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

Professional Cloud Security Engineer

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

QUESTION 1

You are consulting with a client that requires end-to-end encryption of application data (including data in transit, data in use, and data at rest) within Google Cloud. Which options should you utilize to accomplish this? (Choose two.)

A. External Key Manager

B. Customer-supplied encryption keys

C. Hardware Security Module

D. Confidential Computing and Istio

E. Client-side encryption

Correct Answer: DE

Google Cloud customers with additional requirements for encryption of data over WAN can choose to implement further protections for data as it moves from a user to an application, or virtual machine to virtual machine. These protections include IPSec tunnels, Gmail S/MIME, managed SSL certificates, and Istio.
https://cloud.google.com/docs/security/encryption-in-transit

QUESTION 2

Your company\\'s users access data in a BigQuery table. You want to ensure they can only access the data during working hours.

What should you do?

A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.

B. Run a gsutil script that assigns a BigQuery Data Viewer role, and remove it only during the specified working hours.

C. Assign a BigQuery Data Viewer role to a service account that adds and removes the users daily during the specified working hours.

D. Configure Cloud Scheduler so that it triggers a Cloud Functions instance that modifies the organizational policy constraint for BigQuery during the specified working hours.

Correct Answer: A

The correct answer is A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.

IAM conditions in Google Cloud can be used to fine-tune access control according to attributes like time, date, and IP address. In this case, you can create an IAM condition that allows access only during working hours. This condition can be attached to the BigQuery Data Viewer role, ensuring that users can only access the data in the BigQuery table during the specified times.

QUESTION 3

An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier.

Which Cloud Data Loss Prevention API technique should you use to accomplish this?

A. Cryptographic hashing

B. Redaction

C. Format-preserving encryption

D. Generalization

Correct Answer: C

QUESTION 4

You are responsible for protecting highly sensitive data in BigQuery. Your operations teams need access to this data, but given privacy regulations, you want to ensure that they cannot read the sensitive fields such as email addresses and first names. These specific sensitive fields should only be available on a need-to-know basis to the HR team. What should you do?

A. Perform data masking with the DLP API and store that data in BigQuery for later use.

B. Perform data redaction with the DLP API and store that data in BigQuery for later use.

C. Perform data inspection with the DLP API and store that data in BigQuery for later use.

D. Perform tokenization for Pseudonymization with the DLP API and store that data in BigQuery for later use.

Correct Answer: D

Pseudonymization is a de-identification technique that replaces sensitive data values with cryptographically generated tokens. Pseudonymization is widely used in industries like finance and healthcare to help reduce the risk of data in use,

narrow compliance scope, and minimize the exposure of sensitive data to systems while preserving data utility and accuracy.

https://cloud.google.com/dlp/docs/pseudonymization

QUESTION 5

You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow thee application frontend to access the data in the application\\'s mysql instance on port 3306.

What should you do?

A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.

B. Configure an ingress firewall rule that allows communication from the frontend\\'s unique service account to the unique service account of the mysql Compute Engine VM on port 3306.

C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe-tag.

D. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

Correct Answer: B

https://cloud.google.com/sql/docs/mysql/sql-proxy#using-a-service-account