

Отчет по лабораторной работе №9

Отчет о мониторинге и настройке системных журналов

Лупупа Чилеше

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Управление режимами SELinux	6
3	Использование restorecon для восстановления контекста безопасности	8
4	Настройка контекста для нестандартного расположения веб-файлов	10
5	Работа с переключателями SELinux	13

Список иллюстраций

Список таблиц

1 Цель работы

Цель данной лабораторной работы – изучение основ управления режимами SELinux, восстановления контекста безопасности файлов, настройки нестандартного расположения файлов веб-сервера и работы с переключателями SELinux. В ходе выполнения работы студенты научатся изменять режимы работы SELinux, корректировать контексты безопасности с помощью `restorecon`, настраивать SELinux для работы веб-сервера и управлять SELinux-переключателями.

2 Выполнение лабораторной работы

2.1 Управление режимами SELinux

1. Запуск терминала и получение прав администратора Выполнена команда `su`.
2. Просмотр состояния SELinux Команда `sestatus -v` вывела информацию:

```
[root@chileshelepupa ~]# 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
/bin/login                    system_u:object_r:login_exec_t:s0
/bin/sh                        system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                system_u:object_r:sshd_exec_t:s0
[root@chileshelepupa ~]#
```

- SELinux status: показывает, включена ли SELinux.
- Current mode: текущий режим (Enforcing, Permissive, Disabled).
- Policy version: используемая политика безопасности.
- Loaded policy: загруженный набор правил безопасности.
- Mode from config file: режим, установленный в конфигурации

3. Определение текущего режима работы Команда `getenforce` показала Enforcing (принудительный режим).
4. Изменение режима на Permissive

```
[root@chileshelupupa ~]# getenforce
Permissive
[root@chileshelupupa ~]#
```

`setenforce 0` изменил режим на Permissive. `getenforce` подтвердил изменение.

5. Отключение SELinux через конфигурационный файл

```
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

В файле `/etc/sysconfig/selinux` установлено `SELINUX=disabled`. После перезагрузки система подтвердила отключение (`getenforce` вернул Disabled).

6. Попытка включения SELinux без перезагрузки

```
[root@chileshelupupa ~]# setenforce 1
setenforce: SELinux is disabled
[root@chileshelupupa ~]#
```

`setenforce 1` не сработал, так как отключенный SELinux требует перезагрузки.

7. Возвращение режима Enforcing

```
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

В файле `/etc/sysconfig/selinux` установлено `SELINUX=enforcing`. После перезагрузки система запустилась в режиме Enforcing, возможно с предупреждением о необходимости восстановления меток.

3 Использование restorecon для восстановления контекста безопасности

1. Просмотр контекста файла /etc/hosts

```
[root@chilishelupupa ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@chilishelupupa ~]#
```

ls -Z /etc/hosts показал net_conf_t.

2. Копирование файла и изменение контекста

```
[root@chilishelupupa ~]# cp /etc/hosts ~/
[root@chilishelupupa ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@chilishelupupa ~]#
```

cp /etc/hosts ~/ создал копию с контекстом admin_home_t.

3. Перемещение файла обратно и проверка контекста

```
[root@chilishelupupa ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
```

mv ~/hosts /etc сохранило admin_home_t.

4. Исправление контекста

```
[root@chilishelupupa ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@chilishelupupa ~]# 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
[root@chilishelupupa ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@chilishelupupa ~]#
```

restorecon -v /etc/hosts восстановил net_conf_t.

5. Массовое исправление контекста

touch /.autorelabel и перезагрузка инициировали перемаркировку файловой системы

4 Настройка контекста для нестандартного расположения веб-файлов

1. Установка Apache и текстового браузера

```
[root@chileshelupupa ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               569 B/s | 4.1 kB    00:07
Rocky Linux 9 - BaseOS                               497 kB/s | 2.3 MB   00:04
Rocky Linux 9 - AppStream                             5.7 kB/s | 4.5 kB   00:00
Rocky Linux 9 - AppStream                             310 kB/s | 8.5 MB   00:28
Rocky Linux 9 - Extras                               3.1 kB/s | 2.9 kB   00:00
Rocky Linux 9 - Extras                               14 kB/s | 16 kB     00:01
Package httpd-2.4.62-1.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

```
[root@chileshelupupa ~]# dnf -y install lynx
Last metadata expiration check: 0:00:29 ago on Thu 13 Feb 2025 02:01:41 PM MSK.
Dependencies resolved.
=====
Package                Architecture      Version           Repository         Size
=====
Installing:
lynx                   x86_64            2.8.9-20.el9     appstream          1.5 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm                                123 kB/s | 1.5 MB    00:12
-----
Total                                                         116 kB/s | 1.5 MB    00:13
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 1/1
  Installing     : lynx-2.8.9-20.el9.x86_64                  1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64                1/1
  Verifying      : lynx-2.8.9-20.el9.x86_64                  1/1

Installed:
  lynx-2.8.9-20.el9.x86_64

Complete!
```

dnf -y install httpd lynx.

2. Создание каталога и конфигурация Apache

```
[root@chileshelupupa ~]# mkdir /web
[root@chileshelupupa ~]# mkdir /web
mkdir: cannot create directory '/web': File exists
[root@chileshelupupa ~]# ^C
[root@chileshelupupa ~]# ^C
[root@chileshelupupa ~]# cd /web
[root@chileshelupupa web]# touch index.html
[root@chileshelupupa web]# nano index.html
[root@chileshelupupa web]#
```

mkdir /web, добавлен index.html.

```
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#     AllowOverride None
#     # Allow open access:
#     Require all granted
#</Directory>

<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
```

В /etc/httpd/conf/httpd.conf изменен DocumentRoot на /web.

3. Запуск Apache и тестирование через lynx

```
HTTP Server Test Page HTTP Server Test Page powered by: Rocky Linux

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 the 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, email 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"

Notes:

The Rocky Linux distribution is a stable and reproducible platform based on the sources of Red Hat
Enterprise Linux (RHEL). With this in mind, please understand that:
  * Neither the Rocky Linux Project nor the Rocky Enterprise Software Foundation have anything to do with
    this website or its content.
  * The Rocky Linux Project nor the RSEF have "hacked" this webserver. This test page is included with the
    distribution.

For more information about Rocky Linux, please visit the Rocky Linux website.

I am the admin, what do I do?

You may now add content to the webroot directory for your software.

For systems using the Apache Webserver: You can add content to the directory /var/www/html/. Until you do so,
people visiting your website will see this page. If you would like this page to not be shown, follow the
instructions in: /etc/httpd/conf.d/welcome.conf.

For systems using Nginx: You can add your content in a location of your choice and edit the root
configuration directive in /etc/nginx/nginx.conf.
[ Powered by Rocky Linux ] [poweredby.png]

Apache® is a registered trademark of the Apache Software Foundation in the United States and/or other
countries.
Rocky® is a registered trademark of FS Networks, Inc..
```

systemctl start httpd, но страница по умолчанию не отображала новый контент.

4. Изменение контекста безопасности

semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?". restorecon -R -v /web
ВОССТАНОВИЛ КОНТЕКСТ.

5.Повторное тестирование через lynx

```
Welcome to my web-server
```

После перезагрузки веб-страница Welcome to my web-server отобразилась успешно.

5 Работа с переключателями SELinux

1. Просмотр переключателей для FTP

```
[root@chileshelupupa ~]# 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
```

getsebool -a | grep ftp показал ftpd_anon_write off.

2. Просмотр переключателей с пояснениями

```
[root@chileshelupupa ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@chileshelupupa ~]#
```

semanage boolean -l | grep ftpd_anon подтвердил временное изменение.

3. Установка постоянного значения setsebool -P ftpd_anon_write on сохранил изменение после перезагрузки.
4. Проверка состояния после перезагрузки semanage boolean -l | grep ftpd_anon подтвердил on для ftpd_anon_write.