

PRACTICE QUESTIONS

Google Cloud

Associate Cloud Engineer

SHARED BY [u/Smooth-Subnet-6857](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM Google Cloud Associate Cloud Engineer

Shared by [u/Smooth-Subnet-6857](#) on aiexamcerts

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

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

1. An engineer works on two projects from the same laptop and wants separate default project and region settings for each. Which approach does this?
- A Changing the color theme in the Cloud Console for each project
 - B Named gcloud configurations created with gcloud config configurations create and switched with activate
 - C Setting the project only inside each Terraform file
 - D Running gcloud auth revoke at the end of every session

Answer: B

gcloud configurations each hold their own account, project and compute defaults, and gcloud config configurations activate switches between them. A console color theme does not change gcloud defaults. Revoking credentials after each session forces a new sign-in and does not separate the settings.

2. A new project cannot use paid services until a billing account is attached, using the command gcloud billing projects _____ --billing-account=BILLING_ACCOUNT_ID.

Answer: link

gcloud billing projects link attaches the billing account to the project and enables paid services there. The describe subcommand only reads the current link. Creating a budget sends alerts about spending and does not enable billing.

3. A web app's traffic peaks at lunchtime and is quiet overnight. It runs on a managed instance group. Which configuration best matches capacity to demand?
- A An autoscaling policy on the managed instance group based on CPU utilization
 - B A fixed size of 20 instances running all day
 - C One large VM that is resized by hand each morning
 - D A single preemptible VM with no health checks and no autoscaling policy attached

Answer: A

Autoscaling a managed instance group adds and removes instances against a metric such as CPU utilization, which follows the lunchtime peak. A fixed size of 20 pays for idle capacity overnight. Manual resizing and a single VM give no redundancy, which is the tempting shortcut that fails under load.

4. When uniform bucket-level access is enabled on a Cloud Storage bucket, object ACLs become the primary mechanism for controlling access.
- A True
 - B False

Answer: B (False)

With uniform bucket-level access, access is controlled by IAM alone and object ACLs are disabled. The tempting misreading is that ACLs take priority once the setting is on. Enabling it is generally recommended so that access is managed in one place.

5. Which two actions reduce the risk of long-lived service account keys? (Choose two.)
- A Enforcing the iam.disableServiceAccountKeyCreation organization policy
 - B Attaching service accounts directly to compute resources instead of distributing key files
 - C Creating a new key for every developer laptop
 - D Storing key files in a publicly readable bucket for sharing
 - E Keeping key files in the source repository so they are versioned

Answer: A, B

The iam.disableServiceAccountKeyCreation organization policy stops new keys from being created, and attaching service accounts to resources removes the need to distribute key files. A key per laptop multiplies exposure. Public buckets and source repositories leak the key material.

6. A script must run on each new VM in a managed instance group at first boot. Where should the script be set?
- A The instance template metadata under the startup-script key
 - B The billing account settings page
 - C A VPC firewall rule
 - D The bucket lifecycle policy

Answer: A

A startup-script metadata key in the instance template runs when each VM boots, including VMs the group creates later. Billing settings hold payment details, and firewall rules filter traffic rather than run code. Bucket lifecycle policies manage objects.

7. A team wants to send 10 percent of App Engine traffic to a new version during a rollout and keep the old version ready for rollback. Which feature does this?
- A Cloud Scheduler jobs
 - B Traffic splitting across service versions
 - C A Pub/Sub dead-letter topic attached to the service subscription
 - D A VPC peering route

Answer: B

App Engine traffic splitting assigns percentages of traffic across versions of a service, which supports gradual rollouts and quick rollback. Cloud Scheduler triggers jobs on a timetable. A dead-letter topic holds undeliverable messages, and VPC peering routes network traffic between networks.

8. Admin Activity audit logs are kept in the _Required log bucket for _____ days, and that retention cannot be shortened.

Answer: 400 (also accepted: four hundred)

The _Required bucket retains Admin Activity audit logs for 400 days, and that period is fixed. The _Default bucket keeps ordinary logs for 30 days unless its retention is changed. A bucket you create has the retention you set for it.

9. A team wants an email whenever a VM's CPU stays above 80 percent for five minutes. Which Cloud Monitoring feature does this?
- A A billing budget alert on the project
 - B An uptime check on the VM's SSH port
 - C A log-based metric that counts SSH logins on the instance each hour
 - D An alerting policy with a metric threshold condition

Answer: D

An alerting policy with a metric threshold condition and a duration sends notifications when CPU utilization stays above the threshold for the window. A billing budget tracks spending rather than CPU. An uptime check tests reachability, and a log-based metric counts log entries rather than reading CPU values.

10. Which service stores API keys, passwords and certificates with IAM-controlled access, versioning and audit logging?
- A A Cloud Logging sink
 - B A Cloud Monitoring dashboard
 - C Cloud CDN
 - D Secret Manager

Answer: D

Secret Manager stores secret values with IAM access control, versioning and audit logging. A logging sink exports log entries, and a monitoring dashboard displays metrics. Cloud CDN caches content for delivery and is not a secret store.