NAME

chacl − change the access control list of a file or directory

SYNOPSIS

chacl acl pathname...
chacl −b acl dacl pathname...
chacl −d dacl pathname...
chacl −R pathname...
chacl −D pathname...
chacl −B pathname...
chacl −l pathname...
chacl −r pathname...

DESCRIPTION

chacl is an IRIX-compatibility command, and is maintained for those users who are familiar with its use from either XFS or IRIX. Refer to the **SEE ALSO** section below for a description of tools which conform more closely to the (withdrawn draft) POSIX 1003.1e standard which describes Access Control Lists (ACLs).

chacl changes the ACL(s) for a file or directory. The ACL(s) specified are applied to each file in the ***pathname*** arguments.

Each ACL is a string which is interpreted using the *acl_from_text*(3) routine. These strings are made up of comma separated clauses each of which is of the form, tag:name:perm. Where ***tag*** can be:

"user" (or "u")
indicating that the entry is a "user" ACL entry.

"group" (or "g")
indicating that the entry is a "group" ACL entry.

"other" (or "o")
indicating that the entry is an "other" ACL entry.

"mask" (or "m")
indicating that the entry is a "mask" ACL entry.

name is a string which is the user or group name for the ACL entry. A null ***name*** in a user or group ACL entry indicates the file's owner or file's group. ***perm*** is the string "rwx" where each of the entries may be replaced by a "−" indicating no access of that type, e.g. "r−x", "−−x", "−−−".

OPTIONS

−b Indicates that there are two ACLs to change, the first is the file access ACL and the second the directory default ACL.

−d Used to set only the default ACL of a directory.

−R Removes the file access ACL only.

−D Removes directory default ACL only.

−B Remove all ACLs.

−l Lists the access ACL and possibly the default ACL associated with the specified files or directories. This option was added during the Linux port of XFS, and is not IRIX compatible.

−r Set the access ACL recursively for each subtree rooted at ***pathname***(s). This option was also added during the Linux port of XFS, and is not compatible with IRIX.

EXAMPLES

A minimum ACL:

chacl u::rwx,g::r-x,o::r-- file

The file ACL is set so that the file's owner has "rwx", the file's group has read and execute, and others have read only access to the file.

An ACL that is not a minimum ACL, that is, one that specifies a user or group other than the file's owner or owner's group, must contain a mask entry:

chacl u::rwx,g::r-x,o::r--,u:bob:r--,m::r-x file1 file2

To set the default and access ACLs on ***newdir*** to be the same as on ***olddir***, you could type:

```
chacl –b ‘chacl –l olddir | \
   sed –e ’s/.*\[//’ –e ’s#/# #’ –e ’s/]$//’‘ newdir
```

CAUTIONS

chacl can replace the existing ACL. To add or delete entries, you must first do ***chacl –l*** to get the existing ACL, and use the output to form the arguments to *chacl*.

Changing the permission bits of a file will change the file access ACL settings (see *chmod*(1)). However, file creation mode masks (see *umask*(1)) will not affect the access ACL settings of files created using directory default ACLs.

ACLs are filesystem extended attributes and hence are not typically archived or restored using the conventional archiving utilities. See *attr*(5) for more information about extended attributes and see *xfsdump*(8) for a method of backing them up under XFS.

SEE ALSO

getfacl(1), **setfacl**(1), **chmod**(1), **umask**(1), **acl_from_text**(3), **acl**(5), **xfsdump**(8)