Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 89 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 89
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually.
You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.
What should you do?

A. Set up an ACL with OWNER permission to a scope of allUsers.

B. Set up an ACL with READER permission to a scope of allUsers.

C. Set up a default bucket ACL and manage access for users using IAM.

D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

Show Suggested Answer

by skshak at *Sept. 22, 2020, 8:45 p.m.*

Comments

Type your comment...

Submit

Fellipo Highly Voted 4 years, 8 months ago

it's D, https://cloud.google.com/storage/docs/uniform-bucket-level-access#:~:text=When%20you%20enable%20uniform%20bucket,and%20the%20objects%20it%20contains.

upvoted 19 times

Xoxoo Highly Voted 1 year, 10 months ago

Selected Answer: D

To manage access to your Cloud Storage bucket without having to manage access to each object individually, you should set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM .

Uniform bucket-level access allows you to use Identity and Access Management (IAM) alone to manage permissions for all objects contained inside the bucket or groups of objects with common name prefixes . This approach simplifies access management and ensures that all objects in the bucket have the same level of access .

By using IAM, you can grant users specific permissions to access your Cloud Storage bucket, such as read, write, or delete permissions . You can also use Cloud Audit Logs to monitor and manage access to your bucket .

This approach provides a secure environment for your Cloud Storage bucket while ensuring that only authorized users can access it .

upvoted 5 times

Zek Most Recent 7 months, 4 weeks ago

Selected Answer: D

Answer is D
https://cloud.google.com/storage/docs/uniform-bucket-level-access#overview

upvoted 1 times

Zek 7 months, 4 weeks ago

Not A, B or C because "ACLs are used only by Cloud Storage and have limited permission options, but they allow you to grant permissions on a per-object basis"

upvoted 1 times

BPzen 8 months ago

Selected Answer: D

Explanation:
When you want to avoid managing access to individual objects in a Google Cloud Storage bucket, Uniform bucket-level access simplifies access control by enforcing consistent permissions at the bucket level. It disables per-object ACLs and enables centralized access management using IAM roles and permissions.

upvoted 1 times

tia_gll 1 year, 4 months ago

Selected Answer: D

ans is D

upvoted 1 times

nccdebug 1 year, 5 months ago

Ans: D. https://cloud.google.com/storage/docs/uniform-bucket-level-access

upvoted 1 times

AzureDP900 2 years, 8 months ago

D is right

upvoted 3 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: D

D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

upvoted 5 times

cloudprincipal 3 years, 1 month ago

Selected Answer: D

https://cloud.google.com/storage/docs/uniform-bucket-level-access#enabled

upvoted 3 times

ramravella 4 years ago

Answer is A. Read the note below in the below URL

https://cloud.google.com/storage/docs/access-control/lists

Note: You cannot grant discrete permissions for reading or writing ACLs or other metadata. To allow someone to read and write ACLs, you must grant them OWNER permission.

write ACLs, you must grant them OWNER permission.

upvoted 1 times

Zuy01 3 years, 11 months ago

the question mention "do not want the uploader of an object to always have full control of the object" that's mean you shouldn't grant the owner permission, hence the best ans is D.

upvoted 3 times

saurabh1805 4 years, 9 months ago

I will go with uniform level access and manage access via IAM,

Hence D.

upvoted 2 times

passtest100 4 years, 10 months ago

SHOULD BE D

upvoted 2 times

skshak 4 years, 10 months ago

Answer C https://cloud.google.com/storage/docs/access-control
Uniform (recommended): Uniform bucket-level access allows you to use Identity and Access Management (IAM) alone to manage permissions. IAM applies permissions to all the objects contained inside the bucket or groups of objects with common name prefixes. IAM also allows you to use features that are not available when working with ACLs, such as IAM Conditions and Cloud Audit Logs.

upvoted 1 times

skshak 4 years, 9 months ago

Sorry, It is D. It was typo.

upvoted 3 times

mlyu 4 years, 9 months ago

the question stated they need cloud audit log for the GCS access, however uniform bucket-level access has restriction on the cloud audit log.
See https://cloud.google.com/storage/docs/uniform-bucket-level-access
The following restrictions apply when using uniform bucket-level access:
Cloud Logging and Cloud Audit Logs cannot export to buckets that have uniform bucket-level access enabled.

upvoted 1 times

FatCharlie 4 years, 8 months ago

They're not saying they want to export the logs to the bucket. They're just saying they want to "use Cloud Audit Logs to manage access to your bucket" (whatever that means).

upvoted 1 times