

???????????? ???? ?
????????????

Команды групп

Команда	Описание
sudo adduser username	интерактивно создает пользователя с паролем и группой. Поведение настраивается в файлах /etc/adduser.conf Нельзя использовать в скриптах. При помощи encryptfs-utils можно зашифровать домашнюю директорию --encrypt-home
sudo useradd username	создает пользователя без группы и пароля. Поведение настраивается флагами и /etc/login.defs. -m создает домашнюю директорию -d определяет домашнюю директорию -s определяет консоль по умолчанию
groups	Список групп
sudo visudo	Настройка прав групп -f fname определяет дополнительный файл из include директории
sudo usermod -a -G sudo sergey	Добавить пользователя в группу sudo. -a оставляет существующие группы. Без -a пользователь будет исключен из остальных групп
sudo userdel username	Удалить пользователя
last	Последние авторизовавшиеся пользователи

Информация о пользователях, паролях, группах

/etc/passwd /etc/shadow /etc/group /etc/gshadow

Служба nss отвечает за хранение данных в любых хранилищах (вплоть до SQL).
/etc/nsswitch.conf

Определение библиотек, установленных у службы nss

```
~$ find /lib/ -name 'libnss_*'  
/lib/x86_64-linux-gnu/libnss_compat.so.2  
/lib/x86_64-linux-gnu/libnss_files.so.2
```

```
/lib/x86_64-linux-gnu/libnss_hesiod.so.2
/lib/x86_64-linux-gnu/libnss_systemd.so.2
/lib/x86_64-linux-gnu/libnss_dns.so.2
```

Настройка visudo

Элемент	Описание
#	Комментарий
% в начале строки	Работа с группой. %sudo обозначает настройку группы sudo
Структура назначения прав	%sudo ALL=(ALL) ALL обозначает, что группа sudo может выполнять на всех хостах от имени всех пользователей любые действия
NOPASSWD:	без ввода пароля sudo %sudo ALL=(ALL) NOPASSWD: ALL
User_Alias alias_name = username1, username2	Псевдоним для имен пользователей. User_Alias WEBADMINS = sergey, dimitry
Cmnd_Alias alias_name = cmnd1, cmnd2	Псевдоним для команд. Cmnd_Alias SOFTWARE /bin/apt /bin/apt-get Если команда перечисляется без субкоманд, то пользователю даются права на все субкоманды. Иначе, при перечислении субкоманд - только на них. Но при добавлении субкоманд требуется указывать полную строку. Например, если указать /usr/bin/systemctl status, то пользователь будет иметь право вызвать эту команду, но она нефункциональна - требует имя сервиса, а его задать уже нельзя. Можно использовать * /usr/bin/systemctl status * /usr/bin/systemctl * sshd В списке могут быть и файлы, доступные для редактирования. Например /usr/bin/nano /etc/ssh/sshd_config
WEBADMINS ALL=(ALL) SOFTWARE	Пользователи WEBADMINS могут запускать команды SOFTWARE через sudo
Host_Alias MAILSERVERS = smtp	Используется при распространении единого файла sudoers на все машины в сети. Ограничивает хосты, где работает данное правило WEBADMINS WEBSERVERS=(ALL) WEBCOMMANDS
Defaults timestamp_timeout = 0	Таймаут при необходимости ввода пароля sudo. Можно назначить только определенным пользователям Defaults:dmitry timestamp_timeout = 0

Элемент	Описание
@includedir dirname	для логического разбиения одного файла на группы. Подключается любой файл, если он не содержит в названии точку (.) или не заканчивается тильдой (~). Файлы анализируются в лексическом порядке. Например, /etc/sudoers.d/01_first анализируется перед /etc/sudoers.d/10_second. После анализа файлов в каталоге контроль возвращается к файлу, который содержал директиву @includedir.

Получается нужны шаблоны для определения действий в зависимости от роли пользователей. Их может быть немало)

Требования к паролю

```
sudo apt install libpam-pwquality
```

Настройки требований к паролю в файле /etc/security/pwquality.conf

Параметр	Описание
minlen=8	Минимальная длина пароля
minclass=3	Минимальное количество классов символов в пароле

Период обновления пароля

```
chage -l username
```

Блокировка пароля при неправильном вводе

Практически, нельзя устанавливать блокировку пароля после 3 неправильных вводов.

/etc/pam.d/login

Revision #9

Created 15 August 2025 18:10:20 by Admin

Updated 8 October 2025 01:51:19 by Admin