NAME

gpasswd − administer /etc/group and /etc/gshadow

SYNOPSIS

gpasswd [*option*] *group*

DESCRIPTION

The **gpasswd** command is used to administer /etc/group, and /etc/gshadow. Every group can have administrators, members and a password.

System administrators can use the **−A** option to define group administrator(s) and the **−M** option to define members. They have all rights of group administrators and members.

gpasswd called by a group administrator with a group name only prompts for the new password of the *group*.

If a password is set the members can still use **newgrp**(1) without a password, and non−members must supply the password.

Notes about group passwords

Group passwords are an inherent security problem since more than one person is permitted to know the password. However, groups are a useful tool for permitting co−operation between different users.

OPTIONS

Except for the **−A** and **−M** options, the options cannot be combined.

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

−a, **−−add** *user*
Add the *user* to the named *group*.

−d, **−−delete** *user*
Remove the *user* from the named *group*.

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

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

−r, **−−remove−password**
Remove the password from the named *group*. The group password will be empty. Only group members will be allowed to use **newgrp** to join the named *group*.

−R, **−−restrict**
Restrict the access to the named *group*. The group password is set to "!". Only group members with a password will be allowed to use **newgrp** to join the named *group*.

−A, **−−administrators** *user*,...
Set the list of administrative users.

−M, **−−members** *user*,...
Set the list of group members.

CAVEATS

This tool only operates on the /etc/group and /etc/gshadow files. Thus you cannot change any NIS or LDAP group. This must be performed on the corresponding server.

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.

SEE ALSO

newgrp(1), **groupadd**(8), **groupdel**(8), **groupmod**(8), **grpck**(8), **group**(5), **gshadow**(5).