Google Discussions

EXAM PROFESSIONAL DATA ENGINEER TOPIC 1 QUESTION 200 DISCUSSION

Actual exam question from Google's Professional Data Engineer
Question #: 200
Topic #: 1
[All Professional Data Engineer Questions]

Government regulations in the banking industry mandate the protection of clients' personally identifiable information (PII). Your company requires PII to be access controlled, encrypted, and compliant with major data protection standards. In addition to using Cloud Data Loss Prevention (Cloud DLP), you want to follow
Google-recommended practices and use service accounts to control access to PII. What should you do?

A. Assign the required Identity and Access Management (IAM) roles to every employee, and create a single service account to access project resources.

B. Use one service account to access a Cloud SQL database, and use separate service accounts for each human user.

C. Use Cloud Storage to comply with major data protection standards. Use one service account shared by all users.

D. Use Cloud Storage to comply with major data protection standards. Use multiple service accounts attached to IAM groups to grant the appropriate access to each group.

Show Suggested Answer

by ducc at *Sept. 3, 2022, 4:04 a.m.*

Comments

Type your comment...

Submit

NicolasN Highly Voted 1 year, 11 months ago

Selected Answer: A

[A] is the only acceptable answer.
[B] rejected (no need to elaborate)
[C] and [D] rejected. Why should we be obliged to use Cloud Storage? Other storage options in Google Cloud aren't compliant with "major data protection standards"?
==========
[D] has another rejection reason, the following quotes:
From <https://cloud.google.com/iam/docs/service-accounts>: "You can add service accounts to a Google group, then grant roles to the group. However, adding service accounts to groups is not a best practice. Service accounts are used by applications, and each application is likely to have its own access requirements"
From <https://cloud.google.com/iam/docs/best-practices-service-accounts#groups>: "Avoid using groups for granting service accounts access to resources"

upvoted 18 times

MaxNRG 10 months, 2 weeks ago

A single shared service account or granting every employee direct access violates security best practices, so not [A].

upvoted 3 times

KC_go_reply 1 year, 4 months ago

Rejecting C + D solely based on Cloud Storage, which CAN be used in this scenario, is not sound reasoning.

upvoted 5 times

cetanx Highly Voted 1 year, 9 months ago

Selected Answer: D

for A: please refer to this link below which suggests "Sharing a single service account across multiple applications can complicate the management of the service account" - meaning it's not a best practice.
https://cloud.google.com/iam/docs/best-practices-service-accounts#single-purpose
Also, what if we have hundreds of users, does it really make sense to manage each user's IAM individually?

for D: it's indeed not one of the best practices but I believe it's much more managable and better than A

upvoted 14 times

skhaire Most Recent 2 months ago

Selected Answer: D

Without Cloud storage, I believe just DLP does not provide encryption. DLP can redact or mask data, not encrypt it. Only on Cloud storage, encryption can be performed. So seems like option D is the closest choice, though service accounts should NOT be attached to IAM groups.

upvoted 1 times

MaxNRG 10 months, 2 weeks ago

Selected Answer: D

To align with Google's recommended practices for managing access to personally identifiable information (PII) in compliance with banking industry regulations, let's analyze the options:

A. Assign the required IAM roles to every employee, and create a single service account to access project resources: While assigning specific IAM roles to employees is a good practice for access control, using a single service account for all access to PII is not ideal. Service accounts should be used for applications and automated processes, not as a shared account for multiple users or employees.

upvoted 2 times

MaxNRG 10 months, 2 weeks ago

B. Use one service account to access a Cloud SQL database, and use separate service accounts for each human user: Again, service accounts are intended for automated tasks or applications, not for individual human users. Assigning separate service accounts to each human user is not a recommended practice and does not align with the principle of least privilege.

upvoted 1 times

MaxNRG 10 months, 2 weeks ago

C. Use Cloud Storage to comply with major data protection standards. Use one service account shared by all users: Using Cloud Storage can indeed help comply with data protection standards, especially when configured correctly with encryption and access controls. However, sharing a single service account among all users is not a best practice. It goes against the principle of least privilege and does not provide adequate granularity for access control.

upvoted 1 times

MaxNRG 10 months, 2 weeks ago

D. Use Cloud Storage to comply with major data protection standards. Use multiple service accounts attached to

D. Use Cloud Storage to comply with major data protection standards. Use multiple service accounts attached to IAM groups to grant the appropriate access to each group: This approach is more aligned with best practices. Using Cloud Storage can ensure compliance with data protection standards. Creating multiple service accounts, each with specific access controls attached to different IAM groups, allows for more granular and controlled access to PII. This setup adheres to the principle of least privilege, ensuring that each service (or group of services) only has access to the resources necessary for its function.

Based on these considerations, option D is the most appropriate choice. It ensures compliance with data protection standards, uses Cloud Storage for secure data management, and employs multiple service accounts tied to IAM groups for granular access control, aligning well with Google-recommended practices and regulatory requirements in the banking industry.

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: D

D. Not the best, but seems most reasonable out of 4.

upvoted 2 times

vamgcp 1 year, 3 months ago

Selected Answer: D

Option D - Using multiple service accounts attached to IAM groups helps enforce the principle of least privilege. Each group can be assigned only the necessary permissions, reducing the risk of unauthorized access to sensitive data.

upvoted 2 times

MoeHaydar 1 year, 3 months ago

Selected Answer: D

Google Cloud Storage is designed to comply with major data protection standards. Creating multiple service accounts and attaching them to IAM groups provides granular control over who has access to the data. This approach is aligned with the principle of least privilege, a security best practice where a user is given the minimum levels of access necessary to complete their tasks.

upvoted 2 times

KC_go_reply 1 year, 4 months ago

Selected Answer: D

It´s not A because
1. assigning IAM roles to single users instead of groups is not Google best practice, and
2. the question explicitly states that we want to use multiple service accounts.

upvoted 2 times

Ender_H 1 year, 5 months ago

Selected Answer: D

D. Use Cloud Storage to comply with major data protection standards. Use multiple service accounts attached to IAM groups to grant the appropriate access to each group.

- Google Cloud Storage is built for secure and compliant data storage. It supports compliance with major data protection standards, which is essential in the banking industry where data protection regulations are stringent.
- Service accounts in Google Cloud represent non-human users (applications or services) that need to authenticate and be authorized to access specific Google Cloud resources.
- Creating multiple service accounts attached to IAM groups allows you to manage access control in a granular manner. This follows the principle of least privilege, providing each group with only the permissions they need to perform their tasks, which is a recommended practice for managing access to sensitive data like PII.

upvoted 2 times

Ender_H 1 year, 5 months ago

D. Use Cloud Storage to comply with major data protection standards. Use one service account shared by all users.

- Sharing one service account among all users is not a secure practice. It goes against the principle of least privilege and does not allow for granular control over access permissions. If the shared service account were to be compromised, all resources accessible by the account would be at risk.

upvoted 1 times

juliobs 1 year, 7 months ago

Why are so many questions like this?
None of the answers is best practice.

upvoted 6 times

alfguemat 11 months, 1 week ago

I would like to ask your question to those who decide the questions on the exams. I don't understand what they're trying to do, many of the questions cause divided responses, because they don't have a clear answer. The certification process is

a waste of time.

upvoted 1 times

SuperVee 1 year, 7 months ago

Selected Answer: D

I could be wrong but I think the wording in D caused this confusion, so it is an English problem. -- "Use multiple service accounts attached to IAM groups to grant the appropriate access to each group"
I believe what D really means is that you can create a group for a bunch of people who only need access to resource A, so attach a Service account to the group and service account only have access to A.
Then you create another group for another bunch of people who only need access to resource B, so attach a service account to this group. this service account can only access to B.
So each group/service account has a very specific access target, and purpose of the group is very narrowly defined which is allowed by best practice. However, wording in option D merged all these into one sentence causing confusions.
Option A is an administrative nightmare to manage IAM for a larger user population which is actually also against GCP best practices.

upvoted 5 times

Aamir185 1 year, 8 months ago

Selected Answer: D

D it is

upvoted 2 times

AzureDP900 1 year, 10 months ago

D is right

upvoted 1 times

Amar2022 1 year, 10 months ago

Selected Answer: A

A is the correct one

upvoted 1 times

jkhong 1 year, 10 months ago

Selected Answer: A

Agree with NicolasN, D is bad practice. For D this may result in permission creep, where a group is granted access to an increasing number of resources. Only grant service accounts specific access to resources.

upvoted 1 times

odacir 1 year, 10 months ago

Selected Answer: A

A is the answer, as NicalsN says.
https://cloud.google.com/iam/docs/service-accounts#groups

upvoted 1 times

Andrix2405 1 year, 10 months ago

Selected Answer: A

Avoid using groups for granting service accounts access to resources -> D

upvoted 2 times

Andrix2405 1 year, 10 months ago

Sorry A

upvoted 1 times

Load full discussion...