# Online Google Professional-Cloud-Security-Engineer Version - Professional-Cloud-Security-Engineer Training Kit


BONUS!!! Download part of ActualVCE Professional-Cloud-Security-Engineer dumps for free: https://drive.google.com/open?id=1NAJPgRZlVSpdp5rk_sAazwZK8dm9YH8I

With the rapid market development, there are more and more companies and websites to sell Professional-Cloud-Security-Engineer guide question for learners to help them prepare for exam, but many study materials have very low quality and low pass rate, this has resulting in many candidates failed the exam, some of them even loss confidence of their exam. As for the safe environment and effective product, why don't you have a try for our Professional-Cloud-Security-Engineer Test Question, never let you down! Before your purchase, there is a free demo for you. You can know the quality of our Professional-Cloud-Security-Engineer guide question earlier.

Google Professional-Cloud-Security-Engineer (Google Cloud Certified - Professional Cloud Security Engineer) Certification Exam is designed to test the knowledge, skills, and expertise of candidates in securing cloud environments using Google Cloud Platform (GCP) technologies. Google Cloud Certified - Professional Cloud Security Engineer Exam certification exam is aimed at cloud security professionals who have the necessary skills to design, implement, and manage security solutions using GCP. Google Cloud Certified - Professional Cloud Security Engineer Exam certification is an industry-recognized credential that validates the candidate's ability to handle security challenges in cloud environments.

**>> Online Google Professional-Cloud-Security-Engineer Version <<**

## Professional-Cloud-Security-Engineer Study Questions are Most Powerful Weapon to Help You Pass the Google Cloud Certified - Professional Cloud Security Engineer Exam exam - ActualVCE

If you are determined to enter into Google company or some companies who are the product agents of Google, a good certification will help you obtain more jobs and high positions. ActualVCE release high passing-rate Professional-Cloud-Security-Engineer exam simulations to help you obtain certification in a short time. If you obtain a certification you will get a higher job or satisfying benefits with our Professional-Cloud-Security-Engineer Exam Simulations. Every day there is someone choosing our exam materials. If this is what you want, why are you still hesitating?

Google Professional-Cloud-Security-Engineer Exam is a certification that validates the expertise of individuals in securing applications, data, and infrastructure on the Google Cloud Platform. Professional-Cloud-Security-Engineer exam is designed for professionals who want to demonstrate their knowledge of security controls and techniques used to protect cloud resources. Google Cloud Certified - Professional Cloud Security Engineer Exam certification is highly valued in the IT industry and is a testament to an individual's skills in cloud security.

To pass the exam, individuals must demonstrate a deep understanding of Google Cloud security tools and techniques, including identity and access management, network security, data encryption, and compliance. They must also be able to design and implement security solutions that are tailored to specific organizational needs, and be able to monitor and troubleshoot these solutions to ensure ongoing security and compliance.

## Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q252-Q257):

**NEW QUESTION # 252**
Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.
What should you do?

- A. Use customer-supplied encryption keys to manage the key encryption key (KEK).
- B. Use the Cloud Key Management Service to manage the data encryption key (DEK).
- C. Use the Cloud Key Management Service to manage the key encryption key (KEK).
- D. Use customer-supplied encryption keys to manage the data encryption key (DEK).

**Answer: C**

Explanation:
Explanation
This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.
https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption
https://codelabs.developers.google.com/codelabs/encrypt-and-decrypt-data-with-cloud-kms#0

**NEW QUESTION # 253**
Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester.
Which two tasks should your team perform to handle this request? (Choose two.)

- A. Grant the Project Editor role at the organizational level to a designated group of users.
- B. Add a designated group of users to the Project Creator role at the organizational level.
- C. Grant the billing account creator role to the designated DevOps team.
- D. Remove all users from the Project Creator role at the organizational level.
- E. Create an Organization Policy constraint, and apply it at the organizational level.

**Answer: B,E**

**NEW QUESTION # 254**
You work for an ecommerce company that stores sensitive customer data across multiple Google Cloud regions. The development team has built a new 3-tier application to process orders and must integrate the application into the production environment. You must design the network architecture to ensure strong security boundaries and isolation for the new application, facilitate secure remote maintenance by authorized third-party vendors, and follow the principle of least privilege. What should you do?

- A. Create separate VPC networks for each tier. Use VPC peering between application tiers and other required VPCs. Provide vendors with SSH keys and root access only to the instances within the VPC for maintenance purposes.
- B. Create a single VPC network and create different subnets for each tier. Create a new Google project specifically for the third-party vendors. Grant the vendors ownership of that project and the ability to modify the Shared VPC configuration.
- C. Create a single VPC network and create different subnets for each tier. Create a new Google project specifically for the

third-party vendors and grant the network admin role to the vendors. Deploy a VPN appliance and rely on the vendors' configurations to secure third-party access.

- D. Create separate VPC networks for each tier. Use VPC peering between application tiers and other required VPCs. Enable Identity-Aware Proxy (IAP) for remote access to management resources, limiting access to authorized vendors.

**Answer: D**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
This question combines three security requirements: strong isolation (segmentation), secure remote access, and least privilege.
Strong Isolation: Creating separate VPC networks for each tier (C) provides the strongest network isolation /segmentation, limiting the blast radius compared to a single VPC with subnets (B, D). VPC peering is the standard way to allow controlled communication between these separate VPCs.
Extract: "Isolate sensitive data in its own VPC network." (Source 2.5) Segmentation via separate VPCs is a standard best practice for isolating sensitive workloads.
Secure Remote Access and Least Privilege: Identity-Aware Proxy (IAP) is the recommended Google Cloud service to provide secure remote access to virtual machine instances without requiring a public IP or VPN, which aligns with the zero-trust principle of explicit validation and least privilege by verifying user identity and context. Granting SSH keys and root access (A) or the Network Admin role (B) or Project Ownership (D) violates the principle of least privilege.
Extract: "Access control: Enforce access controls based on user identity and context by using solutions like...
Identity-Aware Proxy (IAP). By doing this, you shift security from the network perimeter to individual users and devices. This approach enables granular access control and reduces the attack surface." (Source 2.2) Extract: "BeyondCorp uses Google Cloud tools, such as... and Identity-Aware Proxy, to push the perimeter from the network to individual devices and users." (Source 2.3)
Extract: "IAP protects GCP-hosted applications by verifying user identity and context before granting access... When you grant a user access to an application or resource by IAP, they're subject to the fine-grained access controls implemented by the product in use without requiring a VPN." (Source 2.3) Option C is the only one that satisfies all three requirements by using separate VPCs (strong isolation) and IAP (secure remote access with least privilege).

**NEW QUESTION # 255**
A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE).
How should the DevOps team accomplish this?

- A. Use Puppet or Chef to push out the patch to the running container.
- B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
- C. Update the application code or apply a patch, build a new image, and redeploy it.
- D. Configure containers to automatically upgrade when the base image is available in Container Registry.

**Answer: C**

Explanation:
When a vulnerability patch is released for a running container in Google Kubernetes Engine (GKE), the recommended approach is to update the application code or apply the patch directly to the codebase. Then, a new container image should be built incorporating these changes. After building the new image, it should be deployed to replace the running containers. This method ensures that the containers run the updated, secure code.
Steps:
Update Application Code: Modify the application code or dependencies to incorporate the vulnerability patch.
Build New Image: Use a tool like Docker to build a new container image with the updated code.
Push New Image: Push the new container image to the Container Registry.
Update Deployments: Update the Kubernetes deployment to use the new image. This can be done by modifying the image tag in the deployment YAML file.
Redeploy Containers: Apply the updated deployment configuration using kubectl apply -f <deployment-file>.
yaml, which will redeploy the containers with the new image.
References:
Google Cloud: Container security
Kubernetes: Updating an application

**NEW QUESTION # 256**
A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use

customer-supplied encryption keys (CSEK).
How should the team complete this task?

- A. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.
- B. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.
- C. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.
- D. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.

**Answer: A**

Explanation:
https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#gsutil

**NEW QUESTION # 257**
.....

learn.csisafety.com.au, jobs.electronicsweekly.com, scalar.usc.edu, zenwriting.net, Disposable vapes

BONUS!!! Download part of ActualVCE Professional-Cloud-Security-Engineer dumps for free: https://drive.google.com/open?id=1NAJPgRZlVSpdp5rk_sAazwZK8dm9YH8I