? EASY (Q1–Q10)

Q1. Logging in Bash scripts is mainly used to:
A. Increase execution speed
B. Record script activity and errors
C. Modify system files
D. Stop scripts

Q2. Which operator redirects standard output to a log file?
A. <
B. >
C. |
D. &

Q3. Which command appends output to an existing log file?
A. >
B. >>
C. <
D. |

Q4. Which command records system uptime for monitoring?
A. free
B. uptime
C. df
D. ls

Q5. Which file is commonly used to store custom script logs?
A. /etc/passwd
B. /var/log/script.log
C. /bin/log
D. /proc/log

Q6. Which command monitors running processes?
A. cat
B. ps
C. cp
D. mv

Q7. Which operator redirects standard error?
A. >
B. 1>
C. 2>
D. &>

Q8. Which Bash variable stores command exit status?
A. $$

B. $?
C. $!
D. $0

Q9. Which command monitors disk usage?
A. df
B. free
C. top
D. uname

Q10. Which monitoring task detects service failure?
A. Logging
B. Backup
C. Health check
D. Compression

□ MEDIUM (Q11–Q25)

Q11. Which redirection captures both stdout and stderr?
A. > file
B. 2> file
C. &> file
D. < file

Q12. Which Bash command adds timestamps to logs?
A. echo
B. date
C. time
D. cal

Q13. Which monitoring script checks CPU load?
A. df
B. uptime
C. free
D. ls

Q14. Which file permission is recommended for log files?
A. 777
B. 755
C. 644
D. 600

Q15. Which Bash construct repeatedly checks system status?
A. if

B. case
C. loop
D. function

Q16. Which command monitors memory usage periodically?
A. free
B. watch free
C. df
D. uname

Q17. Which tool schedules periodic monitoring scripts?
A. at
B. cron
C. sleep
D. watch

Q18. Which monitoring metric indicates disk bottleneck?
A. CPU idle
B. iowait
C. free memory
D. load average only

Q19. Which command logs output with timestamps automatically?
A. logger
B. echo
C. printf
D. log

Q20. Which Bash test checks if a log file exists?
A. -r
B. -w
C. -f
D. -x

Q21. Which log rotation tool prevents log files from growing indefinitely?
A. rsyslog
B. journald
C. logrotate
D. cron

Q22. Which monitoring script action triggers alerts?
A. Normal output
B. Threshold breach
C. Backup completion
D. Script start

Q23. Which Bash redirection suppresses all output?
A. > /dev/null
B. < /dev/null
C. | /dev/null
D. & /dev/null

Q24. Which monitoring best practice improves diagnosis?
A. Disable logs
B. Minimal checks
C. Meaningful log messages
D. No timestamps

Q25. Which command logs kernel messages useful for monitoring?
A. dmesg
B. journalctl
C. uptime
D. top

🟢 HARD (Q26–Q40)

Q26. Why should monitoring scripts be lightweight?
A. Reduce code length
B. Avoid adding system load
C. Simplify syntax
D. Reduce logs

Q27. Which Bash construct handles unexpected script termination?
A. break
B. continue
C. trap
D. exit

Q28. Which logging approach supports centralized monitoring?
A. Local text files only
B. Console output
C. Syslog integration
D. Temporary files

Q29. Which monitoring scenario requires alert escalation?
A. Normal CPU usage
B. Temporary spike
C. Persistent threshold violation
D. Script execution

Q30. Which Bash risk occurs when logs are world-writable?
A. Faster logging
B. Log tampering
C. Reduced disk usage
D. Improved auditing

Q31. Which monitoring metric best indicates memory exhaustion?
A. CPU idle
B. Swap usage
C. Disk space
D. Network throughput

Q32. Which logging practice improves forensic investigations?
A. Log overwriting
B. No rotation
C. Timestamped and immutable logs
D. Console-only logs

Q33. Which Bash monitoring script detects zombie processes?
A. df
B. ps
C. uptime
D. free

Q34. Which alerting method integrates with enterprise systems?
A. echo
B. wall
C. Email/Webhook notifications
D. print

Q35. Which monitoring error causes false positives?
A. Correct thresholds
B. Static thresholds only
C. Adaptive thresholds
D. Trend analysis

Q36. Which Bash feature ensures logs flush on exit?
A. exit
B. break
C. trap EXIT
D. continue

Q37. Which monitoring design improves scalability?
A. Single monolithic script
B. Distributed checks

C. Manual monitoring
D. No logs

Q38. Which security best practice protects monitoring scripts?
A. World-executable permissions
B. Hard-coded credentials
C. Restricted permissions
D. Disable logging

Q39. Which monitoring metric helps capacity planning?
A. One-time CPU usage
B. Historical trend data
C. Script exit code only
D. Error count

Q40. Which principle best guides logging and monitoring strategy?
A. Maximum verbosity always
B. Minimal visibility
C. Actionable, reliable, and secure observability
D. Disable alerts