NAME

chgpasswd − update group passwords in batch mode

SYNOPSIS

chgpasswd [*options*]

DESCRIPTION

The **chgpasswd** command reads a list of group name and password pairs from standard input and uses this information to update a set of existing groups. Each line is of the format:

group_name:*password*

By default the supplied password must be in clear−text, and is encrypted by **chgpasswd**.

The default encryption algorithm can be defined for the system with the **ENCRYPT_METHOD** variable of /etc/login.defs, and can be overwritten with the **−e**, **−m**, or **−c** options.

This command is intended to be used in a large system environment where many accounts are created at a single time.

OPTIONS

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

−c, **−−crypt−method**
Use the specified method to encrypt the passwords.

The available methods are DES, MD5, NONE, and SHA256 or SHA512 if your libc support these methods.

−e, **−−encrypted**
Supplied passwords are in encrypted form.

−h, **−−help**
Display help message and exit.

−m, **−−md5**
Use MD5 encryption instead of DES when the supplied passwords are not encrypted.

−R, **−−root** *CHROOT_DIR*
Apply changes in the *CHROOT_DIR* directory and use the configuration files from the *CHROOT_DIR* directory.

−s, **−−sha−rounds**
Use the specified number of rounds to encrypt the passwords.

The value 0 means that the system will choose the default number of rounds for the crypt method (5000).

A minimal value of 1000 and a maximal value of 999,999,999 will be enforced.

You can only use this option with the SHA256 or SHA512 crypt method.

By default, the number of rounds is defined by the SHA_CRYPT_MIN_ROUNDS and SHA_CRYPT_MAX_ROUNDS variables in /etc/login.defs.

CAVEATS

Remember to set permissions or umask to prevent readability of unencrypted files by other users.

You should make sure the passwords and the encryption method respect the system's password policy.

CONFIGURATION

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

ENCRYPT_METHOD (string)
This defines the system default encryption algorithm for encrypting passwords (if no algorithm are

specified on the command line).

It can take one of these values: *DES* (default), *MD5*, *SHA256*, *SHA512*.

Note: this parameter overrides the **MD5_CRYPT_ENAB** variable.

Note: This only affect the generation of group passwords. The generation of user passwords is done by PAM and subject to the PAM configuration. It is recommended to set this variable consistently with the PAM configuration.

MAX_MEMBERS_PER_GROUP (number)
Maximum members per group entry. When the maximum is reached, a new group entry (line) is started in /etc/group (with the same name, same password, and same GID).

The default value is 0, meaning that there are no limits in the number of members in a group.

This feature (split group) permits to limit the length of lines in the group file. This is useful to make sure that lines for NIS groups are not larger than 1024 characters.

If you need to enforce such limit, you can use 25.

Note: split groups may not be supported by all tools (even in the Shadow toolsuite). You should not use this variable unless you really need it.

MD5_CRYPT_ENAB (boolean)
Indicate if passwords must be encrypted using the MD5−based algorithm. If set to *yes*, new passwords will be encrypted using the MD5−based algorithm compatible with the one used by recent releases of FreeBSD. It supports passwords of unlimited length and longer salt strings. Set to *no* if you need to copy encrypted passwords to other systems which don't understand the new algorithm. Default is *no*.

This variable is superseded by the **ENCRYPT_METHOD** variable or by any command line option used to configure the encryption algorithm.

This variable is deprecated. You should use **ENCRYPT_METHOD**.

Note: This only affect the generation of group passwords. The generation of user passwords is done by PAM and subject to the PAM configuration. It is recommended to set this variable consistently with the PAM configuration.

SHA_CRYPT_MIN_ROUNDS (number), **SHA_CRYPT_MAX_ROUNDS** (number)
When **ENCRYPT_METHOD** is set to *SHA256* or *SHA512*, this defines the number of SHA rounds used by the encryption algorithm by default (when the number of rounds is not specified on the command line).

With a lot of rounds, it is more difficult to brute forcing the password. But note also that more CPU resources will be needed to authenticate users.

If not specified, the libc will choose the default number of rounds (5000).

The values must be inside the 1000−999,999,999 range.

If only one of the **SHA_CRYPT_MIN_ROUNDS** or **SHA_CRYPT_MAX_ROUNDS** values is set, then this value will be used.

If **SHA_CRYPT_MIN_ROUNDS** > **SHA_CRYPT_MAX_ROUNDS**, the highest value will be used.

Note: This only affect the generation of group passwords. The generation of user passwords is done by PAM and subject to the PAM configuration. It is recommended to set this variable consistently with the PAM configuration.

FILES

/etc/group
: Group account information.

/etc/gshadow
: Secure group account information.

/etc/login.defs
: Shadow password suite configuration.

SEE ALSO

gpasswd(1), **groupadd**(8), **login.defs**(5).