Problems With The /etc/utmp File

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

The /etc/utmp file is used by the who, w and uptime commands to display when the system was last booted and who is currently logged in. This document is describes possible solutions to a corrupted utmp file and is applicable to AIX versions 3.2 and 4.1.

The W Command Reports Incorrect Idle Time

If the w command shows idle time greater than the uptime of the system the following fixes should be installed:

```
For Version 3.2 - APAR IX51806
For Version 4.1 - APAR IX52141
```

Indicators of utmp Corruption

Corruption of the utmp file show up in two different ways:

1. The uptime and w command shows a time greater than 8000 days since the system was last booted.
2. Users are shown as still logged in when in fact they are not.

Both types of corruption can be caused by many reasons since both AIX commands and third party applications write to the utmp file.

Problem: Uptime greater than 8000 days

If record number 0 is overwritten by anyone (normally a third party program), the uptime shows up as greater than 8000 days.

Solution:

There is no way to correct the invalid boot time except by rebooting the system. The utmp file is created new with each boot.

To attempt to discover who or what overwrote the first entry in the file you can use:

```
/usr/sbin/acct/fwtmp < /etc/utmp  >/tmp/out
[ the fwtmp command must first be installed,
for AIX 3.2 install bosext2.acct.obj
for AIX 4.1 install bos.acct ]
```

To create a readable version of the utmp file and look at record 0. A valid entry looks something like this:

```
system boot 0 2 0000 0000 818538505 Sat Dec 9 13:48:25
CST 1995
```

Instead of the system boot entry, you will probably find a entry like:

```
jones pts/2 19193 7 0000 0000 818683926 Mon Dec 11 06:12:06
CST 1995
```

This would mean whatever program jones on pts/2 used to login with, corrupted the time stamp. A program should never overwrite the first two entries in the utmp file. You would have to talk with jones to see what he did. This is almost always caused by a third party program that is incorrectly writing to the utmp file or a corrupted file system where the data is invalid.

Users shown as logged in with who or w commands when

they are not currently logged in.

When a user logs into the system, the /usr/sbin/getty program writes a entry in /etc/utmp like:

```
AIX 3.2:
sandy pts/17 39667 7 0000 0000 818690973 Mon Dec 11
08:09:33 CST 1995
 *                      *
Field #1 = user's name
Field #2 = tty used to login on
Field #3 = PID (process id)
Field #4 = type of entry
AIX 4.1:
sandy pts/23 pts/23 7 42300 0000 0000 818973357
[more data..]   .
 *                             *
Field #1 = user's name
Field #2 = /etc/inittab id
Field #3 = tty used to login  on
Field #4 = type of entry
Field #5 = PID (process id)
```

The types of entries can be seen by examining the /usr/include/utmp.h file under ut_type. Type 7 is a USER_PROCESS.

When a user logs out, it is the responsibility of the last process running to update the entry in the utmp file. After a logout, the entry should look like:

```
AIX 3.2:
pts/17 39667 8 0000 0000 818690973 Mon Dec 11 08:09:33
CST 1995
*             *
AIX 4.1:
pts/23 pts/23 8 42300 0000 0000 818973357
[more data..[
*              *
```

The user name is erased and the state is changed from a 7 to a 8 (DEAD_PROCESS).

The who command will only show entries that are in state 7.

How to find out what program caused the corruption:

1. Set up auditing on writes to the utmp file.
2. Have cron do the who command each minute and send the results to a file.
3. When you notice corruption with the who or w command, check the cron output files to determine when the corruption occurred.
4. Look in the audit log to determine what process was writing to the utmp file at the time the corruption occurred.

   For an example of how to setup auditing to audit utmp, request document # 4824 from 800-IBM-4-FAX. Non U.S. call 415-855-4329 from a fax machine phone.

This is an example of an audit log output:

```
event      login  status   time                     command
---------- ------ -------  ----------------------   -------
UTMP_WRITE root   OK       Tue Dec 19 17:00:29 1995 telnetd
```

The example above shows that telnetd wrote to the file at 17:00:29.

Known Problems

1. For AIX 3.2:

   Fixed in AIX 3.2.5

   IX38013 Xterm (X11 Release 4) can corrupt utmp

   IX37873 w command hangs under AIX 3.2.4

   Fixed in AIX 3.2.5.1

   IX45401 Telnet corrupts utmp under certain circumstances

   IX44950 Rlogind does not write exit utmp entry in some cases

   IX43576 Init intermittently fails to write utmp entries

   IX43059 HCF does not clean up utmp file after logoff

   IX46168 Rlogin causes utmp corruption

   IX45319 /bin/logout believes corrupted utmp entries (caused by corrupted utmp)

   IX44956 Xterm does not mark utmp entry on exit

   IX46179 w command hangs when su - is used, 3.2.5 (caused by corrupted utmp) defect in ptydd drivers

   IX40003 Who -u piped to commands causes garbage with many users logged in (problem with the who command, utmp is ok)

   Fixed Post 3.2.5.1

   IX56333 w command hangs if the port was improperly closed. Not a utmp problem but a port problem, the fix is to timeout and check the rest of the ports.

2. For AIX 4.1

   Fixed in AIX 4.1.3

   IX49832 Telnetd may cause utmp corruption

   Fixed in AIX 4.1.4

   IX52089 Dscreen cannot write to utmp. Needs setuid root

   Fixed Post 4.1.4

   IX55358 PTY Slave Hangs at Drain Time

How to fix the utmp file

Rebooting clears the utmp file and is the recommended method of correcting the results of corruption.

The following is an awk script that can be used to **attempt** to clean out bad entries in the /etc/utmp file. It may not clean certain types of corruption and a reboot will be required to clean up the file.

Warning: Since the utmp file is constantly being changed, there is always the possibility that an attempt at correction (other than by rebooting) MAY corrupt the /etc/utmp file. This script is for AIX 3.2. See the NOTE in the script for the change needed for AIX 4.1 usage.

```
#!/usr/bin/ksh
# utmp_clean.awk
# 12/12/95
# awk script to clean out entries in the /etc/utmp file
# that have no current matching correct process in the
process table.
# This MUST be run by the root user, either from the
command line or
# from the root crontab entry.
#
if [ ! -s /usr/sbin/acct/fwtmp ]
then
# accounting not installed
print "Accounting must be installed first,
fwtmp file does not exist   "
exit
fi
#
SUM=1
NEWSUM=0
while [ "$SUM" != "$NEWSUM" ]
     do
          SUM=$(/usr/bin/sum /etc/utmp)
          /usr/sbin/acct/fwtmp </etc/utmp >/tmp/utmp.out
          ps au |awk '{print $2,$1,$7}' |grep -v USER >/tmp/ps.out
          NEWSUM=$(/usr/bin/sum /etc/utmp)
          # loop until the file is unchanged
          # on a busy system, this may take a long time.
     done
#
cat /tmp/utmp.out | awk '
# load the array
BEGIN {
counter=0
holder = ""
ss=1
while (ss == 1)
     {
     ss = (getline holder < "/tmp/ps.out")
     if (ss == 0)
          break
     n=split(holder,temp)
     combine=sprintf("%s %s",temp[2],
temp[3])
     lookup[temp[1]]=combine
     }
} # end of BEGIN section
{
if ((length($4) == 1) && ($4 == 7))
{
# NOTE: for the next line, the number in brackets is
# for AIX 3.2 only for AIX 4.1 change the
```

```
# [$3] to [$5]
     ps_name=lookup[$3]
if (length(ps_name)  > 0) #found a ps table entry
with same pid
{
# entry needs to be checked for accuracy
          # only if the name and tty match, write the entry
utmp_name=sprintf("%s %s",$1,$2)
     if ( ps_name == utmp_name)
     print $0
}
}
else # Not a entry to look at, just pass it along
{
          print $0
}
}' > /tmp/utmp.tmp
/usr/sbin/acct/fwtmp -ic </tmp/utmp.tmp  >/tmp/utmp.new
# Only if the /etc/utmp file is still unchanged from when
# we last looked will the file be overwritten with the
# updated copy.
#           WARNING WARNING WARNING
# There is a chance that this step may corrupt the
/etc/utmp file
# if a process changes it after we look and before we
can write it.
CURRENTSUM=$(/usr/bin/sum /etc/utmp)
if [ "$CURRENTSUM" = "$SUM" ]
     then
     /usr/bin/cp /tmp/utmp.new /etc/utmp
     print "utmp sucessfully updated on ",$(date)
     else
     print "utmp was too busy on ",$(date)," to update now,
try again later"
fi
rm /tmp/ps.out
rm /tmp/utmp.out
rm /tmp/utmp.tmp
rm /tmp/utmp.new
```

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 (utmp.problems.cmd, 4FAX# 2548)

DSMLBR529E 'KP' WOULD EXCEED MAXIMUM SIZE.
DSMMOM395I 'UTMPSUB' LINE 256: .LT
DSMMOM397I 'UTMPSUB' WAS IMBEDDED AT LINE 690 OF '.EDFIM'
DSMMOM397I '.EDFIM' WAS IMBEDDED AT LINE 10 OF '.IM'
DSMMOM397I '.IM' WAS IMBEDDED AT LINE 12 OF 'UTMP'
DSMBEG323I STARTING PASS 2 OF 2.
DSMLBR529E 'KP' WOULD EXCEED MAXIMUM SIZE.
DSMMOM395I 'UTMPSUB' LINE 256: .LT
DSMMOM397I 'UTMPSUB' WAS IMBEDDED AT LINE 690 OF '.EDFIM'
DSMMOM397I '.EDFIM' WAS IMBEDDED AT LINE 10 OF '.IM'
DSMMOM397I '.IM' WAS IMBEDDED AT LINE 12 OF 'UTMP'