

# FILE PERMISSION -ACL - SUDO ACCESS

## To Assign or change Permission

```
root@localhost:~# touch
touch: missing file operand
Try 'touch --help' for more information.
root@localhost:~# touch 1
root@localhost:~# ls
1 anaconda-ks.cfg initial-setup-ks.cfg
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# mkdir 2
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 root root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chmod -R 755 1
root@localhost:~# ls -ll
total 8
-rwxr-xr-x. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 root root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chmod -R 000 1
root@localhost:~# ls -ll
ls: cannot access '1': No such file or directory
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 root root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chown -R vivek:root 2
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 vivek root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chown -R vivek:vivekgroup 2
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 vivek vivekgroup 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~#
```

S

## To change user & group ownership using chown command

```
root@localhost:~# ls -ll
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# mkdir 2
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 root root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chmod -R 755 1
root@localhost:~# ls -ll
total 8
-rwxr-xr-x. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 root root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chmod -R 000 1
root@localhost:~# ls -ll
ls: cannot access '1': No such file or directory
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 root root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# chown -R vivek:root 2
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 vivek root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~# umask
0022
root@localhost:~# chgrp root 2
root@localhost:~# ls -ll
total 8
-rw-r--r--. 1 root root 0 Feb 7 05:38 1
drwxr-xr-x. 2 vivek root 6 Feb 7 05:39 2
-rw-r--r--. 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r--. 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
root@localhost:~#
```

## Changing group ownership using chgrp command

```
[root@localhost /]# chgrp vivekgroup vivek
[root@localhost /]# ls -ll
total 25
lrwxrwxrwx. 1 root root 7 Aug 12 2018 bin -> usr/bin
dr-xr-xr-x. 5 root root 4096 Jan 20 06:47 boot
drwxr-xr-x. 20 root root 3360 Feb 8 02:10 dev
drwxr-xr-x. 139 root root 8192 Feb 8 02:20 etc
drwxr-xr-x. 6 root root 57 Feb 8 02:17 home
lrwxrwxrwx. 1 root root 7 Aug 12 2018 lib -> usr/lib
lrwxrwxrwx. 1 root root 9 Aug 12 2018 lib64 -> usr/lib64
drwxr-xr-x. 2 root root 6 Aug 12 2018 media
drwxr-xr-x. 3 root root 18 Jan 20 06:39 mnt
drwxr-xr-x. 2 root root 6 Aug 12 2018 opt
dr-xr-xr-x. 267 root root 0 Feb 8 02:10 proc
drwxr-xr-x. 2 root root 6 Feb 7 01:57 quota
dr-xr-x---. 6 root root 256 Feb 8 02:09 root
drwxr-xr-x. 42 root root 1200 Feb 8 02:10 run
lrwxrwxrwx. 1 root root 8 Aug 12 2018 sbin -> usr/sbin
drwxr-xr-x. 2 root root 6 Aug 12 2018 srv
dr-xr-xr-x. 13 root root 0 Feb 8 02:10 sys
drwxrwxrwt. 27 root root 4096 Feb 8 02:20 tmp
drwxr-xr-x. 12 root root 144 Jan 20 06:34 usr
drwxr-xr-x. 21 root root 4096 Jan 20 06:46 var
drwxrwxrwx. 3 root vivekgroup 1024 Feb 7 06:25 vivek
```

```
pooja@localhost:vivek
[root@localhost vivek]# rm 2
rm: remove regular empty file '2'? y
[root@localhost vivek]# rm -f 3
[root@localhost vivek]# rm -f 4
[root@localhost vivek]# rm -f 5
[root@localhost vivek]# su vivek
[vivek@localhost vivek]$ cd /vivek
[vivek@localhost vivek]$ touch 1 3
[vivek@localhost vivek]$ ls -ll
total 29
-rw-rw-r--. 1 vivek vivekgroup 0 Feb 8 02:30 1
-rw-rw-r--. 1 vivek vivekgroup 0 Feb 8 02:30 3
-rwxrwxrwx. 1 root root 6144 Feb 7 06:55 aquota.group
-rwxrwxrwx. 1 root root 7168 Feb 7 06:55 aquota.user
drwxrwxrwx. 2 root root 12288 Feb 7 06:20 aquota.user
[vivek@localhost vivek]$ su pooja
password:
[pooja@localhost vivek]$ cd /vivek
[pooja@localhost vivek]$ touch 2 4
[pooja@localhost vivek]$ ls -ll
total 31
-rw-rw-r--. 1 vivek vivekgroup 0 Feb 8 02:30 1
-rw-rw-r--. 1 pooja vivekgroup 0 Feb 8 02:30 2
-rw-rw-r--. 1 pooja vivekgroup 0 Feb 8 02:30 3
-rw-rw-r--. 1 pooja vivekgroup 0 Feb 8 02:30 4
-rwxrwxrwx. 1 root root 6144 Feb 7 06:55 aquota.group
-rwxrwxrwx. 1 root root 7168 Feb 7 06:55 aquota.user
drwxrwxrwx. 2 root root 12288 Feb 7 06:20 aquota.user
[pooja@localhost vivek]$ rm 2
[pooja@localhost vivek]$ ls -ll
total 30
-rw-rw-r--. 1 vivek vivekgroup 0 Feb 8 02:30 1
-rw-rw-r--. 1 vivek vivekgroup 0 Feb 8 02:30 3
-rw-rw-r--. 1 pooja vivekgroup 0 Feb 8 02:30 4
-rwxrwxrwx. 1 root root 6144 Feb 7 06:55 aquota.group
-rwxrwxrwx. 1 root root 7168 Feb 7 06:55 aquota.user
drwxrwxrwx. 2 root root 12288 Feb 7 06:20 aquota.user
[pooja@localhost vivek]$ touch 2
[pooja@localhost vivek]$ rm 1
rm: remove write-protected regular empty file '1'? y
[pooja@localhost vivek]$ ls -ll
total 30
-rw-rw-r--. 1 pooja vivekgroup 0 Feb 8 02:31 2
-rw-rw-r--. 1 vivek vivekgroup 0 Feb 8 02:30 3
-rw-rw-r--. 1 pooja vivekgroup 0 Feb 8 02:30 4
-rwxrwxrwx. 1 root root 6144 Feb 7 06:55 aquota.group
-rwxrwxrwx. 1 root root 7168 Feb 7 06:55 aquota.user
drwxrwxrwx. 2 root root 12288 Feb 7 06:20 aquota.user
[pooja@localhost vivek]$
```

## To change the existing umask use the following command

```
[root@localhost ~]# umask
0022
[root@localhost ~]# umask 0077
[root@localhost ~]# umask
0077
[root@localhost ~]# umask 0022
[root@localhost ~]# umask
0022
[root@localhost ~]#
```

## FILE PERMISSION -ACL - SUDO ACCESS

### SPECIAL PERMISSIONS OR ADVANCED PERMISSION

#### SUID – SET USER ID

To set and unset setuid bit on init command

```
[root@localhost ~]# ls -lh
total 10K
drwxr-xrwx. 3 root root 1.0K Feb  9 03:58 acl
-rw----- 1 root root 1.4K Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1.6K Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 21 Feb  9 03:56 sudocopy
drwxrwxr-x+ 2 root root  6 Feb  8 21:40 vivek
[root@localhost ~]# chmod g+s acl
[root@localhost ~]# ls -lh
total 10K
drwxr-srwx. 3 root root 1.0K Feb  9 03:58 acl
-rw----- 1 root root 1.4K Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1.6K Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 21 Feb  9 03:56 sudocopy
drwxrwxr-x+ 2 root root  6 Feb  8 21:40 vivek
[root@localhost ~]# chmod g-s acl
[root@localhost ~]# ls -lh
total 10K
drwxr-xrwx. 3 root root 1.0K Feb  9 03:58 acl
-rw----- 1 root root 1.4K Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1.6K Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x. 2 root root 21 Feb  9 03:56 sudocopy
drwxrwxr-x+ 2 root root  6 Feb  8 21:40 vivek
[root@localhost ~]#
```

#### SGID – SET GROUP ID

```
p@localhost/home
bash-4.4$ ping 192.168.22.13
bash: /usr/sbin/ping: Permission denied
bash-4.4$ ping 192.168.22.13 -t
bash: /usr/sbin/ping: Permission denied
bash-4.4$ su root
Password:
[root@localhost home]# chmod u+s /usr/bin/ping
[root@localhost home]# ls -l /usr/bin/ping
-rwsr-xr-x. 1 root root 80136 Jul 10 2019 /usr/bin/ping
[root@localhost home]# su p
[p@localhost home]# ping 192.168.133.2
bash: /usr/sbin/ping: Permission denied
[p@localhost home]# ls -l
total 4
drwx----- 3 p p 78 Feb  8 04:12 p
drwx----- 15 vgandhi vgandhi 4096 Feb  8 03:35 vgandhi
drwxr-xr-x. 2 root root  6 Feb  8 03:40 vivek
[p@localhost home]# su root
Password:
[root@localhost home]# chmod 0+x /usr/bin/ping
chmod: invalid mode: '0+x'
Try 'chmod --help' for more information.
[root@localhost home]# chmod o+x /usr/bin/ping
[root@localhost home]# ls -l /usr/bin/ping
-rwsr-xr-x. 1 root root 80136 Jul 10 2019 /usr/bin/ping
[root@localhost home]# su p
[p@localhost home]# ping 192.168.222.33
PING 192.168.222.33 (192.168.222.33) 56(84) bytes of data:
From 192.168.254.2 icmp_seq=1 Destination Net Unreachable
From 192.168.254.2 icmp_seq=2 Destination Net Unreachable
From 192.168.254.2 icmp_seq=3 Destination Net Unreachable
From 192.168.254.2 icmp_seq=4 Destination Net Unreachable
From 192.168.254.2 icmp_seq=5 Destination Net Unreachable
From 192.168.254.2 icmp_seq=6 Destination Net Unreachable
^C
--- 192.168.222.33 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 115ms

[p@localhost home]# su root
Password:
[root@localhost home]# ls
p vgandhi vivek
[root@localhost home]# chown -R root:root vgandhi
[root@localhost home]# ls -lh
total 4.0K
drwx----- 3 p p 78 Feb  8 04:12 p
drwx----- 15 root root 4.0K Feb  8 03:35 vgandhi
drwxr-xr-x. 2 root root  6 Feb  8 03:40 vivek
[root@localhost home]#
```

## STICKY BIT

```
vivek@localhost/vivek
[vivek@localhost vivek]$ touch 1 6
[vivek@localhost vivek]$ chmod o+t vivek
chmod: cannot access 'vivek': No such file or directory
[vivek@localhost vivek]$ cd /
[vivek@localhost /]$ chmod o+t vivek
chmod: changing permissions of 'vivek': Operation not permitted
[vivek@localhost /]$ su root
Password:
[root@localhost /]# chmod o+t vivek
[root@localhost /]# ls -ll
total 25
drwxrwxr-x. 1 root root      7 Aug 12 2018 bin -> usr/bin
dr-xr-xr-x. 5 root root    4096 Jan 20 06:47 boot
drwxr-xr-x. 20 root root    3360 Feb  8 02:10 dev
drwxr-xr-x. 139 root root   8192 Feb  8 02:20 etc
drwxr-xr-x. 6 root root      57 Feb  8 02:17 home
lrwxrwxrwx. 1 root root      7 Aug 12 2018 lib -> usr/lib
lrwxrwxrwx. 1 root root     9 Aug 12 2018 lib64 -> usr/lib64
drwxr-xr-x. 2 root root      6 Aug 12 2018 media
drwxr-xr-x. 3 root root     18 Jan 20 06:39 mnt
drwxr-xr-x. 2 root root      6 Aug 12 2018 opt
dr-xr-xr-x. 255 root root    0 Feb  8 02:10 proc
drwxr-xr-x. 2 root root      6 Feb  7 01:57 quota
dr-xr-xr-x. 6 root root     256 Feb  8 02:09 root
drwxr-xr-x. 42 root root   1200 Feb  8 02:10 run
lrwxrwxrwx. 1 root root      8 Aug 12 2018/sbin -> usr/sbin
drwxr-xr-x. 2 root root      6 Aug 12 2018 srv
dr-xr-xr-x. 13 root root    0 Feb  8 02:10 sys
drwxrwxrwt. 28 root root   4096 Feb  8 02:37 tmp
drwxr-xr-x. 12 root root     144 Jan 20 06:34 usr
drwxr-xr-x. 21 root root   4096 Jan 20 06:46 var
drwxrwxrwt. 3 root vivekgroup 1024 Feb  8 02:35 vivek
[root@localhost /]# su vivek
[vivek@localhost /]# cd vivek
[vivek@localhost vivek]$ ls
1 2 3 4 6 aquota.group aquota.user
[vivek@localhost vivek]$ ls -ll
total 32
-rw-rw-r--. 1 vivek vivekgroup 0 Feb  8 02:35 1
-rw-rw-r--. 1 pooja vivekgroup 0 Feb  8 02:31 2
-rw-rw-r--. 1 vivek vivekgroup 0 Feb  8 02:30 3
-rw-rw-r--. 1 pooja vivekgroup 0 Feb  8 02:30 4
-rw-rw-r--. 1 vivek vivekgroup 0 Feb  8 02:35 6
-rwxrwxrwx. 1 root root      6144 Feb  7 06:55 aquota.group
-rwxrwxrwx. 1 root root      7168 Feb  7 06:55 aquota.user
drwxrwxrwx. 2 root root    12288 Feb  7 06:20
[vivek@localhost vivek]$ rm 2
rm: cannot remove '2': Operation not permitted
[vivek@localhost vivek]$
```



## ACCESS CONTROL LIST (ACL)

### Create a partition and format it with ext4 file system

```
[root@localhost home]# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sr0                  11:0    1   7.9G  0  rom
nvme0n1             259:0    0   20G  0  disk
├─nvme0n1p1         259:1    0    1G  0  part /boot
├─nvme0n1p2         259:2    0   19G  0  part
│   └─rhel-root     253:0    0   17G  0  lvm  /
│       └─rhel-swap  253:1    0    2G  0  lvm  [SWAP]
└─nvme0n2           259:3    0    1G  0  disk
[root@localhost home]# fdisk /dev/nvme0n2

Welcome to fdisk (util-linux 2.32.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-2097151, default 2048):
Last sector, +sectors or +size[K,M,G,T,P] (2048-2097151, default 2097151): +100M

Created a new partition 1 of type 'Linux' and of size 100 MiB.
Partition #1 contains a linux_raid_member signature.

Do you want to remove the signature? [Y]es/[N]o: y

The signature will be removed by a write command.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

[root@localhost home]# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sr0                  11:0    1   7.9G  0  rom
nvme0n1             259:0    0   20G  0  disk
├─nvme0n1p1         259:1    0    1G  0  part /boot
├─nvme0n1p2         259:2    0   19G  0  part
│   └─rhel-root     253:0    0   17G  0  lvm  /
│       └─rhel-swap  253:1    0    2G  0  lvm  [SWAP]
└─nvme0n2           259:3    0    1G  0  disk
└─nvme0n2p1         259:5    0   100M 0  part
```

### Format disk

```
[root@localhost home]# mkfs.ext4 /dev/nvme0n2p1
mke2fs 1.45.4 (23-Sep-2019)
Creating filesystem with 102400 1k blocks and 25688 inodes
Filesystem UUID: 590471dc-809b-4d6f-88c4-506960d38511
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```

## FILE PERMISSION -ACL - SUDO ACCESS

```

[root@localhost ~]# mkdir acl
[root@localhost ~]# ls
acl  anaconda-ks.cfg  initial-setup-ks.cfg
[root@localhost ~]#

```

## Mount a file system with ACL

```
[root@localhost home]# vim /etc/fstab
```

```
root@localhost:~#  
# /etc/fstab  
# Created by anaconda on Thu Jan 20 06:33:56 2022  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(8), findfs(8), mount(8) and/or blkid(8) for more info.  
#  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
#  
/dev/mapper/rhel-root / xfs defaults 0 0  
UUID=ca31d6d7-94f9-4e81-ba54-8b3415328df7 /boot xfs defaults 0 0  
/dev/mapper/rhel-swap swap swap defaults 0 0  
/dev/nvme0n2p1 /root/acl ext4 defaults,acl 1 1
```

The screenshot shows a terminal window titled "root@localhost:~#" displaying the contents of the "/etc/fstab" file. The file was created by anaconda on Thursday, January 20, 2022 at 06:33:56. It contains several comments explaining the purpose of the file and instructions on how to update it after editing. The main entries define the root filesystem (/dev/mapper/rhel-root) as xfs with default options, the boot partition (identified by UUID ca31d6d7-94f9-4e81-ba54-8b3415328df7) as xfs with default options, the swap space (dev/mapper/rhel-swap) as swap with default options, and the /root directory (on nvme0n2p1) as ext4 with specific options (defaults,acl) and a noatime flag.

```
[root@localhost ~]# vim /etc/fstab
[root@localhost ~]# lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0                  11:0    1    7.9G  0  rom
nvme0n1              259:0    0    20G  0  disk
├─nvme0n1p1          259:1    0     1G  0  part /boot
├─nvme0n1p2          259:2    0    19G  0  part
│   └─rhel-root      253:0    0    17G  0  lvm  /
│       └─rhel-swap   253:1    0     2G  0  lvm  [SWAP]
└─nvme0n2            259:3    0     1G  0  disk
    └─nvme0n2p1      259:5    0   100M  0  part
[root@localhost ~]# mount -a
[root@localhost ~]# lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0                  11:0    1    7.9G  0  rom
nvme0n1              259:0    0    20G  0  disk
├─nvme0n1p1          259:1    0     1G  0  part /boot
├─nvme0n1p2          259:2    0    19G  0  part
│   └─rhel-root      253:0    0    17G  0  lvm  /
│       └─rhel-swap   253:1    0     2G  0  lvm  [SWAP]
└─nvme0n2            259:3    0     1G  0  disk
    └─nvme0n2p1      259:5    0   100M  0  part /root/acl
[root@localhost ~]# partprobe
Warning: Unable to open /dev/sr0 read-write (Read-only file system). /dev/sr0 has been opened read-only.
```

```
[root@localhost ~]# cat /boot/config-4.18.0-193.el8.x86_64 |grep acl
```

```
[root@localhost ~]# rpm -qa |grep acl
libacl-2.2.53-1.el8.x86_64
acl-2.2.53-1.el8.x86_64
```

### To apply or setting the acl use below syntax

```
[root@localhost ~]# setfacl -m u:vivek:rwX acl
[root@localhost ~]# ls -l
total 10
drwxrwxr-x+ 3 root root 1024 Feb  8 21:27 acl
-rw----- 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x 2 root root  6 Feb  8 21:40 vivek
[root@localhost ~]# getfacl acl
# file: acl
# owner: root
# group: root
user::rwX
user:vivek:rwX
group::r-x
mask::rwX
other::r-x
```

### Removing all ACL permissions from a file or directory

```
drwxrwxrwx+ 3 root root 1024 Feb  8 21:27 acl
-rw----- 1 root root 1387 Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1542 Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x 2 root root  6 Feb  8 21:40 vivek
[root@localhost ~]# ls -lh /home
total 4.0K
drwx----- 3 p  p  99 Feb  8 05:12 p
drwx----- 15 root root 4.0K Feb  8 03:35 vgandhi
drwxr-xr-x 2 root root  6 Feb  8 03:40 vivek
[root@localhost ~]# ls -l acl
total 12
drwx----- 2 root root 12288 Feb  8 21:27 lost+found
[root@localhost ~]# setfacl -b acl
[root@localhost ~]# ls -lh
total 9.0K
drwxr-xrwx 3 root root 1.0K Feb  8 21:27 acl
-rw----- 1 root root 1.4K Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1.6K Jan 20 06:48 initial-setup-ks.cfg
drwxr-xr-x 2 root root  6 Feb  8 21:40 vivek
```

### -d displays the default ACL

```
[root@localhost ~]# getfacl -d vivek
# file: vivek
# owner: root
# group: root
```

### Check all details

```
drwxr-xrwx 3 root root 1.0K Feb  8 21:27 acl
-rw----- 1 root root 1.4K Jan 20 06:45 anaconda-ks.cfg
-rw-r--r-- 1 root root 1.6K Jan 20 06:48 initial-setup-ks.cfg
drwxrwxr-x+ 2 root root  6 Feb  8 21:40 vivek
[root@localhost ~]# getfacl vivek
# file: vivek
# owner: root
# group: root
user::rwX
user:vivek:rwX
group::r-x
mask::rwX
other::r-x
```

## FILE PERMISSION -ACL - SUDO ACCESS

### ENHANCED USER SECURITY WITH SUDO

#### Check command

```
[root@localhost home]# sudo -U vivek -l
User vivek is not allowed to run sudo on localhost.
[root@localhost home]#
```

#### First copy sudo file

```
[root@localhost ~]# mkdir sudocopy
[root@localhost ~]# ls
acl  anaconda-ks.cfg  initial-setup-ks.cfg  sudocopy  vivek
[root@localhost ~]# cp -rf /etc/sudoers /root/sudocopy
[root@localhost ~]# ls sudocopy
sudoers
```

#### visudo command to edit this file

```
[root@localhost home]# visudo
visudo: /etc/sudoers.tmp unchanged
```

#### Open visudo open Edit numeric

```
33 # Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig, /usr/bin/systemctl start, /usr/bin/systemctl stop, /usr/bin/
status, /usr/bin/systemctl enable, /usr/bin/systemctl disable
34
35 ## Updating the locate database
36 # Cmnd_Alias LOCATE = /usr/bin/updatedb
37
38 ## Storage
39 # Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount
40
41 ## Delegating permissions
42 # Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp
43
44 ## Processes
45 # Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall
46
47 ## Drivers
:se nu
```

#### users

```
94 ##
95 ##      user      MACHINE=COMMANDS
96 ##
97 ## The COMMANDS section may have other options added to it.
98 ##
99 ## Allow root to run any commands anywhere
100 root    ALL=(ALL)        ALL
101
102 ## Allows members of the 'sys' group to run networking, software,
103 ## service management apps and more.
104 # %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS
105
106 ## Allows people in group wheel to run all commands
107 %wheel  ALL=(ALL)        ALL
108
109 ## Same thing without a password
110 # %wheel    ALL=(ALL)        NOPASSWD: ALL
111
112 ## Allows members of the users group to mount and unmount the
113 ## cdrom as root
114 # %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom
115
116 ## Allows members of the users group to shutdown this system
117 # %users  localhost=/sbin/shutdown -h now
118
119 ## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
120 #includedir /etc/sudoers.d
```



### Different user All access but required password

```
98 ##
99 ## Allow root to run any commands anywhere
100 root    ALL=(ALL)        ALL
101 vivek    ALL=(ALL)        ALL
102 ## Allow members of the wheel group to run any
```

```
[root@localhost home]# su vivek
bash-4.4$ useradd user1
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
bash-4.4$ sudo useradd user1
```

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 vivek:
bash-4.4$ grep user1 /etc/passwd
user1:x:2001:2002::/home/user1:/bin/bash
```

### Different user All access not required password

```
98 ##
99 ## Allow root to run any commands anywhere
100 root    ALL=(ALL)        ALL
101 vivek    ALL=(ALL)        NOPASSWD:    ALL
102
```

```
[root@localhost home]# su vivek
bash-4.4$ sudo useradd vivek1
bash-4.4$ grep user1 /etc/passwd
user1:x:2001:2002::/home/user1:/bin/bash
bash-4.4$ grep user1 /etc/passwd
user1:x:2001:2002::/home/user1:/bin/bash
bash-4.4$ sudo userdel vivek1
bash-4.4$ sudo userdel user1
bash-4.4$ cd /home
bash-4.4$ ls
p  user1  vgandhi  vivek  vivek1
bash-4.4$ rm -rf user1
rm: cannot remove 'user1': Permission denied
bash-4.4$ sudo rm -rf user1
bash-4.4$ sudo rm -rf vivek1
bash-4.4$ ls
p  vgandhi  vivek
```

## Exclude specific commands

```
[root@localhost home]# which useradd
/usr/sbin/useradd
[root@localhost home]# which adduser
/usr/sbin/adduser
[root@localhost home]#
```

```
98 ##
99 ## Allow root to run any commands anywhere
100 root    ALL=(ALL)        ALL
101 vivek   ALL=(ALL)        ALL,!/usr/sbin/useradd,!/usr/sbin/adduser
102
```

```
[root@localhost home]# su vivek
bash-4.4$ sudo useradd vivek2
[sudo] password for vivek:
Sorry, user vivek is not allowed to execute '/sbin/useradd vivek2' as root on localhost.localdomain.
bash-4.4$
```

## Allow specific commands

```
98 ##
99 ## Allow root to run any commands anywhere
100 root    ALL=(ALL)        ALL
101 vivek   ALL=(ALL)        /usr/sbin/useradd,/usr/sbin/adduser
102
```

```
bash-4.4$ sudo useradd us
[sudo] password for vivek:
bash-4.4$ ls
p us vgandhi vivek
bash-4.4$ sudo rm -rf us
Sorry, user vivek is not allowed to execute '/bin/rm -rf us' as root on localhost.localdomain.
bash-4.4$
```

## Sudo for group command with password

```
[root@localhost home]# usermod -G vivekgroup vivek
[root@localhost home]# id vivek
uid=1001(vivek) gid=1001(vivek) groups=1001(vivek),1011(vivekgroup)
```

```
106
107 ## Allows people in group wheel to run all commands
108 %wheel  ALL=(ALL)        ALL
109 %vivekgroup  ALL=(ALL)    ALL
110 ## Same thing without a password
111 # %wheel  ALL=(ALL)        NOPASSWD: ALL
112
113 ## Allows members of the users group to mount and unmount the
114 ## cdrom as root
:wq!
```

## Sudo for group command comment mode

```
105 # %wheel  NETWORKING, CDROM, SERVICES, STORAGE, DEVICES, LUKS,
106
107 ## Allows people in group wheel to run all commands
108 %wheel  ALL=(ALL)        ALL
109 # %vivekgroup  ALL=(ALL)    ALL
110
111 ## Same thing without a password
112 # %wheel  ALL=(ALL)        NOPASSWD: ALL
113
114
```

### Sudo for group command without password

```
106
107 ## Allows people in group wheel to run all commands
108 %wheel  ALL=(ALL)      ALL
109
110 ## Same thing without a password
111 # %wheel      ALL=(ALL)      NOPASSWD: ALL
112 %vivekgroup   ALL=(ALL)      NOPASSWD: ALL
113
```

### Sudo for group command comment mode

```
106
107 ## Allows people in group wheel to run all commands
108 %wheel  ALL=(ALL)      ALL
109
110 ## Same thing without a password
111 # %wheel      ALL=(ALL)      NOPASSWD: ALL
112 # %vivekgroup  ALL=(ALL)      NOPASSWD: ALL
113
```

### Command alias

```
[root@localhost home]# useradd a1
[root@localhost home]# passwd a1
Changing password for user a1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost home]# which chown
/usr/bin/chown
[root@localhost home]# which chmod
/usr/bin/chmod
[root@localhost home]#
```

```
[root@localhost home]# visudo
```

```
21
22 cmnd_Alias CUSTOM = /usr/bin/chmod, /usr/bin/chown
23
```

```
## Allow root to run any commands anywhere
root    ALL=(ALL)      ALL
a1      ALL=(ALL)      CUSTOM
```

