

# UNIX/Linux : Access control lists (ACLs) basics

**Why we need ACLs ?** Every file on any UNIX file will have a owner/group and set of permissions. Imagine a case when multiple users need access to the same file and the users are from different groups. The file access control lists (FACLs) or simply ACLs are the list of additional user/groups and their permission to the file.

**How to know when a file has ACL attached to it** It is very easy to know when a file has a attached ACL to it. `ls -l` command would produce a output as show below.

```
# ls -l
-rw-r--r--+ 1  root  root  0  Sep  19  14:41  file
```

Note the **+** sign at the end of the permissions. This confirms that the file has an ACL attached to it.

## Viewing ACLs

To display details ACL information of a file use the `getfacl` command.

```
# getfacl /tmp/test
```

```
# file: test
# owner: root
# group: root
user::rw-
user:john:rw-
user:sam:rwx
group::r--
mask::rwx
other:---
```

Notice the 3 different `user:` lines. The first line lists the standard file permissions of the owner of the file. The 2 other user permissions are the individual permission for the user john and sam. The mask field here only applies to the additional permissions we have given to the user and groups. If the mask is set to `rwx` the read, write and execute permissions will be granted to additional user/groups. If the mask is set to `r-x`, the write permission will not be granted to additional user/groups. In general, **DO NOT** set mask to anything other **than rwx**. **The mask value does not affect the standard UNIX user/group/others permissions.**

## File with no ACLs

If you run the `getfacl` command on a file with no ACLs the additional “user:” lines and “mask” line will not be shown and standard file permissions will be shown.

```
# getfacl test
```

```
# file: test
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

## Creating and Managing ACLs

The **setfacl** command is used to set ACL on the given file. To give a rw access to user john on the file `/tmp/test` :

```
# setfacl -m u:john:rw /tmp/test
```

- The **-m** option tells setfacl to modify ACLs on the file(s) mentioned in command line. Instead of user john we can have a group to have a specific permission on the file :

```
# setfacl -m g:accounts:rw /tmp/test
```

- ACLs for multiple user and groups can also be set with single command :

```
# setfacl -m u:john:rw,g:accounts:rw /tmp/test
```

## Default ACLs on directories

Default ACLs are only created on directories. When you set default ACLs on directories, any files created within that directory will also have that default ACL assigned automatically.

**To create a default ACL on a directory:**

```
# setfacl -m default:u:john:rw /accounts
```

```
# getfacl accounts/
```

```
# file: accounts/
# owner: root
# group: root
```

```
user::rwx
group::r-x
other::r-x
default:user::rwx
default:user:john:rw-
default:group::r-x
default:mask::rwx
default:other::r-x
```

*Now create a new file in the accounts directory and list the ACL on the file :*

```
# touch /accounts/test
```

```
# getfacl test
# file: test
# owner: root
# group: root
user::rw-
user:john:rw-
group::r-x      #effective:r--
mask::rw-
other::r--
```

## Removing ACLs

To remove ACL, use the `setfacl` command with `-x` option :

```
# setfacl -x u:john /tmp/test
```

The above command removes the ACL for the user `john` on the file `/tmp/test`. The ACLs for other user/groups if any remains unaffected.

**To remove all ACLs associated to a file use the `-b` option with `setfacl` :**

```
# setfacl -b /tmp/test
```

## Backing up the ACLs

Many a times, the backup software may not copy the metadata related to the ACL on the files. In that case you may want to backup the ACL information on the files. Now, the ACL on all the files in a directory (including all sub directories) can be copied in a single file.

```
# cd /accounts
```

```
# getfacl -R * > accounts_facl      ( -R -> recursive )
```

## Restoring the ACLs

When you restore the files in /accounts directory, you would have to restore the ACLs associated with the files in that directory. To do that use the ACL backup file accounts\_facl along with the -restore option :

```
# setfacl --restore=accounts_facl
```

Quelle: <https://www.thegeekdiary.com/unix-linux-access-control-lists-acls-basics/>

Last update: **2019/03/07 13:51**