Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 295 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 295

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your organization heavily utilizes serverless applications while prioritizing security best practices. You are responsible for enforcing image provenance and compliance with security standards before deployment. You leverage Cloud Build as your continuous integration and continuous deployment (CI/CD) tool for building container images. You must configure Binary Authorization to ensure that only images built by your Cloud Build pipeline are deployed and that the images pass security standard compliance checks. What should you do?

A. Create a Binary Authorization attestor that uses a scanner to assess source code management repositories. Deploy images only if the attestor validates results against a security policy.

B. Create a Binary Authorization attestor that utilizes a scanner to evaluate container image build processes. Define a policy that requires deployment of images only if this attestation is present.

C. Create a Binary Authorization attestor that retrieves the Cloud Build build ID of the container image. Configure a policy to allow deployment only if there's a matching build ID attestation.

D. Utilize a custom Security Health Analytics module to create a policy. Enforce the policy through Binary Authorization to prevent deployment of images that do not meet predefined security standards.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 9:45 p.m.*

Comments

Type your comment...

Submit

danidee111 1 month, 2 weeks ago

Selected Answer: B

The attestation is created by signing the image's unique digest. You don't directly need the Cloud Build build ID of the container image. I think the word 'Utilizes' is misleading, but you can interpret it as the attestation checks to see if a scanner(Artifact Analysis) was utilized.

upvoted 2 times

KLei 8 months, 2 weeks ago

Selected Answer: C

Google has built-in security container. So not scanner is need. opt out A B

Add a Verification Method:
Use a built-in security scanner (e.g., Container Analysis) to evaluate the image against compliance policies.

upvoted 1 times

jmaquino 9 months ago

C, but I have doubts about this part: and that the images pass security standard compliance checks. What should you do?
Because Security Command Center can do that

upvoted 1 times

jmaquino 9 months ago

C:
Binary Authorization (overview) is a Google Cloud product that enforces deploy-time constraints on applications. Its Google Kubernetes Engine (GKE) integration allows users to enforce that containers deployed to a Kubernetes cluster are cryptographically signed by a trusted authority and verified by a Binary Authorization attestor.

You can configure Binary Authorization to require attestations based on the location of the source code to prevent container images built from unauthorized source from being deployed.

upvoted 1 times

json4u 9 months, 2 weeks ago

Selected Answer: C

I think it's C.

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

C - Image Provenance: By using the Cloud Build build ID as the attestation, you can directly link the deployed image to the specific build process that created it. This ensures that only images built by your trusted CI/CD pipeline are deployed.
Security Standards Compliance: You can integrate security checks into your Cloud Build pipeline, such as vulnerability scanning or compliance audits. If an image fails these checks, the build process can be aborted, preventing the creation of a non-compliant image.
Policy Enforcement: The Binary Authorization policy ensures that only images with the correct build ID attestation are deployed, effectively enforcing the security standards you've defined in your CI/CD pipeline.

upvoted 1 times

> **jmaquino** 9 months ago
>
> I think it would be C, if this part were not there: that the images pass security standard compliance checks. What should you do?
>
> Binary Authorization can integrate with Security Command Center to provide Single Pane of Glass view for Policy Violations. Log Violations to Audit logging. Integrate with KMS for signing the image. Also integrate with Cloud Build, GKE and Cloud Run for Deployments. It can also integrate with 3rd Party Solutions like Cloudbees, Palo Alto Networks & Terraform
>
> upvoted 1 times

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses