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.geekcert.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

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Correct Answer: BC

https://cloud.google.com/vpc/docs/vpc-peering#key_properties

QUESTION 2

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.

What should you do?

A. Set up an ACL with OWNER permission to a scope of allUsers.

B. Set up an ACL with READER permission to a scope of allUsers.

C. Set up a default bucket ACL and manage access for users using IAM.

D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

Correct Answer: D

https://cloud.google.com/storage/docs/uniform-bucket-level-access#enabled
https://cloud.google.com/storage/docs/access-control/lists

QUESTION 3

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 4

A customer deploys an application to App Engine and needs to check for Open Web Application Security Project (OWASP) vulnerabilities.

Which service should be used to accomplish this?

A. Cloud Armor

B. Google Cloud Audit Logs

C. Cloud Security Scanner

D. Forseti Security

Correct Answer: C

Reference:

https://cloud.google.com/security-scanner/

https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview#detectors_and_compliance

Web Security Scanner supports categories in the OWASP Top Ten, a document that ranks and provides remediation guidance for the top 10 most critical web application security risks, as determined by the Open Web Application Security

Project (OWASP).

QUESTION 5

Your organization wants full control of the keys used to encrypt data at rest in their Google Cloud environments. Keys must be generated and stored outside of Google and integrate with many Google Services including BigQuery. What should you do?

A. Use customer-supplied encryption keys (CSEK) with keys generated on trusted external systems. Provide the raw CSEK as part of the API call.

B. Create a KMS key that is stored on a Google managed FIPS 140-2 level 3 Hardware Security Module (HSM).

Manage the Identity and Access Management (IAM) permissions settings, and set up the key rotation period.

C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

D. Create a Cloud Key Management Service (KMS) key with imported key material. Wrap the key for protection during import. Import the key generated on a trusted system in Cloud KMS.

Correct Answer: C

The correct answer is C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

Cloud EKM allows you to use encryption keys that are stored and managed in a third-party key management system deployed outside of Google\\'s infrastructure. This gives your organization full control over the keys used to encrypt data at rest in Google Cloud environments, including BigQuery.