

NAME

setfacl – set file access control lists

SYNOPSIS

setfacl [-bkndRLPvvh] [{-m|-x} acl_spec] [{-M|-X} acl_file] file ...

setfacl --restore=file

DESCRIPTION

This utility sets Access Control Lists (ACLs) of files and directories. On the command line, a sequence of commands is followed by a sequence of files (which in turn can be followed by another sequence of commands, ...).

The options *-m*, and *-x* expect an ACL on the command line. Multiple ACL entries are separated by comma characters (','). The options *-M*, and *-X* read an ACL from a file or from standard input. The ACL entry format is described in Section ACL ENTRIES.

The *--set* and *--set-file* options set the ACL of a file or a directory. The previous ACL is replaced. ACL entries for this operation must include permissions.

The *-m* (*--modify*) and *-M* (*--modify-file*) options modify the ACL of a file or directory. ACL entries for this operation must include permissions.

The *-x* (*--remove*) and *-X* (*--remove-file*) options remove ACL entries. Only ACL entries without the *perms* field are accepted as parameters, unless `POSIXLY_CORRECT` is defined.

When reading from files using the *-M*, and *-X* options, setfacl accepts the output getfacl produces. There is at most one ACL entry per line. After a Pound sign ('#'), everything up to the end of the line is treated as a comment.

If setfacl is used on a file system which does not support ACLs, setfacl operates on the file mode permission bits. If the ACL does not fit completely in the permission bits, setfacl modifies the file mode permission bits to reflect the ACL as closely as possible, writes an error message to standard error, and returns with an exit status greater than 0.

PERMISSIONS

The file owner and processes capable of `CAP_FOWNER` are granted the right to modify ACLs of a file. This is analogous to the permissions required for accessing the file mode. (On current Linux systems, root is the only user with the `CAP_FOWNER` capability.)

OPTIONS

-b, *--remove-all*

Remove all extended ACL entries. The base ACL entries of the owner, group and others are retained.

-k, *--remove-default*

Remove the Default ACL. If no Default ACL exists, no warnings are issued.

-n, *--no-mask*

Do not recalculate the effective rights mask. The default behavior of setfacl is to recalculate the ACL mask entry, unless a mask entry was explicitly given. The mask entry is set to the union of all permissions of the owning group, and all named user and group entries. (These are exactly the entries affected by the mask entry).

- mask*
Do recalculate the effective rights mask, even if an ACL mask entry was explicitly given. (See the *-n* option.)
- d, --default*
All operations apply to the Default ACL. Regular ACL entries in the input set are promoted to Default ACL entries. Default ACL entries in the input set are discarded. (A warning is issued if that happens).
- restore=file*
Restore a permission backup created by 'getfacl -R' or similar. All permissions of a complete directory subtree are restored using this mechanism. If the input contains owner comments or group comments, and setfacl is run by root, the owner and owning group of all files are restored as well. This option cannot be mixed with other options except '--test'.
- test*
Test mode. Instead of changing the ACLs of any files, the resulting ACLs are listed.
- R, --recursive*
Apply operations to all files and directories recursively. This option cannot be mixed with '--restore'.
- L, --logical*
Logical walk, follow symbolic links. The default behavior is to follow symbolic link arguments, and to skip symbolic links encountered in subdirectories. This option cannot be mixed with '--restore'.
- P, --physical*
Physical walk, skip all symbolic links. This also skips symbolic link arguments. This option cannot be mixed with '--restore'.
- version*
Print the version of setfacl and exit.
- help*
Print help explaining the command line options.
- End of command line options. All remaining parameters are interpreted as file names, even if they start with a dash.
- If the file name parameter is a single dash, setfacl reads a list of files from standard input.

ACL ENTRIES

The setfacl utility recognizes the following ACL entry formats (blanks inserted for clarity):

[d[efault]:] [u[ser]:] *uid* [:*perms*]

Permissions of a named user. Permissions of the file owner if *uid* is empty.

[d[efault]:] g[roup]: *gid* [:*perms*]

Permissions of a named group. Permissions of the owning group if *gid* is empty.

[d[efault]:] m[ask][:] [:*perms*]

Effective rights mask

[d[efault]:] o[ther][:] [:*perms*]

Permissions of others.

Whitespace between delimiter characters and non-delimiter characters is ignored.

Proper ACL entries including permissions are used in modify and set operations. (options *-m*, *-M*, *--set* and *--set-file*). Entries without the *perms* field are used for *deletion* of entries (options *-x* and *-X*).

For *uid* and *gid* you can specify either a name or a number.

The *perms* field is a combination of characters that indicate the permissions: read (*r*), write (*w*), execute (*x*), execute only if the file is a directory or already has execute permission for some user (*X*). Alternatively, the *perms* field can be an octal digit (0-7).

AUTOMATICALLY CREATED ENTRIES

Initially, files and directories contain only the three base ACL entries for the owner, the group, and others. There are some rules that need to be satisfied in order for an ACL to be valid:

- * The three base entries cannot be removed. There must be exactly one entry of each of these base entry types.
- * Whenever an ACL contains named user entries or named group objects, it must also contain an effective rights mask.
- * Whenever an ACL contains any Default ACL entries, the three Default ACL base entries (default owner, default group, and default others) must also exist.
- * Whenever a Default ACL contains named user entries or named group objects, it must also contain a default effective rights mask.

To help the user ensure these rules, `setfacl` creates entries from existing entries under the following conditions:

- * If an ACL contains named user or named group entries, and no mask entry exists, a mask entry containing the same permissions as the group entry is created. Unless the `-n` option is given, the permissions of the mask entry are further adjusted to include the union of all permissions affected by the mask entry. (See the `-n` option description).
- * If a Default ACL entry is created, and the Default ACL contains no owner, owning group, or others entry, a copy of the ACL owner, owning group, or others entry is added to the Default ACL.
- * If a Default ACL contains named user entries or named group entries, and no mask entry exists, a mask entry containing the same permissions as the default Default ACL's group entry is added. Unless the `-n` option is given, the permissions of the mask entry are further adjusted to include the union of all permissions affected by the mask entry. (See the `-n` option description).

EXAMPLES

Granting an additional user read access
`setfacl -m u:lisa:r file`

Revoking write access from all groups and all named users (using the effective rights mask)
`setfacl -m m::rx file`

Removing a named group entry from a file's ACL
`setfacl -x g:staff file`

Copying the ACL of one file to another
`getfacl file1 | setfacl --set-file=- file2`

Copying the access ACL into the Default ACL
`getfacl -a dir | setfacl -d -M- dir`

CONFORMANCE TO POSIX 1003.1e DRAFT STANDARD 17

If the environment variable `POSIXLY_CORRECT` is defined, the default behavior of `setfacl` changes as follows: All non-standard options are disabled. The “default:” prefix is disabled. The `-x` and `-X` options also accept permission fields (and ignore them).

AUTHOR

Andreas Gruenbacher, <a.gruenbacher@computer.org>.

Please send your bug reports, suggested features and comments to the above address.

SEE ALSO

getfacl(1), **chmod(1)**, **umask(1)**, **acl(5)**