



Google

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container.
What should they do?

- A. Use Cloud Build to build the container images.
- B. Build small containers using small base images.
- C. Delete non-used versions from Container Registry.
- D. Use a Continuous Delivery tool to deploy the application.

Answer: D

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

Which two implied firewall rules are defined on a VPC network? (Choose two.)

- A. A rule that allows all outbound connections
- B. A rule that denies all inbound connections
- C. A rule that blocks all inbound port 25 connections
- D. A rule that blocks all outbound connections
- E. A rule that allows all inbound port 80 connections

Answer: AB

NEW QUESTION 4

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 5

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 6

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 7

Your team wants to limit users with administrative privileges at the organization level. Which two roles should your team restrict? (Choose two.)

- A. Organization Administrator
- B. Super Admin

- C. GKE Cluster Admin
- D. Compute Admin
- E. Organization Role Viewer

Answer: AB

NEW QUESTION 8

A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs. What should you do?

- A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold
- B. Enable notifications.
- C. Create an Alerting Policy in Stackdriver using the CPU usage metri
- D. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
- E. Log every execution of the script to Stackdriver Loggin
- F. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
- G. Log every execution of the script to Stackdriver Loggin
- H. Configure BigQuery as a log sink, and create aBigQuery scheduled query to count the number of executions in a specific timeframe.

Answer: C

NEW QUESTION 9

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 company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery. What should you do?

- A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
- B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
- C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
- D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Answer: D

NEW QUESTION 10

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 13

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet. Which two strategies should your team use to meet these requirements? (Choose two.)

- A. Configure Private Google Access on the Compute Engine subnet
- B. Avoid assigning public IP addresses to the Compute Engine cluster.
- C. Make sure that the Compute Engine cluster is running on a separate subnet.
- D. Turn off IP forwarding on the Compute Engine instances in the cluster.
- E. Configure a Cloud NAT gateway.

Answer: BE

NEW QUESTION 16

When working with agents in a support center via online chat, an organization's customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for review by internal or external analysts for customer service trend analysis. Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

- A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.
- B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.
- C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.
- D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Answer: D

Explanation:

Reference; <https://cloud.google.com/dlp/docs/deidentify-sensitive-data>

NEW QUESTION 18

An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters. Which Cloud Identity password guidelines can the organization use to inform their new requirements?

- A. Set the minimum length for passwords to be 8 characters.
- B. Set the minimum length for passwords to be 10 characters.
- C. Set the minimum length for passwords to be 12 characters.
- D. Set the minimum length for passwords to be 6 characters.

Answer: C

NEW QUESTION 21

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 26

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

- A. Central management of routes, firewalls, and VPNs for peered networks
- B. Non-transitive peered networks; where only directly peered networks can communicate
- C. Ability to peer networks that belong to different Google Cloud Platform organizations
- D. Firewall rules that can be created with a tag from one peered network to another peered network
- E. Ability to share specific subnets across peered networks

Answer: AD

NEW QUESTION 28

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network. How should your team design this network?

- A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.
- B. Create a different subnet for the frontend application and database to ensure network isolation.
- C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.
- D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Answer: A

NEW QUESTION 30

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet. How should this be accomplished?

- A. Create a firewall rule to block internet traffic from the VM.
- B. Provision a NAT Gateway to access the Cloud Storage API endpoint.
- C. Enable Private Google Access on the VPC.
- D. Mount a Cloud Storage bucket as a local filesystem on every VM.

Answer: B

NEW QUESTION 34

Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization. Which logging export strategy should you use to meet the requirements?

- A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM projec
- B. 2. Subscribe SIEM to the topic.
- C. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM projec
- D. 2. Process Cloud Storage objects in SIEM.

- E. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project
- F. 2. Subscribe SIEM to the topic.
- G. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project
- H. 2. Process Cloud Storage objects in SIEM.

Answer: B

NEW QUESTION 36

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 37

You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources. Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts. Which two actions should you take? (Choose two.)

- A. Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
- B. Use the Google Admin console to view which managed users are using a personal account for their recovery email.
- C. Add users to your managed Google account and force users to change the email addresses associated with their personal accounts.
- D. Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.
- E. Send an email to all of your employees and ask those users with corporate email addresses for personal Google accounts to delete the personal accounts immediately.

Answer: BE

NEW QUESTION 42

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack. Which solution should this customer use?

- A. VPC Flow Logs
- B. Cloud Armor
- C. DNS Security Extensions
- D. Cloud Identity-Aware Proxy

Answer: C

NEW QUESTION 47

As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name. Which cost reduction options should you recommend?

- A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
- B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
- C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
- D. Use FindingLimits and TimespanConfig to sample data and minimize transformation units.

Answer: C

NEW QUESTION 49

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

Answer: D

NEW QUESTION 50

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented. Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
- B. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect
- C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
- D. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN

Answer: B

NEW QUESTION 52

Your team wants to make sure Compute Engine instances running in your production project do not have public IP addresses. The frontend application Compute Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this requirement. How should your team meet these requirements?

- A. Enable Private Access on the VPC network in the production project.
- B. Remove the Editor role and grant the Compute Admin IAM role to the engineers.
- C. Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
- D. Set up a VPC network with two subnets: one with public IPs and one without public IPs.

Answer: C

NEW QUESTION 55

Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

- A. ISO 27001
- B. ISO 27002
- C. ISO 27017
- D. ISO 27018

Answer: C

Explanation:

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.

NEW QUESTION 56

An organization receives an increasing number of phishing emails. Which method should be used to protect employee credentials in this situation?

- A. Multifactor Authentication
- B. A strict password policy
- C. Captcha on login pages
- D. Encrypted emails

Answer: D

NEW QUESTION 59

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud. What solution would help meet the requirements?

- A. Ensure that firewall rules are in place to meet the required controls.
- B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
- C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
- D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

Answer: B

NEW QUESTION 62

A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing. How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

- A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
- B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
- C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
- D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Answer: D

NEW QUESTION 64

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 the Cloud Key Management Service to manage the data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage the 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 69

A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries. Where should you export the logs?

- A. BigQuery datasets
- B. Cloud Storage buckets
- C. StackDriver logging
- D. Cloud Pub/Sub topics

Answer: C

NEW QUESTION 72

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 75

A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published. Which Google Cloud Service should be used to achieve this?

- A. Cloud Key Management Service
- B. Cloud Data Loss Prevention API
- C. BigQuery
- D. Cloud Security Scanner

Answer: D

NEW QUESTION 80

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

Answer: C

NEW QUESTION 84

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on-premises for an indefinite time. The organization wants a scalable and cost-efficient solution. Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates
- B. Cloud Storage using a scheduled task and gsutil
- C. Compute Engine Virtual Machines using Persistent Disk
- D. Cloud Datastore using regularly scheduled batch upload jobs

Answer: A

NEW QUESTION 85

.....

Relate Links

100% Pass Your Professional-Cloud-Security-Engineer Exam with Exambible Prep Materials

<https://www.exambible.com/Professional-Cloud-Security-Engineer-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>