

# Система управления контролем доступа SELinux

# Политика безопасности

**Политика безопасности** – это набор правил, определяющих методы обработки, защиты и распространения информации.

Политика безопасности должна быть **полной, непротиворечивой, рассматривать все возможности доступа** субъектов системы к её объектам.

Политика безопасности включает в себя

- 1) технические аспекты**
- 2) организационные аспекты**
- 3) правовые аспекты.**

# Модели управления доступом

## 1) Дискриционная модель управления доступом -

Объекту ставится в соответствие владелец и группа владельца, для которых задаются права.

2) **Расширение модели дискриционного доступа** - списки доступа (Assess Control Lists, ACL, расширенные атрибуты, внеядерные атрибуты )

## 3) Мандатная модель доступа -

Объектам и субъектам системы ставится в соответствие метка безопасности или мандат. При доступе метки безопасности сравниваются.

# Определения

**Идентификация** — процедура, в результате выполнения которой для субъекта выявляется его уникальный признак (идентификатор), однозначно определяющий его в информационной системе

**Аутентификация** (право на вход) — процедура проверки подлинности, например, проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных

**Авторизация** — предоставление определенному лицу прав на выполнение определенных действий. Авторизация может быть:

- 1) статической — доступ решается один раз;
- 2) динамической — доступ разрешается на время обращения к объекту.



# Авторизация

В UNIX- и Linux-системах используется **субъект-субъектная модель доступа и статическая авторизация**. К понятию «права доступа к объектам файловой системы» можно отнести **владение объектом и режим доступа**.

Любой объект файловой системы обязательно должен иметь владельца, **при создании файла владельцем назначается тот, кто создал файл**.

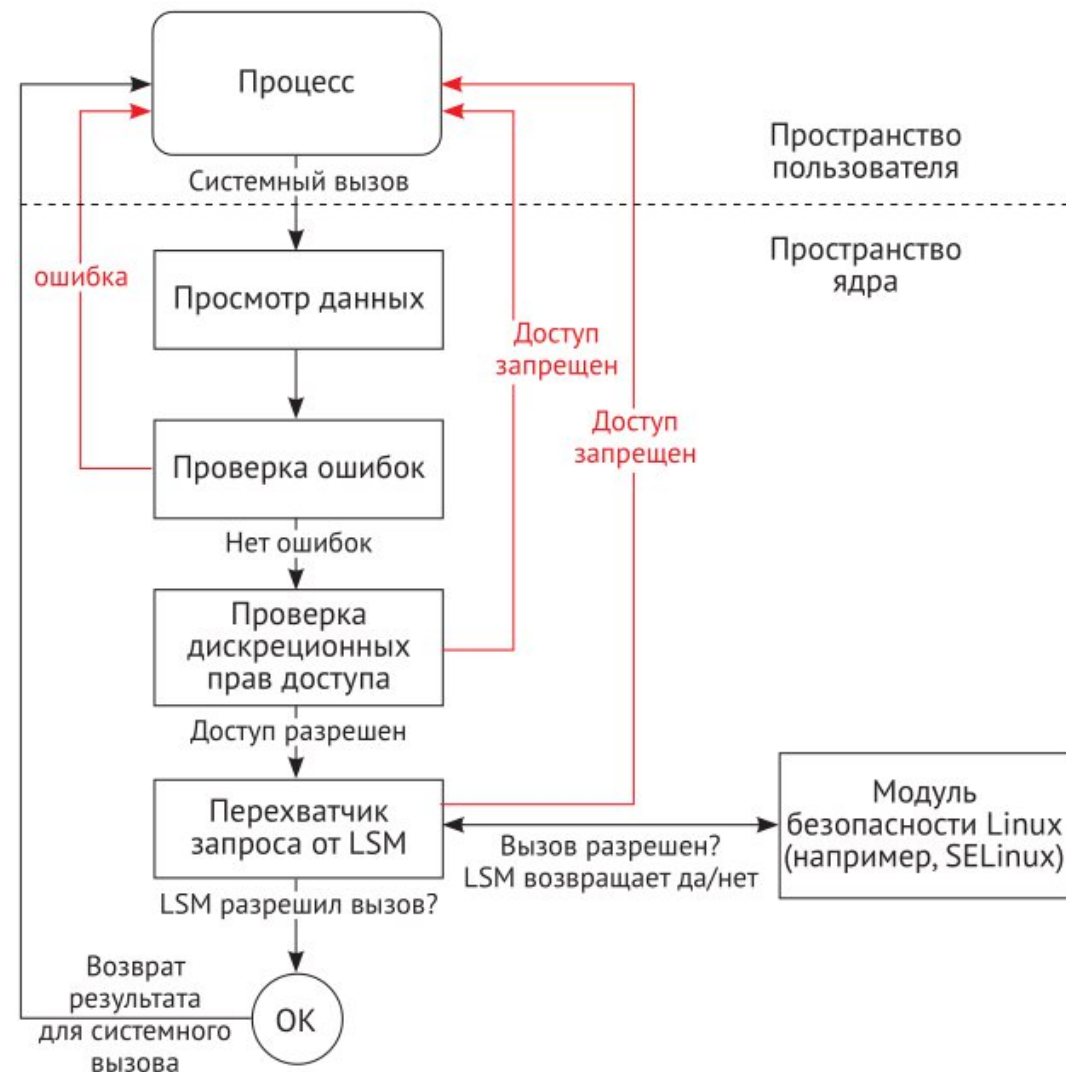
Основные элементы:

- действительный **субъект: процесс**
- номинальный **субъект: пользователь и группа**
- **объект: файл**

Основные принципы данного подхода реализованы в парадигме «**пользователи-группы-права доступа**».

# SELinux (Security Enhanced Linux)

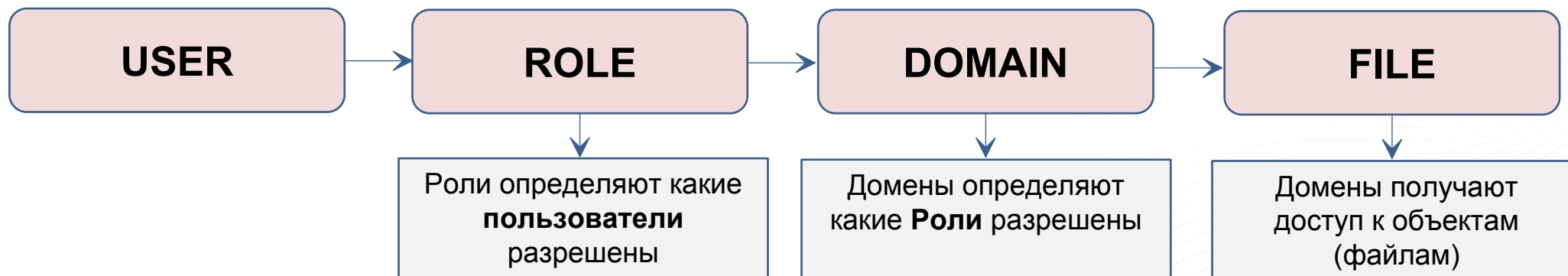
SELinux — реализация системы принудительного контроля доступа.



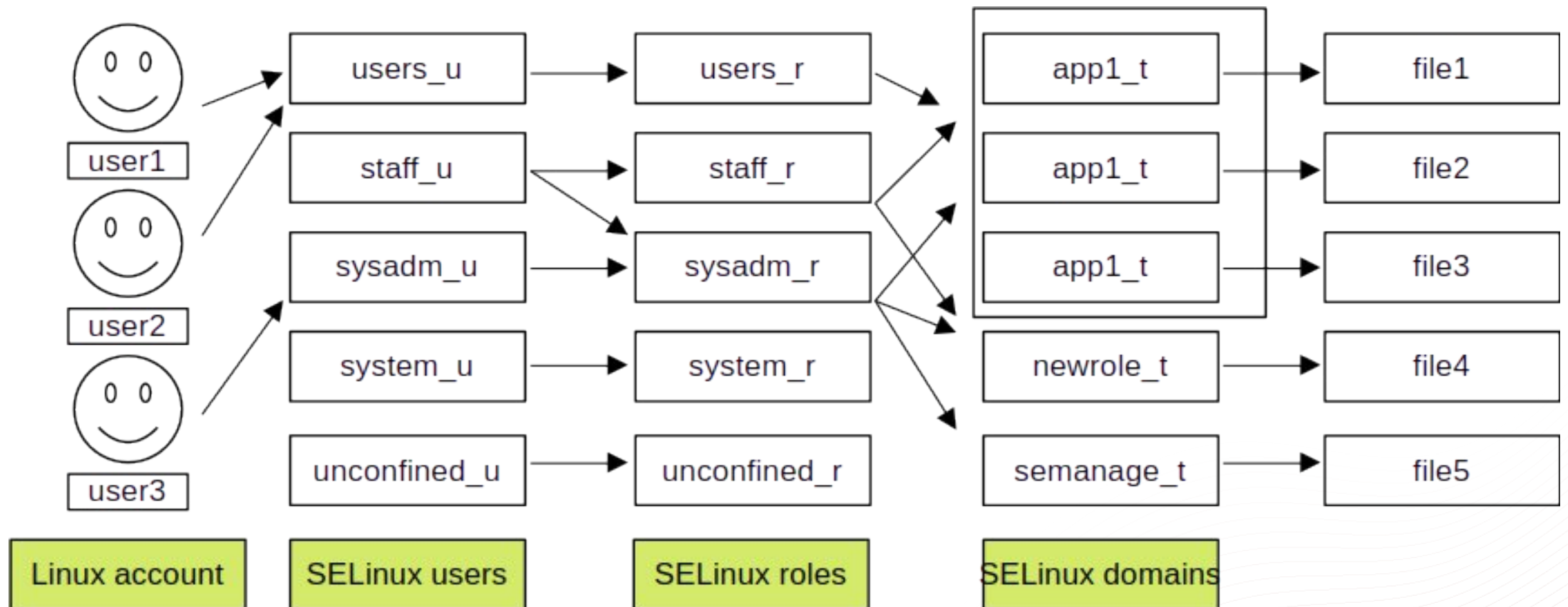
# SELinux (Security Enhanced Linux)

- **Домен** — это некоторый набор действий **процесса**.
- **Роль** — это совокупность нескольких доменов.
- **Тип** — набор действий, которые допустимы по отношению к **каталогам и файлам**.
- **Контекст безопасности** — это совокупность всех атрибутов.
- **Политика безопасности** — это набор правил, который регулирует ролеи, домены.

**Принцип** — процесс (субъект) и файл(объект), должны находиться в одном домене/типе.



# SELinux (Security Enhanced Linux)



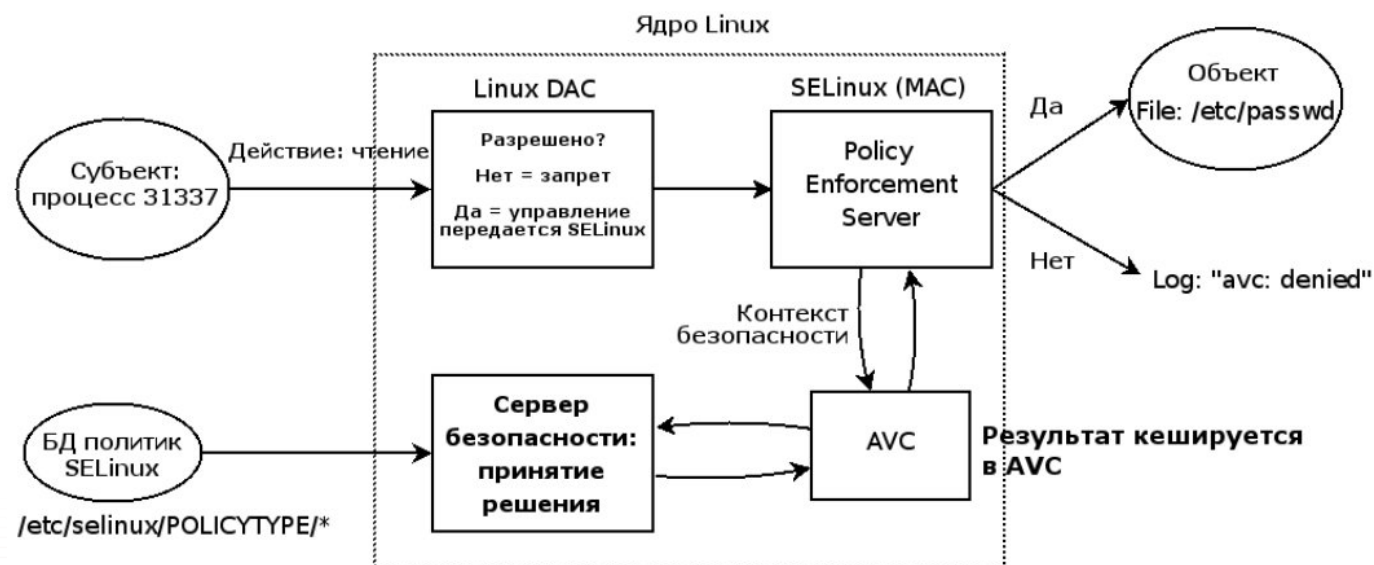
# Модели управления доступом SELinux

Политики, которые можно применить

**selinux-policy-minimum** — устанавливает ТОЛЬКО базовый пакет политики и неограниченный.pp

**selinux-policy-mls** — эталонный вариант политики SE Linux с поддержкой MLS. Он позволяет назначать на данные метки типа "Совершенно секретно"

**selinux-policy-targeted** — всем всё разрешено, за исключением процессов, для которых правила явно заданы



# SELinux (Security Enhanced Linux)

Контекст безопасности можно посмотреть в командах, используя ключ **Z**

**<сущность>:<роль>:<домен/тип>:<уровень:категория>**

**<сущность> или тип пользователя** — это субъект ( процесс или программа).

**<роль>** — список разрешенных операций. Роли необъединяются.

**<домен/тип>** — набор минимальных действий, необходимый для выполнения операции. «**Домен**» применяется к **процессам**, «**Тип**» — к **файлам и папкам**.

**<уровень:категория>** — в стандартных политиках не применяется (только в MLS).

```
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
system_u:object_r:fusefs_t:s0
```

```
system_u:system_r:systemd_userdbd_t:s0
```



# SELinux (Security Enhanced Linux)

## Причины отказа доступа от SELinux:

- Неправильно маркированный файл.
- Процесс работает в неправильном контексте.
- Ошибка в политике.
- Попытка вторжения.

Файл конфигурации **/etc/selinux/config**

**SELINUX=permissive**  
**SELINUXTYPE=targeted**

# SELinux (Security Enhanced Linux)

Эта утилита используется для получения состояния системы, в которой работает SELinux. Проверить включен ли SELinux можно командой

**sestatus**

```
SELinux статус:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux корневой каталог:      /etc/selinux
Загруженное имя политики:      targeted
Текущий режим:                 enforcing
Режим из файла конфигурации:   enforcing
Состояние политики MLS:       enabled
Policy deny_unknown status:    allowed
Проверка защиты памяти:        actual (secure)
Максимальная версия политики ядра: 33
```



# Режимы работы SELinux

Посмотреть статус **getenforce**. Установить временный статус **setenforce**

**Enforcing:** все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале. Это режим по умолчанию. (**setenforce 1**)

**Permissive:** информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы. (**setenforce 0**)

**Disabled:** Полное отключение системы принудительного контроля доступа.

# Контекст безопасности

**seinfo** – утилита получения информации о политике SELinux

Сканирует на известные параметры политику: **/sys/fs/selinux/policy**

Просмотр типов привязанных к роли

```
# seinfo -r unconfined_r -x
```

```
#seinfo --portcon=22
```

# Контекст безопасности

Просмотр действующих правил (boolean) SELinux:

**getsebool -a**

То же самое с кратким описанием правила:

**semanage boolean -l**

Просмотр известных SELinux портов

**semanage port -l**

Включение / отключение правила:

**setsebool <boolean> <value>**

где value — on, 1 или true для включения; off, 0 или false для выключения правила

# Ошибки доступа от SELinux

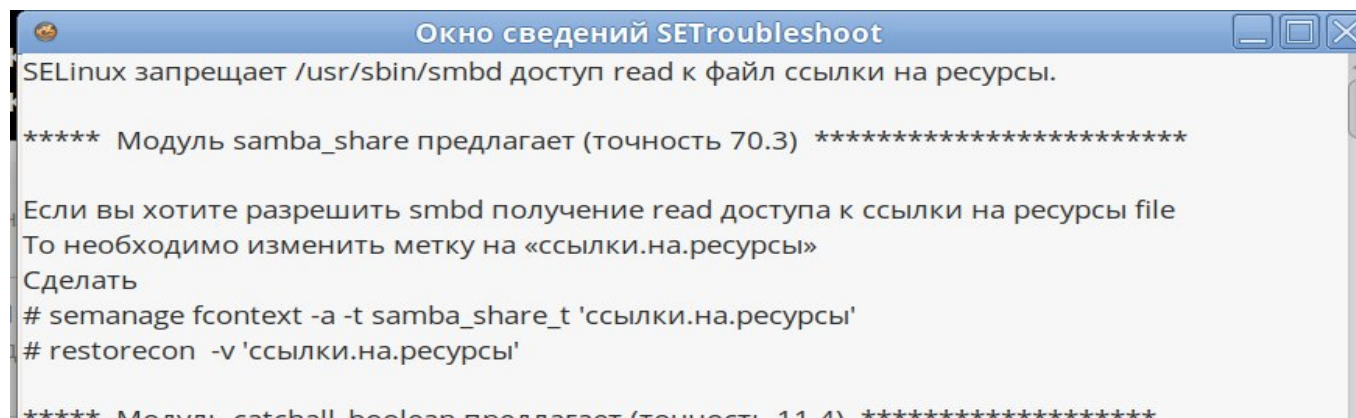
Подробный вывод информации об ошибках:

**sealert -a /var/log/audit/audit.log**

Подробный вывод информации об ошибках в графическом виде:

**sealert -b**

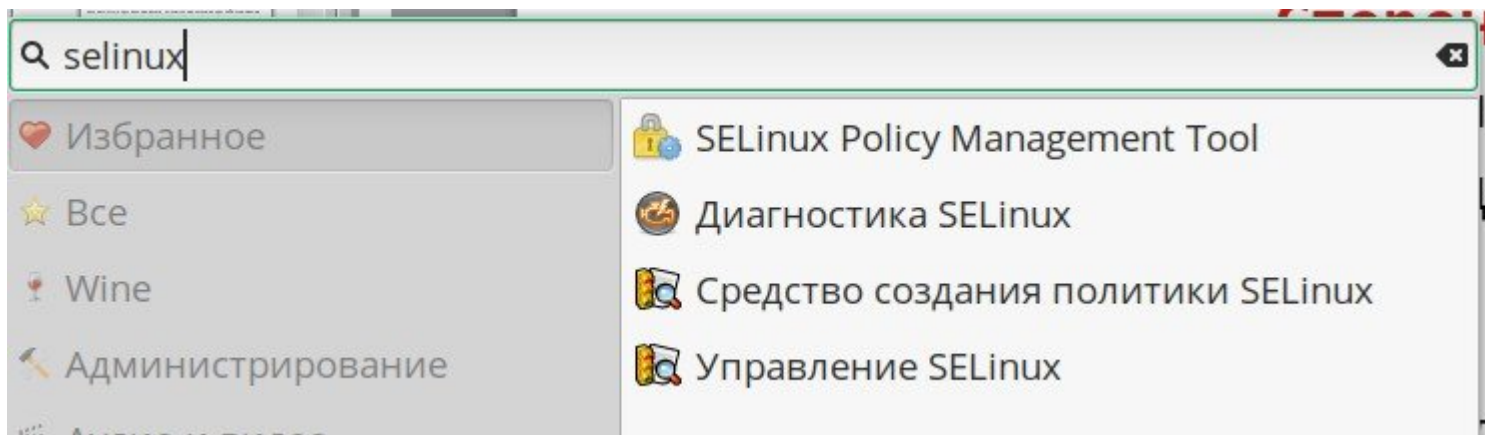
Предлагается решение – установить новый контекст и сбросить правила.



# Управление SELinux

В графической оболочке по умолчанию программы управления SeLinex

- Программа настройка конфигурации
- Диагностика SELinux
- Программа формирования политик SELinux
- Администрирование SELinux



# Управление SELinux

Кроме SELinux-пользователя `unconfined_u`, который по умолчанию присваивается всем пользователям системы, в целевой политике также описано несколько непривилегированных пользователей, которых можно использовать для создания гостевых учетных записей, процессы которых будут очень ограничены в правах (возможности и различия этих пользователей смотри в таблице "Пользователи по умолчанию SELinux"). Чтобы создать такого пользователя, достаточно выполнить следующую команду:

**`useradd -Z xguest_u имя_пользователя`**

Кроме этого можно сделать его пользователем по умолчанию, так что ограниченными будут все вновь созданные Linux-пользователи:

**`semanage login -m -S targeted -s "xguest_u" -r s0 __default__`**

Посмотреть список текущих SELinux-пользователей можно так:

**`# /usr/sbin/semanage login -l`**

# Управление SELinux

Скажи mv – нет! Во время установки дистрибутива все файлы получают определенный контекст безопасности, а все файлы, созданные в процессе работы, — контекст безопасности, определяемый правилами на основе родительского каталога (например, если создать файл внутри каталога /etc, его тип автоматически станет etc\_t, а для файлов каталога /var/www/html — httpd\_sys\_content\_t). Однако это работает только в отношении вновь созданных файлов. Во время перемещения файла с помощью mv его контекст сохраняется, что может привести к отказу в доступе (например, Apache не сможет получить доступ к файлу, если его тип не httpd\_sys\_content\_t).



**Спасибо за внимание!**

**[www.red-soft.ru](http://www.red-soft.ru)**  
**[redos@red-soft.ru](mailto:redos@red-soft.ru)**

