EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 155 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 155
Topic #: 1
[All Associate Cloud Engineer Questions]

You are storing sensitive information in a Cloud Storage bucket. For legal reasons, you need to be able to record all requests that read any of the stored data. You want to make sure you comply with these requirements. What should you do?

A. Enable the Identity Aware Proxy API on the project.

B. Scan the bucket using the Data Loss Prevention API.

C. Allow only a single Service Account access to read the data.

D. Enable Data Access audit logs for the Cloud Storage API.

Show Suggested Answer

by francisco_guerra at *Aug. 13, 2020, 2:57 a.m.*

Comments

Type your comment...

Submit

ESP_SAP Highly Voted 4 years, 2 months ago

Correct Answer is (D):

Logged information
Within Cloud Audit Logs, there are two types of logs:

Admin Activity logs: Entries for operations that modify the configuration or metadata of a project, bucket, or object.

Data Access logs: Entries for operations that modify objects or read a project, bucket, or object. There are several sub-types of data access logs:

ADMIN_READ: Entries for operations that read the configuration or metadata of a project, bucket, or object.

DATA_READ: Entries for operations that read an object.

DATA_WRITE: Entries for operations that create or modify an object.

https://cloud.google.com/storage/docs/audit-logs#types

upvoted 32 times

francisco_guerra Highly Voted 4 years, 2 months ago

D is the correct one

upvoted 19 times

SSPC 4 years, 2 months ago

Yes D is the correct

upvoted 6 times

PiperMe Most Recent 7 months, 3 weeks ago

D is the best answer:
- Data Access audit logs are specifically designed to track Google Cloud API operations related to data, including reads from Cloud Storage buckets.
- These logs include details about the user or service account making the request, the time, and the specific data resource accessed.
- Having this audit trail is essential for demonstrating adherence to regulations around sensitive data handling.
Why Others Aren't as Ideal:
A: Identity-Aware Proxy (IAP): IAP focuses on controlling access to web apps behind firewalls but doesn't inherently log all data read operations.
B: Data Loss Prevention (DLP): DLP is excellent for identifying sensitive data within your bucket but doesn't provide a continuous audit log of every access.
C: Restricting Access: While limiting access is a security best practice, it doesn't address the legal requirement to log every read operation.

upvoted 2 times

scanner2 1 year, 1 month ago

Selected Answer: D

Enable Data access audit logs for Cloud storage bucket
https://cloud.google.com/storage/docs/audit-logging

upvoted 2 times

Captain1212 1 year, 1 month ago

Selected Answer: D

D is the correct answer

upvoted 1 times

calm_fox 1 year, 10 months ago

Selected Answer: D

Only logical option

upvoted 1 times

AzureDP900 2 years, 4 months ago

D is right for this use case

upvoted 1 times

Akash7 2 years, 5 months ago

D is correct as Data Access logs pertaining to Cloud Storage operations are not recorded by default. You have to enable them ...
https://cloud.google.com/storage/docs/audit-logging

upvoted 2 times

wael_tn 2 years, 6 months ago

Selected Answer: D

I think it's D

upvoted 1 times

Surat 2 years, 9 months ago

I also vote for D

upvoted 2 times

Vinoth9289 3 years, 1 month ago

D is the correct Answer

upvoted 2 times

WakandaF 3 years, 5 months ago

seems that B is the right!

Cloud Data Loss Prevention (DLP) helps you to understand and manage such sensitive data. It provides fast, scalable classification and redaction for sensitive data elements. Using the Data Loss Prevention API and Cloud Functions, you can automatically scan this data before it is uploaded to the shared storage bucket.

upvoted 1 times

YAS007 3 years, 2 months ago

the question doesn't ask you to manage or understand sensitive data :
" you need to be able to record all requests that read any of the stored data"

upvoted 3 times

victory108 3 years, 7 months ago

D - Enable Data Access audit logs for the Cloud Storage API.

upvoted 1 times

EABDAJA 3 years, 7 months ago

D is correct

upvoted 1 times

GCP_Student1 3 years, 7 months ago

D. Enable Data Access audit logs for the Cloud Storage API.

upvoted 2 times

swatititame 3 years, 11 months ago

• D. Enable Data Access audit logs for the Cloud Storage API.

upvoted 1 times

RockAJ 4 years ago

Ans is D

upvoted 2 times

Load full discussion...

Social Media

Facebook , Twitter
YouTube , Reddit
Pinterest

We are the biggest and most updated IT certification exam material website.
Using our own resources, we strive to strengthen the IT professionals community for free.