

Отчет по лабораторной работе 9

Генералов Даниил, НПИбд-01-21, 1032202280

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	18
5	Контрольные вопросы	19

Список иллюстраций

3.1	sestatus	8
3.2	getenforce	9
3.3	selinux-autorelabel	9
3.4	restorecon	10
3.5	dnf	11
3.6	DocumentRoot	12
3.7	lynx	13
3.8	semanage	14
3.9	dnf	15
3.10	curl	16
3.11	setsebool	17
5.1	setenforce	19
5.2	getsebool	20
5.3	audit2why	21
5.4	semanage	22
5.5	/var/log/audit/audit.log	23
5.6	semanage fcontext	24
5.7	ausearch	24

Список таблиц

1 Цель работы

В рамках этой лабораторной работы требуется выполнить операции по управлению SELinux.

2 Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов веб- службы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

3 Выполнение лабораторной работы

Сначала я проверил текущую конфигурацию SELinux. Я увидел, что:

- SELinux включен
- Виртуальная файловая система SELinux находится по адресу `/sys/fs/selinux`
- корень настроек SELinux находится по адресу `/etc/selinux`
- текущая политика SELinux называется `targeted`
- текущий режим SELinux называется `enforcing`
- режим, прописанный в `config-file` – `enforcing`
- Multi-Layer Security включен
- политика для запрещения доступа к объектам неизвестных категорий разрешена
- проверка безопасности памяти включена
- ядро поддерживает версии политик до 33

После этого я переключил SELinux из режима `Enforcing` в `Permissive`.

```

Rocky Linux 9.0 (Blue Onyx)
Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64

dmgeneralov login: root
Password:
Last login: Sat Dec  3 14:02:57 on tty1
[root@dmgeneralov ~]# 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_tty_device_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@dmgeneralov ~]# getenforce
Enforcing
[root@dmgeneralov ~]# setenforce 0
[root@dmgeneralov ~]# getenforce
Permissive
[root@dmgeneralov ~]#

```

Рис. 3.1: sestatus

Затем я выключил SELinux в файле настройки /etc/sysconfig/selinux и перезагрузил систему, после чего getenforce показывает, что SELinux не только Permissive, но и Disabled.


```
Rocky Linux 9.0 (Blue Onyx)
Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64

dmgeneralov login: root
Password:
Last login: Sat Dec 10 09:56:02 on tty1
[root@dmgeneralov ~]# getenforce
Disabled
[root@dmgeneralov ~]# setenforce 1
setenforce: SELinux is disabled
[root@dmgeneralov ~]#
```

Рис. 3.2: getenforce

После еще одного изменения и перезагрузки система сначала сделала повторное создание меток SELinux, а затем после перезагрузки SELinux был опять включен.

```
[ 5.547632] lpc_ich 0000:00:1f.0: I/O space for GPIO uninitialized
[ 5.556449] input: PC Speaker as /devices/platform/pcspkr/input/input5
[ 5.557761] i801_smbus 0000:00:1f.3: SMBus using PCI interrupt
Starting Relabel all filesystems...
[ 5.592387] i2c i2c-0: 1/1 memory slots populated (from DMI)
[ 5.594696] i2c i2c-0: Memory type 0x07 not supported yet, not instantiating
SPD
[ 5.610644] audit: type=1404 audit(1678656005.126:7): enforcing=0 old_enforci
ng=1 audit=4294967295 ses=4294967295 enabled=1 old-enabled=1 lsavselinux res=1
[ 5.571485] selinux-autorelabel[681]: *** Warning -- SELinux targeted policy
relabel is required.
[ 5.572423] selinux-autorelabel[681]: *** Relabeling could take a very long t
ime, depending on file
[ 5.573194] selinux-autorelabel[681]: *** system size and speed of hard drive
s.
[ 5.655206] [drm] pci: virtio-vga detected at 0000:00:01.0
[ 5.658224] virtio-pci 0000:00:01.0: vgaarb: deactivate vga console
[ 5.703266] Console: switching to colour dummy device 80x25
[ 5.703649] [drm] features: -virgl +edid -resource_blob -host_visible
[ 5.716642] [drm] number of scanouts: 1
[ 5.716659] [drm] number of cap sets: 0
[ 5.719311] [drm] Initialized virtio_gpu 0.1.0 0 for virtio0 on minor 0
[ 5.743366] RAPL PMU: API unit is 2^-32 Joules, 8 fixed counters, 18737418240
ms overflow timer
[ 5.755913] Console: switching to colour frame buffer device 160x50
[ 5.792245] virtio_gpu virtio0: [drm] fb0: virtio_gpu frame buffer device
[ 5.800286] snd_hda_codec_generic hdaudioC8D0: autoconfig for Generic: line_outs=1 (0x3/0x0/0x0/0x0/0x0) type:line
[ 5.800430] snd_hda_codec_generic hdaudioC8D0: speaker_outs=0 (0x0/0x0/0x0/0x0/0x0)
[ 5.800477] snd_hda_codec_generic hdaudioC8D0: hp_outs=0 (0x0/0x0/0x0/0x0/0x0)
[ 5.800514] snd_hda_codec_generic hdaudioC8D0: mono_out=0x0
[ 5.800546] snd_hda_codec_generic hdaudioC8D0: inputs:
[ 5.800591] snd_hda_codec_generic hdaudioC8D0: Line=0x5
[ OK ] Started /usr/sbin/lvm vgchange -any --autoactivation event rl.
[ 5.930200] iTCO_vendor_support: vendor-support=0
[ 5.951529] iTCO_wdt iTCO_wdt.1.auto: Found a ICH9 TCO device (Version=2, TCOBASE=0x0660)
[ 5.954056] iTCO_wdt iTCO_wdt.1.auto: Initialized. heartbeat=30 sec (nowayout=0)
[ OK ] Reached target Sound Card.
[ 6.140202] intel_pmc_core intel_pmc_core.0: initialized
[ 19.091341] selinux-autorelabel[686]: Relabeling /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kernel
/debug /sys/kernel/tracing
```

Рис. 3.3: selinux-autorelabel

Затем я посмотрел, как изменяется контекст файла /etc/hosts: сначала он был в контексте net_conf_t, затем я скопировал его в /root и он стал admin_home_t, а затем я скопировал его обратно и использовал restorecon, чтобы вернуть его

B net_conf_t.

```
Rocky Linux 9.0 (Blue Onyx)
Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64

dmgeneralov login: root
Password:
Last login: Sat Dec 10 10:04:25 on tty1
[root@dmgeneralov ~]# getenforce
Enforcing
[root@dmgeneralov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@dmgeneralov ~]# cp /etc/hosts ~
[root@dmgeneralov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@dmgeneralov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@dmgeneralov ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@dmgeneralov ~]# 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@dmgeneralov ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@dmgeneralov ~]# _
```

Рис. 3.4: restorecon

Я создал /web/index.html и поставил httpd и lynx.

```

[root@dmgeneralov ~]# dnf -y install lynx httpd
Rocky Linux 9 - BaseOS
Rocky Linux 9 - BaseOS
Rocky Linux 9 - AppStream
Rocky Linux 9 - AppStream
Rocky Linux 9 - Extras
Rocky Linux 9 - Extras
Package httpd-2.4.53-7.el9.x86_64 is already installed.
Dependencies resolved.
=====
Package                        Architecture                Version
=====
Installing:
  lynx                          x86_64                       2.8.9-19.el9

Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-19.el9.x86_64.rpm
=====
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :
  Installing     : lynx-2.8.9-19.el9.x86_64
  Running scriptlet: lynx-2.8.9-19.el9.x86_64
  Verifying      : lynx-2.8.9-19.el9.x86_64

Installed:
  lynx-2.8.9-19.el9.x86_64

Complete!
[root@dmgeneralov ~]# mkdir /web
[root@dmgeneralov ~]# echo "Welcome to my web-server" > /web/index.html
[root@dmgeneralov ~]#

```

Рис. 3.5: dnf

Я дал разрешение на использование /web как корня сервера.

```

<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/web_"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    # AllowOverride None
    # # Allow open access:
    # Require all granted
</Directory>

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

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
"/etc/httpd/conf/httpd.conf" 364L, 12104B written

```

Рис. 3.6: DocumentRoot

Видно, что доступна страница по умолчанию с кодом 403. Значит, SELinux не разрешает серверу открывать /web.

```
HTTP Server Test Page HTTP Server Test Page powered by: Rocky Linux

This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky Linux system. If you can read this page, it
means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or could be going through maintenance.

If you would like the let the administrators of this website know that you've seen this page instead of the page you've expected, you should send them
an email. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:

The Rocky Linux distribution is a stable and reproducible platform based on the sources of Red Hat Enterprise Linux (RHEL). With this in mind, please
understand that:
  * Neither the Rocky Linux Project nor the Rocky Enterprise Software Foundation have anything to do with this website or its content.
  * The Rocky Linux Project nor the RESF have "hacked" this webserver: This test page is included with the distribution.

For more information about Rocky Linux, please visit the Rocky Linux website.

I am the admin, what do I do?

You may now add content to the webroot directory for your software.

For systems using the Apache Webserver: You can add content to the directory /var/www/html/. Until you do so, people visiting your website will see
this page. If you would like this page to not be shown, follow the instructions in: /etc/httpd/conf.d/welcome.conf.

For systems using Nginx: You can add your content in a location of your choice and edit the root configuration directive in /etc/nginx/nginx.conf.
[ Powered by Rocky Linux ] [poweredby.png]

Apache® is a registered trademark of the Apache Software Foundation in the United States and/or other countries.
NGINX® is a registered trademark of FS Networks, Inc..

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
Back, Forward, Reload, G, W, S, O, P, Q, C, E, H, L, F, B, A, K, I, N, G, T, O, P, S, T, A, T, U, S, I, N, G, L, I, N, K, S
```

Рис. 3.7: lynx

Я попытался изменить контекст с помощью semanage, но эта программа не доступна.

```

Commands: Use arrow keys to move; ? for help; q to quit; < to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.

Exiting via interrupt: 2

[root@dmgeneralov ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
-bash: semanage: command not found
[root@dmgeneralov ~]# setenforce 0
[root@dmgeneralov ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
-bash: semanage: command not found
[root@dmgeneralov ~]# /sbin/sem
-bash: /sbin/sem: No such file or directory
[root@dmgeneralov ~]# /sbin/semodule
At least one mode must be specified.
usage: /sbin/semodule [option]... MODE...
Manage SELinux policy modules.
MODES:
  -R, --reload           reload policy
  -B, --build            build and reload policy
  -D, --disable_dontaudit Remove dontaudits from policy
  -i, --install=MODULE_PKG install a new module
  -r, --remove=MODULE_NAME remove existing module at desired priority
  -l[KIND], --list-modules[=KIND] display list of installed modules
                                KIND: standard list highest priority, enabled modules
                                      full list all modules
  -X, --priority=PRIORITY set priority for following operations (1-999)
  -e, --enable=MODULE_NAME enable module
  -d, --disable=MODULE_NAME disable module
  -E, --extract=MODULE_NAME extract module
Options:
  -s, --store            name of the store to operate on
  -N, -n, --noreload    do not reload policy after commit
  -h, --help            print this message and quit
  -v, --verbose         be verbose
  -P, --preserve_tunables Preserve tunables in policy
  -C, --ignore-module-cache Rebuild CIL modules compiled from HLL files
  -p, --path            use an alternate path for the policy root
  -S, --store-path      use an alternate path for the policy store root
  -c, --cil extract module as cil. This only affects module extraction.
  -H, --hll extract module as hll. This only affects module extraction.
  -m, --checksum        print module checksum (SHA256).
  --rebuild-if-modules-changed
                        force policy rebuild if module content changed since
                        last rebuild (based on checksum)
[root@dmgeneralov ~]# dnf install semanage
Last metadata expiration check: 0:05:09 ago on Sat 10 Dec 2022 10:20:22 AM MSK.
No match for argument: semanage
Error: Unable to find a match: semanage
[root@dmgeneralov ~]#

```

Рис. 3.8: semanage

Как оказалось, нужно установить пакет `polycoreutils-python-utils`.

```
root@dmgeneralov ~]# dnf provides semanage
Last metadata expiration check: 0:06:54 ago on Sat 10 Dec 2022 10:20:22 AM MSK.
policycoreutils-python-utils-3.4-4.el9.noarch : SELinux policy core python utilities
Repo      : appstream
Matched from:
Filename   : /usr/sbin/semanage

root@dmgeneralov ~]# yay policycoreutils-python-utils
-bash: yay: command not found
root@dmgeneralov ~]# dnf install policycoreutils-python-utils
Last metadata expiration check: 0:07:20 ago on Sat 10 Dec 2022 10:20:22 AM MSK.
Dependencies resolved.
=====
Package                                Architecture      Version            Repository          Size
=====
Installing:
policycoreutils-python-utils          noarch            3.4-4.el9          appstream            69 k
Upgrading:
audit                                  x86_64            3.0.7-103.el9      baseos               252 k
audit-libs                            x86_64            3.0.7-103.el9      baseos               116 k
libselinux                            x86_64            3.4-3.el9          baseos                85 k
libselinux-utils                      x86_64            3.4-3.el9          baseos               159 k
libsemanage                           x86_64            3.4-2.el9          baseos               118 k
libsepol                              x86_64            3.4-1.1.el9        baseos               315 k
policycoreutils                      x86_64            3.4-4.el9          baseos               282 k
python3-libselinux                   x86_64            3.4-3.el9          appstream            105 k
Installing dependencies:
checkpolicy                           x86_64            3.4-1.el9          appstream            346 k
python3-audit                         x86_64            3.0.7-103.el9      appstream             83 k
python3-libsemanage                  x86_64            3.4-2.el9          appstream             80 k
python3-policycoreutils              noarch            3.4-4.el9          appstream             2.0 M
python3-setools                      x86_64            4.4.0-5.el9        baseos                546 k
python3-setuptools                   noarch            53.0.0-10.el9      baseos                841 k
=====
Transaction Summary
=====
Install 7 Packages
Upgrade 8 Packages

Total download size: 5.4 M
Is this ok [y/N]: _
```

Рис. 3.9: dnf

После этого изменения веб-сервер начал выдавать нужную страницу.

```

<p><strong>For systems using
<a href="https://nginx.org">Nginx</strong></a>:
You can add your content in a location of your
choice and edit the <code>root</code> configuration directive
in <code>/etc/nginx/nginx.conf</code>.</p>

<div id="logos">
  <a href="https://rockylinux.org/" id="rocky-poweredby"></a> <!-- Rocky -->
   <!-- webserver -->
</div>
</div>

<footer class="col-sm-12">
  <a href="https://apache.org">Apache</a> is a registered trademark of <a href="https://apache.org">the Apache Software Foundation</a> in the United
  States and/or other countries.<br />
  <a href="https://nginx.org">NGINX</a> is a registered trademark of <a href="https://">F5 Networks, Inc.</a>.
</footer>

</body>
</html>
[root@dmgeneralov ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
ValueError: File context for /web(/.*)? already defined
[root@dmgeneralov ~]# getenforce
Enforcing
[root@dmgeneralov ~]# curl localhost | head
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left     Speed
100 7620 100 7620    0     0   372k    0 --:--:-- --:--:-- --:--:--   372k
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /*<![CDATA[*/
    {
      html {
[root@dmgeneralov ~]# ^C
[root@dmgeneralov ~]# 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@dmgeneralov ~]# curl localhost | head
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left     Speed
100   25 100   25    0     0   2777    0 --:--:-- --:--:-- --:--:--   2777
Welcome to my web-server
[root@dmgeneralov ~]#

```

Рис. 3.10: curl

Наконец, я посмотрел на флаги настройки SELinux для ftpd. Я увидел, что раньше ftpd_anon_write был выключен, а затем я изменил его с помощью setsebool -P, что изменило как его текущую настройку, так и перманентную настройку. Это можно увидеть по тому, что в semanage boolean оба параметра указаны on.


```

[root@dmgeneralov ~]# 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@dmgeneralov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@dmgeneralov ~]# setsebool -P ftpd_anon_write on
[ 1491.644664] SELinux: Converting 358 SID table entries...
[ 1491.653714] SELinux: policy capability network_peer_controls=1
[ 1491.653745] SELinux: policy capability open_perms=1
[ 1491.653757] SELinux: policy capability extended_socket_class=1
[ 1491.653770] SELinux: policy capability always_check_network=0
[ 1491.653783] SELinux: policy capability cgroup_seclabel=1
[ 1491.653795] SELinux: policy capability nnp_nosuid_transition=1
[ 1491.653808] SELinux: policy capability genfs_seclabel_symlinks=0
[root@dmgeneralov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
[root@dmgeneralov ~]#

```

Рис. 3.11: setsebool

4 Выводы

Я получил опыт работы с SELinux.

5 Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

setenforce 0

```
Rocky Linux 9.0 (Blue Onyx)
Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64

dmgeneralov login: root
Password:
Last login: Sat Dec  3 14:02:57 on tty1
[root@dmgeneralov ~]# 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

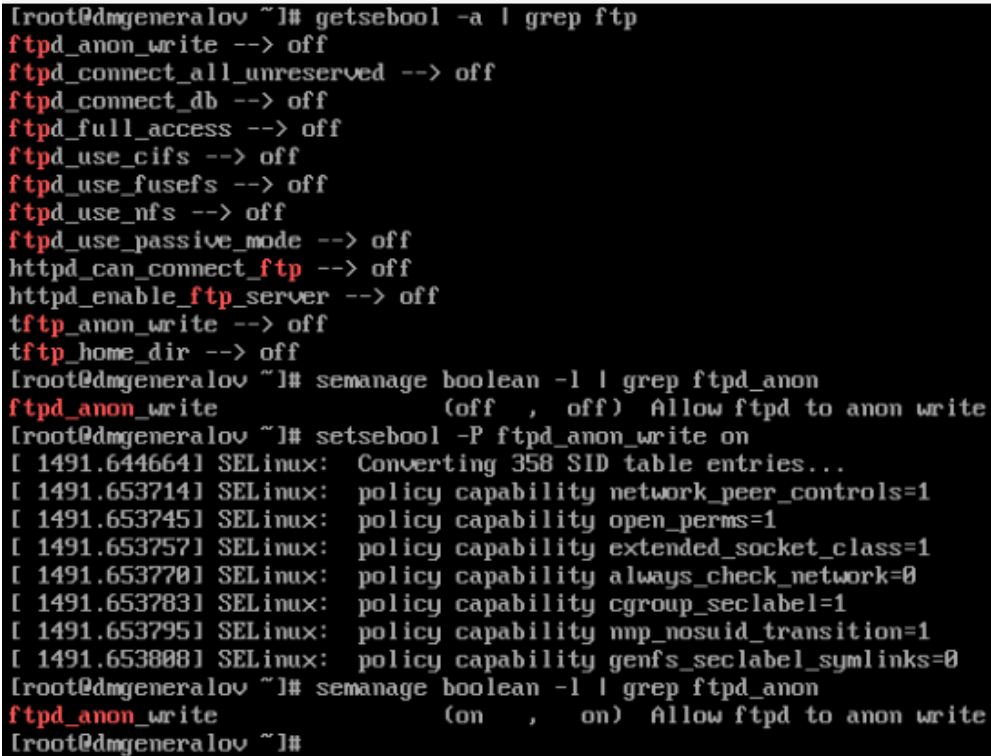
Process contexts:
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                 system_u:system_r:init_t:s0
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:        unconfined_u:object_r:user_tty_device_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@dmgeneralov ~]# getenforce
Enforcing
[root@dmgeneralov ~]# setenforce 0
[root@dmgeneralov ~]# getenforce
Permissive
[root@dmgeneralov ~]#
```

Рис. 5.1: setenforce

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

`getsebool -a`



```
[root@dmgeneralov ~]# 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@dmgeneralov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@dmgeneralov ~]# setsebool -P ftpd_anon_write on
[ 1491.644664] SELinux: Converting 358 SID table entries...
[ 1491.653714] SELinux: policy capability network_peer_controls=1
[ 1491.653745] SELinux: policy capability open_perms=1
[ 1491.653757] SELinux: policy capability extended_socket_class=1
[ 1491.653770] SELinux: policy capability always_check_network=0
[ 1491.653783] SELinux: policy capability cgroup_seclabel=1
[ 1491.653795] SELinux: policy capability nnp_nosuid_transition=1
[ 1491.653808] SELinux: policy capability genfs_seclabel_symlinks=0
[root@dmgeneralov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
[root@dmgeneralov ~]#
```

Рис. 5.2: getsebool

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

`audit2why`

```

[root@dmgeneralov ~]# ausearch -m avc -l tail -5
-----
time-->Sat Dec 10 10:29:47 2022
type=PROCTITLE msg=audit(1670657387.368:521): proctitle=2F7573722F7362696E2F6674747064002D44464F524547524F554E44
type=SYSCALL msg=audit(1670657387.368:521): arch=c8000000 syscall=262 success=no exit=-13 a0=ffffff9c a1=7f376000a5b0 a2=7f375effc7c0 a3=100 items=0 ppid=2136 p
id=2139 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)
type=AVC msg=audit(1670657387.368:521): avc: denied { getattr } for pid=2139 comm="httpd" path="/web/index.html" dev="dm-0" ino=8986270 scontext=system_u:sys
tem_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0
[root@dmgeneralov ~]# ausearch -m avc -l tail -5 | audit2why
type=AVC msg=audit(1670657387.368:521): avc: denied { getattr } for pid=2139 comm="httpd" path="/web/index.html" dev="dm-0" ino=8986270 scontext=system_u:sys
tem_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0

Was caused by:
    Missing type enforcement (TE) allow rule.

    You can use audit2allow to generate a loadable module to allow this access.

[root@dmgeneralov ~]#
Display all 1192 possibilities? (y or n)_

```

Рис. 5.3: audit2why

4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?

```

semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?" restorecon
-R -v /web

```

```

<p><strong>For systems using
<a href="https://nginx.org">NgInx</strong></a>:
You can add your content in a location of your
choice and edit the <code>root</code> configuration directive
in <code>/etc/nginx/nginx.conf</code>.</p>

<div id="logos">
  <a href="https://rockylinux.org/" id="rocky-poweredby"></a> <!-- Rocky -->
   <!-- webserver -->
</div>
</div>

<footer class="col-sm-12">
  <a href="https://apache.org">Apache</a> is a registered trademark of <a href="https://apache.org">the Apache Software Foundation</a> in the United
  States and/or other countries.<br />
  <a href="https://nginx.org">NGINX</a> is a registered trademark of <a href="https://">F5 Networks, Inc.</a>.
</footer>

</body>
</html>
[root@dmgeneralov ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
ValueError: File context for /web(/.*)? already defined
[root@dmgeneralov ~]# getenforce
Enforcing
[root@dmgeneralov ~]# curl localhost | head
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
             Dload  Upload   Total   Spent    Left   Speed
100  7620 100  7620    0     0   372k    0 --:--:-- --:--:-- --:--:--  372k
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /*<![CDATA[*/
    }
  }
  <html {
[root@dmgeneralov ~]# ^C
[root@dmgeneralov ~]# 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@dmgeneralov ~]# curl localhost | head
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
             Dload  Upload   Total   Spent    Left   Speed
100   25 100   25    0     0   2777    0 --:--:-- --:--:-- --:--:--  2777
Welcome to my web-server
[root@dmgeneralov ~]#

```

Рис. 5.4: semanage

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

/etc/sysconfig/selinux

6. Где SELinux регистрирует все свои сообщения?

/var/log/audit/audit.log


```

[root@dmgeneralov ~]# semanage fcontext -l | grep ftpd
/etc/(x)?inetd\.d/ftptd      regular file      system_u:object_r:ftptd_etc_t:s0
/etc/cron\.monthly/proftpd   regular file      system_u:object_r:ftptd_exec_t:s0
/etc/proftpd\.conf           regular file      system_u:object_r:ftptd_etc_t:s0
/etc/rc\.d/init\.d/proftpd   regular file      system_u:object_r:ftpd_initrc_exec_t:s0
/etc/rc\.d/init\.d/vsftpd     regular file      system_u:object_r:ftpd_initrc_exec_t:s0
/tftpbboot                   directory         system_u:object_r:tftpd_dir_t:s0
/tftpbboot/.*                all files         system_u:object_r:tftpd_dir_t:s0
/usr/bin/ftpd                 regular file      system_u:object_r:publicfile_exec_t:s0
/usr/bin/ftpdctl              regular file      system_u:object_r:ftpdctl_exec_t:s0
/usr/kerberos/sbin/ftpd       regular file      system_u:object_r:ftpd_exec_t:s0
/usr/lib/systemd/system/proftpd.* regular file      system_u:object_r:iptables_unit_file_t:s0
/usr/lib/systemd/system/vsftpd.* regular file      system_u:object_r:iptables_unit_file_t:s0
/usr/libexec/webmin/vsftpd/webalizer/xfer_log regular file      system_u:object_r:xferlog_t:s0
/usr/sbin/atftpd              regular file      system_u:object_r:tftpd_exec_t:s0
/usr/sbin/ftpdwho             regular file      system_u:object_r:ftpd_exec_t:s0
/usr/sbin/in\.ftpd            regular file      system_u:object_r:ftpd_exec_t:s0
/usr/sbin/in\.tftpd           regular file      system_u:object_r:tftpd_exec_t:s0
/usr/sbin/muddleftpd          regular file      system_u:object_r:ftpd_exec_t:s0
/usr/sbin/proftpd             regular file      system_u:object_r:ftpd_exec_t:s0
/usr/sbin/vsftpd              regular file      system_u:object_r:ftpd_exec_t:s0
/var/lib/tftpbboot(/.*)?     all files         system_u:object_r:tftpd_dir_rw_t:s0
/var/lock/subsys/.*.ftpd     regular file      system_u:object_r:ftpd_lock_t:s0
/var/log/muddleftpd\.log.*   regular file      system_u:object_r:xferlog_t:s0
/var/log/proftpd(/.*)?       all files         system_u:object_r:xferlog_t:s0
/var/log/proftpd\.log        regular file      system_u:object_r:xferlog_t:s0
/var/log/vsftpd.*            regular file      system_u:object_r:xferlog_t:s0
/var/run/proftpd.*           all files         system_u:object_r:ftpd_var_run_t:s0
[root@dmgeneralov ~]#

```

Рис. 5.6: semanage fcontext

- Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

ausearch -m avc

```

[root@dmgeneralov ~]# ausearch -m avc | tail -5
----
time-->Sat Dec 18 10:29:47 2022
type=PROCTITLE msg=audit(1678657387.368:521): proctitle=2F7573722F73626962F6874747064002D44464F524547524F554E44
type=SYSCALL msg=audit(1678657387.368:521): arch=c800003e syscall=262 success=no exit=-13 a0=ffffffffffc a1=7f376880a5b0 a2=7f375effc7e0 a3=100 items=0 ppid=2136 p
id=2139 auid=4294967295 uid=40 gid=40 euid=40 suid=40 fsuid=40 egid=40 sgid=40 fsgid=40 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system
_u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1678657387.368:521): avc: denied (getattr) for pid=2139 comm="httpd" path="/web/index.html" dev="dm-0" ino=8986270 scontext=system_u:sys
tem_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0
[root@dmgeneralov ~]# ausearch -m avc | tail -5 | audit2why
type=AVC msg=audit(1678657387.368:521): avc: denied (getattr) for pid=2139 comm="httpd" path="/web/index.html" dev="dm-0" ino=8986270 scontext=system_u:sys
tem_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0

Was caused by:
Missing type enforcement (TE) allow rule.

You can use audit2allow to generate a loadable module to allow this access.

[root@dmgeneralov ~]#
Display all 1192 possibilities? (y or n)_

```

Рис. 5.7: ausearch