

**NAME**

pwck – verify the integrity of password files

**SYNOPSIS**

**pwck** [options] [*PASSWORDFILE* [ *SHADOWFILE* ]]

**DESCRIPTION**

The **pwck** command verifies the integrity of the users and authentication information. It checks that all entries in */etc/passwd* and */etc/shadow* have the proper format and contain valid data. The user is prompted to delete entries that are improperly formatted or which have other uncorrectable errors.

Checks are made to verify that each entry has:

- the correct number of fields
- a unique and valid user name
- a valid user and group identifier
- a valid primary group
- a valid home directory
- a valid login shell

Checks for shadowed password information are enabled when the second file parameter *SHADOWFILE* is specified or when */etc/shadow* exists on the system.

These checks are the following:

- every *passwd* entry has a matching shadow entry, and every shadow entry has a matching *passwd* entry
- passwords are specified in the shadowed file
- shadow entries have the correct number of fields
- shadow entries are unique in shadow
- the last password changes are not in the future

The checks for correct number of fields and unique user name are fatal. If the entry has the wrong number of fields, the user will be prompted to delete the entire line. If the user does not answer affirmatively, all further checks are bypassed. An entry with a duplicated user name is prompted for deletion, but the remaining checks will still be made. All other errors are warnings and the user is encouraged to run the **usermod** command to correct the error.

The commands which operate on the */etc/passwd* file are not able to alter corrupted or duplicated entries. **pwck** should be used in those circumstances to remove the offending entry.

**OPTIONS**

The **-r** and **-s** options cannot be combined.

The options which apply to the **pwck** command are:

**--badname**

Allow names that do not conform to standards.

**-h, --help**

Display help message and exit.

**-q, --quiet**

Report errors only. The warnings which do not require any action from the user won't be displayed.

**-r, --read-only**

Execute the **pwck** command in read-only mode.

**-R, --root *CHROOT\_DIR***

Apply changes in the *CHROOT\_DIR* directory and use the configuration files from the *CHROOT\_DIR* directory. Only absolute paths are supported.

**-s, --sort**

Sort entries in */etc/passwd* and */etc/shadow* by UID.

By default, **pwck** operates on the files */etc/passwd* and */etc/shadow*. The user may select alternate files with the *passwd* and *shadow* parameters.

## CONFIGURATION

The following configuration variables in */etc/login.defs* change the behavior of this tool:

**NONEXISTENT** (string)

If a system account intentionally does not have a home directory that exists, this string can be provided in the */etc/passwd* entry for the account to indicate this. The result is that **pwck** will not emit a spurious warning for this account.

**PASS\_MAX\_DAYS** (number)

The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, *-1* will be assumed (which disables the restriction).

**PASS\_MIN\_DAYS** (number)

The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not specified, *0* will be assumed (which disables the restriction).

**PASS\_WARN\_AGE** (number)

The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.

## FILES

*/etc/group*

Group account information.

*/etc/passwd*

User account information.

*/etc/shadow*

Secure user account information.

## EXIT VALUES

The **pwck** command exits with the following values:

*0*

success

*1*

invalid command syntax

*2*

one or more bad password entries

*3*

can't open password files

*4*

can't lock password files

*5*

can't update password files

*6*

can't sort password files

**SEE ALSO**

**group(5), grpck(8), passwd(5), shadow(5), usermod(8).**