EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 197 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 197
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You run applications on Cloud Run. You already enabled container analysis for vulnerability scanning. However, you are concerned about the lack of control on the applications that are deployed. You must ensure that only trusted container images are deployed on Cloud Run.

What should you do? (Choose two.)

A. Enable Binary Authorization on the existing Cloud Run service.

B. Set the organization policy constraint constraints/run.allowedBinaryAuthorizationPolicies to the list or allowed Binary Authorization policy names.

C. Enable Binary Authorization on the existing Kubernetes cluster.

D. Use Cloud Run breakglass to deploy an image that meets the Binary Authorization policy by default.

E. Set the organization policy constraint constraints/compute.trustedImageProjects to the list of projects that contain the trusted container images.

Show Suggested Answer

by K1SMM at *Aug. 2, 2023, 11:56 p.m.*

Comments

Type your comment...

Submit

chimz2002 Highly Voted 1 year, 3 months ago

Selected Answer: AB

options A and B are right. video explanation, feel free to watch from the beginning - https://youtu.be/b7GdpEEvGDQ?t=249

upvoted 5 times

zanhsieh Most Recent 7 months, 1 week ago

Selected Answer: AB

AB.
C: No. The question doesn't have "the existing Kubernetes cluster".
D: No. Why breakglass if we already took opt A?
E: No. "compute.trustedImageProjects" is for Compute Engine. See the link below:
https://cloud.google.com/compute/docs/images/restricting-image-access#trusted_images
https://cloud.google.com/binary-authorization/docs/run/requiring-binauthz-cloud-run#set_the_organization_policy

upvoted 1 times

desertlotus1211 1 year ago

https://youtu.be/b7GdpEEvGDQ?t=249

this video exaplins at 4:30 into it

upvoted 2 times

Xoxoo 1 year, 4 months ago

Selected Answer: AE

To ensure that only trusted container images are deployed on Cloud Run, you should take the following actions:

Option A: Enable Binary Authorization on the existing Cloud Run service.

Binary Authorization allows you to create policies that specify which container images are allowed to be deployed. By enabling Binary Authorization on your Cloud Run service, you can enforce these policies, ensuring that only trusted container images are deployed.
Option E: Set the organization policy constraint constraints/compute.trustedImageProjects to the list of projects that contain the trusted container images.

This organization policy constraint allows you to specify which projects are considered trusted sources of container images. By setting this constraint, you can control where trusted container images can be sourced from.

upvoted 1 times

Xoxoo 1 year, 4 months ago

Options B, C, and D are not directly related to controlling container image deployments on Cloud Run:

Option B: This option appears to refer to a policy constraint related to Cloud Run but doesn't specifically address Binary Authorization, which is the tool for enforcing image trust.

Option C: Enabling Binary Authorization on a Kubernetes cluster is useful for controlling container image deployments in Kubernetes, but it doesn't directly apply to Cloud Run, which is a different serverless container platform.

Option D: The concept of "Cloud Run breakglass" is not a standard term or method for controlling image deployments. Binary Authorization is the recommended approach for enforcing container image trust.

upvoted 1 times

Xoxoo 1 year, 4 months ago

Option E: Set the organization policy constraint constraints/compute.trustedImageProjects to the list of projects that contain the trusted container images.

This organization policy constraint allows you to specify which projects are considered trusted sources of container images. By setting this constraint, you can control where trusted container images can be sourced from.

upvoted 1 times

ArizonaClassics 1 year, 5 months ago

AE Satisfies the concept

upvoted 1 times

anshad666 1 year, 5 months ago

Selected Answer: AB

look like AB
https://cloud.google.com/binary-authorization/docs/run/requiring-binauthz-cloud-run

https://cloud.google.com/binary-authorization/docs/run/requiring-binauthz-cloud-run

upvoted 2 times

cyberpunk21 1 year, 5 months ago

Selected Answer: AE

A speaks about authorization and E talks about using trusted images so AE are correct

upvoted 1 times

Mithung30 1 year, 5 months ago

Selected Answer: AB

Correct answer is AB
https://cloud.google.com/binary-authorization/docs/run/requiring-binauthz-cloud-run#set_the_organization_policy

upvoted 2 times

hykdlidesd 1 year, 5 months ago

I think AB cause E is for compute engine

upvoted 1 times

pfilourenco 1 year, 5 months ago

Selected Answer: AB

A & B: https://cloud.google.com/binary-authorization/docs/run/requiring-binauthz-cloud-run

upvoted 2 times

K1SMM 1 year, 5 months ago

AE

https://cloud.google.com/binary-authorization/docs/configuring-policy-console?hl=pt-br#cloud-run

upvoted 2 times