Latest Version: 6.0

Question: 1

A cloud customer has an on-premises key management system and wants to generate, protect, rotate, and audit encryption keys with it.
How can the customer use Cloud Storage with their own encryption keys?

A. Declare usage of default encryption at rest in the audit report on compliance
B. Upload encryption keys to the same Cloud Storage bucket
C. Use Customer Managed Encryption Keys (CMEK)
D. Use Customer-Supplied Encryption Keys (CSEK)

Answer: D

Question: 2

A customer wants to grant access to their application running on Compute Engine to write only to a specific Cloud Storage bucket.
How should you grant access?

A. Create a service account for the application, and grant Cloud Storage Object Creator permissions to the project.
B. Create a service account for the application, and grant Cloud Storage Object Creator permissions at the bucket level.
C. Create a user account, authenticate with the application, and grant Google Storage Admin permissions at the bucket level.
D. Create a user account, authenticate with the application, and grant Google Storage Admin permissions at the project level.

Answer: B

Question: 3

Which encryption algorithm is used with Default Encryption in Cloud Storage?

A. AES-256
B. SHA512
C. MD5
D. 3DES

Question: 4

You have defined subnets in a VPC within Google Cloud Platform. You need multiple projects to create Compute Engine instances with IP addresses from these subnets. What should you do?

A. Configure Cloud VPN between the projects.
B. Set up VPC peering between all related projects.
C. Change the VPC subnets to enable private Google access.
D. Use Shared VPC to share the subnets with the other projects.

Answer: D

Question: 5

Your company is deploying their applications on Google Kubernetes Engine. You want to follow Google-recommended practices.
What should you do to ensure that the container images used for new deployments contain the latest security patches?

A. Use Google-managed base images for all containers.
B. Use Container Analysis to detect vulnerabilities in images.
C. Use an update script as part of every container image startup.
D. Use exclusively private images in Container Registry.

Answer: A

Question: 6

A Cloud Development team needs to use service accounts extensively in their local development. You need to provide the team with the keys for these service accounts. You want to follow Google-recommended practices.
What should you do?

A. Implement a daily key rotation process that generates a new key and commits it to the source code repository every day.
B. Implement a daily key rotation process, and provide developers with a Cloud Storage bucket from which they can download the new key every day.
C. Create a Google Group with all developers. Assign the group the IAM role of Service Account User, and have developers generate and download their own keys.

D. Create a Google Group with all developers. Assign the group the IAM role of Service Account Admin, and have developers generate and download their own keys.

Answer: B

Question: 7

An organization is working on their GDPR compliance strategy. It wants to ensure that controls are in place to ensure that customer PII is stored in Cloud Storage buckets without third-party exposure.
Which Google Cloud solution should the organization use to verify that PII is stored in the correct place without exposing PII internally?

A. Cloud Storage Bucket Lock
B. Cloud Data Loss Prevention API
C. VPC Service Controls
D. Cloud Security Scanner

Answer: B

Question: 8

You are responsible for implementing a payment processing environment that will use Kubernetes and need to apply proper security controls.
What should you do?

A. Implement and enforce two-factor authentication.
B. Activate a firewall to prevent all egress traffic.
C. Establish minimum password length requirements for all systems.
D. Require file integrity monitoring and antivirus scans of pods and nodes.

Answer: D

Question: 9

You want to protect the default VPC network from all inbound and outbound internet traffic. What action should you take?

A. Create a Deny All inbound internet firewall rule.
B. Create a Deny All outbound internet firewall rule.
C. Create a new subnet in the VPC network with private Google access enabled.
D. Create instances without external IP addresses only.

Question: 10

Your company is storing files on Cloud Storage. To comply with local regulations, you want to ensure that uploaded files cannot be deleted within the first 5 years.
It should not be possible to lower the retention period after it has been set. What should you do?

A. Apply a retention period of 5 years to the bucket, and lock the bucket.
B. Enable Temporary hold and apply a retention period of 5 years to the bucket.
C. Use Cloud IAM to ensure that nobody has an IAM role that has the permissions to delete files from Cloud Storage.
D. Create an object lifecycle rule using the Age condition and the Delete action. Set the Age condition to 5 years.

Answer: A