Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 186 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 186
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You have stored company approved compute images in a single Google Cloud project that is used as an image repository. This project is protected with VPC Service Controls and exists in the perimeter along with other projects in your organization. This lets other projects deploy images from the image repository project. A team requires deploying a third-party disk image that is stored in an external Google Cloud organization. You need to grant read access to the disk image so that it can be deployed into the perimeter.

What should you do?

A. Allow the external project by using the organizational policy, constraints/compute.trustedImageProjects.

B. 1. Update the perimeter.
2. Configure the egressTo field to include the external Google Cloud project number as an allowed resource and the serviceName to compute.googleapis.com.
3. Configure the egressFrom field to set identityType to ANY_IDENTITY.

C. 1. Update the perimeter.
2. Configure the ingressFrom field to set identityType to ANY_IDENTITY.
3. Configure the ingressTo field to include the external Google Cloud project number as an allowed resource and the serviceName to compute.googleapis.com.

D. 1. Update the perimeter.
2. Configure the egressTo field to set identityType to ANY_IDENTITY.
3. Configure the egressFrom field to include the external Google Cloud project number as an allowed resource and the serviceName to compute.googleapis.com.

Show Suggested Answer

by Alejondri at *Aug. 4, 2023, 12:05 p.m.*

Comments

Type your comment...

Submit

zanhsieh 7 months, 1 week ago

Selected Answer: B

B. See the Google official example below:
https://cloud.google.com/vpc-service-controls/docs/secure-data-exchange#grant-access-third-party-compute-engine-disk-image
Note that the image mentioned in the question is a Compute Engine image, not a Docker image.
A: No. This option meant for the public image, not a private, 3rd party owned image.
C: No. This option should be put on the 3rd party image project side.
D: No. The egressTo doesn't have identityType field. See the format in:
https://cloud.google.com/vpc-service-controls/docs/configure-identity-groups#configure-identity-group-egress

upvoted 1 times

Pime13 7 months, 2 weeks ago

Selected Answer: B

Option C involves configuring the ingressFrom and ingressTo fields, which are used to control incoming traffic into the perimeter. However, in this scenario, you need to allow outgoing traffic from your VPC Service Controls perimeter to the external project to access the third-party disk image.
Option D is not suitable because it incorrectly configures the egressFrom and egressTo fields. Specifically, it sets the identityType to ANY_IDENTITY in the egressTo field, which is not necessary. Instead, you need to specify the external Google Cloud project number as an allowed resource in the egressTo field.
Option B correctly configures the egressTo field to include the external project number and the serviceName to compute.googleapis.com, while setting the identityType to ANY_IDENTITY in the egressFrom field. This ensures that the necessary outbound traffic is allowed from your VPC Service Controls perimeter to the external project.

upvoted 1 times

pico 8 months, 2 weeks ago

Selected Answer: C

why:

VPC Service Controls and Perimeters: VPC Service Controls create perimeters around your resources to control access. You need to explicitly configure how resources can enter or exit this perimeter.
Ingress vs. Egress: Since you want to allow a resource (the disk image) from outside the perimeter to be deployed inside, this is an ingress operation. Egress refers to resources moving out of the perimeter.
ANY_IDENTITY: This setting allows any authenticated Google Cloud identity to access the resource. This is necessary because the disk image is in a different organization.

upvoted 1 times

dija123 10 months ago

Selected Answer: B

Agree with B

upvoted 2 times

desertlotus1211 11 months, 3 weeks ago

You're pulling the image in, so you must egress out.

Answer b.

upvoted 2 times

pbrvgl 1 year, 2 months ago

Alternative C. It's about an OUTSIDE project willing to deploy a trusted image WITHIN the perimeter. That's "Ingress", as defined here:
https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules#definition-ingress-egress

upvoted 1 times

MaryKey 1 year, 4 months ago

Selected Answer: C

The question asks about ingress. You are not asked to modify external organisation's policy (unless you are!)

upvoted 1 times

ArizonaClassics 1 year, 5 months ago

The correct option would be:

**B. 1. Update the perimeter.
2. Configure the egressTo field to include the external Google Cloud project number as an allowed resource and the serviceName to compute.googleapis.com.

Configure the egressFrom field to set identityType to ANY_IDENTITY.**
This approach allows for controlled egress from your project to the external project to get the disk image while maintaining the VPC Service Controls.

upvoted 1 times

cyberpunk21 1 year, 5 months ago

Selected Answer: B

External cloud organization so egress not ingress. I choose option B.

upvoted 4 times

anshad666 1 year, 5 months ago

Selected Answer: B

A Compute Engine client within a service perimeter calling a Compute Engine create operation where the image resource is outside the perimeter.
https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules#:~:text=Egress%20Refers%20to%20any%20access,resource%20is%20outside%20the%20perimeter.

upvoted 4 times

ymkk 1 year, 5 months ago

I choose option C.
Since the external disk image needs to be deployed into the perimeter, resources inside the perimeter need read access to the external disk image. This requires configuring ingress rules in the perimeter.

upvoted 4 times

ymkk 1 year, 5 months ago

Why not C?

upvoted 1 times

pfilourenco 1 year, 5 months ago

Selected Answer: B

B is the correct

upvoted 2 times

Alejondri 1 year, 5 months ago

I think It's B

upvoted 1 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses