Область подкачки (swap): особенности применения и обеспечения безопасности

Подкачка (свопинг) в Linux

SWAP – один из механизмов виртуальной памяти, при котором отдельные фрагменты памяти перемещаются из ОЗУ в так называемые области подкачки (swap area или swap space), расположенные на вторичном хранилище данных (отдельный дисковый раздел или просто файл в файловой системе), освобождая ОЗУ для загрузки других активных фрагментов памяти.

Более подробно о механизмах подкачки можно прочитать в Википедии или в Wikipedia или в документации.

Данная статья применима к:

- ОС СН Смоленск 1.6
- ОС СН Смоленск 1.5 (частично)
- ОС СН Ленинград 8.1
- ОС ОН Орёл 2.12 (в части, не касающейся мандатного разграничения доступа)

Необходимость использования подкачки

Наличие области подкачки является важной составляющей системы управления памятью, и необходимо для нормального функционирования системы.

При этом

получение резервного объема оперативной памяти не является основным назначением подкачки.
Её основным назначением является обеспечение эффективного высвобождения и балансировка использования имеющейся памяти.

Фактически, использование области подкачки в качестве «дополнительного резервного объёма» является ненормальной ситуацией, и требует принятия мер по расширению аппаратных средств.

В Linux-системах существуют различные типы страниц оперативной памяти, каждый из которых имеет свои особенности, но для понимания нужности подкачки существенны два типа:

1. Страницы, содержимое которых можно восстановить, повторно прочитав это содержимое из файлов (страницы с командами исполняемых процессов, кеши их файловых данных), т.н. файловый кеш;
2. Страницы данных о распределении памяти между процессами, т.н. анонимные страницы, не имеющие исходных файлов.

И основное назначение области подкачки — это освобождать в оперативной памяти место для файлового кеша за счет выгрузки неактуальных анонимных страниц.Таким образом, удаление области подкачки не предотвратит увеличение общего количества дисковых операций при заполнении оперативной памяти, а просто заменит дисковые операции вытеснения анонимных страниц на повторные дисковые операции файлового чтения. Это не только менее эффективно, так как выбор страниц для обновления оказывается меньше, но, в свою очередь, также ведёт к ещё большему переполнению памяти.

Дополнительно область подкачки обычно используется для организации режимов сна (hibernation или suspend to disk). При входе в такие режимы в область подкачки сохраняется полная копия оперативной памяти. (В современных системах можно обеспечить режим сна без использования области подкачки, с сохранением содержимого оперативной памяти в файлах).

Выбор и настройка параметров подкачки

Размещение областей подкачки: дисковый раздел или файл?

Современные Linux-системы позволяют размещать области подкачки как в специально выделенных дисковых разделах, так и в файлах. Независимо от способа размещения, современные версии ядра Linux обеспечивают примерно одинаковую скорость работы подкачки, определяя файлы подкачки, и используя прямой доступ к ним. При работе с дисковыми накопителями существенным фактором, негативно влияющим на скорость подкачки при работе с файлами может стать фрагментация этих файлов, поэтому для дисковых накопителей предпочтительным может быть использование дисковых разделов. При использовании твердотельных накопителей фрагментация файлов безразлична. В любом случае, возможность динамически отключать/подключать файловые области подкачки позволяет рационально использовать дисковое пространство, изменяя размеры области подкачки по необходимости без прерывания работы системы.

При установке Astra Linux по умолчанию автоматически создаётся область подкачки в отдельном дисковом разделе.
Проверить, где размещена (размещены) область (области) подкачки можно командой

```
sudo swapon
```

При необходимости проверить фрагментацию файла можно командой filefrag:

sudo filefrag -v /example.swap

Уменьшить фрагментацию файла в файловой системе Ext4 можно командой e4defrag:

sudo e4defrag -v /example.swap

При размещении файлов на твердотельных накопителях выполнение дефрагментации не имеет никакого смысла.

Размер областей подкачки

В общем случае, для Astra Linux правильным начальным выбором может являться объём области подкачки 2-3ГБ с последующим уточнением по итогам эксплуатации. Если предполагается использовать режим сна (**hibernation** или **suspend to disk**) с сохранением образа оперативной памяти, то нужный объём зависит от объёма оперативной памяти, и в таком случае хорошим первоначальным вариантом размера области подкачки является объём, равный объёму оперативной памяти плюс 2-3ГБ.

Основным параметром настройки подкачки является значение параметра ядра **vm.swappiness**, определяющее объем свободной памяти (в процентах), при котором начинается вытеснение страниц. Проверить значение этого параметра можно командой

```
sudo sysctl vm.swappiness
```

Настройка подкачки

По умолчанию значение параметра **vm.swappiness** равно 60, т.е. вытеснение страниц памяти в область подкачки начинается тогда, когда объём свободной памяти становится меньше 60%.
Считается, что данное значение хорошо работает для большинства систем. Изменить значение параметра **vm.swappiness** можно командой

```
sysctl -w vm.swappiness=<_>
```

Минимальное значение атрибута, при котором будет работать подкачка равно единице.

При задании нулевого значения параметра **vm.swappiness** подкачка отключается полностью.

Безопасность данных, находящихся в области подкачки

Страницы памяти, которые динамически копируются из оперативной памяти в область подкачки в процессе работы компьютера, могут содержать конфиденциальную информацию, не закрытую какими-либо защитными преобразованиями. Таким образом, наличие доступа на чтение к области подкачки создаёт угрозу утечки конфиденциальной информации.

Отдельную проблему с точки зрения безопасности представляет собой хранение в области подкачки содержимого оперативной памяти выключенных компьютеров. Копия содержимого оперативной памяти может остаться в области подкачки:

- при неожиданном отключении компьютера в результате аппаратного сбоя;
- при неожиданном отключении электропитания;
- и всегда остаётся там в компьютерах, находящихся в режиме сна.

При наличии физического доступа к оборудованию такие данные можно прочитать независимо от установленных дискреционных и мандатных ограничений .

Рекомендации по обеспечению безопасности области подкачки

В Astra Linux SE (Смоленск 1.6, Ленинград 8.1) разделу подкачки, создаваемому при установке системы, автоматически присваивается метка безопасности с максимальными уровнями конфиденциальности и целостности и максимальным набором категорий доступа:

- Уровень конфиденциальности 3;
- Уровень целостности 63;
- Набор категорий доступа полный.

Таким образом при установке Astra Linux SE (Смоленск 1.6, Ленинград 8.1) автоматически обеспечивается защита от чтения области подкачки непривилегированными пользователями.

Однако, у администратора системы есть возможность после установки добавить свои области подкачки (см. команды mkswap/swapon/swapoff, а также системные вызовы swapon()/swapoff()). При этом операционная система не проверяет установленные для добавляемой области подкачки права доступа, и администратору следует самостоятельно указать нужные ограничения дискреционных и мандатных прав доступа. Например, для размещения области подкачки в файле /swap_area можно использовать следующую последовательность команд:

```
# создаем файл размером 1Gb
sudo fallocate -l 1G /swap_area

# ограничиваем дискреционные права доступа (для Astra Linux SE/Astra Linux CE)
sudo chown root:root /swap_area
sudo chmod 600 /swap_area

# ограничиваем мандатные права доступа (только для ОС СН Astra Linux SE)
# - уровень конфиденциальности 3
# - уровень целостности 63
# - открыты все категории доступа
sudo pdpl-file 3:63:-1 /swap_area

# размечаем область подкачки
sudo mkswap /swap_area

# включаем область подкачки в работу
sudo swapon /swap_area
```

Для гарантированного удаления информации из области подкачки при выводе этой области подкачки из работы можно использовать:

- для накопителей на магнитных дисках (применимо только в ОС СН Astra Linux SE):
  - для файлов в дисковых разделах с файловой системой Ext2/Ext3/Ext4 – параметр монтирования файловой системы secdel в /etc/fstab;
  - для разделов подкачки — инструмент командной строки swap-wiper с указанием имени раздела подкачки в качестве аргумента. Подробнее см. «Руководство администратора», п. 8.1).
- для твердотельных накопителей (см. Твердотельные накопители (SSD): особенности применения) (в ОС ОН Astra Linux CE и в ОС СН Astra Linux SE):
  - для файлов в дисковых разделах с файловой системой Ext4 – параметр монтирования файловой системы discard в /etc/fstab;
  - для разделов подкачки – команду blkdiscard:

```
sudo blkdiscard /dev/sda5
```

Инструмент swap-wiper, входящий в состав ОС СН Astra Linux SE (Смоленск 1.6, Смоленск 1.5, Ленинград 8.1) предназначен для стирания данных, находящихся в дисковых разделах подкачки, при выключении системы .
Этот инструмент доступен в файле /usr/lib/parsec/bin/swap-wiper и предназначен для автоматического стирания областей подкачки при выключении компьютера. Инструмент swap-wiper по умолчанию заблокирован в его файле настроек

Для использования инструмента следует в файле /etc/parsec/swap_wiper.conf установить значение атрибута ENABLED=Y, после чего инструмент будет автоматически применяться при выключении системы..

Установить атрибут ENABLED=Y можно с помощью текстового редактора, или с помощью штатного графического инструмента управления безопасностью fly-admin-smc, доступного через графическое меню:

"Пуск" - "Панель управления" - "Безопасность" - "Политика безопасности" - "Настройки безопасности" - "Политика очистки памяти", "Очистка разделов подкачки")

Стирание информации на твердотельных накопителях не гарантируется, подробности см. Твердотельные накопители (SSD): особенности применения

Для обеспечения надёжной защиты от несанкционированного доступа данных в областях подкачки рекомендуется использовать предусмотренную в Astra Linux SE/CE возможность автоматического защитного преобразования данных дисков и областей подкачки. Такое решение несколько повышает нагрузку на процессор, но существенно повышает сохранность конфиденциальной информации как при использовании твердотельных накопителей, так и при внезапном отключении компьютера или при нахождении компьютера в режиме сна.

В качестве дополнительной меры безопасности можно рекомендовать использование систем резервного электропитания, обеспечивающих при сбоях электропитания автоматическое штатное отключение компьютеров, включающее очистку областей подкачки.

В крайнем случае, при невозможности или, исходя из конкретной модели нарушителя, недостаточности применения описанных выше мер защиты следует полностью отключить механизмы подкачки, для чего выполнить
либо запрещение выгрузки страниц (значение 0 параметра ядра vm.swappiness):

```
sysctl -w vm.swappiness=0
```

либо полное отключение всех областей подкачки (параметр -a или --all команды swapoff):

```
swapoff -a
```

с последующим выполнением очистки освободившихся областей подкачки.

Рекомендации по обеспечению безопасности ПО

При разработке собственного ПО

При разработке собственного ПО для защиты памяти, содержащей незащищенные конфиденциальные данные, следует применять системные вызовы **mlock ()** и **mlockall()**:

```
#include <sys/mman.h>
int mlock(const void *addr, size_t len);
int munlock(const void *addr, size_t len);
int mlockall(int flags);
int munlockall(void);
```

Вызовы **mlock**() и **mlockall**() блокируют часть или всё виртуальное адресное пространство процесса в оперативной памяти, предотвращая выгрузку страниц в область подкачки. Вызовы **munlock**() и **munlockall**() выполняют обратное действие, разрешая менеджеру памяти ядра при необходимости выгружать страницы в область подкачки. Подробности применения см.

```
man mlock
```

При применении ПО сторонних разработчиков

При применении программ сторонних разработчиков для снижения вероятности выгрузки памяти процесса в область подкачки можно использовать механизм cgroups, позволяющий назначить отдельному процессу (группе процессов) групповой атрибут memory.swappiness с нулевым значением. Этот атрибут по смыслу в целом аналогичен описанному выше атрибуту ядра vm.swappiness, однако его нулевое значение **не гарантирует полную невозможность выгрузки**, так как настройки ядра имеют больший приоритет, чем настройки групп, и ядро может выгрузить такие процессы при дефиците памяти.

ПО ядра и безопасность подкачки

Память ядра (модулей ядра) не подлежит выгрузке в область подкачки, соответственно, не подвержена связанным с нахождением в области подкачки рискам.

Однако, уровень привилегий ядра позволяет осуществлять доступ к любым системным ресурсам, соответственно, модули ядра сами являются потенциальной угрозой конфиденциальности области подкачки.

В отношении модулей ядра следует применять общепринятые меры безопасности: использовать только подписанные модули ядра, полученные из доверенных источников, а при возможности — контролировать исходные тексты на наличие необычных системных вызовов. Дополнительной мерой защиты также является применение защитного преобразования данных.