

Linux diagnostics

Inspect networking, storage, services and logs without changing configuration.

Interfaces and routes

`ip -brief address`

Show interface addresses and state.

`ip route show`

Show the IPv4 routing table.

`ip -6 route show`

Show the IPv6 routing table.

Sockets and DNS

`ss -lntup`

List listening TCP/UDP sockets numerically. Process details may require extra privileges.

`dig example.com A`

Query an address record if dig is installed.

`dig @1.1.1.1 example.com MX`

Ask a specific resolver for MX records.

Storage and capacity

`df -h`

Show mounted filesystem usage in human-readable units.

`df -i`

Check inode use when free space alone does not explain a write failure.

Services on systemd hosts

`systemctl --failed`

Show units in a failed state.

`systemctl status ssh.service --no-pager`

Inspect a service; substitute its actual unit name. Some distributions use `sshd.service`.

Journal queries

`journalctl -b -p err --no-pager`

Show error and higher-priority entries from this boot.

`journalctl -u ssh.service --since "1 hour ago"`

Inspect one unit over a recent period.

`journalctl -n 100 --no-pager`

Show the most recent 100 journal entries.

How to approach an incident

Record UTC time and symptoms first. Check interface state, routes, DNS and the listening service separately. Keep the original error message and correlate it with nearby log entries. A successful ping does not prove an application works.

Environment notes

Commands depend on installed packages, permissions and the init system. These examples do not modify configuration, but DNS queries leave the machine and logs may reveal sensitive data. Read the local man page for version-specific details.