forkstat

Forkstat is a program that logs process fork(), exec() and exit() activity. It is useful for monitoring system behaviour and to track down rogue processes that are spawning off processes and potentially abusing the system.

Note that forkstat uses the Linux netlink connector to gather process activity and this may miss events if the system is overly busy. Netlink connector also requires root privilege.

forkstat command line options:

- -d strip off the directory path from the process name
- -D specify run duration in seconds.
- -e select which events to monitor.
- -h show brief help summary
- -l set stdout to line-buffered mode
- -r run with real time FIFO scheduler.
- -s show short process name information
- -S show event statistics at end of the run.
- -q run quietly and enable -S option.
- -x show extra process related information.

Example Output:
[crayon-6a9d5f5c4f4a1473728691/]
Source:

- forkstat git repository
- forkstat tarball
- forkstat manual (PDF)