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

QUESTION 1

An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege.

Which option meets the requirement of your team?

A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance\\'s IP address and allows the application to read from the bucket without credentials.

B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.

C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.

D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Correct Answer: C

If the environment variable GOOGLE_APPLICATION_CREDENTIALS is set, ADC uses the service account key or configuration file that the variable points to. If the environment variable GOOGLE_APPLICATION_CREDENTIALS isn\\'t set, ADC uses the service account that is attached to the resource that is running your code. https://cloud.google.com/docs/authentication/ production#passing_the_path_to_the_service _account_key_in_code

QUESTION 2

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 3

Which two implied firewall rules are defined on a VPC network? (Choose two.)

A. A rule that allows all outbound connections

B. A rule that denies all inbound connections

C. A rule that blocks all inbound port 25 connections

D. A rule that blocks all outbound connections

E. A rule that allows all inbound port 80 connections

Correct Answer: AB

Implied IPv4 allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination Implied IPv4 deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them. https://cloud.google.com/vpc/docs/firewalls?hl=en#default_firewall_rules

QUESTION 4

You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards.

What should you do?

A. Use multi-factor authentication for admin access to the web application.

B. Use only applications certified compliant with PA-DSS.

C. Move the cardholder data environment into a separate GCP project.

D. Use VPN for all connections between your office and cloud environments.

Correct Answer: C

https://cloud.google.com/solutions/best-practices-vpc-design "Setting up your payment-processing environment" section in https://cloud.google.com/solutions/pci-dss- compliance-in-gcp.

QUESTION 5

You are developing a new application that uses exclusively Compute Engine VMs. Once a day, this application will execute five different batch jobs. Each of the batch jobs requires a dedicated set of permissions on Google Cloud resources outside of your application. You need to design a secure access concept for the batch jobs that adheres to the least-privilege principle.

What should you do?

A. 1. Create a general service account "g-sa" to orchestrate the batch jobs.

2.

Create one service account per batch job `b-sa-[1-5]\\'. Grant only the permissions required to run the individual batch jobs to the service accounts and generate service account keys for each of these service accounts.

3.

Store the service account keys in Secret Manager. Grant g-sa access to Secret Manager and run the batch jobs with

the permissions of b-sa-[1-5].

B. 1. Create a general service account "g-sa" to execute the batch jobs.

2.

Grant the permissions required to execute the batch jobs to g-sa.

3.

Execute the batch jobs with the permissions granted to g-sa.

C. 1. Create a workload identity pool and configure workload identity pool providers for each batch job.

2.

Assign the workload identity user role to each of the identities configured in the providers.

3.

Create one service account per batch job "b-sa-[1-5]", and grant only the permissions required to run the individual batch jobs to the service accounts.

4.

Generate credential configuration files for each of the providers. Use these files to execute the batch jobs with the permissions of b-sa-[1-5].

D. 1. Create a general service account "g-sa" to orchestrate the batch jobs.

2.

Create one service account per batch job "b-sa-[1-5]", and grant only the permissions required to run the individual batch jobs to the service accounts.

3.

Grant the Service Account Token Creator role to g-sa. Use g-sa to obtain short-lived access tokens for b-sa-[1-5] and to execute the batch jobs with the permissions of b-sa-[1-5].

Correct Answer: D

The correct answer is D. 1. Create a general service account "g-sa" to orchestrate the batch jobs. 2. Create one service account per batch job "b-sa-[1-5]", and grant only the permissions required to run the individual batch jobs to the service accounts. 3. Grant the Service Account Token Creator role to g-sa. Use g-sa to obtain short-lived access tokens for b-sa-[1-5] and to execute the batch jobs with the permissions of b-sa-[1-5].

This approach adheres to the principle of least privilege by ensuring that each batch job has only the permissions it needs to run. The general service account "g-sa" is used to orchestrate the batch jobs, and the Service Account Token Creator role allows it to obtain short-lived access tokens for the batch job service accounts "b-sa-[1-5]". This setup allows the batch jobs to be executed with the permissions of the respective service accounts.