# Free Questions for Professional-Cloud-Security-Engineer by certscare

## Shared by Hernandez on 15-04-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/ owner). The organization contains thousands of Google Cloud Projects Security Command Center Premium has surfaced multiple cpen_myscl_port findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.

What should you do?

## Options:

**A-** Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0 0 0 0/0 with priority 0.

**B-** Create a hierarchical firewall policy configured at the organization to deny all connections from 0 0 0 0/0.

**C-** Create a Google Cloud Armor security policy to deny traffic from 0 0 0 0/0.

**D-** Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

## Answer:

B

# Question 2

**Question Type:** MultipleChoice

Your company must follow industry specific regulations. Therefore, you need to enforce customer-managed encryption keys (CMEK) for all new Cloud Storage resources in the organization called org1.

What command should you execute?

## Options:

**A-** * organization policy: constraints/gcp.restrictStorageNonCraekServices
* binding at: orgl
* policy type: deny
* policy value: storage.gcogleapis.com

**B-** * organization policy: constraints/gcp.restrictHonCmekServices
* binding at: orgl
* policy type: deny
* policy value: storage.googleapis.com

**C-** * organization policy:constraints/gcp.restrictStorageNonCraekServices
* binding at: orgl
* policy type: allow
* policy value: all supported services

**D-** * organization policy: constramts/gcp.restrictNonCmekServices
* binding at: orgl
* policy type: allow
* policy value: storage.googleapis.com

### Answer:

A

# Question 3

**Question Type:** MultipleChoice

Your organization is using GitHub Actions as a continuous integration and delivery (Cl/CD) platform. You must enable access to Google Cloud resources from the Cl/CD pipelines in the most secure way.

What should you do?

### Options:

**A-** Create a service account key and add it to the GitHub pipeline configuration file.

**B-** Create a service account key and add it to the GitHub repository content.

**C-** Configure a Google Kubernetes Engine cluster that uses Workload Identity to supply credentials to GitHub.

**D-** Configure workload identity federation to use GitHub as an identity pool provider.

### Answer:

D

# Question 4

**Question Type:** MultipleChoice

Your company is moving to Google Cloud. You plan to sync your users first by using Google Cloud Directory Sync (GCDS). Some employees have already created Google Cloud accounts by using their company email addresses that were created outside of GCDS. You must create your users on Cloud Identity.

What should you do?

### Options:

**A-** Configure GCDS and use GCDS search rules lo sync these users.

**B-** Use the transfer tool to migrate unmanaged users.

**C-** Write a custom script to identify existing Google Cloud users and call the Admin SDK Directory API to transfer their account.

**D-** Configure GCDS and use GCDS exclusion rules to ensure users are not suspended.

### Answer:

D

## Question 5

**Question Type:** **MultipleChoice**

Your company requires the security and network engineering teams to identify all network anomalies and be able to capture payloads within VPCs. Which method should you use?

### Options:

**A-** Define an organization policy constraint.

**B-** Configure packet mirroring policies.

**C-** Enable VPC Flow Logs on the subnet.

**D-** Monitor and analyze Cloud Audit Logs.

### Answer:

B

### Explanation:

https://cloud.google.com/vpc/docs/packet-mirroring

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

## Question 6

**Question Type:** **MultipleChoice**

You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your VPCs based on network logs. However, you want to explore your environment using network payloads and headers. Which Google Cloud product should you use?

## Options:

**A-** Cloud IDS

**B-** VPC Service Controls logs

**C-** VPC Flow Logs

**D-** Google Cloud Armor

**E-** Packet Mirroring

## Answer:

E

## Explanation:

https://cloud.google.com/vpc/docs/packet-mirroring

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.