



- Expert Verified, Online, Free.

 MENU



Google Discussions



Exam Associate Cloud Engineer All Questions

View all questions & answers for the Associate Cloud Engineer exam

Go to Exam

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 26 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 26

Topic #: 1

[\[All Associate Cloud Engineer Questions\]](#)

You need to set up permissions for a set of Compute Engine instances to enable them to write data into a particular Cloud Storage bucket. You want to follow Google-recommended practices. What should you do?

- A. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/devstorage.write_only'.
- B. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/cloud-platform'.
- C. Create a service account and add it to the IAM role 'storage.objectCreator' for that bucket.
- D. Create a service account and add it to the IAM role 'storage.objectAdmin' for that bucket.

Show Suggested Answer

by [coldpar](#) at March 15, 2020, 10:11 p.m.

Comments

Type your comment...

Submit

? ? **coldpar** Highly Voted ? 4 years, 7 months ago

As per as the least privilege recommended by google, C is the correct Option, A is incorrect because the scope doesn't exist. B incorrect because it will give him full of control

? ? ? upvoted 58 times

? ? **johnconnor** 2 years, 3 months ago

Check here, it is A-> <https://cloud.google.com/storage/docs/authentication>
<https://cloud.google.com/storage/docs/authentication>

? ? ? upvoted 1 times

? ? **Bedmed** 1 year, 10 months ago

In the Document, it includes https://www.googleapis.com/auth/devstorage.read_write scope

? ? ? upvoted 1 times

? ? **CVGCP** 1 year, 4 months ago

There is no scope called write-only, as per the reference document.

? ? ? upvoted 1 times

? ? **karim1321** 1 year, 4 months ago

In the Document, 'write -only' does not exist. Just read-only

? ? ? upvoted 2 times

? ? **robor97** 3 years, 10 months ago

The scope does exist -

<https://download.huihoo.com/google/gdgdevkit/DVD1/developers.google.com/compute/docs/api/how-tos/authorization.html>

? ? ? upvoted 2 times

? ? **gielda211** 2 years, 6 months ago

it doesn't exist. show us this on official google website

? ? ? upvoted 2 times

? ? **peter77** 3 years, 1 month ago

No it doesn't. You have read-only, read-write, full-control and others... but "write-only" is not a thing.

<https://cloud.google.com/storage/docs/authentication>

? ? ? upvoted 4 times

? ? **XRiddlerX** Highly Voted ? 4 years, 3 months ago

In reviewing this, it looks to be a multiple answer question. According to Best Practices in this Google Doc (https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#best_practices) you grant the instance the scope and the permissions are determined by the IAM roles of the service account. In this case, you would grant the instance the scope and the role (storage.objectCreator) to the service account.

Ans B and C

Role from GCP Console:

ID = roles/storage.objectCreator

Role launch stage = General Availability

Description = Access to create objects in GCS.

3 assigned permissions

resourceManager.projects.get

resourceManager.projects.list

storage.objects.create

? ? ? upvoted 18 times

? ? **nickyshil** 2 years, 2 months ago

There are many access scopes available to choose from, but a best practice is to set the cloud-platform access scope, which is an OAuth scope for most Google Cloud services, and then control the service account's access by granting it IAM roles..you have an app that reads and writes files on Cloud Storage, it must first authenticate to the Cloud Storage API. You can create an instance with the cloud-platform scope and attach a service account to the instance <https://cloud.google.com/compute/docs/access/service-accounts>

? ? ? upvoted 1 times

? ? **ryumada** 2 years, 2 months ago

Reading the second point of the best practice. You should grant your VM the <https://www.googleapis.com/auth/cloud-platform> scope to allow access to most of Google Cloud APIs.

So, that the IAM permissions are completely determined by the IAM roles you granted to the service account.

The conclusion is you should not mess up with the VM scopes to grant access to Google Services, instead you should grant the access via IAM roles of the service account you attached to the VM.


https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#best_practices

   upvoted 2 times

  **Enamfrancis** Most Recent  4 weeks, 1 day ago

C because of 'storage.objectCreator'

   upvoted 1 times

  **andreiboaghe95** 4 months, 1 week ago

Selected Answer: C

Correct answer is C

   upvoted 1 times

  **BAofBK** 11 months, 2 weeks ago

Correct answer is D

   upvoted 1 times

  **gsmasad** 11 months, 3 weeks ago

Selected Answer: C

storage.objectCreator contains sufficient privileges to do the job & so admin is not required

   upvoted 1 times

  **YourCloudGuru** 1 year ago

Selected Answer: C

The correct answer is C.

The other options are not accurate and go against the principle of giving least required access.

A is incorrect as there is no role as write_only

B is not a good option as it gives full control of google cloud services where as we are looking for write data into a particular cloud storage bucket



D. is not a good option as it gives full control over objects

Sources:

<https://cloud.google.com/storage/docs/authentication>

<https://cloud.google.com/storage/docs/access-control/iam-roles>

   upvoted 4 times

  **Captain1212** 1 year, 1 month ago

Selected Answer: C


c seems more correct, you need to go iam to provide the permissions , b and d will give it more or full access

   upvoted 1 times

  **Neha_Pallavi** 1 year, 3 months ago

Associate Cloud Engineer exam booked very soon. kindly share the all the questions and any other support exam to clear this

   upvoted 2 times

  **Shubha1** 1 year, 2 months ago

Hi Neha, Please let me know how your exam was? I am taking the exam soon. Thanks



   upvoted 1 times

  **ExamsFR** 1 year, 3 months ago

Selected Answer: C

C is correct

   upvoted 1 times

  **rosh199** 1 year, 3 months ago

C is correct

   upvoted 1 times

  **CVGCP** 1 year, 4 months ago

Selected Answer: C

C is correct answer

   upvoted 3 times

? ? **trainingexam** 1 year, 4 months ago

Selected Answer: C

The ask is how the “Compute Engine instances to enable them to write data into a particular Cloud Storage bucket”. A service account is a special kind of account used by an application or compute workload, rather than a person. When you set up an instance to run as a service account, you determine the level of access the service account has by the IAM roles that you grant to the service account. If the service account has no IAM roles, then no resources can be accessed using the service account on that instance.

The best Practice suggested by Google is refer in this link: https://cloud.google.com/compute/docs/access/service-accounts#scopes_best_practice <https://cloud.google.com/storage/docs/access-control/iam-roles> shows that storage.objectCreator is best choice of the role for this problem statement.

? ? ? upvoted 1 times

? ? **Praxii** 1 year, 5 months ago

Selected Answer: C

The correct answer is C.

There is no role as write only its read only hence A is incorrect.

? ? ? upvoted 1 times

? ? **Ashish_Tayal** 1 year, 6 months ago

Selected Answer: C

IAM Work on Principal of least privilege,

? ? ? upvoted 1 times

? ? **smanoj85** 1 year, 7 months ago

Option C is the correct answer. To grant a set of Compute Engine instances permissions to write data to a particular Cloud Storage bucket, you should create a service account and add it to the IAM role 'storage.objectCreator' for that bucket. This IAM role allows the service account to create new objects in the bucket, but it does not allow it to modify or delete existing objects. Option A is incorrect because the access scope 'https://www.googleapis.com/auth/devstorage.write_only' does not exist. Option B is incorrect because the access scope 'https://www.googleapis.com/auth/cloud-platform' grants permissions for all Google Cloud Platform services, which is overly broad and not recommended. Option D is incorrect because the IAM role 'storage.objectAdmin' provides full control over the bucket, which is more access than necessary to allow the Compute Engine instances to write data to the bucket.

? ? ? upvoted 2 times

? ? **red_panda** 1 year, 7 months ago

Selected Answer: C

According to least privileges, the correct answer is C

? ? ? upvoted 1 times

[Load full discussion...](#)

Start Learning for free



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.



© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.