Latest Version: 6.0

Question: 1

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?
Response:

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: 2

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?
Response:

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

Answer: B

Question: 3

A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned. What should the customer do?
Response:

A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.

D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

Answer: C

Question: 4

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?
Response:

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

Question: 5

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?
Response:

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: 6

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

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.

Answer: B

Question: 7

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

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

Answer: A

Question: 8

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?
Response:

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: 9

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?
Response:

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: 10

A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.
Which two approaches can you take to meet the requirements?
(Choose two.)
Response:

A. Configure the project with Cloud VPN.
B. Configure the project with Shared VPC.
C. Configure the project with Cloud Interconnect.
D. Configure the project with VPC peering.
E. Configure all Compute Engine instances with Private Access.

Answer: AC