



- Expert Verified, Online, **Free**.

MENU



Google Discussions



Exam Associate Cloud Engineer All Questions

View all questions & answers for the Associate Cloud Engineer exam

[Go to Exam](#)

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 152 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 152

Topic #: 1

[\[All Associate Cloud Engineer Questions\]](#)

Your company runs its Linux workloads on Compute Engine instances. Your company will be working with a new operations partner that does not use Google Accounts. You need to grant access to the instances to your operations partner so they can maintain the installed tooling. What should you do?

- A. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.
- B. Tag all the instances with the same network tag. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag.
- C. Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.
- D. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.







[Show Suggested Answer](#)







by [francisco_guerra](#) at Aug. 13, 2020, 2:54 a.m.






Comments

Type your comment...

[Submit](#)

  **kulikBro** Highly Voted  3 years, 6 months ago
A - <https://cloud.google.com/iap/docs/external-identities>
   upvoted 34 times

  **Bhagirathi** Highly Voted  3 years, 11 months ago
full of confusions for any reader....
You guys all say A, B, C & D but which one is correct ?
   upvoted 23 times

  **yc25744** 3 years, 3 months ago
nothing
   upvoted 7 times

  **sivakarthick16** Most Recent  1 week, 4 days ago

Selected Answer: D

A is incorrect because the operations partner does not have a Google account. Activating and enabling Cloud IAP (Identity-Aware Proxy) for the Compute Engine instances would only allow access to users with Google Accounts. In this case, the third-party service provider does not use Google Accounts, so this option would not enable their access.

   upvoted 1 times

  **denno22** 1 week, 4 days ago

Selected Answer: A

IAP controls access to your applications and resources. It leverages user identity and the context of a request to determine if a user should be allowed access. IAP is a building block toward BeyondCorp, an enterprise security model that enables employees to work from untrusted networks without using a VPN.

By default, IAP uses Google identities and IAM. By leveraging Identity Platform instead, you can authenticate users with a wide range of external identity providers, such as:

Email/password
OAuth (Google, Facebook, Twitter, GitHub, Microsoft, etc.)
SAML
OIDC
Phone number
Custom
Anonymous

This is useful if your application is already using an external authentication system, and migrating your users to Google accounts is impractical.

   upvoted 1 times

  **kurayish** 1 month ago

Selected Answer: D

Cloud IAP requires users to authenticate with a Google Account, which the operations partner does not use.

So D,

SSH key authentication is a standard and secure method for granting access to Linux systems. This avoids the need for creating Google Accounts and provides direct access to the instances.

   upvoted 1 times

  **Timfdklfajlksdjlakf** 1 month, 3 weeks ago

Selected Answer: D

Using SSH keys is an effective and secure way to provide access to your instances without requiring Google Accounts, aligning with the needs of your new operations partner.

   upvoted 1 times

  **Namik** 2 months ago

Selected Answer: D

D. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

Explanation:

Direct SSH access: This method provides direct SSH access to the instances, allowing the operations partner to manage the installed tooling efficiently.

No Google account required: The operations partner doesn't need a Google account, as SSH keys are the authentication mechanism.

Security: While you'll need to manage SSH keys carefully, this method offers a secure way to grant access to specific users.

Why not other options:

- A. Enable Cloud IAP: Cloud IAP is primarily for web applications, not SSH access.
- B. Firewall rule: While this could technically work, it's less secure than SSH keys and more complex to manage.
- C. Cloud VPN: Setting up a VPN is overkill for this scenario and introduces additional complexity.

By choosing option D, you provide the operations partner with the necessary access while maintaining security.

? ? ? upvoted 2 times

? ? **SureNot** 3 months, 1 week ago

Selected Answer: D

If you go with answer A, explain please what credentials will be used to authentication?

? ? ? upvoted 1 times

? ? **ccpmad** 5 months ago

Selected Answer: D

"new operations partner that does not use Google Accounts."

All answering A, but the question does not say that the new partner is going to use Google Accounts now. So it is D. Is not a good idea to enter with ssh key pairs, but there is not other option if the new partner has to enter vms and does not have Google accounts.

? ? ? upvoted 1 times

? ? **thewalker** 11 months ago

Selected Answer: A

A is clean: https://cloud.google.com/iap/docs/concepts-overview#when_to_use_iap

? ? ? upvoted 2 times

? ? **Captain1212** 1 year, 1 month ago

Selected Answer: A

A seems more correct, as to provide the access

? ? ? upvoted 1 times

? ? **Praxii** 1 year, 5 months ago

Selected Answer: A

Answer is A. Although to enable IAP, you do need to create a firewall rule on tcp 22. But if this question wasn't multiple choice then A is correct.

"IAP is a building block toward BeyondCorp, an enterprise security model that enables employees to work from untrusted networks without using a VPN." - So C is not required when A can suffice.

? ? ? upvoted 1 times

? ? **innoculous_chris** 1 year, 6 months ago

Selected Answer: C

<https://cloud.google.com/iap/docs/concepts-overview>

IAP is only for google accounts and applies to access to AppEngine, HTTP(s) LB. It explicitly doesn't protect VMs.

? ? ? upvoted 1 times

? ? **ccpmad** 5 months ago

ok, if it is C, then the partner is in the same internal network, How can they enter the linux vms? they need ssh access....

? ? ? upvoted 1 times

? ? **innoculous_chris** 1 year, 6 months ago

please ignore...Answer should be A..<https://cloud.google.com/iap/docs/external-identities>..this page shows it works for VMs and non-google accounts.

? ? ? upvoted 5 times

? ? **ccpmad** 5 months ago

Ignore you, A is not possible, because the question does not say since now the partner will use google accounts....

? ? ? upvoted 1 times

? ? **krishna37** 1 year, 10 months ago

Selected Answer: A

Please watch this video.

<https://www.youtube.com/watch?v=jZdXyWQuIW0>

? ? ? upvoted 4 times

? ? **[Removed]** 1 year, 10 months ago

R is the straight forward answer to allow the partner to access via SSH without a Google account. For those suggesting A

B is the straight forward answer to allow the partner to access via OAuth without a Google account. For those suggesting A, carefully read <https://cloud.google.com/iap/docs/external-identities> and you'll notice that external identity isn't available from IAP out of the box and requires Identity Platform.

? ? ? upvoted 2 times

? ? **Pr44** 1 year, 11 months ago

Selected Answer: A

Question ask about granting access to new operations partner and that can be done by first option only.

? ? ? upvoted 1 times

? ? **Charumathi** 2 years ago

Selected Answer: A

A is the correct answer,

IAP controls access to your App Engine apps and Compute Engine VMs running on Google Cloud. It leverages user identity and the context of a request to determine if a user should be allowed access. IAP is a building block toward BeyondCorp, an enterprise security model that enables employees to work from untrusted networks without using a VPN.

By default, IAP uses Google identities and IAM. By leveraging Identity Platform instead, you can authenticate users with a wide range of external identity providers, such as:

Email/password

OAuth (Google, Facebook, Twitter, GitHub, Microsoft, etc.)

SAML

OIDC

Phone number

Custom

Anonymous

This is useful if your application is already using an external authentication system, and migrating your users to Google accounts is impractical.

? ? ? upvoted 7 times

[Load full discussion...](#)

Start Learning for free



Social Media

[Facebook](#) , [Twitter](#)

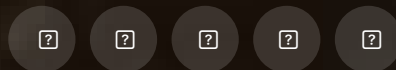
[YouTube](#) , [Reddit](#)

[Pinterest](#)



We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.



© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics

Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial

Analyst® are registered trademarks owned by CFA Institute.