



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.pass4itsure.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



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



**QUESTION 1**

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.

What should you do?

- A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.
- B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.
- C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.
- D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: B

<https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk>

QUESTION 2

An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.

Which Cloud Identity password guidelines can the organization use to inform their new requirements?

- A. Set the minimum length for passwords to be 8 characters.
- B. Set the minimum length for passwords to be 10 characters.
- C. Set the minimum length for passwords to be 12 characters.
- D. Set the minimum length for passwords to be 6 characters.

Correct Answer: A

Default password length is 8 characters.

<https://support.google.com/cloudidentity/answer/33319?hl=en>

<https://support.google.com/cloudidentity/answer/139399?hl=en#:~:text=It%20can%20be%20between%208,decide%20to%20change%20their%20password.>

QUESTION 3

You have a highly sensitive BigQuery workload that contains personally identifiable information (PII) that you want to



ensure is not accessible from the internet. To prevent data exfiltration only requests from authorized IP addresses are allowed to query your BigQuery tables.

What should you do?

- A. Use service perimeter and create an access level based on the authorized source IP address as the condition.
- B. Use Google Cloud Armor security policies defining an allowlist of authorized IP addresses at the global HTTPS load balancer.
- C. Use the Restrict allowed Google Cloud APIs and services organization policy constraint along with Cloud Data Loss Prevention (DLP).
- D. Use the Restrict Resource service usage organization policy constraint along with Cloud Data Loss Prevention (DLP).

Correct Answer: A

QUESTION 4

You are migrating an application into the cloud. The application will need to read data from a Cloud Storage bucket. Due to local regulatory requirements, you need to hold the key material used for encryption fully under your control and you require a valid rationale for accessing the key material.

What should you do?

- A. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys. Configure an IAM deny policy for unauthorized groups.
- B. Generate a key in your on-premises environment to encrypt the data before you upload the data to the Cloud Storage bucket. Upload the key to the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and have the external key system reject unauthorized accesses.
- C. Encrypt the data in the Cloud Storage bucket by using Customer Managed Encryption Keys backed by a Cloud Hardware Security Module (HSM). Enable data access logs.
- D. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises. Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.

Correct Answer: D

The correct answer is D. Generate a key in your on-premises environment and store it in a Hardware Security Module (HSM) that is managed on-premises. Use this key as an external key in the Cloud Key Management Service (KMS). Activate Key Access Justifications (KAJ) and set the external key system to reject unauthorized accesses.

This approach allows you to maintain full control over the key material used for encryption, as the key is generated and stored in an on-premises HSM. By using this key as an external key in Cloud KMS, you can leverage Google Cloud's key management capabilities while still maintaining control over the key material. Activating Key Access Justifications provides a valid rationale for accessing the key material, as it allows you to monitor and justify each attempt to use the key.

QUESTION 5



A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.

Which two steps should the company take to meet these requirements? (Choose two.)

- A. Create a project with multiple VPC networks for each environment.
- B. Create a folder for each development and production environment.
- C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
- D. Create an Organizational Policy constraint for each folder environment.
- E. Create projects for each environment, and grant IAM rights to each engineering user.

Correct Answer: BC

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

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

[PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam Questions](#)