

 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 175 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 175

Topic #: 1

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

You are consulting with a client that requires end-to-end encryption of application data (including data in transit, data in use, and data at rest) within Google Cloud.

Which options should you utilize to accomplish this? (Choose two.)

- A. External Key Manager
- B. Customer-supplied encryption keys
- C. Hardware Security Module
- D. Confidential Computing and Istio
- E. Client-side encryption

[Show Suggested Answer](#)

by  Baburao at Sept. 3, 2022, 7:20 p.m.

Comments

Type your comment...


[Submit](#)

 GHOST1985 [Highly Voted](#) 2 years, 10 months ago

Selected Answer: DE

Confidential Computing enables encryption for "data-in-use"
Client Side encryption enables security for "data in transit" from Customer site to GCP
Once data is at rest, use Google's default encryption for "data at rest"

   upvoted 12 times

  **Baburao** **Highly Voted**  2 years, 10 months ago

I feel this should be DE.
Confidential Computing enables encryption for "data-in-use"
Client Side encryption enables security for "data in transit" from Customer site to GCP
Once data is at rest, use Google's default encryption for "data at rest"

   upvoted 8 times

  **Pime13** **Most Recent**  7 months, 2 weeks ago

Selected Answer: DE

Confidential Computing and Istio (Option D): Confidential Computing protects data in use by running workloads in secure enclaves, ensuring that data remains encrypted even during processing. Istio can help secure data in transit by providing mutual TLS (mTLS) for service-to-service communication within your Kubernetes clusters.

Client-side encryption (Option E): Client-side encryption ensures that data is encrypted before it is sent to Google Cloud, protecting data in transit and at rest. This approach allows you to maintain control over the encryption keys and ensures that data is encrypted throughout its lifecycle.



   upvoted 1 times

  **DattaHinge** 10 months, 1 week ago

Selected Answer: BC

B. Customer-supplied encryption keys: This is crucial for achieving true end-to-end encryption. By providing your own encryption keys, you maintain complete control over the data, even Google Cloud cannot decrypt it without your keys.
C. Hardware Security Module (HSM): HSMs provide a secure environment for storing and managing your encryption keys. This adds an extra layer of security, ensuring that your keys are protected from unauthorized access.

   upvoted 2 times

  **desertlotus1211** 1 year, 10 months ago

I'll go with answer CD:
<https://cloud.google.com/kubernetes-engine/docs/how-to/encrypting-secrets#creating-key>



   upvoted 2 times

  **Andrei_Z** 1 year, 10 months ago

Selected Answer: BD

Option E (Client-side encryption) typically refers to encrypting data on the client side before sending it to the cloud, and it can complement the other options but is not one of the primary mechanisms for achieving end-to-end encryption within Google Cloud itself.

   upvoted 3 times

  **desertlotus1211** 1 year, 10 months ago

the key in the question is 'within GCP'... So E cannot be correct


   upvoted 2 times

  **cyberpunk21** 1 year, 11 months ago

Selected Answer: DE

D - Ensures encryption for data in use and transit
E - Ensures Encryption at rest

   upvoted 2 times

  **TNT87** 2 years, 4 months ago

Selected Answer: BE

Why not B, E?

   upvoted 1 times

  **gcpengineer** 2 years, 2 months ago

how u will ensure data is getting encrypted at transit

   upvoted 1 times

  **pmrifo** 2 years, 7 months ago

https://cloud.google.com/compute/confidential-vm/docs/about-cvm#end-to-end_encryption

   upvoted 1 times

  **Littleivy** 2 years, 8 months ago

Selected Answer: DE

Selected Answer: DE

Google Cloud customers with additional requirements for encryption of data over WAN can choose to implement further protections for data as it moves from a user to an application, or virtual machine to virtual machine. These protections include IPsec tunnels, Gmail S/MIME, managed SSL certificates, and Istio.

<https://cloud.google.com/docs/security/encryption-in-transit>

👍 ↩ 🚩 upvoted 4 times

🗒️ 👤 **AwesomeGCP** 2 years, 9 months ago

Selected Answer: DE

D. Confidential Computing and Istio
E. Client-side encryption

👍 ↩ 🚩 upvoted 3 times

🗒️ 👤 **zellick** 2 years, 10 months ago

Selected Answer: AE

AE is my answer.

👍 ↩ 🚩 upvoted 1 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses



© 2024 ExamTopics