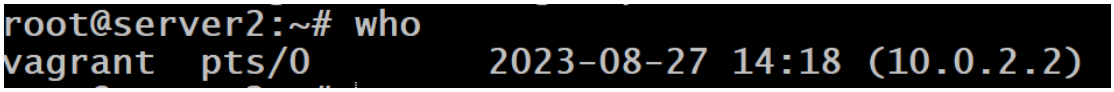
Monitor users

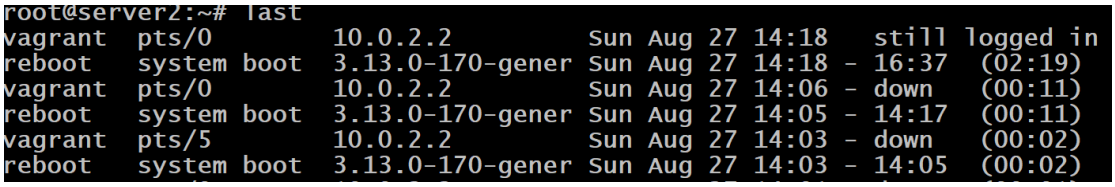
who command

who command is a tool print information about users who are currently logged in. who command only see a real user who
logged in.



Last

To view a list of recent user logins, simply run the last command



Options available with the last command include −

-a − Display the hostname of the system in the output.

-d − Display the DNS name of the host instead of the IP address.

-f − Use the specified file as the data source instead of the default file.

-i − Display the IP address of the host instead of the hostname.

-n − Limit the number of lines of output.

-R − Print the system's hostname and IP address in reverse DNS format.

-x − Show system reboot messages in the output.

Understand the Output

If we run the last command without any options, it will generate a history report of all accesses −

$ last
reboot system boot 5.5.13-arch2-1 Fri Apr 10 08:02 still running
kent pts/0 192.168.0.63 Tue Apr 7 22:01 - 23:03 (01:02)
reboot system boot 5.5.8-arch1-1 Tue Mar 10 20:49 - 20:49 (00:00)
kent pts/5 tmux(6716).%6 Thu Mar 26 18:58 - 19:01 (7+23:02)
root tty1 slash Fri Feb 21 18:45 - down (00:01)
kent pts/0 80.242.164.60 Thu Feb 20 11:39 - 11:43 (00:04)
guest pts/0 192.168.0.63 Sun Jan 26 19:15 - 21:32 (02:17)
kent pts/2 tmux(2044).%1 Wed Jan 8 22:39 - 01:09 (02:29)

Now, let's look at the access report generated above and understand the meaning of each column −

The first column shows the name of the logged in user.

The second column indicates how the user is connected to the system, for example via pts (pseudo-terminal) or tty (teletype). But if it was a restart task, it will show system boot.

The third column indicates where the user logged in from. The value could be −

a hostname or an IP address - if the user connected from a remote computer

empty value - if the user connected via a tty

a kernel version - if it is a reboot task

some application specific values, for example, tmux(6716).%6 means ProcessName(PID).WindowID

The fourth column indicates when the login activity occurred.

The fifth column shows the logout time. They can be the following values −

a timestamp − if the user logged out

still running − if the system startup is still running

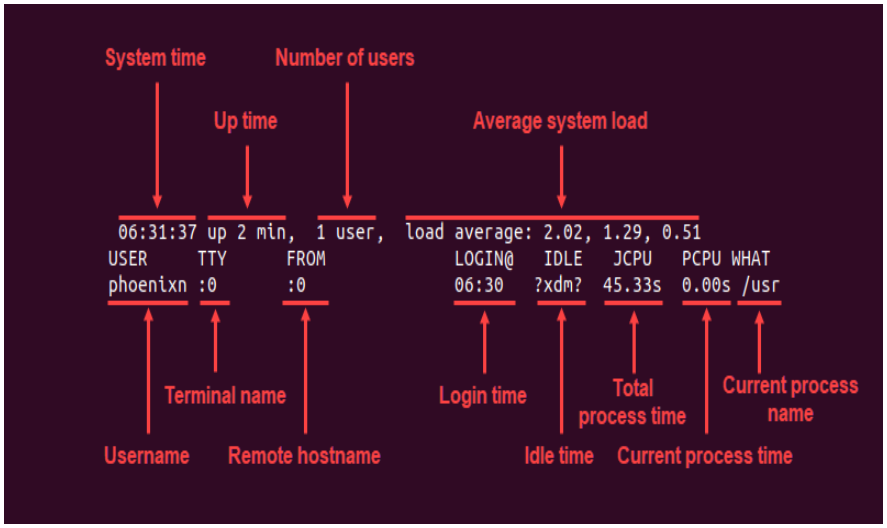
still logged in − if the user is still logged in

down − the system shuts down normally

crash − if there is no logout entry in the “/var/log/wtmp” file; this usually means that the system has crashed

w

The Linux w command is a system utility that displays information about currently logged-in users. It uses the following syntax:



The first line of the output shows system information:

- **System time:** The current system time.
- **Up time:** How long the system has logged in.
- **Number of users:** The number of users currently logged in.
- **Average system load:** The average number of jobs running on the system in the last 1, 5, and 15 minutes, respectively.

The second line shows user and process information:

- `USER`: The names of currently logged in users.
- `TTY`: The name of the terminal the user is logging in from.
- `FROM`: The name or IP address of the terminal or host the user is logging in from.
- `LOGIN@`: The time the user logged in, in a 24-hour format.
- `IDLE`: The time since the user last used the terminal; displays **?xdm?** if the user is currently active.
- `JCPU`: The total run time of all system processes attached to the user's terminal.
- `PCPU`: Elapsed time for the user's current process.
- `WHAT`: The name of the user's current process.

id

The id command is a basic Linux command used to confirm the identity of a specified Linux user. It is also used to find user and group names, along with the UID and GID of any user in Linux.

```
root@server2:~# id
uid=0(root) gid=0(root) groups=0(root)
```