

## Re: wtmp filling up

**Source:** <http://unix.derkeiler.com/Mailing-Lists/AIX-L/2005-05/0191.html>

---

**From:** Mark Ray (*raym\_at\_US.IBM.COM*)

**Date:** 05/23/05

Date: Mon, 23 May 2005 14:11:23 -0400  
To: aix-l@Princeton.EDU

Tom:

Two questions: 1) How long has this been going on? and 2) Can you correlate turning accounting on with the time wtmp started to grow rapidly? Alternatively, could someone else with root privilege have been experimenting with accounting?

BTW: Before you fill /var and your system caches, you can always just "touch" the wtmp file to zero it out.

Mark Ray  
IBM Global Services

Lamar Saxon  
<Lamar.Saxon@AMER  
ICREDIT.COM> To  
Sent by: IBM AIX aix-l@Princeton.EDU  
Discussion List cc  
<aix-l@Princeton.  
EDU> Subject

Re: wtmp filling up

05/23/2005 01:45  
PM

Please respond to  
IBM AIX  
Discussion List

To format wtmp for readability you need to use the fwtmp command, not the tail command like:

```
/usr/lib/acct/fwtmp < /var/adm/wtmp
```

Send the output of that for further analysis...

Re: wtmp filling up

AIX-L: Re: wtmp filling up

Lamar

From: IBM AIX Discussion List [mailto:aix-l@Princeton.EDU] On Behalf Of Tom Wood  
Sent: Monday, May 23, 2005 11:45 AM  
To: aix-l@Princeton.EDU  
Subject: wtmp filling up

My /var/adm/wtmp file is increasing in size very fast - 246 in about 15 minutes (from a > /var/adm/wtmp command).

File wtmp shows the file is a text file, but is it a special format? When I attempt to tail -f it, this is what I get:

```
aixdb:/var/adm# tail -f wtmp
BÃ'Ã_netmeeting.agg-ioraclej
```

```
BÃ'Ã_netmeeting.agg-ioraclejBÃ'Ã_netmeeting.agg-ioracle.Ã_j
B.
BÃ'netmeeting.agg-ioracle.
```

```
BÃ'netmeeting.agg-ioracleFBÃ'netmeeting.agg-ioracleFBÃ'neÃ^a
```

I recognize the -netmeeting.agg-Iâ™ as part of a w2k machine name, and oracle may be the user attempting to connect, but what/where is the other -stuffâ™ coming from?

Thanks.

Tom

\*\*\*\*\*

IMPORTANT: The information contained in this message is privileged and confidential. It is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, any dissemination or reproduction of it is strictly prohibited. If you have received this communication in error, please contact us at postmaster@Rezlink.com immediately. Thank you.

\*\*\*\*\*

Privileged and Confidential. This e-mail, and any attachments there to, is intended only for use by the addressee(s) named herein and may contain privileged or confidential information. If you have received this e-mail in error, please notify me immediately by a return e-mail and delete this e-mail. You are hereby notified that any dissemination, distribution or copying of this e-mail and/or any attachments thereto, is strictly prohibited.

Re: wtmp filling up