

 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 125 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 125

Topic #: 1

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

You are setting up a CI/CD pipeline to deploy containerized applications to your production clusters on Google Kubernetes Engine (GKE). You need to prevent containers with known vulnerabilities from being deployed. You have the following requirements for your solution:

Must be cloud-native -

-

⇒ Must be cost-efficient




⇒ Minimize operational overhead

How should you accomplish this? (Choose two.)

- A. Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.
- B. Use a Cloud Function triggered by log events in Google Cloud's operations suite to automatically scan your container images in Container Registry.
- C. Use a cron job on a Compute Engine instance to scan your existing repositories for known vulnerabilities and raise an alert if a non-compliant container image is found.
- D. Deploy Jenkins on GKE and configure a CI/CD pipeline to deploy your containers to Container Registry. Add a step to validate your container images before deploying your container to the cluster.
- E. In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster.

Comments

[Submit](#)

  **mikesp** [Highly Voted](#)  2 years, 1 month ago

[Selected Answer: AE](#)

On-demand container analysis can be integrated into a Cloud Build Pipeline:
<https://cloud.google.com/container-analysis/docs/ods-cloudbuild>
Also binary attestation is a complementary mechanism "cloud-native".

   upvoted 9 times

  **Xoxoo** [Most Recent](#)  10 months, 1 week ago

[Selected Answer: AE](#)

A. Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.

This approach integrates vulnerability scanning into your CI/CD pipeline using native Google Cloud services.

E. In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster.

This approach enforces security policies through Binary Authorization, ensuring only images with proper attestations (i.e., no known vulnerabilities) are deployed.

   upvoted 2 times

  **zelck** 1 year, 10 months ago

[Selected Answer: AE](#)

AE is the answer.

<https://cloud.google.com/container-analysis/docs/container-analysis>

Container Analysis is a service that provides vulnerability scanning and metadata storage for containers. The scanning service performs vulnerability scans on images in Container Registry and Artifact Registry, then stores the resulting metadata and makes it available for consumption through an API.

<https://cloud.google.com/binary-authorization/docs/attestations>

After a container image is built, an attestation can be created to affirm that a required activity was performed on the image such as a regression test, vulnerability scan, or other test. The attestation is created by signing the image's unique digest. During deployment, instead of repeating the activities, Binary Authorization verifies the attestations using an attestor. If all of the attestations for an image are verified, Binary Authorization allows the image to be deployed.

   upvoted 4 times

  **AzureDP900** 1 year, 8 months ago

Agreed

   upvoted 1 times

  **szl0144** 2 years, 2 months ago

AE is the answer, C has too much manual operations

   upvoted 1 times

  **ExamQnA** 2 years, 2 months ago

Ans: A,E

https://cloud.google.com/architecture/binary-auth-with-cloud-build-and-gke#setting_the_binary_authorization_policy

   upvoted 2 times

Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses

