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 51 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 51

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project.

What should you do?

A. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.

B. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted projects as the exceptions in a deny operation.

C. In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.

D. In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.

Show Suggested Answer

by ownez at *Aug. 30, 2020, 10:43 p.m.*

Comments

Type your comment...

Submit

DebasishLowes Highly Voted 3 years, 10 months ago

Ans : A

upvoted 13 times

nccdebug Most Recent 11 months, 2 weeks ago

Correct Answer is: A. Option B suggests listing the trusted projects as exceptions in a deny operation, which is not necessary or recommended. It's simpler and more secure to explicitly allow only the trusted project

upvoted 1 times

Xoxoo 1 year, 4 months ago

Selected Answer: A

To limit the images that can be used as the source for boot disks and store these images in a dedicated project, you should use option A:

A. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.

Here's why this option is appropriate:

Organization-Wide Control: Creating an organization-level constraint allows you to enforce the policy organization-wide, ensuring consistent image usage across all projects within the organization.

Whitelist Approach: By listing the trusted project as a whitelist in an "allow" operation, you explicitly specify which project can be trusted as the source for boot disks. This is a more secure approach because it only allows specific trusted projects.

Dedicated Project: You mentioned that the images are stored in a dedicated project, and this option aligns with that requirement.

upvoted 3 times

Xoxoo 1 year, 4 months ago

Option B introduces complexity by listing the trusted projects as exceptions in a "deny" operation, which can become challenging to manage as more projects are added.

upvoted 1 times

Joanale 1 year, 7 months ago

Actually the default policy is allow * and if you put a constraint it must be as "deny" rule with exceptionsPrincipals or denial conditions. So answer is B, there's no "whitelist".

upvoted 1 times

meh009 2 years, 1 month ago

Selected Answer: A

https://cloud.google.com/compute/docs/images/restricting-image-access#gcloud

Look at the glcoud examples and it will make sense why A is correct

upvoted 3 times

AzureDP900 2 years, 2 months ago

A is right
Use the Trusted image feature to define an organization policy that allows principals to create persistent disks only from images in specific projects.

upvoted 2 times

AzureDP900 2 years, 2 months ago

https://cloud.google.com/compute/docs/images/restricting-image-access

upvoted 1 times

AwesomeGCP 2 years, 3 months ago

Selected Answer: A

Answer A. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.

upvoted 2 times

piyush_1982 2 years, 6 months ago

To me the answer seems to be B.
https://cloud.google.com/compute/docs/images/restricting-image-access

By default, instances can be created from images in any project that shares images publicly or explicitly with the user. So there is an implicit allow.
Option B states that we need to deny all the projects from being used as a trusted project and add "Trusted Project" as an exception to that rule.

upvoted 4 times

piyush_1982 2 years, 6 months ago

Nope, I think I am getting confused. The correct answer is A.

upvoted 1 times

simbu1299 2 years, 10 months ago

Selected Answer: A

Answer is A

upvoted 2 times

danielklein09 2 years, 10 months ago

Answer is B. You don’t whitelist in an allow operation. Since there is an implicit allow, the purpose of the whitelist has been defeated.

upvoted 3 times

gcpengineer 1 year, 8 months ago

implicit deny

upvoted 1 times

CHECK666 4 years, 4 months ago

A is the answer. you need to allow operations.

upvoted 1 times

ownez 4 years, 5 months ago

I agree with B.

"https://cloud.google.com/compute/docs/images/restricting-image-access"

upvoted 2 times

ownez 4 years, 5 months ago

Answer is A.

"Use the Trusted image feature to define an organization policy that allows your project members to create persistent disks only from images in specific projects."

"After sharing your images with other users, you can control where those users employ those resources within your organization. Set the constraints/compute.storageResourceUseRestrictions constraint to define the projects where users are permitted to use your storage resources."

upvoted 4 times

Sheeda 4 years, 5 months ago

Yes, A made sense to me too.

upvoted 1 times