

Отчет по лабораторной работе № 6

Мандатное разграничение прав в Linux

Лебедев Ярослав Борисович

Содержание

Цель работы	3
Выполнение лабораторной работы	4
Выводы	14
Список литературы	15

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache [1].

Выполнение лабораторной работы

Подготовка лабораторного стенда и методические рекомендации

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика `targeted` и режим `enforcing` используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл `/etc/selinux/config`, так и проверить используемый режим и политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится (Рис.1).

```
[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

4. В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName: ServerName test.ru` чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе (Рис.2).

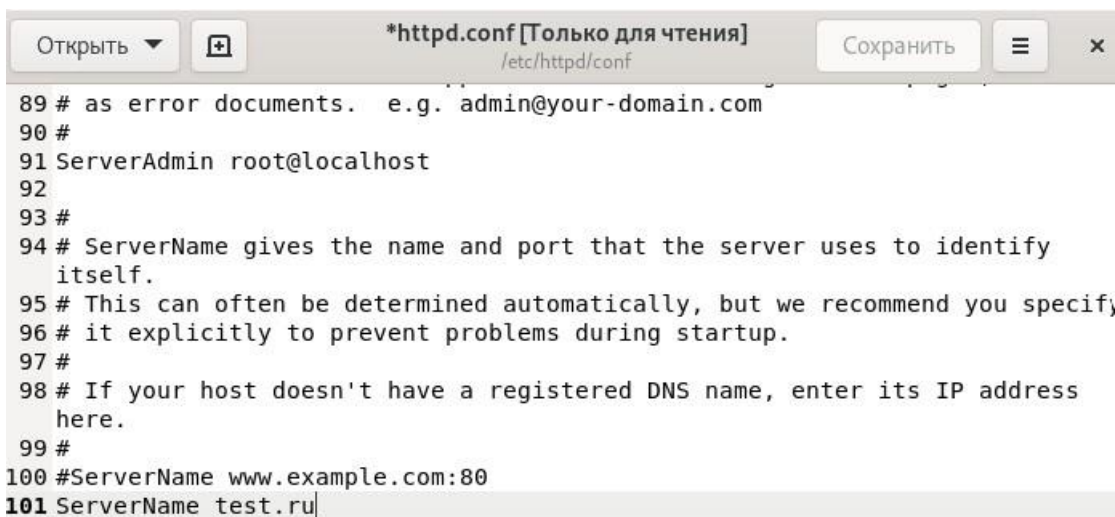


Рис.2. Подготовка. Пункт 4

5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами

iptables -F

iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT

либо добавить разрешающие правила:

iptables -I INPUT -p tcp -dport 80 -j ACCEPT

iptables -I INPUT -p tcp -dport 81 -j ACCEPT

iptables -I OUTPUT -p tcp -sport 80 -j ACCEPT

iptables -I OUTPUT -p tcp -sport 81 -j ACCEPT

6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные links, lynx, wget и графические konqueror, opera, firefoxили др.

Порядок выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforceи sestatus (Рис.3).
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 (Рис.3).

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` (Рис.3)

```
[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

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off» (Рис.4).

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 (Рис.5):

test

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (Рис.5).

```
[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
Sensitivities:           1
Types:                   4995
Users:                   8
Booleans:                347
Allow:                   63727
Auditallow:              163
Type_trans:              251060
Type_member:             35
Role_allow:              38
Constraints:             72
MLS Constrain:           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.:             382
Neverallow:              0
Dontaudit:               8391
Type_change:             87
Range_trans:             5958
Role_trans:              418
Validatetrans:           0
MLS Val. Tran:           0
Polcap:                  5
Typebounds:              0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:               0
Fs_use:                  33
Portcon:                 651
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

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён (Рис.6).

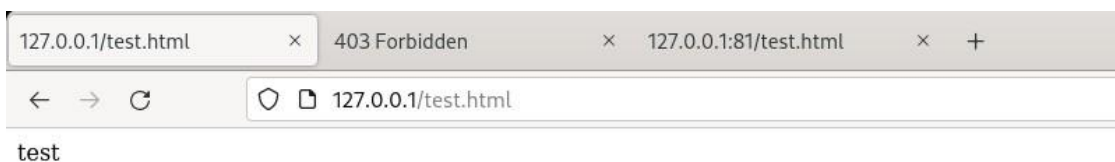


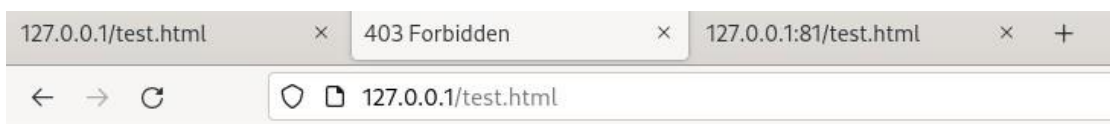
Рис.6. Пункт 11

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 `/ргос` 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 (Рис.7).
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` После этого проверьте, что контекст поменялся (Рис.7).

```
[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

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` (Рис.8).



Forbidden

You don't have permission to access this resource.

Рис.8. Пункт 14

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 auditd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно (Рис.9-10).

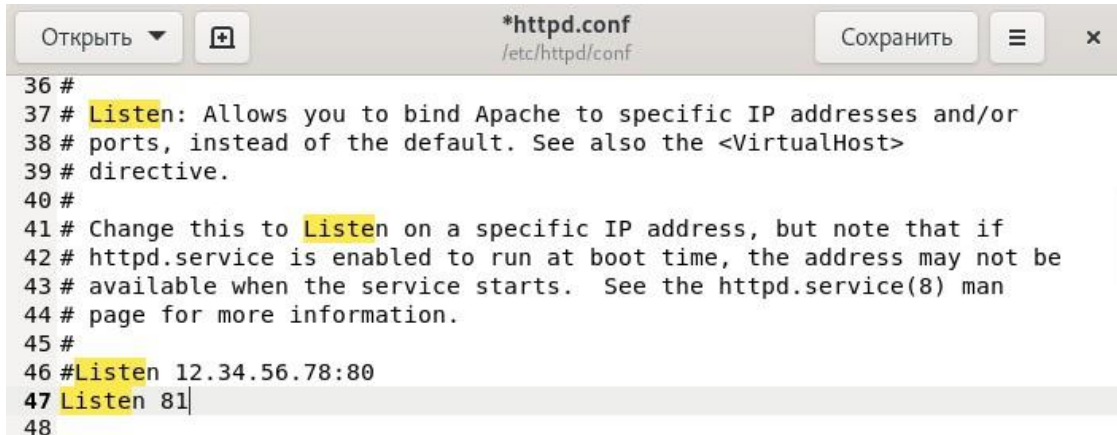
```
[root@yblebedev yblebedev]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 11 19:08 /var/www/html/test.html
[root@yblebedev yblebedev]# tail /var/log/messages
Oct 11 19:11:12 yblebedev systemd[1]: Started dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 11 19:11:13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

```
[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 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=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(1665504670.969:297): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
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" subj=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=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
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" exe="/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" exe="/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/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
```

Рис.10. Пункт 15 часть 2

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 (Рис.11).



```
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

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? (Рис.12) – Сервер запустился, потому что система настроена таким образом, что можно прослушивать указанный порт.
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 (Рис.12).


```

[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 -nl /var/log/messages
tail: неверное количество строк: «l»
[root@yblebedev yblebedev]# tail -nl /var/log/messages
Oct 11 19:13:51 yblebedev httpd[41105]: Server configured, listening on: port 81
[root@yblebedev yblebedev]# tail -nl /var/log/http/error_log
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
[root@yblebedev yblebedev]# tail -nl /var/log/http/access_log
tail: невозможно открыть '/var/log/http/access_log' для чтения: Нет такого файла или каталога
[root@yblebedev yblebedev]# tail -nl /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

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 (Рис.13).
20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? (Рис.13) – Сервер запустился, потому что система настроена таким образом, что можно прослушивать указанный порт.
21. Верните контекст `httpd_sys_content_t` к 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» (Рис.13-14).

```
[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:
           0"
     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

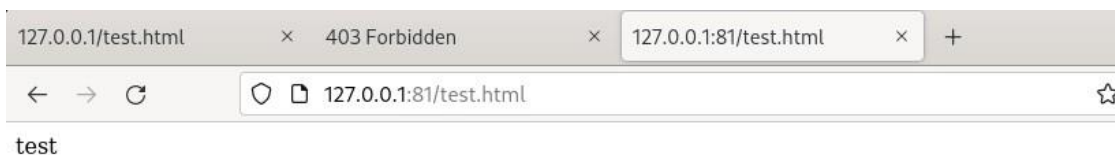


Рис.14. Пункт 21 часть 2

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
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` (Рис.15)

```
[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.

Список литературы

1. Методические материалы курса