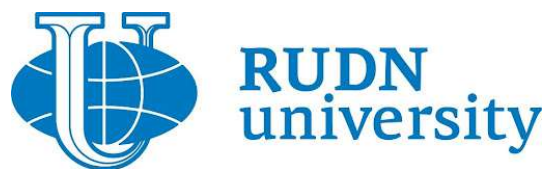


---

# Лабораторная работа №6

Мандатное разграничение прав в Linux

Доборщук В.В., НФИбд-01-18



27 ноября 2021

## **Содержание**

<b>Цель работы</b>	<b>4</b>
<b>Теоретическое введение</b>	<b>5</b>
<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>Заключение</b>	<b>14</b>

## Список иллюстраций

1	Проверка <code>sestatus</code> и Apache-сервера . . . . .	6
2	Определение сервера Apache в списке процессов . . . . .	6
3	<code>sestatus -bigrep httpd</code> . . . . .	7
4	Статистика <code>seinfo</code> . . . . .	8
5	Директории <code>/var/www/</code> . . . . .	8
6	Создание <code>test.html</code> . . . . .	9
7	Проверка в браузере по 127.0.0.1 . . . . .	9
8	Проверка контекста <code>test.html</code> . . . . .	9
9	Изменение контекста <code>test.html</code> . . . . .	10
10	Проверка измененного контекста в браузере . . . . .	10
11	Анализ log-файлов . . . . .	11
12	Изменение TCP-порта . . . . .	12
13	Успешный перезапуск Apache . . . . .	12
14	Назначение порта по <code>semanage</code> и изменение контекста . . . . .	13
15	Проверка измененного контекста в браузере (успешно) . . . . .	13
16	Возврат к основным конфигурациям . . . . .	13

## Цель работы

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

### Задачи:

- познакомиться с SELinux;
- проверить работу с SELinux с веб-сервером Apache;

## **Теоретическое введение**

Для выполнения данной лабораторной работы мы использовали данные источники, в виде описания лабораторной работы, а также свободные источники в интернете.

## Выполнение лабораторной работы

Предварительно подготовили стенд и установили сервер Apache.

```
[vdoborschuk@localhost ~]$ getenforce
Enforcing
[vdoborschuk@localhost ~]$ 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
[vdoborschuk@localhost ~]$ sudo 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 Sat 2021-11-27 23:05:10 MSK; 7min ago
     Docs: man:httpd.service(8)
  Main PID: 14884 (httpd)
    Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 11260)
   Memory: 33.0M
    CGroup: /system.slice/httpd.service
            └─14884 /usr/sbin/httpd -DFOREGROUND
              └─15060 /usr/sbin/httpd -DFOREGROUND
                └─15061 /usr/sbin/httpd -DFOREGROUND
                  └─15062 /usr/sbin/httpd -DFOREGROUND
                    └─15063 /usr/sbin/httpd -DFOREGROUND

ноя 27 23:05:10 localhost.vdoborschuk systemd[1]: Starting The Apache HTTP Server...
ноя 27 23:05:10 localhost.vdoborschuk systemd[1]: Started The Apache HTTP Server.
ноя 27 23:05:10 localhost.vdoborschuk httpd[14884]: Server configured, listening on: port 80
[vdoborschuk@localhost ~]$
```

Рис. 1: Проверка sestatus и Apache-сервера

```
[vdoborschuk@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 14884 0.0 0.6 282928 11960 ? Ss 23:05 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 15060 0.0 0.4 296812 8668 ? S 23:05 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 15061 0.0 0.8 1354600 16500 ? Sl 23:05 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 15062 0.0 0.7 1485728 14460 ? Sl 23:05 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 15063 0.0 0.8 1354600 16500 ? Sl 23:05 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vdobors+ 33314 0.0 0.0 12136 1132 pts/0 S+ 23:13 0:00 grep --color=auto httpd
[vdoborschuk@localhost ~]$
```

Рис. 2: Определение сервера Apache в списке процессов

Не удалось определить текущее состояние переключателей SELinux, т.к. не под-  
держивается -bigrep аргумент.

```
[vdoborschuk@localhost ~]$ 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.
[vdoborschuk@localhost ~]$ sestatus --bigrep httpd
sestatus: invalid option -- '-'

Usage: sestatus [OPTION]

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

Without options, show SELinux status.
[vdoborschuk@localhost ~]$ sestatus --help
sestatus: invalid option -- '-'

Usage: sestatus [OPTION]

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

Without options, show SELinux status.
[vdoborschuk@localhost ~]$
```

**Рис. 3:** sestatus -bigrep httpd

```
[vdoborschuk@localhost ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      132      Permissions:      464
Sensitivities: 1      Categories:      1024
Types:        4961     Attributes:       255
Users:        8        Roles:           14
Booleans:     338      Cond. Expr.:     386
Allow:        112594   Neverallow:      0
Auditallow:   166      Dontaudit:       10358
Type_trans:   252747   Type_change:     87
Type_member:  35       Range_trans:     5781
Role_allow:   38       Role_trans:      421
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:          34
Genfscon:     107      Portcon:         642
Netifcon:     0        Nodecon:         0

[vdoborschuk@localhost ~]$
```

**Рис. 4:** Статистика seinfo

Определили тип файлов директорий /var/www/...

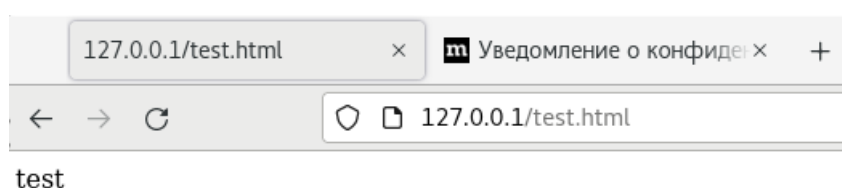
```
[vdoborschuk@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 ноя 12 07:58 html
[vdoborschuk@localhost ~]$ ls -lZ /var/www/html
итого 0
[vdoborschuk@localhost ~]$
```

**Рис. 5:** Директории /var/www/



```
[vdoborschuk@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58 html
[vdoborschuk@localhost ~]$ ls -lZ /var/www/html
итого 0
[vdoborschuk@localhost ~]$ sudo vi /var/www/html/test.html
[vdoborschuk@localhost ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 23:16 test.html
[vdoborschuk@localhost ~]$
```

**Рис. 6:** Создание test.html



**Рис. 7:** Проверка в браузере по 127.0.0.1

Далее не удалось изучить справку, т.к. man по предложенной инструкции не существует.

```
[vdoborschuk@localhost ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
[vdoborschuk@localhost ~]$ ls -Z /var/www/html/test
ls: невозможно получить доступ к '/var/www/html/test': Нет такого файла или каталога
[vdoborschuk@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

**Рис. 8:** Проверка контекста test.html

```
[vdoborschuk@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[vdoborschuk@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

**Рис. 9:** Изменение контекста test.html



**Рис. 10:** Проверка измененного контекста в браузере

Далее, проанализировали log-файлы, убедившись, что при таком контексте мы не сможем получить информацию из test.html через браузер.

```
[vdoborschuk@localhost ~]$ ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 ноя 27 23:16 /var/www/html/test.html
[vdoborschuk@localhost ~]$ tail -n 10 /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[vdoborschuk@localhost ~]$ sudo tail -n 10 /var/log/messages
Nov 27 23:21:37 localhost org.gnome.Shell.desktop[2134]: Window manager warning: last_user_time (1659220) is gr
eater than comparison timestamp (1659190). This most likely represents a buggy client sending inaccurate times
tamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Nov 27 23:21:37 localhost org.gnome.Shell.desktop[2134]: Window manager warning: W2 appears to be one of the of
fending windows with a timestamp of 1659220. Working around...
Nov 27 23:21:37 localhost org.gnome.Shell.desktop[2134]: Window manager warning: last_user_time (1659314) is gr
eater than comparison timestamp (1659275). This most likely represents a buggy client sending inaccurate times
tamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Nov 27 23:21:37 localhost org.gnome.Shell.desktop[2134]: Window manager warning: W2 appears to be one of the of
fending windows with a timestamp of 1659314. Working around...
Nov 27 23:21:37 localhost org.gnome.Shell.desktop[2134]: Window manager warning: last_user_time (1659350) is gr
eater than comparison timestamp (1659314). This most likely represents a buggy client sending inaccurate times
tamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Nov 27 23:21:37 localhost org.gnome.Shell.desktop[2134]: Window manager warning: W2 appears to be one of the of
fending windows with a timestamp of 1659350. Working around...
Nov 27 23:22:03 localhost org.gnome.Shell.desktop[2134]: Window manager warning: last_user_time (1685571) is gr
eater than comparison timestamp (1685476). This most likely represents a buggy client sending inaccurate times
tamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Nov 27 23:22:03 localhost org.gnome.Shell.desktop[2134]: Window manager warning: W2 appears to be one of the of
fending windows with a timestamp of 1685571. Working around...
Nov 27 23:22:12 localhost org.gnome.Shell.desktop[2134]: Window manager warning: last_user_time (1694407) is gr
eater than comparison timestamp (1694372). This most likely represents a buggy client sending inaccurate times
tamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Nov 27 23:22:12 localhost org.gnome.Shell.desktop[2134]: Window manager warning: W2 appears to be one of the of
fending windows with a timestamp of 1694407. Working around...
[vdoborschuk@localhost ~]$ sudo tail -n 5 /var/log/audit/audit.log
type=CRED_DISP msg=audit(1638044533.655:330): pid=37578 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" host
name=? addr=? terminal=/dev/pts/0 res=success' [UID="root" AUID="vdoborschuk"
type=USER_ACCT msg=audit(1638044545.175:331): pid=38085 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r
:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="vdoborschuk" exe="/us
r/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success' [UID="vdoborschuk" AUID="vdoborschuk"
type=USER_CMD msg=audit(1638044545.175:332): pid=38085 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:
unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/vdoborschuk" cmd=7461696C202D6E2035202F7661722F6C6F672F61756469742F
61756469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success' [UID="vdoborschuk" AUID="vdoborschuk"
type=CRED_REFR msg=audit(1638044545.175:333): pid=38085 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" host
name=? addr=? terminal=/dev/pts/0 res=success' [UID="root" AUID="vdoborschuk"
type=USER_START msg=audit(1638044545.181:334): pid=38085 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023 msg='op=PAM:session open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="
root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success' [UID="root" AUID="vdoborschuk"
[vdoborschuk@localhost ~]$
```

Рис. 11: Анализ log-файлов

```
# same ServerRoot for multiple httpd
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to
# ports, instead of the default. See
# directive.
#
# Change this to Listen on specific IP
# prevent Apache from glomming onto a
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support
```

Рис. 12: Изменение TCP-порта

```
[vdoborschuk@localhost ~]$ sudo vim /etc/httpd/conf/httpd.conf
[vdoborschuk@localhost ~]$ sudo vim /etc/httpd/conf/httpd.conf
[vdoborschuk@localhost ~]$ sudo systemctl restart httpd
[vdoborschuk@localhost ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 23:24:21 MSK; 9s ago
     Docs: man:httpd.service(8)
  Main PID: 38717 (httpd)
    Status: "Started, listening on: port 81"
    Tasks: 213 (limit: 11260)
   Memory: 24.9M
    CGroup: /system.slice/httpd.service
            └─38717 /usr/sbin/httpd -DFOREGROUND
              └─38718 /usr/sbin/httpd -DFOREGROUND
                └─38722 /usr/sbin/httpd -DFOREGROUND
                  └─38723 /usr/sbin/httpd -DFOREGROUND
                    └─38724 /usr/sbin/httpd -DFOREGROUND

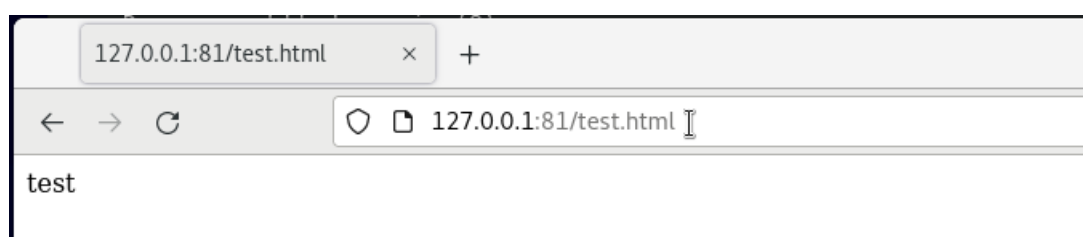
ноя 27 23:24:20 localhost.vdoborschuk systemd[1]: Starting The Apache HTTP Server...
ноя 27 23:24:21 localhost.vdoborschuk systemd[1]: Started The Apache HTTP Server.
ноя 27 23:24:21 localhost.vdoborschuk httpd[38717]: Server configured, listening on: port 81
[vdoborschuk@localhost ~]$
```

Рис. 13: Успешный перезапуск Apache

Нам не потребовалось проверять лог-файлы, все прошло успешно.

```
[vdoborschuk@localhost ~]$ semanage port -a -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[vdoborschuk@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[vdoborschuk@localhost ~]$ sudo 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
[vdoborschuk@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

**Рис. 14:** Назначение порта по semanage и изменение контекста



**Рис. 15:** Проверка измененного контекста в браузере (успешно)

```
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[vdoborschuk@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[vdoborschuk@localhost ~]$ sudo vi /etc/httpd/conf/httpd.conf
[vdoborschuk@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[vdoborschuk@localhost ~]$ sudo rm /var/www/html/test.html
[vdoborschuk@localhost ~]$
```

**Рис. 16:** Возврат к основным конфигурациям

## **Заключение**

В результате выполнения работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.