

[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 231 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 231

Topic #: 1

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

You are migrating an application into the cloud. The application will need to read data from a Cloud Storage bucket. Due to local regulatory requirements, you need to hold the key material used for encryption fully under your control and you require a valid rationale for accessing the key material.

What should you do?

- A. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys. Configure an IAM deny policy for unauthorized groups.
- B. Generate a key in your on-premises environment to encrypt the data before you upload the data to the Cloud Storage bucket. Upload the key to the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and have the external key system reject unauthorized accesses.
- C. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys backed by a Cloud Hardware Security Module (HSM). Enable data access logs.
- D. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises. Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.



[Show Suggested Answer](#)

by  gcp4test at Aug. 4, 2023, 2:26 p.m.

Comments

Type your comment...

Submit

  **Pime13** 7 months, 3 weeks ago

Selected Answer: D

External key - means: Cloud External Key Manager
Access Justifications - it is part a Cloud External Key Manager

   upvoted 1 times

  **Sundar_Pichai** 11 months, 1 week ago

Selected Answer: D

"Provide justification for key usage" is your hint in this question. That leaves B or D. You can't upload custom keys to KMS. D.

   upvoted 1 times

  **MisterHairy** 1 year, 8 months ago

Selected Answer: D

The correct answer is D. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises. Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.

This approach allows you to maintain full control over the key material used for encryption, as the key is generated and stored in an on-premises HSM. By using this key as an external key in Cloud KMS, you can leverage Google Cloud's key management capabilities while still maintaining control over the key material. Activating Key Access Justifications provides a valid rationale for accessing the key material, as it allows you to monitor and justify each attempt to use the key.

   upvoted 2 times

  **ArizonaClassics** 1 year, 10 months ago

D. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises. Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.

This is the correct approach for the following reasons:

By generating a key in your on-premises environment and storing it in an HSM that you manage, you're ensuring that the key material is fully under your control.

Using the key as an external key in Cloud KMS allows you to use the key with Google Cloud services without having the key stored on Google Cloud.

Activating Key Access Justifications (KAJ) provides a reason every time the key is accessed, and you can configure the external key system to reject unauthorized access attempts.

   upvoted 1 times

  **anshad666** 1 year, 11 months ago

Selected Answer: D

D- key material used for encryption fully under your control and you require a valid rationale for accessing the key material



   upvoted 1 times

  **ymkk** 1 year, 11 months ago

Selected Answer: D

Option D meets the key control requirements and ensures regulatory compliance.

   upvoted 1 times

  **akg001** 1 year, 11 months ago

Selected Answer: D

D looks correct.

   upvoted 1 times

  **gcp4test** 1 year, 11 months ago

Selected Answer: D

External key - means: Cloud External Key Manager
Access Justifications - it is part a Cloud External Key Manager

   upvoted 4 times



Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

