

🔗 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 16 DISCUSSION

Actual exam question from Google's Professional Data Engineer

Question #: 16

Topic #: 1

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

Your startup has never implemented a formal security policy. Currently, everyone in the company has access to the datasets stored in Google BigQuery. Teams have freedom to use the service as they see fit, and they have not documented their use cases. You have been asked to secure the data warehouse. You need to discover what everyone is doing. What should you do first?

- A. Use Google Stackdriver Audit Logs to review data access.
- B. Get the identity and access management (IAM) policy of each table
- C. Use Stackdriver Monitoring to see the usage of BigQuery query slots.
- D. Use the Google Cloud Billing API to see what account the warehouse is being billed to.

[Show Suggested Answer](#)

by [deleted] at March 16, 2020, 11:25 a.m.

Comments

Type your comment...

[Submit](#)

👤 **Radhika7983** Highly Voted 4 years, 6 months ago

Table access control is now possible in big query. However, before even checking table access control permission which is not set by the company as a formal security policy yet. we need to first understand by looking at the big query immutable

network by the company as a formal security policy yet, we need to first understand by looking at the big query immutable audit logs as who is accessing what DAT sets and tables. Based on the information, access control policy at dataset and table level can be set.

So the correct answer is A

   upvoted 7 times

  **Cloud_Student** Highly Voted  4 years, 9 months ago

A - need to check first who is accessing which table

   upvoted 5 times

  **cqrm3n** Most Recent  3 months, 2 weeks ago

Selected Answer: A

Stackdriver Audit Logs is now called Cloud Audit logs. To secure a data warehouse, the first step is to understand how the datasets are being accessed and used. Cloud Audit logs can track data access as it provides a detailed log of all data access operations.

   upvoted 1 times

  **MaxNRG** 7 months, 1 week ago

A is correct because this is the best way to get granular access to data showing which users are accessing which data.

B is not correct because we already know that all users already have access to all data, so this information is unlikely to be useful. It will also not show what users have done, just what they can do.

C is not correct because slot usage will not inform security policy.

D is not correct because a billing account is typically shared among many people and will only show the amount of data queried and stored

<https://cloud.google.com/bigquery/docs/reference/auditlogs/#mapping-audit-entries-to-log-streams>

<https://cloud.google.com/bigquery/docs/monitoring#slots-available>

   upvoted 2 times

  **rocky48** 7 months, 1 week ago

Selected Answer: A

A. Use Google Stackdriver Audit Logs to review data access.

Reviewing the audit logs provides visibility into who is accessing your data, when they are doing so, and what actions they are taking within BigQuery. This is crucial for understanding current data usage and potential security risks.

Option B (getting the IAM policy of each table) is important but more focused on controlling access rather than discovering what everyone is currently doing.

Option C (using Stackdriver Monitoring to see query slots usage) can help with monitoring and optimizing your BigQuery usage but doesn't provide a comprehensive view of what users are doing with the data.

Option D (using the Google Cloud Billing API) is more related to tracking billing information rather than understanding what users are doing with the data.

   upvoted 2 times

  **rtcpost** 7 months, 1 week ago

Selected Answer: A

To begin securing your data warehouse in Google BigQuery and gain insights into what everyone is doing with the datasets, the first step you should take is:

A. Use Google Stackdriver Audit Logs to review data access.

Reviewing the audit logs provides visibility into who is accessing your data, when they are doing so, and what actions they are taking within BigQuery. This is crucial for understanding current data usage and potential security risks.

Option B (getting the IAM policy of each table) is important but more focused on controlling access rather than discovering what everyone is currently doing.

Option C (using Stackdriver Monitoring to see query slots usage) can help with monitoring and optimizing your BigQuery usage but doesn't provide a comprehensive view of what users are doing with the data.

Option D (using the Google Cloud Billing API) is more related to tracking billing information rather than understanding what users are doing with the data.

   upvoted 4 times

  **NeoNitin** 7 months, 1 week ago

A. Use Google Stackdriver Audit Logs to review data access.

In this scenario, you have been asked to secure the data warehouse in Google BigQuery. To do that, you first need to understand what everyone is doing with the data, i.e., who is accessing it and what actions they are performing. Google Stackdriver Audit Logs can provide you with a detailed record of all the data access and actions taken by users in Google

BigQuery. It's like having a logbook that keeps track of who enters the library, which books they read, and what they do with the books.

C just give how many people accessing the same dataset at given time

C. Another tool you have is called "Stackdriver Monitoring." It helps you see how many people are using the library at the same time. It's like knowing how many readers are in the library at any given moment.


   upvoted 1 times

  **RT_G** 7 months, 1 week ago

Selected Answer: A

A - Since the question is to discover what everyone is doing. Also the question has indicated that no security policies have been implemented.

   upvoted 1 times

  **rtcpost** 7 months, 1 week ago

Selected Answer: A

A. Use Google Stackdriver Audit Logs to review data access.

Reviewing the audit logs provides visibility into who is accessing your data when they are doing so, and what actions they are taking within BigQuery. This is crucial for understanding current data usage and potential security risks.


   upvoted 1 times

  **philli1011** 1 year, 3 months ago

A is the answer.

But recently, I think Dataplex is used for data governance .

   upvoted 1 times

  **imran79** 1 year, 7 months ago

A. Use Google Stackdriver Audit Logs to review data access.

Stackdriver Audit Logs provide detailed logs on who accessed what resources and when, including data in BigQuery. Reviewing these logs will give you insight into which users and service accounts are accessing datasets, what operations they are performing, and when these accesses occur. This would be a crucial first step in understanding current usage and subsequently in crafting a security policy.

   upvoted 1 times

  **suku2** 1 year, 7 months ago

Selected Answer: A

Stackdriver audit logs is where we will view which datasets are being accessed by whom

   upvoted 1 times

  **bha11111** 2 years, 1 month ago

Selected Answer: A

In order to take a decision you need to analyze the access logs

   upvoted 1 times

  **niketd** 2 years, 2 months ago

"Discover what everyone is doing" will happen through Audit logs, hence correct answer is A

   upvoted 1 times

  **Nirca** 2 years, 4 months ago

Selected Answer: A

"...to secure the data warehouse" is to list all tables/views/Mviews VS. who is accessing these objects. Slot info is not relevant.

   upvoted 1 times

  **fedebos8** 2 years, 5 months ago

Selected Answer: A

A is correct.

   upvoted 1 times

  **nkunwar** 2 years, 7 months ago

Selected Answer: A

Audit log ..logs activities against resources , is the best place to discover about activities against BQ

   upvoted 1 times

[Load full discussion...](#)



Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

