**Create and manage Access Control Lists (ACLs).**

**Presentation**

When basic file permissions are not enough, you can use ACL.

ACL stands for Access Control Lists.

**Prerequisites**

However, before doing this, you have to check if the partition permits ACLs.  
To check that ACLs work, type:

# mount

/dev/mapper/vg\_root-lv\_root on / type ext4 **(rw)**

In this case, you have to edit the **/etc/fstab** file, add **“,acl”** after the **defaults** or **rw** option and, then, remount the partition:

# mount -o remount /

**ACL Configuration**

To allow **read/write** access to the user **bob** on the file called **f** (**-m** for modify, **u** for user, **rw-** for read/write access), type:

# setfacl **-m** **u**:**bob**:**rw-** **f**

To request access control list status on the same file **f**, type:

# getfacl **f**

# file: **f**

# owner: root

# group: root

user::rw-

user:**bob**:**rw-**

group::r--

mask::rw-

other::r--

To remove permissions allowed to the user **bob** (**-x** for remove, **u** for user), type:

# setfacl **-x** **u**:**bob** **f**

To remove all the ACLs on a file called **f** (**-b** for remove-all), type:

# setfacl **-b** **f**

To allow **read/execute** permissions to the group called **team** on a directory **dir** and all the files inside (**-R** for recursive, **-m** for modify, **g** for group, **r-x** for read/execute access), type:

# setfacl **-R** **-m** **g**:**team**:**r-x** **dir**

To get the result, type:

# getfacl **dir**

# file: **dir**

# owner: root

# group: root

user::rwx

group::r-x

group:**team**:**r-x**

mask::r-x

other::r-x