

Лабораторная работа №9

Основы администрирования операционных систем

Верниковская Е. А., НПИбд-01-23

1 ноября 2024

Российский университет дружбы народов, Москва, Россия

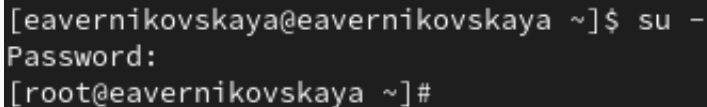
Вводная часть

Получить навыки работы с контекстом безопасности и политиками SELinux.

1. Продемонстрировать навыки по управлению режимами SELinux.
2. Продемонстрировать навыки по восстановлению контекста безопасности SELinux.
3. Настроить контекст безопасности для нестандартного расположения файлов вебслужбы.
4. Продемонстрировать навыки работы с переключателями SELinux.

Выполнение лабораторной работы

Запускаем терминала и получаем полномочия суперпользователя, используя *su* - (рис. 1)

A terminal window with a dark background and light gray text. The prompt is [eavernikovskaya@eavernikovskaya ~]\$ and the command entered is su -. The next line shows Password: and the final line shows the root prompt [root@eavernikovskaya ~]#.

```
[eavernikovskaya@eavernikovskaya ~]$ su -
Password:
[root@eavernikovskaya ~]#
```

Рис. 1: Режим суперпользователя

Посмотрим текущую информацию о состоянии SELinux, используя *sestatus -v* (рис. 2)

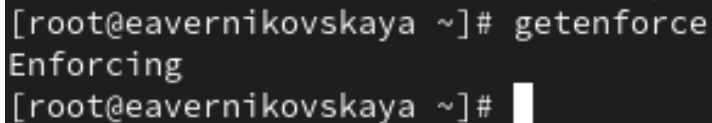
```
[root@eavernikovskaya ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:          unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
[root@eavernikovskaya ~]#
```

Рис. 2: Состояние SELinux (1)

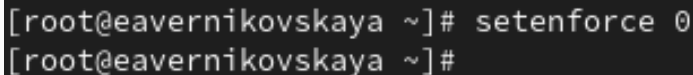
Посмотрим, в каком режиме работает SELinux: *getenforce*. По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing) (рис. 3)

A terminal window with a dark background and light gray text. The prompt is [root@eavernikovskaya ~]#. The command getenforce is entered, and the output is Enforcing. The prompt is repeated at the end of the line.

```
[root@eavernikovskaya ~]# getenforce
Enforcing
[root@eavernikovskaya ~]#
```

Рис. 3: Режим работы SELinux (1)

Изменим режим работы SELinux на разрешающий (Permissive): *setenforce 0*
(рис. 4)

A terminal window with a dark background and light gray text. The prompt is [root@eavernikovskaya ~]#. The command setenforce 0 is entered on the first line. On the second line, the prompt [root@eavernikovskaya ~]# is shown again, indicating the command has been executed.

```
[root@eavernikovskaya ~]# setenforce 0  
[root@eavernikovskaya ~]#
```

Рис. 4: Изменение режима работы SELinux на Permissive

После, снова вводим *getenforce* (рис. 5)

```
[root@eavernikovskaya ~]# getenforce
Permissive
[root@eavernikovskaya ~]#
```

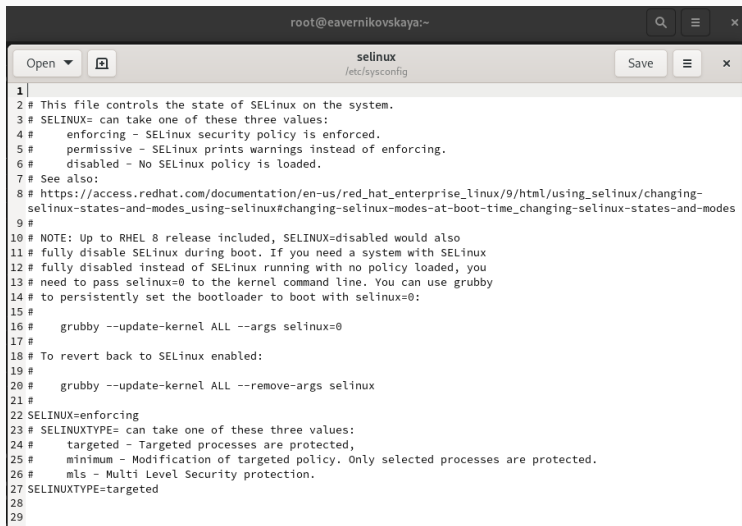
Рис. 5: Режим работы SELinux (2)

В файле `/etc/sysconfig/selinux` с помощью редактора устанавливаем параметр `disabled: SELINUX=disabled` (рис. 6), (рис. 7), (рис. 8)

```
[root@eavernikovskaya ~]# gedit /etc/sysconfig/selinux
```

Рис. 6: Открытие файла `/etc/sysconfig/selinux` (1)

Управление режимами SELinux



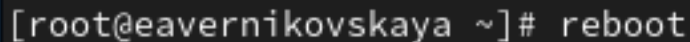
```
1 |
2 # This file controls the state of SELinux on the system.
3 # SELINUX= can take one of these three values:
4 #   enforcing - SELinux security policy is enforced.
5 #   permissive - SELinux prints warnings instead of enforcing.
6 #   disabled - No SELinux policy is loaded.
7 # See also:
8 # https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-
   selinux-states-and-modes_using-selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes
9 #
10 # NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
11 # fully disable SELinux during boot. If you need a system with SELinux
12 # fully disabled instead of SELinux running with no policy loaded, you
13 # need to pass selinux=0 to the kernel command line. You can use grubby
14 # to persistently set the bootloader to boot with selinux=0:
15 #
16 #   grubby --update-kernel ALL --args selinux=0
17 #
18 # To revert back to SELinux enabled:
19 #
20 #   grubby --update-kernel ALL --remove-args selinux
21 #
22 SELINUX=enforcing
23 # SELINUXTYPE= can take one of these three values:
24 #   targeted - Targeted processes are protected,
25 #   minimum - Modification of targeted policy. Only selected processes are protected.
26 #   mls - Multi Level Security protection.
27 SELINUXTYPE=targeted
28
29
```

Рис. 7: Файл /etc/sysconfig/selinux (1)

```
21 #  
22 SELINUX=disabled
```

Рис. 8: SELINUX=disabled

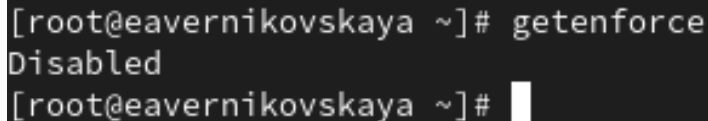
Далее перезапускаем систему (рис. 9)



```
[root@eavernikovskaya ~]# reboot
```

Рис. 9: Перезапуск системы

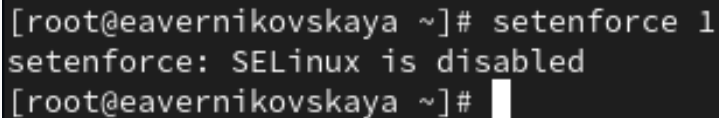
После перезагрузки запускаем терминал и получаем полномочия администратора. Далее смотрим статус SELinux. Мы увидим, что SELinux теперь отключён (рис. 10)

A terminal window with a dark background and light gray text. The prompt is [root@eavernikovskaya ~]#. The command 'getenforce' has been entered, and the output 'Disabled' is shown on the next line. The prompt is repeated on the third line with a white cursor block.

```
[root@eavernikovskaya ~]# getenforce
Disabled
[root@eavernikovskaya ~]#
```

Рис. 10: Режим работы SELinux (3)

Попробуем переключить режим работы SELinux: *setenforce 1*. Мы не сможем этого сделать, так как SELinux отключён (рис. 11)



```
[root@eavernikovskaya ~]# setenforce 1
setenforce: SELinux is disabled
[root@eavernikovskaya ~]#
```

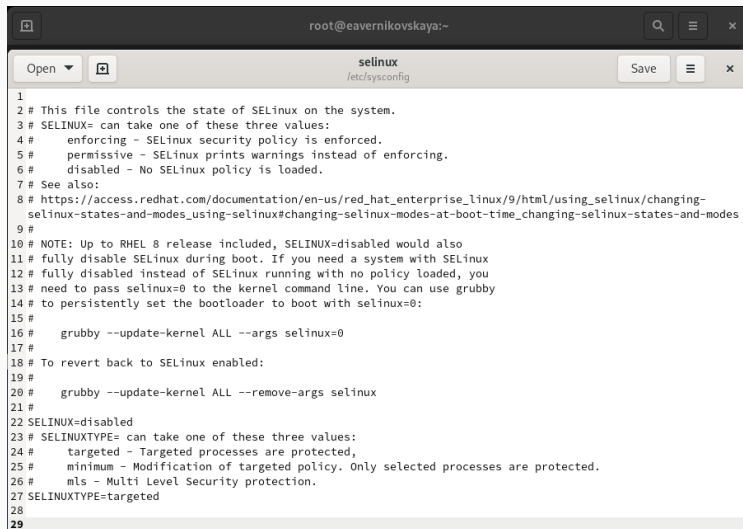
Рис. 11: Попытка изменения режима работы SELinux

В файле `/etc/sysconfig/selinux` с помощью редактора устанавливаем параметр `enforcing`: *SELINUX=enforcing* (рис. 12), (рис. 13), (рис. 14)

```
[root@eavernikovskaya ~]# gedit /etc/sysconfig/selinux
```

Рис. 12: Открытие файла `/etc/sysconfig/selinux` (2)

Управление режимами SELinux



```
1
2 # This file controls the state of SELinux on the system.
3 # SELINUX= can take one of these three values:
4 #     enforcing - SELinux security policy is enforced.
5 #     permissive - SELinux prints warnings instead of enforcing.
6 #     disabled - No SELinux policy is loaded.
7 # See also:
8 # https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-
9 # selinux-states-and-modes_using-selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes
10 #
11 # NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
12 # fully disable SELinux during boot. If you need a system with SELinux
13 # fully disabled instead of SELinux running with no policy loaded, you
14 # need to pass selinux=0 to the kernel command line. You can use grubby
15 # to persistently set the bootloader to boot with selinux=0:
16 #
17 # grubby --update-kernel ALL --args selinux=0
18 #
19 # To revert back to SELinux enabled:
20 #
21 # grubby --update-kernel ALL --remove-args selinux
22 #
23 SELINUX=disabled
24 # SELINUXTYPE= can take one of these three values:
25 #     targeted - Targeted processes are protected,
26 #     minimum - Modification of targeted policy. Only selected processes are protected.
27 #     mls - Multi Level Security protection.
28 SELINUXTYPE=targeted
29
```

Рис. 13: Файл /etc/sysconfig/selinux (2)

```
21 #  
22 SELINUX=enforcing
```

Рис. 14: SELINUX=enforcing

Управление режимами SELinux

Снова перезагружаем систему. Во время загрузки системы мы, получили предупреждающее сообщение о необходимости восстановления меток SELinux (рис. 15)

```
[ 0.068978] RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to  
RETbleed attacks, data leaks possible!  
[ 1.394849] systemd[1]: Invalid DMI field header.  
[ 2.223646] Warning: Unmaintained driver is detected: e1000  
[ 2.588165] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 2.588166] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 2.588167] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 6.611882] selinux-autorelabel[700]: *** Warning -- SELinux targeted policy relabel is required.  
[ 6.612881] selinux-autorelabel[700]: *** Relabeling could take a very long time, depending on file  
[ 6.612328] selinux-autorelabel[700]: *** system size and speed of hard drives.  
[ 6.623363] selinux-autorelabel[700]: Running: /sbin/fixfiles -T 0 restore  
[ 20.214337] selinux-autorelabel[706]: Warning: Skipping the following R/O filesystems:  
[ 20.214728] selinux-autorelabel[706]: /run/credentials/systemd-sysctl.service  
[ 20.214823] selinux-autorelabel[706]: /run/credentials/systemd-tmpfiles-setup-dev.service  
[ 20.215883] selinux-autorelabel[706]: /run/credentials/systemd-tmpfiles-setup.service  
[ 20.216047] selinux-autorelabel[706]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys  
l/debug /sys/kernel/tracing
```

Рис. 15: Перезагрузка системы + предупреждающее сообщение

Управление режимами SELinux

После перезагрузки в терминале с полномочиями администратора посмотрим текущую информацию о состоянии SELinux. Система работает в принудительном режиме (enforcing) использования SELinux (рис. 16)

```
[root@eavernikovskaya ~]# sestatus -v
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

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:          unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                    system_u:object_r:passwd_file_t:s0
/etc/shadow                    system_u:object_r:shadow_t:s0
/bin/bash                      system_u:object_r:shell_exec_t:s0
/bin/login                     system_u:object_r:login_exec_t:s0
/bin/sh                        system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                   system_u:object_r:getty_exec_t:s0
/sbin/init                     system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                 system_u:object_r:sshd_exec_t:s0
[root@eavernikovskaya ~]#
```

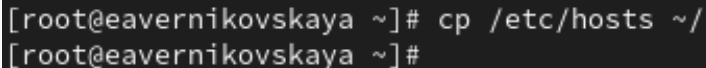
Рис. 16: Состояние SELinux (2)

Посмотрим контекст безопасности файла `/etc/hosts`: `ls -Z /etc/hosts`. Мы увидим, что у файла есть метка контекста `net_conf_t` (рис. 17)

```
[root@eavernikovskaya ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@eavernikovskaya ~]#
```

Рис. 17: Контекст безопасности файла `/etc/hosts` (1)

Скопируем файл `/etc/hosts` в домашний каталог, с помощью `cp /etc/hosts ~/` (рис. 18)



```
[root@eavernikovskaya ~]# cp /etc/hosts ~/
[root@eavernikovskaya ~]#
```

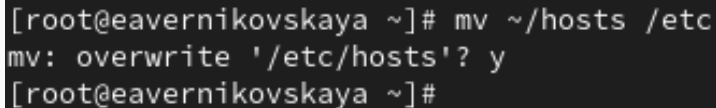
Рис. 18: Копирование файла `/etc/hosts` в домашний каталог

Проверяем контекст файла ~/hosts: `ls -Z ~/hosts`. Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin_home_t (рис. 19)

```
[root@eavernikovskaya ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@eavernikovskaya ~]#
```

Рис. 19: Контекст безопасности файла ~/hosts

Попытаемся перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc`: `mv ~/hosts /etc` (рис. 20)



```
[root@eavernikovskaya ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@eavernikovskaya ~]#
```

Рис. 20: Перезапись существующего файла `hosts` из домашнего каталога в каталог `/etc`

Далее проверим, что тип контекста по-прежнему установлен на `admin_home_t`:
`ls -Z /etc/hosts` (рис. 21)

```
[root@eavernikovskaya ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@eavernikovskaya ~]#
```

Рис. 21: Контекст безопасности файла `/etc/hosts` (2)

Далее исправим контекст безопасности: `restorecon -v /etc/hosts` Опция `-v` покажет процесс изменения (рис. 22)

```
[root@eavernikovskaya ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@eavernikovskaya ~]#
```

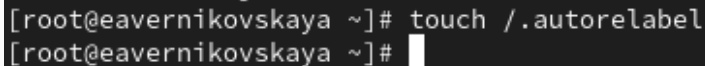
Рис. 22: Исправление контекста безопасности

Проверим, что тип контекста изменился (рис. 23)

```
[root@eavernikovskaya ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@eavernikovskaya ~]#
```

Рис. 23: Контекст безопасности файла /etc/hosts (3)

Для массового исправления контекста безопасности на файловой системе вводим `touch /.autorelabel` (рис. 24)



```
[root@eavernikovskaya ~]# touch /.autorelabel  
[root@eavernikovskaya ~]#
```

Рис. 24: Массовое исправление контекста безопасности

Использование restorecon для восстановления контекста безопасности

После перезапускаем систему. Во время перезапуска нажимаем клавишу Esc, чтобы мы видели загрузочные сообщения. Мы увидим, что файловая система автоматически перемаркирована (рис. 25)

```
1 [ OK ] Finished Mount Root and Kernel File System.
2 [ OK ] Reached target Preparation for Network.
3 [ OK ] Reached target Swap.
4 [ OK ] Mounted RES Control File System.
5 [ OK ] Mounted RES Control File System.
6 [ OK ] Mounted RES Control File System.
7 [ OK ] Mounted RES Control File System.
8 [ OK ] Mounted RES Control File System.
9 [ OK ] Mounted RES Control File System.
10 [ OK ] Mounted RES Control File System.
11 [ OK ] Mounted RES Control File System.
12 [ OK ] Mounted RES Control File System.
13 [ OK ] Mounted RES Control File System.
14 [ OK ] Mounted RES Control File System.
15 [ OK ] Mounted RES Control File System.
16 [ OK ] Mounted RES Control File System.
17 [ OK ] Mounted RES Control File System.
18 [ OK ] Mounted RES Control File System.
19 [ OK ] Mounted RES Control File System.
20 [ OK ] Mounted RES Control File System.
21 [ OK ] Mounted RES Control File System.
22 [ OK ] Mounted RES Control File System.
23 [ OK ] Mounted RES Control File System.
24 [ OK ] Mounted RES Control File System.
25 [ OK ] Mounted RES Control File System.
26 [ OK ] Mounted RES Control File System.
27 [ OK ] Mounted RES Control File System.
28 [ OK ] Mounted RES Control File System.
29 [ OK ] Mounted RES Control File System.
30 [ OK ] Mounted RES Control File System.
31 [ OK ] Mounted RES Control File System.
32 [ OK ] Mounted RES Control File System.
33 [ OK ] Mounted RES Control File System.
34 [ OK ] Mounted RES Control File System.
35 [ OK ] Mounted RES Control File System.
36 [ OK ] Mounted RES Control File System.
37 [ OK ] Mounted RES Control File System.
38 [ OK ] Mounted RES Control File System.
39 [ OK ] Mounted RES Control File System.
40 [ OK ] Mounted RES Control File System.
41 [ OK ] Mounted RES Control File System.
42 [ OK ] Mounted RES Control File System.
43 [ OK ] Mounted RES Control File System.
44 [ OK ] Mounted RES Control File System.
45 [ OK ] Mounted RES Control File System.
46 [ OK ] Mounted RES Control File System.
47 [ OK ] Mounted RES Control File System.
48 [ OK ] Mounted RES Control File System.
49 [ OK ] Mounted RES Control File System.
50 [ OK ] Mounted RES Control File System.
51 [ OK ] Mounted RES Control File System.
52 [ OK ] Mounted RES Control File System.
53 [ OK ] Mounted RES Control File System.
54 [ OK ] Mounted RES Control File System.
55 [ OK ] Mounted RES Control File System.
56 [ OK ] Mounted RES Control File System.
57 [ OK ] Mounted RES Control File System.
58 [ OK ] Mounted RES Control File System.
59 [ OK ] Mounted RES Control File System.
60 [ OK ] Mounted RES Control File System.
61 [ OK ] Mounted RES Control File System.
62 [ OK ] Mounted RES Control File System.
63 [ OK ] Mounted RES Control File System.
64 [ OK ] Mounted RES Control File System.
65 [ OK ] Mounted RES Control File System.
66 [ OK ] Mounted RES Control File System.
67 [ OK ] Mounted RES Control File System.
68 [ OK ] Mounted RES Control File System.
69 [ OK ] Mounted RES Control File System.
70 [ OK ] Mounted RES Control File System.
71 [ OK ] Mounted RES Control File System.
72 [ OK ] Mounted RES Control File System.
73 [ OK ] Mounted RES Control File System.
74 [ OK ] Mounted RES Control File System.
75 [ OK ] Mounted RES Control File System.
76 [ OK ] Mounted RES Control File System.
77 [ OK ] Mounted RES Control File System.
78 [ OK ] Mounted RES Control File System.
79 [ OK ] Mounted RES Control File System.
80 [ OK ] Mounted RES Control File System.
81 [ OK ] Mounted RES Control File System.
82 [ OK ] Mounted RES Control File System.
83 [ OK ] Mounted RES Control File System.
84 [ OK ] Mounted RES Control File System.
85 [ OK ] Mounted RES Control File System.
86 [ OK ] Mounted RES Control File System.
87 [ OK ] Mounted RES Control File System.
88 [ OK ] Mounted RES Control File System.
89 [ OK ] Mounted RES Control File System.
90 [ OK ] Mounted RES Control File System.
91 [ OK ] Mounted RES Control File System.
92 [ OK ] Mounted RES Control File System.
93 [ OK ] Mounted RES Control File System.
94 [ OK ] Mounted RES Control File System.
95 [ OK ] Mounted RES Control File System.
96 [ OK ] Mounted RES Control File System.
97 [ OK ] Mounted RES Control File System.
98 [ OK ] Mounted RES Control File System.
99 [ OK ] Mounted RES Control File System.
100 [ OK ] Mounted RES Control File System.
```

Рис. 25: Перезагрузка системы + загрузочные сообщения

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Устанавливаем необходимое программное обеспечение (рис. 26), (рис. 27)

```
[root@eavernikovskaya ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               3.0 kB/s | 4.1 kB      00:01
Rocky Linux 9 - BaseOS                               1.9 MB/s | 2.3 MB      00:01
Rocky Linux 9 - AppStream                             10 kB/s | 4.5 kB      00:00
Rocky Linux 9 - AppStream                             3.5 MB/s | 8.0 MB      00:02
Rocky Linux 9 - Extras                               5.8 kB/s | 2.9 kB      00:00
Package httpd-2.4.57-11.el9_4.1.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@eavernikovskaya ~]#
```

Рис. 26: Установка httpd

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

```
[root@eavernikovskaya ~]# dnf -y install lynx
Last metadata expiration check: 0:00:25 ago on Fri 01 Nov 2024 01:27:52 PM MSK.
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
  lynx                  x86_64            2.8.9-20.el9      appstream         1.5 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm                                1.3 MB/s | 1.5 MB    00:01
-----
Total
816 kB/s | 1.5 MB    00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : lynx-2.8.9-20.el9.x86_64      1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64    1/1
  Verifying      : lynx-2.8.9-20.el9.x86_64      1/1

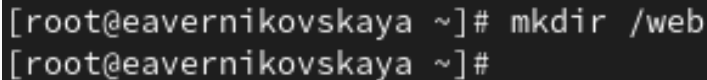
Installed:
  lynx-2.8.9-20.el9.x86_64

Complete!
[root@eavernikovskaya ~]#
```

Рис. 27: Установка lynx

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Создаём новое хранилище для файлов web-сервера: *mkdir /web* (рис. 28)



```
[root@eavernikovskaya ~]# mkdir /web  
[root@eavernikovskaya ~]#
```

Рис. 28: Создание хранилища для файлов web-сервера

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Создаём файл index.html в каталоге с контентом веб-сервера (рис. 29)

```
[root@eavernikovskaya ~]# cd /web  
[root@eavernikovskaya web]# touch index.html  
[root@eavernikovskaya web]#
```

Рис. 29: Создание файла index.html в каталоге с контентом веб-сервера

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Пишем в созданном файле index.html следующий текст: Welcome to my web-server (рис. 30), (рис. 31), (рис. 32)

```
[root@eavernikovskaya web]# gedit /web/index.html
```

Рис. 30: Открытие файла index.html

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

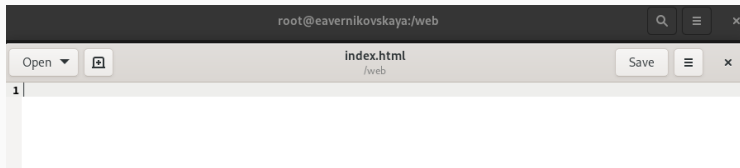


Рис. 31: Файл index.html

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

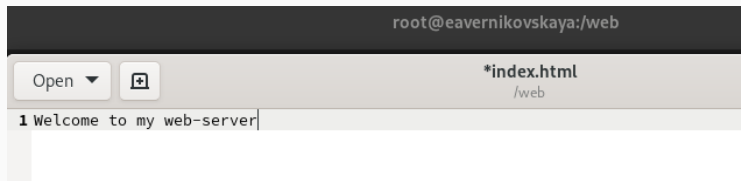


Рис. 32: Редактирование файла index.html

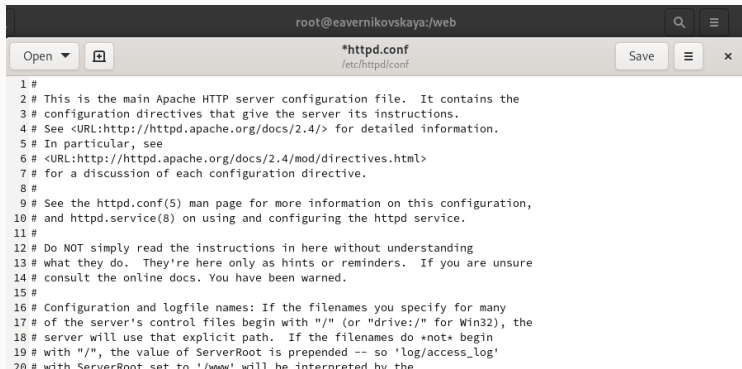
Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

В файле `/etc/httpd/conf/httpd.conf` закомментируем строку *DocumentRoot* `“/var/www/html”` и ниже добавим строку *DocumentRoot* `“/web”` (рис. 33), (рис. 34), (рис. 35)

```
[root@eavernikovskaya web]# gedit /etc/httpd/conf/httpd.conf
```

Рис. 33: Открытие файла `etc/httpd/conf/httpd.conf`

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера



```
1 #
2 # This is the main Apache HTTP server configuration file. It contains the
3 # configuration directives that give the server its instructions.
4 # See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
5 # In particular, see
6 # <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
7 # for a discussion of each configuration directive.
8 #
9 # See the httpd.conf(5) man page for more information on this configuration,
10 # and httpd.service(8) on using and configuring the httpd service.
11 #
12 # Do NOT simply read the instructions in here without understanding
13 # what they do. They're here only as hints or reminders. If you are unsure
14 # consult the online docs. You have been warned.
15 #
16 # Configuration and logfile names: If the filenames you specify for many
17 # of the server's control files begin with "/" (or "drive:/" for Win32), the
18 # server will use that explicit path. If the filenames do *not* begin
19 # with "/", the value of ServerRoot is prepended -- so 'log/access_log'
20 # with ServerRoot set to '/www' will be interpreted by the
```

Рис. 34: Файл etc/httpd/conf/httpd.conf

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

```
124 # DocumentRoot "/var/www/html"  
125 DocumentRoot "/web"
```

Рис. 35: Редактирование файла `etc/httpd/conf/httpd.conf` (1)

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Затем в этом же файле ниже закомментируем раздел

```
<Directory "/var/www">  
    AllowOverride None  
    Require all granted  
</Directory>
```

и добавим следующий раздел, определяющий правила доступа: (рис. 36)

```
<Directory "/web">  
    AllowOverride None  
    Require all granted  
</Directory>
```

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

```
# <Directory "/var/www">  
    # AllowOverride None  
    # Allow open access:  
    # Require all granted  
# </Directory>  
  
<Directory "/web">  
    AllowOverride None  
    Require all granted  
</Directory>
```

Рис. 36: Редактирование файла etc/httpd/conf/httpd.conf (2)

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

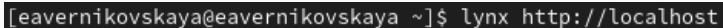
Запускаем веб-сервер и службу httpd (рис. 37)

```
[root@eavernikovskaya web]# systemctl start httpd  
[root@eavernikovskaya web]# systemctl enable httpd  
[root@eavernikovskaya web]#
```

Рис. 37: Запуск веб-сервера и службы httpd

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

В терминале под учётной записью нашего пользователя обращаемся к веб-серверу в текстовом браузере lynx: *lynx http://localhost* (рис. 38)



```
[eavernikovskaya@eavernikovskaya ~]$ lynx http://localhost
```

Рис. 38: lynx http://localhost (1)

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

После этого мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла `index.html` (для выхода из `lynx` нажимается `q`) (рис. 39)

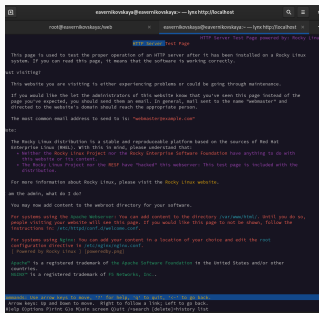
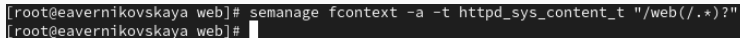


Рис. 39: Веб-страница Red Hat по умолчанию

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

В терминале с полномочиями администратора применяем новую метку контекста к /web: `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` (рис. 40)



```
[root@eavernikovskaya web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
[root@eavernikovskaya web]#
```

Рис. 40: Применение новой метку контекста к /web

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Восстановим контекст безопасности: *restorecon -R -v /web* (рис. 41)

```
[root@eavernikovskaya web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
[root@eavernikovskaya web]#
```

Рис. 41: Восстановление контекста безопасности

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

В терминале под учётной записью нашего пользователя снова обращаемся к веб-серверу: `lynx http://localhost`. Теперь мы получили доступ к своей пользовательской веб-странице. На экране есть запись «Welcome to my web-server» (рис. 42), (рис. 43)

```
[eavernikovskaya@eavernikovskaya ~]$ lynx http://localhost
```

Рис. 42: lynx http://localhost (2)

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

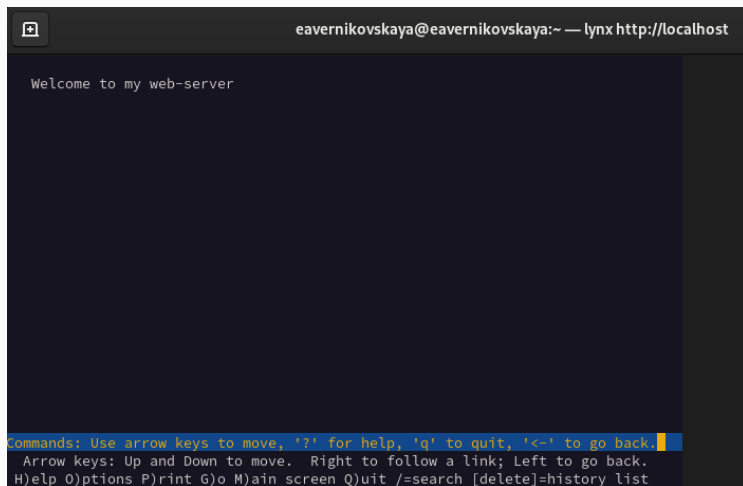


Рис. 43: Наша пользовательская веб-страница

Работа с переключателями SELinux

Посмотрим список переключателей SELinux для службы ftp: `getsebool -a | grep ftp`. Мы увидим переключатель `ftpd_anon_write` с текущим значением `off` (рис. 44)

```
[root@eavernikovskaya ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@eavernikovskaya ~]#
```

Рис. 44: Список переключателей SELinux для службы ftp

Для службы `ftpd_anon` посмотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен: `semanage boolean -l | grep ftpd anon` (рис. 45)

```
[root@eavernikovskaya ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (off , off) Allow ftpd to anon write
[root@eavernikovskaya ~]#
```

Рис. 45: Список переключателей с пояснением для службы `ftpd_anon`

Изменим текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`: *`setsebool ftpd_anon_write on`* (рис. 46)

```
[root@eavernikovskaya ~]# setsebool ftpd_anon_write on  
[root@eavernikovskaya ~]#
```

Рис. 46: Изменение текущего значения переключателя службы `ftpd_anon_write` с `off` на `on`

Повторно смотрим список переключателей SELinux для службы `ftpd_anon_write`: *getsebool ftpd_anon_write* (рис. 47)

```
[root@eavernikovskaya ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@eavernikovskaya ~]#
```

Рис. 47: Список переключателей SELinux для службы `ftpd_anon_write`

Посмотрим список переключателей с пояснением: *semanage boolean -l | grep ftpd_anon*. Мы видим, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена (рис. 48)

```
[root@eavernikovskaya ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (on , off) Allow ftpd to anon write
[root@eavernikovskaya ~]#
```

Рис. 48: Список переключателей с пояснением для службы ftpd_anon_write (1)

Изменим постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`: `setsebool -P ftpd_anon_write on` (рис. 49)



```
[root@eavernikovskaya ~]# setsebool -P ftpd_anon_write on
[root@eavernikovskaya ~]#
```

Рис. 49: Изменение постоянного значения переключателя для службы `ftpd_anon_write` с `off` на `on`

Снова посмотрим список переключателей: *semanage boolean -l | grep ftpd_anon*.
Теперь постоянная настройка включена (рис. 50)

```
[root@eavernikovskaya ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (on , on) Allow ftpd to anon write
[root@eavernikovskaya ~]#
```

Рис. 50: Список переключателей с пояснением для службы ftpd_anon_write (2)

Подведение итогов

В ходе выполнения лабораторной работы мы получили навыки и работы с контекстом безопасности и политиками SELinux

1. Лабораторная работа №9 [Электронный ресурс] URL:
https://esystem.rudn.ru/pluginfile.php/2400723/mod_resource/content/4/010-selinux.pdf