



**Free Questions for Professional-Cloud-Security-Engineer by
certsinside**

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

Your organization uses Google Workspace Enterprise Edition for authentication. You are concerned about employees leaving their laptops unattended for extended periods of time after authenticating into Google Cloud. You must prevent malicious people from using an employee's unattended laptop to modify their environment.

What should you do?

Options:

- A- Create a policy that requires employees to not leave their sessions open for long durations.
- B- Review and disable unnecessary Google Cloud APIs.
- C- Require strong passwords and 2SV through a security token or Google authenticate.
- D- Set the session length timeout for Google Cloud services to a shorter duration.

Answer:

D

Question 2

Question Type: MultipleChoice

Your organization is transitioning to Google Cloud. You want to ensure that only trusted container images are deployed on Google Kubernetes Engine (GKE) clusters in a project. The containers must be deployed from a centrally managed Container Registry and signed by a trusted authority.

What should you do?

Choose 2 answers

Options:

- A-** Configure the Binary Authorization policy with respective attestations for the project.
- B-** Create a custom organization policy constraint to enforce Binary Authorization for Google Kubernetes Engine (GKE).
- C-** Enable Container Threat Detection in the Security Command Center (SCC) for the project.
- D-** Configure the trusted image organization policy constraint for the project.
- E-** Enable Pod Security standards and set them to Restricted.

Answer:

A, D

Question 3

Question Type: MultipleChoice

You are routing all your internet facing traffic from Google Cloud through your on-premises internet connection. You want to accomplish this goal securely and with the highest bandwidth possible.

What should you do?

Options:

- A-** Create an HA VPN connection to Google Cloud Replace the default 0 0 0 0/0 route.
- B-** Create a routing VM in Compute Engine Configure the default route with the VM as the next hop.
- C-** Configure Cloud Interconnect with HA VPN Replace the default 0 0 0 0/0 route to an on-premises destination.
- D-** Configure Cloud Interconnect and route traffic through an on-premises firewall.

Answer:

D

Question 4

Question Type: MultipleChoice

Your organization wants to be continuously evaluated against CIS Google Cloud Computing Foundations Benchmark v1 3 0 (CIS Google Cloud Foundation 1 3). Some of the controls are irrelevant to your organization and must be disregarded in evaluation. You need to create an automated system or process to ensure that only the relevant controls are evaluated.

What should you do?

Options:

- A-** Mark all security findings that are irrelevant with a tag and a value that indicates a security exception Select all marked findings and mute them on the console every time they appear Activate Security Command Center (SCC) Premium.
- B-** Activate Security Command Center (SCC) Premium Create a rule to mute the security findings in SCC so they are not evaluated.
- C-** Download all findings from Security Command Center (SCC) to a CSV file Mark the findings that are part of CIS Google Cloud Foundation 1 3 in the file Ignore the entries that are irrelevant and out of scope for the company.
- D-** Ask an external audit company to provide independent reports including needed CIS benchmarks. In the scope of the audit clarify that some of the controls are not needed and must be disregarded.

Answer:

B

Question 5

Question Type: MultipleChoice

You are a Cloud Identity administrator for your organization. In your Google Cloud environment groups are used to manage user permissions. Each application team has a dedicated group Your team is responsible for creating these groups and the application teams can manage the team members on their own through the Google Cloud console. You must ensure that the application teams can only add users from within your organization to their groups.

What should you do?

Options:

- A-** Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.
- B-** Set an Identity and Access Management (IAM) policy that includes a condition that restricts group membership to user principals that belong to your organization.
- C-** Define an Identity and Access Management (IAM) deny policy that denies the assignment of principals that are outside your organization to the groups in scope.
- D-** Export the Cloud Identity logs to BigQuery Configure an alert for external members added to groups Have the alert trigger a Cloud Function instance that removes the external members from the group.

Answer:

B

Question 6

Question Type: MultipleChoice

Your organization processes sensitive health information. You want to ensure that data is encrypted while in use by the virtual machines (VMs). You must create a policy that is enforced across the entire organization.

What should you do?

Options:

- A-** Implement an organization policy that ensures that all VM resources created across your organization use customer-managed encryption keys (CMEK) protection.
- B-** Implement an organization policy that ensures all VM resources created across your organization are Confidential VM instances.
- C-** Implement an organization policy that ensures that all VM resources created across your organization use Cloud External Key Manager (EKM) protection.
- D-** No action is necessary because Google encrypts data while it is in use by default.

Answer:

A

Question 7

Question Type: MultipleChoice

Your organization is rolling out a new continuous integration and delivery (CI/CD) process to deploy infrastructure and applications in Google Cloud. Many teams will use their own instances of the CI/CD workflow. It will run on Google Kubernetes Engine (GKE). The CI/CD pipelines must be designed to securely access Google Cloud APIs.

What should you do?

Options:

- A-** * 1 Create a dedicated service account for the CI/CD pipelines
- * 2 Run the deployment pipelines in a dedicated nodes pool in the GKE cluster
- * 3 Use the service account that you created as identity for the nodes in the pool to authenticate to the Google Cloud APIs

- B-** * 1 Create service accounts for each deployment pipeline
- * 2 Generate private keys for the service accounts
- * 3 Securely store the private keys as Kubernetes secrets accessible only by the pods that run the specific deployment pipeline

- C-** * 1 Create individual service accounts (or each deployment pipeline
- * 2 Add an identifier for the pipeline in the service account naming convention

- * 3 Ensure each pipeline runs on dedicated pods
- * 4 Use workload identity to map a deployment pipeline pod with a service account
- D-** * 1 Create two service accounts one for the infrastructure and one for the application deployment
- * 2 Use workload identities to let the pods run the two pipelines and authenticate with the service accounts
- * 3 Run the infrastructure and application pipelines in separate namespaces

Answer:

C

Question 8

Question Type: MultipleChoice

Your organization must comply with the regulation to keep instance logging data within Europe. Your workloads will be hosted in the Netherlands in region europe-west4 in a new project. You must configure Cloud Logging to keep your data in the country.

What should you do?

Options:

- A- Configure the organization policy constraint gcp.resourceLocations to europe-west4.
- B- Set the logging storage region to europe-west4 by using the gcloud CLI logging settings update.
- C- Create a new log bucket in europe-west4. and redirect the _Default bucket to the new bucket.
- D- Configure log sink to export all logs into a Cloud Storage bucket in europe-west4.

Answer:

C

**To Get Premium Files for Professional-Cloud-Security-Engineer
Visit**

<https://www.p2pexams.com/products/professional-cloud-security-engineer>

For More Free Questions Visit

<https://www.p2pexams.com/google/pdf/professional-cloud-security-engineer>

