Лабораторная работа №6

Мандатное разграничение прав в Linux

Ильин Андрей Владимирович

Содержание

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Задачи

1. Настроить и запустить сервер Apache.
2. Исследовать влияние различных параметров на работу сервера.

# Теоретическое введение

## Термины

* Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями. [1]
* Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. [2]
* Расширенные атрибуты файловых объектов (далее - расширенные атрибуты) - поддерживаемая некоторыми файловыми системами возможность ассоциировать с файловыми объектами произвольные метаданные. [3]
* Security Enhanced Linux (SELinux) – это система контроля доступа, которая в настоящее время встраиватся в большинство Linux-дистрибутивов. [4]

## Окружение

* Rocky Linux - это корпоративная операционная система с открытым исходным кодом, разработанная таким образом, чтобы быть на 100% совместимой с Red Hat Enterprise Linux. Он находится в стадии интенсивной разработки сообществом. [5]
* Git - это распределенное программное обеспечение для контроля версиями. [6]
* VirtualBox - это кросс-платформенное ПО для виртуализации x86 и AMD64/Intel64 с открытым кодом для корпоративного и домашнего использования. [7]

# Выполнение лабораторной работы

1. Убедимся, что SELinux работает в режиме enforcing политики targeted. (рис. [1](#fig:001))

getenforce  
sestatus

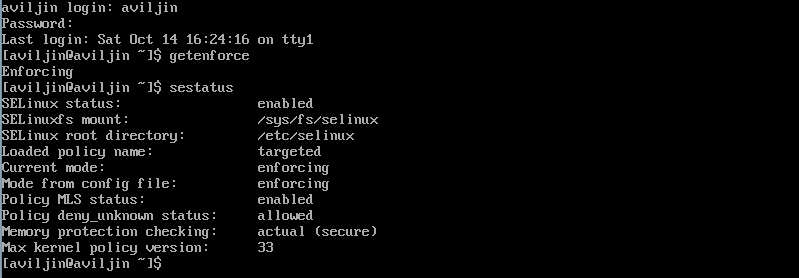


Figure 1: Проверка SELinux

1. Запустим веб-сервер. Убедимся, что он работает. (рис. [2](#fig:002))

service httpd start  
service httpd status

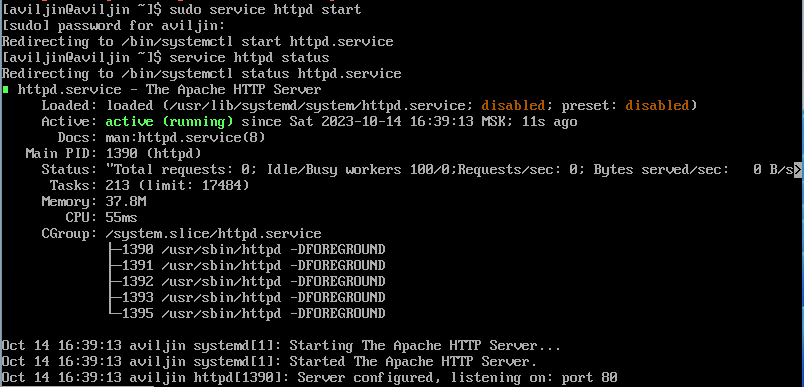


Figure 2: Статус веб-сервера

1. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности. (рис. [3](#fig:003))

ps auxZ | grep httpd

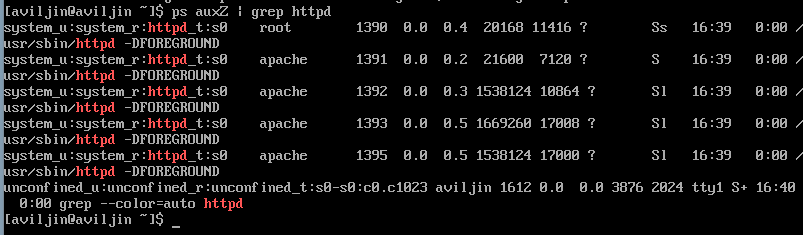


Figure 3: Контекст безопасности Apache

1. Посмотрим текущее состояние переключателей SELinux для Apache. (рис. [4](#fig:004))

sestatus -b | grep httpd

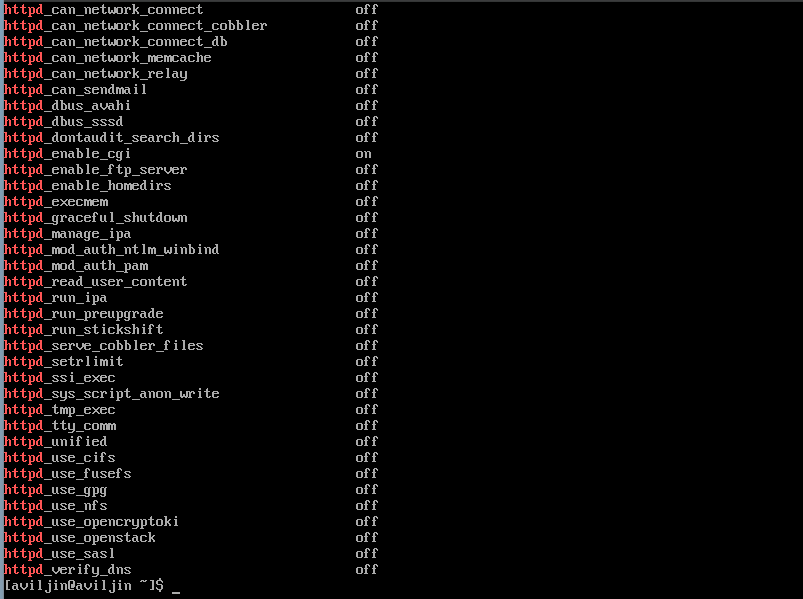


Figure 4: Переключатели SELinux для Apache

1. Посмотрим статистику по политике. (рис. [5](#fig:005))

seinfo

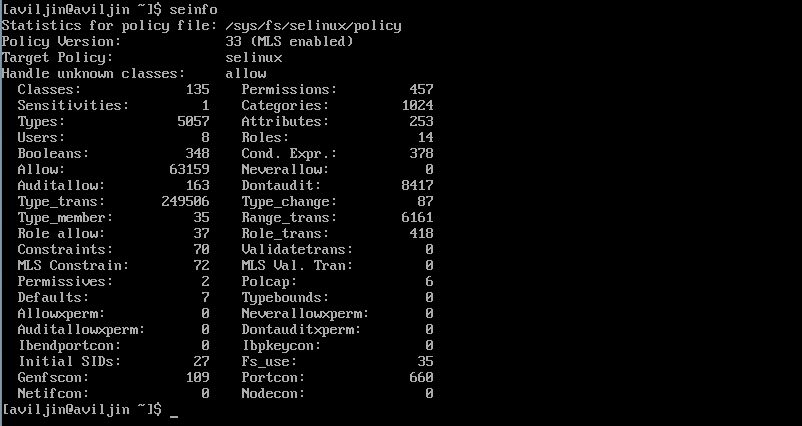


Figure 5: Статистика по политике

1. Определиv тип файлов и поддиректорий, находящихся в директориях /var/www, /var/www/html. Определиv круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. [6](#fig:006))

ls -lZ /var/www  
ls -lZ /var/www/html  
ls -alF /var/www

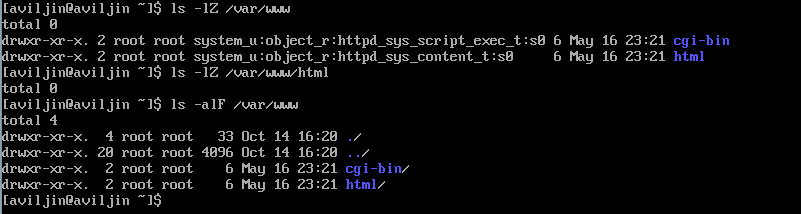


Figure 6: Тип файлов и поддиректорий Apache

1. Создаlbv от имени суперпользователя html-файл в /var/www/html/test.html. Проверим контекст созданного файла. Обратимся к файлу через веб-сервер. (рис. [7](#fig:007), [8](#fig:008))

<html>  
 <body>  
 test  
 </body>  
</html>

touch /var/www/html/test.html  
vim /var/www/html/test.html  
ls -Z /var/www/html/test.html  
lynx http://127.0.0.1/test.html

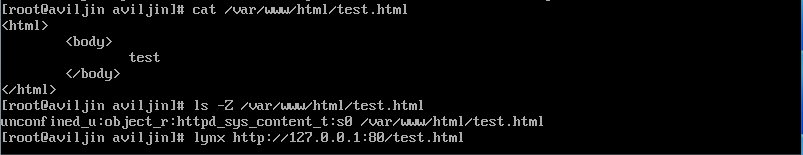


Figure 7: Создание html.test



Figure 8: Просмотр http://127.0.0.1/test.html (1)

1. Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t. Попробуем ещё раз получить доступ к файлу через веб-сервер. Просмотрим log-файлы веб-сервера Apache. (рис. [9](#fig:009), [10](#fig:010), [11](#fig:011))

chcon -t samba\_share\_t /var/www/html/test.html  
ls -Z /var/www/html/test.html  
lynx http://127.0.0.1/test.html  
tail /var/log/audit/audit.log

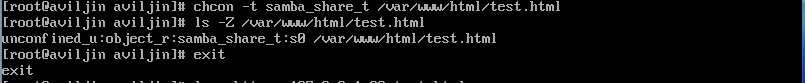


Figure 9: Изменение контекст файла test.html



Figure 10: Просмотр http://127.0.0.1/test.html (2)



Figure 11: Просмотр audit.log

1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81. Перезапустим веб-сервер Apache. (рис. [12](#fig:012), [13](#fig:013))

vim /etc/httpd/conf/httpd.conf  
service httpd restart  
service httpd status

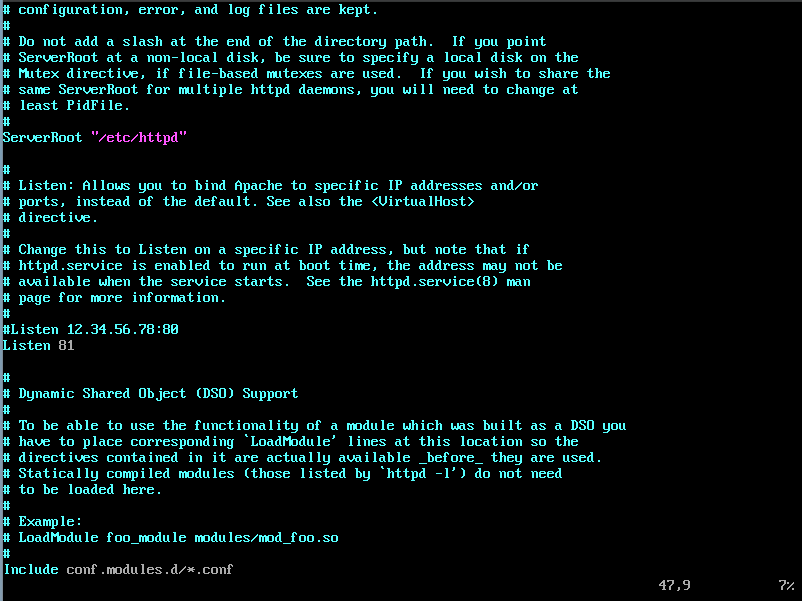


Figure 12: Изменение httpd.conf на прослушование ТСР-порта 81

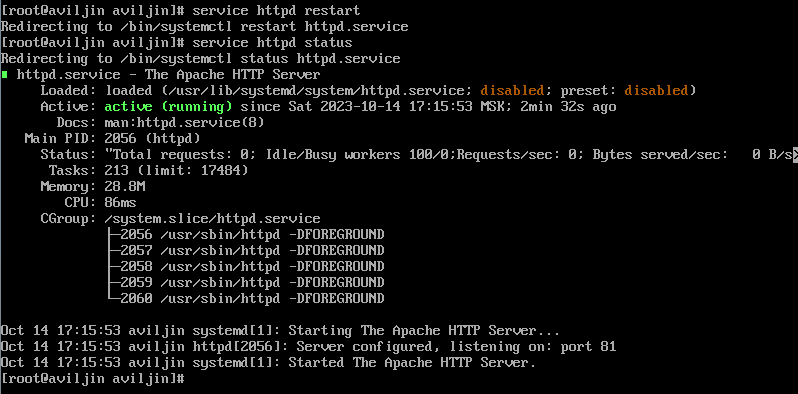


Figure 13: Перезапуск Apache

1. Проанализируем лог-файлы. Добавим порт 81 в список портов. (данный порт, как оказалось, уже был в списке, из-за этого не произошло сбоя). Перезапустим сервер. Вернем контекст httpd\_sys\_cоntent\_\_t. Попробуем получить доступ к файлу через веб-сервер (рис. [14](#fig:014), [15](#fig:015))

tail -n5 /var/log/messages  
  
semanage port -a -t http\_port\_t -р tcp 81  
semanage port -l | grep http\_port\_t  
service httpd restart  
  
chcon -t httpd\_sys\_content\_t /var/www/html/test.html  
lynx http://127.0.0.1/test.html

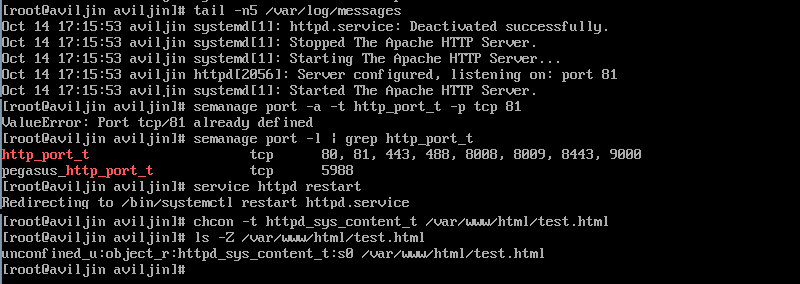


Figure 14: Добавление порта 81 в список портов



Figure 15: Просмотр http://127.0.0.1/test.html (3)

# Анализ результатов

Работа выполненна без непредвиденных проблем в соответствии с руководством. Ошибок и сбоев не произошло.

# Выводы

Нам удалось развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache. Такде мы настроили и запустили сервер Apache. Исследовали влияние различных параметров на работу сервера.

# Список литературы

1. Терминал Linux [Электронный ресурс]. URL: [{https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%20(%D0%B8%D0%BB%D0%B8%20%C2%ABBash%C2%BB%2C,%D1%81%20%D1%84%D0%B0%D0%B9%D0%BB%D0%B0%D0%BC%D0%B8%20%D0%B8%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8}](%7Bhttps://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%20(%D0%B8%D0%BB%D0%B8%20%C2%ABBash%C2%BB%2C,%D1%81%20%D1%84%D0%B0%D0%B9%D0%BB%D0%B0%D0%BC%D0%B8%20%D0%B8%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8%7D).

2. Права доступа [Электронный ресурс]. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.

3. Расширенные атрибуты [Электронный ресурс]. URL: [{https://wiki.astralinux.ru/pages/viewpage.action?pageId=149063848#:~:text=Common%20Edition%202.12-,%D0%A7%D1%82%D0%BE%20%D1%82%D0%B0%D0%BA%D0%BE%D0%B5%20%D1%80%D0%B0%D1%81%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5%20%D0%B0%D1%82%D1%80%D0%B8%D0%B1%D1%83%D1%82%D1%8B,%D1%81%20%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D1%8B%D0%BC%D0%B8%20%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%B0%D0%BC%D0%B8%20%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BC%D0%B5%D1%82%D0%B0%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5}](%7Bhttps://wiki.astralinux.ru/pages/viewpage.action?pageId=149063848#:~:text=Common%20Edition%202.12-,%D0%A7%D1%82%D0%BE%20%D1%82%D0%B0%D0%BA%D0%BE%D0%B5%20%D1%80%D0%B0%D1%81%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5%20%D0%B0%D1%82%D1%80%D0%B8%D0%B1%D1%83%D1%82%D1%8B,%D1%81%20%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D1%8B%D0%BC%D0%B8%20%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%B0%D0%BC%D0%B8%20%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BC%D0%B5%D1%82%D0%B0%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5%7D).

4. Введение в SELinux под CentOS Stream [Электронный ресурс]. URL: <https://ruvds.com/ru/helpcenter/vvedenie-v-selinux-pod-centos-stream/>.

5. Документация Rocky Linux [Электронный ресурс]. URL: <https://docs.rockylinux.org/>.

6. Git-Guides [Электронный ресурс]. URL: <https://github.com/git-guides>.

7. VirtualBox [Электронный ресурс]. URL: <https://www.virtualbox.org/>.