← Google Discussions

Exam Professional Cloud Security Engineer All Questions
View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

📄 EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 93 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 93

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials.
What should you do?

A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.

B. Enable Domain Restricted Sharing Organization Policy and Bucket Policy Only on the Cloud Storage bucket.

C. Enable Private Access in Project A and B networks with strict firewall rules to allow communication between the networks.

D. Enable VPC Peering between Project A and B networks with strict firewall rules to allow communication between the networks.

Show Suggested Answer

by 👤 **Jerrard** at *Oct. 7, 2020, 9:03 p.m.*

Comments

Type your comment...

Submit

FatCharlie `Highly Voted 👍` 3 years, 8 months ago

The answer is A. This is question is covered by an example given for VPC Service Perimeters

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

👍 ↩ 🏳 upvoted 20 times

AzureDP900 1 year, 8 months ago

A is right

👍 ↩ 🏳 upvoted 2 times

---

alleinallein `Most Recent ⊙` 1 year, 3 months ago

Why not D?

👍 ↩ 🏳 upvoted 1 times

---

shayke 1 year, 7 months ago

`Selected Answer: A`

A - a classic VPCSC question

👍 ↩ 🏳 upvoted 2 times

AwesomeGCP 1 year, 9 months ago

`Selected Answer: A`

A. Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.

👍 ↩ 🏳 upvoted 3 times

---

cloudprincipal 2 years, 1 month ago

`Selected Answer: A`

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

👍 ↩ 🏳 upvoted 2 times

---

nilb94 2 years, 11 months ago

A - VPC Service Controls

👍 ↩ 🏳 upvoted 3 times

---

jeeet_ 3 years, 1 month ago

Answer is most positively A.
VPC service controls lets Security team create fine-grained Perimeter across projects within organization.
-> Security perimeter for API-Based services like Bigtable instances, Storage and Bigquery datasets.. are a kind of super powers for VPC Service control.
well in my test, I chose option B, but
Domain Restricted Organization policies are for limiting resource sharing based on domain.
so if you're out in internet, and have credentials you still can access resources based on your domain access level. So B option is wrong.

👍 ↩ 🏳 upvoted 2 times

HateMicrosoft 3 years, 4 months ago

The correct answer is: A
This is obtained by the VPC Service Controls by the perimeter setup.

Overview of VPC Service Controls
https://cloud.google.com/vpc-service-controls/docs/overview

👍 ↩ 🏳 upvoted 2 times

---

jonclem 3 years, 8 months ago

I would say option A is a better fit due to VPC Service Controls.

👍 ↩ 🏳 upvoted 3 times

---

jonclem 3 years, 8 months ago

I'd be inclined to agree, option B seems a better fit. Here's my reasoning behind it:
https://cloud.google.com/access-context-manager/docs/overview

👍 ↩ 🏳 upvoted 1 times

---

jonclem 3 years, 8 months ago

please ignore this comment, wrong question.

👍 ↩ 🏳 upvoted 1 times

---

saurabh1805 3 years, 9 months ago

what is being asked is data exfiltration as well and which can be only achieved via VPC permiter and created a bridge between both project.

👍 ↩ 🏳 upvoted 1 times

Ducle 3 years, 8 months ago

A is better

upvoted 2 times

Jerrard 3 years, 9 months ago

B. https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

upvoted 1 times

Ducle 3 years, 8 months ago

A is better

upvoted 2 times

Jerrard 3 years, 9 months ago