

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1

Проверить работу SELinux на практике совместно с веб-сервером Apache.

## Подготовка

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика targeted и режим enforcing используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.

```
[root@wangyao ~]# 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:    28

[root@wangyao ~]# sudo yum install httpd
已加载插件：fastestmirror, langpacks
Loading mirror speeds from cached hostfile

[root@wangyao ~]# sudo systemctl status httpd
● 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)
[root@wangyao ~]# sudo systemctl start httpd
[root@wangyao ~]# sudo systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@wangyao ~]#
```

2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл `/etc/selinux/config`, так и проверить используемый режим и политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.

4. В конфигурационном файле `*/etc/httpd/httpd.conf` необходимо задать параметр `ServerName`:

`ServerName test.ru`

чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.



5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp.

Отключить фильтр можно командами

```
iptables -F
```

```
iptables -P
```

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

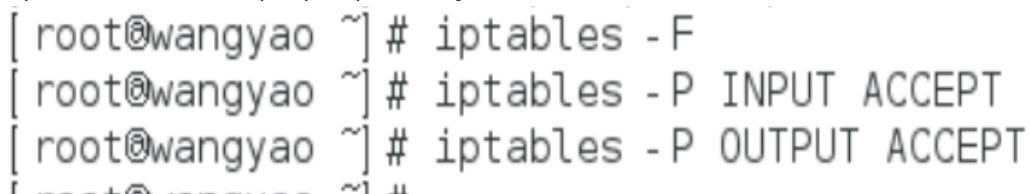
либо добавить разрешающие правила:

```
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
```



6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные *links*, *lynx*, *wget* и графические *konqueror*, *opera*, *firefox* или др.

# процесс выполнения задания

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

```
[root@wangyao ~]# getenforce
Enforcing
[root@wangyao ~]# 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:      28
```

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

`service httpd status`

или

`/etc/rc.d/init.d/httpd status`

Если не работает, запустите его так же, но с параметром `start`.

```
[root@wangyao ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor
   Active: active (running) since 六 2024-10-05 16:24:40 CST; 7min ago
     Docs: man: httpd(8)
           man: apachectl(8)
   Main PID: 5168 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
   CGroup: /system.slice/httpd.service
           └─5168 /usr/sbin/httpd - DFOREGROUND
           └─5242 /usr/sbin/httpd - DFOREGROUND
           └─5243 /usr/sbin/httpd - DFOREGROUND
```

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd`
- или

```

ps -eZ | grep httpd
[ root@wangyao ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root      5168  0.0  0.0 226144  5084 ?
n/httpd - DFOREGROUND
system_u:system_r:httpd_t:s0      apache    5242  0.0  0.0 228228  3140 ?
n/httpd - DFOREGROUND
system_u:system_r:httpd_t:s0      apache    5243  0.0  0.0 228228  3140 ?
n/httpd - DFOREGROUND
system_u:system_r:httpd_t:s0      apache    5244  0.0  0.0 228228  3140 ?
n/httpd - DFOREGROUND
system_u:system_r:httpd_t:s0      apache    5245  0.0  0.0 228228  3140 ?
n/httpd - DFOREGROUND
system_u:system_r:httpd_t:s0      apache    5246  0.0  0.0 228228  3140 ?
n/httpd - DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 5676 0.0  0.0 112
grep --color=auto httpd

```

4. Посмотрите текущее состояние переключателей SELinux для Apache с

помощью команды

```
sestatus -bigrep httpd
```

Обратите внимание, что многие из них находятся в положении «off».

```
[root@wangyao ~]# 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
Max kernel policy version:    28
```

```
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
```

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```
[root@wangyao ~]# semanage login -l
```

登录名	SELinux 用户	MLS/MCS 范围	服务
__default__	unconfined_u	s0-s0:c0,c1023	*
root	unconfined_u	s0-s0:c0,c1023	*
system_u	system_u	s0-s0:c0,c1023	*

```
[root@wangyao ~]# semanage role -l
usage: semanage [-h]
                    {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
                    ...
semanage: error: argument subcommand: invalid choice: 'role' (choose from 'import', 'export', 'login', 'user', 'port', 'ibpkey', 'ibendport', 'interface', 'module', 'node', 'fcontext', 'boolean', 'permissive', 'dontaudit')
```

6. Определите тип файлов и поддиректорий, находящихся в директории

/var/www, с помощью команды

```
ls -lZ /var/www
```

```
[ root@wangyao ~] # 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 html
```

7. Определите тип файлов, находящихся в директории /var/www/html:

```
ls -lZ /var/www/html
```

```
[ root@wangyao ~] # ls -lZ /var/www/html
```

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

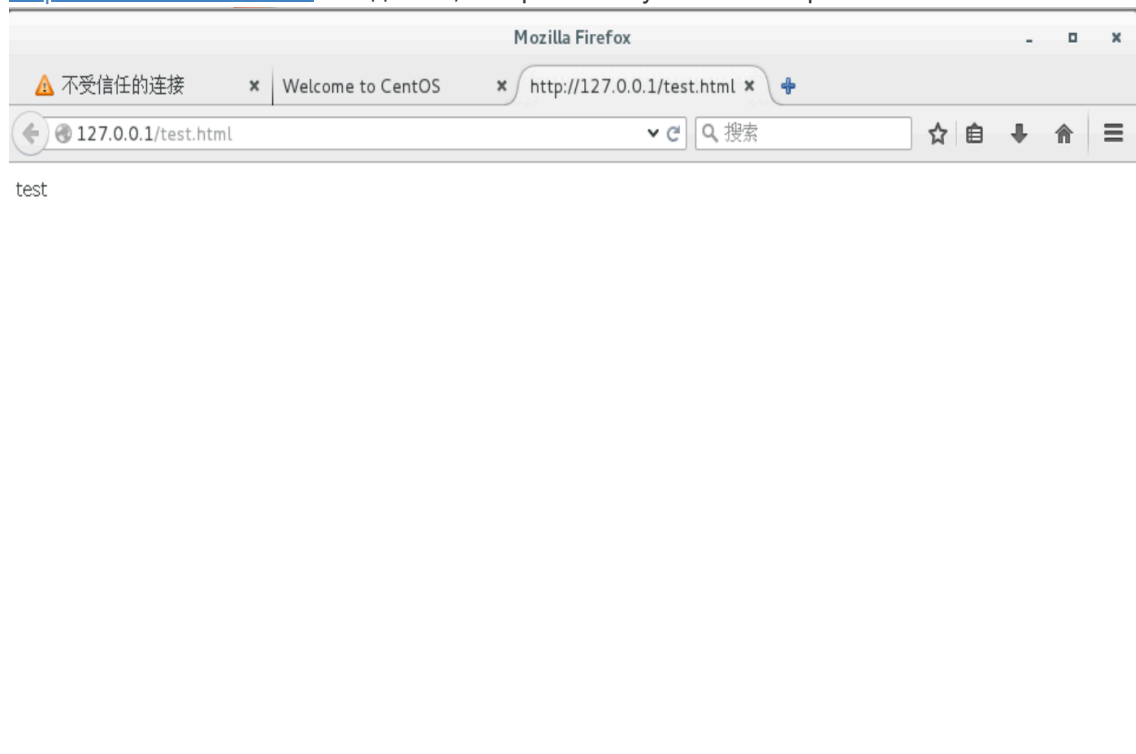
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл

/var/www/html/test.html следующего содержания:

```
[ root@wangyao ~] # echo '<html><body>test</body></html>' > /var/www/html/test.html
[ root@wangyao ~] # ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён.



12. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z.
- ```
ls -Z /var/www/html/test.html
```

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), 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. (В директории /proc файлы, относящиеся к процессам, могут иметь роль system\_r. Если активна политика MLS, то могут использоваться и другие роли, например, secadm\_r. Данный случай мы рассматривать не будем, как и предназначение :s0).

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.

```
[root@wangyao ~]# 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@wangyao ~]#
```

13. Измените контекст файла /var/www/html/test.html с

httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t:

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

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

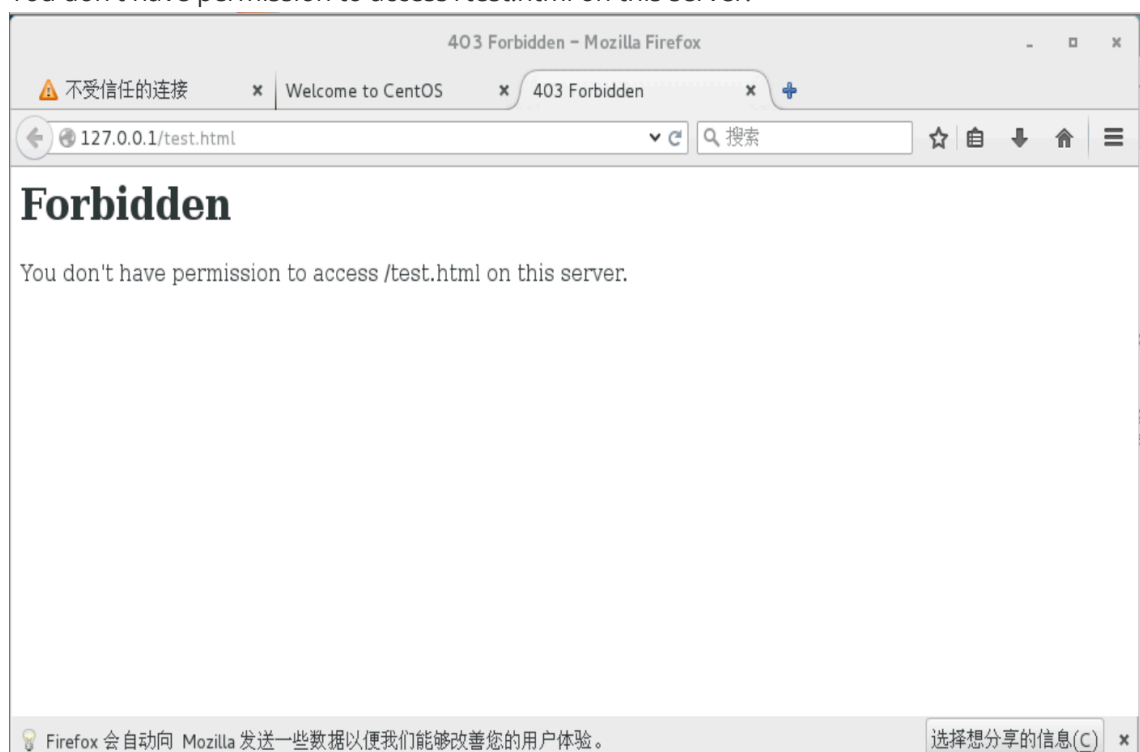
После этого проверьте, что контекст поменялся.

```
[root@wangyao ~]# chcon -t samba_share_t /var/www/html/test.html
[root@wangyao ~]# 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
```

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Вы должны получить сообщение об ошибке:

Forbidden

You don't have permission to access /test.html on this server.





15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

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

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл:

```
tail /var/log/messages
```

Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно.

```
[root@wangyao ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 31 10月  5 16:48 /var/www/html/test.html
[root@wangyao ~]# tail /var/log/messages
Oct  5 16:54:10 wangyao dbus[1122]: [system] Successfully activated service 'org.freedesktop.Setroubleshootd'
Oct  5 16:54:10 wangyao dbus-daemon: dbus[1122]: [system] Successfully activated service 'org.freedesktop.Setroubleshootd'
Oct  5 16:54:11 wangyao setroubleshoot: failed to retrieve rpm info for /
Oct  5 16:54:11 wangyao dbus-daemon: 'list' object has no attribute 'split'
Oct  5 16:54:11 wangyao setroubleshoot: Plugin Exception: restorecon source
```

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

```
#Listen 12.34.56.78:80
Listen 81
```

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

**Перезапуск Apache (systemctl restart httpd) необходим для того, чтобы новые настройки вступили в силу и были применены корректно. Это гарантирует стабильную работу сервиса и помогает избежать возможных конфликтов и ошибок.**

```
[root@wangyao ~]# systemctl restart httpd
[root@wangyao ~]#
```

18. Проанализируйте лог-файлы:

```
tail -nl /var/log/messages
```

Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи.

```
[root@wangyao ~]# tail -n 10 /var/log/messages
Oct  5 16:56:11 wangyao dbus-daemon: dbus[1122]: [system] Successfully activated service 'org.freedesktop.NMDispatcher'
Oct  5 16:56:11 wangyao nm-dispatcher: Dispatching action 'dhcp4-change' for
Oct  5 16:57:25 wangyao firefox.desktop: 1728118645868#011addons.repository.repopulating cache
Oct  5 16:57:26 wangyao firefox.desktop: 1728118646305#011addons.update-checker was not valid XML
Oct  5 16:57:26 wangyao firefox.desktop: 1728118646315#011addons.update-checker was not valid XML
Oct  5 16:57:28 wangyao systemd: Stopping The Apache HTTP Server...
Oct  5 16:57:29 wangyao systemd: Stopped The Apache HTTP Server.
Oct  5 16:57:29 wangyao systemd: Starting The Apache HTTP Server...
```



19. Выполните команду

```
semanage port -a -t http_port_t -p tcp 81
```

После этого проверьте список портов командой

```
semanage port -l | grep http_port_t
```

Убедитесь, что порт 81 появился в списке.

```
[root@wangyao ~]# systemctl restart httpd
```

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

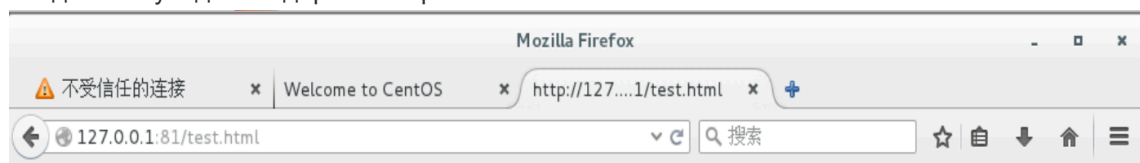
**Номер порта изменен**

21. Верните контекст httpd\_sys\_content\_t к файлу /var/www/html/ test.html:

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

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

Вы должны увидеть содержимое файла — слово «test».



test



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

23.

```
#Listen 12.34.56.78:80
Listen 80
```

24. Удалите привязку http\_port\_t к 81 порту:

```
semanage port -d -t http_port_t -p tcp 81
```

и проверьте, что порт 81 удалён.

```
root@wangyao ~]# semanage port -d -t http_port_t -p tcp 81
```

ValueError: 在策略中定义了端口 tcp/81, 无法删除。

```
root@wangyao ~]# semanage port -l | grep http_port_t
```

```
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
megasus http_port_t tcp 5988
```

25. Удалите файл /var/www/html/test.html:

```
rm /var/www/html/test.html
```

```
[root@wangyao ~]# rm /var/www/html/test.html  
rm: 是否删除普通文件 "/var/www/html/test.html"? y
```

## ВЫВОДЫ

---

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1