

🔗 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 171 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 171

Topic #: 1

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

You have created an OS image that is hardened per your organization's security standards and is being stored in a project managed by the security team. As a Google Cloud administrator, you need to make sure all VMs in your Google Cloud organization can only use that specific OS image while minimizing operational overhead. What should you do? (Choose two.)

- A. Grant users the compute.imageUser role in their own projects.
- B. Grant users the compute.imageUser role in the OS image project.
- C. Store the image in every project that is spun up in your organization.
- D. Set up an image access organization policy constraint, and list the security team managed project in the project's allow list.
- E. Remove VM instance creation permission from users of the projects, and only allow you and your team to create VM instances.

[Show Suggested Answer](#)

by Baburao at Sept. 3, 2022, 7:06 p.m.

Comments

Type your comment...

Submit

  **zelck** Highly Voted 2 years, 4 months ago



Selected Answer: BD

BD is the answer.

<https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>
- constraints/compute.trustedImageProjects

This list constraint defines the set of projects that can be used for image storage and disk instantiation for Compute Engine. If this constraint is active, only images from trusted projects will be allowed as the source for boot disks for new instances.

   upvoted 10 times

  **AzureDP900** 2 years, 2 months ago

Thank you for sharing link, BD correct

   upvoted 1 times

  **Betotoxicity** Most Recent 10 months ago

Selected Answer: BD

BD.

To ensure all VMs in your organization use the specific hardened OS image while minimizing operational overhead, you should choose two options that achieve:

1. Centralized Image Management: The image should be stored in a single, secure location.
2. Restricted Image Access: VMs across the organization should only be able to access this specific image.

   upvoted 2 times

  **Xoxoo** 1 year, 4 months ago

Selected Answer: BD

To make sure all VMs in your Google Cloud organization can only use that specific OS image while minimizing operational overhead, you can take the following steps:

- 1) Grant users the compute.imageUser role in the OS image project . This allows users to use the OS image in their projects without granting them additional permissions .
- 2) Set up an image access organization policy constraint, and list the security team managed project in the project's allow list . This ensures that only authorized users can access the OS image .

Therefore, options B and D are the correct answers.

   upvoted 2 times

  **cyberpunk21** 1 year, 5 months ago

Selected Answer: BD

BD are correct

   upvoted 2 times

  **Littleivy** 2 years, 2 months ago

Selected Answer: BD

Need to grant permission of project owned the image




   upvoted 2 times

  **rrvv** 2 years, 3 months ago

Answer should be B and D

review the example listed here to grant the IAM policy to a service account

https://cloud.google.com/deployment-manager/docs/configuration/using-images-from-other-projects-for-vm-instances#granting_access_to_images

   upvoted 2 times

  **Littleivy** 2 years, 2 months ago

Need to grant permission of project owned the image

   upvoted 1 times

  **AwesomeGCP** 2 years, 3 months ago

Selected Answer: BD

B. Grant users the compute.imageUser role in the OS image project.

D. Set up an image access organization policy constraint, and list the security team managed project in the project's allow list

113L

   upvoted 3 times

  **GHOST1985** 2 years, 4 months ago

Selected Answer: AD

the compute.imageUser is a Permission to list and read images without having other permissions on the image. Granting this role at the project level gives users the ability to list all images in the project and create resources, such as instances and persistent disks, based on images in the project.

<https://cloud.google.com/compute/docs/access/iam#compute.imageUser>

   upvoted 3 times

  **GHOST1985** 2 years, 4 months ago

Sorry Answer BD

   upvoted 2 times

  **Baburao** 2 years, 4 months ago

I think it should be BD instead of AD.

Users should have access to the project where the secured image is stored which is "Security Team's project". Users will obviously need permission to create VM in their own project but to use image from another project, they need "imageUser" permission on that project.

   upvoted 3 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses



© 2024 ExamTopics