Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 305 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 305
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization is using Vertex AI Workbench Instances. You must ensure that newly deployed Instances are automatically kept up-to-date and that users cannot accidentally alter settings in the operating system. What should you do?

A. Enforce the disableRootAccesa and requireAutoUpgradeSchedule organization policies for newly deployed Instances.

B. Enable the VM Manager and ensure the corresponding Google Compute Engine instances are added.

C. Implement a firewall rule that prevents Secure Shell access to the corresponding Google Compute Engine instances by using tags.

D. Assign the AI Notebooks Runner and AI Notebooks Viewer roles to the users of the AI Workbench Instances.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 10:10 p.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: A

https://cloud.google.com/vertex-ai/docs/workbench/instances/manage-metadata

upvoted 1 times

BPzen 8 months ago

Selected Answer: B

Why B is Correct:
VM Manager:

VM Manager automates the management of Compute Engine instances, including patch management and configuration updates.
By enabling VM Manager, you ensure that operating systems of Vertex AI Workbench instances are automatically kept up-to-date with the latest security patches and updates.
Automatic Enrollment:

When VM Manager is enabled, you can enroll the corresponding GCE instances and enforce compliance with organizational policies.
Control Over System Configurations:

VM Manager allows you to enforce configuration settings, preventing users from making unauthorized changes to the OS.

upvoted 1 times

json4u 9 months, 2 weeks ago

Selected Answer: A

It's A.
Well explained below.

upvoted 2 times

abdelrahman89 9 months, 3 weeks ago

A - disableRootAccess: This organization policy prevents users from accessing the root account of the underlying Google Compute Engine instance, which helps to prevent accidental configuration changes.
requireAutoUpgradeSchedule: This organization policy ensures that instances are automatically upgraded to the latest operating system patches, keeping them secure and up-to-date.

upvoted 3 times