CERTLABZ CERTIFICATION BOARD

Certified DevOps Practitioner (CDOP)

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 DevOps practitioner 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: DevOps Foundations — DATA

Sarah Miller reviews the delivery stats before and after a DevOps rollout.

Metric	Value
Deploy frequency	Weekly
Lead time	6 days
Change fail rate	18%
Recovery time	4 hours

Table 1.1 Delivery stats before the rollout.

What does lead time measure?

A. Speed of delivery
B. Server uptime
C. Cost per deployment
D. Number of engineers

Correct answer: A

Lead time measures how long a change takes to reach production, so it reflects the speed of delivery. Uptime, cost and headcount are separate concerns and do not define lead time.

Question 2 — Domain 2: Version Control and Continuous Integration — CONFIG

James Carter documents the daily workflow his team follows.

```
commit -> push -> pipeline
pipeline: build + test
merge small changes often
```

Listing 2.1 The team workflow.

What does this describe?

A. Quarterly manual merges
B. Big-bang integration
C. Continuous integration
D. Code freeze policy

Correct answer: C
The workflow commits often, runs an automated build and test on each push, and merges small changes frequently, which is continuous integration. Quarterly merges, big-bang integration and code freezes all delay feedback instead.

Question 3 — Domain 3: Continuous Delivery and Deployment — CONFIG

Olivia Davis reviews a release configuration that uses two identical environments.

```
strategy: blue-green
route: 100% to green
rollback: switch to blue
```

Listing 3.1 The release configuration.

What enables an instant rollback here?

A. Rebuilding from scratch
B. Blue kept on standby
C. Deleting old servers
D. Manual database edits

Correct answer: B
A blue-green deployment keeps the previous blue version on standby, so traffic can switch back instantly if green fails. Rebuilding, deleting servers or editing the database by hand cannot restore service that quickly.

Question 4 — Domain 4: Infrastructure and Configuration — DATA

David Brown maps how each environment is currently configured.

Environment	Config source
Dev	Hand edited
Staging	Hand edited
Prod	Hand edited
Result	Drift and errors

Table 4.1 How each box is configured today.

What prevents this drift?

A Edit each box by hand
B Skip all versioning
C Longer change windows
D Infra as code

Correct answer: D
Defining infrastructure as code keeps every environment built from the same versioned source, which removes the drift caused by hand editing each box. Longer windows and skipped versioning do not stop drift.

Question 5 Domain 5: Monitoring, Logging and Feedback DATA

Emma Wilson matches each observability signal to the question it answers.

Signal	Question
Metrics	How much or how fast
Logs	What happened
Traces	Where time went
Alerts	When to act

Table 5.1 Signals and their questions.

Which signal shows a slow request path?

A Metrics
B Traces
C Static docs
D Alerts

Correct answer: B
Traces follow a single request across services and show where the time was spent, making them the right signal for a slow request path. Metrics and alerts summarise or notify but do not map the path.

Question 6 — Domain 6: Security, Reliability and Culture — DATA

Liam Anderson maps each practice to the benefit it delivers.

Practice	Aim
Least privilege	Limit blast radius
Secrets vault	Hide credentials
Blameless review	Learn from failure
SLOs	Set a reliability target

Table 6.1 Practices and their aims.

Which practice limits access rights?

A. Least privilege
B. Shared root logins
C. Public secrets file
D. Ignore audit logs

Correct answer: A
Least privilege grants each account only the access it needs, which limits the blast radius if credentials are misused. Shared root logins and public secrets widen access rather than limiting it.

Question 7 — Domain 1: DevOps Foundations

Two teams blame each other for a failed release and share nothing between them. Which cultural change best fixes this?

A. Separate the teams fully
B. Punish the on-call
C. Blameless shared goals
D. Add more handoffs

Correct answer: C
A blameless culture with shared goals moves two teams from blaming each other to learning from failure together. Separating the teams, adding handoffs or punishing on-call staff deepens the divide.

Question 8 — Domain 2: Version Control and Continuous Integration

A team keeps long-lived feature branches that diverge for weeks, causing painful merges. What practice reduces this pain?

A. Long release branches

B Never merge to main

C Skip code review

D Merge to trunk daily

Correct answer: D
Merging to the trunk daily keeps changes small and integrated, which avoids the painful merges caused by branches that diverge for weeks. Long branches and skipped review make integration harder.

Question 9 Domain 3: Continuous Delivery and Deployment

A deployment fails and the team has no automated way to revert, so users see errors for hours. What capability is required?

A Slower releases

B Automated rollback

C Manual server login

D Longer freeze window

Correct answer: B
Automated rollback lets the team revert a failed deployment quickly, so users are not left with errors for hours. Slower releases, manual logins and longer freezes do not restore service fast.

Question 10 Domain 5: Monitoring, Logging and Feedback

An outage is noticed only when a customer calls, because no alerts exist on the key signals. What should the team add?

A Proactive alerting

B Silence all warnings

C Fewer log entries

D Wait for callers

Correct answer: A
Proactive alerting on the key signals lets the team detect an outage before customers call. Silencing warnings, cutting logs or removing dashboards would only reduce visibility further.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document CDOP-001. https://certlabz.com/certifications/certified-devops-practitioner.html