

Управление SELinux

Майоров Дмитрий Андреевич

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Выводы	14

Список иллюстраций

2.1	6
2.2	6
2.3	7
2.4	7
2.5	7
2.6	8
2.7	8
2.8	8
2.9	8
2.10	9
2.11	9
2.12	9
2.13	9
2.14	10
2.15	10
2.16	11
2.17	11
2.18	12
2.19	12
2.20	12
2.21	13
2.22	13
2.23	13

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

Получаем полномочия администратора. Смотрим текущую информацию о SELinux. SELinux включен(enabled) и находится в принудительном режиме работы (enforcing). Тип политики: targeted. Конфигурационный режим: enforcing. Состояние политики: MS status не задан, deny_unknown разрешен. Проверка защиты памяти активна. Версия ядра политики: 33

```
root@mayorovda:~# sestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode Setting desired:           ----
Mode Setting active:            ----
```

Рисунок 2.1

Смотрим, в каком режиме работает SELinux. Он работает в принудительном режиме. Изменяем режим работы на разрешающий.

```
root@mayorovda:~# getenforce
Enforcing
root@mayorovda:~# setenforce 0
root@mayorovda:~# getenforce
Permissive
```

Рисунок 2.2

Открываем файл /etc/sysconfig/selinux для редактирования и устанавливаем следующий параметр. Перезагружаем систему



```
# SELINUX=disabled
# SELINUXTYPE=can_tai
```

Рисунок 2.3

Смотрим статус SELinux. Видим, что он отключен. Пробуем переключить режим работы. Система говорит, что SELinux отключен. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы

```
root@mayorovda:~# getenforce
Disabled
root@mayorovda:~# setenforce 1
setenforce: SELinux is disabled
```

Рисунок 2.4

Открываем файл /etc/sysconfig/selinux для редактирования и устанавливаем следующий параметр. Перезагружаем систему



```
# SELINUX=enforcing
# SELINUXTYPE=can_tai
```

Рисунок 2.5

Смотрим текущую информацию о SELinux. Убеждаемся, что он работает в принудительном режиме

```
root@mayorovda:~# 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
```

Рисунок 2.6

Смотрим контекст безопасности файла /etc/hosts. Копируем его в домашний каталог. Проверяем контект файла. Параметр контекста изменился на admin_home_t

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

Рисунок 2.7

Пытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc. Убеждаемся, что тип контекста по-прежнему установлен на admin_home_t

```
root@mayorovda:~# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@mayorovda:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
```

Рисунок 2.8

Исправляем контекст безопасности. Убеждаемся, что он изменился

```
root@mayorovda:~# 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@mayorovda:~# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
```

Рисунок 2.9

Для массового исправления контекста безопасности на файловой системе вводим следующую команду и перезагружаем систему. При перезагрузке смотрим загрузочные сообщения. Видим, что файловая система перемаркирована

```
root@mayorovda:~# touch /.autorelabel  
root@mayorovda:~# reboot
```

Рисунок 2.10

```
[ 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.  
5.179669] selinux-autorelabel[989]: *** Warning -- SELinux targeted policy relabel  
5.172098] selinux-autorelabel[989]: *** Relabeling could take a very long time, de-  
5.173332] selinux-autorelabel[989]: *** system size and speed of hard drives.  
5.177961] selinux-autorelabel[989]: Running: /sbin/fixfiles -T 8 restore  
10.652472] selinux-autorelabel[996]: Warning: Skipping the following R/O filesystems:  
10.655467] selinux-autorelabel[996]: /run/credentials/systemd-journal.service  
10.655819] selinux-autorelabel[996]: Relabeling / /boot /dev /dev/hugepages /dev/mq  
/debug /sys/kernel/tracing
```

Рисунок 2.11

Устанавливаем необходимое программное обеспечение

```
root@mayorovda:~# dnf -y install httpd  
Rocky Linux 10 - BaseOS           12 kB/s | 4.3 kB   00:00  
Rocky Linux 10 - AppStream        14 kB/s | 4.3 kB   00:00  
Rocky Linux 10 - Extras           8.2 kB/s | 3.1 kB   00:00  
Package httpd-2.4.63-4.el10_1.3.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
root@mayorovda:~# dnf -y install lynx
```

Рисунок 2.12

Создаем новое хранилище для файлов web-сервера. Создаем файл index.html

```
root@mayorovda:~# mkdir /web  
root@mayorovda:~# cd /web  
root@mayorovda:/web# touch index.html
```

Рисунок 2.13

Открываем этот файл для редактирования и помещаем туда следующий текст

```
GNU nano 8.1          index
Welcome to my web-server
```

Рисунок 2.14

В файле /etc/httpd/conf/httpd.conf комментируем строку DocumentRoot «/var/www/html» и ниже добавляем строку DocumentRoot «/web»

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

Рисунок 2.15

Также ниже комментируем раздел и добавляем другой раздел, определяющий правила доступа

```
#<Directory "/var/www">
#    AllowOverride None
#    # Allow open access:
#    # Require all granted
#</Directory>

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

— — —

Рисунок 2.16

Запускаем веб-сервер и службу httpd

```
root@mayorovda:/web# systemctl start httpd
root@mayorovda:/web# systemctl enable httpd
```

Рисунок 2.17

Открываем веб-сервер в текстовом браузере. Видим страницу REd Hat по умолчанию

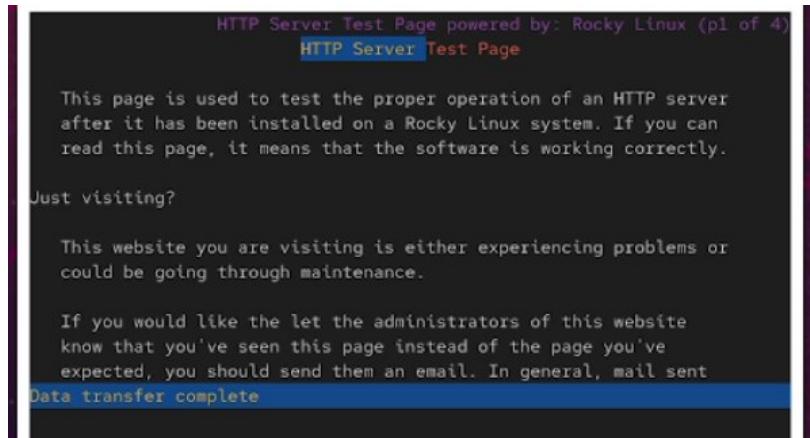


Рисунок 2.18

Применяем новую метку контекста к /web и восстанавливаем контекст безопасности

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

Рисунок 2.19

Перезагружаем систему и снова обращаемся к веб серверу. Теперь видим там запись, которую мы оставляли в файле index.html

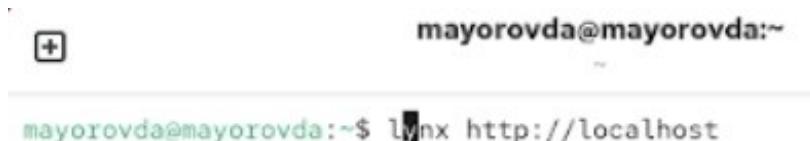


Рисунок 2.20

Смотрим список переключателей SELinux для службы ftp

```
mayorovda@mayorovda:~$ su -
Password:
Last login: Tue Feb  3 15:15:02 MSK 2026 on pts/0
root@mayorovda:~# 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
■
```

Рисунок 2.21

Для службы `ftpd_anon` смотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен

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

Рисунок 2.22

Изменяем текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`. Снова смотрим список переключателей для службы `ftpd_anon`. Смотрим список всех переключателей

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

Рисунок 2.23

Изменяем постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`. Смотрим список переключателей. Видим, что переключатель включен

3 Выводы

Получены навыки работы с контекстом безопасности и политиками SELinux.