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 262 DISCUSSION

Actual exam question from Google's Professional Data Engineer

Question #: 262

Topic #: 1

[All Professional Data Engineer Questions]

You are on the data governance team and are implementing security requirements. You need to encrypt all your data in BigQuery by using an encryption key managed by your team. You must implement a mechanism to generate and store encryption material only on your on-premises hardware security module (HSM). You want to rely on Google managed solutions. What should you do?

A. Create the encryption key in the on-premises HSM, and import it into a Cloud Key Management Service (Cloud KMS) key. Associate the created Cloud KMS key while creating the BigQuery resources.

B. Create the encryption key in the on-premises HSM and link it to a Cloud External Key Manager (Cloud EKM) key. Associate the created Cloud KMS key while creating the BigQuery resources.

C. Create the encryption key in the on-premises HSM, and import it into Cloud Key Management Service (Cloud HSM) key. Associate the created Cloud HSM key while creating the BigQuery resources.

D. Create the encryption key in the on-premises HSM. Create BigQuery resources and encrypt data while ingesting them into BigQuery.

Show Suggested Answer

by scaenruy at *Jan. 3, 2024, 5:44 p.m.*

Comments

Type your comment...

Submit

raaad Highly Voted 1 year, 4 months ago

Selected Answer: B

- Cloud EKM allows you to use encryption keys managed in external key management systems, including on-premises HSMs, while using Google Cloud services.
- This means that the key material remains in your control and environment, and Google Cloud services use it via the Cloud EKM integration.
- This approach aligns with the need to generate and store encryption material only on your on-premises HSM and is the correct way to integrate such keys with BigQuery.

======
Why not Option C
- Cloud HSM is a fully managed service by Google Cloud that provides HSMs for your cryptographic needs. However, it's a cloud-based solution, and the keys generated or managed in Cloud HSM are not stored on-premises. This option doesn't align with the requirement to use only on-premises HSM for key storage.

upvoted 18 times

Pime13 Most Recent 3 months, 4 weeks ago

Selected Answer: B

check raaad's comment.

upvoted 1 times

meh_33 8 months, 4 weeks ago

Selected Answer: B

Option B, I agree with Raaad on the approach

upvoted 1 times

f74ca0c 11 months, 3 weeks ago

Selected Answer: B

https://cloud.google.com/kms/docs/ekm#ekm-management-mode

upvoted 3 times

f74ca0c 11 months, 3 weeks ago

B- https://cloud.google.com/kms/docs/ekm#ekm-management-mode
Coordinated external keys are made possible by EKM via VPC connections that use EKM key management from Cloud KMS. If your EKM supports the Cloud EKM control plane, then you can enable EKM key management from Cloud KMS for your EKM via VPC connections to create coordinated external keys. With EKM key management from Cloud KMS enabled, Cloud EKM can request the following changes in your EKM:

upvoted 1 times

Matt_108 1 year, 3 months ago

Selected Answer: B

Option B, I agree with Raaad on the approach

upvoted 2 times

scaenruy 1 year, 4 months ago

Selected Answer: C

C. Create the encryption key in the on-premises HSM, and import it into Cloud Key Management Service (Cloud HSM) key. Associate the created Cloud HSM key while creating the BigQuery resources.

upvoted 3 times