

Linux sadservers

"Saint John": what is writing to this log file?

- `ps auxf`
- `lsof /path/to/file`
- `fuser /path/to/file`
- `pwdx PID: pwd del fichero PID`

1. You can use `ps` to list all processes and see if you see something related, for example with: `ps auxf`. Ignore system processes [in brackets].

A better way is to use the command to list open files: `lsof`.

2. Find the name (first column) and Process ID (PID, second column) of the process related to `/var/log/bad.log` by running `lsof` and filtering the rows to the one(s) containing `bad.log`.

You can also use the "fuser" command to quickly find the offending process: `fuser /var/log/bad.log`.

3. Run: `lsof |grep bad.log` and get the PID (second column). "Saint John": what is writing to this log file?

With the PID of the process, it's not necessary but we can find its current working directory (program location) by doing `pwdx PID` or for more detail: `lsof -p PID` and check the `cwd` row. This will allow us to check its ownership and perhaps inspect its offending code if it's a script (not a binary).

(Open window once more to see the complete solution).

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:seguridad:sadservers?rev=1715770494>

Last update: **15/05/2024 03:54**

