← **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 274 DISCUSSION**

Actual exam question from Google's Professional Data Engineer
Question #: 274
Topic #: 1
[All Professional Data Engineer Questions]

You have a BigQuery table that ingests data directly from a Pub/Sub subscription. The ingested data is encrypted with a Google-managed encryption key. You need to meet a new organization policy that requires you to use keys from a centralized Cloud Key Management Service (Cloud KMS) project to encrypt data at rest. What should you do?

A. Use Cloud KMS encryption key with Dataflow to ingest the existing Pub/Sub subscription to the existing BigQuery table.

B. Create a new BigQuery table by using customer-managed encryption keys (CMEK), and migrate the data from the old BigQuery table.

C. Create a new Pub/Sub topic with CMEK and use the existing BigQuery table by using Google-managed encryption key.

D. Create a new BigQuery table and Pub/Sub topic by using customer-managed encryption keys (CMEK), and migrate the data from the old BigQuery table.

Show Suggested Answer

by 👤 **Smakyel79** at *Jan. 7, 2024, 5:14 p.m.*

Comments

Type your comment...

Submit

👤 **raaad** `Highly Voted 👍` 1 year, 3 months ago

Selected Answer: B

- New BigQuery Table with CMEK: This option involves creating a new BigQuery table configured to use a CMEK from Cloud KMS. It directly addresses the need to use a CMEK for data at rest in BigQuery.
- Migrate Data: Migrating data from the old table (encrypted with a Google-managed key) to the new table (encrypted with CMEK) ensures that all existing data complies with the new policy.

👍 ↩ 🚩 upvoted 11 times

    👤 **Matt_108** 1 year, 3 months ago

    But also pub/sub has some data at rest, e.g. messages with retention period.
    To comply with the organisation policy, we need to adapt also pub/sub

    👍 ↩ 🚩 upvoted 6 times

        👤 **AllenChen123** 1 year, 3 months ago

        No, "The ingested data is encrypted with a Google-managed encryption key", target is ingested data in BigQuery.

        👍 ↩ 🚩 upvoted 2 times

        👤 **ML6** 1 year, 2 months ago

        Correct, but the question states 'use keys from a centralized Cloud KMS project', so only D is correct.

        👍 ↩ 🚩 upvoted 3 times

            👤 **cloud_rider** 5 months, 1 week ago

            PubSub is an application and holds data on the fly, this data does not mean data at rest. The data that is ingested in GSC only means data at rest so B is the right answer.

            👍 ↩ 🚩 upvoted 1 times

                👤 **Blackstile** 2 months, 1 week ago

                The question did not say anything about the retention policy. Therefore, the correct answer is B.
                A tip for the exam: never answer what was not asked.

                👍 🚩 upvoted 1 times

👤 **Matt_108** `Highly Voted 👍` 1 year, 3 months ago

Selected Answer: D

Option D - I get the discussion about B and D, but also pub/sub has some data at rest, e.g. messages with retention period.
To comply with the organisation policy, we need to adapt also pub/sub

👍 ↩ 🚩 upvoted 8 times

👤 **Blackstile** `Most Recent ⊙` 2 months, 1 week ago

The question did not say anything about the retention policy. Therefore, the correct answer is B.
A tip for the exam: never answer what was not asked.

👍 ↩ 🚩 upvoted 1 times

👤 **plum21** 3 months ago

Selected Answer: D

There is data at rest in Pub/Sub, which is stated here in the docs: https://cloud.google.com/pubsub/docs/encryption
At rest data -> Application layer -> CMEK encryption

👍 ↩ 🚩 upvoted 2 times

👤 **Pime13** 3 months, 4 weeks ago

Selected Answer: B

B.
There is no need to create a new pubsub topic since it can be updated with the note that change is not retroactive.
https://cloud.google.com/pubsub/docs/encryption#update_cmek_for_a_topic

👍 ↩ 🚩 upvoted 1 times

👤 **m_a_p_s** 4 months, 3 weeks ago

Selected Answer: B

B. You don't need to create a new topic in order to use the new CMEK. Existing topic can be updated to use the new key:
https://cloud.google.com/pubsub/docs/encryption#update_cmek_for_a_topic

👍 ↩ 🚩 upvoted 1 times

👤 **SamuelTsch** 6 months, 1 week ago

Selected Answer: B

should be B. Pub/Sub is not designed for storing data at rest.

👍 ↩ 🚩 upvoted 2 times

👤 **gr3yWind** 6 months, 1 week ago

Agree with raaad

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **shanks_t** 8 months, 2 weeks ago

Requirement for Cloud KMS keys: The new organization policy requires using keys from a centralized Cloud KMS project for encrypting data at rest. This necessitates the use of customer-managed encryption keys (CMEK).
BigQuery table encryption: The existing BigQuery table is encrypted with a Google-managed key. To meet the new policy, a new table needs to be created with CMEK.
Pub/Sub topic encryption: Since the data is ingested directly from a Pub/Sub subscription, the Pub/Sub topic also needs to use CMEK to ensure end-to-end encryption with customer-managed keys.
Data migration: The existing data in the old BigQuery table needs to be migrated to the new CMEK-encrypted table to ensure all data complies with the new policy

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **carmltekai** 9 months, 3 weeks ago

"The best solution here is B. Create a new BigQuery table by using customer-managed encryption keys (CMEK), and migrate the data from the old BigQuery table.

Here's why:

Customer-Managed Encryption Keys (CMEK): CMEKs allow you to have granular control over your encryption keys, complying with the organization's policy to use keys from a centralized Cloud KMS project.
Data Migration: Since the data in the existing table is already encrypted with a Google-managed key, you cannot retroactively change the encryption key for that table. Migrating the data to a new table with the correct encryption is the most efficient way to meet compliance.

👍 ↩ 🚩 upvoted 2 times

    ☐ 👤 **carmltekai** 9 months, 3 weeks ago

    Why other options aren't suitable:

    A: Dataflow can't retroactively change the encryption of data that's already in BigQuery.
    C: Creating a new Pub/Sub topic with CMEK wouldn't address the data that's already in BigQuery.
    D: While creating a new Pub/Sub topic might be useful in the long run, it's not necessary for solving the immediate compliance issue with the existing data."

    👍 ↩ 🚩 upvoted 1 times

        ☐ 👤 **iooj** 9 months ago

        You have some data in Pub/Sub at rest as well which is immediate compliance issue.

        👍 ↩ 🚩 upvoted 1 times

☐ 👤 **Anudeep58** 10 months, 3 weeks ago

D. Create a new BigQuery table and Pub/Sub topic by using customer-managed encryption keys (CMEK), and migrate the data from the old BigQuery table.

This approach comprehensively addresses the requirement to use CMEK from a centralized Cloud KMS project for encrypting data at rest:

Create a new Pub/Sub topic configured to use CMEK from the centralized Cloud KMS project.
Create a new BigQuery table with CMEK enabled, using the same centralized Cloud KMS project.
Update the ingestion process to use the new Pub/Sub topic to feed data into the new BigQuery table.
Migrate existing data from the old BigQuery table to the new BigQuery table to ensure all data complies with the new encryption policy.

👍 ↩ 🚩 upvoted 3 times

☐ 👤 **AlizCert** 11 months ago

B, been there, done that...

👍 ↩ 🚩 upvoted 2 times

    ☐ 👤 **AlizCert** 11 months ago

    sry, I mean D

    👍 ↩ 🚩 upvoted 2 times

☐ 👤 **josech** 11 months, 2 weeks ago

BigQuery and Pub/Sub shall be encrypted using CMEK using new versions of each one.
https://cloud.google.com/pubsub/docs/encryption#using-cmek

👍 ↩ 🏳 **upvoted 3 times**

⊟ 👤 **chrissamharris** 11 months, 3 weeks ago

Selected Answer: B

Data at rest in requirement = Big Query ONLY.

Pub/Sub is data in movement - overkill for the solution

👍 ↩ 🏳 **upvoted 2 times**

⊟ 👤 **f74ca0c** 11 months, 3 weeks ago

Selected Answer: D

D- BigQuery and Pub/sub are automatically encrypted but here we need to apply a more secured policy by using CMEK so we need to use it for bigquery and pub/sub to meet this policy

👍 ↩ 🏳 **upvoted 1 times**

⊟ 👤 **LaxmanTiwari** 1 year ago

Selected Answer: B

B. Create a new BigQuery table by using customer-managed encryption keys (CMEK), and migrate the data from the old BigQuery table. Most Voted

👍 ↩ 🏳 **upvoted 2 times**

    ⊟ 👤 **LaxmanTiwari** 1 year ago

    it should be B as the data in pub sub is already encrypted , please read it carefully and use Copilot or chat gpt to have confirmation.

    👍 ↩ 🏳 **upvoted 1 times**

⊟ 👤 **amanbawa96** 1 year, 1 month ago

Selected Answer: B

BigQuery allows you to encrypt data at rest using either Google-managed encryption keys or customer-managed encryption keys (CMEK) from Cloud KMS.
Since the new policy requires using keys from a centralized Cloud KMS project, you need to create a new BigQuery table that is configured to use CMEK for encryption.
After creating the new table with CMEK, you can migrate the data from the old table (encrypted with Google-managed keys) to the new table (encrypted with CMEK).
This approach ensures that the data in the BigQuery table is encrypted using the required CMEK while preserving the existing data.

Creating a new BigQuery table and Pub/Sub topic with CMEK is not necessary because the focus is on encrypting the data at rest in BigQuery. The existing Pub/Sub subscription can still be used to ingest data into the new BigQuery table.

👍 ↩ 🏳 **upvoted 1 times**

Load full discussion…