EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 220 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 220

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You manage one of your organization's Google Cloud projects (Project A). A VPC Service Control (SC) perimeter is blocking API access requests to this project, including Pub/Sub. A resource running under a service account in another project (Project B) needs to collect messages from a Pub/Sub topic in your project. Project B is not included in a VPC SC perimeter. You need to provide access from Project B to the Pub/Sub topic in Project A using the principle of least privilege.

What should you do?

A. Configure an ingress policy for the perimeter in Project A, and allow access for the service account in Project B to collect messages.

B. Create an access level that allows a developer in Project B to subscribe to the Pub/Sub topic that is located in Project A.

C. Create a perimeter bridge between Project A and Project B to allow the required communication between both projects.

D. Remove the Pub/Sub API from the list of restricted services in the perimeter configuration for Project A.

Show Suggested Answer

by gcp4test at *Aug. 4, 2023, 2:57 p.m.*

Comments

Type your comment...

Submit

MoAk 8 months, 1 week ago

Selected Answer: A

The answer is Answer A. Why? Because Project B does not belong in a service perimeter itself. You cannot create a perimeter bridge without being part of a service perimeter. Answer is A.

https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters

upvoted 1 times

Sundar_Pichai 11 months, 1 week ago

Selected Answer: A

I spent some time going back and forth on this question. I believe the Answer is A.

C can't be right because project B isn't part of another perimeter.

upvoted 2 times

jujanoso 1 year ago

Selected Answer: A

Principle of Least Privilege: By configuring an ingress policy, you can precisely define which specific service account from Project B is allowed to access the Pub/Sub topic in Project A. This approach ensures that only the necessary access is granted, aligning with the principle of least privilege.

upvoted 1 times

shanwford 1 year, 3 months ago

Selected Answer: A

Should be (A) according https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters .A perimeter bridge works between projects in different service perimeters. So Project B is not in a perimeter, so bridge wil not work here.

upvoted 1 times

b6f53d8 1 year, 5 months ago

Selected Answer: B

https://cloud.google.com/vpc-service-controls/docs/use-access-levels#create_an_access_level

upvoted 1 times

Nachtwaker 1 year, 4 months ago

Can't be B:
You can only use public IP address ranges in the access levels for IP-based allowlists. You cannot include an internal IP address in these allowlists. Internal IP addresses are associated with a VPC network, and VPC networks must be referenced by their containing project using an ingress or egress rule, or a service perimeter.
https://cloud.google.com/vpc-service-controls/docs/use-access-levels#create_an_access_level:~:text=You%20can%20only,service%20perimeter.

upvoted 2 times

MisterHairy 1 year, 8 months ago

Selected Answer: C

The correct answer is C. You should create a perimeter bridge between Project A and Project B to allow the required communication between both projects.

VPC Service Controls (SC) help to mitigate data exfiltration risks. They provide a security perimeter around Google Cloud resources to constrain data within a VPC and help protect it from being leaked.

In this case, a resource in Project B needs to access a Pub/Sub topic in Project A, but Project A is within a VPC SC perimeter that's blocking API access. A perimeter bridge can be created to allow communication between the two projects. This solution adheres to the principle of least privilege because it only allows the specific communication required, rather than changing the perimeter settings or access levels which could potentially allow more access than necessary.

the principle of least privilege is about giving a user or service account only those privileges which are essential to perform its intended function. Options A and B could potentially grant more access than necessary, which is why they are not the best solutions. Option C, creating a perimeter bridge, allows just the specific communication required, adhering to the principle of least privilege.

upvoted 1 times

shmoeee 1 year, 4 months ago

The question does not say that Project B is in a perimeter. Ans B can't be correct unless you're assuming

upvoted 2 times

desertlotus1211 1 year, 10 months ago

Answer B:
https://cloud.google.com/vpc-service-controls/docs/use-access-levels#create_an_access_level

To grant controlled access to protected Google Cloud resources in service perimeters from outside a perimeter, use access levels.

The following examples explain how to create an access level using different conditions:

IP address
User and service accounts (principals)
Device policy

upvoted 1 times

Andrei_Z 1 year, 10 months ago

Selected Answer: B

By creating an access level, you can specify precisely who in Project B should have access to subscribe to the Pub/Sub topic in Project A, ensuring that access is granted to only the necessary individuals or service accounts. This approach aligns more closely with the principle of least privilege.

upvoted 1 times

cyberpunk21 1 year, 11 months ago

Selected Answer: C

A. Can be correct but if we configure ingress policy all projects can access or ping this project so too much risk.
C. perimeter can be created between two perimeters, but bridge can only be created between two perimeters they haven't mentioned that project b is in perimeter. we have to assume it.

upvoted 2 times

cyberpunk21 1 year, 11 months ago

My bad i choose option A, https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules#definition-ingress-egress

upvoted 3 times

anshad666 1 year, 11 months ago

Selected Answer: A

Ingress: Refers to any access by an API client from outside the service perimeter to resources within a service perimeter. Example:

A Cloud Storage client outside a service perimeter calling Cloud Storage read, write, or copy operations on a Cloud Storage resource within the perimeter.

upvoted 2 times

Mithung30 1 year, 11 months ago

Answer is C. https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters

upvoted 2 times

gcp4test 1 year, 11 months ago

Selected Answer: A

A - is correct

Cant be C, bridge is between pramiter, but project B it is not in any pramiter

upvoted 3 times

mjcts 1 year, 5 months ago

This is the correct reason why the answer is A

upvoted 1 times

- Home
- Examtopics PRO

- All Exams
- Training Courses