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 205 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 205

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You are running applications outside Google Cloud that need access to Google Cloud resources. You are using workload identity federation to grant external identities Identity and Access Management (IAM) roles to eliminate the maintenance and security burden associated with service account keys. You must protect against attempts to spoof another user's identity and gain unauthorized access to Google Cloud resources.

What should you do? (Choose two.)

A. Enable data access logs for IAM APIs.

B. Limit the number of external identities that can impersonate a service account.

C. Use a dedicated project to manage workload identity pools and providers.

D. Use immutable attributes in attribute mappings.

E. Limit the resources that a service account can access.

Show Suggested Answer

by pfilourenco at *Aug. 4, 2023, 9:20 a.m.*

## Comments

Type your comment...

Submit

**Xoxoo** Highly Voted 1 year, 4 months ago

Selected Answer: CD

Best practices for protecting against spoofing threats:

Use a dedicated project to manage workload identity pools and providers.
Use organizational policy constraints to disable the creation of workload identity pool providers in other projects.
Use a single provider per workload identity pool to avoid subject collisions.
Avoid federating with the same identity provider twice.
Protect the OIDC metadata endpoint of your identity provider.
Use the URL of the workload identity pool provider as audience.
Use immutable attributes in attribute mappings.
Use non-reusable attributes in attribute mappings.
Don't allow attribute mappings to be modified.
Don't rely on attributes that aren't stable or authoritative.

Therefore, Option C and D are correct

upvoted 7 times

> **Nachtwaker** 10 months, 3 weeks ago
>
> Agree, See https://cloud.google.com/iam/docs/best-practices-for-using-workload-identity-federation#protecting_against_spoofing_threats
>
> Because CD is in the list and E is not, preferred CD
>
> upvoted 1 times

**desertlotus1211** Most Recent 11 months, 4 weeks ago

D,E is correct
Immutable attributes in the attribute mappings ensure that the identity information provided by the external identity provider cannot be easily altered. T

By applying the principle of least privilege, limiting the resources a service account can access ensures that even if an external identity is compromised or misconfigured, the potential impact is minimized.

upvoted 2 times

**cyberpunk21** 1 year, 5 months ago

Selected Answer: CD

CD looks good to me

upvoted 1 times

**anshad666** 1 year, 5 months ago

Selected Answer: CD

https://cloud.google.com/iam/docs/best-practices-for-using-workload-identity-federation#protecting_against_spoofing_threats

upvoted 1 times

**alkaloid** 1 year, 5 months ago

Selected Answer: CD

https://cloud.google.com/iam/docs/best-practices-for-using-workload-identity-federation

upvoted 1 times

**pfilourenco** 1 year, 5 months ago

Selected Answer: CD

C & D - https://cloud.google.com/iam/docs/best-practices-for-using-workload-identity-federation#protecting_against_spoofing_threats

upvoted 2 times

EXAMTOPICS

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses