

🔗 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 222 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 222

Topic #: 1

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

Your company recently published a security policy to minimize the usage of service account keys. On-premises Windows-based applications are interacting with Google Cloud APIs. You need to implement Workload Identity Federation (WIF) with your identity provider on-premises.

What should you do?

- A. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS). Configure a rule to let principals in the pool impersonate the Google Cloud service account.
- B. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS). Let all principals in the pool impersonate the Google Cloud service account.
- C. Set up a workload identity pool with an OpenID Connect (OIDC) service on the same machine. Configure a rule to let principals in the pool impersonate the Google Cloud service account.
- D. Set up a workload identity pool with an OpenID Connect (OIDC) service on the same machine. Let all principals in the pool impersonate the Google Cloud service account.

[Show Suggested Answer](#)

by [Mithung30](#) at Aug. 4, 2023, 1:20 p.m.

Comments

Type your comment...

Submit

🗄️ 👤 **Mithung30** Highly Voted 11 months, 4 weeks ago

A. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS). Configure a rule to let principals in the pool impersonate the Google Cloud service account. This is the best option because it allows you to control who can impersonate the Google Cloud service account.

👍 ↩️ 🚩 upvoted 5 times

🗄️ 👤 **MMNB2023** Most Recent 8 months, 1 week ago

Selected Answer: A

The right answer including least privilege principle

👍 ↩️ 🚩 upvoted 3 times

🗄️ 👤 **Xoxoo** 10 months, 1 week ago

Selected Answer: A

Here's why option A is the preferred choice:

Workload Identity Pool: Using your corporate ADFS for identity federation is a common and secure way to manage identities and access to Google Cloud resources.

Configure a Rule: Configuring a rule in the workload identity pool allows you to specify which principals (users or entities) in your corporate ADFS can impersonate the Google Cloud service account. This approach adheres to the principle of least privilege by allowing only specific users or entities to impersonate the service account.

👍 ↩️ 🚩 upvoted 3 times

🗄️ 👤 **cyberpunk21** 11 months, 1 week ago

Selected Answer: A

A is correct, B is also correct, but it causes chaos.

👍 ↩️ 🚩 upvoted 3 times

🗄️ 👤 **akg001** 11 months, 3 weeks ago

Selected Answer: A

A is correct

👍 ↩️ 🚩 upvoted 4 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses

