



Российский разработчик и поставщик
решений на основе программного обеспечения
с открытым исходным кодом



Управление пользователями

Многопользовательская парадигма

Linux – многопользовательская ОС пользователи обладают личной частью системы, которую он может использовать.

Существует пользователь с именем **root (UID=0)**, который имеет право осуществлять в системе **ЛЮБЫЕ** операции.

!!! Назначив пользователю права на администрирование ОС, то по факту такой пользователь не становится суперпользователем во всех смыслах данного понятия.

Многопользовательская парадигма

Учётная запись пользователя — это необходимая для системы информация о пользователе.

Аутентификация — системная процедура, позволяющая однозначно определить пользователя.

Системные файлы

`/etc/passwd` — сведения о пользователях

`/etc/shadow` — сведения о паролях

`/etc/group` — сведения о группах

Многопользовательская парадигма

Файл со строочными сведениями о пользователе `/etc/passwd`:

login	:	x	:	UID	:	GID	:	Описание (GECOS)	:	Home dir	:	оболочка
-------	---	---	---	-----	---	-----	---	------------------	---	----------	---	----------

Если поле пароля содержит * или !, пользователю нельзя войти в систему по паролю. Другие методы входа по-прежнему разрешены.

Файл со строочными сведениями о группах `/etc/group`:

имя	:	x	:	GID	:	пользователи, включённые в неск. групп
-----	---	---	---	-----	---	--

Многопользовательская парадигма

Файл со строчными сведениями о паролях пользователей
`/etc/shadow`

Параметры записи о пользователе можно посмотреть командой
`chage -l <username>`

1	:	2	:	3	:	4	:	5	:	6	:	7	:	8	:	9
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

- 1 — UID
- 2 — хэшированный пароль
- 3 — количество дней с момента последней смены пароля от 1 января 1970 года
- 4 — число дней до смены пароля
- 5 — число дней, после которых пароль *должен* быть сменён
- 6 — число дней до смены пароля, когда система извещает об этом пользователя
- 7 — число дней после окончания действия пароля, когда ещё можно работать
- 8 — число дней, по истечении которых пароль будет заблокирован
- 9 — служебное поле (пока не используется)

Многопользовательская парадигма

Зашифрованный пароль – hash пароля:

Пароль использует формату **\$type\$salt\$hashed**.

\$type – метод криптографического алгоритма хеширования:

\$1\$ – MD5

\$2a\$ – Blowfish

\$2y\$ – Eksblowfish

\$5\$ – SHA-256

\$6\$ – SHA-512



Команды управления пользователями

useradd — добавить нового пользователя

passwd — установить пароль пользователя

usermod — изменить параметры учетной записи пользователя

userdel — удалить учетную запись пользователя

groupadd — создать новую группу

gpasswd — управление группами

groupmod — изменить параметры группы

groupdel — удалить группу

Изменение данных учетной записи пользователя

usermod [<опции>] <имя_пользователя>

- a** – добавить пользователя в группу. Работает вместе с опцией -G
- g** – выбрать новую основную группу для пользователя
- l** – изменить имя пользователя на новое
- L** – заблокировать пароль пользователя
- p** – изменить пароль
- u** – изменить параметр UID .

Создание/изменение пароля пользователя

`passwd [<опции>] <имя_пользователя>`

- d** - удалить пароль пользователя, после этого он не сможет войти
- l** - запретить пользователю входить в систему
- u** - отменяет действие параметра -l
- S** - отобразить информацию об аккаунте
- n** - минимальное количество дней между сменами пароля

Удаление пользователя

userdel [<опции>] <имя_пользователя>

-f – принудительное удаление, даже если пользователь авторизован.

Можно предварительно завершить все процессы пользователя

killall -9 -u <username>

-r – удалить домашнюю директорию пользователя

-Z – удалить все SELinux объекты для этого пользователя

Добавление группы

groupadd [<опции>] <имя_группы>

- g** – установить значение идентификатора группы GID вручную
- K** - изменить параметры по умолчанию автоматической генерации GID
- o** - разрешить добавление группы с неunikальным GID
- p** - задаёт пароль для группы
- r** - указывает, что группа системная

Утилиты для работы с учетными записями пользователей

- **useradd** – создание учетной записи пользователя
- **usermod** – изменение параметров учетной записи пользователя
- **userdel** – удаление учетной записи пользователя
- **groupadd** – создание учетной записи группы
- **groupmod** – изменение параметров учетной записи группы записи группы.
- **groupdel** – удаление учетной используются
- Файл /etc/login.defs настройки по умолчанию, которые используются данными утилитами

Утилиты для управления паролями

passwd изменить пароль пользователя, с жизненным циклом пароля: также настроить атрибуты, связанные с жизненным циклом пароля

chage — данная утилита предназначена для установки и просмотра атрибутов пароля и записи:

- l – посмотреть атрибуты пароля

gpaswd — утилита предназначена для установки пароля группы

Пользователи и группы

Файл **/etc/login.defs**. Управляет поведением инструментов из компонента **shadow-utils**. Ни один из этих инструментов не использует механизм PAM.

В файле указаны некоторые параметры системы формирования паролей и логинов.

Остальные параметры указаны в настройках модулей PAM, например в файле **/etc/pam.d/system-auth**

Модули PAM

Проверить использование **PAM** какой либо программой.

```
ldd /bin/passwd | grep pam
```

PAM (Pluggable Authentication Modules) — подключаемые модули аутентификации пользователей.

Конфигурационные файлы находятся в каталоге `/etc/pam.d`

Внимание! Безрассудная правка конфигурационных файлов может сделать вашу систему неработоспособной! Поэтому **убедитесь, что у вас под рукой есть резервная копия** всех конфигов.

Модули PAM

PAM (Pluggable Authentication Modules) — подключаемые модули аутентификации пользователей.

Конфигурационные файлы находятся в каталоге `/etc/pam.d`

4 основные функции системы PAM:

auth — функции которые позволяют определить, что вы это вы (по паролю, по смарт-карте и т.д.)

account — управление учетными записями. Например запрет на работу в определенное время суток.

session — выделение пользователю необходимых для работы ресурсов. Например разрешение на монтирование каталогов.

password — изменение аутентификационных данных пользователя. Например управление паролями пользователя.

Модули PAM

PAM (Pluggable Authentication Modules)

Структура файлов в каталоге /etc/pam.d

Имя файла это имя программы к которой относится конфигурация.

Файл состоит из 3 полей

<тип функции> <действие системы> <имя модуля>

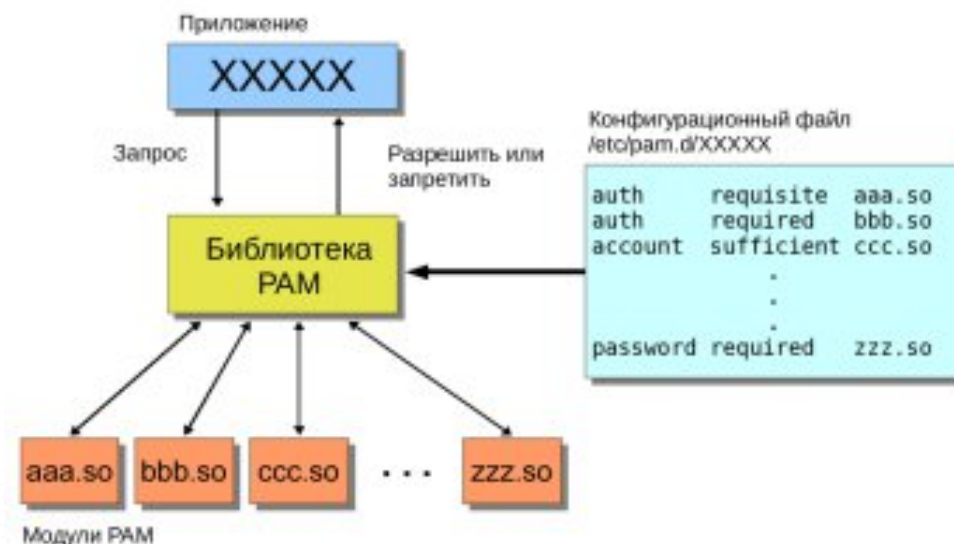
Действия системы могут быть:

required

requisite

optional

sufficient



Модули PAM

PAM (Pluggable Authentication Modules)

required — если модуль выдал ошибку, то система PAM возвращает ошибку после выполнения всей цепочки.

requisite — если модуль выдал ошибку, то дальнейшее выполнение прерывается и система PAM возвращает ошибку. Иначе выполнение цепочки продолжается.

optional — этот параметр никак не влияет на ход цепочки.

sufficient — если модуль вернул успех, то система PAM возвращает приложению успех, и дальнейшее выполнение цепочки прерывается. Если неудача, то продолжается выполнение цепочки.

Модули PAM

Модуль **pam_access.so** – Позволяет определить, каким пользователям позволено входить в систему и с каких IP-адресов.

Его конфигурация - /etc/security/access.conf

разрешение:пользователи:происхождение

```
# User "root" should be able to have access from domain.  
# Uses string matching also.  
#+:root:.foo.bar.org  
#
```

pam_pwquality.so – Позволяет управлять парольной политикой.

Его конфигурация - /etc/security/pwquality.conf

Модули PAM

Модуль **pam_time**

Может установить ограничения на доступ к системе и к конкретным приложениям в разное время. **/etc/security/time.conf**

services;ttys;users;times

Разрешим myuser работать Понедельник, вторник, четверг в 08:00-10:00 и 20:00-21:30. Для этого в /etc/security/time.conf пишем

***;*;myuser;MoTuTh0800-1000|MoTuTh2000-2130**

В файлах /etc/pam.d/login, /etc/pam.d/sshd после строк **auth*** добавим

account required pam_time.so

Модули PAM

Модуль PAM_USB - двухфакторная аутентификация

Позволяет использовать USB для автоматической аутентификации.

После настроек конфиг будет в `/etc/pamusb.conf`

pamusb-conf --add-device <Auth-Stick> – добавляем устройство

pamusb-conf --add-user='petrov' – добавляем пользователя

В файлах `/etc/pam.d/system-auth` и `/etc/pam.d/password-auth` нужно в начало файла добавить одну из строк строку:

auth sufficient pam_usb.so – только ключ или пароль

auth required pam_usb.so – ключ + пароль

Суперпользователь, особенности работы с правами администратора

Смена текущего пользователя в системе — **su**

su [options] [-] [user]

[options] — ключи команды

[-] — смена контекста выполнения оболочки на контекст указанного пользователя. Переменные \$PATH, \$HOME, \$SHELL, \$USER, \$LOGNAME.

[user] — имя пользователя, под которым продолжит работать командная оболочка.

Суперпользователь, особенности работы с правами администратора

Смена текущего пользователя в системе — **su**

su [options] [-] [user]

- c, --command=command** — запускает приложение под указанным аккаунтом;
- s, --shell=shell** — происходит запуск для заданного пользователя указанной оболочки;
- , -l, --login** — смена контекста выполнения на контекст заданного пользователя, аналогична смене пользователя системы для shell;
- g, --group=group** — вызов пользователя, состоящего в заданной группе. Используется только для пользователя root;
- h, --help** — вызов справки для команды..

Суперпользователь, особенности работы с правами администратора

su — смена пользователя на root;

su - — смена пользователя на root с заменой некоторых переменных;

su -s /bin/sh user01 — запуск оболочки sh для user01;

su -c 'mc' user01 — запуск Midnight Commander для user01;

su -c 'ls /boot' — Просмотр содержимого /boot пользователем root;

Чтобы выйти из оболочки, открытой командой su можно использовать встроенную команду **exit** или сочетание клавиш **Ctrl+d**.

Суперпользователь, особенности работы с правами администратора

Позволяет вам запускать программы от имени других пользователей.

sudo опции программа параметры

- A** или **--askpass** – использовать графическую утилиту для запроса пароля, если эта программа настроена.
- b** или **--background** – запускает программу в фоновом режиме;
- g** – запустить команду с указанной группой;
- h** – выполнить команду от имени другого хоста;
- i** или **--login** – смена пользователя. И смена переменных окружения;
- k** – отключить возможность временного запоминания пароля;
- l** или **--list** - список доступных команд для удалённых пользователей;

Суперпользователь, особенности работы с правами администратора

Позволяет вам запускать программы от имени других пользователей.

sudo **опции** **программа** **параметры**

- s** или **--shell** – позволяет запустить командный интерпретатор;
- U** или **--User** – вместе с опцией **-l** посмотреть привилегии для пользователя;
- T** или **--timeout** – позволяет установить время выполнения команды, команда будет завершена принудительно, если время закончилось;
- u** – указать имя пользователя для выполнения программы;
- – означает, что следующие опции обрабатывать не нужно.

Практическая работа

1. Просмотрите в файле `/etc/passwd` поля с информацией о пользователях вашей системы. (Какой символ используется для разделения полей в `/etc/passwd`? Сколько полей используется для описания каждого пользователя? Сколько пользователей в вашей системе?)
2. Сколько различных входных оболочек используется в вашей системе?
3. Добавьте трех новых пользователей с соответствующими домашними директориями: `student7`, `student8`, `student9`. Задайте пароли для каждого из них.
4. Создайте группу `course` и добавьте в нее всех трех пользователей.
5. Для пользователя `student7` выставите ограничение: срок действия пароля 5 месяцев и предупреждение об окончании срока действия пароля 7 дней
6. Заблокируйте пользователя `student8`. Проверьте, что блокировка подействовала.
7. Войдите в систему под пользователем `student9`
8. Войдите в систему под пользователем `student7`. Попробуйте перейти в директорию пользователя `student9` и создать файл `file1`.
9. Войдите в систему под пользователем `root`. Разблокируйте пользователя `student8`. Проверьте, что блокировка снята



Спасибо за внимание!

www.red-soft.ru
redos@red-soft.ru

