

ACL (Access Control List)

Standard Linux file permissions are satisfactory when files are used by only a single owner, and a single group of people. However, some use cases require that files are accessed with different file permission sets by multiple users and groups, that time Access Control Lists (ACLs) provide this function.

File systems need to be mounted with ACL support enabled. XFS file systems have built-in ACL support. Other file systems, such as ext3 or ext4 created on Red Hat Enterprise Linux 8, have the `acl` option enabled by default, although on earlier versions you should confirm that ACL support is enabled. To enable file-system ACL support, use the `ACL` option with the `mount` command or in the file system's entry in `/etc/fstab` configuration file.

SYNTAX:

```
#setfacl -m u:<USER>:<PERMISSION> <FILE/DIRECTORY>
    →Set ACL permission for specified user

#setfacl -m g:<GROUP>:<PERMISSION> <FILE/DIRECTORY>
    →Set ACL permission for specified group

#setfacl -x u:<USER>:<PERMISSION> <FILE/DIRECTORY>
    →Remove ACL permission of specified user

#setfacl -x g:<GROUP>:<PERMISSION> <FILE/DIRECTORY>
    →Remove ACL permission of specified group

#setfacl -m u::<PERMISSION> <FILE/DIRECTORY>
    →Set user permission on File Base Permission

#setfacl -m g::<PERMISSION> <FILE/DIRECTORY>
    →Set group permission on File Base Permission

#setfacl -m o::<PERMISSION> <FILE/DIRECTORY>
    →Set Other permission on File Base Permission

#getfacl <FILE/DIRECTORY>
    →Display File's ACL permission
```

EG:

```
[root@servera ~]# mkdir /redhat

[root@servera ~]# ls -ld /redhat/

drwxr-xr-x. 2 root root 6 Jul 22 19:37 /redhat/

[root@servera ~]# getfacl /redhat/
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat/  
# owner: root  
# group: root  
user::rwx  
group::r-x  
other::r-x
```

```
[root@servera ~]# setfacl -m u::r-x /redhat
```

→ *change base permission of user owner*

```
[root@servera ~]# ls -ld /redhat/
```

```
dr-xr-xr-x. 2 root root 6 Jul 22 19:37 /redhat/
```

```
[root@servera ~]# getfacl /redhat/  
getfacl: Removing leading '/' from absolute path names  
# file: redhat/  
# owner: root  
# group: root  
user::r-x  
group::r-x  
other::r-x
```

```
[root@servera ~]# setfacl -m g::r /redhat
```

→ *change base permission of group owner*

```
[root@servera ~]# ls -ld /redhat/
```

```
dr-xr--r-x. 2 root root 6 Jul 22 19:37 /redhat/
```

```
[root@servera ~]# getfacl /redhat/  
getfacl: Removing leading '/' from absolute path names  
# file: redhat/  
# owner: root  
# group: root  
user::r-x  
group::r--  
other::r-x
```

```
[root@servera ~]# setfacl -m o::r /redhat
```

→ *change base permission of other*

```
[root@servera ~]# ls -ld /redhat/
```

```
dr-xr--r--. 2 root root 6 Jul 22 19:37 /redhat/
```

```
[root@servera ~]# getfacl /redhat/  
getfacl: Removing leading '/' from absolute path names  
# file: redhat/  
# owner: root  
# group: root
```

```
user::r-x
group::r--
other::r--
```

USER ACL

EG:

```
[root@servera ~]# ls -ld /redhat/
dr-xr--r--. 2 root root 6 Jul 22 19:37 /redhat/
```

```
[root@servera ~]# chmod 770 /redhat/
[root@servera ~]# ls -ld /redhat/
drwxrwx---. 2 root root 6 Jul 22 19:37 /redhat/
```

```
[root@servera ~]# useradd jack; useradd john ; useradd jerry
[root@servera ~]# tail -1 /etc/passwd
jerry:x:1010:1010::/home/jerry:/bin/bash
```

```
[root@servera ~]# su - jack           → other user for dir /redhat
[jack@servera ~]$ cd /redhat/
-bash: cd: /redhat/: Permission denied
[jack@servera ~]$ exit
logout
```

```
[root@servera ~]# su - john           → other user for dir /redhat
[john@servera ~]$ cd /redhat/
-bash: cd: /redhat/: Permission denied
[john@servera ~]$ exit
logout
```

```
[root@servera ~]# su - jerry          → other user for dir /redhat
[jerry@servera ~]$ cd /redhat/
-bash: cd: /redhat/: Permission denied
[jerry@servera ~]$
```

logout

```
[root@servera ~]# setfacl -m u:jack:rwX /redhat
```

→Applying user ACL on /redhat

```
[root@servera ~]# ls -ld /redhat/
```

```
drwxrwx---+ 2 root root 6 Jul 22 19:37 /redhat/
```

```
[root@servera ~]# getfacl /redhat/
```

```
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat/
```

```
# owner: root
```

```
# group: root
```

```
user::rwX
```

```
user:jack:rwX
```

```
group::rwX
```

```
mask::rwX
```

```
other:---
```

```
[root@servera ~]# su - jack
```

```
[jack@servera ~]$ cd /redhat/ →x permission
```

```
[jack@servera redhat]$ touch abc1 →w permission
```

```
[jack@servera redhat]$ ll →r permission
```

```
total 0
```

```
-rw-r--r--. 1 jack jack 0 Jul 22 19:43 abc1
```

```
[jack@servera redhat]$ exit
```

logout

```
[root@servera ~]# ls -ld /redhat/
```

```
drwxrwx---+ 2 root root 18 Jul 22 19:43 /redhat/
```

```
[root@servera ~]# setfacl -m u:john:r-x,u:jerry:r-- /redhat/
```

```
[root@servera ~]# ls -ld /redhat/
```

```
drwxrwx---+ 2 root root 18 Jul 22 19:43 /redhat/
```

```
[root@servera ~]# getfacl /redhat/
```

```
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat/
```

```
# owner: root
```

```
# group: root
```

```
user::rwX
```

```
user:jack:rwx
user:john:r-x
user:jerry:r--
group::rwx
mask::rwx
other::---
```

```
[root@servera ~]# su - john
```

```
[john@servera ~]$ cd /redhat/      → x permission
```

```
[john@servera redhat]$ ls          → r permission
```

```
abc1
```

```
[john@servera redhat]$ touch sample → w permission
```

```
touch: cannot touch 'sample': Permission denied
```

```
[john@servera redhat]$ exit
```

```
logout
```

```
[root@servera ~]# su - jerry
```

```
[jerry@servera ~]$ cd /redhat/      → x permission
```

```
-sh: cd: /redhat/: Permission denied
```

```
[jerry@servera ~]$ ls /redhat/      → r permission
```

```
ls: cannot access '/redhat/abc1': Permission denied
```

```
abc1
```

```
[jerry@servera ~]$ touch /redhat/test → w permission
```

```
touch: cannot touch '/redhat/test': Permission denied
```

```
[jerry@servera ~]$
```

```
logout
```

-R → Recursive

```
[root@servera ~]# getfacl -R /redhat
```

```
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat/
```

```
# owner: root
```

```
# group: root
```

```
user::rwx
user:jack:rwx
user:john:r-x
user:jerry:r--
group::rwx
mask::rwx
other::---
```

```
# file: redhat/abc1
```

```
# owner: jack
```

```
# group: jack
```

```
user::rw-
```

```
group::r--
```

```
other::r--
```

```
[root@servera ~]# setfacl -Rm u:jerry:rwx /redhat/
```

```
[root@servera ~]# getfacl -R /redhat/
```

```
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat/
```

```
# owner: root
```

```
# group: root
```

```
user::rwx
```

```
user:jack:rwx
```

```
user:john:r-x
```

```
user:jerry:rwx
```

```
group::rwx
```

```
mask::rwx
```

```
other::---
```

```
# file: redhat/abc1
```

```
# owner: jack
```

```
# group: jack
```

```
user::rw-
```

```
user:jerry:rwx
```

```
group::r--
```

```
mask::rwx
```

```
other::r--
```

```
[root@servera ~]# ls -ld /redhat/
```

```
drwxrwx---+ 2 root root 18 Jul 22 19:43 /redhat/
```

```
[root@servera ~]# ls -l /redhat/
```

-rw-rwxr--+ 1 jack jack 0 Jul 22 19:43 abc1

```
[root@servera ~]# getfacl /redhat/
getfacl: Removing leading '/' from absolute path names
# file: redhat/
# owner: root
# group: root
user::rwxuser:jack:rwx
user:john:r-x
user:jerry:rwx
group::rwx
mask::rwx
other::---
```

GROUP ACL

```
[root@servera ~]# groupadd groupA ; groupadd groupB
```

```
[root@servera ~]# tail /etc/passwd
```

```
tom:x:1001:1001::/home/tom:/bin/bash
```

```
ritesh:x:1002:1002::/home/ritesh:/bin/bash
```

```
lukesh:x:1003:1006::/home/lukesh:/bin/bash
```

```
nishant:x:1004:100::/home/nishant:/bin/bash
```

```
sushil:x:1005:1006::/home/sushil:/bin/bash
```

```
[root@servera ~]# gpasswd -M ritesh,lukesh groupA
```

```
[root@servera ~]# gpasswd -M nishant,sushil groupB
```

```
[root@servera ~]# tail -2 /etc/group
```

```
groupA:x:1011:ritesh,lukesh
```

```
groupB:x:1012:nishant,sushil
```

```
[root@servera ~]# su - ritesh → other user
```

```
[ritesh@servera ~]$ cd /redhat/
```

```
-bash: cd: /redhat/: Permission denied
```

```
[ritesh@servera ~]$ exit
```

```
logout
```

[root@servera ~]# **su - sushil** → *other user*

[sushil@servera ~]\$ cd /redhat/

-bash: cd: /redhat/: Permission denied

[sushil@servera ~]\$ exit

logout

[root@servera ~]# **setfacl -m g:groupA:rwx /redhat/**

[root@servera ~]# **getfacl /redhat/**

getfacl: Removing leading '/' from absolute path names

file: redhat/

owner: root

group: root

user::rwx

user:jack:rwx

user:john:r-x

user:jerry:rwx

group::rwx

group:groupA:rwx

mask::rwx

other:---

[root@servera ~]# **su - ritesh** → *Group Member of 'groupA'*

[ritesh@servera ~]\$ cd /redhat/

[ritesh@servera redhat]\$ touch test

[ritesh@servera redhat]\$ ls

abc1 test

[ritesh@servera redhat]\$ exit

logout

[root@servera ~]# **su - lukesh** → *Group Member of 'groupA'*

[lukesh@servera ~]\$ cd /redhat/

[lukesh@servera redhat]\$ touch sample

[lukesh@servera redhat]\$ ll

total 0

-rw-rwxr--+ 1 jack jack 0 Jul 22 19:43 abc1

-rw-r--r-- 1 lukesh sales 0 Jul 23 18:49 sample

-rw-r--r--. 1 ritesh ritesh 0 Jul 23 18:49 test

[lukesh@servera redhat]\$ exit

logout

[root@servera ~]# **setfacl -m u:lukesh:- /redhat**

→ applying user acl to member of group, the priority of permission goes to user ACL in such case

[root@servera ~]# **getfacl /redhat/**
getfacl: Removing leading '/' from absolute path names
file: redhat/
owner: root
group: root
user::rwx
user:lukesh:---
user:jack:rwx
user:john:r-x
user:jerry:rwx
group::rwx
group:groupA:rwx
mask::rwx
other::---

[root@servera ~]# **su - lukesh**

[lukesh@servera ~]\$ **cd /redhat/** → user ACL is working

-bash: cd: /redhat/: Permission denied

[lukesh@servera ~]\$ exit

logout

-R → Recursive

[root@servera ~]# **setfacl -Rm g:groupB:rx /redhat/**

[root@servera ~]# **getfacl -R /redhat/**
getfacl: Removing leading '/' from absolute path names
file: redhat/
owner: root
group: root
user::rwx
user:lukesh:---
user:jack:rwx
user:john:r-x
user:jerry:rwx
group::rwx

```
group:groupA:rwx
group:groupB:r-x
mask::rwx
other::---
```

```
# file: redhat/abc1
# owner: jack
# group: jack
user::rw-
user:jerry:rwx
group::r--
group:groupB:r-x
mask::rwx
other::r--
```

```
# file: redhat/test
# owner: ritesh
# group: ritesh
user::rw-
group::r--
group:groupB:r-x
mask::r-x
other::r--
```

```
# file: redhat/sample
# owner: lukesh
# group: sales
user::rw-
group::r--
group:groupB:r-x
mask::r-x
other::r--
```

```
[root@servera ~]# ls -ld /redhat
```

```
drwxrwx---+ 2 root root 44 Jul 23 18:49 /redhat/
```

```
[root@servera ~]# ls -l /redhat/
```

```
-rw-rwxr--+ 1 jack jack 0 Jul 22 19:43 abc1
```

```
-rw-r-xr--+ 1 lukesh sales 0 Jul 23 18:49 sample
```

```
-rw-r-xr--+ 1 ritesh ritesh 0 Jul 23 18:49 test
```

Remove ACL

SYNTAX:

#setfacl -x u:<username> <file/dir> → remove user ACL

#setfacl -x g:<groupname> <file/dir> → remove group ACL

EG:

```
[root@servera ~]# setfacl -x u:jack /redhat
```

```
[root@servera ~]# getfacl /redhat
```

getfacl: Removing leading '/' from absolute path names

file: redhat

owner: root

group: root

user::rwx

user:luke:---

user:john:r-x

user:jerry:rwx

group::rwx

group:groupA:rwx

group:groupB:r-x

mask::rwx

other::---

```
[root@servera ~]# setfacl -x g:groupA /redhat/
```

```
[root@servera ~]# getfacl /redhat/
```

getfacl: Removing leading '/' from absolute path names

file: redhat/

owner: root

group: root

user::rwx

user:luke:---

user:john:r-x

user:jerry:rwx

group::rwx

group:groupB:r-x

mask::rwx

other::---

```
[root@servera ~]# setfacl -Rx u:luke,g:groupB /redhat → Remove acl recursively
```

```
[root@servera ~]# getfacl -R /redhat
```

getfacl: Removing leading '/' from absolute path names

file: redhat

owner: root

group: root

user::rwx

user:john:r-x

```
user:jerry:rwX
group::rwX
mask::rwX
other::---
```

```
# file: redhat/abc1
# owner: jack
# group: jack
user::rw-
user:jerry:rwX
group::r--
mask::rwX
other::r--
```

```
# file: redhat/test
# owner: ritesh
# group: ritesh
user::rw-
group::r--
mask::r--
other::r--
```

```
# file: redhat/sample
# owner: lukesh
# group: sales
user::rw-
group::r--
mask::r--
other::r--
```

```
[root@servera ~]# ls -ld /redhat/
drwxrwx---+ 2 root root 44 Jul 23 18:49 /redhat/

[root@servera ~]# ls -l /redhat/

total 0

-rw-rwxr---+ 1 jack jack 0 Jul 22 19:43 abc1
-rw-r--r---+ 1 lukesh sales 0 Jul 23 18:49 sample
-rw-r--r---+ 1 ritesh ritesh 0 Jul 23 18:49 test
```

REMOVE ACL COMPLETELY

-b → base permission

```
[root@servera ~]# setfacl -b /redhat

[root@servera ~]# ls -ld /redhat
```

```
drwxrwx---. 2 root root 44 Jul 23 18:49 /redhat
```

```
[root@servera ~]# ls -l /redhat
```

```
total 0
```

```
-rw-rwxr---+ 1 jack jack 0 Jul 22 19:43 abc1
```

```
-rw-r--r---+ 1 lukesh sales 0 Jul 23 18:49 sample
```

```
-rw-r--r---+ 1 ritesh ritesh 0 Jul 23 18:49 test
```

```
[root@servera ~]# getfacl /redhat -R
```

```
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat
```

```
# owner: root
```

```
# group: root
```

```
user::rwx
```

```
group::rwx
```

```
other::---
```

```
# file: redhat/abc1
```

```
# owner: jack
```

```
# group: jack
```

```
user::rw-
```

```
user:jerry:rwx
```

```
group::r--
```

```
mask::rwx
```

```
other::r--
```

```
# file: redhat/test
```

```
# owner: ritesh
```

```
# group: ritesh
```

```
user::rw-
```

```
group::r--
```

```
mask::r--
```

```
other::r--
```

```
# file: redhat/sample
```

```
# owner: lukesh
```

```
# group: sales
```

```
user::rw-
```

```
group::r--
```

```
mask::r--
```

```
other::r--
```

```
[root@servera ~]# setfacl -Rb /redhat
```

```
[root@servera ~]# getfacl /redhat -R
```

```
getfacl: Removing leading '/' from absolute path names
```

```
# file: redhat
```

```
# owner: root
```

```
# group: root
```

```
user::rwx
```

```
group::rwx
```

```
other::---
```

```
# file: redhat/abc1
```

```
# owner: jack
```

```
# group: jack
```

```
user::rw-
```

```
group::r--
```

```
other::r--
```

```
# file: redhat/test
```

```
# owner: ritesh
```

```
# group: ritesh
```

```
user::rw-
```

```
group::r--
```

```
other::r--
```

```
# file: redhat/sample
```

```
# owner: lukesh
```

```
# group: sales
```

```
user::rw-
```

```
group::r--
```

```
other::r--
```

```
[root@servera ~]# ls -ld /redhat
```

```
drwxrwx--- 2 root root 44 Jul 23 18:49 /redhat
```

```
[root@servera ~]# ls -l /redhat
```

```
-rw-r--r-- 1 jack jack 0 Jul 22 19:43 abc1
```

```
-rw-r--r-- 1 lukesh sales 0 Jul 23 18:49 sample
```

```
-rw-r--r-- 1 ritesh ritesh 0 Jul 23 18:49 test
```
