

Процессы и права



Процессы и права

Процессы

- /proc
- Получение списка процессов
- Приоритеты
- Сигналы

Права

- SUID
- SGID
- Sticky bit
- umask
- ACL
- Атрибуты

В Linux все сущности представлены как файлы

Даже процессы



/proc

Виртуальная файловая система, генерируемая ядром, содержимое находится в ОЗУ

В ней содержатся файлы с информацией о процессах и общих показателях системы

Интересные файлы в /proc

- `/proc/meminfo` – информация об ОЗУ
- `/proc/cpuinfo` – информация о процессоре
- `/proc/config.gz` – конфиг текущего ядра
- `/proc/cmdline` – параметры, переданные ядру при загрузке
- `/proc/filesystems` – поддерживаемые в данный момент ФС
- `/proc/mounts` – текущие точки монтирования

В /proc есть директории

Название соответствует номеру процесса

В каждой директории содержится информация о процессе и его параметры



Интересные файлы в директориях процессов

- `cmdline` – полная команда, которой процесс был запущен
- `cwd` – ссылка на текущую рабочую директорию процесса
- `exe` – ссылка на исполняемый файл процесса
- `environ` – переменные окружения процесса

Зачем?



Информация из /proc используется системным ПО

Её можно использовать для написания своего системного ПО, чтобы не вызывать `bash`-команды из кода

Полезно для глубокого поиска проблем в работе любого ПО



Просмотр процессов

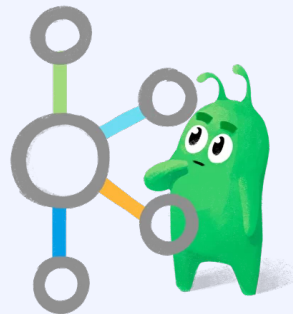
- ps
- top
- htop
- atop

Приоритеты процессов

Приоритеты варьируются от **-20**(min) до **19**(max)

Изменить приоритет запущенного процесса можно через `renice`

Запустить новый процесс, с установленным приоритетом, можно через `nice -n`



Сигналы

- 15 — SIGTERM — просьба завершить работу
- 9 — SIGKILL — приказ немедленно умереть
- 2 — SIGINT — завершение из терминала (Ctrl + C)
- 19 — SIGSTOP — поставить на паузу (Ctrl + Z)
- 18 — SIGCONT — снять с паузы
- 11 — SIGSEGV — ошибка обращения к ОЗУ

Расширенные права

SUID

Бит разрешения, позволяющий исполнять файл с правами владельца

Самый популярный пример – команда `sudo`

SGID

Бит разрешения, позволяющий исполнять файл с правами группы

однако

директории, для которых он указан, будут наследовать группу владельца директории для всех поддиректорий

Sticky bit

Разрешение для директории, которое позволяет удалять файлы в директории только если пользователь является владельцем файла

Как и SGID, это разрешение полезно при организации общих многопользовательских директорий

umask

Устанавливает права по умолчанию

Настройки `umask` применяются к правам как битовая маска и “отнимает” соответствующие права по умолчанию.

Максимальное значение `umask`:

файлы – 666

директории – 777

ACL

Access Control List

Расширенная система прав

Позволяет гибко настроить права доступа к файлам и директориям на многопользовательских системах.

Есть нюанс



Некоторые средства создания бекапов не бекапят правила ACL

Правила ACL задаются командой **setfacl**

Просматриваются командой **getfacl**

Атрибуты файлов

Устанавливают дополнительные параметры

Задать – **chattr**

Посмотреть – **lsattr**

Самые интересные:

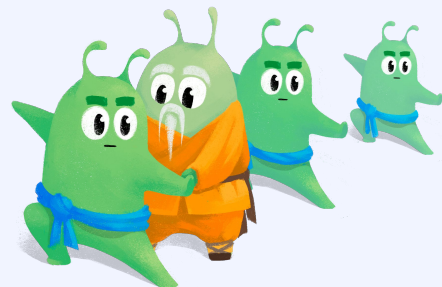
i – immutable

a – append



В следующей серии:

Джедайские приёмы работы с командной строкой Linux



Вопросы?

