# Отчёт по лабораторной работе 9

**Управление SELinux**

Вишняков Родион Сергеевич

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Выполнение лабораторной работы

Получаем полномочия администратора

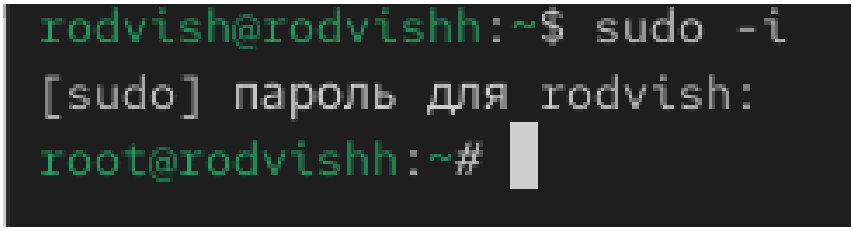


Рис. 2.1: root

Просмотрели текущую информацию о состоянии SELinux

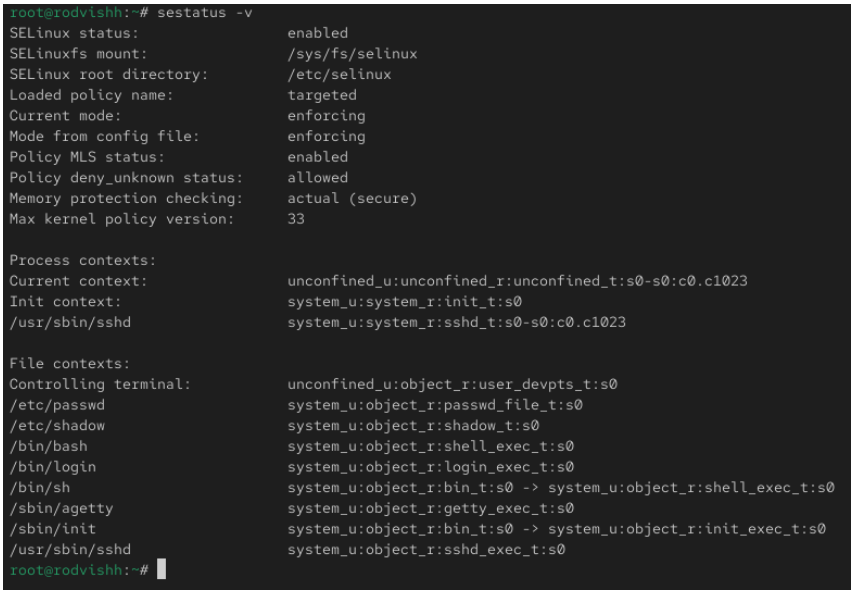


Рис. 2.2: SELinux

Посмотрели, в каком режиме работает SELinux

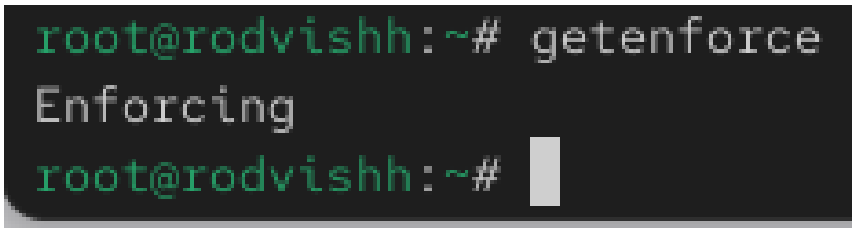


Рис. 2.3: SELinux

В файле /etc/sysconfig/selinux с помощью редактора установили заданное значение

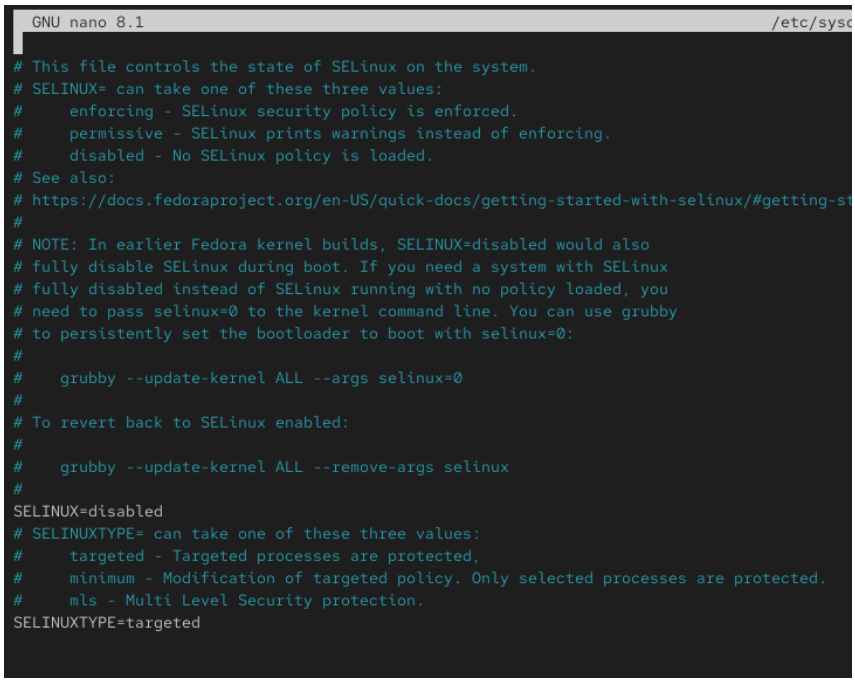


Рис. 2.4: Изменение редактора

Посмотрели статус SELinux

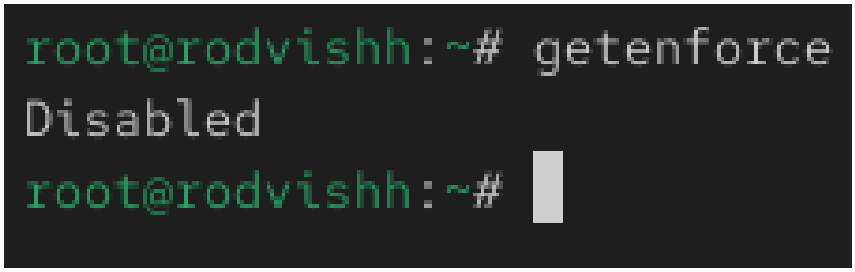


Рис. 2.5: SELinux

Попробовали переключить режим работы SELinux

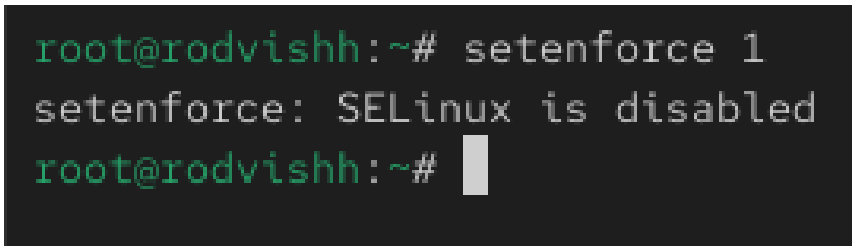


Рис. 2.6: SELinux

В файле /etc/sysconfig/selinux с помощью редактора установили заданное значение

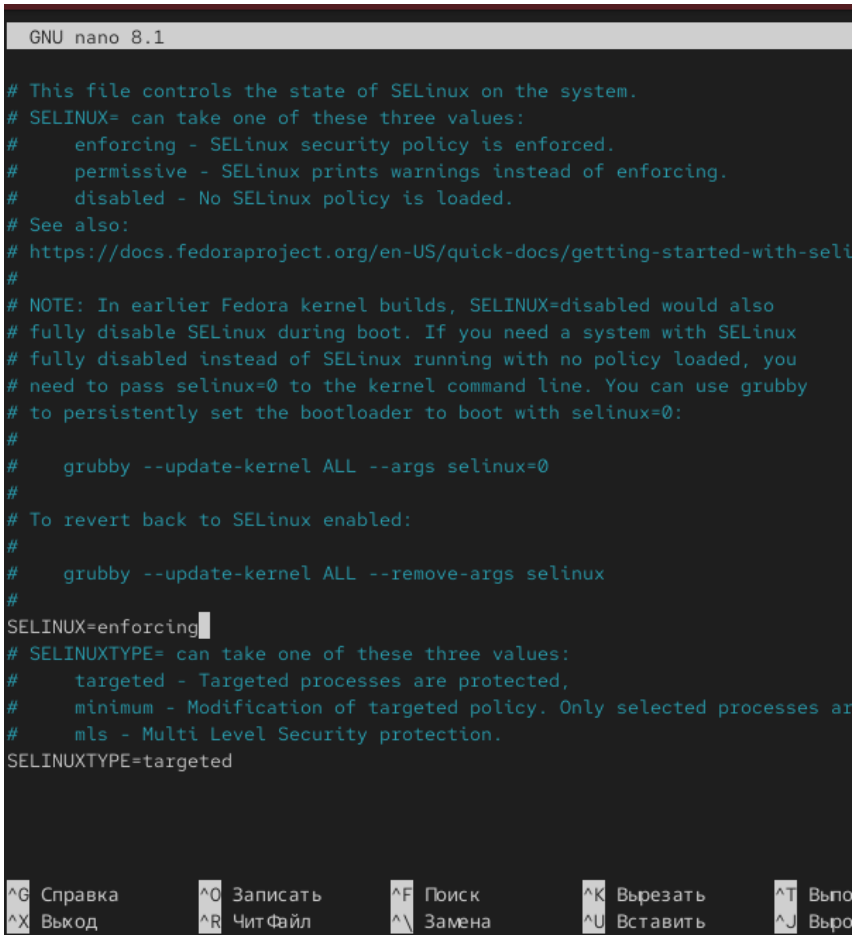


Рис. 2.7: Изменение редактора

Просмотрели текущую информацию о состоянии SELinux

```
root@rodvishh:~# sestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
root@rodvishh:~#
```

Рис. 2.8: SELinux

Посмотрели контекст безопасности файла /etc/hosts

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 2.9: Контекст безопасности файла

Скопировали файл /etc/hosts в домашний каталог и проверили контекст файла ~/hosts

```
root@rodvishh:~# cp /etc/hosts ~/
root@rodvishh:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@rodvishh:~#
```

Рис. 2.10: Создание файла сценария

Попытались перезаписать существующий файл hosts из домашнего каталога в ката- лог /etc

```
root@rodvishh:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'?
root@rodvishh:~#
```

Рис. 2.11: Файл hosts

Убедились, что тип контекста по-прежнему установлен на admin_home_t

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 2.12: admin_home_t

Исправили контекст безопасности

```
root@rodvishh:~# restorecon -v /etc/hosts
root@rodvishh:~#
```

Рис. 2.13: Контекст безопасности

Убедились, что тип контекста изменился

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 2.14: Тип контекста

Для массового исправления контекста безопасности на файловой системе ввели

```
root@rodvishh:~# touch /.autorelabel
root@rodvishh:~#
```

Рис. 2.15: Массовое исправления контекста

Получаем полномочия администратора

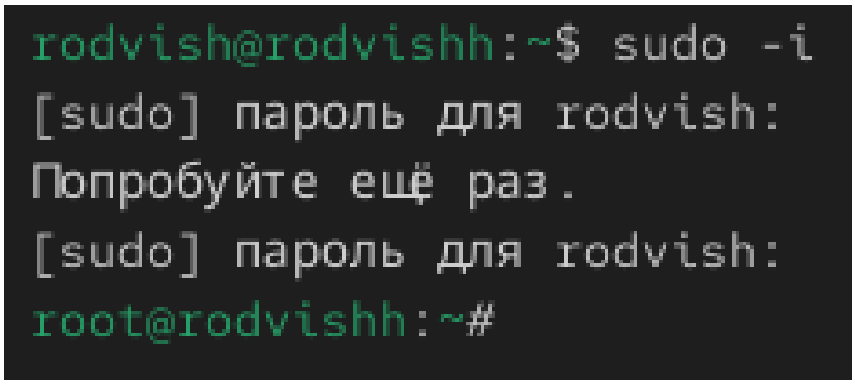


Рис. 2.16: root

Установливаем необходимое программное обеспечение

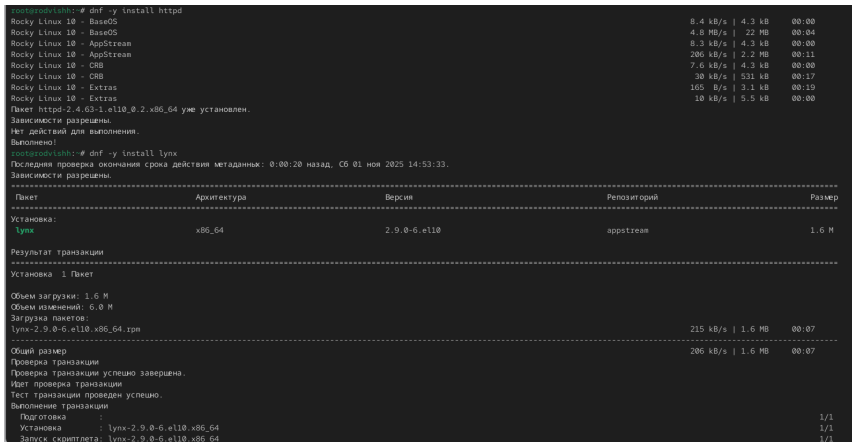


Рис. 2.17: Необходимое программное обеспечение

Создали новое хранилище для файлов web-сервера


Рис. 2.18: Новое хранилище

Создали файл index.html в каталоге с контентом веб-сервера и поместили в файл следующий текст

```
root@rodvishh:~# cd /web
root@rodvishh:/web# touch index.html
root@rodvishh:/web# echo "Welcome to my web-server" > /web/index.html
root@rodvishh:/web#
```

Рис. 2.19: index.html

Проделываем различные действия со строками в файле /etc/httpd/conf/httpd.conf

```
#
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
    # AllowOverride None
     # Allow open access:
     #Require all granted
#</Directory>
<Directory "/web">
        AllowOverride None
        Require all granted
</Directory>
# Further relax access to the default document
```

Рис. 2.20: /etc/httpd/conf/httpd.conf

Запустили веб-сервер и службу httpd

```
root@rodvishh:/web# systemctl start httpd
root@rodvishh:/web# systemctl enable httpd
root@rodvishh:/web#
```

Рис. 2.21: Служба httpd и веб-сервер

Обратились к веб-серверу в текстовом браузере lynx

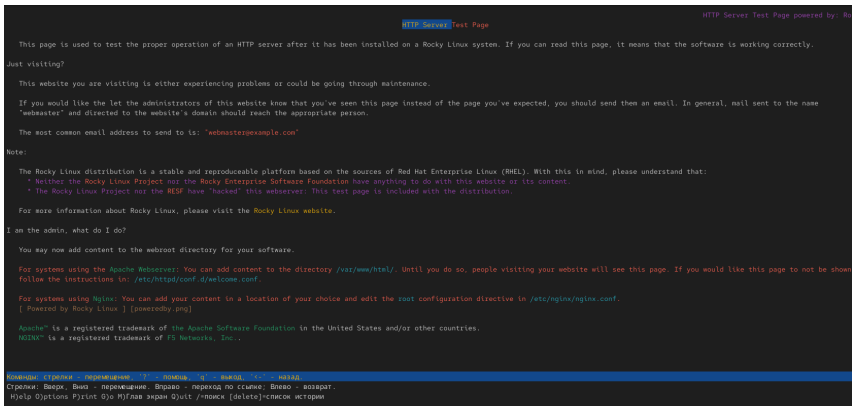


Рис. 2.22: lynx

В терминале с полномочиями администратора применили новую метку контекста к /web


Рис. 2.23: Новая метку контекста к /web

Восстановили контекст безопасности


Рис. 2.24: Контекст безопасности

Снова обращаемся к веб-серверу

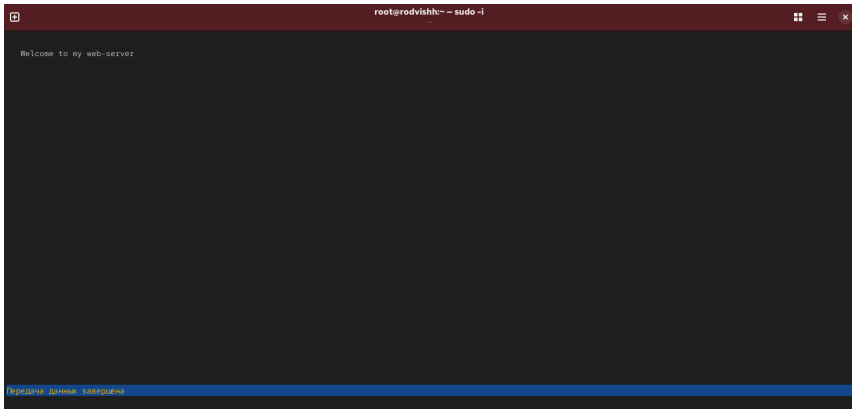


Рис. 2.25: Веб-сервер

Посмотрели список переключателей SELinux для службы ftp

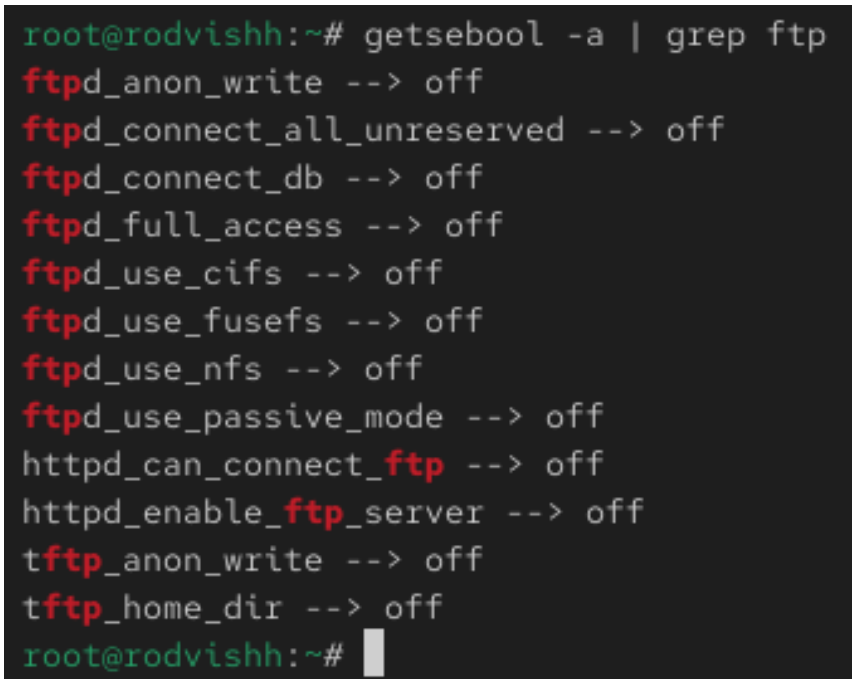


Рис. 2.26: Список переключателей SELinux

Посмотрели список переключателей с пояснением

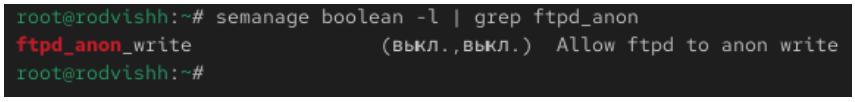


Рис. 2.27: Список переключателей с пояснением

Изменили текущее значение переключателя для службы ftpd_anon_write с off на on


Рис. 2.28: Значение переключателя

Повторно посмотрели список переключателей SELinux для службы ftpd_anon_write

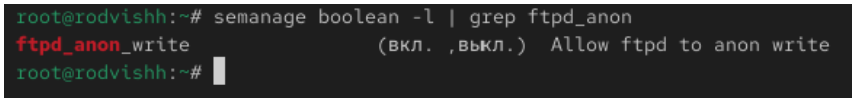


Рис. 2.29: Список переключателей SELinux

Изменили постоянное значение переключателя для службы ftpd_anon_write с off на on

```
root@rodvishh:~# setsebool -P ftpd_anon_write on
```

Рис. 2.30: Постоянное значение переключателя

Посмотрели список переключателей

```
root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write                (вкл. , вкл.)  Allow ftpd to anon write
root@rodvishh:~#
```

Рис. 2.31: Список переключателей

# 3 Вывод

Мы получили навыки работы с контекстом безопасности и политиками SELinux.

# 4 Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? Ответ: Команда setenforce 0.

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? Ответ: Команда getsebool -a.

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? Ответ: Имя пакета setroubleshoot.

4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd_sys_content_t к каталогу /web? Ответ: Команда chcon -t httpd_sys_content_t /web или команды semanage fcontext -a -t httpd_sys_content_t ’/web(/.*)?’ и затем restorecon -Rv /web.

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? Ответ: Файл /etc/selinux/config.

6. Где SELinux регистрирует все свои сообщения? Ответ: В журнале аудита /var/log/audit/audit.log и в системном журнале /var/log/messages.

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию? Ответ: Команда sepolicy ftp или semanage boolean -l | grep ftp.

8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать? Ответ: Временно перевести SELinux в разрешающий режим с помощью команды setenforce 0 и проверить, исчезла ли проблема.