

🔗 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 122 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 122

Topic #: 1

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

Your organization acquired a new workload. The Web and Application (App) servers will be running on Compute Engine in a newly created custom VPC. You are responsible for configuring a secure network communication solution that meets the following requirements:

- ⇒ Only allows communication between the Web and App tiers.
- ⇒ Enforces consistent network security when autoscaling the Web and App tiers.
- ⇒ Prevents Compute Engine Instance Admins from altering network traffic.

What should you do?

- A. 1. Configure all running Web and App servers with respective network tags. 2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.
- B. 1. Configure all running Web and App servers with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.
- C. 1. Re-deploy the Web and App servers with instance templates configured with respective network tags. 2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.
- D. 1. Re-deploy the Web and App servers with instance templates configured with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

[Show Suggested Answer](#)

by KillerGoogle at May 11, 2022, 3:54 a.m.

Comments

Type your comment...

Submit

  **KillerGoogle** Highly Voted  3 years, 2 months ago

D <https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags>


   upvoted 15 times

  **csrazdan** Highly Voted  2 years, 8 months ago

Selected Answer: D

The requirement can be fulfilled by both network tags and service accounts. To update both compute instances will have to be stopped. That means options A and B are out. Option C is out because Compute Engine Instance Admins can change network tags and avoid firewall rules. Deployment has to be done based on the instance template so that no configuration can be changed to divert the traffic.

   upvoted 8 times

  **Sundar_Pichai** Most Recent  11 months ago

Selected Answer: D

It's D because of its use of auto-scaling. If autoscaling wasn't part of the question, then B would have been suitable.

It can't be network level tags because admins can change those.

   upvoted 2 times

  **Ric350** 2 years, 4 months ago

Can you create an instance template with a service account? How do you automate that and how does it name the service accounts for each new instance??

   upvoted 1 times

  **TNT87** 2 years, 4 months ago

You can set up a new instance to run as a service account through the Google Cloud console, the Google Cloud CLI, or directly through the API. Go to the Create an instance page. Specify the VM details. In the Identity and API access section, choose the service account you want to use from the drop-down list.

<https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances>

   upvoted 2 times




  **AzureDP900** 2 years, 8 months ago

D is right

   upvoted 1 times

  **risc** 2 years, 9 months ago

This depends on what is meant by "re-deploy"? Service accounts can also be changed by simply stopping the VM and starting it again once the SA was changed. Is this already a re-deploy?

   upvoted 3 times

  **AwesomeGCP** 2 years, 9 months ago

Selected Answer: D

D. 1. Re-deploy the Web and App servers with instance templates configured with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

   upvoted 1 times

  **zelck** 2 years, 10 months ago

Selected Answer: D

D is the answer.

<https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags>

A service account represents an identity associated with an instance. Only one service account can be associated with an instance. You control access to the service account by controlling the grant of the Service Account User role for other IAM principals. For an IAM principal to start an instance by using a service account, that principal must have the Service Account User role to at least use that service account and appropriate permissions to create instances (for example, having the Compute Engine Instance Admin role to the project).

   upvoted 2 times

  **cloudprincipal** 3 years, 1 month ago

Selected Answer: D

Agreed, it has to be D
<https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags>
👍 ↩ 🚩 upvoted 2 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



© 2024 ExamTopics