Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 33 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 33

Topic #: 1

[All Professional Cloud Security Engineer Questions]

A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs).
The jobs are bursty and must be completed quickly. They have a requirement to be able to control the key lifecycle.
Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

A. Customer-supplied encryption keys (CSEK)

B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)

C. Encryption by default

D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Show Suggested Answer

by animesh54 at *May 2, 2022, 6:58 a.m.*

Comments

Type your comment...

Submit

⊟ animesh54 Highly Voted 👍 2 years, 8 months ago

Selected Answer: B

Customer Managed Encryption keys using KMS lets users control the key management and rotation policies and Compute Engine Disks support CMEKs

upvoted 7 times

AwesomeGCP Highly Voted 2 years, 3 months ago

Selected Answer: B

Correct Answer: B
Explanation/Reference:
Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

upvoted 5 times

trashbox Most Recent 8 months, 3 weeks ago

Selected Answer: B

"Control over the key lifecycle" is the key. The KMS is the most appropriate solution.

upvoted 1 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses