NAME

passwd − password file

DESCRIPTION

The */etc/passwd* file is a text file that describes user login accounts for the system. It should have read permission allowed for all users (many utilities, like **ls**(1) use it to map user IDs to usernames), but write access only for the superuser.

In the good old days there was no great problem with this general read permission. Everybody could read the encrypted passwords, but the hardware was too slow to crack a well-chosen password, and moreover the basic assumption used to be that of a friendly user-community. These days many people run some version of the shadow password suite, where */etc/passwd* has an 'x' character in the password field, and the encrypted passwords are in */etc/shadow*, which is readable by the superuser only.

If the encrypted password, whether in */etc/passwd* or in */etc/shadow*, is an empty string, login is allowed without even asking for a password. Note that this functionality may be intentionally disabled in applications, or configurable (for example using the "**nullok**" or "**nonull**" arguments to **pam_unix**(8)).

If the encrypted password in */etc/passwd* is "*NP*" (without the quotes), the shadow record should be obtained from an NIS+ server.

Regardless of whether shadow passwords are used, many system administrators use an asterisk (*) in the encrypted password field to make sure that this user can not authenticate themself using a password. (But see NOTES below.)

If you create a new login, first put an asterisk (*) in the password field, then use **passwd**(1) to set it.

Each line of the file describes a single user, and contains seven colon-separated fields:

```
name:password:UID:GID:GECOS:directory:shell
```

The field are as follows:

name This is the user's login name. It should not contain capital letters.

password This is either the encrypted user password, an asterisk (*), or the letter 'x'. (See **pwconv**(8) for an explanation of 'x'.)

UID The privileged *root* login account (superuser) has the user ID 0.

GID This is the numeric primary group ID for this user. (Additional groups for the user are defined in the system group file; see **group**(5)).

GECOS This field (sometimes called the "comment field") is optional and used only for informational purposes. Usually, it contains the full username. Some programs (for example, **finger**(1)) display information from this field.

GECOS stands for "General Electric Comprehensive Operating System", which was renamed to GCOS when GE's large systems division was sold to Honeywell. Dennis Ritchie has reported: "Sometimes we sent printer output or batch jobs to the GCOS machine. The gcos field in the password file was a place to stash the information for the $IDENTcard. Not elegant."

directory This is the user's home directory: the initial directory where the user is placed after logging in. The value in this field is used to set the **HOME** environment variable.

shell This is the program to run at login (if empty, use */bin/sh*). If set to a nonexistent executable, the user will be unable to login through **login**(1). The value in this field is used to set the **SHELL** environment variable.

FILES

/etc/passwd

NOTES

If you want to create user groups, there must be an entry in */etc/group*, or no group will exist.

If the encrypted password is set to an asterisk (*), the user will be unable to login using **login**(1), but may still login using **rlogin**(1), run existing processes and initiate new ones through **rsh**(1), **cron**(8), **at**(1), or mail filters, etc. Trying to lock an account by simply changing the shell field yields the same result and additionally allows the use of **su**(1).

SEE ALSO

chfn(1), **chsh**(1), **login**(1), **passwd**(1), **su**(1), **crypt**(3), **getpwent**(3), **getpwnam**(3), **group**(5), **shadow**(5), **vipw**(8)