NAME

passwd, **master.passwd**, **pwd.db**, **spwd.db** - format of the password file

DESCRIPTION

The **passwd** files are the local source of password information. They can be used in conjunction with the Hesiod domains ‘passwd’ and ‘uid’, and the NIS maps ‘passwd.byname’, ‘passwd.byuid’, ‘master.passwd.byname’, and ‘master.passwd.byuid’, as controlled by nsswitch.conf(5).

For consistency, none of these files should ever be modified manually.

The **master.passwd** file is readable only by root, and consists of newline separated records, one per user, containing ten colon (‘:’) separated fields. These fields are as follows:

name User’s login name.

password User’s *encrypted* password.

uid User’s id.

gid User’s login group id.

class User’s login class.

change Password change time.

expire Account expiration time.

gecos General information about the user.

home_dir
User’s home directory.

shell User’s login shell.

The **passwd** file is generated from the **master.passwd** file by pwd_mkdb(8), has the *class*, *change*, and *expire* fields removed, and the *password* field replaced by a ‘*’ character.

The *name* field is the login used to access the computer account, and the *uid* field is the number associated with it. They should both be unique across the system (and often across a group of systems) since they control file access.

While it is possible to have multiple entries with identical login names and/or identical user id's, it is usually a mistake to do so. Routines that manipulate these files will often return only one of the multiple entries, and that one by random selection.

The login name must not begin with a hyphen ('-'), and cannot contain 8-bit characters, tabs or spaces, or any of these symbols: ',:+&#%^()!@~*?<>=|\/";'. The dollar symbol ('$') is allowed only as the last character for use with Samba. No field may contain a colon (':') as this has been used historically to separate the fields in the user database.

Case is significant. Login names 'Lrrr' and 'lrrr' represent different users. Be aware of this when interoperating with systems that do not have case-sensitive login names.

In the **master.passwd** file, the *password* field is the *encrypted* form of the password, see crypt(3). If the *password* field is empty, no password will be required to gain access to the machine. This is almost invariably a mistake, so authentication components such as PAM can forcibly disallow remote access to passwordless accounts. Because this file contains the encrypted user passwords, it should not be readable by anyone without appropriate privileges.

A password of '*' indicates that password authentication is disabled for that account (logins through other forms of authentication, e.g., using ssh(1) keys, will still work). The field only contains encrypted passwords, and '*' can never be the result of encrypting a password.

An encrypted password prefixed by '*LOCKED*' means that the account is temporarily locked out and no one can log into it using any authentication. For a convenient command-line interface to account locking, see pw(8).

The *group* field is the group that the user will be placed in upon login. Since this system supports multiple groups (see groups(1)) this field currently has little special meaning.

The *class* field is a key for a user's login class. Login classes are defined in login.conf(5), which is a termcap(5) style database of user attributes, accounting, resource, and environment settings.

The *change* field is the number of seconds from the epoch, UTC, until the password for the account must be changed. This field may be left empty to turn off the password aging feature; a value of zero is equivalent to leaving the field empty.

The *expire* field is the number of seconds from the epoch, UTC, until the account expires. This field may be left empty to turn off the account aging feature; a value of zero is equivalent to leaving the field empty.

The *gecos* field normally contains comma (‘,’) separated subfields as follows:

name user’s full name
office user’s office number
wphone
user’s work phone number
hphone
user’s home phone number

The full *name* may contain an ampersand (‘&’) which will be replaced by the capitalized login *name* when the *gecos* field is displayed or used by various programs such as finger(1), sendmail(8), etc.

The *office* and phone number subfields are used by the finger(1) program, and possibly other applications.

The user’s home directory, *home_dir*, is the full UNIX path name where the user will be placed on login.

The *shell* field is the command interpreter the user prefers. If there is nothing in the *shell* field, the Bourne shell (*/bin/sh*) is assumed. The conventional way to disable logging into an account once and for all, as it is done for system accounts, is to set its *shell* to */sbin/nologin* (see nologin(8)).

HESIOD SUPPORT

If ‘dns’ is specified for the ‘passwd’ database in nsswitch.conf(5), then **passwd** lookups occur from the ‘passwd’ Hesiod domain.

NIS SUPPORT

If ‘nis’ is specified for the ‘passwd’ database in nsswitch.conf(5), then **passwd** lookups occur from the ‘passwd.byname’, ‘passwd.byuid’, ‘master.passwd.byname’, and ‘master.passwd.byuid’ NIS maps.

COMPAT SUPPORT

If ‘compat’ is specified for the ‘passwd’ database, and either ‘dns’ or ‘nis’ is specified for the ‘passwd_compat’ database in nsswitch.conf(5), then the **passwd** file also supports standard ‘+/-’ exclusions and inclusions, based on user names and netgroups.

Lines beginning with a ‘-’ (minus sign) are entries marked as being excluded from any following inclusions, which are marked with a ‘+’ (plus sign).

If the second character of the line is a ‘@’ (at sign), the operation involves the user fields of all entries in the netgroup specified by the remaining characters of the *name* field. Otherwise, the remainder of the *name* field is assumed to be a specific user name.

The ‘+’ token may also be alone in the *name* field, which causes all users from either the Hesiod domain **passwd** (with ‘passwd_compat: dns’) or ‘passwd.byname’ and ‘passwd.byuid’ NIS maps (with ‘passwd_compat: nis’) to be included.

If the entry contains non-empty *uid* or *gid* fields, the specified numbers will override the information retrieved from the Hesiod domain or the NIS maps. Likewise, if the *gecos*, *dir* or *shell* entries contain text, it will override the information included via Hesiod or NIS . On some systems, the *passwd* field may also be overridden.

FILES

/etc/passwd	ASCII password file, with passwords removed
/etc/pwd.db	db(3)-format password database, with passwords removed
/etc/master.passwd	ASCII password file, with passwords intact
/etc/spwd.db	db(3)-format password database, with passwords intact

COMPATIBILITY

The password file format has changed since 4.3BSD. The following awk script can be used to convert your old-style password file into a new style password file. The additional fields *class*, *change* and *expire* are added, but are turned off by default (setting these fields to zero is equivalent to leaving them blank). Class is currently not implemented, but change and expire are; to set them, use the current day in seconds from the epoch + whatever number of seconds of offset you want.

```
BEGIN { FS = ":"}
{ print $1 ":" $2 ":" $3 ":" $4 "::0:0:" $5 ":" $6 ":" $7 }
```

SEE ALSO

chpass(1), login(1), passwd(1), crypt(3), getpwent(3), login.conf(5), netgroup(5), nsswitch.conf(5), adduser(8), nologin(8), pw(8), pwd_mkdb(8), vipw(8), yp(8)

Managing NFS and NIS (O’Reilly & Associates)

HISTORY

A **passwd** file format first appeared in Version 1 AT&T UNIX.

The NIS **passwd** file format first appeared in SunOS.

The Hesiod support first appeared in FreeBSD 4.1. It was imported from the NetBSD Project, where it first appeared in NetBSD 1.4.

BUGS

User information should (and eventually will) be stored elsewhere.

Placing ‘compat’ exclusions in the file after any inclusions will have unexpected results.