Sudo (Русский)

Ссылки по теме

- **Пользователи и группы**
- **su**

Эта страница нуждается в сопроводителе

Статья не гарантирует актуальность информации. Помогите русскоязычному сообществу поддержкой подобных страниц. См. **Команда переводчиков ArchWiki**

Состояние перевода: На этой странице представлен перевод статьи **Sudo**. Дата последней синхронизации: 2015-06-29. Вы можете **помочь** синхронизировать перевод, если в английской версии произошли **изменения**.

sudo (англ. *substitute user do*, дословно «подменить пользователя и выполнить») позволяет системному администратору делегировать полномочия, чтобы дать некоторым пользователям (или группе пользователей) возможность запускать некоторые (или все) команды с правами суперпользователя или любого другого пользователя, обеспечивая контроль над командами и их аргументами.

Contents

[hide]

- 1Обоснование
- 2Установка
- 3Использование
- 4Настройка
  - 4.1Просмотр текущих настроек
  - 4.2Использование visudo
  - 4.3Примеры настроек
  - 4.4Права доступа к файлам sudoers по умолчанию
  - 4.5Время действия введённого пароля
- 5Советы и рекомендации
  - 5.1Автодополнение по нажатию Tab в bash
  - 5.2Один тайм-аут на все сеансы терминала
  - 5.3Всегда показывать замечание о безопасности
  - 5.4Переменные окружения
  - 5.5Перенос псевдонимов
  - 5.6Шутливые оскорбления
  - 5.7Пароль суперпользователя
  - 5.8Отключение учетной записи root
    - 5.8.1gksu
    - 5.8.2kdesu
  - 5.9Еще один пример настройки
  - 5.10Настройка sudo с помощью вкладываемых в /etc/sudoers.d файлов
- 6Решение проблем
  - 6.1Проблемы с TTY через SSH
  - 6.2Показать привилегии пользователя
  - 6.3Наложение umask
  - 6.4Опции по умолчанию

Обоснование

Sudo - это альтернатива **su** для выполнения команд с правами суперпользователя (root). В отличие от **su**, который запускает оболочку с правами root и даёт всем дальнейшим командам

root права, sudo предоставляет временное повышение привилегий для одной команды. Предоставляя привилегии root только при необходимости, использование sudo снижает вероятность того, что опечатка или ошибка в выполняемой команде произведут в системе разрушительные действия.

Sudo может также использоваться для выполнения команд от имени других пользователей; кроме того, sudo логирует все команды и неудачные попытки доступа для аудита безопасности.

Установка

Установите пакет **sudo**.

Чтобы начать использовать `sudo` как непривилегированный пользователь, его нужно настроить должным образом. Для этого прочтите раздел о настройке.

Использование

Пользователи могут предварять команды словом `sudo`, чтобы исполнять их с привилегиями суперпользователя (или другого пользователя).

Например, для использования pacman:

```
$ sudo pacman -Syu
```

Смотрите **руководство по sudo** для получения дополнительной информации.

Настройка

Просмотр текущих настроек

Выполните `sudo -ll` для вывода текущей конфигурации sudo.

Использование visudo

Файл настроек `/etc/sudoers` **всегда** следует редактировать с помощью команды `visudo`. `visudo` блокирует файл `sudoers`, сохраняет изменения во временный файл и проверяет, что файл грамматически корректен, перед тем как скопировать его в `/etc/sudoers`.

Важно:

- Крайне важно, чтобы файл `sudoers` был без синтаксических ошибок! Любая ошибка делает sudo неработоспособным. **Всегда** редактируйте его только с помощью `visudo` для предотвращения ошибок.
- Из **visudo(8)**: *Обратите внимание, что это дыра в безопасности, поскольку позволяет пользователю запускать любую программу, какую он захочет, просто прописав её в VISUAL или EDITOR.*

visudo использует `vi` в качестве текстового редактора по умолчанию. В core репозитории sudo скомпилирована с `--with-env-editor` по умолчанию и использует переменные `VISUAL` и `EDITOR`. `EDITOR` не используется, если задана переменная `VISUAL`.

Чтобы сделать nano редактором **visudo** в течение текущего shell сеанса, задайте и экспортируйте переменную `EDITOR` перед тем, как выполнять **visudo**.

Он будет использован, если вы не определили другой редактор, установив **переменные окружения** `VISUAL` или `EDITOR` (используемые в таком порядке) в качестве желаемого редактора, например `nano`. Выполните команду с правами суперпользователя:

```
# EDITOR=nano visudo
```

Для изменения редактора на постоянной основе для текущего пользователя, прочтите **установка переменных окружения для пользователя**. Для того, чтобы установить выбранный редактор на постоянной основе для всей системы, но только для `visudo`, добавьте следующее в `/etc/sudoers` (предположим, что вы предпочитаете `nano` в качестве редактора):

```
# Сброс окружения
Defaults      env_reset
# Установка nano в качестве редактора по умолчанию и запрет visudo
использовать EDITOR/VISUAL.
Defaults      editor=/usr/bin/nano, !env_editor
```

Примеры настроек

Настройка sudo осуществляется добавлением записей в файл `/etc/sudoers`. Чтобы дать пользователю привилегии суперпользователя, когда он вводит `sudo` перед командой, добавьте следующую строку:

```
имя_пользователя   ALL=(ALL) ALL
```

Разрешить пользователю выполнять все команды от любого пользователя, но только на машине с определенным названием хоста:

```
имя_пользователя   название_хоста=(ALL) ALL
```

Предоставить членам группы `wheel` доступ sudo:

```
%wheel      ALL=(ALL) ALL
```

Чтобы не спрашивать пароль у пользователя:

```
Defaults:имя_пользователя      !authenticate
```

Разрешить выполнять только конкретные команды и только пользователю на определенном хосте:

```
имя_пользователя
название_хоста=/usr/bin/halt,/usr/bin/poweroff,/usr/bin/reboot,/usr/bin/pacma
n -Syu
```

Примечание: Наиболее общие опции должны идти в начале файла, а наиболее частные - наоборот, в конце файла, так как более нижние строки переопределяют более верхние. В частности, добавляемая строка должна быть после строки `%wheel`, если ваш пользователь находится в этой группе.

Разрешить выполнять конкретно определённые команды только для пользователя на определенном хосте и без пароля:

```
имя_пользователя название_хоста= NOPASSWD:
/usr/bin/halt,/usr/bin/poweroff,/usr/bin/reboot,/usr/bin/pacman -Syu
```

Подробный пример для `sudoers` доступен в `/usr/share/doc/sudo/examples/sudoers`. Также смотрите **руководство по sudoers** для получения более подробной информации.

Права доступа к файлам sudoers по умолчанию

Файл `sudoers` должен иметь владельца root и группу root (0). Права доступа всегда должны быть установлены как `r--r-----` (0440). Эти права установлены по умолчанию, однако если вы случайно измените их, они должны быть немедленно изменены обратно, иначе sudo не будет работать.

```
# chown -c root:root /etc/sudoers
# chmod -c 0440 /etc/sudoers
```

Время действия введённого пароля

Возможно, вы захотите изменить промежуток времени, в течение которого sudo действует без ввода пароля. Этого легко добиться добавив опцию `timestamp_timeout` в `/etc/sudoers`:

```
Defaults:имя_пользователя timestamp_timeout=время_в_минутах
```

Например, чтобы установить тайм-аут на 20 минут:

```
Defaults:имя_пользователя timestamp_timeout=20
```

Совет: Если вы хотите чтобы sudo всегда требовал ввод пароля, установите `timestamp_timeout` равным 0. Чтобы срок действия пароля никогда не истекал, установите любое отрицательное значение.

Советы и рекомендации

Автодополнение по нажатию Tab в bash

Смотрите **дополнение по нажатию Tab**[broken link: invalid section].

Один тайм-аут на все сеансы терминала

Важно: Это позволит любому процессу воспользоваться вашим открытым сеансом sudo.

Если вы не хотите вводить пароль снова каждый раз, когда открываете новый терминал, отключите **tty_tickets**:

```
Defaults !tty_tickets
```

Всегда показывать замечание о безопасности

По умолчанию, `/etc/sudoers` настроен так, что *sudo* выводит замечание о безопасности только при первом открытии сеанса:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

```
   #1) Respect the privacy of others.
   #2) Think before you type.
   #3) With great power comes great responsibility.
```

Чтобы это сообщение выводилось всегда, отредактируйте `/etc/sudoers`. Замените:

```
Defaults lecture=once
```

на:

```
Defaults lecture=always
```

или просто добавьте эту строку, если её нет.

Переменные окружения

Если у вас много переменных окружения или вы экспортировали ваши настройки прокси через `export http_proxy="..."`, когда вы используете sudo, эти переменные не будут переданы в открытый сеанс, если вы не запустите sudo в опцией `-E`.

```
$ sudo -E pacman -Syu
```

Рекомендованный способ сохранения переменных окружения - это прописать их в `env_keep`:

```
/etc/sudoers
```

```
Defaults env_keep += "ftp_proxy http_proxy https_proxy no_proxy"
```

Перенос псевдонимов

Если у вас установлено много псевдонимов, вы могли заметить, что они не переносятся в сеанс sudo. Однако, это легко исправить. Просто добавьте в ваш `~/.bashrc` или `/etc/bash.bashrc` строку:

```
alias sudo='sudo '
```

Шутливые оскорбления

Вы можете сконфигурировать sudo так, чтобы при вводе неверного пароля он выводил шутливые оскорбления вместо стандартного сообщения "Sorry, try again". Найдите строку `Defaults` в `/etc/sudoers` и добавьте `insults` в список опции, разделяя их запятыми. Конечный результат может выглядеть так:

```
#Defaults specification
Defaults insults
```

Для проверки, введите `sudo -K`, чтобы завершить текущий сеанс и позволить sudo заново запросить пароль.

Пароль суперпользователя

Вы можете сконфигурировать sudo так, чтобы он спрашивал пароль суперпользователя вместо пароля текущего пользователя, добавив `targetpw` или `rootpw` в список опций Defaults в `/etc/sudoers`:

```
Defaults targetpw
```

Чтобы не разглашать пароль root пользователям, вы можете запретить это определённым группам:

```
Defaults:%wheel targetpw
%wheel ALL=(ALL) ALL
```

Отключение учетной записи root

Вы можете захотеть отключить возможность входа систему пользователя root. Без этого атакующие сначала должны будут угадать имя пользователя, сконфигурированного как sudoer, а также пароль этого пользователя. Смотрите для примера **Secure Shell (Русский)#Отключение**.

Важно: Будьте осторожны. Вы можете попасть в свою ловушку, если отключите вход систему пользователя root. Sudo по умолчанию не установлен, и его стандартная конфигурация не позволяет ни получить доступ к правам root без пароля, ни дать такой доступ вам по вашему собственному паролю. Убедитесь, что пользователь правильно сконфигурирован как sudoer *перед* отключением аккаунта суперпользователя!

Примечание: Если вы уже попали в ловушку, смотрите **Password Recovery (Русский)** для получения помощи.

Пароль пользователя root можно заблокировать с помощью `passwd`:

```
# passwd -l root
```

Аналогичная команда разблокирует пароль пользователя root:

```
$ sudo passwd -u root
```

Также вы можете отредактировать `/etc/shadow` и заменить зашифрованный пароль root на "!":

```
root:!:12345::::::
```

Тогда, чтобы задать новый пароль и тем самым разблокировать пользователя root:

```
$ sudo passwd root
```

gksu

Чтобы *gksu* использовал sudo по умолчанию, выполните:

```
$ gconftool-2 --set --type boolean /apps/gksu/sudo-mode true
```

kdesu

kdesu можно использовать в KDE для запуска графических программ с привилегиями суперпользователя. Вероятно, что kdesu по умолчанию будет пытаться использовать su, даже если аккаунт root отключен. К счастью, можно сказать kdesu использовать sudo вместо su. Создайте/отредактируйте
файл `~/.kde4/share/config/kdesurc` (или `~/.config/kdesurc` для kf5 версии kdesu):

```
[super-user-command]
super-user-command=sudo
```

или используйте следующую команду (используйте *kwriteconfig5* для kf5 версии kdesu):

```
$ kwriteconfig --file kdesurc --group super-user-command --key super-user-
command sudo
```

Также вы можете установить **kdesudo**[AUR] из **AUR**, который поддерживает улучшенное автодополнение по Tab при вводе команды.

Еще один пример настройки

Допустим, вы создали 3 пользователей: admin, devel и joe. Пользователь "admin" используется для journalctl, systemctl, mount, kill и iptables; "devel" используется для установки пакетов и редактирования настроек; "joe" - пользователь, под которым вы вошли в систему. Чтобы разрешить "joe" перезагружаться, выключать систему и использовать netctl, мы должны сделать следующее:

Отредактировать /etc/pam.d/su и /etc/pam.d/su-1 Потребовать, чтобы пользователь был в группе wheel, но никого в неё не добавлять.

```
#%PAM-1.0
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel"
group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
auth            required        pam_wheel.so use_uid
auth            required        pam_unix.so
account         required        pam_unix.so
session         required        pam_unix.so
```

Ограничить вход по SSH для группы 'ssh'. В эту группу будет входить только "joe".

```
groupadd -r ssh
gpasswd -a joe ssh
echo 'AllowGroups ssh' >> /etc/ssh/sshd_config
```

Перезапустите sshd.service

Добавить пользователей в другие группы.

```
for g in power network ;do ;gpasswd -a joe $g ;done
```

```
for g in network power storage ;do ;gpasswd -a admin $g ;done
```

Установить права на настройки так, чтобы devel мог редактировать их.

```
chown -R devel:root /etc/{http,openvpn,cups,zsh,vim,screenrc}
Cmnd_Alias  POWER       =   /usr/bin/shutdown -h now, /usr/bin/halt,
/usr/bin/poweroff, /usr/bin/reboot
Cmnd_Alias  STORAGE     =   /usr/bin/mount -o nosuid,nodev,noexec,
/usr/bin/umount
Cmnd_Alias  SYSTEMD     =   /usr/bin/journalctl, /usr/bin/systemctl
Cmnd_Alias  KILL        =   /usr/bin/kill, /usr/bin/killall
Cmnd_Alias  PKGMAN      =   /usr/bin/pacman
Cmnd_Alias  NETWORK     =   /usr/bin/netctl
Cmnd_Alias  FIREWALL    =   /usr/bin/iptables, /usr/bin/ip6tables
Cmnd_Alias  SHELL       =   /usr/bin/zsh, /usr/bin/bash
%power      ALL         =   (root)  NOPASSWD: POWER
%network    ALL         =   (root)  NETWORK
%storage    ALL         =   (root)  STORAGE
root        ALL         =   (ALL)   ALL
admin       ALL         =   (root)  SYSTEMD, KILL, FIREWALL
devel       ALL         =   (root)  PKGMAN
Joe         ALL         =   (devel) SHELL, (admin) SHELL
```

С такими настройками вам практически никогда не понадобится входить как суперпользователь.

"Joe" может подсоединиться к своему домашнему WiFi.

```
sudo netctl start home
sudo poweroff
```

"Joe" не может использовать netctl от имени другого пользователя.

```
sudo -u admin -- netctl start home
```

Когда "joe" хочет воспользоваться journalctl или убить зависший процесс, он может переключиться на нужного пользователя:

```
sudo -i -u devel
sudo -i -u admin
```

Но "joe" не может переключиться на суперпользователя.

```
sudo -i -u root
```

Если "joe" хочет начать gnu-screen сессию как admin, он может сделать это следующим образом:

```
sudo -i -u admin
admin% chown admin:tty `echo $TTY`
admin% screen
```

Настройка sudo с помощью вкладываемых в /etc/sudoers.d файлов

sudo обрабатывает файлы, содержащиеся в директории `/etc/sudoers.d/`. Это означает, что вместо того, чтобы редактировать `/etc/sudoers`, вы можете менять настройки в отдельных файлах и перемещать их в эту директорию. Это даёт два преимущества:

- Вам не понадобится редактировать файл `sudoers.pacnew`;
- Если с новой записью будет проблема, вы можете просто уничтожить соответствующий файл, вместо необходимости редактировать `/etc/sudoers`.

Формат записей в этих вкладываемых файлах такой же, как и в самом файле `/etc/sudoers`. Чтобы редактировать их напрямую, используйте `visudo -f /path/to/file`. Смотрите раздел **Including other files from within sudoers** в **`sudoers(5)`** для дополнительной информации.

Решение проблем

Проблемы с TTY через SSH

По умолчанию SSH не выделяет tty при выполнении удалённой команды. Без tty sudo не может отключить отображение пароля при его вводе. Вы можете воспользоваться ssh опцией `-tt`, чтобы заставить его выделять tty (или `-t` дважды).

`Defaults` опция `requiretty` всего лишь позволяет запускать sudo пользователям, если они имеют tty.

```
# Disable "ssh hostname sudo <cmd>", because it will show the password in
clear text. You have to run "ssh -t hostname sudo <cmd>".
#
#Defaults    requiretty
```

Показать привилегии пользователя

Вы можете узнать какими привилегиями обладает конкретный пользователь следующей командой:

```
$ sudo -lU имя_пользователя
```

Или узнать ваши собственные привилегии командой:

```
$ sudo -l

Matching Defaults entries for yourusename on this host:
    loglinelen=0, logfile=/var/log/sudo.log, log_year, syslog=auth,
mailto=webmaster@gmail.com, mail_badpass, mail_no_user,
```

```
    mail_no_perms,env_reset, always_set_home, tty_tickets, lecture=always,
pwfeedback, rootpw, set_home

User yourusename may run the following commands on this host:

    (ALL) ALL
    (ALL) NOPASSWD: /usr/bin/lsof, /bin/nice, /usr/bin/su, /usr/bin/locate,
/usr/bin/find, /usr/bin/rsync, /usr/bin/strace,
    (ALL) /bin/kill, /usr/bin/nice, /usr/bin/ionice, /usr/bin/top,
/usr/bin/killall, /usr/bin/ps, /usr/bin/pkill
    (ALL) /usr/bin/gparted, /usr/bin/pacman
    (ALL) /usr/local/bin/synergyc, /usr/local/bin/synergys
    (ALL) /usr/bin/vim, /usr/bin/nano, /usr/bin/cat
    (root) NOPASSWD: /usr/local/bin/synergyc
```

Наложение umask

Sudo накладывает на значение **umask** пользователя свою собственную (которая по умолчанию установлена в 0022). Это предотвращает sudo от создания файлов с более либеральными правами доступа, чем это позволяет umask пользователя. Несмотря на то, что это разумное значение по умолчанию, если не используется измененная umask, это может привести к ситуации, когда программа, запущенная через sudo может создавать файлы с правами доступа отличными от тех, которые создаются при запуске программы непосредственно суперпользователем. Для исправления таких ошибок sudo предоставляет возможность исправить umask, даже если желаемая umask более либеральна, чем установлено в umask пользователя. Добавив такие строки (используйте `visudo`) вы измените поведение sudo по умолчанию:

```
Defaults umask = 0022
Defaults umask_override
```

Это установит sudo umask в umask суперпользователя по умолчанию (0022) и переопределит поведение по умолчанию, всегда используя указанную umask и независимо от umask пользователя.

Опции по умолчанию

На сайте авторов есть **список всех опций**, которые можно использовать с командой `Defaults` в файле `/etc/sudoers`.

Смотрите **[1]** список опций (извлечён из исходного кода версии 1.8.7) представленный в формате, оптимизированном для `sudoers`.