Группы и пользователи в Debian GNU/Linux

> *Большинство дистрибутивов GNU/Linux по умолчанию создают различные группы пользователей с определенными разрешениями для определенных функций. Ниже приведен список некоторых групп и пользователей, обычно встречающихся в Debian GNU/Linux.*

Список групп

Группа	Функция / Примечания
root	Суперпользователь: полный доступ к системе. Обычно `root` к этой группе должен принадлежать только пользователь.
adm	Мониторинг системных задач. Позволяет использовать `xconsole` и читать файлы `/var/log` без использования команд `su` или `sudo`. Обычно для администраторов. Название группы происходит от того, что `/var/log` она была изначально , `/usr/adm`а позже `/var/adm`
audio	Разрешает доступ к аудио устройствам.
backup	Разрешить сохранение и восстановление без предоставления пользователю root.
bin	Присутствует для совместимости с устаревшими приложениями. Новые приложения не должны использовать данные .
cdrom	Разрешает доступ к оптическому приводу.
daemon	Службы, которые необходимо записать на диск. Из соображений безопасности желательно, чтобы у каждой службы была своя группа.
dialout	Прямой доступ к последовательным портам. Члены этой группы могут перенастраивать модем, звонить куда угодно и т.д.
dip	Он позволяет вам использовать такие инструменты, как `pppd`, `pon` и `poff` устанавливать соединения с другими системами, используя предопределенные файлы конфигурации в формате `/etc/ppp/peers`. Название группы расшифровывается как «Коммутируемый IP-адрес».
disk	*Прямой* доступ к дискам. Практически эквивалентно доступу, который у вас есть `root` на дисках. Обычно пользователь не должен принадлежать к этой группе или может сделать что-то не так, например `cat /dev/zero > /dev/sda`.
fax	Позволяет отправлять и получать факсы.
floppy	Разрешает доступ к дисководу.
games	Используется некоторыми играми для сохранения очков.
gdm	Используется GDM (Gnome Display Manager).
gnats	Используется `gnats`.
haldaemon	Используется уровнем аппаратной абстракции.

halt	Позволяет войти в систему, чтобы выключить систему.
irc	Используется службами IRC . (Требуется статический пользователь из-за ошибки в `ircd`)
klog	Используется журналом `klogd` ядра.
kmem	Для программ, которым требуется прямой доступ для чтения к системной памяти. Эта группа может читать `/dev/kmem` и другие подобные файлы. Это в значительной степени пережиток BSD.
list	Для управления списком рассылки. Некоторые программы этого типа также используют пользователя с таким же именем.
lp	Прямой доступ к параллельному порту. Эта группа традиционно используется полиграфическими службами.
lpadmin	Позволяет добавлять, изменять и удалять принтеры из foomatic, cups и, возможно, других баз данных принтеров.
mail	Написание в `/var/mail`. Используется агентами MTA и MUA.
majordom	Исторически использовался мажордомом. Он не устанавливается на новые системы.
man	Иногда используется программой `man` для записи в `/var/cache/man`.
messagebus	Используется службой dbus (dbus-daemon-l)
news	Запись в папки новостей. Используется службами и другими новостными программами (протокола nntp).
nogroup	Используется службами, не требующими владения какими-либо файлами. Обычно в сочетании с пользователем `nobody`.
operator	Существует только по историческим причинам для уведомления операторов, которые вошли в систему. Для повышения привилегий предпочтительно использовать утилиту sudo.
plugdev	Разрешает доступ к съемным устройствам, даже если для них не установлено значение `/etc/fstab`. Полезно для локальных пользователей, которым необходимо вставлять USB-накопители и т. д. Используется программой pmount (которая всегда монтирует съемные устройства с параметрами `nodev` и `nosuid`).
postfix	Используется MTA Postfix.
postgres	Управление базой данных PostgreSQL. Обычно используется только пользователем `postgres`
proxy	Для служб (обычно прокси-служб), у которых нет выделенных идентификаторов пользователей и которым необходимо иметь собственные файлы. Обычно используется `squid`и `pdnsd`.
saned	добавление `sane-utils`.
sasl	Разрешает запись в `/etc/sasldb`и/или `/etc/sasldb2`, которые используются для аутентификации sasl. Обычно используется для аутентификации серверами IMAP, POP и SMTP.
scanner	Позволяет использовать сканеры.

shadow	Позволяет читать `/etc/shadow`. Используется некоторыми программами, которым необходим доступ к этому файлу.
shutdown	Позволяет войти в систему, чтобы выключить систему.
src	Владелец исходного кода, в том числе `/usr/src`. Его можно использовать, чтобы дать пользователю возможность управлять исходным кодом.
ssh	Для предотвращения атак ptrace. Используется ssh-агентом.
staff	Поработаем над `/usr/local`, `/var/local`и `/home`. Обычно для доверенных администраторов.
sudo	Членам этой группы не нужно вводить свои пароли при использовании `sudo`. см `/usr/share/doc/sudo/OPTIONS`. .
sync	Позволяет войти в систему для синхронизации системы. Обычно используется пользователем синхронизации (с оболочкой `/bin/sync`)
sys	Присутствует из соображений совместимости.
syslog	Используется `syslog`, журнал общего назначения.
tape	Разрешает доступ к ленточному накопителю.
tty	Используется `write`и `wall` для записи в ttys других пользователей. Устройства `tty`и `/dev/vcs` относятся к этой группе.
uucp	Используется подсистемой UUCP.
users	Для группировки новых пользователей.
utmp	Позволяет записывать в `/var/run/utmp`, `/var/log/lastlog`, и подобные файлы. Используется некоторыми эмуляторами терминала.
video	Разрешает доступ к видео устройствам.
voice	Голосовая почта. Полезно для систем, использующих модемы в качестве автоответчиков.
wheel	Используем команду `su`. По умолчанию отключено .
www-data	Для записи данных веб-серверами. Пользователь `www-data`не должен *владеть* веб-контентом, иначе скомпрометированный сервер позволит переписать веб-сайт.

Чтобы узнать, какие файлы в вашей системе принадлежат к определенной группе, вы можете запустить команду, подобную следующей:

> *find / -xdev -group nombredelgrupo*

(Параметр **`-xdev`** предотвращает пересечение точек монтирования.)

Список пользователей без соответствующей группы

Некоторые пользователи не имеют соответствующей группы, а используют другую из упомянутых выше.

Пользователь	Функция / Примечания
sshd	Пользователь с низким уровнем привилегий, используемый sshd для связи с сетью до успешной аутентификации.

fetchmail	используется программой `fetchmail`.
cupsys	Используется CUPS (Common Un*x Printing System). Входит в группу lp.

Чтобы узнать, к каким группам принадлежит конкретный пользователь, вы можете запустить команду, подобную следующей:

> *id имяпользователя*

Оценки

В Debian GNU/Linux при создании нового пользователя по умолчанию также создается новая группа с тем же именем, поэтому с правильным umask (0002) и bit SETGID, установленным в каталоге проекта, она будет создана автоматически. назначает правильную группу файлам, созданным в этом каталоге.

Может показаться, что было бы более эффективно, если бы все новые пользователи принадлежали к группе `users`, как это традиционно делал UN*X, но это затрудняет управление разрешениями, когда один и тот же пользователь работает над несколькими проектами.

Однако вы можете изменить это поведение, изменив `/etc/adduser.conf`. Значение переменной необходимо изменить `USERGROUPS`на 'no', чтобы при создании пользователя не создавалась новая группа, а `USERS_GID` также изменить значение GID группы, к которой будут принадлежать пользователи.