



PROFESSIONAL-CLOUD-SECURITY-ENGINEER^{Q&As}

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/professional-cloud-security-engineer.html>

100% Passing Guarantee
100% Money Back Assurance





Following Questions and Answers are all new published by Google
Official Exam Center



VCE & PDF

PassApply.com

<https://www.passapply.com/professional-cloud-security-engineer.html>
2024 Latest passapply PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF
and VCE dumps Download

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

- A. Use Cloud Storage as a federated Data Source.
- B. Use a Cloud Hardware Security Module (Cloud HSM).
- C. Customer-managed encryption keys (CMEK).
- D. Customer-supplied encryption keys (CSEK).

Correct Answer: C

If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys, use Cloud Key Management Service to manage your keys. This scenario is known as customer-managed encryption keys (CMEK). <https://cloud.google.com/bigquery/docs/encryption-at-rest>

Reference: <https://cloud.google.com/bigquery/docs/encryption-at-rest>

QUESTION 2

Your organization hosts a financial services application running on Compute Engine instances for a third-party company. The third-party company's servers that will consume the application also run on Compute Engine in a separate Google

Cloud organization. You need to configure a secure network connection between the Compute Engine instances.

You have the following requirements:

1.
The network connection must be encrypted.
 2.
The communication between servers must be over private IP addresses. What should you do?
- A. Configure a Cloud VPN connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
 - B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
 - C. Configure a VPC Service Controls perimeter around your Compute Engine instances, and provide access to the third party via an access level.
 - D. Configure an Apigee proxy that exposes your Compute Engine-hosted application as an API, and is encrypted with TLS which allows access only to the third party.



Correct Answer: B

Google encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted. https://cloud.google.com/docs/security/encryption-in-transit#cio-level_summary

QUESTION 3

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.

How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Correct Answer: D

There is mention about simulating in Web Security Scanner. "Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions." <https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings#xss> Reference: <https://cloud.google.com/security-scanner/docs/remediate-findings>

QUESTION 4

Your team wants to limit users with administrative privileges at the organization level. Which two roles should your team restrict? (Choose two.)

- A. Organization Administrator
- B. Super Admin
- C. GKE Cluster Admin
- D. Compute Admin
- E. Organization Role Viewer

Correct Answer: AB

Reference: <https://cloud.google.com/resource-manager/docs/creating-managing-organization>



QUESTION 5

Users are reporting an outage on your public-facing application that is hosted on Compute Engine. You suspect that a recent change to your firewall rules is responsible. You need to test whether your firewall rules are working properly. What should you do?

- A. Enable Firewall Rules Logging on the latest rules that were changed. Use Logs Explorer to analyze whether the rules are working correctly.
- B. Connect to a bastion host in your VPC. Use a network traffic analyzer to determine at which point your requests are being blocked.
- C. In a pre-production environment, disable all firewall rules individually to determine which one is blocking user traffic.
- D. Enable VPC Flow Logs in your VPC. Use Logs Explorer to analyze whether the rules are working correctly.

Correct Answer: A

<https://cloud.google.com/vpc/docs/using-flow-logs> <https://cloud.google.com/vpc/docs/firewall-rules-logging>

[Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps](#)

[PROFESSIONAL-CLOUD-SECURITY-ENGINEER Practice Test](#)

[PROFESSIONAL-CLOUD-SECURITY-ENGINEER Study Guide](#)