Free Questions for Professional-Cloud-Security-Engineer

Shared by Kane on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to enable VPC Service Controls and allow changes to perimeters in existing environments without preventing access to resources. Which VPC Service Controls mode should you use?

Options:

A- Cloud Run

B- Native

C- Enforced

D- Dry run

Answer:

D

Explanation:

In dry run mode, requests that violate the perimeter policy are not denied, only logged. Dry run mode is used to test perimeter configuration and to monitor usage of services without preventing access to resources. https://cloud.google.com/vpc-service-controls/docs/dry-run-mode

Question 2

Question Type: MultipleChoice

You need to implement an encryption-at-rest strategy that protects sensitive data and reduces key management complexity for non-sensitive dat

a. Your solution has the following requirements:

Schedule key rotation for sensitive data.

Control which region the encryption keys for sensitive data are stored in.

Minimize the latency to access encryption keys for both sensitive and non-sensitive data.

What should you do?

Options:

A- Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.

B- Encrypt non-sensitive data and sensitive data with Cloud Key Management Service.

C- Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.

D- Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Answer:

D

Explanation:

Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provideflexibility of controlling the key residency and rotation schedule, use google provided key for non-sensitive and encrypt sensitive data with Cloud Key Management Service

Question 3

Question Type: MultipleChoice

You want to make sure that your organization's Cloud Storage buckets cannot have data publicly available to the internet. You want to enforce this across all Cloud Storage buckets. What should you do?

Options:

A- Remove Owner roles from end users, and configure Cloud Data Loss Prevention.

B- Remove Owner roles from end users, and enforce domain restricted sharing in an organization policy.

C- Configure uniform bucket-level access, and enforce domain restricted sharing in an organization policy.

D- Remove *.setIamPolicy permissions from all roles, and enforce domain restricted sharing in an organization policy.

Answer:

C

Explanation:

- Uniform bucket-level access:
https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use

- Domain Restricted Sharing:
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#public_data_sharing

Question 4

Question Type: MultipleChoice

You run applications on Cloud Run. You already enabled container analysis for vulnerability scanning. However, you are concerned about the lack of control on the applications that are deployed. You must ensure that only trusted container images are deployed on Cloud Run.

What should you do?

Choose 2 answers

Options:

A- Enable Binary Authorization on the existing Kubernetes cluster.
B- Set the organization policy constraint constraints/run. allowedBinaryAuthorizationPolicie to the list of allowed Binary Authorization policy names.
C- Set the organization policy constraint constraints/compute.trustedimageProjects to the list of protects that contain the trusted container images.
D- Enable Binary Authorization on the existing Cloud Run service.
E- Use Cloud Run breakglass to deploy an image that meets the Binary Authorization policy by default.

Answer:

B, D

Question 5

Question Type: MultipleChoice

Your organization s customers must scan and upload the contract and their driver license into a web portal in Cloud Storage. You must remove all personally identifiable information (Pll) from files that are older than 12 months. Also you must archive the anonymized files for retention purposes.

What should you do?

Options:

A- Set a time to live (TTL) of 12 months for the files in the Cloud Storage bucket that removes PH and moves the files to the archive storage class.
B- Create a Cloud Data Loss Prevention (DLP) inspection job that de-identifies Pll in files created more than 12 months ago and archives them to another Cloud Storage bucket. Delete the original files.
C- Schedule a Cloud Key Management Service (KMS) rotation period of 12 months for the encryption keys of the Cloud Storage files containing Pll to de-identify them Delete the original keys.
D- Configure the Autoclass feature of the Cloud Storage bucket to de-identify Pll Archive the files that are older than 12 months Delete the original files.

Answer:

B

Question 6

Question Type: MultipleChoice

You need to use Cloud External Key Manager to create an encryption key to encrypt specific BigQuery data at rest in Google Cloud. Which steps should you do first?

Options:

A- 1. Create or use an existing key with a unique uniform resource identifier (URI) in your Google Cloud project.
2. Grant your Google Cloud project access to a supported external key management partner system.

B- 1. Create or use an existing key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS).
2. In Cloud KMS, grant your Google Cloud project access to use the key.
C- 1. Create or use an existing key with a unique uniform resource identifier (URI) in a supported external key management partner system.
2. In the external key management partner system, grant access for this key to use your Google Cloud project.
D- 1. Create an external key with a unique uniform resource identifier (URI) in Cloud Key Management Service (Cloud KMS).
2. In Cloud KMS, grant your Google Cloud project access to use the key.

Answer:

C

Explanation:

https://cloud.google.com/kms/docs/ekm#how_it_works

- First, you create or use an existing key in a supported external key management partner system. This key has a unique URI or key path.

- Next, you grant your Google Cloud project access to use the key, in the external key management partner system.

- In your Google Cloud project, you create a Cloud EKM key, using the URI or key path for the externally-managed key.

Question 7

Question Type: MultipleChoice

You are setting up a CI/CD pipeline to deploy containerized applications to your production clusters on Google Kubernetes Engine (GKE). You need to prevent containers with known vulnerabilities from being deployed. You have the following requirements for your solution:

Must be cloud-native

Must be cost-efficient

Minimize operational overhead

How should you accomplish this? (Choose two.)

Options:

A- Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.
B- Use a Cloud Function triggered by log events in Google Cloud's operations suite to automatically scan your container images in Container Registry.
C- Use a cron job on a Compute Engine instance to scan your existing repositories for known vulnerabilities and raise an alert if a non-compliant container image is found.
D- Deploy Jenkins on GKE and configure a CI/CD pipeline to deploy your containers to Container Registry. Add a step to validate your container images before deploying your container to the cluster.
E- In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster.

Answer:

A, E

Explanation:

https://cloud.google.com/container-analysis/docs/container-analysis

Container Analysis is a service that provides vulnerability scanning and metadata storage for containers. The scanning service performs vulnerability scans on images in Container Registry and Artifact Registry, then stores the resulting metadata and makes it available for consumption through an API.

https://cloud.google.com/binary-authorization/docs/attestations

After a container image is built, an attestation can be created to affirm that a required activity was performed on the image such as a regression test, vulnerability scan, or other test. The attestation is created by signing the image's unique digest.

During deployment, instead of repeating the activities, Binary Authorization verifies the attestations using an attestor. If all of the attestations for an image are verified, Binary Authorization allows the image to be deployed.

Question 8

Question Type: MultipleChoice

Your organization previously stored files in Cloud Storage by using Google Managed Encryption Keys (GMEK). but has recently updated the internal policy to require Customer Managed Encryption Keys (CMEK). You need to re-encrypt the files quickly and efficiently with minimal cost.

What should you do?

Options:

A- Encrypt the files locally, and then use gsutil to upload the files to a new bucket.

B- Copy the files to a new bucket with CMEK enabled in a secondary region

C- Reupload the files to the same Cloud Storage bucket specifying a key file by using gsutil.

D- Change the encryption type on the bucket to CMEK, and rewrite the objects

Answer:

D

Explanation:

Rewriting the objects in-place within the same bucket, specifying the new CMEK for encryption, allows you to re-encrypt the data without downloading and re-uploading it, thus minimizing costs and time.

https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys