System Accounting — General Information

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

About this Document

This document contains information on various aspects of system accounting for all levels of AIX 3.2.

Documentation . . . 1
Setting Up System Accounting . . . 1
The Information Generated by System Accounting . . . 2
How System Accounting is Initiated . . . 2
System Accounting Directories . . . 3
Space in /var for System Accounting . . . 3
  More Detail about Space Used in /var . . . 3
Daytime Processes . . . 3
Nighttime Processes . . . 4
Common Problems . . . 4
System Accounting Error Information . . . 4
About the Accounting Programs . . . 5
  dodisk . . . 5
  ckpacct . . . 5
  runacct . . . 5
  monacct . . . 5
Detailed Information about runacct . . . 5
  Before the States Begin . . . 6
  SETUP — Basic Setup of Files to be Used . . . 6
  WTMPFIX — Fix Any Corruption in the wtmp File . . . 7
  CONNECT1 — Produce Connect Time Info in ctmp.h Format . . . 7
  CONNECT2 — Convert ctmp.h Records to tacct Records . . . 7
  PROCESS — Create Process Accounting Info . . . 7
  MERGE — Merge the ctacct and ptacct Files Together . . . 7
  FEES — Merge in Fee Accounting Info . . . 8
  DISK — Merge in Disk Accounting Info . . . 8
  QUEUEACCT — Merge in Queue Accounting Info . . . 8
  MERGEACCT — Create Daily tacct Files . . . 8

CMS — Create Command Summaries 8
USEREXIT — Run Any Extra Accounting Programs 9
CLEANUP — Clean Up Temp Files and Write Daily Report 9
Detailed Information about monacct 9
Additional Accounting Possibilities 9
Reader's Comments 11

Documentation

System accounting, which comes from BDS or System V, is documented in chapter 14 of the System Management Guide or in InfoExplorer.

You can also find additional information in the following book:

UNIX Administration Guide for System V
(Chapter 7 is on System Accounting)
by Rebecca Thomas and Rik Sarrow
Publisher: Prentice and Halo
ISBN 0-13-942889-5

Setting Up System Accounting

If the accounting LPP is not installed, you will need to install it before setting up system accounting. The LPP is bosext2.acct.obj.

Information on setting up system accounting can be found in the following document from 1-800-IBM-4FAX (outside the U.S. call (415) 855-4329 from a fax machine phone):

2486 Setup of System Accounting in AIX 3.2

The description of accounting setup in InfoExplorer and the manuals may not be as up-to-date as the above fax. The fax includes the use of an "adm" user to run the accounting programs.

The Information Generated by System Accounting

Accounting generates daily reports in /var/adm/acct/sum. The file names are rprtMMDD, where MM is the month and DD is the date.

The first of each month, a monthly report will be created and the daily reports will be removed. This will be in /var/adm/acct/fiscal and will be called fiscrptMM, where MM is the month. The report will be for the previous month. For example, fiscrpt02 is the monthly report for January.

The reports contain the following information:

- Lineuse — Amount of time spent on each line (tty, pts), percent of time on line, number of sessions on line, number of logons, and number of logoffs.

- Daily usage report — Shows per user the following:
  - Minutes of CPU used, PRIME and NONPRIME
  - Average kilobytes of memory (KCORE), PRIME and NONPRIME
  - Minutes of CONNECT TIME during PRIME and NONPRIME
  - Number of DISK BLOCKS used (from dodisk)
  - Amount of FEES (if computing)
  - Number of PROCESSES
  - Number of SESSIONS
  - Number of DISK SAMPLES
- Daily command summary — Shows per command the following:
  - Number of times command was run
  - Total KCOREMIN (average kilobytes of memory used times the number of minutes the program ran, the product of the total CPU time, and the mean size in kilobytes)
  - Total CPU minutes
  - Total Real minutes
  - Mean size in kilobytes (memory)
  - Mean CPU time in minutes
  - Hog factor
  - Characters transferred
  - Blocks read
- Monthly command summary — Same as daily command summary
- Last login information

How System Accounting is Initiated

Follow the steps in the fax for setting up accounting (mentioned in the section "Setting Up System Accounting"). The steps include:

- Adding a call to /usr/sbin/acct/startup in /etc/rc to cause accounting data collection to be started when the machine is rebooted.
- Adding crontab entries to run accounting reports.

System Accounting Directories

/usr/sbin/acct	All accounting programs
/usr/lib/acct	Files linked to /usr/sbin/acct
/var/adm	wtmp, pacct, and qacct files
/var/adm/acct/fiscal	Monthly reports
/var/adm/acct/nite	Working directory for nighttime accounting processes
/var/adm/acct/sum	Daily reports

Chapter 14 in the System Management Guide briefly describes each file in these directories.

Space in /var for System Accounting

Accounting will cause /var to grow. Running accounting with defaults takes one physical partition (4MB) in /var. You may wish to increase this to at least two physical partitions (8MB). Monitor /var to see if you need to increase the size. Accounting is not the only reason that /var may be full; the queueing system is also in /var and may especially take up space if a lot of printing is done.

More Detail about Space Used in /var

Each command that is run adds 40 bytes to the pacct file. So, 25000 commands a day requires 1 MB of free space in /var for the pacct files. This space is freed nightly.

The daily reports could require anywhere from 1-3 MB throughout the month. This space is freed at the end of each month. The monthly reports should require less than 1 MB of free space throughout the year. These numbers will vary with the amount of activity on the system.

Daytime Processes

Logins and logouts are logged in /var/adm/wtmp. It's cleared out nightly by runacct. If accounting isn't running, this file will grow. This file does not have to exist if you're not running accounting, but it is useful. To see an ASCII version of wtmp, /etc/utmp, or /etc/security/failedlogin, use the fwtmp command.

All daily process activity is logged in /var/adm/pacct. Each process completed increases this file by 40 bytes. For heavily used systems, this file can use large amounts of space in /var.

/usr/sbin/acct/ckpacct checks the size of /var/adm/pacct and the amount of free space in /var. It is run from cron and should be run at intervals appropriate for your system.

If /var/adm/pacct is over 1000 blocks, ckpacct will switch the pacct file. This means it will copy pacct to pacct# (# starts with 1 and increases to the next unused number) and clear out pacct again.

If the free space in /var falls below 500 blocks, then ckpacct turns off accounting until space is made available. This will result in loss of accounting data during the period that accounting is turned off. ckpacct will turn accounting on again when more space is available. **There is no notification** unless you set the MAILCOM variable.

```
MAILCOM="mail user_name"
```

You can set it in the ckpacct script or somewhere in the shell, such as in /etc/profile or /etc/environment. If MAILCOM is set in both places, the setting in chkpacct is used.

Nighttime Processes

Accounting is kicked off by cron, usually during the late hours of the day (if set up according to the setup fax). The scripts that are usually run at night are:

dodisk Analyzes the amount of disk usage per user

runacct Creates the daily reports

monacct Runs once a month to create monthly reports from daily ones

These scripts will be explained in more detail later in this document.

Common Problems

Information about known problems with accounting is available in the following document from 1-800-IBM-4FAX (outside the U.S., call 415-855-4329 from a fax machine phone):

2486 Setup of System Accounting in AIX 3.2

System Accounting Error Information

/var/adm/acct/nite/accterr will contain the most system accounting error information.

/var/adm/acct/nite/active will contain information about the steps that have been completed during the runacct script.

/var/adm/acct/nite/statefile lists the current state of runacct.

You probably will not receive any mail from cron because cron redirects output to the accterr file or to /dev/null; however, if you set up the cron jobs not to do this, you will get mail from cron.

Also, you will not get mail from the runacct script unless you uncomment the MAILCOM line in /usr/sbin/acct/runacct.

About the Accounting Programs

dodisk

dodisk performs disk usage accounting on all file systems that have "account = true" in /etc/filesystems. dodisk will create a file for use by runacct called /var/adm/acct/nite/dacct. The dodisk command needs to be started at least 10-30 minutes before runacct to allow it to complete before runacct starts. If the dacct file isn't finished before runacct tries to process it, then you will have bad data in the daily reports.

ckpacct

ckpacct checks /var to make sure it doesn't run out of space. It also makes sure that /var/adm/pacct doesn't get too large to be manageable, by renaming pacct to pacctxx and starting a new pacct file when pacct grows over 500 disk blocks. The normal interval for running ckpacct is once an hour. It should be run more often on systems that are heavily used. The more commands that are run, the faster the pacct files grow.

runacct

runacct will perform daily accounting and generate daily reports in the /var/adm/acct/sum directory. This command is divided into STATEs (procedures). If the process breaks, it can be started again at the correct STATE. You should not use any parameters when you call runacct unless you're trying to start the process over from a failed attempt. There is much more information below.

monacct

monacct will clean up daily reports and create a monthly report in /var/adm/acct/fiscal. There is more information on this below.

Detailed Information about runacct

The runacct command can take two arguments; however, they should only be used to start a runacct that previously failed. The documentation states that the command usage is

```
runacct [MMDD] [STATE ... ]
```

but the correct syntax is

```
runacct [MMDD [STATE]]
```

Before restarting runacct, refer to the "Restarting runacct Procedures" in InfoExplorer for **necessary** cleanup to be performed; otherwise, the runacct command will fail to run properly.

If you are restarting runacct, use the MMDD for the day that runacct was running (that is, if runacct failed on 0623, run "runacct 0623"). It will continue at the point of failure. You can also specify a certain STATE at which to start. This is only be necessary if you want to skip a STATE or redo one that has been done. The valid STATEs are:

```
SETUP
WTMPFIX
CONNECT1
CONNECT2
PROCESS
MERGE
FEES
DISK
QUEUEACCT
MERGETACCT
CMS
USEREXIT
CLEANUP
```

Any state other than these is invalid and generates errors in the active file.

The following sections list the actions during each state of runacct.

Before the States Begin

- Set the statefile for SETUP.
- Set up variables.
- Set up lock files.
- Check /var for sufficient space.

  Note: Since free space in /var is checked **only** at the beginning, running jobs that exhaust the space in /var (such as print jobs) may cause runacct to fail.

- Check for parameters that were passed in:
  - If one parameter, restart accounting for MMDD at the current STATE that is in statefile.
  - If two parameters, restart accounting for MMDD at specified STATE.

SETUP — Basic Setup of Files to be Used

- Write date and list of files to active file.
- Switch current pacct file.
- Move each pacct file to a file name of Spacct#.MMDD.
- Copy current wtmp file to nite/wtmp.MMDD.
- Append line with current time to end of nite/wtmp.MMDD.
- Clear current wtmp file.
- Write to active file that "file setups complete".
- Set the statefile for WTMPFIX.

WTMPFIX — Fix Any Corruption in the wtmp File

- Clear nite/tmpwtmp and nite/wtmperror.
- Run wtmpfix on nite/wtmp.MMDD.
  - Standard out goes to nite/wtmp.MMDD.
  - Standard error goes to nite/wtmperror.
- Write to active file that "wtmp processing complete".
- Set the statefile for CONNECT1.

CONNECT1 — Produce Connect Time Info in ctmp.h Format

- Clear the lineuse, reboots, ctmp, and log files in nite directory.
- Run acctcon1 against tmpwtmp (the new wtmp file).
  - Reboot info is written to reboots file (this is the 1st part of the daily report).
  - Lineuse info is written to lineuse file (this is the 2nd part of the daily report).
  - Connect time info is written to ctmp (ctmp.h format).
  - Errors are written to log file (shouldn't be any).
- Set the statefile for CONNECT2.

CONNECT2 — Convert ctmp.h Records to tacct Records

- Clear ctacct.MMDD file.
- Run acctcon2 with input from ctmp and output to ctacct.MMDD.
- Write to active file that "connect acctg complete".
- Set the statefile for PROCESS.

PROCESS — Create Process Accounting Info

- Run acctprc1 against each of the Spacct#.MMDD files.
  - Output to acctprc2, creating corresponding ptacct#.MMDD files.
  - Write to active file for each Spacct#.MMDD file.
- Write to active file that "all process acctg complete for MMDD".
- Set the statefile for MERGE.

MERGE — Merge the ctacct and ptacct Files Together

- Copy ctacct.MMDD file to daytacct.
- Merge each ptacct#.MMDD file into the daytacct file. (This is done with acctmerge and two temporary files — tmpdayt and daytacct.old.)
- Write to active file that "tacct merge to create daytacct complete".
- Set the statefile for FEES.

FEES — Merge in Fee Accounting Info

- If /var/adm/fee exists, then merge fee info into daytacct file.
- Write to active file that "fee processing is complete".
- Set the statefile for DISK.

DISK — Merge in Disk Accounting Info

- If /var/adm/acct/nite/dacct exists (from dodisk) then merge dacct into daytacct file
- Write to active file that "merged disk records".
- Set up statefile for QUEUEACCT.

QUEUEACCT — Merge in Queue Accounting Info

- If /var/adm/qacct exists then merge it into the daytacct file.
- Write to active file that "queueing system records complete".
- Set up statefile for MERGEACCT.

MERGEACCT — Create Daily tacct Files

- Copy nite/daytacct to sum/tacctMMDD file.
- Copy sum/tacct to sum/tacctprev.
- Merge sum/tacctprev and sum/tacctMMDD together into sum/tacct.
- Write to active file that "updated sum/tacct".
- Set up statefile for CMS.

CMS — Create Command Summaries

- Clear sum/daycms.
- Copy sum/cms to sum/cmsprev.
- Run acctcms against Spacct*.MMDD.
  - Output to sum/daycms (a binary file).
- Run acctcms against sum/daycms and sum/cmsprev.
  - Output to sum/cms (a binary file).
- Run acctcms against sum/daycms.
  - Output to nite/daycms (ASCII file).
- Run acctcms against sum/cms.
  - Output to nite/cms (ASCII file).
- Run lastlogin MMDD to update sum/loginlog.
- Write to active file that "command summaries complete".
- Set up statefile for USEREXIT.

USEREXIT — Run Any Extra Accounting Programs

- If /var/adm/siteacct exists, run it. siteacct should be a script to do additional accounting. It doesn't exist unless created.
- Set up statefile for CLEANUP.

CLEANUP — Clean Up Temp Files and Write Daily Report

- Clear /var/adm/fee.
- Remove Spacct*.MMDD.
- Run prdaily to create sum/rprtMMDD (daily report).
- Remove nite/lock.
- Remove nite/ptacct#.MMDD and nite/ctacct.MMDD.
- Remove nite/wtmp.MMDD, nite/wtmperrorMMDD, and nite/activeMMDD.
- Move nite/tmpwtmp to nite/owtmp.
- Write to active file that "system accounting completed at TIME".
- Set up statefile for COMPLETE.

Detailed Information about monacct

monacct performs these steps:

- Move sum/tacct to fiscal/tacctMM
- Remove sum/tacct*.
- Clear sum/tacct.
- Move sum/cms to fiscal/cmsMM.
- Clear sum/cms.
- Remove sum/rprt*.
- Create fiscal/fiscrptMM from fiscal/tacctMM.
- Append command summary to fiscal/fiscrptMM from fiscal/cmsMM.
- Append lastlogin info to fiscal/fiscrptMM from sum/loginlog.

Additional Accounting Possibilities

The daily report might be all that is needed; however, if you want to see commands a specific user ran, you can run acctcom. It generates a file with one line for each command run and indicates the time the command was run and who ran it. (See InfoExplorer for a complete list of flags for the acctcom command. Only the minimum syntax is used in the examples that follow.)

Since runacct deletes the pacct files, which are needed by acctcom, you need to either run acctcom first or save the pacct files before runacct is run.

If you run acctcom before runacct, use the following syntax to run acctcom. Note that the output will be rather large.

```
acctcom /var/adm/pacct* > somefile
```

If you wish to save the pacct files before runacct, the recommended method is to change runacct to save the files before it continues processing:

1. Become the adm user.
2. Run the following commands:

```
cd /var/adm
mkdir oldpacct     #(directory to save pacct files in)
```

3. Become the root user.
4. Start an edit session on /usr/sbin/acct/runacct.
5. Find the following line:

```
mv ${_i} S${_i}.${_date}
```

6. Just above the line that you found, add the following:

```
cp ${_i} /var/adm/oldpacct/${_i}
```

If you ran the modified runacct before acctcom, use the following syntax to run acctcom:

```
acctcom /var/adm/oldpacct/pacct* > somefile
rm /var/adm/oldpacct/pacct*
```

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

END OF DOCUMENT (accounting.cmd)