NAME

shadow − shadowed password file

DESCRIPTION

shadow is a file which contains the password information for the system's accounts and optional aging information.

This file must not be readable by regular users if password security is to be maintained.

Each line of this file contains 9 fields, separated by colons (“:”), in the following order:

login name
It must be a valid account name, which exist on the system.

encrypted password
Refer to **crypt(3)** for details on how this string is interpreted.

If the password field contains some string that is not a valid result of **crypt(3)**, for instance ! or *, the user will not be able to use a unix password to log in (but the user may log in the system by other means).

This field may be empty, in which case no passwords are required to authenticate as the specified login name. However, some applications which read the /etc/shadow file may decide not to permit any access at all if the password field is empty.

A password field which starts with an exclamation mark means that the password is locked. The remaining characters on the line represent the password field before the password was locked.

date of last password change
The date of the last password change, expressed as the number of days since Jan 1, 1970.

The value 0 has a special meaning, which is that the user should change her password the next time she will log in the system.

An empty field means that password aging features are disabled.

minimum password age
The minimum password age is the number of days the user will have to wait before she will be allowed to change her password again.

An empty field and value 0 mean that there are no minimum password age.

maximum password age
The maximum password age is the number of days after which the user will have to change her password.

After this number of days is elapsed, the password may still be valid. The user should be asked to change her password the next time she will log in.

An empty field means that there are no maximum password age, no password warning period, and no password inactivity period (see below).

If the maximum password age is lower than the minimum password age, the user cannot change her password.

password warning period
The number of days before a password is going to expire (see the maximum password age above) during which the user should be warned.

An empty field and value 0 mean that there are no password warning period.

password inactivity period
The number of days after a password has expired (see the maximum password age above) during which the password should still be accepted (and the user should update her password during the next login).

After expiration of the password and this expiration period is elapsed, no login is possible using the current user's password. The user should contact her administrator.

An empty field means that there are no enforcement of an inactivity period.

account expiration date
The date of expiration of the account, expressed as the number of days since Jan 1, 1970.

Note that an account expiration differs from a password expiration. In case of an account expiration, the user shall not be allowed to login. In case of a password expiration, the user is not allowed to login using her password.

An empty field means that the account will never expire.

The value 0 should not be used as it is interpreted as either an account with no expiration, or as an expiration on Jan 1, 1970.

reserved field
This field is reserved for future use.

FILES

/etc/passwd
User account information.

/etc/shadow
Secure user account information.

/etc/shadow−
Backup file for /etc/shadow.

Note that this file is used by the tools of the shadow toolsuite, but not by all user and password management tools.

SEE ALSO

chage(1), **login(1)**, **passwd(1)**, **passwd(5)**, **pwck(8)**, **pwconv(8)**, **pwunconv(8)**, **su(1)**, **sulogin(8)**.