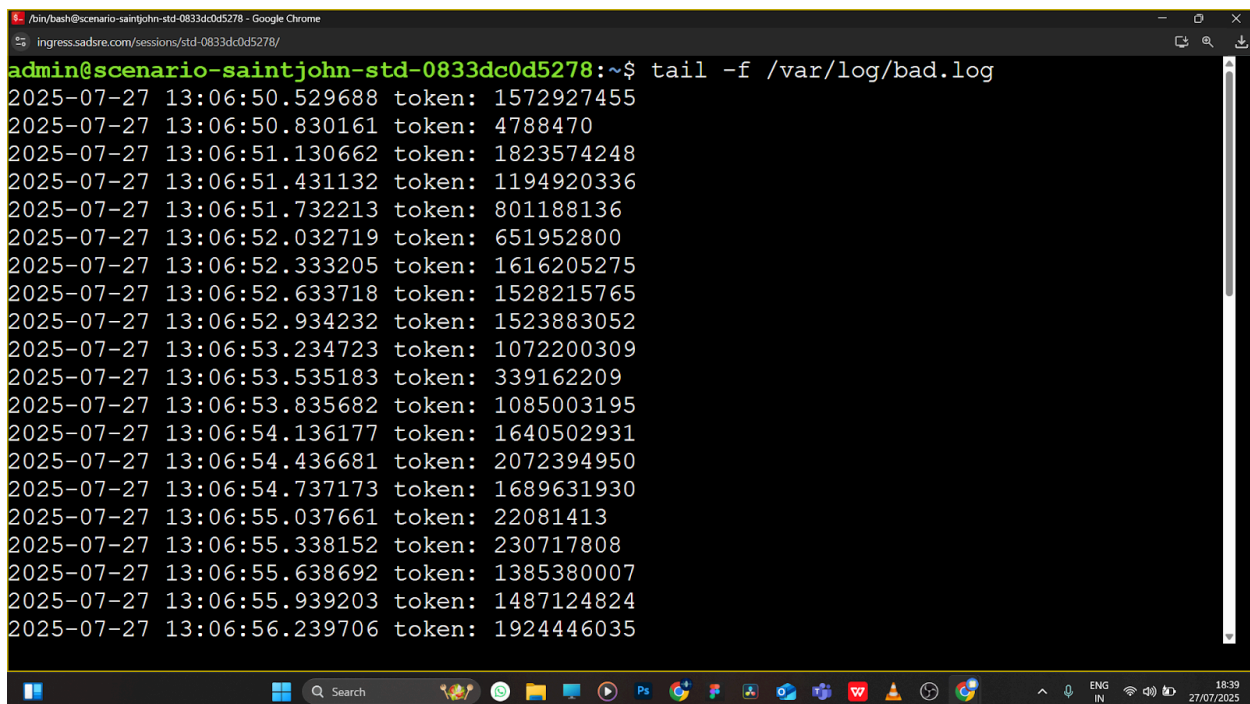


PROBLEM 1 : Saint John": what is writing to this log file?

Command to solve

- `ls -l /var/log/bad.log`
- `kill -9 7` --> 7 is the PID of the Process
- `bash /home/admin/agent/check.sh`
-

Detailed explanation as per Video : <https://youtu.be/HUOEJ12PspM>



```
admin@scenario-saintjohn-std-0833dc0d5278:~$ tail -f /var/log/bad.log
2025-07-27 13:06:50.529688 token: 1572927455
2025-07-27 13:06:50.830161 token: 4788470
2025-07-27 13:06:51.130662 token: 1823574248
2025-07-27 13:06:51.431132 token: 1194920336
2025-07-27 13:06:51.732213 token: 801188136
2025-07-27 13:06:52.032719 token: 651952800
2025-07-27 13:06:52.333205 token: 1616205275
2025-07-27 13:06:52.633718 token: 1528215765
2025-07-27 13:06:52.934232 token: 1523883052
2025-07-27 13:06:53.234723 token: 1072200309
2025-07-27 13:06:53.535183 token: 339162209
2025-07-27 13:06:53.835682 token: 1085003195
2025-07-27 13:06:54.136177 token: 1640502931
2025-07-27 13:06:54.436681 token: 2072394950
2025-07-27 13:06:54.737173 token: 1689631930
2025-07-27 13:06:55.037661 token: 22081413
2025-07-27 13:06:55.338152 token: 230717808
2025-07-27 13:06:55.638692 token: 1385380007
2025-07-27 13:06:55.939203 token: 1487124824
2025-07-27 13:06:56.239706 token: 1924446035
```

- `Tail -f <filename> -n 100`
- `Head <filename>`
- `cat <filename>`

```
./bin/bash@scenario-saintjohn-std-0833dc0d5278 - Google Chrome
ingress.sadsre.com/sessions/std-0833dc0d5278/
2025-07-27 13:06:54.436681 token: 2072394950
2025-07-27 13:06:54.737173 token: 1689631930
2025-07-27 13:06:55.037661 token: 22081413
2025-07-27 13:06:55.338152 token: 230717808
2025-07-27 13:06:55.638692 token: 1385380007
2025-07-27 13:06:55.939203 token: 1487124824
2025-07-27 13:06:56.239706 token: 1924446035
2025-07-27 13:06:56.540144 token: 1581453637
2025-07-27 13:06:56.840668 token: 1488083510
2025-07-27 13:06:57.141282 token: 832741981
^C
admin@scenario-saintjohn-std-0833dc0d5278:~$ cd /home/admin/
.bash_logout .bashrc .profile agent/ badlog.py
admin@scenario-saintjohn-std-0833dc0d5278:~$ cd /home/admin/agent/
check.sh sadagent sadagent.txt
admin@scenario-saintjohn-std-0833dc0d5278:~$ cd /home/admin/agent/
admin@scenario-saintjohn-std-0833dc0d5278:~/agent$ cat check.sh
#!/bin/bash

log_file="/var/log/bad.log"
```

```
./bin/bash@scenario-saintjohn-std-0833dc0d5278 - Google Chrome
ingress.sadsre.com/sessions/std-0833dc0d5278/
#!/bin/bash

log_file="/var/log/bad.log"

if [ -f "$log_file" ]; then
    current_size=$(stat -c %s "$log_file")
    sleep 0.5
    new_size=$(stat -c %s "$log_file")

    if [ "$current_size" -eq "$new_size" ]; then
        echo -n "OK"
    else
        echo -n "NO"
    fi
else
    echo -n "NO"
fi

admin@scenario-saintjohn-std-0833dc0d5278:~/agent$ lsof /var/log/bad.log
COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE/OFF  NODE  NAME
badlog.py  7  admin   3w   REG   0,956   348009 20079 /var/log/bad.log
admin@scenario-saintjohn-std-0833dc0d5278:~/agent$
```

- lsof <finalname>
- Kill -9 <pid> -9 sends SIGKILL
-15 sends SIGTERM

- **OTHER COMMANDS THAT CAN BE USED SO SOLVE THE PROBLEM**

- `Ps aux | grep <process or file name>`
- `Fuser <filename or process name >`