

[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 215 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 215

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You are a Cloud Identity administrator for your organization. In your Google Cloud environment, groups are used to manage user permissions. Each application team has a dedicated group. Your team is responsible for creating these groups and the application teams can manage the team members on their own through the Google Cloud console. You must ensure that the application teams can only add users from within your organization to their groups.

What should you do?

- A. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.
- B. Set an Identity and Access Management (IAM) policy that includes a condition that restricts group membership to user principals that belong to your organization.
- C. Define an Identity and Access Management (IAM) deny policy that denies the assignment of principals that are outside your organization to the groups in scope.
- D. Export the Cloud Identity logs to BigQuery. Configure an alert for external members added to groups. Have the alert trigger a Cloud Function instance that removes the external members from the group.

[Show Suggested Answer](#)

by [gcp4test](#) at Aug. 4, 2023, 3:06 p.m.

Comments

Type your comment...

Submit

  **Portugapt** Highly Voted  1 year, 6 months ago

Selected Answer: A

1) https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#google_groups

2) https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#forcing_access

Alternatively, you can grant access to a Google group that contains the relevant service accounts:

Create a Google group within the allowed domain.

Use the Google Workspace administrator panel to turn off domain restriction for that group.

Add the service account to the group.

Grant access to the Google group in the IAM policy.

3) <https://support.google.com/a/answer/167097>

You can granularly enforce this requirement on a group. No need for company wide.
This is also done in the Google Workspace Admin console.




My bet is on A.

   upvoted 6 times

  **Portugapt** 1 year, 6 months ago

Organization wide*

   upvoted 1 times

  **MoAk** Most Recent  8 months, 1 week ago

Selected Answer: A

The objective of the Q is asking you as the CI admin to ensure that project admins cannot add members from outside of your organisation. The fine grained control of said member can be controlled later via IAM. Again, the objective is for us to ensure we do not allow the project admins to do this and so this can only be achieved by Answer A.

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#google_groups

   upvoted 1 times

  **Sundar_Pichai** 11 months, 1 week ago

Selected Answer: A

I'll go with A,

Google IAM conditions allow you to set fine-grained access controls on resources. However, these conditions focus on:

Resource type

Request time

The identity making the request

The source IP address

The device or network conditions

In other words, It is not possible to directly write a Google IAM policy that restricts group membership to within the company domain. Google IAM policies are used to manage access to resources, but they do not control the membership of Google Groups.

   upvoted 1 times

  **3d9563b** 1 year ago

Selected Answer: A

By configuring the relevant groups in the Google Workspace Admin console to restrict membership to internal users, you implement a direct and preventive measure that aligns well with the requirement to manage permissions through groups securely.



   upvoted 1 times

  **winston9** 1 year, 5 months ago

Selected Answer: B

B is correct here

   upvoted 3 times

  **Xoxoo** 1 year, 10 months ago

Selected Answer: B

To ensure that application teams can only add users from within your organization to their groups, you should use option B:

B. Set an Identity and Access Management (IAM) policy that includes a condition that restricts group membership to user principals that belong to your organization.

Here's why option B is the recommended choice:

1) IAM Policy with Conditions: You can define an IAM policy for the groups that includes a condition specifying that only user principals belonging to your organization can be added as members. This condition enforces the requirement that only users within your organization can be added to the groups.

   upvoted 2 times



  **Xoxoo** 1 year, 10 months ago

Option A, which suggests changing the configuration in the Google Workspace Admin console, typically doesn't provide fine-grained control over group membership based on organization membership.

Option C is also not recommended because it defines an IAM deny policy that denies the assignment of principals outside your organization to the groups in scope. This approach can be complex and difficult to manage, especially if you have a large number of groups



Option D, "Export the Cloud Identity logs to BigQuery," and configuring an alert and Cloud Function to remove external members, is a more reactive approach and may not prevent external members from being added in the first place.

   upvoted 1 times

  **desertlotus1211** 1 year, 10 months ago

The question is not asking about Workspace Item. It's application teams need to add member to a group within the organization, not external. So how does this relate to Workspace?

   upvoted 2 times

  **ananta93** 1 year, 10 months ago

Selected Answer: A

Answer is A. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.

   upvoted 2 times

  **ArizonaClassics** 1 year, 10 months ago

The goal is to ensure that only users from within your organization can be added to specific Google Cloud groups managed by application teams. Here are some considerations for each option:

A. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.

If you are using Google Workspace (or Google Workspace for Education), you have the option to prevent external members from being added to a group directly through the Admin console. This is a straightforward way to enforce the policy and doesn't require extra monitoring or automation.

   upvoted 1 times

  **ArizonaClassics** 1 year, 11 months ago

The most direct and effective way to ensure that only users from within your organization can be added to the Google Cloud groups is:

A. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.

In Google Workspace Admin Console, you have the option to configure groups such that only users from within your organization can be added. This doesn't require you to rely on reactive measures like monitoring and alerts or to rely on IAM policies, which could be more complex to manage for this specific requirement. You can directly specify who can be a member of these groups by altering their settings in the Admin Console

   upvoted 1 times

  **GCBC** 1 year, 11 months ago

The correct answer is B. Set an Identity and Access Management (IAM) policy that includes a condition that restricts group membership to user principals that belong to your organization.

An IAM policy is a set of permissions that you can attach to a Google Cloud resource, such as a group. The policy defines

who can access the resource and what actions they can perform.

In this case, you can create an IAM policy that restricts group membership to user principals that belong to your organization. This will prevent the application teams from adding users from outside your organization to their groups.

This condition will restrict the policy to users who belong to your organization's domain.

Once you have created the policy, you can attach it to the groups that you want to protect. To do this, go to the Groups page in the Google Cloud console and select the groups that you want to protect. Then, click Edit and select the policy that you created.

👍 ↩ 🚩 upvoted 3 times

🗨️ 👤 **anshad666** 1 year, 11 months ago

Selected Answer: A

<https://support.google.com/a/answer/167097?hl=en&sjid=9952232817978914605-AP>

👍 ↩ 🚩 upvoted 3 times

🗨️ 👤 **Kush92me** 1 year, 11 months ago

A is correct, anyone who has access to google admin portal can check.

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **cyberpunk21** 1 year, 11 months ago

Selected Answer: A

A is correct

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **cyberpunk21** 1 year, 11 months ago

Selected Answer: C

C is correct

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **anshad666** 1 year, 11 months ago

Selected Answer: C

<https://support.google.com/a/answer/167097?hl=en&sjid=9952232817978914605-AP>

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **anshad666** 1 year, 11 months ago

There is a typo, it should A

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **gcp4test** 1 year, 11 months ago

Selected Answer: A

A - group can be configured to prevent adding external members.

👍 ↩ 🚩 upvoted 2 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



