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 176 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 176
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You need to enforce a security policy in your Google Cloud organization that prevents users from exposing objects in their buckets externally. There are currently no buckets in your organization. Which solution should you implement proactively to achieve this goal with the least operational overhead?

A. Create an hourly cron job to run a Cloud Function that finds public buckets and makes them private.

B. Enable the constraints/storage.publicAccessPrevention constraint at the organization level.

C. Enable the constraints/storage.uniformBucketLevelAccess constraint at the organization level.

D. Create a VPC Service Controls perimeter that protects the storage.googleapis.com service in your projects that contains buckets. Add any new project that contains a bucket to the perimeter.

Show Suggested Answer

by Random_Mane at *Sept. 6, 2022, 1:41 a.m.*

Comments

Type your comment...

Submit

cyberpunk21 11 months, 1 week ago

Selected Answer: B

B is correct, C talks about access which we don't need

upvoted 2 times

pedrojorge 1 year, 6 months ago

Selected Answer: B

B, "When you apply the publicAccessPrevention constraint on a resource, public access is restricted for all buckets and objects, both new and existing, under that resource."

upvoted 4 times

TonytheTiger 1 year, 7 months ago

Exam Question Dec 2022

upvoted 3 times

AzureDP900 1 year, 8 months ago

B is right

upvoted 2 times

AzureDP900 1 year, 8 months ago

Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public. When you enforce public access prevention, no one can make data in applicable buckets public through IAM policies or ACLs. There are two ways to enforce public access prevention:

You can enforce public access prevention on individual buckets.

If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

upvoted 2 times

AwesomeGCP 1 year, 9 months ago

Selected Answer: B

B. Enable the constraints/storage.publicAccessPrevention constraint at the organization level.

upvoted 2 times

zellck 1 year, 10 months ago

Selected Answer: B

B is the answer.

https://cloud.google.com/storage/docs/public-access-prevention
Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public.
If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

upvoted 4 times

Random_Mane 1 year, 10 months ago

Selected Answer: B

B. https://cloud.google.com/storage/docs/org-policy-constraints
"When you apply the publicAccessPrevention constraint on a resource, public access is restricted for all buckets and objects, both new and existing, under that resource."

upvoted 2 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses

© 2024 ExamTopics