

🔗 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 254 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 254

Topic #: 1

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

Your organization has applications that run in multiple clouds. The applications require access to a Google Cloud resource running in your project. You must use short-lived access credentials to maintain security across the clouds. What should you do?

- A. Create a managed workload identity. Bind an attested identity to the Compute Engine workload.
- B. Create a service account key. Download the key to each application that requires access to the Google Cloud resource.
- C. Create a workload identity pool with a workload identity provider for each external cloud. Set up a service account and add an IAM binding for impersonation.
- D. Create a VPC firewall rule for ingress traffic with an allowlist of the IP ranges of the external cloud applications.

[Show Suggested Answer](#)

by [yokoyan](#) at Sept. 6, 2024, 1:23 a.m.

Comments

Type your comment...



[Submit](#)

👤 [assassin1subzero](#) 4 days, 10 hours ago

Selected Answer: C

Short lived credentials C

   upvoted 1 times

  **Pime13** 7 months, 3 weeks ago

Selected Answer: C



Why Option C:

Short-Lived Credentials: Workload Identity Federation allows you to use short-lived credentials, which are more secure than long-lived service account keys.

Cross-Cloud Compatibility: By creating a workload identity pool and providers for each external cloud, you can securely authenticate and authorize applications running in different cloud environments.

IAM Binding for Impersonation: This setup allows you to grant specific permissions to the service account, ensuring that only authorized actions are performed.

   upvoted 1 times

  **BPzen** 8 months ago

Selected Answer: C

For applications running in multiple clouds that need access to Google Cloud resources, the Workload Identity Federation feature is the most secure and scalable solution. It allows you to grant external workloads access to Google Cloud resources using short-lived credentials, eliminating the need to manage long-lived service account keys.

Workload Identity Pool:

Create a pool to represent identities from external clouds.

Workload Identity Provider:

Set up a provider for each external cloud to validate identities from those environments.

Short-Lived Credentials:



Use Google's Security Token Service (STS) to exchange tokens from external identity providers for short-lived Google Cloud credentials.

Service Account Impersonation:

Set up a Google Cloud service account with the required permissions.

Add an IAM binding to allow the external identity to impersonate the service account.

   upvoted 1 times

  **koo_kai** 9 months, 2 weeks ago

Selected Answer: C

It's C

   upvoted 2 times

  **1e22522** 10 months, 3 weeks ago

Selected Answer: C

It's C

   upvoted 2 times

  **SQLbox** 10 months, 3 weeks ago

C is the correct answer

   upvoted 2 times

  **ABotha** 10 months, 3 weeks ago

Correct Answer: C

Short-lived access credentials: Workload Identity Federation (WIF) allows you to issue short-lived access tokens to external applications, reducing the risk of credential theft and misuse.

Multiple clouds: You can create a workload identity pool for each external cloud, allowing applications from different environments to access your Google Cloud resources securely.

Centralized management: WIF provides a centralized way to manage access to your Google Cloud resources, simplifying administration and improving security.

Impersonation: By setting up a service account and adding an IAM binding for impersonation, you can allow external applications to act as the service account, granting them the necessary permissions to access your Google Cloud resources.

   upvoted 4 times

  **yokoyan** 10 months, 3 weeks ago

Selected Answer: A

I think it's A.

   upvoted 1 times

  **yokoyan** 8 months, 1 week ago

After reading ABotha's comment, I'm starting to think that C is correct.

   upvoted 2 times



Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

