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 129 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 129

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You are a security administrator at your company. Per Google-recommended best practices, you implemented the domain restricted sharing organization policy to allow only required domains to access your projects. An engineering team is now reporting that users at an external partner outside your organization domain cannot be granted access to the resources in a project. How should you make an exception for your partner's domain while following the stated best practices?

A. Turn off the domain restriction sharing organization policy. Set the policy value to "Allow All."

B. Turn off the domain restricted sharing organization policy. Provide the external partners with the required permissions using Google's Identity and Access Management (IAM) service.

C. Turn off the domain restricted sharing organization policy. Add each partner's Google Workspace customer ID to a Google group, add the Google group as an exception under the organization policy, and then turn the policy back on.

D. Turn off the domain restricted sharing organization policy. Set the policy value to "Custom." Add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy, and then turn the policy back on.

Show Suggested Answer

by bartlomiejwaw at *May 10, 2022, 9:53 p.m.*

Comments

Type your comment...

Submit

mikesp Highly Voted 3 years, 1 month ago

Selected Answer: D

The question is that is necessary to add identities from another Domain to cloud identity. The only way to do that is by adding the Customer Ids as exception. The procedure does not support adding groups, etc...
The groups and the corresponding users can be added later on with Cloud Identity once that the domain of their organization is allowed:
The allowed_values are Google Workspace customer IDs, such as C03xgje4y. Only identities belonging to a Google Workspace domain from the list of allowed_values will be allowed on IAM policies once this organization policy has been applied. Google Workspace human users and groups must be part of that Google Workspace domain, and IAM service accounts must be children of an organization resource associated with the given Google Workspace domain

upvoted 13 times

AzureDP900 2 years, 8 months ago

Agreed with your explanaiton

upvoted 1 times

bartlomiejwaw Highly Voted 3 years, 2 months ago

Selected Answer: C

Policy should be turned on at the end. Adding the whole group as an exception is far more reasonable than adding all identities.

upvoted 5 times

mT3 3 years, 2 months ago

I agree
Ref: https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy

upvoted 1 times

adriannieto 2 years, 5 months ago

Agree, it should be C

upvoted 1 times

gcpengineer 2 years, 2 months ago

u can not add customer ID to a google group

upvoted 1 times

adriannieto 2 years, 5 months ago

To add more context here's the forcing access doc.
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#forcing_access

upvoted 1 times

fad3r 2 years, 4 months ago

If you actually follow this link this is discussing service accounts.

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.

This does not mention service accounts. It just as easily be users or other resources.

upvoted 1 times

BPzen Most Recent 8 months ago

Selected Answer: D

Why D is Correct:
Custom Exceptions for Partner Domains:

By setting the policy to "Custom," you can explicitly list the external partner's Cloud Identity or Google Workspace customer ID as an exception.
This allows resources to be shared with the specified external domain while maintaining domain restriction for all other domains

domains.
Enforcing Best Practices:

Turning the policy back on ensures that the domain restricted sharing remains enforced across your organization.
Granular Control:

Using customer IDs ensures that only the intended partner domain is granted access. This approach avoids unnecessary exposure to other domains.

upvoted 1 times

Xoxoo 1 year, 10 months ago

Selected Answer: D

To make an exception for your partner's domain while following the stated best practices, you can add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy. To do this, you need to turn off the domain restricted sharing organization policy and set the policy value to "Custom" . You can then add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy and turn the policy back on .

Alternatively, you can add each partner's Google Workspace customer ID to a Google group, add the Google group as an exception under the organization policy, and then turn the policy back on . This approach is useful when you have multiple external partners that need access to your resources .

upvoted 3 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: D

D. Turn off the domain restricted sharing organization policy. Set the policy value to "Custom." Add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy, and then turn the policy back on.

upvoted 2 times

zellck 2 years, 10 months ago

Selected Answer: D

D is the answer.

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy
The domain restriction constraint is a type of list constraint. Google Workspace customer IDs can be added and removed from the allowed_values list of a domain restriction constraint. The domain restriction constraint does not support denying values, and an organization policy can't be saved with IDs in the denied_values list.

All domains associated with a Google Workspace account listed in the allowed_values will be allowed by the organization policy. All other domains will be denied by the organization policy.

upvoted 3 times

AzureDP900 2 years, 8 months ago

Thank you for detailed explanation

upvoted 1 times

sumundada 3 years ago

Selected Answer: D

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

upvoted 3 times

Medofree 3 years, 2 months ago

The right answer is D.

Because we add the "Customer ID" as exception and not Google group.

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

upvoted 1 times

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses