

Лабораторная работа №6: отчет.

Мандатное разграничение прав в Linux.

Евдокимов Максим Михайлович. Группа - НФИбд-01-20.

Содержание

Цель работы	4
Задание	5
Подготовка	6
Пункт 1	6
Пункт 2	6
Выполнение лабораторной работы	8
Пункт 1	8
Пункт 2	8
Пункт 3	9
Пункт 4	10
Пункт 5	10
Пункт 6	11
Пункт 7	11
Пункт 8	11
Пункт 9	12
Пункт 10	12
Пункт 11	12
Пункт 12	13
Пункт 13	13
Пункт 14	14
Пункт 15	14
Пункт 16	15
Пункт 17	15
Пункт 18	15
Пункт 19	16
Пункт 20	16
Пункт 21	17
Пункт 22	17
Пункт 23	18
Пункт 24	18
Выводы	19
Список литературы	20

Список иллюстраций

1	Подготовка к выполнению 1	6
2	Подготовка к выполнению 2	7
3	Подготовка к выполнению 3	7
1	Проверка параметров	8
2	Проверка веб-сервиса	9
3	Находим сервис	9
4	Проверка переключателей	10
5	Просмотр статистики	10
6	Анализ файлов в www	11
7	Анализ файлов в html	11
8	Проверка уровня допуска	11
9	Создание локальной веб-страницы	12
10	Проверка контекста	12
11	Просмотр сайта	13
12	Изучаем справку	13
13	Изменяем контекст	13
14	Пробуем зайти	14
15	Проверяем доступ к файлу	14
16	Запуск прослушивание	15
17	Перезапуск веб-сервиса	15
18	Анализ лог-файлов	16
19	Активация порта	16
20	Повторный запуск сайта	16
21	Возвращаем изменения 1	17
22	Возвращаем изменения 2	17
23	Возвращаем изменения 3	18
24	Удаляем файл	18

Цель работы

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

Задание

1. Истновить Apache и настроить его и систему для работы.
2. Изучить основы упрвления и создания локальных сайтов.
3. Изучить основы SELinux и его работы совместно с веб-сервером Apache.

Подготовка

Пункт 1

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux. А также иметь установленный пакет Apache или его аналог httpd.

Пункт 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.

```
[max@Max ~]$ sudo systemctl enable httpd
[sudo] пароль для max:
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[max@Max ~]$ █
```

Рис. 1: Подготовка к выполнению 1

В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName "test.ru"` чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.

```

[max@Max ~]$ gedit /etc/httpd/httpd.conf
[max@Max ~]$ sudo gedit /etc/httpd/httpd.conf
[sudo] пароль для max:

** (gedit:30416): WARNING **: 11:47:23.078: Set document metadata failed: Устано
вка атрибута metadata::gedit-spell-language не поддерживается

** (gedit:30416): WARNING **: 11:47:23.081: Set document metadata failed: Устано
вка атрибута metadata::gedit-encoding не поддерживается

** (gedit:30416): WARNING **: 11:47:35.585: Set document metadata failed: Устано
вка атрибута metadata::gedit-position не поддерживается
[max@Max ~]$ gedit /etc/httpd/httpd.conf
[max@Max ~]$

```

Рис. 2: Подготовка к выполнению 2

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

```

[max@Max ~]$ sudo iptables -F
[max@Max ~]$ sudo iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[max@Max ~]$ iptables -I INPUT -p tcp --dport 80 -j ACCEPT
iptables v1.4.21: can't initialize iptables table `filter': Permission denied (y
ou must be root)
Perhaps iptables or your kernel needs to be upgraded.
[max@Max ~]$ sudo iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[max@Max ~]$ sudo iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[max@Max ~]$ sudo iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[max@Max ~]$ sudo iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[max@Max ~]$ █

```

Рис. 3: Подготовка к выполнению 3

Выполнение лабораторной работы

Пункт 1

Воходим в систему с полученными учётными данными и убеждаемся, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”.

```
[max@Max ~]$ getenforce
Enforcing
[max@Max ~]$ 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:     31
[max@Max ~]$ █
```

Рис. 1: Проверка параметров

Пункт 2

Обратимся с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает “service httpd status”.


```
[max@Max ~]$ 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 preset
   : disabled)
   Active: active (running) since Вт 2023-10-03 11:41:16 MSK; 11min ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Main PID: 29324 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/s
ec"
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─29324 /usr/sbin/httpd -DFOREGROUND
              └─29331 /usr/sbin/httpd -DFOREGROUND
                └─29332 /usr/sbin/httpd -DFOREGROUND
                  └─29333 /usr/sbin/httpd -DFOREGROUND
                    └─29334 /usr/sbin/httpd -DFOREGROUND
                      └─29335 /usr/sbin/httpd -DFOREGROUND

окт 03 11:41:16 Max.localdomain systemd[1]: Starting The Apache HTTP Serv....
окт 03 11:41:16 Max.localdomain httpd[29324]: AH00558: httpd: Could not r...e
окт 03 11:41:16 Max.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[max@Max ~]$
```

Рис. 2: Проверка веб-сервиса

Пункт 3

Найдём веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду “ps -eZ | grep httpd”

```
[max@Max ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 29324 0.0 0.2 230448 4452 ? S
s 11:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29331 0.0 0.1 232532 2852 ? S
11:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29332 0.0 0.1 232532 2852 ? S
11:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29333 0.0 0.1 232532 2852 ? S
11:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29334 0.0 0.1 232532 2852 ? S
11:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 29335 0.0 0.1 232532 2852 ? S
11:41 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 max 32113 0.0 0.0 112832
976 pts/0 R+ 11:53 0:00 grep --color=auto httpd
[max@Max ~]$
```

Рис. 3: Находим сервис

Пункт 4

Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”.

```
[max@Max ~]$ 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.
[max@Max ~]$
```

Рис. 4: Проверка переключателей

Пункт 5

Посмотрим статистику по политике с помощью команды seinfo, такжеопределите множество пользователей, ролей, типов.

```
[max@Max ~]$ httpd seinfo
Usage: httpd [-D name] [-d directory] [-f file]
             [-C "directive"] [-c "directive"]
             [-k start|restart|graceful|graceful-stop|stop]
             [-v] [-V] [-h] [-l] [-L] [-t] [-T] [-S] [-X]

Options:
  -D name           : define a name for use in <IfDefine name> directives
  -d directory      : specify an alternate initial ServerRoot
  -f file           : specify an alternate ServerConfigFile
  -C "directive"    : process directive before reading config files
  -c "directive"    : process directive after reading config files
  -e level          : show startup errors of level (see LogLevel)
  -E file           : log startup errors to file
  -v               : show version number
  -V               : show compile settings
  -h               : list available command line options (this page)
  -l               : list compiled in modules
  -L               : list available configuration directives
  -t -D DUMP_VHOSTS : show parsed vhost settings
  -t -D DUMP_RUN_CFG : show parsed run settings
  -S               : a synonym for -t -D DUMP_VHOSTS -D DUMP_RUN_CFG
  -t -D DUMP_MODULES : show all loaded modules
  -M               : a synonym for -t -D DUMP_MODULES
  -t               : run syntax check for config files
  -T               : start without DocumentRoot(s) check
  -X               : debug mode (only one worker, do not detach)
[max@Max ~]$
```

Рис. 5: Просмотр статистики

Пункт 6

Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды “ls -lZ /var/www”.

```
[max@Max ~]$ 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
[max@Max ~]$
```

Рис. 6: Анализ файлов в www

Пункт 7

Определим тип файлов, находящихся в директории /var/www/html командой “ls -lZ /var/www/html”.

```
[max@Max ~]$ ls -lZ /var/www/html
[max@Max ~]$ sudo ls -lZ /var/www/html
[max@Max ~]$ sudo ls -l /var/www/html
итого 0
[max@Max ~]$
```

Рис. 7: Анализ файлов в html

Пункт 8

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html командой “ls -al /var/www/html”.

```
[max@Max ~]$ ls -al /var/www/html
итого 0
drwxr-xr-x. 2 root root 6 май 30 17:01 .
drwxr-xr-x. 4 root root 33 окт 3 11:41 ..
[max@Max ~]$ ls -al /var/www/
итого 4
drwxr-xr-x. 4 root root 33 окт 3 11:41 .
drwxr-xr-x. 21 root root 4096 окт 3 11:41 ..
drwxr-xr-x. 2 root root 6 май 30 17:01 cgi-bin
drwxr-xr-x. 2 root root 6 май 30 17:01 html
[max@Max ~]$
```

Рис. 8: Проверка уровня допуска

Пункт 9

Создаём от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

test

```
[max@Max ~]$ su
Пароль:
[root@Max max]# sd
bash: sd: команда не найдена...
Аналогичная команда: 'cd'
[root@Max max]# cd
[root@Max ~]# touch /var/www/html/test.html
[root@Max ~]# gedit /var/www/html/test.html
```

Рис. 9: Создание локальной веб-страницы

Пункт 10

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

```
[root@Max ~]# cd /var/www/html
[root@Max html]# ls -Z
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@Max html]#
```

Рис. 10: Проверка контекста

Пункт 11

Обратимся к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Убедимся, что файл был успешно отображён.



Рис. 11: Просмотр сайта

Пункт 12

Изучем справку “man httpd_selinux” и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html, проверив контекст файла можно командой “ls -Z /var/www/html/test.html”.

```
[root@Max html]# man httpd_selinux
Нет справочной страницы для httpd_selinux
[root@Max html]# 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@Max html]#
```

Рис. 12: Изучаем справку

Пункт 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 командами “chcon -t samba_share_t /var/www/html/test.html” и “ls -Z /var/www/html/test.html”.

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

Рис. 13: Изменяем контекст

Пункт 14

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. И получаем сообщение об ошибке Forbidden.



Рис. 14: Пробуем зайти

Пункт 15

Проанализируем ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? “ls -l /var/www/html/test.html”. Просмотрим log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: “tail /var/log/messages”.

```
[root@Max html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 окт  3 11:59 /var/www/html/test.html
[root@Max html]# tail /var/log/messages
Oct  3 12:03:40 Max dbus[715]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct  3 12:03:41 Max dbus[715]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct  3 12:03:41 Max setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct  3 12:03:41 Max setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SE
Linux messages run: sealert -l f08dc3fc-57eb-4beb-80bd-86c718c60840
Oct  3 12:03:41 Max python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin re
storecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default
label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permis
sions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.
html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage
fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1
.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html
file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allo
w this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Oct  3 12:03:53 Max dbus[715]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct  3 12:03:55 Max dbus[715]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct  3 12:03:56 Max setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct  3 12:03:56 Max setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SE
Linux messages run: sealert -l f08dc3fc-57eb-4beb-80bd-86c718c60840
Oct  3 12:03:56 Max python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin re
storecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default
label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permis
sions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.
html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage
fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1
.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html
file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allo
w this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
[root@Max html]#
```

Рис. 15: Проверяем доступ к файлу

Пункт 16

Запустим 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.

```
[root@Max html]# sudo gedit /etc/httpd/httpd.conf
** (gedit:32611): WARNING **: 12:05:07.412: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:32611): WARNING **: 12:05:07.429: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
** (gedit:32611): WARNING **: 12:05:12.914: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается
[root@Max html]#
```

Рис. 16: Запуск прослушивание

Пункт 17

Выполнив перезапуск веб-сервера Apache.

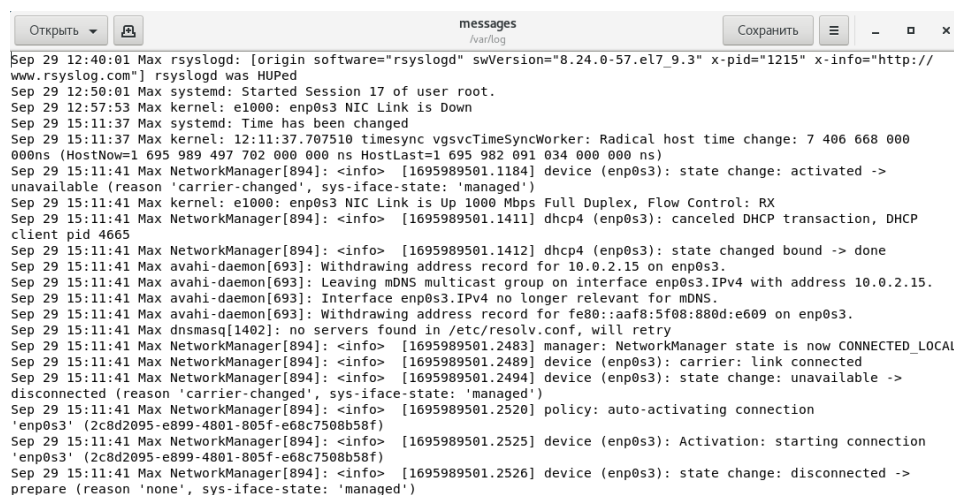
```
[root@Max html]# sudo systemctl restart httpd
[root@Max html]# sudo systemctl reload httpd
[root@Max html]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Вт 2023-10-03 12:06:20 MSK; 12s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 32649 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
  Process: 32689 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 32664 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           └─32664 /usr/sbin/httpd -DFOREGROUND
             └─32701 /usr/sbin/httpd -DFOREGROUND
               └─32702 /usr/sbin/httpd -DFOREGROUND
                 └─32703 /usr/sbin/httpd -DFOREGROUND
                   └─32704 /usr/sbin/httpd -DFOREGROUND
                     └─32705 /usr/sbin/httpd -DFOREGROUND

окт 03 12:06:19 Max.localdomain systemd[1]: Stopped The Apache HTTP Server.
окт 03 12:06:19 Max.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 03 12:06:20 Max.localdomain httpd[32664]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name: /usr/sbin/httpd -DFOREGROUND
окт 03 12:06:20 Max.localdomain systemd[1]: Started The Apache HTTP Server.
окт 03 12:06:25 Max.localdomain systemd[1]: Reloading The Apache HTTP Server.
окт 03 12:06:25 Max.localdomain httpd[32689]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name: /usr/sbin/httpd -DFOREGROUND
окт 03 12:06:25 Max.localdomain systemd[1]: Reloaded The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@Max html]#
```

Рис. 17: Перезапуск веб-сервиса

Пункт 18

Проанализируем лог-файлы командой “tail -nl /var/log/messages”. Также посмотрим файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи.



```
Sep 29 12:40:01 Max rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-57.el7_9.3" x-pid="1215" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
Sep 29 12:50:01 Max systemd: Started Session 17 of user root.
Sep 29 12:57:53 Max kernel: e1000: enp0s3 NIC Link is Down
Sep 29 15:11:37 Max systemd: Time has been changed
Sep 29 15:11:37 Max kernel: 12:11:37.707510 timesync vgsvcTimeSyncWorker: Radical host time change: 7 406 668 000 000ns (HostNow=1 695 989 497 702 000 000 ns HostLast=1 695 982 091 034 000 000 ns)
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.1184] device (enp0s3): state change: activated -> unavailable (reason 'carrier-changed', sys-iface-state: 'managed')
Sep 29 15:11:41 Max kernel: e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.1411] dhcp4 (enp0s3): canceled DHCP transaction, DHCP client pid 4665
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.1412] dhcp4 (enp0s3): state changed bound -> done
Sep 29 15:11:41 Max avahi-daemon[693]: Withdrawing address record for 10.0.2.15 on enp0s3.
Sep 29 15:11:41 Max avahi-daemon[693]: Leaving mDNS multicast group on interface enp0s3.IPv4 with address 10.0.2.15.
Sep 29 15:11:41 Max avahi-daemon[693]: Interface enp0s3.IPv4 no longer relevant for mDNS.
Sep 29 15:11:41 Max avahi-daemon[693]: Withdrawing address record for fe80::aaf8:5f08:880d:e609 on enp0s3.
Sep 29 15:11:41 Max dnsmasq[1402]: no servers found in /etc/resolv.conf, will retry
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.2483] manager: NetworkManager state is now CONNECTED_LOCAL
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.2489] device (enp0s3): carrier: link connected
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.2494] device (enp0s3): state change: unavailable -> disconnected (reason 'carrier-changed', sys-iface-state: 'managed')
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.2520] policy: auto-activating connection 'enp0s3' (2c8d2095-e899-4801-805f-e68c7508b58f)
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.2525] device (enp0s3): Activation: starting connection 'enp0s3' (2c8d2095-e899-4801-805f-e68c7508b58f)
Sep 29 15:11:41 Max NetworkManager[894]: <info> [1695989501.2526] device (enp0s3): state change: disconnected -> prepare (reason 'none', sys-iface-state: 'managed')
```

Рис. 18: Анализ лог-файлов

Пункт 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`”. Убедимся, что порт 81 появился в списке.

```
[root@Max html]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@Max html]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@Max html]#
```

Рис. 19: Активация порта

Пункт 20

Пробуем запустить веб-сервер Apache ещё раз. И он работает.

```
[root@Max html]# sudo systemctl start httpd
[root@Max html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@Max html]#
```

Рис. 20: Повторный запуск сайта

Пункт 21

Вернём 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 попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.



Рис. 21: Возвращаем изменения 1

Пункт 22

Исправим обратно конфигурационный файл `apache`, вернув `Listen 80`.

```
[root@Max html]# gedit /etc/httpd/httpd.conf
(gedit:713): GLib-GIO-CRITICAL **: 12:15:03.296: g_dbus_proxy_new_sync: assertion 'G_IS_DBUS_CONNECTION (connection)' failed
(gedit:713): dconf-WARNING **: 12:15:03.334: failed to commit changes to dconf: Соединение закрыто
(gedit:713): dconf-WARNING **: 12:15:03.462: failed to commit changes to dconf: Соединение закрыто
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
Error creating proxy: Соединение закрыто (g-io-error-quark, 18)
(gedit:713): dconf-WARNING **: 12:15:04.878: failed to commit changes to dconf: Соединение закрыто
(gedit:713): dconf-WARNING **: 12:15:04.878: failed to commit changes to dconf: Соединение закрыто
(gedit:713): dconf-WARNING **: 12:15:04.878: failed to commit changes to dconf: Соединение закрыто
** (gedit:713): WARNING **: 12:15:10.025: Set document metadata failed: Установка атрибута metadata::gedit-spell-language не поддерживается
** (gedit:713): WARNING **: 12:15:10.030: Set document metadata failed: Установка атрибута metadata::gedit-encoding не поддерживается
** (gedit:713): WARNING **: 12:15:11.794: Set document metadata failed: Установка атрибута metadata::gedit-position не поддерживается
(gedit:713): dconf-WARNING **: 12:15:11.977: failed to commit changes to dconf: Соединение закрыто
[root@Max html]#
```

Рис. 22: Возвращаем изменения 2

Пункт 23

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@Max html]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@Max html]#
```

Рис. 23: Возвращаем изменения 3

Пункт 24

Удалим файл /var/www/html/test.html командой “rm /var/www/html/test.html”.

```
[root@Max html]# sudo rm /var/www/html/test.html
[root@Max html]#
```

Рис. 24: Удаляем файл

Выводы

В ходе работы был изучен пакет `httpd` (аналог `apache`), а также основы по работе с ним и с SELinux.

Список литературы

1. Лабораторная №6
2. Основы работы с SELinux
3. Информация о работе с пакетными менеджерами
4. Установка Apache на CentOS через yum
5. Работа с Apache/httpd