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 42 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 42
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.
What should they do?

A. Use Cloud Build to build the container images.

B. Build small containers using small base images.

C. Delete non-used versions from Container Registry.

D. Use a Continuous Delivery tool to deploy the application.

Show Suggested Answer

by xhova at *April 4, 2020, 7:11 a.m.*

Comments

Type your comment...

Submit

xhova Highly Voted 5 years, 3 months ago
Ans is B

Small containers usually have a smaller attack surface as compared to containers that use large base images.

https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-how-and-why-to-build-small-container-images

upvoted 31 times

smart123 5 years ago

I agree

upvoted 2 times

3d9563b Most Recent 1 year ago

Selected Answer: B

Building small containers using minimal and well-maintained base images directly reduces the attack surface and improves the security posture of your containers when they are deployed on GKE.

upvoted 1 times

okhascorpio 1 year, 5 months ago

Selected Answer: B

the correct answer is having as few tools in your image as possible, Source: Remove unnecessary tools
https://cloud.google.com/architecture/best-practices-for-building-containers?hl=en
I guess it can be achieved by option "B" building a small container from a small source image.

upvoted 1 times

Afe3saa7 1 year, 5 months ago

Selected Answer: B

A. Use Cloud Build to build the container images.
Will give you the tools to build an image but not ensure any risk reduction

B. Build small containers using small base images.
Images with a smaller footprint, stripped of all binaries/libraries/functions that are not used will make it harder for an attacker to find leverage to move laterally or vertically, hence >>reducing the attack/risk surface<< for the image.

C. Delete non-used versions from Container Registry.
Non-used images are not running live and hence are not exploitable. Removing non-used images from the registry will not reduce the attack surface of the running application.

D. Use a Continuous Delivery tool to deploy the application.
Same as A.

upvoted 1 times

Xoxoo 1 year, 10 months ago

Selected Answer: B

To minimize the attack surface of a container that will run on Google Kubernetes Engine and be internet-facing, the DevOps team should:

B. Build small containers using small base images.

Building small containers using minimal base images reduces the attack surface by eliminating unnecessary software and dependencies, which can potentially contain vulnerabilities. This approach enhances security and reduces the risk of potential attacks. Using small base images, such as Alpine Linux or distroless images, is a best practice for container security.

upvoted 3 times

civilizador 1 year, 12 months ago

Answer is B, because this GCP exam, the GCP docs are always source of truth even though you might not be agree with them occasionally but even if you are not agree you need to choose the answer proposed in GCP docs as the best practice. Here is the link to google official best practices for building containers. and here is the snippet regarding this particular question: https://cloud.google.com/architecture/best-practices-for-building-containers#build-the-smallest-image-possible

Build the smallest image possible
Building a smaller image offers advantages such as faster upload and download times, which is especially important for the cold start time of a pod in Kubernetes: the smaller the image, the faster the node can download it. However, building a small image can be difficult because you might inadvertently include build dependencies or unoptimized layers in your final image.

upvoted 2 times

[Removed] 2 years ago

Selected Answer: B

"B"
For smaller attacker surface, use smaller images by removing any unnecessary tools/software from the image.

https://cloud.google.com/solutions/best-practices-for-building-containers

upvoted 2 times

alleinallein 2 years, 3 months ago

Selected Answer: C

Importance: MEDIUM

To protect your apps from attackers, try to reduce the attack surface of your app by removing any unnecessary tools.

https://cloud.google.com/architecture/best-practices-for-building-containers

upvoted 2 times

adb4007 1 year, 8 months ago

So build a small image is the answer, not ?

upvoted 1 times

mahi9 2 years, 5 months ago

Selected Answer: C

it is viable

upvoted 1 times

rotorclear 2 years, 9 months ago

Selected Answer: B

B definitely

upvoted 1 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

zellck 2 years, 10 months ago

Selected Answer: B

B is the answer.

upvoted 1 times

jitu028 2 years, 10 months ago

Ans is B - https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-how-and-why-to-build-small-container-images

Security and vulnerabilities
Aside from performance, there are significant security benefits from using smaller containers. Small containers usually have a smaller attack surface as compared to containers that use large base images.

upvoted 3 times

giovy_82 2 years, 11 months ago

Selected Answer: B

the only answer that will really reduce attack surface while exposing apps to internet is B, small containers (e.g. single web page?)

upvoted 3 times

Medofree 3 years, 3 months ago

B. Because you will have less programs in the image thus less vulnerabilities

upvoted 1 times

lxs 3 years, 7 months ago

Selected Answer: C

A. Use Cloud Build to build the container images.
If you build a container using Cloud Build or not the surface is the same
B. Build small containers using small base images.
It is indeed best practice, but I doubt if small base images can reduce the surface. It is still the same app version with the same vulnerabilities etc.
C. Delete non-used versions from Container Registry.
Unused, historical versions are additional attack surface. attacker can exploit old, unpatched image which indeed the surface extention.
D. Use a Continuous Delivery tool to deploy the application.
This is just a method of image delivery. The app is the same.

upvoted 3 times

Afe3saa7 1 year, 5 months ago

Alejsaa7 1 year, 5 months ago

non-used images in containter registry are as they suggest not running live, hence are not exploitable. deleting images in the registry will not change the attack surface of the mentioned image.

upvoted 1 times

DebasishLowes 4 years, 4 months ago

Ans : B. Small the base image there is less vulnerability and less chance of attack.

upvoted 2 times

Load full discussion...