

Лабораторная работа №9

Управление SELinux

Комягин А. Н.

23 октября 2024

Российский университет дружбы народов, Москва, Россия

Получить навыки работы с контекстом безопасности и политиками SELinux.

Выполнение лабораторной работы

Управление режимами SELinux

Состояние и режим работы SELinux

```
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 ~]#
```

SELINUX=disabled

```
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  
#  
# 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
```



root@ankomyagin:~

```
[ankomyagin@ankomyagin ~]$ su -
```

```
Password:
```

```
[root@ankomyagin ~]# getenforce
```

```
Disabled
```

```
[root@ankomyagin ~]# setenforce 1
```

```
setenforce: SELinux is disabled
```

```
[root@ankomyagin ~]#
```

SELINUX=enforcing

```
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
```

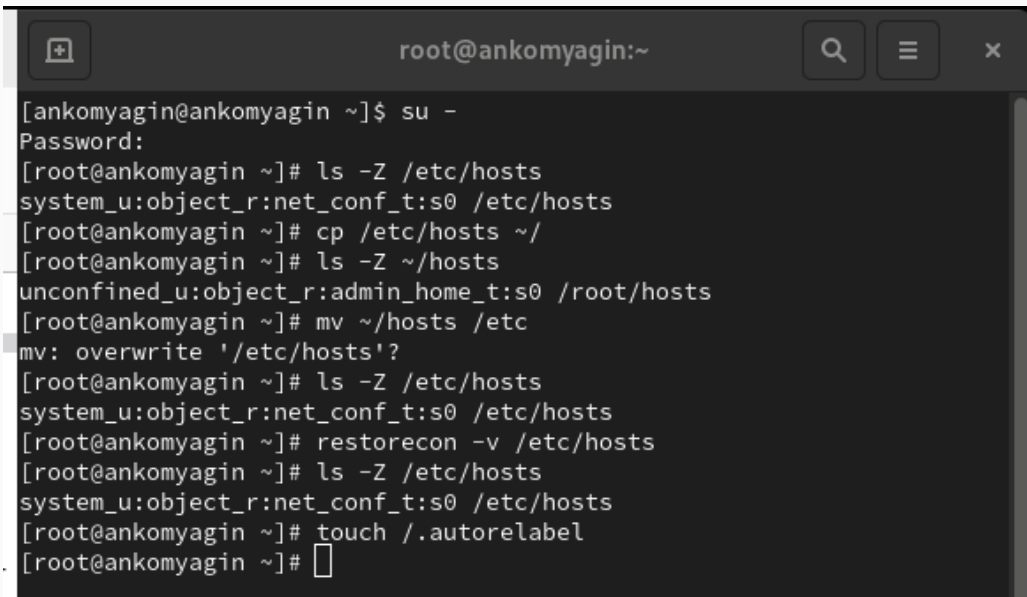

информация о состоянии

```
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: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
[ankomyagin@ankomyagin ~]$
```

Использование restorecon для восстановления контекста безопасности

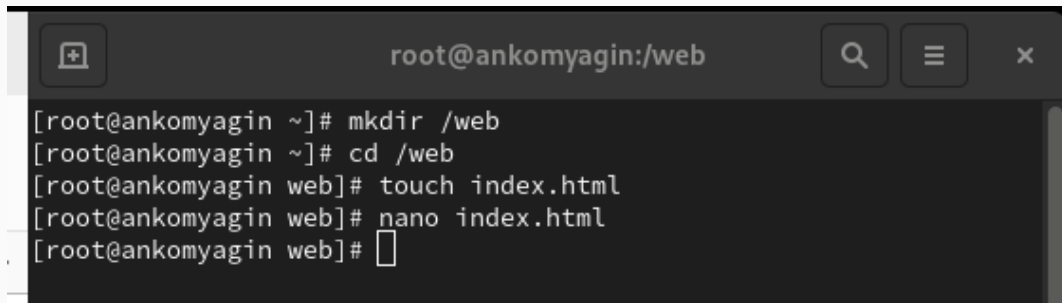


```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[root@ankomyagin ~]# cp /etc/hosts ~/.  
[root@ankomyagin ~]# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
[root@ankomyagin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

перемаркировка

```
Starting Relabel all filesystems...
[ OK ] Finished Restore /run/initramfs on shutdown.
[ 4.393776] selinux-autorelabel[758]: *** Warning -- SELinux targeted policy relabel is required.
[ 4.394212] selinux-autorelabel[758]: *** Relabeling could take a very long time, depending on file
[ 4.394555] selinux-autorelabel[758]: *** system size and speed of hard drives.
[ 4.400667] selinux-autorelabel[758]: Running: /sbin/fixfiles -T 0 restore
[ 9.360203] selinux-autorelabel[764]: Warning: Skipping the following R/O filesystems:
[ 9.360605] selinux-autorelabel[764]: /run/credentials/systemd-sysctl.service
[ 9.360855] selinux-autorelabel[764]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 9.361087] selinux-autorelabel[764]: /run/credentials/systemd-tmpfiles-setup.service
[ 9.361353] selinux-autorelabel[764]: 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
```

```
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 ~]#
```



```
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]#
```

редактирование /etc/httpd/conf/httpd.conf

```
root@ankomyagin:/web
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 worki>
# 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 directo>
# symbolic links and aliases may be used to point to other locati>
#

# 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>

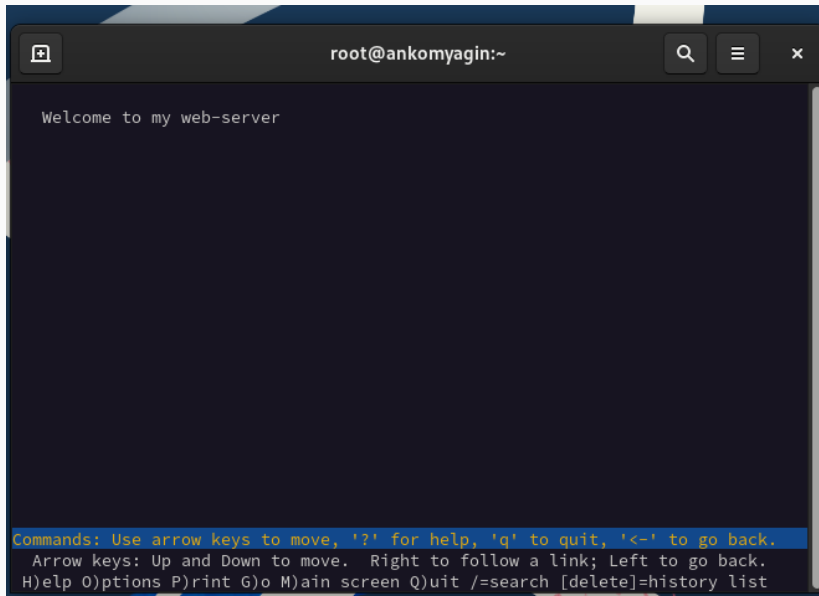
<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>

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

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



```
[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
```



```
root@ankomyagin:~  
  
Welcome to my web-server  
  
Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.  
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
```

Работа с переключателями SELinux

Контрольные вопросы

1. Команда для временного перевода SELinux в разрешающий режим:

setenforce 0

(для временного перехода в разрешающий режим используется setenforce 1).

2. Команда для получения списка всех доступных переключателей SELinux:

`getsebool -a`

3. Имя пакета для получения легко читаемых сообщений журнала SELinux:

Пакет называется setroubleshoot.

4. Команды для применения типа контекста `httpdsyscontent_t` к каталогу `/web`:

```
**semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?" restorecon -R /web**
```

5. Файл, который нужно изменить для полного отключения SELinux:

Файл конфигурации SELinux находится по пути `/etc/selinux/config`. В нем нужно изменить строку:

SELINUX=disabled

6. Место, где SELinux регистрирует свои сообщения:

SELinux регистрирует свои сообщения в журнале аудита, обычно это файл `/var/log/audit/audit.log`, а также может использоваться системный журнал (`journalctl`).

7. Команда для получения информации о доступных типах контекстов для службы ftp:

```
seinfo -t | grep ftp
```

ИЛИ

```
sesearch -allow -s ftp_t
```

8. Самый простой способ узнать, связано ли поведение сервиса с SELinux:

Использовать команду `audit2why` для анализа сообщений журнала аудита:

```
ausearch -m avc -ts recent | audit2why
```

Это покажет, были ли какие-либо отказанные доступы, связанные с SELinux.

Вывод

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