Управление SELinux

Часть 1

Славинский В.В.

1 ноября 2025

Российский университет дружбы народов, Москва, Россия Россия

Информация

Докладчик

::::::::::::::: {.columns align=center} ::: {.column width="70%"}

- Славинский Владислав Вадимович
- Студент
- Российский университет дружбы народов
- [1132246169@pfur.ru]

::: ::: {.column width="30%"}

Вводная часть

Просмотр информации о состоянии SELinux с помощью root прав

Запускаем терминал в режиме суперпользователя через su - и просмотрим текущую информацию о состоянии SELinux: sestatus -v. 1) SELinux status: enabled - это строчка означает, что SELinux активирован. 2) SELinux mount - SELinux смонтирована в каталоге /sys/fs/selinux, SELinux root directory - корневой каталог конфигурации SELinux находится в /etc/selinux, 3) Loaded policy name - загружена политика безопасности типа targeted, которая защищает только определенные системные процессы, 4) Current mode: enforcing - принудительный режим работы, SELinux активно блокирует действия, нарушающие политику безопасности, 5) Mode from config file: enforcing - режим конфигурационного файла установлен как enforcing, что означает сохранение этого режима после перезагрузки, 6) Policy MLS status: enabled - поддержка многоуровневой безопасности активирована (Multi-Level-Security), 7) Policy deny_unknown status: allowed - неизвестные действия по умолчанию разрешены, 8) Memory protection checking: actual (secure) - проверка защиты памяти выполнеяется на безопасном уровне, 9) Max kernel policy version: 33 - максимальная поддерживаемая версия политики ядра 33, 10) Current context - Текущий процесс (терминал)

Посмотрим, в каком режиме работает SELinux: getenforce. Видим, что работает в режиме enforcing (в режиме принудительного исполнения.

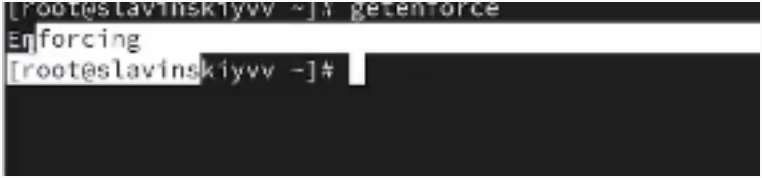


Рис. 2: sc2

Изменения режима работы

Изменим режим работы SELinux на разрешающий (Permissive): setenforce 0. Потом введем снова getenforce.

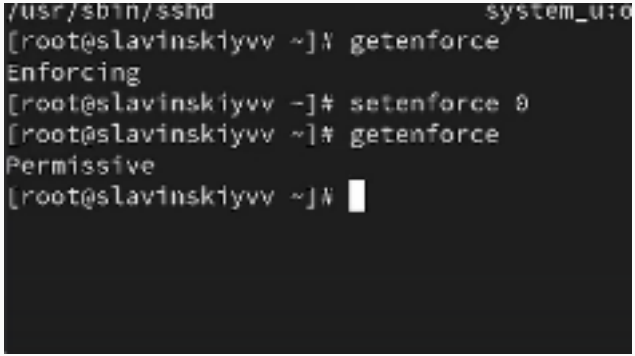
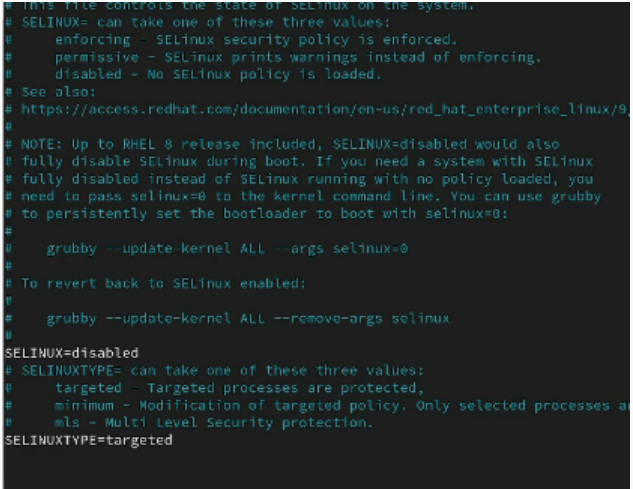


Рис. 3: sc3

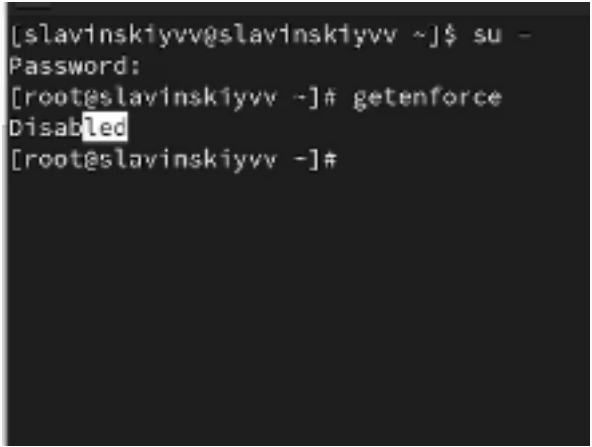
Изменение файла и перезапуск системы

В файле /etc/sysconfig/selinux с помощью редактора установим SELINUX=disabled и перезапустим систему.



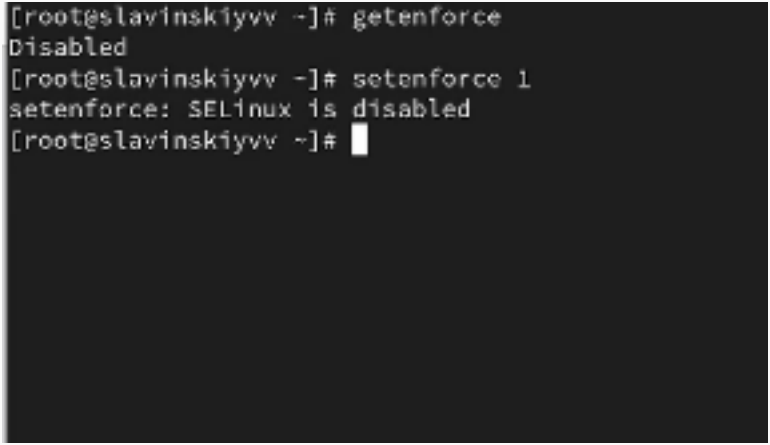
Перезагрузки и проверка статуса SELinux

После перезагрузки запустим терминал и получим полномочия администратора.Посмотрим статус SELinux: getenforce. Мы видим, что SELinux теперь отключён.



Попытка переключить режим работы SELinux

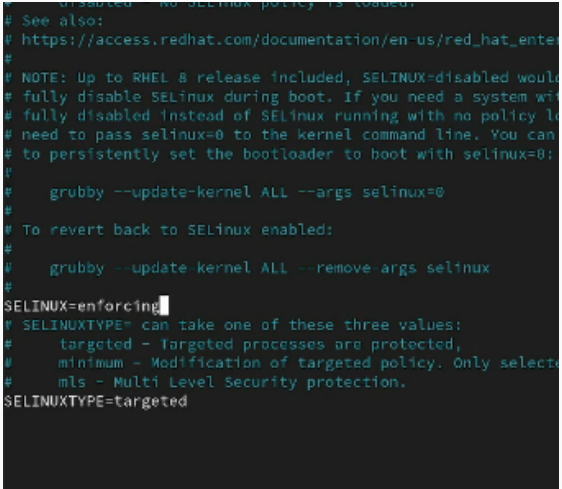
Попробуем переключить режим работы SELinux: setenforce 1. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы



Редактирование файла и перезагрузка системы

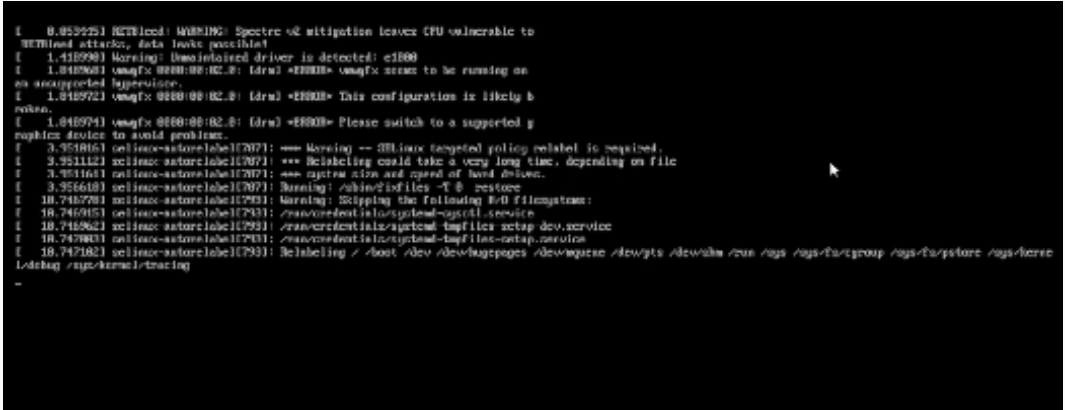
Откроем файл /etc/sysconfig/selinux с помощью редактора и установим: SELINUX=enforcing.

Затем перезагрузим систему.



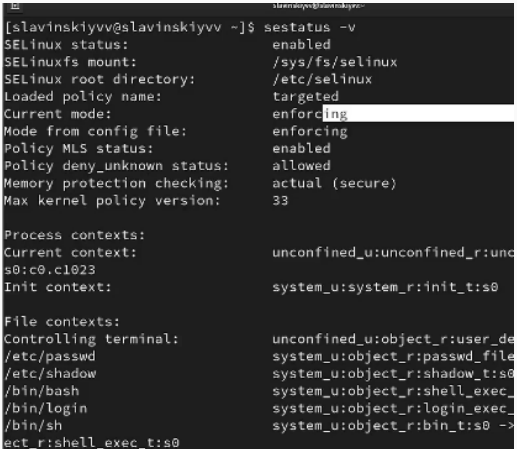
Перезагрузка системы

Во время загрузки системы мы получаем предупреждающее сообщение (Relabeling could take a very long time) о необходимости восстановления меток SELinux, это занимает некоторое время, а также труебется дополнительная перезагрузка системы.



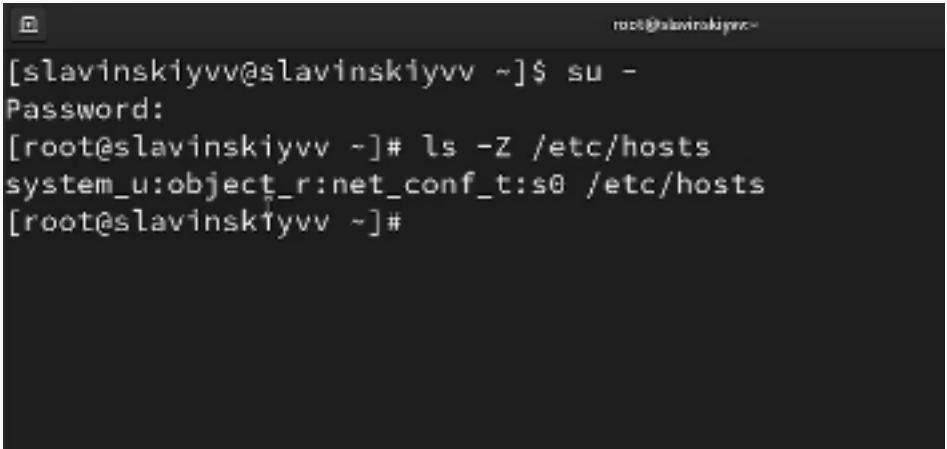
Проверка статуса

После перезагрузки в терминале с полномочиями администратора просмотрим текущую информацию о состоянии SELinux: sestatus -v. Видим, что система работает в режиме enforcing.



Просмотр контекста безопасности файла

Запустим терминал и получим полномочия администратора. Затем посмотрим контекст безопасности файла /etc/hosts: ls -Z /etc/hosts. Видим, что присутствует метка net_conf_t, что указывает на тип файла сетевой конфигурации.



Копирование файла в домашний каталог

Скопируем файл /etc/hosts в домашний каталог: cp /etc/hosts ~/, проверим контекст файла ~/hosts: ls -Z ~/hosts. Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin_home_t.

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

Перезапись файла из домашнего каталога

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: mv ~/hosts /etc. И убедимся, что что тип контекста по-прежнему установлен на admin_home_t: ls -Z /etc/hosts.

```
[slavinskiyvv@slavinskiyvv ~]$ su -
Password:
[root@slavinskiyvv ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@slavinskiyvv ~]# cp /etc/hosts ~/
[root@slavinskiyvv ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@slavinskiyvv ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@slavinskiyvv ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@slavinskiyvv ~]#
```

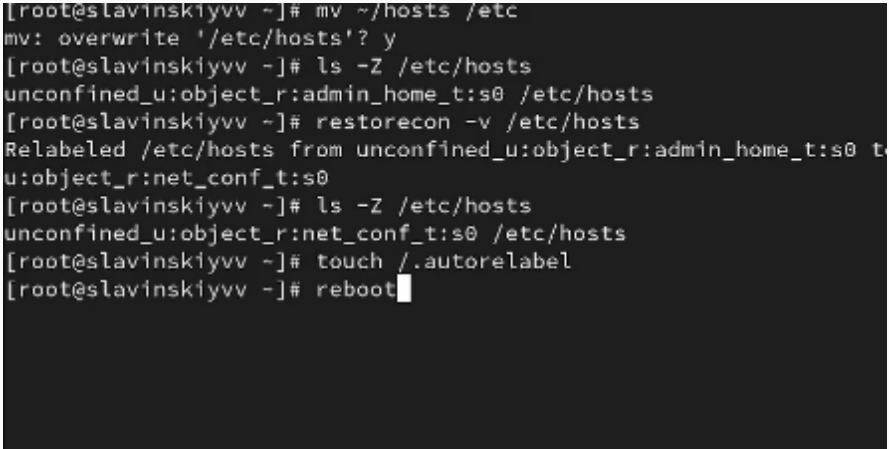
Исправление конекста безопасности

Исправим контекст безопасности: restorecon -v /etc/hosts. Опция -v покажет нам процесс изменения. И проверим, что что тип контекста изменился: ls -Z /etc/hosts.

```
[root@slavinskiyvv ~]# cp /etc/hosts ~/
[root@slavinskiyvv ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@slavinskiyvv ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@slavinskiyvv ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@slavinskiyvv ~]# 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@slavinskiyvv ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@slavinskiyvv ~]#
```

Массовое исправление контекста безопасности

Для массового исправления контекста безопасности на файловой системе введем touch /.autorelabel и перезагрузим систему. Во время перезапуска нажмем клавишу esc чтобы мы увидели загрузочные сообщения.



Перемаркированные сообщения на перезагрузке

Вот какие сообщения выводятся при перезагрузке.

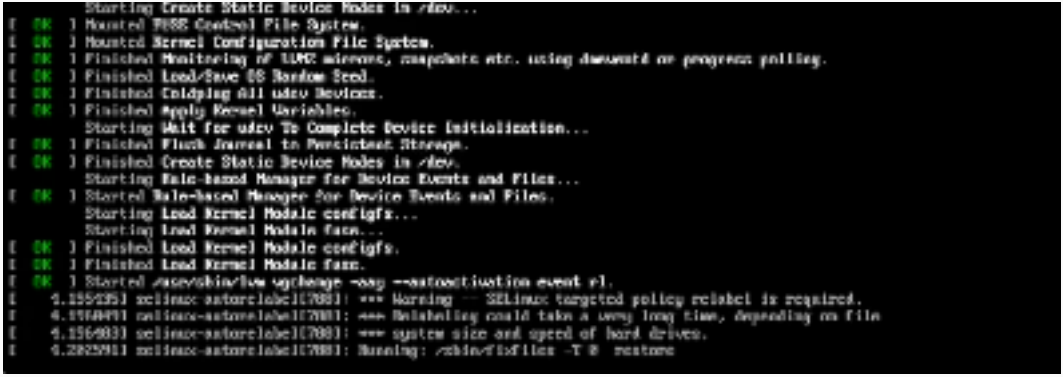
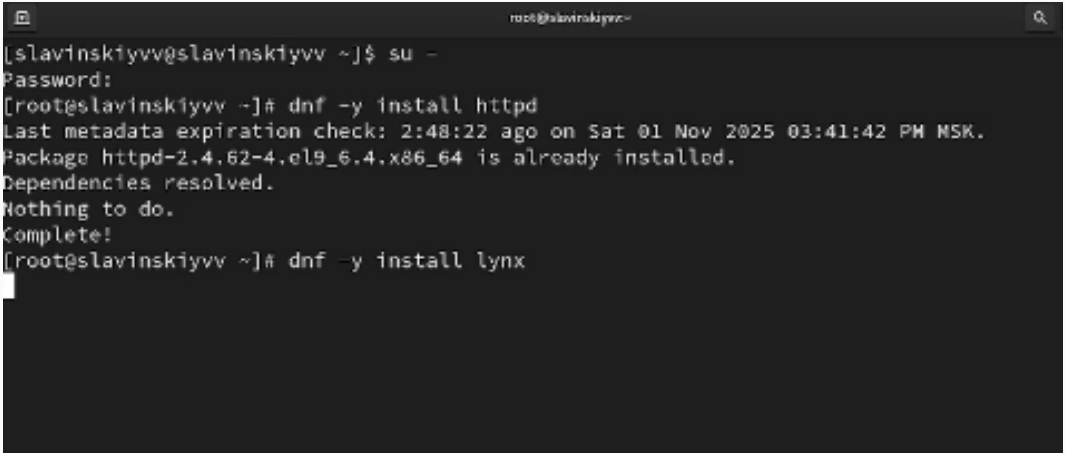


Рис. 15: sc15

Установка ПО

Запустим терминал в режиме администратора. Затем установим необходимое программное обеспечение: dnf -y install httpd, dnf -y install lynx.



Создание нового хранилища для файлов web-сервера

Создадим новое хранилище для файлов web-сервера: mkdir /web. Создадим файл index.html в каталоге с контентом веб-сервера: cd /web, touch index.html.

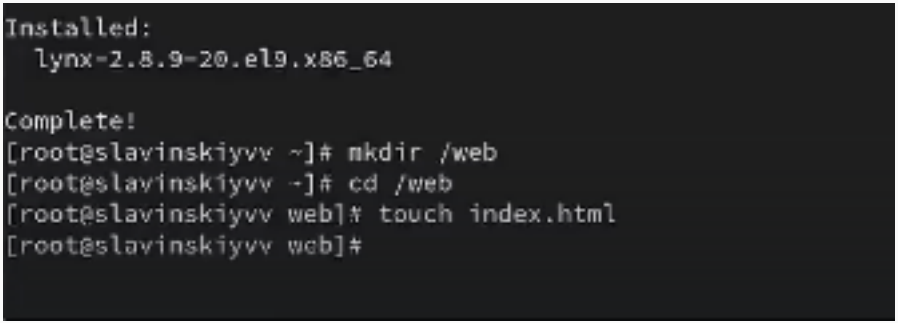
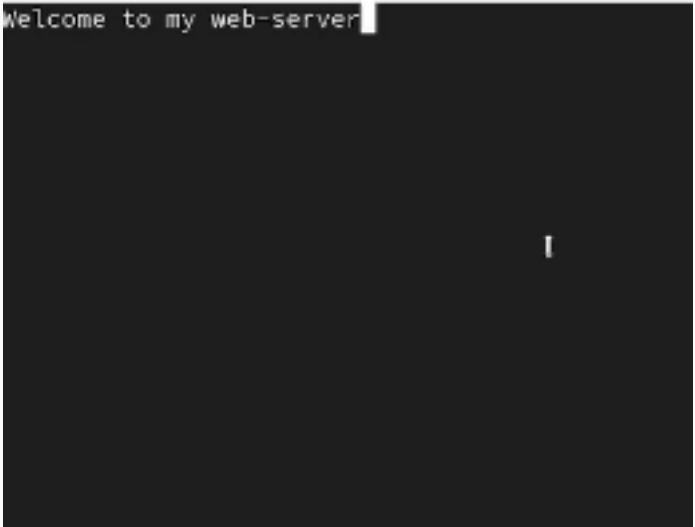


Рис. 17: sc17

Вставка текста

Поместим в этот файл следующий текст: Welcome to my web-server.



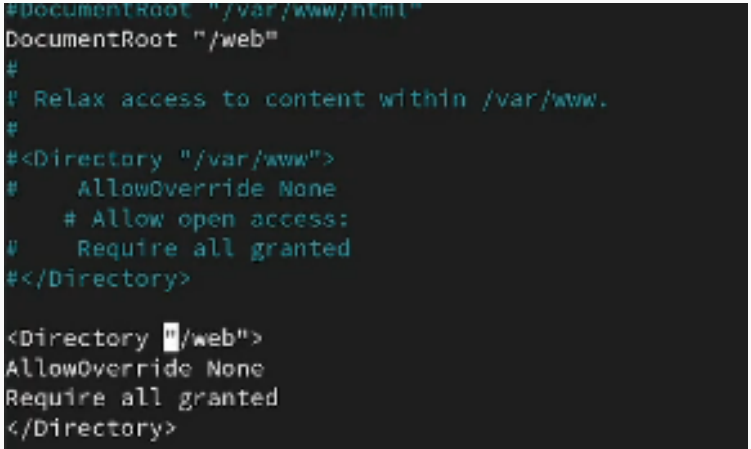
Редактирование файла httpd.conf

В файле /etc/httpd/conf/httpd.conf закомментируем строку DocumentRoot “/var/www/html” и ниже добавим строку DocumentRoot “/web”.

Рис. 19: sc19

Редактирование файла httpd.conf

Затем в этом же файле ниже закомментируем раздел <Directory “/var/www”> AllowOverride None Require all granted и добавим следующий раздел, определяющий правила доступа: <Directory “/web”> AllowOverride None Require all granted .



Запустим веб-сервер и службу httpd: systemctl start httpd, systemctl enable httpd.

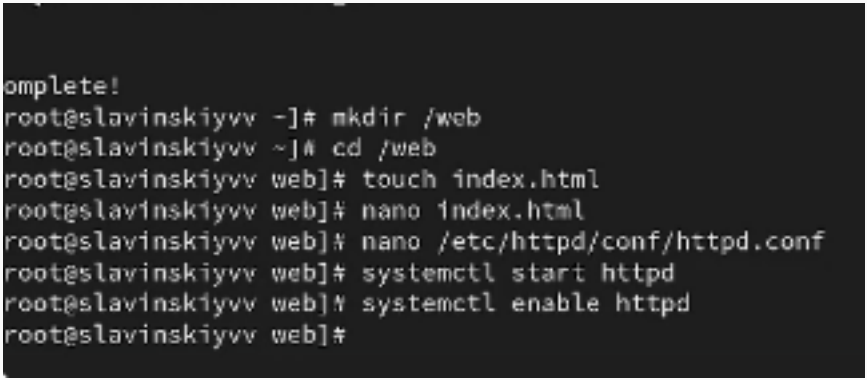
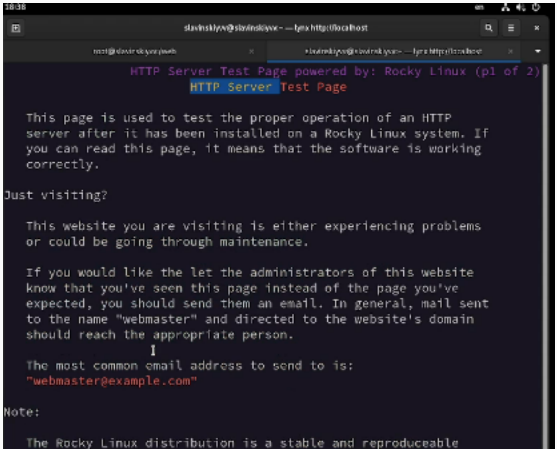


Рис. 21: sc21

В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx введем: lynx http://localhost. Мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.



Применение новой метки контекста

В терминале с полномочиями администратора применим новую метку контекста к /web: semanage fcontext -a -t httpd_sys_content_t “/web(/.*)?“.

```
Complete!
[root@slavinskiyvv ~]# mkdir /web
[root@slavinskiyvv ~]# cd /web
[root@slavinskiyvv web]# touch index.html
[root@slavinskiyvv web]# nano index.html
[root@slavinskiyvv web]# nano /etc/httpd/conf/httpd.conf
[root@slavinskiyvv web]# systemctl start httpd
[root@slavinskiyvv web]# systemctl enable httpd
[root@slavinskiyvv web]# semanage fcontext -a -t httpd_sys_content_t "/w
eb(/.*)?"
[root@slavinskiyvv web]#
```


Рис. 23: sc23

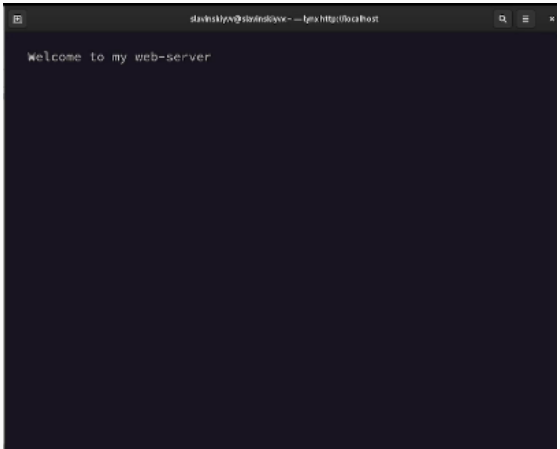
Восстановим контекст безопасности: restorecon -R -v /web.

```
[root@slavinskiyvv web]# semanage fcontext -a -t httpd_sys_content_t "/w
eb(/.*)?"
[root@slavinskiyvv web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:o
bject_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unc
onfined_u:object_r:httpd_sys_content_t:s0
[root@slavinskiyvv web]#
```

Рис. 24: sc24

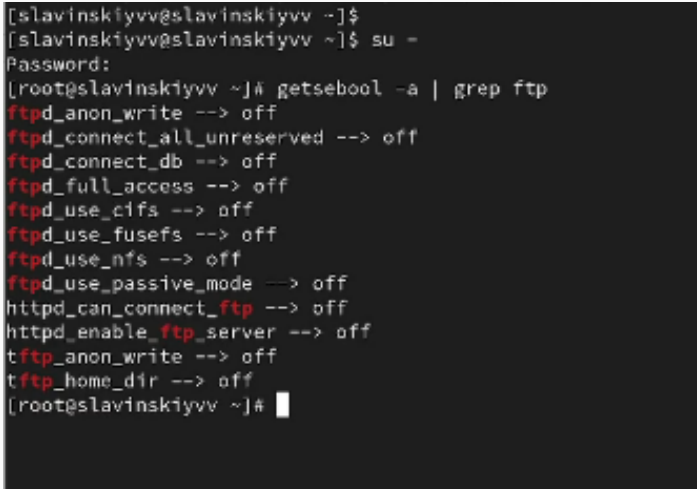
Проверка веб-сервера

В терминале под учётной записью своего пользователя снова обратимся к веб-серверу: lynx http://localhost. У нас ничего не произошло. Значит перезапускаем систему и опять обращаемся к веб-серверу. Как видим, у нас все получилось.



Список переключателей SELinux

Через полномочия администратора посмотрим список переключателей SELinux для службы ftp: getsebool -a | grep ftp.



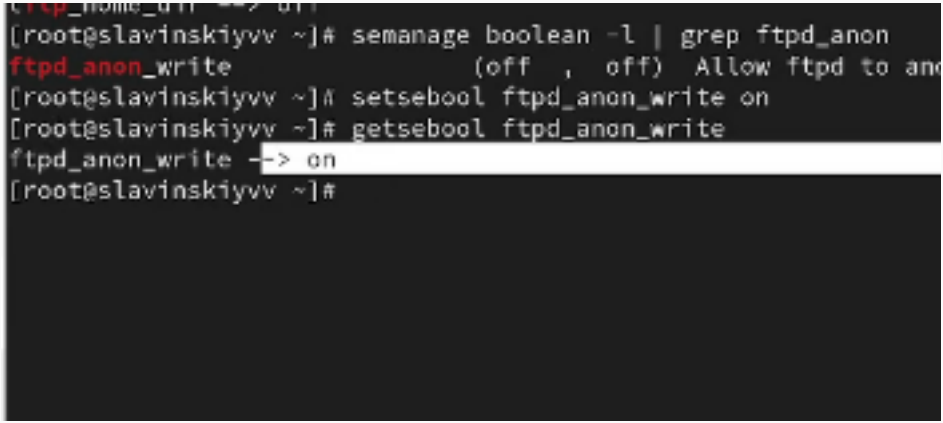
Список переключателей

Для службы ftpd_anon посмотрим список переключателей: semanage boolean -l | grep ftpd_anon. Первое значение off - текущее состояние выполнение времени, второе значение off - постоянное состояние. Ftpd_anon_write разрешает или запрещает анонимным пользователям FTP выполнять операции записи.

```
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@slavinskiyvv ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write                (off  ,  off)  Allow ftpd to anon write
[root@slavinskiyvv ~]#
```

Изменения значения переключателя

Изменим текущее значение переключателя для службы ftpd_anon_write с off на on: setsebool ftpd_anon_write on. Повторно посмотрим список переключателей SELinux для службы ftpd_anon_write: getsebool ftpd_anon_write.



Просмотр списка переключателей

Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon. Видим, что настройка времени выполнения включена, но постоянная настройка выключена.

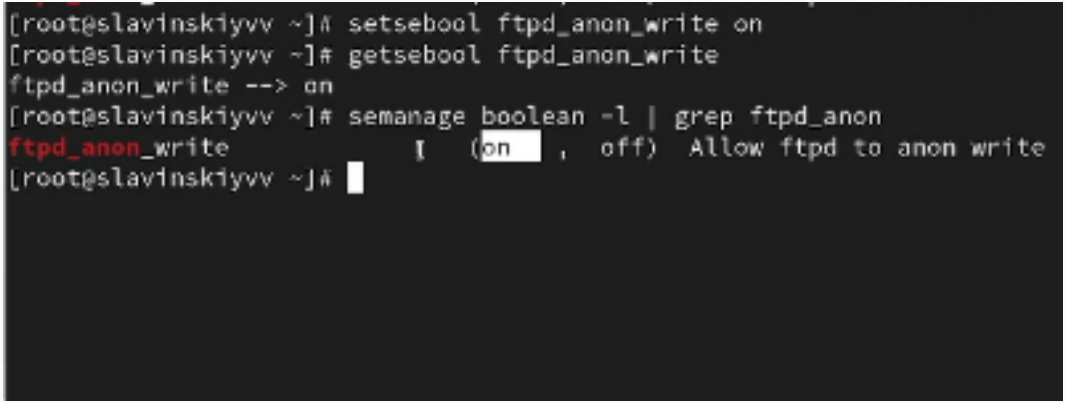


Рис. 29: sc29

Изменение постоянного значения переключателя

Изменим постоянное значение переключателя для службы ftpd_anon_write с off на on: setsebool -P ftpd_anon_write on. Посмотрим список переключателей: semanage boolean -l | grep ftpd_anon. Теперь у нас fttpd_anon_write полностью включен. Оба значения установлены на on: 1) включены состояние во время выполнения и постоянное состояние после перезагрузки. Теперь анонимные пользователи FTP могут выполнять операции записи на сервер.

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