

# 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).

## "Saskatoon": counting IPs.

- `awk '{print $1}'`
- `cut -d' ' -f1`
- `sort: -h, numérico humano, -r reverso`
- `uniq -c: cuenta elementos únicos`

1. To get the first field (IP) of the file, you can do `awk '{print $1}' access.log` or using "cut" with delimiter of space (`-d' '`) and picking the first field (`-f1`): `cat access.log |cut -d' ' -f1`. You may want to append a pipe `| head` or `| tail` as you construct the command to see how your filters are working.

2. After the previous step, you want to sort the IPs so they are together and can be counted: `cat access.log | awk '{print $1}' |sort`

3. Now you want to do the count with "uniq -c", so we have so far: `awk '{print $1}' access.log |sort|uniq -c`

4. Finally you want to sort the results with "sort" (goes in ascending order) and get the latest one (with "tail -1" for example), or sort in reverse order with "sort -r" and get the top result: `awk '{print $1}' access.log|sort|uniq -c|sort -`

```
r|head -1.
```

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

Solution: One posible way is `awk '{print $1}' access.log|sort|uniq -c|sort -r|head -1|awk '{print $2}' > /home/admin/highestip.txt`

From:

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

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:seguridad:sadservers?rev=1715776670>

Last update: **15/05/2024 05:37**

