Администрирование Linux
Лекция 6
Атрибуты файлов и права доступа

Иртегов Д.В.
Новосибирский гос. Университет
2014

Файлы в Unix

- последовательность байтов
- операционная система не накладывает никакого формата
- адресация с точностью до байта
- дисковый файл автоматически расширяется при записи
- метка конца файла не входит в данные файла
- файл также является универсальным интерфейсом с внешним устройством

Каталоги

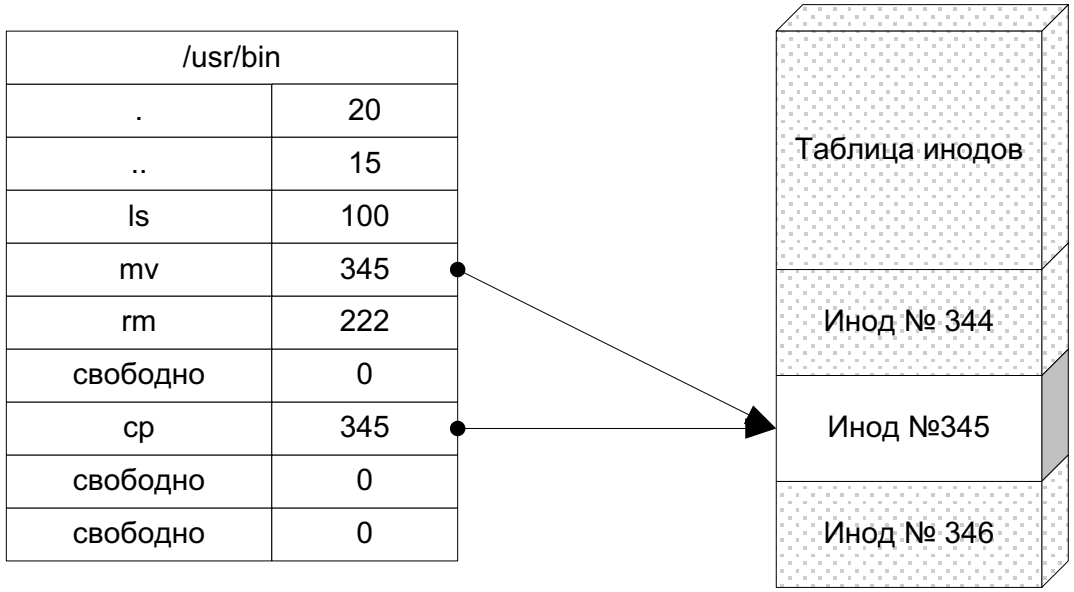
- Файлы специального типа (d)
- Могут содержать список файлов/подкаталогов или быть точкой монтирования
- Можно смонтировать ФС на непустой каталог,
  - тогда его содержимое станет недоступно но с диска никуда не денется

Атрибуты файла

- Тип
  - Регулярный файл
  - Каталог
  - Символическая ссылка
  - Блочное/символьное устройство
  - Другие спец. файлы: named pipe, unix socket, door (Solaris), etc
- Длина (у спецфайлов может не быть)
- Количество связей
- Три даты: создания, модификации, доступа
- Права доступа
  - Хозяин и группа
  - rwx-маска: чтение, запись, исполнение для хозяина, группы, остальных
  - setuid, setgid, sticky bit
  - Posix ACL (не на всех файловых системах)

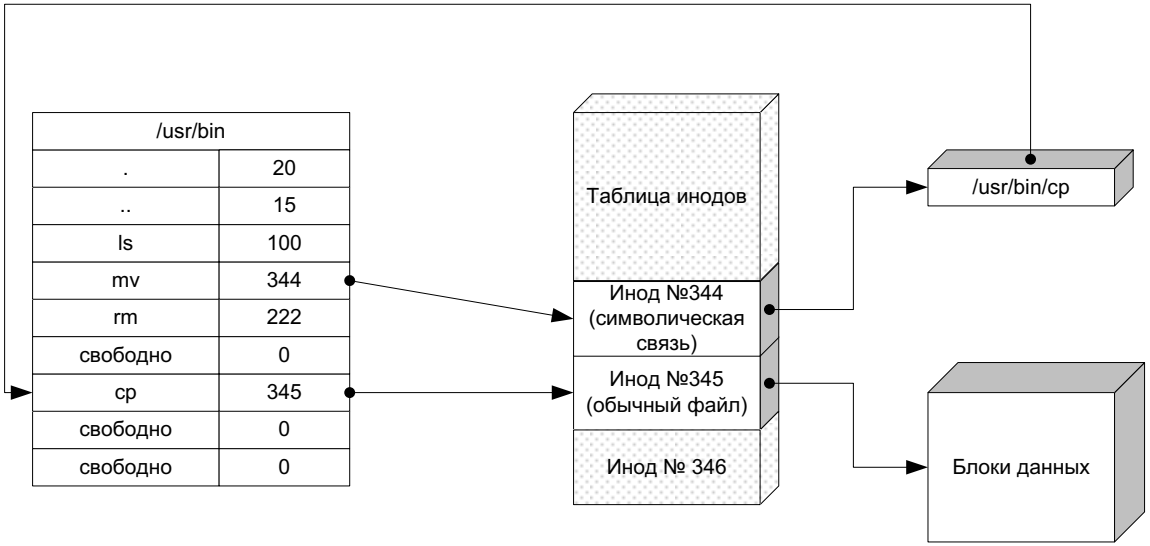
Жесткие связи

- Создаются командой ln
- Удаляются командой rm
- Уходящий последним гасит свет
- Нельзя создавать на каталоги
- Нельзя создавать на другую ФС



Символические связи

- Создаются командой ln –s
- Удаляются командой rm
- Можно удалить файл раньше связи получится связь в никуда
- Можно создавать на каталоги и другие ФС



Setuid

- Каждый процесс в Unix имеет два uid
  - Реальный – кем он был запущен
  - Эффективный – используется при проверке прав
- При запуске программы с битом setuid, euid процесса == uid хозяина программы
- Мы уже видели три setuid программы:
  - su, sudo, passwd
  - На самом деле, их довольно много

Полезные программы

- ls -l – показывает наиболее важные атрибуты
  - ls -l --time=[atime,ctime] – выдать atime/ctime вместо mtime
  - ls --color – цвет в зависимости от типа и расширения файла
  - ls -F – добавить символ в зависимости от типа
- chown/chmod/chgrp – изменение традиционных юниксовых прав
- getfacl/setfacl – просмотр и изменение POSIX ACL
- du – disk usage
- df – disk free
- find – рекурсивный поиск по атрибутам
- locate – быстрый поиск по имени

POSIX ACL

- Расширение традиционных прав
- Список записей вида [d]:[ugm]:id:rwx
  - d: права по умолчанию (только каталоги)
  - User, group, other, mask (тип записи)
  - Id пользователя или группы
  - Права чтения, записи и исполнения
    - Заглавное X означает установить бит x только для каталогов
- Файлы с непустыми POSIX ACL помечаются знаком + в выдаче ls -l

find(1)

- find fromwhere condition[s] action[s]
- Conditions:
  - -name pattern
  - -atime,-mtime,-ctime – по трем временам
  - -type d,f,s,b,c
  - -perm – по правам доступа
  - -user
- Actions
  - -print
  - -exec cmd ‘{ }’ \;
- find / -perm -4000 -print – список всех setuid-файлов
- find /tmp -atime +7 -exec rm –f ‘{}’ \;

Упражнение

- Найти все setuid-файлы в системе
- Найти все файлы в /bin, являющиеся символическими ссылками

Резервное копирование

Резервное копирование

- Спасает в случае
  - Сбоев оборудования
  - Логических ошибок, приведших к потере данных (ошибка администратора, ошибка в ПО)
  - Ошибок пользователей
  - Взломов
- Полезно при
  - Изменении конфигурации дисковой подсистемы
  - Апгрейде ПО, миграции данных на новую версию системы,
  - любых серьезных реорганизациях системы и прикладного ПО

Модели резервного копирования

- Полное
- Дифференциальное
  - Данные, измененные с момента последнего полного бэкапа
- Инкрементальное (инкрементное)
  - Данные, измененные с момента предыдущего полного ИЛИ инкрементного бэкапа
- Как быть с файлами, изменяемыми во время бэкапа?
  - Останавливать все сервисы/переходить в single user
  - LVM snapshots (будем изучать)

Куда копировать?

- Магнитные ленты
  - Долгое время были основным средством
  - Сейчас выходят из употребления: емкость дисков быстро растет => лентопротяжки быстро устаревают, а они дорогие
- Постоянно подключенные жесткие диски
  - Уязвимы при пожаре в серверной, краже сервера, взломе сервера, ошибках администратора
- Подключаемые по USB/ESATA жесткие диски
  - В современном датацентре это безумие
- Доступный по сети внешний сервер/дисковый массив

Способы резервного копирования

- Образ диска
  - dd if=/dev/sda1 of=/mnt/backup/$timestamp
  - cp centos.vdi /mnt/backup/$timestamp
- Образы с учетом структуры ФС
  - Acronis Trueimage, clonezilla
  - dump/restore (ext2-4 only)
- Файловые архивы
  - tar
  - cpio
- rsync

Сравнение технологий бэкапа

- Образ диска
  - + легко восстанавливать
  - + восстанавливает все, включая загрузчик
  - - содержит также свободное пространство
    - Образы структуры ФС в этом плане умнее
  - - возможен только полный бэкап
  - - неудобно частичное восстановление
  - - проблемы при восстановлении на диск с плохими блоками
- Пофайловые бэкапы/rsync
  - + не включает свободное пространство
  - + возможен инкрементный/дифференциальный бэкап
  - + удобно частичное восстановление
  - - восстановление загрузчика надо делать отдельно

dump/restore

- Работает мимо драйвера ФС через специальную библиотеку
- Сохраняет номера инодов
- В большинстве случаев, быстрее tar/cpio
- Exclude file list нужно задавать при помощи номеров инодов, а не имен файлов
  - find /directory/I/do/not/need -printf "%i\n" > /tmp/exclude
- dump -D /etc/dumpdates -$L /fs|/dev/sda1 -f archive
- dump -Q | restore -Q создают индекс для быстрого поиска отдельных файлов в архиве
- restore имеет собственную командную строку для выбора отдельных файлов и их последующего восстановления

tar, cpio

- Tape ARchive
  - tar cvf filename /dir/to/backup
- CoPy Input/Output
  - find / -print | cpio -o > file
  - cpio ориентирован на получение файлов из файла/stdin, поэтому его обычно используют в сочетании с find для генерации списка файлов

Как передавать архивы по сети?

- При помощи ssh
  - dump $OPTS -f - | ssh dump@archive.node dd of=…
  - ssh dump@source-node sudo dump … | dd of=…
  - ssh -c cbc-blowfish
- Упаковка
  - dump … | gzip | ssh
  - gzip на 2GHz Xeon <= 1Gb/s Ethernet
  - bzip2 на 2GHz Xeon ~= 100Mb/s Ethernet

Упражнение

- Настройте ежедневный (в час ночи) инкрементальный бэкап ваших контейнеров при помощи dump|ssh на parallels.nsu.ru:/home2/$user
  - Там должно хватить места
  - Для генерации имени файла, используйте синтаксис $(date '+%y-%m-%d')

rsync

- Remote SYNChronization
- Репликатор: сравнивает локальный каталог с удаленным и копирует измененные файлы
- Может работать через
  - собственный протокол – на сервере должен быть запущен rsyncd
  - ssh/rsh - на сервере должна быть доступна команда rsync
  - Локально – продвинутый вариант cp -Ru
- rsync -av --rsh="ssh -l dump" /home backup:/storage/…
- Вообще-то не предназначен для бэкапа
- Удобен, когда у вас много мелких файлов
  - Например для бэкапа домашних каталогов пользователей

Упражнение на начало следующего занятия

- Посмотреть файлы бэкапов
- Посмотреть списки файлов при помощи restore
- Посмотреть, какие файлы были изменены yum за прошедшую неделю, и есть ли старые версии в бэкапах