

🔗 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 113 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 113

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You are troubleshooting access denied errors between Compute Engine instances connected to a Shared VPC and BigQuery datasets. The datasets reside in a project protected by a VPC Service Controls perimeter. What should you do?

- A. Add the host project containing the Shared VPC to the service perimeter.
- B. Add the service project where the Compute Engine instances reside to the service perimeter.
- C. Create a service perimeter between the service project where the Compute Engine instances reside and the host project that contains the Shared VPC.
- D. Create a perimeter bridge between the service project where the Compute Engine instances reside and the perimeter that contains the protected BigQuery datasets.

[Show Suggested Answer](#)

by [👤 Tabayashi](#) at April 29, 2022, 3:18 a.m.

Comments

Type your comment...

[Submit](#)

🗨️ 👤 **risc** [Highly Voted](#) 👍 2 years, 9 months ago

Selected Answer: A

(A)

For VMs inside shared VPC, the host project needs to be added to the perimeter as well. I had real-life experience with this. However, this creates new security issues as all other VMs in other projects which are attached to shared subnets in the same host project then are also able to access the perimeter. Google recommends setting up Private Service Connect Endpoints to achieve subnet segregation for VPC-SC usage with Host projects.

   upvoted 13 times

  **BPzen** **Most Recent** 8 months ago

Selected Answer: D

Why D. Create a perimeter bridge is Correct:
Problem Analysis:

The BigQuery datasets reside within a service perimeter.

The Compute Engine instances are in a service project connected to a Shared VPC, and they are outside the BigQuery perimeter.

Access is being denied because the Compute Engine instances are not within the same service perimeter as the BigQuery datasets.

Solution:

A perimeter bridge allows resources in the service project (where Compute Engine instances reside) to securely communicate with resources in the service perimeter (where the BigQuery datasets reside).

This ensures compliance with VPC Service Controls while allowing the required access.

   upvoted 2 times

  **SQLbox** 10 months, 2 weeks ago

VPC Service Controls are designed to protect Google Cloud resources (such as BigQuery) from unauthorized access by restricting access to those resources based on service perimeters.

- In this scenario, the Compute Engine instances are trying to access BigQuery datasets, which are within a VPC Service Controls perimeter.
- Compute Engine instances are in a service project, and to allow them to access resources (BigQuery) within the service perimeter, that service project must be added to the service perimeter.

   upvoted 1 times

  **winston9** 1 year, 5 months ago

Selected Answer: A

It's A



check this: <https://cloud.google.com/compute/docs/instances/protecting-resources-vpc-service-controls#shared-vpc-with-vpc-service-controls>

   upvoted 1 times

  **b6f53d8** 1 year, 6 months ago

Why not D ? In my opinion, we need A and B to resolve issue, so why not D ?

   upvoted 1 times

  **desertlotus1211** 1 year, 11 months ago

Answer A:

Select the projects that you want to secure within the perimeter.

Click Projects.

In the Add Projects window, select the projects you want to add.

If you are using Shared VPC, make sure to add the host project and service projects.

<https://cloud.google.com/run/docs/securing/using-vpc-service-controls>

   upvoted 1 times

  **bruh_1** 2 years, 3 months ago

B. Add the service project where the Compute Engine instances reside to the service perimeter.

Explanation:



The VPC Service Controls perimeter restricts data access to a set of resources within a VPC network. To allow Compute Engine instances in the service project to access BigQuery datasets in the protected project, the service project needs to be added to the service perimeter.

   upvoted 4 times

  **gcpengineer** 2 years, 2 months ago

but the instance will communicate via the host project from the shared subnet

   upvoted 2 times

  **Ric350** 2 years, 4 months ago

It's A and here's why. The question establishes there's already VPC Service Control Perimeter and a shared VPC. Since the dataset resides in a project protected by a VPC SC perimeter, you wouldn't create a NEW service perimeter. Further, since we know per the question there's a SHARED VPC established & you're TROUBLESHOOTING, per the doc below, it makes sense that they're both not in the same VPC SC perimeter and why access is failing.
https://cloud.google.com/vpc-service-controls/docs/troubleshooting#shared_vpc

The question isn't clear where the compute engine instance or dataset live in respect to the VPC SC perimeter. But it's clear, they are both NOT in the same VPC SC perimeter and the question states the BQ dataset is already protected. So B, C and D are wrong and only A ensure BOTH are in the same VPC SC perimeter regardless of which ones live in the host or service project.



   upvoted 2 times

  **Littleivy** 2 years, 8 months ago

Selected Answer: A

As the scenario is for troubleshooting, I'll choose A as answer since it's more likely people would forget to include host project to the service perimeter

   upvoted 2 times

  **AzureDP900** 2 years, 8 months ago

A. Add the host project containing the Shared VPC to the service perimeter. Looks good to me based on requirements

   upvoted 2 times

  **soltium** 2 years, 9 months ago

Selected Answer: B

Weird question, you need A n B.
I'll choose B.

   upvoted 3 times

  **AwesomeGCP** 2 years, 9 months ago

Selected Answer: A

A. Add the host project containing the Shared VPC to the service perimeter.

   upvoted 1 times

  **zelck** 2 years, 10 months ago

Selected Answer: A

A is the answer.

<https://cloud.google.com/vpc-service-controls/docs/service-perimeters#secure-google-managed-resources>
If you're using Shared VPC, you must include the host project in a service perimeter along with any projects that belong to the Shared VPC.



   upvoted 3 times

  **GHOST1985** 2 years, 10 months ago

Selected Answer: A

"If you're using Shared VPC, you must include the host project in a service perimeter along with any projects that belong to the Shared VPC" => <https://cloud.google.com/vpc-service-controls/docs/service-perimeters>

   upvoted 1 times

  **Chute5118** 3 years ago

Selected Answer: B

"If you're using Shared VPC, you must include the host project in a service perimeter along with any projects that belong to the Shared VPC."

<https://cloud.google.com/vpc-service-controls/docs/service-perimeters>

B

   upvoted 2 times




  **GHOST1985** 2 years, 10 months ago

i think you mean Answer A :)

   upvoted 1 times

  **Aiffone** 3 years ago

i think the Answer should be C (a combination of A and B)

   upvoted 1 times

  **mikesp** 3 years, 1 month ago

Selected Answer: B

Selected Answer: B

Change my answer.

   upvoted 2 times

[Load full discussion...](#)



Platform

> [Home](#)

> [All Exams](#)

> [Examtopics PRO](#)

> [Training Courses](#)



© 2024 ExamTopics