

PRACTICE QUESTIONS

Google Cloud

Professional Cloud Architect

SHARED BY [u/Eager-Hawk-2679](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM Google Cloud Professional Cloud Architect

Shared by [u/Eager-Hawk-2679](#) on aiexamcerts

10 practice questions for the Google Cloud Professional Cloud Architect exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/google-cloud/professional-cloud-architect. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. A bank must keep transaction data in Germany and needs disaster recovery in a second location that also stays in Germany. Which design meets both requirements?
 - A A single global location with no regional boundary
 - B Two regions located in Germany with a replicated disaster recovery copy
 - C A multi-region that spans Asia and Europe
 - D A bucket in Iowa with cross-continent replication

Answer: B

Keeping the primary and the recovery resources in two German regions satisfies residency while providing regional redundancy. A global design or a multi-region spanning Asia and Europe places data outside Germany. A bucket in Iowa with replication moves the data outside the country as well.

2. Cloud Armor security policies can inspect and filter HTTP requests when attached to a regional external passthrough Network Load Balancer.
 - A True
 - B False

Answer: B (False)

Layer 7 request filtering works on Application Load Balancers, while passthrough balancers only support IP-based rules. The misconception is that every load balancer type gets full HTTP filtering. Choose the balancer type first when a design needs request-level rules.

3. A monolith database suffers write contention, and the team plans to split it. Which early step reduces risk most?
 - A Shard the entire database in one weekend
 - B Identify the most contended write paths and migrate one domain at a time
 - C Remove all indexes to speed up writes
 - D Turn off backups so the migration runs faster

Answer: B

Mapping domains and contended write paths, then moving one slice at a time, lowers risk and lets the team verify each step. A full one-weekend split has no practical rollback path. Removing indexes and disabling backups increase risk rather than reducing it.

4. Cloud KMS keys that are protected by FIPS 140-2 Level 3 hardware security modules use the protection level called _____.

Answer: Cloud HSM (also accepted: HSM)

Cloud HSM keys are protected by hardware security modules validated to FIPS 140-2 Level 3, a stronger tier than software keys. Software protection keeps key material in Cloud KMS software. External key management keeps keys outside Google Cloud, which is a different option.

5. Which two practices strengthen security for Cloud Storage buckets that hold sensitive data? (Choose two.)

- A Enabling uniform bucket-level access and granting access through IAM groups
- B Making the bucket public so partners can download it more easily
- C Enforcing Public Access Prevention
- D Storing long-lived HMAC keys in the bucket's metadata
- E Disabling object versioning to reduce storage costs

Answer: A, C

Uniform bucket-level access centralizes control in IAM, and Public Access Prevention blocks accidental public exposure. A public bucket, keys stored in metadata and disabled versioning each weaken protection or recovery.

6. A CI/CD pipeline running outside Google Cloud must deploy resources without storing long-lived keys. Which mechanism fits?

- A A downloaded JSON key committed to the repository
- B A long-lived service account key stored as a CI secret
- C Workload Identity Federation with the pipeline's OIDC token
- D Owner access granted to every developer and contractor on the project

Answer: C

Workload Identity Federation exchanges a provider's short-lived OIDC token for Google Cloud access, so no key file exists to leak. A key committed to a repository is the exact risk to avoid. A stored service account key is still a long-lived credential, and broad Owner grants are unsafe.

7. Workloads on GKE need to call Cloud Storage, and each workload should have its own identity without node-level keys. Which mechanism does this?
- A A JSON key mounted into the pod as a Secret
 - B The node's default service account with the Editor role
 - C An API token baked into the container image
 - D Workload Identity mapping a Kubernetes service account to a Google service account

Answer: D

Workload Identity maps a Kubernetes service account to a Google Cloud service account, so each workload gets scoped credentials without distributing keys. A mounted JSON key is still a long-lived secret. Giving every pod the node's account with Editor is overly broad, and tokens baked into images leak through registries.

8. BigQuery on-demand pricing is based on the number of rows a query returns, not on the bytes it scans.
- A True
 - B False

Answer: B (False)

On-demand pricing is based on bytes processed, so a query that returns few rows can still be expensive if it scans a lot. The misconception is that the output size drives the bill. Partitioning and clustering reduce scanned bytes.

9. A service has a 99.9 percent availability SLO. Roughly how much error budget does it have in a 30-day month?
- A About 43 minutes
 - B About 4 hours of error budget
 - C About 7 hours
 - D About 1 minute

Answer: A

A 99.9 percent SLO leaves 0.1 percent of time as error budget, about 43 minutes in a 30-day month. Four hours matches roughly 99.5 percent, and seven hours matches about 99 percent. One minute is far stricter than the stated target.

10. An application has a 15-minute recovery time objective and a 1-minute recovery point objective for its database. Which Cloud SQL configuration best matches these targets?
- A A single zonal instance with a nightly backup
 - B A regional high availability instance with point-in-time recovery
 - C A weekly export to Cloud Storage
 - D A read replica in another region that is never promoted to primary

Answer: B

High availability gives automatic failover within minutes, and point-in-time recovery limits data loss to the last few minutes of logs. A nightly backup can lose up to a day of data. Weekly exports and an unpromoted replica cannot meet either objective.