

# Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

<https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/>



#### NEW QUESTION 1

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.

What should you do?

- A. Set up an ACL with OWNER permission to a scope of allUsers.
- B. Set up an ACL with READER permission to a scope of allUsers.
- C. Set up a default bucket ACL and manage access for users using IAM.
- D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

**Answer:** A

#### NEW QUESTION 2

Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services. Which two settings must remain disabled to meet these requirements? (Choose two.)

- A. Public IP
- B. IP Forwarding
- C. Private Google Access
- D. Static routes
- E. IAM Network User Role

**Answer:** CD

#### NEW QUESTION 3

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised. What should you do?

- A. Enforce 2-factor authentication in GSuite for all users.
- B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
- C. Provision user passwords using GSuite Password Sync.
- D. Configure Cloud VPN between your private network and GCP.

**Answer:** D

#### NEW QUESTION 4

A customer has an analytics workload running on Compute Engine that should have limited internet access. Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.

The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

- A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
- B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
- C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.
- D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

**Answer:** C

#### NEW QUESTION 5

Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules, subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection. The networking resources will need to be controlled by the network security team.

Which type of networking design should your team use to meet these requirements?

- A. Shared VPC Network with a host project and service projects
- B. Grant Compute Admin role to the networking team for each engineering project
- C. VPC peering between all engineering projects using a hub and spoke model
- D. Cloud VPN Gateway between all engineering projects using a hub and spoke model

**Answer:** A

#### NEW QUESTION 6

Your company is storing sensitive data in Cloud Storage. You want a key generated on-premises to be used in the encryption process. What should you do?

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

**Answer:** A

#### NEW QUESTION 7

You will create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices. What should you do?

- A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
- B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
- C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
- D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

**Answer:** A

#### NEW QUESTION 8

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.)

- 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:** DE

#### NEW QUESTION 9

In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized. Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

- A. App Engine
- B. Cloud Functions
- C. Compute Engine
- D. Google Kubernetes Engine
- E. Cloud Storage

**Answer:** AC

#### NEW QUESTION 10

A customer wants to deploy a large number of 3-tier web applications on Compute Engine.

How should the customer ensure authenticated network separation between the different tiers of the application?

- A. Run each tier in its own Project, and segregate using Project labels.
- B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
- C. Run each tier in its own subnet, and use subnet-based firewall rules.
- D. Run each tier with its own VM tags, and use tag-based firewall rules.

**Answer:** C

#### NEW QUESTION 10

A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned.

What should the customer do?

- 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

#### NEW QUESTION 13

When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

- A. Ensure that the app does not run as PID 1.
- B. Package a single app as a container.
- C. Remove any unnecessary tools not needed by the app.
- D. Use public container images as a base image for the app.
- E. Use many container image layers to hide sensitive information.

**Answer:** BC

#### NEW QUESTION 16

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:** B

#### NEW QUESTION 18

You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards. What should you do?

- A. Use multi-factor authentication for admin access to the web application.
- B. Use only applications certified compliant with PA-DSS.
- C. Move the cardholder data environment into a separate GCP project.
- D. Use VPN for all connections between your office and cloud environments.

**Answer: D**

#### NEW QUESTION 22

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment. How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

**Answer: D**

#### NEW QUESTION 24

A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online. What should they do?

- A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
- B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.
- C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
- D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

**Answer: A**

#### NEW QUESTION 28

A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means. Which connectivity option should be implemented?

- A. VPC peering
- B. Cloud VPN
- C. Cloud Interconnect
- D. Shared VPC

**Answer: B**

#### NEW QUESTION 30

A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite. How should you best advise the Systems Engineer to proceed with the least disruption?

- A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
- B. Register a new domain name, and use that for the new Cloud Identity domain.
- C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.
- D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

**Answer: C**

#### NEW QUESTION 33

Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account. What should you do?

- A. \* 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.\* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.\* 3. Click Hide Matching Entries
- B. \* 4. Make sure the resulting list is empty.
- C. \* 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.\* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.\* 3. Click Show Matching Entries
- D. \* 4. Make sure the resulting list is empty.
- E. \* 1. In BigQuery, select the related dataset.\* 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
- F. \* 1. Go to the IAM section on the project.\* 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

**Answer: C**



#### NEW QUESTION 35

A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location. How should the company accomplish this?

- A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.
- B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location.
- C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.
- D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

**Answer: D**

#### NEW QUESTION 38

A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places. Which Storage solution are they allowed to use?

- A. Cloud Bigtable
- B. Cloud BigQuery
- C. Compute Engine SSD Disk
- D. Compute Engine Persistent Disk

**Answer: B**

#### NEW QUESTION 41

You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow the application frontend to access the data in the application's mysql instance on port 3306. What should you do?

- A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.
- B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306.
- C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B.
- D. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged with fe-tag.
- E. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B.
- F. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

**Answer: B**

#### NEW QUESTION 46

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.

Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses. Which solution should your team implement to meet these requirements?

- A. Cloud Armor
- B. Network Load Balancing
- C. SSL Proxy Load Balancing
- D. NAT Gateway

**Answer: A**

#### NEW QUESTION 49

Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.

What should your team do to meet these requirements?

- A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
- B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
- C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
- D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

**Answer: B**

#### NEW QUESTION 54

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.

What should you do to meet these requirements?

- A. Create a Folder per department under the Organization.
- B. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
- C. Create a Folder per department under the Organization.
- D. For each department's Folder, assign the Project Browser role to the Google Group related to that department.

- E. Create a Project per department under the Organizatio
- F. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
- G. Create a Project per department under the Organizatio
- H. For each department's Project, assign the Project Browser role to the Google Group related to that department.

**Answer:** C

#### NEW QUESTION 57

An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege. Which option meets the requirement of your team?

- A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
- B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
- C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.
- D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

**Answer:** C

#### NEW QUESTION 61

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys. What should you do?

- A. Create a single KeyRing for all persistent disks and all Keys in this KeyRin
- B. Manage the IAM permissions at the Key level.
- C. Create a single KeyRing for all persistent disks and all Keys in this KeyRin
- D. Manage the IAM permissions at the KeyRing level.
- E. Create a KeyRing per persistent disk, with each KeyRing containing a single Ke
- F. Manage the IAM permissions at the Key level.
- G. Create a KeyRing per persistent disk, with each KeyRing containing a single Ke
- H. Manage the IAM permissions at the KeyRing level.

**Answer:** C

#### NEW QUESTION 63

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

**Answer:** BD

#### NEW QUESTION 68

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Security-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Security-Engineer Product From:

<https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/>

## Money Back Guarantee

### Professional-Cloud-Security-Engineer Practice Exam Features:

- \* Professional-Cloud-Security-Engineer Questions and Answers Updated Frequently
- \* Professional-Cloud-Security-Engineer Practice Questions Verified by Expert Senior Certified Staff
- \* Professional-Cloud-Security-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* Professional-Cloud-Security-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year