

# **Лабораторная работа № 9. Управление SELinux**

**Отчёт**

Сергеев Даниил Олегович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Ход выполнения лабораторной работы</b>	<b>7</b>
3.1	Управление режимами SELinux . . . . .	7
3.2	Использование restorecon для восстановления контекста безопасности . . . . .	10
3.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера . . . . .	12
3.4	Работа с переключателями SELinux . . . . .	15
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>18</b>
<b>5</b>	<b>Вывод</b>	<b>20</b>
	<b>Список литературы</b>	<b>21</b>

# Список иллюстраций

3.1	Вывод команды <code>sestatus -v</code> (1)	8
3.2	Вывод команды <code>sestatus -v</code> (2)	8
3.3	Вывод команды <code>sestatus -v</code> (3)	8
3.4	Изменение режимов SELinux с помощью <code>setenforce</code>	9
3.5	Установка режима <code>SELINUX=disabled</code>	9
3.6	Попытка переключение режима SELinux	10
3.7	Восстановление меток SELinux после перезапуска	10
3.8	Контекст безопасности файла после копирования	11
3.9	Восстановление контекста безопасности <code>/etc/hosts</code>	11
3.10	Автоматическая перемаркировка SELinux во время перезапуска системы	11
3.11	Проверка патеков <code>httpd</code> , <code>lynx</code>	12
3.12	Изменение конфигурации <code>httpd</code>	13
3.13	Запуск <code>httpd</code>	13
3.14	Веб-страница до настройки контекста безопасности	14
3.15	Настройка контекста для веб-сервера	14
3.16	Обновленная веб-страница	15
3.17	Переключатели для службы <code>ftp</code> , <code>ftpd_anon</code>	16
3.18	Переключатель для службы <code>ftpd_anon</code> после изменения значения	16
3.19	Переключатели для службы <code>ftp</code> , <code>ftpd_anon</code>	17
4.1	Вывод <code>seinfo</code>	19

## **Список таблиц**

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

[1]

## 2 Задание

- Продемонстрировать навыки по управлению режимами SELinux
- Продемонстрировать навыки по восстановлению контекста безопасности SELinux
- Настроить контекст безопасности для нестандартного расположения файлов веб-службы
- Продемонстрировать навыки работы с переключателями SELinux

## 3 Ход выполнения лабораторной работы

### 3.1 Управление режимами SELinux

Запустим терминал, получим права администратора (su -) и посмотрим текущую информацию о состоянии SELinux с помощью команды `sestatus -v`.

Опишем информацию, выведенную на экран:

- SELinux status - статус работы службы SELinux;
- SELinuxfs mount - временная точка монтирования файловой системы SELinux;
- SELinux root directory - расположение файлов конфигурации SELinux;
- Loaded policy name - тип загруженной на данный момент политики SELinux;
- Current mode - текущий режим работы SELinux (Enforcing - блокировка нарушений и их фиксация, permissive - только фиксация нарушений, disabled - SELinux отключен);
- Mode from config file - режим работы, указанный в файле конфигурации `/etc/selinux/config`;
- Policy MLS status - статус политики MLS;
- Policy deny\_unknown status - статус переключателя (флага) `deny_unknown` в текущей политике;
- Memory protection checking - режим работы защиты памяти;

- Max kernel policy version - максимальная версия политики, поддерживаемая ядром Linux.

```
[root@dosergeev ~]# 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
```

Рис. 3.1: Вывод команды sestatus -v (1)

- Process contexts - контексты безопасности процессов из конфига /etc/sestatus.conf.

```
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
```

Рис. 3.2: Вывод команды sestatus -v (2)

- File contexts - контексты безопасности файлов из конфига /etc/sestatus.conf.

```
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
```

Рис. 3.3: Вывод команды sestatus -v (3)

Используя команду getenforce посмотрим, в каком режиме работает SELINUX. На данный момент он находится в режиме Enforcing. Изменим режим работы на



Permissive: setenforce 0; И снова проверим режим: на этот раз он изменился на Permissive.

```
[root@dosergeev ~]# getenforce
Enforcing
[root@dosergeev ~]# setenforce 0
[root@dosergeev ~]# getenforce
Permissive
```

Рис. 3.4: Изменение режимов SELinux с помощью setenforce

В файле `/etc/sysconfig/selinux` изменим состояние режима на `disabled` и перезапустим систему.

```
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/selinux" 29L, 1262B
```

22,16

Рис. 3.5: Установка режима SELINUX=disabled

После перезагрузки запустим терминал под учетной записью root и посмотрим текущий статус. Вывелась строка Disabled - значит SELinux отключен. Попробуем переключить режим работы на enforcing (setenforce 1). Так как SELinux отключен, на экран вывелась ошибка

- setenforce: SELinux is disabled

```
[dosergeev@dosergeev ~]$ getenforce
Disabled
[dosergeev@dosergeev ~]$ setenforce 1
setenforce: SELinux is disabled
[dosergeev@dosergeev ~]$ v
```

Рис. 3.6: Попытка переключение режима SELinux

Снова откроем файл `/etc/sysconfig/selinux` с помощью редактора и установим режим `SELINUX=enforcing` вручную. Перезагрузим систему.

Во время загрузки выводится предупреждающее сообщение о восстановлении меток SELinux.

```
[ 10.313904] selinux-autorelabel[770]: *** Warning -- SELinux targeted policy relabel is required.
[ 10.314238] selinux-autorelabel[770]: *** Relabeling could take a very long time, depending on file
[ 10.314367] selinux-autorelabel[770]: *** system size and speed of hard drives.
[ 10.337913] selinux-autorelabel[770]: Running: /sbin/fixfiles -T 0 restore
[ 21.984579] selinux-autorelabel[776]: Warning: Skipping the following R/O filesystems:
[ 21.984835] selinux-autorelabel[776]: /run/credentials/systemd-sysctl.service
[ 21.984914] selinux-autorelabel[776]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 21.984986] selinux-autorelabel[776]: /run/credentials/systemd-tmpfiles-setup.service
```

Рис. 3.7: Восстановление меток SELinux после перезапуска

После перезапуска снова введем команду `sestatus -v`, чтобы проверить режим: теперь выводится принудительный режим `Enforcing`, как и было запланировано.

## 3.2 Использование `restorecon` для восстановления контекста безопасности

Просмотрим контекст безопасности файла `/etc/hosts`. У файла наблюдается отметка контекста: `net_conf_t`. Скопируем этот файл в домашний каталог и снова проверим контекст. На этот раз установлено: `admin_home_t`.

```
[dosergeev@dosergeev ~]$ su -
Password:
[root@dosergeev ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@dosergeev ~]# cp /etc/hosts ~/
[root@dosergeev ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@dosergeev ~]#
```

Рис. 3.8: Контекст безопасности файла после копирования

Попытаемся перезаписать файл `/etc/hosts` уже существующим файлом из домашнего каталога и убедимся, что контекст изменился. Так как он действительно изменился, исправим все до прежних настроек, используя `restorecon -v /etc/hosts`. Теперь контекст снова равен `net_conf_t`.

```
[root@dosergeev ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@dosergeev ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@dosergeev ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@dosergeev ~]# ls -Z /etc/host
ls: cannot access '/etc/host': No such file or directory
[root@dosergeev ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@dosergeev ~]#
```

Рис. 3.9: Восстановление контекста безопасности `/etc/hosts`

Для массового исправления контекста создадим файл `.autorelabel` в корневом каталоге и перезапустим систему. Во время перезагрузки нажмем `Esc`, чтобы проверить загрузочные сообщения. SELinux запустил автоматическую перемаркировку контекста.

```
OK ] Finished Restore /run/initramfs on shutdown.
t 11.442656] selinux-autorelabel(768): *** Warning -- SELinux targeted policy relabel is required.
t 11.443936] selinux-autorelabel(768): *** Relabeling could take a very long time, depending on file
t 11.445384] selinux-autorelabel(768): *** system size and speed of hard drives.
t 11.473574] selinux-autorelabel(768): Running: /sbin/fixfiles -T 0 restore
t 24.221587] selinux-autorelabel(774): Warning: Skipping the following R/O filesystems:
t 24.222586] selinux-autorelabel(774): /run/credentials/systemd-sysctl.service
t 24.223244] selinux-autorelabel(774): /run/credentials/systemd-tmpfiles-setup-dev.service
t 24.223969] selinux-autorelabel(774): /run/credentials/systemd-tmpfiles-setup.service
t 24.224678] selinux-autorelabel(774): Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kernel
l/debug /sys/kernel/tracing
```

Рис. 3.10: Автоматическая перемаркировка SELinux во время перезапуска системы

### 3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Проверим установку пакетов httpd и lynx.

```
[root@dosergeev ~]# dnf -y install httpd
Last metadata expiration check: 1:01:34 ago on Sat 01 Nov 2025 06:05:04 PM MSK.
Package httpd-2.4.62-4.el9_6.4.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@dosergeev ~]# dnf -y install lynx
Last metadata expiration check: 1:01:42 ago on Sat 01 Nov 2025 06:05:04 PM MSK.
Package lynx-2.8.9-20.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@dosergeev ~]#
```

Рис. 3.11: Проверка пакетов httpd, lynx

Так как они установлены, приступим к следующему заданию.

Создадим новое хранилище для файлов веб-сервера: `mkdir /web`; Также создадим индекс (в новом каталоге): `touch index.html`.

В индекс запишем сообщение - Welcome to my web-server.

Откроем файл `/etc/httpd/conf/httpd.conf` на редактирование. Закомментируем строку `DocumentRoot` и тег (раздел) `Directory`, после чего добавим те же строки, заменив пути `/var/www/html` и `/var/www` на `/web`.

```
# 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>
```

Рис. 3.12: Изменение конфигурации httpd

Запустим веб-сервер и службу httpd.

```
[root@dosergeev web]# systemctl start httpd
[root@dosergeev web]# systemctl enable httpd
[root@dosergeev web]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-11-01 19:05:43 MSK; 6min ago
     Docs: man:httpd.service(8)
    Main PID: 1143 (httpd)
```

Рис. 3.13: Запуск httpd

Откроем терминал под своей основной учетной записью и обратимся к веб-серверу по адресу localhost в текстовом браузере lynx. Так как контекст безопасности не настроен, выводится веб-страница Red Hat по умолчанию, а не содержимое index.html

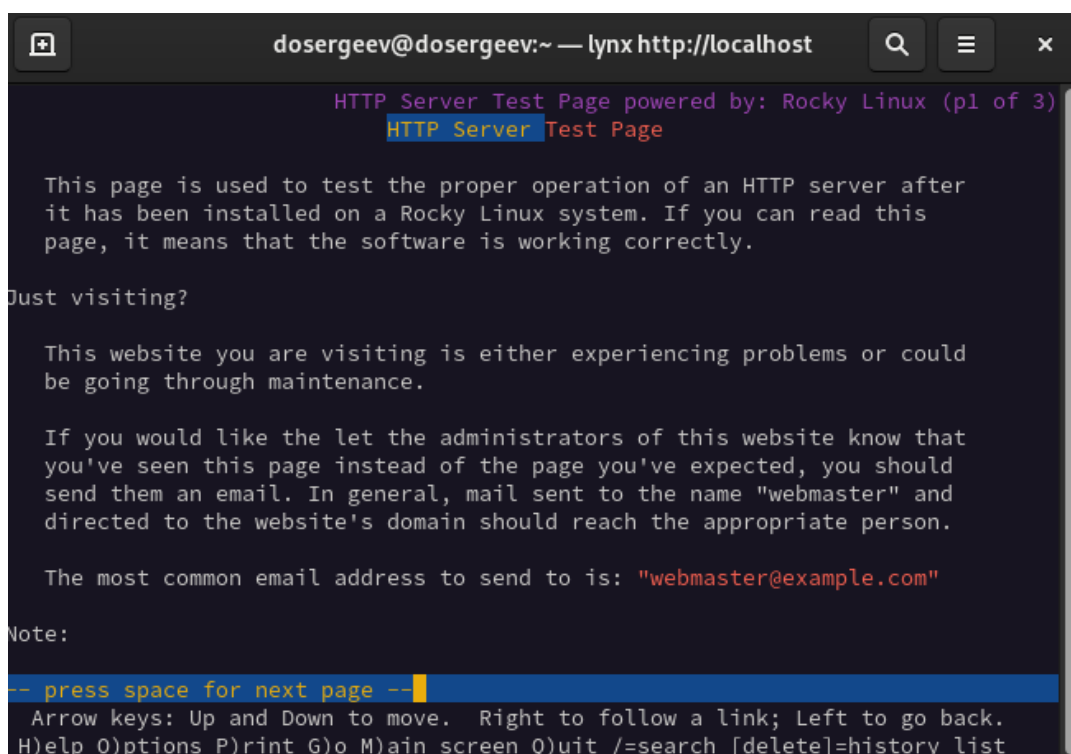


Рис. 3.14: Веб-страница до настройки контекста безопасности

В терминале с полномочиями администратора установим новую метку контекста к /web и восстановим контекст безопасности.

```
[root@dosergeev web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@dosergeev web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
[root@dosergeev web]#
```

Рис. 3.15: Настройка контекста для веб-сервера

Попробуем снова обратиться к странице. Она не обновилась, поэтому перезапустим систему чтобы обновить настройки SELinux.

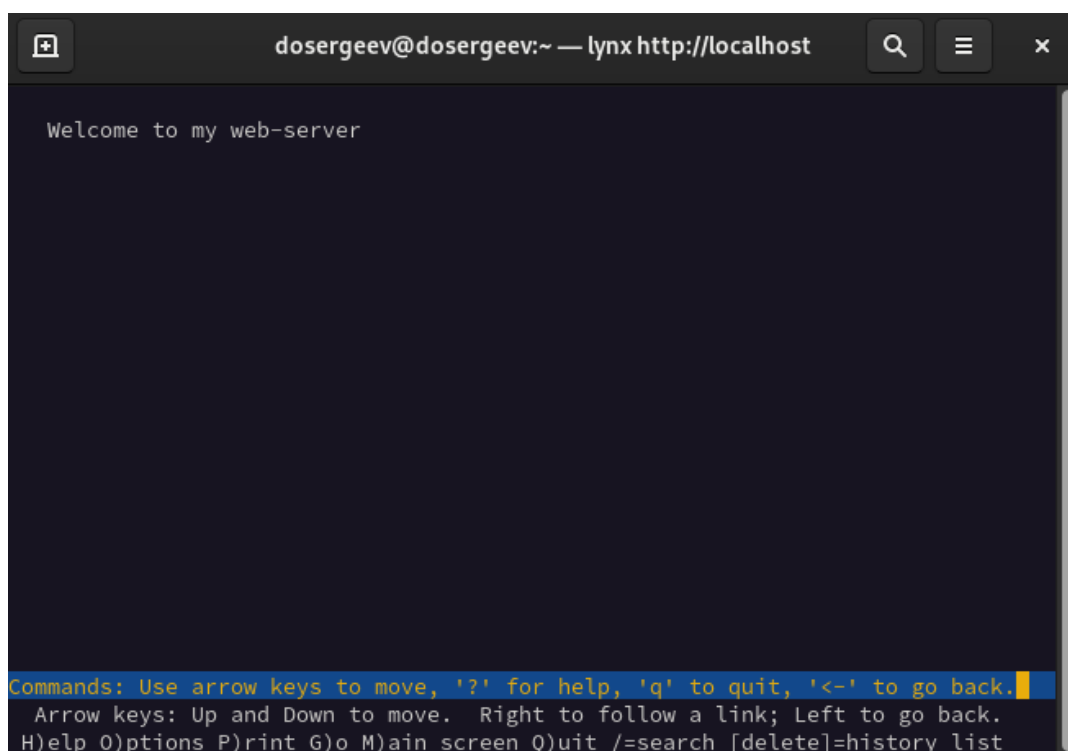


Рис. 3.16: Обновленная веб-страница

Теперь на экране отображена запись “Welcome to my web-server”.

### 3.4 Работа с переключателями SELinux

Снова запустим терминал под учетной записью root и посмотрим список переключателей SELinux для службы ftp. Отметим, что параметр ftpd\_anon\_write имеет значение off. Просмотрим список переключателей с пояснением для службы ftpd\_anon.

```
[root@dosergeev ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@dosergeev ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
```

Рис. 3.17: Переключатели для службы ftp, ftpd\_anon

Вывелся только один переключатель: ftpd\_anon\_write. Он имеет параметры (off - настройка времени выполнения отключена, off - постоянная настройка отключена) и краткое описание: “Позволить ftpd анонимную запись”.

Изменим текущее значение переключателя ftpd\_anon\_write с off на on: setsebool ftpd\_anon\_write on; Повторно посмотрим список переключателей (в том числе и с пояснением): getsebool ftpd\_anon\_write.

```
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@dosergeev ~]# setsebool ftpd_anon_write on
[root@dosergeev ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@dosergeev ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
[root@dosergeev ~]#
```

Рис. 3.18: Переключатель для службы ftpd\_anon после изменения значения

Настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Изменим постоянное значение переключателя с off на on: setsebool-P ftpd\_anon\_write on; Посмотрим список: semanage boolean-l | grep ftpd\_anon



```
[root@dosergeev ~]# setsebool -P ftpd_anon_write on
[root@dosergeev ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (on , on) Allow ftpd to anon write
[root@dosergeev ~]#
```

Рис. 3.19: Переключатели для службы ftp, ftpd\_anon

Теперь переключатель имеет состояние (on , on). Это значит, что теперь он включен как постоянная настройка и как настройка времени выполнения.

## 4 Ответы на контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

- `setenforce 0`

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

- `getsebool -a`

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

- `setroubleshoot`

4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?

- `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` - добавляет правило в политику
- `restorecon -R -v /web` - обновляет политику

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

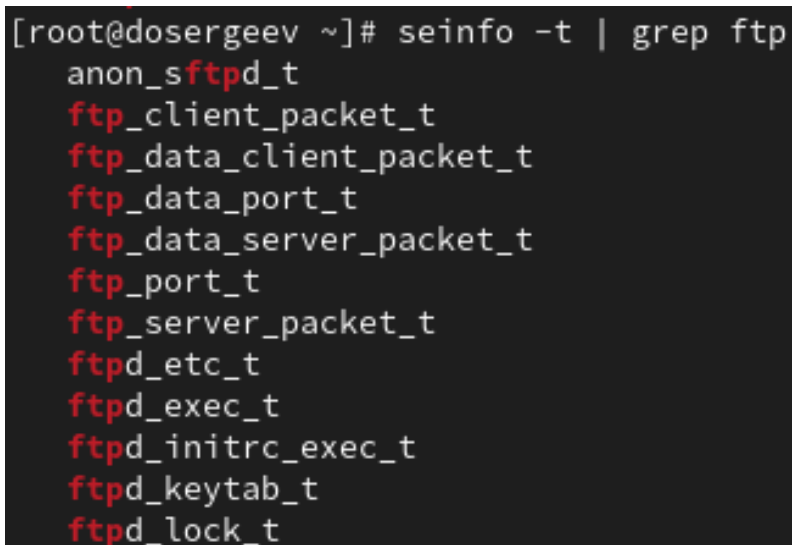
- `/etc/selinux/config` или `/etc/sysconfig/selinux`

6. Где SELinux регистрирует все свои сообщения?

- /var/log/audit/audit.log

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

- seinfo -t | grep ftp



```
[root@dosergeev ~]# seinfo -t | grep ftp
anon_ftp_t
ftp_client_packet_t
ftp_data_client_packet_t
ftp_data_port_t
ftp_data_server_packet_t
ftp_port_t
ftp_server_packet_t
ftpd_etc_t
ftpd_exec_t
ftpd_initrc_exec_t
ftpd_keytab_t
ftpd_lock_t
```

Рис. 4.1: Вывод seinfo

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?

- Можно перевести SELinux в разрешающий режим (setenforce 0). Таким образом, если проблема связана с SELinux, то сервис перестанет блокироваться политикой, возобновив свою работу. Для дальнейшего анализа можно посмотреть журналы, ведь в режиме permissive SELinux все ещё отправляет логи.

## 5 Вывод

В результате выполнения лабораторной работы я получил навыки работы с контекстом безопасности и политиками SELinux, научился настраивать контекст безопасности для нестандартного расположения файлов веб сервера и переключатели для служб на примере ftp.

## Список литературы

1. Kulyabov, Korolykova. Лабораторная работа № 9. Управление SELinux. [https://esystem.rudn.ru/pluginfile.php/2843497/mod\\_resource/content/4/010-selinux.pdf](https://esystem.rudn.ru/pluginfile.php/2843497/mod_resource/content/4/010-selinux.pdf); RUDN.