◐ **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 319 DISCUSSION**

Actual exam question from Google's Professional Data Engineer

Question #: 319

Topic #: 1

[All Professional Data Engineer Questions]

You are preparing an organization-wide dataset. You need to preprocess customer data stored in a restricted bucket in Cloud Storage. The data will be used to create consumer analyses. You need to follow data privacy requirements, including protecting certain sensitive data elements, while also retaining all of the data for potential future use cases. What should you do?
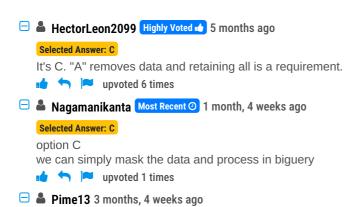
A. Use the Cloud Data Loss Prevention API and Dataflow to detect and remove sensitive fields from the data in Cloud Storage. Write the filtered data in BigQuery.

B. Use customer-managed encryption keys (CMEK) to directly encrypt the data in Cloud Storage. Use federated queries from BigQuery. Share the encryption key by following the principle of least privilege.

C. Use Dataflow and the Cloud Data Loss Prevention API to mask sensitive data. Write the processed data in BigQuery.

D. Use Dataflow and Cloud KMS to encrypt sensitive fields and write the encrypted data in BigQuery. Share the encryption key by following the principle of least privilege.

Show Suggested Answer

by 👤 **HectorLeon2099** at *Dec. 4, 2024, 5:49 p.m.*

Comments

```
Type your comment...
```

Submit

⊟ 👤 **HectorLeon2099** `Highly Voted 👍` 5 months ago

`Selected Answer: C`

It's C. "A" removes data and retaining all is a requirement.

👍 ↩ 🏳 **upvoted 6 times**

⊟ 👤 **Nagamanikanta** `Most Recent ⊘` 1 month, 4 weeks ago

`Selected Answer: C`

option C
we can simply mask the data and process in biguery

👍 ↩ 🏳 **upvoted 1 times**

⊟ 👤 **Pime13** 3 months, 4 weeks ago

`Selected Answer: C`

C. Use Dataflow and the Cloud Data Loss Prevention API to mask sensitive data. Write the processed data in BigQuery.

This approach ensures that sensitive data elements are protected through masking, which meets data privacy requirements. At the same time, it retains the data in a usable form for future analyses

👍 ↩ 🏳 **upvoted 3 times**