Section 1: System Info & Uptime

Q1: Show system info

```
uname -a  # Kernel version, architecture
```

Q2: Show CPU info

```
lscpu  # Cores, threads, flags
```

Q3: Show memory info

```
free -h  # Total, used, free, swap
```

Q4: Uptime & load

```
uptime  # Load averages
```

Q5: Top processes

```
top  # Real-time CPU/mem usage
htop  # Interactive view
```

Section 2: Filesystem & Storage

Q6: List disks

```
lsblk
fdisk -l
```

Q7: Check disk usage

```
df -h
```

Q8: Check inode usage

```
df -i
```

Q9: Resize ext4 filesystem

```
resize2fs /dev/sdX1
```

Q10: Resize XFS filesystem

```
xfs_growfs /mountpoint
```

Q11: LVM commands

```
lvdisplay
display LV info
vgdisplay
pvdisplay
lvextend -L +10G /dev/mapper/vg-lv
```

Q12: Detect inode exhaustion

```
df -i  # Look for IUse% = 100%
```

Section 3: Processes & Scheduling

Q13: Find high CPU processes

```
top
ps -eo pid,ppid,cmd,%cpu,%mem --sort=-%cpu | head
pidstat 1
```

Q14: Check process tree

```
pstree -p
```

Q15: Kill a process

```
kill PID  # SIGTERM
kill -9 PID  # SIGKILL
```

Q16: Stuck process in D state

```
ps -o pid,stat,wchan,cmd  # D = uninterruptible sleep
```

Q17: Cron vs systemd timers - Cron: periodic jobs - systemd timers: dependency-aware, logs in journalctl

Section 4: Networking

Q18: Check listening ports

```
sudo ss -tulpn | grep :PORT
```

Q19: Active connections summary

```
ss -s
```

Q20: Interface statistics

```
ifconfig -a
ip -s link
```

Q21: Routing table

```
ip route
route -n
```

Q22: Ping & traceroute

```
ping 8.8.8.8
traceroute google.com
```

Q23: Firewall rules

```
iptables -L -v
nft list ruleset
```

Q24: Packet capture

```
tcpdump -i eth0 port 80
```

Q25: DNS lookup

```
dig example.com
nslookup example.com
```

Section 5: Memory & Performance

Q26: Check memory usage

```
free -m
vmstat 1
```

Q27: Detect memory leaks - Monitor memory trend: `free -m` / `vmstat 1` - Per-process: `pmap -x PID` - Profiling: `valgrind`, `smem` **Q28: Disk I/O stats**

```
iostat -x 1
```

Q29: Per-process CPU/mem

```
pidstat 1
```

Q30: Logs analysis

```
journalctl -xe
```

Q31: System call tracing

```
strace -p PID
```

Q32: CPU profiling

```
perf top
perf record -p PID
```

Section 6: System Reliability & Troubleshooting

Q33: Recover Linux after kernel update failure - Boot previous kernel in GRUB - Rescue/single-user mode - Check `/boot` & `/etc/fstab` - Reinstall kernel if needed

Q34: OOM killer - Logs: `dmesg | grep -i killed` - Control: `oom_score_adj`, cgroups, overcommit

Q35: Check core dumps

```
coredumpctl list
```

Q36: Service restart & debug

```
systemctl status service
journalctl -u service -b
systemctl restart service
```

Section 7: Logs & Monitoring

Q37: Live logs monitoring

```
tail -f /var/log/syslog
```

Q38: Search logs

```
grep -i error /var/log/* | less
```

Q39: Long-term metrics - Tools: `sar`, `collectl`, `prometheus node_exporter`

Section 8: Containers & Virtualization

Q40: Container stats

```
docker stats
kubectl top pods
```

Q41: Exec into container

```
docker exec -it CONTAINER bash
```

Q42: Check cgroups usage

```
cat /sys/fs/cgroup/memory/docker/<container-id>/memory.usage_in_bytes
```

Q43: Namespaces - Isolate PID, network, mount, user **Q44: cgroups + namespaces** - Namespaces = isolation - cgroups = resource limits

Section 9: Security & Users

Q45: List users & groups

```
cat /etc/passwd
cat /etc/group
```

Q46: Change file permissions & ownership

```
chmod 755 file
chown user:group file
```

Q47: Check sudo privileges

```
sudo -l
```

Q48: Find SUID/SGID files

```
find / -perm /6000
```

Q49: Audit login events

```
ausearch -m USER_LOGIN
```

Section 10: Advanced Networking & Kernel Tuning

Q50: Bandwidth test

```
iperf3 -c server
```

Q51: Established connections

```
ss -tan state established
```

Q52: Kernel tuning

```
sysctl -a
sysctl -w net.core.somaxconn=1024
```

Q53: Debug slow disk I/O

```
iostat -x 1
iotop
dmesg | grep -i error
```

Q54: Continuous monitoring

```
vmstat 1
iostat -x 1
pidstat 1
```

Section 11: Real-World Troubleshooting Scenarios

- **Disk full:** `df -h`, `du -sh /var/*`, delete/archive logs, check inode usage
- **High CPU:** `top`, `pidstat`, `strace`, analyze logs
- **Stuck process D:** `ps -o pid,stat,wchan,cmd`, check disk/NFS, `lsof`
- **OOM killed process:** `dmesg | grep -i killed`, tune cgroups, restart process
- **Network issue:** `ping`, `traceroute`, `ss -s`, `iptables -L`, `tcpdump`
- **Service crash:** `journalctl -u service`, check limits, dependencies, restart

---

Tips for Interview: - Practice all commands in a sandbox environment - Explain reasoning behind each step - Focus on debugging workflow and systematic troubleshooting - Understand differences between tools and Linux internals

---

End of Cheat Sheet