<https://os.cybbh.io/public/os/latest/012_linux_auditing_&_logging/linlog_fg.html>

echo ‘kern.debug’

echo kern.\*

journalctl

cat /etc/rsyslog.conf

xpath -q -e ‘//@addr|//@portid’ output.xml

xpath -q -e “//\*[@up=’253’]//@down” output.xml

xpath -q -e ‘//\*[@addr=’10.50.29.254’’/../..//@starttime" output.xml

xpath -q -e “//\*[@up=’253’]/../../..//@srtt” output.xml

| Selectors | Action |
| --- | --- |
| facility. severity | /path/to/log/location |

1. Facility is the source, or event, that generated the log
2. Severity is how urgent an event is from 0 (Emergency) to 7 (Debug)
3. path/to/log/location is where the log is stored and/or any action taken on the event before storage (like sending it to a remote server)

| Numerical Code | Facility |
| --- | --- |
| 0 | kernel messages |
| 1 | user-level messages |
| 2 | mail system |
| 3 | system daemons |
| 4 | security/authorization messages |
| 5 | messages made by syslogd |
| 6 | line printer subsystem |
| 7 | network news subsystem |

Table 3. Syslog Message Severities [RFC 5424](https://tools.ietf.org/html/rfc5424#page-9)Numerical CodeSeverity

0

Emergency

1

Alert

2

Critical

3

Error

4

Warning

5

Notice

6

Informational

7

Debug