Google Discussions

Exam Professional Data Engineer All Questions
View all questions & answers for the Professional Data Engineer exam

Go to Exam

EXAM PROFESSIONAL DATA ENGINEER TOPIC 1 QUESTION 298 DISCUSSION

Actual exam question from Google's Professional Data Engineer
Question #: 298
Topic #: 1
[All Professional Data Engineer Questions]

One of your encryption keys stored in Cloud Key Management Service (Cloud KMS) was exposed. You need to re- encrypt all of your CMEK-protected Cloud Storage data that used that key, and then delete the compromised key. You also want to reduce the risk of objects getting written without customer-managed encryption key (CMEK) protection in the future. What should you do?

A. Rotate the Cloud KMS key version. Continue to use the same Cloud Storage bucket.

B. Create a new Cloud KMS key. Set the default CMEK key on the existing Cloud Storage bucket to the new one.

C. Create a new Cloud KMS key. Create a new Cloud Storage bucket. Copy all objects from the old bucket to the new one bucket while specifying the new Cloud KMS key in the copy command.

D. Create a new Cloud KMS key. Create a new Cloud Storage bucket configured to use the new key as the default CMEK key. Copy all objects from the old bucket to the new bucket without specifying a key.

Show Suggested Answer

by rahulvin at *Dec. 30, 2023, 9:18 p.m.*

Comments

Type your comment...

Submit

raaad Highly Voted 10 months ago

Selected Answer: D

- New Key Creation: A new Cloud KMS key ensures a secure replacement for the compromised one.
- New Bucket: A separate bucket prevents potential conflicts with existing objects and configurations.
- Default CMEK: Setting the new key as default enforces encryption for all objects in the bucket, reducing the risk of unencrypted data.
- Copy Without Key Specification: Copying objects without specifying a key leverages the default key, simplifying the process and ensuring consistent encryption.
- Old Key Deletion: After copying, the compromised key can be safely deleted.

upvoted 10 times

rahulvin Highly Voted 10 months, 1 week ago

Selected Answer: D

Wrong:
A - rotating external key doesn't trigger re-encryption of data already in GCS: https://cloud.google.com/kms/docs/rotate-key#rotate-external-coordinated
C - Setting key during copy doesn't take care of objects that are later uploaded to the bucket, that will still use the default key

upvoted 8 times

desertlotus1211 Most Recent 1 month, 1 week ago

Selected Answer: C

If no key is specified, and the bucket's default CMEK key is used, there's a risk that some objects might fall back to Google-managed encryption, especially if misconfigured

upvoted 1 times

JyoGCP 8 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

ML6 8 months, 2 weeks ago

Selected Answer: D

The correct answer is D. Rotating the key does not seem to re-encrypt:

In the event that a key is compromised, regular rotation (!!) limits the number of actual messages vulnerable to compromise (!!).
If you suspect that a key version is compromised, disable it and revoke access to it as soon as possible.
Source: https://cloud.google.com/kms/docs/key-rotation#why_rotate_keys

upvoted 3 times

ML6 8 months, 2 weeks ago

Note: When you rotate a key, data encrypted with previous key versions is not automatically re-encrypted with the new key version. You can learn more about re-encrypting data.
Source: https://cloud.google.com/kms/docs/key-rotation#how_often_to_rotate_keys

upvoted 3 times

Medmah 9 months, 2 weeks ago

I don't understand why only Matt select A

https://cloud.google.com/sdk/gcloud/reference/kms/keys/update

This seems to do the job, am I wrong ?

upvoted 2 times

Matt_108 9 months, 3 weeks ago

Selected Answer: A

Definitely A

upvoted 1 times

ML6 8 months, 2 weeks ago

Rotating does not mean you re-encrypt data.

upvoted 1 times

EXAMTOPICS

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses

© 2024 ExamTopics