

# Лабораторная работа №6

---

Морозова У.К.

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

## Подготовка к лабораторной работе

---

# Подготовка к лабораторной работе

```
ukmorozova@localhost:~ — sudo yum update
[ukmorozova@localhost ~]$ sudo yum update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for ukmorozova:
google-chrome                12 kB/s | 3.7 kB      00:00
Rocky Linux 9 - BaseOS        265 B/s | 4.1 kB      00:15
Rocky Linux 9 - BaseOS        2.3 MB/s | 2.3 MB      00:00
Rocky Linux 9 - AppStream     13 kB/s | 4.5 kB      00:00
Rocky Linux 9 - AppStream     5.9 MB/s | 8.0 MB      00:01
Rocky Linux 9 - Extras        7.1 kB/s | 2.9 kB      00:00
Rocky Linux 9 - Extras        28 kB/s | 15 kB      00:00
Dependencies resolved.
=====
Package                        Arch  Version                                Repository  Size
=====
Upgrading:
firefox                        x86_64 128.3.0-1.el9_4                        appstream   122 M
google-chrome-stable          x86_64 129.0.6668.100-1                       google-chrome 109 M
iwl100-firmware                noarch 39.31.5.1-143.3.el9_4                  baseos      181 k
iwl1000-firmware               noarch 1:39.31.5.1-143.3.el9_4                 baseos      182 k
iwl105-firmware                noarch 18.168.6.1-143.3.el9_4                  baseos      260 k
iwl135-firmware                noarch 18.168.6.1-143.3.el9_4                  baseos      269 k
iwl2000-firmware               noarch 18.168.6.1-143.3.el9_4                  baseos      263 k
iwl2030-firmware               noarch 18.168.6.1-143.3.el9_4                  baseos      271 k
iwl3160-firmware               noarch 1:25.30.13.0-143.3.el9_4                 baseos      538 k
iwl5000-firmware               noarch 8.83.5.1-143.3.el9_4                    baseos      179 k
iwl5150-firmware               noarch 8.24.2.2-143.3.el9_4                    baseos      178 k
iwl6000g2a-firmware            noarch 18.168.6.1-143.3.el9_4                  baseos      246 k
iwl6000g2b-firmware            noarch 18.168.6.1-143.3.el9_4                  baseos      246 k
```

## Выполнение лабораторной работы

---

```
[ukmorofova@localhost ~]$ getenforce
Enforcing
[ukmorofova@localhost ~]$ sestatus
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
```

Рис. 3: getenforce и sestatus

```
[ukmorozova@localhost ~]$ sudo systemctl start httpd
[ukmorozova@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Thu 2024-10-10 17:58:32 MSK; 6s ago
     Docs: man:httpd.service(8)
  Main PID: 29253 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 177 (limit: 23036)
    Memory: 22.0M
       CPU: 101ms
    CGroup: /system.slice/httpd.service
            └─29253 /usr/sbin/httpd -DFOREGROUND
              └─29254 /usr/sbin/httpd -DFOREGROUND
                └─29255 /usr/sbin/httpd -DFOREGROUND
                  └─29256 /usr/sbin/httpd -DFOREGROUND
                    └─29257 /usr/sbin/httpd -DFOREGROUND

Oct 10 17:58:32 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 10 17:58:32 localhost.localdomain httpd[29253]: AH00558: httpd: Could not reliably determine
Oct 10 17:58:32 localhost.localdomain httpd[29253]: Server configured, listening on: port 80
Oct 10 17:58:32 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

Рис. 4: httpd



```
[ukmorofova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 29253 0.0 0.3 20152 11316 ? Ss 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29254 0.0 0.1 22032 7364 ? S 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29255 0.0 0.3 1440204 11256 ? Sl 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29256 0.0 0.3 1571340 13504 ? Sl 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29257 0.0 0.2 1440204 11188 ? Sl 17:58 0:0
0 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ukmorofo+ 29437 0.0 0.2 236780 9128 pts/0 S
+ 17:58 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ukmorofo+ 29497 0.0 0.0 221796 2432 pts/1 S
+ 18:03 0:00 grep --color=auto httpd
[ukmorofova@localhost ~]$
```

Рис. 5: веб-сервер Apache

```
[ukmorozeva@localhost ~]$ sestatus -b httpd
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
```

```
Policy booleans:
abrt_anon_write                  off
abrt_handle_event                off
abrt_upload_watch_anon_write     on
antivirus_can_scan_system        off
antivirus_use_jit                off
auditadm_exec_content            on
authlogin_nsswitch_use_ldap      off
authlogin_radius                 off
authlogin_yubikey                off
awstats_purge_apache_log_files   off
boinc_execmem                    on
cdrecord_read_content            off
cluster_can_network_connect      off
cluster_manage_all_files         off
cluster_use_execmem              off
cobbler_anon_write               off
cobbler_can_network_connect      off
cobbler_use_sftp                  off
```

```

[ukmorozova@localhost ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:          135      Permissions:          457
Sensitivities:    1        Categories:          1024
Types:            5145     Attributes:           259
Users:            8        Roles:                15
Booleans:         356     Cond. Expr.:         388
Allow:            65504    Neverallow:          0
Auditallow:       176     Dontaudit:           8682
Type_trans:       271770  Type_change:          94
Type_member:      37      Range_trans:         5931
Role allow:       40      Role_trans:          417
Constraints:      70     Validatetrans:        0
MLS Constrain:    72     MLS Val. Tran:        0
Permissives:      4       Polcap:               6
Defaults:         7       Typebounds:           0
Allowxperm:       0       Neverallowxperm:      0
Auditallowxperm:  0       Dontauditxperm:       0
Ibendportcon:     0       Ibpkeycon:            0
Initial SIDs:     27      Fs_use:               35
Genfscon:         109     Portcon:              665
Netifcon:         0       Nodecon:              0

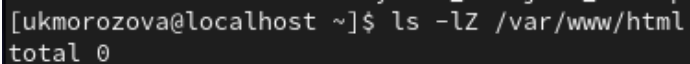
[ukmorozova@localhost ~]$

```



```
[ukmorofova@localhost ~]$ ls -lZ /var/www  
total 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug  8 19:30 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Aug  8 19:30 html
```

Рис. 8: /var/www



```
[ukmorofova@localhost ~]$ ls -lZ /var/www/html  
total 0
```

Рис. 9: /var/www/html

```
[ukmorofova@localhost ~]$ sudo touch /var/www/html/test.html  
[sudo] password for ukmorofova:  
[ukmorofova@localhost ~]$ sudo gedit /var/www/html/test.html
```

Рис. 10: Создание файла

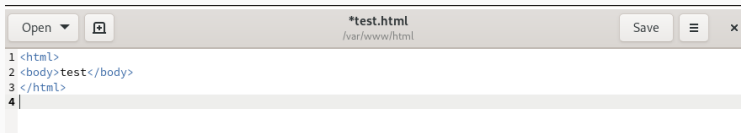


Рис. 11: test.html

```
[ukmorofova@localhost ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>

[ukmorofova@localhost ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 10 18:09 test.html
```

Рис. 12: контекст test.html

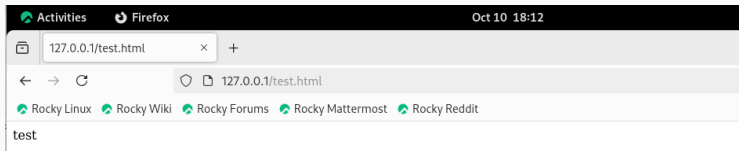


Рис. 13: test.html



```
[ukmorofova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[ukmorofova@localhost ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted
[ukmorofova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[ukmorofova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[ukmorofova@localhost ~]$
```

Рис. 14: Изменение контекста

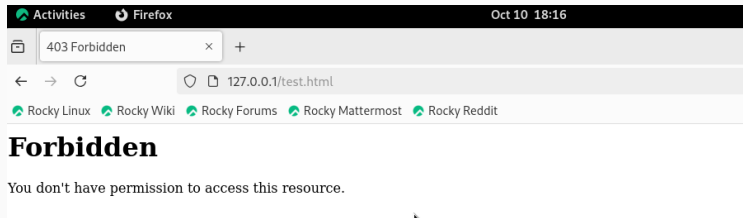


Рис. 15: Ошибка

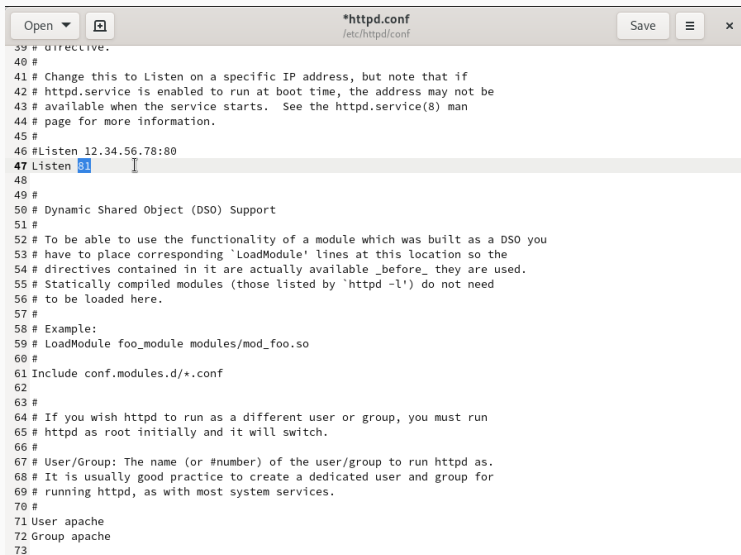
```

[ukmorozova@localhost ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 10 18:09 /var/www/html/test.html
[ukmorozova@localhost ~]$ sudo tail /var/www/html/test.html
<html>
<body>test</body>
</html>

[ukmorozova@localhost ~]$ sudo tail /var/log/messages
Oct 10 18:16:20 localhost setroubleshoot[30495]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 10 18:16:20 localhost systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 10 18:16:20 localhost systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 04d5c87a-8095-4188-97d3-369f0ad06bf7
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that htt

```

Рис. 16: log-файлы веб-сервера Apache



```
39 # directive.
40 #
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 0.0.0.0:80
48
49 #
50 # Dynamic Shared Object (DSO) Support
51 #
52 # To be able to use the functionality of a module which was built as a DSO you
53 # have to place corresponding 'LoadModule' lines at this location so the
54 # directives contained in it are actually available _before_ they are used.
55 # Statically compiled modules (those listed by 'httpd -l') do not need
56 # to be loaded here.
57 #
58 # Example:
59 # LoadModule foo_module modules/mod_foo.so
60 #
61 Include conf.modules.d/*.conf
62
63 #
64 # If you wish httpd to run as a different user or group, you must run
65 # httpd as root initially and it will switch.
66 #
67 # User/Group: The name (or #number) of the user/group to run httpd as.
68 # It is usually good practice to create a dedicated user and group for
69 # running httpd, as with most system services.
70 #
71 User apache
72 Group apache
73
```

```
[ukmorozova@localhost ~]$ sudo tail -n1 /var/log/messages  
Oct 10 18:21:52 localhost systemd[1]: setroubleshootd.service: Deactivated successfully.  
[ukmorozova@localhost ~]$
```

Рис. 18: лог-файлы

```
[ukmorozova@localhost ~]$ sudo tail /var/log/messages
Oct 10 18:16:20 localhost setroubleshoot[30495]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 10 18:16:20 localhost systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 10 18:16:20 localhost systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@.service.
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getat
tr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 04d5
c87a-8095-4188-97d3-369f0ad06bf7
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getat
tr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence)
suggests *****#012#012If you want to fix the label. #012/var/www/html/test.h
tml default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attem
pt may have been stopped due to insufficient permissions to access a parent directory in which ca
se try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/
test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#0
12#012If you want to treat test.html as public content#012Then you need to change the label on te
st.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_con
tent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugi
n catchall (1.41 confidence) suggests *****#012#012If you believe that htt
pd should be allowed getatrr access on the test.html file by default.#012Then you should report t
his as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow thi
s access for now by executing:#012# ausearch -q 'httpd' --raw | audit2allow -M my-httpd#012# semod
ule -X 300 -i my-httpd.pp#012
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getat
tr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 04d5
c87a-8095-4188-97d3-369f0ad06bf7
Oct 10 18:16:23 localhost setroubleshoot[30495]: SELinux is preventing /usr/sbin/httpd from getat
tr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence)
suggests *****#012#012If you want to fix the label. #012/var/www/html/test.h
tml default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attem
pt may have been stopped due to insufficient permissions to access a parent directory in which ca
se try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/
```

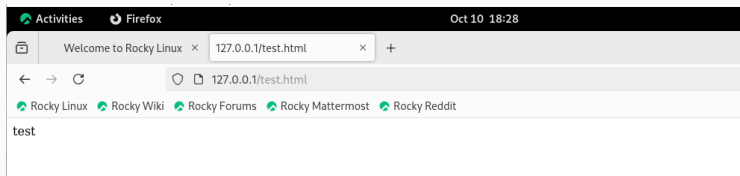


Рис. 20: веб-сервер Apache

## Выводы

---



Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверили работу SELinx на практике совместно с веб-сервером Apache.