

Отчёт по лабораторной работе №2

Управление пользователями и группами

Ришард Когенгар

Содержание

1 Цель работы	5
2 Ход выполнения	6
3 Ход выполнения	7
3.1 Переключение учётных записей пользователей и настройка прав доступа	7
3.2 Создание учётных записей пользователей и настройка окружения	12
3.3 Работа с группами	15
3.4 Вывод	16
4 Контрольные вопросы	17

Список иллюстраций

3.1	Определение текущего пользователя и его идентификаторов	8
3.2	Переключение на пользователя root	9
3.3	Просмотр файла /etc/sudoers через visudo	10
3.4	Создание пользователей alice и bob	11
3.5	Редактирование файла login.defs	12
3.6	Изменение файла .bashrc в /etc/skel	13
3.7	Проверка домашнего каталога пользователя carol	14
3.8	Изменение параметров пароля пользователя carol	15
3.9	Проверка групп пользователей	16

Список таблиц

1 Цель работы

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

2 Ход выполнения

3 Ход выполнения

3.1 Переключение учётных записей пользователей и настройка прав доступа

1. Выполнен вход в систему под обычной учётной записью пользователя **rishard** и открыт терминал.

Для определения текущего пользователя использована команда `whoami`, в результате чего на экран выведено имя пользователя **rishard**.

Для получения расширенной информации об учётной записи выполнена команда `id`.

В выводе отображены:

- `uid=1000(rishard)` – уникальный идентификатор пользователя;
- `gid=1000(rishard)` – идентификатор основной группы;
- `groups=1000(rishard), 10(wheel)` – перечень групп, в которые входит пользователь;
- контекст безопасности SELinux.

Наличие группы **wheel** указывает на возможность использования команды `sudo`.

```
rishard@rishardkogengar:~$ whoami
rishard
rishard@rishardkogengar:~$ id
uid=1000(rishard) gid=1000(rishard) groups=1000(rishard),10(wheel) context=uncon
fined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
rishard@rishardkogengar:~$
rishard@rishardkogengar:~$ su
Password:
root@rishardkogengar:/home/rishard# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
root@rishardkogengar:/home/rishard#
exit
rishard@rishardkogengar:~$ █
```

Рис. 3.1: Определение текущего пользователя и его идентификаторов

2. Выполнено переключение на учётную запись администратора с помощью команды **su**.

После ввода пароля пользователя **root** выполнена команда **id**.

Полученный вывод подтверждает работу под суперпользователем:

- **uid=0(root)** и **gid=0(root)** – идентификаторы администратора;
- пользователь входит исключительно в группу **root**, что соответствует стандартной конфигурации системы.

```
rishard@rishardkogengar:~$ whoami
rishard
rishard@rishardkogengar:~$ id
uid=1000(rishard) gid=1000(rishard) groups=1000(rishard),10(wheel) context=uncon
fined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
rishard@rishardkogengar:~$
rishard@rishardkogengar:~$ su
Password:
root@rishardkogengar:/home/rishard# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
root@rishardkogengar:/home/rishard#
exit
rishard@rishardkogengar:~$ █
```

Рис. 3.2: Переключение на пользователя root

3. Выполнен выход из учётной записи **root** с помощью команды **exit**, после чего управление возвращено пользователю **rishard**.
4. Для безопасного просмотра и редактирования файла конфигурации прав доступа выполнена команда **sudo -i visudo**.

Использование утилиты **visudo** обязательно, так как она:

- блокирует файл **/etc/sudoers** от одновременного редактирования;
- проверяет синтаксис перед сохранением;
- предотвращает ошибки конфигурации, которые могут привести к потере административного доступа.

The screenshot shows a terminal window with the title bar "rishard@rishardkogengar:~ - sudo -i visudo". The terminal displays the contents of the /etc/sudoers file. The file includes comments about the main part of the sudoers file, syntax, and various command grants for root and other users. It also includes sections for the sys group, wheel group, and users group, along with a section for drop-in files and a note about includedir. The bottom right corner of the terminal shows the status "111, 0-1 Bot".

```
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user      MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root      ALL=(ALL)      ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel    ALL=(ALL)      ALL

## Same thing without a password
# %wheel      ALL=(ALL)      NOPASSWD: ALL
#
## Allows members of the users group to mount and umount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
```

Рис. 3.3: Просмотр файла /etc/sudoers через visudo

5. В файле /etc/sudoers обнаружена строка `%wheel ALL=(ALL) ALL`.

Данная запись означает, что все пользователи, входящие в группу **wheel**, имеют право выполнять любые команды от имени любого пользователя с использованием sudo.

Группа **wheel** применяется для централизованного управления административными привилегиями.

6. Создан пользователь **alice**, включённый в группу **wheel**, с помощью команды `sudo -i useradd -G wheel alice`.

Проверка выполнена командой `id alice`, вывод которой подтверждает принадлежность пользователя к группе **wheel**.

7. Для пользователя **alice** установлен пароль командой `sudo -i passwd alice`.

8. Выполнено переключение на учётную запись **alice** с помощью команды su alice.

9. Под учётной записью **alice** создан пользователь **bob** командой sudo useradd bob.

После этого установлен пароль командой sudo passwd bob.

Проверка с помощью id bob показала, что пользователь **bob** входит только в свою основную группу и не обладает административными правами.

```
rishard@rishardkogengar:~$ sudo -i useradd -G wheel alice
rishard@rishardkogengar:~$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)
rishard@rishardkogengar:~$ sudo -i passwd alice
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
rishard@rishardkogengar:~$ su alice
Password:
alice@rishardkogengar:/home/rishard$ sudo useradd bob
```

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.

For security reasons, the password you type will not be visible.

```
[sudo] password for alice:
alice@rishardkogengar:/home/rishard$ sudo passwd bob
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@rishardkogengar:/home/rishard$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
alice@rishardkogengar:/home/rishard$ █
```

Рис. 3.4: Создание пользователей alice и bob

3.2 Создание учётных записей пользователей и настройка окружения

10. Выполнен вход под учётной записью **root** и открыт для редактирования файл `/etc/login.defs`.

В файле изменены параметры:

- `CREATE_HOME yes` — включено автоматическое создание домашнего каталога пользователя;
- `USERGROUPS_ENAB no` — отключено создание персональной группы с именем пользователя, используется группа **users**.



The screenshot shows a terminal window titled "alice@rishardkogengar:/home/rishard - vim /etc/login.defs". The file content is as follows:

```
#USERDEL_CMD    /usr/sbin/userdel_local
#
# Enables userdel(8) to remove user groups if no members exist.
#
USERGROUPS_ENAB no

#
# If set to a non-zero number, the shadow utilities will make sure that
# groups never have more than this number of users on one line.
# This permits to support split groups (groups split into multiple lines,
# with the same group ID, to avoid limitation of the line length in the
# group file).
#
# 0 is the default value and disables this feature.
#
#MAX_MEMBERS_PER_GROUP  0

#
# If useradd(8) should create home directories for users by default (non
# system users only).
# This option is overridden with the -M or -m flags on the useradd(8)
# command-line.
#
CREATE_HOME      yes

#
# Force use shadow, even if shadow passwd & shadow group files are
# missing.
#
#FORCE_SHADOW     yes
-- INSERT --
```

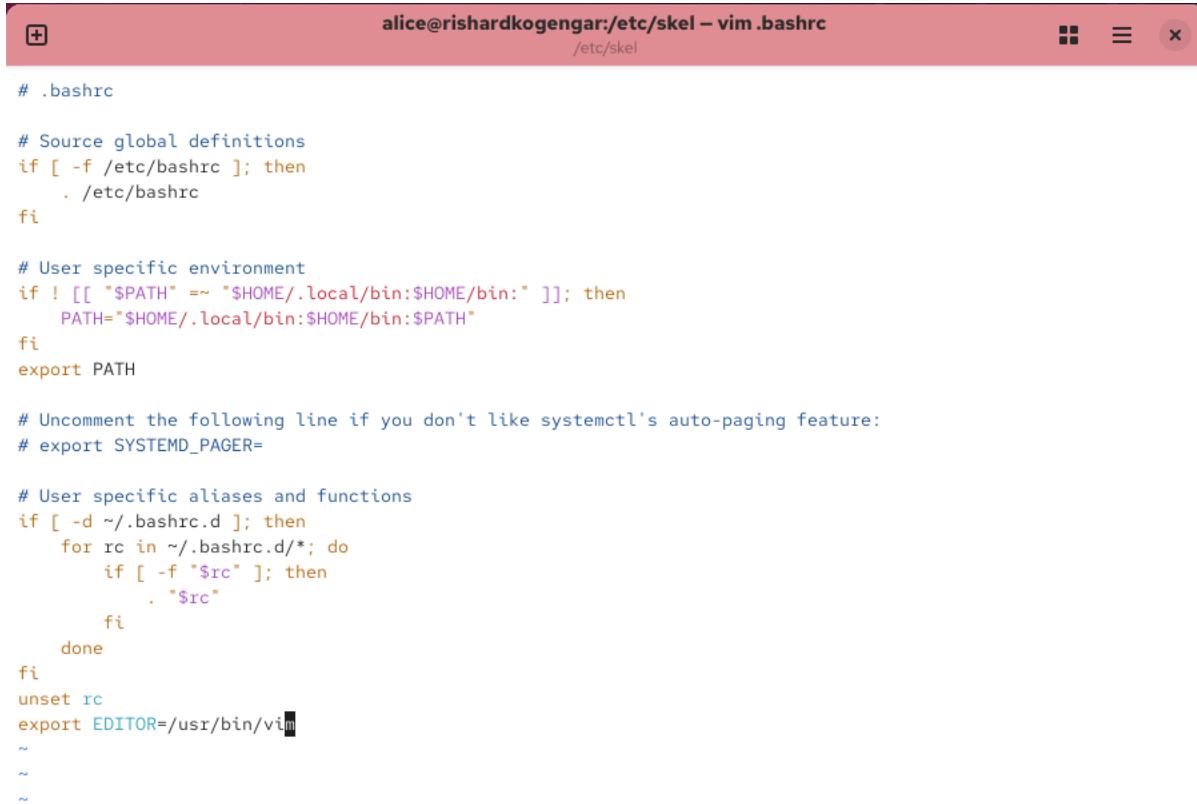
At the bottom right of the terminal window, there are status indicators: "280,19" and "96%".

Рис. 3.5: Редактирование файла `login.defs`

11. Выполнен переход в каталог `/etc/skel`.

В каталоге созданы директории **Pictures** и **Documents**, которые автоматически копируются в домашние каталоги новых пользователей.

12. В файле `/etc/skel/.bashrc` добавлена строка `export EDITOR=/usr/bin/vim`. Данная настройка задаёт текстовый редактор **vim** в качестве редактора по умолчанию для пользователей системы.



The screenshot shows a terminal window titled "alice@rishardkogengar:/etc/skel – vim .bashrc". The file content is as follows:

```
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]; then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
if [ -d ~/.bashrc.d ]; then
    for rc in ~/.bashrc.d/*; do
        if [ -f "$rc" ]; then
            . "$rc"
        fi
    done
fi
unset rc
export EDITOR=/usr/bin/vim
```

Рис. 3.6: Изменение файла `.bashrc` в `/etc/skel`

13. Под учётной записью **alice** создан пользователь **carol**, после чего для него установлен пароль.
14. Выполнен вход под пользователем **carol** и проверены параметры учётной записи и содержимое домашнего каталога.

Установлено, что:

- основной группой пользователя является **users** с идентификатором `gid=100`;

- в домашнем каталоге автоматически созданы директории **Pictures** и **Documents**.

```
root@rishardkogengar:/etc/skel# su alice
alice@rishardkogengar:/etc/skel$ sudo -i useradd carol
alice@rishardkogengar:/etc/skel$ sudo passwd carol
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@rishardkogengar:/etc/skel$ su carol
Password:
carol@rishardkogengar:/etc/skel$ id
uid=1003(carol) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
carol@rishardkogengar:/etc/skel$ cd
carol@rishardkogengar:~$ ls -Al
total 12
-rw-r--r--. 1 carol users 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 carol users 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 carol users 549 Jan 18 12:50 .bashrc
drwxr-xr-x. 2 carol users 6 Jan 18 12:49 Documents
drwxr-xr-x. 4 carol users 39 Jan 18 12:17 .mozilla
drwxr-xr-x. 2 carol users 6 Jan 18 12:49 Pictures
carol@rishardkogengar:~$
```

Рис. 3.7: Проверка домашнего каталога пользователя carol

15. Выполнен анализ записи пользователя **carol** в файле /etc/shadow.

Запись содержит зашифрованный пароль, дату последней смены пароля и параметры срока его действия.

16. Изменены параметры срока действия пароля пользователя **carol**:

- минимальный срок использования пароля — 30 дней;
- предупреждение об истечении срока — за 3 дня;
- максимальный срок действия пароля — 90 дней.

Повторная проверка в файле /etc/shadow подтвердила внесённые изменения.

```

carol@rishardkogengar:~$ su alice
Password:
alice@rishardkogengar:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$WhOHmS/CI3TzpqEOGoNwN1$YoJsNrMuB4zbmfqtWDqav09/lR08G2Q/t6N1/zT9Yx2:20471:0:99999:7:::
alice@rishardkogengar:/home/carol$ sudo passwd -n 30 -w 3 -x 90 carol
passwd: password changed.
alice@rishardkogengar:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$WhOHmS/CI3TzpqEOGoNwN1$YoJsNrMuB4zbmfqtWDqav09/lR08G2Q/t6N1/zT9Yx2:20471:30:90:3:::
alice@rishardkogengar:/home/carol$ sudo grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001:/home/alice:/bin/bash
/etc/shadow:alice:$y$j9T$VZ0y6VU26jH/V5vgUlg5F/$J1xAf5lSjpuoxTXaP/0vFjAmI2mVsgU3j66aNqjVcB7:20471:0:99999:7:::
/etc/group:wheel:x:10:rishard,alice
/etc/group:alice:x:1001:
alice@rishardkogengar:/home/carol$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:100:::/home/carol:/bin/bash
/etc/shadow:carol:$y$j9T$WhOHmS/CI3TzpqEOGoNwN1$YoJsNrMuB4zbmfqtWDqav09/lR08G2Q/t6N1/zT9Yx2:20471:30:90:3:::
alice@rishardkogengar:/home/carol$ 
```

Рис. 3.8: Изменение параметров пароля пользователя carol

17. Выполнена проверка наличия идентификатора пользователя **alice** в файлах **/etc/passwd**, **/etc/shadow** и **/etc/group**.

Пользователь **alice** присутствует во всех трёх файлах.

Проверка для пользователя **carol** показала, что его идентификатор присутствует не во всех файлах, что соответствует ожидаемому результату.

3.3 Работа с группами

18. Под учётной записью **alice** созданы группы **main** и **third**.

19. Пользователи добавлены в группы:

- **alice** и **bob** – в группу **main**;
- **carol** – в группу **third**.

20. Проверка с помощью команды **id carol** показала, что:

- основной группой пользователя является **users**;
- вторичной группой является **third**.

21. Проверка остальных пользователей подтвердила:

- пользователь **alice** состоит в группах **alice**, **wheel** и **main**;

- пользователь **bob** состоит в группах **bob** и **main**.

```
alice@rishardkogengar:/home/carol$  
alice@rishardkogengar:/home/carol$ sudo groupadd main  
alice@rishardkogengar:/home/carol$ sudo groupadd third  
alice@rishardkogengar:/home/carol$ sudo usermod -aG main alice  
alice@rishardkogengar:/home/carol$ sudo usermod -aG main bob  
alice@rishardkogengar:/home/carol$ sudo usermod -aG third carol  
alice@rishardkogengar:/home/carol$ id carol  
uid=1003(carol) gid=100(users) groups=100(users),1004(third)  
alice@rishardkogengar:/home/carol$ id alice  
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel),1003(main)  
alice@rishardkogengar:/home/carol$ id bob  
uid=1002(bob) gid=1002(bob) groups=1002(bob),1003(main)  
alice@rishardkogengar:/home/carol$ █
```

Рис. 3.9: Проверка групп пользователей

3.4 Вывод

В ходе выполнения лабораторной работы были изучены и отработаны основные операции управления пользователями и группами в операционной системе Linux. Выполнено переключение между учётными записями обычного пользователя и администратора, рассмотрены принципы работы идентификаторов пользователей и групп, а также механизм предоставления административных прав через группу **wheel** и утилиту **sudo**.

Были созданы новые учётные записи пользователей и группы, настроены параметры их домашнего окружения и политики управления паролями, а также проверено корректное применение заданных настроек. Полученные результаты подтверждают правильную конфигурацию системы и соответствие выполненных действий требованиям задания.

4 Контрольные вопросы

1. При помощи каких команд можно получить информацию о номере (идентификаторе), назначенному пользователю Linux, и о группах, в которые включён пользователь?

Для получения информации об идентификаторе пользователя и его группах используются следующие команды:

`id` – выводит UID, GID и список всех групп пользователя. Пример: `id alice`
`groups` – отображает перечень групп, в которые входит пользователь. Пример: `groups alice`

`getent passwd <user>` – позволяет получить UID и GID пользователя из системной базы.

2. Какой UID имеет пользователь root? При помощи какой команды можно узнать UID пользователя? Приведите примеры.

Пользователь **root** всегда имеет идентификатор **UID = 0**.

Узнать UID пользователя можно с помощью команды `id`.

Примеры:

`id root` – выводит UID=0 для пользователя root

`id alice` – выводит UID обычного пользователя

3. В чём состоит различие между командами su и sudo?

Команда `su` используется для полного переключения на другую учётную запись, чаще всего на root, с вводом пароля этого пользователя.

Команда `sudo` позволяет выполнить отдельную команду с повышенными привилегиями, не выполняя полный вход под root, при этом используется пароль

текущего пользователя (если он имеет соответствующие права).

4. В каком конфигурационном файле определяются параметры sudo?

Основные параметры работы команды sudo определяются в конфигурационном файле /etc/sudoers, а также во включаемых файлах каталога /etc/sudoers.d.

5. Какую команду следует использовать для безопасного изменения конфигурации sudo?

Для безопасного изменения конфигурации sudo следует использовать команду visudo, так как она проверяет синтаксис файла перед сохранением и предотвращает его повреждение.

6. Если вы хотите предоставить пользователю доступ ко всем командам администрирования системы через sudo, членом какой группы он должен быть?

Пользователь должен быть членом группы **wheel**, так как для неё в файле /etc/sudoers обычно задано правило %wheel ALL=(ALL) ALL.

7. Какие файлы и каталоги можно использовать для определения параметров, которые будут применяться при создании учётных записей пользователей? Приведите примеры настроек.

При создании учётных записей используются следующие файлы и каталоги: /etc/login.defs – задаёт параметры создания пользователей (например, CREATE_HOME, USERGROUPS_ENAB).

/etc/skel – шаблон домашнего каталога пользователя (файлы .bashrc, .bash_profile, каталоги Documents, Pictures).

8. Где хранится информация о первичной и дополнительных группах пользователей Linux? Поясните такие записи для пользователя alice.

Информация о пользователях и группах хранится в файлах:

/etc/passwd – содержит UID и идентификатор основной группы (GID);

/etc/group – содержит сведения о дополнительных группах;

/etc/shadow – содержит данные о паролях и их сроках действия.

Для пользователя **alice**:

- в `/etc/passwd` указаны её UID и основной GID;
- в `/etc/group` указано членство в дополнительных группах, например **wheel** и **main**.

9. Какие команды можно использовать для изменения информации о пароле пользователя (например, о сроке действия пароля)?

Для управления параметрами пароля используются команды:

`passwd` — изменение пароля пользователя;
`passwd -x` — установка максимального срока действия пароля;
`passwd -n` — минимальный срок использования пароля;
`passwd -w` — срок предупреждения об истечении пароля;
`chage` — расширенное управление сроками действия пароля.

10. Какую команду следует использовать для прямого изменения информации в файле `/etc/group` и почему?

Для безопасного изменения файла `/etc/group` следует использовать команду `vigr`, так как она обеспечивает проверку целостности файла и блокировку от одновременного редактирования, что предотвращает повреждение системной базы групп.