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 100 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 100
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You need to implement an encryption at-rest strategy that reduces key management complexity for non-sensitive data and protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule. FIPS 140-2 L1 compliance is required for all data types. What should you do?

A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.

B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service

C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.

D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Show Suggested Answer

by mouchu at *May 17, 2022, 9:44 a.m.*

Comments

Type your comment...

Submit

Chute5118 Highly Voted 3 years ago

Selected Answer: D

Both B and D seem correct tbh. D might be "more correct" depending on the interpretation.

"reduces key management complexity for non-sensitive data" - Google default encryption
"protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule" - Customer Managed Key

upvoted 6 times

AzureDP900 2 years, 8 months ago

I agree, D is right

upvoted 2 times

zellck Highly Voted 2 years, 10 months ago

Selected Answer: D

D is the answer.

upvoted 5 times

Zek Most Recent 7 months, 3 weeks ago

Selected Answer: D

https://cloud.google.com/kms/docs/key-management-service#choose
For example, you might use software keys for your least sensitive data and hardware or external keys for your most sensitive data.

FIPS 140-2 Level 1 validated applies to both Google default encryption and Cloud Key Management Service (KMS)

upvoted 1 times

dija123 1 year, 4 months ago

Selected Answer: D

D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service (KMS)

upvoted 1 times

MHD84 1 year, 11 months ago

corrcet Answer is D, both KMS and default encryption are FIPS 140-2 L1 compliance https://cloud.google.com/kms/docs/key-management-service#choose

upvoted 3 times

[Removed] 2 years ago

Selected Answer: D

"D"
Default encryption is Fips 140-2 L2 compliant (reference A below). Cloud KMS provides the rotation convenience desired (reference B below).

References:
A- https://cloud.google.com/docs/security/encryption/default-encryption
B- https://cloud.google.com/docs/security/key-management-deep-dive

upvoted 3 times

passex 2 years, 7 months ago

"reduces key management" & "FIPS 140-2 L1 compliance is required for all data types" - strongly suggests answer B

upvoted 1 times

rrvv 2 years, 10 months ago

As FIPS 140-2 L1 compliance is required for all types of data, Cloud KMS should be used to manage encryption. Correct answer is B

https://cloud.google.com/docs/security/key-management-deep-dive#software-protection-level:~:text=The%20Cloud%20KMS%20binary%20is%20built%20against%20FIPS%20140%2D2%20Level%201%E2%80%93validated%20Cryptographic%20Primitives%20of%20this%20module

upvoted 1 times

sumundada 3 years ago

Selected Answer: D

Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provideflexibility of controlling the key residency and rotation schedule, use google provided key for non-sensitive and encrypt sensitive data with Cloud Key Management Service

upvoted 3 times

nacying 3 years, 1 month ago

Selected Answer: B

base on "FIPS 140-2 L1 compliance is required for all data types"

upvoted 3 times

cloudprincipal 3 years, 1 month ago

Selected Answer: D

KMS is ok for fips 140-2 level 1
https://cloud.google.com/docs/security/key-management-deep-dive#platform-overview

upvoted 2 times

cloudprincipal 3 years, 1 month ago

Regarding FIPS 140-2 level 1 and GCP default encryption:

Google Cloud uses a FIPS 140-2 validated Level 1 encryption module (certificate 3318) in our production environment.

https://cloud.google.com/docs/security/encryption/default-encryption?hl=en#encryption_of_data_at_rest

upvoted 2 times

mikesp 3 years, 1 month ago

In my opinion, the answer is B. The question says that it is necessary to control "key residency and rotation schedule" for both types of data. Default encryption at rest does not provide that but Cloud KMS does. Furthermore, Cloud KMS is FIPS140-2 level 1.
https://cloud.google.com/docs/security/key-management-deep-dive

upvoted 3 times

csrazdan 2 years, 7 months ago

The answer is D.
1. reduce key management complexity for non-sensitive data --> Google Managed key
2. protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule --> KMS

upvoted 1 times

szl0144 3 years, 2 months ago

D is the wander

upvoted 3 times

mouchu 3 years, 2 months ago

Answer = D

upvoted 3 times

EXAMTOPICS

Platform

Home
Examtopics PRO
All Exams
Training Courses

© 2024 ExamTopics