Welcome to ExamTopics

EXAMTOPICS

- Expert Verified, Online, Free.

MENU

Google Discussions

Exam Associate Cloud Engineer All Questions

View all questions & answers for the Associate Cloud Engineer exam

Go to Exam

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 97 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 97

Topic #: 1

[All Associate Cloud Engineer Questions]

You are building a product on top of Google Kubernetes Engine (GKE). You have a single GKE cluster. For each of your customers, a Pod is running in that cluster, and your customers can run arbitrary code inside their Pod. You want to maximize the isolation between your customers' Pods. What should you do?

A. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

B. Use the Container Analysis API to detect vulnerabilities in the containers used by your customers' Pods.

C. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

D. Use the cos_containerd image for your GKE nodes. Add a nodeSelector with the value cloud.google.com/gke-os-distribution: cos_containerd to the specification of your customers' Pods.

Show Suggested Answer

by PAUGURU at *May 1, 2022, 5:29 a.m.*

Comments

Type your comment...

Submit

akshaychavan7 Highly Voted 2 years, 5 months ago

Let me be honest, I did not have any clue to answer this question. However, I spotted the keyword, 'isolation', from the question and a keyword, 'sandbox' from the answers and guessed the answer which turned out to be correct.
So, yes it is C!

upvoted 22 times

Sac3433 Highly Voted 2 years, 5 months ago

Correct answer is C: You can enable GKE Sandbox on your cluster to isolate untrusted workloads in sandboxes on the node. GKE Sandbox is built using gVisor, an open source project: https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview?hl=en#protecting_nodes_from_untrusted_workloads

upvoted 11 times

Cynthia2023 Most Recent 9 months, 3 weeks ago

Selected Answer: C

gVisor is a sandboxing technology that provides an additional layer of isolation between running containers. It's particularly useful in scenarios where containers might be running untrusted or arbitrary code, as it helps in mitigating the risk of kernel exploits.
By configuring a node pool with gVisor and specifying runtimeClassName: gvisor in the Pod specifications, each Pod is run within this sandboxed environment, thereby enhancing isolation between the Pods.

upvoted 6 times

> Cynthia2023 9 months, 3 weeks ago
>
> A. Binary Authorization: While Binary Authorization is a security control that ensures only trusted container images are deployed on GKE, it doesn't provide isolation between running Pods. It's more about image integrity and compliance.
> B. Container Analysis API: This API is used for scanning container images for vulnerabilities. While important for security, it doesn't directly contribute to runtime isolation between Pods.
> D. Using cos_containerd Image: The Container-Optimized OS with containerd (cos_containerd) is a secure choice for the node image in GKE. However, it doesn't provide the same level of isolation for arbitrary code execution in Pods as gVisor. The nodeSelector parameter is used to schedule Pods on specific nodes but doesn't enhance inter-Pod isolation.
>
> upvoted 2 times
>
> Cynthia2023 9 months, 3 weeks ago
>
> • Implementing gVisor can impact the performance of the containers due to the additional layer of abstraction. However, for scenarios requiring high security and isolation, particularly when running arbitrary code, the trade-off can be justified.
>
> upvoted 2 times

BAofBK 11 months, 2 weeks ago

The correct answer is C

upvoted 2 times

lov75 1 year, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

mattcl 1 year, 11 months ago

GKE Sandbox https://cloud.google.com/kubernetes-engine/docs/concepts/sandbox-pods

upvoted 3 times

theBestStudent 2 years, 2 months ago

Selected Answer: C

As it has been mentioned already: https://cloud.google.com/kubernetes-engine/docs/how-to/sandbox-pods?hl=en

https://cloud.google.com/kubernetes-engine/docs/how-to/sandbox-pods?hl=en#working_with

upvoted 2 times

AzureDP900 2 years, 4 months ago

gVisor is the way to isolate. Those who already preparing for CKS can answer this question without even thinking further. C is right

upvoted 3 times

haroldbenites 2 years, 4 months ago

Go for C

upvoted 1 times

PAUGURU 2 years, 5 months ago

Selected Answer: C

https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview?

hl=en#protecting_nodes_from_untrusted_workloads

upvoted 2 times

Start Learning for free

Social Media

Facebook , Twitter

YouTube , Reddit

Pinterest

EXAMTOPICS

We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.

© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.