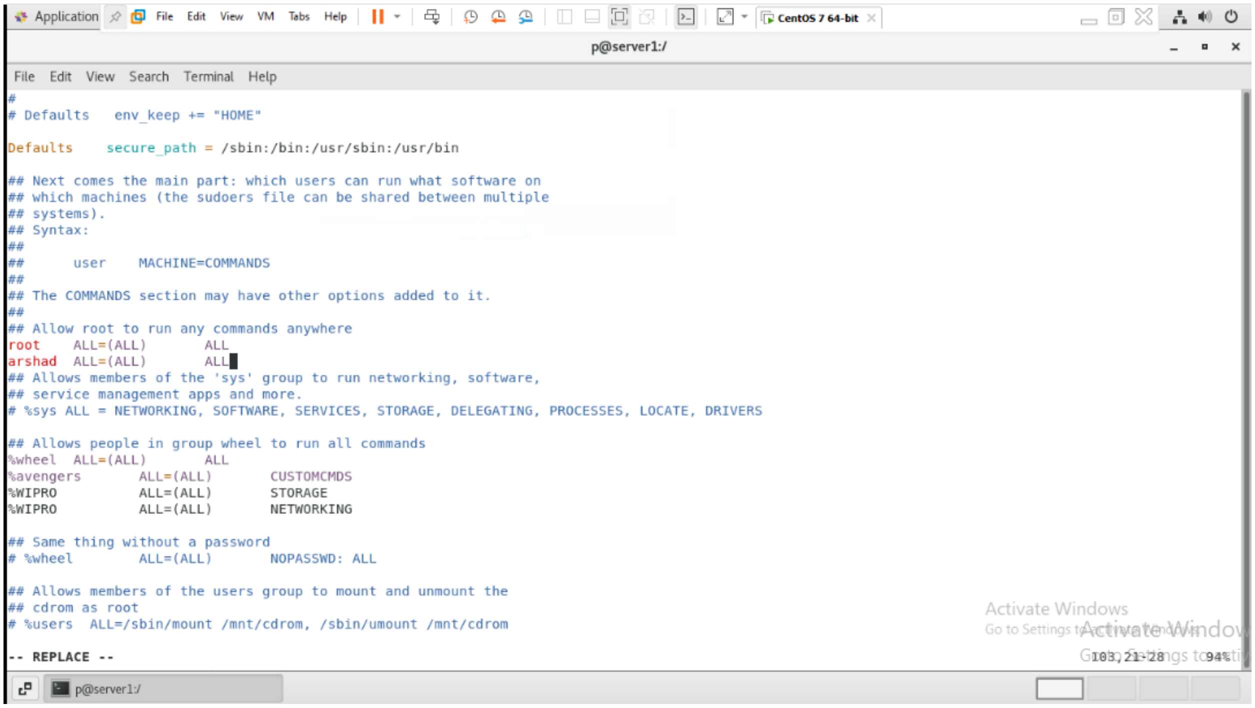
```
[root@server1 /]# which useradd
/usr/sbin/useradd
[root@server1 /]# which ls
alias ls='ls --color=auto'
        /usr/bin/ls
[root@server1 /]# which sudo
/usr/bin/sudo
[root@server1 /]# 
```

To add user into Sudoers File :

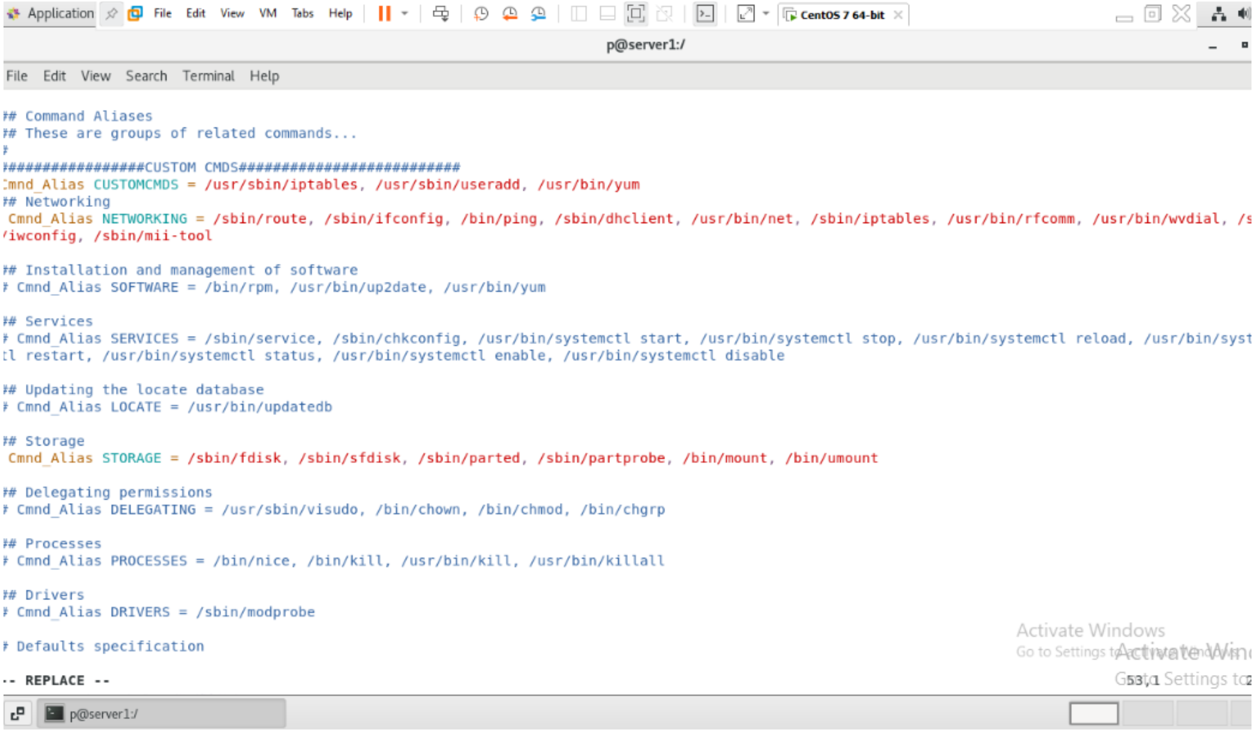


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
p@server1:/
File Edit View Search Terminal Help

```
[root@server1 /]# EDITOR=vim visudo
visudo: /etc/sudoers.tmp unchanged
[root@server1 /]#
```



```
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
arshad  ALL=(ALL)       ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
%avengers       ALL=(ALL)       CUSTOMCMDS
%WIPRO          ALL=(ALL)       STORAGE
%WIPRO          ALL=(ALL)       NETWORKING

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

-- REPLACE --                                                                    103,21-28     94%
```

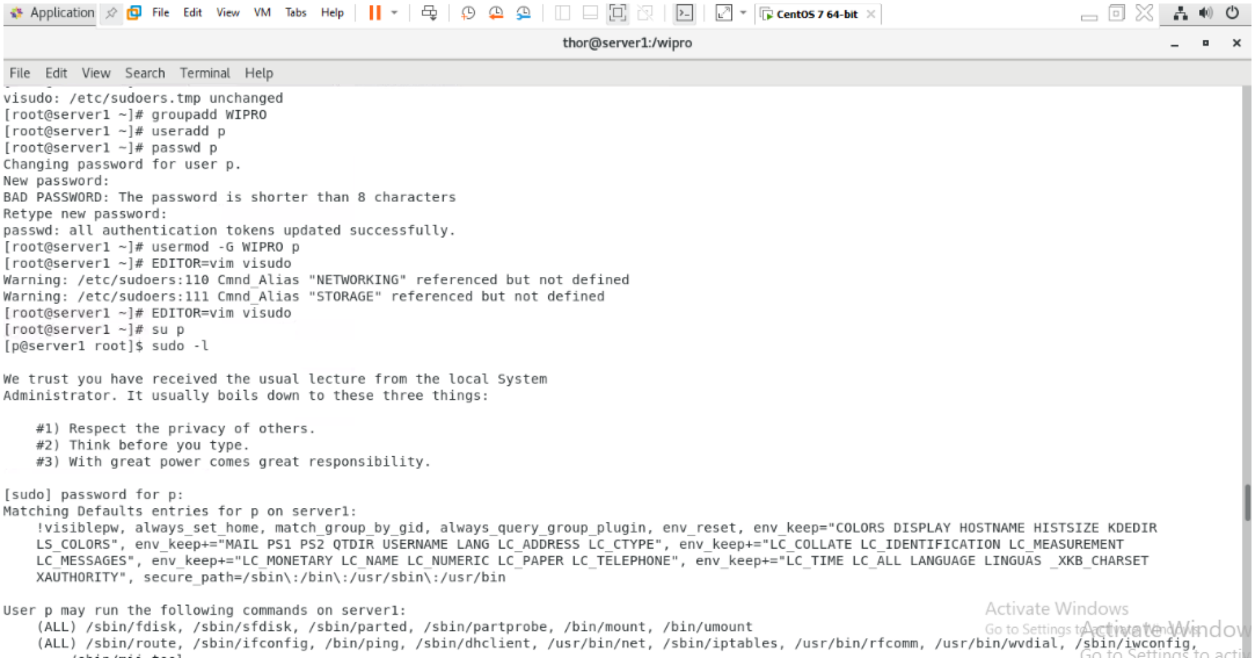


```
## Command Aliases
## These are groups of related commands...
#
################CUSTOM CMDS##########################
Cmnd_Alias CUSTOMCMDS = /usr/sbin/iptables, /usr/sbin/useradd, /usr/bin/yum
## Networking
 Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /s
/iwconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig, /usr/bin/systemctl start, /usr/bin/systemctl stop, /usr/bin/systemctl reload, /usr/bin/syst
ctl restart, /usr/bin/systemctl status, /usr/bin/systemctl enable, /usr/bin/systemctl disable

## Updating the locate database
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
 Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
# Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
# Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification

-- REPLACE --                                                                      53,1
```

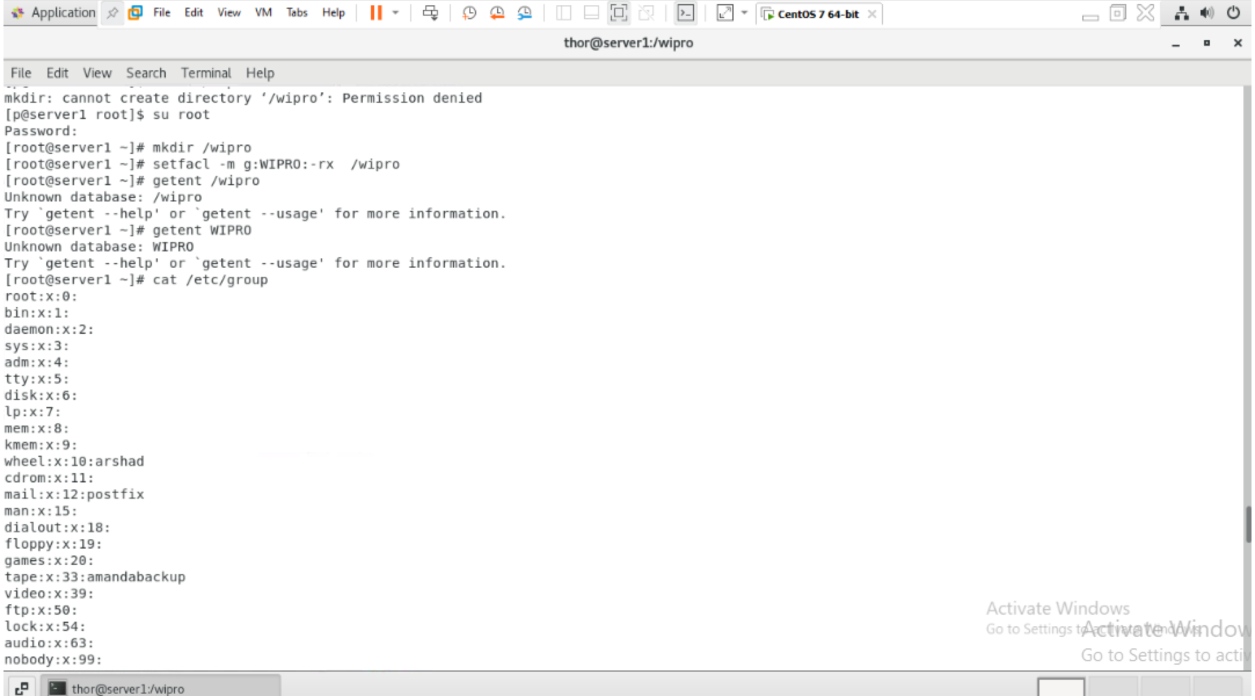
These are multiple ways to into sudoers file .

TASK 3

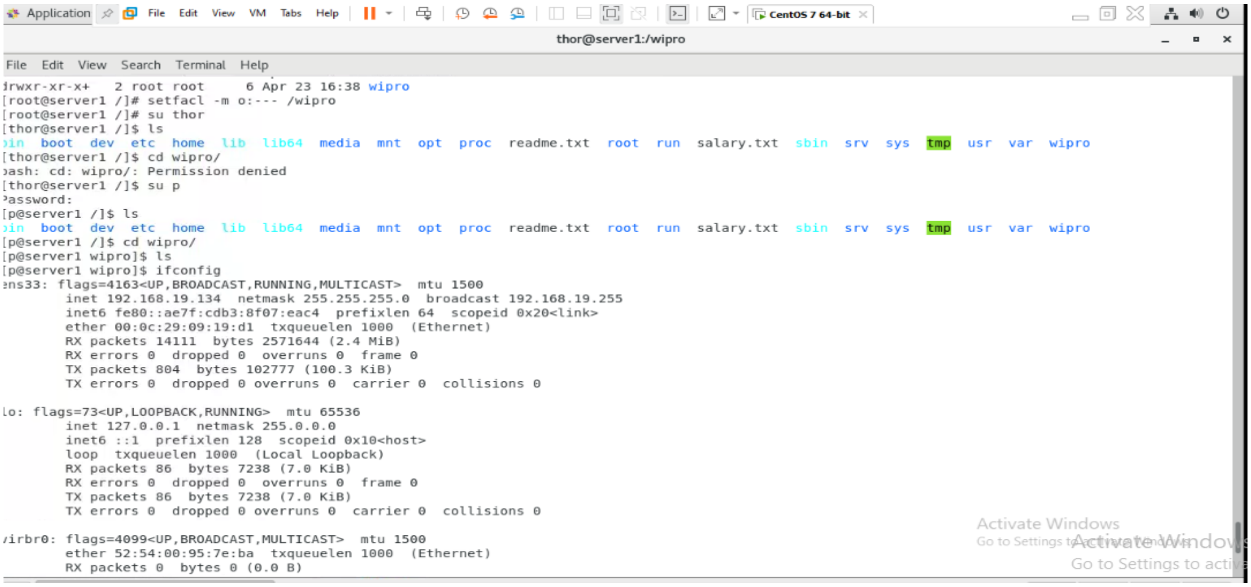
Create a group “wipro” . Create a user with your last name and give WIPRO group networking and storage permissions and verify . Also , create a new folder “/wipro” and allow the access of read & execution on this group and verify.


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
thor@server1:/wipro
File Edit View Search Terminal Help

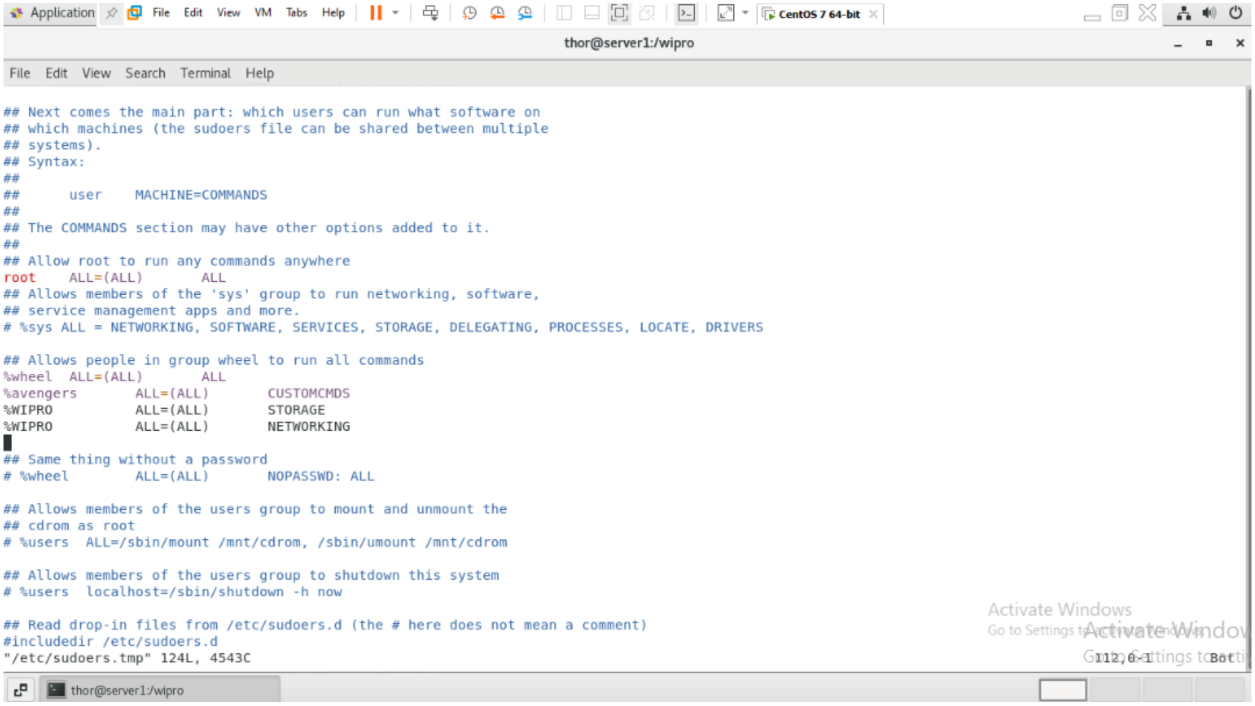
```
visudo: /etc/sudoers.tmp unchanged
[root@server1 ~]# groupadd WIPRO
[root@server1 ~]# useradd p
[root@server1 ~]# passwd p
Changing password for user p.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server1 ~]# usermod -G WIPRO p
[root@server1 ~]# EDITOR=vim visudo
Warning: /etc/sudoers:110 Cmnd_Alias "NETWORKING" referenced but not defined
Warning: /etc/sudoers:111 Cmnd_Alias "STORAGE" referenced but not defined
[root@server1 ~]# EDITOR=vim visudo
[root@server1 ~]# su p
[p@server1 root]$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for p:
Matching Defaults entries for p on server1:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR
    LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
    LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User p may run the following commands on server1:
    (ALL) /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount
    (ALL) /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig,
```



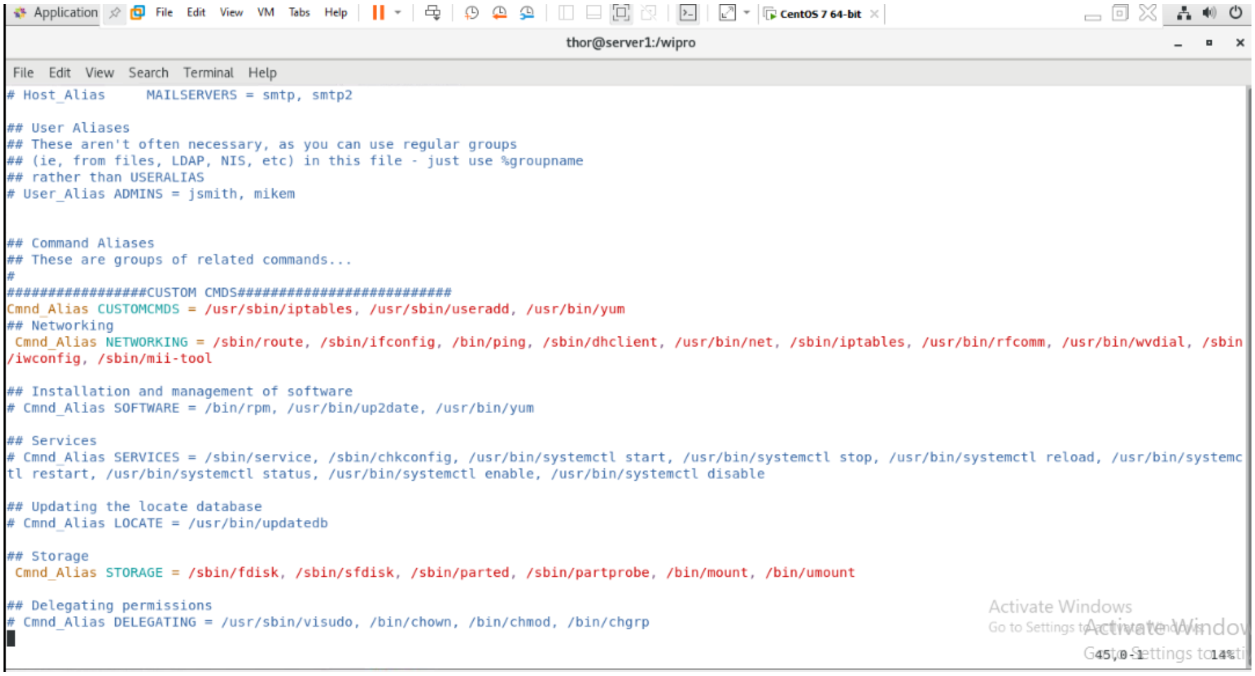
```
mkdir: cannot create directory ‘/wipro’: Permission denied
[p@server1 root]$ su root
Password:
[root@server1 ~]# mkdir /wipro
[root@server1 ~]# setfacl -m g:WIPRO:-rx  /wipro
[root@server1 ~]# getent /wipro
Unknown database: /wipro
Try `getent --help' or `getent --usage' for more information.
[root@server1 ~]# getent WIPRO
Unknown database: WIPRO
Try `getent --help' or `getent --usage' for more information.
[root@server1 ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:arshad
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:amandabackup
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
```


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
thor@server1:/wipro
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.

```
irwxr-xr-x+   2 root root     6 Apr 23 16:38 wipro
[root@server1 /]# setfacl -m o:--- /wipro
[root@server1 /]# su thor
[thor@server1 /]$ ls
oin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  readme.txt  root  run  salary.txt  sbin  srv  sys  tmp  usr  var  wipro
[thor@server1 /]$ cd wipro/
oash: cd: wipro/: Permission denied
[thor@server1 /]$ su p
Password:
[p@server1 /]$ ls
oin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  readme.txt  root  run  salary.txt  sbin  srv  sys  tmp  usr  var  wipro
[p@server1 /]$ cd wipro/
[p@server1 wipro]$ ls
[p@server1 wipro]$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.134  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::ae7f:cdb3:8f07:eac4  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:09:19:d1  txqueuelen 1000  (Ethernet)
        RX packets 14111  bytes 2571644 (2.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 804  bytes 102777 (100.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 86  bytes 7238 (7.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86  bytes 7238 (7.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 52:54:00:95:7e:ba  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
```


Application
File Edit View VM Tabs Help
CentOS 7 64-bit
thor@server1:/wipro
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
thor@server1:/wipro

```

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
%avengers       ALL=(ALL)       CUSTOMCMDS
%WIPRO          ALL=(ALL)       STORAGE
%WIPRO          ALL=(ALL)       NETWORKING

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
"/etc/sudoers.tmp" 124L, 4543C                                                    112,0-1       Bot
```



```
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem


## Command Aliases
## These are groups of related commands...
#
################CUSTOM CMDS#########################
Cmnd_Alias CUSTOMCMDS = /usr/sbin/iptables, /usr/sbin/useradd, /usr/bin/yum
## Networking
 Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin
/iwconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig, /usr/bin/systemctl start, /usr/bin/systemctl stop, /usr/bin/systemctl reload, /usr/bin/systemc
tl restart, /usr/bin/systemctl status, /usr/bin/systemctl enable, /usr/bin/systemctl disable

## Updating the locate database
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
 Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

                                                                                                          45,0-1        14%
```

Here i created the user with lastname called “p” . So only this user can access the wipro directory . Because i did ACL on group “WIPRO”. And user “p” is belongs to that group. If any other user is trying to do any task using the directory , they will got the error “permission denied” .