Отчет по лабораторной работе №9

Отчет о мониторинге и настройке системных журналов

Чилеше . Л

27 января 2003

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Информация

Докладчик

- Лупупа Чилеше
- Студент
- Студент Группы НПИбд-03-23
- Российский университет дружбы народов

Вводная часть

Цель работ

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.

Управление режимами SELinux

Просмотр состояния SELinux

Команда sestatus -v вывела информацию:

```
[root@chileshelupups ~]# sestatus ~v
SELinux status:
                                ba.ldana
SFLinuxfs mount:
                                /sys/fs/selinux
SELinux root directory:
                                /etc/selinux
Loaded policy name:
                                targeted
Current mode:
                                enforcing
Mode from config file:
                                enforcing
Policy MLS status:
                                ba.I dana
Policy deny unknown status:
                                allowed
Memory protection checking:
                                actual (secure)
Max kernel policy version:
Process contexts:
Current context:
                                unconfined usunconfined rsunconfined tis0-s0:c0.c1823
Init context:
                                system wisystem riinit tis0
/usr/sbin/sshd
                                system_u:system_r:sshd_t:s0-s8:c0.c1823
File contexts:
Controlling terminal:
                                unconfined_u:object_r:user_devpts_t:s0
/etc/passed
                                system u:object r:passwd file t:s0
/etc/shadow
                                system wichfect rishadow tish
/bin/bash
                                system u:object r:shell exec t:s0
/bin/login
                                system u:object r:login exec t:sD
/b1m/sh
                                system wiobject ribin tis8 -> system wiobject rishell exec tis8
sbin/agetty
                                system_u:object_r:getty_exec_t:s0
sbin/finit
                                system upobject ribin tisB -> system upobject ribit exec tisB
hier/shin/sehd
                                system wighfast risshif over tish
```

Определение текущего режима работы

Команда getenforce показала Enforcing (принудительный режим).

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

Изменение режима на Permissive

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

setenforce 0 изменил режим на Permissive. getenforce подтвердил изменение.

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).

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.

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.

восстановления контекста безопасности

Использование restorecon для

Просмотр контекста файла /etc/hosts

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

ls -Z /etc/hosts показал net_conf_t.

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

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

Перемещение файла обратно и проверка контекста

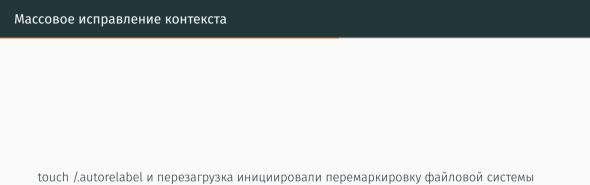
```
[root@chileshelupupa ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
```

mv ~/hosts /etc сохранило admin_home_t.

Исправление контекста

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

restorecon -v /etc/hosts восстановил net_conf_t.



Настройка контекста для нестандартного расположения

веб-файлов

Установка Apache и текстового браузера

```
[root@chileshelupupa ~]# dnf -v install httpd
Rocky Linux 9 - BaseOS
                                                                                            R/s | 4.1 kR
                                                                                                              88:87
Rocky Linux 9 - BaseOS
                                                                                                              00:04
Rocky Linux 9 - AppStream
                                                                                                              00:00
Rocky Linux 9 - AppStream
                                                                                        310 kR/s | 8.5 MR
                                                                                                              89:28
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@chileshelumuma ~l# dnf -v install lvnx
Last metadata expiration check: 8:00:29 ago on Thu 13 Feb 2025 02:01:41 PM MSK.
                                                   2.8.9-20.et9
                                                                                                                 1.5 H
Transaction Summary
Install 1 Package
otal download size: 1.5 M
installed size: 6.1 M
Downloading Packages:
vnx-2.8.9-28.el9.x86.64.rpm
                                                                                      123 kB/s | 1.5 MB
                                                                                      116 kB/s | 1.5 MB
Running transaction check
Transaction check succeeded.
Running transaction test
 ransaction test succeeded
Running transaction
              : lunx-2.8.9-28.el9.x85 64
 Running scriptlet: lunx-2.8.9-28.el9.x86 64
               : lunx-2.8.9-28.e19.x86 64
 lynx-2.8.9-20.el9.x86.64
```

```
[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.

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

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

Запуск Apache и тестирование через lynx

This page is used to test the proper operation of an HTTP server after it has been installed on a Bocky Linux system. If you can read this page, it means that the software is working correctly. ust wisiting? 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 amboite love 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 ambuite's domain should reach the appropriate person. The most common small address to send to in: Suchmaniaries small com? The Snoky Linux distribution is a stable and reproduceable platform based on the sources of Sed Hat Enterprise Linux (BHEL), With this in mind, please understand that: For more information about Socky Linux, please visit the Socky Linux sebsite. on the admin, what do I do? You may now add content to the webrant directory for your software. Apache" is a registered trademark of the Apache Software Coundation in the United States and/or other HOTHEr is a registered trademark of FS between, Inc. .

Изменение контекста безопасности

```
[root@chileshelupupa web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@chileshelupupa web]# 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
[root@chileshelupupa web]# ■
```

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

Повторное тестирование через lynx

Welcome to my web-server

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

Общие рекомендации

Работа с переключателями SELinux

```
[root@chileshelupupa ~]# getsebool -a | grep ftp
  d anon write --> off
  d connect all unreserved --> off
  d connect db --> off
  d full access --> off
  d use cifs --> off
  d use fusefs --> off
  d use nfs --> off
  d use passive mode --> off
httpd can connect ftp --> off
httpd enable ftp server --> off
tftp anon write --> off
 tp home dir --> off
```

getsebool -a | grep ftp показал ftpd_anon_write off.

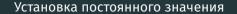
Просмотр переключателей с пояснениями

```
[root@chileshelupupa ~]# semanage boolean -l | grep ftpd_anon

ftpd_anon_write

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

semanage boolean -l | grep ftpd_anon подтвердил временное изменение.



setsebool -P ftpd_anon_write on сохранил изменение после перезагрузки.

Проверка состояния после перезагрузки

semanage boolean -l | grep ftpd_anon подтвердил on для ftpd_anon_write.