NAME
setfacl - modify the Access Control List (ACL) for a file or files

SYNOPSIS
```
setfacl [-r] -s acl_entries file

setfacl [-r] -md acl_entries file

setfacl [-r] -f acl_filefile
```

DESCRIPTION
For each file specified, setfacl will either replace its entire ACL, including the default ACL on a directory, or it will add, modify, or delete one or more ACL entries, including default entries on directories.

When the setfacl command is used, it may result in changes to the file permission bits. When the user ACL entry for the file owner is changed, the file owner class permission bits will be modified. When the group ACL entry for the file group class is changed, the file group class permission bits will be modified. When the other ACL entry is changed, the file other class permission bits will be modified.

If you use the chmod(1) command to change the file group owner permissions on a file with ACL entries, both the file group owner permissions and the ACL mask are changed to the new permissions. Be aware that the new ACL mask permissions may change the effective permissions for additional users and groups who have ACL entries on the file.

A directory may contain default ACL entries. If a file or directory is created in a directory that contains default ACL entries, the newly created file will have permissions generated according to the intersection of the default ACL entries and the permissions requested at creation time. The umask(1) will not be applied if the directory contains default ACL entries. If a default ACL is specified for a specific user (or users), the file will have a regular ACL created. Otherwise, only the mode bits will be initialized according to the intersection described above. The default ACL should be thought of as the maximum discretionary access permissions that may be granted.

acl_entries Syntax
For the -m and -s options, acl_entries are one or more comma-separated ACL entries.

An ACL entry consists of the following fields separated by colons:

entry_type
Type of ACL entry on which to set file permissions. For example, entry_type can be user (the owner of a file) or mask (the ACL mask).

uid or gid
User name or user identification number. Or, group name or group identification number.

perms
Represents the permissions that are set on entry_type. perms can be indicated by the symbolic characters rwx or a number (the same permissions numbers used with the chmod command).

The following table shows the valid ACL entries (default entries may only be specified for directories):

| ACL Entry | Description |
|---|---|
| u[ser]::perms | File owner permissions. |
| g[roup]::perms | File group owner permissions. |
| o[ther]:perms | Permissions for users other than the file owner or members of file group owner. |

| | |
|---|---|
| m[ask]:perms | The ACL mask. The mask entry indicates the maximum permissions allowed for users (other than the owner) and for groups. The mask is a quick way to change permissions on all the users and groups. |
| u[ser]:uid:perms | Permissions for a specific user. For uid, you can specify either a user name or a numeric UID. |
| g[roup]:gid:perms | Permissions for a specific group. For gid, you can specify either a group name or a numeric GID. |
| d[efault]:u[ser]::perms | Default file owner permissions. |
| d[efault]:g[roup]::perms | Default file group owner permissions. |
| d[efault]:o[ther]:perms | Default permissions for users other than the file owner or members of the file group owner. |
| d[efault]:m[ask]:perms | Default ACL mask. |
| d[efault]:u[ser]:uid:perms | Default permissions for a specific user. For uid, you can specify either a user name or a numeric UID. |
| d[efault]:g[roup]:gid:perms | Default permissions for a specific group. For gid, you can specify either a group name or a numeric GID. |

For the -d option, acl_entries are one or more comma-separated ACL entries without permissions. Note that the entries for file owner, file group owner, ACL mask, and others may not be deleted.

## OPTIONS

The options have the following meaning:

-d acl_entries
: Deletes one or more entries from the file. The entries for the file owner, the file group owner, and others may not be deleted from the ACL. Notice that deleting an entry does not necessarily have the same effect as removing all permissions from the entry.

-f acl_file
: Seta a file's ACL with the ACL entries contained in the file named acl_file. The same constraints on specified entries hold as with the -s option. The entries are not required to be in any specific order in the file. Also, if you specify a dash '-' for acl_file, standard input is used to set the file's ACL.

  The character "#" in acl_file may be used to indicate a comment. All characters, starting with the "#" until the end of the line, will be ignored. Note that if the acl_file has been created as the output of the getfacl(1) command, any effective permissions, which will follow a "#", will be ignored.

-m acl_entries
: Adds one or more new ACL entries to the file, and/or modifies one or more existing ACL entries on the file. If an entry already exists for a specified uid or gid, the specified permissions will replace the current permissions. If an entry does not exist for the specified uid or gid, an entry will be created. When using the -m option to modify a default ACL, you must specify a complete default ACL (user, group, other, mask, and any additional entries) the first time.

-r
: Recalculates the permissions for the ACL mask entry. The permissions specified in the ACL mask entry are ignored and replaced by the maximum permissions necessary to grant the access to all additional user, file group owner, and additional group entries in the ACL. The permissions in the additional user, file group owner, and additional group entries are left unchanged.

```
     -s acl_entries
           Sets a file's ACL. All old ACL entries are removed and
           replaced  with  the  newly  specified ACL. The entries
           need not be in any specific order. They will be sorted
           by the command before being applied to the file.

           Required entries:

              o  Exactly one user entry specified  for  the  file
                 owner.

              o  Exactly one  group  entry  for  the  file  group
                 owner.

              o  Exactly one other entry specified.

     If there are additional user and group entries:


              o  Exactly one mask entry  specified  for  the  ACL
                 mask  that  indicates  the  maximum  permissions
                 allowed for users (other  than  the  owner)  and
                 groups.

              o  Must not be duplicate user entries with the same
                 uid.

              o  Must not be duplicate  group  entries  with  the
                 same gid.

     If file is a directory, the following  default  ACL  entries
     may be specified:


              o  Exactly one default  user  entry  for  the  file
                 owner.

              o  Exactly one default group  entry  for  the  file
                 group owner.

              o  Exactly one default mask entry for the ACL mask.

              o  Exactly one default other entry.

           There may be additional default user entries and addi-
           tional  default group entries specified, but there may
           not be duplicate additional default user entries  with
           the  same uid, or duplicate default group entries with
           the same gid.

EXAMPLES

     Example 1: Adding read permission only

     The following example adds one ACL entry to file abc,  which
     gives user shea read permission only.

     setfacl -m user:shea:r-- abc

     Example 2: Replacing a file's entire ACL

     The following example replaces the entire ACL for  the  file
     abc,  which  gives  shea  read  access,  the  file owner all
     access, the file group owner read access only, the ACL  mask
     read/write access, and others no access.

     setfacl -s user:shea:rwx,user::rwx,group::rw-,mask:r--,other:--- abc

     Notice that after this command, the file permission bits are
     rwxr-----.  Even  though  the  file group owner was set with
     read/write permissions, the ACL mask entry limits it to have
     only  read  permissions.  The  mask entry also specifies the
     maximum permissions available to  all  additional  user  and
     group ACL entries. Once again, even though the user shea was
     set with all access, the mask limits it to  have  only  read
     permissions.  The  ACL mask entry is a quick way to limit or
     open access to all the user and group entries in an ACL. For
     example,  by changing the mask entry to read/write, both the
     file group owner and user shea  would  be  given  read/write
     access.
```

Example 3: Setting the same ACL on two files

The following example sets the same ACL on file abc as the file xyz.

```
getfacl xyz | setfacl -f - abc
```

## FILES

/etc/passwd
: password file

/etc/group
: group file

## ATTRIBUTES

See attributes(5) for descriptions of the following attributes:

| ATTRIBUTE TYPE | ATTRIBUTE VALUE |
|---|---|
| Availability | SUNWcsu |

## SEE ALSO

getfacl(1), umask(1), aclcheck(3SEC), aclsort(3SEC), group(4), passwd(4), attributes(5), chmod(1)

SunOS 5.9 Last change: 11 Dec 2001