CERTLABZ CERTIFICATION BOARD

Certified Open Source Systems Administrator (COSA)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working open source systems administrator would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1 — Domain 1: Linux Foundations — DATA

Sarah Miller reviews where a Linux system keeps different kinds of files.

Path	Holds
/etc	config files
/home	user homes
/var/log	log files
/boot	boot files

Table 1.1 Common top-level paths.

Which path holds the editable system configuration files?

A. /etc
B. /home
C. /var/log
D. /boot

Correct answer: A
System configuration files live under /etc, which is where an administrator edits service and host settings. The /home tree holds user data, /var/log holds logs, and /boot holds the kernel and boot loader files.

Question 2

Domain 2: Users, Storage and Filesystems

CONFIG

James Carter checks why writes to a data volume are failing.

```
$ df -h /data
Filesystem   Use%  Mounted
/dev/sdb1    100%  /data
write: No space left
```

Listing 2.1 Output while writes fail.

What is the immediate cause of the failed writes?

A. Out of memory pages
B. DNS failure
C. Disk is full
D. Bad RAM

Correct answer: C
The volume mounted at /data reports 100 percent used, so there is no free space for new writes. Freeing or extending the filesystem restores writes. Memory, DNS and hardware faults would not report a full disk.

Question 3

Domain 3: Networking and Services

CONFIG

Emma Wilson lists the sockets a host is listening on.

```
$ ss -tlnp
State   Local Port
LISTEN  22
LISTEN  80
```

Listing 3.1 Listening TCP ports.

Which service most likely owns the connection on port 22?

A. HTTPS proxy
B. DNS resolver
C. NTP daemon
D. SSH

Correct answer: D
Port 22 is the well-known port for SSH, the remote login and administration service. Port 80 is plain HTTP. DNS, NTP and an HTTPS proxy use other ports, so none of them owns port 22.

Question 4

Domain 4: Scripting and Automation

CONFIG

David Brown reviews a cleanup script that mishandles some filenames.

```
#!/bin/sh
for f in *.log
do rm $f
done
```

Listing 4.1 The current script.

What single change makes the script handle all filenames safely?

A. Quote "$f"
B. Add a sleep call
C. Run it as root
D. Raise the nice value

Correct answer: A
An unquoted $f is split on spaces and expanded as a glob, so filenames with spaces break the command. Quoting it as "$f" passes each name as one argument. Running as root, sleeping or changing priority does not fix the quoting fault.

Question 5

Domain 5: Security and Hardening

DATA

Olivia Davis audits the current state of a new server.

Setting	State
Root SSH login	enabled
Password auth	enabled
Host firewall	off
Auto updates	off

Table 5.1 Server settings today.

Which change is the soundest first hardening step?

A. Add more system RAM
B. Disable root login
C. Open all the ports
D. Share the password

Correct answer: B
Allowing direct root login over SSH gives an attacker a known account to target, so disabling it and using an unprivileged login with sudo is a standard first step. Adding RAM does nothing for security, and opening ports or sharing passwords weakens the host.

Question 6

Domain 6: Operations and Troubleshooting

CONFIG

Liam Anderson finds a service will not start.

```
$ systemctl status web
Active: failed
Main process exit code: 1
hint: see journalctl
```

Listing 6.1 Status of a failed service.

What is the best next step to diagnose the failure?

A. Reboot the server
B. Delete the unit file
C. Read the logs
D. Ignore the failure

Correct answer: C
The status output points to the service logs, so reading them with journalctl reveals the actual error before any change is made. Rebooting hides the cause, deleting the unit removes the service, and ignoring it leaves the outage in place.

Question 7

Domain 1: Linux Foundations

On a Linux system, what is the primary role of the kernel?

A. Edits config text
B. Serves web pages
C. Prints documents
D. Manages hardware

Correct answer: D
The kernel is the core of the operating system and manages hardware, memory and process scheduling on behalf of user programs. Editing text, serving pages and printing are jobs for ordinary applications that run on top of the kernel.

Question 8

Domain 2: Users, Storage and Filesystems

A user reports they cannot write to a shared directory. What should the administrator check first?

A. Check permissions

B Reinstall the whole OS

C Add swap space

D Change the shell

Correct answer: A
A write that is refused in a shared directory is almost always a permissions or ownership problem, so checking the mode and group is the first step. Reinstalling the system, adding swap or changing the login shell does not address directory access.

Question 9 Domain 4: Scripting and Automation

An administrator needs a maintenance script to run automatically every day at a set time. Which tool fits best?

A Trigger a reboot

B A cron job

C A new symlink

D A shell pipe

Correct answer: B
A cron job schedules a command to run on a fixed daily or weekly timetable, which is exactly what recurring maintenance needs. A reboot, a symlink and a pipe do not schedule anything on their own.

Question 10 Domain 5: Security and Hardening

When assigning access on a multi-user server, what does the principle of least privilege mean in practice?

A Give everyone full root

B Disable all logging

C Share all the keys

D Grant least rights

Correct answer: D
Least privilege means each account and service gets only the minimum rights needed to do its work, which limits the damage from a mistake or a compromise. Granting full root to everyone, disabling logging or sharing keys all widen risk rather than reduce it.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document COSA-001. https://certlabz.com/certifications/certified-open-source-systems-administrator.html