

Отчёт по лабораторной работе №9

Управление SELinux

Наурузова Айшат Магомедовна

Содержание

1	Цель работы	5
2	Ход выполнения	6
3	Ход выполнения	7
3.1	Управление режимами SELinux	7
3.2	Использование restorecon для восстановления контекста безопасности	11
3.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	13
3.4	Работа с переключателями SELinux	15
4	Контрольные вопросы	17
5	Заключение	20

Список иллюстраций

3.1	Просмотр состояния SELinux	8
3.2	Отключение SELinux в конфигурационном файле	9
3.3	SELinux отключён, попытка включения невозможна	10
3.4	Включение SELinux обратно в enforcing-режиме	10
3.5	Автоматическое восстановление контекста SELinux при перезагрузке	11
3.6	Восстановление контекста файла /etc/hosts	12
3.7	Автоматическое перемаркирование файловой системы	12
3.8	Создание каталога и файла index.html	13
3.9	Изменение конфигурации Apache	14
3.10	Стандартная страница Apache	14
3.11	Применение контекста безопасности SELinux	15
3.12	Корректное отображение пользовательской страницы	15
3.13	Работа с переключателями SELinux для службы FTP	16

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Ход выполнения

3 Ход выполнения

3.1 Управление режимами SELinux

После входа в систему были получены административные права с помощью команды:

```
su -
```

Для проверки текущего состояния SELinux использовалась команда:

```
sestatus -v
```

На экран была выведена подробная информация о политике безопасности:

- **SELinux status:** enabled — SELinux активен.
- **SELinuxfs mount:** /sys/fs/selinux — каталог, где смонтирована файловая система SELinux.
- **SELinux root directory:** /etc/selinux — основной путь для конфигурационных файлов.
- **Loaded policy name:** targeted — используется целевая политика (targeted policy).
- **Current mode:** enforcing — система работает в режиме принудительного контроля доступа.

- **Mode from config file:** enforcing — то же значение прописано в конфигурационном файле.
- **Policy MLS status:** enabled — включена многоуровневая защита (Multi-Level Security).
- **Policy deny_unknown status:** allowed — неизвестные объекты разрешены.
- **Max kernel policy version:** 33 — версия политики ядра Linux.

```

amnauruzova@amnauruzova:~$ su
Password:
root@amnauruzova:/home/amnauruzova# 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@amnauruzova:/home/amnauruzova# getenforce
Enforcing
root@amnauruzova:/home/amnauruzova# setenforce 0
root@amnauruzova:/home/amnauruzova# getenforce
Permissive
root@amnauruzova:/home/amnauruzova#

```

Рис. 3.1: Просмотр состояния SELinux

Для просмотра текущего режима работы SELinux введена команда:

`getenforce`

Результат — **Enforcing**, что подтверждает активный режим безопасности.

Далее режим был изменён на разрешающий (Permissive):

`setenforce 0`

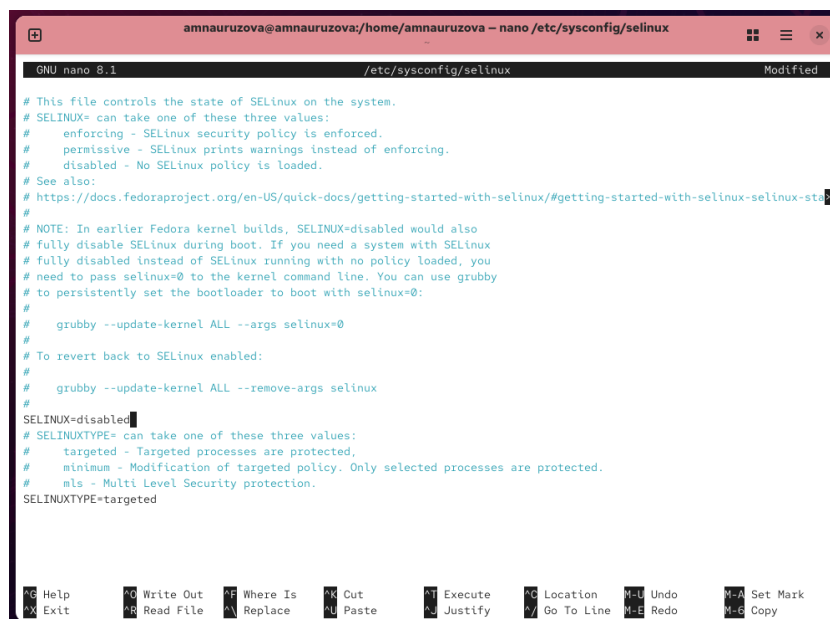
После повторной проверки (`getenforce`) статус изменился на **Permissive**, что

означает: SELinux теперь не блокирует действия, но записывает предупреждения.

Затем в конфигурационном файле `/etc/sysconfig/selinux` с помощью текстового редактора **nano** было изменено значение параметра:

`SELINUX=disabled`

и сохранены изменения.



```
GNU nano 2.9.1 /etc/sysconfig/selinux Modified
# 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-state
#
# 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

^G Help      ^O Write Out ^R Where Is  ^K Cut       ^T Execute  ^C Location ^U Undo     ^M Set Mark
^X Exit      ^B Read File ^\ Replace  ^N Paste     ^_ Justify  ^G Go To Line ^E Redo    ^Y Copy
```

Рис. 3.2: Отключение SELinux в конфигурационном файле

После перезагрузки системы и повторного входа под пользователем **root** команда `getenforce` показала:

`Disabled`

Попытка принудительно включить SELinux (`setenforce 1`) завершилась сообщением:

`setenforce: SELinux is disabled`

Это означает, что при отключённом состоянии невозможно изменить режим без перезапуска системы.

```

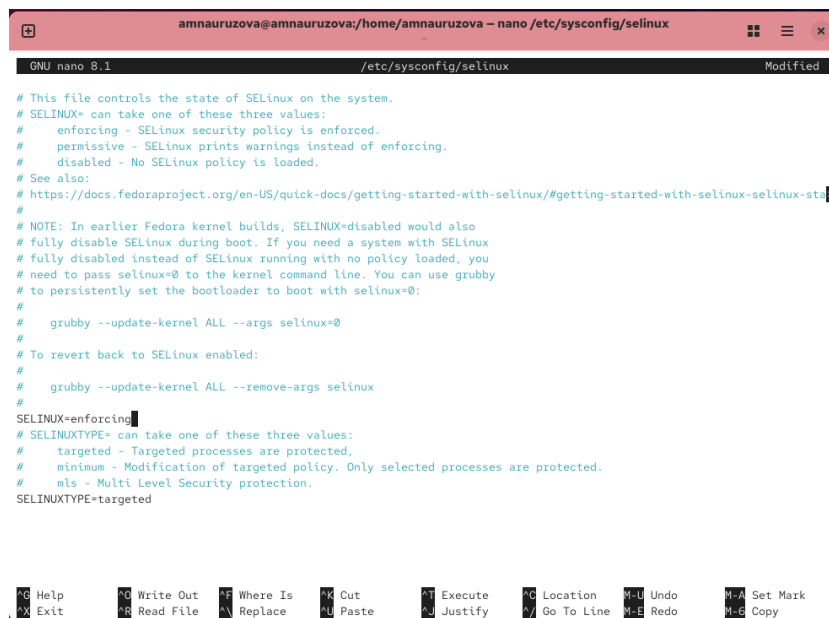
amnauruzova@amnauruzova:~$ su
Password:
root@amnauruzova:/home/amnauruzova# getenforce
Disabled
root@amnauruzova:/home/amnauruzova# setenforce 1
setenforce: SELinux is disabled
root@amnauruzova:/home/amnauruzova# █

```

Рис. 3.3: SELinux отключён, попытка включения невозможна

Для повторного включения SELinux в файл `/etc/sysconfig/selinux` было возвращено значение:

`SELINUX=enforcing`



```

GNU nano 8.1 /etc/sysconfig/selinux Modified

# 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-state
#
# 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

⌘ Help  ⌘ Write Out  ⌘ Where Is  ⌘ Cut  ⌘ Execute  ⌘ Location  ⌘ Undo  ⌘ Set Mark
⌘ Exit  ⌘ Read File  ⌘ Replace  ⌘ Paste  ⌘ Justify  ⌘ Go To Line  ⌘ Redo  ⌘ Copy

```

Рис. 3.4: Включение SELinux обратно в enforcing-режиме

После перезагрузки система начала автоматическое восстановление меток SELinux, что подтверждают сообщения службы **selinux-autorelabel.service**:

Warning – SELinux targeted policy relabel is required.

Relabeling could take a very long time, depending on system size and speed.

Процесс завершился корректно.

```
[ OK ] Reached target sysinit.target - System Initialization.
[ OK ] Started alsa-state.service - Manage Sound Card State (restore and store).
[ OK ] Reached target sound.target - Sound Card.
Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
Starting selinux-autorelabel.service - Relabel all filesystems...
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
[ 6.118278] selinux-autorelabel(827): *** Warning -- SELinux targeted policy relabel is required.
[ 6.119651] selinux-autorelabel(827): *** Relabeling could take a very long time, depending on file
[ 6.119240] selinux-autorelabel(827): *** system size and speed of hard drives.
[ 6.121146] selinux-autorelabel(827): Running: /sbin/fixfiles -T 0 restore
[ 9.273428] selinux-autorelabel(834): Warning: Skipping the following R/O filesystems:
[ 9.274136] selinux-autorelabel(834): /run/credentials/systemd-journald.service
[ 9.274929] selinux-autorelabel(834): Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /s
l/debug /sys/kernel/tracing
```

Рис. 3.5: Автоматическое восстановление контекста SELinux при перезагрузке

Повторная проверка состояния SELinux (`sestatus -v`) показала, что система снова работает в режиме **Enforcing** и политика безопасности применяется корректно.

3.2 Использование `restorecon` для восстановления контекста безопасности

После входа с правами администратора была просмотрена метка контекста файла `/etc/hosts`:

```
ls -Z /etc/hosts
```

Результат показал тип контекста **net_conf_t** — это корректная метка для сетевых конфигурационных файлов.

Далее файл был скопирован в домашний каталог:

```
cp /etc/hosts ~/
```

Повторная проверка (`ls -Z ~/hosts`) показала, что у новой копии контекст изменился на **admin_home_t**, поскольку копирование в домашний каталог создаёт файл с меткой, соответствующей окружению пользователя.

После этого файл был перемещён обратно в каталог `/etc`:

```
mv ~/hosts /etc
```

Теперь `/etc/hosts` имел контекст **admin_home_t**, что некорректно для данного пути.

Для восстановления правильной метки был применён инструмент **restorecon**:

```
restorecon -v /etc/hosts
```

Результат вывода подтвердил изменение контекста обратно на **net_conf_t**:

Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_c

```
root@amnauruzova:/home/amnauruzova#  
root@amnauruzova:/home/amnauruzova# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
root@amnauruzova:/home/amnauruzova# cp /etc/hosts ~/  
root@amnauruzova:/home/amnauruzova# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
root@amnauruzova:/home/amnauruzova# mv ~/hosts /etc  
mv: overwrite '/etc/hosts'? y  
root@amnauruzova:/home/amnauruzova# ls -Z /etc/hosts  
unconfined_u:object_r:admin_home_t:s0 /etc/hosts  
root@amnauruzova:/home/amnauruzova# 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@amnauruzova:/home/amnauruzova# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
root@amnauruzova:/home/amnauruzova# touch /.autorelabel  
root@amnauruzova:/home/amnauruzova#
```

Рис. 3.6: Восстановление контекста файла /etc/hosts

Для массового восстановления контекстов безопасности на всей файловой системе была выполнена команда:

```
touch /.autorelabel
```

и произведена перезагрузка системы.

Во время запуска служба **selinux-autorelabel.service** автоматически провела полную перемаркировку файлов, о чём свидетельствуют соответствующие сообщения:

Warning – SELinux targeted policy relabel is required.

Relabeling could take a very long time...

```
Starting systemd-tmpfiles-setup.service - Create System Files and Directories...  
[ OK ] Finished plymouth-read-write.service - Tell Plymouth To Write Out Runtime Data.  
[ OK ] Finished systemd-tmpfiles-setup.service - Create System Files and Directories.  
Starting systemd-update-utmp.service - Record System Boot/Shutdown in UTMP...  
[ OK ] Finished systemd-update-utmp.service - Record System Boot/Shutdown in UTMP.  
[ OK ] Reached target sysinit.target - System Initialization.  
[ OK ] Startedalsa-state.service - Manage Sound Card State (restore and store).  
[ OK ] Reached target sound.target - Sound Card.  
Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...  
Starting selinux-autorelabel.service - Relabel all filesystems...  
[ OK ] Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.  
[ 5.569544] selinux-autorelabel[831]: *** Warning -- SELinux targeted policy relabel is required.  
[ 5.571871] selinux-autorelabel[831]: *** Relabeling could take a very long time, depending on file  
[ 5.571241] selinux-autorelabel[831]: *** system size and speed of hard drives.  
[ 5.571858] selinux-autorelabel[831]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 3.7: Автоматическое перемаркирование файловой системы

После завершения загрузки SELinux функционировал в штатном режиме, а все контексты безопасности были восстановлены.

3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

После получения административных прав было установлено необходимое программное обеспечение для работы веб-сервера Apache и текстового браузера Lynx:

```
dnf -y install httpd
```

```
dnf -y install lynx
```

Далее был создан новый каталог, который будет использоваться как корневая директория веб-сервера:

```
mkdir /web
```

Внутри каталога /web создан файл index.html с содержимым:

```
Welcome to my web server
```

```
root@amnauruzova:/home/amnauruzova# mkdir /web
root@amnauruzova:/home/amnauruzova# cd /web
root@amnauruzova:/web# touch index.html
root@amnauruzova:/web# echo "Welcome to my web server" > index.html
root@amnauruzova:/web# nano /etc/httpd/conf/httpd.conf
root@amnauruzova:/web# systemctl start httpd
root@amnauruzova:/web# systemctl enable httpd
root@amnauruzova:/web#
```

Рис. 3.8: Создание каталога и файла index.html

В конфигурационном файле /etc/httpd/conf/httpd.conf были внесены изменения.

Закомментирована строка по умолчанию:

```
#DocumentRoot "/var/www/html"
```

и добавлена новая:

```
DocumentRoot "/web"
```

Также был добавлен новый раздел, определяющий разрешения для каталога /web:

```
#
# 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"

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

Рис. 3.9: Изменение конфигурации Apache

После сохранения изменений службы были запущены и добавлены в автозагрузку:

```
systemctl start httpd
```

```
systemctl enable httpd
```

При первом обращении к веб-серверу через текстовый браузер Lynx по адресу `http://localhost` отобразилась стандартная тестовая страница Rocky Linux, а не созданный файл `index.html`.

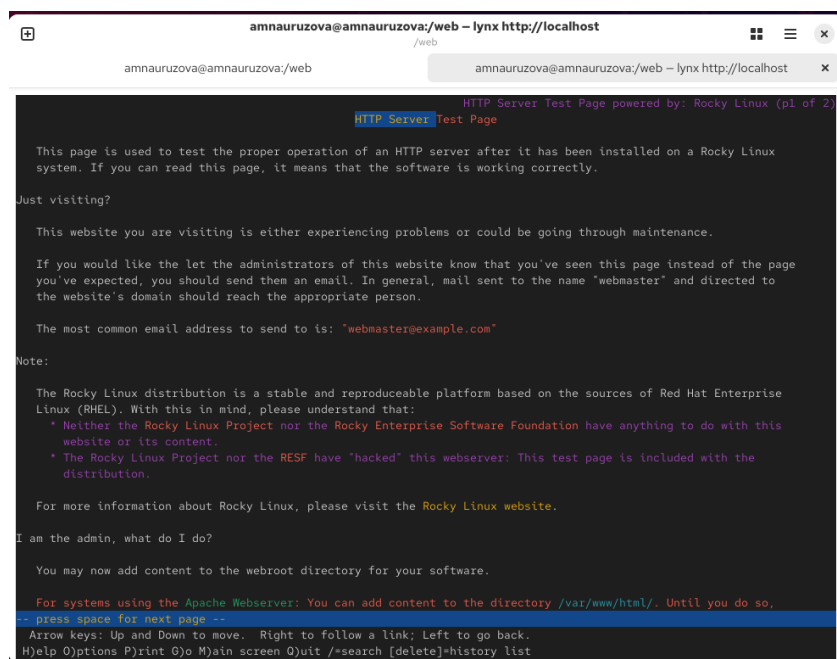


Рис. 3.10: Стандартная страница Apache

Это произошло из-за несоответствия контекста безопасности SELinux для нового каталога /web.

Для исправления был добавлен правильный контекст безопасности с помощью команды:

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

После этого был выполнен пересмотр меток контекста:

```
restorecon -R -v /web
```

Результат показал изменение контекста:

- /web и index.html были перемаркированы на **httpd_sys_content_t**, что позволяет Apache читать эти файлы.

```
root@amnauruzova:/web#  
root@amnauruzova:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
root@amnauruzova:/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@amnauruzova:/web# systemctl restart httpd  
root@amnauruzova:/web#
```

Рис. 3.11: Применение контекста безопасности SELinux

После перезапуска службы Apache (`systemctl restart httpd`) при повторном обращении через Lynx появилась пользовательская веб-страница с текстом:

Welcome to my web server

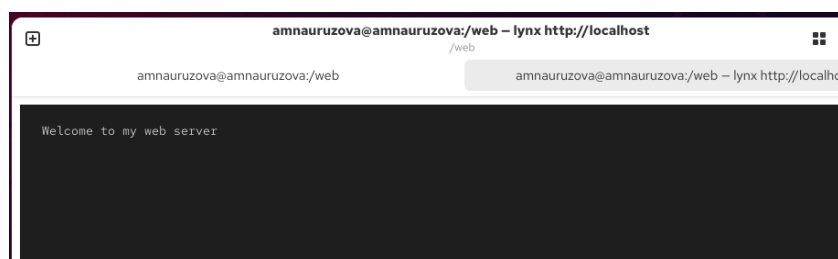


Рис. 3.12: Корректное отображение пользовательской страницы

3.4 Работа с переключателями SELinux

Для исследования работы SELinux-переключателей была выполнена команда:
`getsebool -a | grep ftp`

Результат показал, что переключатель **ftpd_anon_write** имеет значение **off**, то есть запись для анонимных пользователей через FTP отключена.

Далее просмотрен список переключателей SELinux с описанием для службы ftpd_anon:

```
semanage boolean -l | grep ftpd_anon
```

Вывод подтвердил, что параметр ftpd_anon_write отвечает за разрешение записи анонимных пользователей FTP и по умолчанию отключён.

Затем переключатель был активирован временно (до перезагрузки системы):

```
setsebool ftpd_anon_write on
```

Проверка (getsebool ftpd_anon_write) показала, что текущее значение стало **on**.

Однако при просмотре с помощью `semanage boolean -l` постоянное значение оставалось **off**, то есть изменение не сохраняется после перезагрузки.

Для сохранения параметра в постоянной конфигурации была выполнена команда:

```
setsebool -P ftpd_anon_write on
```

Теперь проверка показала, что оба значения (временное и постоянное) равны **on**.

```
root@amnauruzova:~# 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@amnauruzova:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
root@amnauruzova:~# setsebool ftpd_anon_write on
root@amnauruzova:~# getsebool ftpd_anon_write
ftpd_anon_write --> on
root@amnauruzova:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
root@amnauruzova:~# setsebool -P ftpd_anon_write on
root@amnauruzova:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
root@amnauruzova:~#
```

Рис. 3.13: Работа с переключателями SELinux для службы FTP

4 Контрольные вопросы

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

Для временного перевода SELinux в разрешающий режим используется команда:
`setenforce 0`

Эта команда переключает режим с **Enforcing** (принудительный) на **Permissive** (разрешающий) до следующей перезагрузки системы.

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

Чтобы просмотреть полный список всех переключателей SELinux, применяется команда:

`getsebool -a`

Она выводит текущее состояние (включено или выключено) для всех булевых параметров SELinux.

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

Для удобного чтения и анализа сообщений SELinux в журнале аудита используется пакет:

`setroubleshoot`

Он предоставляет понятные уведомления и расшифровки ошибок SELinux через системный журнал.

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

Для назначения правильного контекста безопасности веб-каталогу выполняются следующие команды:

1. Добавление нового контекста:

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

2. Применение контекста ко всем файлам и подкаталогам:

```
restorecon -R -v /web
```

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

Для полного отключения SELinux необходимо отредактировать конфигурационный файл:

```
/etc/sysconfig/selinux
```

В нём нужно изменить строку:

```
SELINUX=disabled
```

6. Где SELinux регистрирует все свои сообщения?

Все события SELinux записываются в системный журнал по пути:

```
/var/log/audit/audit.log
```

В этом файле содержатся подробные записи обо всех действиях, заблокированных или разрешённых политикой SELinux.

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

Чтобы получить список типов контекстов и булевых параметров, относящихся к службе FTP, используется команда:

```
semanage boolean -l | grep ftp
```

Она выводит доступные параметры и их текущее состояние (включено или выключено).

8. 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?

Самый простой способ временно проверить влияние SELinux — перевести его в разрешающий режим командой:

```
setenforce 0
```

Если после этого служба заработала корректно, значит, проблема связана с политикой SELinux.

После проверки рекомендуется вернуть систему в прежний режим:

```
setenforce 1
```

5 Заключение

В ходе работы были изучены режимы SELinux, выполнена настройка контекстов безопасности для веб-сервера и FTP-службы, а также освоены основные инструменты администрирования и диагностики SELinux.