Лабораторная работа № 9

Управление SELinux

Сергеев Д. О.

01 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Сергеев Даниил Олегович
- Студент
- Направление: Прикладная информатика
- Российский университет дружбы народов
- 1132246837@pfur.ru

Цель работы

Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

Задание

Задание

- Продемонстрировать навыки по управлению режимами SELinux
- Продемонстрировать навыки по восстановлению контекста безопасности SELinux
- Настроить контекст безопасности для нестандартного расположения файлов веб-службы
- Продемонстрировать навыки работы с переключателями SELinux

Ход выполнения лабораторной работы

Управление режимами SELinux

```
[root@dosergeev ~]# 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
```

Рис. 1: Вывод команды sestatus -v (1)

```
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
```

Рис. 2: Вывод команды sestatus -v (2)

```
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: Вывод команды sestatus -v (3)

```
[root@dosergeev ~]# getenforce
Enforcing
[root@dosergeev ~]# setenforce 0
[root@dosergeev ~]# getenforce
Permissive
```

Рис. 4: Изменение режимов SELinux с помощью setenforce

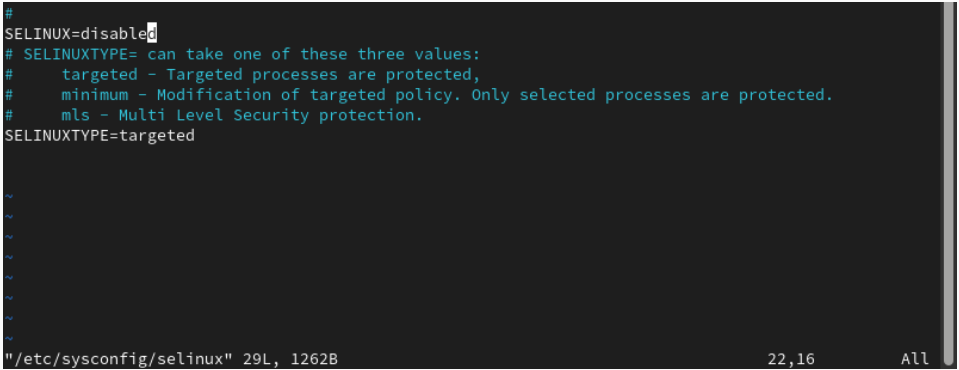


Рис. 5: Установка режима SELINUX=disabled

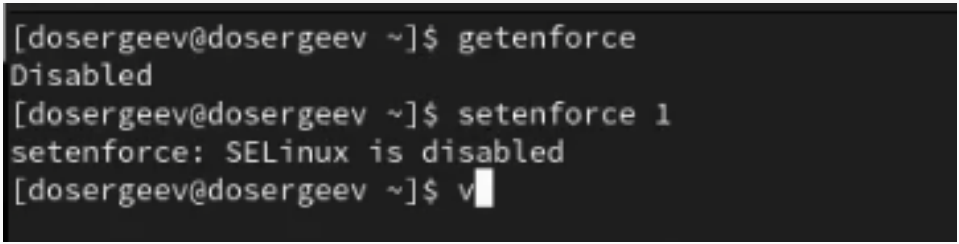


Рис. 6: Попытка переключение режима SELinux

Снова откроем файл /etc/sysconfig/selinux с помощью редактора и установим режим SELINUX=enforcing вручную. Перезагрузим систему.

Во время загрузки выводится предупреждающее сообщение о восстановлении меток SElinux.

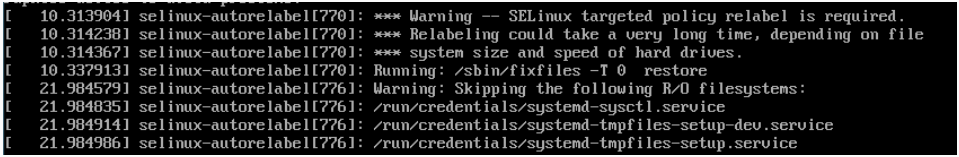


Рис. 7: Восстановление меток SELinux после перезапуска

Использование restorecon для восстановления контекста безопасности

```
[dosergeev@dosergeev ~]$ su -
Password:
[root@dosergeev ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@dosergeev ~]# cp /etc/hosts ~/
[root@dosergeev ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@dosergeev ~]#
```

Рис. 8: Контекст безопасности файла после копирования

Использование restorecon для восстановления контекста безопасности

```
[root@dosergeev ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@dosergeev ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@dosergeev ~]# 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@dosergeev ~]# ls -Z /etc/host
ls: cannot access '/etc/host': No such file or directory
[root@dosergeev ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@dosergeev ~]#
```

Рис. 9: Восстановление контекста безопасности /etc/hosts

Использование restorecon для восстановления контекста безопасности

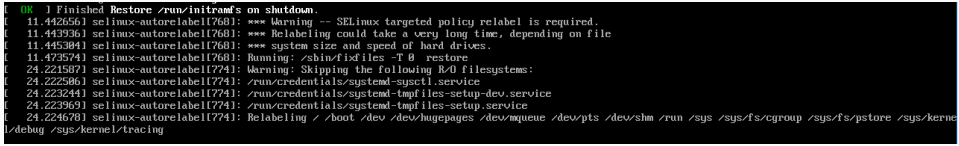


Рис. 10: Автоматическая перемаркировка SELinux во время перезапуска системы

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

```
[root@dosergeev ~]# dnf -y install httpd
Last metadata expiration check: 1:01:34 ago on Sat 01 Nov 2025 06:05:04 PM MSK.
Package httpd-2.4.62-4.el9_6.4.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@dosergeev ~]# dnf -y install lynx
Last metadata expiration check: 1:01:42 ago on Sat 01 Nov 2025 06:05:04 PM MSK.
Package lynx-2.8.9-20.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@dosergeev ~]#
```

Рис. 11: Проверка патеков httpd, lynx

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Создадим новое хранилище для файлов веб-сервера: mkdir /web; Также создадим индекс (в новом каталоге): touch index.html.

В индекс запишем сообщение - Welcome to my web-server.

Откроем файл /etc/httpd/conf/httpd.conf на редактирование. Закомментируем строку DocumentRoot и тег (раздел) Directory, после чего добавим те же строки, заменив пути /var/www/html и /var/www на /web.

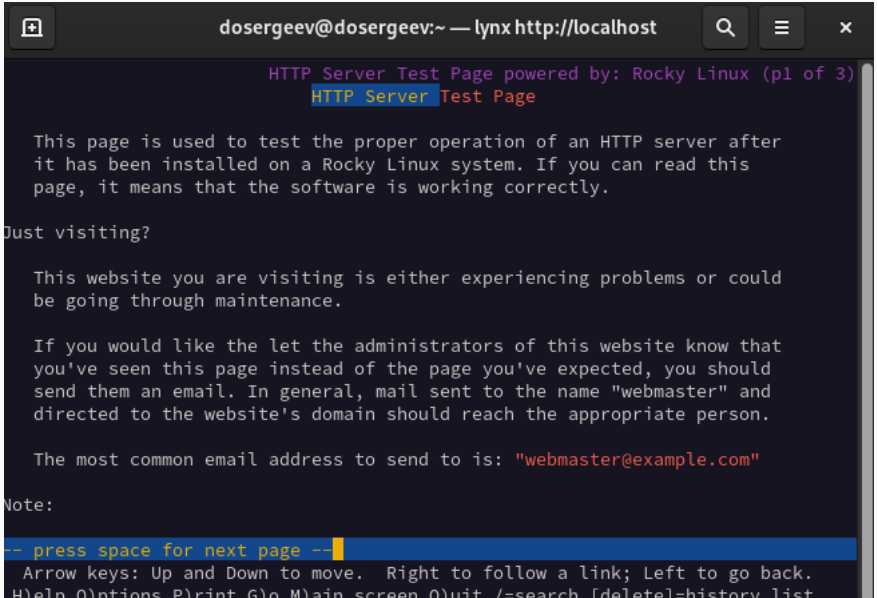
Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

```
# 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>
```

```
[root@dosergeev web]# systemctl start httpd
[root@dosergeev web]# systemctl enable httpd
[root@dosergeev web]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-11-01 19:05:43 MSK; 6min ago
       Docs: man:httpd.service(8)
   Main PID: 1143 (httpd)
```

Рис. 13: Запуск httpd

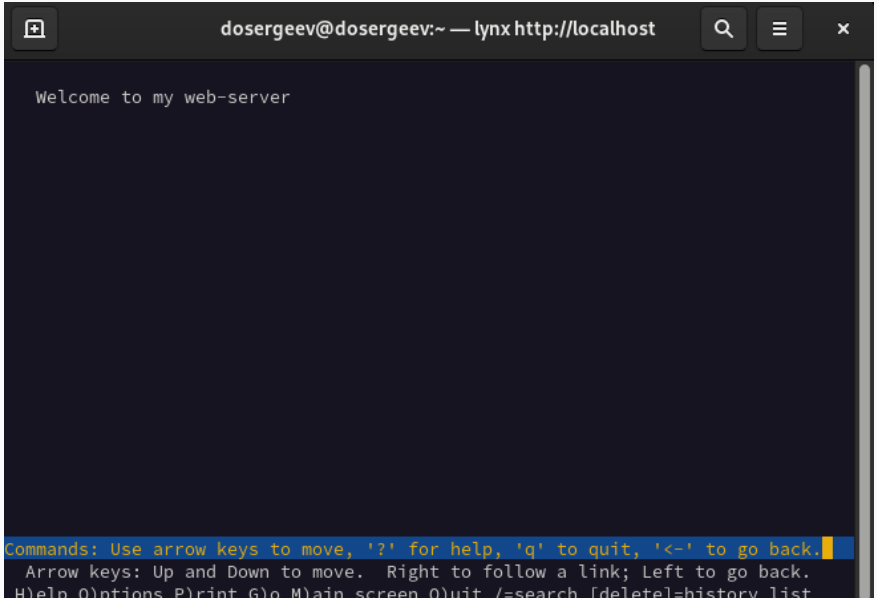
Настройка контекста безопасности для нестандартного расположения файлов веб-сервера



В терминале с полномочиями администратора установим новую метку контекста к /web и восстановим контекст безопасности.

```
[root@dosergeev web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@dosergeev web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_conten
t_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@dosergeev web]#
```

Рис. 15: Настройка контекста для веб-сервера


dosergeev@dosergeev:~ — lynx http://localhost
Welcome to my web-server
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.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list

Работа с переключателями SELinux

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

Рис. 17: Переключатели для службы ftp, ftpd_anon

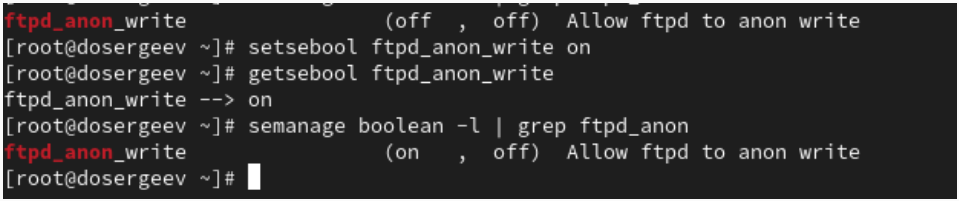


Рис. 18: Переключатель для службы ftpd_anon после изменения значения

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

Рис. 19: Переключатели для службы ftp, ftpd_anon

Теперь переключатель имеет состояние (on , on). Это значит, что теперь он включен как постоянная настройка и как настройка времени выполнения.

Ответы на контрольные вопросы

Ответы на контрольные вопросы

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

- setenforce 0

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

- getsebool -a

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

- setroubleshoot

Ответы на контрольные вопросы

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(/.*)?” - добавляет правило в политику
- restorecon -R -v /web - обновляет политику

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

- /etc/selinux/config или /etc/sysconfig/selinux

6. Где SELinux регистрирует все свои сообщения?

- /var/log/audit/audit.log

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

- seinfo -t | grep ftp

```
[root@dosergeev ~]# seinfo -t | grep ftp
   anon_sftpd_t
   ftp_client_packet_t
   ftp_data_client_packet_t
   ftp_data_port_t
   ftp_data_server_packet_t
   ftp_port_t
   ftp_server_packet_t
   ftpd_etc_t
   ftpd_exec_t
   ftpd_initrc_exec_t
```

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?

- Можно перевести SELinux в разрешающий режим (setenforce 0). Таким образом, если проблема связана с SELinux, то сервис перестанет блокироваться политикой, возобновив свою работу. Для дальнейшего анализа можно просмотреть журналы, ведь в режиме permissive SELinux все ещё отправляет логи.

Вывод

Вывод

В результате выполнения лабораторной работы я получил навыки работы с контекстом безопасности и политиками SELinux, научился настраивать контекст безопасности для нестандартного расположения файлов веб сервера и переключатели для служб на примере ftp.