Enabling Process Accounting on Linux HOWTO

Albert M.C. Tam

bertie@scn.org

Kristin Thomas – Converted document from HTML to DocBook v4.1 (SGML)

2001−02−09

Revision History

Revision 1.1	2001−02−09	Revised by: KET
Revision 1.0	1997−08−08	Revised by: AMCT

Describes the basics of enabling process accounting on Linux.

Table of Contents

1. Preamble........1

2. Introduction........2

3. What is process accounting?........3

4. Current Status of Process Accounting under Linux........4

5. Requirements for Process Accounting on Linux........5
- 5.1. Kernel........5
- 5.2. Process Accounting Software........5

6. Process Accounting Setup on Linux........6

7. Miscellaneous Process Accounting Commands........7

1. Preamble

2. Introduction

This document describes how to enable system process accounting on a Linux host and the usage of various process accounting commands. It is intended for users running kernel versions greater than or equal to 1.3.73 (tested on RedHat" 4.1 kernel 2.0.27). Kernels older than 1.3.73 may need a patch in order to use the process accounting feature.

Feel free to send any feedback or comments to bertie@scn.org if you find an error, or if any information is missing. I appreciate it.

---

3. What is process accounting?

Process accounting is the method of recording and summarizing commands executed on Linux. The modern Linux kernel is capable of keeping process accounting records for the commands being run, the user who executed the command, the CPU time, and much more.

Process accounting enables you to keep detailed accounting information for the system resources used, their allocation among users, and system monitoring.

4. Current Status of Process Accounting under Linux

Process accounting support has been integrated into the newer kernels (version >= 1.3.73). If you are running an older kernel, you may need some patch files. The patches are available from ftp://iguana.hut.fi/pub/linux/Kernel/process_accounting

5. Requirements for Process Accounting on Linux

5.1. Kernel

A Linux kernel version greater than or equal to version 1.3.73 is required, and I recommended 2.x. The kernel source is available from http://sunsite.unc.edu/pub/Linux/kernel/v2.0

5.2. Process Accounting Software

Depending on the Linux distribution you have, you may not have the process accounting software package installed on your system. If you don't have it, try downloading the package from http://sunsite.unc.edu/pub/Linux/system/admin/quota−acct−modified.tgz

6. Process Accounting Setup on Linux

1. Compile and install process accounting software.

   The process accounting software package is available from http://sunsite.unc.edu/pub/Linux/system/admin/quota−acct−modified.tgz

2. Modify your system init script and turn on process accounting at boot time.

   Here's an example:

   ```
   # Turn process accounting on.
   if [ -x /sbin/accton ]
   then
                   /sbin/accton /var/log/pacct
                   echo "Process accounting turned on."
   fi
   ```

3. Create accounting record file "`pacct.`"

   Your process accounting software will print out all commands executed to the file `/var/log/pacct` by default.

   To create the accounting record file:

   ```
   touch /var/log/pacct
   ```

   This record file should be owned by root, and it has read−write permission for root and read permission for anybody else:

   ```
   chown root /var/log/pacct
   chmod 0644 /var/log/pacct
   ```

4. Reboot.

   Now reboot your system for changes you made to take effect.

7. Miscellaneous Process Accounting Commands

ac

ac prints out statistics about users' connection times in hours based on the logins and logouts in the current `/var/log/wtmp` file. **ac** is also capable of printing out time totals for each day (–d option), and for each user (–p option).

accton

accton is used to turn on or turn off process accounting. The file is normally executed at system bootup or shutdown via system init scripts.

last

last goes through the `/var/log/wtmp` file and prints out information about users' connection times.

sa

sa summarizes accounting information from previously executed commands, software I/O operation times, and CPU times, as recorded in the accounting record file `/var/account/pacct`.

lastcomm

lastcomm prints out the information about all previously executed commands, recorded in `/var/account/pacct`.