



0,00

Рейтинг

King Servers

Хостинг-провайдер «King Servers»



itNews 20 января 2014 в 12:51

SELinux – описание и особенности работы с

Блог компании King Servers



О SELinux на Хабре уже писали, однако, не так много опубликовано подробных мануалс публикуем именно такой, подробный мануал по SELinux, начиная от информации по сис политик.

Реклама

Для того, чтобы не превращать пост в «простыню», сложную для понимания, мы решили разделить мануал на две части. Первая будет рассказывать о самой системе, и некоторых ее особенностях. Вторая – о настройке политик. Сейчас публикуем первую часть, чуть позже будет опубликована и вторая часть.

1. Введение

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена.

1.1 Некоторые актуальные задачи.

Для того, чтобы понять, в чем состоит практическая ценность SELinux, рассмотрим несколько примеров, когда стандартная система контроля доступа недостаточна. Если SELinux отключен, то вам доступна только классическая дискреционная система контроля доступа, которая включает в себя DAC (избирательное управление доступом) или ACL(списки контроля доступа). То есть речь идет о манипулировании правами на запись, чтение и исполнение на уровне пользователей и групп пользователей, чего в некоторых случаях может быть совершенно недостаточно. Например:

— Администратор не может в полной мере контролировать действия пользователя. Например, пользователь вполне способен дать всем остальным пользователям права на чтение собственных конфиденциальных файлов, таких как ключи SSH.

— Процессы могут изменять настройки безопасности. Например, файлы, содержащие в себе почту пользователя должны быть доступны для чтения только одному конкретному пользователю, но почтовый клиент вполне может изменить права доступа так, что эти файлы будут доступны для чтения всем.

— Процессы наследуют права пользователя, который их запустил. Например, зараженная трояном версия браузера Firefox в состоянии читать SSH-ключи пользователя, хотя не имеет для того никаких оснований.

По сути, в традиционной модели избирательного управления доступом (DAC), хорошо реализованы только два уровня доступа — пользователь и суперпользователь. Нет простого метода, который позволил бы устанавливать для каждого пользователя необходимый минимум привилегий.

Конечно, есть множество методов обхода этих проблем в рамках классической модели безопасности, но ни один из них не является универсальным.

1.1.1 Основные термины, используемые в SELinux:

Домен — список действий, которые может выполнять процесс. Обычно в качестве домена определяется минимально-возможный набор действий, при помощи которых процесс способен функционировать. Таким образом, если процесс дискредитирован, злоумышленнику не удастся нанести большого вреда.

Роль — список доменов, которые могут быть применены. Если какого-то домена нет в списке доменов какой-то роли, то действия из этого домена не могут быть применены.

Тип — набор действий, которые допустимы по отношению к объекту. Тип отличается от домена тем, что он может применяться к пайпам, каталогам и файлам, в то время как домен применяется к процессам.

Контекст безопасности — все атрибуты SELinux — роли, типы и домены.

1.2 Решение проблем традиционной модели безопасности.

SELinux следует модели минимально необходимых привилегий для каждого сервиса, пользователя и программы намного более строго. По умолчанию установлен «запретительный режим», когда каждый элемент системы имеет только те права, которые жизненно необходимы ему для функционирования. Если же пользователь, программа или сервис пытаются изменить файл или получить доступ к ресурсу, который явно не необходим для решения их, то им будет просто отказано в доступе, а такая попытка будет зарегистрирована в журнале.



SELinux реализована на уровне ядра, так что прикладные приложения могут совсем ничего не знать о версии этой системы принудительного контроля доступа, особенностях её работы и т.д. В случае грамотной настройки, SELinux никак не повлияет на функционирование сторонних программ и сервисов. Хотя, если приложение способно перехватывать сообщения об ошибках этой системы контроля доступа, удобство пользования таки приложением существенно возрастает. Ведь в случае попытки доступа к защищенному ресурсу или файлу, SELinux передает в основное приложение ошибку из семейства «access denied». Но лишь немногие приложения используют получаемые от SELinux коды возврата системных вызовов.

Вот несколько примеров использования SELinux, которые позволяют увидеть, каким образом можно увеличить степень безопасности всей системы.

— Создание и настройка списка программ, которые могут читать ssh-ключи.

— Предотвращение несанкционированного доступа к данным через *mail*-клиент.

— Настройка браузера таким образом, чтобы он мог читать в домашней папке пользователя только необходимые для функционирования файлы и папки.

2. Режимы работы SELinux

SELinux имеет три основных режим работы, при этом по умолчанию установлен режим Enforcing. Это довольно жесткий режим, и в случае необходимости он может быть изменен на более удобный для конечного пользователя.

Enforcing: Режим по-умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: В случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Disabled: Полное отключение системы принудительного контроля доступа.

Вы можете посмотреть текущий режим и другие настройки SELinux (а в случае необходимости и изменить его) при помощи специального GUI-инструмента, доступного в меню «Администрирование» (`system-config-selinux`). Если же вы привыкли работать в консоли, то можете посмотреть текущий статус командой `sestatus`.

```
# sestatus
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:         enforcing
Policy version:                21
Policy from config file:       targeted
```

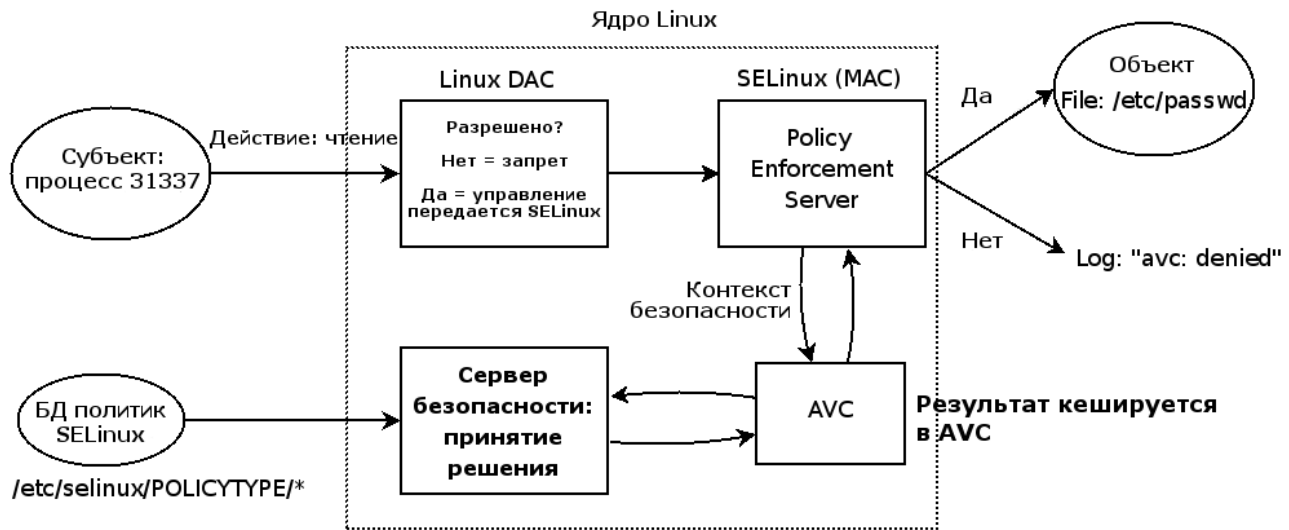
Также вы можете узнать статус SELinux при помощи команды `getenforce`.

Команда «`setenforce`» позволяет быстро переключаться между режимами Enforcing и Permissive, изменения вступают в силу без перезагрузки. Но если вы включаете или отключаете SELinux, требуется перезагрузка, ведь нужно заново устанавливать метки безопасности в файловой системе.

Для того, чтобы выбрать режим по-умолчанию, который будет применяться при каждой загрузке системы, задайте значение строки 'SELINUX=' в файле `/etc/selinux/config`, задав один из режимов — 'enforcing', 'permissive' или 'disabled'. Например: 'SELINUX=permissive'.

3. Политики SELinux

Как отмечалось ранее, SELinux по-умолчанию работает в режиме Enforcing, когда любые действия, кроме разрешенных, автоматически блокируются, каждая программа, пользователь или сервис обладают только теми привилегиями, которые необходимы им для функционирования, но не более того. Это довольно жесткая политика, которая обладает как плюсами — наибольший уровень информационной безопасности, так и минусами — конфигурирование системы в таком режиме сопряжено с большими трудозатратами системных администраторов, к тому же, велик риск того, что пользователи столкнутся с ограничением доступа, если захотят использовать систему хоть сколько-нибудь нетривиальным образом. Такой подход допустим в Enterprise-секторе, но неприемлем на компьютерах конечных пользователей. Многие администраторы просто отключают SELinux на рабочих станциях, чтобы не сталкиваться с подобными проблемами.



Для того, чтобы избежать этого, для ключевых приложений и сервисов, таких как, например, httpd, named, dhcpd, mysqld, определены заранее сконфигурированные целевые политики, которые не позволят злоумышленнику получить доступ к важным данным. Те же приложения, для которых политика не определена, выполняются в домене `unconfined_t` и не защищаются SELinux. Таким образом, правильно выбранные целевые политики позволяют добиться приемлемого уровня безопасности, не создав при этом для пользователя лишних проблем.

4. Контроль доступа в SELinux

SELinux предоставляет следующие модели управления доступом:

Type Enforcement (TE): основной механизм контроля доступа, используемый в целевых политиках. Позволяет детально, на самом низком уровне управлять разрешениями. Самый гибкий, но и самый трудоемкий для системного администратора механизм.

Role-Based Access Control (RBAC): в этой модели права доступа реализуются в качестве ролей. Ролью называется разрешения на выполнение определенных действий одним или несколькими элементами системы над другими частями системы. По-сути, RBAC является дальнейшим развитием TE.

Multi-Level Security (MLS): многоуровневая модель безопасности, в которой всем объектам системы присваивается определенный уровень доступа. Разрешение или запрет доступа определяется только соотношением этих уровней.

Все процессы и файлы в рамках SELinux имеют контекст безопасности.

Давайте посмотрим на контекст на практике, подробно рассмотрев стартовую страницу веб-сервера Apache, находящуюся по адресу `/var/www/html/index.html`

```
$ ls -Z /var/www/html/index.html
-rw-r--r--  username username system_u:object_r:httpd_sys_content_t /var/www/html/index.html
```

В дополнение к стандартным правам доступа к файлу, мы можем видеть контекст безопасности SELinux: `system_u: object_r: httpd_sys_content_t`.

Контекст базируется на `user:role:type:mls`, но поля `user:role:type` отображаются, в то время как поле `mls` скрыто. Также мы можем видеть целевую политику, в данном случае `httpd_sys_content_t`.

Теперь рассмотрим контекст безопасности SELinux для процесса 'httpd' (веб-сервер Apache):

```
$ ps axZ | grep httpd
system_u:system_r:httpd_t      3234 ?        Ss      0:00 /usr/sbin/httpd
```

Как мы видим, этот процесс запущен на домене `httpd_t`.

Ну а теперь давайте посмотрим на контекст безопасности файла в нашем домашнем каталоге:

```
$ ls -Z /home/username/myfile.txt
-rw-r--r--  username username user_u:object_r:user_home_t  /home/username/myfile.txt
```

Мы видим, что файл имеет тип `user_home_t`, этот тип присваивается по умолчанию всем файлам в домашнем каталоге. Доступ разрешен только между элементами с одинаковым типом, именно поэтому веб-сервер Apache может без проблем читать файл `/var/www/html/index.html`, который имеет тип `httpd_sys_content_t`. В то же самое время, так как Apache запущен на домене `httpd_t` и не имеет заполненных полей `userid:username`, он не может получить доступ к файлу `home/username/myfile.txt`, хотя этот файл доступен для чтения процессам, для которых не определена целевая политика. Таким образом, если веб-сервер Apache будет взломан, то злоумышленник не сможет получить доступ к файлам или запускать процессы, которые не находятся в домене `httpd_t`.

5. Устранение проблем SELinux

Рано или поздно происходит ситуация, когда вы сталкиваетесь с ситуацией, когда SELinux запрещает вам доступ к чему-то. Есть несколько основных причин отказа доступа:

- Неправильно маркированный файл.
- Процесс работает в неправильном контексте
- Ошибка в политике. Процесс требует доступ к файлу, который не был учтен при создании политики.
- Попытка вторжения.

Первые три причины отказа доступа разрешаются достаточно легко, в то время как во время попытки вторжения звучит сигнал тревоги и пользователю посылается соответствующее уведомление.

Для того, чтобы разобраться с любой проблемой, достаточно просмотреть журнал SELinux. По умолчанию он записывается процессом `auditd` в файл `/var/log/audit/audit.log`. Если этот процесс не запущен, то SELinux ведет журнал в файле `/var/log/messages`, в этом случае все сообщения системы контроля доступа маркируются ключом `AVC`, что позволяет быстро отфильтровать нужные строки, например, при помощи команды `grep`.

В последние версии дистрибутивов (начиная с CentOS 5), включена утилита с графическим интерфейсом пользователя, которая позволяет отображать журнал SELinux в удобном и понятном для пользователя виде. Вызвать её можно из консоли, набрав `sealert -b`. Утилита входит в состав пакета `setroubleshoot`. В том случае, если X-сервер не запущен, вы можете сгенерировать понятные и удобные для человека отчеты следующей командой:

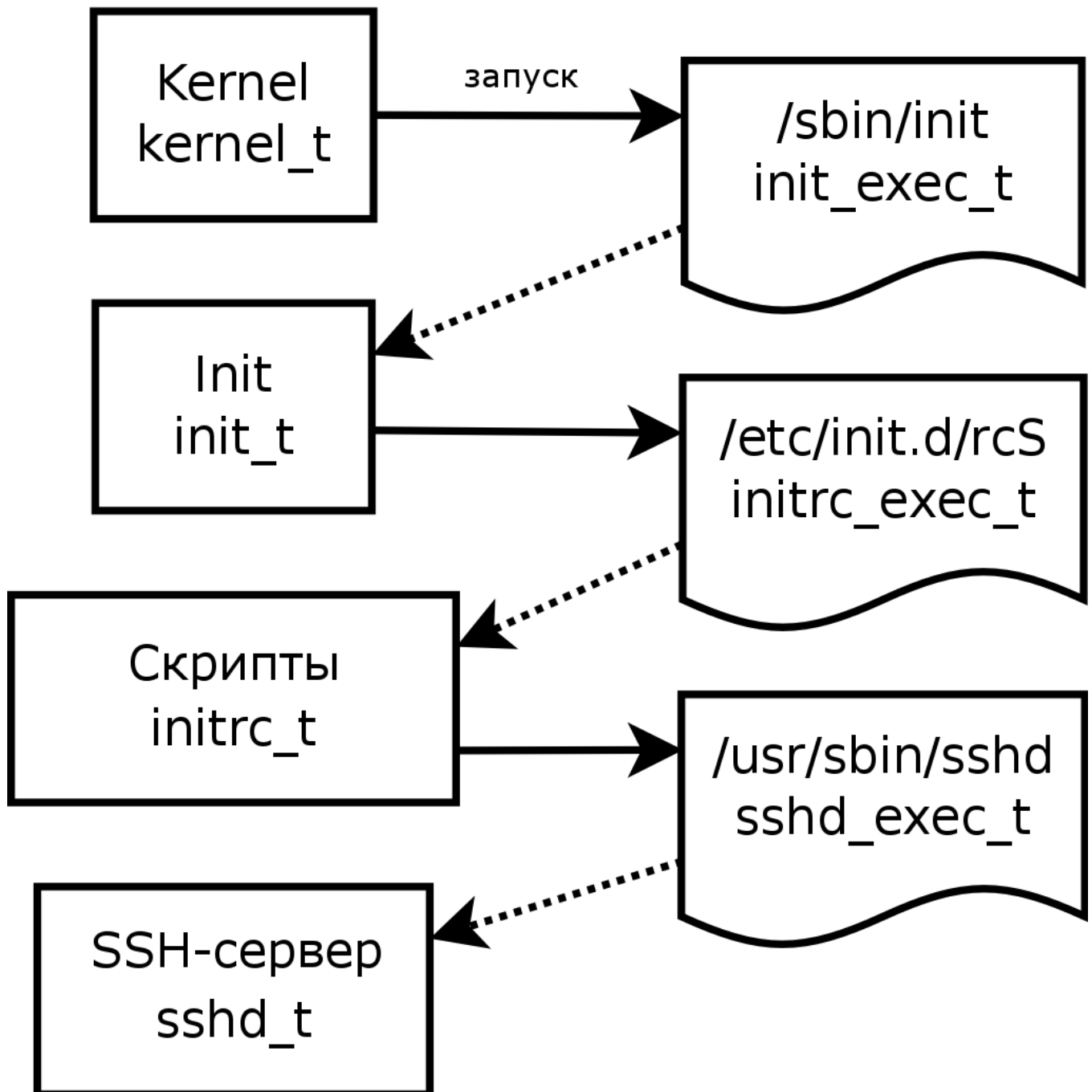
```
sealert -a /var/log/audit/audit.log > /path/to/mylogfile.txt
```

5.1 Изменение меток контекста безопасности файлов.

Команда «`chcon`» позволяет изменять контекст SELinux для файлов или каталогов точно таким же образом, как команды «`chown`» и «`chmod`» позволяют менять владельца файла или права доступа к нему в рамках стандартной системы контроля доступа.

Процессы и домены

Объекты и типы



Рассмотрим несколько примеров.

Предположим, что в системе установлен веб-сервер Apache и нам необходимо изменить папку, в которой хранятся сайты (по умолчанию это /var/www/html/) на, допустим, /html/ и создать в этом каталоге файл index.html.

```
# mkdir /html
# touch /html/index.html
# ls -Z /html/index.html
-rw-r--r--  root root user_u:object_r:default_t      /html/index.html
# ls -Z | grep html
drwxr-xr-x  root root user_u:object_r:default_t      html
```

Выше мы видим, что и каталог /html, и файл /html/index.html в рамках контекста безопасности имеют тип default_t. Это означает, что если мы запустим Apache и попробуем начать работать с этим каталогом или файлом, то SELinux откажет нам в доступе. И

это будет абсолютно правильно, ведь правильный контекст безопасности для файлов, взаимодействующих с Apache, это `httpd_sys_content_t`.

Изменим контекст и проверим правильно ли все сделано:

```
# chcon -v --type=httpd_sys_content_t /html
context of /html changed to user_u:object_r:httpd_sys_content_t
# chcon -v --type=httpd_sys_content_t /html/index.html
context of /html/index.html changed to user_u:object_r:httpd_sys_content_t
# ls -Z /html/index.html
-rw-r--r--  root root user_u:object_r:httpd_sys_content_t    /html/index.html
# ls -Z | grep html
drwxr-xr-x  root root user_u:object_r:httpd_sys_content_t    html
```

Не обязательно вручную обрабатывать каждый файл и каждый каталог, можно просто воспользоваться опцией рекурсивного обхода каталога `-R`:

```
# chcon -Rv --type=httpd_sys_content_t /html
```

Подобные изменения контекста безопасности будут сохраняться между перезагрузками, однако, при изменении меток файловых систем, изменения пропадут. В процессе обслуживания и эксплуатации, подобное не редкость. Правильным решением в такой ситуации будет (после тестирования, конечно) создать дополнительное правило, после чего объединить его с местными локальными правилами. Таким образом, оно будет иметь более высокий приоритет, чем базовые правила.

Для того, чтобы SELinux корректно работал даже после изменения меток файловых систем, мы можем использовать как инструменты для управления SELinux с GUI-интерфейсом, так и консольную утилиту `semanage`:

```
semanage fcontext -a -t httpd_sys_content_t "/html(/.*)?"
```

В примере выше мы присвоили контекст `httpd_sys_content_t` всем файлам, находящимся в каталоге `/html`.

5.2 Восстановление контекста безопасности SELinux.

Команда «`restorecon`» позволяет изменить контекст безопасности на тот, который был присвоен по-умолчанию.

Снова используем в качестве примера веб-сервер Apache. Предположим, что пользователь отредактировал в своем домашнем каталоге копию файла `index.html` и переместил (командой `mv`) его в каталог, в котором хранятся сайты (`/var/www/html`).

Следует обратить внимание, что при копировании (команда `cp`) контекст безопасности файла будет совпадать с контекстом каталога назначения, при перемещении же, контекст безопасности будет совпадать с контекстом источника. Конечно, мы могли бы использовать команду `chcon` для изменения контекста безопасности, но так как перемещенные файлы находятся сейчас в каталоге `/var/www/html`, мы можем просто восстановить параметры контекста для всех файлов, находящихся в этом каталоге.

Для того, чтобы восстановить контекст только для файла `index.html`, мы можем применить команду:

```
# restorecon -v /var/www/html/index.html
```

Если же мы хотим рекурсивно обойти весь каталог и изменить контекст для всех содержащихся в нем файлов, используем следующую команду:

```
# restorecon -Rv /var/www/html
```


5.3 Изменение меток для всей файловой системы.

Иногда бывает необходимо заново устанавливать метки безопасности во всей файловой системе. Чаще всего такую операцию производят при повторном включении SELinux, после того, как система была на некоторое время отключена. Также это бывает нужно, если мы меняем тип управления политиками на strict (в этом случае все процессы работают в своих специальных доменах, в домене unconfined_t не может работать никто).

Для того, чтобы автоматически переразметить файловую систему при следующей перезагрузке, введите следующие команды:

```
# touch /.autorelabel  
# reboot
```

Иногда автоматическая переразметка не срабатывает (чаще всего в тех случаях, когда дистрибутив с выключенной системой SELinux был обновлен). В таком случае воспользуйтесь следующей командой:

```
# genhomedircon  
# touch /.autorelabel  
# reboot
```

5.4 Предоставление доступа к портам.

Нередко мы хотим, чтобы сервисы, подобные Apache, имели возможность прослушивать нестандартные порты и принимать на них входящие соединения. Базовые политики SELinux позволяют получить доступ только к заранее предопределенным портам, которые жестко связаны с тем или иным сервисом. Допустим, мы хотим, чтобы Apache прослушивал 81 порт. В таком случае, нам надо добавить правило при помощи команды semanage:

```
# semanage port -a -t http_port_t -p tcp 81
```

Полный список портов, к которым SELinux предоставляет доступ, можно просмотреть следующим образом:

```
# semanage port -l
```

В следующей, второй части мануала, мы покажем возможность гибкой настройки политик системы.

Теги: selinux, мануалы

Хабы: Блог компании King Servers

↑ +72 ↓ 689 169k 13 Поделиться



@itNews

Сетевые технологии и оборудование, гаджеты



King Servers

Хостинг-провайдер «King Servers»

ПОХОЖИЕ ПУБЛИКАЦИИ

22 января 2014 в 16:10

SELinux — описание и особенности работы с системой. Часть 2

↑ +43

👁 33,5k

🔖 355







💬 7

Реклама




Комментарии 13

 **versofate**  20 января 2014 в 14:38   ↑ +4 ↓

Варнинг: селинух писан АНБ.
И в догонку статья: stopdisablinglinux.com/

 **versofate**  20 января 2014 в 15:48     ↑ +1 ↓


Забыл теги «sarcasm» — отхватил минусов. По ссылке, кстати, тоже неплохое введение в selinux с редхатовской конференции.

 **onix74** 20 января 2014 в 15:25   ↑ +3 ↓




Наверное, первая статья, после прочтения которой, первая мысль была не «Ну, на фиг! Это всё сложно!», а «Да блин, всё разумно и не так уж страшно!».
Спасибо! Жду продолжение.

 **stoplinux** 20 января 2014 в 15:54   ↑ 0 ↓




Не дискретная, а дискреционная

 **KingServers** 20 января 2014 в 15:58     ↑ +1 ↓

Сейчас поправим

 **Wintch** 20 января 2014 в 19:25   ↑ +2 ↓

«когда любые действия кроме запрещенных автоматически блокируются»
Спасибо большое за статью!

 **dsx** 20 января 2014 в 22:42   ↑ +6 ↓

Продолжение статьи (для тех, кому лень ждать, когда автор напишет продолжение статьи): <file:///usr/share/doc/debian-handbook/html/sect.selinux.html>

 **iaf** 21 января 2014 в 00:41   ↑ +2 ↓

MLS... Разрешение или запрет доступа определяется только соотношением этих уровней.

Это далеко не так — см. [mlsconstraints](#).

Еще несколько примеров, на мой взгляд, логических несоответствий:

Рано или поздно происходит ситуация, когда вы сталкиваетесь с ситуацией, когда SELinux запрещает **вам** доступ к чему-то. Есть несколько основных причин отказа [вам] доступа:

...

— Попытка вторжения.

SELinux имеет **три** основных *режима работы*...

Disabled: Полное отключение...

Также мы можем видеть **целевую политику**, в данном случае **httpd_sys_content_t**.

Мне казалось, что *подробный мануал* предполагает ответ на вопросы «почему?» и «как?», например: «почему поле mls скрыто?».

Или: согласно статье, в чем отличие init_t от init_exec_t?

Или: почему совет с genhomedircon не восстанавливает контекст /var/www/index2.html?

И т.п.

Как сказал бы Эрик Картман, you're breaking mah balls, man, you're breaking mah' balls.

Ложка мегаконструктива: если уж вы действительно решились на описание «гибкой настройки» политик, то попробуйте базироваться на CIL. Это сейчас hot topic в среде разработчиков SELinux, и он будет следующим форматом описания/настройки взамен текущего.



xave 21 января 2014 в 11:01



0



SeLinux вещь нужная и замечательная, но после каждого обновления этого пакета в системе (Fedora), все правила, заданные через setsebool -P, обнуляются. Очень сильно раздражает.



foboss 21 января 2014 в 12:00



0



Можно оформить свои правила в модуле и подключить его через «semodule -i»

НЛО прилетело и опубликовало эту надпись здесь



grossws 21 января 2014 в 12:47



0



Была на хабре неплохая статья: habrahabr.ru/post/199202/. Она, правда, с упором на MLS, но также там есть полезные сведения, как диагностировать, отлаживать и исправлять политики.

НЛО прилетело и опубликовало эту надпись здесь

Только полноправные пользователи могут оставлять комментарии. Войдите, пожалуйста.

САМОЕ ЧИТАЕМОЕ

Сутки

Неделя

Месяц

SARS нерукотворный? Генеалогия уханьского коронавируса

↑ +260

👁 86k

🔖 203

💬 333

Вы не хотите усиливать иммунитет. Или крайности организма человеческого

↑ +50

👁 23,6k

🔖 74

💬 28

Как Amazon пытается заставить людей покупать... меньше

+29

18,5k

14

23

Современный самолёт by design защищён от биологической угрозы (COVID-19) лучше, чем вы думаете

+56

14,6k

35

64

На картах Ростова, Санкт-Петербурга и других городов России начались виртуальные митинги

+26

13k

8

41

Ваш аккаунт	Разделы	Информация	Услуги
Войти	Публикации	Устройство сайта	Реклама
Регистрация	Новости	Для авторов	Тарифы
	Хабы	Для компаний	Контент
	Компании	Документы	Семинары
	Пользователи	Соглашение	Мегапроекты
	Песочница	Конфиденциальность	

Если нашли опечатку в посте, выделите ее и нажмите Ctrl+Enter, чтобы сообщить автору.

