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 172 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 172

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You're developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two main requirements:

✑ Least-privilege access must be enforced at all times.

✑ The DevOps team must be able to access the required resources only during the deployment issue.

How should you grant access while following Google-recommended best practices?

A. Assign the Project Viewer Identity and Access Management (IAM) role to the DevOps team.

B. Create a custom IAM role with limited list/view permissions, and assign it to the DevOps team.

C. Create a service account, and grant it the Project Owner IAM role. Give the Service Account User Role on this service account to the DevOps team.

D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

Show Suggested Answer

by Baburao at *Sept. 3, 2022, 7:10 p.m.*

Comments

Type your comment...

Submit

Baburao Highly Voted 2 years, 10 months ago

I think the answer should D. Option B gives them "Always On" permissions but the question asks for "Just in time" permissions. So, this is possible only with a Service Account. Once the incident response team resolves the issue, the service account key can be disabled.

upvoted 18 times

> **pfilourenco** 1 year, 12 months ago
>
> You can create "Just in time" permissions with IAM conditions.
>
> upvoted 7 times

Mauratay Most Recent 5 months ago

Selected Answer: B

It follows best practices and has traceability

upvoted 1 times

KLei 7 months ago

Selected Answer: D

IAM role to DevOps team member is wrong - not fulfill least privilege principle
Service account with "limited list/view permissions" to DevOps team member is correct
- least privilege principle
- more flexibility

upvoted 2 times

Pime13 7 months, 2 weeks ago

Selected Answer: B

i vote B.
Options A and C grant broader permissions than necessary, which does not align with the least-privilege principle. Option D involves using a service account, which is not the best practice for granting temporary access to human users.
By creating a custom IAM role, you ensure that the DevOps team has the precise permissions needed for their tasks, and you can easily adjust or revoke these permissions as necessary

upvoted 2 times

BPzen 8 months ago

Selected Answer: D

Why Option D is Best:
Least-Privilege Access:
Permissions are limited to only what is necessary for the investigation by tailoring the service account's IAM role.
Controlled Access:
By managing the service account or its impersonation permissions, you can ensure the DevOps team can access the resources only during deployment issues.

upvoted 1 times

Mr_MIXER007 11 months ago

Selected Answer: D

D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

This option allows you to create a service account with limited access rights (list/view), and the DevOps team will be able to use this service account only when needed. This is consistent with the principle of least privilege and incident-only access.

upvoted 1 times

Mr_MIXER007 11 months ago

Selected Answer: D

D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

This option allows you to create a service account with limited access rights (list/view), and the DevOps team will be able to use this service account only when needed. This is consistent with the principle of least privilege and incident-only access.

upvoted 1 times

jujanoso 1 year ago

Selected Answer: D

D. This approach allows the creation of a service account with specific limited permissions necessary for investigating deployment issues. The DevOps team can then be granted the Service Account User role on this service account. This setup ensures that the DevOps team can use the service account with appropriate permissions only when needed, fulfilling both ensures that the DevOps team can use the service account with appropriate permissions only when needed, fulfilling both requirements of least-privilege access and temporary access

upvoted 1 times

shanwford 1 year, 3 months ago

Selected Answer: D

Its (D) according https://cloud.google.com/iam/docs/best-practices-service-accounts "Some applications only require access to certain resources at specific times or under specific circumstances....In such scenarios, using a single service account and granting it access to all resources goes against the principle of least privilege"

upvoted 2 times

Bettoxicity 1 year, 3 months ago

Selected Answer: D

D.

-Least Privilege: By creating a service account with restricted permissions (limited list/view access to specific resources), you adhere to the principle of least privilege. The DevOps team can only access the information needed for investigation without broader project-level control.
-Temporary Access: Service accounts are not tied to individual users. Once the investigation is complete, you can simply revoke access to the service account from the DevOps team, effectively removing their access to the resources. This ensures temporary access for the specific incident.

upvoted 1 times

glb2 1 year, 4 months ago

Selected Answer: B

Answer is B, it sets least-privilege access.

upvoted 2 times

dija123 1 year, 4 months ago

Selected Answer: D

Any DevOps Engineer knows verywell, it is D

upvoted 1 times

Nachtwaker 1 year, 4 months ago

Selected Answer: B

B or D, I prefer B because of traceability, impersonating an account is harder to audit in relation to using personal account.

upvoted 3 times

dija123 1 year, 4 months ago

Selected Answer: D

I go with D,
While B seems to allows defining specific permissions, it adds complexity to the access control strategy and might still grant more access than necessary.

upvoted 1 times

JoaquinJimenezGarcia 1 year, 7 months ago

Selected Answer: B

B follows the google best practices

upvoted 3 times

rglearn 1 year, 10 months ago

Selected Answer: B

Answer should be B

upvoted 2 times

desertlotus1211 1 year, 10 months ago

The real answer shouldn be 'breakglass' tool.

upvoted 2 times

Load full discussion...

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses