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 226 DISCUSSION

Actual exam question from Google's Professional Data Engineer

Question #: 226

Topic #: 1

[All Professional Data Engineer Questions]

Your organization has two Google Cloud projects, project A and project B. In project A, you have a Pub/Sub topic that receives data from confidential sources. Only the resources in project A should be able to access the data in that topic. You want to ensure that project B and any future project cannot access data in the project A topic. What should you do?

A. Add firewall rules in project A so only traffic from the VPC in project A is permitted.

B. Configure VPC Service Controls in the organization with a perimeter around project A.

C. Use Identity and Access Management conditions to ensure that only users and service accounts in project A. can access resources in project A.

D. Configure VPC Service Controls in the organization with a perimeter around the VPC of project A.

Show Suggested Answer

by e70ea9e at *Dec. 30, 2023, 9:52 a.m.*

Comments

Type your comment...

Submit

⊟ datapassionate Highly Voted 1 year, 3 months ago

Selected Answer: C

And I would agree with GPT. The question is about that who can do what within GCP environment. It's all about permissions and access management, not about networking.

upvoted 11 times

raaad Highly Voted 1 year, 4 months ago

Selected Answer: B

Option B:
-It allows us to create a secure boundary around all resources in Project A, including the Pub/Sub topic.
- It prevents data exfiltration to other projects and ensures that only resources within the perimeter (Project A) can access the sensitive data.
- VPC Service Controls are specifically designed for scenarios where you need to secure sensitive data within a specific context or boundary in Google Cloud.

upvoted 7 times

MithunDesai Most Recent 8 months, 3 weeks ago

Selected Answer: B

The best solution to prevent project B and any future projects from accessing data in project A&#x27;s Pub/Sub topic is B. Configure VPC Service Controls in the organization with a perimeter around project A.

upvoted 3 times

meh_33 8 months, 4 weeks ago

Selected Answer: B

B is correct Raaad is always right

upvoted 3 times

fabiogoma 11 months, 2 weeks ago

Selected Answer: B

Setting up a perimeter around project A is future proof, the question asks to "ensure that project B and any future project cannot access data in the project A topic", IAM is not future proof.

Reference: https://cloud.google.com/vpc-service-controls/docs/overview#isolate

p.s: VPC Service Controls is not the same thing as VPC, instead its a security layer on top of a VPC and it should be used together with IAM, not one or the other (https://cloud.google.com/vpc-service-controls/docs/overview#how-vpc-service-controls-works)

upvoted 4 times

virat_kohli 11 months, 2 weeks ago

Selected Answer: C

C. Use Identity and Access Management conditions to ensure that only users and service accounts in project A. can access resources in project A. [SIMPLE!!!]

upvoted 2 times

JyoGCP 1 year, 2 months ago

Selected Answer: B

I'll go with "B. Configure VPC Service Controls in the organization with a perimeter around project A."

upvoted 2 times

datapassionate 1 year, 3 months ago

GPT:
C. Use Identity and Access Management conditions to ensure that only users and service accounts in project A can access resources in project A.

Analysis: This is the most appropriate option. IAM allows you to define who (which users or service accounts) has what access to your GCP resources. By setting IAM policies with conditions specific to Project A, you can ensure that only designated entities within Project A have access to its resources, including the Pub/Sub topic.
D. Configure VPC Service Controls in the organization with a perimeter around the VPC of project A.

upvoted 1 times

datapassionate 1 year, 3 months ago

A. Add firewall rules in project A so only traffic from the VPC in project A is permitted.

Analysis: Firewall rules in GCP are used to control traffic to and from instances within Google Cloud Virtual Private Clouds (VPCs). However, they don't specifically control access to Pub/Sub resources. Pub/Sub access is managed through IAM, not VPC firewall rules.

upvoted 1 times

datapassionate 1 year, 3 months ago

B. Configure VPC Service Controls in the organization with a perimeter around project A.

Analysis: VPC Service Controls provide a security perimeter for your data, but they are more focused on preventing data exfiltration; this might be more complex and broader than necessary for the specific requirement of restricting access to a Pub/Sub topic.

upvoted 1 times

datapassionate 1 year, 3 months ago

D. Configure VPC Service Controls in the organization with a perimeter around the VPC of project A.

Analysis: Similar to option B, this is focused on securing network boundaries rather than specific resource access within GCP. While it could provide an additional layer of security, it's not the most direct way to control access to a specific Pub/Sub topic.

upvoted 1 times

e70ea9e 1 year, 4 months ago

Selected Answer: B

VPC Service Controls enforce a security perimeter around entire projects, ensuring that resources within project A (including the Pub/Sub topic) are inaccessible from any other project, including project B and future projects.
This aligns with the requirement to prevent cross-project access.

upvoted 4 times