

[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 300 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 300

Topic #: 1

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

You work for an ecommerce company that stores sensitive customer data across multiple Google Cloud regions. The development team has built a new 3-tier application to process orders and must integrate the application into the production environment.

You must design the network architecture to ensure strong security boundaries and isolation for the new application, facilitate secure remote maintenance by authorized third-party vendors, and follow the principle of least privilege. What should you do?

- A. Create separate VPC networks for each tier. Use VPC peering between application tiers and other required VPCs. Provide vendors with SSH keys and root access only to the instances within the VPC for maintenance purposes.
- B. Create a single VPC network and create different subnets for each tier. Create a new Google project specifically for the third-party vendors and grant the network admin role to the vendors. Deploy a VPN appliance and rely on the vendors' configurations to secure third-party access.
- C. Create separate VPC networks for each tier. Use VPC peering between application tiers and other required VPCs. Enable Identity-Aware Proxy (IAP) for remote access to management resources, limiting access to authorized vendors.
- D. Create a single VPC network and create different subnets for each tier. Create a new Google project specifically for the third-party vendors. Grant the vendors ownership of that project and the ability to modify the Shared VPC configuration.

[Show Suggested Answer](#)

by [abdelrahman89](#) at Oct. 4, 2024, 9:55 p.m.

Comments

Type your comment...

[Submit](#)

  **Pime13** 7 months, 3 weeks ago

Selected Answer: C

This approach ensures that each tier of the application is isolated within its own VPC, enhancing security. VPC peering allows necessary communication between tiers while maintaining isolation. Using Identity-Aware Proxy (IAP) for remote access ensures that only authorized vendors can access management resources, adhering to the principle of least privilege.



   upvoted 1 times

  **json4u** 9 months, 2 weeks ago

Selected Answer: C

It's C.

   upvoted 1 times

  **abdelrahman89** 9 months, 3 weeks ago

C - Separate VPCs: Creating separate VPC networks for each tier provides a strong isolation boundary, reducing the risk of unauthorized access or lateral movement.

VPC Peering: Using VPC peering between application tiers and other required VPCs allows for secure communication while maintaining isolation.

Identity-Aware Proxy (IAP): Enabling IAP for remote access to management resources provides a secure and controlled way for authorized vendors to access the application. IAP requires authentication and authorization, ensuring that only authorized individuals can access the resources.

Least Privilege: This approach adheres to the principle of least privilege by granting vendors only the necessary access to perform their maintenance tasks.

   upvoted 2 times

EXAMTOPICS

Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)



© 2024 ExamTopics