Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Understanding /var/account/pacct OR /var/account/acct – Acct File Format

Posted by Vivek Gite <vivek@nixcraft.com>

Q. Can you explain /var/account/pacct or /var/log/account/pacct file under Linux / UNIX operating systems?

A. A acct file (/var/account/acct or /var/account/pacct) format is common in UNIX / Linux / BSD operating systems. The kernel will start the process accounting and stores in /var/account/pacct or /var/log/account/pacct file which the system wide **unix process accounting** or **unix accounting file** for UNIX / Linux like operating systems. The location and name of the file depends upon UNIX / Linux variant: [1]

- FreeBSD / OpenBSD default accounting file: **/var/account/acct**
- Red Hat / RHEL / CentOS / Fedora Linux : **/var/account/pacct**
- Debian / Ubuntu Linux : **/var/log/account/pacct**
- Sun Solaris UNIX default accounting file : **/var/adm/pacct**

accton command

The accton utility is used for switching system accounting on or off. If called with the argument acctfile, system accounting is enabled. The acctfile specified must exist prior to starting system accounting, or accton will return an error. You can run accton as follows:

```
# accton /path/to/file
# accton /var/account/acct
```

Under Red Hat / CentOS Linux, you can enter following command to start accounting service:

```
# chkconfig [2] psacct on
# /etc/init.d/psacct
```

Under Ubuntu / Debian Linux, you need to enter following command to start accounting service:

```
# update-rc.d [3] acct defaults
/etc/init.d/acct start
```

acct file format

The kernel maintains the following acct information structure for all processes. If a process terminates, and accounting is enabled, the kernel calls the acct(2) function call to prepare and append the record to the accounting file.

```
#define AC_COMM_LEN 16

     /*
      * Accounting structure version 2 (current).
      * The first byte is always zero.
      * Time units are microseconds.
      */

     struct acctv2 {
             uint8_t  ac_zero;               /* zero identifies new version */
             uint8_t  ac_version;            /* record version number */
             uint16_t ac_len;                /* record length */

             char     ac_comm[AC_COMM_LEN]; /* command name */
             float    ac_utime;              /* user time */
             float    ac_stime;              /* system time */
             float    ac_etime;              /* elapsed time */
```

```
        time_t    ac_btime;             /* starting time */
        uid_t     ac_uid;               /* user id */
        gid_t     ac_gid;               /* group id */
        float     ac_mem;               /* average memory usage */
        float     ac_io;                /* count of IO blocks */
        __dev_t   ac_tty;               /* controlling tty */

        uint16_t ac_len2;               /* record length */
        union {
                __dev_t   ac_align;     /* force v1 compatible alignment */

#define AFORK   0x01                    /* forked but not exec'ed */
/* ASU is no longer supported */
#define ASU     0x02                    /* used super-user permissions */
#define ACOMPAT 0x04                    /* used compatibility mode */
#define ACORE   0x08                    /* dumped core */
#define AXSIG   0x10                    /* killed by a signal */
#define ANVER   0x20                    /* new record version */

                uint8_t  ac_flag;       /* accounting flags */
        } ac_trailer;

#define ac_flagx ac_trailer.ac_flag
};
```

If a terminated process was created by an execve(2), the name of the executed file (at most ten characters of it) is saved in the field ac_comm and its status is saved by setting one of more of the following flags in ac_flag: AFORK, ACOMPAT, ACORE and ASIG. ASU is no longer supported. ANVER is always set in the above structure.

How do I use acct file?

You need to use acct file using lastcomm or sa command. Please see following article for practial usage of acct file:

- How to keep a detailed audit trail of what's being done on your Linux systems [4]

Recommended readings:

Refer to man pages and acct.h header file:

```
man 5 acct
man 1 lastcomm
man 2 acct
man 2 execve
man 8 sa
man 1 accton
vi /usr/include/linux/acct.h [5]
vi /usr/include/sys/acct.h [6]
```


URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/linux/**
[2] chkconfig: **http://www.cyberciti.biz/faq/rhel5-update-rcd-command/**
[3] update-rc.d: **http://www.cyberciti.biz/faq/howto-runlevel-configuration-tool-to-start-service/**
[4] How to keep a detailed audit trail of what's being done on your Linux systems: **http://www.cyberciti.biz/tips/howto-log-**

user-activity-using-process-accounting.html

[5] /usr/include/linux/acct.h: **http://www.cyberciti.biz/files/dev/acct.h.linux.txt**

[6] /usr/include/sys/acct.h: **http://www.cyberciti.biz/files/dev/acct.h.bsd.txt**
