

🔗 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 228 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 228

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You manage a mission-critical workload for your organization, which is in a highly regulated industry. The workload uses Compute Engine VMs to analyze and process the sensitive data after it is uploaded to Cloud Storage from the endpoint computers. Your compliance team has detected that this workload does not meet the data protection requirements for sensitive data. You need to meet these requirements:

- Manage the data encryption key (DEK) outside the Google Cloud boundary.
- Maintain full control of encryption keys through a third-party provider.
- Encrypt the sensitive data before uploading it to Cloud Storage.
- Decrypt the sensitive data during processing in the Compute Engine VMs.
- Encrypt the sensitive data in memory while in use in the Compute Engine VMs.

What should you do? (Choose two.)

- Configure Customer Managed Encryption Keys to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.
- Configure Cloud External Key Manager to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.
- Create Confidential VMs to access the sensitive data.
- Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.
- Create a VPC Service Controls service perimeter across your existing Compute Engine VMs and Cloud Storage buckets.



Show Suggested Answer

by  ppandher at Aug. 3, 2023, 2:54 p.m.

## Comments

Type your comment...

Submit

  **Pime13** 7 months, 3 weeks ago

**Selected Answer: BD**

You must create a new VM instance to enable Confidential VM. Existing instances can't be converted to Confidential VM instances.

<https://cloud.google.com/confidential-computing/confidential-vm/docs/supported-configurations#limitations>

   upvoted 2 times

  **Zek** 7 months, 3 weeks ago

**Selected Answer: BC**

You must create a new VM instance to enable Confidential VM. Existing instances can't be converted to Confidential VM instances.

<https://cloud.google.com/confidential-computing/confidential-vm/docs/supported-configurations#limitations>

   upvoted 1 times

  **MoAk** 8 months, 1 week ago

**Selected Answer: BC**

D is 100% wrong. you cannot migrate existing VMs to enable a confidential VM.

<https://cloud.google.com/confidential-computing/confidential-vm/docs/supported-configurations#limitations>

   upvoted 2 times

  **Mr\_MIXER007** 10 months, 3 weeks ago

**Selected Answer: BD**


B and D go with

   upvoted 1 times

  **Mr\_MIXER007** 10 months, 3 weeks ago


B and D go with

   upvoted 1 times

  **EVEGCP** 1 year, 8 months ago

BC : Confidential VM does not support live migration.

<https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance#considerations>

   upvoted 2 times

  **MisterHairy** 1 year, 8 months ago

**Selected Answer: BC**

Correction. When enabling Confidential Computing, it must be done when the VM instance is first created. Therefore, the right answer is C. Create Confidential VMs to access the sensitive data is the more accurate choice.

   upvoted 2 times

  **MisterHairy** 1 year, 8 months ago

**Selected Answer: BD**



The correct choices are:

B. Configure Cloud External Key Manager to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs. Cloud External Key Manager allows you to use encryption keys stored outside of Google's infrastructure, providing full control over the key material.

D. Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data. Confidential VMs offer a breakthrough technology that encrypts data in-use, allowing you to work on sensitive data sets without exposing the data to the rest of the system.

Option C involves creating new Confidential VMs, but it's more efficient to migrate the existing Compute Engine VMs to Confidential VMs as stated in Option D.


   upvoted 1 times

  **mjcts** 1 year, 5 months ago

As per documentation: "You can only enable Confidential Computing on a VM when you first create an instance"

Therefore it's C not D

   upvoted 3 times

  **gkarthik1919** 1 year, 10 months ago

BC . Agree.

   upvoted 1 times

  **i\_am\_robot** 1 year, 10 months ago

**Selected Answer: BD**

To meet the specified data protection requirements for sensitive data, including managing the data encryption key (DEK) outside the Google Cloud boundary and encrypting the sensitive data in memory while in use in the Compute Engine VMs, you should:

B. Configure Cloud External Key Manager to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.

D. Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.

   upvoted 2 times



  **ArizonaClassics** 1 year, 10 months ago

B. Configure Cloud External Key Manager (EKM) to encrypt the sensitive data before it is uploaded to Cloud Storage, and decrypt the sensitive data after it is downloaded into your VMs.

Migrate the Compute Engine VMs to Confidential VMs to access the sensitive data.

Confidential VMs allow you to encrypt data in use (in memory). These VMs ensure that data remains encrypted when it's being used and processed. This aligns with the requirement to encrypt sensitive data in memory while in use in the Compute Engine VMs.


   upvoted 1 times

  **desertlotus1211** 1 year, 10 months ago

Answer B&C:

You cannot migrate a regular CE VM to Confidential. You must a new Confidential VM, and then decommission the other one.

   upvoted 2 times

  **ymkk** 1 year, 10 months ago


**Selected Answer: BC**

B,C is the answer.

Confidential VM does not support live migration. You can only enable Confidential Computing on a VM when you first create the instance.

<https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance>

   upvoted 4 times

  **Andrei\_Z** 1 year, 10 months ago

**Selected Answer: BC**

I would go with BC as well



   upvoted 2 times

  **cyberpunk21** 1 year, 11 months ago

**Selected Answer: BC**

confidential VM doesn't support live migration.



   upvoted 4 times

  **anshad666** 1 year, 11 months ago

**Selected Answer: BC**




C because Confidential VM does not support live migration.

   upvoted 1 times

  **akilaz** 1 year, 11 months ago

**Selected Answer: BC**

That's right, no idea why BD is the correct answer.

   upvoted 1 times

[Load full discussion...](#)



## Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)



© 2024 ExamTopics