

Операционные системы

Управление SELinux

Вишняков Родион Сергеевич

Российский университет дружбы народов, Москва, Россия

01 ноября

Section 1

Цели и задачи работы

Цель лабораторной работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

Задача лабораторной работы

Научиться навыкам работы с контекстом безопасности и политиками SELinux.

Section 2

Процесс выполнения лабораторной работы

Получаем полномочия администратора

```
rodvish@rodvishh:~$ sudo -i  
[sudo] пароль для rodvish:  
root@rodvishh:~#
```

Рис. 1: root

Просмотрели текущую информацию о состоянии SELinux

```
root@rodvishh:~# 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@rodvishh:~#
```

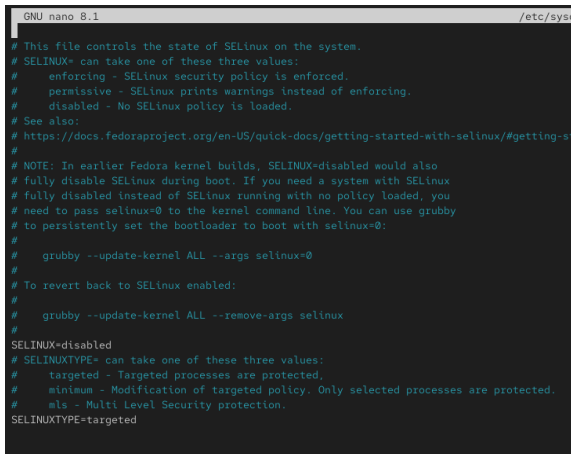
Рис. 2: SELinux

Посмотрели, в каком режиме работает SELinux

```
root@rodvishh:~# getenforce
Enforcing
root@rodvishh:~# █
```

Рис. 3: SELinux

В файле /etc/sysconfig/selinux с помощью редактора установили заданное значение



```
GNU nano 8.1 /etc/sysc
# 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
#
# 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
```

Рис. 4: Изменение редактора

Посмотрели статус SELinux

```
root@rodvishh:~# getenforce
Disabled
root@rodvishh:~#
```

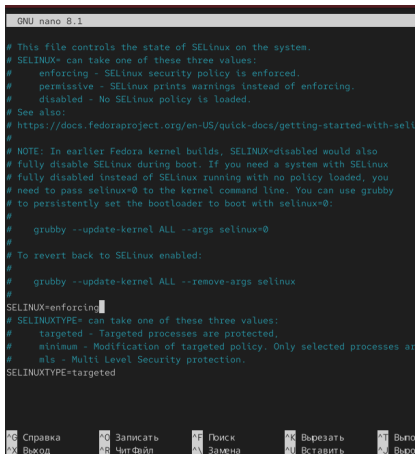
Рис. 5: SELinux

Попробовали переключить режим работы SELinux

```
root@rodvishh:~# setenforce 1  
setenforce: SELinux is disabled  
root@rodvishh:~# █
```

Рис. 6: SELinux

В файле /etc/sysconfig/selinux с помощью редактора установили заданное значение



```
GNU nano 8.1

# 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/
#
# 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
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

^G Справка      ^O Записать    ^P Поиск       ^K Вырезать    ^T Вып
^X Выход        ^R Чит.Файл   ^L Замена     ^J Вставить    ^U Выр
```

Рис. 7: Изменение редактора

Просмотрели текущую информацию о состоянии SELinux

```
root@rodvishh:~# 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@rodvishh:~#
```

Рис. 8: SELinux

Посмотрели контекст безопасности файла /etc/hosts

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 9: Контекст безопасности файла

Скопировали файл /etc/hosts в домашний каталог и проверили контекст файла ~/hosts

```
root@rodvishh:~# cp /etc/hosts ~/
root@rodvishh:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@rodvishh:~#
```

Рис. 10: Создание файла сценария

Попытались перезаписать существующий файл hosts из домашнего каталога в ката-

лог /etc

A terminal window with a dark background and green text. The prompt is 'root@rodvishh:~#'. The command 'mv ~/hosts /etc' is entered. The output is 'mv: переписать '/etc/hosts'?'. The prompt is repeated, followed by a grey cursor block.

```
root@rodvishh:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'?
root@rodvishh:~#
```

Рис. 11: Файл hosts

Убедились, что тип контекста по-прежнему установлен на `admin_home_t`

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 12: `admin_home_t`

Исправили контекст безопасности

```
root@rodvishh:~# restorecon -v /etc/hosts  
root@rodvishh:~#
```

Рис. 13: Контекст безопасности

Убедились, что тип контекста изменился

```
root@rodvishh:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@rodvishh:~#
```

Рис. 14: Тип контекста

Для массового исправления контекста безопасности на файловой системе ввели



```
root@rodvishh:~# touch /.autorelabel  
root@rodvishh:~#
```

Рис. 15: Массовое исправления контекста

Получаем полномочия администратора

```
rodvish@rodvishh:~$ sudo -i  
[sudo] пароль для rodvish:  
Попробуйте ещё раз.  
[sudo] пароль для rodvish:  
root@rodvishh:~#
```

Рис. 16: root

Устанавливаем необходимое программное обеспечение

```
root@rodvishh:~# dnf -y install httpd
Rocky Linux 10 - BaseOS                               8.4 kB/s | 4.3 kB  00:00
Rocky Linux 10 - BaseOS                               4.8 MB/s | 22 MB  00:04
Rocky Linux 10 - AppStream                             8.3 kB/s | 4.3 kB  00:00
Rocky Linux 10 - AppStream                             206 kB/s | 2.2 MB  00:11
Rocky Linux 10 - CRB                                   7.6 kB/s | 4.3 kB  00:00
Rocky Linux 10 - CRB                                   30 kB/s | 531 kB  00:17
Rocky Linux 10 - Extras                                165 B/s | 3.1 kB  00:19
Rocky Linux 10 - Extras                                10 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@rodvishh:~# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:20 назад, Сб 01 ноя 2025 14:53:33.
Зависимости разрешены.
=====
Пакет                Архитектура          Версия                Резпозиторий          Размер
-----
Установка:
lynx                  x86_64                2.9.0-6.el10          appstream              1.6 M
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.6 M
Объем изменений: 6.0 M
Загрузка пакетов:
lynx-2.9.0-6.el10.x86_64.rpm                                215 kB/s | 1.6 MB  00:07
-----
Общий размер                                              206 kB/s | 1.6 MB  00:07
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
Подготовка :
Установка : lynx-2.9.0-6.el10.x86_64                      1/1
Запуск скрипта: lynx-2.9.0-6.el10.x86_64                  1/1
```

Рис. 17: Необходимое программное обеспечение

Создали новое хранилище для файлов web-сервера

```
root@rodvishh:~# mkdir /web  
root@rodvishh:~# █
```

Рис. 18: Новое хранилище

Создали файл index.html в каталоге с контентом веб-сервера и поместили в файл следующий текст

```
root@rodvishh:~# cd /web
root@rodvishh:/web# touch index.html
root@rodvishh:/web# echo "Welcome to my web-server" > /web/index.html
root@rodvishh:/web#
```

Рис. 19: index.html

Проделываем различные действия со строками в файле /etc/httpd/conf/httpd.conf

```
#  
#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
```

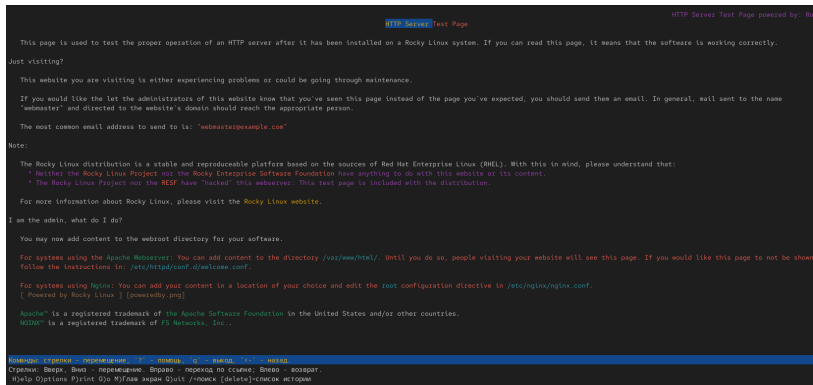
Рис. 20: /etc/httpd/conf/httpd.conf

Запустили веб-сервер и службу httpd

```
root@rodvishh:/web# systemctl start httpd  
root@rodvishh:/web# systemctl enable httpd  
root@rodvishh:/web# █
```

Рис. 21: Служба httpd и веб-сервер

Обратились к веб-серверу в текстовом браузере lynx



```
HTTP Server Test Page
HTTP Server Test Page powered by: R...

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.

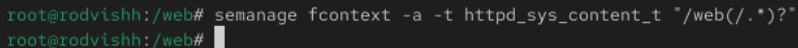
For systems using Nginx: You can add your content in a location of your choice and edit the root configuration directive in /etc/nginx/nginx.conf.
[ Powered by Rocky Linux ] [poweredby.png]

Apache is a registered trademark of the Apache Software Foundation in the United States and/or other countries.
NetScape is a registered trademark of Netscape Communications Corporation.

Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, 'x' - назад
Стрелки: Вверх, Вниз - перемещение, Вправо - переход по ссылке, Влево - возврат.
H)elp O)ptions P)rint Q)u) M)глаз экран Q)uit /-поиск [delete]-список истории
```

Рис. 22: lynx

В терминале с полномочиями администратора применили новую метку контекста к /web



```
root@rodvishh:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
root@rodvishh:~#
```

Рис. 23: Новая метка контекста к /web

Восстановили контекст безопасности

```
root@rodvishh:/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@rodvishh:/web#
```

Рис. 24: Контекст безопасности

Снова обращаемся к веб-серверу

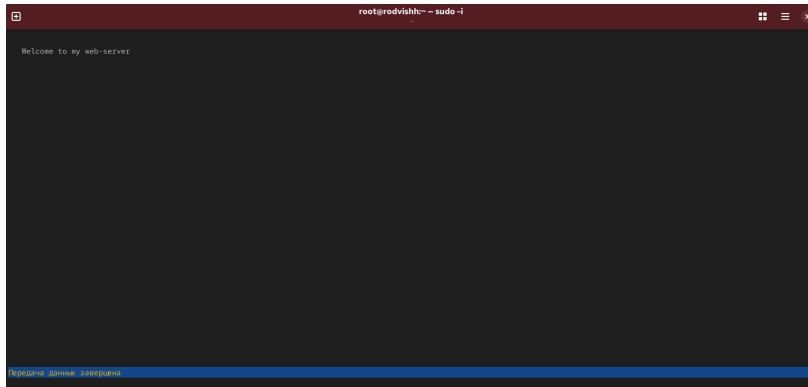


Рис. 25: Веб-сервер

Посмотрели список переключателей SELinux для службы ftp

```
root@rodvishh:~# 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@rodvishh:~#
```

Рис. 26: Список переключателей SELinux

Посмотрели список переключателей с пояснением

```
root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (выкл.,выкл.) Allow ftpd to anon write
root@rodvishh:~#
```

Рис. 27: Список переключателей с пояснением

Изменили текущее значение переключателя для службы ftpd_anon_write с off на on

```
root@rodvishh:~# setsebool ftpd_anon_write on  
root@rodvishh:~#
```

Рис. 28: Значение переключателя

Повторно посмотрели список переключателей SELinux для службы ftpd_anon_write

```
root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write                (вкл. ,вкл.) Allow ftpd to anon write
root@rodvishh:~# █
```

Рис. 29: Список переключателей SELinux

Изменили постоянное значение переключателя для службы ftpd_anon_write с off на on

```
root@rodvishh:~# setsebool -P ftpd_anon_write on
```

Рис. 30: Постоянное значение переключателя

Посмотрели список переключателей

```
root@rodvishh:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (вкл. , вкл.) Allow ftpd to anon write
root@rodvishh:~#
```

Рис. 31: Список переключателей

Section 3

Вывод по проделанной работе

Мы получили навыки работы с контекстом безопасности и политиками SELinux.