Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 159 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 159
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You discovered that sensitive personally identifiable information (PII) is being ingested to your Google Cloud environment in the daily ETL process from an on- premises environment to your BigQuery datasets. You need to redact this data to obfuscate the PII, but need to re-identify it for data analytics purposes. Which components should you use in your solution? (Choose two.)

A. Secret Manager

B. Cloud Key Management Service

C. Cloud Data Loss Prevention with cryptographic hashing

D. Cloud Data Loss Prevention with automatic text redaction

E. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

Show Suggested Answer

by GHOST1985 at *Sept. 12, 2022, 3:53 p.m.*

Comments

Type your comment...

Submit

GHOST1985 Highly Voted 2 years, 4 months ago

Selected Answer: BE

B: you need KMS to store the CryptoKey
https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#crypt

E: for the de-identity you need to use CryptoReplaceFfxFpeConfig or CryptoDeterministicConfig
https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#cryptodeterministicconfig
https://cloud.google.com/dlp/docs/deidentify-sensitive-data

upvoted 14 times

Ric350 1 year, 10 months ago

BE is correct. Ghost links are correct and this link here shows a reference architecture using cloud KMS and Cloud DLP
https://cloud.google.com/architecture/de-identification-re-identification-pii-using-cloud-dlp

upvoted 6 times

mjcts Most Recent 1 year ago

Selected Answer: BE

KMS for storing the encryption key
Deterministic encryption so that you can reverse the process

upvoted 1 times

gkarthik1919 1 year, 4 months ago

BE are right. D is incorrect because automatic text redaction will remove the sensitive PII data which is not the requirement .

upvoted 2 times

anshad666 1 year, 5 months ago

Selected Answer: BE

looks viable

upvoted 1 times

gcpengineer 1 year, 8 months ago

why shd anyone use KMS to determine PII?

upvoted 1 times

YourFriendlyNeighborhoodSpider 4 months, 1 week ago

Good question.....

upvoted 1 times

gcpengineer 1 year, 8 months ago

Selected Answer: DE

DE is the ans

upvoted 1 times

gcpengineer 1 year, 8 months ago

BE is the answer

upvoted 1 times

AzureDP900 2 years, 2 months ago

B & E is right

upvoted 2 times

AwesomeGCP 2 years, 3 months ago

Selected Answer: BE

B. Cloud Key Management Service
E. Cloud Data Loss Prevention with deterministic encryption using AES-SIV

upvoted 4 times

zellck 2 years, 4 months ago

Selected Answer: BE

BE is the answer.

upvoted 4 times

waikiki 2 years, 4 months ago

No. As a result of checking the documentation, crypto key = This is a data encryption key (DEK) (as opposed to a key encryption key (KEK) stored by Cloud Key Management Service (Cloud KMS).

upvoted 1 times

Ric350 1 year, 10 months ago

It's BE. BE is correct. Ghost links are correct and this link here shows a reference architecture using cloud KMS and Cloud

DLP
https://cloud.google.com/architecture/de-identification-re-identification-pii-using-cloud-dlp

upvoted 2 times