passwd(1)

НАЗВАНИЕ

passwd - изменение пароля регистрационного имени и атрибутов пароля

СИНТАКСИС

passwd [**регистрационное_имя**]
passwd [-l | -d] [-f] [-x **max**] [-n **min**] [-w **warn**] **регистрационное_имя**
passwd -s [-a]
passwd -s [**регистрационное_имя**]

ОПИСАНИЕ

Команда **passwd** позволяет любому пользователю изменить пароль или получить список атрибутов текущего пароля для своего **регистрационного_имени**. Привилегированные пользователи могут запускать **passwd** для выполнения этих функций для любого пользователя, а также для установки атрибутов пароля для любого пользователя. Эту команду можно использовать для изменения паролей в базе данных *сетевой информационной службы* (Network Information Service или, сокращенно, NIS).
Пароль обычно задается администратором при создании учетной записи пользователя для владельца **регистрационного_имени**. В дальнейшем пользователь может изменить пароль либо выполнив команду **passwd** без опций, либо задав опцию **-p** в ходе регистрации.
Чтобы использовать второй метод, введите **-p** сразу после приглашения регистрации (перед вводом **регистрационного_имени**):

login: -p регистрационное_имя

В этом случае система регистрации вызывает команду **passwd**.
Подробнее см. на странице справочного руководства **login(1)**.

Синтаксис команды

Любой пользователь может задавать опцию **-s**:

-s Показывает атрибуты пароля для **регистрационного_имени** пользователя.

Только привилегированный пользователь может использовать следующие опции:

-l Блокирует запись пароля для **регистрационного_имени**.

-d Удаляет пароль для **регистрационного_имени**, так что у пользователя с этим **регистрационным_именем** пароль не запрашивается.

-f Заставляет пользователя изменить пароль при следующей регистрации в системе, делая пароль для **регистрационного_имени** устаревшим.

-x max Задает для пользователя с указанным **регистрационным_именем** количество дней, в течение которых пароль будет действителен.

-n min Задает минимальное количество дней между изменениями пароля для пользователя с указанным **регистрационным_именем**. Всегда используйте эту опцию с опцией **-x**, если только **max** не установлен в **-1** (устаревание отключено). В этом случае, **min** устанавливать не нужно.

-w warn Задает за сколько дней (относительно **max**) пользователя с данным **регистрационным_именем** будут предупреждать о предстоящем устаревании пароля.

-s Показывает атрибуты пароля для **регистрационного_имени** пользователя.

-s -a Показывает атрибуты паролей для всех пользователей.

Правила построения паролей

При создании паролей необходимо выполнять следующие требования:

Пароль должен содержать не менее **PASSLENGTH** символов, как определено в файле **/etc/default/passwd**. Значение **PASSLENGTH** должно быть не менее 3. Учитываются только первые восемь символов пароля.

Пароль должен содержать не менее двух буквенных символов и одной цифры или специального символа. (В данном случае к буквенным символам относятся все прописные и строчные буквы.)
Пароль должен отличаться от регистрационного имени пользователя и от любого слова, получаемого *циклическим* (circular shift) или *обратным* (reverse shift) *сдвигом* этого регистрационного имени. (Соответствующие прописные и строчные буквы считаются совпадающими.)
Новый пароль должен отличаться от старого хотя бы на три символа.

Если для пользователя с помощью команды **useradd** (или **usermod**) была указана *программа порождения пароля* (password generator program), **passwd** вызывает ее для порождения ряда возможных паролей, предлагаемых на выбор пользователю; когда используется программа порождения пароля, никакие из обычно действующих правил построения пароля не проверяются.

Действие

При использовании для изменения пароля, **passwd** запрашивает у обычных пользователей их старый пароль, если он задан. Если с момента задания старого пароля прошло достаточно много времени, **passwd** затем предлагает пользователю дважды ввести новый пароль; в противном случае программа прекращает работу. Затем, **passwd** проверяет, удовлетворяет ли новый пароль описанным выше правилам построения. При вводе нового пароля второй раз, две копии нового пароля сравниваются. Если они не совпадают, цикл запроса нового пароля повторяется, но не более двух раз.
Привилегированные пользователи могут изменять любой пароль; команда **passwd** не запрашивает у привилегированного пользователя старый пароль. От привилегированных пользователей не требуется соблюдать правила построения и устаревания пароля. Эти пользователи могут создать *пустой пароль* (null password), нажимая RETURN в ответ на приглашение ввести новый пароль. (Это отличается от **passwd -d**, поскольку приглашение Password: все равно выдается.)

Локальные пароли и пароли NIS

Пароли и связанная с ними информация хранятся в системе в двух файлах, **/etc/passwd** и **/etc/shadow**. Для пользователей NIS поддерживается также база данных NIS, содержащая пароли. В случае если для пользователя имеются записи как в локальном файле **/etc/passwd**, так и в базе данных NIS, то, какой именно пароль изменяется, определяется, в основном, двумя факторами:

- записи в локальной базе данных *идентификации и проверки идентичности* (Identification and Authentication (I&A) database):
  если для пользователя имеется запись в этой базе данных, всегда изменяется локальный пароль. Эта база данных обычно создается во время загрузки программой **creatiadb(1M)**. Учтите, что регистрационные имена пользователей, начинающиеся с символа + или -, игнорируются программой **creatiadb** и поэтому для них нет соответствующих записей в базе данных I&A.
- пароль указан в локальном файле **/etc/shadow**:
  если для пользователя указан пароль в локальном файле **/etc/shadow**, именно этот пароль и будет всегда изменяться, независимо от того, если для данного пользователя запись в базе данных паролей NIS или нет. Если в записи пользователя в **/etc/shadow** пароля нет, **passwd** изменит пользовательскую запись в базе данных паролей NIS.

Устаревание паролей

Пароли действительны в течение ограниченных периодов времени (определяемых системным администратором), после чего их необходимо изменить. Поэтому необходимо хранить информацию о периоде активности для каждого пароля. Когда приближается дата истечения срока действия пароля, его владельцу предлагается выбрать новый пароль в течение определенного количества ближайших дней. Процесс отслеживания сроков действия паролей и уведомления пользователей о необходимости сменить пароль называется *устареванием паролей* (password aging).
Информация о паролях всех пользователей системы хранится в файле **/etc/shadow**, который могут читать только привилегированные пользователи
Каждая строка пользователя в файле **/etc/shadow** содержит четыре параметра, определяющих устаревание пароля:

lastchanged:
Дата последнего изменения пароля пользователя. (Учтите, что эта дата определяется с использованием времени по Гринвичу и поэтому может отличаться на целый день в других часовых поясах.)

minimum:

Количество дней, которые должны пройти со дня последнего изменения, прежде чем пароль пользователя можно будет изменить.

maximum:

Количество дней после последнего изменения, в течение которых пароль будет действителен (после чего его придется изменить). Это количество не учитывает день установки пароля.

warn:

Сколько дней пользователь будет получать предупреждения о приближающемся окончании периода действия пароля. Так, например, если значение **warn** равно 7, владелец **регистрационного_имени** начнет получать предупреждения за неделю до окончания периода действия пароля.

Последние три из этих параметров можно установить опциями командной строки **-n**, **-x** и **-w**, соответственно. При отсутствии опций, их значения берутся из файла **/etc/default/passwd**. Раздел "Стандартные значения" описывает эти параметры.

Если **minimum** больше, чем **maximum**, пользователь не может изменить пароль. Устаревание для **регистрационного_имени** немедленно отключается, если **maximum** установлен равным -1. Если **maximum** установлен в 0, пользователь будет вынужден изменить пароль при следующем сеансе входа после дня последнего изменения и одновременно отключается устаревание пароля.

Устаревание пароля никогда не отключается напрямую командой **"passwd -x 0 регистрационное_имя"**. На самом деле эта команда устанавливает поле **maximum** в 0. Если поле **lastchanged** не равно 0, поля, связанные с устареванием, будут очищены при следующем использовании команды **passwd** для изменения пароля пользователя. Однако если поле **lastchanged** установлено в 0, связанные с устареванием поля не изменяются.

Если предполагалось, что связанные с устареванием поля очистятся, но этого не произошло, возможно, вопреки вашим представлениям, поле **lastchanged** было установлено в 0. Это могло произойти по двум причинам.

Вы (администратор) могли вызвать устаревание пароля пользователя, выполняя команду **passwd -f регистрационное_имя**. В этом случае значение **lastchanged** устанавливается в 0.

Поле **maximum** могло быть пустым при выполнении команды **passwd -x 0 регистрационное_имя**. В этом случае сама команда **passwd** устанавливает значение поля **lastchanged** в 0.

Показ атрибутов пароля

Когда команда **passwd** используется для показа атрибутов пароля, результаты выдаются в следующем формате:

```
login_name status lastchanged minimum maximum warn
```

или, если отсутствует информация, связанная с устареванием пароля,

```
login_name status
```

Поля определены следующим образом:

login_name	Регистрационное имя пользователя.
status	Статус пароля для **регистрационного_имени**: **PS** означает наличие пароля, **LK** означает, что регистрация заблокирована, а **NP** означает отсутствие пароля.

Значения последних четырех полей рассмотрены в разделе "Устаревание паролей".

Стандартные значения

Присваивая значения набору параметров в файле **/etc/default/passwd**, администратор может управлять устареванием и длиной паролей. Можно задать следующие параметры.

MINWEEKS

Минимальное количество недель перед тем, как пароль можно будет изменить. Сразу после установки системы этот параметр имеет значение 0.

MAXWEEKS

Максимальное количество недель, в течение которых пароль можно не изменять. Сразу после установки системы этот параметр имеет значение 24.

WARNWEEKS

Количество недель перед устареванием пароля, когда необходимо предупреждать пользователя. Сразу после установки системы этот параметр имеет значение 1.

PASSLENGTH

Минимальное количество символов в пароле. Сразу после установки системы этот параметр имеет значение 6.

Обратите внимание, что аргументы опций команды **passwd** (**min**, **max** и **warn**), а также соответствующие поля файла **/etc/shadow** (**minimum**, **maximum** и **warn**) задают параметры устаревания в днях; тогда как соответствующие поля файла **/etc/default/passwd** (**MINWEEKS**, **MAXWEEKS** и **WARNWEEKS**), - в неделях.

Если устаревание пароля для пользователя отключено, но стандартные значения параметров устаревания в **/etc/default/passwd** заданы, устаревание паролей будет включено при изменении пароля пользователя.

ДИАГНОСТИКА

В случае успешного завершения команда **passwd** заканчивается с *кодом возврата* (return code) 0. Ниже перечислены возможные причины сбоя:

нет права доступа
(permission denied)

неверное сочетание опций
(invalid combination of options)

неожиданный сбой; файл паролей не изменен
(unexpected failure; password file unchanged)

неожиданный сбой; файл(ы) паролей отсутствует
(unexpected failure; password file(s) missing)

файл(ы) паролей занят; попробуйте еще раз позже
(password file(s) busy; try again later)

недопустимый аргумент опции
(invalid argument to option)

неожиданный сбой
(unexpected failure)

неизвестный идентификатор
(unknown ID)

устаревание отключено
(aging disabled)

ФАЙЛЫ

/etc/shadow
/etc/passwd
/etc/oshadow
/etc/opasswd
/etc/default/passwd
/usr/lib/locale/локаль/LC_MESSAGES/uxcore.abi
файл сообщений для текущего языка (см. LANG в **environ(5)**.)
/etc/security/ia/index
индекс в /etc/security/ia/master
/etc/security/ia/master
содержит всю информацию I&A о пользователях

ПРИМЕЧАНИЯ

Если **root** выполняет команду **passwd -d** для удаления пароля пользователя, для которого действует устаревание пароля, этот пользователь не сможет добавить новый пароль, пока не устареет пустой (NULL) пароль. Так будет даже если флаг **PASSREQ** в файле **/etc/default/login** установлен в YES. Это приводит к тому, что у пользователя не будет пароля. Рекомендуется всегда использовать опцию **-f** совместно с **-d** для удаления пароля. Таким образом, можно гарантировать, что пользователь будет вынужден изменить свой пароль при следующем входе в систему.

ССЫЛКИ

crypt(3G), **id(1M)**, **login(1)**, **passwd(4)**, **pwconv(1M)**, **shadow(4)**, **su(1M)**, **useradd(1M)**, **userdel(1M)**, **usermod(1M)**