← **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 144 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 144

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your company's new CEO recently sold two of the company's divisions. Your Director asks you to help migrate the Google Cloud projects associated with those divisions to a new organization node. Which preparation steps are necessary before this migration occurs? (Choose two.)

    A. Remove all project-level custom Identity and Access Management (IAM) roles.

    B. Disallow inheritance of organization policies.

    C. Identify inherited Identity and Access Management (IAM) roles on projects to be migrated.

    D. Create a new folder for all projects to be migrated.

    E. Remove the specific migration projects from any VPC Service Controls perimeters and bridges.

Show Suggested Answer

by 👤 **GHOST1985** at *Sept. 10, 2022, 4:31 p.m.*

Comments

Type your comment...

Submit

⊟ 👤 **Don10** [Highly Voted 👍] 2 years, 10 months ago

D. https://cloud.google.com/resource-manager/docs/project-migration#import_export_folders

E. https://cloud.google.com/resource-manager/docs/project-migration#vpcsc_security_perimeters

👍 ↩ ⚑ upvoted 11 times

⊟ 👤 **marmar11111** `Highly Voted 👍` 2 years, 8 months ago

https://cloud.google.com/resource-manager/docs/project-migration#plan_policy

When you migrate your project, it will no longer inherit the policies from its current place in the resource hierarchy, and will be subject to the effective policy evaluation at its destination. We recommend making sure that the effective policies at the project's destination match as much as possible the policies that the project had in its source location. https://cloud.google.com/resource-manager/docs/project-migration#import_export_folders

Policy inheritance can cause unintended effects when you are migrating a project, both in the source and destination organization resources. You can mitigate this risk by creating specific folders to hold only projects for export and import, and ensuring that the same policies are inherited by the folders in both organization resources. You can also set permissions on these folders that will be inherited to the projects moved within them, helping to accelerate the project migration process.

👍 ↩ ⚑ upvoted 7 times

⊟ 👤 **BPzen** `Most Recent ⊘` 8 months ago

IAM Role Inheritance:
Projects inherit IAM roles from the organization or folder they belong to. When a project is moved to a new organization, these inherited roles are lost.
Before migration, identify the inherited roles and reassign them explicitly at the project level if needed.

VPC Service Controls Limitation:
Projects in a VPC Service Controls perimeter or bridge cannot be moved between organizations. The perimeter must be updated to exclude the projects before migration.
After the migration, you can reconfigure the projects to include them in a new or existing perimeter within the new organization.

👍 ↩ ⚑ upvoted 1 times

⊟ 👤 **3574e4e** 8 months, 2 weeks ago

C:
Identity and Access Management policies and organization policies are inherited through the resource hierarchy, and can block a service from functioning if not set properly. Determine the effective policy at the project's destination in your resource hierarchy to ensure the policy aligns with your governance objectives. [https://cloud.google.com/resource-manager/docs/create-migration-plan#plan_policy]

E:
You cannot migrate a project that is protected by a VPC Service Controls security perimeter. [https://cloud.google.com/resource-manager/docs/handle-special-cases#vpcsc_security_perimeters]

D is recommended but not mandatort [https://cloud.google.com/resource-manager/docs/create-migration-plan#import_export_folders]

👍 ↩ ⚑ upvoted 2 times

⊟ 👤 **MoAk** 8 months ago

This is the way.

👍 ↩ ⚑ upvoted 1 times

⊟ 👤 **3d9563b** 1 year ago

To prepare for migrating Google Cloud projects to a new organization node, you should identify inherited IAM roles on the projects to understand permission implications and remove the projects from any VPC Service Controls perimeters to avoid access issues during migration. These steps help ensure a smooth transition and maintain access control and security throughout the process.

👍 ↩ ⚑ upvoted 1 times

⊟ 👤 **b6f53d8** 1 year, 6 months ago

C&E in my opinion

👍 ↩ ⚑ upvoted 2 times

⊟ 👤 **mjcts** 1 year, 6 months ago

All the steps are relevant in some scenarios, but the most important 2 are C and E

👍 ↩ 🚩 upvoted 3 times

☐ 👤 **Crotofroto** 1 year, 7 months ago

Selected Answer: CE

A. Removing all the project-level IAM will make you not know what permissions were there to be able to migrate them.
B. Disallowing inheritance of organization policies will affect other projects.
C. Identify inherited Identity and Access Management (IAM) roles on projects to be migrated. Correct, this will help you to migrate the IAM
D. You don't need a new folder to migrate the projects
E. Remove the specific migration projects from any VPC Service Controls perimeters and bridges. Correct, this is necessary because the project is no longer part of the organization.

👍 ↩ 🚩 upvoted 4 times

☐ 👤 **phd72** 1 year, 8 months ago

A, C

https://cloud.google.com/resource-manager/docs/handle-special-cases

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **Xoxoo** 1 year, 10 months ago

Selected Answer: CE

Before migrating Google Cloud projects associated with sold divisions to a new organization node, the following preparation steps are necessary:

C. Identify inherited Identity and Access Management (IAM) roles on projects to be migrated: You should identify any IAM roles that are inherited by the projects you plan to migrate. This is important because you want to ensure that you understand the existing access controls and permissions associated with these projects. Identifying inherited IAM roles allows you to plan how to manage permissions during and after the migration.

E. Remove the specific migration projects from any VPC Service Controls perimeters and bridges: If the projects you are migrating are currently part of any VPC Service Controls perimeters or bridges, you should remove them from these configurations. This ensures that the projects can be migrated without being restricted by VPC Service Controls, and it allows you to manage their access controls separately in the new organization node.

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **ananta93** 1 year, 10 months ago

Selected Answer: CE

The Answer is CE

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **desertlotus1211** 1 year, 10 months ago

https://cloud.google.com/resource-manager/docs/create-migration-plan

I think the answer can be BCD...
E is incorrect

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **ymkk** 1 year, 11 months ago

Selected Answer: CE

Because...
A) Custom project roles can be re-granted after migration.
B) Policy inheritance does not change after migration.
D) A new folder is not required before migration.

👍 ↩ 🚩 upvoted 3 times

☐ 👤 **Simon6666** 1 year, 11 months ago

Selected Answer: CD

CD is the ans

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **[Removed]** 2 years ago

Selected Answer: DE

D, E
D- Using import/export folders is recommended for mitigating policy risk.
E- You cannot migrate a project that's in a VPC Service Controls perimeter
References:
https://cloud.google.com/resource-manager/docs/create-migration-plan#import_export_folders
https://cloud.google.com/resource-manager/docs/handle-special-cases#vpcsc_security_perimeters

👍 ↩ 🚩 upvoted 3 times

gcpengineer 2 years, 2 months ago

Selected Answer: CE

CE is the ans

👍 ↩ ⚑ upvoted 4 times

xfall12 2 years, 2 months ago

A E
https://cloud.google.com/resource-manager/docs/handle-special-cases

👍 ↩ ⚑ upvoted 2 times

Load full discussion…