

System Accounting

By Micah Altman

Revision: May. '97
Copyright 1993-7

System Accounting

- What is system accounting?
- Why use these services?
- How do I set up these services?
- Fixing problems
- Further information

Monitoring Your System More Closely

- Use system accounting to record the use of programs on your system:
 - processes being executed on your system
 - data (i/o) throughput for each process
 - processes being run by a particular user
 - resource use by each user
- Use auditing to record changes to your system
 - changes in file data and attributes
 - changes to system configuration
 - changes to authentication
 - changes in communication channels
- Use performance analysis to look at bottlenecks on the system
 - Use logs, and availmon to look at stability of your system

Why monitor your system with accounting?

Accounting information helps with other tasks:

- Troubleshooting
 - know what was running when a problem occurred
 - know what changed when a problem occurred
- Tuning
 - know what is running when a system bottleneck occurs
 - determine if any users are “hogging” the system
 - combine with system performance profiling (sar)
- Security
 - look for high levels of activity

How to set up accounting

- Installation
 - Subsystems:* use `inst` to install `coe2.sw.acct`
- Activation
 - Turning it on/off:* `chkconfig acct [on|off]`
 - Immediate start* `/usr/lib/acct/startup`
 - Immediate stop:* `/usr/lib/acct/shutacct`
- Configuration
 - No configuration necessary. But you may change the following kernel variables (using `sysctl`) to enable extended accounting:
 - `do_extpacct` : do extended process accounting
 - `do_sessacct` : do array session accounting

How accounting works

- What it does
 - IRIX kernel writes a record for each process
 - login and init write records for each logins, startups, reboots, etc.
 - accounting scripts are run by cron to analyze data
- Special programs
 - daily accounting:* `/usr/lib/acct/runacct`
 - monthly accounting:* `/usr/lib/acct/monacct`
 - space saver:* `/usr/lib/acct/ckpacct`
 - disk usage checker:* `dodisk`
- System files
 - process accounting records:* `/var/adm/pacct`

login and shutdown records: /etc/wtmp

- Log files

Daily Log: /var/adm/acct/nite/activeMMDD

Running Log: /var/adm/acct/nite/log

Interpreting Accounting Reports

- Generating reports

daily reports: run /usr/lib/acct/prdaily

monthly reports: automatically generated by /usr/lib/acct/monacct

storage: /var/adm/acct/sum

- What to look for

- user activity

cpu minutes: CPU

core memory: KCORE

disk blocks: DISK BLOCKS

- commands

of times executed: NUMBER COMMANDS

resource use: KCORE, CPU, HOG FACTOR

throughput: CHARS TRANSFRD, BLOCKS READ, REAL-MIN

- system behavior

reboots, shutdowns, crashes

Fixing problems

- Monitoring can reduce system performance

- disk space

- disk and cpu performance

- Common causes of monitoring failures

- system crashes

- corrupted system records

/var/adm/pacct

/etc/wtmp

- fixing problems

- disk space

accounting files: are removed automatically when space use > 2000 blocks

- performance

gather only the data that you need

- corrupted data files or failures

repair

check log files
backup and restore
remove and start over
start satd in “verbose” mode with the -v flag

Lab

Goals

This lab introduces the reader to system accounting and auditing. At the end of this lab the user will be able to perform the following tasks:

- Enable process accounting
- Create daily system use reports

Starting

- Log in as “root”

Lab Instructions

XX.1 Process Accounting

- enable process accounting (chkconfig acct on)
- start process accounting (/usr/lib/acct/startup)
- generate system activity (./activity)
- force the system to run accounting
(/usr/lib/acct/dodisk
/usr/lib/acct/runacct)
- print the daily report to a local file
(/usr/lib/acct/prdaily > acct_file)
- Look in this file. What resources did “activity” use?
Memory CPU Disk

XX.3 Performance Effects

- time the program “activity” :
real____ user____ sys____
- stop accounting
(/usr/lib/acct/shutacct)
- time the program “activity” :
real____ user____ sys____
- is there a difference in these times?

XX.4 Cleaning Up

- stop accounting (/usr/lib/acct/shutacct)
- remove accounting files