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 196 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 196

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your organization previously stored files in Cloud Storage by using Google Managed Encryption Keys (GMEK), but has recently updated the internal policy to require Customer Managed Encryption Keys (CMEK). You need to re-encrypt the files quickly and efficiently with minimal cost.

What should you do?

A. Reupload the files to the same Cloud Storage bucket specifying a key file by using gsutil.

B. Encrypt the files locally, and then use gsutil to upload the files to a new bucket.

C. Copy the files to a new bucket with CMEK enabled in a secondary region.

D. Change the encryption type on the bucket to CMEK, and rewrite the objects.

Show Suggested Answer

by K1SMM at *Aug. 2, 2023, 11:04 p.m.*

Comments

Type your comment...

Submit

pradoUA 1 year, 4 months ago

Selected Answer: D

D is the correct answer

upvoted 1 times

ArizonaClassics 1 year, 5 months ago

The most efficient and cost-effective approach to meet your requirements would be:

D. Change the encryption type on the bucket to CMEK, and rewrite the objects.

Rewriting the objects in-place within the same bucket, specifying the new CMEK for encryption, allows you to re-encrypt the data without downloading and re-uploading it, thus minimizing costs and time.

upvoted 1 times

cyberpunk21 1 year, 5 months ago

Selected Answer: D

D is the option it's a direct question

upvoted 2 times

RuchiMishra 1 year, 5 months ago

Selected Answer: D

https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys

upvoted 2 times

arpgaur 1 year, 5 months ago

re-writing the objects is not quick and efficient. Option D is incorrect.

C. Copy the files to a new bucket with CMEK enabled in a secondary region.Option C is the most efficient and cost-effective solution. It would create a new bucket with CMEK enabled in a secondary region. The files would be copied to the new bucket, and the encryption type would be changed to CMEK. This would allow the files to be accessed using CMEK, while minimizing the impact on performance and availability.

upvoted 3 times

> **ymkk** 1 year, 5 months ago
>
> Copying the files to a new bucket in a secondary region would incur data egress charges and take time.
>
> upvoted 1 times
>
> > **Crotofroto** 1 year, 1 month ago
> >
> > Less time than re-writing and no egress cost as nothing is exiting GCP.
> >
> > upvoted 1 times

akg001 1 year, 5 months ago

option D- y changing the encryption type on the bucket to CMEK and rewriting the objects, you can efficiently re-encrypt the existing files in Cloud Storage using Customer Managed Encryption Keys (CMEK). This option avoids the need to reupload or copy the files and allows you to apply the new encryption policy to the existing objects in the bucket.

upvoted 1 times

K1SMM 1 year, 5 months ago

I think D
https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys?hl=pt-br

upvoted 2 times