Accounting and Quotas

System Administration

UNIX

Accounting

- **UNIX allows for user-based process accounting**
  - designed for usage charging
    - *rather 'raw' and so is a bit hard to use meaningfully*
      - another often-automated activity
  - not designed to assist performance tuning
- **usually an option**
  - requires a specially made kernel
    - *doesn't require much RAM, so best to have it compiled in*
      - but disabled if not wanted
  - puts a (usually small) load on the system
- **enabled by the accton command**
  - usually in /etc/rc.d/rc.sysinit
    - *accton /var/log/pacct*
      - turns accounting on, logged into /var/log/pacct
    - accton
      - turns accounting off
      - *"simply deleting the accounting file doesn't diminish the accounting overhead…the kernel will attempt to keep and write records but have no place to put them"*

Files

- based on the maintenance of a number of files
  - /var/adm/pacct
    - *summarizes information about executed commands*
  - /var/run/utmp
    - *makes it possible to discover information about who is currently using the system*
      - *"Linux utmp entries conform neither to v7/BSD nor to SYSV: they are a mix of the two."*
    - *should always exist*
      - should *never* be writable by anyone other than root
        - security risk
  - /var/log/wtmp
    - *records all logins and logouts*
    - *if it doesn't exist login information isn't maintained*
  - other files
    - *printer accounting files*
      - typically in /var/spool/lpr/...

Image-Based Accounting

- sa
  - reads raw accounting file /var/log/pacct
    - *creates raw summary files /var/log/savacct, /var/log/usracct*
  - produces a number of reports
    - has a large number of options!

```
[ -a | --list-all-names ]
[ -b | --sort-sys-user-div-calls ]
[ -c | --percentages ] [ -d | --sort-avio ]
[ -D | --sort-tio ] [ -f | --not-interactive ]
[ -i | --dont-read-summary-file ]
[ -j | --print-seconds ] [ -k | --sort-cpu-avmem ]
[ -K | --sort-ksec ] [ -l | --separate-times ]
[ -m | --user-summary ] [ -n | --sort-num-calls ]
[ -r | --reverse-sort ] [ -s | --merge ]
[ -t | --print-ratio ] [ -u | --print-users ]
[ -v num | --threshold num ] [ --sort-real-time ]
[ --debug ] [ -V | --version ] [ -h | --help ]
[ --other-usracct-file filename ]
[ --other-savacct-file filename ]
[ [ --other-acct-file ] filename ]
```

Sa Reports

- some useful options:
  - -l: when reporting, provide separate user and system times
    - *times given in minutes*
  - -m: print number of processes and times on a per-user basis
  - -u: for each command, print user, execution time and command name

```
# sa -l
    66      0.31re    0.18u     0.06s
    4       0.00re    0.11u     0.01s   troff
    6       0.05re    0.03u     0.01s   grotty
    6       0.05re    0.01u     0.01s   less
    6       0.05re    0.01u     0.01s   man
    2       0.00re    0.01u     0.01s   w
    2       0.00re    0.01u     0.01s   ps
    6       0.05re    0.01u     0.00s   groff
    6       0.05re    0.00u     0.01s   sh
    4       0.00re    0.00u     0.00s   gtbl
    10      0.05re    0.00u     0.00s   sh      *
    4       0.00re    0.00u     0.00s   ls
    2       0.00re    0.00u     0.00s   netstat
    4       0.00re    0.00u     0.00s   cat
    2       0.00re    0.00u     0.00s   who
    2       0.00re    0.00u     0.00s   accton

# sa -m
                66              0.31re          0.24cp
bob             58              0.31re          0.22cp
root            8               0.00re          0.02cp
```

```
# sa -u
root        0.03 cpu accton
root        0.06 cpu ls
root        0.36 cpu w
root        0.06 cpu who
bob         0.12 cpu less
bob         0.34 cpu grotty
bob         0.12 cpu groff
bob         0.03 cpu sh             *
bob         0.12 cpu sh
bob         0.15 cpu man
bob         0.03 cpu cat
bob         0.01 cpu sh             *
bob         0.10 cpu gtbl
bob         1.81 cpu troff
bob         0.10 cpu less
bob         0.37 cpu grotty
bob         0.08 cpu groff
bob         0.05 cpu sh             *
bob         0.08 cpu sh
bob         0.08 cpu man
bob         0.03 cpu cat
bob         0.02 cpu sh             *
bob         0.08 cpu gtbl
bob         1.61 cpu troff
bob         0.21 cpu less
bob         0.32 cpu grotty
bob         0.09 cpu groff
bob         0.03 cpu sh             *
bob         0.09 cpu sh
bob         0.14 cpu man
bob         0.05 cpu ls
bob         0.08 cpu netstat
bob         0.33 cpu ps
```

Connect-Time Accounting

- ac
  - report on connect time (in hours) based on the logins/logouts noted in the current /var/log/wtmp file
    - *maintained by init and login. Neither of these creates the file; if it doesn't exist, no accounting is done*
  - simpler than sa
    - *intended for a different task*
      - probably more generally useful…
    - *still has a fairly large number of options, though!*

```
[ -d | --daily-totals ] [ -y | --print-year ]
[ -p | --individual-totals ] [ people ]
[ -f | --file filename ] [ -a | --all-days ]
[ --complain ] [ --reboots ] [ --supplants ]
[ --timewarps ] [ --compatibility ]
[ --tw-leniency num ] [ --tw-suspicious num ]
[ -z | --print-zeros ] [ --debug ]
[ -V | --version ] [ -h | --help ]
```

Ac Reports

- useful options:
  - -y: print year
  - -d: print daily totals
  - -p: per-user statistics

```
# ac -d -p -y
                bob                                     3.30
Nov  7 1998     total        3.30
                root                                    3.44
                bob                                    16.84
Nov  8 1998     total       20.27
                bob                                     4.46
Nov  9 1998     total        4.46
                bob                                     4.46
Nov 10 1998     total        4.46
                bob                                     1.86
Nov 14 1998     total        1.86
                root                                    0.45
Nov 17 1998     total        0.45
                bob                                     5.61
Nov 18 1998     total        5.61
                bob                                     0.75
Nov 21 1998     total        0.75
                bob                                     3.94
Nov 22 1998     total        3.94
                bob                                     0.51
Nov 23 1998     total        0.51
                bob                                     1.75
Nov 24 1998     total        1.75
                bob                                     4.40
Nov 25 1998     total        4.40
                bob                                     3.20
Nov 26 1998     total        3.20
                root                                    5.23
                bob                                     4.15
Nov 27 1998     total        9.38
                root                                   17.45
                bob                                     5.50
Today           total       22.95

# ac -p
        root                                   26.53
        bob                                    60.62
        total       87.15
```

Last And *Lastb*

- displays a list of all users logged in (and out) since /var/log/wtmp was created
  - names of users and ttys can be given, in which case last will show only those entries matching the arguments
  - the pseudo user reboot logs in each time the system is rebooted; *last reboot* will show a log of all reboots since the log file was created
- lastb
  - the same as last, except that it looks at /var/log/btmp, which contains all the bad login attempts
    - *file may not exist if this information is not wanted*

```
# last bob
bob      ttyp2        aunty      Sat Nov 28 14:50   still logged in
bob      ttyp0        aunty      Sat Nov 28 14:33   still logged in
bob      ttyp0        aunty      Fri Nov 27 18:36 - 20:05  (01:28)
bob      ttyp1        aunty      Fri Nov 27 16:52 - 18:10  (01:17)
bob      ttyp0        aunty      Fri Nov 27 16:47 - 18:10  (01:22)
[snip]
bob      ttyp1        aunty      Sat Nov  7 21:41 - 08:36  (10:55)
bob      ttyp0        aunty      Sat Nov  7 20:50 - 21:49  (00:58)

wtmp begins Sat Nov  7 20:50:32 1998
```

```
# last reboot
reboot   system boot      Wed Nov 25 02:47
reboot   system boot      Mon Nov 23 21:05
reboot   system boot      Sun Nov 22 20:41
reboot   system boot      Sat Nov 21 14:15
reboot   system boot      Wed Nov 18 17:35
reboot   system boot      Tue Nov 17 20:54
reboot   system boot      Sat Nov 14 10:10
reboot   system boot      Tue Nov 10 07:43
reboot   system boot      Mon Nov  9 18:56

wtmp begins Sat Nov  7 20:50:32 1998
```

SysV Accounting Facility

- **ignore!**
  - *"System V accounting is much more elaborate than under BSD. It is a complex system of commands, and shell scripts and C programs, called by one another in long sequences, all purported to be totally automated and requiring little or no intervention. In reality, it's a design only a fervent partisan could love. The manual pages alternate between assuring the reader that the system is robust, reliable and trouble-free and describing convoluted procedures for patching corrupted accounting data files. Be forewarned."*
  - *(see p.675, Frisch)*
  - it doesn't actually *do* more than the BSD style accounting scheme does
    - reflects SysV's design-by-committee approach :(

Other Accounting

- **printing**
  - pac
  - we'll look at this when we cover printing
- **applications, databases, etc. may also maintain accounting information**
  - many network systems maintain accounting for security purposes
    - *especially samba, web & ftp servers*
      - look at these later

Log Maintenance

- **many logs will grow without limit unless maintained**
  - responsibility of the administrator to deal with these
    - write a shell script to do cleanup, etc.
- **logrotate**
  - facility to deal with log maintenance
    - *allows automatic rotation, compression, removal, and mailing of log files*
    - *customizable: each log file may be handled daily, weekly, monthly, or when it grows too large.*
  - standard framework means you don't need to write your own scripts
  - normally run from a cron job
    - *will not modify a log multiple times in one day unless the criteria for that log is based on it's size and logrotate runs multiple times each day*

Logrotate Configuration

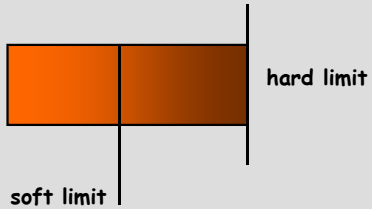
```
# /etc/logrotate.conf
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# send errors to root
errors root

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    rotate 1
}

/var/log/lastlog {
    monthly
    rotate 1
}

# other stuff
/var/log/httpd/access.log {
    rotate 5
    mail www
    errors www
    size=100k
    postrotate
      /usr/bin/killall -HUP httpd
    endscript
}
```

```
# /etc/logrotate.d/syslog
/var/log/messages {
    postrotate
        /usr/bin/killall -HUP syslogd
    endscript
}

/var/log/secure {
    postrotate
        /usr/bin/killall -HUP syslogd
    endscript
}

/var/log/maillog {
    postrotate
        /usr/bin/killall -HUP syslogd
    endscript
}

/var/log/spooler {
    postrotate
        /usr/bin/killall -HUP syslogd
    endscript
}
```

Quota Management

- *"…designed to let users have large temporary files, provided that long-term they obey a much stricter limit."*
- **an optional package**
  - usually installed into the kernel alongside accounting
- **has a bad reputation for slowing the system down**
  - once maybe, but not with today's hardware…

Two Kinds Of Quota



- **hard limit**
  - can never be exceeded: programs that try to get storage are given an error indication
- **soft limit**
  - gives a warning but allows limit to be exceeded for a specified period of time
    - *user may logout but will be warned on login*
    - *eventually, system will not let user allocate more space and may not let the user logout until he/she is back below the soft limit*
- **two things can be limited**
  - inodes
    - *can restrict the number of files a user can create*
  - blocks
    - *can restrict the size of data stored by the user*
- **quotas operate on a per-filesystem basis**
  - user may fill up one filesystem but have plenty of space on another

Files

- quota information is held in a file called *quotas* at the root of *each* filesystem
  - for linux, there are two files: *quota.group* and *quota.user*
    - *only AIX, Digital UNIX and Linux allow group-based quotas*
- qoutas are only maintained if a filesystem is marked in /etc/fstab

```
/dev/sdb1       /home      ext2     rw,usrquota,grpquota        1 2
```

- quotas are typically started at boot time
  - from /etc/rc.d/rc.sysinit

```
echo "Turning on user and group quotas for local filesystems"
/sbin/quotaon -a
```

  - quotas are also checked at boot time

```
/sbin/quotacheck -v -R -a
```

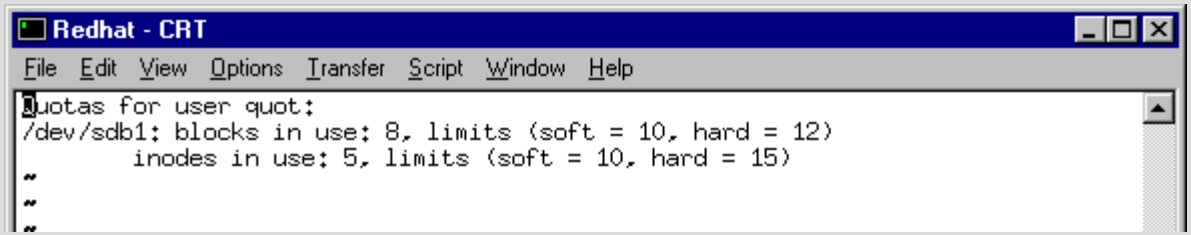
- can be stopped at any time with quotaoff

Reporting And Editing Quotas

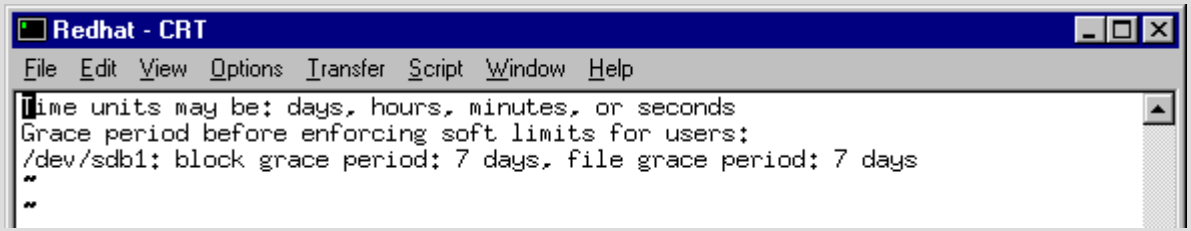
- repquota is used to report the current status

```
# repquota /home
                        Block limits                File limits
User            used soft hard    grace   used soft  hard     grace
root    --      916    0    0              182    0     0
bob     --    81198    0    0             1550    0     0
pcguest --        8    0    0                5    0     0
quot    -+        8   10   12               15   10    15     7days
```

- edquota is used to edit a user's quota limits
  - need to use this, since the quota files are binary and can't be edited by hand



  - edquota -t sets the soft time limits



A Simple Example

- shows an inode limit being reached

```
$ for i in 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
> do
> echo touching $i
> touch $i
> done
touching 1
touching 2
touching 3
touching 4
touching 5
touching 6
/home: warning, user file quota exceeded
touching 7
touching 8
touching 9
touching 10
touching 11
/home: write failed, user file limit reached
touch: 11: Disc quota exceeded
touching 12
touch: 12: Disc quota exceeded
touching 13
touch: 13: Disc quota exceeded
touching 14
touch: 14: Disc quota exceeded
touching 15
touch: 15: Disc quota exceeded
touching 16
touch: 16: Disc quota exceeded
touching 17
touch: 17: Disc quota exceeded
$ ls -a
.             .bash_profile  2             6
..            .bashrc        3             7
.Xdefaults    1              4             8
.bash_logout  10             5             9
```