shadow

THE MAN-PAGES BOOK

Maintainers:

Alejandro Colomar <alx@kernel.org> 2023-present (4.14 stable)
Iker Pedrosa <ipedrosa@redhat.com> 2022-present
Christian Brauner <christian@brauner.io> 2019-present
Serge E. Hallyn <serge@hallyn.com> 2014-present
Nicolas François <nicolas.francois@centraliens.net> 2007-2014
Tomasz Kłoczko <kloczek@pld.org.pl> 2000-2007
Marek Michałkiewicz <marekm72@gmail.com> 1995-2000

НАЗВАНИЕ

chage − изменяет информацию об устаревании пароля пользователя

СИНТАКСИС

chage [*options*] *LOGIN*

ОПИСАНИЕ

Программа **chage** изменяет количество дней между датой смены пароля и датой последней смены пароля. Эта информация используется системой для определения момента, когда пользователь должен сменить свой пароль.

ПАРАМЕТРЫ

Параметры команды **chage**:

−d, **−−lastday** *LAST_DAY*
Set the number of days since January 1st, 1970 when the password was last changed. The date may also be expressed in the format YYYY−MM−DD (or the format more commonly used in your area). If the *LAST_DAY* is set to *0* the user is forced to change his password on the next log on.

−E, **−−expiredate** *EXPIRE_DATE*
Установить дату устаревания учётной записи пользователя, которая задаётся числом дней прошедших с 1 января 1970 года. Дата может быть также задана в виде ГГГГ−ММ−ДД (или в форме согласно региональным настройкам). Пользователь, чья учётная запись была заблокирована, должен обратиться к системному администратору, если хочет в дальнейшем работать с системой.

For example the following can be used to set an account to expire in 180 days:

```
chage −E $(date −d +180days +%Y−%m−%d)
```

Значение *−1* в параметре ДАТА_УСТАРЕВАНИЯ отменяет устаревание учётной записи.

−h, **−−help**
Показать краткую справку и закончить работу.

−i, **−−iso8601**
When printing dates, use YYYY−MM−DD format.

−I, **−−inactive** *INACTIVE*
Установить количество дней неактивности после устаревания пароля перед тем как учётная запись будет заблокирована. В параметре ДНЕЙ задаётся количество дней неактивности. Пользователь, чья учётная запись была заблокирована, должен обратиться к системному администратору, если хочет в дальнейшем работать с системой.

Значение *−1* в параметре ДНЕЙ отменяет неактивность учётной записи.

−l, **−−list**
Показать информацию об устаревании учётной записи.

−m, **−−mindays** *MIN_DAYS*
Задать минимальное количество дней между сменами пароля. Нулевое значение этого поля указывает на то, что пользователь может менять свой пароль когда захочет.

−M, **−−maxdays** *MAX_DAYS*
Установить максимальное количество дней работоспособности пароля. Если сумма значений МАКС_ДНЕЙ и ПОСЛ_ДЕНЬ раньше текущего дня, то пользователю придётся изменить свой пароль перед использованием учётной записи. Для того, чтобы это не было неожиданностью можно воспользоваться параметром **−W**, который активирует выдачу предупреждения о смене пароля пользователя заранее.

Значение *−1* в параметре МАКС_ДНЕЙ отменяет проверку пароля.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes to configuration files under the root filesystem found under the directory *PREFIX_DIR*. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−W, **−−warndays** *WARN_DAYS*
Установить количество дней выдачи предупреждения, перед тем как потребуется смена пароля. Параметр ПРЕДУП_ДНЕЙ считается в днях, в течении которых пользователь будет получать предупреждение об устаревании пароля, перед тем как это случится.

Если ни один параметр не указан, то **chage** переходит в интерактивный режим, предлагая запустившему пользователю изменить значения всех полей своей учётной записи. Вводимое значение заменяет текущее значение поля; если введена пустая строка, то текущее значение остаётся неизменным. Текущее значение показано в скобках *[ ]*.

ЗАМЕЧАНИЕ

Программа **chage** требует наличия файла теневых паролей.

The chage program will report only the information from the shadow password file. This implies that configuration from other sources (e.g. LDAP or empty password hash field from the passwd file) that affect the user's login will not be shown in the chage output.

The **chage** program will also not report any inconsistency between the shadow and passwd files (e.g. missing x in the passwd file). The **pwck** can be used to check for this kind of inconsistencies.

Программа **chage** работает только от суперпользователя, за исключением вызова с параметром **−l**, который может использоваться непривилегированным пользователем для определения даты устаревания своего пароля.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
success

1
permission denied

2
invalid command syntax

15
can't find the shadow password file

СМОТРИТЕ ТАКЖЕ

passwd(5), *shadow*(5).

НАЗВАНИЕ

chfn − изменяет информацию о пользователе

СИНТАКСИС

chfn [*options*] [*LOGIN*]

ОПИСАНИЕ

The **chfn** command changes user fullname, office room number, office phone number, and home phone number information for a user's account. This information is typically printed by *finger*(1) and similar programs. A normal user may only change the fields for her own account, subject to the restrictions in /etc/login.defs. (The default configuration is to prevent users from changing their fullname.) The superuser may change any field for any account. Additionally, only the superuser may use the **−o** option to change the undefined portions of the GECOS field.

Части поля GECOS не должны содержать двоеточий. За исключением части другая, в них не должно содержаться запятых и знаков равно. Также рекомендуется избегать символов не в кодировке US−ASCII, но это касается только номеров телефонов. Часть другая используется для хранения информации об учётной записи, которая используется другими приложениями.

ПАРАМЕТРЫ

Параметры команды **chfn**:

−f, **−−full−name** *FULL_NAME*
Изменяет ФИО пользователя.

−h, **−−home−phone** *HOME_PHONE*
Изменяет номер домашнего телефона пользователя.

−o, **−−other** *OTHER*
Изменяет другую информацию GECOS о пользователе. Эта часть используется для хранения информации об учётной записи, используемой другими приложениями, и может изменяться только суперпользователем.

−r, **−−room** *ROOM_NUMBER*
Изменяет номер комнаты пользователя.

−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.

−u, **−−help**
Показать краткую справку и закончить работу.

−w, **−−work−phone** *WORK_PHONE*
Изменяет номер рабочего телефона пользователя.

Если ни один параметр не указан, то **chfn** переходит в интерактивный режим, предлагая запустившему пользователю изменить данные своей учётной записи. Вводимое значение заменяет текущее значение записи; если введена пустая строка, то текущее значение остаётся неизменным. Текущее значение показано в скобках **[ ]**. При вызове без параметров программа **chfn** изменяет учётную запись запустившего пользователя.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/login.defs
содержит конфигурацию подсистемы теневых паролей

/etc/passwd
содержит информацию о пользователях

СМОТРИТЕ ТАКЖЕ

chsh(1), *login.defs*(5), *passwd*(5).

НАЗВАНИЕ

chsh − изменяет регистрационную оболочку пользователя

СИНТАКСИС

chsh [*options*] [*LOGIN*]

ОПИСАНИЕ

Программа **chsh** изменяет регистрационную оболочку пользователя. Она определяет какая команда будет запущена после регистрации пользователя в системе. Обычный пользователь может изменять регистрационную оболочку только для своей учётной записи; суперпользователь может изменять регистрационную оболочку любой учётной записи.

ПАРАМЕТРЫ

Параметры команды **chsh**:

−h, **−−help**
Показать краткую справку и закончить работу.

−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, **−−shell** *SHELL*
Имя новой регистрационной оболочки пользователя. Если задать пустое значение, то будет использована регистрационная оболочка по умолчанию.

Если параметр **−s** не задан, то **chsh** переходит в интерактивный режим, предлагая пользователю изменить свою регистрационную оболочку. Вводимое значение заменяет текущее значение поля; если введена пустая строка, то текущее значение остаётся неизменным. Текущее значение регистрационной оболочки указано в скобках *[ ]*.

ЗАМЕЧАНИЕ

Все допустимые имена регистрационных оболочек должны быть указаны в файле /etc/shells. На суперпользователя это ограничение не действует и поэтому ему разрешено указывать любое значение. Для учётной записи с ограниченной регистрационной оболочкой пользователь не может изменить свою регистрационную оболочку. Поэтому /bin/rsh в файле /etc/shells лучше не указывать, так как, если пользователь случайно изменит свою регистрационную оболочку на эту ограниченную оболочку, то не сможет восстановить её первоначальное значение.

For this reason, placing /bin/rsh in /etc/shells is discouraged since accidentally changing to a restricted shell would prevent the user from ever changing her login shell back to its original value.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
содержит информацию о пользователях

/etc/shells
содержит список разрешённых регистрационных оболочек

/etc/login.defs
содержит конфигурацию подсистемы теневых паролей

СМОТРИТЕ ТАКЖЕ

chfn(1), *login.defs*(5), *passwd*(5).

НАЗВАНИЕ

expiry − проверяет и изменяет пароль согласно политике устаревания

СИНТАКСИС

expiry *option*

ОПИСАНИЕ

Программа **expiry** проверяет (параметр **−c**) сколько ещё времени будет работоспособен текущий пароль и вынуждает изменить его (параметр **−f**), если это требуется. Она может запускаться обычным пользователем.

ПАРАМЕТРЫ

Параметры команды **expiry**:

−c, **−−check**
Проверяет и изменяет срок действия пароля у текущего пользователя.

−f, **−−force**
Принудительно меняет пароль, если его срок действия истёк.

−h, **−−help**
Показать краткую справку и закончить работу.

ФАЙЛЫ

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

СМОТРИТЕ ТАКЖЕ

passwd(5), *shadow*(5).

НАЗВАНИЕ

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

СИНТАКСИС

gpasswd [*option*] *group*

ОПИСАНИЕ

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

Системные администраторы могут использовать параметр **−A**, чтобы назначить группе администратора(ов) и параметр **−M** для определения списка членов, а также имеют все права администраторов и членов группы.

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.

Замечания о паролях групп

Пароли групп имеют врождённую проблему с безопасностью, так как пароль знает более одного человека. Однако, группы являются полезным инструментом совместной работы различных пользователей.

ПАРАМЕТРЫ

За исключением параметров **−A** и **−M**, параметры нельзя использовать вместе.

Параметры команды **gpasswd**:

−a, **−−add** *user*
Добавить пользователя в указанную группу.

−d, **−−delete** *user*
Удалить пользователя из указанной группы.

−h, **−−help**
Показать краткую справку и закончить работу.

−Q, **−−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.

−r, **−−remove−password**
Удалить пароль указанной группы. Пароль группы будет пустым. Только члены группы смогут использовать **newgrp** для входа в указанную группу.

−R, **−−restrict**
Ограничить доступ к указанной группе. Пароль группы становится равным «!». Только члены группы имеющие пароль смогут использовать **newgrp** для входа в указанную группу.

−A, **−−administrators** *user*,...
Задать список администраторов группы.

−M, **−−members** *user*,...
Задать список членов группы.

ПРЕДОСТЕРЕЖЕНИЯ

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.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/gshadow

содержит защищаемую информацию о группах

СМОТРИТЕ ТАКЖЕ

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

НАЗВАНИЕ

groups − показывает имена групп запустившего программу пользователя

СИНТАКСИС

groups [*user*]

ОПИСАНИЕ

The **groups** command displays the current group names or ID values. If the value does not have a corresponding entry in /etc/group, the value will be displayed as the numerical group value. The optional *user* parameter will display the groups for the named user.

ЗАМЕЧАНИЕ

Systems which do not support supplementary groups (see *initgroups*(3)) will have the information from /etc/group reported. The user must use **newgrp** or **sg** to change his current real and effective group ID.

ФАЙЛЫ

/etc/group
: содержит информацию о группах

СМОТРИТЕ ТАКЖЕ

newgrp(1), *getgid*(2), *getgroups*(2), *getuid*(2), *initgroups*(3).

НАЗВАНИЕ

login − начинает сеанс в системе

СИНТАКСИС

login [−p] [−h *host*] [*username*] [*ENV=VAR*...]

login [−p] [−h *host*] −f *username*

login [−p] −r *host*

ОПИСАНИЕ

Программа **login** используется для запуска нового сеанса в системе. Как правило, эта программа вызывается автоматически и выводит приглашение *login:* на терминал пользователя. Программа **login** может восприниматься оболочкой командной строки не как простая программа и вызываться не как подпроцесс. При вызове из оболочки **login** должна запускаться посредством вызова **exec login**, что приводит к завершению работы пользователя в текущей оболочке (и, таким образом, вновь входящий в систему пользователь не попадёт в сеанс вызвавшего). Попытка запустить **login** из любой оболочки, отличной от регистрационной, приводит к сообщению об ошибке.

В какой−то момент пользователя попросят ввести свой пароль . Чтобы не допустить раскрытия, символы при вводе пароля не отображаются. Разрешено очень маленькое количество попыток ввода неправильного пароля, перед тем как **login** закончит работу и прервёт подключение.

If password aging has been enabled for your account, you may be prompted for a new password before proceeding. You will be forced to provide your old password and the new password before continuing. Please refer to *passwd*(1) for more information.

После успешного входа в систему, будут показаны сообщения от системы и о наличии почты. Можно отключить вывод файла системных сообщений из файла /etc/motd, создав в домашнем каталоге файл нулевой длины с именем .hushlogin. Сообщение о наличии почты может быть одним из: «У вас есть новая почта .», «У вас есть почта .» или «У вас нет почты .», в зависимости от наполненности почтового ящика.

Значение идентификатора учётной записи и группы будет взято из файла /etc/passwd. Значения переменных **$HOME**, **$SHELL**, **$PATH**, **$LOGNAME** и **$MAIL** устанавливаются согласно соответствующим полям учётной записи пользователя. Также могут быть установлены значения ulimit, umask и nice из поля GECOS.

В некоторых системах переменной окружения **$TERM** будет присвоен тип терминала линии tty, согласно данным из файла /etc/ttytype.

Также может быть выполнен сценарий инициализации пользовательского интерпретатора команд. Подробней об этой функции смотрите соответствующую справочную страницу.

Субсистемный вход в систему можно распознать по наличию символа «*» в начале регистрационной оболочки. Заданный домашний каталог будет использован как корень новой файловой системы, в которой регистрируется пользователь.

The **login** program is NOT responsible for removing users from the utmp file. It is the responsibility of *getty*(8) and *init*(8) to clean up apparent ownership of a terminal session. If you use **login** from the shell prompt without **exec**, the user you use will continue to appear to be logged in even after you log out of the "subsession".

ПАРАМЕТРЫ

−f

Не выполнять аутентификацию, пользователь уже прошёл проверку.

Замечание: в этом случае имя_пользователя обязательно.

−h

Имя удалённого узла, на который нужно войти.

−p

Сохранить окружение.

−r

Выполнить протокол autologin для rlogin.

Параметры **−r**, **−h** и **−f** используются только если **login** запускается суперпользователем.

ПРЕДОСТЕРЕЖЕНИЯ

Данная версия **login** может быть собрана с разными параметрами и только некоторые из них смогут быть использованы на любой машине.

Расположение файлов может отличаться на разных системах.

The **login** program is NOT responsible for removing users from the utmp file. It is the responsibility of *getty*(8) and *init*(8) to clean up apparent ownership of a terminal session. If you use **login** from the shell prompt without **exec**, the user you use will continue to appear to be logged in even after you log out of the "subsession".

Как и для любой программы, запуск **login** может быть подделан. Если неуполномоченные пользователи имеют физический доступ к машине, то атакующий может использовать это для получения пароля следующего человека, который будет работать за машиной. Под Linux пользователи могут использовать механизм SAK для установления достоверного пути и таким образом предотвращения атаки.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/var/run/utmp
: содержит список работающих сеансов в системе

/var/log/wtmp
: содержит список завершённых сеансов работы с системой

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/motd
: содержит системные сообщения за день

/etc/nologin
: при существовании файла блокируется доступ в систему обычным пользователям

/etc/ttytype
: содержит список типов терминалов

$HOME/.hushlogin
: при существовании файла системные сообщения при входе в систему не выводятся

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

СМОТРИТЕ ТАКЖЕ

mail(1), *passwd*(1), *sh*(1), *su*(1), *login.defs*(5), *nologin*(5), *passwd*(5), *securetty*(5), *getty*(8).

НАЗВАНИЕ

newgrp − выполняет регистрацию пользователя в новой группе

СИНТАКСИС

newgrp [−] [*group*]

ОПИСАНИЕ

Программа **newgrp** используется для изменения ID текущей группы в работающем сеансе. Если указан необязательный параметр −, то окружение пользователя будет инициализировано повторно, как если бы пользователь заново вошёл в систему, иначе имеющееся окружение, включая текущий рабочий каталог, изменено не будет.

Программа **newgrp** изменяет идентификатор текущей реальной группы на заданный или на группу по умолчанию, указанную в файле /etc/passwd, в случае если имя группы не указано. Программа **newgrp** также пытается добавить группу в список групп пользователя. Если пользователь не является суперпользователем, то его попросят ввести пароль, даже если он его не имеет (в файле /etc/shadow, если для этого пользователя имеется запись в файле теневых паролей, иначе используется файл /etc/passwd), а группа имеет, или если пользователь не является членом группы, а группа имеет пароль. Если пользователь не является членом группы, а у группы пустой пароль, то пользователю будет отказано в доступе.

Если есть запись для этой группы в файле /etc/gshadow, то список членов и пароль этой группы будут взяты из этого файла, иначе используется запись из файла /etc/group.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

СМОТРИТЕ ТАКЖЕ

id(1), *login*(1), *su*(1), *sg*(1), *gpasswd*(1), *group*(5), **gshadow**(5).

НАЗВАНИЕ

passwd − изменяет пароль пользователя

СИНТАКСИС

passwd [*options*] [*LOGIN*]

ОПИСАНИЕ

Программа **passwd** изменяет пароли пользовательских учётных записей. Обычный пользователь может изменить пароль только своей учётной записи, суперпользователь может изменить пароль любой учётной записи. Программа **passwd** также изменяет информацию об учётной записи или срок действия пароля.

Изменение пароля

Сначала пользователя попросят ввести старый пароль, если он был. Этот пароль зашифровывается и сравнивается с имеющимся. У пользователя есть только одна попытка ввести правильный пароль. Для суперпользователя этот шаг пропускается, для того чтобы можно было изменить забытый пароль.

После ввода пароля проверяется информация об устаревании пароля, чтобы убедиться, что пользователю разрешено изменять пароль в настоящий момент. Если нет, то **passwd** не производит изменение пароля и завершает работу.

Затем пользователю предложат дважды ввести новый пароль. Значение второго ввода сравнивается с первым и для изменения пароли из обеих попыток должны совпасть.

Then, the password is tested for complexity. **passwd** will reject any password which is not suitably complex. Care must be taken not to include the system default erase or kill characters.

Выбор пароля

Безопасность пароля зависит от стойкости алгоритма шифрования и размера пространства ключа. В старых системах *UNIX* метод шифрования основывался на алгоритме NBS DES. Сейчас рекомендуют более новые методы (смотрите **ENCRYPT_METHOD**). Размер пространства ключа зависит от степени произвольности выбранного пароля.

При обеспечении безопасности пароля выбирают нечто среднее между сложным паролем и сложностью работы с ним. По этой причине, вы не должны использовать пароль, который является словом из словаря или который придётся записать из−за его сложности . Также, пароль не должен быть названием чего−либо, номером вашей лицензии, днём рождения и домашним адресом. Обо всём этом легко догадаться, что приведёт к нарушению безопасности системы.

As a general guideline, passwords should be long and random. It's fine to use simple character sets, such as passwords consisting only of lowercase letters, if that helps memorizing longer passwords. For a password consisting only of lowercase English letters randomly chosen, and a length of 32, there are 26^32 (approximately 2^150) different possible combinations. Being an exponential equation, it's apparent that the exponent (the length) is more important than the base (the size of the character set).

You can find advice on how to choose a strong password on http://en.wikipedia.org/wiki/Password_strength

ПАРАМЕТРЫ

Параметры команды **passwd**:

−a, **−−all**
: Этот параметр можно использовать только вместе с **−S** для вывода статуса всех пользователей.

−d, **−−delete**
: Удалить пароль пользователя (сделать его пустым). Это быстрый способ заблокировать пароль учётной записи. Это сделает указанную учётную запись беспарольной.

−e, **−−expire**
: Немедленно сделать пароль устаревшим. В результате это заставит пользователя изменить пароль при следующем входе в систему.

−h, **−−help**
: Показать краткую справку и закончить работу.

−i, **−−inactive** *INACTIVE*
Этот параметр используется для блокировки учётной записи по прошествии заданного числа дней после устаревания пароля. То есть, если пароль устарел и прошло более указанных ДНЕЙ, то пользователь больше не сможет использовать данную учётную запись.

−k, **−−keep−tokens**
Указывает, что изменение пароля нужно выполнить только для устаревших ключей аутентификации (паролей). Пользователи хотят оставить свои непросроченные ключи нетронутыми.

−l, **−−lock**
Заблокировать пароль указанной учётной записи. Этот параметр блокирует пароль, изменяя его значение на вариант, который не может быть шифрованным паролем (добавляется символ «!» в начало пароля).

Заметим, что это не блокирует учётную запись. Пользователь всё ещё может войти в систему с помощью другого способа аутентификации (например, с помощью ключа SSH). Чтобы заблокировать учётную запись, администратор должен использовать команду **usermod −−expiredate 1** (это установит дату устаревания учётной запись равной 2 января 1970 года).

Посетитель с заблокированным паролем не может изменить свой пароль.

−n, **−−mindays** *MIN_DAYS*
Задать минимальное количество дней между сменами пароля. Нулевое значение этого поля указывает на то, что пользователь может менять свой пароль когда захочет.

−q, **−−quiet**
Не выводить сообщений при работе.

−r, **−−repository** *REPOSITORY*
Изменить пароль в РЕПОЗИТОРИИ.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes to configuration files under the root filesystem found under the directory *PREFIX_DIR*. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−S, **−−status**
Показать состояние учётной записи. Информация о состоянии содержит 7 полей. Первое поле содержит имя учётной записи. Второе поле указывает, заблокирован ли пароль учётной записи (L), она без пароля (NP) или у неё есть рабочий пароль (P). Третье поле хранит дату последнего изменения пароля. В следующих четырёх полях хранятся минимальный срок, максимальный срок, период выдачи предупреждения и период неактивности пароля. Эти сроки измеряются в днях.

−u, **−−unlock**
Разблокировать пароль указанной учётной записи. Этот параметр разблокирует пароль, возвращая его прежнее значение (которое было перед использованием параметра **−l**).

−w, **−−warndays** *WARN_DAYS*
Установить число дней выдачи предупреждения, перед тем как потребуется смена пароля. В параметре ПРЕД_ДНЕЙ указывается число дней перед тем как пароль устареет, в течении которых пользователю будут напоминать, что пароль скоро устареет.

−x, **−−maxdays** *MAX_DAYS*
Установить максимальное количество дней, в течении которых пароль остаётся рабочим. После МАКС_ДНЕЙ пароль нужно изменить.

Значение *−1* в параметре МАКС_ДНЕЙ отменяет проверку пароля.

−s, **−−stdin**
This option is used to indicate that passwd should read the new password from standard input, which can be a pipe.

ПРЕДОСТЕРЕЖЕНИЯ

Сложность пароля проверяется на разных машинах по разному. Пользователю настоятельно рекомендуется выбирать пароль такой сложности, чтобы ему нормально работалось.

Пользователи не могут изменять свои пароли в системе, если включён NIS и они не вошли на сервер NIS.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

/etc/login.defs
содержит конфигурацию подсистемы теневых паролей

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
success

1
permission denied

2
invalid combination of options

3
unexpected failure, nothing done

4
unexpected failure, passwd file missing

5
passwd file busy, try again

6
invalid argument to option

СМОТРИТЕ ТАКЖЕ

chpasswd(8), *makepasswd*(1), *passwd*(5), *shadow*(5), *login.defs*(5), *usermod*(8).

The following web page comically (yet correctly) compares the strength of two different methods for choosing a password: "https://xkcd.com/936/"

НАЗВАНИЕ

sg − выполняет команду с правами другой группы

СИНТАКСИС

sg [−] [group [−c] command]

ОПИСАНИЕ

Команда **sg** работает подобно команде **newgrp**, но в качестве параметра ожидает команду. Команда будет выполнена оболочкой /bin/sh. В большинстве оболочек, откуда может запускаться **sg**, команду из нескольких слов нужно заключать в кавычки. Другим отличием между **newgrp** и **sg** является то, что некоторые оболочки воспринимают **newgrp** особенным образом, заменяя себя новым экземпляром оболочки, которую создаёт **newgrp**. Этого не происходит с командой **sg**, поэтому после завершения работы **sg** вы возвращаетесь в предыдущую группу.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

СМОТРИТЕ ТАКЖЕ

id(1), *login*(1), *newgrp*(1), *su*(1), *gpasswd*(1), *group*(5), **gshadow**(5).

НАЗВАНИЕ

su − изменяет ID пользователя или делает его суперпользователем

СИНТАКСИС

su [*options*] [−] [*username* [*args*]]

ОПИСАНИЕ

The **su** command is used to become another user during a login session. Invoked without a **username**, **su** defaults to becoming the superuser. The − option may be used to provide an environment similar to what the user would expect had the user logged in directly. The **−c** option may be used to treat the next argument as a command by most shells.

Options are recognized everywhere in the argument list. You can use the −− argument to stop option parsing. The − option is special: it is also recognized after −−, but has to be placed before **username**.

Пользователю предложат ввести пароль, если он задан. При неверном пароле возникает сообщение об ошибке. Все попытки, удачные и неудачные, протоколируются системой с целью обнаружения злоупотреблений.

Текущее окружение передаётся новой оболочке. Значение **$PATH** сбрасывается в значение /bin:/usr/bin для обычных пользователей или в /sbin:/bin:/usr/sbin:/usr/bin для суперпользователя. Эти значения можно изменить в переменных **ENV_PATH** и **ENV_SUPATH** в файле /etc/login.defs.

Субсистемный вход в систему можно распознать по наличию символа «*» в начале регистрационной оболочки. Заданный домашний каталог будет использован как корень новой файловой системы, в которой регистрируется пользователь.

ПАРАМЕТРЫ

Параметры команды **su**:

−c, **−−command** *COMMAND*
Указать команду, которая будет запущена оболочкой в виде параметра для **−c**.

The executed command will have no controlling terminal. This option cannot be used to execute interactive programs which need a controlling TTY.

−, **−l**, **−−login**
Предоставляет окружение, как если бы пользователь непосредственно регистрировался в системе.

When − is used, it must be specified before any **username**. For portability it is recommended to use it as last option, before any **username**. The other forms (**−l** and **−−login**) do not have this restriction.

−s, **−−shell** *SHELL*
Оболочка, которая будет запущена.

The invoked shell is chosen from (highest priority first):

The shell specified with −−shell.

If **−−preserve−environment** is used, the shell specified by the **$SHELL** environment variable.

The shell indicated in the /etc/passwd entry for the target user.

/bin/sh if a shell could not be found by any above method.

Если заданный пользователь имеет ограниченную оболочку (то есть оболочка в поле пользовательской записи в файле /etc/passwd отсутствует в файле /etc/shells), то параметр **−−shell** или переменная окружения **$SHELL** не будут учтены, если **su** не была запущена суперпользователем.

−m, **−p**, **−−preserve−environment**
Preserve the current environment, except for:

$PATH
reset according to the /etc/login.defs options **ENV_PATH** or **ENV_SUPATH** (see below);

$IFS
reset to «<space><tab><newline>», if it was set.

Если заданный пользователь имеет ограниченную оболочку, то этот параметр не сработает (если **su** не запускается суперпользователем).

Note that the default behavior for the environment is the following:

The **$HOME**, **$SHELL**, **$USER**, **$LOGNAME**, **$PATH**, and **$IFS** environment variables are reset.

If **−−login** is not used, the environment is copied, except for the variables above.

If **−−login** is used, the **$TERM**, **$COLORTERM**, **$DISPLAY**, and **$XAUTHORITY** environment variables are copied if they were set.

If **−−login** is used, the **$TZ**, **$HZ**, and **$MAIL** environment variables are set according to the /etc/login.defs options **ENV_TZ**, **ENV_HZ**, **MAIL_DIR**, and **MAIL_FILE** (see below).

If **−−login** is used, other environment variables might be set by the **ENVIRON_FILE** file (see below).

ПРЕДОСТЕРЕЖЕНИЯ

Данная версия программы **su** может быть собрана с разными параметрами и только некоторые из них смогут быть использованы на любой машине.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

/etc/login.defs
содержит конфигурацию подсистемы теневых паролей

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

При успешном выполнении **su** возвращает код выхода команды, которая была выполнена.

Если выполнение команды завершилось по сигналу, то **su** возвращает номер этого сигнала плюс 128.

Если su завершила команду (так как был запрос сделать это и команда не завершилась в положенное время), то **su** завершается с кодом 255.

Some exit values from **su** are independent from the executed command:

0
success (**−−help** only)

1
System or authentication failure

126
The requested command was not found

127
The requested command could not be executed

СМОТРИТЕ ТАКЖЕ

login(1), *login.defs*(5), *sg*(1), *sh*(1).

НАЗВАНИЕ

shadow, getspnam − процедуры для работы с файлом шифрованных паролей

СИНТАКСИС

#include <shadow.h>

*struct spwd *getspent();*

*struct spwd *getspnam(char *name);*

void setspent();

void endspent();

*struct spwd *fgetspent(FILE *fp);*

*struct spwd *sgetspent(char *cp);*

*int putspent(struct spwd *p, FILE *fp);*

int lckpwdf();

int ulckpwdf();

ОПИСАНИЕ

shadow управляет содержимым файла теневых паролей, /etc/shadow. Структура в файле *#include*:

```
struct spwd {
    char          *sp_namp; /* user login name */
    char          *sp_pwdp; /* encrypted password */
    long int      sp_lstchg; /* last password change */
    long int      sp_min; /* days until change allowed. */
    long int      sp_max; /* days before change required */
    long int      sp_warn; /* days warning for expiration */
    long int      sp_inact; /* days before account inactive */
    long int      sp_expire; /* date when account expires */
    unsigned long int sp_flag; /* reserved for future use */
}
```

Значение каждого поля:

- sp_namp − указатель на строку с именем пользователя, завершающуюся нулевым символом
- sp_pwdp − указатель на строку с паролем, завершающуюся нулевым символом
- sp_lstchg − количество дней, когда был изменён пароль последний раз, начиная с 1 января 1970 года
- sp_min − количество дней, когда можно не менять пароль
- sp_max − количество дней, которое должно пройти, чтобы нужно было поменять пароль
- sp_warn − количество дней, когда будет выдаваться предупреждение о скором устаревании пароля перед тем как пароль устареет
- sp_inact − количество дней, которые должны пройти после устаревания пароля, когда начинать считать, что учётная запись неактивна и заблокирована
- sp_expire − дней, после которых учётная запись будет заблокирована, начиная с 1 января 1970 года
- sp_flag − зарезервировано

ОПИСАНИЕ

Функции *getspent*, *getspname*, *fgetspent* и *sgetspent* возвращают указатель на структуру *struct spwd*. *getspent* возвращает следующую запись из файла, а *fgetspent* возвращает следующую запись из заданного канала, предполагая, что это файл правильного формата.*sgetspent* возвращает указатель на *struct spwd*, используя предоставленную строку в качестве входящих данных. *getspnam* ищет начиная с текущей позиции в файле запись по имени *name*.

Функции *setspent* и *endspent* можно использовать для перемещения в начало и конец файла теневых паролей соответственно.

Функции *lckpwdf* и *ulckpwdf* используются для получения монопольного доступа к файлу /etc/shadow. *lckpwdf* пытается выполнить блокировку с помощью *pw_lock* в течении 15 секунд. Далее выполняется попытка получить вторую блокировку с помощью *spw_lock* в течении времени оставшегося от первоначальных 15 секунд. При неудаче в любой из блокировок в течении 15 секунд, функция *lckpwdf* возвращает −1. Если обе блокировки прошли успешно возвращается 0.

ДИАГНОСТИКА

Функции возвращают NULL, если все записи кончились или произошла ошибка во время работы. Функции, возвращающие *int*, возвращают 0 при успешном выполнении и −1 в случае неудачи.

ПРЕДОСТЕРЕЖЕНИЯ

Данные функции могут использоваться только суперпользователем, так как доступ к файлу теневых паролей ограничен.

ФАЙЛЫ

/etc/shadow

содержит защищаемую информацию о пользователях

СМОТРИТЕ ТАКЖЕ

getpwent(3), *shadow*(5).

НАЗВАНИЕ

faillog − файл протокола неудачных попыток входа в систему

ОПИСАНИЕ

В файле /var/log/faillog содержатся счётчики неудачных попыток входа и ограничения для каждой учётной записи.

Этот файл состоит из записей постоянной длины, упорядоченных по числовому идентификатору учётной записи. Каждая запись содержит количество неудачных попыток входа с момента последнего успешного входа в систему, максимальное количество неудачных попыток перед тем как учётная запись будет заблокирована, терминал, с которого осуществлялась последняя неудачная попытка входа, дату этого события и интервал (в секундах) на сколько учётная запись будет заблокирована в случае неудачной попытки.

Структура файла:

```
struct    faillog {
              short   fail_cnt;
              short   fail_max;
              char    fail_line[12];
              time_t  fail_time;
              long    fail_locktime;
};
```

ФАЙЛЫ

/var/log/faillog
журнал неудавшихся попыток входа в систему

СМОТРИТЕ ТАКЖЕ

faillog(8)

НАЗВАНИЕ

gshadow − файл с защищаемой информацией о группах

ОПИСАНИЕ

Файл /etc/gshadow содержит защищаемую информацию о группах.

Этот файл должен быть недоступен обычному пользователю, если нужно обеспечить безопасность паролей.

Каждая строка файла содержит поля, отделёнными друг от друга двоеточием:

group name
Должно содержать правильное имя группы, которая существует в системе.

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 *, users will not be able to use a unix password to access the group (but group members do not need the password).

The password is used when a user who is not a member of the group wants to gain the permissions of this group (see *newgrp*(1)).

Это поле может быть пустым; в этом случае только члены группы могут пользоваться правами группы.

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.

Данный пароль заменяет любой пароль, указанный в файле /etc/group.

administrators
Список имён пользователей, перечисленных через запятую.

Администраторы могут менять пароль или членство в группе.

Администраторы также имеют те же права, что и члены группы (смотрите далее).

members
Список имён пользователей, перечисленных через запятую.

Члены могут иметь доступ к группе без ввода пароля.

Вы должны использовать тот же список пользователей что и в /etc/group.

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/gshadow
содержит защищаемую информацию о группах

СМОТРИТЕ ТАКЖЕ

gpasswd(5), *group*(5), *grpck*(8), *grpconv*(8), *newgrp*(1).

НАЗВАНИЕ

limits − файл контроля ресурсов

ОПИСАНИЕ

В файле *limits* (по умолчанию /etc/limits или определяется значением LIMITS_FILE в файле config.h) описываются ограничения, которые можно изменять. Этот файл должен принадлежать суперпользователю и право на чтение должно быть только у суперпользователя.

По умолчанию учётная запись «root» ничем не ограничена. Фактически, никак нельзя установить ограничения с помощью этой процедуры на учётные записи, имеющие права суперпользователя (учётные записи с UID равным 0).

Каждая строка описывает ограничение для одного пользователя имеет вид:

user LIMITS_STRING

или в виде:

@group LIMITS_STRING

СТРОКА_ОГРАНИЧЕНИЙ — это строка, в которой указаны сразу несколько ограничений. Каждое ограничение состоит из буквенного идентификатора и числового значения.

Допустимые идентификаторы:

- A: максимальное адресное пространство (КБ)
- C: максимальный размер файла core (КБ)
- D: максимальный размер данных (КБ)
- F: maximum file size (KB)
- K: file creation mask, set by *umask*(2).
- I: максимальное значение уступчивости (nice) (0..39, преобразуемые в 20..−19)
- L: максимальное число возможных регистраций в системе этого пользователя
- M: максимальное синхронизируемое адресное пространство памяти (КБ)
- N: максимальное число открытых файлов
- O: максимальный приоритет реального времени
- P: process priority, set by *setpriority*(2).
- R: максимальный размер резидентного сегмента (КБ)
- S: максимальный размер стека (КБ)
- T: максимальное время использования процессора (минут)
- U: максимальное число процессов

Например, значение *L2D2048N5* допустимо для СТРОКИ_ОГРАНИЧЕНИЙ. Для удобства чтения, следующие записи эквивалентны:

```
username L2D2048N5
username L2 D2048 N5
```

Be aware that after *username* the rest of the line is considered a limit string, thus comments are not allowed. An invalid limits string will be rejected (not considered) by the **login** program.

Запись по умолчанию выглядит как username "*". Если у вас есть несколько записей по умолчанию в файле *LIMITS_FILE*, то будет использоваться последняя.

Ограничения, задаваемые в виде «*@group*», применяются к членам указанной группы *group*.

If more than one line with limits for a user exist, only the first line for this user will be considered.

If no lines are specified for a user, the last *@group* line matching a group whose the user is a member of will be considered, or the last line with default limits if no groups contain the user.

Чтобы полностью снять ограничения с пользователя, используется одиночное тире «−».

Чтобы снять ограничение с пользователя, вместо числового значения ограничения можно использовать одиночное тире «−».

Также заметьте, что все настройки ограничений делаются ДЛЯ КОНКРЕТНОЙ УЧЁТНОЙ ЗАПИСИ. Они не являются глобальными и не постоянны. Возможно глобальные ограничения и появятся, но пока это только в планах ;)

ФАЙЛЫ

/etc/limits

СМОТРИТЕ ТАКЖЕ

login(1), *setpriority*(2), *setrlimit*(2).

НАЗВАНИЕ

login.defs − содержит конфигурацию подсистемы теневых паролей

ОПИСАНИЕ

Файл /etc/login.defs содержит настройки подсистемы теневых паролей (shadow password suite). Этот файл является обязательным. Отсутствие данного файла не повлияет на работу системы, но, вероятно, приведёт к выполнению нежелаемых операций.

Файл представляет собой обычный текстовый файл; каждая строка описывает один параметр настройки. Строки состоят из названия параметра и его значения, которые разделяются пробельным символом. Пустые строки и комментарии игнорируются. Комментарии начинаются со знака фунта «#», который должен быть первым непробельным символом в строке.

Значения параметров могут быть четырёх типов: строки, логические значения, числа и длинные числа. Строки состоят из любых печатных символов. Под логическими значениями подразумеваются *yes* или *no*. Неопределённый логический параметр или имеющий значение, отличное от указанных выше, считается как имеющий значение *no*. Числа (обычные и длинные) можно задавать в десятичной, восьмеричной (перед значением ставится «*0*») или шестнадцатеричной (перед значением ставится «*0x*») системах счисления. Максимальные значения параметра обычного и длинного числа зависят от архитектуры компьютера.

Возможны следующие параметры настройки:

Параметры **PASS_MAX_DAYS**, **PASS_MIN_DAYS** и **PASS_WARN_AGE** используются только при создании учётной записи. Любые изменения этих параметров не влияют на уже существующие учётные записи.

ПЕРЕКРЁСТНЫЕ ССЫЛКИ

Следующие перекрёстные ссылки отражают связь между программами и их параметрам из набора для работы с теневыми паролями.

chfn
: CHFN_AUTH CHFN_RESTRICT LOGIN_STRING

chgpasswd
: ENCRYPT_METHOD MAX_MEMBERS_PER_GROUP MD5_CRYPT_ENAB SHA_CRYPT_MAX_ROUNDS SHA_CRYPT_MIN_ROUNDS

chpasswd
: ENCRYPT_METHOD MD5_CRYPT_ENAB SHA_CRYPT_MAX_ROUNDS SHA_CRYPT_MIN_ROUNDS

chsh
: CHSH_AUTH LOGIN_STRING

gpasswd
: ENCRYPT_METHOD MAX_MEMBERS_PER_GROUP MD5_CRYPT_ENAB SHA_CRYPT_MAX_ROUNDS SHA_CRYPT_MIN_ROUNDS

groupadd
: GID_MAX GID_MIN MAX_MEMBERS_PER_GROUP SYS_GID_MAX SYS_GID_MIN

groupdel
: MAX_MEMBERS_PER_GROUP

groupmems
: MAX_MEMBERS_PER_GROUP

groupmod
: MAX_MEMBERS_PER_GROUP

grpck
: MAX_MEMBERS_PER_GROUP

grpconv
: MAX_MEMBERS_PER_GROUP

grpunconv
: MAX_MEMBERS_PER_GROUP

lastlog
: LASTLOG_UID_MAX

login
: CONSOLE CONSOLE_GROUPS DEFAULT_HOME ENV_HZ ENV_PATH ENV_SUPATH ENV_TZ ENVIRON_FILE ERASECHAR FAIL_DELAY FAILLOG_ENAB FAKE_SHELL FTMP_FILE HUSHLOGIN_FILE ISSUE_FILE KILLCHAR LASTLOG_ENAB LASTLOG_UID_MAX LOGIN_RETRIES LOGIN_STRING LOGIN_TIMEOUT LOG_OK_LOGINS LOG_UNKFAIL_ENAB MAIL_CHECK_ENAB MAIL_DIR MAIL_FILE MOTD_FILE NOLOGINS_FILE PORTTIME_CHECKS_ENAB QUOTAS_ENAB TTYGROUP TTYPERM TTYTYPE_FILE ULIMIT UMASK USERGROUPS_ENAB

newgrp / sg
: SYSLOG_SG_ENAB

newusers
: ENCRYPT_METHOD GID_MAX GID_MIN MAX_MEMBERS_PER_GROUP MD5_CRYPT_ENAB HOME_MODE PASS_MAX_DAYS PASS_MIN_DAYS PASS_WARN_AGE SHA_CRYPT_MAX_ROUNDS SHA_CRYPT_MIN_ROUNDS SUB_GID_COUNT SUB_GID_MAX SUB_GID_MIN SUB_UID_COUNT SUB_UID_MAX SUB_UID_MIN SYS_GID_MAX SYS_GID_MIN SYS_UID_MAX SYS_UID_MIN UID_MAX UID_MIN UMASK

passwd
: ENCRYPT_METHOD MD5_CRYPT_ENAB OBSCURE_CHECKS_ENAB PASS_ALWAYS_WARN PASS_CHANGE_TRIES PASS_MAX_LEN PASS_MIN_LEN SHA_CRYPT_MAX_ROUNDS SHA_CRYPT_MIN_ROUNDS

pwck
: PASS_MAX_DAYS PASS_MIN_DAYS PASS_WARN_AGE

pwconv
: PASS_MAX_DAYS PASS_MIN_DAYS PASS_WARN_AGE

su
: CONSOLE CONSOLE_GROUPS DEFAULT_HOME ENV_HZ ENVIRON_FILE ENV_PATH ENV_SUPATH ENV_TZ LOGIN_STRING MAIL_CHECK_ENAB MAIL_DIR MAIL_FILE QUOTAS_ENAB SULOG_FILE SU_NAME SU_WHEEL_ONLY SYSLOG_SU_ENAB USERGROUPS_ENAB

sulogin
: ENV_HZ ENV_TZ

useradd
: CREATE_HOME GID_MAX GID_MIN HOME_MODE LASTLOG_UID_MAX MAIL_DIR MAX_MEMBERS_PER_GROUP PASS_MAX_DAYS PASS_MIN_DAYS PASS_WARN_AGE SUB_GID_COUNT SUB_GID_MAX SUB_GID_MIN SUB_UID_COUNT SUB_UID_MAX SUB_UID_MIN SYS_GID_MAX SYS_GID_MIN SYS_UID_MAX SYS_UID_MIN UID_MAX UID_MIN UMASK

userdel
: MAIL_DIR MAIL_FILE MAX_MEMBERS_PER_GROUP USERDEL_CMD USERGROUPS_ENAB

usermod
: LASTLOG_UID_MAX MAIL_DIR MAIL_FILE MAX_MEMBERS_PER_GROUP

СМОТРИТЕ ТАКЖЕ

login(1), *passwd*(1), *su*(1), *passwd*(5), *shadow*(5), *pam*(8).

НАЗВАНИЕ

login.access − файл контроля доступа в систему

ОПИСАНИЕ

В файле *login.access* определяются комбинации (пользователь, узел) и/или (пользователь, терминал), которым будет разрешён или запрещён вход в систему.

Когда кто−то пытается войти в систему выполняется сканирование файла *login.access* в поисках первой совпадающей записи (пользователь, узел), или в случае не сетевого входа, первой совпадающей записи (пользователь, терминал). Из найденной записи выбирается поле прав доступа, по которому определяется разрешать ли данной учётной записи вход в систему или нет.

Каждая строка таблицы контроля доступа в систему состоит из трёх полей разделённых символом «:» и выглядит так:

права_доступа:пользователи:источники

The first field should be a "+" (access granted) or "−" (access denied) character. The second field should be a list of one or more login names, group names, or *ALL* (always matches). The third field should be a list of one or more tty names (for non−networked logins), host names, domain names (begin with "."), host addresses, internet network numbers (end with "."), *ALL* (always matches) or *LOCAL* (matches any string that does not contain a "." character). If you run NIS you can use @netgroupname in host or user patterns.

Оператор *EXCEPT* помогает в написании компактных правил.

Поиск в файле групп производится только когда имя не совпадает с регистрирующимся пользователем. Рассматриваются группы только с явно прописанными в них пользователями: программа не принимает во внимание значение первичной группы пользователя.

ФАЙЛЫ

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

СМОТРИТЕ ТАКЖЕ

login(1).

НАЗВАНИЕ

passwd − файл паролей

ОПИСАНИЕ

/etc/passwd contains one line for each user account, with seven fields delimited by colons («:»). These fields are:

- имя пользователя для входа в систему
- необязательный зашифрованный пароль
- числовой идентификатор пользователя
- числовой идентификатор группы
- ФИО пользователя или поле комментария
- домашний каталог пользователя
- необязательный интерпретатор командной строки пользователя

If the *password* field is a lower−case «x», then the encrypted password is actually stored in the *shadow*(5) file instead; there *must* be a corresponding line in the /etc/shadow file, or else the user account is invalid.

The encrypted *password* field may be empty, in which case no password is required to authenticate as the specified login name. However, some applications which read the /etc/passwd file may decide not to permit *any* access at all if the *password* field is blank.

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.

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).

The comment field, also known as the gecos field, is used by various system utilities, such as *finger*(1). The use of an ampersand here will be replaced by the capitalised login name when the field is used or displayed by such system utilities.

В поле домашнего каталога хранится начальный рабочий каталог. Программа **login** использует эту информацию для установки значения переменной окружения **$HOME**.

В поле интерпретатора командной строки хранится название интерпретатора командной строки пользователя или программы, которая будет запущена первой. Программа **login** использует эту информацию для установки значения переменной окружения **$SHELL**. Если это поле пустое, то используется значение по умолчанию /bin/sh.

ФАЙЛЫ

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: необязательный файл с шифрованными паролями

/etc/passwd−
: резервная копия файла /etc/passwd

  Заметим, что этот файл используется программами из комплекта утилит shadow, но не всеми инструментами управления пользователями и паролями.

СМОТРИТЕ ТАКЖЕ

crypt(3), *getent*(1), *getpwnam*(3), *login*(1), *passwd*(1), *pwck*(8), *pwconv*(8), *pwunconv*(8), *shadow*(5), *su*(1), *sulogin*(8).

НАЗВАНИЕ

porttime − файл с временами доступа к портам

ОПИСАНИЕ

Файл *porttime* содержит список устройств tty, имена пользователей и разрешённое время входа.

Каждая запись состоит из трёх полей, разделённых двоеточиями. В первом поле содержится список устройств tty (перечисленных через запятую) или звёздочка, указывающая, что все устройства tty попадают под правило этой записи. Во втором поле содержится список имён пользователей (перечисленных через запятую) или звёздочка, указывающая, что все имена пользователей попадают под правило этой записи. В третьем поле содержится список (через запятую) допустимого времени работы.

Каждая запись времени доступа состоит из нуля или более дней недели, обозначенных как *Su*, *Mo*, *Tu*, *We*, *Th*, *Fr* и *Sa*, а также временем начала и конца, записанного через дефис. Сокращение *Wk* можно использовать для обозначения периода с понедельника по пятницу, а *Al* обозначает каждый день. Если день не задан, то предполагается *Al* в качестве значения по умолчанию.

ПРИМЕРЫ

Следующая запись разрешает доступ пользователю **jfh** с любого порта по будням с 9:00 до 17:00.

*:jfh:Wk0900−1700

Следующие записи разрешают доступ только пользователям *root* и *oper* с /dev/console в любое время. Это показывает, что файл /etc/porttime обрабатывается в порядке появления записей в файле. Любой другой пользователь попадёт под правило второй записи, которая не разрешает доступ в любое время.

```
console:root,oper:Al0000−2400
console:*:
```

Следующая запись разрешает доступ пользователю *games* с любого порта в нерабочие часы.

*:games:Wk1700−0900,SaSu0000−2400

ФАЙЛЫ

/etc/porttime
: содержит разрешённое время работы определённых пользователей с определённых портов

СМОТРИТЕ ТАКЖЕ

login(1).

НАЗВАНИЕ

shadow − файл теневых паролей

ОПИСАНИЕ

Файл shadow содержит шифрованные пароли учётных записей пользователей и необязательную информацию об устаревании пароля.

Этот файл должен быть недоступен обычному пользователю, если нужно обеспечить безопасность паролей.

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

login name
Должно содержать правильное имя учётной записи, которая существует в системе.

encrypted password
Это поле может быть пустым, то есть для указанной учётной записи не требуется аутентификация по паролю. Однако, некоторые приложения, читающие файл /etc/shadow, могут вообще отказать в доступе, если поле пароля пусто.

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.

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).

date of last password change
The date of the last password change, expressed as the number of days since Jan 1, 1970 00:00 UTC.

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.

Пустое значение обозначает, что проверка устаревания пароля выключена.

minimum password age
Минимальный срок действия пароля в днях, которые пользователь должен ждать, чтобы поменять пароль.

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

maximum password age
Максимальный срок действия пароля в днях, после которого пользователь должен изменить пароль.

По прошествии этого количества дней пароль может быть ещё действительным. Пользователя нужно попросить изменить пароль при следующем входе.

Пустое значение поля означает, что нет максимального срока действия пароля, нет периода предупреждения о пароле и нет периода неактивности пароля (смотрите далее).

Если максимальный срок действия пароля меньше чем минимальный срок действия пароля, то пользователь не сможет изменить свой пароль.

password warning period
Количество дней до устаревания пароля (смотрите максимальный срок действия пароля) во время которых пользователю выдаётся предупреждение.

Пустое значение поля и 0 отключают период предупреждения о пароле.

password inactivity period
Количество дней после устаревания пароля (смотрите максимальный срок действия пароля)

во время которых пароль всё ещё принимается (и пользователь должен обновить свой пароль при следующем входе).

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

Пустое значение поля означает, что период неактивности отсутствует.

account expiration date
The date of expiration of the account, expressed as the number of days since Jan 1, 1970 00:00 UTC.

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.

Пустое значение обозначает, что учётная запись никогда не устаревает.

Значение 0 не должно использоваться, так как это может рассматриваться как неустаревающая учётная запись или что запись устарела 1 января 1970 года.

reserved field
Это поле зарезервировано для использования в будущем.

ФАЙЛЫ

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

/etc/shadow−
резервная копия файла /etc/shadow

Заметим, что этот файл используется программами из комплекта утилит shadow, но не всеми инструментами управления пользователями и паролями.

СМОТРИТЕ ТАКЖЕ

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

НАЗВАНИЕ

suauth − файл управления командой su

СИНТАКСИС

/etc/suauth

ОПИСАНИЕ

Файл /etc/suauth проверяется каждый раз при запуске команды su. Он влияет на поведение команды su, в зависимости от:

1) the user su is targeting

2) пользователя, запустившего команду su (или группы, членом которой он может быть)

Формат файла показан ниже, строки начинающиеся с # считаются комментарием и игнорируются;

to−id:from−id:ACTION

Где желаемый−id может быть словом *ALL*, списком имён пользователей, перечисленных через запятую («,») или фразы *ALL EXCEPT*, после которой идёт список имён пользователей перечисленных через «,».

from−id is formatted the same as to−id except the extra word *GROUP* is recognized. *ALL EXCEPT GROUP* is perfectly valid too. Following *GROUP* appears one or more group names, delimited by ",". It is not sufficient to have primary group id of the relevant group, an entry in **/etc/group**(5) is necessary.

В поле ДЕЙСТВИЕ может быть только одно из следующих значений:

DENY
: Команда su останавливает выполнение, даже не спрашивая пароль.

NOPASS
: Команда su выполняется без запроса пароля.

OWNPASS
: Чтобы успешно выполнить команду su, пользователь должен ввести свой собственный пароль.

Заметим, что тут используются три поля, разделённых двоеточиями. Никаких пробелов не допускается около двоеточий. Также заметим, что файл просматривается строка за строкой, и первое подходящее правило будет использовано без проверки оставшихся правил. Это позволяет системному администратору осуществлять любой контроль, какой он пожелает.

ПРИМЕР

```
# sample /etc/suauth file
#
# A couple of privileged usernames may
# su to root with their own password.
#
root:chris,birddog:OWNPASS
#
# Anyone else may not su to root unless in
# group wheel. This is how BSD does things.
#
root:ALL EXCEPT GROUP wheel:DENY
#
# Perhaps terry and birddog are accounts
# owned by the same person.
# Access can be arranged between them
# with no password.
```

```
#
terry:birddog:NOPASS
birddog:terry:NOPASS
#
```

ФАЙЛЫ

/etc/suauth

ОШИБКИ РЕАЛИЗАЦИИ

Может быть несколько угроз. Анализатор файла, в частности, не прощает синтаксических ошибок, ожидая, что не будет недопустимых пробелов (кроме как в начале и конце строк) и специальных слов, разделяющих различные вещи.

ДИАГНОСТИКА

Ошибки при анализе файла выводятся с помощью *syslogd*(8) с уровнем ERR средства AUTH.

СМОТРИТЕ ТАКЖЕ

su(1).

НАЗВАНИЕ

chgpasswd − обновляет пароли групп в пакетном режиме

СИНТАКСИС

chgpasswd [*options*]

ОПИСАНИЕ

Программа **chgpasswd** читает список пар «группа пароль » из стандартного входного потока и обновляет информацию о существующих группах. Каждая строка имеет вид:

имя_группы:пароль

По умолчанию, передаваемый пароль должен быть в виде обычного текста и шифруется командой **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.

Данная команда предназначена для работы в крупных системных средах, где за один раз заводится несколько учётных записей.

ПАРАМЕТРЫ

Параметры команды **chgpasswd**:

−c, **−−crypt−method**
Использовать указанный метод для шифрования паролей.

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

−e, **−−encrypted**
Передаваемые пароли заданы в шифрованном виде.

−h, **−−help**
Показать краткую справку и закончить работу.

−m, **−−md5**
Использовать алгоритм шифрования MD5 вместо DES, если пароли передаются не шифрованными.

−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, **−−sha−rounds**
Использовать указанное количество раундов шифрования паролей.

You can only use this option with crypt method: *SHA256 SHA512*

By default, the number of rounds for SHA256 or SHA512 is defined by the SHA_CRYPT_MIN_ROUNDS and SHA_CRYPT_MAX_ROUNDS variables in /etc/login.defs.

A minimal value of 1000 and a maximal value of 999,999,999 will be enforced for SHA256 and SHA512. The default number of rounds is 5000.

ПРЕДОСТЕРЕЖЕНИЯ

Не забудьте установить права или umask, чтобы не позволить чтение не шифрованных файлов другими пользователями.

Вы должны проверить, что пароль и метод шифрования соответствует политике системных паролей.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

СМОТРИТЕ ТАКЖЕ

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

НАЗВАНИЕ

chpasswd − обновляет пароли в пакетном режиме

СИНТАКСИС

chpasswd [*options*]

ОПИСАНИЕ

Программа **chpasswd** читает список пар «пользователь пароль » из стандартного входного потока и обновляет информацию о существующих пользователях. Каждая строка имеет вид:

имя_пользователя:пароль

По умолчанию, передаваемый пароль должен быть в виде обычного текста и шифруется командой **chpasswd**. Также, если есть срок действия пароля, то он будет обновлён.

The default encryption algorithm can be defined for the system with the **ENCRYPT_METHOD** or **MD5_CRYPT_ENAB** variables of /etc/login.defs, and can be overwritten with the **−e**, **−m**, or **−c** options.

chpasswd first updates all the passwords in memory, and then commits all the changes to disk if no errors occurred for any user.

Данная команда предназначена для работы в крупных системных средах, где за один раз заводится несколько учётных записей.

ПАРАМЕТРЫ

Параметры команды **chpasswd**:

−c, **−−crypt−method** *METHOD*
Использовать указанный метод для шифрования паролей.

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

По умолчанию (если не указан параметр**−c**, **−m** или **−e**), метод шифрования определяется переменной **ENCRYPT_METHOD** или **MD5_CRYPT_ENAB** из файла /etc/login.defs.

−e, **−−encrypted**
Передаваемые пароли заданы в шифрованном виде.

−h, **−−help**
Показать краткую справку и закончить работу.

−m, **−−md5**
Использовать алгоритм шифрования MD5 вместо DES, если пароли передаются не шифрованными.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes to configuration files under the root filesystem found under the directory *PREFIX_DIR*. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−s, **−−sha−rounds** *ROUNDS*
Использовать указанное количество раундов шифрования паролей.

You can only use this option with crypt method: *SHA256 SHA512*

By default, the number of rounds for SHA256 or SHA512 is defined by the SHA_CRYPT_MIN_ROUNDS and SHA_CRYPT_MAX_ROUNDS variables in /etc/login.defs.

A minimal value of 1000 and a maximal value of 999,999,999 will be enforced for SHA256 and

SHA512. The default number of rounds is 5000.

ПРЕДОСТЕРЕЖЕНИЯ

Не забудьте установить права или umask, чтобы не позволить чтение не шифрованных файлов другими пользователями.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

СМОТРИТЕ ТАКЖЕ

passwd(1), *newusers*(8), *login.defs*(5), *useradd*(8).

НАЗВАНИЕ

faillog − показывает записи из файла faillog или задаёт предел неудачных попыток входа в систему

СИНТАКСИС

faillog [*options*]

ОПИСАНИЕ

Программа **faillog** показывает содержимое журнала неудачных попыток (файл /var/log/faillog). Также она может быть использована для управления счётчиком неудачных попыток и их ограничением. При запуске **faillog** без параметров выводятся записи faillog только тех пользователей, у которых имеется хотя бы одна неудачная попытка входа.

ПАРАМЕТРЫ

Параметры команды **faillog**:

−a, **−−all**
Показать записи faillog для всех пользователей из базы данных faillog.

Список пользователей можно ограничить с помощью параметра **−u**.

В режиме вывода это ограничивает вывод списком существующих пользователей, но при этом для них выводятся даже пустые записи faillog.

Параметры **−l**, **−m**, **−r**, **−t** изменяют записи пользователей, даже если они не существует в системе. Это полезно для сброса записей пользователей, которые были удалены или для предварительной установки политики для диапазона пользователей.

−h, **−−help**
Показать краткую справку и закончить работу.

−l, **−−lock−secs** *SEC*
Блокировать учётную запись на указанное количество СЕКУНД после неудачной попытки входа.

Для этого параметра требуется право на запись в /var/log/faillog.

−m, **−−maximum** *MAX*
Установить максимальное количество неудачных попыток входа перед блокировкой учётной записи равным МАКС_ЧИСЛО.

Если значение МАКС_ЧИСЛО равно 0, то количество неудачных попыток входа не ограничивается.

Для предотвращения атаки отказа в обслуживании максимальное количество неудачных попыток входа у *root* всегда должно быть равно 0.

Для этого параметра требуется право на запись в /var/log/faillog.

−r, **−−reset**
Сбросить счётчик неудачных попыток входа.

Для этого параметра требуется право на запись в /var/log/faillog.

−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.

−t, **−−time** *DAYS*
Показать записи faillog новее чем ДНЕЙ.

−u, **−−user** *LOGIN|RANGE*
Показать запись faillog или изменить счётчики неудачных попыток и ограничения (если задан параметр **−l**, **−m** или **−r**) только для указанных учётных записей.

Пользователя можно указать по отдельному имени, числовому идентификатору или в виде ДИАПАЗОНА пользователей. Такой ДИАПАЗОН можно задавать в виде максимального и минимального значений(*UID*_МИН−*UID*_МАКС), максимального (−*UID*_МАКС) или минимального (*UID*_МИН−) значения.

Если параметры **−l**, **−m** или **−r** не заданы, то **faillog** показывает записи faillog указанных пользователей.

ПРЕДОСТЕРЕЖЕНИЯ

Программа **faillog** выводит только записи о пользователях, последняя попытка входа которых была неудачной. Чтобы увидеть запись о пользователе, последняя попытка входа которого была удачной, вы должны специально указать имя пользователя с помощью параметра **−u**, или для показа всех пользователей указать параметр **−a**.

ФАЙЛЫ

/var/log/faillog
: журнал неудавшихся попыток входа в систему

СМОТРИТЕ ТАКЖЕ

login(1), *faillog*(5).

НАЗВАНИЕ

groupadd − создаёт новую группу

СИНТАКСИС

groupadd [*OPTIONS*] *NEWGROUP*

ОПИСАНИЕ

Программа **groupadd** создаёт новую группу согласно указанным значениям командной строки и системным значениям по умолчанию. Новая группа будет добавлена в системные файлы.

Groupnames may contain only lower and upper case letters, digits, underscores, or dashes. They can end with a dollar sign. Dashes are not allowed at the beginning of the groupname. Fully numeric groupnames and groupnames . or .. are also disallowed.

Groupnames may only be up to 32 characters long.

ПАРАМЕТРЫ

Параметры команды **groupadd**:

−f, **−−force**
Завершить работу и вернуть состояние успешного выполнения, если группа уже существует. Если используется вместе с параметром **−g** и указанный GID уже существует, то выбирается другой (уникальный) GID (то есть параметр **−g** игнорируется).

−g, **−−gid** *GID*
The numerical value of the group's ID. *GID* must be unique, unless the **−o** option is used. The value must be non−negative. The default is to use the smallest ID value greater than or equal to **GID_MIN** and greater than every other group.

Смотрите также описание **−r** и **GID_MAX**.

−h, **−−help**
Показать краткую справку и закончить работу.

−K, **−−key** *KEY=VALUE*
Изменить значения по умолчанию (GID_MIN, GID_MAX и другие), которые хранятся в файле /etc/login.defs. Можно указать несколько параметров **−K**.

Example: **−K** *GID_MIN=100* **−K** *GID_MAX=499*

Note: **−K** *GID_MIN=10*,*GID_MAX=499* doesn't work yet.

−o, **−−non−unique**
permits the creation of a group with an already used numerical ID. As a result, for this *GID*, the mapping towards group *NEWGROUP* may not be unique.

−p, **−−password** *PASSWORD*
defines an initial password for the group account. PASSWORD is expected to be encrypted, as returned by **crypt** (3).

Without this option, the group account will be locked and with no password defined, i.e. a single exclamation mark in the respective field of ths system account file /etc/group or /etc/gshadow.

Замечание**:** Этот параметр использовать не рекомендуется, так как пароль (или не шифрованный пароль) будет видим другими пользователям в списке процессов.

Вы должны проверить, что пароль соответствует политике системных паролей.

−r, **−−system**
Создать системную группу.

Числовые идентификаторы для системных групп выбираются из диапазона **SYS_GID_MIN**−**SYS_GID_MAX**, определённых в login.defs, а не из **GID_MIN**−**GID_MAX**.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes to configuration files under the root filesystem found under the directory *PREFIX_DIR*. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−U, **−−users**
A list of usernames to add as members of the group.

Поведение по умолчанию (если не указан параметр **−g**, **−N** и **−U**) определяется переменной **USERGROUPS_ENAB** из файла /etc/login.defs.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/gshadow
содержит защищаемую информацию о группах

/etc/login.defs
содержит конфигурацию подсистемы теневых паролей

ПРЕДОСТЕРЕЖЕНИЯ

Нельзя добавить группу NIS или LDAP. Это необходимо делать на соответствующем сервере.

Если имя группы уже существует во внешней базе данных групп, например в NIS или LDAP, то **groupadd** не станет создавать группу.

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
success

2
invalid command syntax

3
invalid argument to option

4
GID is already used (when called without **−o**)

9
group name is already used

10
can't update group file

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *gpasswd*(8), *groupdel*(8), *groupmod*(8), *login.defs*(5), *useradd*(8), *userdel*(8), *usermod*(8).

НАЗВАНИЕ

groupdel − удаляет группу

СИНТАКСИС

groupdel [*options*] *GROUP*

ОПИСАНИЕ

Программа **groupdel** изменяет системные файлы учётных записей, удаляя все записи, относящиеся к ГРУППЕ. Группа с таким именем должна существовать.

ПАРАМЕТРЫ

Параметры команды **groupdel**:

−f, **−−force**
This option forces the removal of the group, even if there's some user having the group as the primary one.

−h, **−−help**
Показать краткую справку и закончить работу.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes in the *PREFIX_DIR* directory and use the configuration files from the *PREFIX_DIR* directory. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

ПРЕДОСТЕРЕЖЕНИЯ

Вы не можете удалить группу, если она является первичной для существующего пользователя. Вы должны удалить пользователя перед тем как удалять группу.

Вы должны вручную проверить все файловые системы, чтобы убедиться, что не осталось файлов, принадлежащих удалённой группе.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/gshadow
содержит защищаемую информацию о группах

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
success

2
invalid command syntax

6
specified group doesn't exist

8
can't remove user's primary group

10
can't update group file

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *gpasswd*(8), *groupadd*(8), *groupmod*(8), *useradd*(8), *userdel*(8), *usermod*(8).

НАЗВАНИЕ

groupmems − управляет членами первичной группы пользователя

СИНТАКСИС

groupmems −a *user_name* | −d *user_name* | [−g *group_name*] | −l | −p

ОПИСАНИЕ

Программа **groupmems** позволяет пользователю управлять списком членов своей группы не имея привилегий суперпользователя. Программа **groupmems** работает в системах, где в качестве первичной группы пользователя является группа с именем совпадающим с именем пользователя (то есть, guest / guest).

Только суперпользователь как администратор может использовать **groupmems**, чтобы изменить список членов не своей группы.

ПАРАМЕТРЫ

Параметры команды **groupmems**:

−a, **−−add** *user_name*
Add a user to the group membership list.

Если существует файл /etc/gshadow и записи о группе нет в файле /etc/gshadow, то будет создана новая запись.

−d, **−−delete** *user_name*
Удалить пользователя из группы.

Если существует файл /etc/gshadow, то пользователь будет удалён из списка членов и администраторов группы.

Если существует файл /etc/gshadow и записи о группе нет в файле /etc/gshadow, то будет создана новая запись.

−g, **−−group** *group_name*
Суперпользователь может указать группу, в которой нужно изменить список членов.

−h, **−−help**
Показать краткую справку и закончить работу.

−l, **−−list**
Показать список членов группы.

−p, **−−purge**
Вычистить всех пользователей из списка членов группы.

Если существует файл /etc/gshadow и записи о группе нет в файле /etc/gshadow, то будет создана новая запись.

−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.

НАСТРОЙКА

The **groupmems** executable should be in mode 2710 as user *root* and in group *groups*. The system administrator can add users to group *groups* to allow or disallow them using the **groupmems** utility to manage their own group membership list.

```
$ groupadd −r groups
$ chmod 2710 groupmems
$ chown root:groups groupmems
$ groupmems −g groups −a gk4
```

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *groupadd*(8), *groupdel*(8), *useradd*(8), *userdel*(8), *usermod*(8).

НАЗВАНИЕ

groupmod − изменяет определение группы в системе

СИНТАКСИС

groupmod [*options*] *GROUP*

ОПИСАНИЕ

Команда **groupmod** изменяет определение указанной ГРУППЫ, изменяя соответствующую запись в базе данных групп.

ПАРАМЕТРЫ

Параметры команды **groupmod**:

−a, **−−append** *GID*
If group members are specified with −U, append them to the existing member list, rather than replacing it.

−g, **−−gid** *GID*
Имя группы будет изменено с ГРУППА на *GID*.

Десятичное значение *GID* должно быть неотрицательным. Это значение должно быть уникальным, если не указан параметр **−o**.

У пользователей, которых эта группа является первичной, будет выполнено соответствующее обновление.

У всех файлов, которые имеют ID старой группы и должны продолжать принадлежать *GROUP*, нужно изменить их ID вручную.

Никаких проверок по **GID_MIN**, **GID_MAX**, **SYS_GID_MIN** или **SYS_GID_MAX** из /etc/login.defs не производится.

−h, **−−help**
Показать краткую справку и закончить работу.

−n, **−−new−name** *NEW_GROUP*
Имя группы будет изменено с ГРУППА на НОВАЯ_ГРУППА.

−o, **−−non−unique**
При использовании с параметром **−g** разрешается изменять *GID* группы не уникальным значением.

−p, **−−password** *PASSWORD*
The encrypted password, as returned by *crypt*(3).

Замечание**:** Этот параметр использовать не рекомендуется, так как пароль (или не шифрованный пароль) будет видим другими пользователям в списке процессов.

Вы должны проверить, что пароль соответствует политике системных паролей.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes in the *PREFIX_DIR* directory and use the configuration files from the *PREFIX_DIR* directory. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−U, **−−users**
A list of usernames to add as members of the group.

Поведение по умолчанию (если не указан параметр **−g**, **−N** и **−U**) определяется переменной

USERGROUPS_ENAB из файла /etc/login.defs.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

/etc/passwd
: содержит информацию о пользователях

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
: E_SUCCESS: success

2
: E_USAGE: invalid command syntax

3
: E_BAD_ARG: invalid argument to option

4
: E_GID_IN_USE: group id already in use

6
: E_NOTFOUND: specified group doesn't exist

9
: E_NAME_IN_USE: group name already in use

10
: E_GRP_UPDATE: can't update group file

11
: E_CLEANUP_SERVICE: can't setup cleanup service

12
: E_PAM_USERNAME: can't determine your username for use with pam

13
: E_PAM_ERROR: pam returned an error, see syslog facility id groupmod for the PAM error message

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *gpasswd*(8), *groupadd*(8), *groupdel*(8), *login.defs*(5), *useradd*(8), *userdel*(8), *usermod*(8).

НАЗВАНИЕ

grpck − проверяет корректность файлов групп

СИНТАКСИС

grpck [options] [*group* [*shadow*]]

ОПИСАНИЕ

The **grpck** command verifies the integrity of the groups information. It checks that all entries in /etc/group and /etc/gshadow 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.

Выполняются следующие проверки:

- правильное количество полей
- уникальность и корректность имени группы
- a valid group identifier (/etc/group only)
- a valid list of members and administrators
- соответствие записи в файле /etc/gshadow (и /etc/group при проверках gshadow)

Ошибки в количестве полей и уникальности имён групп невосстановимы. Если запись содержит неверное число полей, пользователя попросят подтвердить удаление всей строки. Если пользователь ответит отрицательно, дальнейшая проверка выполняться не будет. При ошибке повторения имени группы также возникает запрос на удаление, но в случае отказа проверка будет продолжена. Обо всех остальных ошибках выводится предупреждение и пользователю предлагается запустить команду **groupmod**, чтобы исправить ошибку.

The commands which operate on the /etc/group and /etc/gshadow files are not able to alter corrupted or duplicated entries. **grpck** should be used in those circumstances to remove the offending entries.

ПАРАМЕТРЫ

Параметры **−r**, **−s** не могут использоваться одновременно.

Параметры команды **grpck**:

−h, **−−help**
Показать краткую справку и закончить работу.

−r, **−−read−only**
Запускать команду **grpck** в режиме только для чтения. При этом на все вопросы об изменениях устанавливается ответ нет и участие пользователя не требуется.

−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/group and /etc/gshadow by GID.

−S, **−−silence−warnings**
Suppress more controversial warnings, in particular warnings about inconsistency between group members listed in /etc/group and /etc/ghadow.

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

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/gshadow
содержит защищаемую информацию о группах

/etc/passwd

содержит информацию о пользователях

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
success

1
invalid command syntax

2
one or more bad group entries

3
can't open group files

4
can't lock group files

5
can't update group files

СМОТРИТЕ ТАКЖЕ

group(5), *groupmod*(8), *gshadow*(5), *passwd*(5), *pwck*(8), *shadow*(5).

НАЗВАНИЕ

lastlog − выводит отчёт о последней регистрации в системе всех или указанного пользователя

СИНТАКСИС

lastlog [*options*]

ОПИСАНИЕ

Программа **lastlog** упорядочивает и выводит содержимое файла /var/log/lastlog, который содержит даты последнего входа пользователей в систему. Выводятся имя пользователя, порт и дата последнего входа в систему. По умолчанию (вызов без параметров) показываются записи файла lastlog, отсортированные согласно расположению пользователей в файле /etc/passwd.

ПАРАМЕТРЫ

Параметры команды **lastlog**:

−b, **−−before** *DAYS*
Print only lastlog records older than *DAYS*.

−C, **−−clear**
Clear lastlog record of a user. This option can be used only together with **−u** (**−−user**)).

−h, **−−help**
Показать краткую справку и закончить работу.

−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, **−−set**
Set lastlog record of a user to the current time. This option can be used only together with **−u** (**−−user**)).

−t, **−−time** *DAYS*
Print the lastlog records more recent than *DAYS*.

−u, **−−user** *LOGIN|RANGE*
Показать запись lastlog только для указанного пользователя(ей).

Пользователя можно указать по отдельному имени, числовому идентификатору или в виде ДИАПАЗОНА пользователей. Такой ДИАПАЗОН можно задавать в виде максимального и минимального значений(*UID*_МИН−*UID*_МАКС), максимального (−*UID*_МАКС) или минимального (*UID*_МИН−) значения.

Если пользователь никогда не регистрировался в системе, то будет показано сообщение ** Никогда не входил в систему** вместо названия порта и даты.

Будут показаны записи только для пользователей, имеющих в системе данный момент. В журнале могут существовать записи для удалённых ранее пользователей.

ЗАМЕЧАНИЕ

Файл lastlog содержит информацию о последней регистрации в системе каждого пользователя. Вы не должны применять к нему ротацию журнальных файлов. Этот файл является разреженным, поэтому его размер на диске гораздо меньше, чем показывает команда «**ls −l**» (которая может показывать, что это очень большой файл, если значения идентификаторов пользователей в системе достигают больших значений). Чтобы увидеть реальный размер введите «**ls −s**».

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/var/log/lastlog
содержит список завершённых сеансов работы с системой

ПРЕДОСТЕРЕЖЕНИЯ

Большие промежутки в значениях идентификаторов пользователей приводят к тому, что программа некоторое время ничего не выводит на экран (то есть, если в базе данных lastlog нет

пользователей с идентификаторами с 170 по 800, то во время обработки UID с 171 по 799 программа кажется повисшей).

Having high UIDs can create problems when handling the <term> /var/log/lastlog</term> with external tools. Although the actual file is sparse and does not use too much space, certain applications are not designed to identify sparse files by default and may require a specific option to handle them.

НАЗВАНИЕ

logoutd − контролирует временные интервалы работы в системе

СИНТАКСИС

logoutd

ОПИСАНИЕ

Программа **logoutd** контролирует временные ограничения работы в системе и порты, заданные в файле /etc/porttime. Программа **logoutd** должна запускаться из сценария /etc/rc. Файл /var/run/utmp периодически сканируется и для каждого имени пользователя проверяется, разрешено ли данному пользователю работать в настоящий момент на данном порту. Любой сеанс, который нарушает ограничения, описанные в файле /etc/porttime, будет завершён.

ФАЙЛЫ

/etc/porttime
: содержит разрешённое время работы определённых пользователей с определённых портов

/var/run/utmp
: содержит список работающих сеансов в системе

НАЗВАНИЕ

newusers − обновляет и создаёт новые учётные записи пользователей в пакетном режиме

СИНТАКСИС

newusers [*options*] [*file*]

ОПИСАНИЕ

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
: Имя пользователя.

  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
: Это поле будет зашифровано и использовано как новое значение шифрованного пароля.

pw_uid
: Это поле используется для определения UID пользователя.

  If the field is empty, a new (unused) UID will be defined automatically by **newusers**.

  Если в этом поле указано число, то оно будет использовано в качестве 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.

  Если изменяется UID существующего пользователя, то у файлов, которыми владел этот пользователь, нужно вручную переопределить владельца.

pw_gid
: Это поле используется для определения ID первичной группы пользователя.

  Если в этом поле содержится имя существующей группы (или группы, созданной **newusers** ранее), то в качестве ID первичной группы пользователя будет использован GID этой группы.

  Если в этом поле содержится число, то это число будет использовано как ID первичной группы пользователя. Если с таким GID не существует, то будет создана новая группа с этим GID и именем пользователя.

  Если это поле пусто, то новая группа будет создана с именем пользователя, а GID будет определён **newusers** автоматически (для использования в качестве ID первичной группы пользователя и GID новой группы).

  Если поле содержит имя группы, которой не существует (и которая не была создана **newusers** ранее), то будет создана новая группа с указанным именем, GID будет определён **newusers** автоматически (для использования в качестве ID первичной группы пользователя и GID новой группы).

pw_gecos
: Это поле копируется в поле GECOS записи пользователя.

pw_dir
: Это поле используется для определения домашнего каталога пользователя.

  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.

Если изменяется домашний каталог существующего пользователя, то команда **newusers** не перемещает или копирует содержимое старого каталога в новое место. Это нужно выполнить вручную.

pw_shell
В этом поле задаётся пользовательская оболочка. Никаких проверок поля не делается.

Команда **newusers** сначала пытается создать или изменить всех указанных пользователей, а затем записать эти изменения в базы данных пользователей или групп. Если происходит ошибка (кроме ошибок при последней записи в базы данных), то изменения в базы не сохраняются.

Данная команда предназначена для работы в крупных системных средах, где за один раз обновляется несколько учётных записей.

ПАРАМЕТРЫ

Параметры команды **newusers**:

−−badname
Allow names that do not conform to standards.

−c, **−−crypt−method**
Использовать указанный метод для шифрования паролей.

Возможные методы: DES, MD5, NONE и SHA256 или SHA512, если эти методы поддерживается libc.

−h, **−−help**
Показать краткую справку и закончить работу.

−r, **−−system**
Создать системную учётную запись.

Системные пользователи создаются без информации об устаревании в /etc/shadow, и их числовые идентификаторы выбираются из диапазона **SYS_UID_MIN**−**SYS_UID_MAX**, определённого в login.defs, а не из **UID_MIN**−**UID_MAX** (это же касается и части с **GID** при создании групп).

−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, **−−sha−rounds**
Использовать указанное количество раундов шифрования паролей.

You can only use this option with crypt method: *SHA256 SHA512*

By default, the number of rounds for SHA256 or SHA512 is defined by the SHA_CRYPT_MIN_ROUNDS and SHA_CRYPT_MAX_ROUNDS variables in /etc/login.defs.

A minimal value of 1000 and a maximal value of 999,999,999 will be enforced for SHA256 and SHA512. The default is 5000.

ПРЕДОСТЕРЕЖЕНИЯ

Файл с входными данными должен быть защищён, так как в нём содержатся не шифрованные пароли.

Вы должны проверить, что пароль и метод шифрования соответствует политике системных паролей.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

/etc/subgid
: Per user subordinate group IDs.

/etc/subuid
: Per user subordinate user IDs.

СМОТРИТЕ ТАКЖЕ

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

НАЗВАНИЕ

nologin − вежливо отказывает во входе в систему

СИНТАКСИС

nologin

ОПИСАНИЕ

Программа **nologin** выдаёт сообщение, что учётная запись недоступна и завершает работу с ненулевым кодом возврата. Она предназначена для замены оболочки командной строки в поле оболочки у заблокированных учётных записей.

To disable all logins, investigate *nologin*(5).

If **SSH_ORIGINAL_COMMAND** is populated it will be logged.

СМОТРИТЕ ТАКЖЕ

login(1), *nologin*(5).

ИСТОРИЯ

The **nologin** command appeared in BSD 4.4.

НАЗВАНИЕ

pwck − verify the integrity of password files

СИНТАКСИС

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

ОПИСАНИЕ

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.

Выполняются следующие проверки:

- правильное количество полей
- уникальность и корректность имени пользователя
- корректность идентификатора пользователя и группы
- корректность первичной группы
- корректность домашнего каталога
- корректность регистрационной оболочки

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

Выполняются следующие проверки:

- что каждая запись passwd имеет соответствующую запись shadow и каждая запись shadow имеет соответствующую запись passwd
- пароли указаны в теневом файле
- записи shadow содержат корректное количество полей
- записи shadow уникальны в shadow
- дата последней смены пароля не находится в будущем

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.

Команды, которые работают с файлом /etc/passwd, не могут изменять повреждённые или дублирующиеся записи. Как раз в этом случае и нужно использовать **pwck** для удаления испорченной записи.

ПАРАМЕТРЫ

Параметры **−r**, **−s** не могут использоваться одновременно.

Параметры команды **pwck**:

−−badname
Allow names that do not conform to standards.

−h, **−−help**
Показать краткую справку и закончить работу.

−q, **−−quiet**
Сообщать только об ошибках. Предупреждения, которые не требуют от пользователя никаких действий, показаны не будут.

−r, **−−read−only**
Выполнять команду **pwck** в режиме «только чтение ».

−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**
Отсортировать все записи в файлах /etc/passwd и /etc/shadow по числовому идентификатору пользователя.

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

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

СМОТРИТЕ ТАКЖЕ

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

НАЗВАНИЕ

pwconv, pwunconv, grpconv, grpunconv − преобразует пароли пользователей и групп в/из защищённую форму

СИНТАКСИС

pwconv [*options*]

pwunconv [*options*]

grpconv [*options*]

grpunconv [*options*]

ОПИСАНИЕ

Команда **pwconv** создаёт файл *shadow* из файла *passwd* и необязательно существующего файла *shadow*.

Команда **pwunconv** создаёт файл *passwd* из файлов *passwd* и *shadow*, а затем удаляет файл *shadow*.

Команда **grpconv** создаёт файл *gshadow* из файла *group* и необязательно существующего файла *gshadow*.

Команда **grpunconv** создаёт файл *group* из файлов *group* и *gshadow*, а затем удаляет файл *gshadow*.

Эти четыре программы работают с файлами обычных или теневых паролей пользователей и групп: /etc/passwd, /etc/group, /etc/shadow и /etc/gshadow.

Каждая программа выполняет необходимые блокировки перед преобразованиями. Команды **pwconv** и **grpconv** выполняют схожий порядок действий. Сначала удаляются записи из теневого файла которых нет в главном файле. Затем обновляются записи в теневом файле которые не содержат «x» вместо пароля в главном файле. Далее добавляются отсутствующие теневые записи. Наконец, пароли в главном файле заменяются символом «x». Данные программы можно использовать как для первоначального преобразования, так и для обновления теневого файла, если главный файл редактировался вручную.

Команда **pwconv** использует значения переменных *PASS_MIN_DAYS*, *PASS_MAX_DAYS* и *PASS_WARN_AGE* из файла /etc/login.defs при добавлении новых записей в файл /etc/shadow.

Программы **pwunconv** и **grpunconv** также выполняют схожий порядок действий. Пароли в главном файле обновляются из теневого файла. Записи, которые существуют в главном файле, но не существуют в теневом файле оставляются как есть. По окончании, теневой файл удаляется. Информация об устаревании пароля не учитывается программой **pwunconv**. Конвертируется только возможное.

ПАРАМЕТРЫ

Параметры, применимые к **pwconv**, **pwunconv**, **grpconv** и **grpunconv**:

−h, **−−help**
Показать краткую справку и закончить работу.

−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.

ОШИБКИ РЕАЛИЗАЦИИ

Ошибки в файлах паролей или групп (типа неверных или дублирующихся записей) могут зациклить программу или произойдут какие−то другие странные вещи . Перед конвертацией запустите **pwck** и **grpck**, чтобы исправить возможные ошибки.

НАСТРОЙКА

Следующая переменная настройки в /etc/login.defs изменяет поведение **grpconv** и **grpunconv**:

Следующая переменная настройки в /etc/login.defs изменяет поведение **pwconv**:

ФАЙЛЫ

/etc/login.defs
содержит конфигурацию подсистемы теневых паролей

СМОТРИТЕ ТАКЖЕ

grpck(8), *login.defs*(5), *pwck*(8).

НАЗВАНИЕ

useradd − регистрирует нового пользователя или изменяет информацию по умолчанию о новых пользователях

СИНТАКСИС

useradd [*options*] *LOGIN*

useradd −D

useradd −D [*options*]

ОПИСАНИЕ

При запуске без параметра **−D** команда **useradd** создаёт новую учётную запись пользователя, используя значения из командной строки и системные значения по умолчанию. В зависимости от параметров командной строки, команда **useradd** обновляет системные файлы, а также может создать домашний каталог нового пользователя и скопировать начальные файлы настроек.

По умолчанию, для нового пользователя также создаётся группа (смотрите параметры **−g**, **−N**, **−U** и **USERGROUPS_ENAB**).

ПАРАМЕТРЫ

Параметры команды **useradd**:

−−badname
Allow names that do not conform to standards.

−b, **−−base−dir** *BASE_DIR*
The default base directory for the system if **−d** *HOME_DIR* is not specified. *BASE_DIR* is concatenated with the account name to define the home directory.

Если этот параметр не задан, то команда **useradd** будет использовать базовый каталог, указанный в переменной **HOME** в файле /etc/default/useradd иначе /home (по умолчанию).

−c, **−−comment** *COMMENT*
Any text string. It is generally a short description of the account, and is currently used as the field for the user's full name.

−d, **−−home−dir** *HOME_DIR*
The new user will be created using *HOME_DIR* as the value for the user's login directory. The default is to append the *LOGIN* name to *BASE_DIR* and use that as the login directory name. If the directory *HOME_DIR* does not exist, then it will be created unless the **−M** option is specified.

−D, **−−defaults**
Смотрите далее в подразделе «Изменение значений по умолчанию ».

−e, **−−expiredate** *EXPIRE_DATE*
Дата, когда учётная запись пользователя будет заблокирована. Дата задаётся в формате ГГГГ−ММ−ДД.

Если этот параметр не задан, то команда **useradd** будет использовать дату устаревания по умолчанию, указанную в переменной **EXPIRE** в файле /etc/default/useradd, иначе пустую строку (без устаревания, по умолчанию).

−f, **−−inactive** *INACTIVE*
defines the number of days after the password exceeded its maximum age where the user is expected to replace this password. The value is stored in the shadow password file. An input of 0 will disable an expired password with no delay. An input of −1 will blank the respective field in the shadow password file. See *shadow*(5)for more information.

Если этот параметр не задан, то команда **useradd** будет использовать срок неактивности по умолчанию, указанный в переменной **INACTIVE** в файле /etc/default/useradd или −1 (по умолчанию).

−F, **−−add−subids−for−system**
Update /etc/subuid and /etc/subgid even when creating a system account with **−r** option.

−g, **−−gid** *GROUP*
The name or the number of the user's primary group. The group name must exist. A group number must refer to an already existing group.

If not specified, the behavior of **useradd** will depend on the **USERGROUPS_ENAB** variable in /etc/login.defs. If this variable is set to *yes* (or **−U/−−user−group** is specified on the command line), a group will be created for the user, with the same name as her loginname. If the variable is set to *no* (or **−N/−−no−user−group** is specified on the command line), useradd will set the primary group of the new user to the value specified by the **GROUP** variable in /etc/default/useradd, or 1000 by default.

−G, **−−groups** *GROUP1*[,*GROUP2*,...[,*GROUPN*]]]
A list of supplementary groups which the user is also a member of. Each group is separated from the next by a comma, with no intervening whitespace. The groups are subject to the same restrictions as the group given with the **−g** option. The default is for the user to belong only to the initial group. In addition to passing in the −G flag, you can add the option **GROUPS** to the file /etc/default/useradd which in turn will add all users to those supplementary groups.

−h, **−−help**
Показать краткую справку и закончить работу.

−k, **−−skel** *SKEL_DIR*
Каталог с шаблонами, который содержит файлы и каталоги для копирования в домашний каталог пользователя при создании домашнего каталога командой **useradd**.

Этот параметр можно использовать только с параметром **−m** (или **−−create−home**).

Если этот параметр не задан, то каталог шаблонов определяется переменной **SKEL** из файла /etc/default/useradd, или равен /etc/skel (по умолчанию).

Если возможно, выполняется копирование ACL и расширенных атрибутов.

−K, **−−key** *KEY=VALUE*
Overrides /etc/login.defs defaults (**UID_MIN**, **UID_MAX**, **UMASK**, **PASS_MAX_DAYS** and others).

Example: **−K** *PASS_MAX_DAYS =−1* can be used when creating an account to turn off password aging. Multiple **−K** options can be specified, e.g.: **−K** *UID_MIN =100* **−K** *UID_MAX=499*

−l, **−−no−log−init**
Не добавлять пользователя в базы данных lastlog и faillog.

By default, the user's entries in the lastlog and faillog databases are reset to avoid reusing the entry from a previously deleted user.

If this option is not specified, **useradd** will also consult the variable **LOG_INIT** in the /etc/default/useradd if set to no the user will not be added to the lastlog and faillog databases.

−m, **−−create−home**
Создать домашний каталог пользователя, если он не существует. Файлы и каталоги, содержащиеся в каталоге шаблонов (который можно указать с помощью параметра the **−k** option), будут скопированы в домашний каталог.

По умолчанию, если этот параметр не указан и не задана переменная **CREATE_HOME**, домашний каталог не создаётся.

The directory where the user's home directory is created must exist and have proper SELinux context and permissions. Otherwise the user's home directory cannot be created or accessed.

−M, **−−no−create−home**
Do not create the user's home directory, even if the system wide setting from /etc/login.defs (**CREATE_HOME**) is set to *yes*.

−N, **−−no−user−group**
Не создавать группу с тем же именем как у пользователя, но добавить пользователя в группу, заданную параметром **−g** или переменной **GROUP** из файла /etc/default/useradd.

Поведение по умолчанию (если не указан параметр **−g**, **−N** и **−U**) определяется переменной **USERGROUPS_ENAB** из файла /etc/login.defs.

−o, **−−non−unique**
allows the creation of an account with an already existing UID.

This option is only valid in combination with the **−u** option. As a user identity serves as key to map between users on one hand and permissions, file ownerships and other aspects that determine the system's behavior on the other hand, more than one login name will access the account of the given UID.

−p, **−−password** *PASSWORD*
defines an initial password for the account. PASSWORD is expected to be encrypted, as returned by **crypt** (3). Within a shell script, this option allows to create efficiently batches of users.

Without this option, the new account will be locked and with no password defined, i.e. a single exclamation mark in the respective field of /etc/shadow. This is a state where the user won't be able to access the account or to define a password himself.

Note: Avoid this option on the command line because the password (or encrypted password) will be visible by users listing the processes.

Вы должны проверить, что пароль соответствует политике системных паролей.

−r, **−−system**
Создать системную учётную запись.

Системные пользователи создаются без информации об устаревании в /etc/shadow, и их числовые идентификаторы выбираются из диапазона **SYS_UID_MIN**−**SYS_UID_MAX**, определённого в /etc/login.defs, а не из **UID_MIN**−**UID_MAX** (это же касается и части с **GID** при создании групп).

Note that **useradd** will not create a home directory for such a user, regardless of the default setting in /etc/login.defs (**CREATE_HOME**). You have to specify the **−m** options if you want a home directory for a system account to be created.

Note that this option will not update /etc/subuid and /etc/subgid. You have to specify the **−F** options if you want to update the files for a system account to be created.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes to configuration files under the root filesystem found under the directory *PREFIX_DIR*. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−s, **−−shell** *SHELL*
sets the path to the user's login shell. Without this option, the system will use the **SHELL** variable specified in /etc/default/useradd, or, if that is as well not set, the field for the login shell in /etc/passwd remains empty.

−u, **−−uid** *UID*
Числовое значение идентификатора пользователя (ID). Оно должно быть уникальным, если не используется параметр **−o**. Значение должно быть неотрицательным. По умолчанию используется наименьшее значение ID большее или равное **UID_MIN** и большее чем у остальных пользователей.

Смотрите также описание **−r** и **UID_MAX**.

−U, **−−user−group**
Создать группу с тем же именем что и у пользователя, и добавить пользователя в эту группу.

Поведение по умолчанию (если не указан параметр **−g**, **−N** и **−U**) определяется переменной **USERGROUPS_ENAB** из файла /etc/login.defs.

−Z, **−−selinux−user** *SEUSER*
defines the SELinux user for the new account. Without this option, SELinux uses the default user. Note that the shadow system doesn't store the selinux−user, it uses *semanage*(8) for that.

−−selinux−range *SERANGE*
defines the SELinux MLS range for the new account. Without this option, SELinux uses the default range. Note that the shadow system doesn't store the selinux−range, it uses *semanage*(8) for that.

This option is only valid if the **−Z** (or **−−selinux−user**) option is specified.

Изменение значений по умолчанию
При запуске программы только с параметром **−D** команда **useradd** показывает текущие значения по умолчанию. Если программа запускается с параметром **−D** вместе с другими параметрами, то **useradd** обновляет значения по умолчанию этих указанных параметров. Изменяемые параметры:

−b, **−−base−dir** *BASE_DIR*
sets the path prefix for a new user's home directory. The user's name will be affixed to the end of *BASE_DIR* to form the new user's home directory name, if the **−d** option is not used when creating a new account.

Этот параметр изменяет переменную **HOME** в файле /etc/default/useradd.

−e, **−−expiredate** *EXPIRE_DATE*
sets the date on which newly created user accounts are disabled.

Этот параметр изменяет переменную **EXPIRE** в файле /etc/default/useradd.

−f, **−−inactive** *INACTIVE*
defines the number of days after the password exceeded its maximum age where the user is expected to replace this password. See *shadow*(5)for more information.

Этот параметр изменяет переменную **INACTIVE** в файле /etc/default/useradd.

−g, **−−gid** *GROUP*
sets the default primary group for newly created users, accepting group names or a numerical group ID. The named group must exist, and the GID must have an existing entry.

Этот параметр изменяет переменную **GROUP** в файле /etc/default/useradd.

−s, **−−shell** *SHELL*
defines the default login shell for new users.

Этот параметр изменяет переменную **SHELL** в файле /etc/default/useradd.

ЗАМЕЧАНИЯ

Системный администратор сам решает, какие файлы нужно положить в каталог /etc/skel/ (или в любой другой каталог шаблонов, указанный в /etc/default/useradd или в командной строке).

ПРЕДОСТЕРЕЖЕНИЯ

Нельзя добавить пользователя в группу NIS или LDAP. Это необходимо делать на соответствующем сервере.

Также, если имя пользователя уже существует во внешней базе данных такой как NIS или LDAP, то **useradd** не станет создавать учётную запись пользователя.

Usernames may contain only lower and upper case letters, digits, underscores, or dashes. They can end with a dollar sign. Dashes are not allowed at the beginning of the username. Fully numeric usernames and usernames . or .. are also disallowed. It is not recommended to use usernames beginning with . character as their home directories will be hidden in the **ls** output.

Имена пользователей могут быть длиной не более 32 знаков.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/group
: содержит информацию о группах

/etc/gshadow
: содержит защищаемую информацию о группах

/etc/default/useradd
: значения по умолчанию для создаваемой учётной записи

/etc/shadow−maint/useradd−pre.d/*, /etc/shadow−maint/useradd−post.d/*
: Run−part files to execute during user addition. The environment variable **ACTION** will be populated with useradd and **SUBJECT** with the **username**. useradd−pre.d will be executed prior to any user addition. useradd−post.d will execute after user addition. If a script exits non−zero then execution will terminate.

/etc/skel/
: каталог, содержащий файлы по умолчанию

/etc/subgid
: Per user subordinate group IDs.

/etc/subuid
: Per user subordinate user IDs.

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
: success

1
: can't update password file

2
: invalid command syntax

3
: invalid argument to option

4
: UID already in use (and no **−o**)

6
: specified group doesn't exist

9
: username or group name already in use

10
: can't update group file

12

can't create home directory

14

can't update SELinux user mapping

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *crypt*(3), *groupadd*(8), *groupdel*(8), *groupmod*(8), *login.defs*(5), *newusers*(8), *subgid*(5), **subuid**(5), *userdel*(8), *usermod*(8).

НАЗВАНИЕ

userdel − удаляет учётную запись и файлы пользователя

СИНТАКСИС

userdel [options] *LOGIN*

ОПИСАНИЕ

Команда **userdel** изменяет системные файлы учётных записей, удаляя все записи, относящиеся к указанному имени_пользователя. Заданная учётная запись должна существовать.

ПАРАМЕТРЫ

Параметры команды **userdel**:

−f, **−−force**
: С этим параметром учётная запись будет удалена, даже если пользователь в этот момент работает в системе. Он также заставляет **userdel** удалить домашний каталог пользователя и почтовый ящик, даже если другой пользователь использует тот же домашний каталог или если почтовый ящик не принадлежит данному пользователю. Если значение **USERGROUPS_ENAB** равно *yes* в файле /etc/login.defs и если существует группа с именем удаляемого пользователя, то это группа будет удалена, даже если она всё ещё является первичной группой другого пользователя.

  Замечание*:* Этот параметр опасно использовать; он может привести систему в нерабочее состояние.

−h, **−−help**
: Показать краткую справку и закончить работу.

−r, **−−remove**
: Файлы в домашнем каталоге пользователя будут удалены вместе с самим домашним каталогом и почтовым ящиком. Пользовательские файлы, расположенные в других файловых системах, нужно искать и удалять вручную.

  Имя файла почтового ящика задаётся переменной **MAIL_DIR** в файле login.defs.

−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.

−P, **−−prefix** *PREFIX_DIR*
: Apply changes in the *PREFIX_DIR* directory and use the configuration files from the *PREFIX_DIR* directory. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−Z, **−−selinux−user**
: Удаляет все пользовательские сопоставления SELinux для учётной записи пользователя.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
: содержит информацию о группах

/etc/login.defs
: содержит конфигурацию подсистемы теневых паролей

/etc/passwd
: содержит информацию о пользователях

/etc/shadow
: содержит защищаемую информацию о пользователях

/etc/shadow−maint/userdel−pre.d/*, /etc/shadow−maint/userdel−post.d/*
: Run−part files to execute during user deletion. The environment variable **ACTION** will be

populated with **userdel** and **SUBJECT** with the username. userdel−pre.d will be executed prior to any user deletion. userdel−post.d will execute after user deletion. If a script exits non−zero then execution will terminate.

/etc/subgid
Per user subordinate group IDs.

/etc/subuid
Per user subordinate user IDs.

ВОЗВРАЩАЕМЫЕ ЗНАЧЕНИЯ

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

0
success

1
can't update password file

2
invalid command syntax

6
specified user doesn't exist

8
user currently logged in

10
can't update group file

12
can't remove home directory

ПРЕДОСТЕРЕЖЕНИЯ

Команда **userdel** не позволит удалить учётную запись, если есть запущенные процессы, принадлежащие данной учётной записи. В этом случае вы можете удалить эти процессы или заблокировать пароль пользователя или учётную запись, а затем удалить учётную запись. Если указан параметр **−f**, то учётная запись будет удалена несмотря ни на что.

Вы должны вручную проверить все файловые системы, чтобы убедиться, что не осталось файлов, принадлежащих этому пользователю.

Нельзя удалить NIS атрибуты клиента NIS. Это необходимо сделать на NIS сервере.

Если значение переменной **USERGROUPS_ENAB** равно *yes* в файле /etc/login.defs, то **userdel** удалит группу с именем как у пользователя. Чтобы избежать рассогласованности в базах данных групп и паролей, **userdel** проверит, что данная группа не используется в качестве первичной для другого пользователя, и выдаст предупреждение без удаления, если такое случится. Параметр **−f** поможет удалить группу в любом случае.

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *login.defs*(5), *gpasswd*(8), *groupadd*(8), *groupdel*(8), *groupmod*(8), *subgid*(5), **subuid**(5), *useradd*(8), *usermod*(8).

НАЗВАНИЕ

usermod − изменяет учётную запись пользователя

СИНТАКСИС

usermod [*options*] *LOGIN*

ОПИСАНИЕ

The **usermod** command modifies the system account files.

ПАРАМЕТРЫ

Параметры команды **usermod**:

−a, **−−append**
Добавить пользователя в дополнительную группу(ы). Использовать только вместе с параметром **−G**.

−b, **−−badname**
Allow names that do not conform to standards.

−c, **−−comment** *COMMENT*
update the comment field of the user in /etc/passwd, which is normally modified using the *chfn*(1) utility.

−d, **−−home** *HOME_DIR*
Домашний каталог нового пользователя.

If the **−m** option is given, the contents of the current home directory will be moved to the new home directory, which is created if it does not already exist. If the current home directory does not exist the new home directory will not be created.

−e, **−−expiredate** *EXPIRE_DATE*
The date on which the user account will be disabled. The date is specified in the format *YYYY−MM−DD*. Integers as input are interpreted as days after 1970−01−01.

An input of −1 or an empty string will blank the account expiration field in the shadow password file. The account will remain available with no date limit.

Для этого параметра требуется файл /etc/shadow. При отсутствии в /etc/shadow создаётся необходимая запись.

−f, **−−inactive** *INACTIVE*
defines the number of days after the password exceeded its maximum age during which the user may still login by immediately replacing the password. This grace period before the account becomes inactive is stored in the shadow password file. An input of 0 will disable an expired password with no delay. An input of −1 will blank the respective field in the shadow password file. See *shadow*(5) for more information.

Для этого параметра требуется файл /etc/shadow. При отсутствии в /etc/shadow создаётся необходимая запись.

−g, **−−gid** *GROUP*
The name or numerical ID of the user's new primary group. The group must exist.

Все файлы в домашнем каталоге пользователя, принадлежавшие предыдущей первичной группе пользователя, будут принадлежать новой группе.

Группового владельца файлов вне домашнего каталога нужно изменить вручную.

The change of the group ownership of files inside of the user's home directory is also not done if the home dir owner uid is different from the current or new user id. This is a safety measure for special home directories such as /.

−G, **−−groups** *GROUP1*[,*GROUP2*,...[,*GROUPN*]]]
A list of supplementary groups which the user is also a member of. Each group is separated from

the next by a comma, with no intervening whitespace. The groups must exist.

Если пользователь — член группы, которой в указанном списке нет, то пользователь удаляется из этой группы. Такое поведение можно изменить с помощью параметра **−a**, при указании которого к уже имеющемуся списку групп пользователя добавляется список указанных дополнительных групп.

−l, **−−login** *NEW_LOGIN*
Имя пользователя будет изменено с ИМЯ на НОВОЕ_ИМЯ. Больше ничего не меняется. В частности, вероятно, должно быть изменено имя домашнего каталога и почтового ящика, чтобы отразить изменение имени пользователя.

−L, **−−lock**
Заблокировать пароль пользователя. Это делается помещением символа «!» в начало шифрованного пароля, чтобы приводит к блокировке пароля. Не используйте этот параметр вместе с **−p** или **−U**.

Замечание: если вы хотите заблокировать учётную запись (не только доступ по паролю), также установите значение *EXPIRE_DATE* в *1*.

−m, **−−move−home**
moves the content of the user's home directory to the new location. If the current home directory does not exist the new home directory will not be created.

Этот параметр можно использовать только с параметром **−d** (или **−−home**).

Команда **usermod** пытается изменить владельцев файлов и копирует права, ACL и расширенные атрибуты, но после неё всё равно могут потребоваться некоторые ручные действия.

−o, **−−non−unique**
allows to change the user ID to a non−unique value.

This option is only valid in combination with the **−u** option. As a user identity serves as key to map between users on one hand and permissions, file ownerships and other aspects that determine the system's behavior on the other hand, more than one login name will access the account of the given UID.

−p, **−−password** *PASSWORD*
defines a new password for the user. PASSWORD is expected to be encrypted, as returned by **crypt** (3).

Note: Avoid this option on the command line because the password (or encrypted password) will be visible by users listing the processes.

Вы должны проверить, что пароль соответствует политике системных паролей.

−r, **−−remove**
Remove the user from named supplementary group(s). Use only with the **−G** option.

−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.

−P, **−−prefix** *PREFIX_DIR*
Apply changes within the directory tree starting with *PREFIX_DIR* and use as well the configuration files located there. This option does not chroot and is intended for preparing a cross−compilation target. Some limitations: NIS and LDAP users/groups are not verified. PAM authentication is using the host files. No SELINUX support.

−s, **−−shell** *SHELL*
changes the user's login shell. An empty string for SHELL blanks the field in /etc/passwd and logs the user into the system's default shell.

−u, **−−uid** *UID*

The new value of the user's ID.

Оно должно быть уникальным, если не используется параметр **−o**. Значение должно быть неотрицательным.

Для почтового ящика и всех файлов, которыми владеет пользователь и которые расположены в его домашнем каталоге, идентификатор владельца файла будет изменён автоматически.

Для файлов, расположенных вне домашнего каталога, идентификатор нужно изменять вручную.

The change of the user ownership of files inside of the user's home directory is also not done if the home dir owner uid is different from the current or new user id. This is a safety measure for special home directories such as /.

Никаких проверок по **UID_MIN**, **UID_MAX**, **SYS_UID_MIN** или **SYS_UID_MAX** из /etc/login.defs не производится.

−U, **−−unlock**
Разблокировать пароль пользователя. Это выполняется удалением символа «!» из начала шифрованного пароля. Не используйте этот параметр вместе с **−p** или **−L**.

Замечание: если вы хотите разблокировать учётную запись (не только доступ по паролю), также установите значение *EXPIRE_DATE* (например, в to *99999* или равным значению **EXPIRE** из файла /etc/default/useradd).

−v, **−−add−subuids** *FIRST−LAST*
Add a range of subordinate uids to the user's account.

This option may be specified multiple times to add multiple ranges to a user's account.

No checks will be performed with regard to **SUB_UID_MIN**, **SUB_UID_MAX**, or **SUB_UID_COUNT** from /etc/login.defs.

−V, **−−del−subuids** *FIRST−LAST*
Remove a range of subordinate uids from the user's account.

This option may be specified multiple times to remove multiple ranges to a user's account. When both **−−del−subuids** and **−−add−subuids** are specified, the removal of all subordinate uid ranges happens before any subordinate uid range is added.

No checks will be performed with regard to **SUB_UID_MIN**, **SUB_UID_MAX**, or **SUB_UID_COUNT** from /etc/login.defs.

−w, **−−add−subgids** *FIRST−LAST*
Add a range of subordinate gids to the user's account.

This option may be specified multiple times to add multiple ranges to a user's account.

No checks will be performed with regard to **SUB_GID_MIN**, **SUB_GID_MAX**, or **SUB_GID_COUNT** from /etc/login.defs.

−W, **−−del−subgids** *FIRST−LAST*
Remove a range of subordinate gids from the user's account.

This option may be specified multiple times to remove multiple ranges to a user's account. When both **−−del−subgids** and **−−add−subgids** are specified, the removal of all subordinate gid ranges happens before any subordinate gid range is added.

No checks will be performed with regard to **SUB_GID_MIN**, **SUB_GID_MAX**, or **SUB_GID_COUNT** from /etc/login.defs.

−Z, **−−selinux−user** *SEUSER*
defines the SELinux user to be mapped with *LOGIN*. An empty string ("") will remove the respective entry (if any). Note that the shadow system doesn't store the selinux−user, it uses semanage(8) for that.

−−selinux−range *SERANGE*
defines the SELinux MLS range for the new account. Note that the shadow system doesn't store the selinux−range, it uses *semanage*(8) for that.

This option is only valid if the **−Z** (or **−−selinux−user**) option is specified.

ПРЕДОСТЕРЕЖЕНИЯ

You must make certain that the named user is not executing any processes when this command is being executed if the user's numerical user ID, the user's name, or the user's home directory is being changed. **usermod** checks this on Linux. On other operating systems it only uses utmp to check if the user is logged in.

Вы должны вручную изменить владельца всех файлов **crontab** или заданий **at**.

Вы должны сделать все изменения NIS на сервере NIS самостоятельно.

НАСТРОЙКА

На работу этого инструмента влияют следующие переменные настройки из /etc/login.defs:

ФАЙЛЫ

/etc/group
Group account information

/etc/gshadow
Secure group account information

/etc/login.defs
Shadow password suite configuration

/etc/passwd
User account information

/etc/shadow
Secure user account information

/etc/subgid
Per user subordinate group IDs

/etc/subuid
Per user subordinate user IDs

СМОТРИТЕ ТАКЖЕ

chfn(1), *chsh*(1), *passwd*(1), *crypt*(3), *gpasswd*(8), *groupadd*(8), *groupdel*(8), *groupmod*(8), *login.defs*(5), *subgid*(5), **subuid**(5), *useradd*(8), *userdel*(8).

НАЗВАНИЕ

vipw, vigr − позволяют редактировать файлы паролей, групп, теневых паролей пользователей или групп.

СИНТАКСИС

vipw [*options*]

vigr [*options*]

ОПИСАНИЕ

The **vipw** and **vigr** commands edit the files /etc/passwd and /etc/group, respectively. With the **−s** flag, they will edit the shadow versions of those files, /etc/shadow and /etc/gshadow, respectively. The programs will set the appropriate locks to prevent file corruption. When looking for an editor, the programs will first try the environment variable **$VISUAL**, then the environment variable **$EDITOR**, and finally the default editor, *vi*(1).

ПАРАМЕТРЫ

Параметры команд **vipw** и **vigr**:

−g, **−−group**
Редактировать базу данных групп.

−h, **−−help**
Показать краткую справку и закончить работу.

−p, **−−passwd**
Редактировать базу данных passwd.

−q, **−−quiet**
Не выводить сообщений при работе.

−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, **−−shadow**
Редактировать базу данных shadow или gshadow.

ОКРУЖЕНИЕ

VISUAL
Редактор, который будет вызван.

EDITOR
Редактор, который будет вызван, если не задана переменная **VISUAL**.

ФАЙЛЫ

/etc/group
содержит информацию о группах

/etc/gshadow
содержит защищаемую информацию о группах

/etc/passwd
содержит информацию о пользователях

/etc/shadow
содержит защищаемую информацию о пользователях

СМОТРИТЕ ТАКЖЕ

vi(1), *group*(5), *gshadow*(5) , *passwd*(5), , *shadow*(5).