# FACL权限

文件系统访问控制列表

FACL:filesystem access control list

利用文件的扩展属性，保存了额外的访问控制权限

## getfacl 查看

## setfacl 设置

语法：setfacl [-bkRd] [-m|-x acl 参数] 目标文件名

选项与参数：

-m:设置后续的acl参数，不可与-x一起使用

-x: 删除后续的acl参数，不可与-m一起使用

-b:删除所有的acl参数

-k:删除默认的acl参数

-R:递归设置acl参数

-d:设置默认acl参数，只对目录有效

setfacl -m m:rw inittab

-m设定，可以设定到用户或者是组上

u:uid:perm

g:gid:perm

例子：

#mkdir /backup

#cd /backup

#cp /etc/inittab ./

#getfacl inittab

#setfacl -m u:redhat:rw inittab

## 权限的优先级

owner>facl,user> group > facl group>

所有权限都不能超过mask的权限

setfacl -m m:rwx [filename or directory_name]

-x取消

setfacl -x u:uid file_name

为目录设定默认访问控制列表：

setfacl -d -m u:lisi:rw abc

**例子：**

授权一个用户读权限

setfacl -m u:lisa:r file

Revoking write access from all groups and all named users (using the effective rights mask)撤销所有的组和用户的写权限（使用有效的正确mask）

setfacl -m m::rx file

Removing a named group entry from a file’ s ACL，移除一个组的ACL权限

setfacl -x g:staff file

Copying the ACL of one file to another，复制一个文件的ACL到另一个文件

getfacl file1 | setfacl --set-file=- file2

Copying the access ACL into the Default ACL，复制访问的目录的ACL作为目录的默认ACL

getfacl --access dir | setfacl -d -M- dir

**课后习题：**

1、建立2个目录/ftp/caiwu、/ftp/shichang，用户属主为root，权限设置为750

2、建立caiwubu、shichangbu组

3、建立caijing、shijing用户分为caiwubu和shichangbu经理

4、建立caiyuan01、caiyuan02用户，并加入caiwubu组

5、建立shiyuan01、shiyuan02用户，并加入shichangbu组

6、设置/ftp/caiwu目录权限，caijing可读可写可执行，caiyuan01、caiyuan02可读可执行

7、设置/ftp/shichang目录权限，shijing可读可写可执行，shiyuan01、shiyuan02员工可读可执行