

Лабораторная работа № 6

Мандатное разграничение прав в Linux

выполнил: Лебедев Ярослав Борисович

группа: НФИбд-02-19

РУДН, Москва

Цель и задачи выполнения лабораторной работы:

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

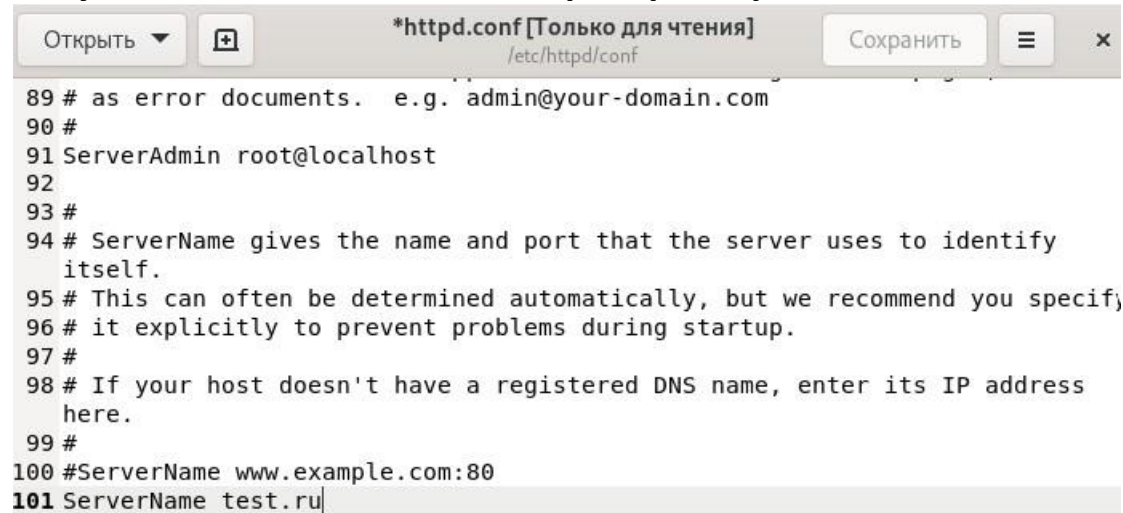
Результаты выполнения лабораторной работы

```
[yblebedev@yblebedev ~]$ sudo dnf install httpd -y
[sudo] пароль для yblebedev:
Rocky Linux 9 - BaseOS                4.0 kB/s | 3.6 kB      00:00
Rocky Linux 9 - BaseOS                1.0 MB/s | 1.7 MB      00:01
Rocky Linux 9 - AppStream             4.8 kB/s | 3.6 kB      00:00
Rocky Linux 9 - AppStream             2.0 MB/s | 6.0 MB      00:02
Rocky Linux 9 - Extras                3.0 kB/s | 2.9 kB      00:00
Зависимости разрешены.
=====
Пакет                Архитектура Версия                Репозиторий    Размер
=====
Установка:
  httpd              x86_64      2.4.51-7.el9_0      appstream      1.4 М
Установка зависимостей:
  apr                x86_64      1.7.0-11.el9        appstream      123 к
  apr-util           x86_64      1.6.1-20.el9        appstream      94 к
  apr-util-bdb       x86_64      1.6.1-20.el9        appstream      13 к
  httpd-filesystem   noarch      2.4.51-7.el9_0      appstream      14 к
  httpd-tools        x86_64      2.4.51-7.el9_0      appstream      81 к
  rocky-logos-httpd  noarch      90.11-1.el9         appstream      24 к
Установка слабых зависимостей:
  apr-util-openssl   x86_64      1.6.1-20.el9        appstream      15 к
  mod_http2          x86_64      1.15.19-2.el9       appstream      149 к
  mod_lua            x86_64      2.4.51-7.el9_0      appstream      61 к

Результат транзакции
=====
Установка 10 Пакетов
```

Рис.1. Подготовка. Пункт 3

Результаты выполнения лабораторной работы



```
89 # as error documents.  e.g. admin@your-domain.com
90 #
91 ServerAdmin root@localhost
92
93 #
94 # ServerName gives the name and port that the server uses to identify
   itself.
95 # This can often be determined automatically, but we recommend you specif;
96 # it explicitly to prevent problems during startup.
97 #
98 # If your host doesn't have a registered DNS name, enter its IP address
   here.
99 #
100 #ServerName www.example.com:80
101 ServerName test.ru
```

Рис.2. Подготовка. Пункт 4

Результаты выполнения лабораторной работы

```
[yblebedev@yblebedev ~]$ getenforce
Enforcing
[yblebedev@yblebedev ~]$ 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
[yblebedev@yblebedev ~]$ 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 preset: disabled)
   Active: active (running) since Tue 2022-10-11 18:50:11 MSK; 15min ago
     Docs: man:httpd.service(8)
  Main PID: 21121 (httpd)
    Status: "Total requests: 4; Idle/Busy workers 100/0;Requests/sec: 0.00426; Bytes served/s>
    Tasks: 213 (limit: 12210)
   Memory: 23.2M
      CPU: 458ms
    CGroup: /system.slice/httpd.service
            └─21121 /usr/sbin/httpd -DFOREGROUND
              └─21743 /usr/sbin/httpd -DFOREGROUND
                └─21744 /usr/sbin/httpd -DFOREGROUND
                  └─21745 /usr/sbin/httpd -DFOREGROUND
                    └─21749 /usr/sbin/httpd -DFOREGROUND

окт 11 18:50:11 yblebedev.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 11 18:50:11 yblebedev.localdomain systemd[1]: Started The Apache HTTP Server.
окт 11 18:50:11 yblebedev.localdomain httpd[21121]: Server configured, listening on: port 80
[yblebedev@yblebedev ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0    21121 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21743 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21744 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21745 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21749 ?        00:00:00 httpd
```

Рис.3. Пункт 1-3

Результаты выполнения лабораторной работы

```
[yblebedev@yblebedev ~]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_opencryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
```

Рис.4. Пункт 4

Результаты выполнения лабораторной работы

```
[yblebedev@yblebedev ~]$ 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

[yblebedev@yblebedev ~]$ 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
[yblebedev@yblebedev ~]$ ls -lZ /var/www/html
итого 0
[yblebedev@yblebedev ~]$ su
Пароль:
[root@yblebedev yblebedev]# echo "<html>
<body>test</body>
</html>" > /var/www/html/test.html
[root@yblebedev yblebedev]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@yblebedev yblebedev]# touch /var/www/html/proverka.html
[root@yblebedev yblebedev]# cat /var/www/html/proverka.html
[root@yblebedev yblebedev]# touch /var/www/html/proverka
[root@yblebedev yblebedev]# cat /var/www/html/proverka
```

Рис.5. Пункт 5-10

Результаты выполнения лабораторной работы

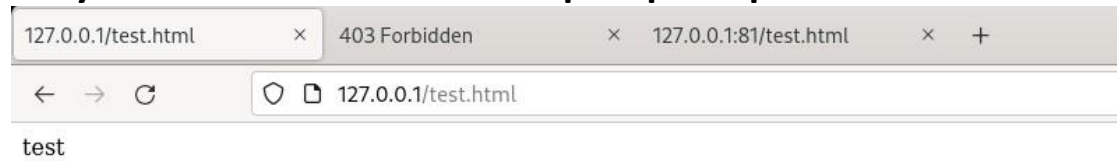
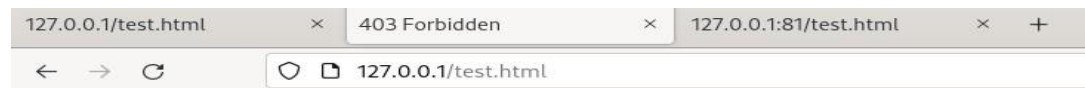


Рис.6. Пункт 11

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

Рис.7. Пункт 12-13



Forbidden

You don't have permission to access this resource.

Рис.8. Пункт 14

Результаты выполнения лабораторной работы

```
[root@yblebedev yblebedev]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 11 19:08 /var/www/html/test.html
[root@yblebedev yblebedev]# tail /var/log/messages
Oct 11 19:11:12 yblebedev systemd[1]: Started dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 11 19:11:13 yblebedev setroubleshoot[40974]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l e3414ec9-de39-4757-977c-27a4e4546521
Oct 11 19:11:13 yblebedev setroubleshoot[40974]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****
*****#012#012Если вы хотите исправить метку.$TARGETЗнак_PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012**** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 11 19:11:13 yblebedev setroubleshoot[40974]: failed to retrieve rpm info for /var/www/html/test.html
Oct 11 19:11:14 yblebedev setroubleshoot[40974]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l e3414ec9-de39-4757-977c-27a4e4546521
Oct 11 19:11:14 yblebedev setroubleshoot[40974]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****
*****#012#012Если вы хотите исправить метку.$TARGETЗнак_PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить 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 доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 11 19:11:24 yblebedev systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Main process exited, code=killed, status=14/ALRM
Oct 11 19:11:24 yblebedev systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Failed with result 'signal'.
Oct 11 19:11:24 yblebedev systemd[1]: dbus-:1.10-org.fedoraproject.Setroubleshootd@0.service: Main process exited, code=killed, status=14/ALRM
Oct 11 19:11:24 yblebedev systemd[1]: dbus-:1.10-org.fedoraproject.Setroubleshootd@0.service: Failed with result 'signal'.
```

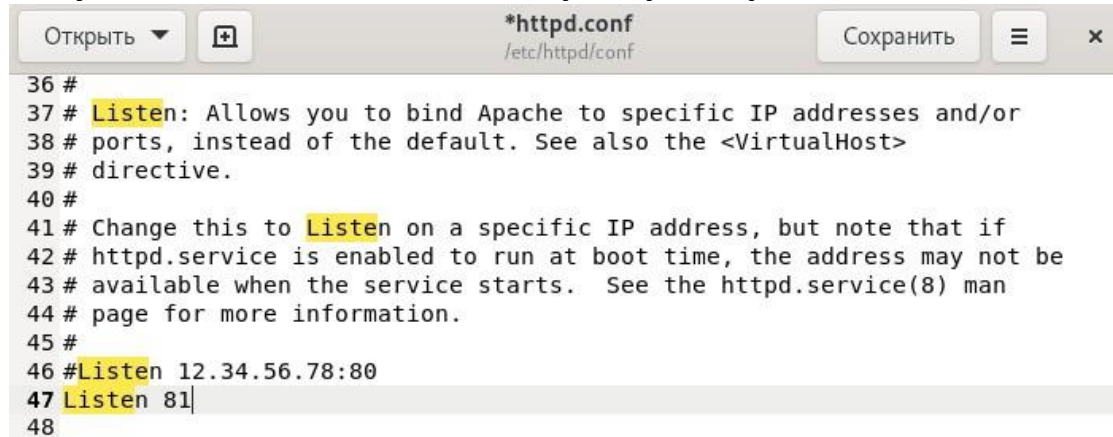
Рис.9. Пункт 15 часть 1

Результаты выполнения лабораторной работы

```
[root@yblebedev yblebedev]# tail /var/log/audit/audit.log
type=AVC msg=audit(1665504670.969:297): avc: denied { getattr } for pid=21749 comm="httpd" path="/var
/www/html/test.html" dev="dm-0" ino=18506661 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u
:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665504670.969:297): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1
=7f242c043cb0 a2=7f2426ff4830 a3=0 items=0 ppid=21121 pid=21749 auid=4294967295 uid=48 gid=48 euid=48 su
id=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" sub
j=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="a
pache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1665504670.969:297): proctitle=2F7573722F7362696E2F6874747064002D44464F52454752
4F554E44
type=AVC msg=audit(1665504670.969:298): avc: denied { getattr } for pid=21749 comm="httpd" path="/var
/www/html/test.html" dev="dm-0" ino=18506661 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u
:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665504670.969:298): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1
=7f242c043d90 a2=7f2426ff4830 a3=100 items=0 ppid=21121 pid=21749 auid=4294967295 uid=48 gid=48 euid=48
suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" s
ubj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID=
"apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1665504670.969:298): proctitle=2F7573722F7362696E2F6874747064002D44464F52454752
4F554E44
type=SERVICE_START msg=audit(1665504670.985:299): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system
_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproject.Setroubleshootd@0 comm="systemd" exe="/usr/
lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665504672.085:300): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system
_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" e
xe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665504684.055:301): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system
_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" ex
e="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665504684.095:302): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system
_u:system_r:init_t:s0 msg='unit=dbus-:1.10-org.fedoraproject.Setroubleshootd@0 comm="systemd" exe="/usr/l
ib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
```

Рис.10. Пункт 15 часть 2

Результаты выполнения лабораторной работы



```
36 #
37 # Listen: Allows you to bind Apache to specific IP addresses and/or
38 # ports, instead of the default. See also the <VirtualHost>
39 # directive.
40 #
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
```

Рис.11. Пункт 16

Результаты выполнения лабораторной работы

```
[root@yblebedev yblebedev]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@yblebedev yblebedev]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@yblebedev yblebedev]# 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 preset: disabled)
   Active: active (running) since Tue 2022-10-11 19:13:51 MSK; 8s ago
     Docs: man:httpd.service(8)
  Main PID: 41105 (httpd)
    Status: "Started, listening on: port 81"
    Tasks: 213 (limit: 12210)
   Memory: 23.2M
      CPU: 60ms
   CGroup: /system.slice/httpd.service
           └─41105 /usr/sbin/httpd -DFOREGROUND
             └─41106 /usr/sbin/httpd -DFOREGROUND
               └─41110 /usr/sbin/httpd -DFOREGROUND
                 └─41111 /usr/sbin/httpd -DFOREGROUND
                   └─41113 /usr/sbin/httpd -DFOREGROUND

окт 11 19:13:51 yblebedev.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 11 19:13:51 yblebedev.localdomain systemd[1]: Started The Apache HTTP Server.
окт 11 19:13:51 yblebedev.localdomain httpd[41105]: Server configured, listening on: port 81
[root@yblebedev yblebedev]#
[root@yblebedev yblebedev]# tail -n1 /var/log/messages
tail: неверное количество строк: «1»
[root@yblebedev yblebedev]# tail -n1 /var/log/messages
Oct 11 19:13:51 yblebedev httpd[41105]: Server configured, listening on: port 81
[root@yblebedev yblebedev]# tail -n1 /var/log/http/error_log
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
[root@yblebedev yblebedev]# tail -n1 /var/log/http/access_log
tail: невозможно открыть '/var/log/http/access_log' для чтения: Нет такого файла или каталога
[root@yblebedev yblebedev]# tail -n1 /var/log/audit/audit.log
type=SERVICE_START msg=audit(1665504831.856:304): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd"
hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
```

Рис.12. Пункт 17-18

Результаты выполнения лабораторной работы

```
[root@yblebedev yblebedev]# 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@yblebedev yblebedev]# 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 preset: disabled)
   Active: active (running) since Tue 2022-10-11 19:13:51 MSK; 2min 1s ago
     Docs: man:httpd.service(8)
   Main PID: 41105 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:
  █
      Tasks: 213 (limit: 12210)
     Memory: 23.2M
        CPU: 110ms
    CGroup: /system.slice/httpd.service
            └─41105 /usr/sbin/httpd -DFOREGROUND
              └─41106 /usr/sbin/httpd -DFOREGROUND
                └─41110 /usr/sbin/httpd -DFOREGROUND
                  └─41111 /usr/sbin/httpd -DFOREGROUND
                    └─41113 /usr/sbin/httpd -DFOREGROUND

окт 11 19:13:51 yblebedev.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 11 19:13:51 yblebedev.localdomain systemd[1]: Started The Apache HTTP Server.
окт 11 19:13:51 yblebedev.localdomain httpd[41105]: Server configured, listening on: port 81
[root@yblebedev yblebedev]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Рис.13. Пункт 19-21

Результаты выполнения лабораторной работы

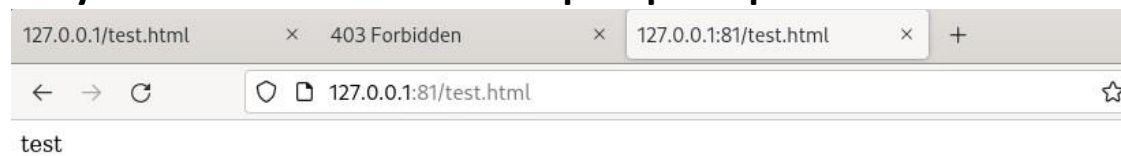


Рис.14. Пункт 21 часть 2

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

Рис.15. Пункт 24

Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache