

# **Лабораторная работа №9**

**Управление SELinux**

Комягин Андрей Николаевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
2.1	Управление режимами SELinux . . . . .	6
2.2	Использование restorecon для восстановления контекста безопасности . . . . .	10
2.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера . . . . .	11
2.4	Работа с переключателями SELinux . . . . .	14
<b>3</b>	<b>Контрольные вопросы</b>	<b>15</b>
<b>4</b>	<b>Вывод</b>	<b>16</b>
	<b>Список литературы</b>	<b>17</b>

## Список иллюстраций

2.1	Состояние и режим работы SELinux . . . . .	6
2.2	SELINUX=disabled . . . . .	8
2.3	Переключение режимов . . . . .	9
2.4	SELINUX=enforcing . . . . .	9
2.5	информация о состоянии . . . . .	10
2.6	контекст безопасности . . . . .	11
2.7	перемаркировка . . . . .	11
2.8	установка по . . . . .	12
2.9	web-сервер . . . . .	12
2.10	редактирование /etc/httpd/conf/httpd.conf . . . . .	13
2.11	запуск сервера и службы . . . . .	13
2.12	новая метка контекста к веб . . . . .	14
2.13	веб-сервер . . . . .	14
2.14	режимы системы . . . . .	14

## **Список таблиц**

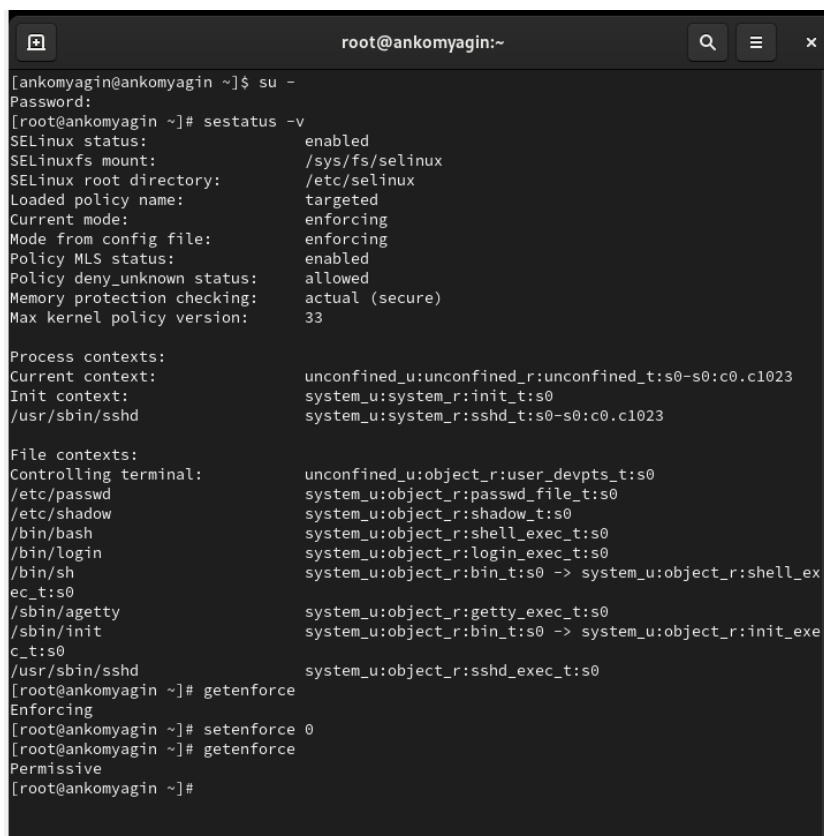
# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

## 2 Выполнение лабораторной работы

### 2.1 Управление режимами SELinux

Посмотрим текущую информацию о состоянии SELinux. Посмотрим, в каком режиме работает SELinux, изменим режим работы SELinux на разрешающий. (рис. 2.1).



```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# 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@ankomyagin ~]# getenforce  
Enforcing  
[root@ankomyagin ~]# setenforce 0  
[root@ankomyagin ~]# getenforce  
Permissive  
[root@ankomyagin ~]#
```

Рис. 2.1: Состояние и режим работы SELinux

#### 1. SELinux status:

- **enabled:** SELinux включен и работает.

**2. SELinuxfs mount:**

- Указывает, где в файловой системе смонтирована файловая система SELinux (/sys/fs/selinux).

**3. SELinux root directory:**

- Путь к директории, где хранятся конфигурационные файлы SELinux (/etc/selinux).

**4. Loaded policy name:**

- **targeted:** Загружена политика “targeted”, которая фокусируется на защите определённых процессов.

**5. Current mode:**

- **enforcing:** SELinux работает в режиме принудительного контроля, что означает, что он будет блокировать действия, которые нарушают политику безопасности.

**6. Mode from config file:**

- Показывает, что режим, указанный в конфигурационном файле, также “enforcing”.

**7. Policy MLS status:**

- **enabled:** Указывает на то, что поддержка многоуровневой безопасности (MLS) включена.

**8. Policy deny\_unknown status:**

- Указывает, разрешено ли блокирование неизвестных объектов.

**9. Memory protection checking:**

- Указывает на проверку защиты памяти.

#### 10. Max kernel policy version:

- Указывает максимальную версию политики ядра.

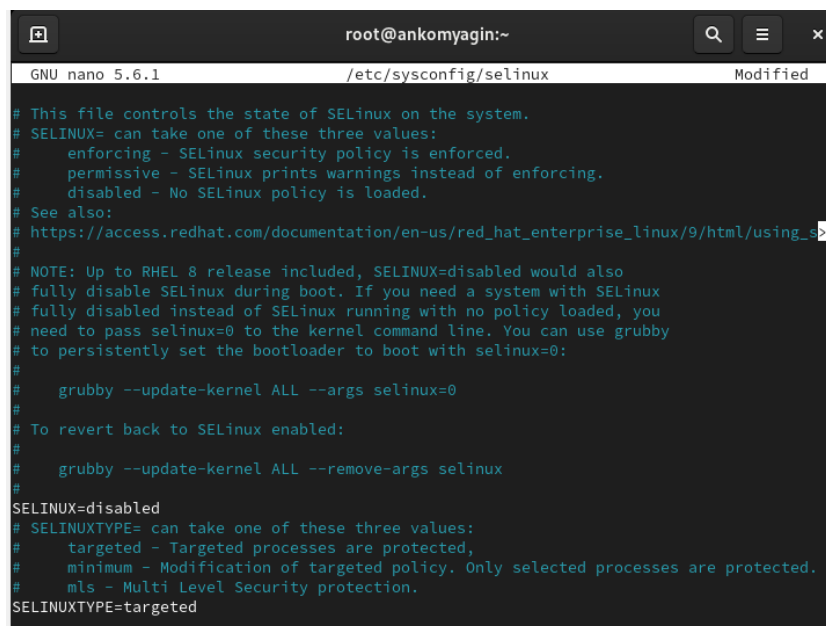
#### 11. Process contexts:

- Отображает контексты процессов, показывая текущие контексты безопасности для различных процессов.

#### 12. File contexts:

- Показаны контексты безопасности для различных файлов.

В файле `/etc/sysconfig/selinux` с помощью редактора установим **SELINUX=disabled** (рис. 2.2).

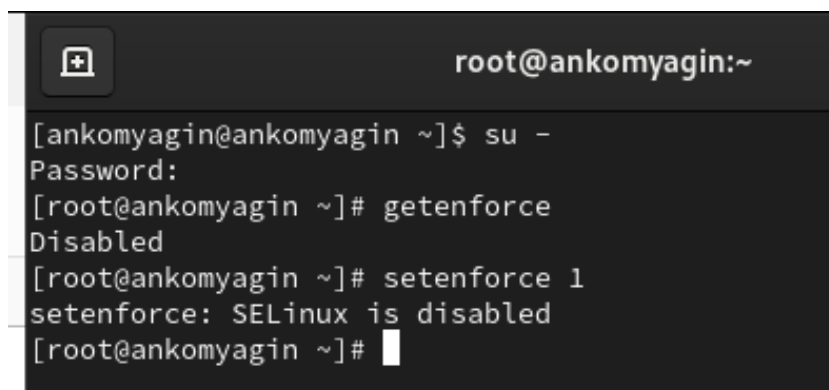


```
root@ankomyagin:~  
GNU nano 5.6.1 /etc/sysconfig/selinux Modified  
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
#   enforcing - SELinux security policy is enforced.  
#   permissive - SELinux prints warnings instead of enforcing.  
#   disabled - No SELinux policy is loaded.  
# See also:  
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/using_selinux-9  
# NOTE: Up to RHEL 8 release included, 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. 2.2: SELINUX=disabled

Посмотрим статус SELinux. Попробуем переключить режим работы SELinux. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы. (рис. 2.3).

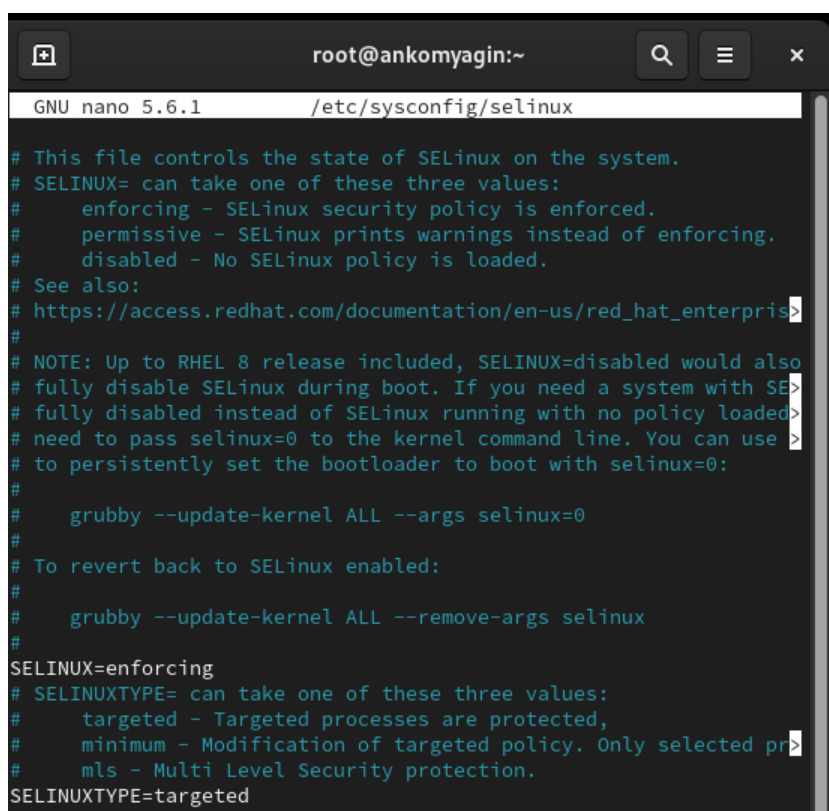


A terminal window titled 'root@ankomyagin:~' showing the process of switching SELinux modes. The user runs 'su -' to become root, then 'getenforce' which returns 'Disabled'. Then 'setenforce 1' is run, which returns 'setenforce: SELinux is disabled'. The prompt returns to root.

```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# getenforce  
Disabled  
[root@ankomyagin ~]# setenforce 1  
setenforce: SELinux is disabled  
[root@ankomyagin ~]#
```

Рис. 2.3: Переключение режимов

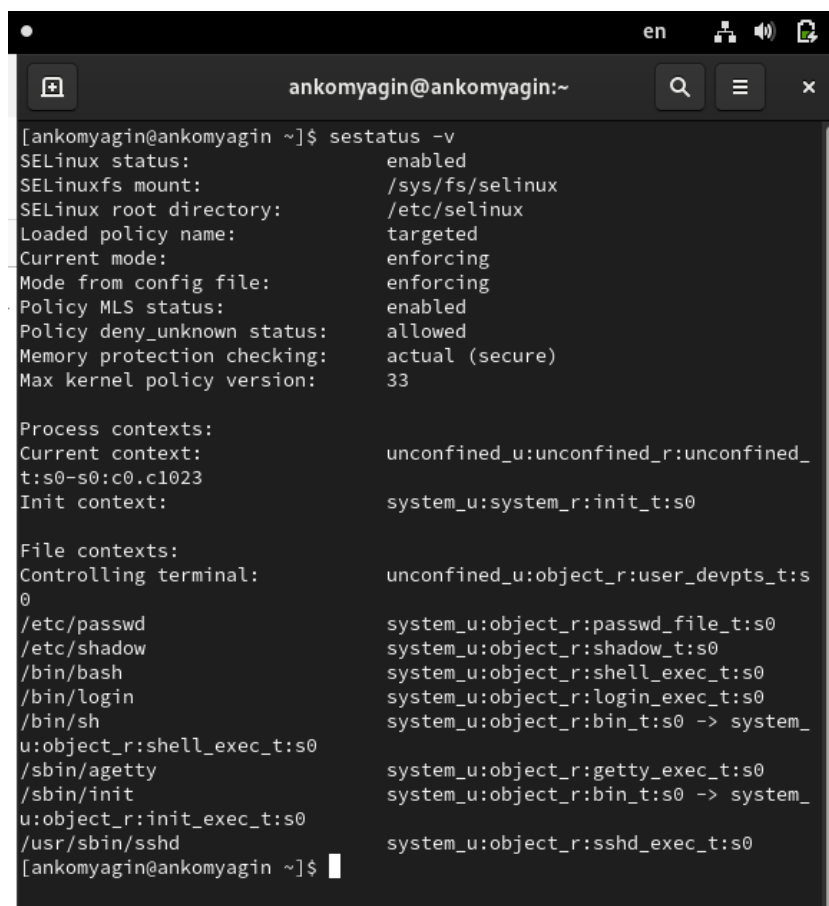
Откроем файл `/etc/sysconfig/selinux` с помощью редактора и установим: **SELINUX=enforcing** (рис. 2.4).

A terminal window titled 'root@ankomyagin:~' showing the contents of the file `/etc/sysconfig/selinux` edited with nano. The file contains instructions for SELinux configuration. The line `SELINUX=enforcing` is visible, along with other configuration options like `SELINUXTYPE=targeted`.

```
root@ankomyagin:~  
GNU nano 5.6.1 /etc/sysconfig/selinux  
# 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://access.redhat.com/documentation/en-us/red_hat_enterpris  
#  
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also  
# fully disable SELinux during boot. If you need a system with SE  
# fully disabled instead of SELinux running with no policy loaded  
# need to pass selinux=0 to the kernel command line. You can use  
# 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 pr  
#   mls - Multi Level Security protection.  
SELINUXTYPE=targeted
```

Рис. 2.4: SELINUX=enforcing

После перезагрузки посмотрим текущую информацию о состоянии SELinux (рис. 2.5).



```
[ankomyagin@ankomyagin ~]$ 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

File contexts:
Controlling terminal:          unconfined_u:object_r:user_devpts_t:s
0
/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
[ankomyagin@ankomyagin ~]$
```

Рис. 2.5: информация о состоянии

## 2.2 Использование restorecon для восстановления контекста безопасности

Посмотрим контекст безопасности файла `/etc/hosts`. Мы увидим, что у файла есть метка контекста `net_conf_t`.

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

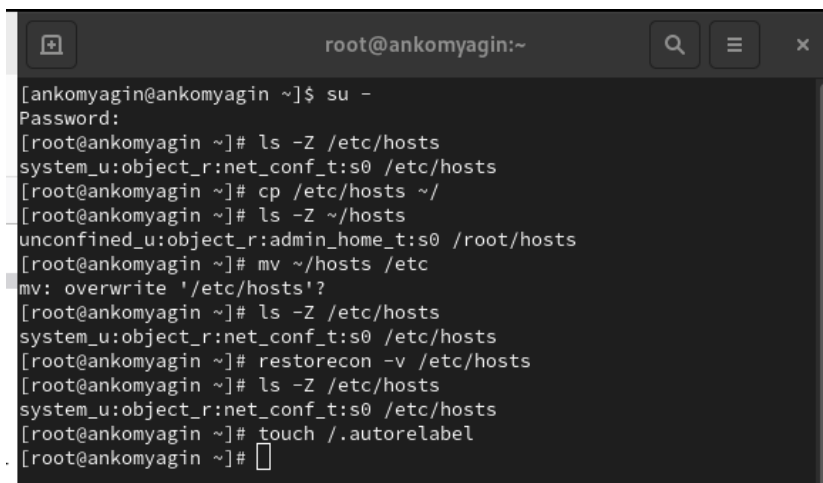
Попытаемся перезаписать существующий файл `hosts` из домашнего каталога в

каталог /etc: mv ~/hosts /etc

Убедимся, что тип контекста по-прежнему установлен на admin\_home\_t:

Исправим контекст безопасности и убедимся, что тип контекста изменился:

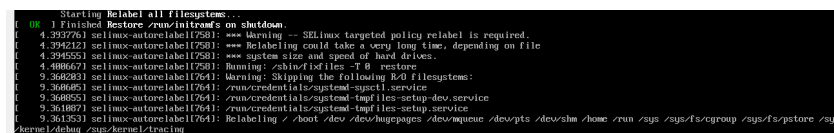
Для массового исправления контекста безопасности на файловой системе введём touch /.autorelabel(рис. 2.6)



```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[root@ankomyagin ~]# cp /etc/hosts ~/  
[root@ankomyagin ~]# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
[root@ankomyagin ~]# mv ~/hosts /etc  
mv: overwrite '/etc/hosts'?  
[root@ankomyagin ~]# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[root@ankomyagin ~]# restorecon -v /etc/hosts  
[root@ankomyagin ~]# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[root@ankomyagin ~]# touch /.autorelabel  
[root@ankomyagin ~]#
```

Рис. 2.6: контекст безопасности

Перезагрузим систему. Файловая система автоматически перемаркирована(рис. 2.7)

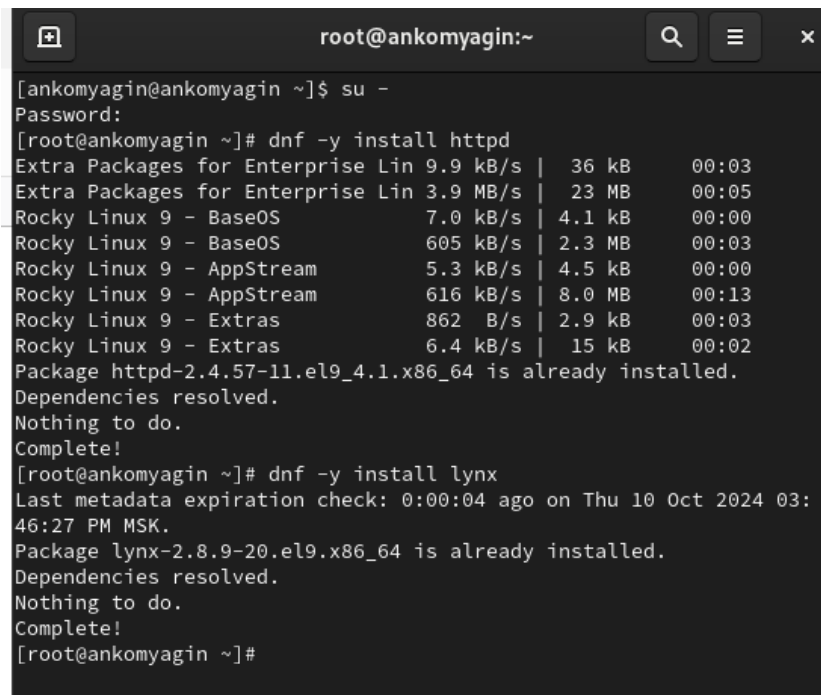


```
Starting Relabel all filesystems...  
[ OK ] Finished Restore /run/initramfs on shutdown.  
[ 4.393763] selinux-autorelabel(1758): *** Warning - SELinux targeted policy relabel is required.  
[ 4.394212] selinux-autorelabel(1758): *** Relabeling could take a very long time, depending on file  
[ 4.394555] selinux-autorelabel(1758): *** system size and speed of hard drives.  
[ 4.400622] selinux-autorelabel(1758): Relabeling /sbin/ldfiles -T 0 restore  
[ 9.368283] selinux-autorelabel(1764): Warning: Skipping the following R/O filesystems:  
[ 9.368659] selinux-autorelabel(1764): /run/credentials/systemd-sysctl.service  
[ 9.368953] selinux-autorelabel(1764): /run/credentials/systemd-tmpfiles-setup-dev.service  
[ 9.369187] selinux-autorelabel(1764): /run/credentials/systemd-tmpfiles-setup.service  
[ 9.369353] selinux-autorelabel(1764): Relabeling /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /home /run /sys /sys/fs/cgroup /sys/fs/pstore /sys  
/kernel/debug /sys/kernel/tracing
```

Рис. 2.7: перемаркировка

## 2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

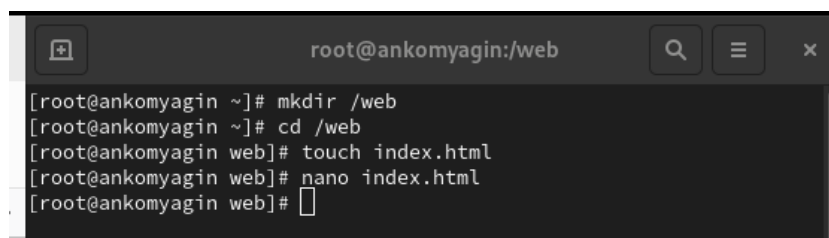
Установим необходимое программное обеспечение (рис. 2.8).



```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# dnf -y install httpd  
Extra Packages for Enterprise Lin 9.9 kB/s | 36 kB 00:03  
Extra Packages for Enterprise Lin 3.9 MB/s | 23 MB 00:05  
Rocky Linux 9 - BaseOS 7.0 kB/s | 4.1 kB 00:00  
Rocky Linux 9 - BaseOS 605 kB/s | 2.3 MB 00:03  
Rocky Linux 9 - AppStream 5.3 kB/s | 4.5 kB 00:00  
Rocky Linux 9 - AppStream 616 kB/s | 8.0 MB 00:13  
Rocky Linux 9 - Extras 862 B/s | 2.9 kB 00:03  
Rocky Linux 9 - Extras 6.4 kB/s | 15 kB 00:02  
Package httpd-2.4.57-11.el9_4.1.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@ankomyagin ~]# dnf -y install lynx  
Last metadata expiration check: 0:00:04 ago on Thu 10 Oct 2024 03:  
46:27 PM MSK.  
Package lynx-2.8.9-20.el9.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@ankomyagin ~]#
```

Рис. 2.8: установка по

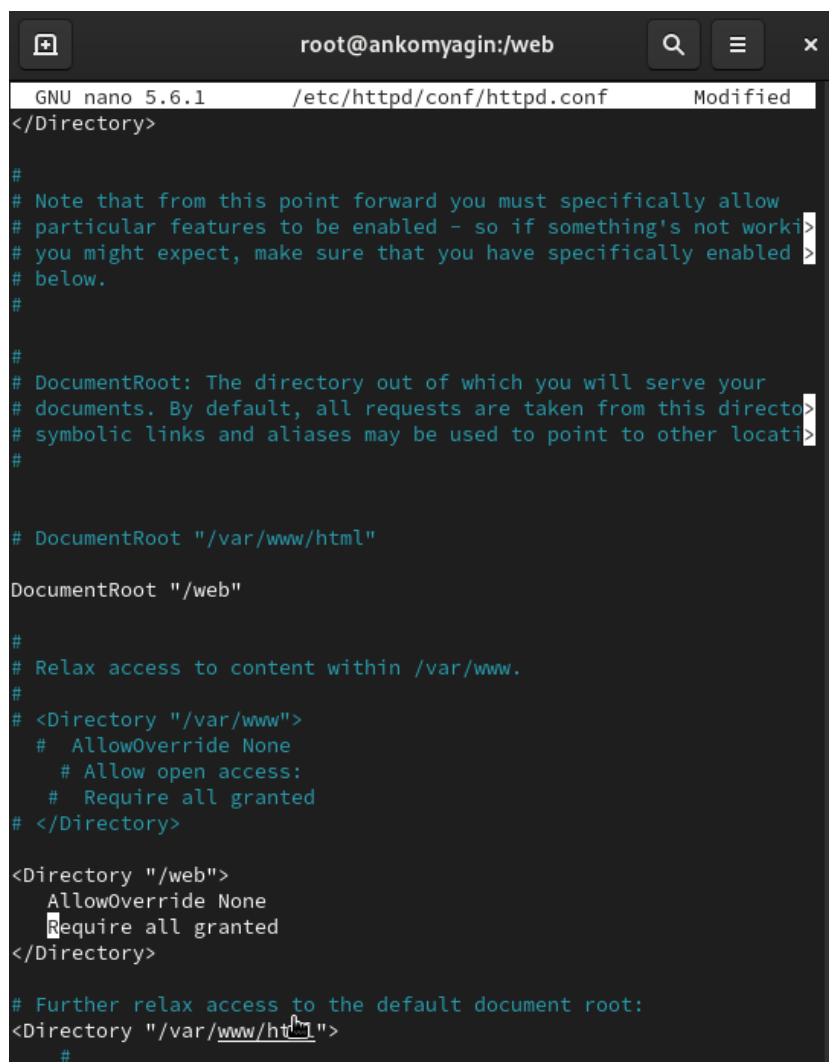
Создадим новое хранилище для файлов web-сервера. Создадим файл index.html в каталоге с контентом веб-сервера и поместим в файл **Welcome to my web-server**(рис. 2.9)



```
root@ankomyagin:/web  
[root@ankomyagin ~]# mkdir /web  
[root@ankomyagin ~]# cd /web  
[root@ankomyagin web]# touch index.html  
[root@ankomyagin web]# nano index.html  
[root@ankomyagin web]#
```

Рис. 2.9: web-сервер

Отредактируем файл **/etc/httpd/conf/httpd.conf**(рис. 2.10)



```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working
# you might expect, make sure that you have specifically enabled
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory
# symbolic links and aliases may be used to point to other locations
#

# DocumentRoot "/var/www/html"
DocumentRoot "/web"

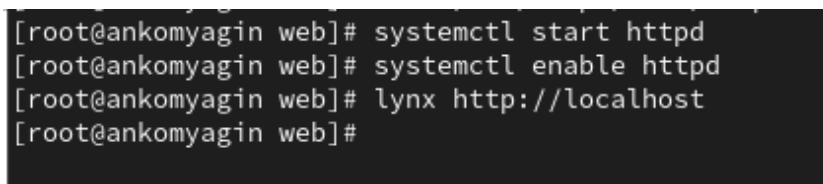
#
# Relax access to content within /var/www.
#
# <Directory "/var/www">
#   AllowOverride None
#   Allow open access:
#   Require all granted
# </Directory>

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

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
```

Рис. 2.10: редактирование /etc/httpd/conf/httpd.conf

Запустим веб-сервер и службу httpd(рис. 2.11)



```
[root@ankomyagin web]# systemctl start httpd
[root@ankomyagin web]# systemctl enable httpd
[root@ankomyagin web]# lynx http://localhost
[root@ankomyagin web]#
```

Рис. 2.11: запуск сервера и службы

Применим новую метку контекста к /web. Восстановим контекст безопасности.  
(рис. 2.12)

```

[root@ankomyagin web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@ankomyagin 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@ankomyagin web]# Lynx http://localhost

```

Рис. 2.12: новая метка контекста к веб

Обратимся к веб-серверу(рис. 2.13)

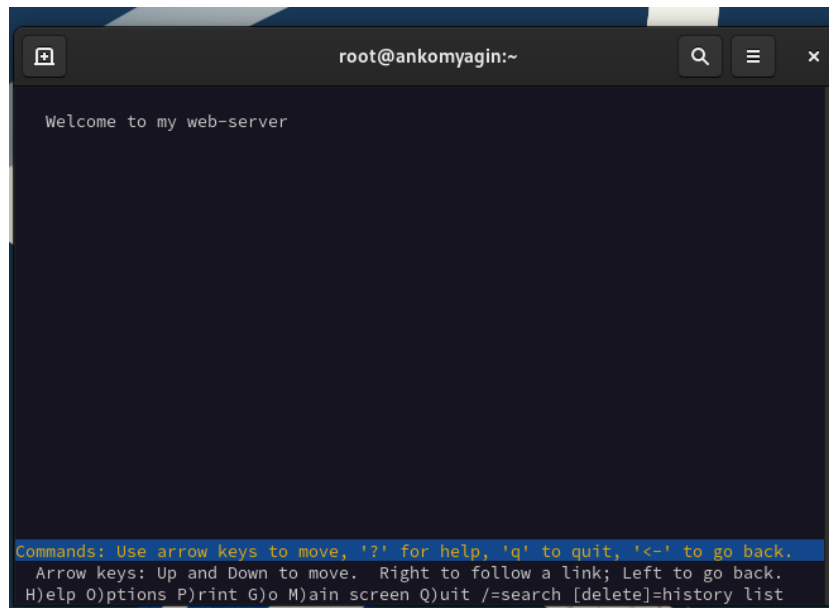


Рис. 2.13: веб-сервер

## 2.4 Работа с переключателями SELinux

Перезагрузим систему командой `reboot`. Вновь перезагрузим систему командой `reboot`. Убедимся, что система загрузилась в графическом режиме(рис. 2.14)

режимы системы

Рис. 2.14: режимы системы

### **3 Контрольные вопросы**

## 4 Вывод

В ходе выполнения лабораторной работы я получил навыки управления системными службами операционной системы посредством systemd.



# Список литературы

Туис, курс Администрирование операционных систем