≡ MENU   🔍

←   **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 182 DISCUSSION**

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 182

Topic #: 1

[All Professional Cloud Security Engineer Questions]

For compliance reporting purposes, the internal audit department needs you to provide the list of virtual machines (VMs) that have critical operating system (OS) security updates available, but not installed. You must provide this list every six months, and you want to perform this task quickly.

What should you do?

    A. Run a Security Command Center security scan on all VMs to extract a list of VMs with critical OS vulnerabilities every six months.

    B. Run a gcloud CLI command from the Command Line Interface (CLI) to extract the VM's OS version information every six months.

    C. Ensure that the Cloud Logging agent is installed on all VMs, and extract the OS last update log date every six months.

    D. Ensure the OS Config agent is installed on all VMs and extract the patch status dashboard every six months.

Show Suggested Answer

by 👤 **K1SMM** at *Aug. 2, 2023, 11:06 a.m.*

Comments

```
Type your comment...
```

▫ 👤 **i_am_robot** 1 year, 1 month ago

Selected Answer: D

The best option would be D. Ensure the OS Config agent is installed on all VMs and extract the patch status dashboard every six months**.

The OS Config agent is a service that provides a fast and flexible way to manage operating system configurations across an entire fleet of virtual machines. It can provide information about the patch state of a VM, including which patches are installed, which patches are available, and the severity of the patches. This would allow you to quickly identify VMs that have critical OS security updates available but not installed.

👍 ↩ 🚩 upvoted 2 times

▫ 👤 **gkarthik1919** 1 year, 4 months ago

D is correct. https://cloud.google.com/compute/docs/vm-manager

👍 ↩ 🚩 upvoted 1 times

▫ 👤 **cyberpunk21** 1 year, 5 months ago

Selected Answer: D

D is correct

👍 ↩ 🚩 upvoted 1 times

▫ 👤 **cyberpunk21** 1 year, 5 months ago

Selected Answer: D

D is correct. C can be correct but not effective as D

👍 ↩ 🚩 upvoted 1 times

▫ 👤 **RuchiMishra** 1 year, 5 months ago

Selected Answer: D

D: https://cloud.google.com/compute/docs/os-patch-management#:~:text=A%20patch%20deployment%20is%20initiated,target%20VMs%20to%20start%20patching. Cannot be A, as VM Manager patch compliance feature is in preview for in SCC. https://cloud.google.com/security-command-center/docs/concepts-vulnerabilities-findings

👍 ↩ 🚩 upvoted 2 times

▫ 👤 **pfilourenco** 1 year, 5 months ago

Selected Answer: D

I think is D since you can't "run" Security Command Center "security" scan's without vm manager enabled.
"If you enable VM Manager with the Security Command Center Premium tier, VM Manager writes its vulnerability reports to Security Command Center by default"

👍 ↩ 🚩 upvoted 1 times

▫ 👤 **Sanjana2020** 1 year, 5 months ago

C- Cloud Logging Agent

👍 ↩ 🚩 upvoted 1 times

▫ 👤 **K1SMM** 1 year, 5 months ago

A Security command center is integrated with vm manager

👍 ↩ 🚩 upvoted 1 times