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 59 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 59
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE).
How should the DevOps team accomplish this?

A. Use Puppet or Chef to push out the patch to the running container.

B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.

C. Update the application code or apply a patch, build a new image, and redeploy it.

D. Configure containers to automatically upgrade when the base image is available in Container Registry.

Show Suggested Answer

by MohitA at *Sept. 2, 2020, 9:03 a.m.*

Comments

Type your comment...

Submit

TNT87 Highly Voted 4 years, 5 months ago
https://cloud.google.com/containers/security
Containers are meant to be immutable, so you deploy a new image in order to make changes. You can simplify patch

Containers are meant to be immutable, so you deploy a new image in order to make changes. You can simply patch management by rebuilding your images regularly, so the patch is picked up the next time a container is deployed. Get the full picture of your environment with regular image security reviews.
C is better

upvoted 15 times

AzureDP900 2 years, 8 months ago

Yes, C is correct

upvoted 1 times

DebasishLowes Highly Voted 4 years, 4 months ago

Ans : C

upvoted 7 times

nah99 Most Recent 8 months, 1 week ago

Selected Answer: B

https://cloud.google.com/kubernetes-engine/docs/resources/security-patching#how_vulnerabilities_are_patched

upvoted 1 times

GCBC 1 year, 11 months ago

C is ans - no auto upgrade will patch

upvoted 2 times

[Removed] 2 years ago

Selected Answer: C

"C"
Containers are immutable and cannot be updated in place. Base image/container must be patched and then gradually introduced to live container pool.

References:
https://cloud.google.com/architecture/best-practices-for-operating-containers#immutability

upvoted 2 times

Ishu_awsguy 2 years, 1 month ago

My vote for B.
This is a biog value add of GKE - inplace upgrades.

upvoted 1 times

Ric350 2 years, 3 months ago

B is 100% the answer.
Fixing some vulnerabilities requires only a control plane upgrade, performed automatically by Google on GKE, while others require both control plane and node upgrades.

To keep clusters patched and hardened against vulnerabilities of all severities, we recommend using node auto-upgrade on GKE (on by default).
https://cloud.google.com/kubernetes-engine/docs/resources/security-patching#how_vulnerabilities_are_patched

upvoted 2 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: C

C. Update the application code or apply a patch, build a new image, and redeploy it.

upvoted 1 times

Medofree 3 years, 3 months ago

Selected Answer: C

Correct ans is C, because "DevOps team needs to update their running containers".

upvoted 2 times

Rhehehe 3 years, 7 months ago

Its actually B.
Patching a vulnerability involves upgrading to a new GKE or Anthos version number. GKE and Anthos versions include versioned components for the operating system, Kubernetes components, and other containers that make up the Anthos platform. Fixing some vulnerabilities requires only a control plane upgrade, performed automatically by Google on GKE, while others require both control plane and node upgrades.

To keep clusters patched and hardened against vulnerabilities of all severities, we recommend using node auto-upgrade on GKE (on by default). On other Anthos platforms, Google recommends upgrading your Anthos components at least monthly.

Ref: https://cloud.google.com/kubernetes-engine/docs/resources/security-patching

upvoted 5 times

StanPeng 3 years, 5 months ago

The qeustion is asking about upgrading application code rather than GKE

upvoted 1 times

Ric350 2 years, 3 months ago

No, the question is asking how vulnerabilities are patched! To keep clusters patched and hardened against vulnerabilities of all severities, we recommend using node auto-upgrade on GKE (on by default).
https://cloud.google.com/kubernetes-engine/docs/resources/security-patching#how_vulnerabilities_are_patched

upvoted 2 times

alexm112 3 years, 5 months ago

Agreed - I think this wasn't available at the time people responded.

B is correct
https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-upgrades

upvoted 2 times

SuperDevops 3 years, 8 months ago

I took the test yesterday and didn't pass, NO ISSUE is from here. The questions are totally new
Whizlabs it´s OK

upvoted 1 times

sriz 3 years, 8 months ago

u got questions from Whizlabs?

upvoted 2 times

Aniyadu 4 years, 6 months ago

The question asked is "team needs to update their running containers" if its was auto enabled there was no need to update manually. so my answer will be C.

upvoted 2 times

Kevinsayn 4 years, 8 months ago

Me voy definitivamente con la C, dado que actualizar los nodos con autoupgrade no tiene nada que ver con los contenedores, la vulnerabilidad en este caso se debe aplicar con respecto a contenedor ósea aplicación por lo que la respuesta C es la correcta.

upvoted 3 times

soukumar369 4 years, 7 months ago

Translaed : 'm definitely going with C, since updating the nodes with autoupgrade has nothing to do with the containers, the vulnerability in this case must be applied with respect to the application bone container so the C answer is correct.

upvoted 1 times

jonclem 4 years, 8 months ago

Answer B is correct as per the Video Google Kubernetes Engine (GKE) Security on Linuxacademy.

upvoted 2 times

Rantu 4 years, 9 months ago

C is the correct answer as this is the way to patch, build, re-deploy

upvoted 3 times

Namaste 4 years, 10 months ago

Answer is C.

upvoted 3 times

ownez 4 years, 10 months ago

I would go for C because some reported CVEs will take time to be published and approval in CVE advisory portal. Once approved, it will notify to all necessary third party.

Hence, this requires a lot of time and left people exposed to the vulnerability.

Answer is C.

upvoted 3 times

Load full discussion...

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses