

# File system Access Control Lists

*Access Control Lists* (ACLs) provide a fine grained and standards (POSIX) friendly approach to permissions than the traditional UNIX file permission model. It lets an administrator employ more sophisticated security models. The three types of UNIX security classes, 'owner', 'group' and 'other' are represented as entries in the Access Control Lists. Additional entries can be added to grant or deny access to specific users or groups.

To enable ACL support in the next generation UNIX file system (UFS2), you need to add 'options UFS\_ACL' to your kernel configuration file, although its enabled by default in the GENERIC kernel. ACLs required 'extended attributes' support which is also available in UFS2 (and UFS1, see below).

It must be noted that a higher level of configuration and system overhead is required to use *Extended Attributes* with UFS1, thus we do not discuss UFS1 ACL configuration in this section. Please consult `/sys/ufs/ufs/README.acls` and `/sys/ufs/ufs/README.extattr` to obtain information on how to configure a UFS1 file system for ACLs and Extended Attributes.

There are two ways to enable UFS ACLs. You can either use the mount option 'acls' which can be added to the `/etc/fstab` configuration file or set it persistently in the file system's superblock with aid of the `tunefs(8)` utility. To disable mount time ACLs, you need to do a full unmount of the file system in question, i.e. ACLs cannot be disabled on a root file system without a system restart. It is preferred that users utilise the `tunefs(8)` utility to enable ACL functionality, as this will prevent accidents from happening, such as mounting a file system without ACLs enabled, which can lead to security problems. It should be noted that disabling ACLs is not recommended as re-enabling them can result in unpredictable behaviour.

```
drwxrwx---+    2 hiten  hiten  512 Jan 24 10:57 ukug
drwxrwx---+    2 hiten  hiten  512 Sep 30 10:20 mgetcl
drwxrwx---+    2 hiten  hiten  512 Sep 12 11:57 bio
drwxr-xr-x     2 hiten  hiten  512 Sep 10 11:54 www
```

The directories with ACLs enabled can be noticed by the '+' (plus) symbol next to their permission modes in the above display. All directories except 'www' are taking advantage of ACLs. To retrieve access control information of a file or directory, you can use the `getfacl(1)` command:

```
hiten@unixguru:~> getfacl hiten-unixdaemons-20030321.tar.bz2
#file:hiten-unixdaemons-20030321.tar.bz2
#owner:1007
#group:1007
user::rw-
group::r--
other::r--
```

The *setfacl(1)* command is used for modifying access control information of a file or directory. The display below shows how to grant read/write permission to the user *grog*:

```
hiten@unixguru:~> setfacl -m u:grog:rw hiten-unixdaemons-20030321.tar.bz2
hiten@unixguru:~> getfacl hiten-unixdaemons-20030321.tar.bz2
# file: hiten-unixdaemons-20030321.tar.bz2
# owner: 1007
# group: 1007
user::rw-
user:grog:rw-
group::r--
mask:rw-
other:r--
```

More information about *setfacl(1)* or *getfacl(1)* can be found in their respective manual pages or in the FreeBSD Handbook. The ACL functionality in FreeBSD is standards compliant.