Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 304 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 304

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You are managing a Google Cloud environment that is organized into folders that represent different teams. These teams need the flexibility to modify organization policies relevant to their work. You want to grant the teams the necessary permissions while upholding Google-recommended security practices and minimizing administrative complexity. What should you do?

A. Create a custom IAM role with the organization policy administrator permission and grant the permission to each team’s folder. Limit policy modifications based on folder names within the custom role’s definition.

B. Assign the organization policy administrator role to a central service account and provide teams with the credentials to use the service account when needed.

C. Create an organization-level tag. Attach the tag to relevant folders. Use an IAM condition to restrict the organization policy administrator role to resources with that tag.

D. Grant each team the organization policy administrator role at the organization level.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 10:06 p.m.*

Comments

Type your comment...

Submit

lendly 1 month, 3 weeks ago

Selected Answer: A

Key Requirements:

Teams need flexibility to modify policies relevant only to their work.

Must align with Google-recommended security practices (principle of least privilege).

Minimize administrative complexity.

Why A is Correct:

Custom Role: By creating a custom IAM role with specific permissions, you ensure teams can only manage policies relevant to their folder.

Granular Access: Granting the custom role to each team's folder ensures they only have permissions for policies within their scope of responsibility.

Minimized Risk: This approach avoids over-permissioning and prevents accidental or malicious policy changes at the organization level.

Alignment with Best Practices: Adheres to the principle of least privilege and ensures resource-level isolation.

upvoted 1 times

1209apl 3 months ago

Selected Answer: C

Answer is C.
The only inputs accepted while defining a new custom role are: Title, Description, ID, Role launch stage & permissions. Any other option like "Limit policy modifications based on folder names" is non-existing within the custom role’s definition as Option A states.

https://cloud.google.com/iam/docs/creating-custom-roles#creating

upvoted 2 times

1209apl 3 months, 1 week ago

Selected Answer: A

Answer is C.
The only inputs accepted while defining a new custom role are: Title, Description, ID, Role launch stage & permissions. Any other option like "Limit policy modifications based on folder names" is non-existing within the custom role’s definition as Option A states.

https://cloud.google.com/iam/docs/creating-custom-roles#creating

upvoted 1 times

p981pa123 6 months, 1 week ago

Selected Answer: A

Tags in Google Cloud are primarily designed for organizing and categorizing resources.While it's possible to create IAM conditions that reference tags (e.g., limiting the use of a role to resources with specific tags), this method is not the most intuitive or straightforward way to manage IAM policies, especially when the main goal is to provide flexible policy management for different teams.
In your case, folder-based isolation with custom IAM roles is a cleaner and more intuitive way to achieve team-level control over organization policies

upvoted 1 times

json4u 9 months, 2 weeks ago

Selected Answer: C

It's C.

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

C - Granular Control: Creating an organization-level tag allows you to precisely control which teams have access to modify organization policies by attaching the tag to relevant folders. This ensures that only authorized teams can make changes.
IAM Condition: Using an IAM condition to restrict the organization policy administrator role to resources with the tag provides a flexible and efficient way to grant permissions while maintaining control. This ensures that the role is only accessible for the intended teams.
Security Best Practices: This approach aligns with Google-recommended security practices by limiting access to organization policies to authorized teams and using IAM conditions to enforce appropriate controls.
Administrative Efficiency: This approach simplifies administration by providing a centralized mechanism for managing permissions and ensuring that only authorized teams can modify organization policies.

upvoted 2 times