Смоленск 1.6: режим киоска

Общие сведения

Режим киоска служит для ограничения прав пользователей в системе.
Для использования функциональных возможностей данного режима необходимо установить пакет parsec-cups.

Степень этих ограничений прав пользователей задается маской киоска.
Ее действие аналогично действию маски umask с тем отличием, что если umask накладывается при создании новых объектов ФС, то маска киоска накладывается на права доступа к файлу при любой попытке пользователя получить доступ.

Маска киоска задается в конфигурационном файле /etc/parsec/kiosk_mask и по умолчанию равна 0000 (режим киоска выключен).
Если маска равна 0003 (типичное значение при включенном режиме киоска), для пользователя блокируется доступ по записи и исполнению ко всем файлам, не принадлежащим ему, либо группе, в которую он входит.
При маске, равной 0000, поведение системы остается стандартным и на права доступа пользователя не накладывается никаких ограничений.
Получить текущую маску киоска можно, прочитав содержимое файла /parsecfs/mode_mask.
Маска киоска применяется только к обычным файлам. К каталогам, сокетам и т.д. маска не применяется.

В режиме киоска (маска по умолчанию) пользователь не имеет возможности запустить ни одну системную программу, т.к. эти действия замаскированы.

Команда mkiosk

Команда mkiosk позволяет задавать права доступа пользователя к конкретным файлам.
Эти права доступа не подвержены действию маски и реализованы в виде ACL на специальные виртуальные файлы ФС parsec, являющиеся ссылками на реальные файлы.
После перезагрузки все установленные ACL будут утеряны.

Права доступа к файлу задаются в виде абсолютного пути к файлу.

Так, например, права только на чтение для файла /etc/hosts можно задать в виде:

```
/etc/hosts r--
```

Права на чтение, запись и исполнение для файла /usr/bin/example.sh задаются в виде:

```
/usr/bin/example.sh rwx
```

Так как задавать все права доступа в командной строке было бы крайне неудобно, существует система профилей.
Это файлы с готовыми наборами прав доступа для запуска каких-либо программ.
Например, есть профиль для запуска bash, профиль для запуска ls и т.д.
Эти профили хранятся в каталоге /etc/parsec/kiosk-profiles. Вместо прав доступа к конкретным файлам, в командной строке команды mkiosk можно указать готовый профиль.
Задание файлов отличается от задания профиля по наличию первого символа `/` в имени файла:
Имена профилей задаются без указания полного пути к ним. В общем случае профиль может содержать в себе права доступа на более сложные действия, чем запуск одной программы.
Существует также профиль с именем default, который используется автоматически при каждом запуске mkiosk.
В нем содержатся права доступа, которые необходимы всегда. Это, например, право на использование динамического линковщика.
Для создания профилей можно использовать команду otrace.

Для автоматизации процесса установки прав доступа для каждого пользователя существует конфигурационный файл, хранящийся в каталоге /etc/parsec/kiosk и содержащий все необходимые права доступа.
По сути это такой же профиль, как и в случае профилей программ, но относящийся к конкретному пользователю.
Этот файл может содержать как явное задание прав доступа к конкретным файлам, так и ссылки на профили программ.
При входе пользователя в систему права доступа из конфигурационного файла будут установлены автоматически при помощи специального PAM-модуля.

Параметры команды приведены в таблице:

Параметр	Описание
-h, --help	Вывести справку и выйти
-u , --user=	Установить права доступа для пользователя
-w, --without-profile	Не использовать профиль указанного пользователя для установки прав доступа. Будут использованы только права доступа из командной строки
-e, --mask	Указать маску киоска. Права доступа на файлы для пользователя будут устанавливаться только в том случае, когда необходимые биты маскируются указанной маской. По умолчанию используется текущая маска киоска из файла /parsecfs/mode_mask

Примеры:
Установить права доступа для пользователя ttt, взятые из его профиля /etc/parsec/kiosk/ttt

```
mkiosk -u ttt
```

Установить права на чтение файла /etc/passwd для пользователя ttt. При этом не учитывать профиль пользователя. Предполагается, что системная маска киоска равна 0003 и, соответственно, замаскированы права на запись и выполнение файлов

```
mkiosk -u ttt --mask=3 --without-profile "/etc/passwd r--"
```

Команда otrace

Команда otrace предназначена для трассировки процессов относительно системных вызовов open() и execve().

Синтаксис:

> otrace [-h, --help] [-s, --silent] [-o, --output=] [-k, --kiosk-dir=] [-p, --pid=] [-u, --user=] [-t, --trace] [-a, --audit-trace] [-m, --merge] [-f, --trace-failed] [-e, --mask=] [command]

Команда otrace используется в процессе конфигурирования режима киоска и служит для автоматизации создания профилей прав доступа.

В режиме киоска (стандартные настройки) пользователю запрещены запись и выполнение файлов, не принадлежащих ему, либо группе, в которую он входит. Чтобы пользователь имел возможность хотя бы войти в систему, необходимо явно указать права доступа ко всем файлам, прямо или косвенно участвующим при этой операции. Права доступа к файлам задаются с помощью установки ACL на специальные файлы-ссылки в ФС parsec. При этом права доступа на реальные файлы не изменяются. При перезагрузке системы все ACL на специальные файлы-ссылки будут утеряны.

Чтобы облегчить задачу установки пользователям прав доступа, используются профили прав доступа. Системные профили хранятся в каталоге /etc/parsec /kiosk-profiles`.
Далее приведен пример профиля, позволяющий запустить команду ls:

```
/bin/ls r-x
/etc/group r--
/etc/ld.so.cache r--
/etc/ld.so.preload r--
/etc/localtime r--
/etc/nsswitch.conf r--
/etc/passwd r--
/etc/selinux/config r--
/lib/libacl.so.1 r--
/lib/libattr.so.1 r--
/lib/libc.so.6 r--
/lib/libdl.so.2 r--
/lib/libnsl.so.1 r--
/lib/libnss_compat.so.2 r--
/lib/libnss_files.so.2 r--
/lib/libnss_nis.so.2 r--
/lib/libpthread.so.0 r--
/lib/librt.so.1 r--
/lib/libselinux.so.1 r--
/proc/mounts r--
/usr/lib/gconv/gconv-modules.cache r--
```

/usr/lib/gconv/KOI8-R.so r--
/usr/lib/locale/locale-archive r--
/usr/share/locale/locale.alias r--
/usr/share/locale/ru/LC_MESSAGES/coreutils.mo r--
/usr/share/locale/ru/LC_TIME/coreutils.mo r--
/usr/share/locale/ru_RU/LC_MESSAGES/coreutils.mo r--
/usr/share/locale/ru_RU/LC_TIME/coreutils.mo r--
/usr/share/locale/ru_RU.utf8/LC_MESSAGES/coreutils.mo r--
/usr/share/locale/ru_RU.UTF-8/LC_MESSAGES/coreutils.mo r--
/usr/share/locale/ru_RU.utf8/LC_TIME/coreutils.mo r--
/usr/share/locale/ru_RU.UTF-8/LC_TIME/coreutils.mo r--
/usr/share/locale/ru.utf8/LC_MESSAGES/coreutils.mo r--
/usr/share/locale/ru.UTF-8/LC_MESSAGES/coreutils.mo r--
/usr/share/locale/ru.utf8/LC_TIME/coreutils.mo r--
/usr/share/locale/ru.UTF-8/LC_TIME/coreutils.mo r--

Для применения профиля к конкретному пользователю используется команда mkiosk.

Если профиль служит для запуска программы, как это было в примере, он должен содержать права доступа не только к исполняемому файлу, но и ко всем используемым библиотекам и всем файлам, которые открывает программа в процессе исполнения. Также необходимы права доступа на динамический линковщик, которые не попадут автоматически в профиль, созданный командой otrace. Минимальные права доступа, которые требуются всегда, содержатся в специальном профиле /etc/parsec/kiosk-profile/default и добавляются туда вручную.

Профили могут описывать права доступа для более сложных задач, чем запуск одной программы.
Чтобы облегчить администрирование, можно использовать профили внутри других профилей.
Если внутри профиля встречается строка с именем другого профиля, то содержимое указанного профиля полностью объединяется с содержимым текущего профиля.
Объединение профилей осуществляется рекурсивно.
Если строка в файле профиля начинается не с символа '/', то она рассматривается как имя профиля.
Команда otrace также поддерживает объединение профилей (см. опцию --merge).

Наконец, существуют профили, относящиеся к отдельным пользователям. Они хранятся в каталоге /etc/parsec/kiosk и заполняются вручную на основе готовых профилей либо стандартных строк, описывающих права доступа к конкретному файлу.
При включенном режиме киоска профили пользователей автоматически применяются при входе пользователя в систему. Это реализовано при помощи специального PAM-модуля и команды mkiosk.

Команда otrace может использовать два различных механизма для трассировки процессов.

Первый --- это программа strace (опция --trace).
Второй --- подсистема аудита PARSEC (опция --audit-trace). Программа strace имеет некоторые ограничения по использованию, поэтому применять её следует только для трассировки довольно простых, не SUID-программ.

В режиме --trace цель трассировки может быть задана либо в командной строке команды otrace в качестве аргумента (тогда указанная программа будет запущена), либо может быть задан PID уже существующего процесса (опция --pid).

В режиме --audit-trace цель трассировки задается так же, как и в режиме --trace. Но кроме описанных, есть еще дополнительный способ задания цели трассировки --- опция --user.
При этом всем существующим процессам, принадлежащим указанному пользователю, будут выставлены соответствующие флаги аудита.
Таким образом, будут трассироваться все действия пользователя. Режим полезен, когда необходимо создать профиль, разрешающий пользователю выполнять целый набор сложных действий и трассировать каждую программу в отдельности затруднительно.

Если используется режим --audit-trace, то в системе не должно быть сторонних процессов, на которых установлены флаги аудита. Иначе в профиль может попасть информация, порожденная сторонними процессами.
В режиме трассировки всех процессов указанного пользователя достаточно, чтобы в системе не было других процессов с установленными флагами аудита и принадлежащих этому пользователю.

Команда otrace` по умолчанию записывает в профиль информацию только о тех действиях процесса (open(), execve()), которые прошли успешно. Однако для большей универсальности можно использовать опцию --trace-failed, которая позволит записать в профиль также информацию и о неудачных попытках. Это полезно, например, если процесс пытается открывать конфигурационные файлы. В момент трассировки файл может не существовать, но впоследствии он может появиться.

Параметры команды приведены в таблице:

Параметр	Описание
-h, --help	Вывести справку и выйти
-s, --silent	Не выводить информационные сообщения
-o , --output=	Записать результаты трассировки в указанный файл. По умолчанию --- stdout
-k , --kiosk-dir=	Указать путь к каталогу с профилями киоска. Используется в операции --trace. По умолчанию --- /etc/parsec/kiosk-profiles

-p , --pid=	Трассировать процесс с указанным идентификатором, а также все порожденные им процессы
-u , --user=	Указать имя пользователя. Используется совместно с --audit-trace или --merge
-t, --trace	Использовать для трассировки процессов команду strace. Не может быть использована совместно с --audit-trace
-a, --audit-trace	Использовать для трассировки процессов подсистему аудита PARSEC. Не может быть использована совместно с --trace
-m, --merge	Объединять все права доступа, указанные каким-либо способом в единый поток с уникальными записями. Права доступа могут быть указаны в явном виде, в виде профилей, в виде профиля пользователя и профиля, используемого по умолчанию (/etc/parsec/kiosk-profiles/default)
-f, --trace-failed	Учитывать неудачные попытки вызова open() и execve(). Права доступа к этим файлам будут заданы согласно параметрам, с которыми процесс пытается получить доступ к ним
-e , --mask=	Указать маску киоска. Это позволяет обрабатывать данные согласно этой маске и учитывать только те файлы, права доступа к которым будут действительно замаскированы. По умолчанию маска равна 7

Примеры:

Запустить и трассировать процесс ls с помощью команды strace. Записать результат в файл /tmp/ls_trace

```
otrace --trace -o /tmp/ls_trace ls /
```

Трассировать запущенные процессы пользователя ttt и все вновь порожденные ими процессы с помощью подсистемы аудита PARSEC. Отслеживать также информацию о неудачных попытках открытия файлов и запуска процессов. Результаты трассировки вывести в stdout

```
otrace --audit-trace -u ttt -f
```

Объединить содержимое профиля пользователя ttt, профиля с именем ls из каталога /etc/parsec/kiosk-profiles и добавить права на чтение и выполнение файла /usr/bin/example.
Предполагать, что системная маска киоска равна 3 и, соответственно, учитывать только те файлы, для которых права доступа должны включать права на запись или выполнение

```
otrace --merge --mask=3 -u ttt ls "/usr/bin/example r-x"
```

Графический инструмент fly-admin-kiosk

Кроме средств для работы в режиме командной строки, в распоряжении администратора имеется графический инструмент fly-admin-kiosk, который может быть использован для настройки и управления режимом киоска.
Описание инструмента см. в электронной справке.

Перед использованием утилиты необходимо сделать резервную копию

- всех системных профилей, находящихся в каталоге /etc/parsec/kiosk-profiles;
- системного профиля fly-dm в каталоге /etc/parsec/kiosk.

Системные профили, устанавливаемые по умолчанию, находятся в пакете parsec-kiosk.

Переместить системный профиль fly-dm из каталога /etc/parsec/kiosk в каталог /etc/parsec/kiosk-profiles, выполнив команду:

```
mv /etc/parsec/kiosk/fly-dm /etc/parsec/kiosk-profiles/fly-dm
```

Создать пользовательский профиль fly-dm в каталоге /etc/parsec/kiosk, выполнив команду:

```
echo fly-dm > /etc/parsec/kiosk/fly-dm
```

Отредактировать содержимое файла /etc/parsec/kiosk-profiles, заключив в кавычки имена файлов:

"/lib64/ld-linux-x86-64.so.2" r-x
"/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2" r-x

Далее можно использовать утилиту fly-admin-kiosk.

Настройка режима киоска для пользователя

Для разрешения входа пользователя в режиме текстовый консоли необходимо, используя механизм sudo, от имени суперпользователя root создать файл профиля для пользователя
имя_пользователя в каталоге /etc/parsec/kiosk и добавить в файл имя_пользователя перечень профилей, необходимых для разрешения входа пользователя, выполнив команды:

```
echo default > /etc/parsec/kiosk/_
echo bash >> /etc/parsec/kiosk/_
```

Для добавления разрешенных для пользователя команд необходимо:

- войти в систему от имени учетной записи пользователя на одной консоли (например, tty1);
- войти в систему от имени учетной записи администратора на другой консоли (например, tty2), используя команду sudo -s, переключиться в сессию суперпользователя root и запустить протоколирование действий пользователя, выполнив команду:

  ```
  otrace -a -o /etc/parsec/kiosk-profile/__ -f --mask=3 -u _
  ```

- дождаться перезапуска сервиса parlogd;
- перейти на консоль пользователя и выполнить все команды, которые должны быть разрешены в дальнейшем;
- завершить сеанс пользователя;
- в консоли суперпользователя root остановить трассировку, нажав клавишу <Enter>;
- подключить полученный новый профиль к пользователю, выполнив команду:

  ```
  echo __ >> /etc/parsec/kiosk/_
  ```

- в консоли суперпользователя root включить режим киоска и перезагрузить ОС, выполнив команды:

  ```
  echo 0003 > /etc/parsec/kiosk_mask
  reboot
  ```

Для разрешения входа пользователя в графическом режиме необходимо:

- проверить наличие профиля fly-dm в файле /etc/parsec/kiosk/fly-dm;
- подключить профиль fly к профилю пользователя имя_пользователя, выполнив от имени суперпользователя root команду:

  ```
  echo fly >> /etc/parsec/kiosk/_
  ```

Для создания профиля fly необходимо:

1. войти в систему в режиме текстовой консоли от имени администратора, используя команду sudo -s, переключиться в сессию суперпользователя root и остановить работу fly-dm|, выполнив команду:

   ```
   service fly-dm stop
   ```

2. проверить наличие логической ссылки /usr/bin/x-session-manager, выполнив команду:

   ```
   ls -l /usr/bin/x-session-manager
   ```

3. удалить указанную логическую ссылку и создать другую с суффиксом .orig, выполнив команды:

```
rm /usr/bin/x-session-manager
ln -s /etc/alternatives/x-session-manager /usr/bin/x-session-manager.orig
```

4. создать текстовый файл /usr/bin/x-session-manager со следующим содержимым:

```
#!/bin/bash
/usr/sbin/otrace -t -f -o /test/fly --mask=3 /usr/bin/x-session-manager.orig $@ &
sleep 20
/usr/bin/fly-wmfunc FLYWM_EXIT
```

5. изменить права на созданный файл, выполнив команду:

```
chmod 777 /usr/bin/x-session-manager
```

6. установить пакет strace, выполнив команду:

```
apt-get install starce
```

7. создать каталог /test с правами 777, выполнив команду:

```
mkdir -m 777 /test
```

8. запустить fly-dm, выполнив команду:

```
service fly-dm start
```

9. выполнить вход пользователя в графическом режиме и подождать 20 секунд до автоматического завершения сессии пользователя (можно открыть стартовую меню-панель Fly, терминал fly-term);
10. в сессии суперпользователя root проверить наличие профиля fly в каталоге /test, выполнив команду:

```
ls -l /test/fly
```

11. удалить файл /usr/bin/x-session-manager, выполнив команду:

```
rm /usr/bin/x-session-manager
```

12. создать логическую ссылку /usr/bin/x-session-manager, выполнив команду:

```
ln -s /etc/alternatives/x-session-manager /usr/bin/x-session-manager
```

13. открыть полученный профиль /test/fly в текстовом редакторе, удалить строки вида ... resumed ..., строки для /proc и строки, содержащие пути, начинающиеся с "./";
14. перенести профиль в каталог профилей, выполнив команду:

```
cp /test/fly /etc/parsec/kiosk-profiles/fly
```

15. подключить профиль fly к профилю пользователя, выполнив команду:

```
echo fly >> /etc/parsec/kiosk/_
```

16. включить режим киоска и перезагрузить ОС, выполнив команды:

```
echo 0003 > /etc/parsec/kiosk_mask
reboot
```

17. выполнить в графическом режиме вход в систему от имени пользователя;
18. если сессия не открывается, то проверить в консоли суперпользователя root содержимое файла /home/имя_пользователя/.xsession-errors, содержащего файлы, права на которые не выставлены в профиле fly, и добавить разрешение вручную.
    Пример строки из файла /home/имя_пользователя/.xsession-errors:

    > /etc/X11/fly-dm/Xsession : line 55 /bin/df: отказано в доступе/
    > Пример добавления строки в профиль fly:
    > echo '"/bin/df" r-x' >> /etc/parsec/kiosk-profiles/fly

19. после изменений применить профиль к пользователю, выполнив команду:

    ```
    mkiosk -u user
    ```

20. при наличии в файле /home/имя_пользователя/.xsession-errors| строки, содержащей текст "unable to create error file"
    проверить наличие в профиле fly команд chmod, rm, cp и файлов XErrorDB, /usr/lib/parsec/bin/x-session-manager и, при необходимости, добавить в профиль полные пути к ним.

Для добавления пользователю разрешения на выполнение конкретных программ (например, firefox) необходимо:

1. выключить режим киоска, выполнив команды:

   ```
   echo 0000 > /etc/parsec/kiosk_mask
   reboot
   ```

2. выполнить в графическом режиме вход в систему от имени пользователя;
3. войти в систему в режиме текстовой консоли от имени администратора, используя команду sudo -s, переключиться в сессию root и запустить протоколирование действий пользователя, выполнив команду:

   ```
   otrace -a -o /etc/parsec/kiosk-profile/firefox -f --mask=3 -u _
   ```

4. дождаться перезапуска сервиса parlogd;
5. перейти в графический интерфейс пользователя и запустить/завершить firefox;
6. завершить сеанс пользователя;
7. в консоли суперпользователя root остановить трассировку, нажав клавишу <Enter>;
8. подключить полученный профиль firefox для пользователя, выполнив команду:

   ```
   echo firefox >> /etc/parsec/kiosk/_
   ```

9. в консоли суперпользователя root включить режим киоска и перезагрузить ОС, выполнив команды:

   ```
   echo 0003 > /etc/parsec/kiosk_mask
   reboot
   ```

Киоск Fly

Для ограничения возможности запуска программ локальным пользователям администратор может использовать графическую утилиту fly-admin-smc. Для этого необходимо в настройках политики безопасности пользователя графической утилиты fly-admin-smc во вкладке <<Графический киоск Fly>> установить флаг <<Режим графического киоска Fly>>. Флаг включает режим киоска при работе с приложениями из списка. Если в списке одно приложение, то режим киоска включается при работе с этим приложением. Если в списке несколько приложений, то запускается Рабочий стол с этими приложениями. Все доступные каталоги, ярлыки и т.\,д. устанавливаются в соответствии с предоставленным доступом.

Настройка режима киоска с помощью графической утилиты fly-admin-smc осуществляется администратором на максимальном уровне мандатного контроля целостности, установленном в ОС.