Google Discussions

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 235 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 235
Topic #: 1
[All Associate Cloud Engineer Questions]

The DevOps group in your organization needs full control of Compute Engine resources in your development project. However, they should not have permission to create or update any other resources in the project. You want to follow Google's recommendations for setting permissions for the DevOps group. What should you do?

A. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

B. Create an IAM policy and grant all compute.instanceAdmin.* permissions to the policy. Attach the policy to the DevOps group.

C. Create a custom role at the folder level and grant all compute.instanceAdmin.* permissions to the role. Grant the custom role to the DevOps group.

D. Grant the basic role roles/editor to the DevOps group.

Show Suggested Answer

by happydays at *Aug. 2, 2023, 2:45 p.m.*

Comments

VijKall Highly Voted 11 months, 3 weeks ago

Selected Answer: A

Answer is A.
roles/viewer gives read only access on Project, so it does not create/update any resources.
roles/compute.admin gives full access to Compute Engine resources.

upvoted 8 times

carlalap Highly Voted 11 months, 1 week ago

Answer is C.
1. The DevOps group needs full control of Compute Engine resources in your development project. --> So, we grants permissions to create and update Compute Engine instances and their related resources, such as disks, images, and snapshots.

A// Create a custom role at the folder level and grant all compute.instanceAdmin.* permissions to the role.

2. They should not have permission to create or update any other resources in the project. --> We do not grant permissions to create or update any other resources in the project, such as Cloud Storage buckets, Cloud Functions, or BigQuery datasets.

A// Grant the custom role to the DevOps group.

upvoted 7 times

goalDigger 9 months, 2 weeks ago

We can only grant a custom role within the project or organization in which we created it. We cannot grant custom roles on other projects or organizations, or on resources within other projects or organizations. Note: We cannot define custom roles at the folder level. So, C cannot be the answer.

upvoted 2 times

ccpmad 4 months, 3 weeks ago

ok, yes, we can not create a custom role at folder level, but we can create the custom role at organization level, and then, go to IAM at folder level, and use that custom role that give permissions at folder level. I have just try it and works.

Moreover, it is not possible A, because question says that Dev group has to have permissions in development project. I think question is not correctly written. Becuase A answer allow Dev Grop to create resources in any project in the organization.

But finally, knowing the question is not writteng correctly, in the exam, I think I will bet for A.

upvoted 1 times

ccpmad 4 months, 3 weeks ago

Yes, I have just read another time answer C. C is not possible because says that creation of the custom role is at folder level. That is not possible.

In real life, we would create the custom role at organization level, and the use it at folder level, so Dev group only have the permissions in their dev projecto.

For this question, in an exam, we have to pick A.

Thank you and good luck

upvoted 1 times

carlalap 11 months, 1 week ago

Furthermore, Google recommends using custom roles to grant the minimum set of permissions that users need to perform their tasks.

upvoted 1 times

vaibhavCodian 11 months ago

completely incorrect

Compute Admin
(roles/compute.admin)

Full control of all Compute Engine resources.

If the user will be managing virtual machine instances that are configured to run as a service account, you must also grant the roles/iam.serviceAccountUser role.

upvoted 1 times

Timfdklfajlksdjlakf Most Recent 1 month, 3 weeks ago

Selected Answer: A

The correct answer is A. Take it or leave it

upvoted 1 times

ngeorgiev2 7 months, 4 weeks ago

Selected Answer: A

"roles/compute.admin" - Full control of all Compute Engine resources.
"roles/compute.instanceAdmin" - If the user will be managing virtual machine instances that are configured to run as a service account, you must also grant the roles/iam.serviceAccountUser role.

Correct answer is definitely A

upvoted 2 times

sinh 9 months, 1 week ago

Selected Answer: B

Google recommends using custom roles

upvoted 1 times

ccpmad 5 months ago

IAM policy is not for a project, is for organization, it is not B

upvoted 3 times

Cynthia2023 9 months, 3 weeks ago

Selected Answer: A

A. Grant roles/viewer and roles/compute.admin:
• The roles/viewer role provides read-only access to most Google Cloud services
• The roles/compute.admin role gives full control over Compute Engine resources, which is appropriate for the DevOps group's needs.

upvoted 2 times

Peto12 10 months, 1 week ago

Selected Answer: B

This one is very tricky, by my opinion correct answer is B.

This wildcard at the end is important "grant all compute.instanceAdmin.*" that means that you need to assign two policies that are already there:

- roles/compute.instanceAdmin.v1
- roles/compute.instanceAdmin (beta)

So if the user has compute.instanceAdmin.v1 he will have full compute access without adding the additional one "roles/iam.serviceAccountUser". Also another argument against answer A is the Google recommendations to use the basic roles only when there is no predefined roles, and this is valid for all kind of environments not just production.

upvoted 3 times

ccpmad 5 months ago

iam policy is for organization, this question is for a project. So it is not B

upvoted 1 times

kuracpalac 7 months, 3 weeks ago

I selected B as well due to the basic roles being mentioned in A, which Google says it's a no no as they are too broad.

upvoted 1 times

ogerber 10 months, 2 weeks ago

Its B, 100%

upvoted 2 times

Abbru00 12 months ago

Selected Answer: A

it's A, No doubt.

- "they should not have permission to create or update any other resources in the project"

that sentence doesn't state that they don't want give acess to other resources, just not create or update.
basic roles/viewer gives permissions for read-only actions:
https://cloud.google.com/iam/docs/understanding-roles

- "Full control of all Compute Engine resources"

- "Full control of all Compute Engine resources"
Compute Admin (roles/compute.admin) gives full control of all Compute Engine resources.
https://cloud.google.com/iam/docs/understanding-roles#compute.admin

compute.instanceAdmin.* does not.

upvoted 3 times

ArtistS 12 months ago

C is definitely wrong. You cant create custom roles at folder level, you can create it at project or organization level

upvoted 1 times

AbdulJeilani 1 year ago

Selected Answer: B

I think its B. since they want full access to compute engine, so compute.instanceAdmin role but to restrict access to other resources, so no folder level access(C) is needed.

According to the web search results, one possible role that can give full access to Compute Engine but no access to other resources is the Compute Instance Admin role. This role allows a user to create and manage instances, disks, images, and snapshots, but not other resources like networks, firewalls, or load balancers.

upvoted 3 times

DBA03 1 year ago

Selected Answer: B

Explanation:

The compute.instanceAdmin.* permissions provide full control over Compute Engine resources, which aligns with the requirement for the DevOps group to have complete control over Compute Engine resources.
Creating an IAM policy and granting these specific permissions ensures the permissions are scoped to the project level, meeting the requirement to grant permissions only within the project and not beyond.
This option grants the necessary permissions for Compute Engine management at the project level while limiting the scope to the specified project.

upvoted 4 times

joao_01 1 year, 1 month ago

Selected Answer: B

For me its B, until anyone says the contrary and why. It give ONLY the permissions required. No more or less.

upvoted 3 times

iooj 1 month, 1 week ago

iam policy is for organization, this question is for a project, so actually - MORE

upvoted 1 times

DannSecurity 1 year, 1 month ago

Answer A
Compute Admin

(roles/compute.admin)
Full control of all Compute Engine resources.

upvoted 2 times

Captain1212 1 year, 1 month ago

Selected Answer: A

A is th correct answer as it provied all the required access

upvoted 2 times

NoCrapEva 1 year, 1 month ago

Selected Answer: A

Compute Admin (roles/compute.admin) = Full control of all Compute Engine resources.
The only permission to have full control of Computer Engine Resources (as required in question)
ref: https://cloud.google.com/iam/docs/understanding-roles#compute.admin

Compute.instanceAdmin does NOT allow FULL control of Compute Engine, only
Permissions to create, modify, and delete virtual machine instances. This includes permissions to create, modify, and delete disks, and also to configure Shielded VM settings.

upvoted 3 times

Az900Exam2021 1 year, 1 month ago

Selected Answer: C

C meets the requirement of permission with least privilege

upvoted 1 times

upvoted 1 times

Load full discussion...