

# Лабораторная работа №9

## Управление SELinux

Перфилов Александр Константинович | Группа НПИбд-03-24

Российский университет дружбы народов, Москва, Россия

31 октября 2025

## Раздел 1

### Информация

# Докладчик

- Перфилов Александр Константинович
- Группа НПИбд-03-24
- Российский университет дружбы народов
- <https://github.com/AlexanderPErfilovKonstantinivich?tab=repositories>

## Цель работы:

Целью данной работы является получение навыков работы с контекстом безопасности и политиками SELinux.

## Задание

- 1 Продemonстрируйте навыки по управлению режимами SELinux.
- 2 Продemonстрируйте навыки по восстановлению контекста безопасности SELinux.
- 3 Настройте контекст безопасности для нестандартного расположения файлов вебслужбы.
- 4 Продemonстрируйте навыки работы с переключателями SELinux.

## Раздел 2

# Результаты и анализ лабораторной работы

# Управление режимами SELinux

- ❶ Для просмотра текущей информации о состоянии SELinux используем `sestatus -v`

```
root@akpperfilov:~# 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
```

# Управление режимами SELinux

## ② Изменение режима работы SELinux на разрешающий (Permissive)

```
root@akpperfilov:~# getenforce
Enforcing
root@akpperfilov:~# setenforce 0
root@akpperfilov:~# getenforce
Permissive
```



## Управление режимами SELinux

- 3 Попробовали переключить режим работы SELinux: `setenforce 1`. Не могла переключаться между отключённым и принудительным режимом без перезагрузки системы.

```
akpperfilov@akpperfilov:~$ su -  
Пароль:  
Последний вход в систему: Пт окт 31 15:48:35 MSK 2025 на pts/0  
root@akpperfilov:~# getenforce  
Disabled  
root@akpperfilov:~# setenforce 1  
setenforce: SELinux is disabled  
root@akpperfilov:~# nano /etc/sysconfig/selinux
```

# Использование restorecon для восстановления контекста безопасности

- 1 Просмотр контекста безопасности файла /etc/hosts: `ls -Z /etc/hosts`.

```
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт окт 31 16:02:28 MSK 2025 на pts/0
root@akpperfilov:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@akpperfilov:~# cp /etc/hosts ~/
root@akpperfilov:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@akpperfilov:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
root@akpperfilov:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@akpperfilov:~# 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
```

## Использование restorecon для восстановления контекста безопасности

- ② Исправление контекста безопасности `restorecon -v /etc/hosts`. Опция `-v` показала процесс изменения. Убедилась, что тип контекста изменился. Для массового исправления контекста безопасности на файловой системе используем `touch /.autorelabel`.

```
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт окт 31 16:02:28 MSK 2025 на pts/0
root@akpperfilov:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@akpperfilov:~# cp /etc/hosts ~/
root@akpperfilov:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@akpperfilov:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
root@akpperfilov:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
```

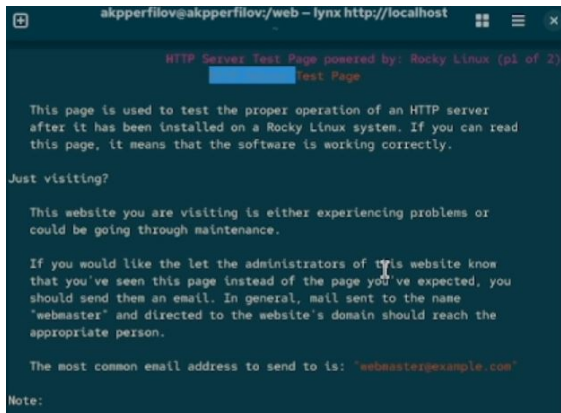
# Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

- 1 Запуск веб-сервера и службы httpd.

```
root@akpperfilov:/web# systemctl start httpd  
root@akpperfilov:/web# systemctl enable httpd
```

## Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

- 2 В терминале под учётной записью своего пользователя обращаемся к веб-серверу в текстовом браузере lynx: `lynx http://localhost`.



```
akpperfilov@akpperfilov:/web – lynx http://localhost
HTTP Server Test Page powered by: Rocky Linux (pi of 2)
Test Page

This page is used to test the proper operation of an HTTP server
after it has been installed on a Rocky Linux system. If you can read
this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or
could be going through maintenance.

If you would like to let the administrators of this website know
that you've seen this page instead of the page you've expected, you
should send them an email. In general, mail sent to the name
"webmaster" and directed to the website's domain should reach the
appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:
```

## Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

- 3 В терминале с полномочиями администратора применяем новую метку контекста к /web: `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)"?"`.  
Восстанавливаем контекст безопасности.

```
root@akpperfilov:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)"?"
root@akpperfilov:~# 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
```

# Работа с переключателями SELinux

- ❶ Вывод списка переключателей SELinux для службы ftp: `getsebool -a | grep ftp`.

```
akpperfilov@akpperfilov:~$ lynx http://localhost
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт окт 31 16:18:40 MSK 2025 на pts/0
root@akpperfilov:~# 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_node --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
root@akpperfilov:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (выкл.,выкл.) Allow ftpd to anon write
root@akpperfilov:~# etsebool ftpd_anon_write on
bash: etsebool: команда не найдена...
root@akpperfilov:~# setsebool ftpd_anon_write on
root@akpperfilov:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (вкл. ,выкл.) Allow ftpd to anon write
root@akpperfilov:~# getsebool ftpd_anon_write
ftpd_anon_write --> on
```

# Работа с переключателями SELinux

- ② Изменение текущего значения переключателя для службы `ftpd_anon_write` с `off` на `on`.

```
akpperfilov@akpperfilov:~$ lynx http://localhost
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт окт 31 16:18:40 MSK 2025 на pts/0
root@akpperfilov:~# 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@akpperfilov:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (выкл.,выкл.) Allow ftpd to anon write
root@akpperfilov:~# etsebool ftpd_anon_write on
bash: etsebool: команда не найдена...
root@akpperfilov:~# setsebool ftpd_anon_write on
root@akpperfilov:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write          (вкл. ,выкл.) Allow ftpd to anon write
root@akpperfilov:~# getsebool ftpd_anon_write
ftpd_anon_write --> on
```



## Работа с переключателями SELinux

- ③ Изменение постоянного значение переключателя для службы `ftpd_anon_write` с `off` на `on`: `setsebool -P ftpd_anon_write on`.

```
akpperfilov@akpperfilov:~$ lynx http://localhost
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт окт 31 16:18:40 MSK 2025 на pts/0
root@akpperfilov:~# 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@akpperfilov:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
root@akpperfilov:~# etsebool ftpd_anon_write on
bash: etsebool: команда не найдена...
root@akpperfilov:~# setsebool ftpd_anon_write on
root@akpperfilov:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write
```

## Раздел 3

### Выводы

## Выводы

В ходе выполнения лабораторной работы были получены навыки работы с контекстом безопасности и политиками