

# Using Access Control Lists for File Sharing

## Category: Files

A common way to share files and/or directories with group members or others is to use the **chmod** command to change the permissions. Yet **chmod** has limitations, so using Access Control Lsts (ACLs) may sometimes be your method of choice.

When you issue the command **chmod g+rwx filename**, for example, all the members in your group (**g**) gain read (**r**) and search/execute (**x**) access to that file, as shown below:

```
% ls -l foo
-rw----- 1 zsmith s0101 9 Jun 10 12:11 foo

% chmod g+rwx foo

% ls -l foo
-rw-r--x-- 1 zsmith s0101 9 Jun 10 12:11 foo
```

However, **chmod** does not allow you to select which members of your group or which specific individuals outside of your group can access your files/directories. For this, use ACLs, which provide a mechanism for finer-grain control of file sharing. There are two ACL commands:

- **setfacl** - set file access control lists

```
SYNOPSIS
    setfacl [-bkndRLPvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] file ...
    setfacl --restore=file
```

A detailed usage explanation of **setfacl** and its options can be found via **man setfacl**. Among the options listed:

1. The **-m** or **-M** option lets you "modify" the ACL, where **-m** expects an ACL on the command line and **-M** expects an ACL from a file or from standard input
2. The **-x** or **-X** option removes the ACL entries
3. The **-R** or **--recursive** option applies operations to all files and directories recursively
4. The **--test** option allows you to test the effect of changing the ACL without actually changing it
5. The **-b** option removes all extended ACL entries except the base entries of the owner, group, and others

- **getfacl** - get file access control lists

```
SYNOPSIS
```

```
getfacl [-dRLPvh] file ...
getfacl [-dRLPvh] -
```

A detailed usage explanation of **getfacl** and its options can be found via **man getfacl**.

Note that **setfacl** operations are supported on all Pleiades, Lou and Columbia filesystems except the Columbia home filesystems.

Before you grant another user or group access to certain files or directories, make sure that access to the parent directory (where the files or directories reside) is also allowed.

## Example 1

To allow another user (jbrown) to have read/execute (**rx**) permission on a file (*foo*) and to view the ACL before and after an ACL change:

```
% ls -l foo
-rw----- 1 zsmith s0101 9 Jun 10 12:11 foo

% getfacl foo
# file: foo
# owner: zsmith
# group: s0101
user::rw-
group::---
other::---

% setfacl -m u:jbrown:rx foo

% getfacl foo
# file: foo
# owner: zsmith
# group: s0101
user::rw-
user:jbrown:r-x
group::---
mask::r-x
other::---

% ls -l foo
-rw-r-x---+ 1 zsmith s0101 9 Jun 10 12:11 foo
```

## Example 2

To remove all extended ACLs in Example 1 except the base entries of the owner, group, and others:

```
% setfacl -b foo

% ls -l foo
-rw----- 1 zsmith s0101 9 Jun 10 12:11 foo

% getfacl foo
# file: foo
# owner: zsmith
# group: s0101
user::rw-
group::---
other::---
```

## Example 3

Continuing from Example 1, to test the granting of read/execute (**rx**) access to another group (group id 24176) without actually doing it:

```
% setfacl --test -m g:24176:rx foo foo: u::rw-,u:jbrown:r-x,g::---,g:g24176:r-x,m::r-x,
# file: foo
# owner: zsmith
# group: s0101
user::rw-
user:jbrown:r-x
group::---
mask::r-x
other::---
```

## Example 4

To allow another user (jbrown) recursive access to a directory (**dir.abc** which contains a file *foo2*):

```
% ls -ld dir.abc
drwx----- 2 zsmith s0101 17 Jun 10 13:19 dir.abc

% ls -l dir.abc
total 0
-rw----- 1 zsmith s0101 0 Jun 10 13:19 foo2

% setfacl -R -m u:jbrown:rx dir.abc

% getfacl dir.abc
# file: dir.abc
# owner: zsmith
# group: s0101
user::rwx
user:jbrown:r-x
group::---
```

```

mask::r-x
other::---

% getfacl dir.abc/foos
# file: dir.abc/foos
# owner: zsmith
# group: s0101
user::rw-
user:jbrown:r-x
group::---
mask::r-x
other::---

% ls -ld dir.abc
drwxr-x---+ 2 zsmith s0101 17 Jun 10 13:19 dir.abc

% ls -l dir.abc
total 0
-rw-r-x---+ 1 zsmith s0101 0 Jun 10 13:19 foos

```

## Example 5

Continuing from Example 4, to recursively remove all permissions user jbrown for a directory:

```

% setfacl -R -x u:jbrown dir.abc

% getfacl dir.abc
# file: dir.abc
# owner: zsmith
# group: s0101
user::rwx
group::---
mask::---
other::---

% getfacl dir.abc/foos
# file: dir.abc/foos
# owner: zsmith
# group: s0101
user::rw-
group::---
mask::---
other::---

```

For more information on ACLs, read **man acl**.

Article ID: 279

Last updated: 08 Aug, 2012

The HEC Environment -> Your Environment -> Files -> Using Access Control Lists for File Sharing

<http://www.nas.nasa.gov/hecc/support/kb/entry/279/?ajax=1>