

# **Лабораторная работа №9**

**Управление SELinux**

Юсупова Ксения Равиловна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
<b>4</b>	<b>Ответы на контрольные вопросы</b>	<b>17</b>
<b>5</b>	<b>Выводы</b>	<b>18</b>

# Список иллюстраций

3.1	Выполнили пункты 1 и 2 из раздела 9.4.1. (Управление режимами SELinux) . . . . .	8
3.2	Выполнили пункты 3 и 4 из раздела 9.4.1. (Управление режимами SELinux) . . . . .	8
3.3	Выполнили пункт 5 из раздела 9.4.1. (Управление режимами SELinux)	9
3.4	Выполнили пункты 6, 7 и 8 из раздела 9.4.1. (Управление режимами SELinux) . . . . .	9
3.5	Выполнили пункты 9 и 10 из раздела 9.4.1. (Управление режимами SELinux) . . . . .	10
3.6	Выполнили пункт 11 из раздела 9.4.1. (Управление режимами SELinux)	11
3.7	Выполнили пункт 1-8 из раздела 9.4.2. (Использование restorecon для восстановления контекста безопасности) . . . . .	12
3.8	Выполнили пункты 1 и 2 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)	12
3.9	Выполнили пункты 3 и 4 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)	13
3.10	Выполнили пункт 4 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера) . .	13
3.11	Выполнили пункт 5 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера) . .	13
3.12	Выполнили пункт 6 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера) . .	13
3.13	Выполнили пункты 7 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)	14
3.14	Выполнили пункт 8 и 9 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)	14
3.15	Выполнили пункт 10 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)	15
3.16	Выполнили пункты 1-8 из раздела 9.4.4 (Работа с переключателями SELinux) . . . . .	16

## **Список таблиц**

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками 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 вебслужбы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

### 3 Выполнение лабораторной работы

Запустили терминал и получили полномочия администратора. Просмотрели текущую информацию о состоянии SELinux. Анализ отчёта показал, что SELinux находится в рабочем состоянии: статус `enabled` означает, что система включена, а режим `enforcing` подтверждает, что политика безопасности активно применяется и все нарушения блокируются. В качестве основной используется стандартная политика `targeted`, которая обеспечивает безопасность, ограничивая только определённые целевые службы, в то время как большинство пользовательских процессов работают без ограничений. Конфигурационные файлы системы расположены в директории `/etc/selinux`. Было установлено, что текущий режим работы совпадает с режимом, заданным в конфигурации на постоянной основе, что обеспечивает стабильность политики после перезагрузки. Анализ контекстов безопасности процессов показал, что текущая пользовательская сессия (`unconfined_t`) не ограничена политикой, в то время как критически важные системные процессы, такие как `init` и демон SSH (`sshd_t`), работают в своих строго заданных доменах. Проверка контекстов ключевых файлов (например, `/etc/passwd`, `/etc/shadow`, `/bin/bash`) подтвердила, что политика корректно различает типы объектов, назначая им соответствующие метки безопасности, такие как `passwd_file_t` и `shadow_t`. (рис. 3.1).

```

[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# 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

```

Рис. 3.1: Выполнили пункты 1 и 2 из раздела 9.4.1. (Управление режимами SELinux)

Посмотрели, в каком режиме работает SELinux. По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing). Изменили режим работы SELinux на разрешающий (Permissive) и снова ввели `getenforce` (рис. 3.2).

```

[root@yu ~]# getenforce
Enforcing
[root@yu ~]# setenforce 0
[root@yu ~]# getenforce
Permissive
[root@yu ~]# cd /etc/sysconfig/selinux
-bash: cd: /root/etc/sysconfig/selinux: Нет такого файла или каталога

```

Рис. 3.2: Выполнили пункты 3 и 4 из раздела 9.4.1. (Управление режимами SELinux)

В файле `/etc/sysconfig/selinux` с помощью редактора установили `SELINUX=disabled` и перезагрузили систему (рис. 3.3).



```
GNU nano 5.6.1 /etc/sysconfig/selinux Изменён
# 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://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html>
#
# NOTE: Up to RHEL 8 release included, 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 p>
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 3.3: Выполнили пункт 5 из раздела 9.4.1. (Управление режимами SELinux)

После перезагрузки запустили терминал и получили полномочия администратора. Посмотрели статус SELinux и увидели, что SELinux теперь отключён. Попробовали переключить режим работы SELinux, мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы.(рис. 3.4).

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# getenforce
Disabled
[root@yu ~]# setenforce 1
setenforce: SELinux is disabled
[root@yu ~]# nano /etc/sysconfig/selinux
```

Рис. 3.4: Выполнили пункты 6, 7 и 8 из раздела 9.4.1. (Управление режимами SELinux)

Открыли файл /etc/sysconfig/selinux с помощью редактора и установили SELINUX=enforcing и перезагрузили систему. Во время загрузки системы получили предупреждающее сообщение о необходимости восстановления меток SELinux, что может занять некоторое время, а также потребовало дополнительной перезагрузки системы.(рис. 3.5).

```
GNU nano 5.6.1 /etc/sysconfig/selinux Изменён
# 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://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html>
#
# NOTE: Up to RHEL 8 release included, 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 p>
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 3.5: Выполнили пункты 9 и 10 из раздела 9.4.1. (Управление режимами SELinux)

После перезагрузки в терминале с полномочиями администратора просмотрели текущую информацию о состоянии SELinux, и убедились, что система работает в принудительном режиме (enforcing) использования SELinux.(рис. 3.6).

```

[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# 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

```

Рис. 3.6: Выполнили пункт 11 из раздела 9.4.1. (Управление режимами SELinux)

Запустили терминал и получили полномочия администратора, посмотрели контекст безопасности файла `/etc/hosts` и увидели, что у файла есть метка контекста `net_conf_t`. Скопировали файл `/etc/hosts` в домашний каталог и проверили контекст файла `~/hosts`. Поскольку копирование считается созданием нового файла, то параметр контекста в файле `~/hosts`, расположенном в домашнем каталоге, стал `admin_home_t`. Попытались перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc` и подтвердили, что хотим сделать это. Убедились, что тип контекста по-прежнему установлен на `admin_home_t` и исправили контекст безопасности. Убедились, что тип контекста изменился. Для массового исправления контекста безопасности на файловой системе ввели `touch /.autorelabel` и перезагрузили систему. Во время перезапуска не забыли нажать клавишу Esc на клавиатуре, чтобы видеть загрузочные сообщения. Увидели, что файловая система автоматически перемаркирована.(рис. 3.7).

```

[root@yu ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@yu ~]# cp /etc/hosts ~/
[root@yu ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@yu ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@yu ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
[root@yu ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@yu ~]# 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@yu ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@yu ~]# touch /.autorelabel
[root@yu ~]# reboot

```

Рис. 3.7: Выполнили пункт 1-8 из раздела 9.4.2. (Использование restorecon для восстановления контекста безопасности)

Запустили терминал и получили полномочия администратора. Установили необходимое программное обеспечение.(рис. 3.8).

```

[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# dnf -y install httpd
Последняя проверка окончания срока действия метаданных: 0:53:42 назад, Ср 29 о
кт 2025 16:56:02.
Пакет httpd-2.4.62-4.el9_6.4.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@yu ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:53:51 назад, Ср 29 о
кт 2025 16:56:02.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий  Размер
=====
Установка:
  lynx      x86_64       2.8.9-20.el9  appstream    1.5 М
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.5 М
Объем изменений: 6.1 М
Загрузка пакетов:
[===          ] --- B/s |  0 B  --:-- ETA

```

Рис. 3.8: Выполнили пункты 1 и 2 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Создали новое хранилище для файлов web-сервера и файл index.html в каталоге с контентом веб-сервера(рис. 3.9).

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

Рис. 3.9: Выполнили пункты 3 и 4 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Поместили в файл данный нам текст(рис. 3.10).

```
GNU nano 5.6.1 index.html Изменён
Welcome to my web-server
```

Рис. 3.10: Выполнили пункт 4 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

В файле `/etc/httpd/conf/httpd.conf` закомментировали строку `DocumentRoot "/var/www/html"` и ниже добавили строку `DocumentRoot "/web"`. Затем в этом же файле ниже закомментируйте необходимый раздел и добавили следующий раздел, определяющий правила доступа(рис. 3.11).

```
# 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>
```

Рис. 3.11: Выполнили пункт 5 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Запустили веб-сервер и службу httpd(рис. 3.12).

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

Рис. 3.12: Выполнили пункт 6 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx увидели веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.(рис. 3.13).

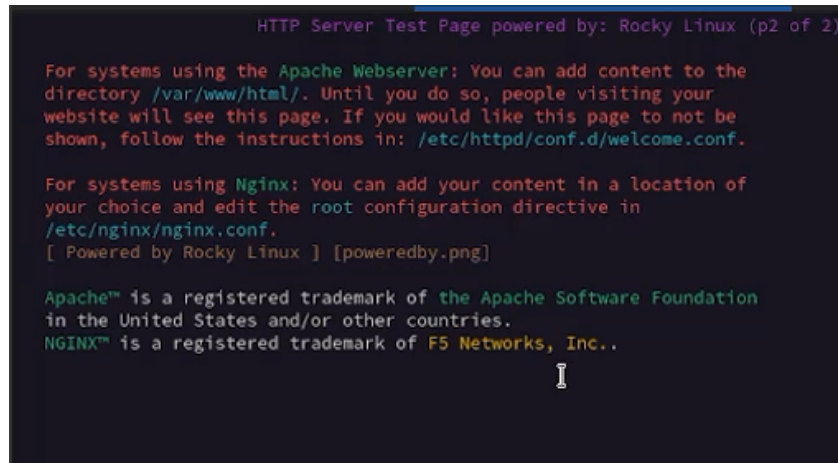


Рис. 3.13: Выполнили пункты 7 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

В терминале с полномочиями администратора применили новую метку контекста и восстановили контекст безопасности(рис. 3.14).

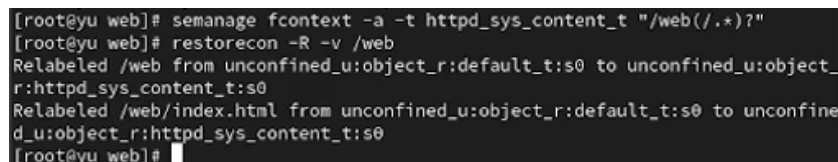


Рис. 3.14: Выполнили пункт 8 и 9 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

В терминале под учётной записью своего пользователя снова обратились к веб-серверу. Теперь мы получили доступ к своей пользовательской веб-странице. На экране отобразилась запись «Welcome to my web-server».(рис. 3.15).

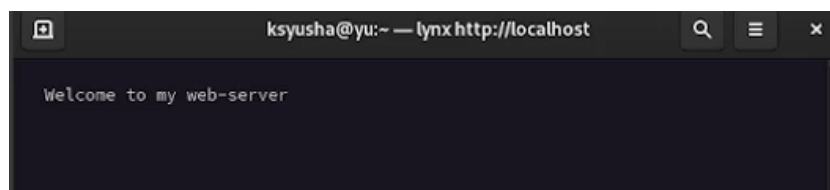


Рис. 3.15: Выполнили пункт 10 из раздела 9.4.3. (Настройка контекста безопасности для нестандартного расположения файлов веб-сервера)

Запустили терминал и получили полномочия администратора. Посмотрели список переключателей SELinux для службы ftp и увидели переключатель ftpd\_anon\_write с текущим значением off. Для службы ftpd\_anon посмотрели список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен. Изменили текущее значение переключателя для службы ftpd\_anon\_write с off на on. Повторно посмотрели список переключателей SELinux для службы ftpd\_anon\_write, посмотрели список переключателей с пояснением. Обратили внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена. Изменили постоянное значение переключателя для службы ftpd\_anon\_write с off на on. Посмотрели список переключателей. В результате было обнаружено, что булев переключатель ftpd\_anon\_write находится в состоянии «вкл.» (on). Это означает, что в рамках действующей политики SELinux анонимным пользователям FTP-сервера явно разрешено выполнять операции записи на сервер. Данное состояние активно в текущий момент и будет сохранено после перезагрузки системы.(рис. 3.16).



```

[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# 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@yu ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@yu ~]# setsebool ftpd_anon_write on
[root@yu ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@yu ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. ,выкл.) Allow ftpd to anon write
[root@yu ~]# setsebool -P ftpd_anon_write on
[root@yu ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@yu ~]#

```

Рис. 3.16: Выполнили пункты 1-8 из раздела 9.4.4 (Работа с переключателями SELinux)



## 4 Ответы на контрольные вопросы

1. Чтобы временно перевести SELinux в разрешающий режим, выполните:  
`setenforce Permissive`
2. Для просмотра всех переключателей (boolean) SELinux используйте:  
`getsebool -a`
3. Пакет для удобного просмотра логов SELinux: `setroubleshoot-server`
4. Чтобы назначить тип `httpd_sys_content_t` для каталога `/web`, выполните:  
`semanage fcontext -a -t httpd_sys_content_t '/web(/.*)?'` затем `restorecon -Rv /web`
5. Полное отключение SELinux производится в файле: `/etc/selinux/config` (нужно изменить параметр `SELINUX=disabled`)
6. Логи SELinux находятся в файле: `/var/log/audit/audit.log`
7. Для просмотра настроек FTP в SELinux используйте: `semanage boolean -l | grep ftp`
8. Чтобы проверить, связана ли проблема с SELinux: Переведите систему в `setenforce Permissive` и проверьте работу службы. Если проблема исчезла — причина в политиках SELinux.

## 5 Выводы

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