

[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 217 DISCUSSION

Actual exam question from Google's Professional Data Engineer

Question #: 217

Topic #: 1

[\[All Professional Data Engineer Questions\]](#)

You have a BigQuery table that contains customer data, including sensitive information such as names and addresses. You need to share the customer data with your data analytics and consumer support teams securely. The data analytics team needs to access the data of all the customers, but must not be able to access the sensitive data. The consumer support team needs access to all data columns, but must not be able to access customers that no longer have active contracts. You enforced these requirements by using an authorized dataset and policy tags. After implementing these steps, the data analytics team reports that they still have access to the sensitive columns. You need to ensure that the data analytics team does not have access to restricted data. What should you do? (Choose two.)

- A. Create two separate authorized datasets; one for the data analytics team and another for the consumer support team.
- B. Ensure that the data analytics team members do not have the Data Catalog Fine-Grained Reader role for the policy tags.
- C. Replace the authorized dataset with an authorized view. Use row-level security and apply filter_expression to limit data access.
- D. Remove the bigquery.dataViewer role from the data analytics team on the authorized datasets.
- E. Enforce access control in the policy tag taxonomy.

[Show Suggested Answer](#)

by [e70ea9e](#) at Dec. 30, 2023, 9:42 a.m.

Comments



Type your comment...

Submit

  **qq589539483084gfrgrgr** Highly Voted 1 year, 3 months ago

Option B & E

   upvoted 7 times

  **datapassionate** Highly Voted 1 year, 3 months ago

Selected Answer: E

B& E

<https://cloud.google.com/bigquery/docs/column-level-security-intro>

   upvoted 5 times

  **Lenifia** Most Recent 10 months ago

Selected Answer: A

the correct options are:

A. Create two separate authorized datasets; one for the data analytics team and another for the consumer support team.
C. Replace the authorized dataset with an authorized view. Use row-level security and apply filter_expression to limit data access.

   upvoted 2 times

  **Lenifia** 10 months ago

Explanation of why other options are incorrect:

B. Ensure that the data analytics team members do not have the Data Catalog Fine-Grained Reader role for the policy tags: This role relates to viewing data in Data Catalog based on policy tags, not directly controlling access to BigQuery data.

D. Remove the bigquery.dataViewer role from the data analytics team on the authorized datasets: Removing this role would block all access to the dataset, which is too restrictive if they still need access to non-sensitive columns.

E. Enforce access control in the policy tag taxonomy: While policy tags are used to enforce access controls, simply enforcing controls in the taxonomy does not directly address the issue of sensitive data access in BigQuery.

   upvoted 2 times

  **GCP001** 1 year, 3 months ago

Selected Answer: E

B & E

B - It will ensure they don't have access to secure columns

E- It will allow to enforce column level security

Ref - <https://cloud.google.com/bigquery/docs/column-level-security-intro>

   upvoted 3 times

  **Matt_108** 1 year, 3 months ago

Selected Answer: B

Option B& E to me

   upvoted 2 times

  **MaxNRG** 1 year, 3 months ago

Selected Answer: A

A & B

The current setup is not effective because the data analytics team still has access to the sensitive columns despite using an authorized dataset and policy tags. This indicates that the policy tags are not being enforced properly, and the data analytics team members are able to view the tags and gain access to the sensitive data.

Separating the data into two distinct authorized datasets is a better approach because it isolates the sensitive data from the non-sensitive data. This prevents the data analytics team from accessing the sensitive columns directly, even if they have access to the authorized dataset for general customer data.

Additionally, revoking the Data Catalog Fine-Grained Reader role from the data analytics team members ensures that they cannot view or modify the policy tags. This limits their ability to bypass the access control imposed by the authorized dataset and policy tags.

   upvoted 3 times



  **Matt_108** 1 year, 3 months ago

Max I feel like it's more B&E.

I do agree on the revoking Data Catalog Fine-grained reader role to avoid the data analytics team to read policy tags



metadata, but if the tags are setup as stated, it's just missing the enforcement of the policy tags themselves. Creating 2 auth dataset is not efficient on big datasets and Data catalog+ policy tags are built to manage these situations. Don't you agree?

   upvoted 3 times

  **imiu** 1 year, 4 months ago

And the second answer? One is option B and the other is option D maybe?

   upvoted 1 times

  **raaad** 1 year, 4 months ago

Selected Answer: B

- The Data Catalog Fine-Grained Reader role allows users to read metadata that is restricted by policy tags.
- If members of the data analytics team have this role, they might bypass the restrictions set by policy tags.
- Ensuring they do not have this role will help enforce the restrictions intended by the policy tags.

   upvoted 3 times

  **e70ea9e** 1 year, 4 months ago

Selected Answer: B

Prevents data analytics team members from viewing sensitive data, even if it's tagged.
Restricts access to policy tags themselves, ensuring confidentiality of sensitive information.

   upvoted 2 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses

