# Отчёт по лабораторной работе №9

**Управление SELinux**

Максат Хемраев

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

# 2 Отчёт по выполнению работы

## 2.1 Управление режимами SELinux

1. После входа в систему под пользователем **mhemraev** были получены полномочия администратора с помощью команды su. Затем была выполнена проверка состояния системы безопасности SELinux.

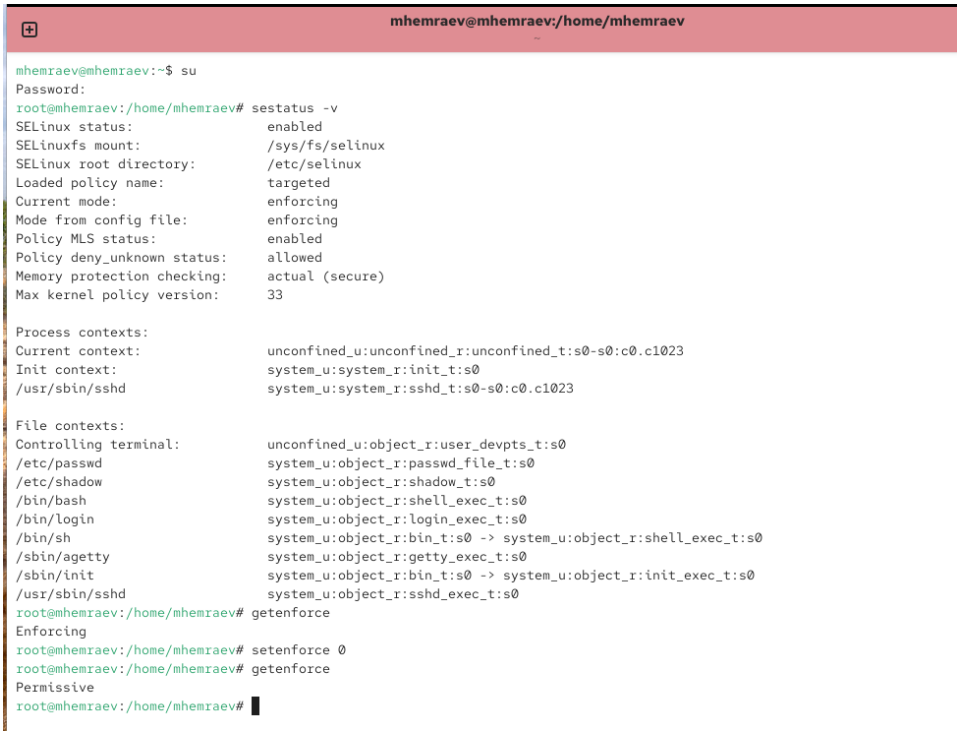


Рис. 2.1: Вывод команды sestatus -v

На экране отобразились следующие параметры:

- **SELinux status: enabled** — система безопасности SELinux активна.

- **SELinuxfs mount: /sys/fs/selinux** — каталог монтирования файловой системы SELinux.

- **SELinux root directory: /etc/selinux** — расположение корневых конфигурационных файлов SELinux.

- **Loaded policy name: targeted** — активна политика типа *targeted*, при которой защите подвергаются только критические системные процессы.

- **Current mode: enforcing** — в данный момент SELinux работает в режиме принудительного контроля доступа.

- **Mode from config file: enforcing** — аналогичный режим задан в конфигурационном файле.

- **Policy MLS status: enabled** — включена поддержка многоуровневой защиты (Multi Level Security).

- **Policy deny_unknown status: allowed** — неизвестные операции разрешены.

- **Memory protection checking: actual (secure)** — защита памяти активна.

В разделе **Process contexts** приведены контексты безопасности для различных процессов, например:

- `/usr/sbin/sshd` выполняется с контекстом `system_u:system_r:sshd_t:s0-s0:c0.c1023`.

А в разделе **File contexts** указаны контексты файлов — `/etc/passwd`, `/etc/shadow`, `/bin/bash` и других системных компонентов.

2. Далее была выполнена проверка режима работы SELinux с помощью команды getenforce, подтвердившая, что система находится в режиме **Enforcing**. После этого SELinux был переведён в **Permissive**-режим, при котором нарушения политик не блокируются, а только фиксируются в журнале. Повторная проверка показала изменение режима.

3. Затем был открыт конфигурационный файл `/etc/sysconfig/selinux` и изменён параметр SELINUX=disabled. После этого система была перезагружена.

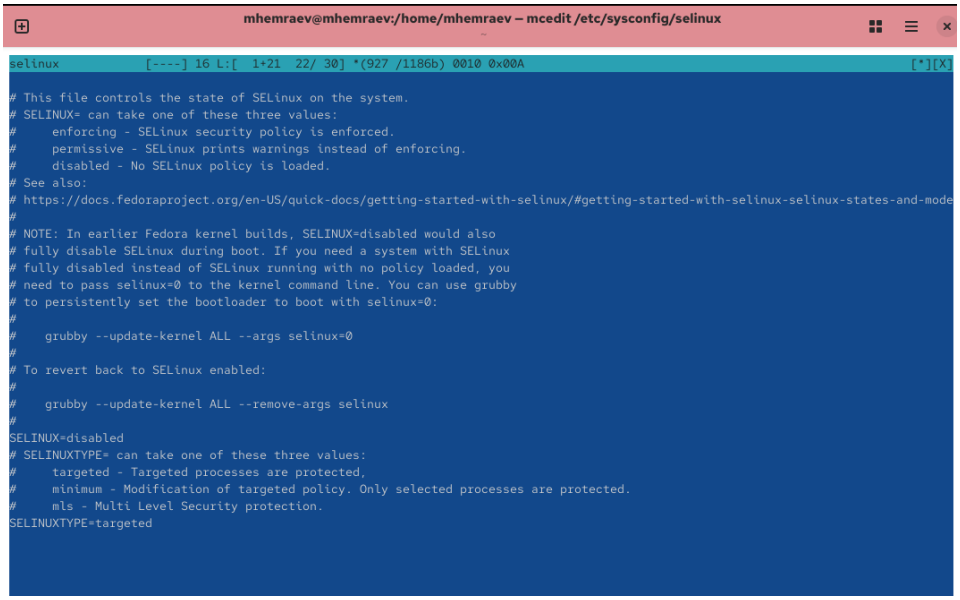


Рис. 2.2: Изменение конфигурации SELinux на disabled

4. После перезапуска проверка показала значение **Disabled**, что подтверждает полное отключение SELinux. Попытка переключить режим с помощью setenforce 1 завершилась сообщением об ошибке, так как при отключённой системе SELinux изменение режима невозможно без перезагрузки.

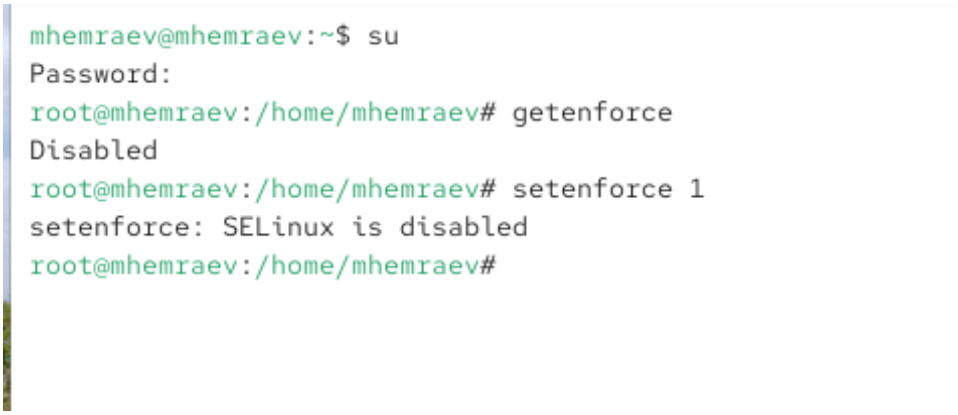


Рис. 2.3: Отключённый SELinux и реакция на setenforce 1

5. Для восстановления контроля доступа снова был отредактирован файл `/etc/sysconfig/selinux`, в котором установлено значение SELINUX=enforcing.

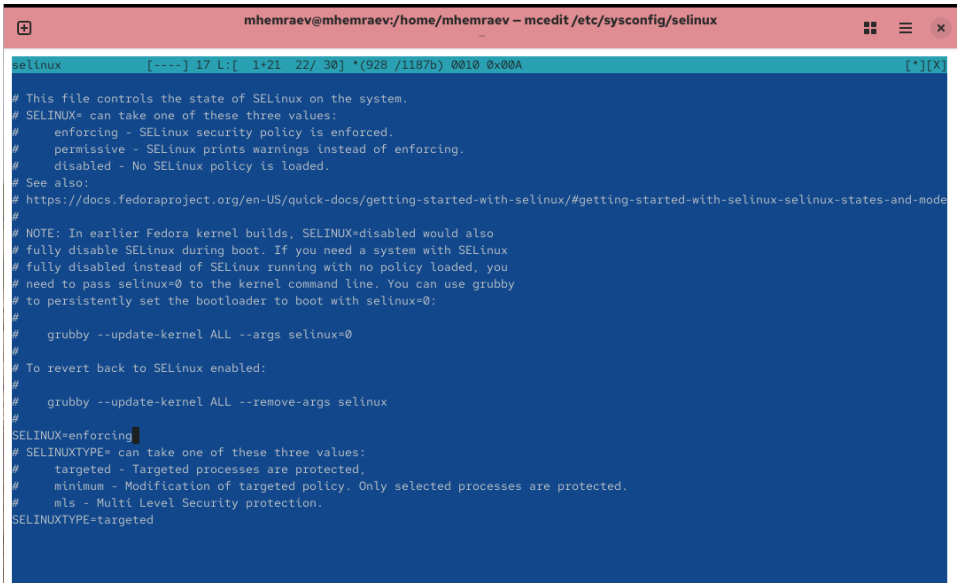


Рис. 2.4: Изменение конфигурации SELinux на enforcing

После очередной перезагрузки система выдала предупреждение о необходимости релабелинга (перемаркировки) контекстов SELinux. Этот процесс выполняется автоматически и может занять значительное время в зависимости от объёма данных.

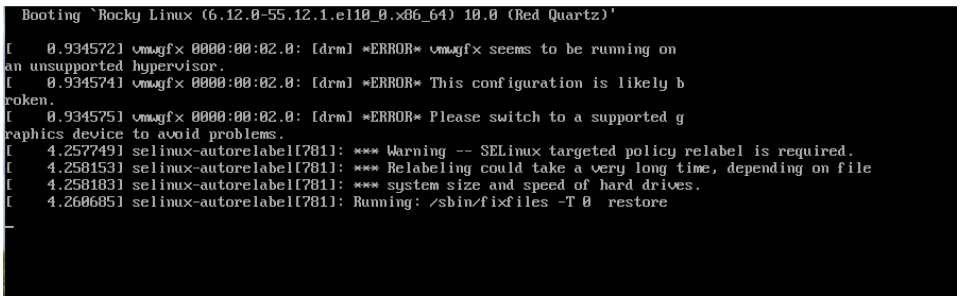


Рис. 2.5: Предупреждение о релабелинге при загрузке системы

6. После завершения загрузки и входа в систему проверка с помощью sestatus -v подтвердила, что SELinux снова работает в режиме **enforcing**, а система функционирует с активной политикой безопасности.

---

## 2.2 Использование restorecon для восстановления контекста безопасности

1. После получения прав администратора была выполнена проверка контекста файла `/etc/hosts`. Контекст определился как `system_u:object_r:net_conf_t:s0`.

2. Затем файл `/etc/hosts` был скопирован в домашний каталог пользователя. Новый файл получил контекст `unconfined_u:object_r:admin_home_t:s0`, поскольку копирование создаёт новый объект в домашнем каталоге.

3. Далее файл из домашнего каталога был перемещён обратно в `/etc`, что привело к сохранению контекста `admin_home_t`, не соответствующего системным стандартам.

4. Для исправления контекста была использована команда restorecon -v /etc/hosts. После выполнения тип контекста был возвращён к исходному значению `net_conf_t`, что соответствует корректной политике безопасности SELinux.

```
mhemraev@mhemraev:~$ su
Password:
root@mhemraev:/home/mhemraev#
root@mhemraev:/home/mhemraev# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@mhemraev:/home/mhemraev# cp /etc/hosts ~/
root@mhemraev:/home/mhemraev# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@mhemraev:/home/mhemraev# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@mhemraev:/home/mhemraev# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@mhemraev:/home/mhemraev# touch /.autorelabel
root@mhemraev:/home/mhemraev#
```

Рис. 2.6: Восстановление контекста безопасности файла /etc/hosts

5. Для глобального восстановления контекстов безопасности на файловой системе была создана специальная метка /.autorelabel. После перезагрузки система автоматически начала процесс полной перемаркировки файлов, что видно по сообщениям во время загрузки.

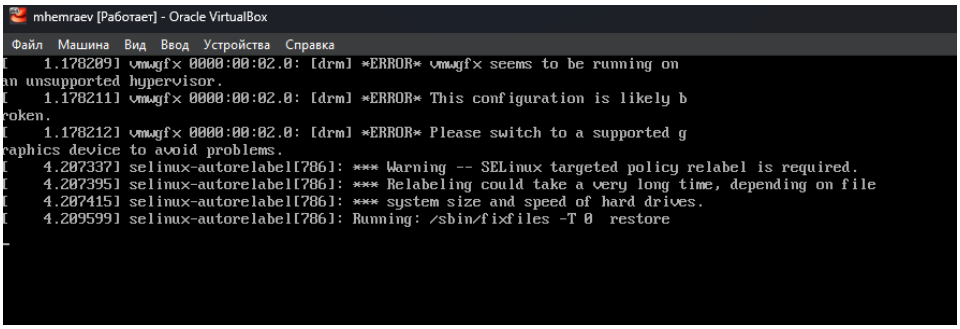


Рис. 2.7: Автоматическая перемаркировка контекстов при загрузке системы

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

1. После получения прав администратора было установлено необходимое программное обеспечение — веб-сервер Apache (**httpd**) и текстовый браузер **lynx**.

2. Для хранения контента веб-сервера был создан новый каталог **/web**, внутри которого создан файл **index.html** с содержимым «Welcome to my web server».

3. В конфигурационном файле `/etc/httpd/conf/httpd.conf` была закомментирована стандартная строка
   `DocumentRoot "/var/www/html"`
   и добавлено новое значение
   `DocumentRoot "/web"`.

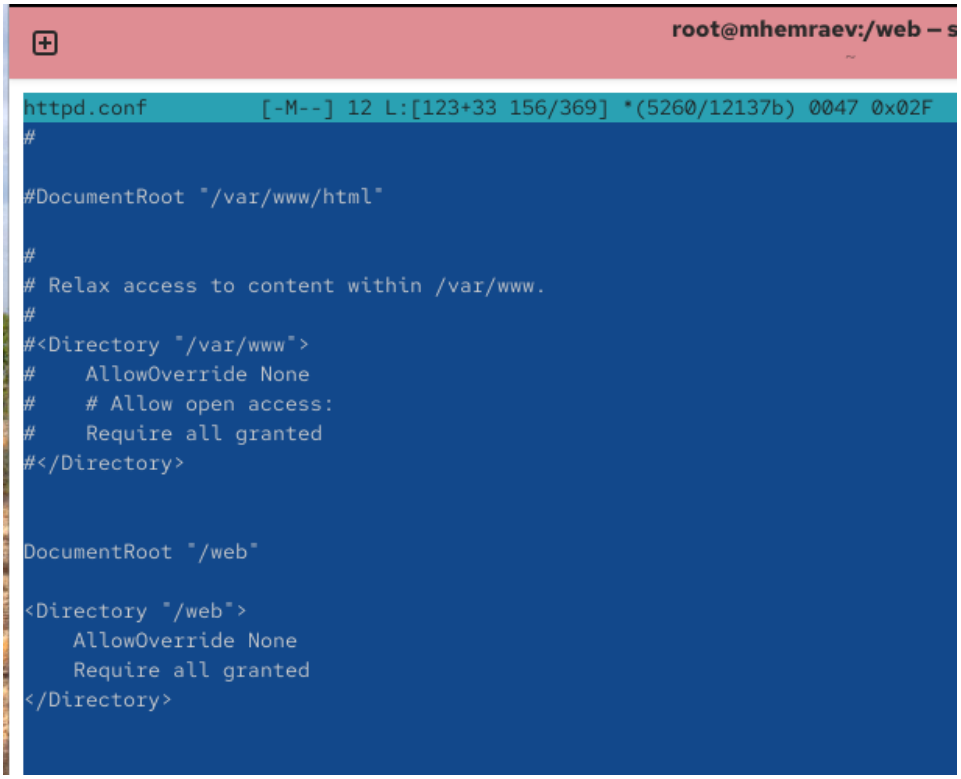


Рис. 2.8: Изменение параметров конфигурации Apache

4. После сохранения изменений веб-сервер был запущен и добавлен в автозагрузку. Проверка в браузере **lynx** при обращении к адресу `http://localhost` показала стандартную тестовую страницу **Rocky Linux**, что свидетельствует о том, что SELinux блокирует доступ Apache к новому каталогу.

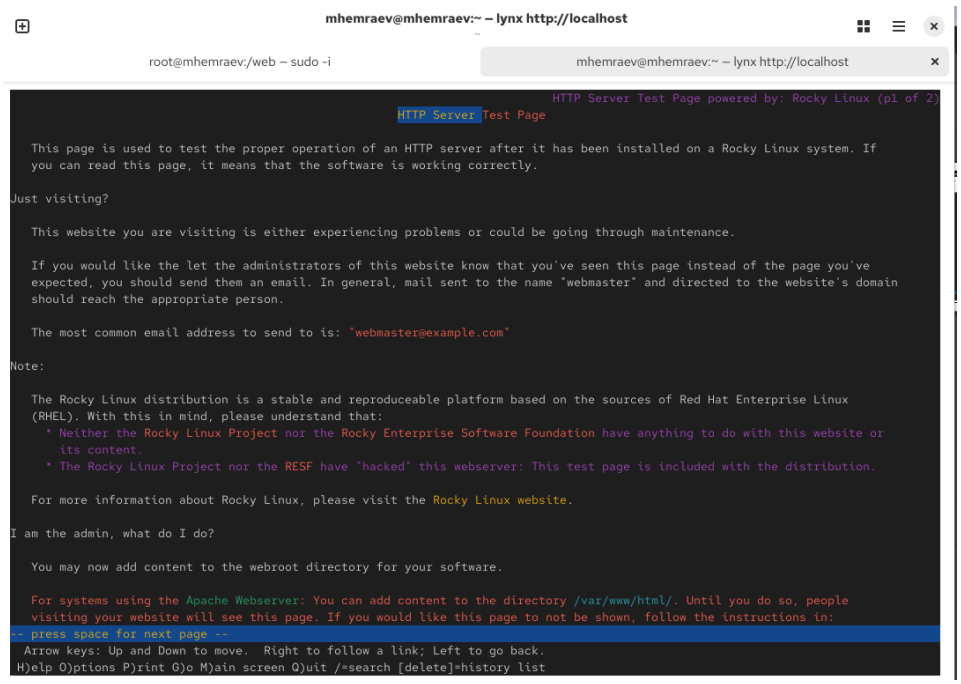


Рис. 2.9: Тестовая страница Apache по умолчанию

5. Для разрешения доступа веб-сервера к каталогу **/web** был создан новый контекст безопасности. С помощью команды semanage fcontext к каталогу и его содержимому была применена метка типа **httpd_sys_content_t**, предназначенная для статических веб-файлов.

6. Затем была выполнена команда restorecon для восстановления контекста безопасности в соответствии с новой политикой. В результате файлы в каталоге **/web** получили корректные метки безопасности.

```
root@mhemraev:~# mkdir /web
root@mhemraev:~# cd /web
root@mhemraev:/web# touch index.html
root@mhemraev:/web# echo "Welcome to my web server" > index.html
root@mhemraev:/web# mcedit /etc/httpd/conf/httpd.conf

root@mhemraev:/web#
root@mhemraev:/web# systemctl start httpd
root@mhemraev:/web# systemctl enable httpd
root@mhemraev:/web#
root@mhemraev:/web# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@mhemraev:/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@mhemraev:/web# systemctl restart httpd
root@mhemraev:/web#
```

Рис. 2.10: Применение контекста безопасности к каталогу /web

7. После перезапуска службы **httpd** повторный запрос через **lynx** к `http://localhost` показал пользовательскую веб-страницу с сообщением «Welcome to my web server». Это подтвердило, что доступ настроен корректно, а SELinux больше не блокирует обращение Apache к пользовательскому каталогу.

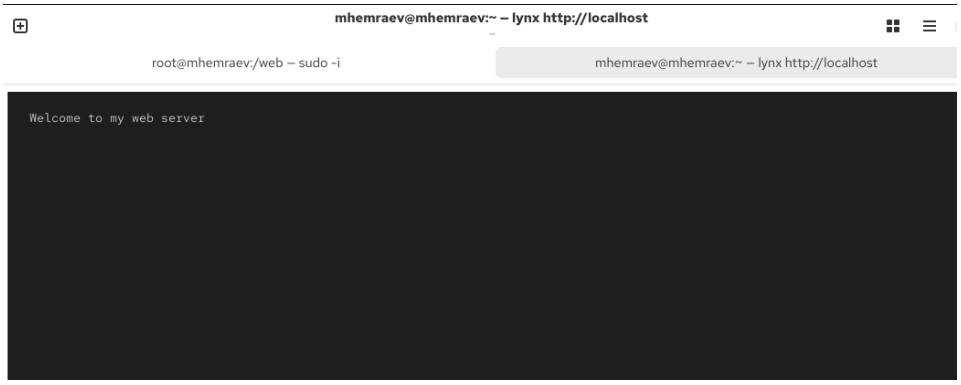


Рис. 2.11: Отображение пользовательской веб-страницы

---

## 2.4 Работа с переключателями SELinux

1. После получения прав администратора был просмотрен список переключателей SELinux, связанных с протоколом FTP. Среди них параметр **ftpd_anon_write** имел значение *off*, что означает запрет на запись для анонимных пользователей.

2. Для службы **ftpd_anon** был запрошен список доступных переключателей с их описанием, после чего выполнено изменение значения переключателя **ftpd_anon_write** на *on* с помощью команды setsebool.

3. Повторная проверка показала, что временное значение переключателя изменилось на *on*, однако постоянная настройка оставалась прежней (*off*).

4. Для сохранения изменения в постоянной конфигурации был применён параметр **-P**, что позволило активировать запись для анонимных пользователей FTP на постоянной основе.

5. Финальная проверка с помощью команды semanage boolean подтвердила, что параметр **ftpd_anon_write** теперь имеет состояние **(on , on)** — то есть включён как во временной, так и в постоянной конфигурации SELinux.


Рис. 2.12: Настройка переключателей SELinux для FTP

# 3 Контрольные вопросы

### 3.0.1 1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

- Для временного перевода SELinux в разрешающий режим используется команда:
  `setenforce 0`
  Она изменяет текущий режим на **Permissive** до следующей перезагрузки системы.

---

### 3.0.2 2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

- Для просмотра полного списка переключателей SELinux применяется команда:
  `getsebool -a`
  Она отображает все доступные булевы параметры (boolean values) и их текущее состояние (*on* или *off*).

---

### 3.0.3 3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

- Необходим пакет: **setroubleshoot**
  Он обеспечивает расшифровку и удобное представление сообщений SELinux, поступающих в системный журнал.

---

### 3.0.4 4. Какие команды вам нужно выполнить, чтобы применить тип контекста httpd_sys_content_t к каталогу /web?

- Необходимо выполнить две команды:

  1. `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` — добавляет новое правило для каталога /web и его содержимого.

  2. `restorecon -R -v /web` — применяет изменения и обновляет контексты безопасности для всех файлов в каталоге.

---

### 3.0.5 5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

- Нужно отредактировать файл конфигурации:
  `/etc/sysconfig/selinux`
  В нём следует установить параметр `SELINUX=disabled`, после чего требуется перезагрузка системы.

---

### 3.0.6 6. Где SELinux регистрирует все свои сообщения?

- Сообщения SELinux сохраняются в журнале аудита:
  `/var/log/audit/audit.log`
  При отсутствии этого файла информация может дублироваться в `/var/log/messages`.

---

### 3.0.7 7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

- Для получения информации о контекстах, связанных с FTP-службой, используется команда:
  `semanage fcontext -l | grep ftp`
  Она выводит список всех определённых контекстов, связанных с файлами и каталогами службы FTP.

---

### 3.0.8 8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

- Самый простой способ — временно перевести SELinux в **Permissive**-режим:
  `setenforce 0`
  Если после этого сервис начнёт работать корректно, значит, проблема была вызвана политиками SELinux.

---

# 4 Заключение

В ходе работы были изучены принципы функционирования SELinux, отработаны практические навыки изменения режимов его работы, настройки контекстов безопасности и управления переключателями для обеспечения корректного и безопасного функционирования системных служб.