EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 38 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 38
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).
How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.

B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.

C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.

D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Show Suggested Answer

by skshak at *Sept. 22, 2020, 8:15 p.m.*

Comments

Type your comment...

Submit

DebasishLowes Highly Voted 4 years, 4 months ago

Ans : B. Because if you encrypt the object using CSEK, then you can't use google cloud console to upload the object.

upvoted 15 times

FatCharlie Highly Voted 4 years, 8 months ago

The fact is, both B & D would work. I lean towards B because it allows you to manage the file using GCP tools later as long as you keep that key around.

B is definitely incomplete though, as the boto file does need to be updated.

upvoted 7 times

gcpengineer 2 years, 2 months ago

it mentions u cant use console for CSEK

upvoted 1 times

3d9563b Most Recent 1 year ago

Selected Answer: B

Using the gsutil command-line tool with the appropriate options to specify the CSEK during the upload process is the proper way to manage customer-supplied encryption keys for Cloud Storage. This ensures that the data is encrypted using the provided key without the key being stored on Google's servers

upvoted 1 times

3d9563b 1 year ago

Selected Answer: D

With Customer-Supplied Encryption Keys (CSEK), you handle the encryption of the data yourself and then upload the encrypted data to Cloud Storage, ensuring you provide the necessary encryption key when required for access control. This method ensures that you maintain control over the encryption process and the security of your data.

upvoted 1 times

salamKvelas 1 year, 1 month ago

`gcloud storage` you can point to a CSEK, but `gsutil` you can not

upvoted 1 times

shanwford 1 year, 3 months ago

Selected Answer: B

Should be (B) - but IMHO "gsutil" is legacy tool, it works with "gcloud": gcloud storage cp SOURCE_DATA gs://BUCKET_NAME/OBJECT_NAME --encryption-key=YOUR_ENCRYPTION_KEY

upvoted 2 times

ppandher 1 year, 9 months ago

I have encrypt the object using 256 Encryption method, When I create a Bucket it gave me option of encryption as Google Managed Keys and Customer Managed keys but NO CSEK, I opted Google Managed as I do not have CMEK created, Now I create that Bucket.I upload my encrypted file to that bucket using Console, now the content of that file shows as Google managed not a CSEK.

To my understanding you need to generate the keys in console encrypt that object and then upload that way it will show on that object as encryption of CSEK.
Option B I opt now.

upvoted 1 times

mildi 2 years ago

Answer D with removed or from console
D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.
D. Encrypt the object, then use the gsutil command line tool

upvoted 1 times

twpower 2 years, 2 months ago

Selected Answer: B

Ans is B

upvoted 1 times

gcpengineer 2 years, 2 months ago

Selected Answer: B

B is the ans . https://cloud.google.com/storage/docs/encryption/customer-supplied-keys

upvoted 2 times

TQM__9MD 2 years, 2 months ago

Selected Answer: D

Object encryption is required. B does not encrypt objects

Object encryption is required. B does not encrypt objects.

upvoted 2 times

aashissh 2 years, 3 months ago

Selected Answer: D

To use customer-supplied encryption keys (CSEK) for encrypting data on Cloud Storage, the security team must encrypt the object first using the encryption key and then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage. Therefore, the correct answer is:

D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

upvoted 2 times

gcpengineer 2 years, 2 months ago

it mentions u cant use console for CSEK

upvoted 1 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: B

https://cloud.google.com/storage/docs/encryption/customer-supplied-keys
Answer B

upvoted 2 times

GHOST1985 2 years, 9 months ago

Selected Answer: B

you can't use google cloud console to upload the object.
https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys#upload_with_your_encryption_key

upvoted 1 times

absipat 3 years, 1 month ago

D of course

upvoted 1 times

Aiffone 3 years, 1 month ago

I will go with D because encrypting the object before uploading means the cutomer manages thier own key.
A is not correct because its not a good practice to upload encryption key to storage object along with the encrypted object.
B is not correct because specifying the location of the encryption key does not change anything
C means Google manages the key.

upvoted 1 times

VivekA 4 years, 8 months ago

Ans: B
CSEK doesn't work on Cloud Shell or Cloud Console for Cloud Storage
https://cloud.google.com/storage/docs/encryption/customer-supplied-keys

upvoted 4 times

VivekA 4 years, 8 months ago

D can't be an option - Refer restriction section.
https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#:~:text=You%20cannot%20use%20the%20Google,a%20customer%2Dsupplied%20encryption%20key.

upvoted 1 times

Load full discussion...