

🔗 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 34 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 34

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud. What should you do?

- A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage the key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

[Show Suggested Answer](#)

by [mte_tech34](#) at Sept. 27, 2020, 7:33 a.m.

Comments

Type your comment...

[Submit](#)

🗨️ [mte_tech34](#) Highly Voted 4 years, 10 months ago


Answer is B.

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption

"The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK)."



   upvoted 25 times

  **passtest100** 4 years, 10 months ago

SHOULD BE A.

NO envelope encryption is mentioned in the question.

   upvoted 5 times

  **Arad** 3 years, 8 months ago

Correct answer is B, and A is wrong!

envelope encryption is default mechanism in CMEK when used for Dataproc, please check this link:

This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

   upvoted 2 times

  **mynk29** 3 years, 5 months ago




I agree but then should answer not be C- customer supplied key?

   upvoted 1 times

  **mynk29** 3 years, 5 months ago

My bad I read it as Customer managed.. even though i now realised i wrote customer supplied. :D

   upvoted 1 times

  **lolanczos** Most Recent  5 months ago

Selected Answer: B

B

The KEK is always managed by the KMS. The KMS never manages the DEK (so A is wrong).

Both C/D are bad options, the customer supplying the encryption key defeats the purpose of the scenario in the question.

   upvoted 1 times

  **BPzen** 8 months ago

Selected Answer: B

To manage encryption for Cloud Dataproc persistent disks, Google Cloud supports Customer-Managed Encryption Keys (CMEK) using Cloud Key Management Service (KMS). In this setup:

Data Encryption Key (DEK):

Google Cloud automatically generates and manages the DEK for encrypting the persistent disk data.

Key Encryption Key (KEK):

The KEK, managed in Cloud KMS, encrypts the DEK. This ensures the customer has control over key management operations, such as key rotation and deletion.




   upvoted 1 times

  **Sarmee305** 1 year, 1 month ago

Selected Answer: B

Answer is B

Cloud KMS allows you to manage KEKs, which in turn are used to encrypt the DEKs. DEKs are then used to encrypt the data. This separation ensures that the more sensitive KEK remains securely managed within the Cloud KMS

   upvoted 1 times

  **dija123** 1 year, 4 months ago

Selected Answer: B

Agree with B

   upvoted 1 times

  **amanshin** 2 years, 1 month ago

The correct answer is B. Use the Cloud Key Management Service to manage the key encryption key (KEK).

Cloud Dataproc uses a two-level encryption model, where the data encryption key (DEK) is encrypted with a key encryption key (KEK). The KEK is stored in Cloud Key Management Service (KMS), which allows you to create, rotate, and destroy the KEK as needed.

If you use customer-supplied encryption keys (CSEKs) to manage the DEK, you will be responsible for managing the CSEKs yourself. This can be a complex and time-consuming task, and it can also increase the risk of data loss if the CSEKs are compromised.



   upvoted 1 times

  **aashishh** 2 years, 3 months ago

Selected Answer: A

Option B, using Cloud KMS to manage the key encryption key (KEK), is not necessary as persistent disks in Cloud Dataproc are already encrypted at rest using AES-256 encryption with a unique DEK generated and managed by Google.

   upvoted 1 times

  **mahi9** 2 years, 5 months ago

Selected Answer: B

The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK)."

   upvoted 1 times

  **sameer2803** 2 years, 5 months ago

there is a diagram in the link. if you understand the diagram, you will get the answer.
<https://cloud.google.com/sql/docs/mysql/cmek#with-cmek>

   upvoted 1 times

  **sameer2803** 2 years, 5 months ago

Answer is B. the documentation says that Google does the data encryption by default and then that encryption key is again encrypted by KEK. which in turn can be managed by Customer.

   upvoted 1 times

  **DA95** 2 years, 7 months ago

Selected Answer: A

Option B, using the Cloud KMS to manage the key encryption key (KEK), is incorrect. The KEK is used to encrypt the DEK, so the DEK is the key that is managed by the Cloud KMS.



   upvoted 1 times

  **Meyucho** 2 years, 8 months ago

Selected Answer: A

B can be right but we never been asked about envelope encryption... so... the solution is to use a customer managed Data Encryption Key

   upvoted 1 times

  **AzureDP900** 2 years, 8 months ago

B. Use the Cloud Key Management Service to manage the key encryption key (KEK).

   upvoted 1 times

  **AwesomeGCP** 2 years, 9 months ago

Selected Answer: B

Answer is B,

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

   upvoted 4 times

  **giovy_82** 2 years, 11 months ago

Selected Answer: B

In my opinion it should be B. reference :

<https://cloud.google.com/kms/docs/envelope-encryption>

How to encrypt data using envelope encryption

The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.

   upvoted 2 times

  **piyush_1982** 2 years, 12 months ago

Selected Answer: A

I think the answer is A.

DEK (Data encryption Key) is the key which is used to encrypt the data. It can be both customer-managed or customer supplied in terms of GCP>

<https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption>

The link above states "This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK)."

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **absipat** 3 years, 1 month ago

b of course

👍 ↩ 🚩 upvoted 1 times

[Load full discussion...](#)



Platform

> [Home](#)

> [All Exams](#)

> [Examtopics PRO](#)

> [Training Courses](#)



© 2024 ExamTopics