

Лабораторная работа № 6

Мандатное разграничение прав в Linux

Морозов М. Е.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

В SELinux права доступа определяются самой системой при помощи специально определённых политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux: через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила SELinux «прозрачны» для приложений, и не требуется никакой их модификации. В состав некоторых дистрибутивов входят готовые политики, в которых права могут определяться на основе совпадения типов процесса (субъекта) и файла (объекта) — это основной механизм SELinux. Две других формы контроля доступа — доступ на основе ролей и на основе многоуровневой системы безопасности.

Выполнение лабораторной работы

Убедимся, что SELinux работает в режиме enforcing политики targeted. Обратимся к веб-серверу и убедимся, что он работает. Найдем apache в списке процессов. Посмотрим статистику по политике. Определим тип файлов и директорий в `/var/www`. Посмотрим список пользователей.

Создадим от имени root файл в `/var/www/html`. Попробуем посмотреть файл в браузере. Изменим контекст файла. Добавим на прослушивание порт 81. Вернем все как было.

Результаты работы команд

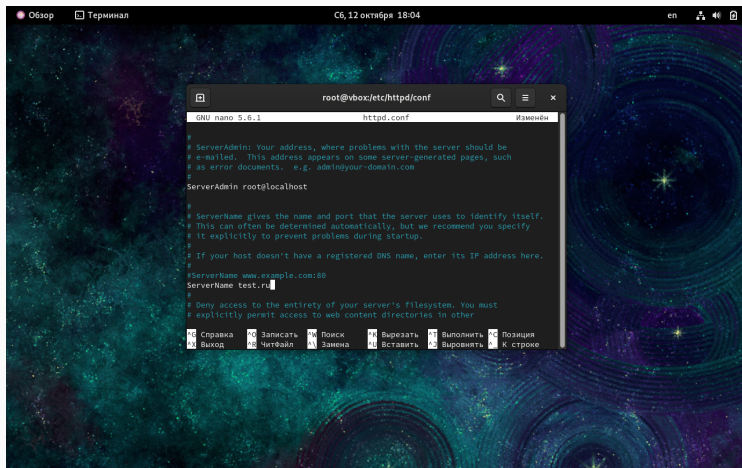


Figure 1: 1


```

Обзор Терминал C6, 12 октября 18:18 en
roo@vbox:/etc/httpd/conf

roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
[roo@vbox conf]$ su
bash: su: команда не найдена...
Аналогичная команда: 'su'
[roo@vbox conf]$ su
Пароль:
[roo@vbox conf]$ ps auxZ | grep httpd
bash: grep: команда не найдена...
[roo@vbox conf]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3367 0.0 0.6 21312 11504 ? Ss 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3368 0.0 0.4 23844 7276 ? S 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3371 0.0 0.6 982596 11092 ? Sl 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3372 0.0 0.7 1113732 13472 ? Sl 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3374 0.0 0.6 982596 11092 ? Sl 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3648 0.0 0.5 237768 9344 pts/0 S+ 18:15 0:00 /bin/systemctl status httpd.service
[roo@vbox conf]$ sestatus -bigrep httpd
bash: sestatus: команда не найдена...
[roo@vbox conf]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[roo@vbox conf]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

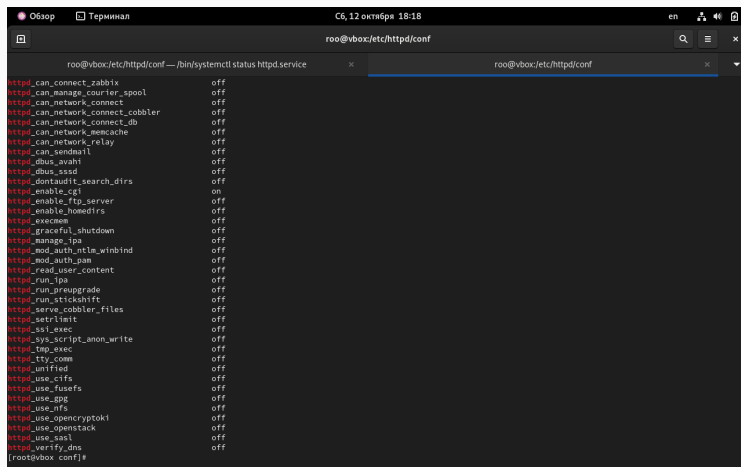
Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[roo@vbox conf]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off

```

Figure 2: 2



The screenshot shows a terminal window with a dark background. The title bar at the top indicates the window is titled 'Обзор' (Overview) and 'Терминал' (Terminal), with the date and time 'Сб, 12 октября 18:18'. The terminal prompt is 'roo@vbox:/etc/httpd/conf'. The command being executed is 'systemctl status httpd.service'. The output is a list of configuration options for the httpd service, each followed by its status, either 'off' or 'on'. The options include various modules and features like 'zabbix', 'courier_spool', 'network_connect', 'network_connect_cobbler', 'network_connect_db', 'network_memcache', 'network_relay', 'sendmail', 'dbus_avahi', 'dbus_sssd', 'dontaudit_search_dirs', 'enable_cgi', 'enable_ftp_server', 'enable_homedirs', 'execmem', 'graceful_shutdown', 'manage_ipa', 'mod_auth_ntlm_winbind', 'mod_auth_pam', 'read_user_content', 'run_ipa', 'run_preupgrade', 'run_stickshift', 'serve_cobbler_files', 'setrlimit', 'ssi_exec', 'sys_script_anon_write', 'tmp_exec', 'tty_coma', 'unified', 'use_cifs', 'use_fusefs', 'use_gpg', 'use_nfs', 'use_opencryptoki', 'use_openstack', 'use_sasl', and 'verify_dns'. The prompt at the bottom is '[root@vbox conf]#'.

```
roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
roo@vbox:/etc/httpd/conf

httpd_can_connect_zabbix      off
httpd_can_manage_courier_spool off
httpd_can_network_connect     off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db  off
httpd_can_network_memcache    off
httpd_can_network_relay       off
httpd_can_sendmail            off
httpd_dbus_avahi              off
httpd_dbus_sssd               off
httpd_dontaudit_search_dirs   off
httpd_enable_cgi              on
httpd_enable_ftp_server       off
httpd_enable_homedirs         off
httpd_execmem                 off
httpd_graceful_shutdown       off
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_coma                off
httpd_unified                  off
httpd_use_cifs                 off
httpd_use_fusefs              off
httpd_use_gpg                  off
httpd_use_nfs                  off
httpd_use_opencryptoki        off
httpd_use_openstack           off
httpd_use_sasl                 off
httpd_verify_dns              off
[root@vbox conf]#
```

Figure 3: 3

4 (рис. 4)

The screenshot shows a terminal window with a dark theme. The title bar indicates the window is titled 'Обзор' (Overview) and 'Терминал' (Terminal), with the date and time 'Сб, 12 октября 18:19'. The terminal prompt is 'roo@vbox:/etc/httpd/conf'. The user has run the command 'systemctl status httpd.service', which displays a table of SELinux statistics. Below this, the user has run 'seinfo', which displays a more detailed set of SELinux statistics. The terminal window has multiple tabs open, with the current tab being 'roo@vbox:/etc/httpd/conf'.

```
roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
Type_member: 37 Range_trans: 5931
Role_allow: 40 Role_trans: 417
Constraints: 70 Validate_trans: 0
MLS_Constrain: 72 MLS_Val. Tran: 0
Permissives: 1 Polcap: 6
Defaults: 7 Typebounds: 0
Allowperm: 0 Neverallowperm: 0
Auditallowperm: 0 Dontauditperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial_SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[root@vbox conf]# 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: 5169 Attributes: 259
Users: 8 Roles: 15
Booleans: 358 Cond. Expr.: 390
Allow: 65633 Neverallow: 0
Auditallow: 176 Dontaudit: 8703
Type_trans: 271851 Type_change: 94
Type_member: 37 Range_trans: 5931
Role_allow: 40 Role_trans: 417
Constraints: 70 Validate_trans: 0
MLS_Constrain: 72 MLS_Val. Tran: 0
Permissives: 1 Polcap: 6
Defaults: 7 Typebounds: 0
Allowperm: 0 Neverallowperm: 0
Auditallowperm: 0 Dontauditperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial_SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[root@vbox conf]#
```

Figure 4: 4

```

Обзор Терминал C6, 12 октября 18:20 en
roo@vbox:/etc/httpd/conf

roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
roo@vbox:/etc/httpd/conf

Permissions: 1 Polcap: 6
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial_SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[root@vbox conf]# 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: 5169 Attributes: 259
Users: 8 Roles: 15
Booleans: 358 Cond. Expr.: 390
Allow: 65633 Neverallow: 0
Auditallow: 176 Dontaudit: 8703
Type_trans: 271851 Type_change: 94
Type_member: 37 Range_trans: 5931
Role_allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constrains: 72 MLS Val. Tran: 0
Permissions: 1 Polcap: 6
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial_SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[root@vbox conf]# ls -lZ /var/www
что-то 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 аар 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 аар 12 16:20 html
[root@vbox conf]#

```

Figure 5: 5

The screenshot shows a terminal window with a dark theme. The title bar indicates the window is titled 'Обзор' (Overview) and 'Терминал' (Terminal), with the system time 'Сб, 12 октября 18:25'. The terminal content shows a user 'roo' at a host 'vbox' in the directory '/var/www/html'. The user runs 'systemctl status httpd.service', which displays a table of SELinux settings. Subsequently, the user runs 'ls -lZ /var/www', 'ls -lZ /var/www/http', and 'ls -lZ /var/www/html', all of which result in permission denied messages. The user then runs 'cd /var/www/html' and 'nano test', creating a file. Finally, the user runs 'ls -lZ /var/www/test.html', which also results in a permission denied message. The terminal output for the SELinux status is as follows:

Type member:	37	Range trans:	5931
Role allow:	40	Role trans:	417
Constraints:	70	Validate trans:	0
MLS Constrains:	72	MLS Val. Tran:	0
Permissives:	1	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

```

[roo@vbox conf]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 12 16:20 html
[roo@vbox conf]# ls -lZ /var/www/http
ls: невозможно получить доступ к '/var/www/http': Нет такого файла или каталога
[roo@vbox conf]# ls -lZ /var/www/html
итого 0
[roo@vbox conf]# cd /var/www/html
[roo@vbox html]# nano test
[roo@vbox html]# nano test.html
[roo@vbox html]# ls -lZ /var/www/test.html
ls: невозможно получить доступ к '/var/www/test.html': Нет такого файла или каталога
[roo@vbox html]# ls
test.html
[roo@vbox html]# ls -lZ test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 окт 12 18:23 test.html
[roo@vbox html]# secon --file var/www/html/test.html
secon: Couldn't get security context for file var/www/html/test.html: No such file or directory
[roo@vbox html]# secon --file test.html
user: unconfined_u
role: object_r
type: httpd_sys_content_t
sensitivity: s0
clearance: s0
mls-range: s0
[roo@vbox html]#

```

Figure 6: 6

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux¹. Проверили работу SELinx на практике совместно с веб-сервером Apache.

1. SELinux [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: <https://ru.wikipedia.org/wiki/SELinux>.