

🔗 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 209 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 209

Topic #: 1

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

Your organization is transitioning to Google Cloud. You want to ensure that only trusted container images are deployed on Google Kubernetes Engine (GKE) clusters in a project. The containers must be deployed from a centrally managed Container Registry and signed by a trusted authority.

What should you do? (Choose two.)

- A. Enable Container Threat Detection in the Security Command Center (SCC) for the project.
- B. Configure the trusted image organization policy constraint for the project.
- C. Create a custom organization policy constraint to enforce Binary Authorization for Google Kubernetes Engine (GKE).
- D. Enable PodSecurity standards, and set them to Restricted.
- E. Configure the Binary Authorization policy with respective attestations for the project.

[Show Suggested Answer](#)

by [K1SMM](#) at Aug. 4, 2023, 2:20 a.m.

### Comments

Type your comment...

[Submit](#)

 **cyberafrica89** 2 months ago

**Selected Answer: BE**

trusted image policies can and are often used to manage and enforce security standards for container images. These policies help ensure that only trusted images, which have been verified and potentially signed, are deployed to environments. This is a crucial security practice for preventing vulnerabilities and ensuring the integrity of container deployments.

   upvoted 1 times

 **p981pa123** 6 months, 1 week ago

**Selected Answer: CE**

The option B. Configure the trusted image organization policy constraint for the project is not directly applicable to Google Kubernetes Engine (GKE) in the way that Binary Authorization is.

Instead, this option refers to configuring an organization policy that ensures that only trusted images are used across all services, but it doesn't directly enforce a signature or attestation policy for images in GKE clusters. This organization policy is more about restricting sources of images (e.g., only allowing images from specific container registries), but it doesn't directly involve GKE enforcement of trust policies.

   upvoted 1 times

 **JohnDohertyDoe** 7 months ago

**Selected Answer: CE**

It cannot be B, because the trusted image policy does not support container images (it is used for Compute Engine images).

Use the Trusted image feature to define an organization policy that allows principals to create persistent disks only from images in specific projects. <https://cloud.google.com/compute/docs/images/restricting-image-access>

   upvoted 2 times

 **pfilourenco** 1 year, 1 month ago

**Selected Answer: CE**

It's C and E.

A -> cannot be because it does not make sense for centrally managing images and validating signed images.

B -> Cannot be, because that org policy only applies to Compute Disk images, not containers (<https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>)

C -> Correct, because we can create custom org policy for GKE to enforce Binary Authorization for image attestation (<https://cloud.google.com/kubernetes-engine/docs/how-to/custom-org-policies#enforce>)

D -> PodSecurity policies are not applicable for this use case

E -> We need to configure Binary Authorization in order to setup attestations to only allow specific images to be deployed in the cluster (<https://cloud.google.com/binary-authorization/docs/setting-up>).

So, it's C and E.


   upvoted 4 times

 **Betotoxicity** 1 year, 3 months ago

**Selected Answer: BE**

BE are correct!

   upvoted 2 times

 **desertlotus1211** 1 year, 6 months ago

What is the 'trusted image organization policy constraint'? Where is it defined and found? Can someone provide it?


   upvoted 1 times

 **oezgan** 1 year, 4 months ago

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

"Enact an image access policy by setting a compute.trustedImageProjects constraint on your project, your folder, or your organization."

   upvoted 1 times

 **Xoxoo** 1 year, 10 months ago

**Selected Answer: BE**



To ensure that only trusted container images are deployed on Google Kubernetes Engine (GKE) clusters in a project and that the containers are deployed from a centrally managed Container Registry and signed by a trusted authority, you should consider the following options:

Configure the trusted image organization policy constraint for the project (Option B): This will allow you to create an organization policy constraint that enforces the use of only trusted images from a specific Container Registry. You can specify the registry that must be used, ensuring that images are sourced only from that trusted location.

Configure the Binary Authorization policy with respective attestations for the project (Option E): Binary Authorization for GKE allows you to create policies that enforce the use of only trusted container images. You can specify which images are trusted

allows you to create policies that enforce the use of only trusted container images. You can specify which images are trusted and require attestation from trusted authorities before deployment. This ensures that only signed and trusted images can be deployed on the GKE clusters in the project.

   upvoted 4 times

  **Xoxoo** 1 year, 10 months ago

Options A, C, and D are not directly related to ensuring the use of trusted container images from a centrally managed Container Registry and signed by a trusted authority:

A. Enabling Container Threat Detection in Security Command Center (SCC) helps with threat detection but does not directly enforce the use of trusted container images.

C. Creating a custom organization policy constraint for Binary Authorization is redundant and unnecessary when Binary Authorization can be configured directly (Option E).

D. Enabling PodSecurity standards to a "Restricted" level enforces certain security policies on pods but does not directly address the issue of ensuring trusted container images.

   upvoted 2 times

  **pradoUA** 1 year, 10 months ago

**Selected Answer: BE**

BE are correct

   upvoted 1 times

  **ArizonaClassics** 1 year, 10 months ago

To ensure that only trusted container images are deployed on Google Kubernetes Engine (GKE) clusters in a project and that these containers are deployed from a centrally managed Container Registry and signed by a trusted authority, you should consider the following two actions:

B. Configure the trusted image organization policy constraint for the project.

Trusted image sources can be specified at the project level using organization policy constraints. This ensures that only images from trusted Container Registries can be deployed.

E. Configure the Binary Authorization policy with respective attestations for the project.

Binary Authorization allows you to specify a policy that will require images to be signed by trusted authorities before they can be deployed. You can configure this with attestations to indicate that certain steps, like vulnerability scanning and code reviews, have been completed.

   upvoted 1 times

  **cyberpunk21** 1 year, 11 months ago

**Selected Answer: BE**

B. This policy ensures that only trusted images from specific Container Registry repositories can be deployed. This meets one of the requirements

E. Binary Authorization ensures that only container images that are signed by trusted authorities can be deployed on GKE. Attestations are a component of this, as they provide a verifiable signature by trusted parties that an image meets certain criteria.

   upvoted 2 times

  **arpgaur** 1 year, 11 months ago

B and E. This will create a policy that enforces Binary Authorization and specifies that only images from the centrally managed Container Registry can be deployed.

C and E. This will create a policy that enforces Binary Authorization and specifies that only images that are signed by a trusted authority can be deployed. However, it does not specify the source of the images.

   upvoted 1 times


  **STomar** 1 year, 11 months ago

Correct Answer: BE

B: Configure the trusted image organization policy constraint for the project.

E: Configure the Binary Authorization policy with respective attestations for the project.

   upvoted 1 times

  **akg001** 1 year, 11 months ago

**Selected Answer: CE**

C and E



   upvoted 2 times

  **Mithung30** 1 year, 11 months ago

Selected Answer: CE

CE is correct

   upvoted 2 times

  **K1SMM** 1 year, 11 months ago

BC is correct answer

   upvoted 2 times

  **gcp4test** 1 year, 11 months ago

B is for Compute Engine images.

I think it is CE

C - custom constraints for Binary Auth on GKE -OK

E - We provide in Binary Auth rule Container Registry from where, we can deploy images

   upvoted 3 times

  **cyberpunk21** 1 year, 11 months ago

it's an org policy constraint it applies to all kinds of images

   upvoted 1 times



## Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses



© 2024 ExamTopics