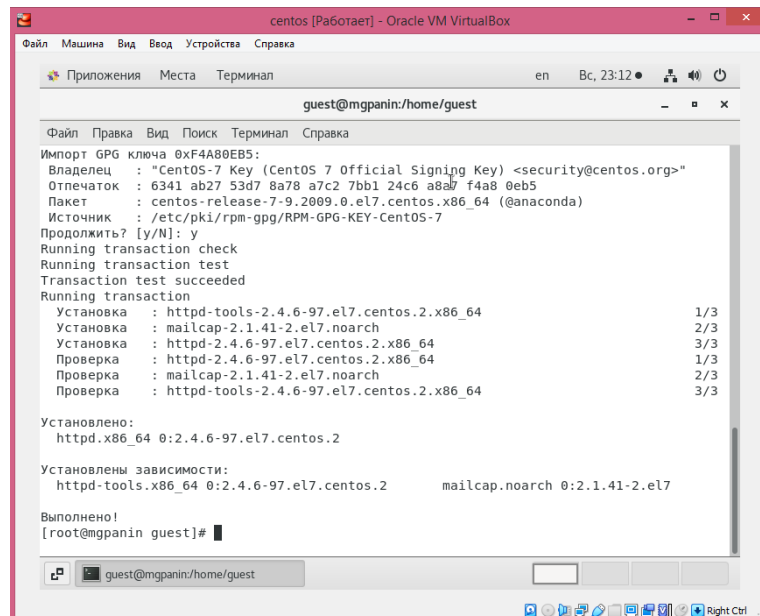


Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Подготовка лабораторного стенда

1. Установим/обновим (за суперпользователя) веб-сервер Apache с помощью команды `yum install httpd`



2. В конфигурационном файле `/etc/httpd/httpd.conf` зададим параметр `ServerName`: `ServerName test.ru` чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
3. Также необходимо проследить, чтобы пакетный фильтр был отключен или в своей рабочей конфигурации позволял подключаться к 80-му и 81-му портам протокола tcp. Добавим разрешающие правила с помощью команд:

```
iptables -I INPUT -p tcp --dport 80 -j ACCEPT
```

```
iptables -I INPUT -p tcp --dport 81 -j ACCEPT
```

```
iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
```

```
iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

```
[root@mgpanin guest]# nano /etc/httpd/conf/httpd.conf
[root@mgpanin guest]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@mgpanin guest]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@mgpanin guest]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@mgpanin guest]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@mgpanin guest]#
```

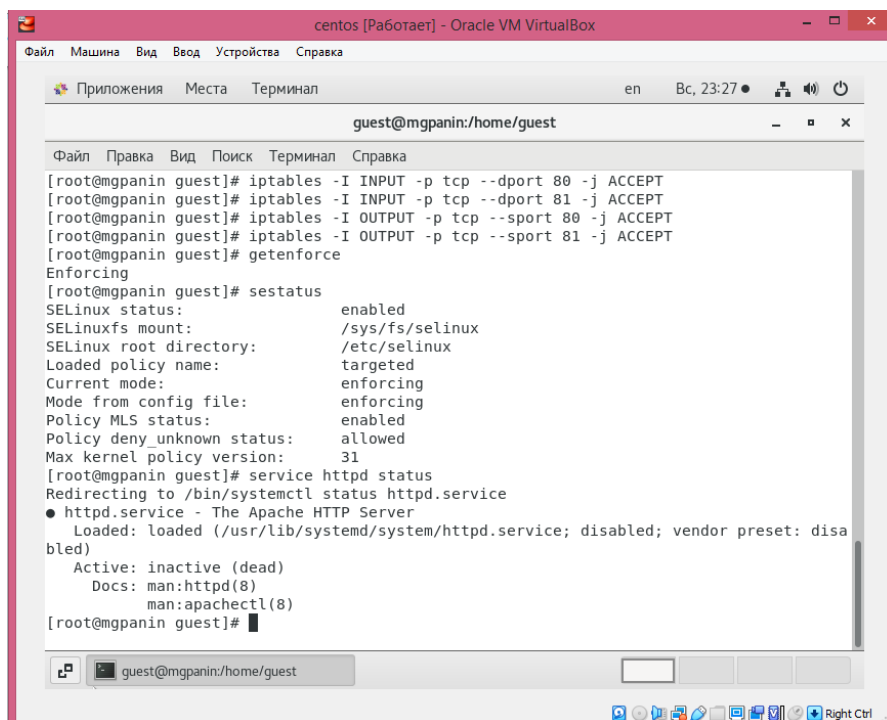
Можно было бы также отключить фильтр командами:

```
iptables -F
```

```
iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
```

Порядок выполнения работы

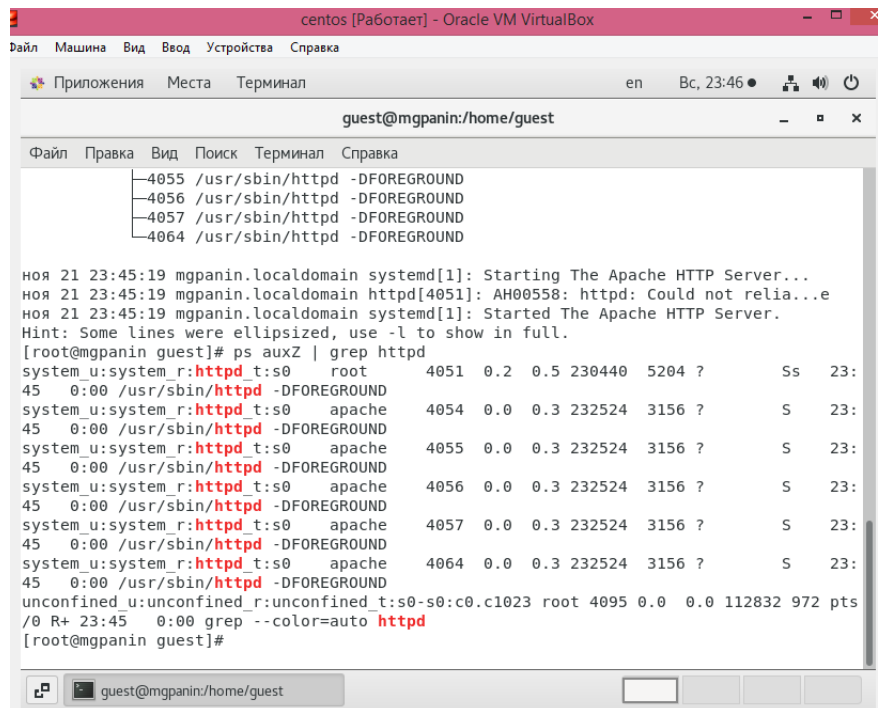
1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus*



The screenshot shows a terminal window titled 'centos [Работает] - Oracle VM VirtualBox'. The terminal is running as 'guest@mgpanin:/home/guest'. The user has executed several commands to configure iptables and check SELinux status. The output shows SELinux is enabled in 'enforcing' mode with the 'targeted' policy. The httpd service status is shown as 'inactive (dead)'.

```
guest@mgpanin:/home/guest
[guest@mgpanin guest]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[guest@mgpanin guest]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[guest@mgpanin guest]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[guest@mgpanin guest]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[guest@mgpanin guest]# getenforce
Enforcing
[guest@mgpanin guest]# 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
Max kernel policy version:    31
[guest@mgpanin guest]# 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; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[guest@mgpanin guest]#
```

2. Обратимся к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает: *service httpd status*
3. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности, используем команду *ps auxZ | grep httpd*



```
centos [Работает] - Oracle VM VirtualBox
Дайл  Машина  Вид  Ввод  Устройства  Справка

Приложения  Места  Терминал  en  Вс, 23:46

guest@mgpanin:/home/guest

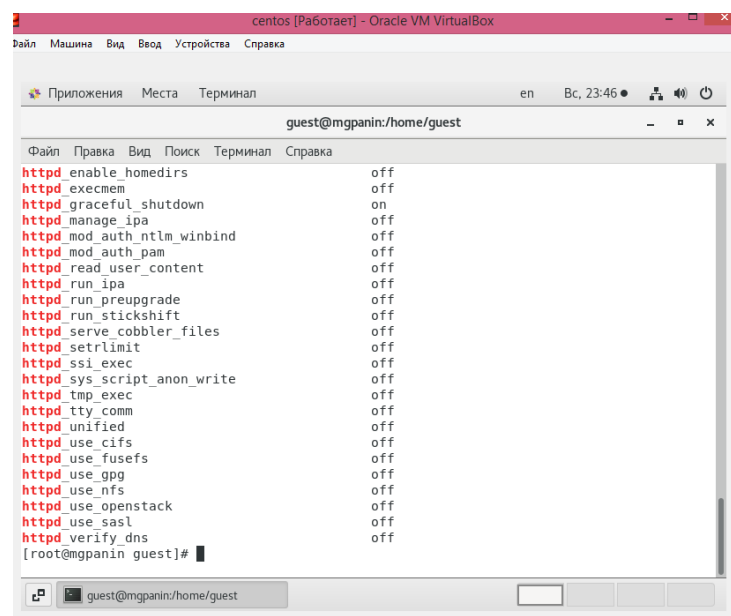
Файл  Правка  Вид  Поиск  Терминал  Справка

-4055 /usr/sbin/httpd -DFOREGROUND
-4056 /usr/sbin/httpd -DFOREGROUND
-4057 /usr/sbin/httpd -DFOREGROUND
-4064 /usr/sbin/httpd -DFOREGROUND

ноя 21 23:45:19 mgpanin.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 21 23:45:19 mgpanin.localdomain httpd[4051]: AH00558: httpd: Could not relia...e
ноя 21 23:45:19 mgpanin.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@mgpanin guest]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 4051 0.2 0.5 230440 5204 ? Ss 23:
45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4054 0.0 0.3 232524 3156 ? S 23:
45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4055 0.0 0.3 232524 3156 ? S 23:
45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4056 0.0 0.3 232524 3156 ? S 23:
45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4057 0.0 0.3 232524 3156 ? S 23:
45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 4064 0.0 0.3 232524 3156 ? S 23:
45 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4095 0.0 0.0 112832 972 pts
/0 R+ 23:45 0:00 grep --color=auto httpd
[root@mgpanin guest]#
```

В нашем случае контекст безопасности `unconfined_u:system_r:httpd_t`

- Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`



```
centos [Работает] - Oracle VM VirtualBox
Дайл  Машина  Вид  Ввод  Устройства  Справка

Приложения  Места  Терминал  en  Вс, 23:46

guest@mgpanin:/home/guest

Файл  Правка  Вид  Поиск  Терминал  Справка

httpd enable_homedirs off
httpd execmem off
httpd graceful_shutdown on
httpd manage_ipa off
httpd mod_auth_ntlm_winbind off
httpd mod_auth_pam off
httpd read_user_content off
httpd run_ipa off
httpd run_preupgrade off
httpd run_stickshift off
httpd serve_cobbler_files off
httpd setrlimit off
httpd ssi_exec off
httpd sys_script_anon_write off
httpd tmp_exec off
httpd tty_comm off
httpd unified off
httpd use_cifs off
httpd use_fusefs off
httpd use_gpg off
httpd use_nfs off
httpd use_openstack off
httpd use_sasl off
httpd verify_dns off
[root@mgpanin guest]#
```

Многие из переключателей находятся в положении «off».

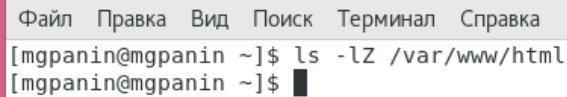
- Посмотрим статистику по политике с помощью команды `seinfo`, также определим множество пользователей, ролей и типов.

Пользователей: 9, ролей: 12, типов: 3920.

- Определим тип файлов и поддиректорий, находящихся в директории `/var/www` с помощью команды `ls -lZ /var/www`

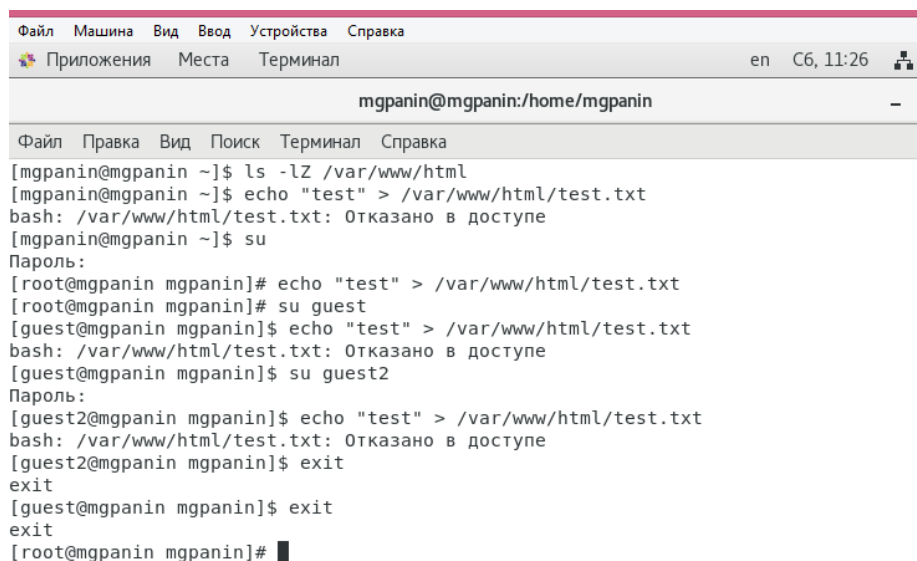
```
[eakhityaev@khityaev ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
```

7. Определим тип файлов, находящихся в директории `/var/www/html` с помощью команды `ls -lZ /var/www/html`



```
Файл  Правка  Вид  Поиск  Терминал  Справка
[mgpanin@mgpanin ~]$ ls -lZ /var/www/html
[mgpanin@mgpanin ~]$
```

8. Определим круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.



```
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал  en  C6, 11:26
mgpanin@mgpanin:/home/mgpanin
Файл  Правка  Вид  Поиск  Терминал  Справка
[mgpanin@mgpanin ~]$ ls -lZ /var/www/html
[mgpanin@mgpanin ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[mgpanin@mgpanin ~]$ su
Пароль:
[root@mgpanin mgpanin]# echo "test" > /var/www/html/test.txt
[root@mgpanin mgpanin]# su guest
[guest@mgpanin mgpanin]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[guest@mgpanin mgpanin]$ su guest2
Пароль:
[guest2@mgpanin mgpanin]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[guest2@mgpanin mgpanin]$ exit
exit
[guest@mgpanin mgpanin]$ exit
exit
[root@mgpanin mgpanin]#
```

Видно, что только суперпользователь может создать файл в данной директории.

9. В следствие этого создадим от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания:

```
<html>
```

```
<body>test</body>
```

```
</html>
```

10. Проверим контекст созданного файла.

```
[root@mgpanin mgpanin]# nano /var/www/html/test.html
[root@mgpanin mgpanin]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.txt
[root@mgpanin mgpanin]# ls -l /var/www/html
итого 8
-rw-r--r--. 1 root root 33 ноя 27 11:28 test.html
-rw-r--r--. 1 root root 5 ноя 27 11:25 test.txt
[root@mgpanin mgpanin]#
```

Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `unconfined_u:object_r:httpd_sys_content_t`

11. Обратимся к файлу через веб-сервер, введя в браузере firefox адрес

<http://127.0.0.1/test.html>

12. Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd` и сопоставим их с типом файла `test.html`. Проверим контекст файла командой `ls -Z /var/www/html/test.html`

```
[root@mgpanin mgpanin]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@mgpanin mgpanin]#
```

Т.к. по умолчанию пользователи CentOS являются свободными (unconfined) от типа, созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. Тип `httpd_sys_content_t` позволяет процессу

httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

13. Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на другой, к которому процесс `httpd` не должен иметь доступа, в нашем случае, на `samba_share_t`:

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```

```
[root@mgpanin mgpanin]# chcon -t samba_share_t /var/www/html/test.html
[root@mgpanin mgpanin]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@mgpanin mgpanin]#
```

Как можно видеть, контекст успешно сменился.

14. Попробуем еще раз получить доступ к файлу через веб-сервер, введя в браузере `firefox` адрес <http://127.0.0.1/test.html>

Мы получили сообщение об ошибке.

15. Проанализируем ситуацию, просмотрев `log`-файлы веб-сервера `Apache`, системный `log`-файл и `audit.log` при условии уже запущенных процессов `setroubleshootd` и `audtd`.

```
[root@mgpanin mgpanin]# tail /var/log/messages
Nov 27 11:34:33 mgpanin journal: ibus_bus_list_engines_async: assertion 'IBUS_IS_BUS (bus)' failed
Nov 27 11:34:33 mgpanin journal: invalid (NULL) pointer instance
Nov 27 11:34:33 mgpanin journal: g_signal_handlers_disconnect_matched: assertion 'G_TYPE_CHECK_INSTANCE (instance)' failed
Nov 27 11:34:40 mgpanin journal: Failed fetch permissions from flatpak permission store : GDBus.Error:org.freedesktop.portal.Error.NotFound: No entry for geolocation
Nov 27 11:34:43 mgpanin dbus[682]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Nov 27 11:34:43 mgpanin systemd: Starting Hostname Service...
Nov 27 11:34:43 mgpanin dbus[682]: [system] Successfully activated service 'org.freedesktop.hostname1'
Nov 27 11:34:43 mgpanin systemd: Started Hostname Service.
Nov 27 11:34:45 mgpanin journal: Exiting
Nov 27 11:35:07 mgpanin org.gnome.Terminal: ###!!! [Child][RunMessage] Error: Channel closing: too late to send/recvd, messages will be lost
[root@mgpanin mgpanin]#
```

Исходя из `log`-файлов, мы можем заметить, что проблема в измененном контексте на шаге 13, т.к. процесс `httpd` не имеет доступа на `samba_share_t`. В системе оказались запущены процессы `setroubleshootd` и `audtd`, поэтому ошибки, связанные с измененным контекстом, также есть в файле `/var/log/audit/audit.log`.

16. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`), заменив в файле `/etc/httpd/conf/httpd.conf` строчку `Listen 80` на `Listen 81`.
17. Перезапустим веб-сервер Apache и попробуем обратиться к файлу через веб-сервер, введя в браузере firefox адрес <http://127.0.0.1/test.html>

```
[root@mgpanin mgpanin]# nano /etc/httpd/conf/httpd.conf
[root@mgpanin mgpanin]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@mgpanin mgpanin]# 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; vendor preset: disabled)
   Active: active (running) since C6 2021-11-27 11:41:16 MSK; 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
    Main PID: 4718 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
      Tasks: 6
     CGroup: /system.slice/httpd.service
             └─4718 /usr/sbin/httpd -DFOREGROUND
               └─4721 /usr/sbin/httpd -DFOREGROUND
                 └─4722 /usr/sbin/httpd -DFOREGROUND
                   └─4723 /usr/sbin/httpd -DFOREGROUND
                     └─4724 /usr/sbin/httpd -DFOREGROUND
                       └─4725 /usr/sbin/httpd -DFOREGROUND

ноя 27 11:41:16 mgpanin.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 11:41:16 mgpanin.localdomain httpd[4718]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using mgpanin.localdomain. Set the 'ServerName' directive globally to suppress this message
ноя 27 11:41:16 mgpanin.localdomain systemd[1]: Started The Apache HTTP Server.
```

Из того, что при запуске файла через браузер появилась ошибка, можно сделать предположение, что в списках портов, работающих с веб-сервером Apache, отсутствует порт 81.

18. Подтвердим свои догадки, проанализировав log-файлы: `tail -n1 /var/log/messages` и просмотрев файлы `/var/log/httpd/error_log`, `/var/log/httpd/access_log` и `/var/log/audit/audit.log`

```
[root@mgpanin mgpanin]# tail -n1 /var/log/messages
tail: невозможно открыть «/var/log/messages» для чтения: Нет такого файла или каталога
[root@mgpanin mgpanin]# tail -n1 /var/log/messages
Nov 27 11:41:16 mgpanin systemd: Started The Apache HTTP Server.
[root@mgpanin mgpanin]# tail /var/log/httpd/error_log
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using mgpanin.localdomain. Set the 'ServerName' directive globally to suppress this message
[Sun Nov 21 23:45:19.856396 2021] [lbmethod_heartbeat:notice] [pid 4051] AH02282: No sl otmem from mod_heartbeat
[Sun Nov 21 23:45:19.910016 2021] [mpm_prefork:notice] [pid 4051] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Sun Nov 21 23:45:19.910037 2021] [core:notice] [pid 4051] AH00094: Command line: '/usr /sbin/httpd -D FOREGROUND'
[Sat Nov 27 11:41:16.889905 2021] [core:notice] [pid 4718] SELinux policy enabled; http d running as context system_u:system_r:httpd_t:s0
[Sat Nov 27 11:41:16.931587 2021] [suexec:notice] [pid 4718] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name,
```



```
[root@mgpanin mgpanin]# tail /var/log/audit/audit.log
type=SERVICE_STOP msg=audit(1638002103.337:227): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-located comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1638002114.042:228): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=USER_ACCT msg=audit(1638002401.723:229): pid=4659 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1638002401.735:230): pid=4659 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1638002401.737:231): pid=4659 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=4 res=1
type=USER_START msg=audit(1638002402.133:232): pid=4659 uid=0 auid=0 ses=4 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1638002402.242:233): pid=4659 uid=0 auid=0 ses=4 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
```

Во всех log-файлах появились записи, кроме /var/log/messages.

19. Выполним команду `semanage port -a -t http_port_t -p tcp 81`

После этого проверим список портов командой `semanage port -l | grep http_port_t`

```
[root@mgpanin mgpanin]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@mgpanin mgpanin]# semanage port -l | grep http_port_t
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus http_port_t tcp 5988
[root@mgpanin mgpanin]#
```

Убедились, что порт 81 присутствует в списке.

20. Попробуем теперь запустить веб-сервер Apache еще раз.

21. Вернем контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`:

`chcon -t httpd_sys_content_t /var/www/html/test.html`

```
[root@mgpanin mgpanin]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@mgpanin mgpanin]#
```

После этого вновь попробуем получить доступ к файлу через веб-сервер, введя в браузере firefox адрес <http://127.0.0.1:81/test.html>

Увидели слово содержимое файла - слово «test».

22. Исправим обратно конфигурационный файл apache, вернув Listen 80.

23. Удалим привязку http_port_t к 81 порту: *semanage port -d -t http_port_t -p tcp 81*. Данную команду выполнить невозможно на моей версии CentOS, поэтому получаем ошибку.

```
[root@khityaev eakhityaev]# semanage port -d -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 определен на уровне политики и не может быть удален
[root@khityaev eakhityaev]# █
```

24. Удалим файл */var/www/html/test.html*: *rm /var/www/html/test.html*

```
[root@mgpanin mgpanin]# nano /etc/httpd/conf/httpd.conf
[root@mgpanin mgpanin]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@mgpanin mgpanin]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@mgpanin mgpanin]# █
```

Вывод

Я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.