

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №9

дисциплина: Основы администрирования операционных систем

Студент: Хамди Мохаммад, 1032235868

МОСКВА

2024 г.

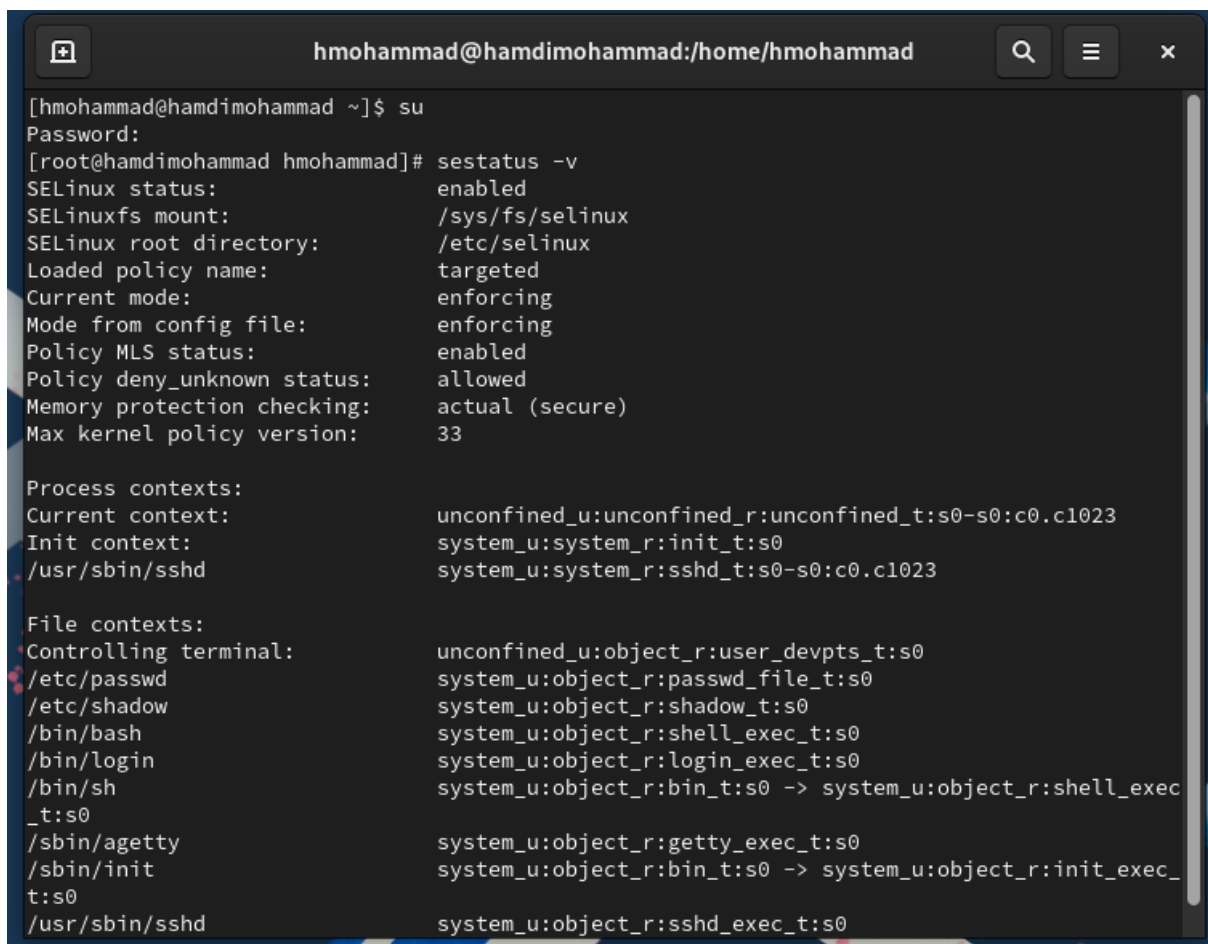
Постановка задачи

Получить навыки работы с контекстом безопасности и политиками SELinux.

Выполнение работы

Управление режимами SELinux

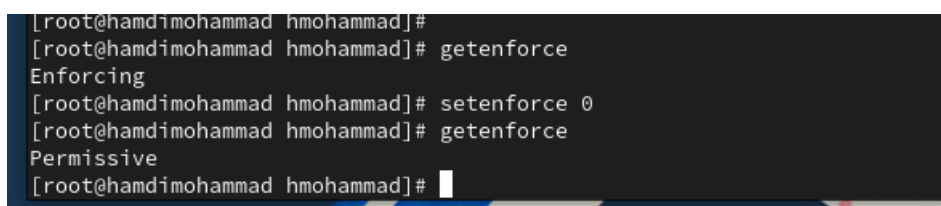
1. Запустите терминал и получите полномочия администратора: `su -`
2. Просмотрите текущую информацию о состоянии SELinux: `sestatus -v` В отчёте построчно поясните выведенную на экран информацию.
3. Посмотрите, в каком режиме работает SELinux: `getenforce` По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing).
4. Измените режим работы SELinux на разрешающий (Permissive): `setenforce 0` и снова введите `getenforce`



```
h mohammad@hamdimohammad:/home/h mohammad
[h mohammad@hamdimohammad ~]$ su
Password:
[root@hamdimohammad h mohammad]# 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

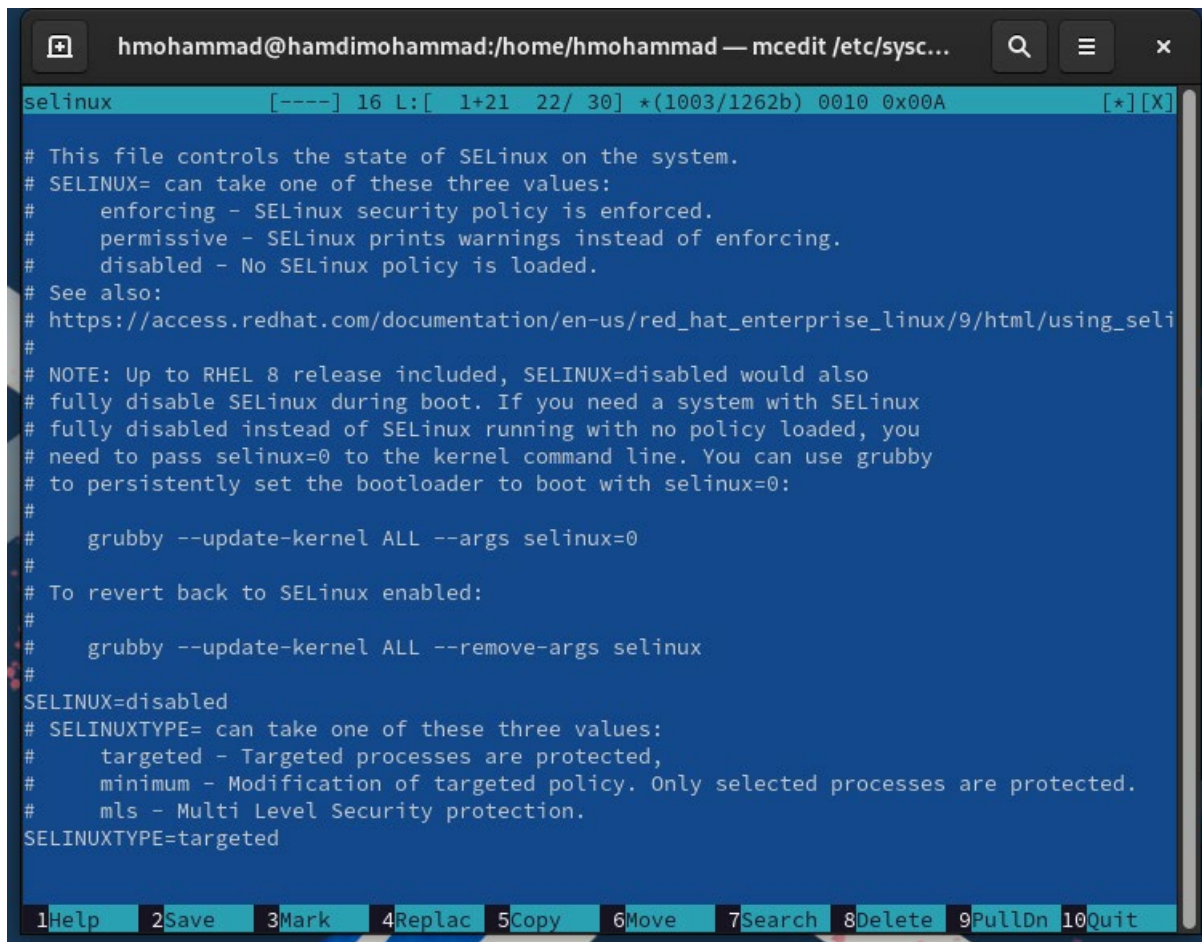
Process contexts:
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                 system_u:system_r:init_t:s0
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023

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@hamdimohammad h mohammad]#
[root@hamdimohammad h mohammad]# getenforce
Enforcing
[root@hamdimohammad h mohammad]# setenforce 0
[root@hamdimohammad h mohammad]# getenforce
Permissive
[root@hamdimohammad h mohammad]#
```

5. В файле `/etc/sysconfig/selinux` с помощью редактора установите `SELINUX=disabled`
Перезагрузите систему.



The screenshot shows a terminal window with the mcedit editor open, editing the file `/etc/sysconfig/selinux`. The editor's title bar reads `hmohammad@hamdimohammad:/home/hmohammad — mcedit /etc/sysc...`. The file content is as follows:

```
selinux [----] 16 L:[ 1+21 22/ 30] *(1003/1262b) 0010 0x00A [*] [X]

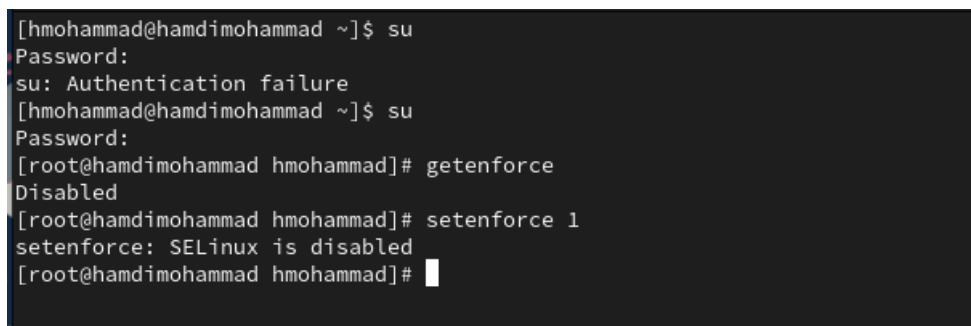
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux
#
# 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
```

The editor's status bar at the bottom shows the following menu items: 1Help, 2Save, 3Mark, 4Replac, 5Copy, 6Move, 7Search, 8Delete, 9PullDn, 10Quit.

6. После перезагрузки запустите терминал и получите полномочия администратора.

7. Посмотрите статус SELinux: `getenforce` Вы увидите, что SELinux теперь отключён.

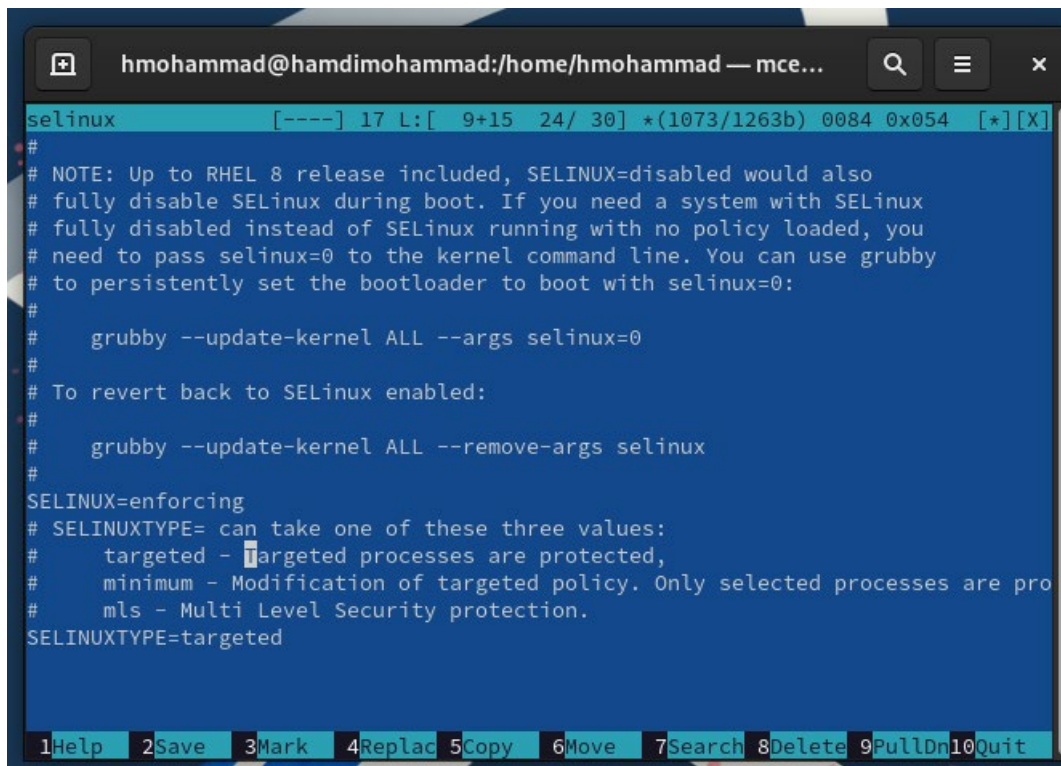
8. Попробуйте переключить режим работы SELinux: `setenforce 1` Какая реакция системы?
Вы не можете переключаться между отключённым и принудительным режимом без перезагрузки системы.



The screenshot shows a terminal session where the user `hmohammad` attempts to switch to the root user using `su`. The password prompt is shown, but the authentication fails. The user then runs `getenforce` and `setenforce 1` as root.

```
[hmohammad@hamdimohammad ~]$ su
Password:
su: Authentication failure
[hmohammad@hamdimohammad ~]$ su
Password:
[root@hamdimohammad hmohammad]# getenforce
Disabled
[root@hamdimohammad hmohammad]# setenforce 1
setenforce: SELinux is disabled
[root@hamdimohammad hmohammad]#
```

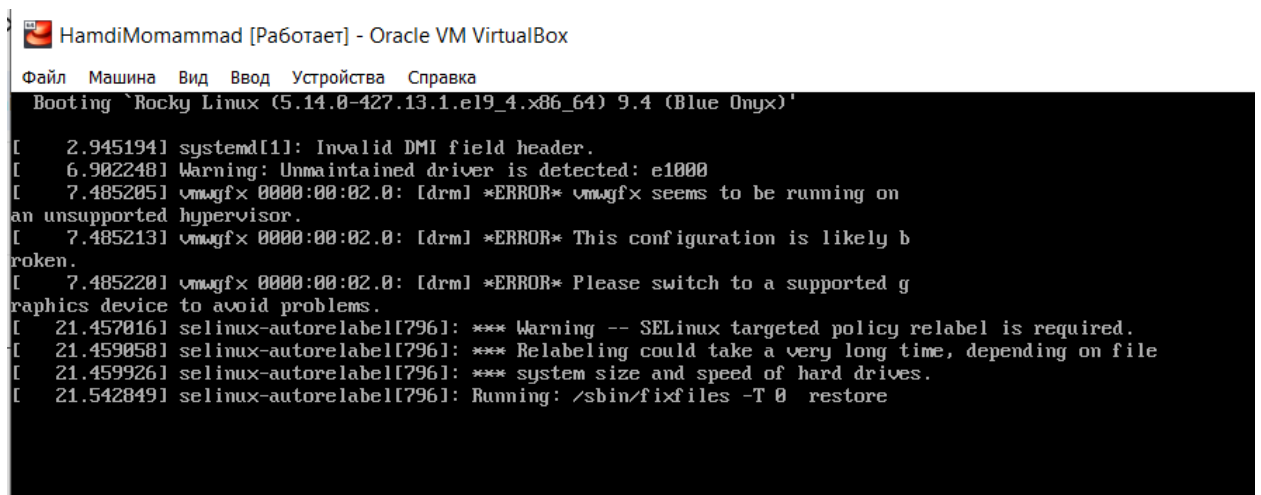
9. Откройте файл `/etc/sysconfig/selinux` с помощью редактора и установите: `SELINUX=enforcing` Перезагрузите систему.



```
hmmohammad@hamdimohammad:/home/hmmohammad — mce...
selinux [----] 17 L:[ 9+15 24/ 30] *(1073/1263b) 0084 0x054 [*][X]
#
# 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=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are pro
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn10Quit
```

10. Во время загрузки системы вы, скорее, всего получите предупреждающее сообщение о необходимости восстановления меток SELinux, что может занять некоторое время, а также потребует дополнительной перезагрузки системы.



```
HamdiMomammad [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Booting 'Rocky Linux (5.14.0-427.13.1.el9_4.x86_64) 9.4 (Blue Onyx)'
```

```
[ 2.945194] systemd[1]: Invalid DMI field header.
[ 6.902248] Warning: Unmaintained driver is detected: e1000
[ 7.485205] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 7.485213] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 7.485220] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 21.457016] selinux-autorelabel[796]: *** Warning -- SELinux targeted policy relabel is required.
[ 21.459058] selinux-autorelabel[796]: *** Relabeling could take a very long time, depending on file
[ 21.459926] selinux-autorelabel[796]: *** system size and speed of hard drives.
[ 21.542849] selinux-autorelabel[796]: Running: /sbin/fixfiles -T 0 restore
```

```
HamdiMammad [Работа] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Booting 'Rocky Linux (5.14.0-427.13.1.el9_4.x86_64) 9.4 (Blue Onyx)'
[ 2.945194] systemd[1]: Invalid DMI field header.
[ 6.982248] Warning: Unmaintained driver is detected: e1000
[ 7.485285] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 7.485213] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 7.485220] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 21.457816] selinux-autorelabel[796]: *** Warning -- SELinux targeted policy relabel is required.
[ 21.459858] selinux-autorelabel[796]: *** Relabeling could take a very long time, depending on file
[ 21.459926] selinux-autorelabel[796]: *** system size and speed of hard drives.
[ 21.542849] selinux-autorelabel[796]: Running: /sbin/fixfiles -T 0 restore
[ 42.538491] selinux-autorelabel[802]: Warning: Skipping the following R/O filesystems:
[ 42.531742] selinux-autorelabel[802]: /run/credentials/systemd-sysctl.service
[ 42.532445] selinux-autorelabel[802]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 42.533396] selinux-autorelabel[802]: /run/credentials/systemd-tmpfiles-setup.service
[ 42.534611] selinux-autorelabel[802]: Relabeling /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kern
el/debug /sys/kernel/tracing
```

11. После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux: `sestatus -v` Убедитесь, что система работает в принудительном режиме (enforcing) SELinux.

```
[hmohammad@hamdimohammad ~]$ 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: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
[hmohammad@hamdimohammad ~]$
```

Использование restorecon для восстановления контекста безопасности

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите контекст безопасности файла /etc/hosts: `ls -Z /etc/hosts` Вы увидите, что у файла есть метка контекста `net_conf_t`.
3. Скопируйте файл /etc/hosts в домашний каталог: `cp /etc/hosts ~/` Проверьте 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`.
4. Попробуйте перезаписать существующий файл hosts из домашнего каталога в каталог /etc: `mv ~/hosts /etc` и подтвердите, что вы хотите сделать это.
5. Убедитесь, что тип контекста по-прежнему установлен на `admin_home_t`: `ls -Z /etc/hosts`
6. Исправьте контекст безопасности: `restorecon -v /etc/hosts` Опция `-v` покажет процесс изменения.
7. Убедитесь, что тип контекста изменился: `ls -Z /etc/hosts`
8. Для массового исправления контекста безопасности на файловой системе введите `touch /.autorelabel` и перезагрузите систему. Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения. Вы увидите, что файловая система автоматически перемаркирована.

```
[root@hamdimohammad hmohammad]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@hamdimohammad hmohammad]# cp /etc/hosts ~
[root@hamdimohammad hmohammad]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@hamdimohammad hmohammad]# mv ~/hosts /etc/
mv: overwrite '/etc/hosts'? y
[root@hamdimohammad hmohammad]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@hamdimohammad hmohammad]# touch /.autorelabel
[root@hamdimohammad hmohammad]#
```

```
HamdiMomammad [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройство Справка
[ 2.936576] systemd[1]: Invalid DMI field header.
[ 6.333630] Warning: Unmaintained driver is detected: e1000
[ 6.794049] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 6.794052] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 6.794054] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 21.674536] selinux-autorelabel[794]: *** Warning -- SELinux targeted policy relabel is required.
[ 21.676274] selinux-autorelabel[794]: *** Relabeling could take a very long time, depending on file
[ 21.677520] selinux-autorelabel[794]: *** system size and speed of hard drives.
[ 21.766258] selinux-autorelabel[794]: Running: /sbin/fixfiles -T 0 restore
[ 43.209698] selinux-autorelabel[800]: Warning: Skipping the following R/O filesystems:
[ 43.210451] selinux-autorelabel[800]: /run/credentials/systemd-sysctl.service
[ 43.211458] selinux-autorelabel[800]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 43.212157] selinux-autorelabel[800]: /run/credentials/systemd-tmpfiles-setup.service
[ 43.212887] selinux-autorelabel[800]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kern
l/debug /sys/kernel/tracing
```


Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Запустите терминал и получите полномочия администратора.
2. Установите необходимое программное обеспечение: `dnf -y install httpd` `dnf -y install lynx`
3. Создайте новое хранилище для файлов веб-сервера: `mkdir /web`
4. Создайте файл `index.html` в каталоге с контентом веб-сервера: `cd /web touch index.html` и поместите в файл следующий текст: `Welcome to my web-server`

```
Running transaction
Preparing      :                               1/1
Installing     : lynx-2.8.9-20.el9.x86_64      1/1
Running scriptlet: lynx-2.8.9-20.el9.x86_64    1/1
Verifying      : lynx-2.8.9-20.el9.x86_64      1/1

Installed:
  lynx-2.8.9-20.el9.x86_64

Complete!
[root@hamdimohammad hmoammad]# mkdir /web
[root@hamdimohammad hmoammad]# cd /web
[root@hamdimohammad web]# touch index.html
[root@hamdimohammad web]# echo "Welcome to my web-server" > index.html
[root@hamdimohammad web]#
```

5. В файле `/etc/httpd/conf/httpd.conf` закомментируйте строку `DocumentRoot "/var/www/html"` и ниже добавьте строку `DocumentRoot "/web"` Затем в этом же файле ниже закомментируйте раздел `AllowOverride None` `Require all granted` и добавьте следующий раздел, определяющий правила доступа: `AllowOverride None` `Require all granted`

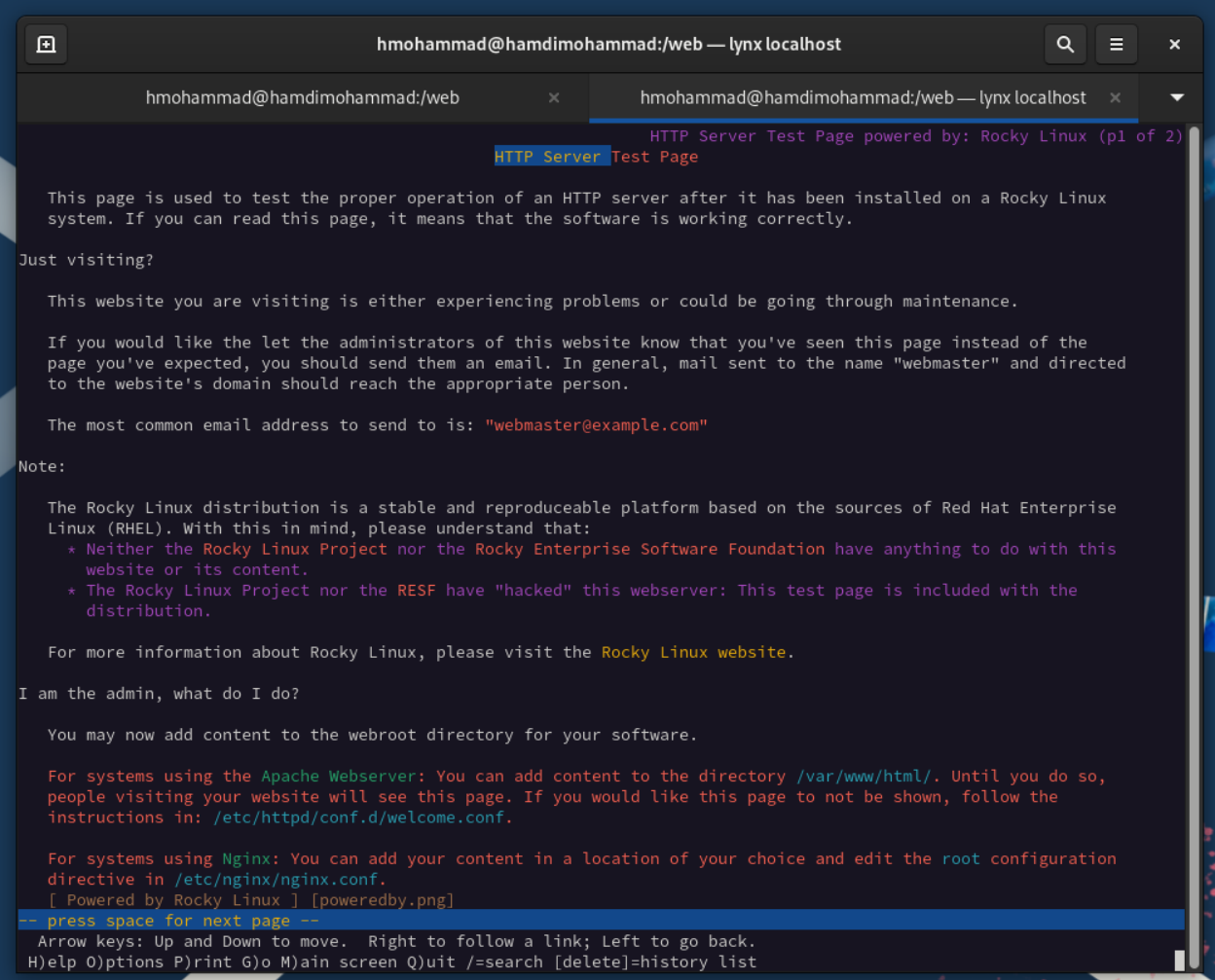
```
hmoammad@hamdimohammad:/web — mcedit /etc/httpd/conf/httpd.conf
httpd.conf  [----]  0 L:[109+18 127/368] *(4549/12136b) 0010 0x00A
  Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
#DocumentRoot "/var/www/html"

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

6. Запустите веб-сервер и службу http: `systemctl start httpd` `systemctl enable httpd`

7. В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: `lynx http://localhost` вы увидите веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла `index.html`. В нижней части терминала с lynx указаны подсказки по навигации. Для выхода из lynx нажмите `q`.



```
hmoammad@hamdimohammad:/web — lynx localhost
hmoammad@hamdimohammad:/web  x  hmoammad@hamdimohammad:/web — lynx localhost  x
HTTP Server Test Page powered by: Rocky Linux (p1 of 2)
HTTP Server Test Page

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 reproduceable 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.

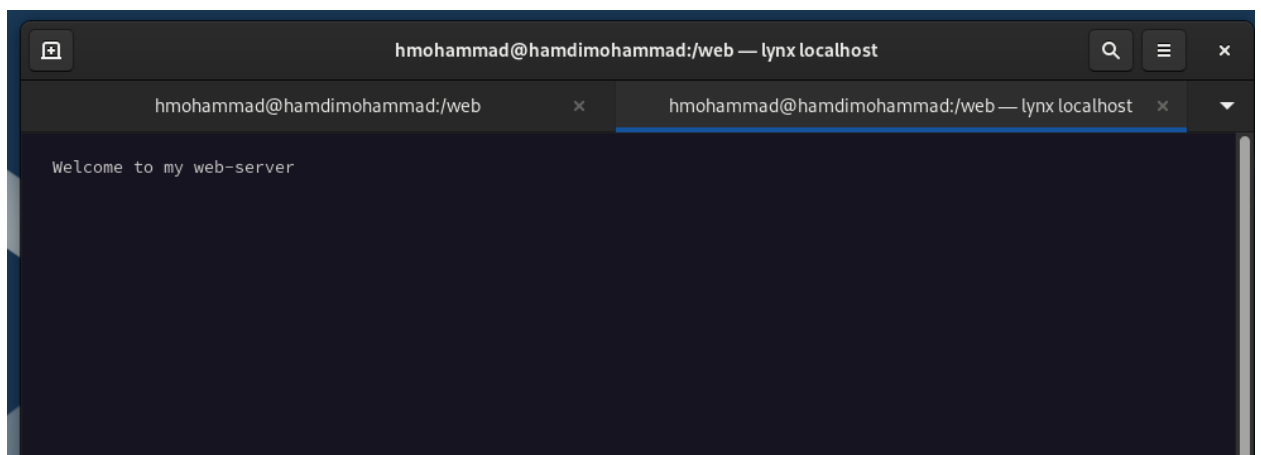
For systems using Nginx: You can add your content in a location of your choice and edit the root configuration
directive in /etc/nginx/nginx.conf.
[ Powered by Rocky Linux ] [poweredby.png]
-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```


8. В терминале с полномочиями администратора примените новую метку контекста к /web:
`semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`

9. Восстановите контекст безопасности: `restorecon -R -v /web`

```
complete.  
[root@hamdimohammad hmohammad]# mkdir /web  
[root@hamdimohammad hmohammad]# cd /web  
[root@hamdimohammad web]# touch index.html  
[root@hamdimohammad web]# echo "Welcome to my web-server" > index.html  
[root@hamdimohammad web]#  
[root@hamdimohammad web]# mcedit /etc/httpd/conf/httpd.conf  
  
[root@hamdimohammad web]#  
[root@hamdimohammad web]# systemctl restart httpd  
[root@hamdimohammad web]#  
[root@hamdimohammad web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"  
[root@hamdimohammad 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@hamdimohammad web]#  
[root@hamdimohammad web]# systemctl restart httpd  
[root@hamdimohammad web]#
```

10. В терминале под учётной записью своего пользователя снова обратитесь к веб-серверу:
`lynx http://localhost` Теперь вы получите доступ к своей пользовательской веб-странице.
Если этого не произошло, то перезагрузите систему и снова попытайтесь получить доступ к
своей пользовательской веб-странице. В случае успеха на экране должна быть отображена
запись «Welcome to my web-server».



Работа с переключателями SELinux

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите список переключателей SELinux для службы ftp: `getsebool -a | grep ftp` Вы увидите переключатель `ftpd_anon_write` с текущим значением `off`.
3. Для службы `ftpd_anon` посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен: `semanage boolean -l | grep ftpd_anon`
4. Измените текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`: `setsebool ftpd_anon_write on`
5. Повторно посмотрите список переключателей SELinux для службы `ftpd_anon_write`: `getsebool ftpd_anon_write`
6. Посмотрите список переключателей с пояснением: `semanage boolean -l | grep ftpd_anon` Обратите внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.
7. Измените постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`: `setsebool -P ftpd_anon_write on`
8. Посмотрите список переключателей: `semanage boolean -l | grep ftpd_anon` В отчёте отразите, какое состояние имеет переключатель?

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

Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

`setenforce 0`

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

`getsebool -a`

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

`setroubleshoot`

4. Какие команды вам нужно выполнить, чтобы применить тип контекста

Чтобы изменить контекст: `chcon -t <type> <file>`

Чтобы восстановить контекст по умолчанию: `restorecon <file>`

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

`/etc/selinux/config`

В файле нужно изменить строку: `SELINUX=disabled`

6. Где SELinux регистрирует все свои сообщения?

`/var/log/audit/audit.log`

Если пакет `auditd` не установлен, сообщения могут быть записаны в:

`/var/log/messages`

7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию?

`semanage fcontext -l | grep ftp`

8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

Временно перевести SELinux в разрешающий режим: `setenforce 0`

Если проблема исчезнет, то, вероятно, она связана с SELinux.

Заключение

Получены навыки работы с SELinux.