

# **Отчет по лабораторной работе №6**

**Мандатное разграничение прав в Linux**

Александр Олегович Воробьев

# Содержание

1	Цель работы	3
2	Последовательность выполнения работы	4
3	Выводы	14

# 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 Последовательность выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

```
[root@aovorobjev conf]# getenforce
Enforcing
[root@aovorobjev conf]# 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
[root@aovorobjev conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pre
   Active: active (running) since Sat 2022-10-15 10:24:35 MSK; 8min ago
     Docs: man:httpd.service(8)
   Main PID: 3379 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
   Tasks: 213 (limit: 21748)
   Memory: 32.9M
     CPU: 924ms
   CGroup: /system.slice/httpd.service
           └─3379 /usr/sbin/httpd -DFOREGROUND
             └─3387 /usr/sbin/httpd -DFOREGROUND
               └─3388 /usr/sbin/httpd -DFOREGROUND
                 └─3389 /usr/sbin/httpd -DFOREGROUND
                   └─3390 /usr/sbin/httpd -DFOREGROUND

окт 15 10:23:54 aovorobjev systemd[1]: Starting The Apache HTTP Server...
окт 15 10:24:14 aovorobjev httpd[3379]: AH00558: httpd: Could not reliably dete
окт 15 10:24:35 aovorobjev httpd[3379]: Server configured, listening on: port 80
окт 15 10:24:35 aovorobjev systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)...skipping...
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pre
   Active: active (running) since Sat 2022-10-15 10:24:35 MSK; 8min ago
```

Figure 2.1: Выполнение команд

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем

компьютере, и убедитесь, что последний работает:

```
service httpd status
```

или

```
/etc/rc.d/init.d/httpd status
```

Если не работает, запустите его так же, но с параметром start.

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду

```
ps auxZ | grep httpd
```

или

```
ps -eZ | grep httpd
```

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`

Обратите внимание, что многие из них находятся в положении «off».

```
[root@aovorobjev conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      3379  0.0  0.2  29452 10296 ?
Ss   10:23   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  3387  0.0  0.2  30948  8800 ?
S    10:24   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  3388  0.0  0.4  2535464 16176 ?
Sl   10:24   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  3389  0.0  0.5  2272296 18216 ?
Sl   10:24   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  3390  0.0  0.3  2337832 14136 ?
Sl   10:24   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3838 0.0 0.0 221396
2068 pts/0 S+ 10:37   0:00 grep --color=auto httpd
[root@aovorobjev conf]# 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.
```

Figure 2.2: поиск веб-сервера в списке процессов

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```
[root@aovorobjev conf]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 133
Sensitivities:           1
Types:                   5002
Users:                   8
Booleans:                347
Allow:                   63996
Auditallow:              168
Type_trans:              258486
Type_member:             35
Role_allow:              38
Constraints:             72
MLS Constrains:          72
Permissives:             0
Defaults:                7
Allowxperm:              0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:            27
Genfscon:                106
Netifcon:                0
Permissions:             454
Categories:              1024
Attributes:              254
Roles:                   14
Cond. Expr.:             381
Neverallow:              0
Dontaudit:               8417
Type_change:             87
Range_trans:             5960
Role_trans:              420
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  5
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  33
Portcon:                 651
Nodecon:                 0
```

Figure 2.3: Статистика

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды  
ls -lZ /var/www
7. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html
8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

test

```
[root@aovorobjev conf]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 13 15
:56 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 13 15
:56 html
[root@aovorobjev conf]# ls -lZ /var/www/html
итого 0
[root@aovorobjev conf]# touch /var/www/html/test.html
[root@aovorobjev conf]# vim /var/www/html/test.html
```

Figure 2.4: Выполнение команд



```
alexander@aovorobjev:/etc/httpd/conf — vim /var/www/html/test.html
<html>
  <body>test</body>
</html>
```

Figure 2.5: Текст файла

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён.

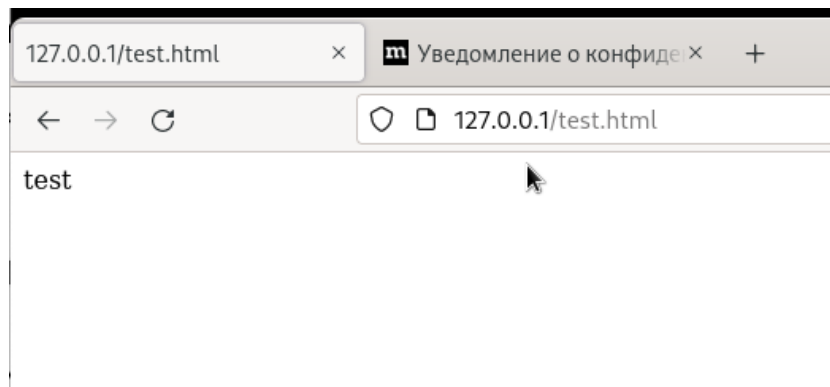


Figure 2.6: Отображение файла

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить

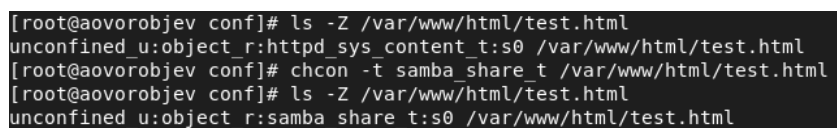
контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`). Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

13. Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`:

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```



```
[root@aovorobjev conf]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@aovorobjev conf]# chcon -t samba_share_t /var/www/html/test.html
[root@aovorobjev conf]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 2.7: Проверка и изменение контекста

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`



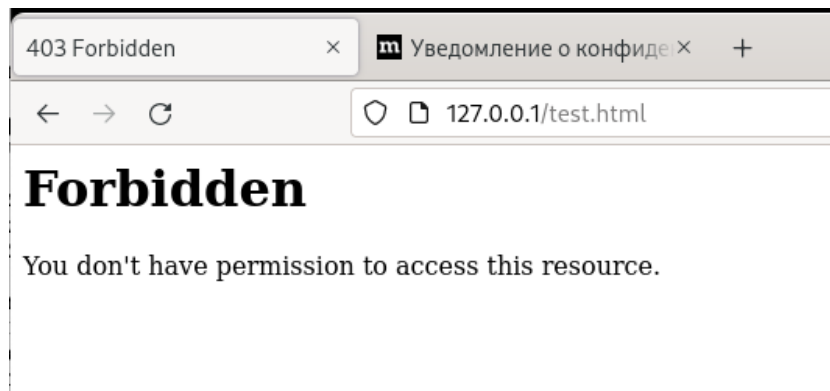


Figure 2.8: Попытка получить доступ к файлу

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

```
[root@aovorobjev conf]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 окт 15 10:44 /var/www/html/test.html
[root@aovorobjev conf]# tail /var/log/messages
Oct 15 10:48:21 aovorobjev systemd[1]: Started dbus-1.10-org.fedoraproject.Setr
oubleshootPrivileged@0.service.
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/htt
pd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений
SELinux: sealert -l 8a9d60c0-903d-4e6b-ade9-9e5338620f55
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/htt
pd доступ getattr к файл /var/www/html/test.html.#012#012**** Модуль restoreco
n предлагает (точность 92.2) *****#012#012Если вы хотите ис
править метку.$TARGETзнак PATH по умолчанию должен быть httpd_sys_content_t#012
То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-
за недостаточных разрешений для доступа к родительскому каталогу, и в этом случ
ае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#01
2# /sbin/restorecon -v /var/www/html/test.html#012#012**** Модуль public_conten
t предлагает (точность 7.83) *****#012#012Если вы хотите лечит
ь test.html как общедоступный контент#012То необходимо изменить метку test.html
с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a
-t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/
test.html'#012#012**** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getatt
r доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об оши
бке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сдел
ать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: failed to retrieve rpm info for
/var/www/html/test.html
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/htt
pd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений
SELinux: sealert -l 8a9d60c0-903d-4e6b-ade9-9e5338620f55
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/htt
pd доступ getattr к файл /var/www/html/test.html.#012#012**** Модуль restoreco
n предлагает (точность 92.2) *****#012#012Если вы хотите ис
править метку.$TARGETзнак PATH по умолчанию должен быть httpd_sys_content_t#012
То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-
за недостаточных разрешений для доступа к родительскому каталогу, и в этом случ
ае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#01
```

Figure 2.9: Проверка log-файлов

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

```
#
#Listen 12.34.56.78:80
Listen 81
```

Figure 2.10: Изменение порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

```
[root@aovorobjev conf]# vim httpd.conf
[root@aovorobjev conf]# systemctl restart httpd
```

Figure 2.11: Перезапуск веб-сервера

## 18. Проанализируйте лог-файлы:

```
tail -nl /var/log/messages
```

Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи.

```
[root@aovorobjev conf]# tail /var/log/messages
Oct 15 10:48:21 aovorobjev systemd[1]: Started dbus-1.10-org.fedoraproject.Setr
oubleshootPrivileged@.service.
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений.
SELinux: sealert -l 8a9d60c0-903d-4e6b-ade9-9e5338620f55
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файл /var/www/html/test.html.#012#012**** Модуль restoreco
n предлагает (точность 92.2) *****#012#012Если вы хотите ис
править метку.$TARGETзнак PATH по умолчанию должен быть httpd_sys_content_t#012
То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-
за недостаточных разрешений для доступа к родительскому каталогу, и в этом случ
ае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#01
2# /sbin/restorecon -v /var/www/html/test.html#012#012**** Модуль public Conte
nt предлагает (точность 7.83) *****#012#012Если вы хотите лечит
ь test.html как общедоступный контент#012То необходимо изменить метку test.html
с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a
-t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/
test.html'#012#012**** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr
г доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об оши
бке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сдел
ать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: failed to retrieve rpm info for
/var/www/html/test.html
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений.
SELinux: sealert -l 8a9d60c0-903d-4e6b-ade9-9e5338620f55
Oct 15 10:48:22 aovorobjev setroubleshoot[4902]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файл /var/www/html/test.html.#012#012**** Модуль restoreco
n предлагает (точность 92.2) *****#012#012Если вы хотите ис
править метку.$TARGETзнак PATH по умолчанию должен быть httpd_sys_content_t#012
То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-
за недостаточных разрешений для доступа к родительскому каталогу, и в этом случ
```

Figure 2.12: Проверка log-файлов

## 19. Выполните команду semanage port -a -t http\_port\_t -p tcp 81 После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке.

```
[root@aovorobjev conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@aovorobjev conf]# 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
```

Figure 2.13: Выполнение команд

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?
21. Верните контекст `httpd_sys_content_t` файлу `/var/www/html/test.html`:  
`chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».

```
[root@aovorobjev conf]# systemctl restart httpd
[root@aovorobjev conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Figure 2.14: Перезапуск веб-сервера

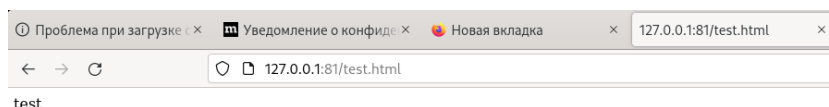


Figure 2.15: Проверка отображения файла

22. Исправьте обратную конфигурационный файл `apache`, вернув `Listen 80`.

```
#Listen 12.34.56.78:80
Listen 80
```

Figure 2.16: Изменение порта

23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

```
[root@aovorobjev conf]# vim httpd.conf
[root@aovorobjev conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@aovorobjev conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'?
[root@aovorobjev conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@aovorobjev conf]# ls /var/www/html
```

Figure 2.17: Удаление привязки и файла

## 3 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinux на практике совместно с веб-сервером Apache.