Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'newusers.8' command

$ man newusers.8

NEWUSERS(8) System Management Commands NEWUSERS(8)

NAME

newusers - update and create new users in batch

SYNOPSIS

newusers [options] [file]

DESCRIPTION

The newusers command reads a file (or the standard input by default) and uses this information to update a set of existing users or to create new users. Each line is in the same format as the standard password file (see passwd(5)) with the exceptions explained below:

pw_name:pw_passwd:pw_uid:pw_gid:pw_gecos:pw_dir:pw_shell

pw_name

This is the name of the user.

It can be the name of a new user or the name of an existing user (or a user created before by newusers). In case of an existing user, the user's information will be changed, otherwise a new user will be created.

pw_passwd

This field will be encrypted and used as the new value of the encrypted password.

pw_uid

This field is used to define the UID of the user.

If the field is empty, a new (unused) UID will be defined

automatically by newusers.

If this field contains a number, this number will be used as the UID.

If this field contains the name of an existing user (or the name of a user created before by newusers), the UID of the specified user will be used.

If the UID of an existing user is changed, the files ownership of the user's file should be fixed manually.

pw_gid

This field is used to define the primary group ID for the user.

If this field contains the name of an existing group (or a group created before by newusers), the GID of this group will be used as the primary group ID for the user.

If this field is a number, this number will be used as the primary group ID of the user. If no groups exist with this GID, a new group will be created with this GID, and the name of the user.

If this field is empty, a new group will be created with the name of the user and a GID will be automatically defined by newusers to be used as the primary group ID for the user and as the GID for the new group.

If this field contains the name of a group which does not exist (and was not created before by newusers), a new group will be created with the specified name and a GID will be automatically defined by newusers to be used as the primary group ID for the user and GID for the new group.

pw_gecos

This field is copied in the GECOS field of the user.

pw_dir

This field is used to define the home directory of the user.

If this field does not specify an existing directory, the specified directory is created, with ownership set to the user being created or updated and its primary group. Note that newusers does not create parent directories of the new user's home directory. The

newusers command will fail to create the home directory if the parent directories do not exist, and will send a message to stderr informing the user of the failure. The newusers command will not halt or return a failure to the calling shell if it fails to create the home directory, it will continue to process the batch of new users specified.

If the home directory of an existing user is changed, newusers does not move or copy the content of the old directory to the new location. This should be done manually.

pw_shell

This field defines the shell of the user. No checks are performed on this field.

newusers first tries to create or change all the specified users, and then write these changes to the user or group databases. If an error occurs (except in the final writes to the databases), no changes are committed to the databases.

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

OPTIONS

The options which apply to the newusers command are:

--badname

Allow names that do not conform to standards.

-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.

-h, --help

Display help message and exit.

-r, --system

Create a system account.

System users will be created with no aging information in /etc/shadow, and their numeric identifiers are chosen in the SYS_UID_MIN-SYS_UID_MAX range, defined in login.defs, instead of

UID_MIN-UID_MAX (and their GID counterparts for the creation of groups).

-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

The input file must be protected since it contains unencrypted passwords.

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. MD5 and DES should not be used for new hashes, see crypt(5) for recommendations.

Note: this parameter overrides the MD5_CRYPT_ENAB variable.

GID_MAX (number), GID_MIN (number)

Range of group IDs used for the creation of regular groups by

useradd, groupadd, or newusers.

The default value for GID_MIN (resp. GID_MAX) is 1000 (resp. 60000).

HOME_MODE (number)

The mode for new home directories. If not specified, the UMASK is used to create the mode.

useradd and newusers use this to set the mode of the home directory they create.

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.

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.

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), which is orders of magnitude too low for modern hardware.

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.

SUB_GID_MIN (number), SUB_GID_MAX (number), SUB_GID_COUNT (number)

If /etc/subuid exists, the commands useradd and newusers (unless the user already have subordinate group IDs) allocate SUB_GID_COUNT unused group IDs from the range SUB_GID_MIN to SUB_GID_MAX for each new user.

The default values for SUB_GID_MIN, SUB_GID_MAX, SUB_GID_COUNT are respectively 100000, 600100000 and 65536.

SUB_UID_MIN (number), SUB_UID_MAX (number), SUB_UID_COUNT (number)

If /etc/subuid exists, the commands useradd and newusers (unless the user already have subordinate user IDs) allocate SUB_UID_COUNT unused user IDs from the range SUB_UID_MIN to SUB_UID_MAX for each new user.

The default values for SUB_UID_MIN, SUB_UID_MAX, SUB_UID_COUNT are respectively 100000, 600100000 and 65536.

SYS_GID_MAX (number), SYS_GID_MIN (number)

Range of group IDs used for the creation of system groups by useradd, groupadd, or newusers.

The default value for SYS_GID_MIN (resp. SYS_GID_MAX) is 101 (resp. GID_MIN-1).

SYS_UID_MAX (number), SYS_UID_MIN (number)

Range of user IDs used for the creation of system users by useradd or newusers.

The default value for SYS_UID_MIN (resp. SYS_UID_MAX) is 101 (resp. UID_MIN-1).

UID_MAX (number), UID_MIN (number)

Range of user IDs used for the creation of regular users by useradd or newusers.

The default value for UID_MIN (resp. UID_MAX) is 1000 (resp. 60000).

UMASK (number)

The file mode creation mask is initialized to this value. If not specified, the mask will be initialized to 022.

useradd and newusers use this mask to set the mode of the home directory they create if HOME_MODE is not set.

It is also used by login to define users' initial umask. Note that this mask can be overridden by the user's GECOS line (if QUOTAS_ENAB is set) or by the specification of a limit with the K identifier in limits(5).

FILES

/etc/passwd

User account information.

/etc/shadow

Secure user account information.

/etc/group

Group account information.

/etc/gshadow

Secure group account information.

/etc/login.defs

Shadow password suite configuration.

/etc/subgid

Per user subordinate group IDs.

/etc/subuid

Per user subordinate user IDs.

SEE ALSO

login.defs(5), passwd(1), subgid(5), subuid(5), useradd(8).