

Лабораторная работа

Номер 9

Приходько Иван Иванович

27 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Приходько Иван Иванович
- Студент
- Российский университет дружбы народов

Получить навыки работы с контекстом безопасности и политиками SELinux.

Поработать с контекстом безопасности и политиками SELinux.

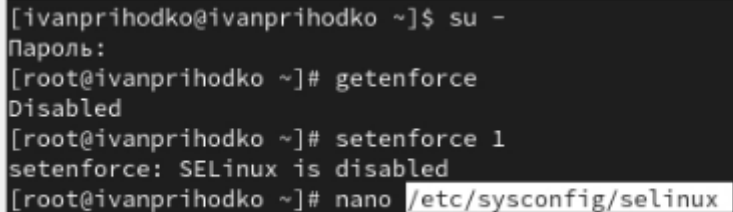
Для начала посмотрим статус SELinux

```
[root@ivanprihodko cron.d]# 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_exe
c_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@ivanprihodko cron.d]# getenforce
Enforcing
```

Теперь в файле отключим SELinux

A terminal window with a dark background and light gray text. The user 'ivanprihodko' is at the prompt '~]\$. They enter 'su -' to become root. The prompt changes to '[root@ivanprihodko ~]#'. They enter 'getenforce' and the output is 'Disabled'. Then they enter 'setenforce 1' and the output is 'setenforce: SELinux is disabled'. Finally, they enter 'nano /etc/sysconfig/selinux', where the file path is highlighted in white.

```
[ivanprihodko@ivanprihodko ~]$ su -  
Пароль:  
[root@ivanprihodko ~]# getenforce  
Disabled  
[root@ivanprihodko ~]# setenforce 1  
setenforce: SELinux is disabled  
[root@ivanprihodko ~]# nano /etc/sysconfig/selinux
```

Рис. 2: Отключение SELinux

```
GNU nano 5.6.1 /etc/sysconfig/selinux Изменён
# 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
```


Теперь вернем SELinux в enforcing

```
GNU nano 5.6.1 /etc/sysconfig/selinux Изменён
# 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/ht>
#
# 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.
```

После перезапусками системы SELinux снова включен

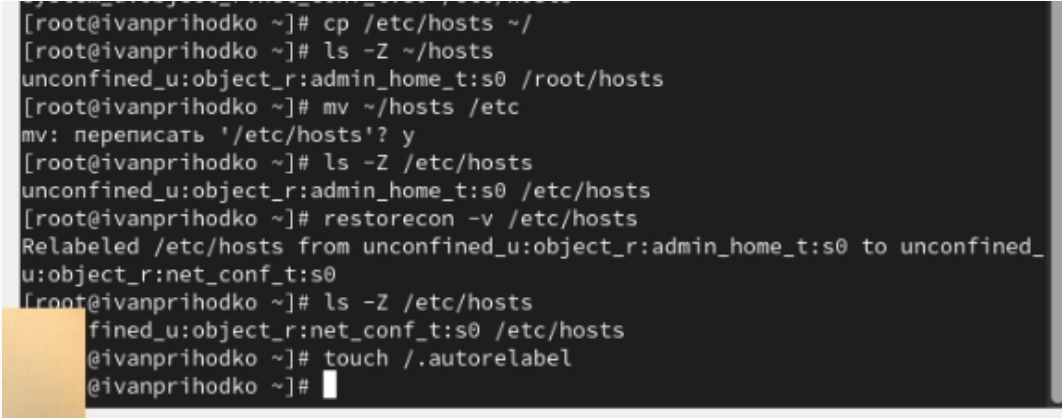
```
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
[root@ivanprihodko ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                    enforcing
Mode 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@ivanprihodko ~]# getenforce
Enforcing
[root@ivanprihodko ~]# ls -Z /etc/hosts
```

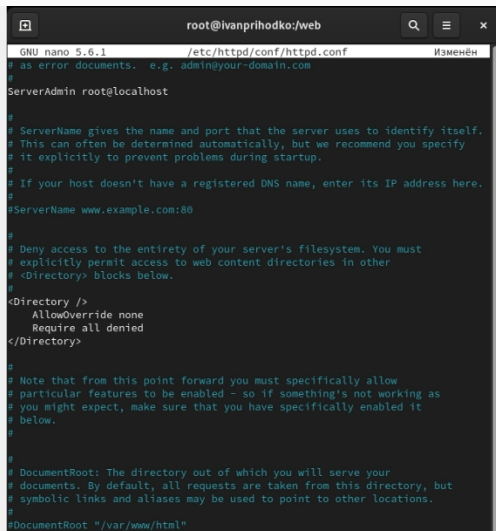
Теперь поработаем с контекстом безопасности файла

A terminal window showing a sequence of commands to move a file and change its SELinux context. The user is root on a machine named ivanprihodko. The commands and their outputs are as follows:

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

Рис. 6: Работа с контекстом безопасности файла

Далее добавим пару строк в httpd.conf



```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Изменён
# as error documents.  e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

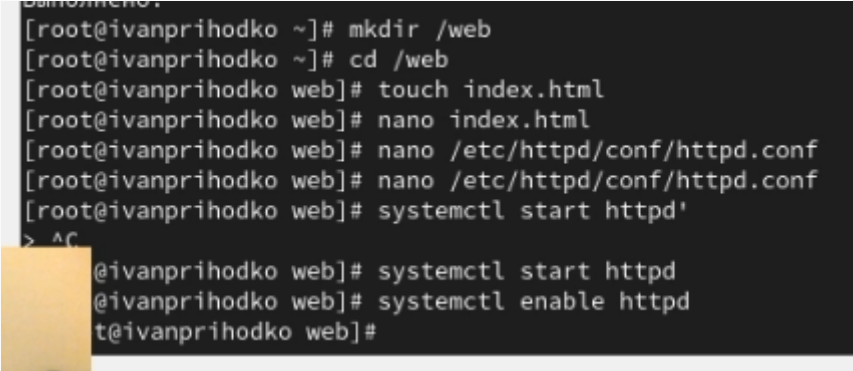
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, 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: 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"
#
# 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>
```

Теперь запустим httpd



```
[root@ivanprihodko ~]# mkdir /web
[root@ivanprihodko ~]# cd /web
[root@ivanprihodko web]# touch index.html
[root@ivanprihodko web]# nano index.html
[root@ivanprihodko web]# nano /etc/httpd/conf/httpd.conf
[root@ivanprihodko web]# systemctl start httpd
> ^C
@ivanprihodko web]# systemctl start httpd
@ivanprihodko web]# systemctl enable httpd
t@ivanprihodko web]#
```

Рис. 9: Запуск httpd

Поработаем немного с httpd и выведем список переключателей SELinux

```
[root@ivanprihodko web]# systemctl start httpd
[root@ivanprihodko web]# systemctl enable httpd
[root@ivanprihodko web]# lynx http://localhost
[root@ivanprihodko web]# su - ivanprihodko
[ivanprihodko@ivanprihodko ~]$ lynx http://localhost
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
[root@ivanprihodko ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
"
[root@ivanprihodko ~]# 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@ivanprihodko ~]# su - ivanprihodko
[ivanprihodko@ivanprihodko ~]$ lynx http://localhost
[ivanprihodko@ivanprihodko ~]$ 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
[ivanprihodko@ivanprihodko ~]$ semanage boolean -l | grep ftpd_anon
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
```

Теперь поработаем с переключателями SELinux

```
[ivanprihodko@ivanprihodko ~]$ semanage boolean -l | grep ftpd_anon
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[ivanprihodko@ivanprihodko ~]$ setsebool ftpd_anon_write on
Could not change active booleans. Please try as root: Permission denied
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
[root@ivanprihodko ~]# 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@ivanprihodko ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@ivanprihodko ~]# setsebool ftpd_anon_write on
[root@ivanprihodko ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@ivanprihodko ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write
[root@ivanprihodko ~]# setsebool -P ftpd_anon_write on
```


В ходе данной работы были получены навыки для работы с контекстом безопасности и политиками SELinux.