

Отчет по лабораторной работе №9

Управление SELinux

Сидорова Арина Валерьевна

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Управление режимами SELinux	5
2.2	Использование restorecon для восстановления контекста безопасности	8
2.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	9
2.4	Работа с переключателями SELinux	12
3	Ответы на контрольные вопросы	14
4	Выводы	15

Список иллюстраций

2.1	getenforce	5
2.2	SELINUX=disabled	6
2.3	SELinux теперь отключён	6
2.4	SELINUX=enforcing	7
2.5	sestatus -v	8
2.6	Использование restorecon для восстановления контекста безопасности	9
2.7	Установим необходимое программное обеспечение	9
2.8	mkdir /web; touch index.html	10
2.9	Редактируем файл	10
2.10	start; enable	11
2.11	веб-страница Red Hat	11
2.12	Применим новую метку и восстановим контекст безопасности	12
2.13	Welcome to my web-server	12
2.14	Работа с переключателями SELinux	13

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

2.1 Управление режимами SELinux

Просмотрим текущую информацию о состоянии SELinux: `sestatus -v`

Посмотрим, в каком режиме работает SELinux: `getenforce`

Изменим режим работы SELinux на разрешающий `setenforce 0` и снова введем `getenforce` (рис. 2.1)

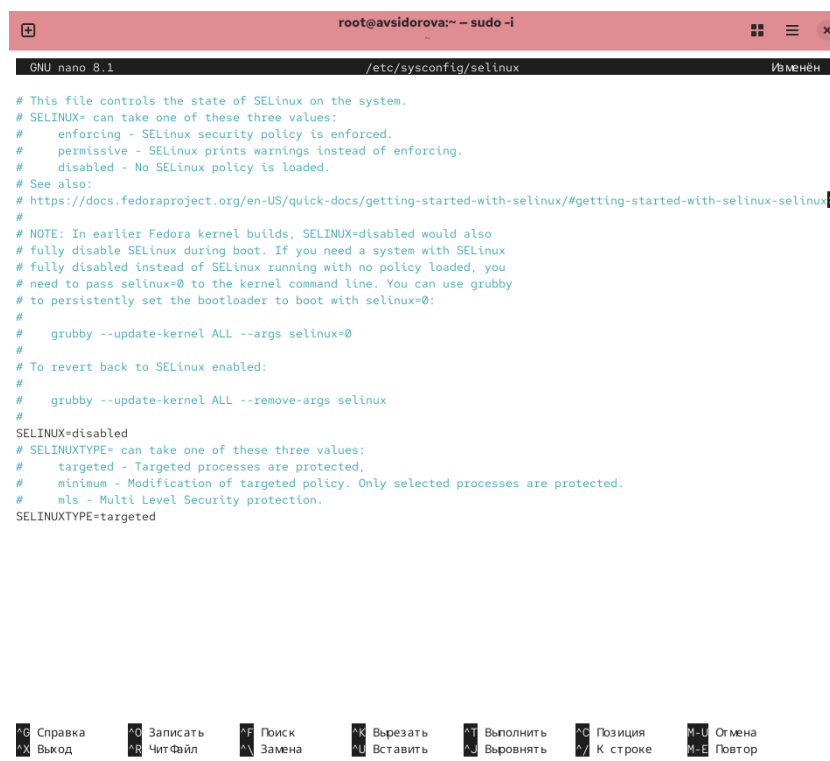
```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
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@avsidorova:~# getenforce
Enforcing
root@avsidorova:~# setenforce 0
root@avsidorova:~# getenforce
Permissive
root@avsidorova:~# █
```

Рис. 2.1: `getenforce`

В файле `/etc/sysconfig/selinux` с помощью редактора установим `SELINUX=disabled`
Перезагрузим систему (рис. 2.2)



```
root@avsidorova:~ - sudo -i
GNU nano 8.1 /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

Справка  Записать  Поиск  Вырезать  Выполнить  Позиция  Отмена
Выход  ЧитФайл  Замена  Вставить  Выровнять  К строке  Повтор
```

Рис. 2.2: SELINUX=disabled

Посмотрим статус SELinux: `getenforce` SELinux теперь отключён.

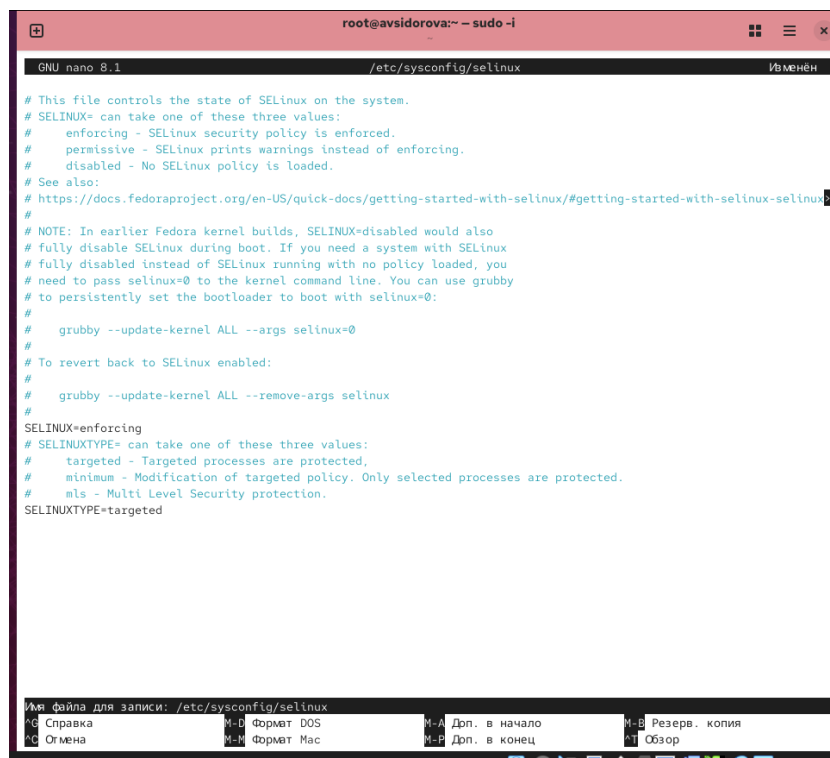
Попробуем переключить режим работы SELinux: `setenforce 1` Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы. (рис. 2.3)



```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# getenforce
Disabled
root@avsidorova:~# setenforce 1
setenforce: SELinux is disabled
root@avsidorova:~#
```

Рис. 2.3: SELinux теперь отключён

Откроем файл `/etc/sysconfig/selinux` с помощью редактора и установим: `SELINUX=enforcing` Перезагрузим систему. (рис. 2.4)



```
GNU nano 8.1 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
#   https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 2.4: `SELINUX=enforcing`

После перезагрузки в терминале с полномочиями администратора посмотрим текущую информацию о состоянии SELinux: `sestatus -v` (рис. 2.5)

```

avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# 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@avsidorova:~#

```

Рис. 2.5: sestatus -v

2.2 Использование restorecon для восстановления контекста безопасности

Посмотрим контекст безопасности файла /etc/hosts. У файла есть метка контекста net_conf_t.

Скопируем файл /etc/hosts в домашний каталог. Проверим контекст файла ~/hosts.

Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin_home_t.

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: mv ~/hosts /etc Убедимся, что тип контекста по-прежнему установлен на admin_home_t.

Исправим контекст безопасности.

Убедимся, что тип контекста изменился: ls -Z /etc/hosts

Для массового исправления контекста безопасности на файловой системе

введем touch /.autorelabel (рис. 2.6)

```
root@avsidorova:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@avsidorova:~# cp /etc/hosts ~/
root@avsidorova:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@avsidorova:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'? да
root@avsidorova:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@avsidorova:~# 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@avsidorova:~# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@avsidorova:~# touch /.autorelabel
root@avsidorova:~#
```

Рис. 2.6: Использование restorecon для восстановления контекста безопасности

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Установим необходимое программное обеспечение (рис. 2.7)

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# dnf -y install httpd
Rocky Linux 10 - BaseOS                               5.3 kB/s | 4.3 kB  00:00
Rocky Linux 10 - BaseOS                               1.6 MB/s | 22 MB  00:14
Rocky Linux 10 - AppStream                             11 kB/s | 4.3 kB  00:00
Rocky Linux 10 - AppStream                             1.7 MB/s | 2.2 MB  00:01
Rocky Linux 10 - Extras                                6.0 kB/s | 3.1 kB  00:00
Rocky Linux 10 - Extras                                6.5 kB/s | 5.5 kB  00:00
Пакет httpd-2.4.63-1.el10_0.2.x86_64 уже установлен.
Зависимости разрешены.
Нет действий для выполнения.
Выполнено!
root@avsidorova:~# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:30 назад, Вт 28 окт 2025 16:15:00.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Резепозиторий  Размер
=====
Установка:
lynx       x86_64       2.9.0-6.el10      appstream      1.6 М
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.6 М
Объем изменений: 6.0 М
Загрузка пакетов:
lynx-2.9.0-6.el10.x86_64.rpm                1.4 MB/s | 1.6 MB  00:01
-----
Общий размер                                1.1 MB/s | 1.6 MB  00:01
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
Подготовка                                     1/1
Установка      : lynx-2.9.0-6.el10.x86_64      1/1
Запуск скрипта: lynx-2.9.0-6.el10.x86_64      1/1

Установлен:
```

Рис. 2.7: Установим необходимое программное обеспечение

Создадим новое хранилище для файлов web-сервера

Создадим файл `index.html` в каталоге с контентом веб-сервера и поместим в файл следующий текст: `Welcome to my web-server` (рис. 2.8)

```

ДЫПОЛНЕНО:
root@avsidorova:~# mkdir /web
root@avsidorova:~# cd /web
root@avsidorova:/web# touch index.html
root@avsidorova:/web# nano index.html
root@avsidorova:/web# nano /etc/httpd/conf/httpd.conf
root@avsidorova:/web#

```

Рис. 2.8: `mkdir /web; touch index.html`

В файле `/etc/httpd/conf/httpd.conf` закомментируем строку `DocumentRoot "/var/www/html"` и ниже добавим строку `DocumentRoot "/web"`. Затем в этом же файле ниже закомментируем раздел `<Directory "/var/www"> AllowOverride None Require all granted` и добавим следующий раздел, определяющий правила доступа: `<Directory "/web"> AllowOverride None Require all granted` (рис. 2.9).

```
GNU nano 8.1 /etc/httpd/conf/httpd.conf
# 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 "/var/www/html"
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"
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
# http://httpd.apache.org/docs/2.4/mod/core.html#options
# for more information.
#
Options Indexes FollowSymLinks
```

Рис. 2.9: Редактируем файл

Запустим веб-сервер и службу httpd: `systemctl start httpd systemctl enable httpd`
(рис. 2.10)

```
root@avsidorova:/web# systemctl start httpd
root@avsidorova:/web# systemctl enable httpd
root@avsidorova:/web# lynx http://localhost
```

Рис. 2.10: start; enable

В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: `lynx http://localhost`

Мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла `index.html`. (рис. 2.11)

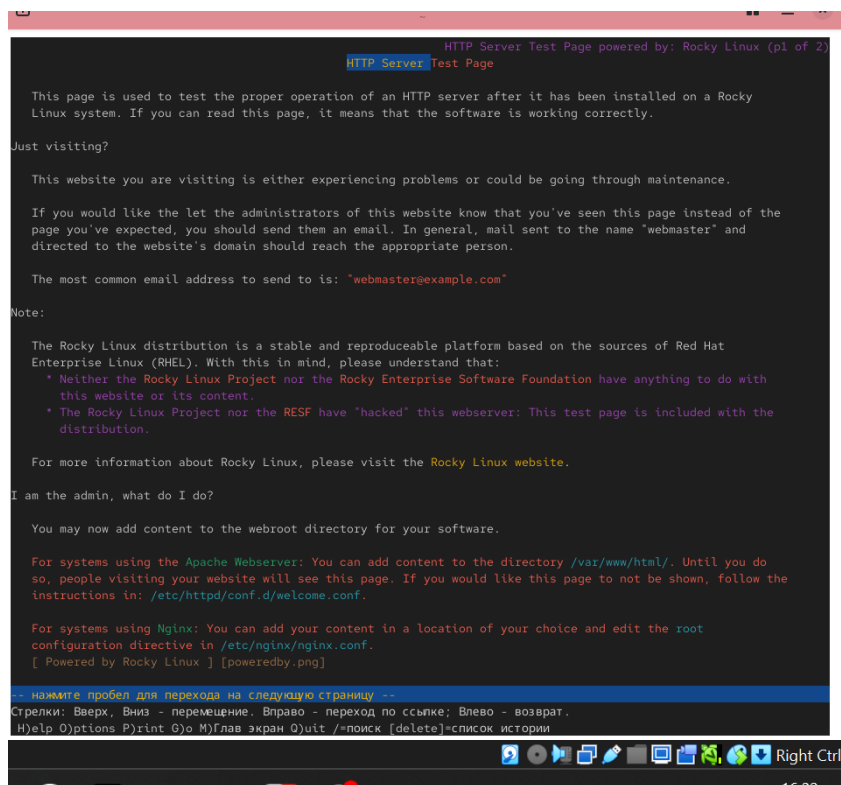


Рис. 2.11: веб-страница Red Hat

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

Восстановим контекст безопасности: `restorecon -R -v /web` (рис. 2.12)

```

root@avsidorova:/web# lynx http://localhost
root@avsidorova:/web# semanage fcontext -a -t httpd_sys_content_t '/web(/.*)?'
root@avsidorova:/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@avsidorova:/web# lynx http://localhost

```

Рис. 2.12: Применим новую метку и восстановим контекст безопасности

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу: `lynx http://localhost` На экране отображена запись «Welcome to my web-server». (рис. 2.13)

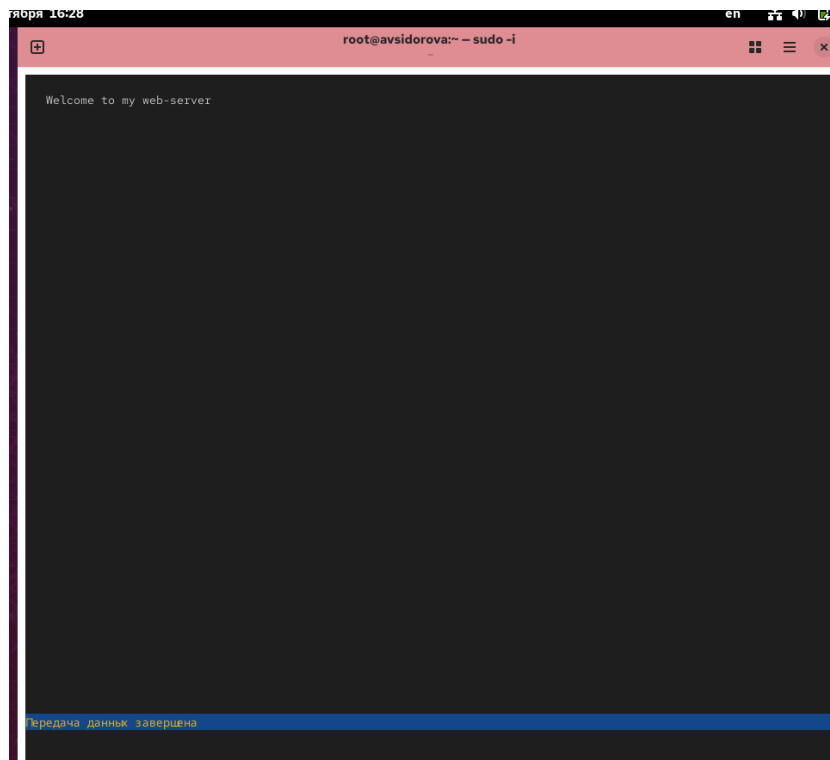


Рис. 2.13: Welcome to my web-server

2.4 Работа с переключателями SELinux

Посмотрим список переключателей SELinux для службы ftp.

Для службы `ftpd_anon` посмотрим список переключателей: `semanage boolean -l | grep ftpd_anon`

Изменим текущее значение переключателя для службы `ftpd_anon_write` с `off` на

on: setsebool ftpd_anon_write on

Повторно посмотрим список переключателей SELinux для службы ftpd_anon_write:
getsebool ftpd_anon_write

Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon Обращим внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Изменим постоянное значение переключателя для службы ftpd_anon_write с off на on: setsebool -P ftpd_anon_write on

Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon (рис. 2.14)

```
root@avsidorova:~#  
root@avsidorova:~# 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@avsidorova:~# semanage boolean -l | grep ftpd_anon  
bash: semanage: команда не найдена...  
root@avsidorova:~# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write  
root@avsidorova:~# setsebool ftpd_anon_write on  
root@avsidorova:~# getsebool ftpd_anon_write  
ftpd_anon_write --> on  
root@avsidorova:~# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write  
root@avsidorova:~# setsebool -P ftpd_anon_write on  
root@avsidorova:~# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write (вкл., вкл.) Allow ftpd to anon write  
root@avsidorova:~#
```

Рис. 2.14: Работа с переключателями SELinux

3 Ответы на контрольные вопросы

1. `setenforce 0`
2. `getsebool -a`
3. `setroubleshoot` или `setroubleshoot-server`
4. `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` затем `restorecon -R /web`
5. `/etc/selinux/config` (параметр `SELINUX=disabled`)
6. `/var/log/audit/audit.log` и `/var/log/messages`
7. `semanage boolean -l | grep ftp` или `getsebool -a | grep ftp`
8. Временно перевести SELinux в режим Permissive (`setenforce 0`) и проверить работу службы

4 Выводы

Получили навыки работы с контекстом безопасности и политиками SELinux.