Linux: /var/log/wtmp - No such file or directory quick fix and why it might be missing on a server

Author : admin

If you have to occasionally log into some client old inherited (not installed by you) Linux servers on and just out of curiosity and for security sake dediced do a quick security (last user login) evaluation, e.g. issued the
last command just to find out you get the error:

```
last: /var/log/wtmp: No such file or directory
```

Perhaps this file was removed by the operator to prevent logging last info.

Then this might be a sure indicator that some **malicious script kiddie (hax0r)** activity has been run over the server or the ex-system administrator if fired recently decided to wipe out all his login tracks among with installing some other nasty **rootkit or backdoor.**

Under some circumstances the error might be caused also by ***badly written end user rotate script bugs (like shell or perl script) bugs or by a buggy deployment of Linux OS virtual machine.***
The **last: /var/log/wtmp: No such file or directory error** is likely to happen **on Ubuntu / Debian / Redhat / CentOS Linux distributions running on a Cloud PaaS service such as Amazon EC2, some of the Cloud services vendors do choose to explicitly remove /var/log/wtmp** for the reason that many of end customers are using their Linux VM servers **(**Xen Virtualization **/ OpenVZ /** LXC **- Linux Containers)** etc. irresponsibly and hence become a victim of script kiddie attacks and the failed logins attempts logged in /var/log/wtmp grow to many gigabytes.

Even some Linux distributions or system administrators of Linux server login hosts that has to keep tens of thousands of login records monthly or are concentrating on simplicity and on an attempt to reduce size has purposefully deleted the last login entry file `/var/log/wtmp` **file to save space.**

But anyways if you happen to be missing this file always bear in mind that you might have been a victim of intrusion and you better run chkrootkit and rkhunter

Run below commands to fix the missing *`/var/log/wtmp`*

```
touch /var/log/wtmp
chmod 0664 /var/log/wtmp
chown root:utmp /var/log/wtmp
```

On some Linux distributions such as Ubuntu and Fedora you might also want to create **/var/log/btmp** *(which is used to log failed login attempts to server)*

```
touch /var/log/btmp
chmod 0664 /var/log/btmp
chown root:utmp /var/log/btmp
```

Once the files are created the **last** command will start logging server in logins and logouts as it is supposed to be again, e.g.:

```
linux:~# last -15
root pts/0 192.168.0.15 Fri May 5 16:41 still logged in
...
```

This article was inspired by a prior article found on root.bg the site is in Bulgarian so unfortunately you might not be able to read it, but as a content and concept it is pretty similar to pc-freak.net, actually the site author ***Nikolay Nikolov*** *(known in Internet Relay Chat IRC under the pseudonym* ***Joni-B****,* happened to be an old friend from youth geek IT years :)

Enjoy