

[Google Discussions](#)

Exam Professional Data Engineer All Questions

View all questions & answers for the Professional Data Engineer exam

[Go to Exam](#)

EXAM PROFESSIONAL DATA ENGINEER TOPIC 1 QUESTION 131 DISCUSSION

Actual exam question from Google's Professional Data Engineer

Question #: 131

Topic #: 1

[\[All Professional Data Engineer Questions\]](#)

As your organization expands its usage of GCP, many teams have started to create their own projects. Projects are further multiplied to accommodate different stages of deployments and target audiences. Each project requires unique access control configurations. The central IT team needs to have access to all projects. Furthermore, data from Cloud Storage buckets and BigQuery datasets must be shared for use in other projects in an ad hoc way. You want to simplify access control management by minimizing the number of policies. Which two steps should you take? (Choose two.)


- A. Use Cloud Deployment Manager to automate access provision.
- B. Introduce resource hierarchy to leverage access control policy inheritance.
- C. Create distinct groups for various teams, and specify groups in Cloud IAM policies.
- D. Only use service accounts when sharing data for Cloud Storage buckets and BigQuery datasets.
- E. For each Cloud Storage bucket or BigQuery dataset, decide which projects need access. Find all the active members who have access to these projects, and create a Cloud IAM policy to grant access to all these users.

[Show Suggested Answer](#)

by [deleted] at *March 22, 2020, 10:12 a.m.*





Comments

Submit





-  **[Removed]** Highly Voted 4 years, 1 month ago

Answer: B, C





Description: Google suggests that we should provide access by following google hierarchy and groups for users with similar roles

   upvoted 31 times
-  **sipsap** 3 years, 5 months ago





"Each project requires unique access control configurations" rules out hirearchy

   upvoted 11 times
-  **AJKumar** Highly Voted 3 years, 10 months ago

C is one option for sure, also C eliminates B as C includes groups and teams hierarchy, A can be eliminated as A talks about only deployment. From Remaining D and E, i find E most relevant to question--as E matches users with teams/groups and projects. Answer C and E.





   upvoted 20 times
-  **hauhau** 2 years, 8 months ago

Question mention minimize IAM policies,but E should create complex policies





   upvoted 5 times
-  **squishy_fishy** Most Recent 6 months, 1 week ago

Answer: A, C.

The Key question is "You want to simplify access control management by minimizing the number of policies". At the company where I work, we use Terraform to create infrastructure and assign needed roles for different environments.





   upvoted 2 times
-  **amittomar** 9 months, 3 weeks ago

It should be AC as it is mentioned in the question itself "You want to simplify access control management by minimizing the number of policies" which rules out B

   upvoted 2 times
-  **zellck** 1 year, 5 months ago

Selected Answer: BC





BC is the answer.

   upvoted 2 times
-  **FrankT2L** 1 year, 11 months ago





Selected Answer: BC

1. Define your resource hierarchy: Google Cloud resources are organized hierarchically. This hierarchy allows you to map your enterprise's operational structure to Google Cloud, and to manage access control and permissions for groups of related resources.
 2. Delegate responsibility with groups and service accounts: we recommend collecting users with the same responsibilities into groups and assigning IAM roles to the groups rather than to individual users.





<https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

   upvoted 7 times
-  **annie1196** 2 years, 3 months ago





A and C is correct, same question I encountered on Udemy.

   upvoted 2 times
-  **tavva_prudhvi** 2 years, 1 month ago

It doesn't mean it's right, please mention the reasons here not only the references.
Not A -> Every project has unique requirements, so "A" automation will not do much.
Not D -> As, Service accounts for computer to computer interactions not applications!
Not E -> E should create complex policies

   upvoted 1 times
-  **desertlotus1211** 1 year, 3 months ago

you explanation for D is incorrect...

   upvoted 3 times
-  **MaxNRG** 2 years, 3 months ago

Selected Answer: BC

B & C

Google Cloud resources are organized hierarchically, where the organization node is the root node in the hierarchy, the projects are the children of the organization, and the other resources are descendents of projects. You can set Cloud Identity and Access Management (Cloud IAM) policies at different levels of the resource hierarchy. Resources inherit the policies of the parent resource. The effective policy for a resource is the union of the policy set at that resource and the policy inherited from its parent.

<https://cloud.google.com/iam/docs/resource-hierarchy-access-control>

   upvoted 8 times

  **MaxNRG** 2 years, 3 months ago

We recommend collecting users with the same responsibilities into groups and assigning Cloud IAM roles to the groups rather than to individual users. For example, you can create a "data scientist" group and assign appropriate roles to enable interaction with BigQuery and Cloud Storage.

Grant roles to a Google group instead of to individual users when possible. It is easier to manage members in a Google group than to update a Cloud IAM policy.

<https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

   upvoted 4 times

  **AzureDP900** 1 year, 4 months ago

BC is the answer

   upvoted 1 times

  **medeis_jar** 2 years, 3 months ago

Selected Answer: AC

<https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

"Each project requires unique access control configurations" -> C eliminates B

A -> "Google Cloud Deployment Manager is an infrastructure deployment service that automates the creation and management of Google Cloud resources. Write flexible template and configuration files and use them to create deployments that have a variety of Google Cloud services"

"..simply the process.."

   upvoted 4 times

  **FP77** 8 months, 3 weeks ago

A makes no sense whatsoever...

   upvoted 1 times

  **MaxNRG** 2 years, 3 months ago

good point, AC looks better, agreed

   upvoted 1 times

  **MaxNRG** 2 years, 3 months ago

... in other hand - "Define your resource hierarchy"

<https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#define-hierarchy>

   upvoted 1 times

  **MaxNRG** 2 years, 3 months ago

So, I stay with BC :)))

   upvoted 3 times

  **hellofrnds** 2 years, 7 months ago

Answer:- C, D

C is used as best practice to create group and assign IAM roles



D "data from Cloud Storage buckets and BigQuery datasets must be shared for use in other projects in an ad hoc way" is mentioned in question. When 2 project communicate, service account should be used

   upvoted 9 times

  **sumanshu** 2 years, 10 months ago

Vote for B & C

   upvoted 4 times

  **daghayeghi** 3 years, 1 month ago

the question says adding permissions ad-hoc way

[c] is correct answer

[d] is right, as the access to bigQuery and cloud storage can be managed automatically by Cloud deployment

"Deployment Manager can also set access control permissions through IAM such that your developers are granted appropriate access as part of the project creation process."

ref: <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

   upvoted 3 times

🗨️ 👤 **VM_GCP** 3 years, 4 months ago

the question says adding permissions ad-hoc way

[c] is correct answer

[d] is right, as the access to bigQuery and cloud storage can be managed automatically by Cloud deployment

"Deployment Manager can also set access control permissions through IAM such that your developers are granted appropriate access as part of the project creation process."

ref: <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>

👍 ↩ 🚩 upvoted 4 times

🗨️ 👤 **sumanshu** 2 years, 10 months ago

D is a service account - it means we need to access via applications. So, D is ruled out

👍 ↩ 🚩 upvoted 4 times

🗨️ 👤 **sumanshu** 2 years, 10 months ago

Doubt, It could be 'D' - because - it's said - data from Cloud Storage buckets and BigQuery datasets must be shared for use in other projects in an ad hoc way.

👍 ↩ 🚩 upvoted 3 times

🗨️ 👤 **awssp12345** 2 years, 10 months ago

Agree with Sumanshu

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **ceak** 3 years, 5 months ago

C & E are the correct answers.

👍 ↩ 🚩 upvoted 3 times

🗨️ 👤 **sumanshu** 2 years, 10 months ago

E is a long process and we need to simply the process...So E is ruled out

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **vito9630** 3 years, 5 months ago

Answer: B, C

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **kavs** 3 years, 5 months ago

BC A ruled out as deployment manager is for infra yaml based deployments D at resource level we can't check hierarchy at org or Proj Level

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **rgpalop** 3 years, 7 months ago

C and E

👍 ↩ 🚩 upvoted 3 times

[Load full discussion...](#)



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



