

Sysdig Command Examples

Sysdig is a Linux system tracing tool that captures and filters system calls and kernel events in real time for forensics and troubleshooting

- ✓ `sysdig -cl` list all available chisels (i.e. built-in scripts)
- ✓ `sysdig -c topprocs_cpu` show top cpu-using processes
- ✓ `sysdig -c topprocs_memory` show top memory hoggers
- ✓ `sysdig -c proc_exec_time` show process execution time
- ✓ `sysdig -c netstat` show active network connections
- ✓ `sysdig -c topconns` show top network connections by total bytes
- ✓ `sysdig -c spy_users` capture interactive shell activities by users
- ✓ `sysdig -j` output each event in json format
- ✓ `sysdig proc.pid=1234` capture all events from a specific process PID
- ✓ `sysdig proc.name=nginx` captured all events from a specific process name
- ✓ `sysdig evt.type=connect` show processes making network connections
- ✓ `sysdig evt.type=accept` show processes with inbound network connections
- ✓ `sysdig evt.type=unlink` list processes deleting files
- ✓ `sysdig -c topfiles_bytes proc.name=httpd` show top files accessed by httpd
- ✓ `sysdig -w output.scap` dump all captured events to a file (-r to read it)
- ✓ `sysdig -C 10 -w output.scap` split the output file every 10MB
- ✓ `sysdig -G 60 -w my-%m-%d_%H:%M:%S.scap` rotate file every 60 seconds
- ✓ `sysdig "evt.type=accept and proc.name!=httpd"` combine two conditions
- ✓ `sysdig -p "%evt.type %evt.args" evt.dir=/tmp` monitor file I/O on /tmp dir
- ✓ `sysdig -A -c echo_fds "fd.filename=passwd"` show I/O activities on passwd
- ✓ `sysdig -pc -c topprocs_cpu container.name=nginx` monitor container cpu
- ✓ `sysdig "proc.name=nmap and evt.type=sendto and fd.dip=10.0.0.1"` detect network scanning activity from nmap targeting 10.0.0.1



Created by
Dan Nanni
study-notes.org

From:

<https://wiki.fortier-family.com/> - Warnaud's Wiki

Permanent link:

<https://wiki.fortier-family.com/cybersecurity/commands/sysdig>

Last update: **2026/04/26 15:29**

