🔍

← **Google Discussions**

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 71 DISCUSSION**

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 71

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.

What should you do?

A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.

B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.

C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.

D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

Show Suggested Answer

by 👤 **MohitA** at *Sept. 2, 2020, 10:19 a.m.*

Comments

Type your comment...

Submit

☐ 👤 **MohitA** [Highly Voted 👍] 3 years, 11 months ago
B, https://cloud.google.com/compute/docs/access/iam
👍 👎 📋 upvoted 16 times

mlyu 3 years, 10 months ago

Although it is not encourage to use custome role, but last sentence in the answer C makes B be the only option

AzureDP900 1 year, 8 months ago

B is right

sudarchary `Highly Voted` 2 years, 6 months ago

B. The only option that adheres to the principle of least privilege and meets
question requirements is B

ArizonaClassics `Most Recent` 10 months, 2 weeks ago

B. Create a custom role with the permission compute.instances.list and grant the Service Account this role: This follows the principle of least privilege by granting only the specific permission needed.

Brosh 1 year, 7 months ago

I don't get why is it not C, you grant that specific service account the role over all instances, is it wrong because that service account will be able to view not only compute instances?

shayke 1 year, 7 months ago

`Selected Answer: B`

B is the right ans - you only want to list the instances

Meyucho 1 year, 7 months ago

`Selected Answer: B`

With C the SA will list ONLY the instances that are configured to use that SA.
The option B will give permissions to list ALL instances.

AwesomeGCP 1 year, 9 months ago

`Selected Answer: B`

B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.

nbrnschwgr 1 year, 11 months ago

C. because google recommends pre-defined narrow scope roles over custom roles.

Roflcopter 1 year, 11 months ago

`Selected Answer: B`

Key here is "and grant the Service Account this role.". C and D are giving this role to ALL instances which is overly permissive. A is wrong. Only choice is B

cloudprincipal 2 years, 1 month ago

`Selected Answer: B`

The roles/compute.viewer provides a lot more privileges than just listing compute instances

cloudprincipal 2 years, 1 month ago

`Selected Answer: C`

Compute Viewer
Read-only access to get and list Compute Engine resources, without being able to read the data stored on them.

https://cloud.google.com/compute/docs/access/iam#compute.viewer

cloudprincipal 2 years, 1 month ago

This is incorrect, as Compute Viewer provides a lot more than what is required

DebasishLowes 3 years, 4 months ago

Ans : B

👍 ↩ 🏴 upvoted 1 times

⊟ 👤 **dtmtor** 3 years, 4 months ago

Ans is B

👍 ↩ 🏴 upvoted 1 times

⊟ 👤 **genesis3k** 3 years, 9 months ago

Answer is B, based on least privilege principle.

👍 ↩ 🏴 upvoted 1 times