

# **Лабораторная работа №6**

**Информационная безопасность**

Леонтьева Ксения Андреевна | НПМбд-01-19

# Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	18
	Список литературы	19

## Список иллюстраций

3.1	Проверка режима enforcing политики targeted . . . . .	7
3.2	Проверка работы веб-сервера . . . . .	8
3.3	Контекст безопасности веб-сервера Apache . . . . .	8
3.4	Текущее состояние переключателей SELinux . . . . .	9
3.5	Статистика по политике . . . . .	10
3.6	Просмотр файлов и поддиректорий в директории /var/www . . .	11
3.7	Создание файла /var/www/html/test.html . . . . .	11
3.8	Обращение к файлу через веб-сервер . . . . .	12
3.9	Изменение контекста . . . . .	12
3.10	Обращение к файлу через веб-сервер . . . . .	13
3.11	Просмотр log-файла . . . . .	13
3.12	Установка веб-сервера Apache на прослушивание TCP-порта 81 . .	14
3.13	Перезапуск веб-сервера и анализ лог-файлов . . . . .	14
3.14	Содержание файла var/log/audit/audit.log . . . . .	15
3.15	Проверка установки порта 81 . . . . .	15
3.16	Возвращение исходного контекста файлу . . . . .	16
3.17	Обращение к файлу через веб-сервер . . . . .	16
3.18	Возвращение Listen 80 и попытка удалить порт 81 . . . . .	17
3.19	Удаление файла test.html . . . . .	17

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

## 2 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена.

SELinux имеет три основных режим работы:

- Enforcing: Режим по-умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- Permissive: В случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- Disabled: Полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам.

Контекст безопасности — все атрибуты SELinux — роли, типы и домены.

Более подробно см. в [1].

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA).

Для чего нужен Apache сервер:

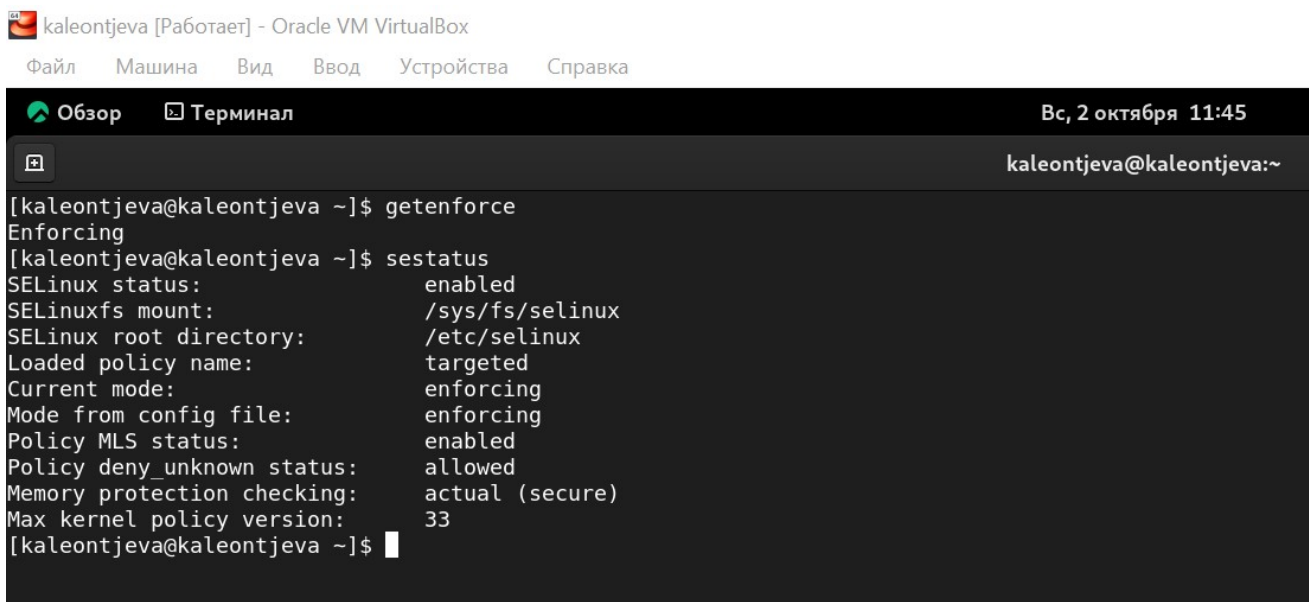
- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

Более подробно см. в [2].

### 3 Выполнение лабораторной работы

Вошла в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus” (рис. 3.1).

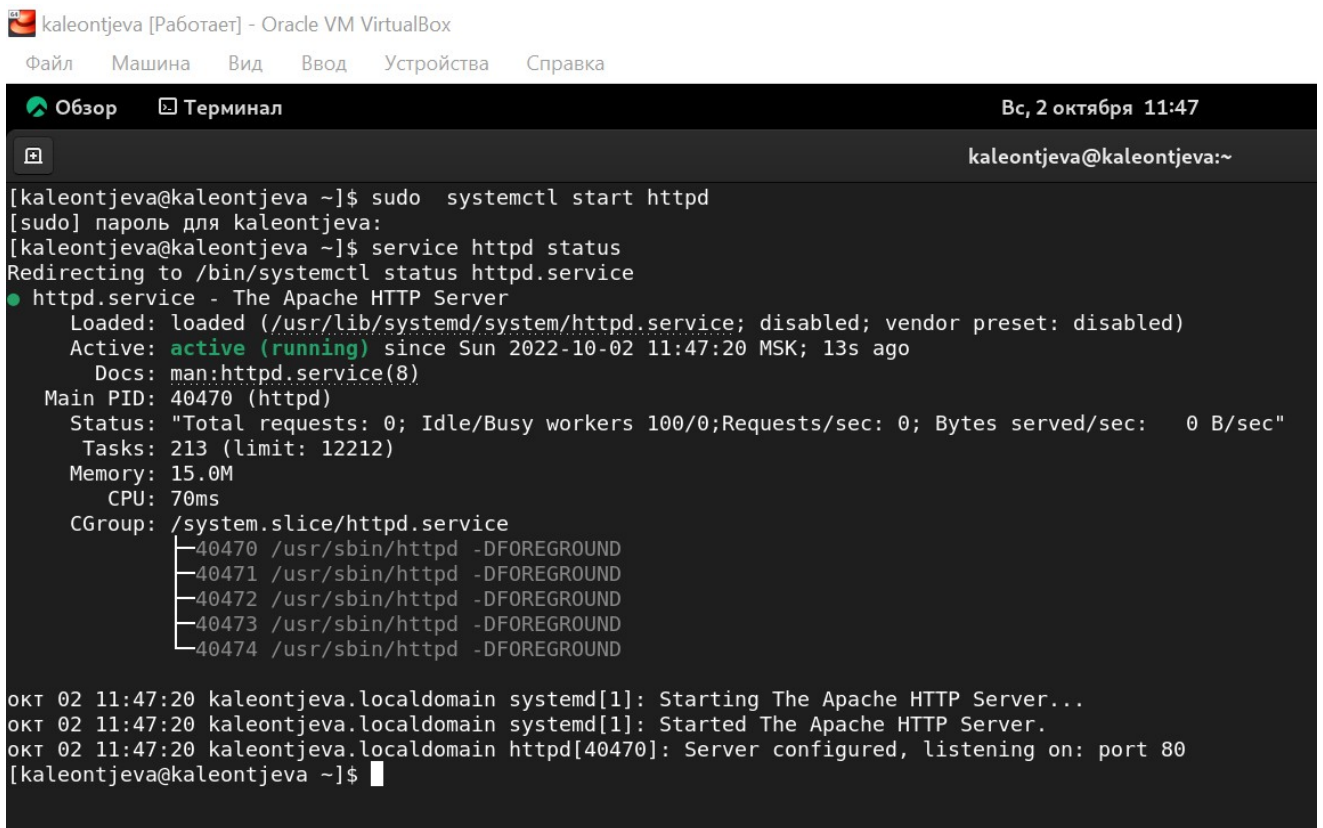


The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[kaleontjeva@kaleontjeva ~]$ getenforce
Enforcing
[kaleontjeva@kaleontjeva ~]$ sestatus
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
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.1: Проверка режима enforcing политики targeted

Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает с помощью команды “service httpd status” (рис. 3.2).



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

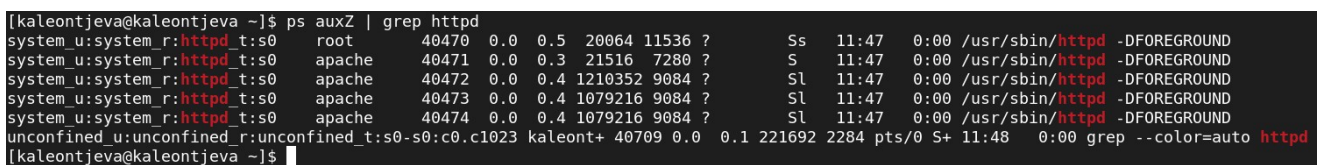
Обзор  Терминал  Вс, 2 октября 11:47
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ sudo systemctl start httpd
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2022-10-02 11:47:20 MSK; 13s ago
     Docs: man:httpd.service(8)
  Main PID: 40470 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 213 (limit: 12212)
    Memory: 15.0M
       CPU: 70ms
    CGroup: /system.slice/httpd.service
            └─40470 /usr/sbin/httpd -DFOREGROUND
              └─40471 /usr/sbin/httpd -DFOREGROUND
                └─40472 /usr/sbin/httpd -DFOREGROUND
                  └─40473 /usr/sbin/httpd -DFOREGROUND
                    └─40474 /usr/sbin/httpd -DFOREGROUND

окт 02 11:47:20 kaleontjeva.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 02 11:47:20 kaleontjeva.localdomain systemd[1]: Started The Apache HTTP Server.
окт 02 11:47:20 kaleontjeva.localdomain httpd[40470]: Server configured, listening on: port 80
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.2: Проверка работы веб-сервера

С помощью команды “ps auxZ | grep httpd” определила контекст безопасности веб-сервера Apache - httpd\_t (рис. 3.3).

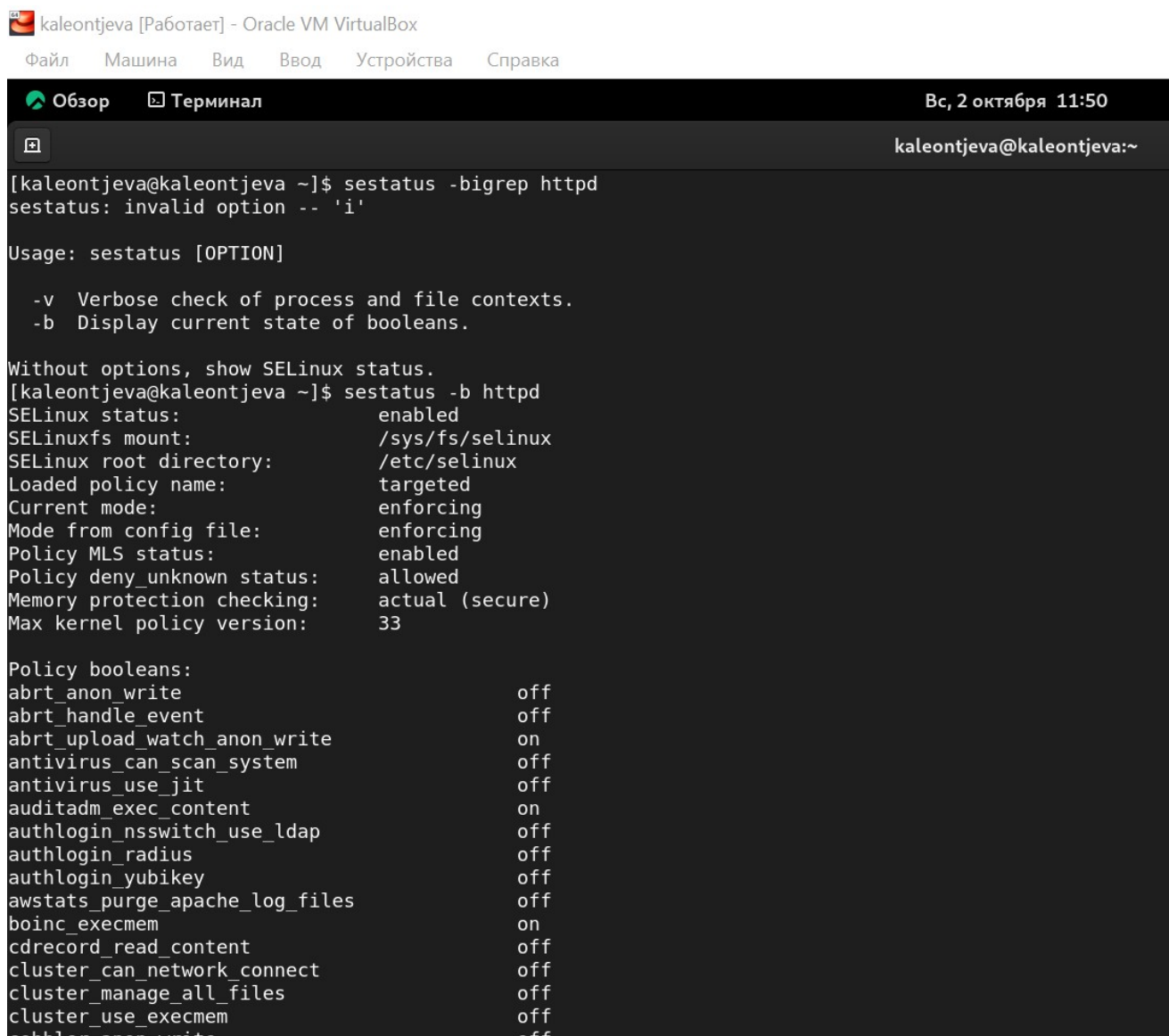


```
[kaleontjeva@kaleontjeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      40470  0.0  0.5 20064 11536 ?        Ss   11:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   40471  0.0  0.3 21516  7280 ?        S    11:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   40472  0.0  0.4 1210352 9084 ?        Sl   11:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   40473  0.0  0.4 1079216 9084 ?        Sl   11:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache   40474  0.0  0.4 1079216 9084 ?        Sl   11:47   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 kaleont+ 40709 0.0  0.1 221692 2284 pts/0 S+   11:48   0:00 grep --color=auto httpd
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.3: Контекст безопасности веб-сервера Apache

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”, многие из переключателей находятся в положении “off” (рис. 3.4).





```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 11:50
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

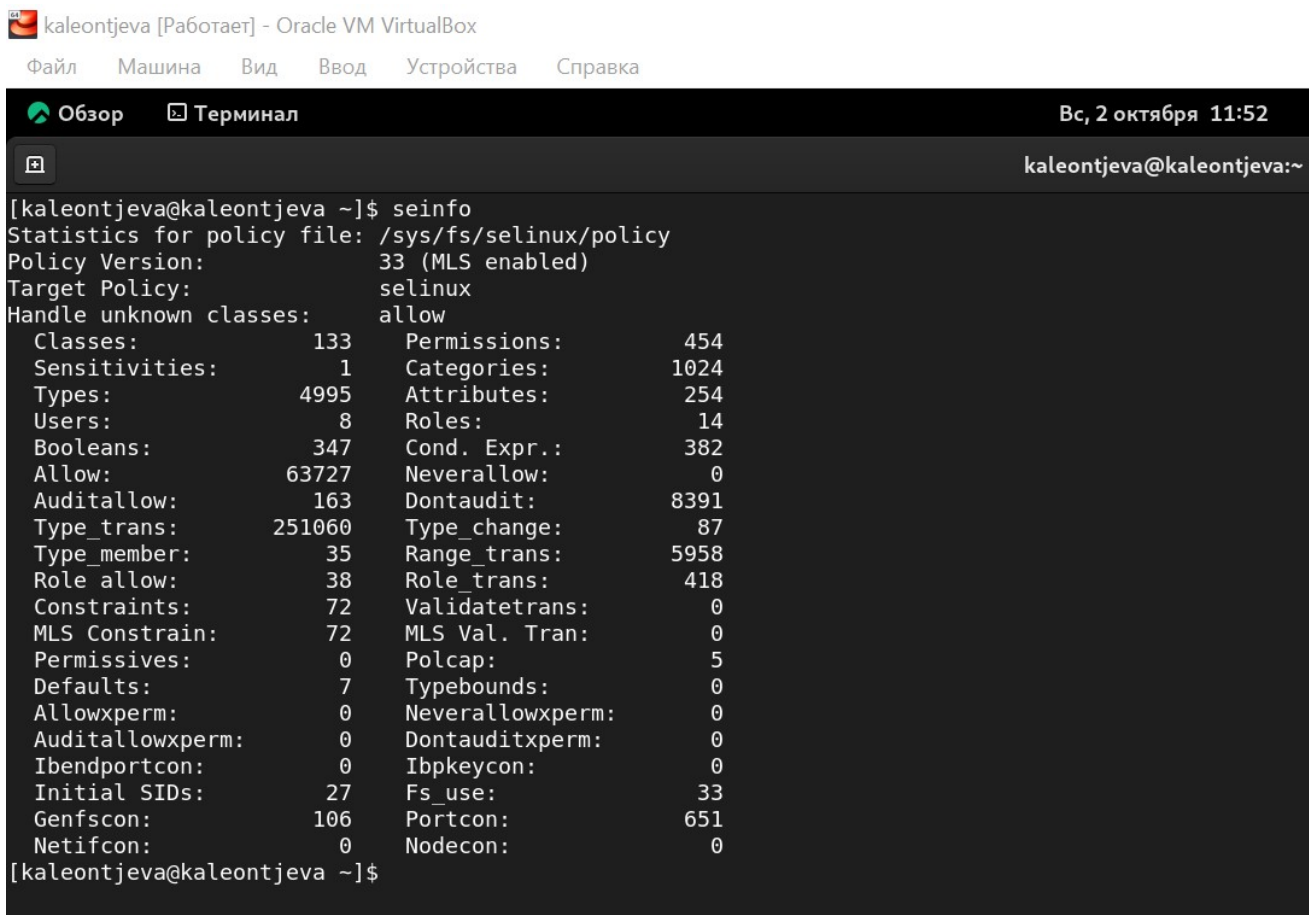
  -v  Verbose check of process and file contexts.
  -b  Display current state of booleans.

Without options, show SELinux status.
[kaleontjeva@kaleontjeva ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap    off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content          off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write             off
```

Рис. 3.4: Текущее состояние переключателей SELinux

Посмотрела статистику по политике с помощью команды “seinfo”. Множество пользователей - 8, ролей - 14, типов 4995 (рис. 3.5).



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 11:52
kaleontjeva@kaleontjeva:~

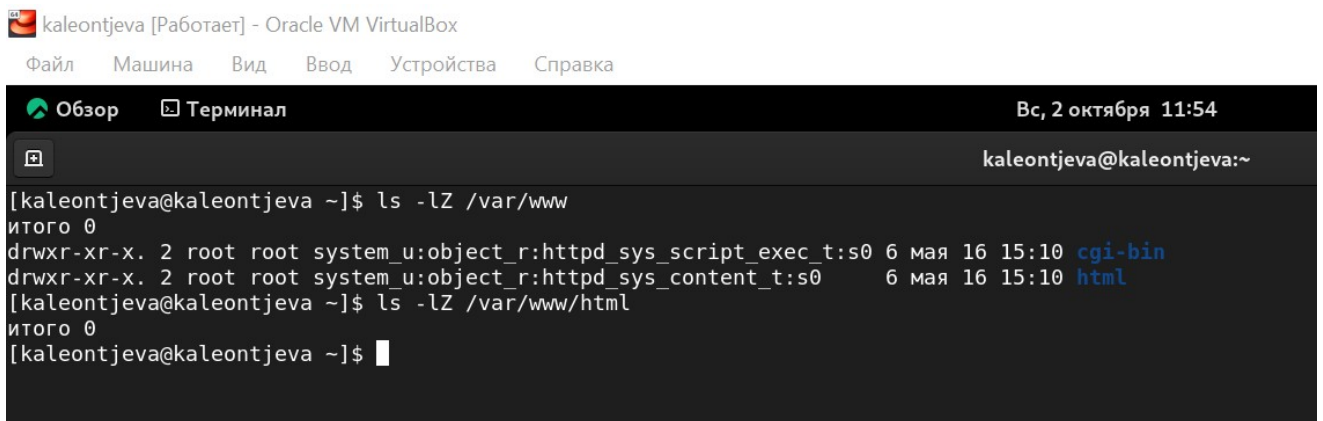
[kaleontjeva@kaleontjeva ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                133      Permissions:            454
Sensitivities:           1      Categories:            1024
Types:                   4995    Attributes:             254
Users:                   8      Roles:                  14
Booleans:                347    Cond. Expr.:           382
Allow:                   63727   Neverallow:             0
Auditallow:              163    Dontaudit:              8391
Type_trans:              251060  Type_change:            87
Type_member:              35     Range_trans:            5958
Role_allow:              38     Role_trans:             418
Constraints:              72     Validatetrans:          0
MLS Constrain:            72     MLS Val. Tran:          0
Permissives:              0      Polcap:                  5
Defaults:                 7      Typebounds:             0
Allowxperm:               0      Neverallowxperm:        0
Auditallowxperm:          0      Dontauditxperm:         0
Ibendportcon:             0      Ibpkeycon:              0
Initial SIDs:             27     Fs_use:                  33
Genfscon:                 106    Portcon:                 651
Netifcon:                 0      Nodecon:                 0

[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.5: Статистика по политике

С помощью команды “ls -lZ /var/www” посмотрела файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определила, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html (рис. 3.6).



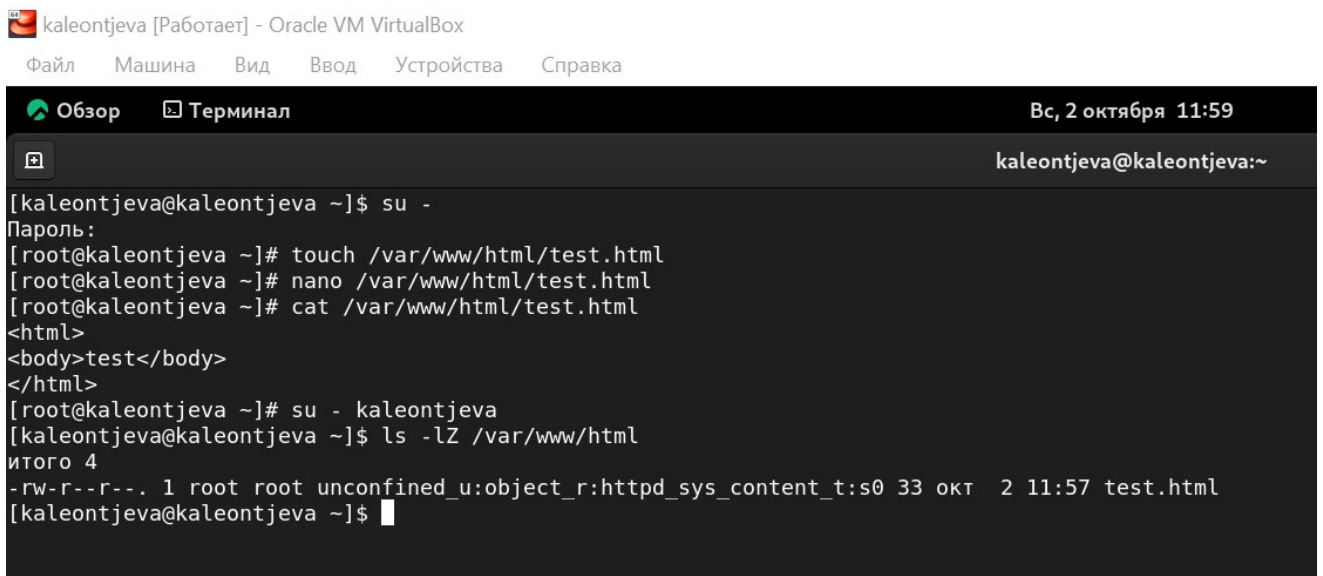
```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 11:54
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15:10 html
[kaleontjeva@kaleontjeva ~]$ ls -lZ /var/www/html
итого 0
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.6: Просмотр файлов и поддиректорий в директории /var/www

От имени суперпользователя создала html-файл /var/www/html/test.html. Кон-  
текст созданного файла - httpd\_sys\_content\_t (рис. 3.7).



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 11:59
kaleontjeva@kaleontjeva:~

[kaleontjeva@kaleontjeva ~]$ su -
Пароль:
[root@kaleontjeva ~]# touch /var/www/html/test.html
[root@kaleontjeva ~]# nano /var/www/html/test.html
[root@kaleontjeva ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@kaleontjeva ~]# su - kaleontjeva
[kaleontjeva@kaleontjeva ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 2 11:57 test.html
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.7: Создание файла /var/www/html/test.html

Обратилась к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”.  
Файл был успешно отображен (рис. 3.8).

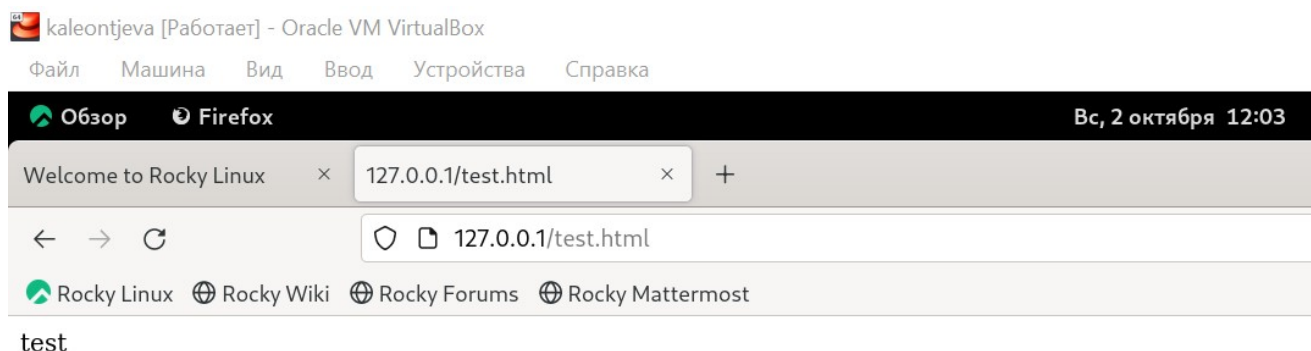


Рис. 3.8: Обращение к файлу через веб-сервер

Изучив справку `man httpd_selinux`, выяснила, что для `httpd` определены следующие контексты файлов: `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`. Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона). Изменила контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверила, что контекст поменялся (рис. 3.9).

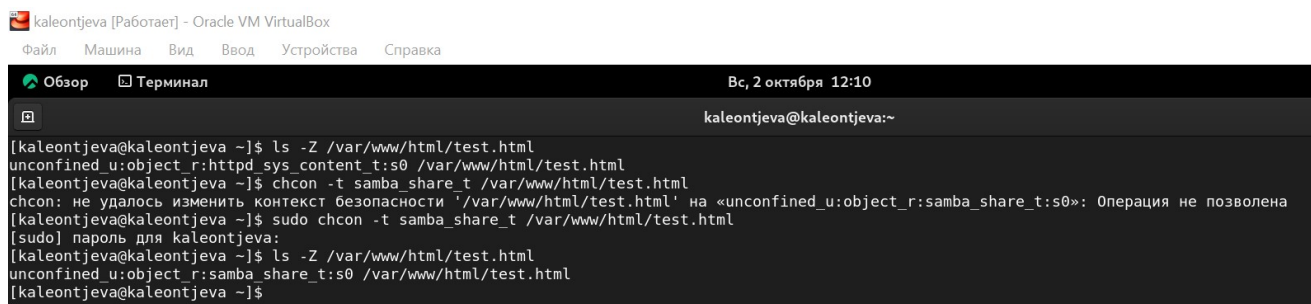


Рис. 3.9: Изменение контекста

Попробовала еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “`http://127.0.0.1/test.html`” и получила сообщение об ошибке (т.к. к установленному ранее контексту процесс `httpd` не имеет доступа) (рис. 3.10).

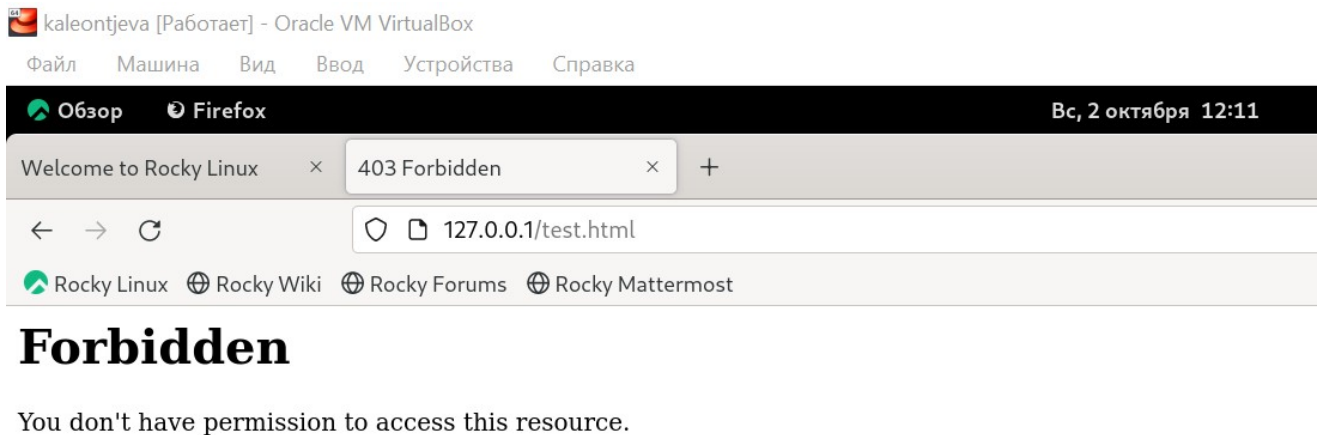


Рис. 3.10: Обращение к файлу через веб-сервер

Командой “`ls -l /var/www/html/test.html`” убедилась, что читать данный файл может любой пользователь. Просмотрела системный лог-файл веб-сервера Apache командой “`sudo tail /var/log/messages`”, отображающий ошибки (рис. 3.11).

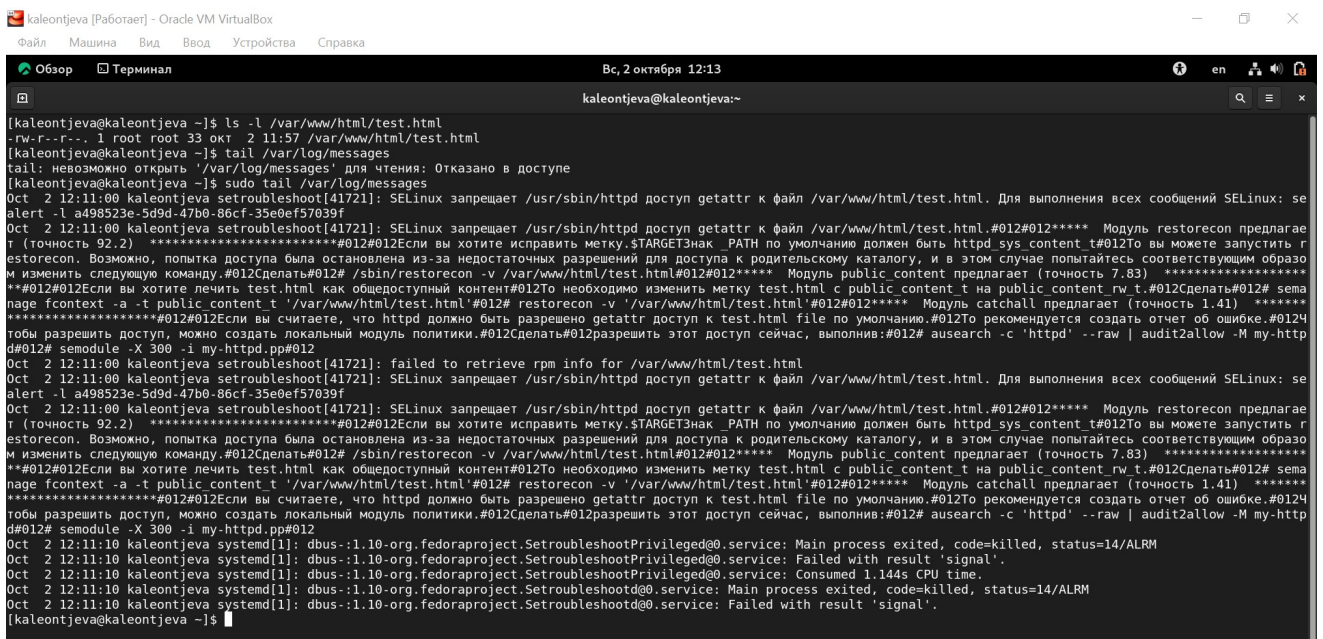
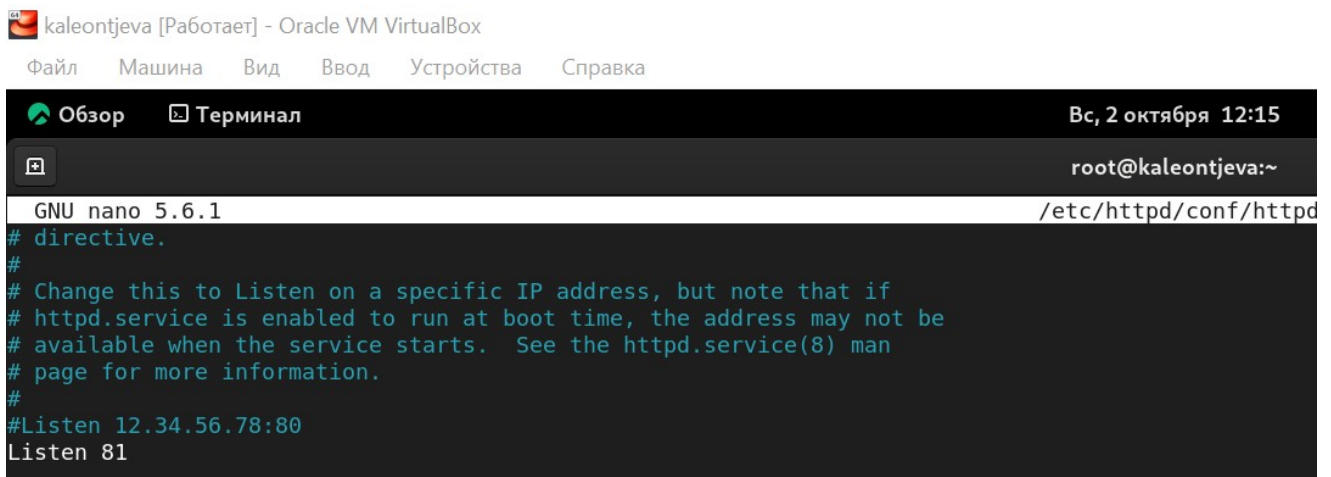


Рис. 3.11: Просмотр log-файла

В файле `/etc/httpd/conf/httpd.conf` заменила строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 3.12).

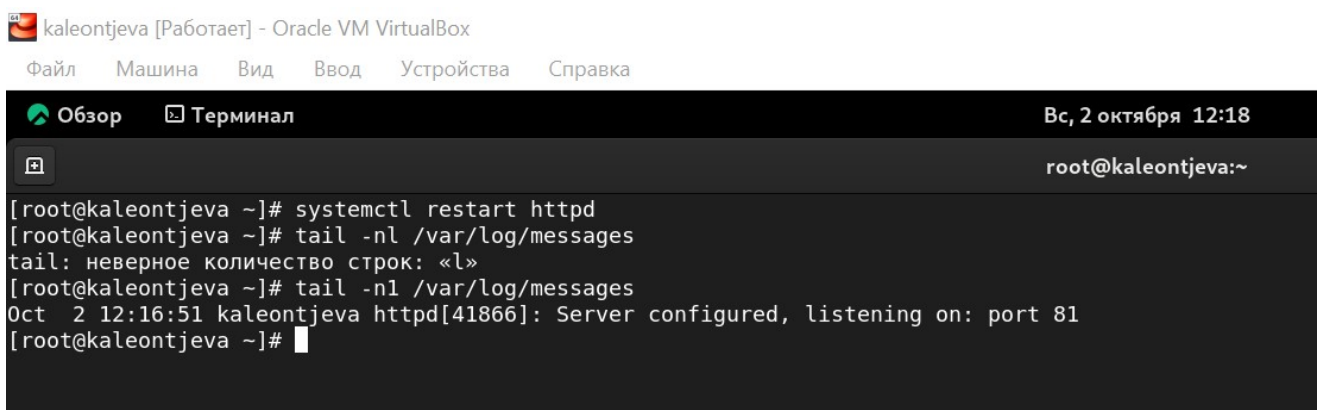


```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 12:15
root@kaleontjeva:~
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 3.12: Установка веб-сервера Apache на прослушивание TCP-порта 81

Перезапускаем веб-сервер Apache и анализирует лог-файлы командой “tail -nl /var/log/messages” (рис. 3.13).



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 12:18
root@kaleontjeva:~
[root@kaleontjeva ~]# systemctl restart httpd
[root@kaleontjeva ~]# tail -nl /var/log/messages
tail: неверное количество строк: «l»
[root@kaleontjeva ~]# tail -nl /var/log/messages
Oct  2 12:16:51 kaleontjeva httpd[41866]: Server configured, listening on: port 81
[root@kaleontjeva ~]#
```

Рис. 3.13: Перезапуск веб-сервера и анализ лог-файлов

Просмотрела файлы “var/log/http/error\_log”, “/var/log/http/access\_log” и “/var/log/audit/audit.log” и выяснила, что запись появилась в последнем файле (рис. 3.14).



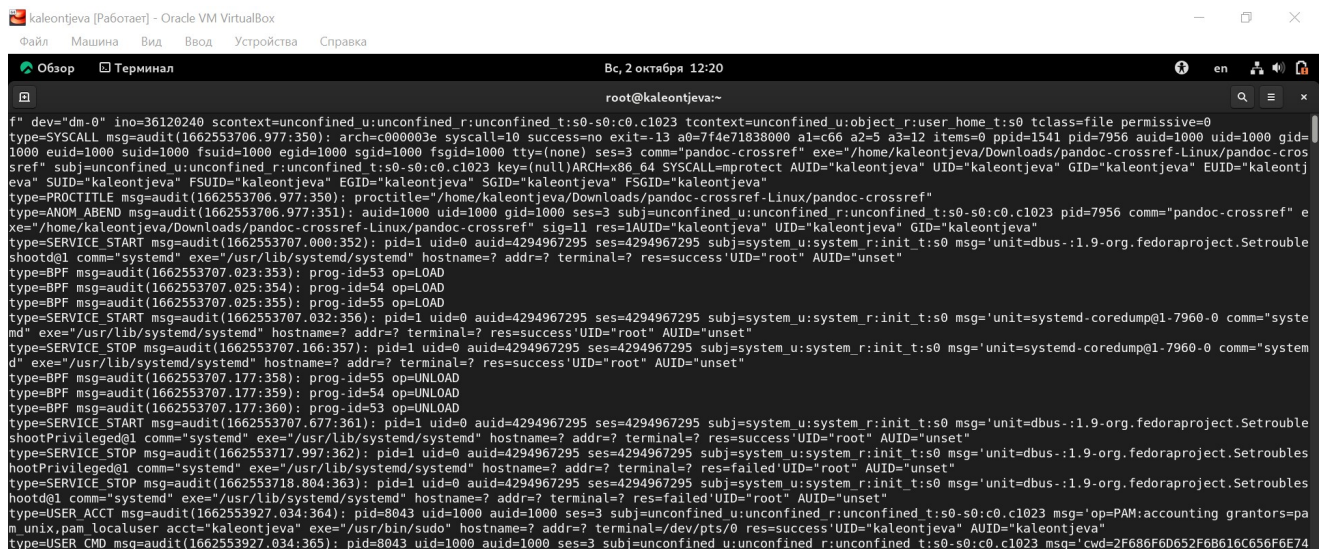


Рис. 3.14: Содержание файла var/log/audit/audit.log

Выполнила команду “semanage port -a -t http\_port\_t -p tcp 81” и убедилась, что порт TCP-81 установлен. Проверила список портов командой “semanage port -l | grep http\_port\_t”, убедилась, что порт 81 есть в списке и запускаем веб-сервер Apache снова (рис. 3.15).

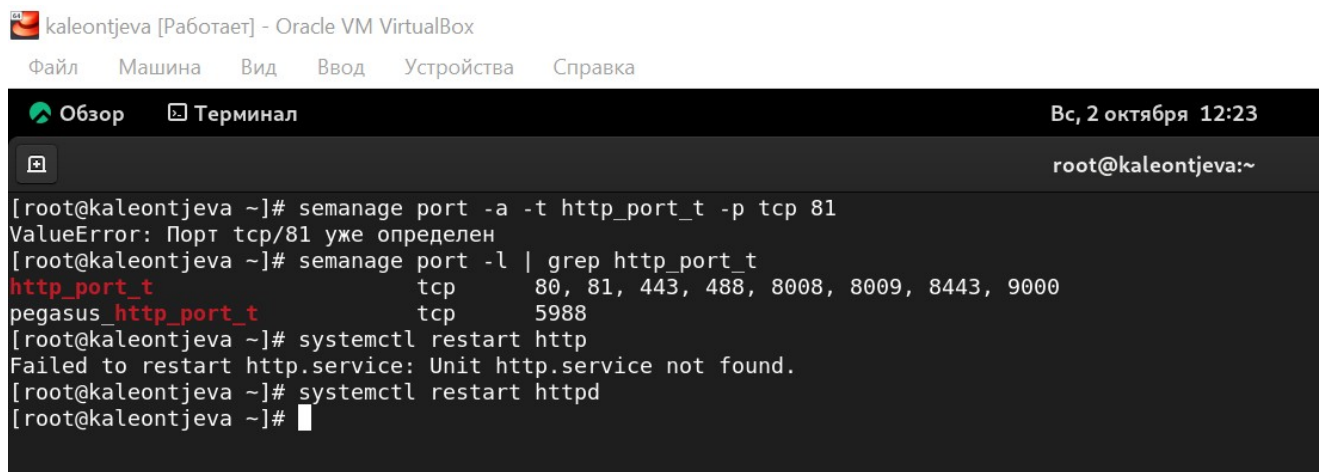
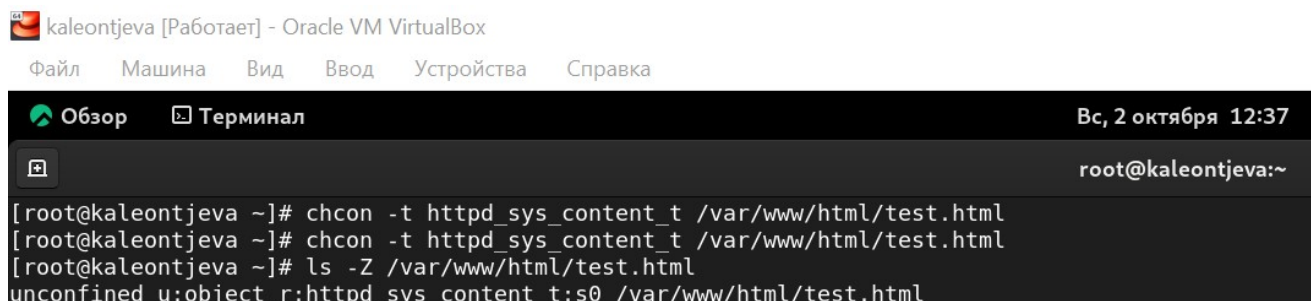


Рис. 3.15: Проверка установки порта 81

Вернула контекст “httpd\_sys\_content\_t” файлу “/var/www/html/test.html” командой “chcon -t httpd\_sys\_content\_t /var/www/html/test.html” (рис. 3.16) и после этого попробовала получить доступ к файлу через веб-сервер, введя адрес

“http://127.0.0.1:81/test.html”, в результате чего увидела содержимое файла - слово “test” (рис. 3.17).



```
kaleontjeva [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 2 октября 12:37
root@kaleontjeva:~
[root@kaleontjeva ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kaleontjeva ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kaleontjeva ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 3.16: Возвращение исходного контекста файлу

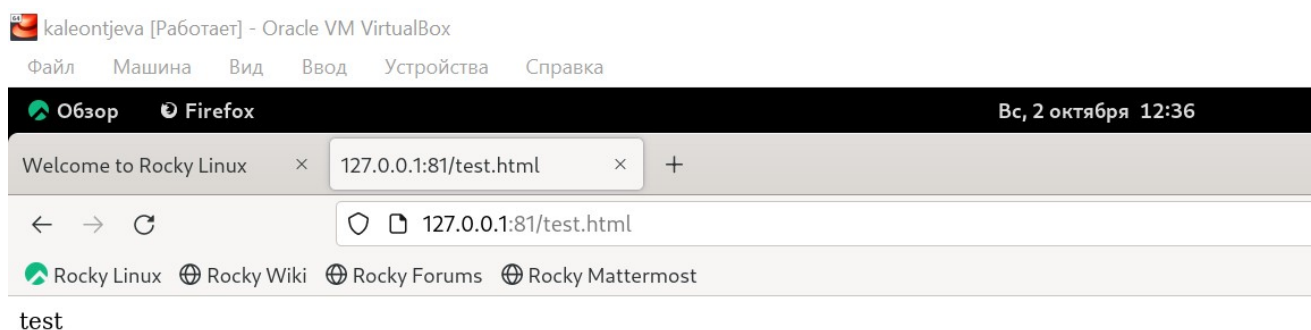


Рис. 3.17: Обращение к файлу через веб-сервер

Исправила обратно конфигурационный файл apache, вернув “Listen 80”. Попыталась удалить привязку http\_port к 81 порту командой “semanage port -d -t http\_port\_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить (рис. 3.18).



The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[root@kaleontjeva ~]# nano /etc/httpd/conf/httpd.conf
[root@kaleontjeva ~]# semanage port -d -t http_port_t -p tcp 81\
>
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@kaleontjeva ~]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@kaleontjeva ~]# cat /etc/httpd/conf/httpd.conf | grep "Listen"
# Listen: Allows you to bind Apache to specific IP addresses and/or
# Change this to Listen on a specific IP address, but note that if
#Listen 12.34.56.78:80
Listen 80
[root@kaleontjeva ~]#
```

Рис. 3.18: Возвращение Listen 80 и попытка удалить порт 81

Удалила файл “/var/www/html/test.html” командой “rm /var/www/html/test.html” (рис. 3.19).

The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[root@kaleontjeva ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@kaleontjeva ~]# ls /var/www/html
[root@kaleontjeva ~]#
```

Рис. 3.19: Удаление файла test.html

## 4 Выводы

В ходе выполнения данной лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.

## Список литературы

1. SELinux – описание и особенности работы с системой [Электронный ресурс]. URL: <https://habr.com/ru/company/kingservers/blog/209644/>.
2. Что такое Apache и зачем он нужен? [Электронный ресурс]. URL: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>.